Integración de la inteligencia de amenazas con CTEM, enfoque proactivo de gestión continua de amenazas

Juan Camilo Ramírez González

Asesor

Christian Hernan Obando Ibarra

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2026

Dedicatoria

Dedico este trabajo a mi madre, Doris González, por su amor, paciencia y apoyo incondicional, que han sido fundamentales en mi formación académica y en la realización de este proyecto.

Agradecimientos

Agradezco al tutor, Christian Obando, por su revisión crítica y los valiosos comentarios que contribuyeron a mejorar la claridad y el rigor académico de este proyecto. Asimismo, expreso mi gratitud a mi madre, Doris González, por el apoyo moral y la motivación constante durante el desarrollo del proyecto, que me permitieron mantener el enfoque y la disciplina necesarios para culminarlo.

Resumen

La ciber inteligencia de amenazas (CTI) juega un papel clave en la ciberseguridad, permitiendo la recopilación proactiva de datos sobre amenazas. Esta información es fundamental para analizar el historial de ataques, mitigar riesgos y predecir futuros ataques, basándose en datos sobre amenazas pasadas y emergentes.

Gracias a la ciber inteligencia, los equipos de seguridad pueden tomar decisiones informadas y adelantarse a los ataques. Al integrar esta inteligencia, las organizaciones pueden priorizar esfuerzos y optimizar recursos para fortalecer su defensa frente a amenazas cibernéticas.

Las herramientas de ciberseguridad por sí solas son ineficaces sin datos actualizados sobre amenazas. La ciber inteligencia de amenazas proporciona información crítica, como indicadores de compromiso (IoC) y las Tácticas, Técnicas y Procedimientos (TTPs) empleadas por los ciberdelincuentes. Sin esta inteligencia, las defensas pueden ser fácilmente eludidas.

Por otro lado, Gestión Continua de la Exposición a Amenazas (CTEM) es un enfoque proactivo y cíclico de gestión continua de vulnerabilidades que permite realizar la priorización de las amenazas, permite realizar la priorización mediante distintos factores como la urgencia, seguridad, disponibilidad de controles de compensación, tolerancia para la superficie de ataque residual, nivel de riesgo que enfrenta la organización, entre otros factores según Gartner. Además, es un enfoque que permite confirmar la probabilidad real de explotación de una vulnerabilidad y hasta donde podría llegar un atacante.

Palabras clave: CTI, SOC, ciberseguridad, CTEM.

Abstract

Cyber threat intelligence plays a key role in cybersecurity, enabling proactive collection of threat data. This information is essential for analyzing attack history, mitigating risks, and predicting future attacks based on data about past and emerging threats.

Thanks to cyber intelligence, security teams can make informed decisions and stay ahead of attacks. By integrating this intelligence, organizations can prioritize efforts and optimize resources to strengthen their defense against cyber threats.

Cybersecurity tools alone are ineffective without up-to-date threat data. Cyber threat intelligence (CTI) provides critical information, such as IoCs and tactics, techniques, and procedures (TTPs) employed by cybercriminals. Without this intelligence, defenses can be easily circumvented.

On the other hand, Continuous Threat Exposure Management CTEM is a proactive and cyclical approach to continuous vulnerability management that allows threats to be prioritized based on various factors such as urgency, security, availability of compensating controls, tolerance for residual attack surface, level of risk faced by the organization, among other factors according to Gartner. In addition, it is an approach that allows the actual probability of exploitation of a vulnerability to be confirmed, as well as how far an attacker could go.

Keywords: CTI, SOC, cybersecurity, CTEM.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

Dada la rápida evolución de las amenazas en ciberseguridad, las organizaciones enfrentan un panorama cada vez más complejo. Los ataques, incluyendo ransomware, phishing, Denegación de Servicio Distribuida (DDoS), entre otros, se vuelven más sofisticados, lo que exige estrategias de defensa proactivas basadas en inteligencia de amenazas.

La inteligencia de amenazas es fundamental en la ciberseguridad actual, ya que permite obtener contexto sobre amenazas pasadas y emergentes, facilitando la anticipación de ataques mediante su análisis. Al combinarse con CTEM, se logra un enfoque proactivo y cíclico, que prioriza la gestión de riesgos considerando el contexto del negocio de cada organización.

Esta monografía tiene como objetivo presentar un modelo que integre la inteligencia de amenazas con CTEM. Se desarrollará un plan de gestión que permita recolectar, analizar y compartir datos de manera efectiva, con el fin de mejorar la identificación de amenazas, predecir ataques y optimizar la gestión de riesgos de forma proactiva.

Planteamiento del Problema

Las ciberamenazas se han convertido en una de las preocupaciones más grandes para las organizaciones de todos los sectores a nivel global, incluyendo el financiero, industrial y gubernamental. La rápida evolución de estas amenazas dificulta su detección temprana y hace que las organizaciones sean cada vez más vulnerables a ataques sofisticados.

Algunas de las principales tendencias actuales en ciberamenazas incluyen:

Ransomware: El ransomware sigue siendo una de las amenazas más prevalentes y destructivas. Los ciberdelincuentes emplean técnicas avanzadas, como cifrado de datos y extorsión doble, lo que significa que además de bloquear el acceso a los datos, también amenazan con publicarlos o venderlos si no se paga el rescate (Kosinski, 2025).

Ataques a la cadena de suministro: Los atacantes están cada vez más enfocados en las vulnerabilidades en la cadena de suministro. En estos ataques se busca la infiltración en los sistemas de empresas al comprometer a sus proveedores.

Phishing y fraude: Los ataques de phishing han evolucionado significativamente, actualmente se utilizan técnicas de ingeniería social más avanzadas, como correos electrónicos y sitios web falsos que imitan perfectamente los de empresas legítimas. Según datos de Microsoft, los ataques de phishing aumentaron un 400% desde 2022, con estafas diarias pasando de 7,000 en 2023 a 100,000 en 2024. Estos ataques son cada vez más difíciles de detectar debido a la sofisticación de las tácticas utilizadas (Microsoft, 2024).

Además, los actores maliciosos están comenzando a utilizar inteligencia artificial generativa para mejorar la eficiencia de sus ataques. Esta tecnología permite la creación de código malicioso más adaptativo y difícil de detectar, así como la automatización de campañas de phishing y otras tácticas.

De acuerdo con los expertos en seguridad de Microsoft, la cooperación global es crucial para enfrentar el aumento de las ciberamenazas. En este contexto, las organizaciones deben adoptar enfoques colaborativos, compartir información sobre amenazas y fortalecer sus defensas colectivas para proteger infraestructuras críticas y datos sensibles (Microsoft, 2024).

Solo en Colombia, en el año 2024 se registraron 36.000 millones de intentos de ataques, según Fortinet, compañía de ciberseguridad reconocidas a nivel global por sus informes sobre tendencias y amenazas digitales (Junco, 2025).

Por otro lado, muchos de los ataques inician con la explotación de una vulnerabilidad, muchos de las organizaciones actualmente no saben cómo priorizar correctamente la gestión de las vulnerabilidades más allá de su severidad técnica asignada por el puntaje Common Vulnerability Scoring System (CVSS), lo que representa una de las mayores problemáticas actualmente en el campo de la ciberseguridad.

¿Cómo puede el diseño de un plan de inteligencia de amenazas, utilizando la metodología CTEM y herramientas de análisis de vulnerabilidades e inteligencia de amenazas, fortalecer la postura de seguridad de una organización?

Justificación

La inteligencia de amenazas es un componente clave en la protección de los activos tecnológicos de las organizaciones, especialmente en el contexto del panorama cibernético que es cada vez más complejo y dinámico (ENISA, 2024; IBM, 2024). Las ciber amenazas evolucionan constantemente, con atacantes que emplean tácticas sofisticadas para vulnerar sistemas y comprometer datos sensibles (IBM, 2024). La inteligencia de amenazas permite a las organizaciones anticiparse a los ataques al proporcionar información crítica sobre las amenazas emergentes. Esta inteligencia facilita la correlación de eventos históricos y actuales relacionados con grupos de Amenazas Persistentes Avanzadas (APT), variantes de malware, phishing, y otros actores maliciosos, lo que ayuda a prevenir incidentes cibernéticos y fortalecer las defensas (ENISA, 2024).

La capacidad para detectar y mitigar amenazas es clave, por lo que la inteligencia de amenazas juega un papel esencial en estas tareas (IBM, 2024). Mediante la identificación de IoC e indicadores de ataque (IoA), los equipos de seguridad pueden mejorar significativamente su postura de seguridad (ENISA, 2024).

Según el informe "Cost of a Data Breach" de 2025 de IBM, el coste promedio global de una vulneración de datos es de 4,44 millones de dólares (Bonderud, 2025). Agregando que empresas de sectores como la sanidad, finanzas y el sector público, pueden enfrentar multas y sanciones que pueden agravar los costos. Razón por la cual es importante que las organizaciones evalúen el retorno de inversión al invertir en soluciones de seguridad.

La metodología de CTEM juega un papel fundamental en la gestión continua de la exposición a amenazas, dado que permite evaluar y priorizar las amenazas de manera continúa

teniendo en cuenta el contexto de las organizaciones sumado a la inteligencia de amenazas (Gartner, 2024).

Teniendo en cuenta lo anterior, la presente Monografía tiene como objetivo estudiar y diseñar un plan integral de inteligencia de amenazas junto con la metodología de CTEM, el cual se caracterizará por abordar los diferentes tipos de inteligencia como lo es la táctica, caracterizada por compartir información (TTPs) de los actores de amenaza, técnica, caracterizada por recopilar datos específicos relacionados con las herramientas, vulnerabilidades y exploits utilizados por los actores de amenaza, operativa, cuyo objetivo es identificar los actores de amenaza y los grupos APT y finalmente estratégica, que se centra en el estudios de las tendencias cambiantes en seguridad (ENISA, 2024; Gartner, 2024). Este plan incluirá un estudio exhaustivo del proceso del ciclo de vida de la inteligencia sobre ciberamenazas, que comprende desde la recolección hasta la distribución y el uso de la información (IBM, 2024). Además, se explorarán metodologías probadas como la Cyber Kill Chain, que permite identificar las fases de un ataque cibernético y, por tanto, mejorar la detección y respuesta. También se estudiarán diversos marcos de trabajo (frameworks) y plataformas de inteligencia de amenazas, como MISP, que facilitan el intercambio de información entre organizaciones, permitiendo una defensa más colaborativa y eficiente (ENISA, 2024). Adicionalmente, se integrará el ciclo continuo de CTEM el cual es fundamental para identificar de manera continua la superficie de ataque, la exposición de amenazas y por lo tanto su priorización (Gartner, 2024).

Objetivos

Objetivo General

Proponer un plan de inteligencia de amenazas junto con CTEM utilizando el ciclo de vida de la inteligencia y el ciclo de la gestión continua de la exposición a amenazas con el fin de fortalecer la postura de seguridad en ciberseguridad.

Objetivos Específicos

Realizar un estudio de plataformas de inteligencia de amenazas y herramientas de análisis de vulnerabilidades de Open source que puedan integrarse al plan de inteligencia de amenazas junto con CTEM, tomando como referencia comparativa soluciones comerciales, con el fin de identificar y escoger alternativas adecuadas para la gestión de amenazas.

Diseñar un plan de recolección de inteligencia que contemple todas las fases del ciclo de vida de la inteligencia de amenazas, utilizando las mejores prácticas que permitan una recopilación continua y orientada al fortalecimiento de la seguridad cibernética, mediante el uso de las herramientas seleccionadas en el objetivo 1.

Evaluar el ciclo de gestión continua de la exposición a amenazas (CTEM) para clasificar, priorizar y contextualizar la información obtenida, identificando cómo esta puede optimizar la gestión de riesgos y amenazas.

Marco Referencial

Antecedentes

A continuación, se comparten los antecedentes clave del proyecto para tener en cuenta en el desarrollo de la monografía:

El Escudo AI y el Marco Red AI: Soluciones de Aprendizaje Automático Para la Inteligencia Sobre Ciberamenazas (CTI)

En el artículo se explica que la ciberseguridad está experimentando una rápida transformación y las tecnologías de vanguardia, como el machine learning y la IA juegan un papel cada vez más crucial en el fortalecimiento de la Identificación de amenazas, la reacción ante incidentes y la defensa anticipada. Entre las soluciones más destacadas se encuentran los marcos Artificial Intelligence Shield (AI Shield) y Red Team Artificial Intelligence (Red AI), los cuales emplean aprendizaje automático para abordar los retos asociados con la inteligencia sobre ciberamenazas (CTI). (Simran, Kumar, & Hans, 2024).

Inteligencia Sobre Ciberamenazas y Aprendizaje Automático

Se informa que se ha comprobado que la inteligencia sobre amenazas cibernéticas es un componente clave en la seguridad defensiva y la ciber protección, con ejemplos que datan de la creación del Financial Services Information Sharing and Analysis Center (FS-ISAC) en 1998. En la actualidad, se requieren métodos automatizados para hacer frente a la magnitud y complejidad de los ataques cibernéticos globales. Para que la inteligencia sobre amenazas sea efectiva, debe ser procesable, actualizada y validada de manera confiable, de modo que pueda integrarse adecuadamente en los sistemas de defensa gestionados por computadoras. (Haass, 2022).

Examinar el Papel de la IA Generativa en la Mejora de la Inteligencia Sobre Amenazas y las Medidas de Ciberseguridad

En el artículo se subraya la relevancia del machine learning, así como el de la Inteligencia artificial (IA) para identificar amenazas de forma proactiva y reducir la incidencia de falsos positivos. Además, se hace hincapié en la falta de profesionales cualificados en ciberseguridad, lo que limita la capacidad de las organizaciones para reaccionar de manera eficiente ante incidentes. Se resalta también la necesidad de integrar datos tanto de fuentes internas (como los firewalls) como de fuentes externas, con el fin de priorizar el análisis de los eventos detectados y facilitar su integración efectiva con los equipos del SOC (Saddi et al., 2024).

Ampliación de los Playbooks de Amenazas Para la Inteligencia Sobre Ciberamenazas: Un Enfoque Novedoso Para la Atribución de APT

Conforme los ciberataques se vuelven más avanzados y frecuentes, la CTI sigue siendo esencial para los defensores. Un elemento clave de la CTI es la atribución de ataques, que ayuda a identificar al grupo o actor detrás de un ataque. Esta información permite a los defensores anticiparse y mejorar su respuesta. El artículo propone un enfoque basado en el análisis de datos para realizar atribuciones precisas de ataques, utilizando manuales de tácticas, técnicas y procedimientos (TTP) de los atacantes. A través de la minería de reglas de asociación en grandes conjuntos de datos de CTI, el enfoque extiende los manuales existentes con TTP estadísticamente probables que un atacante podría emplear (Edie, McKee, & Duby, 2023).

El Papel de la Inteligencia Artificial y Blockchain Para la Futura Inteligencia Sobre Ciberamenazas

Como resultado de la rápida integración de tecnologías inteligentes en la vida cotidiana, el riesgo de ataques cibernéticos ha aumentado considerablemente. Esto ha impulsado la necesidad de adoptar enfoques más sólidos y prácticos para mitigar estos riesgos, especialmente en sistemas inteligentes. La CTI se ha establecido como una herramienta clave para desarrollar soluciones proactivas y avanzadas que permiten detectar y mitigar eficazmente las amenazas cibernéticas. (Pal, Jadidi, Alaeifar, & Foo, 2023).

Marco Conceptual

A continuación, se comparte una lista de conceptos claves a tener en cuenta en el desarrollo de la monografía:

Inteligencia de Ciber Amenazas

Según EC-Council (s.f), la inteligencia de ciber amenazas consiste en el procesamiento de datos a través del empleo de herramientas y diversas técnicas que permite generar información de valor sobre las ciber amenazas existentes o que pueden emerger y pueden representar un riesgo para las organizaciones.

Tipos de CTI

Existen 4 tipos de inteligencia de amenazas, según EC-Council (s.f): Inteligencia estratégica sobre amenazas, Inteligencia estratégica de ciberamenazas, inteligencia táctica de ciberamenazas, inteligencia técnica sobre ciberamenazas, inteligencia operativa sobre ciberamenazas."

Ciclo de Vida de la Inteligencia de Amenazas

De acuerdo con Palo Alto Networks (s.f.), es un proceso que se utiliza para gestionar las ciberamenazas. Permite a las organizaciones proteger sus activos de información mediante las siguientes fases: Dirección/Descubrimiento, Recopilación, Procesamiento, Análisis, Difusión/Acción y Retroalimentación.

Metodología Cyber Kill Chain

De acuerdo con Splunk (s.f), la metodología Cyber Kill Chain describe modelo de cadena de ataque cibernético que consta de siete pasos que desglosan las distintas etapas de un ciberataque: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives.

Modelado de Amenazas

El modelado de amenazas hace referencia el proceso de utilizar escenarios hipotéticos, diagramas de sistemas y pruebas con el fin de ayudar a proteger los sistemas y los datos (Cisco, s.f).

Existen diferentes enfoques de modelados de amenazas, algunas se explican a continuación:

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE). Es una metodología de modelado de amenazas que describe el listado de amenazas definido por sus siglas (Cloudflare, s.f).

Vulnerability Assessment and Scanning Tool (VAST). Es un enfoque de modelado de amenazas diseñada específicamente para abordar tareas complejas en los sistemas empresariales a gran escala (Cloudflare, s.f).

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). Es

una metodología de modelado de amenazas que se utiliza para evaluar el entorno de una organización y determinar los riesgos asociados con TI (Naik et al., 2024).

Protocolo de Semáforo (TLP)

Se creó con la finalidad de promover el intercambio de información de manera segura.

El protocolo TLP consta de 4 definiciones. (CISA, s.f.) de acuerdo con el color de los semáforos, que indican hasta donde puede circular la información más allá del receptor.

TLP: RED. Indica que la información no se puede divulgar, está restringida únicamente para ser accesible por parte de un grupo de personas.

TLP: AMBER. La divulgación de la información es limitada, está restringida para ser accesible a los participantes de una organización y sus clientes.

TLP: GREEN. La divulgación de la información está restringida para que solo pueda ser accesible por parte de los participantes de una comunidad (organizaciones).

TLP: WHITE. La información se puede divulgar sin restricción, puesto que su divulgación no representa un riesgo.

Pirámide del Dolor

La pirámide del dolor representa la categorización de los diferentes indicadores de compromiso, desde el rango más bajo hasta el más alto que tendrían un gran impacto para los actores de amenaza si esto son detectado (Picus Security, 2025).

A continuación, se presenta la lista de indicadores, comenzando desde la base de la pirámide, donde la detección tiene un menor impacto, hasta la parte superior, que involucra indicadores con un mayor impacto: Valores HASH, Direcciones IP, Dominios, Artefactos de red/host, Herramientas, y TTP.

MITRE ATT&CK

MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) es un marco que proporciona una base de conocimientos sobre el comportamiento de los ciberdelincuentes, detallando las diversas etapas de un ataque y las plataformas que suelen ser sus objetivos (MITRE, 2025).

MISP

Es una plataforma abierta de inteligencia sobre amenazas que facilita el intercambio, almacenamiento y correlación de indicadores de compromiso (IoC) de ataques dirigidos, información sobre amenazas, datos relacionados con fraudes financieros, detalles sobre vulnerabilidades e incluso inteligencia antiterrorista (MISP Project, s.f.).

APT

Una APT hace referencia a un tipo de ataque cibernético en el que un atacante o un grupo de atacantes logra infiltrarse en una red de forma encubierta y mantiene una presencia prolongada para llevar a cabo acciones maliciosas, como la sustracción de información sensible (TechTarget, 2025).

Análisis de Hipótesis en Competencia

El análisis de hipótesis en competencia (ACH) es una técnica utilizada en inteligencia de amenazas que implica la recopilación y evaluación de múltiples explicaciones o hipótesis sobre un evento o conjunto de datos relacionado con una amenaza cibernética (Center for Internet Security, 2022).

OSINT

La inteligencia de fuentes abiertas (OSINT) hace referencia a la recolección y la examinación de dato públicos, accesibles y disponibles, para generar inteligencia relevante en el

contexto de la seguridad y las amenazas (Lindemulder & Forrest, 2025).

Dark Web

La inteligencia de amenazas en la Dark Web hace referencia a la recopilación, análisis y monitoreo de datos provenientes de la Dark Web con el objetivo de identificar posibles amenazas cibernéticas y brechas de seguridad. La Dark Web es una sección oculta de la web, accesible solo a través de software especializado como Tor, que permite a los usuarios permanecer anónimos (ZeroFox, s.f.).

Marco Teórico

A continuación, se comparte información clave de diferentes referentes teóricos que pueden ser fundamentales para el desarrollo de la monografía:

Inteligencia Sobre Ciber Amenazas

El articulo explica que, con frecuencia, el desarrollo de una tecnología avanzada debe permitir la recolección de información proveniente de diversas fuentes de inteligencia de amenazas. En muchos casos, los datos obtenidos pueden ser compartidos inmediatamente después de su recopilación, dependiendo del impacto en las operaciones actuales y los requisitos operativos. La inteligencia cruda se compone de fragmentos pequeños de datos relacionados con ciertos eventos y puede contener incertidumbres o errores que deben ser corregidos a través de informes y análisis (Sakib, 2022).

Minería de Inteligencia Sobre Ciber Amenazas Para una Defensa Proactiva de la Ciberseguridad: Un Estudio y Nuevas Perspectivas

La minería sobre CTI, es una metodología usada para descubrir, procesar y analizar datos cruciales acerca de las amenazas informáticas, además, está ganando terreno rápidamente. Sin embargo, la mayoría de las organizaciones se concentran principalmente en aplicaciones básicas,

como la integración de fuentes de datos de amenazas con infraestructuras existentes, tales como sistemas de red, cortafuegos, sistemas de prevención de intrusiones y plataformas como el Security Information and Event Management (SIEM), sin explotar a fondo los conocimientos valiosos que esta nueva inteligencia puede proporcionar (Sun et al., 2023).

Intercambio de Inteligencia Sobre Amenazas Basado en la Nube Para la Defensa Colectiva

Para mejorar la ciberseguridad en un entorno cada vez más interconectado, compartir inteligencia sobre amenazas en la nube es clave para una defensa colectiva efectiva. Las organizaciones deben colaborar estrechamente para detectar y responder de manera eficiente a los diversos riesgos cibernéticos. Este artículo aborda la utilización de la infraestructura en la nube para compartir y analizar datos de inteligencia sobre amenazas, con el objetivo de respaldar la defensa colectiva (Roobini et al., 2024).

HDA-TIP: Un Marco Para la Agregación de Datos Heterogéneos Para la Plataforma de Inteligencia de Amenazas

Hybrid Detection and Analysis Threat Intelligence Platform (HDA-TIP) explica que la inteligencia de amenazas cibernéticas se basa en el análisis de incidentes previos de ciberataques para anticipar y prevenir posibles ataques en el futuro. La evidencia situacional derivada de estos informes crea una base sólida para las estrategias de detección y mitigación de amenazas. Sin embargo, uno de los desafíos más significativos que enfrenta la inteligencia de amenazas es el volumen de información proveniente de diversas fuentes, lo que a menudo genera datos redundantes o irrelevantes (Yasmeen et al., 2023).

CLEVER: Creación de MISP Inteligentes Para la Inteligencia Sobre Ciber amenazas

La inteligencia sobre amenazas cibernéticas es fundamental en la ciberseguridad actual, ya que proporciona el conocimiento necesario para prevenir y defenderse de una amplia variedad

de amenazas cibernéticas. No obstante, uno de los retos más grandes en este campo son los datos incompletos e inconsistentes que pueden generar evaluaciones incorrectas de las amenazas. Esto, a su vez, aumenta el riesgo de que se pasen por alto amenazas reales o, en el peor de los casos, se disparen falsas alarmas. Este artículo presenta CLEVER, una extensión del sistema de intercambio de datos sobre malware (MISP) que incorpora modelos de aprendizaje automático para mejorar la gestión y el procesamiento de los datos de CTI (Wang et al., 2024).

CTEM: Gestión Continua de la Exposición a Amenazas

Es un programa creado por Gartner que permite detectar y priorizar activamente las amenazas más importantes teniendo la cuenta el contexto del negocio de las organizaciones, como por ejemplo su sector (Finanzas, educación, etc) (Gartner, 2024). CTEM se basa en un ciclo continuo y cíclico que contempla 5 fases:

Alcance. El primer paso consiste en determinar la superficie de ataque de la organización, esta puede hacer referencia activos externos (servidores, bases de datos, etc) así como la superficie de ataque externa (direcciones IP Publicas, Uniform Resource Locators (URLs), puertos expuestos, etc).

Descubrimiento. El descubrimiento es una fase fundamental en el programa de CTEM, dado que este puede brindar visibilidad de los activos ocultos de la organización. Muchas de las organizaciones no conocen toda su superficie de ataque lo que representa un gran riesgo, dado que esto corresponde a la superficie de ataque no gestionada. El descubrimiento es fundamental para iniciar con la priorización de los activos.

Priorización. Esta fase consiste en realizar la priorización de las amenazas con mayor probabilidad de ser explotadas, teniendo en cuenta distintos factores como los activos más críticos de la organización, la tolerancia al riesgo, controles de compensación, entre otros.

Validación. La fase de validación consiste en verificar la probabilidad real de explotación de una vulnerabilidad y hasta donde podría llegan un atacante. También se evalúa si el plan actual es suficiente para proteger el negocio.

Movilización. La última fase que es la de movilización consiste en comunicar el plan de CTEM al equipo de seguridad y a las partes interesadas de la empresa. Lo anterior con el fin de asegurar que los equipos implementen los hallazgos de CTEM, reduciendo cualquier obstáculo a las aprobaciones, los procesos de implementación o las medidas de mitigación.

Marco Legal

Ley 1581 de 2012

Es una ley que presenta el derecho constitucional que tienen todas las personas sobre conocer, actualizar y rectificar las informaciones que se hayan recogido sobre estas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (Colombian Congress, 2012).

Ley 1273 de 2009

Es una ley que adiciona el código penal relacionado con delitos informáticos como el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el uso de software malicioso, entre otros (Colombian Congress, 2009).

Política Nacional de Seguridad Digital (CONPES 3995 de 2020)

Es un conjunto de política públicas que brinda lineamientos de Política para Ciberseguridad y Ciberdefensa en Colombia. Su objetivo es proporcionar lineamientos para que los ciudadanos puedan navegar de manera segura en el entorno digital (Departamento Nacional

de Planeación, n. d.).

ISO 27001:2022

Es la norma más reciente y conocida para sistemas de gestión de la seguridad de la información (SGSI). Proporciona a organizaciones de distintos tipos directrices para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (ISO/IEC, 2022).

ISO 27002:2022

Es una norma que establece directrices para establecer, implementar y mejorar SGSI enfocado en ciberseguridad. Proporciona objetivos de control relacionados con aspectos clave de la ciberseguridad, como el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta a incidentes (ISO/IEC, 2022).

ISO 27032:2023

Es una norma que proporciona pautas para mejorar la seguridad de Internet, la seguridad web, la seguridad de la red y la ciberseguridad. Proporciona una visión general y como las mismas pueden relacionarse (ISO/IEC, 2023).

COBIT 2019

Control Objectives for Information and Related Technologies (COBIT 2019) es un framework para la gobernanza y la gestión de la información y la tecnología (I&T) empresarial que respalda el logro de los objetivos de las organizaciones. Se basa en principios como satisfacer las necesidades de las partes interesadas, abarcar la empresa de extremo a extremo, aplicar un único marco integrado, permitir un enfoque holístico y separar la gobernanza de la gestión (ISACA, s.f.).

ITIL 4

Information Technology Infrastructure Library (ITIL 4) es un framework desarrollado para la gestión de servicios en la era digital. Permite comprender cómo las TI impactan la estrategia de las organizaciones y cómo los profesionales pueden utilizar las cuatro dimensiones de la gestión de servicios en un contexto empresarial más amplio. Además, utiliza los principios rectores para abordar el cambio, optimizar el trabajo e introducir prácticas de trabajo flexibles y colaborativas (AXELOS, s.f.).

NIST Cybersecurity Framework 2.0 (CSF 2.0)

Es la última versión del marco de ciberseguridad del National Institute of Standards and Technology (NIST) que ofrece orientación a la industria, las agencias gubernamentales y otras organizaciones para gestionar los riesgos de ciberseguridad (National Institute of Standards and Technology. (2024)).

Marco Contextual

Los ciberataques están evolucionando más a medida que pasa el tiempo, solo en el año 2025 se ha identificado que los ataques de malware, phishing, entre otras amenazas, son más avanzados debido al uso de la IA y de otras tecnologías avanzadas. Los actores de amenaza originarios en China e Irán están haciendo uso de la IA para procesos de descubrimiento y explotación de vulnerabilidades, de acuerdo con el informe Threat Intelligence de Google, publicado en The Wall Street Journal (Volz & McMillan, 2025).

El aumento en los ciberataques también ha tenido un gran impacto en las organizaciones, de acuerdo con International Business Machines (IBM), el costo promedio global de una filtración de datos superó los $4.88 millones en el año 2024, un aumento respecto al año 2023 cuyo promedio fue de los $4.45 millones (Fortinet, s.f.).

En el año 2024, las empresas de los sectores salud y financiero a nivel global fueron las más afectadas. En los casos en que se comprometieron 50 millones de registros o más, los costos promedio fueron de $375 millones. En el caso del sector Finanzas, los ataques que aprovecharon fallas de Tecnologías de la Información (TI) y errores humanos representaron una cuarta parte del total (51%), con un con un 25% y un 24%. Además, las organizaciones de este sector tardaron en promedio 68 días en identificar una brecha y 51 días en contenerla. Aunque el tiempo es inferior al promedio mundial de194 días para identificarlas y 64 días para contenerlas, sigue considerándose como un tiempo amplio, dado que en este un atacante puede realizar bastantes acciones maliciosas (Bonderud, 2025).

Debido al avance en la IA generativa y en las herramientas avanzadas que utilizan los actores de amenazas, las organizaciones se ven obligadas a invertir en defensas más sofisticadas. El IDC (International Data Corporation), empresa de consultoría y análisis de tecnologías de la información, confirmo el costo global en ciberseguridad aumentará en un 12,2 % en 2025 y superará los $377,000 millones para el año 2028. También informo que Estados Unidos y países de Europa Occidental serán los que más inviertan en ciberseguridad con más del 70 % del gasto global, mientras que países de América Latina, Europa Central y Oriental, Oriente Medio y África también experimentarán un fuerte crecimiento (IDC, s.f.).

Ciberataques en Colombia

En el año 2022, la empresa Keralty, multinacional de atención médica sufrió un ataque por parte del grupo de ransomware Ransomhouse, lo cual interrumpió la disponibilidad los sitios web y las operaciones de la empresa y sus subsidiarias EPS Sanitas y Colsanitas. Este ataque afecto al sistema de salud de Colombia. En su momento, el grupo de ransomware compartió una captura de pantalla de VMware ESXi con una nota de rescate con el mensaje ‘Dear Keralty’

(Abrams, 2022).

RansomHouse es un grupo de ransomware que surgió en marzo de 2022 y se clasificó como una amenaza de extorsión multifacética. Los actores de amenaza buscan extraen datos potenciales con el fin de amenazas con publicarlos. Además, RansomHouse se ha posicionado así mismo como una fuerza benéfica, ya que sus filtraciones buscan visibilizar a las empresas en crisis (SentinelOne, 2022).

Otro grupo de actores de amenaza llamado Blind Eagle, también conocido como APT-C-36, sospechoso de provenir de América del Sur también ha ejecutado numerosos ciberataques contra organizaciones colombianas suplantando entidades como la Registraduría Nacional del Estado Civil de Colombia, Dirección Nacional de Impuestos y Aduanas, el Departamento Administrativo Nacional de Estadística, la Policía Nacional Cibernética de Colombia, la Oficina del Procurador General de la República y Migración en Colombia, con el fin de atacar a empresas como el INCI Instituto Nacional Colombiano para Ciegos (INCI), Ecopetrol, Hocol (Filial de Ecopetrol), Fabricante de ruedas en Colombia (IMSA), Byington Colombia, entre otras empresas (Darktrace, 2025).

Colombia cerro el año 2024 con 36.000 millones de intentos de ataques registrados en el país, según Fortinet (Junco, 2025). Así mismo, en lo que va del año 2025 Colombia ha enfrentado en promedio más de 2.700 ciberataques semanales según un informe de LatinPyme, por lo que se prevé que los ataques sigan aumentando (Dorado, 2025).

Diseño Metodológico

En el diseño metodológico de este proyecto se realiza un enfoque híbrido, dado que se combina la investigación cuantitativa y cualitativa. Primero, se aplicará un análisis cuantitativo a través de métricas de desempeño de las herramientas de CTI y gestión de vulnerabilidades para CTEM gratuitas que serán probadas para evaluar su precisión, cobertura, falsos positivos, frecuencia de actualización, entre otros. Por otro lado, se realizará un análisis cualitativo teniendo en cuenta la revisión documental y la valoración de características no medibles experimentalmente de las herramientas de pago. Esta integración permitirá realizar un análisis comparativo entre la práctica y la teoría para obtener conclusiones más sólidas.

Fase 1, Objetivo 1

Actividades

Investigación y Prueba de Herramientas de Ciber Inteligencia de Amenazas y de Análisis de Vulnerabilidades. Se realizará una investigación y análisis comparativo de herramientas utilizadas en los campos de la ciber inteligencia de amenazas y el análisis de vulnerabilidades, con el fin de identificar sus principales funciones, alcances y limitaciones. Para el caso de la ciber inteligencia de amenazas, se revisarán soluciones que permitan la recolección de información de fuentes abiertas, feeds de inteligencia y de la Dark web que permitan brindar contexto de las amenazas y en relación con el análisis de vulnerabilidades, se evaluarán plataformas que permitan detectar vulnerabilidades en equipos de red y aplicaciones web, priorizando los riesgos según el contexto. En ambos casos, se probarán herramientas Open Source y se investigarán herramientas de pago.

Fase 2, Objetivo 2

Actividades

Estudio del Ciclo de Vida de la Inteligencia de Amenazas y Frameworks de CTI. Se realizará una investigación y análisis de las diferentes etapas que contemplan el ciclo de vida de la inteligencia de amenazas, así como como de diferentes frameworks de ciber inteligencia de amenazas como el modelo diamante, MITRE ATT&CK, entre otros.

Estudio de Fuentes OSINT y Feeds de CTI. Se investigará y analizaran diferentes fuentes de inteligencia de amenazas, revisando cómo OSINT puede aportar los datos desde fuentes abiertas como redes sociales, foros o bases de datos de vulnerabilidades, así como de feeds de CTI que pueden proporcionar indicadores de compromiso en tiempo real.

Generar Plan de Recolección de Datos. Se generará un plan de recolección de datos de inteligencia de amenazas desde diferentes fuentes contemplando el ciclo de vida de la inteligencia de amenazas, el cual permita obtener información que aporte a la priorización de amenazas.

Generar Plan de Inteligencia de Amenazas. Se generará un plan de ciber inteligencia de amenazas que contemple el ciclo de vida de la inteligencia de amenazas y permita definir cómo se debe recopilar, procesa, analizar y difundir información relacionada con actores de amenaza, IOC, IoA, vulnerabilidades y campañas maliciosas. El objetivo es crear una estrategia estructurada que convierta datos en conocimiento de alto valor, que pueda permitir a las organizaciones anticiparse a las amenazas, reforzar la detección y apoyar en la toma de decisiones relacionadas con la priorización de amenazas mediante el uso de mejores prácticas.

Fase 3, Objetivo 3

Actividades

Investigación del Ciclo Continuo CTEM. Se investigará el programa de CTEM, de Gartner, con el fin de entender un ciclo continuo y proactivo puede permitir a las organizaciones identificar, priorizar y gestionar de forma proactiva su exposición a amenazas. El análisis tiene como objetivo confirmar como las fases como el descubrimiento de activos, la evaluación de vulnerabilidades, la validación de riesgos y la priorización de amenazas, pueden representar un proceso proactivo a diferencia de los servicios tradicionales de gestión de vulnerabilidades. El objetivo es comprender cómo CTEM puede integrar pruebas continuas de exposición, automatizar procesos, mejorar la postura de seguridad y reducir el tiempo de exposición de amenazas.

Generar Plan de CTEM + CTI. Diseñar un plan que contemple CTEM junto con CTI, con el fin de identificar vulnerabilidades, priorizar riesgos y aplicar medidas de mitigación basadas en información real y contextualizada de amenazas. El plan debe contemplar un proceso proactivo y cíclico que permita reducir el tiempo de exposición frente a amenazas y fortalecer la postura de seguridad.

Definición de Métricas Para la Priorización de Amenazas. Identificar y definir métricas que permitan priorizar de manera activa las amenazas y vulnerabilidades. Se realizará un análisis de indicadores como el Exploit Prediction Scoring System (EPSS) del Forum of Incident Response and Security Teams (FIRST), Known Exploited Vulnerabilities (KEV) del Cybersecurity and Infrastructure Security Agency (CISA) e indicadores clave de desempeño (KPI) que permitan clasificar riesgos según su probabilidad de explotación, impacto potencial y criticidad en los activos.

Documentación Plan de Inteligencia de Amenazas y CTEM. Elaborar la documentación del plan de ciber inteligencia de amenazas y de gestión continua de exposición de amenazas, el cual debe incluir las metodologías, fuentes de información, herramientas y métricas a utilizar. El objetivo es consolidar de manera estructurada toda la información del plan con el fin de que funcione como guía operativa que pueda facilitar la implementación, seguimiento y mejora continua del plan.

Objetivo Específico 1

El propósito de este objetivo es analizar y comparar diferentes herramientas de gestión de vulnerabilidades, tanto de código abierto como de pago (de manera teórica en el caso de las herramientas pago), con el fin de identificar sus capacidades técnicas, su alcance en la detección de vulnerabilidades y su posible integración dentro de un plan de inteligencia de amenazas basado en CTEM.

Así mismo, se incluirá el estudio de plataformas de inteligencia de amenazas, orientadas a la recolección, correlación y análisis de inteligencia táctica, técnica y estratégica. Estas plataformas permitirán evaluar cómo la inteligencia contextual puede fortalecer la priorización y respuesta ante las vulnerabilidades detectadas dentro del ciclo CTEM.

Estudio y Análisis Comparativo de Herramientas de Gestión de Vulnerabilidades

OpenVAS

Open Vulnerability Assessment System (OpenVAS) es una herramienta de análisis de vulnerabilidades ampliamente utilizada en entornos de seguridad informática. La herramienta fue desarrollada por la empresa Greenbone desde 2006, forma parte de la familia de productos de gestión de vulnerabilidades de la compañía y constituye la base de la Community Edition, una versión gratuita y de código abierto (OpenVAS, s.f.).

El escáner permite realizar pruebas autenticadas y no autenticadas sobre distintos sistemas, abarcando múltiples protocolos tanto de red como industriales. Además, cuenta con un motor interno capaz de ejecutar miles de pruebas de seguridad mediante un lenguaje propio que facilita la personalización de los análisis.

Una de sus principales ventajas es que utiliza un feed de vulnerabilidades actualizado de forma diaria, el cual contiene pruebas desarrolladas y verificadas por la comunidad y por

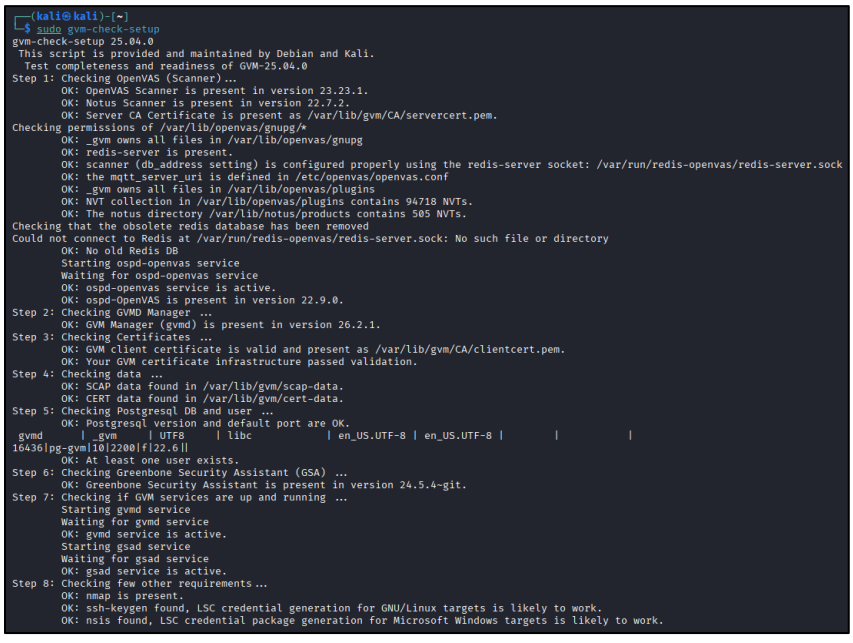
Greenbone. Gracias a ello, OpenVAS puede detectar de manera precisa vulnerabilidades conocidas y emergentes, ofreciendo resultados detallados y priorizados según su criticidad.

Como primer paso, se instala la última versión de OpenVAS (22.9.0) en una máquina virtual Kali Linux (Kali controladora), empleando la edición Community disponible en el repositorio oficial de Greenbone. Esta versión permite realizar escaneos de vulnerabilidades de manera gratuita y cuenta con actualizaciones periódicas de los feeds de seguridad.

En la figura 1 se observa el proceso de instalación de OpenVAS en el entorno Kali Linux, donde se evidencia la ejecución de los comandos necesarios y la correcta configuración inicial del servicio, lo cual garantiza que la herramienta quede operativa para la fase de escaneo de vulnerabilidades.

Figura 1

Instalación OpenVas



Nota. Elaboración propia mediante Kali Linux.

Posteriormente, se actualizan los feeds de seguridad y los NVTs (Network Vulnerability Tests), con el fin de contar con la información más reciente sobre vulnerabilidades conocidas. Este paso es importante porque permite que OpenVAS tenga una base de datos actualizada para detectar fallos de seguridad de forma más precisa durante los escaneos.

En la figura 2 se observa el proceso de actualización de los feeds y NVTs, donde el sistema descarga y sincroniza las bases de datos necesarias para mantener actualizadas las firmas de vulnerabilidades.

Figura 2

Actualización de Feeds y NVTs

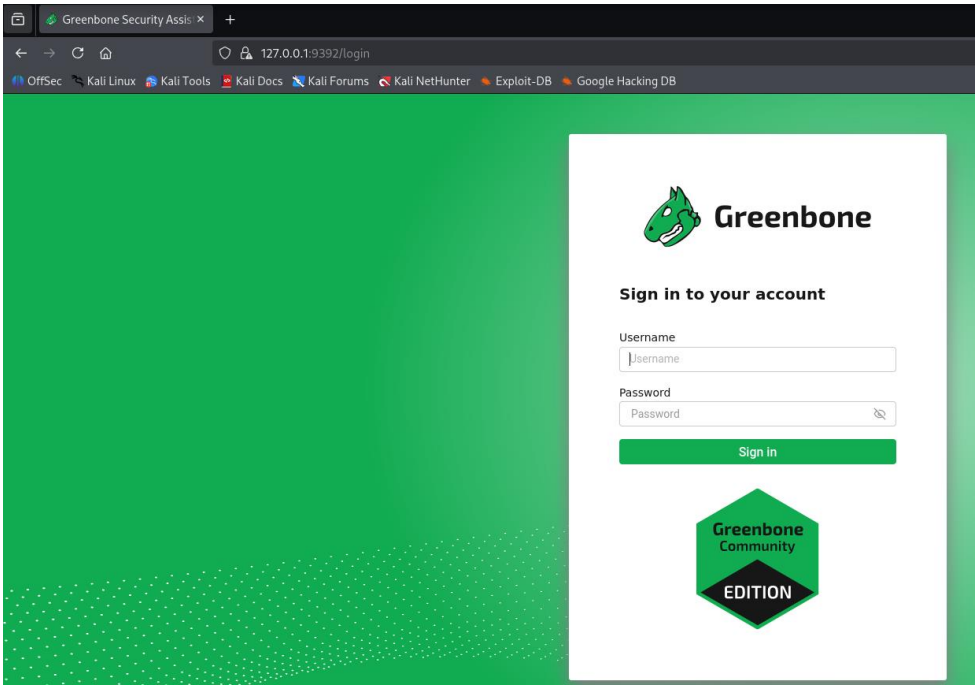
Nota. Elaboración propia mediante Kali Linux.

Finalmente, se accede a la interfaz web de OpenVAS, donde se realiza el inicio de sesión para ingresar al panel de administración de la herramienta.

En la figura 3 se muestra la pantalla de inicio de sesión de OpenVAS, donde se introducen las credenciales de acceso para poder entrar al sistema y continuar con la gestión de los escaneos de vulnerabilidades.

Figura 3

Interfaz de OpenVas



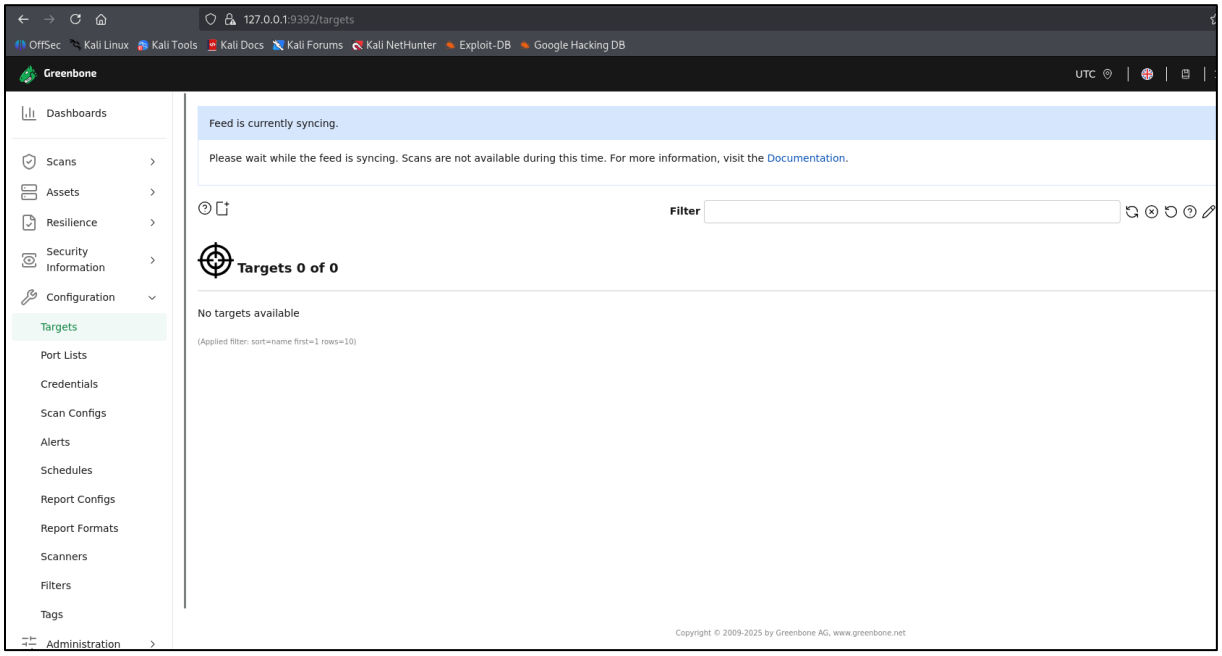
Nota. Elaboración propia mediante el uso de la herramienta OpenVas.

Posteriormente, se ingresa a la interfaz de administración de OpenVAS (Greenbone Security Assistant), donde se gestiona la configuración general de la herramienta para la ejecución de escaneos de vulnerabilidades.

En la figura 4 se observa el panel principal de OpenVAS, en el que se muestra el estado del sistema y la sección de gestión de objetivos, evidenciando además que los feeds de seguridad se encuentran en proceso de sincronización en ese momento.

Figura 4

Interfaz de OpenVas

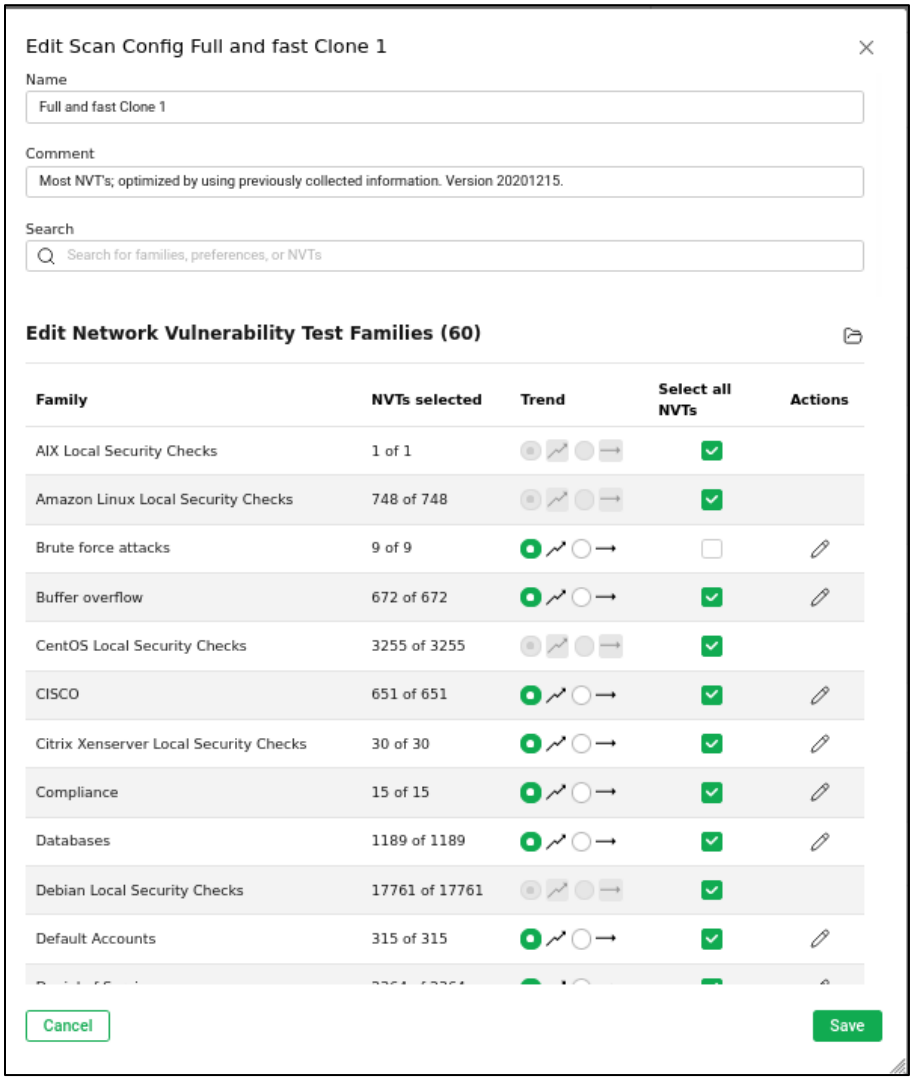


Nota. Elaboración propia mediante el uso de la herramienta OpenVas.

Se realizó la desactivación de Network Vulnerability Tests (NVTs) relacionados con ataques de fuerza bruta, malware y escalamiento de privilegios, dado que estos análisis incrementan significativamente la carga del escaneo y podían prolongar excesivamente su duración y consumo de recursos, afectando la disponibilidad del objetivo escaneado, tal como se puede observar en la figura 5, donde se muestra la configuración del perfil de escaneo.

Figura 5

Configuración Perfil de Escaneo



Nota. Elaboración propia mediante el uso de la herramienta OpenVas.

Explicación Apartados Modulo Scans. Primero esta Tasks. es el punto de partida de todo el proceso de escaneo. En este apartado se crean y administran las tareas de los escaneos, permite seleccionar los objetivos (hosts o rangos IP) a analizar, el tipo de escaneo (por ejemplo, full scan), tareas programadas, el número máximo de NVTs y host a escanear.

Reports. Acá se almacenan los resultados obtenidos tras cada tarea de escaneo. Aquí se puede la cantidad y severidad de las vulnerabilidades detectadas, así como exportar los informes en distintos formatos o compararlos con análisis previos para evaluar la evolución del estado de seguridad mediante una función llamada delta.

Results. Se presentan los hallazgos individuales con un nivel de detalle más técnico. Cada resultado muestra información específica sobre la vulnerabilidad, el puerto afectado, el host implicado, la descripción técnica, su impacto y las referencias CVE. Esta sección es muy importante para revisar evidencias específicas y validar posibles falsos positivos.

Vulnerabilities. En este apartado se agrupan todas las vulnerabilidades detectadas en los diferentes escaneos ejecutados. Este apartado permite consultarlas la severidad, tipo o frecuencia, además de acceder a sus descripciones, puntuaciones CVSS, las referencias y posibles soluciones. Es el punto de referencia para priorizar correcciones y planificar acciones de mitigaNotes, se pueden añadir observaciones o comentarios personalizados relacionados con los resultados de los escaneos. Las notas ayudan a documentar decisiones, justificar falsos positivos o registrar acciones correctivas, lo que resulta especialmente útil cuando varios analistas trabajan sobre los mismos informes o se elabora documentación de auditoría.

Override*s*. En este apartado se gestionan excepciones y ajustes manuales sobre los hallazgos detectados. Desde este apartado se puede modificar la severidad de una vulnerabilidad o marcarla como mitigada cuando ya ha sido tratada, evitando así que se repita en futuros informes. Este apartado ayuda a mantener consistencia y precisión en los resultados del análisis y remediación.

Explicación Apartados Modulo Assets. Primero esta Hosts, en este apartado se gestionan los "hosts" o dispositivos específicos en la red configurados objetivos para el análisis de vulnerabilidades. Los hosts son los equipos o servidores que pueden estar expuestos a riesgos, y en esta sección se puede ver los detalles de cada uno, como sus direcciones IP, los servicios que ejecutan, etc.

Operating Systems. En este apartado se listan los sistemas operativos de los diferentes hosts escaneados. Poder agrupar los hosts por sistema operativo es fundamental para realizar un análisis adecuado de las vulnerabilidades, dado que cada sistema operativo tiene su propio conjunto de vulnerabilidades conocidas y formas de mitigarlas.

TLS Certificates (Certificados TLS). En este apartado se puede visualizar la información sobre los certificados Transport Layer Security (TLS) utilizados en los hosts. Los certificados TLS son esenciales para establecer comunicaciones seguras en la red, en esta sección se puede verificar su validez, fecha de expiración y posibles configuraciones inseguras.

Explicación Apartados Módulos Resilience. Primero esta Remediation Tickets**,** en este módulo se pueden gestionar las tareas necesarias para solucionar vulnerabilidades detectadas. Cada ticket representa una acción correctiva que debe llevarse a cabo. Se puede asignar, hacer seguimiento y verificar su resolución, facilitando la coordinación entre los equipos de seguridad.

Compliance Policies. Aquí se definen las políticas de seguridad o normativas que deben cumplirse (como ISO 27001, PCI-DSS, etc.). Estas políticas sirven como base para evaluar si los sistemas de la organización están alineados con los requisitos legales, regulatorios o internos.

Compliance Audits. Este módulo permite ejecutar auditorías para evaluar el nivel de cumplimiento de los activos con respecto a políticas previamente definidas. Acá se pueden

analizar configuraciones, prácticas y controles implementados en los sistemas para identificar incumplimientos.

Compliance Audit Report. En este módulo se generan informes detallados sobre los resultados de las auditorías de cumplimiento. Estos informes permiten documentar el estado actual de las auditorias, detectar áreas críticas y demostrar conformidad ante auditores.

Explicación Apartados Módulos Security Information. Primero esta NVTs (Network Vulnerability Tests), este módulo contiene la base de datos de pruebas de vulnerabilidades que OpenVas utiliza para detectar fallos en los activos. Cada NVT corresponde a una prueba específica diseñada para identificar una vulnerabilidad concreta en un sistema o servicio.

CVEs (Common Vulnerabilities and Exposures). Este apartado contiene la base de datos de vulnerabilidades públicas registradas bajo el estándar CVE. Cada CVE tiene un identificador único y proporciona información sobre una vulnerabilidad conocida, su impacto, así como información de posibles mitigaciones y remediaciones.

CPEs (Common Platform Enumerations). Este módulo proporciona una lista estándar de nombres para productos de software y hardware. Los CPEs permiten identificar con precisión qué versiones de sistemas o aplicaciones están presentes en un activo, lo que facilita la vinculación con vulnerabilidades específicas.

CERT-Bund Advisories. Este módulo contiene los avisos de seguridad emitidos por el CERT-Bund (Computer Emergency Response Team del gobierno alemán). Estos boletines incluyen información crítica sobre amenazas, vulnerabilidades y recomendaciones de mitigación y remediación.

DFN-CERT Advisories. Este módulo comparte los avisos emitidos por el DFN-CERT, otro equipo de respuesta ante emergencias informáticas, el cual está centrado en organizaciones

académicas y de investigación. Proporciona detalles técnicos sobre vulnerabilidades y consejos mitigación y remediación.

Explicación Apartados Módulos Configuration. El módulo de configuración de OpenVAS comparte varias opciones que permiten ajustar cómo realizan los análisis de vulnerabilidades. En “Targets” se definen los equipos o redes que serán evaluados, mientras que “Port Lists” se especifica qué puertos se analizarán, como por ejemplo todos los puertos TCP/UPD, los asignados por IANA o escaneo a puertos específicos.

En el módulo “Credentials” se pueden configurar credenciales seguras para realizar escaneos autenticados, y en “Scan Configs” se configuran los perfiles de los escaneos y pruebas que se aplicarán.

A través del módulo “Alerts” se pueden configurar notificaciones automáticas, y en “Schedules” se pueden programan los escaneos para ejecutarse en horarios específicos. Además, en los módulos de “Report Configs” y “Report Formats” se puede configurar la estructura y formato de los informes generados.

Por otro lado, en el módulo “Scanners” se puede gestionar los motores de análisis disponibles, en “Filters” se facilita la organización y visualización de resultados a través de filtros, y en “Tags” se puede clasificar los elementos mediante etiquetas de forma ordenada.

Explicación Apartados Módulos Administration. Finalmente, en el módulo de administración de OpenVAS se gestiona de forma centralizada el acceso, la seguridad y el rendimiento del sistema. Desde este apartado se gestionan los usuarios, grupos y permisos, garantizando que cada persona tenga el nivel de acceso adecuado. Además, permite supervisar el estado general de la plataforma, integrar servicios externos de autenticación y mantener un

control organizado sobre el funcionamiento y la actualización del sistema, asegurando una administración eficiente.

Delta. En OpenVAS, un Delta Report (o informe delta) es una función que permite comparar los resultados de dos escaneos de vulnerabilidades realizados sobre los mismos activos en diferentes momentos. Su objetivo es identificar los cambios en el estado de seguridad entre un escaneo anterior y uno más reciente, facilitando el seguimiento de la evolución de las vulnerabilidades en el tiempo.

El informe delta muestra las diferencias entre ambos resultados y clasifica los hallazgos en cuatro tipos principales:

Gone (Eliminada). La vulnerabilidad estaba presente en el informe anterior (más antiguo), pero ya no aparece en el nuevo. Esto indica que el problema fue corregido o dejó de detectarse en el activo.

New (Nueva). La vulnerabilidad aparece en el informe más reciente, pero no existía en el anterior. Representa un hallazgo nuevo que requiere análisis y posible remediación.

Same (Igual). La vulnerabilidad se encuentra en ambos informes y no presenta cambios. Su estado permanece igual entre los dos escaneos.

Changed (Modificada). La vulnerabilidad está presente en ambos informes, pero con alguna diferencia, como un cambio en su severidad, descripción o impacto. Esto puede reflejar una actualización en la base de datos de vulnerabilidades o un cambio en la configuración del activo.

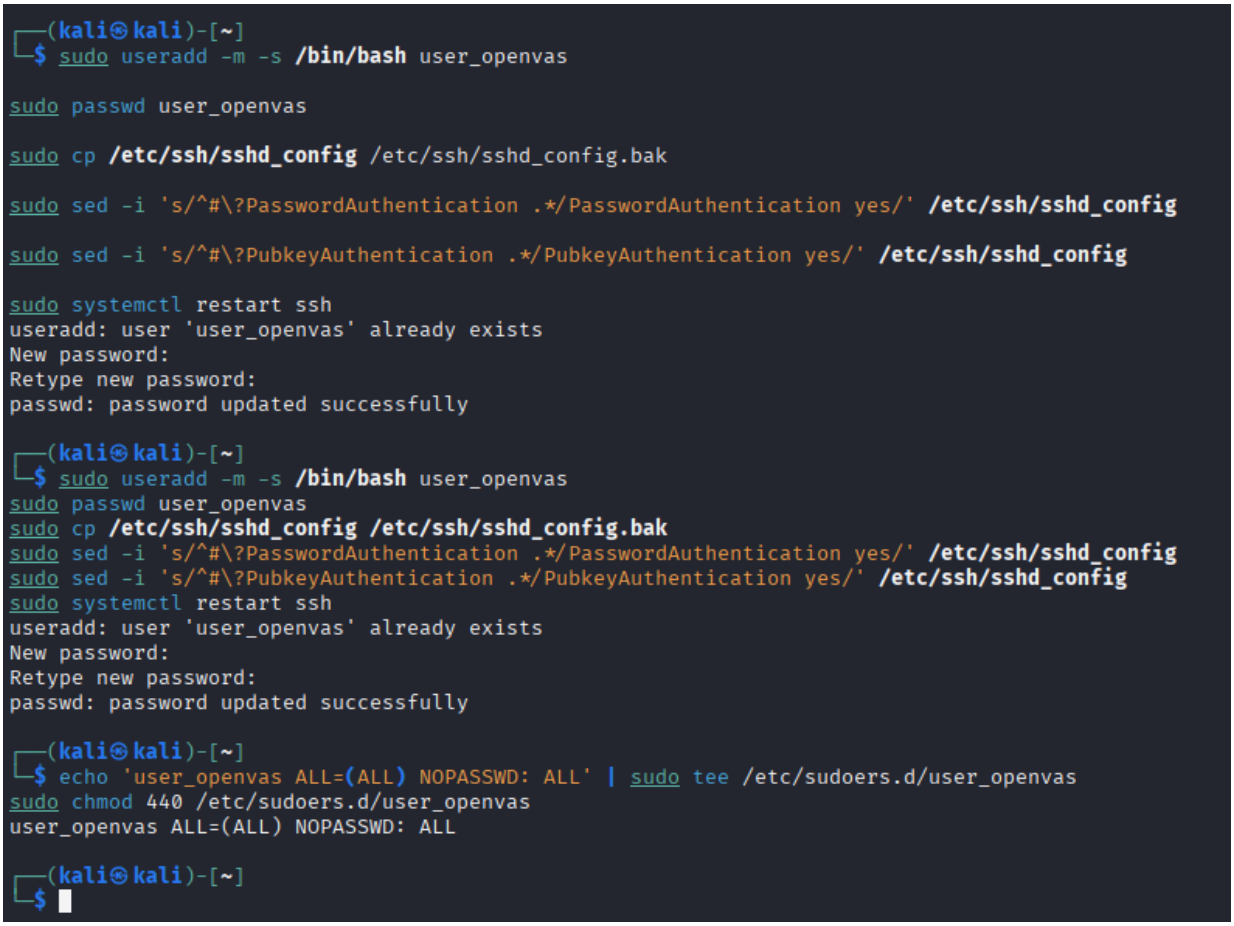
Pruebas Escaneos de Vulnerabilidades. Se realizaron dos tipos de pruebas con OpenVAS: un escaneo autenticado (con credenciales) y un escaneo no autenticado (sin credenciales). El primero permite que el escáner acceda al sistema con privilegios controlados, lo

que posibilita revisar configuraciones internas, parches, servicios y políticas de seguridad, ofreciendo una visión profunda del estado real del equipo. En cambio, el escaneo no autenticado se ejecuta sin credenciales, simulando el comportamiento de un atacante externo que solo puede observar los servicios expuestos en la red. Esta diferencia determina el alcance de cada análisis: mientras el escaneo autenticado identifica vulnerabilidades internas y de configuración, el no autenticado se enfoca en las debilidades visibles desde el exterior.

Se creó en la máquina objetivo una cuenta dedicada denominada *user_openvas* para uso exclusivo del escáner. En el servidor SSH del equipo se habilitó la autenticación mediante contraseña y se reinició el servicio para que los cambios surtieran efecto. Opcionalmente, se consideró la configuración de *sudo* sin petición de contraseña para ese usuario, únicamente en el entorno de laboratorio, con el fin de permitir comprobaciones que requieren privilegios sin interacción manual. En entornos reales, por seguridad no es recomendable otorgar permisos de *sudo* al usuario debido al riesgo de uso no autorizado, tal como se puede observar en la figura 6, donde se muestra la creación del usuario para el escaneo autenticado.

Figura 6

Creación Usuario Escaneo Autenticado



Nota. Elaboración propia mediante el uso de Kali Linux.

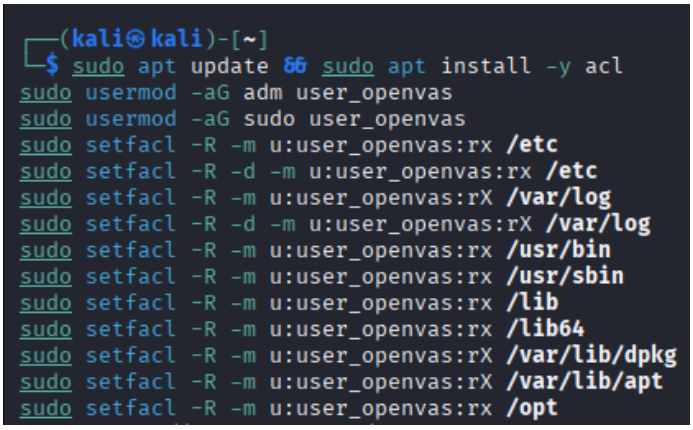
Se dio permisos de lectura y ejecución sobre rutas críticas del sistema como /etc, /var/log, /usr/bin, /usr/sbin, /lib, /lib64, /var/lib/dpkg, /var/lib/apt y /opt, con el fin de facilitar el análisis de configuraciones, registros y versiones de paquetes. Además, se integró al usuario en los grupos administrativos necesarios y, de forma opcional, se añadió una política limitada en sudoers que permite ejecutar ciertos comandos sin contraseña para evitar interrupciones durante las pruebas. Esta configuración busca equilibrar la funcionalidad requerida por el escáner de

vulnerabilidades con un control granular sobre los privilegios, asegurando un entorno seguro y eficiente para la recolección de información del sistema.

Se agregó el usuario a los grupos administrativos como prueba; sin embargo, en entornos reales no es recomendable otorgarle este tipo de permisos. Aunque implique un mayor esfuerzo, lo más adecuado es asignar permisos de lectura de manera granular sobre cada una de las rutas necesarias. Esto permite mantener un mejor control de seguridad, tal como se puede observar en la figura 7, donde se muestra la asignación de permisos al usuario de escaneo autenticado.

Figura 7

Asignación de Permisos Usuario Escaneo Autenticado

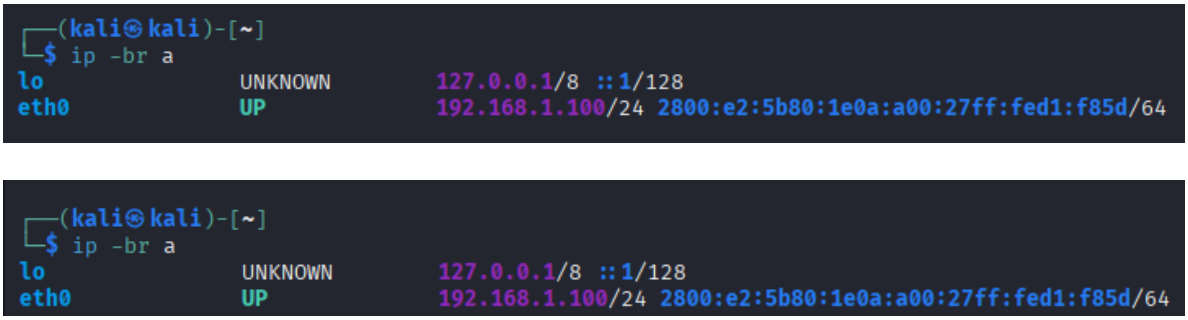


Nota. Elaboración propia mediante el uso de Kali Linux.

Para realizar los escaneos, las direcciones IP de la máquina de escaneo y de la máquina objetivo se configuraron en la misma subred, asegurando conectividad directa y evitando enrutamiento intermedio; esto permite ejecutar las pruebas de manera fiable entre ambos equipos, como se muestra en la figura 8, donde se presentan las direcciones IP de ambas máquinas.

Figura 8

Direcciones IP Maquina Escaneos y Maquina Objetivo

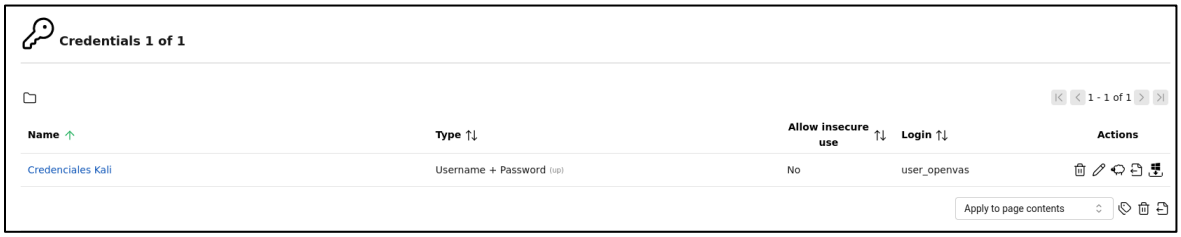


Nota. Elaboración propia mediante el uso de Kali Linux.

Se configuraron las credenciales necesarias en OpenVAS para permitir la ejecución de escaneos autenticados sobre la máquina objetivo, facilitando una evaluación más completa del sistema; en la figura 9 se muestra la evidencia de la configuración de las credenciales en la herramienta.

Figura 9

Evidencia Configuración Credenciales en Openvas

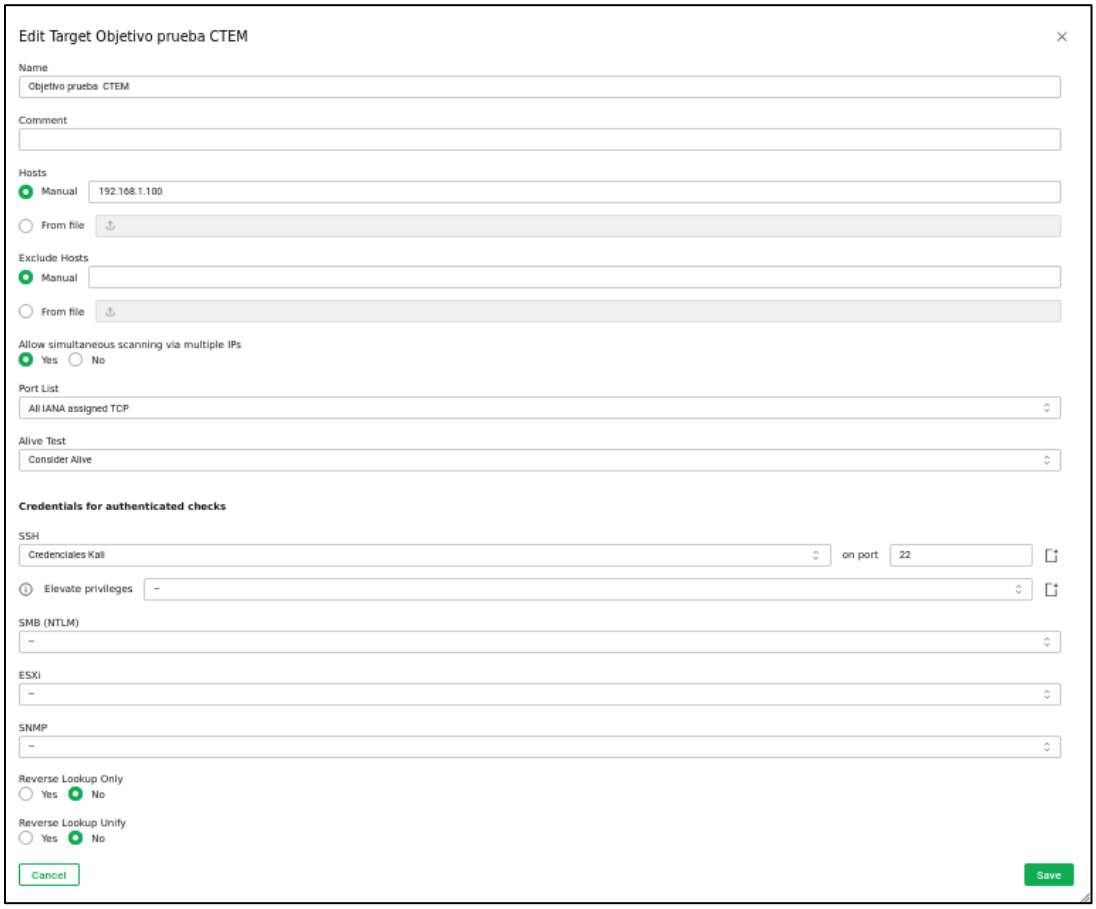


Nota. Elaboración propia mediante el uso de Kali Linux.

Se configuró la máquina objetivo en OpenVAS indicando la dirección IP, el tipo de escaneo y las credenciales necesarias para las pruebas autenticadas; en la figura 10 se observa el formulario de configuración con estos parámetros definidos.

Figura 10

Evidencia Configuración Maquina Objetivo en Openvas

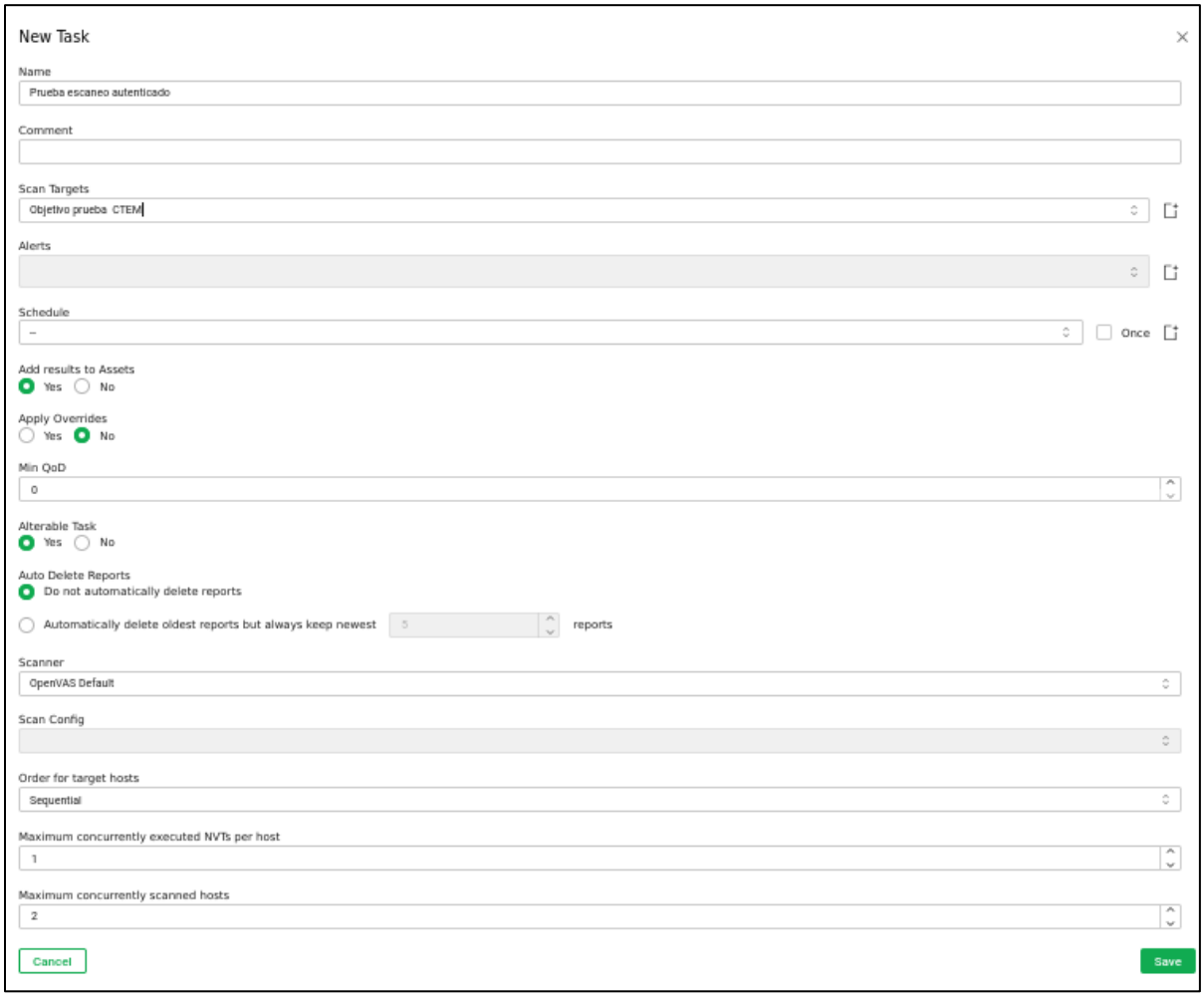


Nota. Elaboración propia mediante el uso de OpenVas.

Se configuró la tarea de escaneo de vulnerabilidades en OpenVAS, seleccionando el objetivo previamente definido y ajustando parámetros como el tipo de escaneo y la gestión de reportes; en la figura 11 se muestra la configuración de esta tarea dentro de la herramienta.

Figura 11

Evidencia Configuración Escaneo de Vulnerabilidades en Openvas

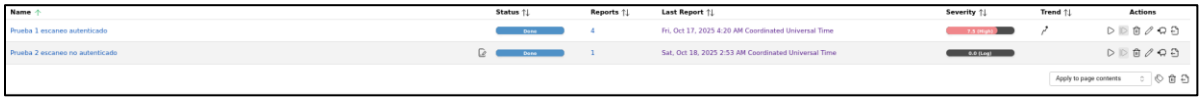


Nota. Elaboración propia mediante el uso de OpenVas.

Se configuraron dos tipos de escaneo en OpenVAS, uno autenticado y otro no autenticado, con el objetivo de comparar los resultados obtenidos en cada caso; en la figura 12 se muestra la evidencia de ambas configuraciones dentro de la herramienta.

Figura 12

Evidencia Configuración Escaneo Autenticado y no Autenticado



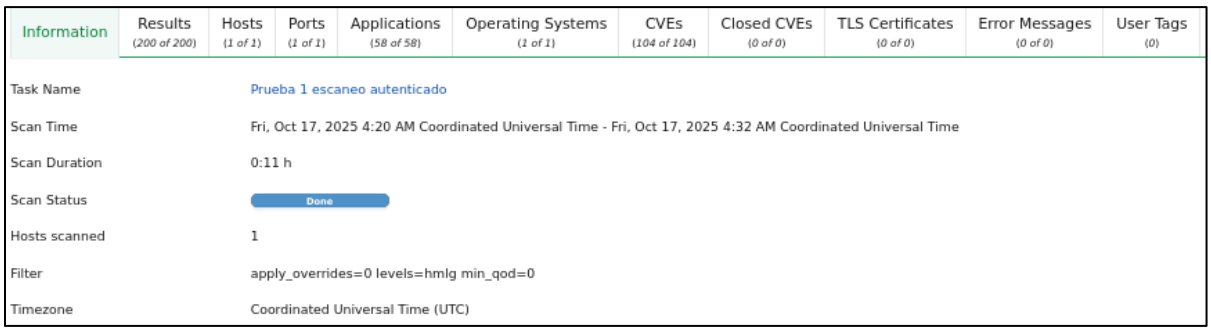
Nota. Elaboración propia mediante el uso de OpenVas.

Resultados Escaneo Autenticado

Una vez finalizado el escaneo autenticado realizado en OpenVAS, se obtuvieron resultados detallados sobre el estado de seguridad del host analizado. El reporte organiza la información en distintas secciones que permiten revisar los servicios activos, puertos abiertos, sistema operativo detectado, aplicaciones instaladas y las vulnerabilidades identificadas con su nivel de severidad. Esto facilita el análisis del entorno y la identificación de los puntos críticos que requieren atención prioritaria, como se muestra en la figura 13, donde se presenta la información general de los resultados del escaneo autenticado.

Figura 13

Información General Resultados Escaneo Autenticado

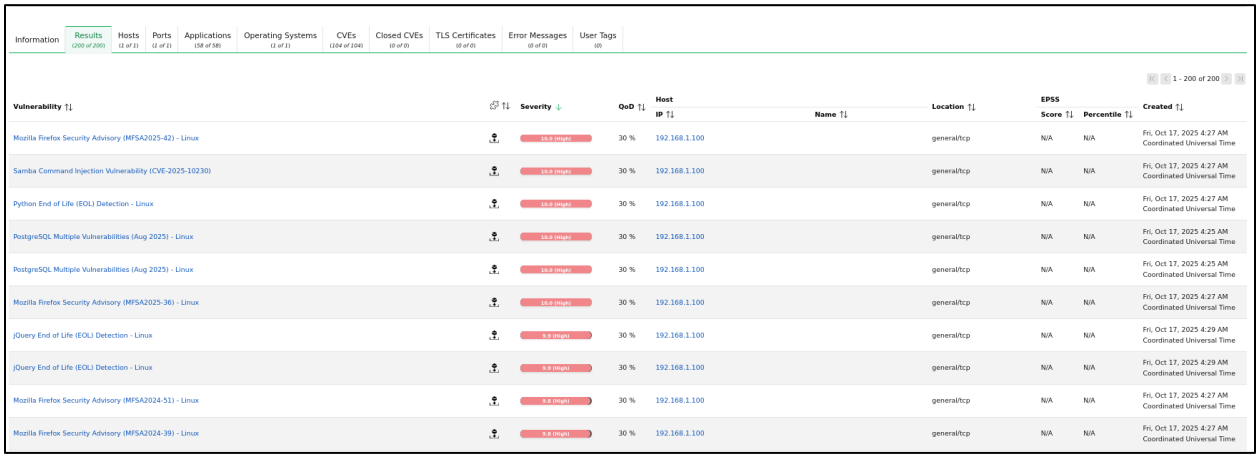


Nota. Elaboración propia mediante el uso de OpenVas.

Durante el escaneo autenticado realizado sobre el host 192.168.1.100, OpenVAS identificó un total de 200 vulnerabilidades activas. Estas se clasifican según su nivel de severidad y afectan a distintos componentes del sistema operativo Linux, servicios en ejecución y aplicaciones instaladas, como se muestra en la figura 14, donde se presentan los resultados del escaneo autenticado.

Figura 14

Resultados Escaneo Autenticado

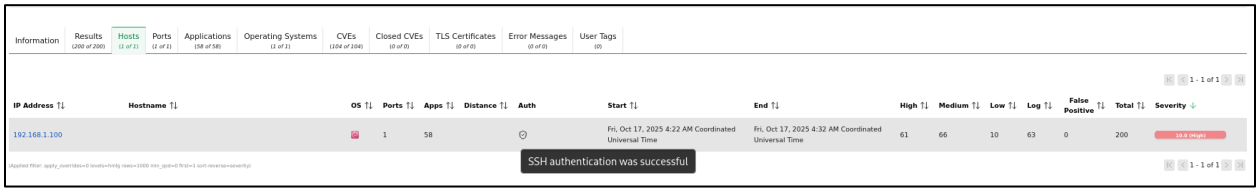


Nota. Elaboración propia mediante el uso de OpenVas.

En la figura 15, se muestra la pestaña Hosts del escaneo autenticado, donde se observa que se identificó un único equipo con dirección IP 192.168.1.100, correspondiente al sistema analizado. También se confirma que la autenticación SSH fue exitosa, lo que permitió obtener información más precisa.

Figura 15

Pestaña Hosts Escaneo Autenticado

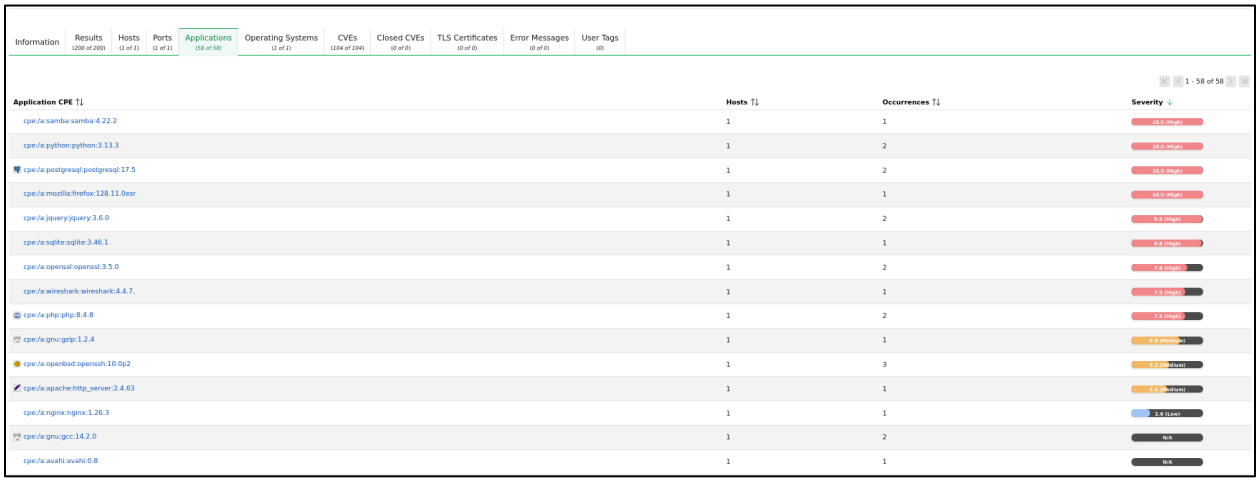


Nota. Elaboración propia mediante el uso de OpenVas.

En la figura 16 se muestra la pestaña Hosts y puertos del escaneo autenticado, donde se identificó un puerto activo y un total de 58 aplicaciones asociadas al sistema analizado.

Figura 16

Pestaña Hosts y Puertos Escaneo Autenticado



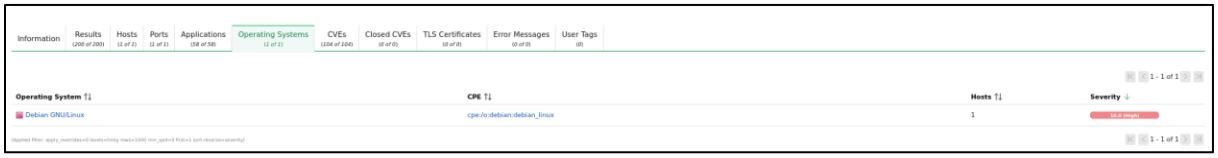
Nota. Elaboración propia mediante el uso de OpenVas.

La detección del sistema operativo en OpenVAS se realiza mediante un proceso de fingerprinting de red, que consiste en analizar las respuestas que el host objetivo envía ante distintos tipos de paquetes y peticiones. El escáner compara esas respuestas con una base de

datos de patrones conocidos (huellas digitales) para estimar qué sistema operativo está ejecutando la máquina. Esta técnica considera factores como los TTL, el tamaño de los paquetes, las opciones TCP/IP, los encabezados y los banners de servicios activos. En este caso, el escáner identificó el sistema como Debian GNU/Linux porque Kali Linux se basa en esa distribución, comparte su kernel y estructura de red, lo que hace que la huella coincida con la de Debian. Por esta razón, OpenVAS no diferencia entre distribuciones derivadas, sino que muestra el sistema base más cercano que puede confirmar con certeza, como se observa en la figura 17, donde se muestra la pestaña de sistema operativo del escaneo autenticado.

Figura 17

Pestaña Sistema Operativo Escaneo Autenticado



Nota. Elaboración propia mediante el uso de OpenVas.

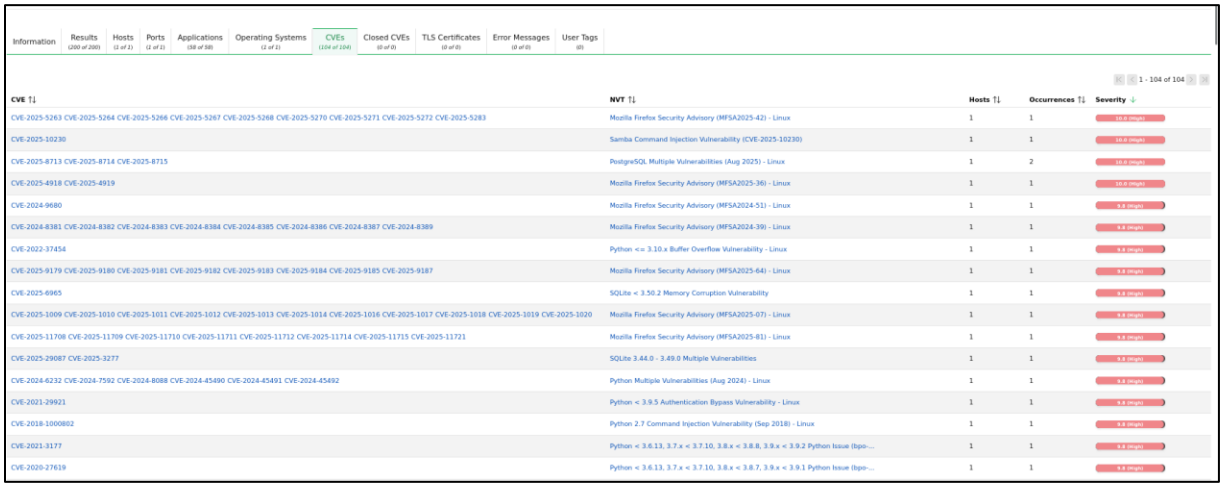
En la sección Common Vulnerabilities and Exposures (CVE) del informe, OpenVAS agrupa las vulnerabilidades detectadas según sus identificadores CVE, permitiendo visualizar de manera ordenada los fallos específicos asociados a cada software o componente del sistema. En este caso, se identificaron 104 CVE, los cuales se organizan junto con los NVTs correspondientes, que indican la prueba ejecutada para detectar esa vulnerabilidad. En la figura 18 se muestra esta sección del informe con el detalle de los CVE encontrados.

No se detectaron Closed CVEs, Transport Layer Security Certificates (TLS Certificates), Error Messages ni User Tags, todos con un valor de 0. Esto puede deberse a varios factores: en primer lugar, el sistema analizado no tiene CVE cerradas, ya que el escaneo fue de detección y no de

verificación de parches o remediaciones aplicadas. En segundo lugar, la ausencia de TLS Certificates indica que no se encontraron servicios Hypertext Transfer Protocol Secure (HTTPS) activos o certificados TLS configurados en el host evaluado. Por otro lado, no se generaron Error Messages durante el análisis, lo que sugiere que el escaneo se ejecutó correctamente sin fallos de conexión o autenticación.

Figura 18

Pestaña Sistema Operativo Escaneo Autenticado



Nota. Elaboración propia mediante el uso de OpenVas.

Estadísticas de los Resultados. En la figura 19 se muestra la descarga de los resultados del escaneo en formato CSV, donde se pueden observar de forma estructurada las estadísticas y campos generados por OpenVAS para cada vulnerabilidad detectada. IP: Dirección Internet Protocol (IP) del host objetivo (192.168.1.100).

Hostname. Domain Name System (DNS) del equipo cuando está disponible.

Port / Port Protocol. Puerto y protocolo donde se detectó la vulnerabilidad (si aplica).

CVSS. Puntuación CVSS de la vulnerabilidad (ej.: 10 indica máxima severidad).

Severity. Clasificación cualitativa derivada de CVSS (Low/Medium/High/Critical). En el ejemplo aparece **High**.

QoD (Quality of Detection). Índice que indica la confianza en la detección (valor mayor = mayor calidad/confianza.

Solution Type. Tipo de solución recomendada por el NVT (por ejemplo, VendorFix = actualización oficial del proveedor).

NVT Name. Nombre del test que encontró la vulnerabilidad.

Summary. Resumen corto del hallazgo.

Specific Result. Resultado detallado del chequeo en ese host: versión instalada, versión corregida, ruta de instalación/puerto, etc.

NVT OID. Network Vulnerability Test Object Identifier (NVT OID) es el identificador único del NVT en la base de datos (OID largo). Sirve para referenciar exactamente la prueba utilizada.

CVEs. Lista de identificadores CVE asociados a los hallazgos.

Task ID / Task Name. Identificador y nombre de la tarea/escaneo que generó ese resultado (Prueba 1 escaneo autenticado).

Timestamp. Fecha y hora en que se generó el hallazgo en horario UTC.

Result ID. Identificador único del resultado dentro del sistema el cual es útil para la trazabilidad consulta por Application Programming Interface (API).

Impact. campo para describir el impacto real/posible (en tu extracto aparece vacío en algunos registros); cuando está presente explica las consecuencias (confidencialidad, integridad, disponibilidad).

Solution. Texto con la acción recomendada (ej.: “Update to version 139” o instrucciones de parcheo).

Affected Software/OS. Producto y versión afectados según la detección (ej.: Mozilla Firefox versions prior to 139).

Vulnerability Insight. Explicación extendida de la vulnerabilidad, por ejemplo, cómo funciona, vectores de ataque y riesgos técnicos.

Vulnerability Detection Method. Modo en que se detectó. Indica si la detección fue por banner, comparación de paquetes, chequeo de versión vía Secure Shell (SSH), etc.

Product Detection Result. Resultado del intento de identificar el producto afectado. Confirma que OpenVAS reconoció el binario/paquete.

BIDs. Lista de identificadores Bugtraq (BIDs) relacionados con el hallazgo.

CERTs. Referencias a avisos/advisories de Computer Emergency Response Teams (CERTs) que documentan la vulnerabilidad.

Figura 19

Descarga Resultados en Formato CSV

IP	Hostname	Port	Port Protocol	CVSS	Severity	QoD	Solution Type	NVT Name	Summary	Specific Result
192.168.1.100				10	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2025-42) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.101				10	Critical	30	VendorFix	Samba Command Injection Vulnerability (CVE-2025-10230)	Samba is prone to a command injection vulnerability via WINS server hook script.	Installed version
192.168.1.102				10	Critical	30	VendorFix	Python End of Life (EOL) Detection - Linux	The Python version on the remote host has reached the end of life (EOL) and should not be us	The "Python" ver
192.168.1.103				10	Critical	30	VendorFix	PostgreSQL Multiple Vulnerabilities (Aug 2025) - Linux	PostgreSQL is prone to multiple vulnerabilities.	Installed version
192.168.1.104				10	Critical	30	VendorFix	PostgreSQL Multiple Vulnerabilities (Aug 2025) - Linux	PostgreSQL is prone to multiple vulnerabilities.	Installed version
192.168.1.105				10	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2025-36) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.106				9,9	Critical	30	VendorFix	jQuery End of Life (EOL) Detection - Linux	The jQuery version on the remote host has reached the end of life (EOL) and should not be us	The "jQuery" ver
192.168.1.107				9,9	Critical	30	VendorFix	jQuery End of Life (EOL) Detection - Linux	The jQuery version on the remote host has reached the end of life (EOL) and should not be us	The "jQuery" ver
192.168.1.108				9,8	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2024-51) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.109				9,8	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2024-39) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.110				9,8	Critical	30	VendorFix	Python <= 3.10.x Buffer Overflow Vulnerability - Linux	Python is prone to a buffer overflow vulnerability in the _sha3 module.	Installed version
192.168.1.111				9,8	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2025-64) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.112				9,8	Critical	30	VendorFix	SQLite < 3.50.2 Memory Corruption Vulnerability	SQLite is prone to a memory corruption vulnerability.	Installed version
192.168.1.113				9,8	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2025-07) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.114				9,8	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2025-81) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.115				9,8	Critical	30	VendorFix	SQLite 3.44.0 - 3.49.0 Multiple Vulnerabilities	SQLite is prone to multiple vulnerabilities.	Installed version
192.168.1.116				9,8	Critical	30	VendorFix	Python Multiple Vulnerabilities (Aug 2024) - Linux	Python is prone to an infinite loop vulnerability leading to a denial of service (DoS).	Installed version
192.168.1.117				9,8	Critical	30	VendorFix	Python < 3.9.5 Authentication Bypass Vulnerability - Linux	Python is prone to an authentication bypass vulnerability.	Installed version
192.168.1.118				9,8	Critical	30	VendorFix	Python 2.7 Command Injection Vulnerability (Sep 2018) - Linux	Python is prone to multiple vulnerabilities.	Installed version
192.168.1.119				9,8	Critical	30	VendorFix	Python < 3.6.13, 3.7.x < 3.7.10, 3.8.x < 3.8.8, 3.9.x < 3.9.2 Python Issue (bpo-42938) - Linux	Python is prone to a buffer overflow vulnerability in 'PyCArg_repr'.	Installed version
192.168.1.120				9,8	Critical	30	VendorFix	Python < 3.6.13, 3.7.x < 3.7.10, 3.8.x < 3.8.7, 3.9.x < 3.9.1 Python Issue (bpo-41944) - Linux	Python is prone to a remote code execution (RCE) vulnerability.	Installed version
192.168.1.121				9,7	Critical	30	VendorFix	Python Multiple Vulnerabilities (Jun 2025) - Linux	Python is prone to multiple vulnerabilities.	Installed version
192.168.1.122				9,7	Critical	30	VendorFix	Python Multiple Vulnerabilities (Jun 2025) - Linux	Python is prone to multiple vulnerabilities.	Installed version
192.168.1.123				9,7	Critical	30	VendorFix	Python Multiple Vulnerabilities (Jun 2025) - Linux	Python is prone to multiple vulnerabilities.	Installed version
192.168.1.124				9,6	Critical	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2024-33) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.125				8,8	High	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2024-55) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.126				7,8	High	30	VendorFix	Python DoS Vulnerability (Jul 2025) - Linux	Python is prone to a denial of service (DoS) vulnerability.	Installed version
192.168.1.127				7,8	High	30	VendorFix	Python Command Injection Vulnerability (Oct 2024) - Linux	Python is prone to a command injection vulnerability in the venv module.	Installed version
192.168.1.128				7,8	High	30	VendorFix	OpenSSL DoS Vulnerability (20250930, CVE-2025-9230) - Linux	OpenSSL is prone to a denial of service (DoS) vulnerability due to a out-of-bounds read & wri	Installed version
192.168.1.129				7,8	High	30	VendorFix	OpenSSL DoS Vulnerability (20250930, CVE-2025-9230) - Linux	OpenSSL is prone to a denial of service (DoS) vulnerability due to a out-of-bounds read & wri	Installed version
192.168.1.130				7,8	High	30	VendorFix	Python DoS Vulnerability (Jul 2025) - Linux	Python is prone to a denial of service (DoS) vulnerability.	Installed version
192.168.1.131				7,8	High	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2024-53) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version
192.168.1.132				7,8	High	30	VendorFix	Python DoS Vulnerability (Jul 2025) - Linux	Python is prone to a denial of service (DoS) vulnerability.	Installed version
192.168.1.133				7,6	High	30	VendorFix	Python Shell Command Injection Vulnerability (bpo-24778) - Linux	Python is prone to a shell command injection vulnerability in the mailcap module.	Installed version
192.168.1.134				7,5	High	30	VendorFix	Mozilla Firefox Security Advisory (MFSA2025-51) - Linux	The remote host is missing an update for Mozilla Firefox, announced via the advisory MFSA20	Installed version

Nota. Elaboración propia a partir de los resultados del escaneo con OpenVas.

Vulnerabilidades por Severidad. La tabla 1 muestra la distribución de vulnerabilidades detectadas según el sistema de puntuación CVSS v3.1, el cual clasifica el nivel de riesgo de cada vulnerabilidad en función de su impacto potencial sobre la confidencialidad, integridad y disponibilidad del sistema. En este caso, se observa que existen 63 vulnerabilidades con puntaje 0.0, catalogadas como “Log”, las cuales no representan riesgo directo, sino que son hallazgos informativos o de auditoría. En el rango 0.1–3.9 (Low) se identificaron 10 vulnerabilidades de bajo riesgo que no requieren atención inmediata. En el nivel medio (4.0–6.9) se concentran 66 vulnerabilidades, lo que sugiere una cantidad considerable de debilidades con impacto moderado que deben gestionarse para reducir exposición. El nivel alto (7.0–8.9) registra 36 vulnerabilidades, las cuales podrían ser explotadas con relativa facilidad y causar daños significativos si no se corrigen. Finalmente, el nivel crítico (9.0–10.0) presenta 25 vulnerabilidades, representando las amenazas más severas que requieren acción inmediata, ya que podrían comprometer totalmente los sistemas afectados. Esta distribución evidencia la necesidad de priorizar la mitigación comenzando por las vulnerabilidades críticas y altas, seguidas por las medias, con el fin de fortalecer la postura de seguridad del entorno evaluado.

Tabla 1

Vulnerabilidades por Severidad

Puntaje CVSS 3.1	Severidad	Total
0.0	Log	63
0.1 – 3.9	Low	10
4.0 – 6.9	Medium	66
7.0 – 8.9	High	36
9.0 – 10.0	Critical	25

Nota. La tabla presenta la distribución de vulnerabilidades identificadas según el puntaje CVSS v3.1, clasificadas por nivel de severidad (Log, Low, Medium, High y Critical) y su cantidad total de ocurrencias en el entorno evaluado.

Vulnerabilidades por QoD. El parámetro QoD indica el nivel de confianza que tiene OpenVAS respecto a la detección de una vulnerabilidad, expresado en porcentaje. En los resultados del escaneo se identificaron los siguientes valores: 97 %, 95 %, 80 %, 50 %, 30 % y 1 %, con una distribución de 200 vulnerabilidades en total.

Como se muestra en la tabla 2, el mayor número de vulnerabilidades se concentró en el QoD del 30 % (124 casos), seguido del 80 % (67 casos), lo que evidencia que la mayoría de los hallazgos provienen de verificaciones remotas o banner checks poco confiables, en las que OpenVAS identifica versiones de aplicaciones sin información precisa del nivel de parcheo. Este comportamiento es común en entornos donde las aplicaciones de código abierto no reportan versiones completas, por lo que se considera una detección potencialmente incierta o que requiere revisión manual.

En contraste, se registraron 2 vulnerabilidades con QoD del 97 % y 1 con QoD del 95 %,

asociadas a chequeos autenticados y verificaciones activas remotas en las que el sistema tuvo acceso al paquete o registro directamente, brindando una alta fiabilidad en la detección. Los valores intermedios, como 50 % (3 casos), reflejan detecciones remotas donde la respuesta pudo ser alterada por dispositivos intermedios (por ejemplo, firewalls), mientras que el 1 % (3 casos) corresponde a simples notas o advertencias generales sobre posibles vulnerabilidades sin confirmación de aplicación afectada.

En conclusión, las estadísticas de QoD reflejan que, aunque OpenVAS detectó un número considerable de vulnerabilidades, la confianza global de las detecciones es en su mayoría media-baja, debido al alto número de resultados con QoD ≤ 80 %, lo que implica la necesidad de validación manual o reescaneos autenticados para confirmar los hallazgos críticos.

Tabla 2

Vulnerabilidades por QoD (Quality of Detection)

QoD	Cantidad de vulnerabilidades
97	2
95	1
80	67
50	3
30	124
1	3

Nota. La tabla presenta la distribución de vulnerabilidades identificadas según el porcentaje de QoD (Quality of Detection), el cual indica el nivel de confianza en la detección realizada por OpenVAS, junto con la cantidad de vulnerabilidades asociadas a cada nivel.

Top de Productos Afectados. La tabla 3 refleja las principales vulnerabilidades detectadas en un único host, agrupadas por su nombre NVTs y el número de coincidencias encontradas por OpenVAS. Aunque todas las detecciones pertenecen al mismo sistema, se observa una alta concentración de fallos repetitivos asociados principalmente a Python, OpenSSH y jQuery, lo que indica múltiples instancias o componentes vulnerables dentro del mismo equipo. Las vulnerabilidades de Python (junio, julio y octubre de 2025) están relacionadas con fallos de denegación de servicio (DoS) y errores de gestión de memoria, mientras que las de jQuery (< 3.5.0) apuntan a riesgos de Cross-Site Scripting (XSS) que afectan a entornos web locales. Por su parte, las detecciones en OpenSSH y OpenBSD OpenSSH < 10.1 evidencian fallos de seguridad en el servicio de acceso remoto, potencialmente explotables para obtener información sensible o comprometer la sesión SSH. En conjunto, los resultados sugieren que el host presenta versiones desactualizadas de librerías críticas, lo cual incrementa su superficie de ataque y refuerza la necesidad de aplicar actualizaciones de seguridad y parches correctivos de manera inmediata.

Tabla 3

Top de Productos Afectados

NVT Name	# Vulnerabilidades
Python Multiple Vulnerabilities (Jun 2025) - Linux	3
Python DoS Vulnerability (Jul 2025) - Linux	3
jQuery 1.0.3 < 3.5.0 XSS Vulnerability	3
jQuery 1.2 < 3.5.0 XSS Vulnerability	3
jQuery < 3.4.0 Object Extensions Vulnerability	3
OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)	3
Python zipfile Module Vulnerability (Oct 2025) - Linux	3
Python DoS Vulnerability (Jun 2025) - Linux	3
Python Use After Free Vulnerability (May 2025) - Linux	3
OpenBSD OpenSSH < 10.1 Multiple Vulnerabilities	3

Nota. La tabla presenta las principales vulnerabilidades identificadas en el host analizado, agrupadas por nombre del NVT (Network Vulnerability Test) y el número de ocurrencias detectadas por OpenVAS para cada una.

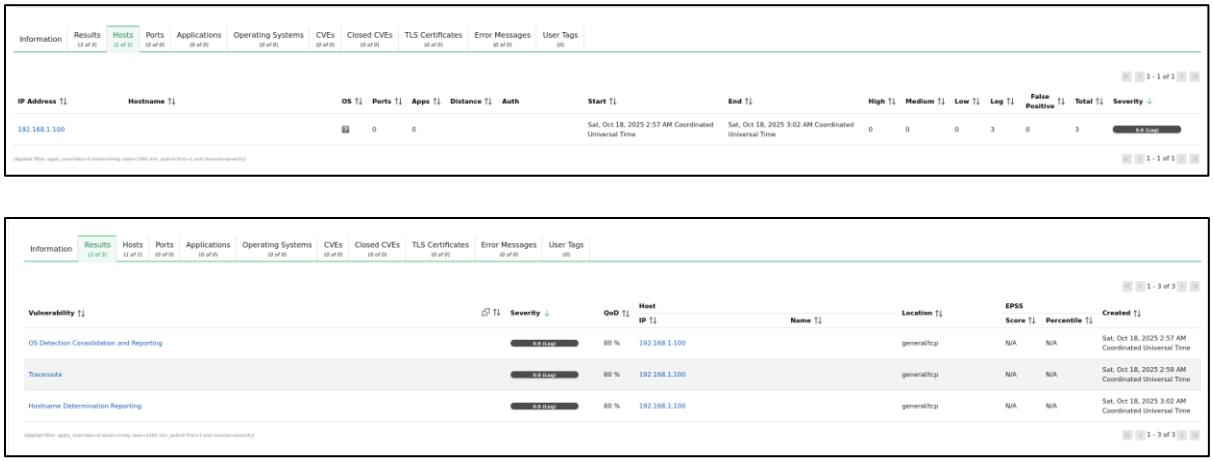
El escaneo autenticado realizado con OpenVAS permitió obtener una visión completa del estado de seguridad del sistema analizado, revelando vulnerabilidades tanto a nivel de servicios de red como de paquetes y aplicaciones instaladas. Al haberse ejecutado con credenciales válidas, OpenVAS tuvo acceso a información detallada del host, lo que posibilitó la detección de versiones específicas de software, librerías desactualizadas, configuraciones inseguras y fallos internos del sistema operativo que no podrían identificarse en un escaneo no autenticado. Este

tipo de análisis combina distintos métodos de detección, incluyendo comprobaciones remotas activas (servicios accesibles por red como SSH, HTTP, Server Message Block (SMB)), revisión de paquetes y registros del sistema (package-based y registry-based checks), y análisis de banners y versiones ejecutables. En conjunto, el escaneo autenticado proporciona un panorama más preciso y confiable de la postura de seguridad del host, permitiendo identificar vulnerabilidades reales con un mayor nivel de verificación (QoD alto) y facilitando la priorización de acciones correctivas basadas en la criticidad CVSS, la frecuencia de los fallos y el riesgo potencial de explotación dentro de la infraestructura analizada.

Prueba Escaneo no Autenticado. En el escaneo no autenticado, los resultados fueron limitados, ya que este tipo de análisis se basa únicamente en la información disponible de forma externa sin acceder al sistema operativo o a los paquetes instalados. En este caso, solo se identificaron tres detecciones relacionadas con el alcance del activo, las cuales corresponden principalmente a servicios o puertos visibles en la red. No se detectaron vulnerabilidades propiamente dichas en la máquina Linux, lo que indica que el host no expone servicios vulnerables de manera directa. En la figura 20 se puede observar este comportamiento, donde únicamente se muestran hallazgos superficiales asociados a la exposición en red. Esto es coherente con la naturaleza de los escaneos no autenticados, que suelen ofrecer una visión superficial y orientada al perímetro, sin capacidad de evaluar configuraciones internas ni versiones de software, por lo que sirven principalmente como punto de partida para identificar la exposición inicial de un sistema en la red.

Figura 20

Resultados Escaneo no Autenticado



Nota. Elaboración propia mediante el uso de OpenVAS.

Nuclei

Nuclei es una herramienta de escaneo de vulnerabilidades utilizada para evaluar aplicaciones modernas, infraestructuras, plataformas en la nube y redes en busca de fallos de seguridad aprovechables. Su funcionamiento se basa en el uso de plantillas (templates) escritas en archivos Ain't Markup Language (YAML), las cuales definen los métodos de detección y clasificación de vulnerabilidades específicas. Cada plantilla describe un posible vector de ataque, indicando el tipo de vulnerabilidad, su nivel de severidad, la prioridad de atención y, en algunos casos, los exploits asociados. Este enfoque basado en plantillas permite que Nuclei no solo detecte amenazas potenciales, sino que también identifique aquellas vulnerabilidades que pueden ser explotadas en escenarios reales, convirtiéndolo en una herramienta fundamental para auditores de seguridad y profesionales del análisis de vulnerabilidades (ProjectDiscovery, 2025).

Principales Características. Nuclei se distingue por ser una herramienta flexible, rápida y muy adaptable para el análisis de vulnerabilidades en aplicaciones, servicios y entornos modernos. Entre sus características más importantes destacan las siguientes:

Una de sus mayores ventajas es su amplia biblioteca de plantillas, desarrolladas por la comunidad y el equipo de ProjectDiscovery, que permiten detectar desde fallos comunes en aplicaciones web hasta configuraciones inseguras en servicios cloud o infraestructura. Gracias a esta base, el usuario puede ejecutar análisis muy específicos sin necesidad de crear scripts desde cero. Además, cuenta con una especificación de objetivo versátil, que admite URL, rangos de IP, dominios o archivos de entrada, facilitando la definición del alcance del escaneo de acuerdo con las necesidades del auditor o del entorno evaluado.

Otra característica esencial es su capacidad de escaneo masivo y paralelo, lo que le permite analizar múltiples objetivos simultáneamente, optimizando tiempo y recursos, especialmente en evaluaciones de gran escala. A esto se suma su personalización flexible, que brinda la posibilidad de modificar o crear plantillas para adaptarlas a controles de seguridad específicos o escenarios particulares.

Nuclei también destaca por su integración con pipelines de Continuous Integration and Continuous Delivery (CI/CD), lo que facilita la automatización de pruebas de seguridad en entornos de desarrollo continuo, detectando vulnerabilidades antes de desplegar nuevas versiones de software. Asimismo, permite integrarse con herramientas de gestión como Jira o Splunk, posibilitando la creación automática de tickets de remediación y seguimiento de vulnerabilidades.

En cuanto a los resultados, genera informes detallados en distintos formatos (JavaScript Object Notation (JSON), YAML, entre otros), incluyendo información sobre la vulnerabilidad,

su nivel de gravedad y recomendaciones de mitigación. Además, soporta autenticación mediante distintos métodos, el uso de variables dinámicas para escaneos parametrizados y la posibilidad de incrustar código personalizado dentro de las plantillas para realizar pruebas avanzadas. Finalmente, una de sus funciones más innovadoras es la generación de plantillas impulsada por inteligencia artificial, que permite crear nuevas pruebas de vulnerabilidad a partir de descripciones en lenguaje natural, agilizando el trabajo del analista y expandiendo constantemente las capacidades de la herramienta.

Escaneos Autenticados. Nuclei también que permite analizar aplicaciones o sistemas que requieren inicio de sesión para acceder a ciertas funcionalidades. En muchos casos, ejecutar un escaneo sin autenticación no basta, ya que las áreas protegidas por credenciales no pueden ser evaluadas, lo que indica que posibles vulnerabilidades dentro de esas zonas quedarían fuera del alcance del análisis.

Nuclei en la versión 3.2.0 introdujo una nueva configuración denominada Secret File, un archivo YAML que contiene la configuración necesaria para realizar la autenticación de forma automatizada. Esta configuración permite que Nuclei pueda iniciar sesión en los objetivos antes de realizar el escaneo, facilitando la detección de vulnerabilidades internas.

Nuclei puede realizar dos tipos de autenticación:

Autenticación Estática. En este tipo de autenticación se usa un secreto fijo, como una clave API o credenciales básicas, que rara vez cambia y sirve para validar directamente una sesión autenticada.

Autenticación Dinámica. En este tipo de autenticación el proceso es más complejo, dado que involucra varios secretos que se actualizan con frecuencia, como ocurre con Open Authorization (OAuth), Single Sign-On (SSO) o inicios de sesión mediante navegadores. En este

proceso, las credenciales iniciales se usan para obtener elementos temporales (por ejemplo, cookies o tokens) que mantienen la sesión activa.

Debido a la complejidad de esto, Nuclei facilita la creación de flujos de autenticación automatizados que pueden capturarse mediante un navegador y luego incorporarse al Secret File. Para asegurar la escalabilidad, el objetivo aprovecha la biblioteca de plantillas YAML de Nuclei, lo que permite crear, reutilizar y extender plantillas de inicio de sesión predeterminadas para distintos servicios o aplicaciones.

En cuanto al alcance de la autenticación, las credenciales o secretos solo se deben aplicar a los dominios que realmente los requieran. Para ello, el Secret File incluye los campos domains y domains-regex, que limitan el uso de cada secreto a un conjunto específico de objetivos, evitando filtraciones accidentales.

Finalmente, dado que el manejo seguro de credenciales es una prioridad, Nuclei no exige almacenar los secretos directamente dentro del archivo YAML y ofrece compatibilidad con sistemas externos de gestión de secretos. Actualmente, Project Discovery está desarrollando integraciones con herramientas como 1Password, HashiCorp Vault y Amazon Web Services (AWS) Secrets Manager, con el fin de fortalecer la seguridad y la administración de credenciales en los procesos de escaneo autenticado (ProjectDiscovery, 2025).

Laboratorio. Inicialmente se realiza la instalación de la última versión de Nuclei en Kali Linux, con el propósito de realizar pruebas automatizadas de vulnerabilidades en aplicaciones Web. En la figura 21 se aprecia el proceso de instalación de la herramienta dentro del entorno de trabajo.

Figura 21

Instalación de Nuclei

Nota. Elaboración propia mediante el uso de Kali Linux.

Se realiza la instalación de las plantillas, tal como se muestra en la figura 22, donde se evidencia el proceso correspondiente.

Figura 22

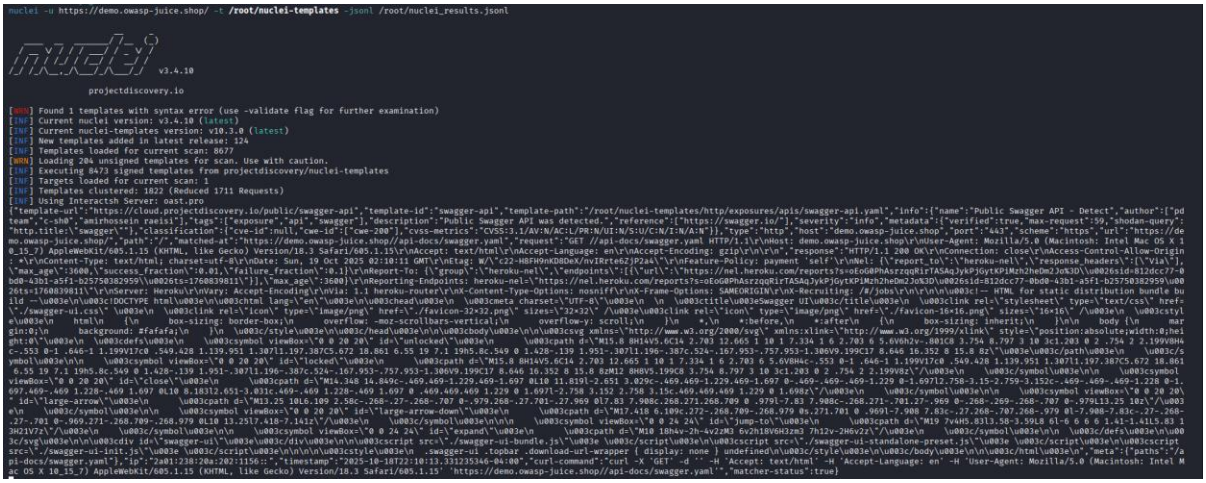
Instalación de Plantillas

Nota. Elaboración propia mediante el uso de la herramienta Nuclei.

Como primera prueba se realiza un escaneo a la URL hxxps[:]//demo[.]owasp-juice[.]shop/, una aplicación web vulnerable creada por Open Web Application Security Project (OWASP) para practicar técnicas de ethical hacking y testing de seguridad. En este caso se ilustra la ejecución del escaneo sobre el entorno de prueba, como se muestra en la figura 23.

Figura 23

Escaneo URL de Prueba de Owasp

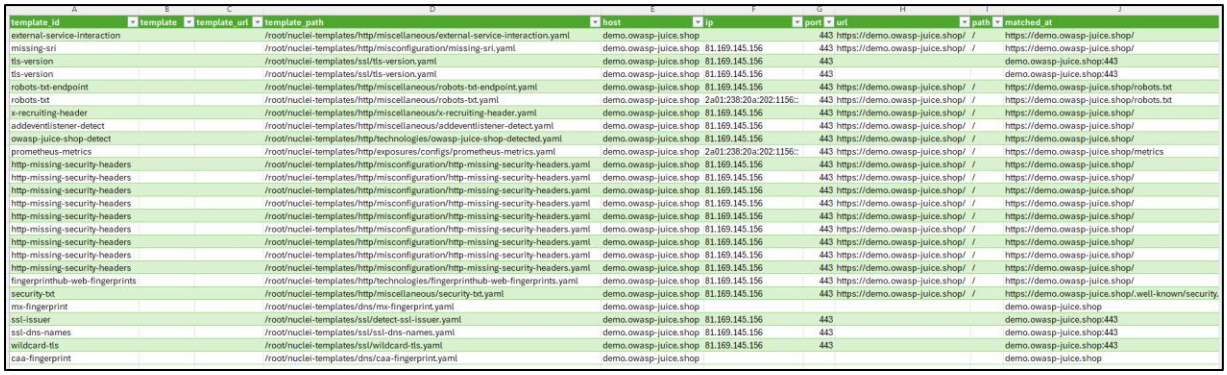


Nota. Elaboración propia mediante el uso de la herramienta Nuclei.

En general, los hallazgos muestran principalmente exposiciones informativas y debilidades de configuración, se identificaron endpoints y metadatos públicos (robots.txt, security.txt, prom métricas, fingerprints y cabeceras como X-Recruiting) y patrones que confirman la tecnología (OWASP Juice Shop), además de indicios de interacción con servicios externos y presencia de código sin SRI, a esto se suman varias advertencias sobre la postura TLS (versiones soportadas, emisor del certificado, Subject Alternative Name (SAN), uso de certificados comodín, registros Certification Authority Authorization (CAA) y huellas de Mail Exchange (MX). Aunque muchas detecciones son de tipo informativas, aportan contexto esencial para priorizar, como por ejemplo para corregir cabeceras de seguridad ausentes, restringir o proteger endpoints de métricas y callbacks, asegurar la integridad de recursos estáticos, endurecer la configuración TLS y revisar registros DNS, lo cual es esencial para reducir la superficie de ataque y permitir centrar esfuerzos en las debilidades importantes. Estos resultados quedan reflejados en la figura 24.

Figura 24

Resultados Escaneo URL de Prueba de Owasp



template_id	template	template_url	template_path	host	ip	port	url	path	matched_at
external-service-interaction			/root/nuclei-templates/http/miscellaneous/external-service-interaction.yaml	demo.owasp-juice.shop		443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
missing-sri			/root/nuclei-templates/http/misconfiguration/missing-sri.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
tls-version			/root/nuclei-templates/ssl/tls-version.yaml	demo.owasp-juice.shop	81.169.145.156	443			demo.owasp-juice.shop:443
tls-version			/root/nuclei-templates/ssl/tls-version.yaml	demo.owasp-juice.shop	81.169.145.156	443			demo.owasp-juice.shop:443
robots-txt-endpoint			/root/nuclei-templates/http/miscellaneous/robots-txt-endpoint.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/robots.txt
robots-txt			/root/nuclei-templates/http/miscellaneous/robots-txt.yaml	demo.owasp-juice.shop	2a01:238:20a:202:1156::	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/robots.txt
x-recruiting-header			/root/nuclei-templates/http/miscellaneous/x-recruiting-header.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
addeventlistener-detect			/root/nuclei-templates/http/miscellaneous/addeventlistener-detect.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
owasp-juice-shop-detect			/root/nuclei-templates/http/technologies/owasp-juice-shop-detected.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
prometheus-metrics			/root/nuclei-templates/http/exposures/configs/prometheus-metrics.yaml	demo.owasp-juice.shop	2a01:238:20a:202:1156::	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/metrics
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
http-missing-security-headers			/root/nuclei-templates/http/misconfiguration/http-missing-security-headers.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
fingerprinthub-web-fingerprints			/root/nuclei-templates/http/technologies/fingerprinthub-web-fingerprints.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/
security-txt			/root/nuclei-templates/http/miscellaneous/security-txt.yaml	demo.owasp-juice.shop	81.169.145.156	443	https://demo.owasp-juice.shop/	/	https://demo.owasp-juice.shop/.well-known/security.
mx-fingerprint			/root/nuclei-templates/dns/mx-fingerprint.yaml	demo.owasp-juice.shop					demo.owasp-juice.shop
ssl-issuer			/root/nuclei-templates/ssl/detect-ssl-issuer.yaml	demo.owasp-juice.shop	81.169.145.156	443			demo.owasp-juice.shop:443
ssl-dns-names			/root/nuclei-templates/ssl/ssl-dns-names.yaml	demo.owasp-juice.shop	81.169.145.156	443			demo.owasp-juice.shop:443
wildcard-tls			/root/nuclei-templates/ssl/wildcard-tls.yaml	demo.owasp-juice.shop	81.169.145.156	443			demo.owasp-juice.shop:443
caa-fingerprint			/root/nuclei-templates/dns/caa-fingerprint.yaml	demo.owasp-juice.shop					demo.owasp-juice.shop

Nota. Elaboración propia a partir de los resultados del escaneo con Nuclei.

***Estadísticas*.** En la tabla 4 se muestran los resultados del escaneo automático, los cuales fueron en su mayoría hallazgos informativos (25 debilidades) y un único hallazgo de severidad media (1 debilidad). En las detecciones se registraron, entre otros, los identificadores reportados: cwe-918; cwe-406 (info) y cwe-200 (medium y varias entradas info). Es importante destacar que un escaneo autenticado (realizado con secret keys, etc.) puede permitir un mejor alcance, tanto en endpoints internos, funcionalidades protegidas y fallos lógicos y, por tanto, ofrece una visión de riesgo más completa; sin embargo, dicho enfoque no es el objetivo principal de este trabajo de investigación para aplicaciones web, se tendrá como referencia para el objetivo número 3 para la evaluación de exposición y la definición de las medidas de priorización, mitigación, remediación y seguimiento.

Tabla 4

Debilidades por Severidad

Severidad	Debilidades
info	25
medium	1

*Nota***.** La tabla presenta la cantidad de debilidades identificadas en el escaneo automático, clasificadas según su nivel de severidad (info y medium), indicando el número de hallazgos registrados en cada categoría.

Como se puede observar en la tabla 5, en total se identificaron diez tipos de debilidades, siendo la más recurrente la ausencia de cabeceras de seguridad HTTP (9 debilidades), seguida por el uso de versiones inseguras de TLS (2 debilidades). Las demás detecciones, como interacciones con servicios externos, falta de integridad en recursos (SRI), presencia de archivos robots.txt, cabeceras informativas, endpoints de métricas o aplicaciones de prueba, aparecieron solo una vez cada una. En general, los hallazgos reflejan configuraciones deficientes y prácticas de seguridad básicas no implementadas, más que vulnerabilidades críticas, lo que sugiere oportunidades de fortalecimiento preventivo en la gestión y configuración del entorno web.

Tabla 5

Top 10 de Debilidades

Debilidad	Número
http-missing-security-headers	9
tls-version	2
external-service-interaction	1
missing-sri	1
robots-txt-endpoint	1
robots-txt	1
x-recruiting-header	1
addeventlistener-detect	1
owasp-juice-shop-detect	1
prometheus-metrics	1

*Nota***.** La tabla presenta las principales debilidades identificadas en el escaneo, clasificadas por tipo de vulnerabilidad o mala configuración y el número de ocurrencias detectadas para cada una en el entorno evaluado.

Qualys VMDR

Vulnerability Management, Detection, and Response (VMDR) de Qualys es una solución que permite gestionar la seguridad de la infraestructura tecnológica de las organizaciones desde una sola plataforma. Está diseñada para descubrir, evaluar, priorizar y remediar vulnerabilidades en tiempo real, cubriendo entornos híbridos, globales, remotos o incluso dispositivos del Internet de las Cosas (IoT). Su objetivo es ofrecer una visión completa del riesgo cibernético y reducirlo

de manera progresiva mediante procesos automatizados y centralizados.

La implementación de VMDR comienza con la identificación y el inventario de activos, garantizando que todos los dispositivos y sistemas conectados, incluidos aquellos no gestionados que aparecen en la red, sean detectados y registrados. Utiliza el Qualys Query Language (QQL) para generar inventarios detallados de hardware, software, etiquetas y configuraciones, facilitando el control y la visibilidad del entorno. A partir de esa información, la herramienta realiza un análisis de vulnerabilidades basado en factores de riesgo reales (TruRisk), proporcionando una visión consolidada y priorizada de las amenazas mediante Qualys Insights, que integra datos de inteligencia y contexto de negocio.

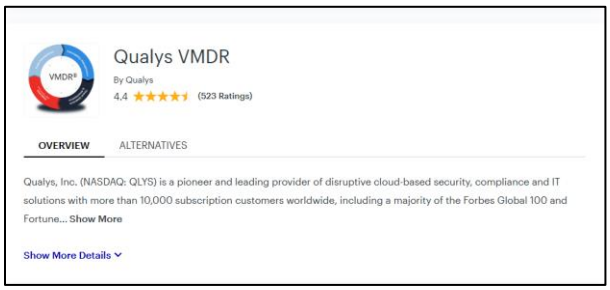
Entre sus principales beneficios se destaca la capacidad de descubrir y monitorear continuamente todos los activos, mantener un inventario preciso y dinámico, y priorizar las vulnerabilidades críticas según su impacto potencial y exposición real. Además, el sistema permite remediar los riesgos de manera automatizada, mejorando la respuesta ante amenazas y fortaleciendo la postura de seguridad general de la organización. En esencia, VMDR convierte la gestión de vulnerabilidades en un proceso continuo y estratégico, donde la detección y respuesta son parte de un mismo flujo de protección integral (Qualys Inc, 2025).

También cabe destacar que Qualys se encuentra dentro del top 10 de los mejores escáneres de vulnerabilidades, según el Cuadrante Mágico de Gartner para Vulnerability Assessment. Este reconocimiento refleja su posición consolidada en el mercado como una de las soluciones más completas y confiables para la gestión continua de vulnerabilidades, gracias a su capacidad de integración, su enfoque automatizado en la detección y respuesta, y su amplia adopción en entornos corporativos de alta demanda (Gartner, 2025). En la figura 25 se presenta el cuadrante de evaluación de soluciones de Vulnerability Assessment según Gartner Peer

Insights, donde se ubica la herramienta dentro del análisis comparativo del mercado.

Figura 25

Cuadrante de Evaluación de Soluciones de VM



Nota. Puntuación Gartner Qualys VMDR. Tomado de. Vulnerability Assessment Reviews and Ratings, Gartner. (2025) https://www.gartner.com/reviews/market/vulnerability-assessment

Explicación de los Principales Paneles de Qualys. El primero se llama Asset Criticality Score (ACS), muestra la puntuación de criticidad de los activos, que va de 1 a 5. Se basa en las etiquetas asignadas a cada activo y ayuda a identificar cuáles son más importantes o sensibles dentro de la organización (Qualys Inc, 2025).

Panel. Es la vista principal donde se presenta, de forma gráfica y resumida, la información sobre vulnerabilidades, activos y otros datos. Desde allí se pueden realizar acciones como imprimir, generar reportes o revisar versiones anteriores del panel.

Qualys Detection Score (QDS). Representa la puntuación de detección de vulnerabilidades, calculada por Qualys. Esta va del 1 al 100 y se clasifica en cuatro niveles: Crítico (90-100), Alto (70-89), Medio (40-69) y Bajo (1-39). Es una referencia clave para priorizar qué vulnerabilidades atender primero.

Qualys ID (QID). Es un identificador único que Qualys asigna a cada vulnerabilidad detectada. Sirve para buscarla o referenciarla fácilmente dentro del sistema.

Qualys Query Language (QQL). Es el lenguaje de consulta que permite buscar información específica dentro de la base de datos de Qualys. Las búsquedas se hacen mediante atributos llamados tokens, que ayudan a filtrar resultados de manera precisa.

Etiquetas (Tags). Son una forma flexible de organizar y clasificar los activos. Permiten agruparlos por características comunes como ubicación, tipo de dispositivo o área de negocio, facilitando su gestión y análisis.

TruRisk Score. Es una métrica que combina la criticidad del activo y la severidad de las vulnerabilidades para determinar el nivel de riesgo real. Este puntaje permite enfocar los esfuerzos de mitigación en los sistemas que representan una mayor amenaza para la organización.

Widgets. Son los elementos visuales que componen los paneles. Pueden mostrar información en distintos formatos, como números, gráficos de barras, tablas o indicadores de riesgo. Los widgets se pueden personalizar o añadir a paneles existentes según las necesidades del análisis.

Gestión de Activos. Durante la fase de gestión de activos, se lleva a cabo la identificación y el registro completo de todos los elementos tecnológicos que forman parte del entorno de la organización. Este proceso permite construir un inventario preciso y dinámico que refleja, en tiempo real, qué recursos existen, dónde se encuentran y cuál es su estado actual.

La detección de activos se realiza principalmente mediante los agentes en la nube (Cloud Agents), que recopilan información directamente desde los dispositivos, sistemas o entornos donde están instalados. También es posible ampliar la cobertura actualizando los agentes existentes para incluirlos dentro del alcance de VMDR.

En este punto, los activos se clasifican mediante etiquetas que facilitan su organización según distintos criterios, como tipo de equipo, ubicación, criticidad o área de negocio. Además, se recopilan datos técnicos detallados sobre cada activo, incluyendo los servicios en ejecución, software instalado y configuraciones relevantes, lo que permite mantener una visión actualizada de toda la infraestructura.

Gestión de Vulnerabilidades. En la fase de gestión de vulnerabilidades, el objetivo principal es identificar las debilidades de seguridad presentes en los activos de la organización y detectar configuraciones incorrectas que puedan representar un riesgo. Esta etapa permite conocer el nivel real de exposición y establecer prioridades para la corrección o mitigación de los hallazgos.

Dentro de la plataforma VMDR de Qualys, la pestaña Vulnerabilidades ofrece una vista integral del estado de seguridad de los sistemas, mostrando los activos afectados, el tipo de vulnerabilidades detectadas, su nivel de severidad y otros indicadores relevantes.

En esta fase, Qualys Insights complementa el análisis aportando información contextual sobre cada vulnerabilidad, como su relación con malware conocido, la existencia de exploits o la probabilidad de ser aprovechada por un atacante. Gracias a esto, los equipos de seguridad pueden enfocar sus esfuerzos en los riesgos más críticos en lugar de tratar todas las detecciones por igual.

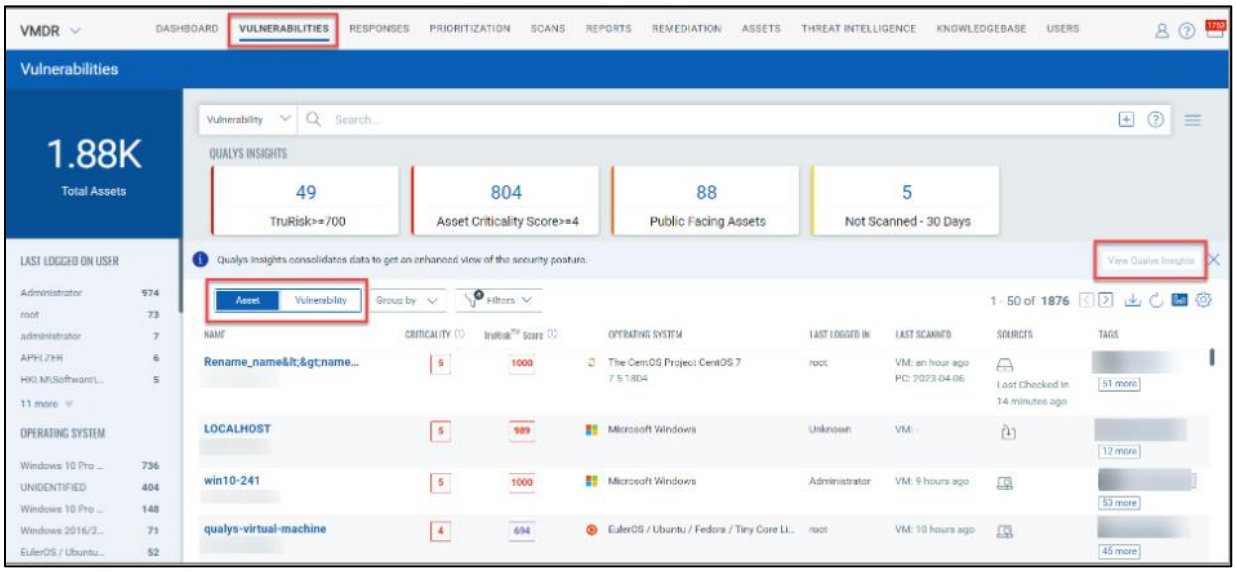
Desde el panel principal de la plataforma, se puede acceder a la aplicación VMDR y seleccionar la opción Vulnerabilidades para consultar los listados detallados de vulnerabilidades y los activos en los que se encuentran. Además, este módulo permite gestionar las acciones de remediación, realizar seguimientos del avance y generar reportes personalizados.

En la figura 26 se presenta la interfaz de la solución Vulnerability Management,

Detection & Response de Qualys, donde se observa la organización del panel principal y el acceso a las distintas funciones del módulo.

Figura 26

Interfaz de la Solución VMDR de Qualys



Nota. Puntuación Gartner Qualys VMDR. Tomado de. Vulnerability Assessment Reviews and Ratings, Gartner. (2025) https://www.gartner.com/reviews/market/vulnerability-assessment

Detección y Priorización de Amenazas. Durante la fase de priorización, VMDR analiza los indicadores de amenaza y determina qué vulnerabilidades representan el mayor riesgo para la organización. Esta etapa permite enfocar los esfuerzos de mitigación en los puntos más críticos, optimizando el uso de recursos y reduciendo el tiempo de exposición.

Para realizar esta priorización, la plataforma ofrece distintos métodos de evaluación, como la antigüedad de la vulnerabilidad (Age), la información de amenazas en tiempo real (RTI – Real-Time Threat Indicators) y el análisis de la superficie de ataque. También puede utilizarse el modo Qualys TruRisk, que combina la criticidad del activo con la severidad y el contexto de la

vulnerabilidad para ofrecer una visión más completa del riesgo real.

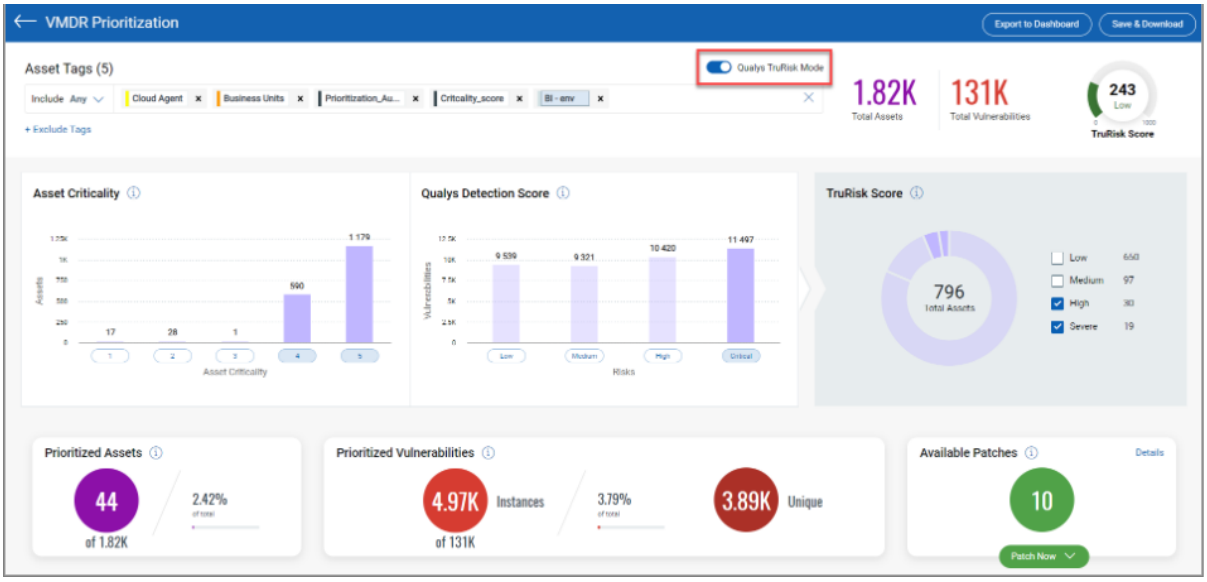
Dependiendo del método seleccionado, el sistema genera un informe de priorización que detalla los activos más importantes, las vulnerabilidades que deben atenderse con mayor urgencia y los parches disponibles para su corrección. Este reporte facilita la toma de decisiones y agiliza las tareas de remediación.

El informe puede guardarse, descargarse o exportarse directamente al panel principal para su seguimiento o análisis posterior.

En la figura 27 se presenta la interfaz del módulo de priorización dentro de la solución Vulnerability Management, Detection & Response de Qualys, donde se observa las estadísticas de las vulnerabilidades priorizadas.

Figura 27

Interfaz de la Solución VMDR de Qualys



Nota. Puntuación Gartner Qualys VMDR. Tomado de. Vulnerability Assessment Reviews and Ratings, Gartner. (2025) https://www.gartner.com/reviews/market/vulnerability-assessment

Respuesta. En la fase de respuesta, VMDR orienta sus acciones hacia la aplicación de medidas correctivas frente a las amenazas detectadas y priorizadas en las fases anteriores. El propósito de esta etapa es mitigar el riesgo mediante actividades como la instalación de parches de seguridad, la renovación de certificados digitales o el ajuste de configuraciones vulnerables en los sistemas afectados.

A partir del informe de priorización obtenido en la etapa previa, los administradores pueden implementar los parches correspondientes en equipos con Windows, Linux o macOS, según la criticidad y el impacto de cada vulnerabilidad. Este informe se organiza en dos partes principales: Resumen y Detalles, que facilitan el seguimiento del proceso de remediación.

Ofrece una visión general del estado de la respuesta, incluyendo los siguientes indicadores:

Activos Priorizados. Número de equipos que cumplen con las condiciones de las técnicas de remediación seleccionadas en la fase de detección y priorización.

Vulnerabilidades Priorizadas. Cantidad de vulnerabilidades encontradas en los activos seleccionados.

Instancias. Total de vulnerabilidades que coinciden con los criterios establecidos para la remediación.

Vulnerabilidades Únicas. Número de vulnerabilidades individuales, sin contar las repeticiones de identificadores QID.

Parches Disponibles. Muestra el total de actualizaciones detectadas por Qualys que permiten corregir las vulnerabilidades identificadas. La plataforma ofrece parches automáticos (Zero-Touch) o manuales para Windows, Linux y Mac.

Además, desde la opción “Parchear ahora”, es posible visualizar los parches pendientes y proceder con su instalación directa en los sistemas correspondientes.

Estados de las Vulnerabilidades. En Qualys VMDR, cada vulnerabilidad detectada pasa por distintos estados dentro del ciclo de gestión. Estos estados permiten dar seguimiento al proceso de detección, corrección y verificación de manera estructurada (Qualys, s.f). A continuación, se explican los estados:

New (Nueva). Este estado indica que la vulnerabilidad ha sido detectada por primera vez en un activo. No existía registro previo de ella en escaneos anteriores, por lo que se considera una detección reciente que aún no ha sido revisada ni tratada por el equipo de seguridad.

Active (Activa). Significa que la vulnerabilidad ya fue identificada con anterioridad y continúa presente en el activo. No se ha aplicado una corrección o la verificación más reciente confirmó que el fallo persiste. En este estado, la vulnerabilidad sigue representando un riesgo y requiere atención.

Reopened (Reabierta). Una vulnerabilidad pasa a este estado cuando se consideraba corregida, pero tras un nuevo análisis o escaneo vuelve a detectarse en el mismo activo. Esto puede ocurrir por una remediación incompleta, una actualización fallida o la reinstalación de software vulnerable.

Fixed (Corregida). Este estado indica que la vulnerabilidad ha sido solucionada. El sistema ha verificado, mediante un nuevo escaneo o evaluación, que el fallo ya no está presente en el activo. La corrección puede haberse logrado mediante la instalación de un parche, la actualización del software o un cambio en la configuración.

Acunetix Web Vulnerability Scanner

Acunetix es una herramienta orientada a la evaluación de seguridad en aplicaciones web que permite identificar vulnerabilidades presentes en sitios y servicios accesibles a través de HTTP o HTTPS. Su funcionamiento se basa en realizar un análisis automatizado del sitio web para detectar fallos de seguridad comunes, como inyección Structured Query Language (SQL), XSS y otros problemas que podrían ser aprovechados por un atacante para comprometer la aplicación.

La herramienta está diseñada para analizar tanto aplicaciones web tradicionales como desarrollos más modernos que utilizan tecnologías como JavaScript o Asynchronous JavaScript and XML (AJAX). Para lograrlo, utiliza un mecanismo de rastreo que explora la estructura del sitio web y localiza páginas, archivos y puntos de entrada dentro de la aplicación. A partir de esta

exploración, Acunetix ejecuta diferentes pruebas de seguridad con el objetivo de identificar vulnerabilidades que puedan afectar la confidencialidad, integridad o disponibilidad de la información (Invicti Security, 2024).

Funcionamiento del Análisis en Acunetix. El proceso de análisis en Acunetix comienza identificando la estructura del sitio web. La herramienta navega automáticamente por las páginas de la aplicación para descubrir enlaces, secciones y recursos disponibles. Durante esta etapa también puede detectar enlaces generados mediante tecnologías dinámicas como JavaScript, así como rutas descritas en archivos como sitemap.xml o robots.txt. Con esta información se construye un mapa de la aplicación que posteriormente se utiliza como base para realizar las pruebas de seguridad.

Después de completar esta exploración, el sistema inicia la fase de evaluación de vulnerabilidades. En esta etapa se envían diferentes tipos de solicitudes a los formularios, parámetros y puntos de entrada de la aplicación con el objetivo de comprobar cómo responde el sistema ante distintos tipos de datos. Este proceso permite identificar vulnerabilidades comunes en aplicaciones web, como fallos de validación de entrada, problemas de configuración o errores que podrían ser explotados por un atacante.

Los resultados del análisis se presentan en un panel donde se muestran las vulnerabilidades detectadas junto con información técnica relevante. Dependiendo del tipo de análisis realizado, la herramienta también puede proporcionar detalles adicionales que ayudan a comprender el origen del problema y orientar el proceso de corrección.

Tecnología AcuSensor. Una de las características que incorpora Acunetix es la tecnología AcuSensor, la cual permite mejorar la precisión de los análisis. Este mecanismo combina el escaneo externo de la aplicación con información obtenida directamente desde el

entorno donde se ejecuta el software. Gracias a esta integración, el sistema puede identificar vulnerabilidades con mayor exactitud y reducir la probabilidad de falsos positivos.

Cuando esta tecnología se encuentra habilitada, el análisis puede incluir información adicional como la ubicación aproximada del problema dentro del código o detalles sobre cómo se genera la vulnerabilidad durante la ejecución de la aplicación. Esto facilita el proceso de corrección para los equipos de desarrollo.

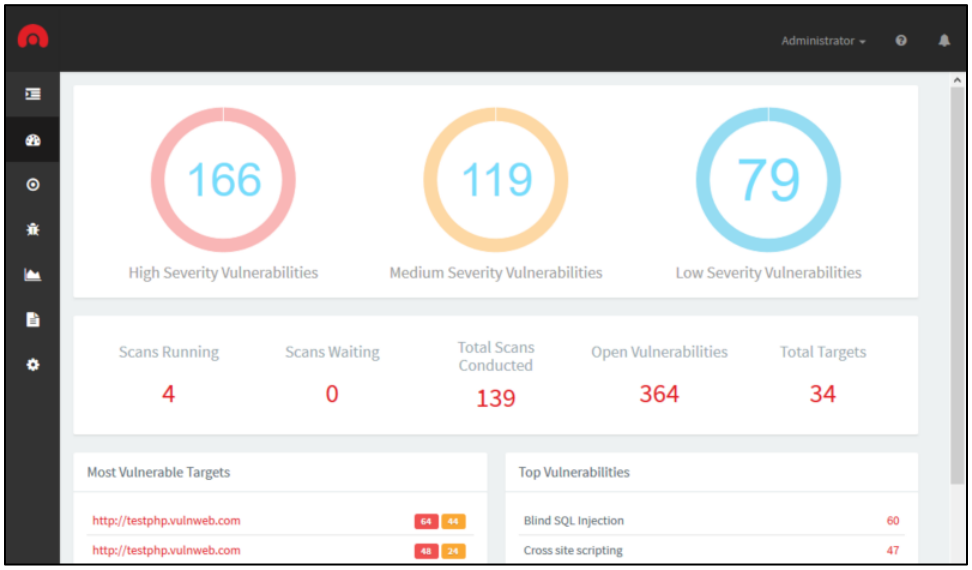
Evaluación Adicional del Entorno. Además del análisis de la aplicación web, algunas versiones de la herramienta también permiten realizar verificaciones básicas sobre el servidor donde se encuentra alojado el sitio. Estas comprobaciones buscan identificar servicios activos, configuraciones inseguras o el uso de protocolos que podrían representar un riesgo para la seguridad del sistema. De esta manera, el análisis no se limita únicamente a la aplicación, sino que también considera aspectos del entorno donde esta se ejecuta.

Dashboards. Acunetix cuenta con dashboards principales, donde se visualizan métricas como el número de vulnerabilidades detectadas por severidad, sitios o aplicaciones web escaneadas**, t**endencias de vulnerabilidades en el tiempo y estado de los escaneos realizados.

El panel de visualización de vulnerabilidades de Acunetix permite consolidar esta información en una vista centralizada, facilitando el seguimiento del estado general de seguridad de las aplicaciones analizadas. Desde este espacio también se pueden observar indicadores globales del entorno evaluado, lo que ayuda a contextualizar los hallazgos más allá de cada escaneo individual. En la figura 28 se presenta este dashboard principal, donde se aprecia la distribución de vulnerabilidades, los activos evaluados y las métricas generales que resumen la actividad de la herramienta.

Figura 28

Panel de Visualización de Vulnerabilidades en la Herramienta Acunetix



Nota. Panel principal de Acunetix. Tomado de. Introduction to the Dashboards, Acunetix. (2024) https://www.acunetix.com/support/docs/a360/getting-started/introduction-to-the-dashboards/

El panel principal comparte un resumen del estado de seguridad de los objetivos analizados, mostrando información agregada mediante gráficos y widgets interactivos.

Además, la plataforma incluye distintos paneles especializados:

Global Dashboard. Vista general del estado de seguridad de todas las aplicaciones analizadas.

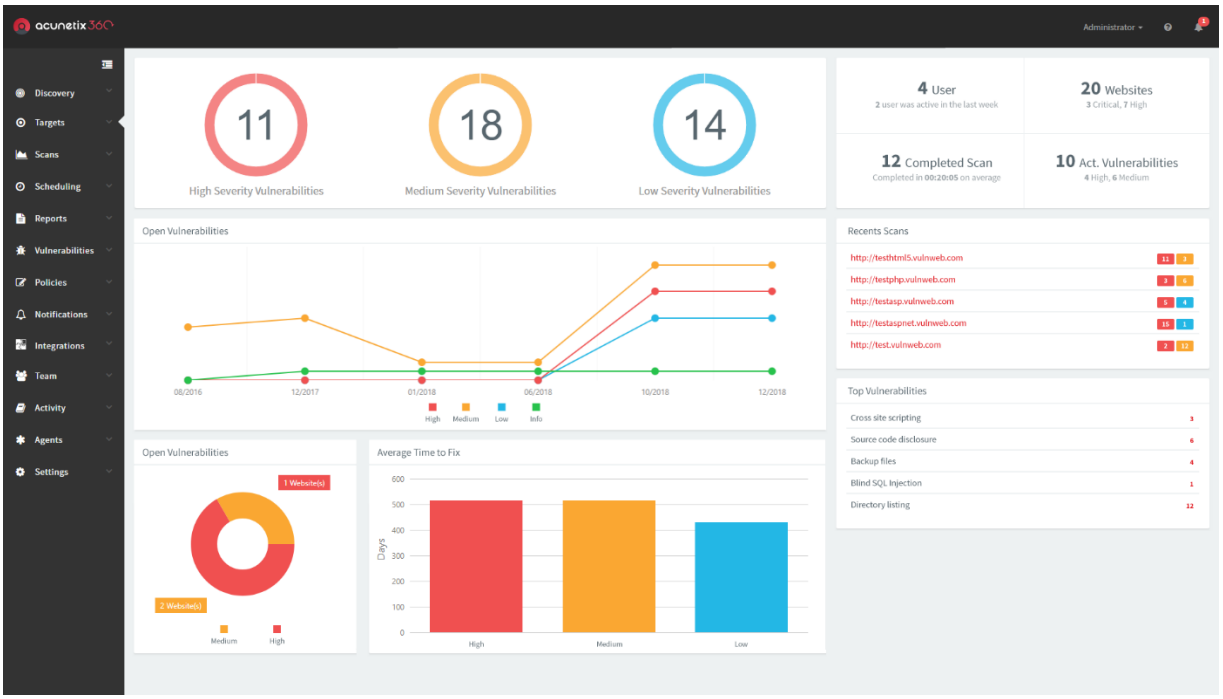
Targets Dashboard. Muestra resultados y métricas de escaneo para un sitio web específico.

Technologies Dashboard. Presenta las tecnologías detectadas en las aplicaciones escaneadas (frameworks, servidores, librerías, etc.).

En la figura 29 se presenta el panel de visualización de vulnerabilidades en Acunetix, donde se integra esta información mediante gráficos y se facilita el monitoreo del estado general de seguridad de los objetivos evaluados.

Figura 29

Panel de Visualización de Vulnerabilidades en la Herramienta Acunetix



Nota. Panel de vulnerabilidades de Acunetix. Tomado de. Introduction to the Dashboards, Acunetix. (2024) https://www.acunetix.com/support/docs/a360/getting-started/introduction-to-the-dashboards/

Comparativo Herramientas de Gestión de Vulnerabilidades

En la Tabla 6 se presenta un comparativo entre las herramientas de escaneo de vulnerabilidades descritas anteriormente.

Tabla 6

Comparativo Herramientas de Gestión de Vulnerabilidades

Criterio	OpenVAS (Greenbone Vulnerability Manager)	Qualys Vulnerability Management, Detection & Response (VMDR)	Nuclei (ProjectDiscovery)	Acunetix
Tipo de herramienta	Escáner de vulnerabilidades open source y comercial. La licencia free tiene limitaciones dado que no tiene todos los NVTs y feed.	Plataforma comercial integral de gestión de vulnerabilidades y cumplimiento.	Escáner de vulnerabilidades ligero basado en plantillas YAML.	Escáner comercial especializado en seguridad de aplicaciones web (DAST).
Tipos de escaneo	Análisis de red, servicios, paquetes, registros del sistema y configuraciones autenticadas	Escaneo de red, sistema, paquetes, agente local y aplicaciones.	Escaneo de red, aplicaciones web, API y servicios expuestos	Escaneo de aplicaciones web, APIs, formularios, autenticación y lógica de aplicación
Método de detección	Basado en plugins (NVTs) que ejecutan pruebas de red, autenticadas o no autenticadas.	Utiliza escaneos autenticados, no autenticados y agentes residentes en el host.	Basado en templates definidos por la comunidad, ejecuta pruebas HTTP, DNS, SSL, etc.	Utiliza crawling automático de la aplicación y pruebas dinámicas de seguridad (DAST).
Autenticación y profundidad de análisis	Autenticado, no autenticado, local (Linux/Windows), remoto, por servicio o IP. En el escaneo no autenticado no se	Autenticado, no autenticado, con agente (monitoreo continuo).	Permite autenticación mediante API o Secret Keys.	Soporta autenticación en aplicaciones web (formularios, tokens, sesiones) para análisis más profundo.

Criterio	OpenVAS (Greenbone Vulnerability Manager)	Qualys Vulnerability Management, Detection & Response (VMDR)	Nuclei (ProjectDiscovery)	Acunetix
	dvidencia mucha información.			
Nivel de análisis	Profundo, especialmente en sistemas autenticados (paquetes, servicios, configuraciones).	Muy profundo, con validación cruzada, análisis continuo y gestión de ciclo de vida de vulnerabilidades.	Superficial, centrado en detección rápida de servicios o patrones vulnerables conocidos.	Profundo en aplicaciones web, incluyendo lógica de aplicación, parámetros y formularios.
Estados de vulnerabilidad	4 niveles: Gone, Same, Changed, New. Permiten rastrear el estado de cada hallazgo.	4 estados principales: New, Active, Reopened, Fixed. Gestiona vulnerabilidades a lo largo del tiempo.	No maneja estados, solo muestra resultados directos por coincidencia de plantilla.	Maneja estados de vulnerabilidad y seguimiento de remediación dentro de la plataforma.
Nivel de confianza / calidad de detección	Usa QoD (Quality of Detection) del 0 al 100% para indicar certeza del hallazgo.	Clasifica vulnerabilidades en confirmadas o potenciales, similar a los niveles altos y medios de QoD.	No tiene un indicador de certeza; depende de la calidad del template utilizado.	Incluye validación automática para reducir falsos positivos en vulnerabilidades web.
Manejo de CVE Y CWE	Mapea vulnerabilidades a CVEs, BIDs y CERTs, con descripciones detalladas.	Asocia CVEs y referencias a parches, con priorización mediante Threat Indicators.	Reporta CVEs y CWE asociados a los templates (si están definidos).	Asocia vulnerabilidades a CVE, CWE y estándares como OWASP Top 10.
Clasificación por severidad	Basada en CVSS v2 y v3.1 (Log, Low, Medium, High, Critical).	Basada en CVSS v3.1 y en motor propio de riesgo contextual.	Usa las severidades definidas por cada plantilla (informativo a crítico).	Basada en CVSS y categorización según impacto en aplicaciones web.

Criterio	OpenVAS (Greenbone Vulnerability Manager)	Qualys Vulnerability Management, Detection & Response (VMDR)	Nuclei (ProjectDiscovery)	Acunetix
Reporte y visualización	Reportes detallados con métricas, QoD, puertos, servicios y CVEs agrupados.	Reportes gráficos avanzados, gestión de remediación y SLA.	Reporte simple en consola o exportable en JSON/CSV.	Panel gráfico con reportes detallados y seguimiento de vulnerabilidades.
Actualización de firmas	Manual o automática mediante Greenbone Feed.	Automática y continua desde la nube de Qualys.	Manual o automática (si se integran repositorios públicos).	Actualizaciones automáticas desde la plataforma del proveedor.
Casos de uso ideales	Escaneo profundo en entornos controlados (laboratorios, servidores internos), pruebas de penetración.	Evaluación continua de vulnerabilidades empresariales y cumplimiento normativo.	Auditorías rápidas, bug bounty, detección de exposición web.	Evaluación de seguridad en aplicaciones web y APIs en entornos empresariales.
Métricas de confianza / precisión	QoD (Quality of Detection): mide la fiabilidad de cada hallazgo (de 0 a 100%)	Clasificación de vulnerabilidades confirmadas o potenciales según validación y evidencia de exploitabilidad	No posee métrica de confianza; la validez depende de la plantilla usada y su mantenimiento	Utiliza mecanismos de verificación automática para validar vulnerabilidades detectadas.
Vulnerabilidades potenciales / inciertas	Detecciones con QoD menor al 80% se consideran posibles falsos positivos o detecciones poco verificadas	Vulnerabilidades potenciales, sin un 100 % de confirmación de que no sean falsos positivos	Posibles falsos positivos si las plantillas no están actualizadas o son genéricas	Baja tasa de falsos positivos debido a validación específica de vulnerabilidades web.

Criterio	OpenVAS (Greenbone Vulnerability Manager)	Qualys Vulnerability Management, Detection & Response (VMDR)	Nuclei (ProjectDiscovery)	Acunetix
Base de datos de vulnerabilidades	NVTs (Network Vulnerability Tests) actualizados desde Greenbone Feed (CVE, CPE, OVAL)	Base propietaria actualizada diariamente con CVE, NVD y datos internos de Qualys Threat Research	Plantillas YAML mantenidas por la comunidad con CVE, exploits, configuraciones erróneas y exposures	Base propietaria actualizada constantemente con vulnerabilidades web y referencias CVE/CWE.

Nota. La tabla presenta un análisis comparativo entre las herramientas OpenVAS, Qualys VMDR, Nuclei y Acunetix, considerando criterios como tipo de herramienta, métodos de escaneo, nivel de análisis, autenticación, métricas de detección (QoD), manejo de vulnerabilidades (CVE/CWE), clasificación de severidad, capacidades de reporte y actualización de firmas, con el fin de identificar sus principales características y diferencias funcionales.

Limitaciones Herramientas Open Source

OpenVas. En herramientas open source como OpenVAS los escaneos dependen principalmente de la conectividad de red. Esto significa que el equipo que realiza el análisis debe tener acceso directo a los dispositivos que se desean evaluar, por lo que normalmente estos deben encontrarse dentro de la misma red de la organización o conectados mediante Virtual Private Network (VPN). Además, esta herramienta no utiliza agentes instalados en los equipos, por lo que si un dispositivo se encuentra fuera de la red corporativa no podrá ser monitoreado fácilmente. También presenta algunas limitaciones en comparación con soluciones comerciales, por ejemplo, una menor cantidad de plantillas de escaneo preconfiguradas, menor nivel de

automatización en ciertos procesos y reportes más básicos, lo que en algunos casos requiere mayor configuración manual por parte del administrador.

Entre otras limitaciones importantes se encuentran las siguientes:

Menor Cantidad de Base de Pruebas de Cobertura de Vulnerabilidades. Las soluciones comerciales suelen tener una base de pruebas más amplia y actualizada, por lo que pueden detectar más vulnerabilidades o hacerlo con mayor rapidez frente a nuevas amenazas.

Menos Plantillas y Automatización de Escaneos. Herramientas comerciales como Qualys incluyen múltiples plantillas preconfiguradas para distintos tipos de análisis (compliance, web, cloud, etc.), mientras que en OpenVAS muchas configuraciones deben crearse manualmente o ajustarse según el entorno.

Reportes y Priorización de Riesgo más Limitados. Las soluciones comerciales suelen incluir dashboards avanzados, métricas de riesgo y reportes ejecutivos listos para auditorías o toma de decisiones, mientras que OpenVAS ofrece reportes más básicos y con menor nivel de personalización

Escalabilidad y Rendimiento. En entornos grandes, los escaneos pueden ser más lentos o requerir optimización de recursos, mientras que plataformas comerciales suelen tener motores de escaneo más optimizados para redes empresariales.

Mayor Esfuerzo de Administración. Otra diferencia importante se relaciona con el tipo de infraestructura que requiere cada solución. En el caso de OpenVAS, al tratarse de una herramienta que normalmente se implementa en entornos locales, es necesario instalar y mantener la infraestructura dentro de la organización. Esto implica desplegar el servidor de escaneo, administrar actualizaciones del sistema, gestionar los feeds de vulnerabilidades y asegurar que los recursos del servidor sean suficientes para realizar los análisis. En entornos

pequeños o de laboratorio esto no representa un problema, pero en organizaciones más grandes puede requerir mayor esfuerzo de administración y mantenimiento.

Por su parte, plataformas comerciales como Qualys utilizan un modelo basado en la nube, por lo que gran parte de la infraestructura es gestionada por el proveedor del servicio. En este caso, la organización solo necesita configurar la plataforma y desplegar los sensores o agentes necesarios, mientras que el procesamiento, almacenamiento de información y actualización de la base de vulnerabilidades se realiza desde la infraestructura del proveedor. Esto reduce la carga operativa interna y facilita la escalabilidad cuando se necesita monitorear un mayor número de activos o integrar sistemas ubicados en diferentes redes o servicios en la nube.

Nuclei. En comparación con herramientas comerciales como Acunetix, el uso de Nuclei presenta algunas limitaciones que pueden afectar su uso en entornos empresariales:

***Dependencia de Plantillas*.** Nuclei funciona a partir de plantillas YAML, por lo que la detección de vulnerabilidades depende de que exista una plantilla disponible. Si no existe, debe crearse manualmente.

***Menor Automatización en el Análisis en Aplicaciones Web*.** A diferencia de Acunetix, Nuclei no realiza crawling completo de la aplicación ni descubre automáticamente todos los endpoints.

***Ausencia de Interfaz Gráfica*.** Se ejecuta principalmente desde línea de comandos, lo que puede dificultar su uso para usuarios con menos experiencia técnica.

Gestión de Reportes más Limitada. Los resultados suelen generarse en formatos simples y requieren procesamiento adicional para generar reportes ejecutivos.

***Menor Integración Empresarial*.** No incluye de forma nativa paneles centralizados, gestión de vulnerabilidades o seguimiento del ciclo de remediación como sí ocurre en

herramientas comerciales.

Al igual que en la comparación entre OpenVAS y Qualys, también existe una diferencia en la infraestructura requerida. En el caso de Nuclei, al ser una herramienta open source, debe ejecutarse desde la infraestructura del usuario, quien debe encargarse de su instalación, configuración y mantenimiento. En cambio, Acunetix puede utilizarse como una solución en la nube, por lo que no requiere desplegar infraestructura propia para realizar los análisis.

Elección Herramientas de Gestión de Vulnerabilidades

Para el desarrollo del tercer objetivo del proyecto, orientado a la evaluación del ciclo de gestión continua de exposición a amenazas (CTEM), se seleccionaron las herramientas OpenVAS y Nuclei. Esta elección se basó principalmente en la disponibilidad de herramientas open source que permitieran implementar pruebas prácticas dentro de un entorno de laboratorio, considerando que no se dispone de licencias para soluciones comerciales como Qualys VMDR o Acunetix.

OpenVAS permite realizar evaluaciones profundas de vulnerabilidades en sistemas y servicios de red mediante su conjunto de Network Vulnerability Tests (NVTs), lo que facilita identificar configuraciones inseguras, servicios expuestos, software vulnerable o parches faltantes dentro de la infraestructura evaluada. Esto permite obtener una visión detallada del estado de seguridad del entorno analizado, siendo especialmente útil en escenarios de laboratorio o pruebas controladas.

Por su parte, Nuclei complementa este análisis al permitir la detección rápida de vulnerabilidades mediante el uso de plantillas definidas por la comunidad. Su enfoque resulta particularmente útil para identificar exposiciones en aplicaciones web, servicios HTTP, APIs y

configuraciones erróneas, lo que aporta agilidad al proceso de identificación de riesgos dentro del ciclo CTEM.

Si bien estas herramientas presentan algunas limitaciones frente a soluciones comerciales como menor automatización, ausencia de agentes de monitoreo continuo, reportes más básicos o dependencia de infraestructura propia, permiten implementar de manera efectiva procesos de identificación y análisis de vulnerabilidades dentro de un entorno académico o de investigación.

En este contexto, la combinación de OpenVAS y Nuclei ofrece un enfoque complementario: OpenVAS aporta mayor profundidad en el análisis de redes y sistemas, mientras que Nuclei permite realizar verificaciones rápidas sobre servicios web y vulnerabilidades conocidas. De esta manera, ambas herramientas permiten cubrir diferentes superficies de ataque y apoyar las etapas iniciales del ciclo CTEM, demostrando que es posible implementar procesos de gestión de vulnerabilidades utilizando herramientas open source cuando no se dispone de soluciones comerciales.

Estudio y Análisis Comparativo de Herramientas de Inteligencia de Amenazas

AlienVault OTX

AlienVault OTX (Open Threat Exchange) Es una plataforma de intercambio de información sobre ciberamenazas que permite a investigadores y profesionales de seguridad compartir datos sobre ataques, vulnerabilidades y comportamientos de actores de amenaza. La idea es que, mediante la colaboración, las organizaciones puedan detectar y reaccionar ante amenazas de manera más rápida y efectiva.

La plataforma funciona mediante “pulsos de amenaza”, que son paquetes de información sobre incidentes específicos. Cada pulso incluye indicadores de compromiso, como direcciones IP, dominios, hashes de archivos o URLs maliciosas, además de una descripción de la amenaza y

el contexto del ataque. Esto permite a los equipos de seguridad integrar esos datos directamente en sus sistemas y herramientas para reforzar la defensa de sus redes.

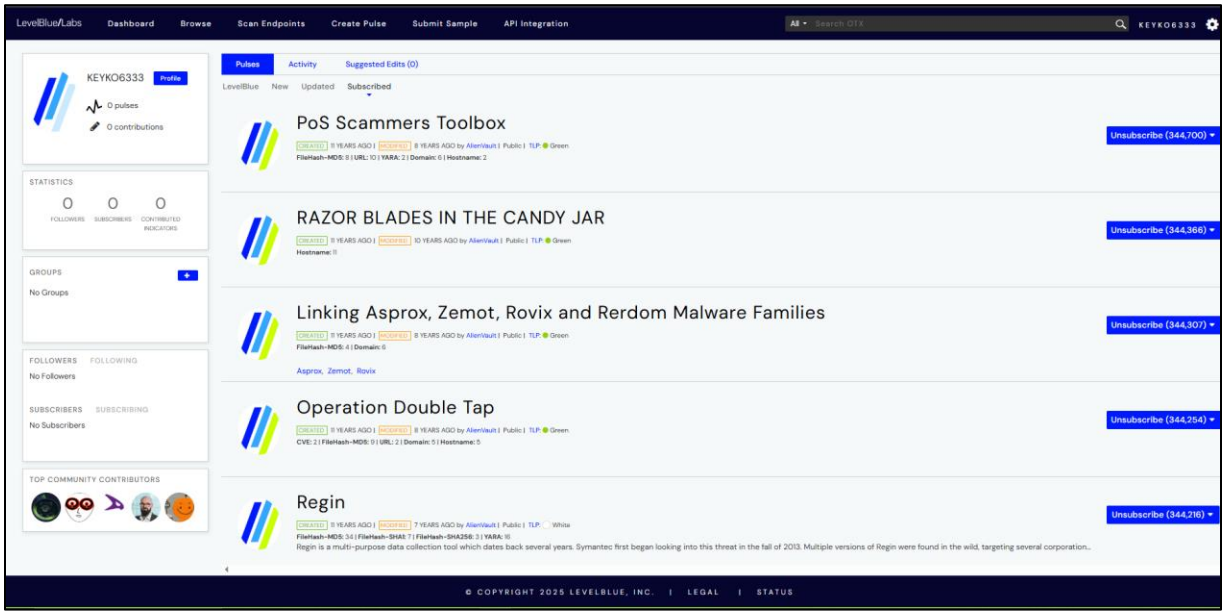
OTX también ofrece integración con otras soluciones de seguridad, tanto gratuitas como comerciales, para que los datos de amenazas puedan utilizarse en la gestión de eventos de seguridad y en análisis de incidentes. Además, es una plataforma abierta, lo que significa que cualquier persona puede registrarse, aportar información y beneficiarse de la inteligencia colectiva de la comunidad.

LevelBlue es la empresa que actualmente mantiene y gestiona OTX. Surgió como una separación de AT&T Cybersecurity y continúa ofreciendo servicios de seguridad, consultoría y herramientas de inteligencia de amenazas, manteniendo activos importantes como OTX y Open Source Security Information Management (OSSIM) (LevelBlue, s.f).

La interfaz general de la plataforma se muestra en la figura 30, donde se concentra la vista principal del sistema con sus distintas secciones de monitoreo y visualización de inteligencia de amenazas.

Figura 30

Interfaz General Alien Vault OTX



Nota. Panel principal de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

Modulo Dashboard. En este módulo se muestra el panel principal, donde se puede visualizar información en tiempo real sobre la actividad de distintas familias de malware detectadas a nivel global. En el centro del panel también se puede observar una representación gráfica denominada Visualization of Malware Clusters, que agrupa los diferentes tipos de malware identificados durante las últimas 24 horas. Cada círculo representa una familia de malware, y su tamaño indica la cantidad de reportes asociados, por ejemplo, destacan las familias Zombie, VB, G3nasom y Berbew, con miles de detecciones registradas.

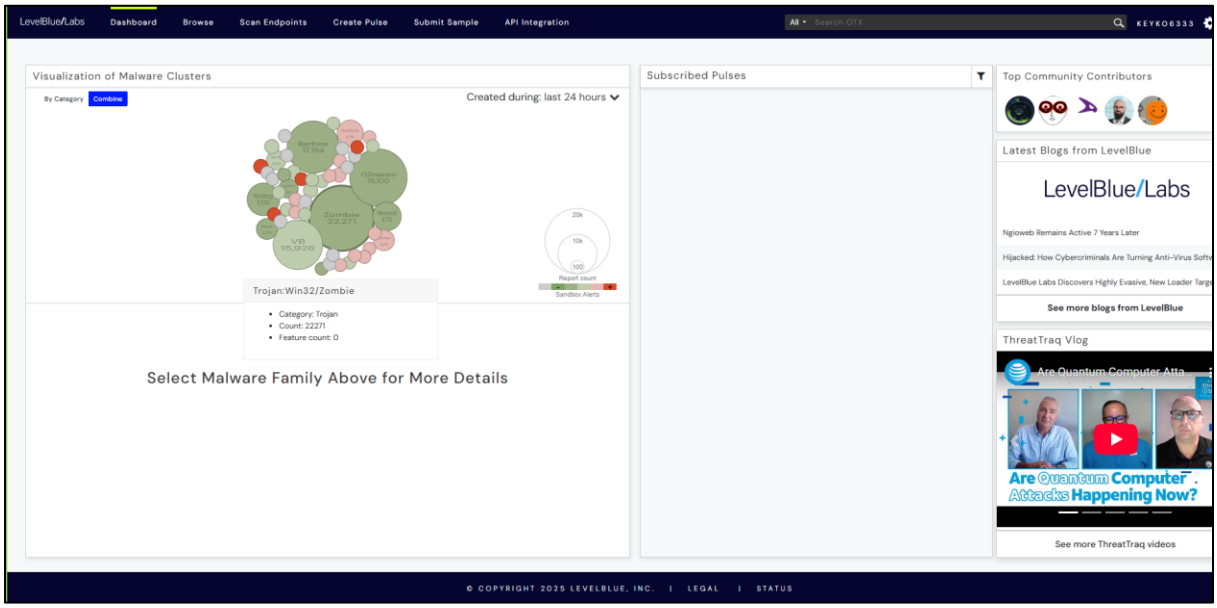
La herramienta permite seleccionar una familia específica para conocer detalles como su categoría, frecuencia de aparición y características principales, tal como se aprecia en el recuadro que muestra información del Trojan:Win32/Zombie. A la derecha del panel se encuentran los

apartados de Top Community Contributors, Latest Blogs y ThreatTraq Vlog, donde se comparte contenido actualizado sobre tendencias y análisis de ciberseguridad, donde entra uno de los factores más importantes que es colaboración de diferentes comunidades de ciberseguridad (LevelBlue, s.f).

La visualización de este módulo se presenta en la figura 31, donde se aprecia la distribución general del dashboard y sus principales componentes.

Figura 31

Modulo Dashboard



Nota. Módulo dashboard de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

Modulo Browse. En la interfaz del módulo Browse, se puede observar una organización de la información relacionada con la inteligencia de amenazas cibernéticas.

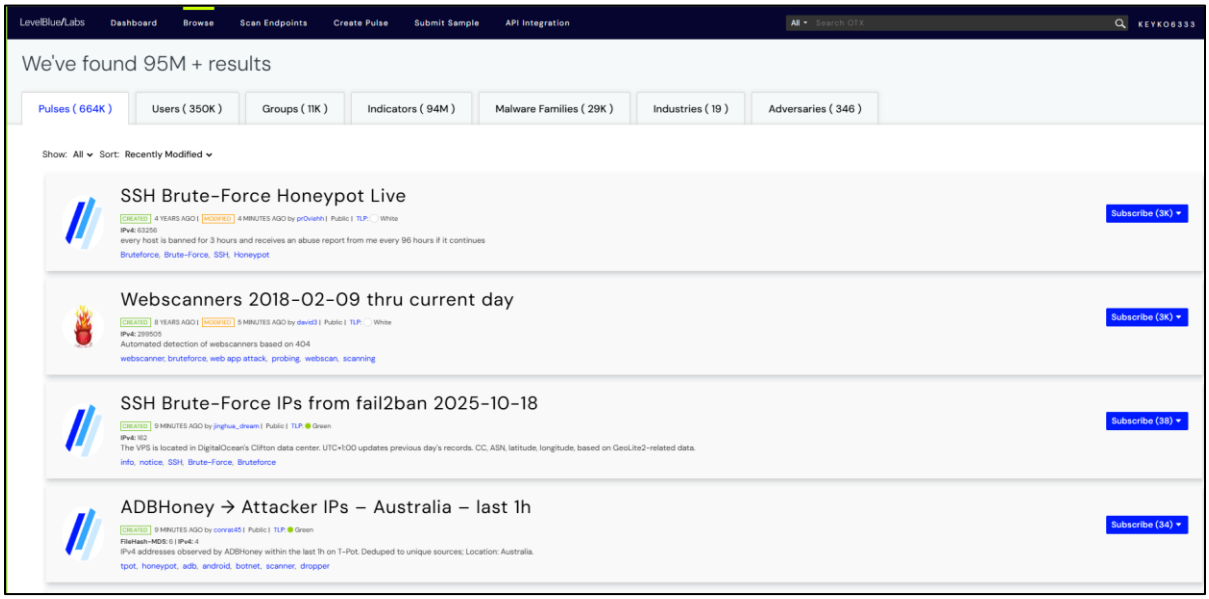
En primer lugar, Pulses muestras alertas o eventos específicos de seguridad que han sido creados por usuarios, y permite suscribirse para recibir actualizaciones sobre estos eventos. En

este caso, hay 664,000 pulsos registrados, lo que indica la cantidad de alertas o patrones de ataque observados y catalogados (LevelBlue, s.f).

La vista general de este módulo se puede apreciar en la figura 32, donde se muestra la disposición de las secciones principales y la forma en que se organiza la información.

Figura 32

Modulo Browse



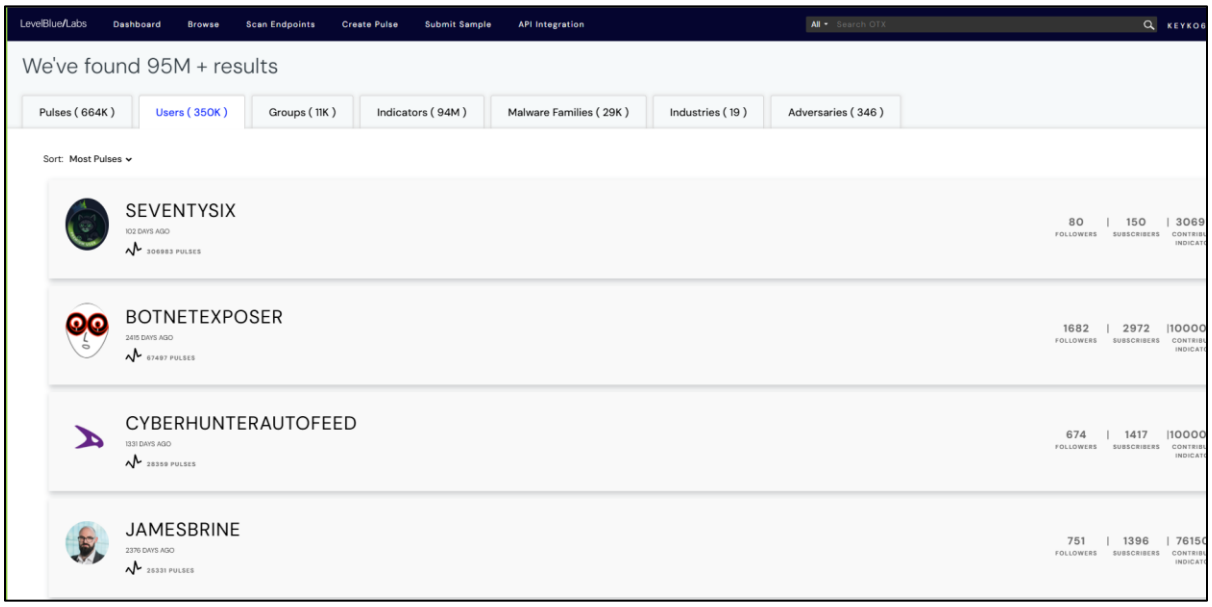
Nota. Módulo Browse de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

La sección de Usuarios refleja la interacción de 350,000 usuarios con la plataforma, los cuales pueden ser analistas, investigadores o profesionales de seguridad que acceden a los datos y comparten inteligencia sobre amenazas. Además, los Grupos agrupan a los usuarios en 11,000 equipos especializados, como pueden ser equipos dedicados al análisis de amenazas específicas como ransomware, APT o botnets, facilitando la colaboración y el intercambio de información dentro de la comunidad (LevelBlue, s.f).

En la figura 33 se puede observar cómo se estructura este módulo de Users dentro de la plataforma, integrando tanto la gestión de usuarios como la organización por grupos de trabajo.

Figura 33

Modulo Users

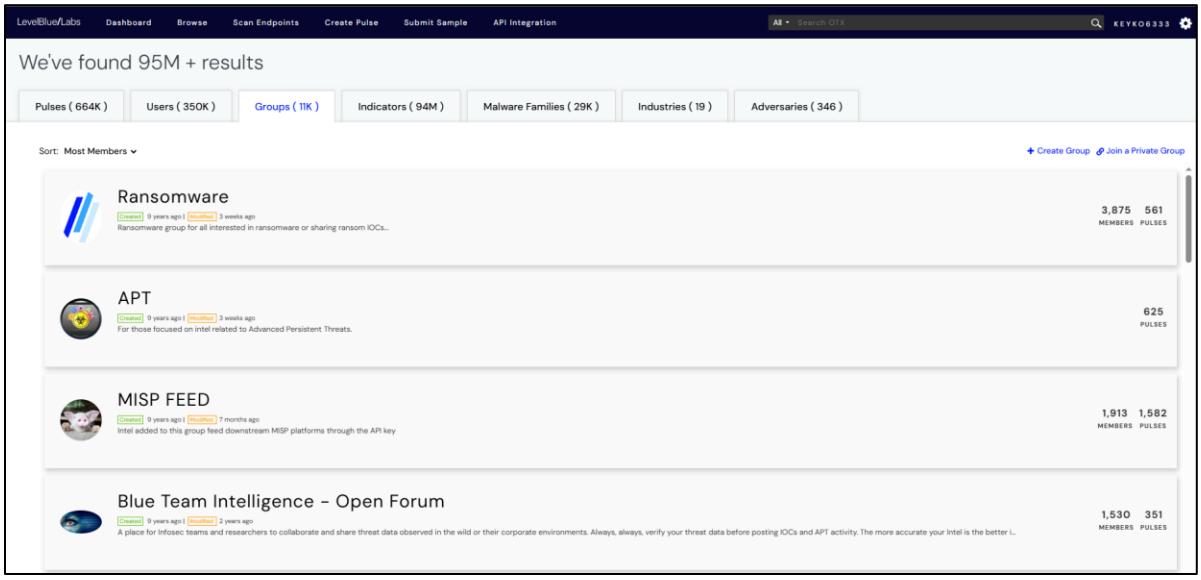


Nota. Módulo Users de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

En la figura 34 se puede observar el módulo Groups, donde la plataforma organiza a la comunidad en distintos grupos de ciberseguridad según sus áreas de interés. Estos equipos incluyen temáticas como Ransomware, APT o feeds de inteligencia, lo que permite agrupar usuarios con objetivos comunes de análisis e investigación. De esta manera se facilita la colaboración y el intercambio de información entre los distintos participantes.

Figura 34

Modulo Groups

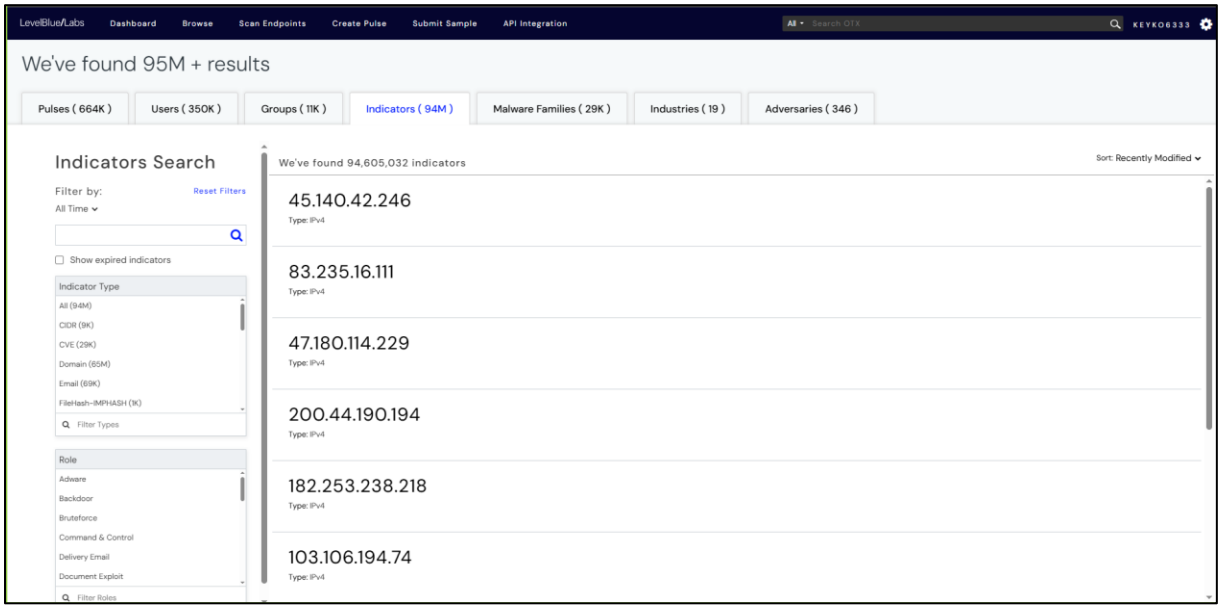


Nota. Módulo Groups de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

En la figura 35 se muestra el módulo Indicators, donde se concentran los indicadores de compromiso asociados a distintas amenazas de ciberseguridad. También se observan los Indicadores (94 millones), que incluyen direcciones IP, dominios y otros elementos utilizados para la identificación de actividad maliciosa, lo que contribuye a la detección y mitigación de posibles amenazas (LevelBlue, s.f.).

Figura 35

Modulo Indicators

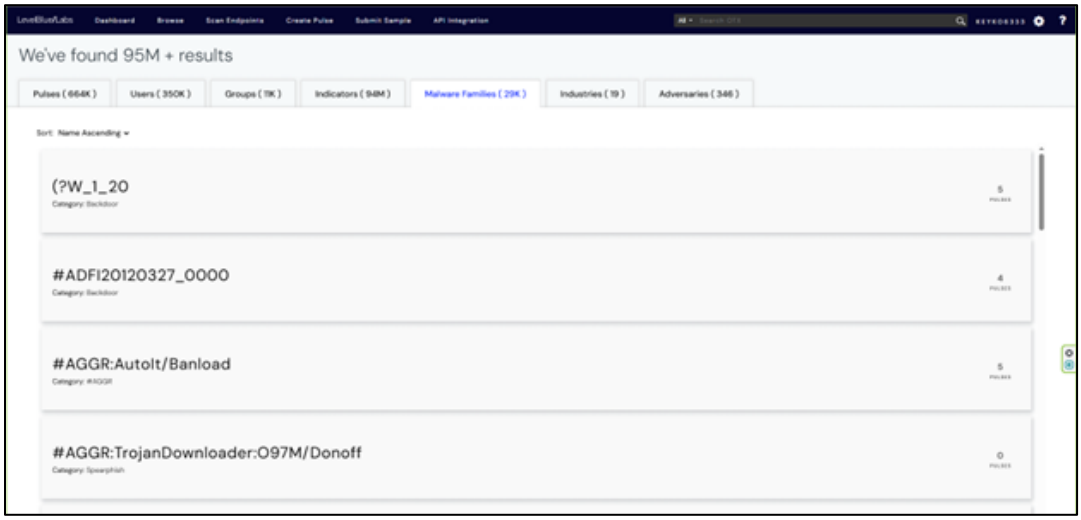


Nota. Módulo Indicators de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

En la figura 36 se presenta el módulo Malware Families, donde se agrupan las distintas familias de malware registradas en la plataforma. Por otro lado, las familias de malware, que ascienden a 29,000 registros, incluyen grupos y tipos documentados como ransomware o troyanos, los cuales han sido catalogados para su análisis dentro del sistema (LevelBlue, s.f.).

Figura 36

Modulo Malware Families

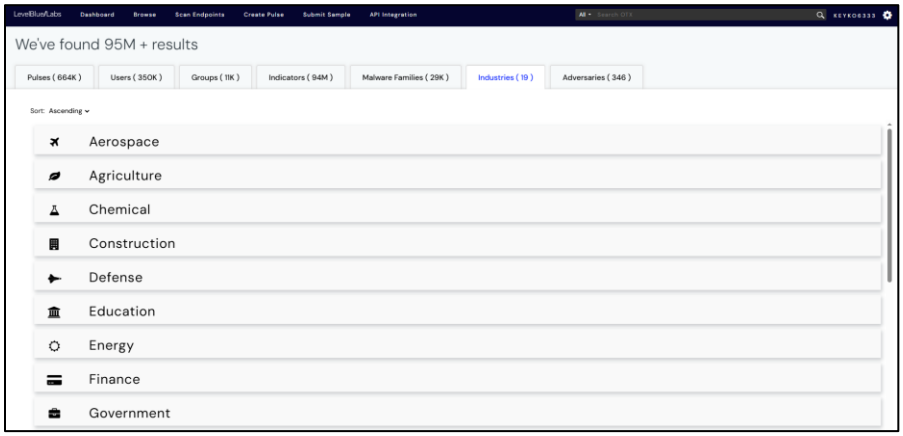


Nota. Módulo Malware Families de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

En la figura 37 se muestra el módulo Industries, donde AlienVault organiza la información de amenazas según los distintos sectores afectados. En cuanto a las Industrias, que son 19 en total, la plataforma permite clasificar y analizar los datos de seguridad en función del entorno empresarial, facilitando la personalización de alertas e inteligencia de amenazas según cada sector (LevelBlue, s.f.).

Figura 37

Modulo Industries

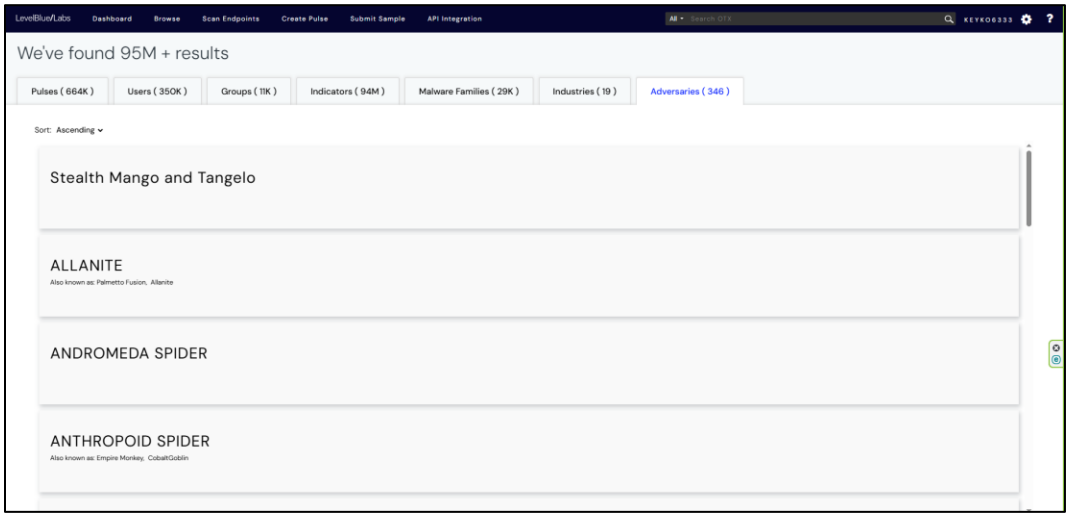


Nota. Módulo Industries de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

En la figura 38 se presenta el módulo Adversaries, donde se agrupan los distintos actores de amenaza identificados en la plataforma. Finalmente, en cuanto a adversarios, que son 346, estos representan grupos como ransomware o APT, los cuales han sido catalogados para facilitar el análisis de sus tácticas, técnicas y objetivos dentro del ecosistema de amenazas (LevelBlue, s.f.).

Figura 38

Modulo Adversaries

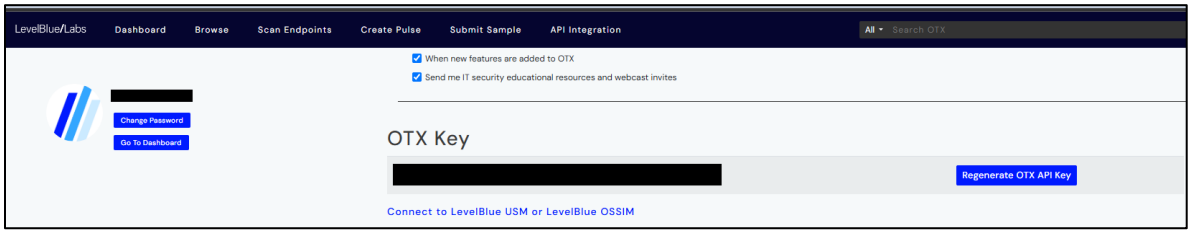


Nota. Módulo Adversaries de Open Threat Exchange (OTX). Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

En la figura 39 se muestra la sección de la API de AlienVault, la cual permite la integración de la plataforma con otros sistemas. También permite el uso de una API, lo cual resulta fundamental para realizar automatizaciones, facilitando la consulta de indicadores, pulses y demás datos de inteligencia de amenazas de forma programática (LevelBlue, s.f).

Figura 39

API Alien Vault



Nota. API de AlienVault OTX. Tomado de. Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

IBM X-Force Exchange

IBM X-Force Exchange es una plataforma colaborativa de inteligencia de amenazas desarrollada por IBM que permite a los analistas y equipos de ciberseguridad compartir, consultar y analizar información sobre amenazas activas en tiempo real. Su principal objetivo es ayudar a las organizaciones a anticiparse a posibles ataques mediante el acceso a una amplia base de datos que contiene indicadores de compromiso, reportes de malware, direcciones IP maliciosas, dominios sospechosos, vulnerabilidades y campañas de ciberataques detectadas globalmente (IBM, 2024).

La plataforma integra fuentes de datos de IBM Security junto con aportes de la comunidad, lo que facilita el intercambio de información verificable y contextual. Además, ofrece herramientas visuales e interactivas para analizar relaciones entre amenazas, observar tendencias, y crear colecciones personalizadas que pueden integrarse con otras soluciones de seguridad mediante APIs

En la interfaz principal, se encuentra una barra de búsqueda avanzada, que permite realizar consultas específicas mediante múltiples parámetros como nombres de aplicaciones,

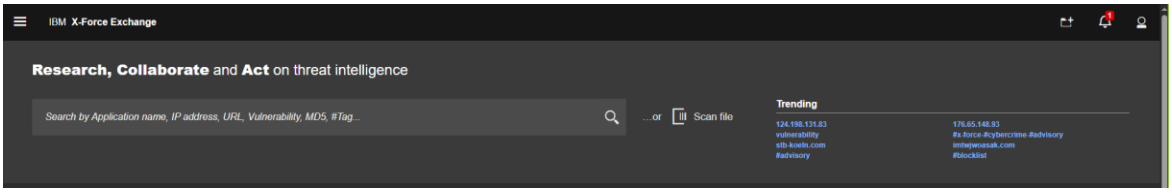
direcciones IP, URLs, vulnerabilidades conocidas, hashes (por ejemplo, Message Digest Algorithm 5 (MD5)

) y etiquetas personalizadas. A la derecha de esta barra, la plataforma ofrece la opción de escaneo de archivos (“Scan file”), lo que permite a los usuarios subir un archivo directamente para su análisis y verificación frente a bases de datos de malware conocidas.

En la figura 40 se observa el módulo de búsqueda, donde en el lado derecho se puede visualizar la sección de tendencias actuales (“Trending”). En esta área se listan indicadores que han ganado relevancia reciente dentro de la comunidad, como direcciones IP sospechosas, dominios maliciosos o etiquetas como #vulnerability, #blocklist o #advisory, lo que facilita la identificación rápida de amenazas emergentes y permite a los analistas mantenerse informados sobre los indicadores de compromiso más relevantes en tiempo real, sirviendo como punto de partida para investigaciones más profundas dentro de la plataforma.

Figura 40

Módulo de Búsqueda



Nota. Módulo de búsqueda de IBM X-Force Exchange. Tomado de. IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

IBM X-Force Threat Analysis Reports. Este módulo comparte informes detallados de análisis de amenazas elaborados por el equipo de IBM X-Force. Los reportes incluyen campañas

de malware, vulnerabilidades explotadas recientemente y perfiles de grupos de amenaza activos (IBM, s.f).

IBM X-Force OSINT Advisories. En esta sección se presentan informes de inteligencia de amenazas recopilada a partir de fuentes OSINT. Los avisos incluyen vulnerabilidades, campañas maliciosas activas y observaciones relevantes extraídas de fuentes públicas (IBM, s.f).

IBM X-Force Threat Group Reports. Este módulo comparte información de perfiles detallados de grupos de amenaza conocidos (como APTs, cibercriminales o actores estatales). Los informes contienen información sobre tácticas, técnicas y procedimientos (TTPs), motivaciones y campañas atribuidas (IBM, s.f).

IBM X-Force Malware Analysis Reports. En este módulo se comparten los análisis técnicos de muestras de malware analizadas por IBM X-Force. Cada informe incluye detalles como vectores de infección, comportamiento del malware, payloads, técnicas de evasión y posibles indicadores de compromiso (IBM, s.f).

IBM X-Force Industry Reports. Este apartado comparte análisis específicos por industria, proporcionando una visión de las amenazas dirigidas a distintos sectores específicos. Los informes permiten identificar tendencias y riesgos particulares en sectores como por ejemplo de servicios financieros Esta información permite adaptar las estrategias de ciberseguridad a las amenazas más relevantes según el sector (IBM, s.f).

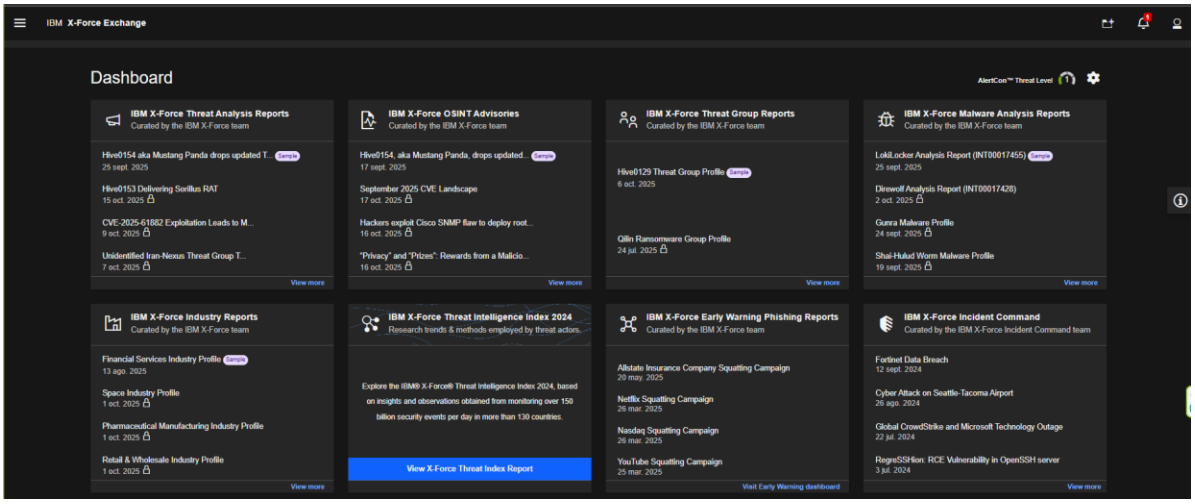
IBM X-Force Threat Intelligence Index 2024. Se trata de un informe consolidado anual que recoge estadísticas y tendencias observadas en el panorama de amenazas global. El índice se basa en el monitoreo de más de 150 mil millones de eventos de seguridad por día en más de 130 países. Este informe proporciona una visión estratégica sobre cómo evolucionan los métodos de los actores maliciosos y cuáles son los vectores de ataque más comunes (IBM, s.f).

IBM X-Force Early Warning Phishing Reports. Este módulo informa de campañas de phishing detectadas de manera temprana, con énfasis en técnicas de brand squatting (suplantación de marcas) (IBM, s.f).

IBM X-Force Incident Command. En la figura 41 se observa la interfaz de dashboards, donde esta sección comparte reportes de incidentes gestionados o monitoreados por el equipo de respuesta a incidentes de IBM. Incluye brechas de datos, ciberataques a infraestructuras críticas y fallos de seguridad relevantes a nivel global (IBM, s.f.).

Figura 41

Interfaz Dashboards



Nota. Interfaz dashboards de IBM X-Force Exchange. Tomado de. IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

X-Force en Colaboración con Quad9. Este módulo destaca la integración de IBM X-Force con el servicio DNS seguro Quad9. Su propósito es ofrecer a los usuarios una capa adicional de protección mediante el bloqueo de solicitudes a dominios maliciosos, lo que refuerza la seguridad en la navegación (IBM, s.f).

X-Force en Colaboración con Guardium. En este apartado se presenta la asociación con IBM Guardium, orientada al análisis de vulnerabilidades en entornos de datos híbridos. El módulo permite evaluar infraestructuras críticas como bases de datos o almacenes de datos, ya sea en la nube o localmente, para detectar vulnerabilidades y aplicar medidas correctivas basadas en estándares reconocidos como Security Technical Implementation Guides (STIG), Center for Internet Security (CIS) y CVE (IBM, s.f).

Early Warning Data. Este módulo comparte datos de advertencia temprana relacionados con dominios recientemente registrados que pueden estar vinculados con actividad maliciosa. Al listar los nombres de dominio y el tiempo desde su registro, el módulo permite a los analistas de seguridad monitorear proactivamente amenazas emergentes y tomar decisiones informadas (IBM, s.f).

Malicious Activity. En este módulo se recopilan y presentan estadísticas de actividad maliciosa detectada en la última hora. Se clasifica por tipo de amenaza, incluyendo comandos y control, spam, malware y escaneo. Este resumen cuantitativo permite evaluar el panorama de amenazas en tiempo real y priorizar respuestas ante incidentes (IBM, s.f).

Vulnerabilities. Este módulo proporciona una lista actualizada de vulnerabilidades de seguridad identificadas globalmente. Incluye información sobre software afectado y tipo de vulnerabilidad, como bypass de seguridad o scripting entre sitios. Esta información es clave para identificar riesgos y aplicar medidas de mitigación de forma oportuna (IBM, s.f).

Public Collections. Este módulo comparte colecciones públicas compartidas por la comunidad de usuarios de X-Force Exchange. Contiene investigaciones, reportes de amenazas, campañas de malware y otros datos relevantes. Al estar disponibles públicamente, facilitan la colaboración y el intercambio de inteligencia de amenazas entre organizaciones (IBM, s.f).

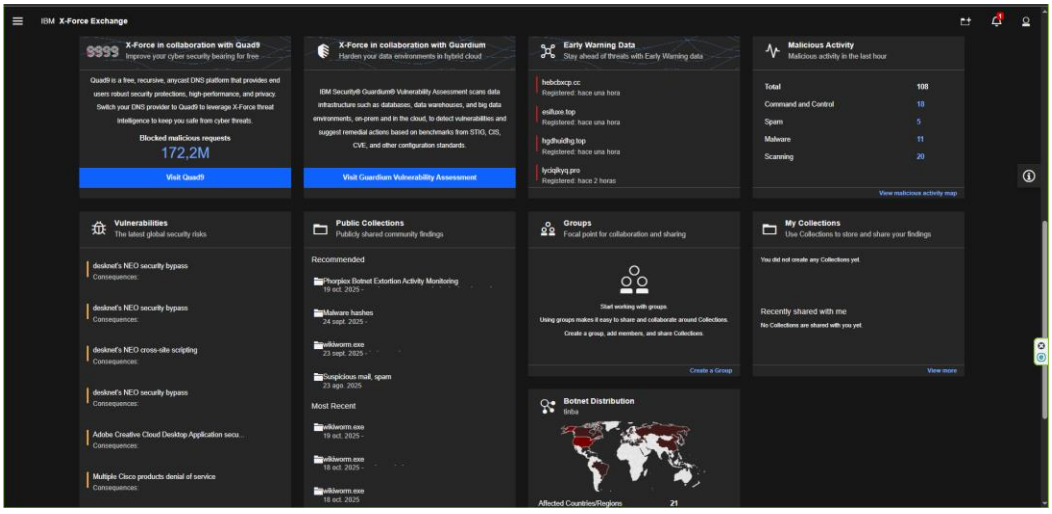
Groups. El módulo de grupos permite a los usuarios crear espacios colaborativos para compartir hallazgos y colecciones de forma privada o entre equipos específicos. Es una herramienta clave para fomentar el trabajo colaborativo dentro de una organización o entre distintos actores del campo de ciberseguridad (IBM, s.f).

My Collections. En este apartado se encuentran las colecciones creadas por el usuario o compartidas con él. Las colecciones permiten almacenar, organizar y acceder fácilmente a datos relevantes sobre amenazas, facilitando el análisis, documentación y referencia en investigaciones futuras (IBM, s.f).

Botnet Distribution. En la figura 42 se presenta un mapa mundial con la distribución geográfica de botnets activas. En este espacio se muestran los países afectados, lo que permite comprender el alcance global de la amenaza y analizar su impacto regional para coordinar respuestas de seguridad más eficaces (IBM, s.f.).

Figura 42

Interfaz Dashboards

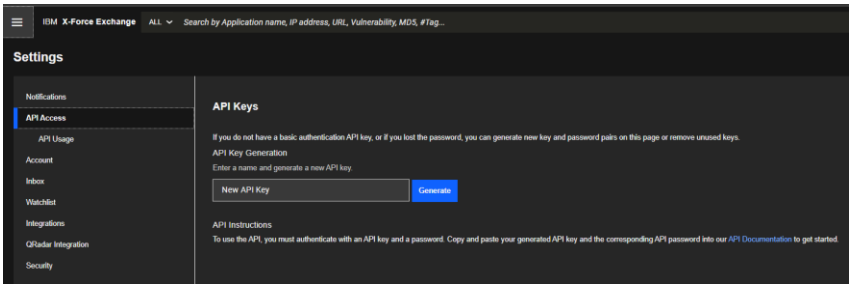


Nota. Interfaz dashboards de IBM X-Force Exchange. Tomado de. IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

API. En la figura 43 se muestra la API de IBM, utilizada para integrar la plataforma con otros sistemas y automatizar la recolección de inteligencia de amenazas. A través de esta interfaz es posible consultar y gestionar información de seguridad de forma directa desde otras herramientas, lo que facilita los procesos de análisis y respuesta (IBM, s.f.).

Figura 43

API IBM



Nota. API de IBM X-Force Exchange. Tomado de. IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

Cisco Talos Intelligence

Talos Intelligence es la división de inteligencia de amenazas de Cisco, especializada en el análisis, detección y mitigación de ciberamenazas a nivel global. El Intelligence Center funciona como una plataforma de consulta que permite a analistas e investigadores acceder a información actualizada sobre reputación de IPs, dominios, URLs, archivos y más. A través de esta herramienta, es posible buscar datos utilizando direcciones IP, nombres de dominio, hashes de archivos utilizando el algoritmo Secure Hash Algorithm 256 (SHA-256), entre otros, con el fin de validar su confiabilidad o identificar comportamientos maliciosos (Cisco Talos Intelligence Group, n. d.).

Web Reputation. Este módulo permite consultar la reputación de una página web específica. El sistema evalúa diversos parámetros para determinar si un sitio es seguro o si ha sido reportado por actividades sospechosas como phishing, malware o distribución de contenido no autorizado. La evaluación puede clasificarse en diferentes niveles de riesgo que ayudan a tomar decisiones rápidas de bloqueo o monitoreo.

Content Categorization. En esta sección se clasifica el contenido de un dominio o URL dentro de una categoría específica (por ejemplo: redes sociales, apuestas, noticias, etc.). Esta categorización es fundamental para la implementación de políticas de filtrado web en entornos corporativos y para entender el propósito del sitio más allá de su reputación.

Sender IP Reputation. Este apartado permite analizar la reputación de una dirección IP utilizada para el envío de correos electrónicos. Se utiliza principalmente para detectar si una IP está vinculada a campañas de spam, phishing o distribución de malware, lo que resulta útil para proteger la infraestructura de correo electrónico empresarial.

Sender Domain Reputation. Similar al análisis por IP, este módulo evalúa la reputación de un dominio utilizado como remitente de correo. Es una herramienta crítica para identificar dominios que participan en actividades maliciosas como suplantación de identidad (spoofing) o distribución masiva de mensajes fraudulentos.

File Reputation. Permite verificar la reputación de archivos mediante el uso de hashes (por ejemplo, SHA256). El sistema compara el hash contra una base de datos de archivos maliciosos conocidos para determinar si el archivo ha sido utilizado previamente en ataques, facilitando así la detección de malware en archivos ejecutables, documentos u otros formatos.

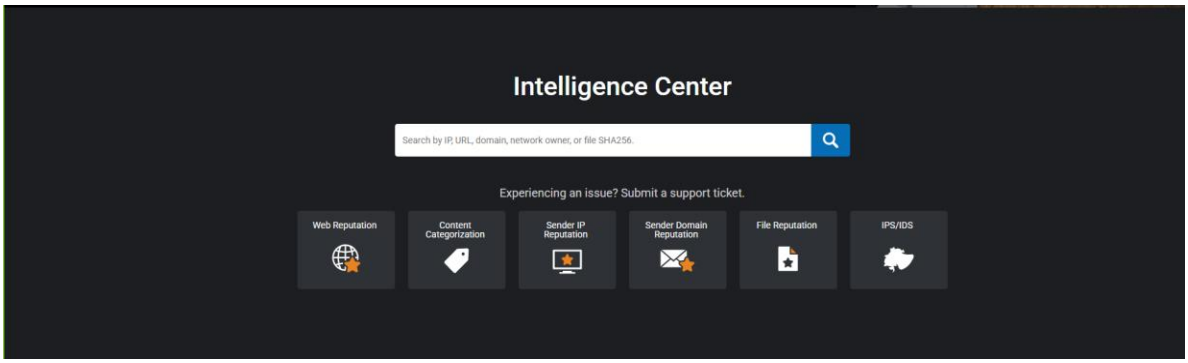
IPS/IDS. Este módulo ofrece información relevante para sistemas de detección y prevención de intrusos (IDS/IPS). Aquí se accede a firmas y reglas diseñadas para identificar

comportamientos anómalos o ataques conocidos dentro de una red, lo cual es clave para mantener la integridad del entorno informático y responder a incidentes de seguridad en tiempo real.

La figura 44 muestra la interfaz de Cisco Talos Intelligence, donde se centralizan las distintas funcionalidades de consulta de inteligencia de amenazas, permitiendo el análisis de reputación de IPs, dominios, archivos y otros indicadores de seguridad en una sola plataforma.

Figura 44

Interfaz de Cisco Talos Intelligence



Nota. Interfaz de Cisco Talos Intelligence. Tomado de. Cisco Talos Intelligence Group. (s. f.) https://talosintelligence.com

API. Tiene una API, pero esta más enfocada al análisis y reputación de direcciones IP.

MISP

MISP es una plataforma de código abierto diseñada para la recopilación, almacenamiento, distribución y correlación de indicadores de compromiso y otra información relevante sobre amenazas cibernéticas. Su principal objetivo es facilitar el intercambio estructurado y colaborativo de información entre organizaciones, equipos de respuesta a incidentes (Computer Security Incident Response Team (CSIRT) /CERT), instituciones

gubernamentales y sector privado. MISP permite automatizar la detección de amenazas, reducir tiempos de respuesta y mejorar la defensa frente a ataques mediante inteligencia de amenazas reutilizable y estandarizada (MISP, s.f).

Características de MISP. La primera es la compartición estructurada de amenazas, facilita el intercambio de datos sobre amenazas mediante un modelo estandarizado.

Correlación de Eventos e Indicadores. Identifica patrones y conexiones entre eventos, actores de amenaza, malware y vectores de ataque.

Colaboración Comunitaria. Permite crear comunidades de confianza para compartir información sensible o clasificada de forma segura.

Soporte de Taxonomías y Clasificaciones. Integra múltiples taxonomías que estandarizan la forma en que se categoriza la información.

Automatización a Través de API REST. Ofrece integración con otras plataformas de seguridad mediante APIs, facilitando flujos automatizados.

Extensión de Módulos. Soporta módulos externos para tareas como enriquecimiento, exportación, importación o integración con otras herramientas.

Módulos destacados de MISP

***MISP Galaxies & Taxonomies*.** Incluye conjuntos de datos estructurados como los galaxy clusters (ej. MITRE ATT&CK, ransomware, grupos de amenazas, etc.) y taxonomías que permiten clasificar eventos e indicadores según estándares reconocidos, como los utilizados por CSIRTs y CERTs.

***MISP Doc & Trainings*.** Proporciona materiales de formación abiertos, incluyendo documentación técnica, presentaciones y entornos virtuales preconfigurados. Esta iniciativa,

liderada por el Computer Incident Response Center Luxembourg (CIRCL), busca facilitar la adopción y correcto uso de MISP en diferentes contextos operativos.

PyMISP. Es una biblioteca de Python que permite interactuar con MISP a través de su API REST. Facilita tareas como consultar eventos, actualizar atributos, subir muestras o buscar indicadores de manera programática, siendo útil para automatizar flujos de trabajo dentro de SOCs o equipos de respuesta.

***MISP Modules*.** Son módulos autónomos escritos en Python 3 que permiten extender las funcionalidades de MISP sin alterar su núcleo. Estos módulos permiten añadir capacidades como enriquecimiento de indicadores, integración con servicios externos, importación/exportación de datos y más. Su arquitectura modular permite una implementación flexible y personalizable (MISP, s.f).

Vulnerabilidades

***Integración con Bases de Datos de Vulnerabilidades*.** MISP puede consumir y correlacionar datos de vulnerabilidades públicas (como NVD o CIRCL's CVE feed). Esto permite que cada evento en MISP pueda incluir referencias a una o varias vulnerabilidades específicas mediante su identificador CVE.

***Enlaces con Otros Elementos de Amenazas*.** Los CVE en MISP no se aíslan, sino que se conectan con malware, actores de amenazas, herramientas utilizadas en ataques o sectores afectados. Esto amplía el contexto técnico y táctico.

***Enriquecimiento Automático*.** A través de módulos de enriquecimiento, MISP puede obtener automáticamente detalles adicionales de un CVE (por ejemplo, puntuación CVSS, descripción técnica, referencias externas) al agregar un identificador a un evento.

***Correlación con Otros Eventos*.** Si múltiples eventos en MISP hacen referencia al mismo CVE, se puede identificar una tendencia o campaña activa que explota esa vulnerabilidad, lo cual es útil para análisis proactivos.

***Exportación Para Herramientas de Gestión de Vulnerabilidades*.** Los datos de CVE también se pueden exportar desde MISP hacia otras plataformas SIEM, herramientas de gestión de parches o dashboards de riesgo (MISP, s.f).

Comparativo Herramientas de Inteligencia de Amenazas

En la Tabla 7 se presenta un comparativo de herramientas de inteligencia de amenazas, analizando diferentes plataformas utilizadas para la recolección, análisis y compartición de información relacionada con ciber amenazas.

Tabla 7

Comparativo Herramientas de Inteligencia de Amenazas

Criterio	AlienVault OTX (LevelBlue)	IBM X-Force Exchange	Cisco Talos Intelligence	MISP (Malware Information Sharing Platform & Threat Sharing)
Descripción general	Plataforma colaborativa de threat intelligence que permite compartir y consumir información sobre amenazas emergentes, impulsada por la comunidad global de seguridad.	Plataforma de IBM que centraliza inteligencia de amenazas global y análisis de riesgos cibernéticos, integrando big data, machine learning y colaboración entre analistas.	División de Cisco dedicada a la investigación, análisis y detección de amenazas a escala global; ofrece reputación de IPs, dominios, archivos y más.	Plataforma de código abierto para la recopilación, análisis y compartición de indicadores de compromiso (IoCs) entre comunidades y organizaciones.
Tipo de inteligencia	Colaborativa y comunitaria (crowdsourced).	Basada en inteligencia corporativa y fuentes globales de IBM.	Inteligencia basada en telemetría global y datos de red de Cisco.	Compartida y federada entre organizaciones (open source y comunitaria).
Indicadores de compromiso (IoC)	Dominios, IPs, URLs, hashes, TTPs (tácticas, técnicas y procedimientos).	IPs, dominios, URLs, vulnerabilidades y malware.	IPs, dominios, URLs, hashes de archivos, remitentes de correo, etc.	IPs, dominios, hashes, URLs, correos, malware y TTPs (STIX/TAXII).
Análisis de reputación	Permite verificar reputación de IPs, dominios y archivos mediante consultas directas y API.	Ofrece reputación y clasificación de riesgo sobre IPs, dominios y URLs.	Ofrece reputación detallada de IPs, dominios, remitentes de correo y archivos.	No tiene módulo de reputación directa, pero permite correlación con fuentes externas que sí la proveen.
Gestión o correlación de	Relaciona IoCs con CVEsy CWEs	Muestra detalles de	Incluye referencias a vulnerabilidades	Permite importar y compartir información de

Criterio	AlienVault OTX (LevelBlue)	IBM X-Force Exchange	Cisco Talos Intelligence	MISP (Malware Information Sharing Platform & Threat Sharing)
vulnerabilidades (CVE/CVSS)	conocidos a través de los *Pulses* compartidos por la comunidad.	vulnerabilidades (CVE, CVSS, exploitabilidad), CWE y su relación con campañas activas.	conocidas en sus firmas IDS/IPS y análisis de malware.	CVEs,CWEs, CPEs y CVSS mediante taxonomías y correlaciones automáticas.
Detección y clasificación de amenazas	Detecta amenazas emergentes y comparte información sobre campañas activas.	Clasifica amenazas por severidad, tipo y afectación global.	Clasifica amenazas según comportamiento (phishing, malware, spam, spoofing).	Permite correlación avanzada y categorización de amenazas con etiquetas y taxonomías.
Fuentes de datos	Comunidad global de seguridad, honeypots y contribuciones de usuarios.	Redes de IBM, partners, honeynets y fuentes OSINT.	Telemetría global de Cisco, datos de red, IDS/IPS y análisis forense.	Organizaciones participantes, CERTs, ISACs, comunidades de investigación.
API / Integración	API REST para integración con SIEM, SOAR y otras herramientas.	API REST y SDK para integrar con soluciones de seguridad corporativa.	API centrada en reputación de IPs y dominios.	APIs completas (STIX/TAXII, JSON, REST) compatibles con SIEM, SOAR y otras plataformas.
Automatización / Compartición	Sí, mediante API y suscripciones a Pulses (colecciones de IoCs).	Sí, exporta datos y permite automatización mediante API.	Limitada a reputación y análisis de IPs.	Altamente automatizable; permite intercambio estructurado automatizado de IoCs.
Visualización de datos	Dashboard interactivo con estadísticas de amenazas, IoCs y tendencias.	Panel analítico avanzado con gráficos de evolución de amenazas.	Interfaz web con módulos separados (Web Reputation, File Reputation, etc.).	Interfaz modular con dashboards y correlación visual de eventos.
Licencia / Costo	Gratuita (registro requerido).	Gratuita con opciones premium corporativas.	Gratuita (uso público).	Gratuita y de código abierto (open source).

Criterio	AlienVault OTX (LevelBlue)	IBM X-Force Exchange	Cisco Talos Intelligence	MISP (Malware Information Sharing Platform & Threat Sharing)
Ventajas principales	Amplia colaboración comunitaria y actualización constante.	Análisis profundo y confiable respaldado por IBM Research.	Base de datos global muy precisa con integración en productos Cisco.	Altamente personalizable, escalable y orientada al intercambio entre organizaciones.
Limitaciones	Dependencia del aporte de la comunidad para mantenerse actualizado.	Algunas funciones avanzadas requieren suscripción.	Limitada en automatización y correlación avanzada.	N/A

*Nota***.** La tabla presenta un análisis comparativo de herramientas de inteligencia de amenazas (AlienVault OTX, IBM X-Force Exchange, Cisco Talos Intelligence y MISP), considerando criterios como tipo de inteligencia, indicadores de compromiso (IoC), análisis de reputación, gestión de vulnerabilidades (CVE/CVSS), fuentes de datos, capacidades de integración mediante API, automatización, visualización, así como sus principales ventajas y limitaciones.

Elección Herramientas de Inteligencia de Amenazas

Para el desarrollo de los objetivos 2 y 3 del proyecto, se seleccionaron las plataformas IBM X-Force Exchange y AlienVault OTX como herramientas principales de inteligencia de amenazas. La decisión se basó en su capacidad para proporcionar información actualizada y contextualizada sobre el contexto de las vulnerabilidades, lo cual puede comprender indicadores de compromiso, actores de amenazas y campañas activas, aspectos fundamentales para fortalecer la gestión continua de la exposición a amenazas.

En el caso de IBM X-Force Exchange, su principal ventaja radica en la amplitud de su base de datos de inteligencia, alimentada por los laboratorios de investigación de IBM y por una extensa red de fuentes globales. Esta herramienta no solo permite identificar vulnerabilidades emergentes, sino también conocer su nivel de explotación en escenarios reales y los grupos de amenazas que las aprovechan, lo que contribuye directamente a la fase de contextualización y priorización del ciclo CTEM.

Por su parte, AlienVault OTX se caracteriza por su enfoque colaborativo y su comunidad activa, que comparte indicadores de amenazas en tiempo real. Su modelo abierto facilita la integración con otras soluciones de seguridad y permite una detección temprana de nuevas campañas o exploits en circulación. Esta capacidad de correlacionar inteligencia compartida con vulnerabilidades detectadas en la infraestructura interna es clave para el objetivo de diseñar un plan de recolección de inteligencia continuo y dinámico, que mantenga la visibilidad ante amenazas emergentes.

Aunque MISP y Talos Intelligence son plataformas destacadas en el ámbito de la inteligencia de amenazas, se optó por no incluirlas en esta fase del proyecto por razones metodológicas. MISP, al ser una plataforma más orientada a la gestión y compartición de información técnica entre organizaciones, requiere un entorno de implementación propio y un mantenimiento constante que excede el alcance del laboratorio planteado. Talos Intelligence, por su parte, ofrece inteligencia de alta calidad, pero con un enfoque más cerrado y menos integrable en procesos internos de análisis y priorización dentro del modelo CTEM.

En conjunto, IBM X-Force Exchange y AlienVault OTX aportan un equilibrio ideal entre automatización, comunidad activa, y capacidad de contextualización, permitiendo fortalecer el

proceso de evaluación y priorización de riesgos dentro del ciclo CTEM, para apoyar la toma de decisiones basada en inteligencia de amenazas.

Integración Entre CTEM e Inteligencia de Amenazas

La gestión continua de la exposición a amenazas requiere un proceso estructurado que va más allá del descubrimiento técnico de vulnerabilidades. El modelo contempla fases como el descubrimiento, la priorización, la validación y la movilización, las cuales deben articularse con información contextual para que la gestión del riesgo sea efectiva.

En la fase de descubrimiento, OpenVAS permite identificar nuevos activos en segmentos privados, servicios vulnerables y configuraciones inseguras dentro de la infraestructura. Este primer paso proporciona visibilidad sobre la superficie de ataque de una organización. Nuclei complementa esta etapa al facilitar la detección rápida de vulnerabilidades en aplicaciones web y APIs.

Sin embargo, el descubrimiento por sí solo no determina el nivel real de riesgo. En la fase de priorización, la integración con plataformas de inteligencia de amenazas como IBM X-Force Exchange y AlienVault OTX permiten dar contexto las vulnerabilidades detectadas. Mediante la consulta de información sobre explotación activa, campañas en curso o actores de amenaza asociados, es posible establecer qué debilidades representan un riesgo alto con primera prioridad y cuáles pueden gestionarse como segunda prioridad.

Posteriormente, en la fase de validación, Nuclei aporta agilidad para confirmar la presencia efectiva de determinadas vulnerabilidades, mientras que la inteligencia externa ayuda a verificar si los indicadores observados coinciden con patrones de ataque conocidos.

Finalmente, en la fase de movilización, la información técnica y contextual obtenida permite tomar decisiones fundamentadas sobre remediación, aplicación de parches o ajustes de

configuración, priorizando recursos de acuerdo con el impacto potencial y la probabilidad de explotación.

Teniendo en cuenta lo anterior, la integración entre herramientas de análisis de vulnerabilidades e inteligencia de amenazas no solo fortalece cada fase del ciclo CTEM, sino que transforma la gestión de la exposición en un proceso dinámico y basado en evidencia tanto interna como externa. Esta relación demuestra que la selección de plataformas no se realizó de forma aislada, sino en función de su capacidad para apoyar de manera coherente y continua el modelo de gestión de amenazas planteado.

Objetivo específico 2

Ciclo de Vida de la Inteligencia de Amenazas

Es un proceso continúo utilizado en ciberseguridad para recolectar, analizar, procesar y transformar datos relacionados con amenazas en información útil. Su objetivo es apoyar la toma de decisiones y fortalecer la postura de seguridad de una organización frente a posibles ataques.

Este modelo no proviene de una única entidad ni corresponde a un estándar formal internacional. Su origen se basa en el ciclo de inteligencia tradicional utilizado por comunidades de inteligencia gubernamentales, el cual fue posteriormente adaptado al ámbito de la ciberseguridad. A partir de esta adaptación, distintas organizaciones del sector han propuesto versiones del ciclo con ligeras variaciones, manteniendo la misma lógica general.

Uno de los enfoques más utilizados en la industria es el propuesto por el SANS Institute (SANS Institute, s.f), que organiza el ciclo en 6 fases.

Planificación y Dirección

En la primera fase se genera el plan de inteligencia de amenazas de acuerdo con los requisitos de inteligencia de amenazas estratégica, se debe definir a que inteligencia se le debe dar prioridad. En esta fase deben participar las partes interesadas de las organizaciones junto con el equipo de inteligencia de amenazas, con el fin de definir los objetivos, recursos, fuentes de recopilación e incluso la determinación de activos más críticos que necesitan protección.

Durante esta fase también las sus funciones y responsabilidades del equipo de inteligencia de amenazas. Adicionalmente, se establece la planificación y los requisitos para las etapas posteriores del ciclo con el fin de que este pueda funcionar adecuadamente.

Recopilación

En la segunda fase se genera se realiza la recopilación de la inteligencia de amenazas

mediante las diferentes fuentes definidas en la fase 1. Puede ser mediante la inteligencia en fuentes abiertas, inteligencia en la Dark Web, Information Sharing and Analysis Centers (ISACs), entre otras fuentes.

Procesamiento y Explotación

Los datos recopilados se deben transformar en un formato adecuado para su procesamiento. El procesamiento puede incluir la clasificación de la información y la transformación en información útil para los consumidores, por ejemplo, mediante la transformación en un formato legible.

Análisis

Después de procesar los datos de la inteligencia recolectada, la información se debe analizar para estimar la probabilidad de un ataque y prepararse para este. Los equipos seguridad como los de Blueteam pueden examinan los datos procesados para identificar patrones, anomalías y otras señales de actividad maliciosa.

Difusión

En esta fase la información se distribuye a las partes interesadas, generalmente la inteligencia incluye información como indicadores de compromiso, indicadores de ataque, TTP de actores de amenazas, informes de inteligencia de amenazas, así como datos de configuración para usar en herramientas para automatizar las fases de la inteligencia de amenazas. El objetivo es generar informes de inteligencia de amenazas para cumplir con los requisitos de las partes interesadas.

Retroalimentación

La última fase consiste en recibir la retroalimentación de las partes interesadas, con el fin de identificar deficiencias y mejorar el plan de inteligencia de amenazas (Palo Alto Networks,

s.f).

Análisis Comparativo de Estudios Sobre el Ciclo de Vida de la Inteligencia de Amenazas

Si bien existe una estructura general que es aceptada para el ciclo de vida de la inteligencia de amenazas, las organizaciones pueden adoptar procesos distintos según sus necesidades, lo que hace que la secuencia y el enfoque de los estudios sobre este ciclo varíen.

Ciclo de Vida Atómico Para la Inteligencia de Ciberamenazas

Los autores Arikan, Koçak y Alkan (2024) plantean que el atomic lifecycle para la inteligencia de amenazas cibernéticas, dado que el modelo actual carece del nivel atómico de detalle necesaria, dado que la inteligencia en la etapa de análisis no es posible discernir si esta inteligencia es compartible o estática con base en la información proporcionada en la etapa operativa, puesto que la generación de inteligencia compartible representa una tarea más compleja. Teniendo en cuenta lo anterior, los autores plantean un ciclo de vida de la inteligencia de amenazas que consta de 8 pasos.

Determinación de Requisitos. Consiste en el proceso de identificar y cuantificar los requisitos.

Planificación. El proceso de planificar cada paso y determinar la asignación de recursos es un aspecto fundamental de la gestión de proyectos.

Recopilación. Se realiza la recopilación de los datos relevantes.

Procesamiento. Se realiza la implementación de técnicas como el filtrado y la transformación, lo cual facilita la mejora en el uso de los datos.

Análisis. Corresponde a la adquisición de inteligencia estática, a la que sólo es accesible la fuente de generación a través de los procesos de análisis, correlación e interpretación.

Producción. La creación de inteligencia interpersonal y compartible en el sistema en formatos estandarizados, como Structured Threat Information Expression (STIX), Open Vulnerability and Assessment Language (OVAL), Common Security Advisory Framework (CSAF), entre otros, o basados en tipos de datos no estructurados.

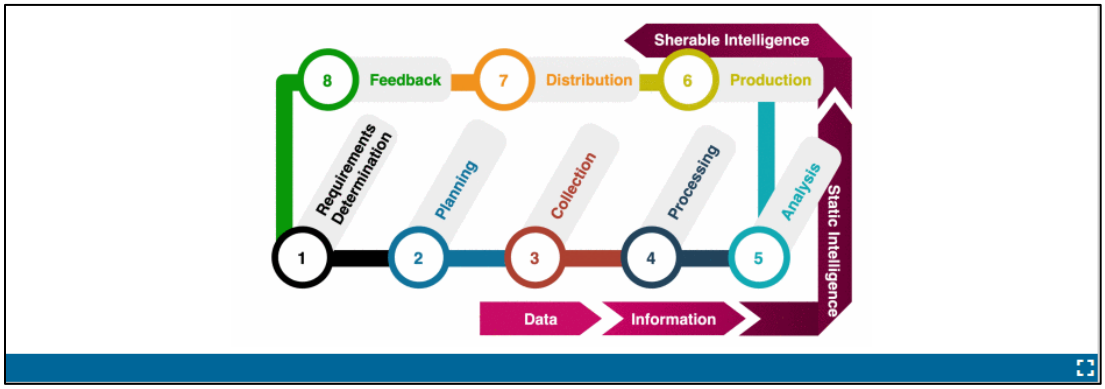
Distribución. El intercambio, distribución y compartición de inteligencia que puede compartirse entre distintas fuentes.

Retroalimentación. La evaluación de la inteligencia representa un elemento central en el proceso de evaluación.

La figura 45 presenta el ciclo de vida de la inteligencia de amenazas cibernéticas, donde se observan las fases que van desde la definición de requerimientos y la planificación, hasta la recolección, procesamiento, análisis y producción de inteligencia. El modelo también contempla la distribución de la información y la retroalimentación, lo que permite mejorar continuamente el proceso y convertir los datos en inteligencia accionable.

Figura 45

Ciclo de Vida Atómico Para Inteligencia de Ciberamenazas



Nota. Ciclo de vida atómico para inteligencia de ciberamenazas. Tomado de. Atomic Lifecycle for Cyber Threat Intelligence, Arikan, S. M., Koçak, A., y Alkan, M. (2024) https://doi.org/10.1109/ISCTrkiye64784.2024.10779304

De acuerdo con los autores, las cinco fases iniciales del nuevo ciclo de vida de la inteligencia sobre ciber amenazas se ha mantenido prácticamente inalteradas. Sin embargo, los autores han modificado la nomenclatura utilizada para describir los resultados generados durante estas fases. Teniendo en cuenta lo anteriores, los datos se obtienen durante la fase de recopilación. Aunque se puede acceder a la información en la fase de procesamiento, la inteligencia estática, que aún no se puede compartir, se genera en la fase de análisis. La inteligencia compartible se obtiene únicamente como resultado de la fase de producción.

La fase de distribución permite la transferencia de inteligencia de amenazas compatible. En este contexto, se pueden emplear diversas plataformas y herramientas de inteligencia de amenazas. Sin embargo, los autores plantean que esta transferencia de inteligencia no tiene por qué ocurrir entre países, instituciones o incluso departamentos de la empresa. Incluso el intercambio de información entre dos dispositivos utilizados en el mismo entorno puede considerarse parte de este proceso. Por lo tanto, los recursos deben definirse según las necesidades y el propósito durante la fase de planificación (Arikan et al., 2024).

Optimización de la Gestión Segura del Ciclo de Vida de la IA con Estrategias Innovadoras de IA Generativa

Spyros et al. (2025) presentan un marco holístico basado en inteligencia artificial para la gestión de la inteligencia de amenazas cibernéticas, un modelo importante para que las organizaciones faciliten la protección de los sistemas contra ciberamenazas nuevos y emergentes.

La recopilación de información Ciber inteligencia de amenazas requiere inicialmente la identificación de las fuentes de inteligencia de amenazas. Las fuentes y la información sobre amenazas que se necesita recopilar de los dispositivos de monitoreo, como Extended Detection and Response (XDR), Firewalls, entre otros, que facilitarán los procesos de toma de decisiones

se definen en este paso. Posteriormente, se debe recopilar la información de las fuentes identificadas de acuerdo con un procedimiento definido. La recopilación puede incluir el uso de fuentes externas (es decir, en línea) así como internas de la organización para extraer una amplia variedad de información. Las fuentes externas incluyen fuentes como feeds de CERT y CSIRT, repositorios de malware, X (anteriormente Twitter) y otros feeds relevantes. Por otro lado, las fuentes internas se definen como fuentes que son internas de la organización e incluyen registros generados por servidores, registros de bases de datos, herramientas de monitoreo de seguridad, entre otros que están en la organización.

Los autores también plantean que en el intercambio de información CTI entre organizaciones, se fortalecen los conocimientos, la experiencia y las capacidades de prevención de cada organización participante frente a las ciber amenazas identificadas anteriormente o amenazas emergentes. El intercambio de CTI facilita el esfuerzo conjunto en la defensa contra ciberataques, ya que más organizaciones pueden recopilar información CTI y, en algunos casos, enriquecer los datos. Además, se mejora la seguridad de cualquier organización que participe en este esquema de colaboración, ya que sus CSIRT pueden planificar y desarrollar las contramedidas necesarias para la detección oportuna de los ataques más recientes.

Teniendo en cuenta lo anterior, los autores proponen ThreatWise AI, un enfoque holístico que permite la recopilación, análisis, el enriquecimiento y distribución de datos de CTI. ThreatWise AI proporciona un n marco que integra diferentes componentes novedosos. Los rastreadores web y de redes sociales desarrollados, y las instancias de Wazuh implementadas, permiten la recopilación, la extracción y el enriquecimiento de CTI, tanto de fuentes externas como internas. Las fuentes internas incluyen, entre otras, registros generados por servidores y bases de datos, herramientas de monitorización de seguridad (p. ej., herramientas IDS e IPS,

instancias de honeypot y otros servicios implementados y operativos dentro de una organización. Las fuentes externas, por otro lado, incluyen fuentes ubicadas fuera de las instalaciones de la organización, como las fuentes de CERT y CSIRT, bases de datos de vulnerabilidades, plataformas de redes sociales y otras fuentes relevantes. Además, el componente IS permite el almacenamiento, la correlación (es decir, el enriquecimiento) y la compartición de la CTI extraída de forma segura y eficiente (Spyros et al., 2025).

Diseño del Plan de Recolección de Inteligencia de Amenazas

Planificación y Dirección

Para la primera etapa, se debe considerar la inteligencia de amenazas estratégica, para esto, se debe tener en cuenta la participación de todas las partes como los equipos de seguridad, incluido el equipo de inteligencia de amenazas, la junta directiva, los Chief Information Security Officer (CISO), entre otras partes.

Objetivos de la Planificación y Dirección. Los objetivos definidos deben tener en cuenta el Core del negocio, por ejemplo, una empresa de transacciones en línea debe garantizar la alta disponibilidad de sus páginas transaccionales. Teniendo en cuenta el contexto del negocio, una empresa puede definir las amenazas a priorizar teniendo en cuenta los activos críticos:

Ataques de DDOS.

Vulnerabilidades en sistemas Operativos Windows, Linux y aplicaciones web.

Campañas de malware y ransomware teniendo en cuenta el contexto del negocio, por ejemplo, el mismo sector de la organización y/o el mismo país o región.

Explotación de vulnerabilidades en el mismo sector.

Fuentes a Integrar. AlienVault OTX: Permite verificar si los indicadores o vulnerabilidades detectadas en el análisis técnico aparecen asociados a campañas de ataque

reales o actividad maliciosa observada por la comunidad global de seguridad.
Aporta contexto operativo al proceso CTEM al relacionar vulnerabilidades con infraestructura maliciosa, malware o indicadores utilizados por atacantes, facilitando una mejor priorización del riesgo.

IBM X-Force Exchange: Permite consultar información contextual sobre vulnerabilidades, actores de amenaza y actividad de explotación observada, lo que ayuda a comprender el impacto potencial de una debilidad detectada.
Facilita la correlación entre vulnerabilidades identificadas en la infraestructura y tendencias globales de ataque, fortaleciendo la fase de priorización dentro del modelo CTEM.

EPSS: Proporciona una estimación probabilística sobre la posibilidad de que una vulnerabilidad sea explotada en el corto plazo, lo que permite priorizar remediaciones basadas en riesgo real y no solo en severidad teórica.
Complementa métricas como CVSS dentro del proceso CTEM, ayudando a enfocar recursos en vulnerabilidades con mayor probabilidad de explotación.

CISA KEV: Permite identificar rápidamente vulnerabilidades que ya están siendo explotadas activamente por atacantes, lo que facilita su priorización inmediata dentro del proceso de gestión de exposición.

Sirve como referencia confiable para validar si las vulnerabilidades detectadas representan una amenaza activa en el entorno global de ciberseguridad.

OWASP: El proyecto OWASP constituye una fuente ampliamente reconocida de conocimiento en seguridad de aplicaciones web. A través de iniciativas como el OWASP Top 10, la organización publica de forma periódica un conjunto de las vulnerabilidades y debilidades más críticas observadas en aplicaciones web a nivel global. Esta información se basa en el

análisis de datos provenientes de múltiples organizaciones de seguridad, investigadores y herramientas de evaluación de vulnerabilidades.

En el contexto de un programa de gestión continua de la exposición a amenazas (CTEM), OWASP constituye una fuente relevante para contextualizar debilidades identificadas durante los procesos de análisis de vulnerabilidades. Sus clasificaciones permiten relacionar vulnerabilidades técnicas detectadas en escaneos con categorías de riesgo ampliamente reconocidas en la industria, muchas de las cuales se encuentran asociadas con debilidades documentadas en **CWE**. Esto facilita comprender el impacto potencial de las vulnerabilidades en aplicaciones web y apoyar su priorización dentro del proceso de gestión de riesgos.

Periodicidad de la Recolección

En el marco del modelo de CTEM, la recolección de información se mantiene como un proceso continuo. La inteligencia de amenazas se revisa a diario, consultando fuentes como AlienVault OTX, IBM X-Force Exchange, el modelo EPSS y el catálogo CISA KEV, con el fin de identificar nuevas vulnerabilidades explotadas, cambios en el nivel de riesgo o campañas de ataque en curso.

Normalización de IOC/IOA

Los IOC E IOA se normalizarán utilizando el estándar STIX 2.1, el cual permite representar información de inteligencia de amenazas de forma estructurada y compatible entre distintas plataformas de seguridad.

Para la generación de estos indicadores se utilizará la librería stix2, desarrollada por OASIS Open, que permite crear objetos de inteligencia como Indicator, Malware o Threat Actor siguiendo la especificación oficial del estándar. Esta librería facilita la generación automática de los objetos en formato JSON, asegurando que los IOC e IOA mantengan una estructura

consistente y puedan integrarse posteriormente con plataformas de inteligencia de amenazas o herramientas de monitoreo como SIEM.

De esta forma, la normalización de los indicadores garantiza interoperabilidad, facilita su intercambio entre herramientas de seguridad y permite su correlación con eventos detectados dentro de la infraestructura.

Motor de Correlación

Dentro de una arquitectura completa de gestión de inteligencia de amenazas, la correlación de indicadores normalmente se realiza mediante plataformas de monitoreo y análisis de eventos de seguridad como un SIEM, que permiten integrar logs, eventos de red e indicadores de compromiso para detectar patrones de ataque.

Sin embargo, la implementación de un SIEM no forma parte del alcance técnico del presente proyecto. Por esta razón, la correlación de los IOC e IOA generados se plantea a nivel conceptual, considerando que en un entorno operativo estos indicadores podrían integrarse con plataformas SIEM como Splunk o Elastic, donde se realizaría el análisis y correlación automática con eventos de seguridad de la infraestructura.

Almacenamiento de la Geometría Temporal de Indicadores

La geometría temporal de los indicadores se gestionará utilizando los campos temporales definidos en el estándar STIX 2.1. Este modelo permite registrar información sobre el ciclo de vida de los indicadores mediante atributos como first_seen, last_seen, valid_from y valid_until, los cuales describen el momento en que un indicador fue observado por primera vez, su última observación y el periodo en el que se considera válido para detección o correlación.

Al utilizar este modelo estructurado, los IOC e IOA pueden conservar su contexto temporal dentro de los objetos STIX generados en formato JSON, lo que facilita su posterior

análisis, actualización o integración con plataformas de inteligencia de amenazas y sistemas de monitoreo de seguridad.

Determinación de Activos Críticos

La identificación de activos críticos es una etapa fundamental dentro de los procesos de gestión de seguridad de la información, ya que permite reconocer aquellos sistemas, datos o servicios cuya afectación podría generar un impacto significativo en la operación de una organización. Determinar estos activos facilita priorizar medidas de protección, orientar el análisis de riesgos y enfocar los esfuerzos de seguridad en los elementos más relevantes de la infraestructura tecnológica.

Para llevar a cabo esta actividad existen diferentes metodologías de análisis utilizadas en el ámbito de la ciberseguridad, entre las que se encuentran Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), OCTAVE y EBIOS Risk Manager. Cada una de estas metodologías propone enfoques distintos para identificar activos, evaluar su criticidad y analizar los riesgos asociados.

OCTAVE. OCTAVE es una metodología centrada en la identificación de activos críticos desde una perspectiva organizacional. Este enfoque se basa en el conocimiento interno de la organización, donde los responsables de procesos identifican la información y los sistemas más importantes para el funcionamiento del negocio. A partir de esta identificación se analizan las amenazas y vulnerabilidades que pueden afectar dichos activos (Carnegie Mellon University, 2001).

EBIOS Risk Manager. EBIOS Risk Manager es una metodología de análisis de riesgos que combina la identificación de activos con el análisis de escenarios de amenaza. Su enfoque se orienta a comprender cómo los actores de amenaza podrían afectar los activos estratégicos de

una organización, considerando tanto factores técnicos como contextuales. Esto permite evaluar riesgos desde una perspectiva más estratégica (ANSSI, 2018).

MAGERIT. MAGERIT es una metodología orientada al análisis y gestión de riesgos en sistemas de información. Su enfoque se basa en la identificación de activos, el análisis de sus dependencias y la evaluación del impacto que tendría su afectación sobre la organización. A partir de este análisis, permite determinar cuáles activos son críticos para la operación del sistema y priorizar su protección considerando dimensiones como disponibilidad, integridad y confidencialidad (Ministerio de Hacienda y Administraciones Públicas, 2012).

Para el desarrollo del proyecto se selecciona MAGERIT debido a que proporciona un enfoque más estructurado para la identificación y análisis de activos dentro de sistemas de información. La metodología permite modelar activos, establecer relaciones de dependencia entre ellos y evaluar su criticidad de forma sistemática, lo que facilita determinar cuáles elementos deben priorizarse dentro del proceso de análisis de seguridad. Además, su estructura metodológica permite documentar de manera clara el proceso de identificación de activos críticos dentro del contexto del proyecto.

En el contexto de MAGERIT, un activo es cualquier componente de un sistema de información susceptible de sufrir un ataque o incidente, ya sea intencionado o accidental, que afecte el funcionamiento o los intereses de la organización (Ministerio de Hacienda y Administraciones Públicas, 2012).

Esto abarca tanto los elementos técnicos como los humanos y organizativos: Información, datos, servicios, aplicaciones, equipos, redes, instalaciones y personas.

Los activos esenciales son dos: La información que se gestiona, y los servicios que se prestan. Estos dos elementos definen los requisitos de seguridad de todo el sistema y sirven como

eje central del análisis. A partir de ellos se identifican otros activos subordinados, como los datos que materializan esa información, las aplicaciones que permiten procesarla, los equipos que la alojan o los soportes donde se almacena.

Entre los activos complementarios también se incluyen las redes de comunicación, las instalaciones físicas, el equipamiento auxiliar (como los sistemas de energía o climatización), los servicios contratados a terceros y, de forma fundamental, el personal que opera o administra el sistema.

Cada tipo de activo requiere medidas de protección distintas. No se protege del mismo modo un servidor físico que un servicio en línea, ni un usuario que un sistema de climatización. Por esa razón, MAGERIT organiza los activos en categorías y capas, de manera que se pueda entender claramente cómo dependen unos de otros (Ministerio de Hacienda y Administraciones Públicas, 2012).

Dependencias Entre Activos. Los activos dentro de una organización no funcionan de forma aislada, sino que forman una estructura de dependencias jerárquicas.

Los activos más importantes, la información y los servicios se apoyan en otros activos inferiores como los equipos, las redes o las instalaciones, e incluso en el personal que los opera.

En este modelo, los activos “superiores” dependen de los “inferiores”. Si ocurre un fallo o una amenaza afecta a un activo de nivel inferior, el daño se propaga hacia los niveles superiores.

Por ejemplo, si se incendia el edificio donde se alojan los servidores, el servicio que ofrece la organización se interrumpe, aunque los usuarios estén a kilómetros de distancia.

Si se roba un portátil con información confidencial, el perjuicio recae sobre la confidencialidad de los datos, incluso si el equipo puede reemplazarse.

Estas relaciones permiten construir árboles o grafos de dependencias, que muestran cómo la seguridad de los activos críticos reside en los activos de soporte. En la práctica, esto implica que proteger adecuadamente los activos de base es esencial para garantizar la seguridad de los activos superiores.

Valoración de los Activos. Conocer el valor de un activo es esencial porque determina el nivel de protección que debe asignársele.

El valor no se refiere a su precio de compra, sino a la importancia o perjuicio que causaría su pérdida. Si un activo no aporta valor o su ausencia no afecta el funcionamiento, no tiene sentido invertir recursos en protegerlo.

Por el contrario, cuanto más crítico sea un activo, mayor será la necesidad de invertir en su protección (Ministerio de Hacienda y Administraciones Públicas, 2012).

En MAGERIT, el valor puede ser propio (el que posee por sí mismo) y acumulado **(**el que hereda por estar relacionado con otros activos de mayor importancia).

Generalmente, el valor central se encuentra en los activos esenciales, información y servicios, mientras que el resto de los activos obtiene su valor al contribuir a que estos funcionen correctamente.

Dimensiones de Valoración. El análisis de cada activo considera diversas dimensiones de seguridad, que reflejan los diferentes tipos de daño posibles:

Confidencialidad: Se refiere al perjuicio que causaría que la información llegara a personas no autorizadas.

Integridad: Evalúa el daño producido si los datos fueran alterados, dañados o eliminados.

Disponibilidad: Mide las consecuencias de no poder acceder a un activo o servicio cuando se necesita.

Además, en sistemas actuales, especialmente los relacionados con servicios electrónicos o administración digital, también se analizan:

Autenticidad: El riesgo de no poder verificar con certeza quién realiza una acción o accede a un recurso.

Trazabilidad: El daño derivado de no poder registrar y auditar adecuadamente el uso de los servicios o el acceso a los datos.

Estas dimensiones permiten caracterizar la seguridad de manera integral, más allá del enfoque tradicional de confidencialidad, integridad y disponibilidad (CID).

Métodos de Valoración. La valoración puede realizarse de dos maneras principales:

Cualitativa: Se basa en escalas de niveles (por ejemplo: bajo, medio, alto) para clasificar la importancia relativa de cada activo. Es rápida y útil cuando no se dispone de datos exactos, aunque su precisión es limitada y solo permite comparaciones aproximadas.

Cuantitativa: Asigna valores numéricos o monetarios, lo que facilita comparar costos y beneficios, calcular pérdidas y justificar inversiones. Aunque es más exigente en tiempo y datos, ofrece resultados mucho más objetivos y permite realizar análisis económicos, como:

Comparar el costo del riesgo frente al costo de las medidas de seguridad.

Evaluar la rentabilidad de una salvaguarda.

Determinar el monto razonable de una prima de seguro.

Establecer prioridades de inversión según el impacto potencial.

En ambos casos, la homogeneidad de criterios es fundamental para poder comparar activos y determinar cuál representa un riesgo mayor.

Detección de Amenazas. Una vez definidos los activos, se analizan las amenazas que pueden afectarlos, ya sean intencionadas (como ciberataques) o accidentales (fallos técnicos o

errores humanos) (Ministerio de Hacienda y Administraciones Públicas, 2012).

MAGERIT propone analizar las amenazas a partir de distintas fuentes de origen, clasificadas en cinco grandes categorías, cada una con características y consecuencias diferentes:

Amenazas de origen natural: Son eventos generados por la naturaleza como terremotos, inundaciones, tormentas eléctricas, incendios forestales, entre otro, ante los cuales los sistemas de información se comportan como víctimas pasivas.

Aunque no pueden evitarse, sí deben contemplarse dentro del análisis para determinar medidas de contingencia o recuperación.

Amenazas del entorno o de origen industrial: Surgen de factores externos relacionados con la infraestructura circundante o con actividades industriales. Pueden incluir cortes de energía, contaminación ambiental, fallos en redes eléctricas, explosiones o fugas químicas. Aunque la organización no tenga control directo sobre estos incidentes, su impacto puede ser severo, por lo que se deben prever mecanismos de protección física y continuidad de servicios.

Defectos en aplicaciones y sistemas: Estas amenazas provienen de errores en el diseño o implementación de software, hardware o firmware, lo que se conoce comúnmente como vulnerabilidades técnicas.

Muchos de estos fallos están documentados bajo la taxonomía CVE, reconocida internacionalmente como referencia para la gestión de vulnerabilidades.

Dichos defectos pueden ser aprovechados por atacantes para comprometer el sistema o provocar interrupciones no intencionadas en los servicios.

Amenazas accidentales causadas por personas: Incluyen los errores u omisiones humanas, como configuraciones incorrectas, borrado accidental de información, ejecución de comandos inapropiados o mal uso de equipos.

Aunque no existe intención de dañar, sus efectos pueden ser igual de graves que los provocados por un ataque.

Amenazas deliberadas o intencionadas: Son las más críticas, ya que implican una acción humana con un propósito específico: Robar información, alterar datos, interrumpir servicios o causar perjuicios económicos o reputacionales.

Entran aquí los ataques informáticos, sabotajes, espionaje, manipulación interna y cualquier otro acto malicioso orientado a vulnerar la seguridad del sistema.

La motivación puede ser económica, política, ideológica o simplemente de venganza.

Una vez identificadas las amenazas potenciales, se procede a evaluar su influencia sobre los activos.

Esta valoración se realiza considerando dos factores principales:

Degradación: Mide el grado de daño o pérdida de valor que sufriría el activo si la amenaza llegara a materializarse.

Probabilidad: Estima la posibilidad de que esa amenaza ocurra efectivamente.

En la tabla 8 se puede observar la valoración cualitativa de riesgos basada en la metodología Magerit, la cual establece niveles que permiten estimar la frecuencia de ocurrencia de una amenaza en función de su probabilidad y dificultad de materialización.

Tabla 8

Valoración Cualitativa de Riesgos

Nivel	Significado	Frecuencia estimada
MA	Muy alta	Casi seguro / fácil
A	Alta	Muy probable / media
M	Media	Posible / difícil
B	Baja	Poco probable / muy difícil
MB	Muy baja	Muy rara / extremadamente difícil

Nota. La tabla presenta la clasificación de los niveles de riesgo (MA, A, M, B, MB), indicando su significado cualitativo y la frecuencia estimada de ocurrencia, de acuerdo con los criterios definidos por la metodología Magerit para el análisis de riesgos. Tomado de. Magerit v3 – Libro I: Método, CCN-CERT. (s. f.) https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

En la tabla 9 se puede observar la valoración cuantitativa de riesgos, en la cual se asignan valores numéricos a cada nivel definido por la metodología Magerit, con el fin de facilitar el análisis y priorización de los riesgos identificados.

Tabla 9

Valoración Cuantitativa de Riesgos

Nivel	Valor numérico aproximado	Frecuencia estimada
MA	5	Casi seguro / fácil
A	4	Muy probable / media
M	3	Posible / difícil
B	2	Poco probable / muy difícil
MB	1	Muy rara / extremadamente difícil

Nota. La tabla presenta la equivalencia entre los niveles de riesgo (MA, A, M, B, MB) y sus valores numéricos aproximados, junto con la frecuencia estimada de ocurrencia, de acuerdo con el enfoque cuantitativo propuesto por la metodología Magerit para la evaluación de riesgos. Tomado de. Magerit v3 – Libro I: Método, CCN-CERT. (s. f.) https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

Salvaguardas. En esta fase, se incorporan las salvaguardas o contramedidas al proceso de análisis de riesgos. Mientras los pasos previos evalúan los riesgos suponiendo que los activos carecen de protección, este paso reconoce que, en la práctica, los sistemas suelen contar con múltiples medidas defensivas.

Las salvaguardas se definen como los mecanismos técnicos, organizativos, físicos o humanos que reducen el riesgo al disminuir la probabilidad de ocurrencia de una amenaza o mitigar sus consecuencias. Estas pueden ir desde políticas internas y capacitación del personal, hasta soluciones tecnológicas, controles de acceso o medidas de seguridad física.

El catálogo de elementos de MAGERIT se dedica relacionar salvaguardas apropiadas

para cada tipo de activo, lo que permite seleccionar las más relevantes considerando:

El tipo de activo que se protege.

Las dimensiones de seguridad involucradas (confidencialidad, integridad, disponibilidad, etc.).

Las amenazas a cubrir.

La existencia de salvaguardas alternativas.

Asimismo, se recomienda aplicar el principio de proporcionalidad, priorizando la protección de activos más valiosos y los riesgos con mayor probabilidad o impacto. Las salvaguardas que no son adecuadas se excluyen mediante dos categorías:

No aplica: Cuando no es técnicamente apropiada.

No se justifica: Cuando resulta desproporcionada respecto al riesgo.

El resultado de este proceso es la declaración de aplicabilidad, un documento que resume qué salvaguardas será implementadas o evaluadas dentro del sistema de protección.

Finalmente, MAGERIT distingue dos efectos principales de las salvaguardas:

Preventivas: Reducen la probabilidad de que una amenaza se materialice.

Limitadoras: Disminuyen el daño o facilitan la detección y recuperación tras un incidente

Estimación del Impacto. Se determina el daño que podría sufrir un activo si una amenaza llegara a materializarse. Este impacto puede ser económico, operativo, reputacional o legal.

En la tabla 10 se puede observar un ejemplo de la identificación y valoración de los activos de información correspondientes a los servidores web, incluyendo su descripción, amenazas identificadas, vulnerabilidades, valoración del riesgo según Magerit y aspectos relacionados con su gestión y protección.

Tabla 10

Sevidores Web

Nombre del activo de información	SERPAGOS01
Descripción	PASARELA DE PAGOS DE LOS CLIENTES
cantidad	2
Tipo de activo de información	SERVIDOR WEB
Identificación de amenazas	Acceso no autorizado: La empresa todavía no ha implementado un CDN que permita proteger los sitios web contra ataques de DDOS Uso no previsto: Un ataque exitoso de DDOS podría afectar la disponibilidad de la pasarela de pagos. Vulnerabilidades aplicaciones web(software): Las aplicaciones web también pueden ser vulnerables, por lo que requieren actualizaciones periódicas y la empresa no ha implementado todavía una política que garantice esto. Difusión de software dañino: La explotación exitosa de una vulnerabilidad en una base de datos podría permitir la difusión de malware, la filtración de datos, entre otras acciones maliciosas.
Valoración del activo según Magerit	Probabilidad del riesgo: Poco probable (B). Impacto del Riesgo: Alto (A). Estimación del impacto MA, Riesgo MA. Valoración del riesgo: Critico (MA).
Proceso al que pertenece	Relación con los clientes.
Sistema Operativo	Ubuntu Server 22.04 LTS
Propietario del activo de información	Área de finanzas
Responsable del activo de información	Andrea Mendez (funcionario)
Custodio del activo de información	Área de infraestructura

Nombre del activo de información	SERPAGOS01
Dueño del dato	Clientes
Tipo de información que gestiona	Reservada, de acuerdo con la ley 1712 de 2014.
Tipo de datos que contiene	datos personales, de acuerdo con la ley 1581 de 2012.
Requiere registrar ante el Registro Nacional de Bases de Datos (RNBD)	sí, debido a que la base de datos contiene información de datos personales.
Ubicación del activo	Oficina, servidor Onpremise

*Nota***.** La tabla presenta la identificación y valoración del activo de información "servidor web", incluyendo atributos como tipo de activo, amenazas, vulnerabilidades, valoración del riesgo, responsables, tipo de información gestionada y requisitos normativos asociados.

En la tabla 11 se puede observar la identificación y valoración de los activos de información correspondientes a los servidores en producción, incluyendo sus principales amenazas, vulnerabilidades y aspectos relacionados con su gestión operativa.

Tabla 11

Servidores en Producción

Nombre del activo de información	Servidor de aplicaciones
Descripción	Alojan las aplicaciones de la empresa
Cantidad	5
Tipo de activo de información	Hardware
Identificación de amenazas	De origen natural: El datacenter en donde está ubicado el servidor no tiene un plan de contingencia contra accidentes naturales. Errores y fallos no intencionados: Existe la posibilidad de que se presenten fallos por una manipulación no adecuada del servidor por parte de los encargados. Avería del Hardware: El servidor puede presentar posibles fallos relacionados con Hardware, debido a que cuenta a cuenta con ventiladores que ya no funcionan correctamente. Contaminación mecánica: Se ha identificado vibraciones en el área donde se encuentran ubicados los servidores por labores de mantenimiento en el edificio porque lo que estas pueden causar daños a los discos duros u otros componentes de los servidores.
Valoración del activo según Magerit	Probabilidad del riesgo: Posible (B), valoración 3. Impacto del Riesgo: Alto (A), Valoración 4. Estimación del impacto MA, Riesgo MA. Valoración del riesgo: Critico (MA), Valoración 21 a 25.
Proceso al que pertenece	GESTIÓN DE APLICACIONES
Propietario del activo de información	Área de IT y Soporte Técnico.
Sistema operativo	Windows Server 2016
Responsable del activo de información	Marlon Agudelo
Custodio del activo de información	Área de IT y Soporte Técnico.
Dueño del dato	N/A
Tipo de información que gestiona	Reservada, de acuerdo con la ley 1712 de 2014.

Nombre del activo de información	Servidor de aplicaciones
Tipo de datos que contiene	Semiprivados, de acuerdo con la ley 1581 de 2012.
Requiere registrar ante el RNBD	No
Ubicación del activo	Data center tier 3 ubicado en Bogotá.

*Nota***.** La tabla presenta la identificación y valoración de los servidores de aplicaciones, considerando amenazas, nivel de riesgo, responsables y características de la información gestionada.

Responsable de la Recolección de Información Sobre Amenazas. El responsable de esta actividad será el equipo de inteligencia de amenazas, encargado de recopilar, analizar y mantener actualizada la información sobre posibles riesgos que puedan afectar a los activos de la organización.

Fuentes de Inteligencia de Amenazas. La recopilación de datos se realizará a partir de los feeds de AlienVault OTX y de IBM X-Force Exchange. La información obtenida se puede integrar en plataformas SIEM como Elastic Search y Splunk mediante API, que funcionan como motor de correlación. La recolección se puede programar de forma automatizada cada 6 horas para asegurar la disponibilidad de información reciente. Todos los indicadores (IPs, dominios, hashes) se normalizarán en formato STIX 2.1, permitiendo analizar la evolución de las amenazas y reforzar la gestión dentro del ciclo CTI.

STIX 2.1 es una versión mejorada del estándar STIX 2.0 para el intercambio de inteligencia de amenazas. Introduce nuevos objetos como Agrupación, Infraestructura, Ubicación, Análisis de malware, Nota y Opinión, y realiza cambios significativos en objetos existentes como malware y todos los SCO (ciber observables). También incorpora nuevos conceptos, como el nivel de confianza en la información. STIX 2.1 permite relacionar

directamente los objetos ciber observables mediante objetos de relación, agrega propiedades para describir avistamientos y ubicaciones, corrige nombres conflictivos en objetos de directorio, archivo, proceso y claves de registro de Windows, y facilita relaciones externas para dominios y direcciones IP. Además, incluye una nueva relación entre indicadores y datos observados denominada “basado en”, optimizando la trazabilidad y análisis de amenazas en entornos de inteligencia cibernética (OASIS, s.f.).

Las plataformas SIEM, como Elastic Search o Splunk, permiten crear índices específicos para almacenar información de inteligencia de amenazas. Esto significa que cada tipo de indicador, como IPs, dominios, hashes, TTPs o CVE puede ser organizado en un índice separado, optimizando la búsqueda, la correlación y el análisis histórico. Además, al mantener índices dedicados para CTI, es posible realizar consultas rápidas, generar dashboards personalizados y conservar la geometría temporal de los indicadores mediante timestamp de recepción, primera y última aparición, en base de datos centralizada en formato temporal para permitir análisis de evolución de amenazas y retroalimentación al CTEM.

Lo anterior puede facilitar la trazabilidad de eventos y la integración con el ciclo de vida de la inteligencia de amenazas.

Recopilación

Con el propósito de ilustrar el desarrollo del plan de recolección de inteligencia de amenazas, se plantea un caso de ejemplo basado en una organización del sector financiero. Este entorno simulado cuenta con una infraestructura tecnológica compuesta por servidores Linux y Windows, los cuales alojan aplicaciones web y servicios internos críticos.

Objetivo de Recopilación. Recolectar información relevante sobre amenazas cibernéticas que puedan afectar a la infraestructura tecnológica del negocio financiero, garantizando que

las fuentes sean confiables, actualizadas y alineadas con los activos críticos identificados durante la planificación.

Contexto del Negocio. La organización pertenece al sector financiero, un entorno altamente regulado y sensible a incidentes de fraude digital, robo de credenciales, ransomware y ataques dirigidos.

Su infraestructura tecnológica se compone de:

Servidores Linux, que alojan aplicaciones web y servicios críticos (bases de datos, API REST, entornos de desarrollo).

En el caso de los servidores que alojan aplicaciones web, estas constituyen un activo crítico debido a su exposición directa a internet y a la gran cantidad de vulnerabilidades que suelen presentar. Las aplicaciones web permiten la interacción con clientes y usuarios finales, ofreciendo servicios financieros, administrativos o informativos, y son un objetivo frecuente de los atacantes. Las aplicaciones que aloja se encuentran los portales de autenticación y banca en línea, los sistemas de gestión de contenido como WordPress, Drupal o Joomla, WSO2 las plataformas de comercio electrónico como Magento, PrestaShop o WooCommerce, entre otras aplicaciones como WSO2 y los paneles administrativos internos o APIs, y las aplicaciones desarrolladas a medida que ofrecen servicios o integraciones específicas dentro de la organización.

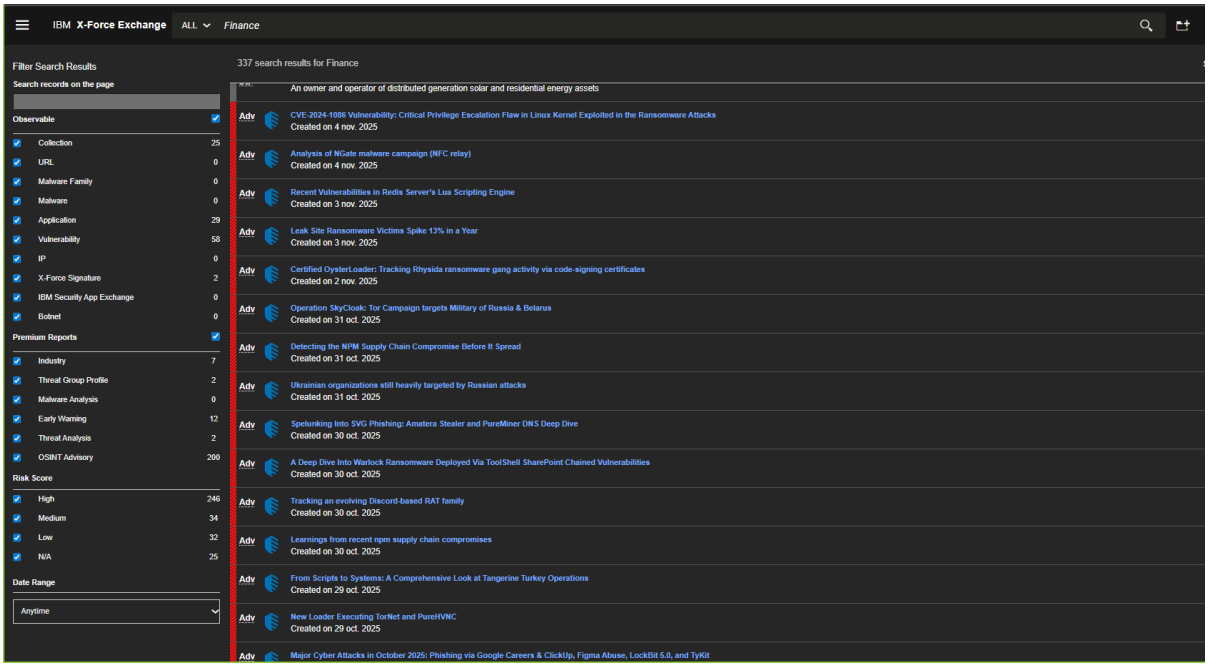
Servidores Windows, que soportan servicios empresariales internos (Active Directory, correo electrónico, autenticación, aplicaciones .NET).

Sector Financiero. Se comienza con la recopilación de noticias y reportes de inteligencia sobre eventos e incidentes de ciberseguridad que impactan al sector financiero.

En la figura 46 se observa la consulta realizada en IBM X-Force Exchange, donde se identificaron 337 resultados relacionados con el sector financiero. Estos abarcan reportes de vulnerabilidades, análisis de malware, campañas de ransomware y advertencias de inteligencia (OSINT Advisories), reflejando la actividad de amenazas enfocadas en este tipo de entornos.

Figura 46

IBM X-Force Exchange: Consulta de Noticias Por Sector Financiero



Nota. Consulta de IOC en IBM X-Force Exchange. Elaboración propia a partir de datos obtenidos de IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

Hallazgos más Relevantes Identificados. A la fecha de consulta (04 de noviembre de 2025), se identificaron los siguientes hallazgos por categoría:

Vulnerabilidades en Linux. CVE-2024-1086 (Alto, CVSS 3.1: 7.8): El 4 de noviembre de 2025, IBM X-Force Exchange compartió un nuevo aviso sobre la vulnerabilidad CVE-2024-1086, la cual sigue siendo explotada activamente en ataques de ransomware, especialmente

dirigidos a organizaciones del sector financiero y de servicios críticos. La alerta surge tras detectarse un incremento reciente en el uso de este fallo por parte de grupos criminales, que lo emplean como punto de entrada para comprometer servidores Linux no actualizados (IBM, 2024).

La vulnerabilidad corresponde a un error de tipo use-after-free en el componente netfilter del kernel de Linux. Este componente gestiona el filtrado de paquetes y la traducción de direcciones de red, por lo que su explotación permite a los atacantes obtener privilegios administrativos y desplegar ransomware o implantar puertas traseras persistentes. Aunque el fallo fue corregido en enero de 2024, las campañas de explotación se intensificaron durante el último trimestre de 2025, lo que motivó la publicación del nuevo informe de IBM.

CISA había incluido esta vulnerabilidad en su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV) desde mayo de 2024, pero la reciente actividad maliciosa sugiere que muchos sistemas aún no han aplicado los parches de seguridad. Además, desde marzo de 2024 circula una prueba de concepto pública (PoC) que facilita su explotación en kernels entre las versiones 5.14 y 6.6, aumentando el riesgo para infraestructuras empresariales.

El informe de IBM también advierte que las vulnerabilidades sin mitigar continúan siendo la principal causa técnica de los ataques de ransomware, representando cerca del 32 % de los incidentes según el State of Ransomware 2025 de Sophos. A esto se suma la persistente amenaza de credenciales comprometidas y campañas de ingeniería social. En un contexto donde el NIST ha registrado más de 40 000 nuevas vulnerabilidades en lo corrido del año, la publicación busca llamar la atención sobre la necesidad de monitoreo continuo, aplicación de parches y gestión proactiva de riesgos.

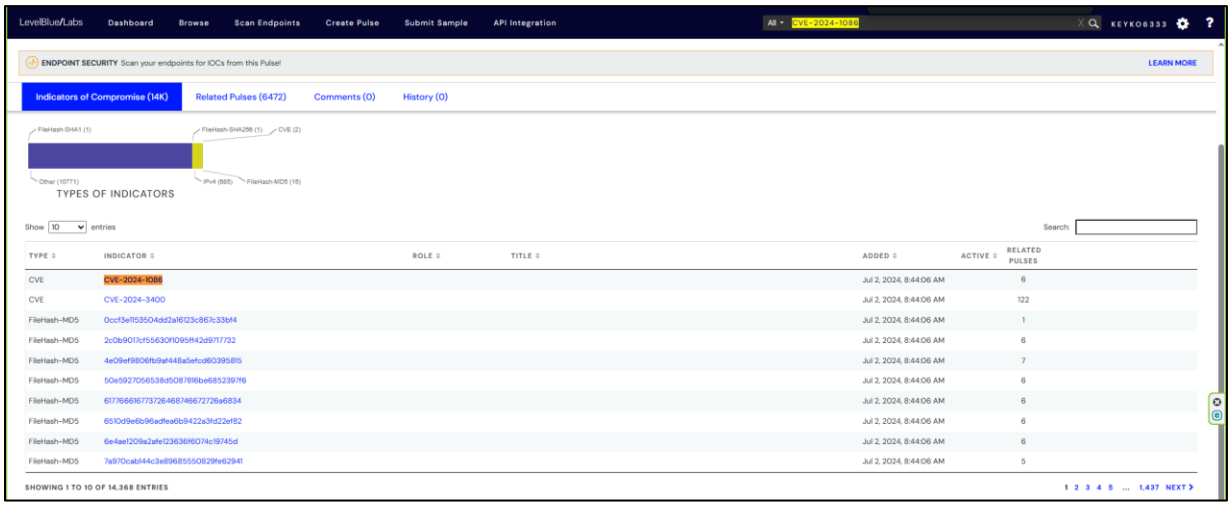
La alerta del 4 de noviembre refleja no solo la importancia de mantener la infraestructura Linux actualizada, sino también el valor de contar con fuentes de inteligencia de amenazas que permitan anticipar los ataques antes de que impacten los sistemas más sensibles del negocio IBM (X-Force Exchange, s.f.).

POC: En este caso se identificó una POC publica que demuestra como explotar la vulnerabilidad en GitHub.

En la figura 47 se pueden observar indicadores de compromiso en AlienVault OTX asociados a posibles intentos de explotación de la vulnerabilidad CVE-2024-1086. Entre los resultados aparecen hashes MD5 y referencias a la vulnerabilidad CVE-2024-3400 de Palo Alto Networks, lo que sugiere una posible relación dentro del mismo contexto de explotación.

Figura 47

Consulta de IOC en Alien Vault



Nota. Consulta de IOC en AlienVault OTX. Elaboración propia a partir de datos obtenidos de Open Threat Exchange (OTX), LevelBlue. (s. f.) https://otx.alienvault.com/

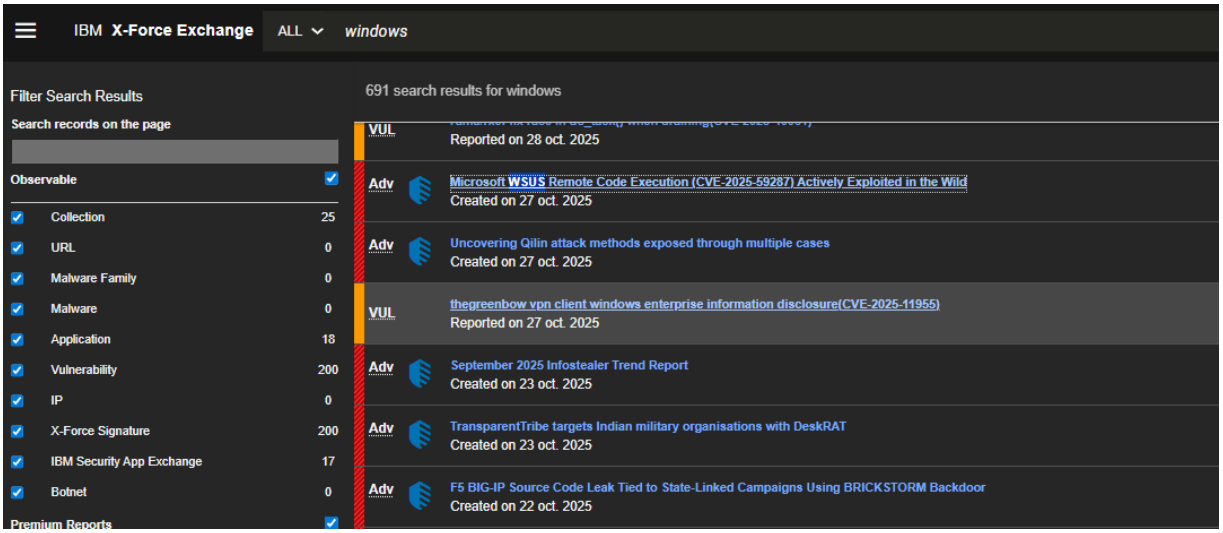
***Vulnerabilidades en Windows*.** La búsqueda con la palabra clave “Windows” en IBM X-Force Exchange muestra varios resultados relacionados con amenazas, vulnerabilidades y campañas activas que afectan a entornos basados en este sistema operativo. Entre los hallazgos se destacan vulnerabilidades críticas, como la ejecución remota de código no autenticado en el servicio Windows Server Update Services (WSUS), y fallos asociados a manipulación de rutas (path manipulation), que podrían permitir a los atacantes ejecutar código o alterar archivos en el sistema. Asimismo, se identifican informes sobre campañas de malware (como ValleyRAT y Gootloader) y actividades de grupos de amenazas persistentes vinculados a espionaje o ransomware.

Estas tendencias reflejan que los sistemas Windows continúan siendo un objetivo prioritario para atacantes debido a su amplia presencia en entornos empresariales y gubernamentales.

En la figura 48 se muestra la consulta de vulnerabilidades asociadas a Windows dentro de IBM X-Force Exchange, donde se agrupan distintos reportes de seguridad relacionados con este sistema operativo.

Figura 48

Consulta de Vulnerabilidades en Windows



Nota. Consulta de vulnerabilidades en Windows. Elaboración propia a partir de datos obtenidos de IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

CVE-2025-59287 (Critico, CVSS3.1: 9.8): Es una vulnerabilidad crítica de deserialización en el servicio WSUS, que representa un riesgo considerable para los servidores que aún no han sido actualizados. El fallo permite que un atacante remoto, sin necesidad de autenticación, ejecute código arbitrario en el sistema debido a una gestión insegura de los datos de WSUS a través del componente AuthorizationCookie. Este error puede ser aprovechado para obtener privilegios de SYSTEM, comprometer completamente el servidor y facilitar movimientos laterales dentro de la red.

Microsoft publicó una actualización de emergencia después de detectar que los parches iniciales no corregían completamente el problema. La gravedad de esta vulnerabilidad radica en que puede explotarse a través de la red sin requerir credenciales válidas, alcanzando una puntuación CVSS de 9.8. Entre los vectores de ataque posibles se encuentran los procesos

GetCookie() y los servicios web de reporte de WSUS, los cuales pueden ser manipulados por actores maliciosos para ejecutar código de manera remota.

Como medida de mitigación, Microsoft recomendó aplicar la actualización de seguridad del 23 de octubre de 2025, limitar el acceso a los puertos de administración de WSUS y deshabilitar el rol del servidor si no es estrictamente necesario, reduciendo así la exposición ante posibles ataques

Existe una prueba de concepto pública en GitHub que demuestra como explotar la vulnerabilidad.

Indicadores de compromiso: En la figura 49 se muestran los indicadores de compromiso (IOC) identificados durante la investigación en IBM X-Force Exchange se encontraron varios indicadores asociados por Darktrace a una campaña de explotación. En términos generales, la evidencia incluye hostnames sobre workers.dev (uso probable de Cloudflare Workers), URIs que apuntan a instaladores .msi (probables payloads) y una dirección IP pública que sirve recursos y podría funcionar como infraestructura de mando y control (C2) (Foulger, 2025).

De forma resumida:

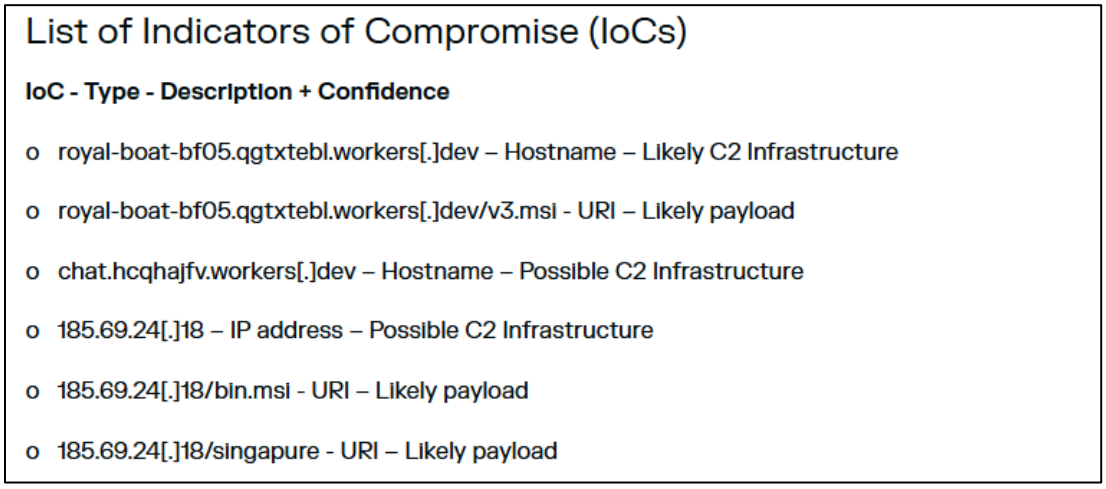
Hostnames y dominios: Probablemente usados como C2 o proxys de entrega.

URIs con archivos .msi: Posible entrega de payloads dirigidos a sistemas Windows.

Dirección IP: Servidor directo que aloja recursos (verificar geolocalización y ASN).

Figura 49

IOC Identificados



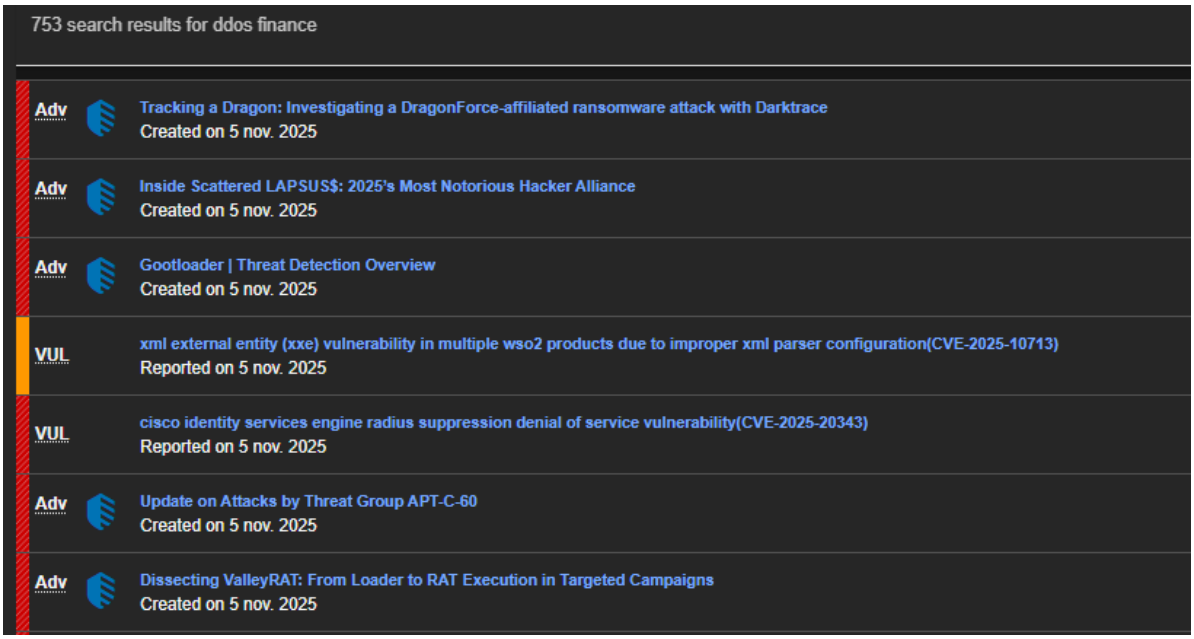
Nota. IOC identificados relacionados con CVE-2025-59287. Tomado de. Darktrace. (2025) https://www.darktrace.com/blog/wsus-exploited-darktraces-analysis-of-post-exploitation-activities-related-to-cve-2025-59287

Ataques de DDOS (Aplicaciones Web). En la figura 50 se visualiza la investigación realizada como parte del proceso de recolección de inteligencia de amenazas, se realizó una búsqueda en la plataforma IBM X-Force Exchange utilizando las palabras clave “DDoS finance”. Los resultados obtenidos incluyen reportes recientes relacionados con campañas de ransomware, vulnerabilidades críticas y amenazas avanzadas que pueden impactar directamente a las entidades del sector financiero. Entre los hallazgos destacan informes sobre actividades del grupo DragonForce, incidentes vinculados a LAPSUS$, así como vulnerabilidades activas como CVE-2025-10713 (asociada a WSO2) y CVE-2025-20343 (relacionada con Cisco Identity Services Engine (ISE)). Estos resultados evidencian la diversidad de tácticas y vectores de ataque utilizados por los actores de amenazas que podrían aprovecharse para ejecutar ataques de

denegación de servicio o comprometer la infraestructura tecnológica de instituciones financieras (X-Force Exchange, s.f.).

Figura 50

Investigación Relacionada con Ataques de DDOS



Nota. Elaboración propia a partir de datos obtenidos de IBM X-Force Exchange, relacionados con ataques DDoS en el sector financiero, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

Entre los resultados más importantes se encuentra la vulnerabilidad detectada en WSO2, aplicación con la que cuenta la organización en el caso hipotético.

CVE-2025-10713 (Medio, CVSS3.1: 6.5): IBM X-Force Exchange publicó una advertencia sobre la vulnerabilidad CVE-2025-10713, la cual afecta a varios productos de WSO2. Este fallo está relacionado con una configuración incorrecta del analizador XML, lo que puede provocar que las aplicaciones procesen datos enviados por los usuarios sin las restricciones necesarias. En la práctica, esto significa que un atacante podría aprovechar la forma

en que el sistema interpreta los archivos XML para acceder a información interna o causar la interrupción de los servicios.

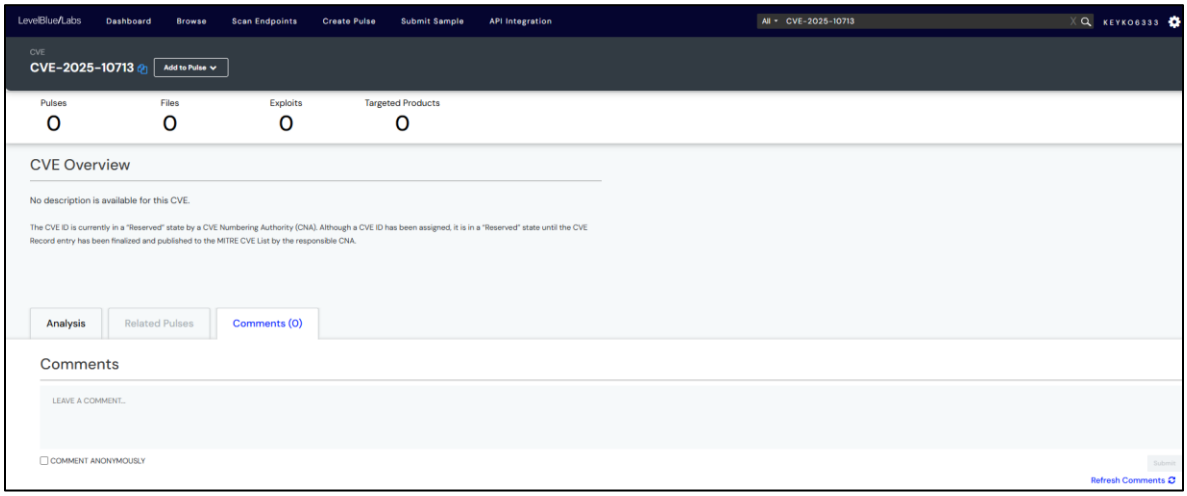
Esta vulnerabilidad pertenece a la categoría XML External Entity (XXE), un tipo de error que ocurre cuando una aplicación permite que el código XML enviado por un usuario haga referencia a archivos o recursos externos. Si un servidor afectado procesa ese XML malicioso, puede revelar archivos del sistema, como configuraciones o contraseñas, o incluso ejecutar acciones que saturen los recursos y provoquen una denegación de servicio.

En la figura 51 se puede observar la investigación relacionada con la vulnerabilidad CVE-2025-10713. Dado que WSO2 se utiliza con frecuencia para exponer y gestionar APIs y servicios web, el impacto directo recae sobre aplicaciones web empresariales, en especial aquellas que manejan datos sensibles o autentican usuarios. Un ataque exitoso podría permitir la lectura de archivos internos, la filtración de información confidencial o la interrupción temporal de servicios críticos, lo que representa un riesgo considerable para sectores como el financiero, donde estos sistemas suelen integrarse con pasarelas de pago y plataformas de gestión de clientes (X-Force Exchange, s.f.).

En Alien Vault OTX no se evidencian pulsos relacionados con la vulnerabilidad, por lo que es muy poco probable que este siendo explotada activamente.

Figura 51

Consulta de IOC CVE-2025-10713



Nota. Elaboración propia a partir de datos obtenidos de Open Threat Exchange (OTX), relacionados con IOC de CVE-2025-10713, LevelBlue. (s. f.) https://otx.alienvault.com/

Procesamiento y Explotación

En esta fase, la información recopilada desde diversas fuentes de inteligencia como AlienVault OTX, IBM X-Force Exchange y repositorios públicos como GitHub, se somete a un proceso de depuración, normalización y clasificación con el fin de convertir los datos brutos en información estructurada y analizable. El propósito es garantizar que los indicadores de compromiso (IoC), vulnerabilidades y evidencias técnicas obtenidas puedan ser interpretadas de manera uniforme y comparadas entre sí para detectar patrones relevantes.

Durante el procesamiento, los datos se organizaron según su tipo de amenaza, nivel de criticidad, sistema afectado y evidencia de explotación. Asimismo, se integraron las pruebas de concepto asociadas y los IoC identificados, clasificándolos en categorías como direcciones IP, dominios, URL y hashes de archivo. Esta estructuración facilita la posterior fase analítica,

permitiendo establecer correlaciones entre vulnerabilidades activamente explotadas y posibles vectores de ataque dentro del entorno de estudio.

En la figura 52 resume los resultados del procesamiento, mostrando de forma consolidada la información validada y transformada durante esta etapa del ciclo de vida de la inteligencia de amenazas. Los datos están presentados en un formato orientado a analistas, que facilita la revisión humana.

Figura 52

Procesamiento de Inteligencia de Amenazas

Vulnerabilidad (CVE)	Sistema afectado	Severidad (CVSS 3.1)	Descripción breve	Prueba de concepto (PoC)	Indicadores de compromiso (IoC)	Fuente	Estado de explotación	EPSS
CVE-2024-1086	Linux	Alto (7.8)	Falla *use-after-free* en el módulo netfilter del kernel que permite escalada local de privilegios.	GitHub – Notselwyn	**Hashes MD5 asociados:** 0ccf3e1153504dd2a16123c867c33bf4 2c0b9017cf55630f1095ff42d9717732 4e09ef9806fb9af448a3efcd60395815 50e5927056538d5087816be6852397f6 617766616773726468746672726a6834 6510d9e6b96adfea6b9422a3fd22ef82 6e4ae1209a2afe123636f6074c19745d 7a970cab144c3e89685550829fe62941	IBM X-Force Exchange, AlienVault OTX	Explotada activamente	0.86
CVE-2025-59287	Windows (WSUS)	Crítico (9.8)	Vulnerabilidad de deserialización que permite ejecución remota de código sin autenticación.	GitHub – tecxx	**Dominios y rutas asociadas:** royal-boat-bf05.qgtxtebl.workers[.]dev chat.hcqhajfv.workers[.]dev royal-boat-bf05.qgtxtebl.workers[.]dev/v3.msi 185.69.24[.]18 185.69.24[.]18/bin.msi 185.69.24[.]18/singapure	IBM X-Force Exchange, Darktrace, AlienVault OTX	Explotada activamente	0.64
CVE-2025-10713	Aplicaciones web (WSO2)	Medio (6.5)	Vulnerabilidad XXE por configuración insegura del analizador XML que puede permitir acceso a archivos internos o DoS.	—	No se evidencian IoC o pulsos relacionados.	IBM X-Force Exchange, AlienVault OTX	No se evidencia explotación activa	N/A

Nota. Elaboración propia a partir de datos obtenidos de IBM X-Force Exchange, IBM. (s. f.) https://exchange.xforce.ibmcloud.com/

A continuación, se presentan los indicadores en formato STIX 2.1 estructurados en JSON, los cuales pueden generarse mediante la librería oficial **stix2**, un proyecto de código

abierto desarrollado en Python por OASIS Open para la creación y manipulación de objetos conformes al estándar STIX. Esta librería permite construir programáticamente entidades como Indicator, Malware o Threat Actor, así como establecer relaciones entre ellas, garantizando que los objetos generados cumplan con la especificación STIX 2.1. Asimismo, facilita la serialización automática en formato JSON válido, lo que permite su integración automatizada con plataformas de inteligencia de amenazas y herramientas de monitoreo como SIEM (por ejemplo, Splunk o Elastic Stack), asegurando interoperabilidad, trazabilidad y capacidades avanzadas de correlación dentro de entornos de ciberseguridad (OASIS Open, 2023).

Adicionalmente, el estándar STIX permite gestionar la dimensión temporal de los indicadores, lo que facilita registrar el ciclo de vida de un IOC o IOA dentro del modelo de inteligencia de amenazas. Para ello, se emplean atributos como *first_seen*, *last_seen*, *valid_from* y *valid_until*, los cuales describen cuándo un indicador fue observado por primera vez, la última vez que se registró actividad asociada y el periodo en el que se considera vigente para procesos de detección o análisis. Esta información temporal resulta especialmente útil para mantener actualizados los repositorios de inteligencia, evitar el uso de indicadores obsoletos y mejorar los procesos de correlación en plataformas de monitoreo y análisis de seguridad.

Varios estudios coinciden en que la inteligencia de amenazas solo resulta útil cuando puede integrarse de forma práctica en los procesos de defensa de una organización. Haass (2022) señala que el volumen actual de información y la velocidad con la que evolucionan las amenazas hacen insuficiente una recopilación aislada de datos; lo realmente importante es la capacidad de organizar, validar y contextualizar esa información para convertirla en insumos que apoyen la toma de decisiones.

En ese sentido, el trabajo desarrollado no se limitó a la búsqueda de indicadores de compromiso o vulnerabilidades relevantes, sino que incorporó una etapa de organización y clasificación de la información obtenida. Los datos recopilados desde fuentes como IBM X-Force Exchange y AlienVault OTX fueron revisados y estructurados según el sistema afectado, el tipo de amenaza, su severidad y la evidencia de explotación disponible. Este ejercicio permitió diferenciar entre hallazgos meramente informativos y aquellos con impacto potencial directo sobre los activos analizados.

Adicionalmente, el mapeo de las amenazas identificadas con el marco MITRE ATT&CK facilitó comprender cómo podrían materializarse los ataques en el entorno evaluado. Más allá de asignar una severidad técnica, este enfoque ayudó a visualizar el comportamiento del adversario y su posible encadenamiento de técnicas, aportando mayor claridad al análisis posterior.

De esta forma, el plan de recolección y procesamiento adoptado se ajusta a las recomendaciones planteadas en la literatura, al priorizar la estructuración y el análisis crítico de la información sobre la simple acumulación de datos. Esto permitió que la inteligencia generada fuera coherente con las necesidades del entorno estudiado y útil para fortalecer las decisiones relacionadas con la gestión de la exposición a amenazas.

Tendencias Actuales en Automatización e Inteligencia se Amenazas. La evolución reciente de la inteligencia de amenazas ha estado marcada por la incorporación de técnicas de automatización y aprendizaje automático orientadas a mejorar la detección temprana y reducir la carga operativa de los equipos de seguridad. Estudios como los de Simran et al. (2024) y Saddi et al. (2024) destacan que el uso de inteligencia artificial permite analizar grandes volúmenes de datos, identificar patrones anómalos y disminuir la tasa de falsos positivos, aspectos especialmente relevantes en entornos donde los recursos humanos son limitados.

Desde una perspectiva más aplicada, Spyros et al. (2025) proponen un enfoque holístico denominado ThreatWise AI, el cual integra la recopilación, análisis, enriquecimiento y distribución de CTI mediante fuentes internas (registros, IDS/IPS, honeypots) y externas (CERT, CSIRT, redes sociales, repositorios de vulnerabilidades). Este enfoque refuerza la importancia de la automatización y el intercambio colaborativo como elementos clave para fortalecer la postura defensiva organizacional.

Aunque el presente trabajo no contempla la implementación directa de modelos de machine learning como los descritos en los marcos AI Shield o Red AI, el diseño del plan de inteligencia adoptó principios compatibles con estas tendencias. En particular, se priorizó la integración de múltiples fuentes externas, la actualización constante de información y la correlación de indicadores con vulnerabilidades internas detectadas en el entorno evaluado.

Asimismo, la revisión de literatura resalta la importancia de combinar datos provenientes de sistemas internos con información externa especializada para lograr una priorización más precisa de eventos y amenazas. En coherencia con esta perspectiva, el plan desarrollado articuló la inteligencia obtenida desde plataformas como IBM X-Force Exchange y AlienVault OTX con los hallazgos del análisis de vulnerabilidades, evitando que ambos procesos operaran de manera aislada.

De esta manera, aunque el laboratorio se desarrolló en un entorno académico y controlado, el enfoque metodológico adoptado refleja las prácticas actuales orientadas a la automatización progresiva de la inteligencia de amenazas, sentando bases que podrían ampliarse en el futuro mediante herramientas más avanzadas de análisis predictivo.

Análisis

En esta fase, la información procesada se examina para identificar patrones, correlaciones

y comportamientos que indiquen posibles amenazas activas o emergentes. Los analistas revisan los indicadores de compromiso recopilados, como direcciones IP, hashes de archivos o dominios sospechosos, con el fin de determinar su relevancia, nivel de riesgo y relación con campañas o vulnerabilidades específicas.

El análisis permite contextualizar los hallazgos dentro del entorno de la organización y priorizar las acciones de mitigación. Esta inteligencia generada sirve de insumo para los equipos de seguridad y contribuye directamente con la etapa de validación del marco CTEM, ya que facilita la verificación de las amenazas que realmente representan un riesgo para los activos críticos o superficies de exposición.

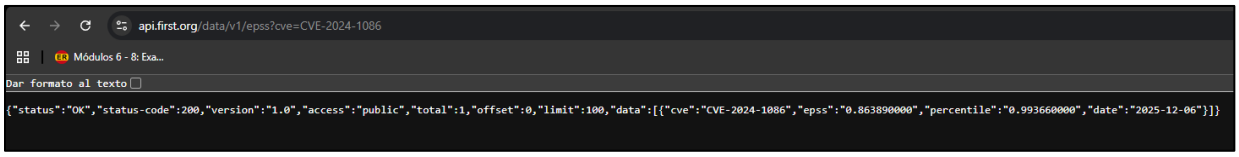
Vulnerabilidad CVE-2024-1086 (Linux). La PoC comparte un exploit local que aprovecha un fallo use-after-free en el subsistema netfilter del kernel Linux. Funciona en la mayoría de kernels entre la v5.14 y la v6.6 (con exclusiones y condiciones según configuración del kernel). El exploit corrompe estructuras en memoria del kernel para ejecutar código en modo kernel, lo que permite escalar privilegios a root. El repositorio incluye el código fuente, un binario compilado y notas sobre requisitos (user namespaces habilitados, nf_tables, arquitectura x86_64) y limitaciones (inestabilidad en entornos con mucha actividad de red, kernel panic intencionado como efecto secundario). También soporta ejecución “fileless” mediante memfd para cargar el binario en memoria. En resumen: PoC de escalamiento local de privilegios, alta tasa de éxito en entornos de laboratorio requiere condiciones específicas del kernel y deja señales (p. ej. crashes/kernel panic) que pueden ayudar en su detección.

En la figura 53 se puede observar la consulta realizada a la API oficial de FIRST para verificar el puntaje EPSS asociado a la vulnerabilidad CVE-2024-1086. La respuesta del servicio indica un valor de 0.86 (86%), lo que implica que, según el modelo de predicción de FIRST, esta

vulnerabilidad tiene una alta probabilidad de ser explotada activamente en el corto plazo. Este resultado refuerza la necesidad de priorizar su tratamiento, ya que EPSS se basa en datos empíricos de actividad maliciosa y no únicamente en la severidad teórica del CVSS.

Figura 53

API EPSS FIRST



Nota. Consulta de puntaje EPSS mediante la API de FIRST. Elaboración propia a partir de datos obtenidos de Exploit Prediction Scoring System (EPSS), FIRST. (s. f.) https://api.first.org/data/v1/epss/

***Tácticas, Técnicas y Procedimientos*.** Se generó una tabla con las TTPs del marco MITRE ATT&CK, considerando los vectores de ataque observados en la prueba de concepto asociada a la vulnerabilidad CVE-2024-1086. Como se muestra en la tabla 12, esta clasificación permite relacionar las acciones descritas en el exploit con las fases del ciclo de ataque, facilitando la identificación de comportamientos que podrían ser detectados por los equipos de defensa y análisis de inteligencia de amenazas.

Tabla 12

Tácticas, Técnicas y Procedimientos (TTPs)

ID	Técnica	Táctica	Explicación en relación con la PoC
T1068	Exploitation for Privilege Escalation	Privilege Escalation	Exploit local *use-after-free* en netfilter para ejecutar código en kernel y obtener privilegios root.
T1059	Command and Scripting Interpreter	Execution	La PoC ejecuta comandos y binarios (./exploit) para lograr la escalada y las acciones posteriores en el sistema.
T1105	Ingress Tool Transfer	Command and control	La PoC demuestra transferencia de binarios (compilado o descargado) que luego se ejecutan en el host; también documenta descarga vía curl.
T1055	Process Injection	Defense Evasion / Persistence	Soporta ejecución fileless (memfd) y técnicas para cargar y ejecutar el payload directamente en memoria, evitando dejar un binario claro en disco.
T1543	Create or Modify System Process / Service	Persistence	Tras escalar privilegios, el actor puede crear servicios o procesos persistentes (systemd, servicios Windows no aplica aquí) para mantener acceso.
T1547	Boot or Logon Autostart Execution	Persistence	La PoC facilita la ruta para instalar mecanismos de arranque (systemd/rc scripts/cron) que permitan la persistencia tras reinicios.
T1021	Remote Services	Lateral Movement	Con privilegios root, el atacante puede habilitar o usar servicios (ssh, rpc) para moverse lateralmente dentro de la red.
T1005	Data from Local System	Collection	El exploit permite leer ficheros locales sensibles (logs, configuraciones, credenciales) usando los privilegios obtenidos.
T1070	Indicator Removal on Host	Defense Evasion	La capacidad de ejecutar en kernel y en memoria facilita la eliminación u ocultación de rastros (limpieza de logs, supresión de evidencias).

Nota. La tabla presenta la relación de tácticas y técnicas del marco MITRE ATT&CK asociadas al escenario analizado, con el fin de identificar los comportamientos del ataque y su correspondencia con las fases del ciclo de intrusión.

Vulnerabilidad CVE-2025-59287 (Windows). La PoC demuestra una ejecución remota de código sin autenticación en WSUS) provocada por una deserialización insegura. En concreto, WSUS descifra y deserializa objetos (AuthorizationCookie) usando BinaryFormatter/SoapFormatter sin validar tipos, lo que permite al atacante enviar una carga XML especialmente construida que, al deserializarse, ejecuta código en el servidor con privilegios SYSTEM. El vector se aprovecha del endpoint de reporting (/ReportingWebService/ReportingWebService.asmx / GetCookie()), donde datos almacenados en la columna MiscData se convierten en objetos; si el contenido incluye un gadget de deserialización válido, la cadena de deserialización dispara ejecución remota. La PoC incluye ejemplos de payload XML y muestra cómo el exploit puede forzar la creación de objetos y ejecución en el servidor, así como la posibilidad de entregar binarios o establecer persistencia tras obtener control.

Mediante la consulta a la API oficial de FIRST se obtuvo el puntaje EPSS correspondiente a la vulnerabilidad CVE-2025-59287. El servicio reportó un valor de 0.64 (64 %), lo que indica una probabilidad moderadamente alta de explotación en escenarios reales. Este resultado permite priorizar su tratamiento dentro del plan de mitigación, dado que EPSS se fundamenta en datos observables de actividad maliciosa y no únicamente en la severidad asignada mediante CVSS.

***Tácticas, Técnicas y Procedimientos*.** Como se muestra en la tabla 13, se presentan las tácticas, técnicas y procedimientos (TTPs) asociados a la vulnerabilidad CVE-2025-59287 en entornos Windows.

Tabla 13

Tácticas, Técnicas y Procedimientos (TTPs)

ID TTP	Técnica	Táctica	Breve explicación en relación con la PoC
T1190	Exploit Public-Facing Application	Initial Access	El ataque explota un endpoint público de WSUS (ReportingWebService) para enviar datos maliciosos que desencadenan la deserialización insegura.
T1203	Exploitation for Client Execution	Execution	La deserialización insegura provoca ejecución de código en el servidor remoto (RCE), ejecutando instrucciones contenidas en el gadget entregado.
T1059	Command and Scripting Interpreter	Execution	Tras la RCE es habitual ejecutar comandos o scripts (por ejemplo, para desplegar payloads, ejecutar cmd/PowerShell) como parte del compromiso.
T1105	Ingress Tool Transfer	Command and Control	La PoC y los write-ups muestran posibilidades de transferencia de binarios/objetos (descarga o creación de ejecutables) para materializar el control del host.
T1543	Create or Modify System Process	Persistence	Con privilegios SYSTEM, el actor puede crear servicios o procesos que garanticen la persistencia del código malicioso en el servidor WSUS.
T1547	Boot or Logon Autostart Execution	Persistence	La deserialización y posterior control permiten instalar mecanismos de arranque automático (tareas programadas, servicios) para mantener acceso tras reinicios.
T1071	Application Layer Protocol	Command and Control	El atacante puede usar HTTP(S) u otros protocolos de aplicación para comunicarse con C2 o para exfiltrar datos desde el servidor comprometido.
T1005	Data from Local System	Collection	La PoC permite, una vez ejecutado código, leer ficheros sensibles del sistema (logs, configuración, credenciales) presentes en el servidor WSUS.
T1552	Unsecured Credentials	Credential Access	La explotación puede exponer credenciales o permitir su recolección desde archivos o memoria, facilitando movimientos posteriores.

ID TTP	Técnica	Táctica	Breve explicación en relación con la PoC
T1486	Data Encrypted for Impact	Impact	El control de SYSTEM puede emplearse como paso previo a despliegues de ransomware o cifrado masivo de datos en el servidor y en la red asociada.

Nota. La tabla presenta la identificación de TTPs asociados a la explotación de una vulnerabilidad en el servicio WSUS.

CVE-2025-10713 (Aplicación web). Tras revisar las fuentes públicas y los avisos oficiales, no se ha encontrado una prueba de concepto pública ni código exploit disponible para la CVE-2025-10713. Los documentos oficiales (advisory de WSO2, NVD y resúmenes en repositorios de seguridad) describen la vulnerabilidad, versiones afectadas y medidas recomendadas, pero no publican payloads explotables ni pasos públicos reproducibles para activarla en entornos reales.

Eso implica que, aunque la vulnerabilidad es real y su impacto técnico (lectura de ficheros, DoS) puede ser grave si se explota, la probabilidad de explotación inmediata es baja en comparación con fallos que ya disponen de PoC/exploits accesibles públicamente.

Difusión

En esta etapa, la información recopilada y analizada en las fases anteriores se comunica a los equipos encargados de la priorización de activos y vulnerabilidades dentro del programa CTEM (Objetivo 3). Esta difusión puede realizarse mediante boletines de seguridad o informes de inteligencia de amenazas personalizados, los cuales permiten enfocar los esfuerzos en los sistemas con mayor riesgo o exposición.

Estos informes pueden incluir elementos como:

Título del evento o hallazgo.

Resumen ejecutivo.

Detalle técnico de la vulnerabilidad (versión afectada, severidad, referencias CVE).

Evaluación del riesgo y probabilidad de explotación.

Recomendaciones de mitigación o parches.

De forma complementaria, los IOC y TTPs pueden incluirse cuando sea necesario apoyar la fase de validación, donde el equipo defensivo verifica posibles intentos de explotación o actividad maliciosa.

Toda esta información debe clasificarse y compartirse bajo un esquema de TLP, garantizando su difusión controlada y adecuada según la sensibilidad del contenido.

El TLP es una forma sencilla de marcar cómo debe compartirse la información de seguridad. La persona que genera el contenido indica el nivel con colores para dejar claro hasta dónde puede llegar su difusión. Si un receptor necesita compartir más allá de lo permitido, debe pedir permiso al autor original.

TLP:RED (Rojo): Información muy sensible, limitada a individuos concretos. No debe compartirse fuera del grupo reducido al que se entrega originalmente, porque su difusión podría afectar la privacidad, la reputación o las operaciones.

TLP:AMBER (Ámbar): Información que puede distribuirse dentro de la organización, pero cuyo uso fuera de ella implica riesgos. Puede compartirse con colegas que necesiten saberlo para protegerse y con clientes que deban tomar medidas. Las fuentes pueden añadir restricciones adicionales (por ejemplo, *AMBER+STRICT* que limita el intercambio solo a la propia organización).

TLP:GREEN (Verde): Información que es útil para otras organizaciones del mismo sector o comunidad. Puede circular entre entidades afines, pero no publicarse en canales públicos. Ideal para alertas sectoriales o recomendaciones de protección conjunta.

TLP:CLEAR (Blanco): Información que no presenta riesgo de uso indebido y puede difundirse libremente. Se puede publicar públicamente, respetando derechos de autor y condiciones de uso.

Retroalimentación

Esta fase se centra en recopilar y analizar la retroalimentación de las partes interesadas respecto a la inteligencia de amenazas que ha sido entregada. Su propósito es determinar si la información proporcionada resultó útil, oportuna, precisa y accionable dentro del contexto operativo de la organización. A partir de estos comentarios, el equipo responsable puede identificar oportunidades de mejora, ajustar los requerimientos de inteligencia, optimizar los métodos de recolección y análisis, y refinar los formatos de presentación. En consecuencia, esta etapa cierra el ciclo y asegura que la producción futura de inteligencia se alinee mejor con las necesidades estratégicas, tácticas y operacionales de la organización.

En línea con esta estructura tradicional, Arikan, Koçak y Alkan (2024) proponen un "ciclo de vida atómico" que introduce mayor granularidad en las fases de análisis y producción, diferenciando explícitamente entre inteligencia estática e inteligencia compartible. Esta distinción resulta relevante cuando se requiere estandarizar los productos en formatos como STIX u OVAL, facilitando su interoperabilidad y distribución controlada.

Conclusión objetivo 2: A partir del desarrollo del estudio y la ejecución práctica sobre las vulnerabilidades, amenazas e indicadores recopilados, se logró cumplir de manera íntegra cada una de las seis fases del ciclo de inteligencia de amenazas, garantizando un proceso completo, estructurado y alineado con los objetivos del plan de inteligencia de amenazas.

Planificación y dirección: Se definió el alcance, los activos críticos, el objetivo de la inteligencia, las fuentes primarias (AlienVault OTX, IBM X-Force Exchange, GitHub,

Darktrace) y las amenazas que se priorizarían.

También se estableció el contexto del sector financiero y la orientación hacia servidores Linux, Windows y aplicaciones web, junto con las amenazas asociadas (DDoS, ransomware, explotación activa de CVEs).

Recopilación: Se recolectó información real y actualizada sobre:

Vulnerabilidades activamente explotadas (CVE-2024-1086, CVE-2025-59287).

Vulnerabilidades medianamente críticas sin PoC pública (CVE-2025-10713).

Resultados sobre el sector financiero.

IOC provenientes de Darktrace, AlienVault OTX e IBM X-Force.

Pruebas de concepto (PoC) en repositorios públicos.

La recolección se realizó conforme al objetivo y a los activos críticos definidos.

Procesamiento y explotación

Toda la información recopilada se depuró, normalizó y clasificó según:

Sistema afectado (Linux, Windows, Web Application).

Tipo de amenaza (RCE, LPE, XXE, DDoS).

Severidad y probabilidad.

Evidencia de explotación.

IOC y TTPs relevantes.

Esta fase permitió transformar datos crudos en información estructurada lista para el análisis.

Análisis: Se evaluó la relevancia de cada amenaza respecto al entorno del caso (sector financiero), identificando:

La explotación activa y alta prioridad de CVE-2024-1086 y CVE-2025-59287.

La baja probabilidad actual de explotación para CVE-2025-10713.

Correlaciones entre PoC, IOC, TTPs y vectores de ataque reales.

Riesgos potenciales en los activos identificados (servidores web, servidores de aplicaciones y WSUS).

Asimismo, se mapearon las amenazas con el marco MITRE ATT&CK usando los TTPs correspondientes.

Difusión: Se elaboró inteligencia procesable para las partes interesadas (incluyendo equipo CTEM), incluyendo:

Descripciones técnicas, impacto y probabilidad.

Evidencia de explotación y PoC.

TTPs y IOC.

Recomendaciones de mitigación.

La difusión se clasificó conforme al esquema TLP (RED, AMBER, GREEN, CLEAR) garantizando un intercambio seguro según la sensibilidad de la información.

Retroalimentación: Finalmente, se estableció el mecanismo de retroalimentación para validar:

La utilidad de los reportes entregados.

La pertinencia de los hallazgos para los equipos operativos.

La mejora del proceso para futuras iteraciones.

Síntesis del diseño del plan de inteligencia

Adicionalmente, el plan de inteligencia desarrollado incorpora elementos operativos que permiten su aplicación dentro del ciclo de vida de la inteligencia de amenazas. En la fase de planificación se definieron las fuentes externas de inteligencia que alimentan el proceso, entre

ellas AlienVault OTX, IBM X-Force Exchange, el modelo EPSS y el catálogo CISA KEV, las cuales permiten contextualizar las vulnerabilidades detectadas en el entorno analizado.

Asimismo, se estableció una periodicidad diferenciada para la recolección de información: la consulta de inteligencia de amenazas se plantea de forma diaria con el fin de identificar cambios en la actividad de explotación o nuevas campañas de ataque, mientras que los escaneos de vulnerabilidades en la infraestructura se realizan semanalmente para mantener actualizada la visibilidad sobre la superficie de exposición.

Con el fin de garantizar interoperabilidad, los indicadores de compromiso y de ataque se normalizan utilizando el estándar STIX 2.1, generando objetos estructurados en formato JSON mediante la librería *stix2*. Este enfoque permite que los indicadores puedan integrarse posteriormente con plataformas de monitoreo o análisis de eventos de seguridad como Splunk o Elastic Stack, donde podrían ser utilizados para procesos de correlación y detección.

Finalmente, la gestión temporal de los indicadores se mantiene dentro de los objetos STIX mediante atributos como *first_seen*, *last_seen*, *valid_from* y *valid_until*, lo que permite registrar su periodo de observación y vigencia dentro del repositorio de inteligencia. Esto facilita mantener actualizados los indicadores utilizados en los procesos de análisis y evita el uso de información obsoleta dentro del ciclo de inteligencia.

Objetivo específico 3

Como resultado del análisis previo de plataformas de inteligencia de amenazas y de la definición de un plan integral de recolección de inteligencia, se cuenta ahora con un conjunto de herramientas y procesos capaces de suministrar información continua, estructurada y alineada con las necesidades de seguridad de las organizaciones. Sobre esta base, el siguiente paso consiste en evaluar el ciclo de gestión continua de la exposición a amenazas, con el fin de determinar cómo la información recopilada puede ser clasificada, priorizada y contextualizada de manera estratégica. Esta evaluación permite comprender el nivel real de exposición, mejorar la toma de decisiones y optimizar la gestión de riesgos mediante un enfoque dinámico y adaptativo frente a amenazas emergentes.

Alcance

La primera fase consiste en establecer el alcance del análisis, lo cual implica definir con precisión la superficie de ataque tanto interna como externa de la organización. La superficie interna abarca los servidores, estaciones de trabajo, dispositivos de usuario final y cualquier otro activo conectado a la red corporativa, considerando sus direcciones IP privadas y servicios asociados. Por su parte, la superficie externa comprende los dominios, URL, direcciones IP públicas, servicios publicados en Internet y cualquier recurso expuesto que pueda ser identificado por un actor malicioso. Determinar este alcance permite orientar adecuadamente las actividades de evaluación, priorizar activos críticos y facilitar una gestión más efectiva de la exposición a amenazas.

Todo el alcance definido puede documentarse y gestionarse dentro de una Configuration Management Database (CMDB), lo que permite mantener un inventario centralizado y actualizado de los activos involucrados. Esto facilita la relación entre los elementos de la

superficie de ataque y los procesos de negocio que soportan. Además, la incorporación de las etapas de clasificación e identificación de activos propuestas por Magerit, ya abordadas en el objetivo 2, fortalece la calidad del inventario, al establecer niveles de criticidad y valorar el impacto asociado a cada activo.

De esta manera, el alcance se integra de forma natural en la fase de planificación y dirección del ciclo de vida de la inteligencia de amenazas, garantizando que las actividades posteriores. como la recolección, análisis y priorización se orienten hacia los activos más relevantes y con mayor exposición. Esto proporciona una base sólida para una gestión de amenazas más efectiva y alineada con la realidad operativa de la organización.

Ejemplo CMBD. Para efectos del ejercicio, se construyó una CMDB que permite centralizar la información esencial de los activos tecnológicos, su clasificación, las relaciones con los responsables, y la valoración de riesgos según Magerit. Esta CMDB sirve como insumo para la fase de definición del alcance, ya que consolida tanto la superficie de ataque interna como externa y facilita la priorización de activos críticos.

***Activos Internos*.** El modelo elaborado incluye diferentes tipos de activos distribuidos en varios segmentos de red, con el fin de simular una infraestructura empresarial ordenada y alineada con buenas prácticas de segmentación. Cada tipo de activo se ubicó en un segmento específico:

Servidores web en la red 10.1.1.0/24,

Servidores internos (bases de datos, aplicaciones) en 10.1.2.0/24,

Controladores de dominio y servicios corporativos en 10.1.3.0/24,

Estaciones de trabajo distribuidas entre 10.1.10.0/24 y 10.1.20.0/24 según el área,

Equipos macOS asignados a redes de dispositivos especializados.

Cada activo cuenta con los campos habituales de una CMDB:

Hostname

Rol

Cantidad

Tipo de activo

Sistema operativo

Dirección IP asignada y segmento

Ubicación física o lógica

Propietario, responsable y custodio,

Dueño del dato cuando aplica

Tipo de información gestionada

Obligatoriedad de registro RNBD en caso de manejar datos personales

Amenazas identificadas

Valoración de probabilidad e impacto según Magerit

Riesgo resultante y criticidad: La valoración de riesgos se realizó aplicando los niveles de probabilidad e impacto establecidos por Magerit, permitiendo caracterizar activos como críticos, altos, medios o bajos según la combinación de sus amenazas, exposición y contexto. Esto permite priorizar acciones de seguridad, definir controles y orientar la planificación dentro del ciclo de vida de la inteligencia de amenazas.

De esta forma, la CMDB presentada funciona como un ejemplo operativo y estructurado, alineado con la práctica profesional en gestión de activos, análisis de riesgos y definición del alcance en procesos de seguridad.

En la figura 54 se presenta la CMDB correspondiente a los activos internos, donde se puede observar la clasificación y organización de los recursos dentro del entorno analizado.

Figura 54

CMDB Activos Internos

Hostname	Rol	Dirección IP	Descripción	Cantidad	Tipo de Activo	SO	Ubicación	Propietario	Responsable	Custodio	Dueño del Dato	Tipo de Información	RNBD	Amenazas Identificadas	Probabilidad (Magerit)	Impacto (Magerit)	Riesgo Resultante	Criticidad
SERPAGOS01	Pasarela de Pagos	10.1.1.10	Servidor web encargado de procesar las transacciones de pago.	2	Servidor Web	Ubuntu Server 22.04 LTS	Oficina – On Premise	Finanzas	Andrea Méndez	Infraestructura	Clientes	Datos personales	Si	Falta de CDN; DDoS; vulnerabilidades sin parche; fuga de datos	B	A	M	Crítico (MA)
WEBAPP02	Portal Institucional	10.1.1.11	Sitio web corporativo e informativo.	1	Servidor Web	Ubuntu 20.04	DMZ	Comunicaciones	Juan Salgado	Infraestructura	Público	Información pública	No	Defacement; CMS vulnerable; fuerza bruta	M	B	M	Medio (M)
WEBAPI03	API de Servicios	10.1.1.12	API que expone servicios internos con tokens.	1	Servidor Web/API	Rocky Linux 9	Data Center	Tecnología	Jorge Ruiz	Infraestructura	Interno	Información interna	No	MITM; tokens comprometidos; vulnerabilidades de librerías	A	M	A	Alto (A)
DBSERV01	Base de Datos Financiera	10.1.2.10	Movimientos contables y reportes financieros.	1	Base de Datos	Windows Server 2019 / SQL Server	Oficina – On Premise	Finanzas	Laura Bernal	Infraestructura	Finanzas	Datos financieros	Si	Inyección SQL; ransomware; fuga de información	M	MA	A	Crítico (MA)
DBSERV02	Base de Datos RRHH	10.1.2.11	Nómina, contratos y expedientes laborales.	1	Base de Datos	Ubuntu / PostgreSQL 14	Oficina – On Premise	Talento Humano	Julián Rivera	Infraestructura	Empleados	Datos personales	Si	Exfiltración; permisos excesivos; falta de cifrado	B	MA	A	Alto (A)
APPSRV01	Servidor de Aplicaciones	10.1.2.12	Facturación y módulo de inventarios.	1	Servidor de Aplicaciones	Windows Server 2022	Oficina – On Premise	Operaciones	Sandra Castillo	Infraestructura	Interno	Información interna	No	Falta de parches; explotación RDP	M	M	M	Medio (M)
FILES01	Servidor de Archivos	10.1.2.13	Documentos y carpetas compartidas.	1	Servidor de Archivos	TrueNAS	Oficina – On Premise	Tecnología	Daniel Moreno	Infraestructura	Interno	Información interna	Si	Ransomware; permisos incorrectos; shares abiertos	A	M	A	Alto (A)
WS-WIN01	Estación Contable	10.1.3.10	Equipo de analista contable.	1	Estación de Trabajo	Windows 10 Pro	Oficina – On Premise	Finanzas	Usuario Final	Soporte TI	Finanzas	Datos financieros	No	Phishing; malware; ransomware	A	A	MA	Crítico (MA)
WS-WIN02	Estación Talento Humano	10.1.3.11	Equipo auxiliar de RRHH.	1	Estación de Trabajo	Windows 11 Pro	Oficina – On Premise	Talento Humano	Usuario Final	Soporte TI	Empleados	Datos personales	Si	Ingeniería social; fuga accidental de datos	M	MA	A	Alto (A)
WS-MAC01	Estación de Diseño	10.1.3.12	Equipo de diseñador gráfico.	1	Estación de Trabajo	macOS Ventura	Oficina – On Premise	Comunicaciones	Usuario Final	Soporte TI	Interno	Información pública	No	Malware por software pirata; vulnerabilidad de Adobe	B	B	B	Bajo (B)
WS-WIN03	Estación de Desarrollo	10.1.3.13	Equipo del desarrollador backend.	1	Estación de Trabajo	Windows 11 Pro	Oficina – On Premise	Tecnología	Usuario Final	Soporte TI	Interno	Código fuente	No	Robo de tokens; dependencias maliciosas	A	M	A	Alto (A)
WS-MAC02	Estación Gerencial	10.1.3.14	Equipo del gerente general.	1	Estación de Trabajo	macOS Sonoma	Oficina – On Premise	Dirección	Usuario Final	Soporte TI	Dirección	Información estratégica	No	Spear-phishing dirigido; robo de credenciales	M	MA	A	Crítico (MA)

Nota. Activos internos consolidados en la CMDB con variables de seguridad para la gestión y priorización de riesgos. Elaboración propia.

Activos Externos. La CMDB de activos públicos se construyó con el propósito de documentar y caracterizar todos aquellos componentes expuestos a Internet que forman parte de la superficie externa de la organización. A diferencia de los activos internos, estos elementos poseen una visibilidad directa hacia el entorno público, lo que incrementa la probabilidad de ataques y requiere una gestión diferenciada en términos de monitoreo, endurecimiento y control continuo.

En esta CMDB se incluyeron activos tales como dominios, subdominios, endpoints de API, servicios de correo público y plataformas de distribución de contenido (CDN). Cada

elemento fue descrito en términos de su función, su relación con los servicios ofrecidos a usuarios externos y su papel dentro de la cadena de prestación de servicios críticos, como la disponibilidad de la pasarela de pagos o la entrega de contenido web.

Dado que estos activos dependen de infraestructura en la nube o de proveedores externos, también se registró información relativa a proveedores, registros DNS, IP públicas asociadas y mecanismos de autenticación o protección, incluyendo tipos de registros como A, AAAA, MX y Text (TXT). Esta información resulta fundamental para realizar evaluaciones de exposición, validar configuraciones de seguridad y facilitar procesos de análisis en plataformas de inteligencia de amenazas o scanners de superficie de ataque.

La valoración de amenazas en estos activos se centró en riesgos específicos para entornos públicos, tales como la suplantación de dominios, el secuestro de DNS, la explotación de APIs de uso público, el abuso del correo en campañas de phishing o la interrupción de servicios mediante ataques de denegación distribuida (DDoS). Asimismo, debido a su exposición directa, la probabilidad asignada suele ser mayor que la de los activos internos, aun cuando su impacto pueda variar según la criticidad del servicio asociado.

La columna de riesgo resultante se calculó aplicando estrictamente la matriz de riesgo utilizada previamente, considerando la probabilidad y el impacto asignados a cada activo. Este análisis permite clasificar la importancia relativa de cada elemento dentro de la superficie pública y priorizar acciones de protección, endurecimiento o monitorización dentro del ciclo CTEM.

En la figura 55 se presenta la CMDB correspondiente a los activos externos, donde se documentan y caracterizan los componentes expuestos a Internet que forman parte de la superficie pública de la organización. Estos activos incluyen dominios, subdominios, endpoints

de API, servicios de correo público y plataformas de distribución de contenido (CDN), todos ellos con visibilidad directa hacia el entorno externo, lo que incrementa su nivel de exposición y riesgo.

Figura 55

CMDB Activos Externos

ID Activo	Nombre del Activo	Descripción	Tipo de Activo	IP Pública	Dominio/Subdominio	Registros DNS Asociados	Ubicación	Propietario	Responsable	Custodio	Dueño del Dato	Tipo de Información	RNBD	Amenazas Identificadas	Probabilidad (Magerit)	Impacto (Magerit)	Riesgo Resultante	Criticidad
PUBWEB01	Dominio Corporativo Principal	Dominio oficial de la organización para servicios web y correo corporativo	Dominio Público	181.50.23.10	**empresa.com**	A, AAAA, MX, TXT (SPF), DKIM, DMARC, CAA	Internet	Área de TI	Infraestructura	ISP / Proveedor DNS	Empresa	Pública / Información institucional	No	Secuestro de dominio, ataques DNS spoofing, phishing aprovechando MX, modificación de registros	M	A	A	Alto (A)
PUBWEB02	Subdominio Pasarela de Pagos	Subdominio expuesto para procesar pagos de clientes	Subdominio Web Público	181.50.23.22	**pay.empresa.com**	A, AAAA, TXT, CAA	Internet	Área de Finanzas	Andrea Méndez	Infraestructura	Clientes	Datos personales y financieros	Si	DDoS por falta de mitigación CDN, explotación de vulnerabilidades web, fuga de datos, manipulación de tráfico	A	A	MA	Crítico (MA)
PUBWEB03	API Pública de Integración	Endpoint API utilizado por aplicaciones externas para integración con servicios de la empresa	API Pública	181.50.23.30	**api.empresa.com**	A, TXT (validación), CAA	Internet	Área de Desarrollo	Juan Castillo	Infraestructura	Empresa	Información técnica expuesta	No	Ataques de fuerza bruta, abuso de API, enumeración, explotación de endpoints no autenticados	M	M	M	Medio (M)
PUBWEB04	Subdominio de Correos	Subdominio dedicado a servicios de correo saliente y entrante	Correo Público	181.50.23.12	**mail.empresa.com**	MX, TXT (SPF), DKIM, DMARC, A, AAAA	Internet	Área de TI	Helpdesk	Proveedor de correo	Empleados / Clientes	Datos personales	Si	Spoofing, phishing, abuso de relay, manipulación de registros TXT	M	A	A	Alto (A)
PUBWEB05	Subdominio CDN Estático	Distribución de contenido estático para mejorar disponibilidad	CDN Público	*IP dinámica según proveedor*	**cdn.empresa.com**	CNAME hacia proveedor CDN	Internet / Proveedor CDN	Área de TI	Infraestructura	Proveedor CDN	Empresa	Contenido público	No	Envenenamiento de caché, explotación de configuraciones CNAME, interrupción de disponibilidad	B	M	M	Bajo (B)

Nota. Activos externos registrados en la CMDB con variables de seguridad para evaluar la exposición y priorización de riesgos. Elaboración propia.

Descubrimiento

Activos Internos. La segunda etapa corresponde al descubrimiento de la superficie de ataque, especialmente de aquellos activos que no se encuentran inventariados o que, por distintas razones, no están bajo la visibilidad directa de la organización. En el caso de los activos internos, es necesario definir previamente las reglas perimetrales que permitan ejecutar escaneos controlados sobre los segmentos autorizados, evitando interferencias con otros servicios o equipos sensibles.

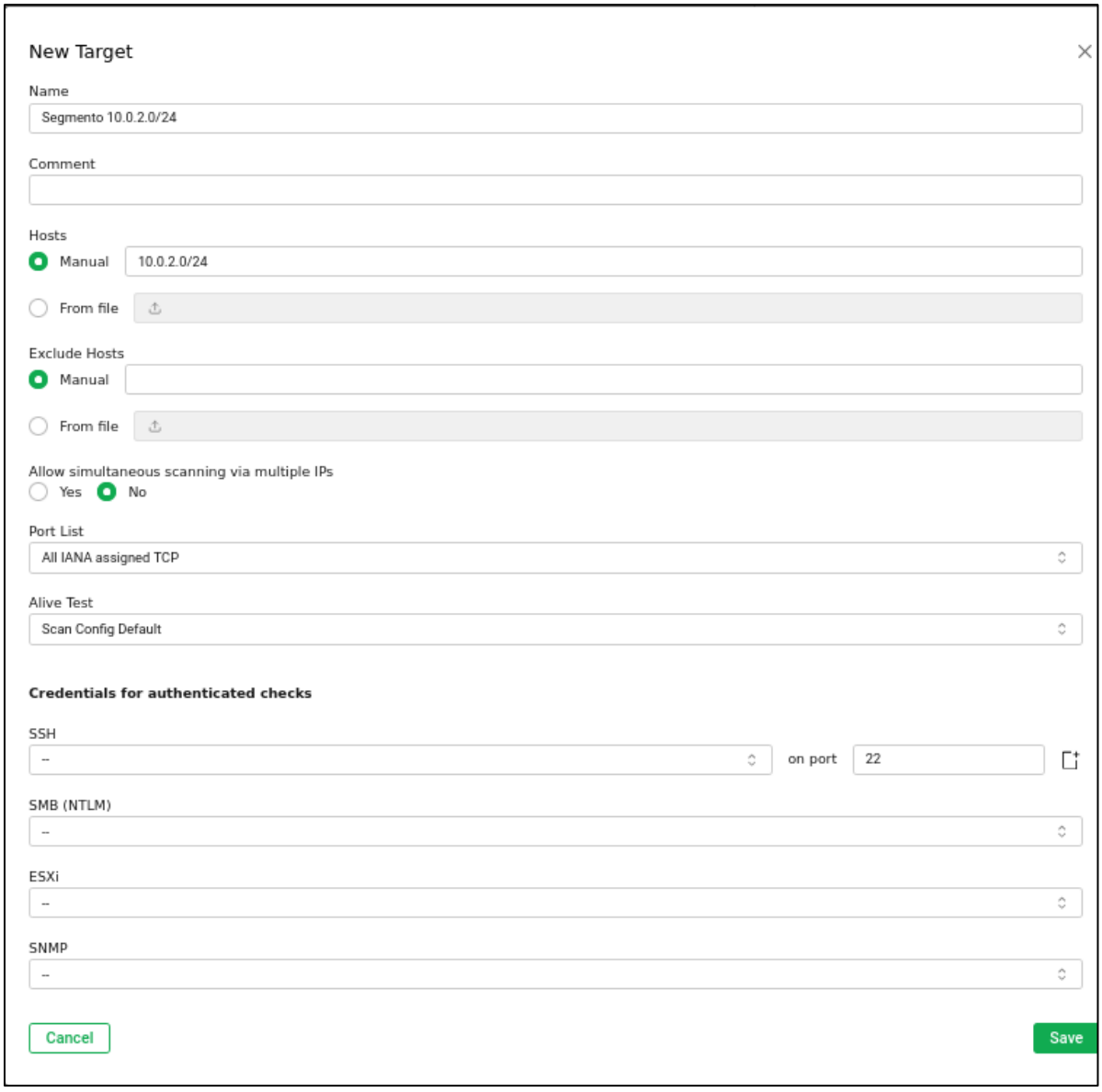
Para esta fase, se emplea OpenVAS como herramienta de apoyo en las tareas de reconocimiento. Con ella es posible realizar escaneos de descubrimiento sobre las redes autorizadas y validar qué activos se encuentran operativos. Como parte de la prueba, se ejecutó un escaneo sobre el segmento 10.0.2.0/24, donde se alojan varias máquinas virtuales de laboratorio, con el objetivo de identificar cuántas de ellas están activas y confirmar su presencia en la red.

Además de esta actividad de enumeración inicial, en esta fase también se realizan escaneos de vulnerabilidades, aplicados tanto a los activos previamente identificados durante la delimitación del alcance como a aquellos nuevos activos detectados durante los escaneos de descubrimiento. De esta manera, cualquier sistema, servicio o dispositivo que emerja del análisis de superficie de ataque es incorporado inmediatamente al inventario provisional y evaluado bajo los mismos criterios de exposición y riesgo, garantizando una revisión completa y coherente con las prácticas de gestión de vulnerabilidades.

En la figura 56 se puede observar la configuración del objetivo para el escaneo de descubrimiento de activos internos.

Figura 56

Configuración Objetivo Escaneo de Descubrimiento

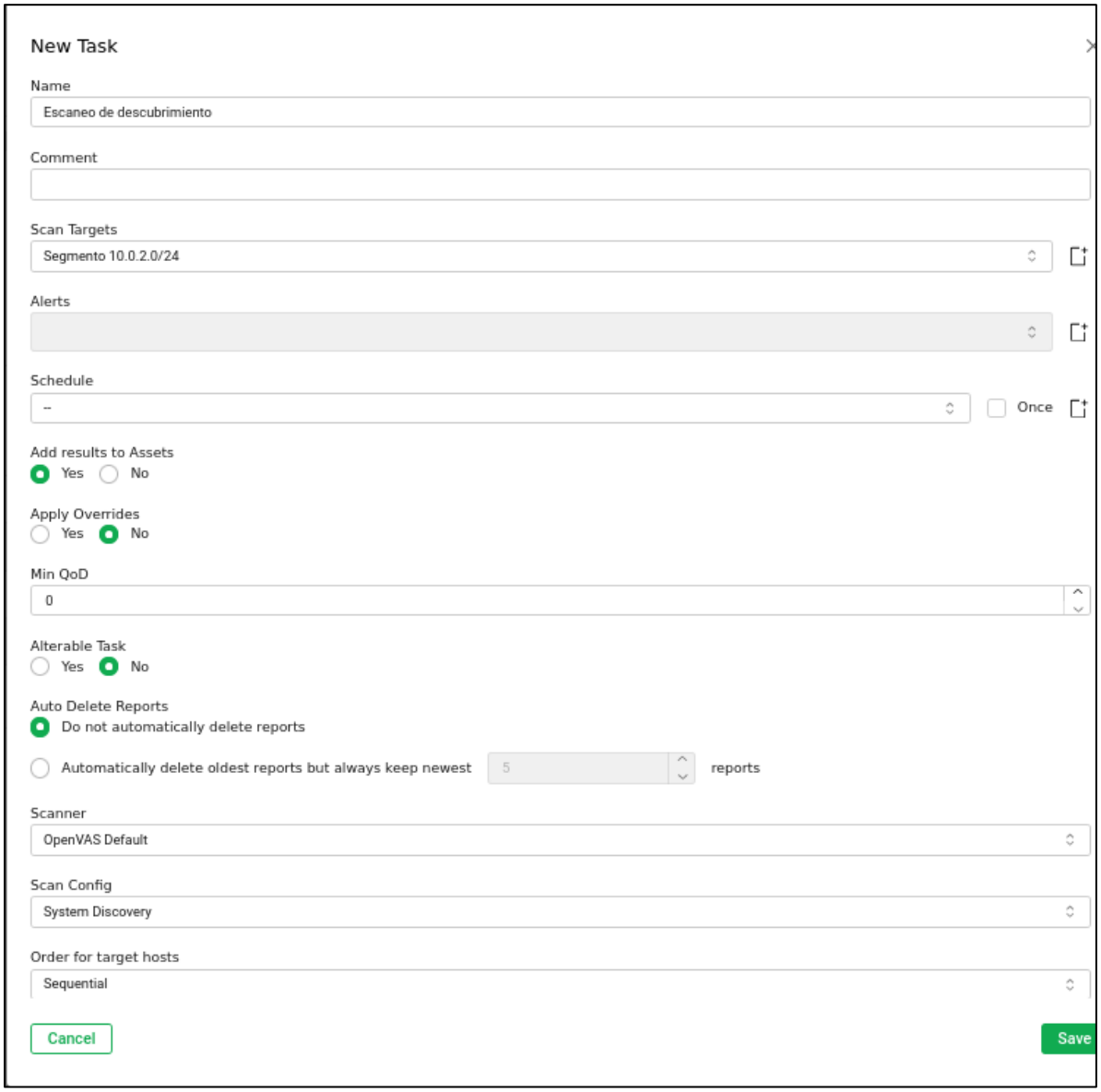


Nota. Configuración del objetivo para escaneo de descubrimiento en OpenVAS. Elaboración propia mediante el uso de OpenVAS.

En la figura 57 se puede observar la configuración de la tarea para el escaneo de descubrimiento de activos internos.

Figura 57

Configuración Task Escaneo de Descubrimiento



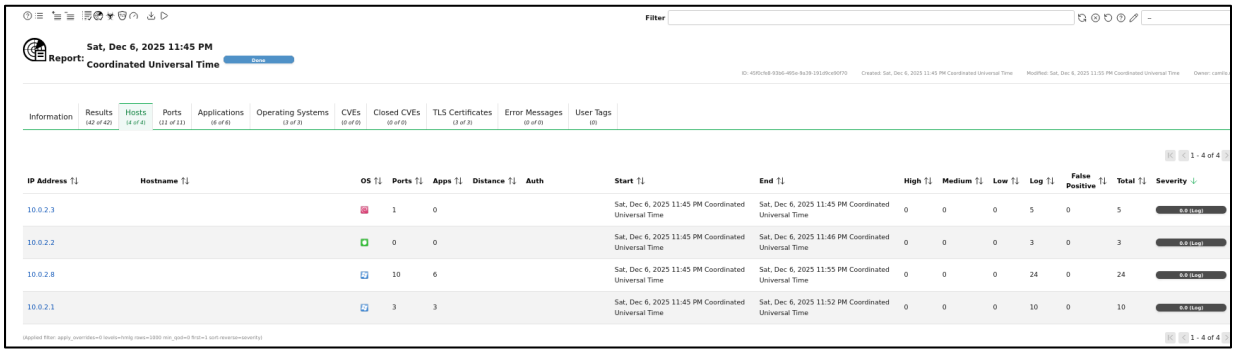
Nota. Configuración de la tarea para escaneo de descubrimiento en OpenVAS. Elaboración propia mediante el uso de OpenVAS.

En la figura 58 se pueden observar los resultados del escaneo de descubrimiento de activos, donde se identificaron cuatro hosts activos correspondientes a las direcciones IP

10.0.2.1, 10.0.2.2, 10.0.2.3 y 10.0.2.8. Dos de ellos fueron clasificados preliminarmente como equipos con sistema operativo Windows, uno como Linux y otro como BSD. No fue posible determinar con precisión las versiones de cada sistema operativo, ya que este nivel de detalle requiere un escaneo autenticado. En este ejercicio se adopta un enfoque de caja negra, por lo que el análisis se limita a la identificación de hosts y características generales sin credenciales de acceso.

Figura 58

Resultados Escaneo de Descubrimiento



Nota. Resultados del escaneo de descubrimiento en OpenVAS. Elaboración propia mediante el uso de OpenVAS.

Para complementar la validación realizada con OpenVAS, se ejecutó un escaneo puntual con Nmap usando el comando nmap 10.0.2.8 -sV, con el propósito de confirmar si el host correspondía a un sistema Windows. Los resultados permitieron corroborarlo, ya que se identificaron puertos y servicios característicos de este sistema operativo. Entre ellos destacan File Transfer Protocol (FTP), SMB, Remote Procedure Call (RPC), Remote Desktop Protocol (RDP), MySQL (MySQL), Windows Remote Management (WinRM) y HTTPS, lo que

evidencia una superficie de exposición amplia si el servidor no cuenta con medidas de endurecimiento adecuadas.

El puerto 21/tcp respondió con un servicio Microsoft ftpd, lo que refleja la presencia de un servicio FTP operativo. Asimismo, los puertos 135, 139 y 445 confirmaron la disponibilidad de servicios propios de entornos Windows, asociados a RPC, Network Basic Input/Output System (NetBIOS) y SMB, respectivamente. Estos hallazgos permiten consolidar la identificación del sistema operativo y aportan una primera visión sobre posibles vectores de riesgo en el servidor.

En la figura 59 se puede observar el resultado del escaneo de puertos realizado con Nmap sobre el host analizado.

Figura 59

Escaneo de Puertos con Nmap

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.8 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 22:25 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.30% done; ETC: 22:25 (0:00:01 remaining)
Nmap scan report for 10.0.2.8
Host is up (0.0011s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Microsoft IIS httpd 10.0
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp open  mysql         MySQL (unauthorized)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:18:88:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.51 seconds
```

Nota. Escaneo de puertos realizado con Nmap. Elaboración propia mediante el uso de Nmap.

Activos Públicos. En el caso de activos expuestos públicamente, la fase de descubrimiento no se realiza de la misma manera que con activos internos. A diferencia de los sistemas en red local, donde se dispone de inventarios, herramientas de gestión y acceso administrativo, los activos públicos requieren técnicas externas de enumeración y, en algunos escenarios, información suministrada directamente por el proveedor o área responsable.

Lo que sí pueden realizar los analistas de CTEM e inteligencia de amenazas es ampliar la identificación de la superficie de ataque asociada a los activos públicos entregados por los proveedores. A partir de las direcciones IP públicas o dominios suministrados, es posible extender la búsqueda mediante técnicas OSINT con el fin de descubrir servicios relacionados, configuraciones expuestas o componentes que no fueron declarados inicialmente.

Para ilustrar el tipo de investigación que se realiza en esta etapa, puede tomarse como ejemplo una consulta de DNS Lookup sobre un dominio ampliamente conocido, como *google.com*. En las figuras 60 y 61 se puede observar una consulta que permite identificar todos los registros DNS asociados (A, AAAA, MX, TXT, CNAME, NS, entre otros), subdominios, servicios vinculados y características relevantes de la infraestructura pública. Aunque se trata de un dominio utilizado únicamente como referencia, demuestra cómo estas técnicas permiten construir un mapa más completo de la superficie de ataque y detectar posibles puntos de exposición que deben ser considerados dentro del inventario de activos públicos.

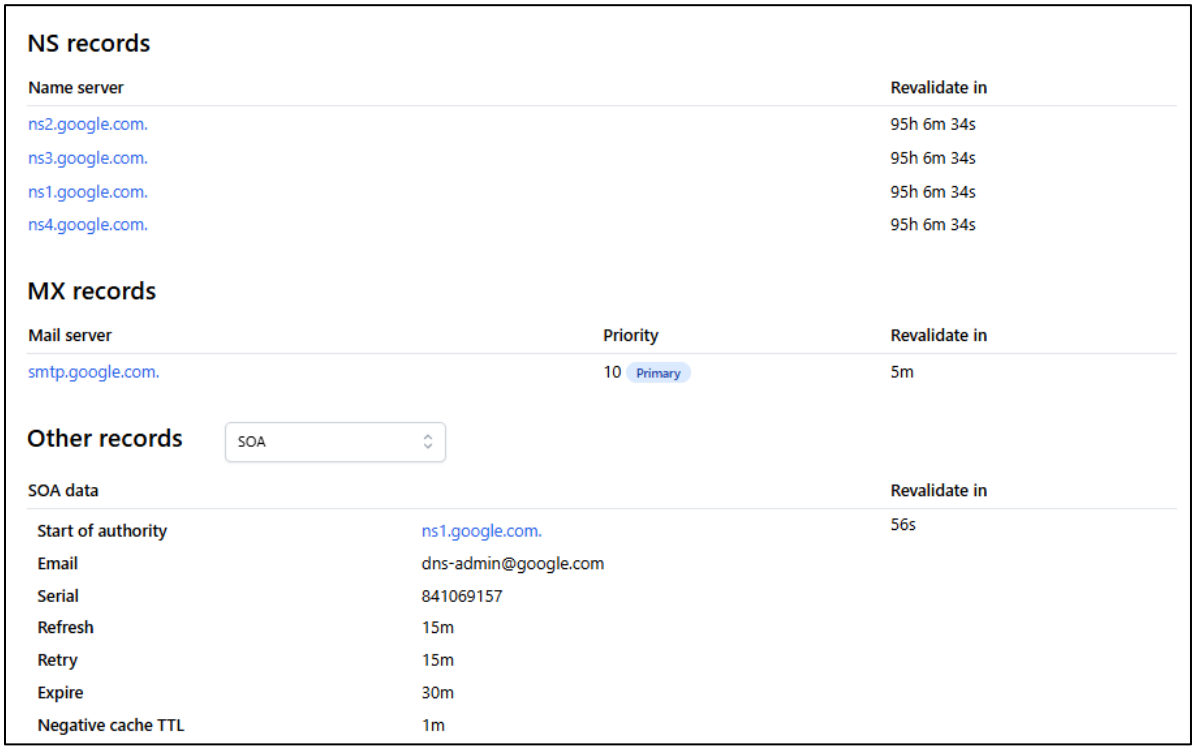
Figura 60

Consulta Registros DNS

Nota. Consulta de registros DNS realizada con la herramienta de Google. Elaboración propia mediante el uso de Google Admin Toolbox.

Figura 61

Consulta Registros DNS



NS records

Name server	Revalidate in
ns2.google.com.	95h 6m 34s
ns3.google.com.	95h 6m 34s
ns1.google.com.	95h 6m 34s
ns4.google.com.	95h 6m 34s

MX records

Mail server	Priority	Revalidate in
smtp.google.com.	10 Primary	5m

Other records SOA

SOA data		Revalidate in
Start of authority	ns1.google.com.	56s
Email	dns-admin@google.com	
Serial	841069157	
Refresh	15m	
Retry	15m	
Expire	30m	
Negative cache TTL	1m	

Nota. Consulta de registros DNS realizada con la herramienta de Google. Elaboración propia mediante el uso de Google Admin Toolbox.

Escaneos de Vulnerabilidades

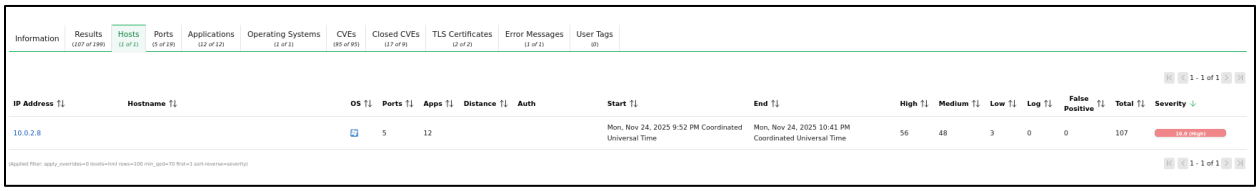
Activos Internos. Siguiendo lo establecido en el objetivo 1, donde se describió el procedimiento para ejecutar un escaneo de vulnerabilidades con OpenVas, se realizó el análisis sobre la dirección IP 10.0.2.8, correspondiente a un servidor Windows Server 2012 vulnerable preparado para este laboratorio, como se observa en la figura 62. El escaneo arrojó un total de 199 vulnerabilidades, aunque únicamente 107 presentan un QoD elevado.

El QoD es un indicador que utiliza OpenVAS para reflejar el nivel de confianza que tiene el motor en la detección realizada. En términos prácticos, un QoD *alto* significa que la herramienta

considera que la vulnerabilidad identificada es muy probablemente real y no un falso positivo. Por este motivo, dichas detecciones se priorizan en el análisis, ya que representan hallazgos con un mayor grado de confirmación técnica.

Figura 62

Resultados Escaneos de Vulnerabilidades

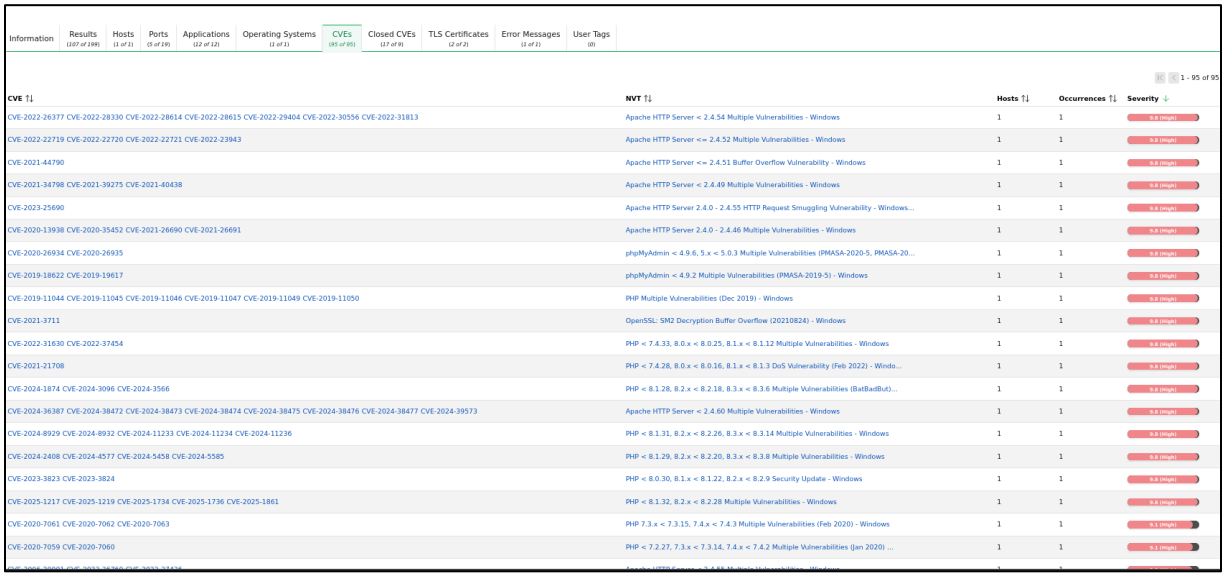


Nota. Resultados de escaneos de vulnerabilidades realizados con OpenVAS. Elaboración propia mediante el uso de OpenVAS.

Además, durante el escaneo se identificó un conjunto amplio de vulnerabilidades críticas y altas asociadas principalmente a Apache HTTP Server, PHP, phpMyAdmin y OpenSSL, con puntajes CVSS que alcanzan valores de 9.8 (High) en múltiples casos, como se muestra en la figura 63. Estas fallas abarcan desbordamientos de búfer, smuggling de solicitudes HTTP, inyección de comandos, denegación de servicio y divulgación de información, todas presentes en versiones desactualizadas de los componentes instalados. En términos generales, la mayoría de los hallazgos se clasifican en niveles High y Medium, concentrándose los de mayor severidad en versiones obsoletas de Apache (2.4.x), PHP (ramas 7.x y 8.x), phpMyAdmin y bibliotecas OpenSSL vulnerables. La presencia simultánea de estas debilidades incrementa significativamente la superficie de ataque y eleva el riesgo resultante, dado que afectan servicios críticos expuestos y susceptibles de explotación remota.

Figura 63

Resultados Escaneos de Vulnerabilidades con Openvas



Information | Results (107 of 199) | Hosts (1 of 1) | Ports (5 of 19) | Applications (12 of 12) | Operating Systems (1 of 1) | CVEs (85 of 95) | Closed CVEs (17 of 9) | TLS Certificates (2 of 2) | Error Messages (1 of 1) | User Tags (0)

1 - 95 of 95

CVE	NVT	Hosts	Occurrences	Severity
CVE-2022-26377 CVE-2022-28330 CVE-2022-28614 CVE-2022-28615 CVE-2022-29404 CVE-2022-30556 CVE-2022-31813	Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2022-22719 CVE-2022-22720 CVE-2022-22721 CVE-2022-23943	Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2021-44790	Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows	1	1	9.8 (High)
CVE-2021-34798 CVE-2021-39275 CVE-2021-40438	Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2023-25690	Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability - Windows...	1	1	9.8 (High)
CVE-2020-13938 CVE-2020-35452 CVE-2021-26690 CVE-2021-26691	Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2020-26934 CVE-2020-26935	phpMyAdmin < 4.9.6, 5.x < 5.0.3 Multiple Vulnerabilities (PMASA-2020-5, PMASA-20...	1	1	9.8 (High)
CVE-2019-18622 CVE-2019-19617	phpMyAdmin < 4.9.2 Multiple Vulnerabilities (PMASA-2019-5) - Windows	1	1	9.8 (High)
CVE-2019-11044 CVE-2019-11045 CVE-2019-11046 CVE-2019-11047 CVE-2019-11049 CVE-2019-11050	PHP Multiple Vulnerabilities (Dec 2019) - Windows	1	1	9.8 (High)
CVE-2021-3711	OpenSSL: SM2 Decryption Buffer Overflow (20210824) - Windows	1	1	9.8 (High)
CVE-2022-31630 CVE-2022-37454	PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2021-21708	PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 DoS Vulnerability (Feb 2022) - Windo...	1	1	9.8 (High)
CVE-2024-1874 CVE-2024-3096 CVE-2024-3566	PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Multiple Vulnerabilities (BatBadBut)...	1	1	9.8 (High)
CVE-2024-36387 CVE-2024-38472 CVE-2024-38473 CVE-2024-38474 CVE-2024-38475 CVE-2024-38476 CVE-2024-38477 CVE-2024-39573	Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2024-8929 CVE-2024-8932 CVE-2024-11233 CVE-2024-11234 CVE-2024-11236	PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2024-2408 CVE-2024-4577 CVE-2024-5458 CVE-2024-5585	PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2023-3823 CVE-2023-3824	PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Windows	1	1	9.8 (High)
CVE-2025-1217 CVE-2025-1219 CVE-2025-1734 CVE-2025-1736 CVE-2025-1861	PHP < 8.1.32, 8.2.x < 8.2.28 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2020-7061 CVE-2020-7062 CVE-2020-7063	PHP 7.3.x < 7.3.15, 7.4.x < 7.4.3 Multiple Vulnerabilities (Feb 2020) - Windows	1	1	9.1 (High)
CVE-2020-7059 CVE-2020-7060	PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities (Jan 2020) ...	1	1	9.1 (High)

Nota. Resultados de escaneos de vulnerabilidades realizados con OpenVAS. Elaboración propia mediante el uso de OpenVAS.

Activos Públicos. En el escaneo de vulnerabilidades a activos públicos, específicamente aplicaciones web expuestas, se toman como referencia los resultados obtenidos con Nuclei en el objetivo 1. Para esta etapa se incluyó la URL hxxps[:]//demo[.]owasp-juice[.]shop/, una aplicación deliberadamente vulnerable desarrollada por OWASP para ejercicios de ethical hacking y pruebas de seguridad, lo que permitió validar el comportamiento del escáner y observar cómo identifica fallos en un entorno controlado.

Normalización Data. Siguiendo el ejemplo de normalización de la información de inteligencia de amenazas desarrollada en el Objetivo 2, donde los indicadores se transformaron a un formato estándar STIX 2.1 para permitir interoperabilidad y análisis automatizado, los resultados de los escaneos de vulnerabilidades realizados con OpenVAS también pueden ser

normalizados de manera similar. Esto implica convertir la información de cada hallazgo como IP, puerto, protocolo, CVE, severidad, QoD, impacto y soluciones recomendadas a objetos STIX 2.1, ya sea como vulnerability para la descripción de la falla o como indicador para los elementos observables relacionados (IPs, dominios, hashes, puertos). Como se muestra en la tabla 14, la normalización permite almacenar, correlacionar y analizar los resultados de manera estructurada, integrar los hallazgos de OpenVAS con otras fuentes de CTI en un SIEM, y garantizar trazabilidad y consistencia en la gestión de vulnerabilidades dentro del ciclo CTEM.

Tabla 14

Normalización Data Mediante STIX 2.1

Campo OpenVAS	STIX 2.1	Detalle
IP	ipv4-addr	Representa la IP
Hostname	domain-name:value (opcional)	Respresenta el hostname
Port	network-traffic:dst_port	Forma parte del ciberobservables (SCO) de tipo tráfico de red
Port Protocol	network-traffic:protocols	TCP/UDP/ICMP
CVSS	x_severity_cvss	Propiedad extendida, valor numérico
Severity	labels	Ej: ["low","medium","high","critical"]
QoD	x_quality_of_detection	Propiedad extendida para indicar confiabilidad
Solution Type	x_solution_type	Ej: patch, mitigación, workaround
NVT Name	x_nvt_name	Nombre del test de OpenVAS
Summary	description	Resumen de la vulnerabilidad
Specific Result	x_specific_result	Resultado específico del NVT
NVT OID	x_nvt_oid	ID único del test
CVEs	external_references	Objeto con source_name: "CVE" y external_id: "CVE-xxxx-xxxx"
Task ID / Task Name	x_task_id, x_task_name	Para trazabilidad del escaneo
Timestamp	valid_from	Fecha y hora de la detección
Result ID	x_result_id	ID único del resultado
Impact	x_impact	Ej: confidentiality/availability/integrity
Solution	x_solution	Instrucciones de mitigación
Affected Software/OS	x_affected_software	Ej: Linux Kernel, Windows Server
Vulnerability Insight	x_vuln_insight	Observaciones adicionales del analista
Vulnerability Detection Method	x_detection_method	Ej: authenticated scan, unauthenticated scan

Campo OpenVAS	STIX 2.1	Detalle
Product Detection Result	x_product_result	Resultado específico de la detección
BIDs	external_references	Como CVE, con source_name: "BID"
CERTs	external_references	Como CVE, con source_name: "CERT"
¿Vulnerabilidad en el KEV de CISA?	x_kev_flag	Booleano
EPSS	x_epss	Valor numérico (0 a 1)

*Nota***.** La tabla presenta la correspondencia entre los campos generados por OpenVAS y su mapeo a objetos y propiedades de STIX 2.1, con el fin de estructurar la información de vulnerabilidades para su integración, análisis y correlación en plataformas de inteligencia de amenazas.

Del mismo modo, los resultados de los escaneos realizados con Nuclei pueden ser normalizados en formato STIX 2.1, como se muestra en la tabla 15.

Tabla 15

Normalización Data Mediante STIX 2.1

Campo Nuclei	STIX 2.1	Detalle
template_id	x_template_id	Identificador único de la plantilla Nuclei que se ejecuta para detectar la vulnerabilidad.
template	x_template_name	Nombre legible de la plantilla utilizada en el escaneo.
template_url	external_references	URL de referencia de la plantilla en el repositorio oficial o fuente de descarga.
template_path	x_template_path	Ruta local donde se encuentra la plantilla en el sistema de escaneo.
host	domain-name:value o ipv4-addr:value (SCO)	Nombre de dominio o IP del host objetivo donde se detecta la vulnerabilidad.
ip	ipv4-addr:value (SCO)	Dirección IP del host afectado.
port	network-traffic:dst_port (SCO)	Puerto de red donde se detecta la vulnerabilidad o servicio.
url	url:value (SCO / indicator)	URL completa del recurso analizado por la plantilla.
path	x_path	Ruta específica dentro del host o URL donde se detecta la vulnerabilidad.
matched_at	first_observed / last_observed	Marca temporal en la que se identificó la coincidencia del patrón de la plantilla.
info_id	x_info_id	Identificador interno de la detección dentro del escaneo.
name	name	Nombre del hallazgo o vulnerabilidad detectada.
severity	labels	Nivel de severidad asignado al hallazgo (ej.: info, low, medium, high, critical).
cve	external_references (source_name: "CVE")	Identificador CVE asociado al hallazgo, si existe.
cwe	external_references (source_name: "CWE")	Identificador CWE relacionado con la categoría de vulnerabilidad detectada.
cvss	x_severity_cvss	Puntuación CVSS asociada a la vulnerabilidad, indicando su gravedad.
description	description	Breve descripción del hallazgo y su contexto.

Campo Nuclei	STIX 2.1	Detalle
remediation	x_solution	Recomendaciones o pasos para mitigar la vulnerabilidad detectada.
references	external_references	URLs, artículos o documentación externa relacionada con la vulnerabilidad o prueba.
tags	labels	Etiquetas que clasifican el hallazgo según tipo, categoría o tecnología.
matcher_name	x_matcher_name	Nombre del matcher utilizado por Nuclei para detectar la vulnerabilidad.
request	x_request	Petición HTTP utilizada por la plantilla para realizar la prueba.
response_trunc	x_response_trunc	Respuesta HTTP truncada del servidor que evidencia el hallazgo.

Nota. La tabla presenta la correspondencia entre los campos generados por Nuclei y su mapeo a objetos y propiedades de STIX 2.1, con el fin de estructurar los hallazgos para su integración, análisis y correlación en plataformas de inteligencia de amenazas.

Priorización

La etapa 3 se enfoca en la priorización, la cual depende de dos elementos fundamentales:

El contexto del activo, es decir, el impacto que tendría para el negocio si ese activo fuera comprometido.

El contexto de la amenaza, en relación con el riesgo real que esta amenaza puede representar para el negocio.

En cuanto al contexto del activo, la CMDB construida en etapas anteriores permite determinar su relevancia para la organización. Allí se documenta su función dentro de los procesos del negocio, el tipo de información que gestiona, los datos regulados que almacena, y las dependencias operativas asociadas. Esto permite diferenciar activos críticos, por ejemplo, servidores web que soportan transacciones, bases de datos con información de clientes o

infraestructuras expuestas públicamente de activos de menor impacto, como estaciones de trabajo administrativas o servicios internos de apoyo. La priorización, en este sentido, considera qué tan grave sería para la organización la pérdida de disponibilidad, confidencialidad o integridad de ese activo.

El segundo componente corresponde al contexto de la amenaza, que se analiza con base en los resultados de los escaneos de vulnerabilidades. Aquí se consideran aspectos como la existencia de exploits públicos, POC, la facilidad de explotación, el nivel de interacción requerido, su uso en campañas maliciosas activas como campañas de Ransomware, entre otros factores. De esta forma, dos vulnerabilidades con la misma severidad CVSS no necesariamente tienen la misma prioridad: Una falla con explotación conocida tendrá prioridad sobre una vulnerabilidad que no está siendo explotada activamente.

La combinación de estos dos factores permite establecer una priorización más precisa y ajustada a la realidad de la organización. Un activo crítico con una vulnerabilidad de explotación sencilla tendrá prioridad inmediata, mientras que un activo de bajo impacto solo escalará si la amenaza asociada representa un riesgo técnico significativo. Esta integración entre valor del activo y severidad de la amenaza es lo que habilita una priorización alineada tanto con las necesidades del negocio como con el panorama real de exposición.

Contexto del Activo. Para ilustrar el contexto del activo, se toma como referencia el servidor Windows Server 2016 con dirección IP 10.0.2.8, identificado en la CMDB como un componente de alta relevancia operativa. En este ejercicio se asume que dicho servidor soporta un proceso esencial para el negocio, ya sea un servicio interno de autenticación, un módulo de gestión financiera o un sistema central para la operación diaria. Esta relación directa con funciones críticas lo convierte en un activo clave dentro de la infraestructura. Su indisponibilidad

afectaría la continuidad del servicio, impactaría los flujos internos y podría detener tareas que dependen de él. Por esta razón se clasifica como un activo crítico dentro del proceso de priorización.

Contexto de las Amenazas. Se tendrá en cuenta los resultados del escaneo de vulnerabilidades realizado a la dirección IP 10.0.2.8 y la inteligencia de amenazas recopilada en el objetivo 2.

En el proceso continuo de gestión de la exposición, existen dos etapas diferenciadas pero complementarias que permiten integrar el contexto técnico con el contexto de inteligencia de amenazas. En la primera, el equipo de inteligencia de amenazas realiza una recolección permanente de información a partir de las fuentes Alien Vault OTX e IBM X- Force, las cuales pueden tener bases de datos de vulnerabilidades, reportes de proveedores, plataformas de monitoreo de exploits, repositorios de PoC y servicios especializados como KEV, EPSS o MITRE ATT&CK. En esta fase, los analistas identifican nuevas vulnerabilidades de interés estratégico, amenazas emergentes, campañas activas y técnicas utilizadas por actores maliciosos. Toda esta información se consolida y se remite al equipo CTEM para que pueda verificar si las vulnerabilidades detectadas tienen alguna relación con la infraestructura real de la organización, aunque en este primer momento no existe certeza de que afecten a los activos internos o públicos.

La segunda etapa ocurre cuando los analistas CTEM ejecutan los escaneos de vulnerabilidades sobre los activos identificados en la CMDB. Este proceso permite determinar qué vulnerabilidades están realmente presentes en los sistemas y cuál es su alcance dentro del entorno de la organización. Una vez obtenidos los resultados, estos se devuelven al equipo de inteligencia de amenazas para que puedan contextualizar cada vulnerabilidad detectada. Este

análisis incluye la consulta del puntaje EPSS, la verificación de su presencia en el catálogo KEV de CISA, la revisión de campañas recientes que la estén explotando, la existencia de exploits públicos, su relevancia para actores conocidos y la asociación con tácticas y técnicas del marco MITRE ATT&CK.

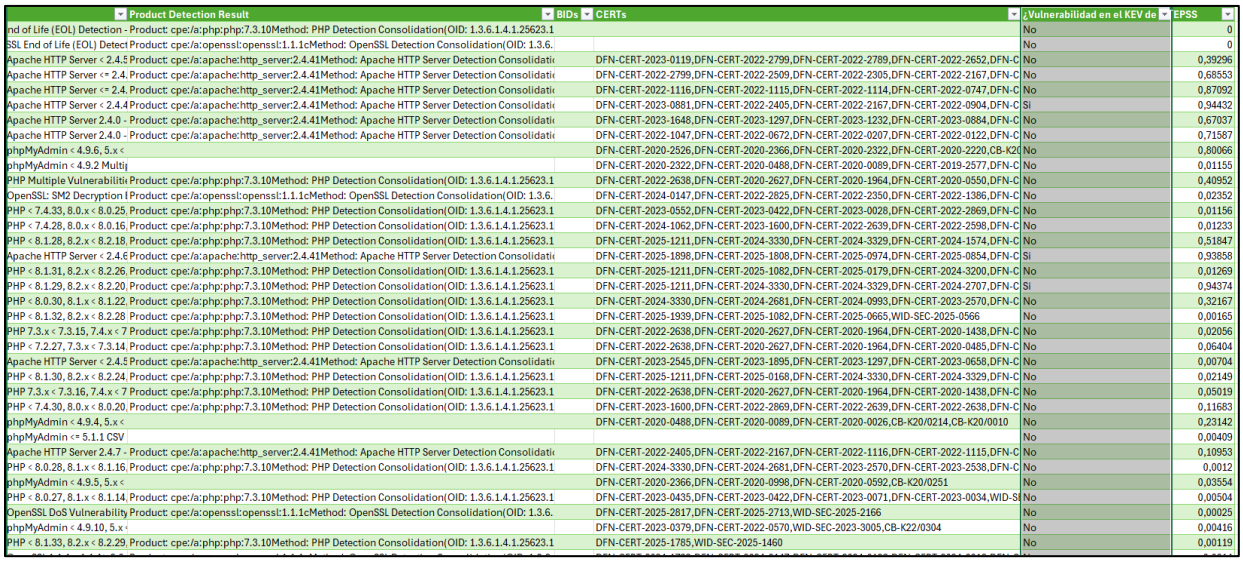
Este flujo bidireccional asegura que la priorización no dependa únicamente de información técnica ni exclusivamente del panorama externo, sino de la suma de ambos factores. De esta manera, una vulnerabilidad como la CVE-2025-59287, identificada inicialmente en el objetivo 2 del plan de recolección de inteligencia y posteriormente confirmada en un servidor Windows interno, puede ser evaluada con un contexto completo. Su PoC pública, la probabilidad de explotación estimada mediante EPSS, su ausencia o presencia en KEV y las TTPs asociadas permiten calificar su riesgo práctico de forma precisa y orientar acciones inmediatas de mitigación.

Contexto de Amenazas Obtenido a Partir del Análisis del Equipo de Inteligencia de Amenazas. Como se muestra en la figura 64 el equipo de inteligencia de amenazas puede proporcionar un reporte complementario que incluye el puntaje EPSS de cada vulnerabilidad, así como la verificación de si la vulnerabilidad se encuentra registrada en el catálogo KEV de CISA.

CISA proporciona los datos de las vulnerabilidades incluidas en el KEV en formatos JSON y CSV (CISA, s.f.), mientras que FIRST ofrece una API que permite consultar el puntaje EPSS de cada vulnerabilidad (FIRST, s.f.).

Figura 64

Resultados de Openvas con el Contexto de las Amenazas



Product Detection Result	BIDs	CERTs	¿Vulnerabilidad en el KEV de	EPSS
nd of Life (EOL) Detection - Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1			No	0
SSL End of Life (EOL) Detect Product: cpe:/a:openssl:openssl:1.1.1cMethod: OpenSSL Detection Consolidation(OID: 1.3.6.			No	0
Apache HTTP Server < 2.4.5 Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2023-0119,DFN-CERT-2022-2799,DFN-CERT-2022-2789,DFN-CERT-2022-2652,DFN-C	No	0,39296
Apache HTTP Server <= 2.4. Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2022-2799,DFN-CERT-2022-2509,DFN-CERT-2022-2305,DFN-CERT-2022-2167,DFN-C	No	0,68553
Apache HTTP Server <= 2.4. Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2022-1116,DFN-CERT-2022-1115,DFN-CERT-2022-1114,DFN-CERT-2022-0747,DFN-C	No	0,87092
Apache HTTP Server < 2.4.4 Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2023-0881,DFN-CERT-2022-2405,DFN-CERT-2022-2167,DFN-CERT-2022-0904,DFN-C	Si	0,94432
Apache HTTP Server 2.4.0 - Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2023-1648,DFN-CERT-2023-1297,DFN-CERT-2023-1232,DFN-CERT-2023-0884,DFN-C	No	0,67037
Apache HTTP Server 2.4.0 - Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2022-1047,DFN-CERT-2022-0672,DFN-CERT-2022-0207,DFN-CERT-2022-0122,DFN-C	No	0,71587
phpMyAdmin < 4.9.6, 5.x <		DFN-CERT-2020-2526,DFN-CERT-2020-2366,DFN-CERT-2020-2322,DFN-CERT-2020-2220,CB-K20	No	0,80066
phpMyAdmin < 4.9.2 Multi		DFN-CERT-2020-2322,DFN-CERT-2020-0488,DFN-CERT-2020-0089,DFN-CERT-2019-2577,DFN-C	No	0,01155
PHP Multiple Vulnerabiliti Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2022-2638,DFN-CERT-2020-2627,DFN-CERT-2020-1964,DFN-CERT-2020-0550,DFN-C	No	0,40952
OpenSSL: SM2 Decryption I Product: cpe:/a:openssl:openssl:1.1.1cMethod: OpenSSL Detection Consolidation(OID: 1.3.6.		DFN-CERT-2024-0147,DFN-CERT-2022-2825,DFN-CERT-2022-2350,DFN-CERT-2022-1386,DFN-C	No	0,02352
PHP < 7.4.33, 8.0.x < 8.0.25, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2023-0552,DFN-CERT-2023-0422,DFN-CERT-2023-0028,DFN-CERT-2022-2869,DFN-C	No	0,01156
PHP < 7.4.28, 8.0.x < 8.0.16, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2024-1062,DFN-CERT-2023-1600,DFN-CERT-2022-2639,DFN-CERT-2022-2598,DFN-C	No	0,01233
PHP < 8.1.28, 8.2.x < 8.2.18, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2025-1211,DFN-CERT-2024-3330,DFN-CERT-2024-3329,DFN-CERT-2024-1574,DFN-C	No	0,51847
Apache HTTP Server < 2.4.6 Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2025-1898,DFN-CERT-2025-1808,DFN-CERT-2025-0974,DFN-CERT-2025-0854,DFN-C	Si	0,93858
PHP < 8.1.31, 8.2.x < 8.2.26, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2025-1211,DFN-CERT-2025-1082,DFN-CERT-2025-0179,DFN-CERT-2024-3200,DFN-C	No	0,01269
PHP < 8.1.29, 8.2.x < 8.2.20, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2025-1211,DFN-CERT-2024-3330,DFN-CERT-2024-3329,DFN-CERT-2024-2707,DFN-C	Si	0,94374
PHP < 8.0.30, 8.1.x < 8.1.22, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2024-3330,DFN-CERT-2024-2681,DFN-CERT-2024-0993,DFN-CERT-2023-2570,DFN-C	No	0,32167
PHP < 8.1.32, 8.2.x < 8.2.28 Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2025-1939,DFN-CERT-2025-1082,DFN-CERT-2025-0665,WID-SEC-2025-0566	No	0,00165
PHP 7.3.x < 7.3.15, 7.4.x < 7 Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2022-2638,DFN-CERT-2020-2627,DFN-CERT-2020-1964,DFN-CERT-2020-1438,DFN-C	No	0,02056
PHP < 7.2.27, 7.3.x < 7.3.14, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2022-2638,DFN-CERT-2020-2627,DFN-CERT-2020-1964,DFN-CERT-2020-0485,DFN-C	No	0,06404
Apache HTTP Server < 2.4.5 Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2023-2545,DFN-CERT-2023-1895,DFN-CERT-2023-1297,DFN-CERT-2023-0658,DFN-C	No	0,00704
PHP < 8.1.30, 8.2.x < 8.2.24, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2025-1211,DFN-CERT-2025-0168,DFN-CERT-2024-3330,DFN-CERT-2024-3329,DFN-C	No	0,02149
PHP 7.3.x < 7.3.16, 7.4.x < 7 Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2022-2638,DFN-CERT-2020-2627,DFN-CERT-2020-1964,DFN-CERT-2020-1438,DFN-C	No	0,05019
PHP < 7.4.30, 8.0.x < 8.0.20, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2023-1600,DFN-CERT-2022-2869,DFN-CERT-2022-2639,DFN-CERT-2022-2638,DFN-C	No	0,11683
phpMyAdmin < 4.9.4, 5.x <		DFN-CERT-2020-0488,DFN-CERT-2020-0089,DFN-CERT-2020-0026,CB-K20/0214,CB-K20/0010	No	0,23142
phpMyAdmin <= 5.1.1 CSV			No	0,00409
Apache HTTP Server 2.4.7 - Product: cpe:/a:apache:http_server:2.4.41Method: Apache HTTP Server Detection Consolidati		DFN-CERT-2022-2405,DFN-CERT-2022-2167,DFN-CERT-2022-1116,DFN-CERT-2022-1115,DFN-C	No	0,10953
PHP < 8.0.28, 8.1.x < 8.1.16, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2024-3330,DFN-CERT-2024-2681,DFN-CERT-2023-2570,DFN-CERT-2023-2538,DFN-C	No	0,0012
phpMyAdmin < 4.9.5, 5.x <		DFN-CERT-2020-2366,DFN-CERT-2020-0998,DFN-CERT-2020-0592,CB-K20/0251	No	0,03554
PHP < 8.0.27, 8.1.x < 8.1.14, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2023-0435,DFN-CERT-2023-0422,DFN-CERT-2023-0071,DFN-CERT-2023-0034,WID-S	No	0,00504
OpenSSL DoS Vulnerability Product: cpe:/a:openssl:openssl:1.1.1cMethod: OpenSSL Detection Consolidation(OID: 1.3.6.		DFN-CERT-2025-2817,DFN-CERT-2025-2713,WID-SEC-2025-2166	No	0,00025
phpMyAdmin < 4.9.10, 5.x <		DFN-CERT-2023-0379,DFN-CERT-2022-0570,WID-SEC-2023-3005,CB-K22/0304	No	0,00416
PHP < 8.1.33, 8.2.x < 8.2.29, Product: cpe:/a:php:php:7.3.10Method: PHP Detection Consolidation(OID: 1.3.6.1.4.1.25623.1		DFN-CERT-2025-1785,WID-SEC-2025-1460	No	0,00119

Nota. Resultados de escaneos de vulnerabilidades realizados con OpenVAS. Elaboración propia mediante el uso de OpenVAS.

Teniendo en cuenta la información recopilada tanto por el equipo de CTEM como por los analistas de inteligencia de amenazas, se estableció un sistema de priorización aplicado sobre los resultados obtenidos en el escaneo de vulnerabilidades realizado con OpenVAS. Cada vulnerabilidad identificada fue enriquecida con información proveniente del catálogo CISA KEV y con el puntaje de probabilidad de explotación del modelo EPSS, permitiendo establecer un esquema de priorización basado en riesgo real y probabilidad de explotación.

El esquema de priorización se definió de la siguiente manera:

Prioridad 1: Vulnerabilidades incluidas en el KEV de CISA. Estas representan un riesgo crítico, dado que han sido identificadas como activamente explotadas en entornos reales. En los resultados obtenidos se registraron 4 vulnerabilidades dentro de este nivel, por lo que requieren remediación inmediata.

Prioridad 2: Vulnerabilidades con puntaje EPSS mayor a 0,7 que no se encuentran en el KEV. Aunque no estén documentadas como parte de campañas activas según CISA, presentan una alta probabilidad de explotación, por lo que se consideran de atención prioritaria. En este nivel se identificaron 10 vulnerabilidades.

Prioridad 3: Vulnerabilidades con puntaje EPSS entre 0,4 y 0,69. Estas representan un riesgo moderado, por lo que su tratamiento puede realizarse dentro de ciclos de remediación planificados. En los resultados analizados se registraron 10 vulnerabilidades dentro de este rango.

Este enfoque permitió transformar los resultados técnicos del escaneo en un proceso de priorización alineado con la fase de priorización del modelo CTEM, donde las vulnerabilidades no se gestionan únicamente por su severidad técnica, sino también considerando evidencia de explotación activa y probabilidad real de ataque, como se muestra en la tabla 16.

Tabla 16

Vulnerabilidades Para Priorizar

Prioridad	Criterio	Cantidad de vulnerabilidades
1	Vulnerabilidades en el KEV de CISA	4
2	Vulnerabilidades con EPSS mayor a 0,7 (sin contar las que ya están en KEV)	10
3	Vulnerabilidades con EPSS entre 0,4 y 0,69	10

*Nota***.** La tabla presenta los criterios de priorización de vulnerabilidades basados en su presencia en el catálogo KEV de CISA y en el puntaje EPSS.

Para ilustrar la aplicación del proceso de priorización, inicialmente se asumió que la vulnerabilidad identificada en el objetivo 2, CVE-2025-59287, se encontraba presente en uno de los activos críticos identificados previamente, específicamente el servidor Windows Server 2016 con dirección IP 10.0.2.8. Esta relación permite analizar el riesgo considerando tanto la criticidad del activo dentro de la infraestructura como la probabilidad de explotación de la vulnerabilidad.

Sin embargo, con el fin de representar un escenario más cercano a un entorno organizacional real, las vulnerabilidades identificadas durante el análisis se distribuyeron entre diferentes activos de la infraestructura. Esta distribución se realizó teniendo en cuenta el nivel de criticidad e impacto de cada activo para el negocio, de acuerdo con la información registrada en la CMDB construida como parte del ejemplo. De esta forma, las vulnerabilidades priorizadas se asociaron a activos con distintos niveles de prioridad, lo que permite observar cómo el riesgo puede variar dependiendo del sistema afectado, como se muestra en la tabla 17.

Tabla 17

Vulnerabilidades y Activos Para Priorizar

Prioridad	Criterio de priorización	Activos asociados	Cantidad de activos	Vulnerabilidades asociadas
1	Activos con criticidad Crítico (MA) debido a su impacto alto sobre la operación o la información sensible	SERPAGOS01, DBSERV01, WS-WIN01, WS-MAC02	4	4 vulnerabilidades en KEV
2	Activos con criticidad Alto (A) que procesan información sensible o soportan servicios internos relevantes	WEBAPI03, DBSERV02, FILES01, WS-WIN02, WS-WIN03	5	10 vulnerabilidades con EPSS > 0,7
3	Activos con criticidad Medio (M) que soportan funciones institucionales con impacto moderado	WEBAPP02, APPSRV01	2	10 vulnerabilidades con EPSS entre 0,4 y 0,69
4	Activos con criticidad Bajo (B) cuyo impacto sobre la operación es limitado	WS-MAC01	1	Sin vulnerabilidades priorizadas

Nota. La tabla presenta la priorización de activos de acuerdo con su nivel de criticidad (Muy Alto, Alto, Medio y Bajo), relacionando los activos asociados, su cantidad y las vulnerabilidades identificadas según criterios como su inclusión en KEV y el puntaje EPSS.

Resultados de Nuclei con el Contexto de las Amenazas y del Activo. Como se muestra en la figura 65, se toma como ejemplo la URL de OWASP escaneada considerando que corresponde a un activo crítico.

Figura 65

Resultados de Nuclei con el Contexto de las Amenazas

matched_at	info_id	name	severity	cve	cwe	¿Vulnerabilidad en OWASP?	Categoría OWASP	cvss	description
https://demo.owasp-juice.shop/	external-service-interaction	External Service Interaction	info		cwe-918	Si	Server-Side Request Forgery (SSRF)		External Service interaction via Host Header Injection.
https://demo.owasp-juice.shop/	external-service-interaction	External Service Interaction	info		cwe-406	No	N/A		External Service interaction via Host Header Injection.
https://demo.owasp-juice.shop/	missing-sri	Missing Subresource Integrity	info			No	N/A		Checks if external script and stylesheet tags in the HTML response
demo.owasp-juice.shop:443	tls-version	TLS Version - Detect	info			No	N/A		TLS version detection is a security process used to determine the ve
demo.owasp-juice.shop:443	tls-version	TLS Version - Detect	info			No	N/A		TLS version detection is a security process used to determine the ve
https://demo.owasp-juice.shop/robots.txt	robots-txt-endpoint	robots.txt endpoint prober	info			No	N/A		
https://demo.owasp-juice.shop/robots.txt	robots-txt	robots.txt file	info			No	N/A		
https://demo.owasp-juice.shop/	x-recruiting-header	X-Recruiting Header	info			No	N/A		Websites that advertise jobs via HTTP headers
https://demo.owasp-juice.shop/	addeventlistener-detect	Add DOM EventListener - Detectio	info			No	N/A		Identifies the use of JavaScript addEventListener calls in the DOM.
https://demo.owasp-juice.shop/	owasp-juice-shop-detect	OWASP Juice Shop	info			No	N/A		
https://demo.owasp-juice.shop/metrics	prometheus-metrics	Prometheus Metrics - Detect	medium		cwe-200	Si	Exposure of Sensitive Information to ar	CVSS:3.1/AV:N/A	Prometheus metrics page was detected.
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	http-missing-security-headers	HTTP Missing Security Headers	info			No	N/A		This template searches for missing HTTP security headers. The imp
https://demo.owasp-juice.shop/	fingerprinthub-web-fingerprints	FingerprintHub Technology Finge	info		cwe-200	Si	Exposure of Sensitive Information to ar		FingerprintHub Technology Fingerprint tests run in nuclei.
https://demo.owasp-juice.shop/.well-known/	security-txt	security.txt File	info			No			File similar to robots.txt but intended to be read by humans wishin
demo.owasp-juice.shop	mx-fingerprint	MX Record Detection	info		cwe-200	Si	Exposure of Sensitive Information to ar		An MX record was detected. MX records direct emails to a mail exc
demo.owasp-juice.shop:443	ssl-issuer	Detect SSL Certificate Issuer	info			No			Extract the issuer's organization from the target's certificate. Issue
demo.owasp-juice.shop:443	ssl-dns-names	SSL DNS Names	info			No			Extract the Subject Alternative Name (SAN) from the target's certific
demo.owasp-juice.shop:443	wildcard-tls	Wildcard TLS Certificate	info			No			Checks a sites certificate to see if there are wildcard CN or SAN ent
demo.owasp-juice.shop	caa-fingerprint	CAA Record	info		cwe-200	Si	Exposure of Sensitive Information to ar		A CAA record was discovered. A CAA record is used to specify whic

Nota. Resultados de escaneos de vulnerabilidades realizados con Nuclei. Elaboración propia mediante el uso de Nuclei.

Teniendo en cuenta los resultados obtenidos durante el análisis de vulnerabilidades en la aplicación OWASP Juice Shop, se realizó una priorización adicional considerando su relación con el OWASP y las categorías definidas en el OWASP Top 10.

Las debilidades que se encuentran asociadas a categorías del OWASP Top 10 fueron clasificadas como prioridad 1, debido a que representan riesgos ampliamente conocidos en aplicaciones web y suelen ser explotados en escenarios reales. Dentro de este grupo se identificaron cinco ocurrencias, correspondientes principalmente a Server-Side Request Forgery (CWE-918) y Exposure of Sensitive Information (CWE-200).

En un segundo nivel se ubicaron debilidades que cuentan con clasificación CWE pero que no están directamente relacionadas con el OWASP Top 10, como CWE-406, las cuales pueden contribuir a escenarios de explotación dependiendo del contexto del sistema.

Finalmente, se clasificaron como prioridad baja los hallazgos informativos relacionados con detección de tecnologías, encabezados HTTP faltantes o configuraciones del sistema, los cuales no representan vulnerabilidades críticas por sí mismos, pero pueden facilitar actividades de reconocimiento por parte de un atacante, como se muestra en la tabla 18.

Tabla 18

Debilidades Para Priorizar

Prioridad	Criterio	Cantidad de vulnerabilidades
1	Vulnerabilidades asociadas a categorías del OWASP Top 10	5
2	Debilidades clasificadas como CWE pero que no aparecen en OWASP Top 10	1
3	Hallazgos informativos o de configuración detectados durante el escaneo	21

Nota. La tabla presenta la clasificación de debilidades según criterios de priorización basados en su relación con el OWASP Top 10, categorías CWE y hallazgos informativos, indicando la cantidad de vulnerabilidades asociadas a cada nivel.

Para la identificación de vulnerabilidades en aplicaciones web se utilizó la herramienta Nuclei. El escaneo se realizó sobre la URL del proyecto OWASP con fines demostrativos, con el objetivo de mostrar el funcionamiento de la herramienta y el tipo de hallazgos que pueden obtenerse durante una evaluación de seguridad web.

No obstante, para efectos del ejercicio y con el fin de aproximar el análisis a un entorno organizacional real, las vulnerabilidades identificadas se distribuyeron entre los activos de tipo servidor web registrados en la CMDB construida como ejemplo. En este caso se consideraron específicamente los activos SERPAGOS01 (Pasarela de Pagos), WEBAPP02 (Portal Institucional) y WEBAPI03 (API de Servicios), los cuales representan sistemas que exponen servicios web dentro de la infraestructura.

Como se muestra en la tabla 19, esta distribución permite analizar cómo las vulnerabilidades detectadas podrían afectar distintos servicios web de la organización, teniendo

en cuenta el rol que cumple cada activo dentro de la operación del negocio y su nivel de criticidad dentro de la infraestructura tecnológica.

Tabla 19

Debilidades y Activos Para Priorizar

Prioridad	Criterio de priorización	Activos asociados	Cantidad de activos	Debilidades asociadas
1	Activos web con criticidad Crítico (MA) debido a su impacto directo en servicios expuestos a clientes y procesamiento de datos sensibles	SERPAGOS01	1	5 debilidades OWASP Top 10
2	Activos web con criticidad Alto (A) que soportan servicios internos mediante APIs y autenticación basada en tokens	WEBAPI03	1	1 debilidad clasificada como CWE
3	Activos web con criticidad Media (M) que soportan funciones institucionales y contenido público	WEBAPP02	1	21 hallazgos informativos o de configuración

Nota. La tabla presenta la relación entre los niveles de prioridad, los criterios de priorización, los activos web asociados y la cantidad de debilidades identificadas, con el fin de evidenciar el impacto según la criticidad de cada activo.

De esta manera, la priorización no se realiza únicamente sobre la base de la severidad teórica de las vulnerabilidades, sino que se centra en aquellas que representan un riesgo real para

la organización, facilitando la asignación de recursos y la planificación de acciones de mitigación efectivas.

Validación

La fase 4 corresponde a la validación de vulnerabilidades y escenarios de ataque. En esta etapa se busca comprobar si los atacantes pudieran realmente aprovechar las vulnerabilidades identificadas, evaluando todas las posibles vías de explotación sobre los activos críticos. Para ello, se puede considerar la información recolectada en el objetivo 2, incluyendo los vectores de ataque y las TTPs identificadas, lo que permite contextualizar mejor los riesgos y anticipar posibles movimientos del atacante.

Además, se analiza la capacidad de respuesta de los sistemas y procedimientos actuales, verificando si son lo suficientemente rápidos y efectivos para proteger el negocio ante un incidente real. Es fundamental que todos los actores del negocio estén alineados sobre los factores que desencadenan la remediación, asegurando un consenso sobre los criterios de actuación y la prioridad de las acciones correctivas. Esta etapa permite cerrar el ciclo de gestión de riesgos, pasando de la identificación y priorización de vulnerabilidades a la validación práctica de su impacto y la efectividad de las defensas implementadas.

Aplicación de Controles (Mitigaciones). En caso de que la organización no pueda aplicar un parche de manera inmediata para corregir una vulnerabilidad, es posible implementar controles compensatorios o de otro tipo que mitiguen el riesgo. Las pruebas de ethical hacking permiten validar la efectividad de estos controles, simulando intentos de explotación sobre los activos protegidos. De esta manera, se puede determinar si el control compensatorio impide el aprovechamiento de la vulnerabilidad y si realmente reduce el riesgo al nivel esperado. Esta

validación práctica garantiza que las medidas implementadas cumplan su función antes de que la vulnerabilidad sea corregida de forma definitiva.

Además, la implementación de un control satisfactorio permite reducir el nivel de riesgo de la vulnerabilidad.

***Tipos de Controles*.** En el contexto de seguridad de la información, los controles se pueden clasificar en tres grandes tipos, según su función y objetivo:

Controles preventivos: Estos controles buscan impedir que ocurra un incidente de seguridad. Actúan antes de que se materialice una amenaza. Ejemplos: firewalls, autenticación multifactor, cifrado de datos, políticas de contraseñas, segmentación de red, y parches de software aplicados de manera oportuna.

Controles detectivos: Su objetivo es identificar y alertar sobre actividades sospechosas o incidentes en curso. No evitan directamente la amenaza, pero permiten reaccionar de manera oportuna. Ejemplos: Sistemas de detección de intrusos, registros de auditoría, monitoreo de red, alertas de SIEM y escaneos de vulnerabilidades periódicos.

En el objetivo 2 se identificaron indicadores de compromiso, tales como hashes de archivos maliciosos y firmas de IPS, asociados a intentos de explotación de la vulnerabilidad CVE-2025-59287. Estos IOC funcionan como controles detectivos, permitiendo al equipo de seguridad monitorear activamente la red y los sistemas para identificar posibles intentos de explotación antes de que se produzca un compromiso real. De esta manera, se refuerza la capacidad de respuesta y se valida la efectividad de controles compensatorios que la organización pueda implementar cuando no es posible aplicar un parche de manera inmediata.

Controles correctivos: Se enfocan en mitigar o remediar el impacto de un incidente una vez que este ha ocurrido. Pueden incluir la restauración de servicios, recuperación de datos y

aplicación de parches o actualizaciones. Ejemplos: restauración desde copias de seguridad, cierre de puertos vulnerables, bloqueos de cuentas comprometidas, y reconfiguración de sistemas afectados.

En escenarios donde no se puede aplicar un parche inmediatamente, se suelen usar controles compensatorios, que pueden ser preventivos o detectivos, diseñados para reducir el riesgo temporalmente mientras se implementa la solución definitiva. Por ejemplo, limitar el acceso a un servicio vulnerable, aplicar filtrado de tráfico o monitoreo intensivo de actividad sospechosa.

Pruebas de Penetración

Si bien la validación mediante pruebas de penetración es una actividad fundamental dentro del ciclo CTEM, no se profundizará en su ejecución, debido a que estas pruebas son realizadas usualmente por un equipo especializado en ethical hacking y no constituyen el foco principal de esta monografía. No obstante, con el fin de ejemplificar el proceso de validación técnica, se presentará una prueba básica utilizando Metasploit, orientada únicamente a demostrar de manera conceptual cómo un analista puede verificar si una vulnerabilidad es explotable o si un control compensatorio aplicado por la organización resulta eficaz para bloquear el ataque.

Prueba de Intento de Explotación de la Vulnerabilidad CVE-2025-59287. Para verificar si existían módulos de explotación relacionados con la vulnerabilidad CVE-2025-59287 dentro de Metasploit, se ejecutó el comando search cve:2025-59287.

El propósito de este comando es consultar la base de datos interna del framework y filtrar todos los módulos cuyo registro esté asociado con el identificador CVE especificado. Al finalizar la búsqueda, Metasploit reportó un módulo coincidente.

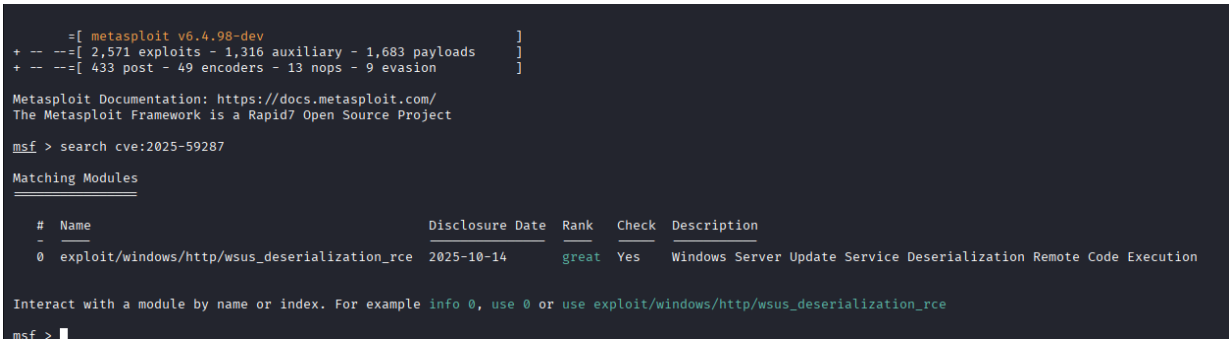
Este resultado confirma que la vulnerabilidad asociada a WSUS cuenta con un exploit

desarrollado y publicado en Metasploit, catalogado con un nivel de fiabilidad Great, lo cual indica que es estable y que suele funcionar de forma consistente en condiciones reales, como se muestra en la figura 66. El módulo corresponde exactamente al vector de ataque descrito en el objetivo 2: una ejecución remota de código derivada de la deserialización insegura en el servicio WSUS.

Además, Metasploit indica que el módulo incluye funcionalidad de Check, lo que permite verificar si un host es vulnerable antes de ejecutar el exploit, lo que resulta útil en la fase de validación.

Figura 66

Prueba de Ethical Hacking Para Validación



Nota. Pruebas de ethical hacking realizadas para validación. Elaboración propia mediante el uso de Metasploit.

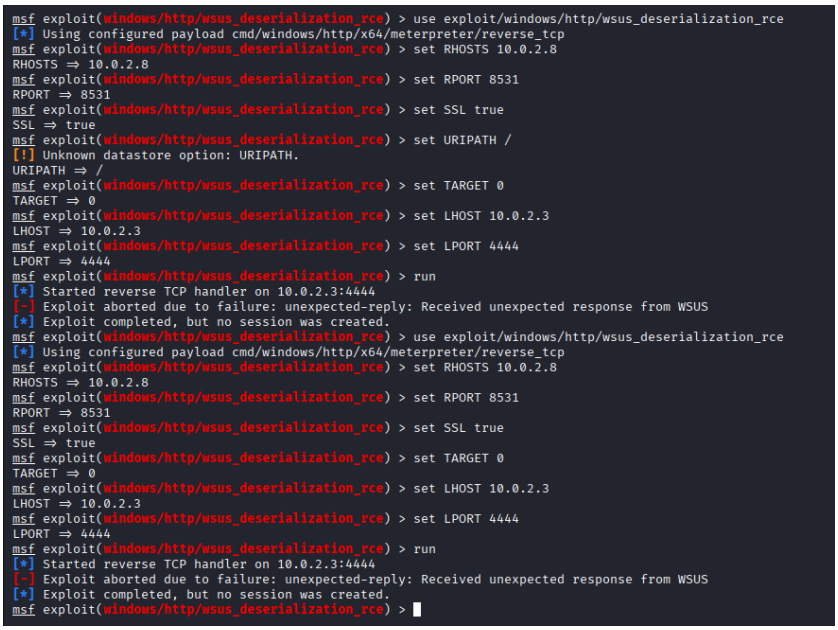
Para intentar validar la vulnerabilidad identificada, se configuraron los parámetros del módulo wsus_deserialization_rce en Metasploit. Se estableció la dirección del host objetivo (RHOSTS = 10.0.2.8), el puerto utilizado por el servicio WSUS (RPORT = 8531) y se habilitó el uso de cifrado (SSL = true) para coincidir con la configuración detectada durante el reconocimiento. También se definió el objetivo por defecto del módulo (TARGET = 0) y se

configuró la dirección del equipo de prueba como origen de la conexión inversa (LHOST = 10.0.2.3) junto con el puerto de escucha correspondiente (LPORT = 4444).

Una vez ejecutado el comando run, como se muestra en la figura 67, el módulo inició correctamente el manejador de conexión inversa, pero el intento de explotación no avanzó debido a que el servidor respondió con un mensaje inesperado para la secuencia requerida por el exploit. Como resultado, Metasploit reportó el mensaje “Received unexpected response from WSUS” y no se generó ninguna sesión. Esto indica que, en este escenario de laboratorio, el comportamiento del servicio no coincide con las condiciones necesarias para que la explotación se materialice.

Figura 67

Prueba de Ethical Hacking Para Validación



Nota. Pruebas de ethical hacking realizadas para validación. Elaboración propia mediante el uso de Metasploit.

En un escenario real, aunque la vulnerabilidad identificada, como CVE-2025-59287, se encuentre en el catálogo KEV de CISA, la prueba realizada mostró que no fue posible explotarla en el activo evaluado. Esto indica que, si bien la vulnerabilidad representa un riesgo reconocido globalmente, su nivel de explotabilidad en este entorno específico es limitado. Por ello, la priorización de mitigación debe enfocarse primero en aquellas vulnerabilidades que sean actualmente explotables y que representen un riesgo más inmediato para los activos críticos. El equipo de CTEM y de gestión de vulnerabilidades evalúa factores como la existencia de exploits públicos, la probabilidad de explotación medida con EPSS y la presencia en KEV, de manera que los recursos de remediación se asignen eficientemente a los riesgos concretos que afectan la operación del negocio, mientras que las vulnerabilidades que aún no son explotables se programan para corrección planificada. Esta estrategia garantiza una protección efectiva de la infraestructura sin descuidar la cobertura integral de seguridad.

Movilización

La movilización constituye la última fase del proceso de CTEM, y su objetivo principal es asegurar que los hallazgos identificados durante las etapas de descubrimiento, priorización y validación sean implementados efectivamente por los equipos responsables. Esta etapa busca reducir obstáculos relacionados con aprobaciones, procesos de implementación o medidas de mitigación, garantizando que la acción sobre vulnerabilidades y riesgos se lleve a cabo de manera organizada y oportuna.

Se pueden emplear plataformas de gestión de seguridad como ServiceNow, que permiten centralizar los hallazgos, documentar flujos de trabajo y coordinar la ejecución entre los distintos equipos de seguridad y de infraestructura.

Priorización y Planificación de Remediación. En esta fase, los equipos de seguridad evalúan nuevamente los activos y vulnerabilidades para determinar qué acciones deben ejecutarse primero. Esto implica:

Revisar la criticidad de los activos según su impacto en el negocio, basándose en la CMDB.

Validar los hallazgos de vulnerabilidades según su EPSS, presencia en el KEV de CISA y existencia de exploits conocidos.

Validar los hallazgos de debilidades en aplicaciones web identificadas durante el escaneo, según su clasificación en las categorías del OWASP Top 10.

Asignar ventanas de remediación para la aplicación de parches o controles compensatorios, asegurando que la ejecución tenga un impacto mínimo en la operación del negocio y respetando los tiempos planificados para mantenimiento.

Definir qué vulnerabilidades pueden corregirse de inmediato y cuáles requieren controles compensatorios temporales, permitiendo priorizar los recursos de manera eficiente.

Asignación de Responsabilidades. Cada vulnerabilidad o hallazgo identificado se asigna a los responsables correspondientes de cada activo, asegurando claridad en la propiedad de la ejecución. Se establecen flujos de trabajo claros entre el equipo de CTEM y el equipo de infraestructura, encargado de aplicar los parches o controles.

Esto incluye:

Documentar el flujo de aprobación para cambios y remediaciones.

Definir los estados de los casos desde su identificación hasta la mitigación.

Coordinar las ventanas de aplicación de parches o controles para minimizar impacto operativo.

Validación de Controles y Mitigacion*es.* En caso de que algunas vulnerabilidades no puedan ser parcheadas inmediatamente, se aplican controles compensatorios, tales como:

Monitoreo de indicadores de compromiso identificados en la fase de inteligencia de amenazas (por ejemplo, hashes de archivos maliciosos o firmas de IPS relacionadas con intentos de explotación).

Segmentación de red o limitación de acceso a los servicios afectados.

Implementación de sistemas de prevención y detección que bloqueen el vector de ataque identificado.

Lo ideal es que los controles se encuentren debidamente documentados en una matriz de riesgos, con el fin de evaluar factores como el riesgo inherente, el riesgo residual, el riesgo aceptado, el riesgo mitigado y el riesgo transferido. Esto permite analizar el nivel de exposición real de la organización y la efectividad de los controles implementados, facilitando una gestión estructurada y trazable del riesgo.

Registro y Seguimiento. Todas las acciones, aprobaciones y remediaciones se registran en la plataforma de gestión, permitiendo:

Documentar la trazabilidad de cada vulnerabilidad desde su descubrimiento hasta su mitigación.

Hacer seguimiento del cumplimiento de las ventanas de aplicación de parches.

Validar que los flujos de comunicación entre CTEM e infraestructura se respeten y funcionen según lo planificado.

Mejora Continua. Al finalizar la movilización, los resultados y métricas obtenidas se retroalimentan en el ciclo de CTEM:

Se revisa la efectividad de los controles aplicados y parches implementados.

Se ajustan criterios de priorización, considerando nuevas amenazas, cambios en la criticidad de los activos o resultados de pruebas de validación.

Se documentan lecciones aprendidas, optimizando los procesos de escaneo, validación y movilización para futuras iteraciones.

Se asegura que el ciclo de detección, evaluación, priorización y remediación evolucione de manera constante, aumentando la resiliencia de la organización frente a nuevas vulnerabilidades.

Indicadores KPI. Con el fin de medir la efectividad del programa de CTEM, se pueden calcular los siguientes indicadores:

Reducción de Vulnerabilidades Priorizadas en el Mes. Este indicador mide qué porcentaje de vulnerabilidades con prioridad 1, 2 y 3 se han remediado en un periodo determinado, permitiendo evaluar la eficacia del programa en la reducción del riesgo.

$$\text{Reducción (\%)} = \frac{Vulnerabilidades\ priorizadas\ remediadas\ en\ el\ mes}{Total\ de\ vulnerabilidades\ priorizadas\ al\ inicio\ del\ mes} * 100$$

Si al inicio del mes había 50 vulnerabilidades priorizadas y se mitigaron 30 durante el mes, el indicador tendría un valor del 60%, se puede definir una meta del 90%, por ejemplo.

MTTR. El Tiempo promedio de remediación (MTTR) mide el tiempo promedio que tarda el equipo en aplicar un parche a una vulnerabilidad desde que se detecta. Permite evaluar la eficiencia operacional del ciclo CTEM.

$$MTTR = \frac{\sum(Fecha\ remediación - Fecha\ detección)}{Número\ de\ vulnerabilidades\ remediadas}$$

Síntesis CTEM

El objetivo de evaluar el ciclo de gestión continua de la exposición a amenazas (CTEM) para clasificar, priorizar y contextualizar la información obtenida se cumplió satisfactoriamente.

A lo largo del trabajo se demostraron todas las etapas del ciclo: Desde la identificación de activos y vulnerabilidades, pasando por la priorización basada en el impacto sobre el negocio y el contexto de amenazas (EPSS, KEV de CISA, existencia de exploits), hasta la validación mediante pruebas controladas y la movilización de planes de remediación. Se evidenció cómo la información recopilada por los analistas de inteligencia de amenazas, combinada con los escaneos y pruebas de CTEM, permite asignar recursos de manera eficiente, reducir riesgos concretos para la operación del negocio y establecer flujos claros de remediación entre equipos de seguridad e infraestructura. Esto confirma que el ciclo CTEM proporciona una metodología sólida para optimizar la gestión de riesgos y amenazas en la organización.

Conclusiones

El estudio comparativo de plataformas de inteligencia de amenazas y análisis de vulnerabilidades permitió identificar soluciones adecuadas para apoyar la gestión continua de la exposición a amenazas. Tras evaluar distintos enfoques técnicos y funcionales, se seleccionaron OpenVAS y Nuclei como herramientas principales para la detección y gestión de vulnerabilidades, debido a su equilibrio entre profundidad técnica, flexibilidad, capacidad de personalización y la no dependencia de licencias comerciales. En el ámbito de la inteligencia de amenazas, se eligieron IBM X-Force Exchange y AlienVault OTX, por su aporte en contextualización, automatización y actualización constante de inteligencia de amenazas. Estas selecciones reflejan una integración coherente entre análisis técnico y conocimiento contextual, permitiendo establecer una base sólida para la correlación entre vulnerabilidades detectadas y amenazas activas. En conjunto, las herramientas elegidas pueden fortalecer el ciclo CTEM al facilitar un proceso continuo de descubrimiento, evaluación y priorización del riesgo, cumpliendo así el primer objetivo propuesto en este proyecto.

En relación con el objetivo 2, el diseño del plan de recolección de inteligencia de amenazas permitió establecer un marco metodológico sólido para estructurar un proceso alineado con las mejores prácticas del ciclo de vida de la inteligencia. Durante la fase de planificación y dirección se identificaron los activos críticos mediante metodologías como MAGERIT, determinando las principales amenazas que pueden afectar la continuidad y disponibilidad de los servicios esenciales de una organización. De igual manera, se definieron los objetivos estratégicos y las fuentes iniciales de inteligencia, tanto internas como externas, y se asignaron roles y responsabilidades a los equipos involucrados, garantizando una coordinación efectiva entre las áreas técnicas y de seguridad.

En la fase de procesamiento, la información obtenida de diversas fuentes, como AlienVault OTX, IBM X-Force Exchange y repositorios públicos como GitHub, fue depurada, normalizada y clasificada, transformando los datos brutos en información estructurada y analizable. Se organizaron IoC, vulnerabilidades y evidencias técnicas según el tipo de amenaza, nivel de criticidad, sistemas afectados y pruebas de explotación. Además, se incorporaron pruebas de concepto y atributos técnicos, como direcciones IP, dominios, URI y hashes de archivo, facilitando su posterior correlación.

Para asegurar la interoperabilidad, los indicadores fueron representados mediante el estándar STIX en formato JSON, utilizando la librería stix2 desarrollada por OASIS Open. Esta implementación permitió generar entidades como indicadores, malware o actores de amenaza, así como establecer relaciones entre ellas, favoreciendo su integración con plataformas de monitoreo y análisis de seguridad como Splunk o Elastic Stack. El uso de atributos temporales permitió gestionar de manera eficiente el ciclo de vida de los indicadores, evitando la utilización de información obsoleta y optimizando los procesos de correlación.

Durante la fase de análisis, la información procesada se examinó para identificar patrones, correlaciones y comportamientos asociados a posibles amenazas activas o emergentes. Se evaluaron los IoC recopilados para determinar su relevancia, nivel de riesgo y relación con campañas o vulnerabilidades específicas, como la CVE-2024-1086. Este análisis permitió contextualizar los hallazgos y generar inteligencia útil para priorizar acciones de mitigación.

En la fase de difusión, los resultados se informaron como ejemplo, que los resultados se compartieron con los equipos responsables de la gestión de activos y vulnerabilidades, apoyando la priorización y validación del programa CTEM. La información se presentó mediante informes de inteligencia y boletines de seguridad que incluían detalles técnicos, evaluación de riesgos,

probabilidad de explotación y recomendaciones de mitigación. Los IoC y las tácticas, técnicas y procedimientos también se integraron para respaldar la detección y respuesta ante posibles intentos de explotación, siguiendo esquemas de clasificación como el TLP para proteger la información sensible.

Finalmente, se explicó que la fase de retroalimentación se centra en recopilar y analizar los comentarios de las partes interesadas sobre la inteligencia de amenazas entregada. Su propósito es evaluar si la información resultó útil, oportuna, precisa y accionable dentro del contexto operativo de la organización. A partir de esta retroalimentación, es posible identificar oportunidades de mejora, ajustar los requerimientos de inteligencia, optimizar los métodos de recolección y análisis, y refinar los formatos de presentación. De esta manera, esta etapa cierra el ciclo de inteligencia y asegura que la producción futura se alinee de manera más efectiva con las necesidades estratégicas, tácticas y operacionales de la organización. En conjunto, el desarrollo de las fases planteadas demuestra que el objetivo se alcanzó al estructurar un plan integral de inteligencia de amenazas que abarca recolección, procesamiento, análisis, difusión y mejora continua de la información crítica para la gestión de riesgos y amenazas.

El objetivo 3 se cumplió mediante la aplicación del ciclo de gestión continua de la exposición a amenazas propuesto por Gartner, el cual permitió clasificar, priorizar y contextualizar la información obtenida durante el análisis de vulnerabilidades y debilidades identificadas en los activos evaluados. A través de este enfoque fue posible relacionar los hallazgos técnicos con la criticidad de los activos definida en la CMDB, así como con métricas de priorización como EPSS, la presencia en el catálogo KEV de CISA y la clasificación de debilidades según el OWASP Top 10.

Este enfoque proactivo y sistemático facilita la detección temprana de ataques, la

priorización efectiva de contramedidas y la mejora continua en la gestión de la ciberseguridad. La incorporación de indicadores de compromiso, tácticas, técnicas y procedimientos, junto con un esquema controlado de difusión bajo protocolos TLP, permite que la información de inteligencia sea compartida de forma segura y responsable entre los equipos involucrados.

El ejercicio desarrollado demuestra que la gestión de vulnerabilidades y de la exposición a amenazas requiere un enfoque continuo y contextualizado. La combinación de inteligencia de amenazas, priorización basada en la criticidad del negocio, validación de controles y seguimiento mediante métricas permite mejorar la capacidad de una organización para identificar, analizar y mitigar riesgos de forma más eficiente. De esta manera, el enfoque CTEM contribuye a fortalecer la resiliencia de la infraestructura tecnológica, optimizar la asignación de recursos de seguridad y apoyar la toma de decisiones estratégicas en la gestión del riesgo.

Recomendaciones

Se recomienda implementar de forma integrada las herramientas seleccionadas (OpenVAS, Nuclei, IBM X-Force Exchange y AlienVault OTX), asegurando su correcta interoperabilidad para fortalecer el proceso de identificación, correlación y priorización de amenazas dentro del ciclo CTEM.

Es necesario establecer un proceso continuo de gestión de vulnerabilidades que permita actualizar periódicamente la información proveniente de fuentes de inteligencia, incluyendo IoC, vulnerabilidades emergentes y cambios en los puntajes EPSS, con el fin de mantener la vigencia del análisis.

Se sugiere formalizar el plan de recolección de inteligencia de amenazas diseñado, garantizando la ejecución de todas las fases del ciclo de vida de la inteligencia como un proceso cíclico y permanente dentro de la organización.

Se recomienda priorizar la remediación de vulnerabilidades en función de la criticidad de los activos, la presencia en KEV y la probabilidad de explotación, con el fin de optimizar la asignación de recursos y reducir el riesgo de incidentes de seguridad.

Es importante implementar mecanismos de automatización en el procesamiento y análisis de la información, utilizando estándares como STIX y plataformas SIEM, que permitan mejorar la eficiencia en la correlación de eventos y la detección de amenazas.

Se sugiere fortalecer los procesos de difusión de inteligencia mediante el uso de esquemas como TLP, asegurando que la información sea compartida de manera controlada entre los equipos responsables.

Se recomienda establecer un proceso de retroalimentación continua que permita evaluar la utilidad de la inteligencia generada, identificando oportunidades de mejora en las fuentes,

herramientas y metodologías utilizadas.

Referencias

Abrams, L. (2022, November 30). Keralty ransomware attack impacts Colombia's health care system. BleepingComputer. https://www.bleepingcomputer.com/news/security/keralty-ransomware-attack-impacts-colombias-health-care-system/

ANSSI. (2018). La méthode EBIOS Risk Manager – Le guide. https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide

Arikan, S. M., Koçak, A., & Alkan, M. (2024). Atomic lifecycle for cyber threat intelligence. In Proceedings of the 2024 17th International Conference on Information Security and Cryptology (ISCTürkiye) (pp. 1–6). IEEE. https://doi.org/10.1109/ISCTrkiye64784.2024.10779304

AXELOS. (s.f.). ITIL 4 framework. https://www.axelos.com/certifications/itil-service-management/what-is-itil

Bonderud, D. (2025, August 8). Cost of a data breach 2024: Financial industry. IBM. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

Center for Internet Security. (2022). Words of estimative probability, analytic confidences, and structured analytic techniques. https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques

CISA. (s.f.). Traffic light protocol (TLP) definitions and usage. https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Cisco Talos Intelligence Group. (n. d.). Comprehensive threat intelligence. Talos Intelligence. Retrieved October 19, 2025, from https://talosintelligence.com/

Cisco. (s.f.). What is threat modeling? https://www.cisco.com/c/en/us/products/security/what-is-threat-modeling.html

Cloudflare. (s.f.). What is threat modeling? https://www.cloudflare.com/es-la/learning/security/glossary/what-is-threat-modeling/

Colombian Congress. (2009). Law 1273 of 2009 – Protection of information and data [Ley 1273 de 2009 – Gestor Normativo]. Gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Colombian Congress. (2012). Law 1581 of 2012 – Data Protection Law [Ley 1581 de 2012 – Gestor Normativo]. Gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Darktrace. (2025, June 25). Patch and persist: Darktrace's detection of Blind Eagle (APT-C-36). https://www.darktrace.com/blog/patch-and-persist-darktraces-detection-of-blind-eagle-apt-c-36

Departamento Nacional de Planeación. (s.f.). Documento CONPES 3995: Política nacional de seguridad digital. https://colaboracios.fnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Dorado, D. (2025, September 1). Colombia enfrenta más de 2.700 ciberataques semanales. Latinpyme. https://latinpyme.com/colombia-enfrenta-mas-de-2-700-ciberataques-semanales/

EC-Council. (s.f.). What is cyber threat intelligence. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/what-is-cyber-threat-intelligence/

Edie, K., McKee, C., & Duby, A. (2023). Extending Threat Playbooks for Cyber Threat Intelligence: A Novel Approach for APT Attribution. ISDFS 2023 - 11th International Symposium on Digital Forensics and Security. https://doi.org/10.1109/ISDFS58141.2023.10131867

European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

FIRST. (s.f.). Exploit Prediction Scoring System (EPSS). Retrieved December 7, 2025, from https://www.first.org/epss/api

Fortinet. (s.f.). Top cybersecurity statistics: Facts, stats and breaches for 2025. https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Foulger, E. (2025, October 29). Darktrace's analysis of post-exploitation activities on CVE-2025-59287. Darktrace. https://www.darktrace.com/blog/wsus-exploited-darktraces-analysis-of-post-exploitation-activities-related-to-cve-2025-59287

Gartner. (2024). What is CTEM (Continuous Threat Exposure Management)? https://www.gartner.com/en/articles/what-is-ctem

Gartner. (2025). Vulnerability assessment reviews and ratings. Gartner Peer Insights. https://www.gartner.com/reviews/market/vulnerability-assessment

Haass, J. C. (2022). Cyber Threat Intelligence and Machine Learning. Proceedings - 2022 4th International Conference on Transdisciplinary AI, TransAI 2022, 156–159. https://doi.org/10.1109/TRANSAI54797.2022.00033

IBM. (2024). X-Force threat intelligence index 2024. https://www.ibm.com/reports/threat-intelligence

IBM. (s.f.). IBM X-Force Exchange. IBM Cloud. https://exchange.xforce.ibmcloud.com/

IBM. (s.f.). Vulnerability report: CVE-2024-1086. IBM Cloud. Retrieved November 5, 2025, from https://exchange.xforce.ibmcloud.com/osint/guid:08142128630a44509aff354de467d3d7

International Data Corporation (IDC). (2025). Worldwide security spending to increase by 12.2% in 2025 as global cyberthreats rise. https://my.idc.com/getdoc.jsp?containerId=prEUR253264525

Invicti Security. (2024). Introduction to Acunetix. https://www.acunetix.com/support/docs/introduction/

ISACA. (s.f.). COBIT: Control objectives for information and related technologies. https://www.isaca.org/resources/cobit

ISO/IEC. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection Information security management systems Requirements. International Organization for Standardization. https://www.iso.org/standard/27001

ISO/IEC. (2022). ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection Information security controls. International Organization for Standardization. https://www.iso.org/standard/75652.html

ISO/IEC. (2023). ISO/IEC 27032:2023- Cybersecurity Guidelines for Internet security. International Organization for Standardization. https://www.iso.org/standard/76070.html

Junco, D. (2025, September 15). La otra pandemia: El crecimiento de los ciberataques en Colombia y cómo hacerles frente [The other pandemic: The growth of cyberattacks in Colombia and how to confront them]. Universidad Católica de Colombia. https://www.ucatolica.edu.co/portal/la-otra-pandemia-el-crecimiento-de-los-ciberataques-en-colombia-y-como-hacerles-frente/

Kosinski, M. (2025, diciembre 8). What is ransomware? IBM. https://www.ibm.com/think/topics/ransomware

LevelBlue. (s.f.). Open Threat Exchange (OTX). https://otx.alienvault.com/

Lindemulder, G., & Forrest, A. (2025). What is OSINT (open-source intelligence)? IBM. https://www.ibm.com/think/topics/osint

Microsoft. (2024). El aumento de las amenazas cibernéticas exige una defensa y cooperación globales más sólidas. https://news.microsoft.com/es-xl/el-aumento-de-las-amenazas-ciberneticas-exige-una-defensa-y-cooperacion-globales-mas-solidas/

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método. Consejo Superior de Administración Electrónica. https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

MISP. (s.f.). MISP documentation and support. MISP Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing. https://www.misp-project.org/documentation/

MITRE. (2025). MITRE ATT&CK®. https://www.mitre.org/news-insights/publication/mitre-attack

N. Naik, P. Grace, P. Jenkins, & S. Prajapat (Eds.). (2024). A comparative analysis of threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. Springer. https://doi.org/10.1007/978-3-031-74443-3_16

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

OASIS. (s.f.). Introduction to STIX. GitHub. https://oasis-open.github.io/cti-documentation/stix/intro.html

OpenVAS. (s.f.). Open Vulnerability Assessment Scanner. https://www.openvas.org/

Pal, S., Jadidi, Z., Alaeifar, P., & Foo, E. (2023). The Role of Artificial Intelligence and Blockchain for Future Cyber Threat Intelligence. Proceedings of the International Conference on Sensing Technology, ICST. https://doi.org/10.1109/ICST59744.2023.10460772

Palo Alto Networks. (s.f.). What is the threat intelligence lifecycle? https://www.paloaltonetworks.com/cyberpedia/what-is-the-threat-intelligence-life-cycle

Picus Security. (2025). What is pyramid of pain? https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain

ProjectDiscovery. (2025). Authenticated scans. ProjectDiscovery Documentation. https://docs.projectdiscovery.io/opensource/nuclei/authenticated-scans

ProjectDiscovery. (2025). Nuclei - Fast and Customizable Vulnerability Scanner. https://nuclei.projectdiscovery.io

Qualys Inc. (2025). Vulnerability Management, Detection, and Response (VMDR): Unified solution for continuous risk reduction. https://www.qualys.com

Qualys Inc. (s.f.). Qualys.com. https://success.qualys.com/support/s/article/000003222

Roobini, M. S., Chowdary, M. B., Srinivas, Y., Jayanthi, S., & Srividhya, E. (2024). Cloud based threat intelligence sharing for collective defence. En Proceedings of the 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging Technologies in Digital Transformation (ICONSTEM 2024). https://doi.org/10.1109/ICONSTEM60960.2024.10568663

Saddi, V. R., Gopal, S. K., Mohammed, A. S., Dhanasekaran, S., & Naruka, M. S. (2024). Examine the Role of Generative AI in Enhancing Threat Intelligence and Cyber Security

Measures. 2024 2nd International Conference on Disruptive Technologies, ICDT 2024, 537–542. https://doi.org/10.1109/ICDT61202.2024.10489766

Sakib, S. M. (2022, abril 19). Cyber threat intelligence. https://orcid.org/0000-0001-9310-3014

SANS Institute. (s.f.). Threat intelligence: Planning and direction. https://www.sans.edu/cyber-research/36857/

SentinelOne. (2022, November 30). RansomHouse: In-Depth analysis, detection, and mitigation. https://www.sentinelone.com/anthology/ransomhouse/

Simran, Kumar, S., & Hans, A. (2024). The AI Shield and Red AI Framework: Machine Learning Solutions for Cyber Threat Intelligence(CTI). 2024 International Conference on Intelligent Systems for Cybersecurity, ISCS 2024. https://doi.org/10.1109/ISCS61804.2024.10581195

Splunk. (s.f.). Cyber kill chains: Strategies & tactics. https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

Spyros, A., Koritsas, I., Papoutsis, A., Panagiotou, P., Chatzakou, D., Kavallieros, D., … Kompatsiaris, I. (2025). AI-based holistic framework for cyber threat intelligence management. IEEE Access, 13, 20820–20846. https://doi.org/10.1109/ACCESS.2025.3533084

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

TechTarget. (2025). What is an advanced persistent threat (APT)? https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT

Volz, D., & McMillan, R. (2025, September 19). Chinese and Iranian hackers are using U.S. AI products to bolster cyberattacks. The Wall Street Journal. https://www.wsj.com/tech/ai/chinese-and-iranian-hackers-are-using-u-s-ai-products-to-bolster-cyberattacks-ff3c5884

Wang, H., Iacovazzi, A., Kim, S., & Raza, S. (2024). CLEVER: Crafting intelligent MISP for cyber threat intelligence. En Proceedings of the 49th IEEE Conference on Local Computer Networks (LCN), 1–9. https://doi.org/10.1109/LCN60385.2024.10639749

Yasmeen, A., Ullah, K. K., & Muhammad, A. (2023). HDA-TIP: A framework for heterogeneous data aggregation for threat intelligence platform. En Proceedings of the 17th International Conference on Ubiquitous Information Management and Communication (IMCOM 2023).

ZeroFox. (s.f.). Dark web threat intelligence. https://www.zerofox.com/glossary/dark-web-threat-intelligence/

Apéndices

Apéndices A

Resultados Completos del Escaneo de Nuclei

Link de acceso: Anexos grado.

Apéndices B

Resultados Completos del Escaneo de OpenVas

Link de acceso: Anexos grado.

Apéndices C

CMDB

Link de acceso: Anexos grado.

Apéndices D

Ejemplo de Conversión de Datos a STIX

Link de acceso: Anexos grado.

Apéndices E

Glosario

Acunetix

Herramienta especializada en el análisis automatizado de vulnerabilidades en aplicaciones web, diseñada para identificar fallas de seguridad como inyección SQL, cross-site scripting y configuraciones inseguras.

Alien Vault OTX (Open Threat Exchange)

Plataforma colaborativa de inteligencia de amenazas que permite compartir y consultar indicadores de compromiso relacionados con actividades maliciosas observadas en diferentes organizaciones.

Advanced Persistent Threat (APT)

Tipo de amenaza avanzada caracterizada por ataques dirigidos, persistentes y cuidadosamente planificados, generalmente realizados por grupos organizados con amplios recursos y objetivos específicos.

Ataque de Día Cero (Zero-day)

Vulnerabilidad desconocida para el fabricante del software y para la cual aún no existe un parche de seguridad disponible, lo que representa un riesgo elevado cuando es explotada por atacantes.

Black Hat

Individuo que realiza actividades de hacking con fines maliciosos o ilegales, buscando explotar vulnerabilidades para obtener beneficios económicos, causar daño o acceder a información sensible.

Blue Team

Equipo de seguridad responsable de proteger la infraestructura tecnológica de una organización mediante la detección, análisis y respuesta a incidentes de seguridad.

Caja Blanca (White Box Testing)

Metodología de ruebas de seguridad en la que el evaluador dispone de información completa sobre el sistema objetivo, como arquitectura, código fuente o credenciales.

Caja Gris (Gray Box Testing)

Enfoque de pruebas de penetración en el que el analista cuenta con información parcial del sistema evaluado, lo que permite simular escenarios más realistas de ataque.

Caja Negra (Black Box Testing)

Metodología de evaluación de seguridad en la que el evaluador no dispone de información previa sobre el sistema objetivo, simulando la perspectiva de un atacante externo.

Campaña de Amenazas

Conjunto de actividades maliciosas relacionadas entre sí, ejecutadas por un mismo actor o grupo de ataque con el objetivo de comprometer sistemas o recolectar información durante un periodo determinado.

Cisco Talos Intelligence

Equipo de investigación en ciberseguridad que analiza amenazas globales y publica información sobre malware, vulnerabilidades y campañas de ataque para apoyar la defensa de infraestructuras digitales.

Continuous Threat Exposure Management (CTEM)

Enfoque estratégico orientado a identificar, evaluar y priorizar de manera continua las exposiciones de seguridad dentro de una organización, con el fin de reducir el riesgo asociado a vulnerabilidades explotables.

Common Vulnerabilities and Exposures (CVE)

Identificador estándar utilizado para catalogar públicamente vulnerabilidades de seguridad conocidas en software y hardware, permitiendo su referencia y seguimiento de forma unificada.

Common Vulnerability Scoring System (CVSS)

Sistema de puntuación utilizado para evaluar la gravedad de una vulnerabilidad de seguridad considerando factores como el impacto potencial y la facilidad de explotación.

Common Weakness Enumeration (CWE)

Catálogo que clasifica debilidades comunes en el desarrollo de software que pueden derivar en vulnerabilidades de seguridad.

Cyber Kill Chain

Modelo que describe las diferentes etapas que sigue un ataque cibernético, desde la fase de reconocimiento hasta la ejecución final del compromiso del sistema.

Cyber Threat Intelligence

Proceso de recopilación, análisis e interpretación de información relacionada con amenazas cibernéticas con el propósito de anticipar ataques y mejorar la capacidad de defensa de una organización.

Diamond Model of Intrusion Analysis

Modelo analítico utilizado en inteligencia de amenazas que relaciona cuatro elementos principales de un ataque: Adversario, infraestructura, capacidad y víctima.

Dominio Malicioso

Nombre de dominio utilizado por atacantes para alojar malware, distribuir campañas de phishing o establecer comunicación con sistemas comprometidos.

Ethical Hacking

Práctica autorizada que consiste en evaluar la seguridad de sistemas informáticos utilizando técnicas similares a las de los atacantes con el objetivo de identificar vulnerabilidades y fortalecer los mecanismos de defensa.

EPSS (Exploit Prediction Scoring System)

Sistema que estima la probabilidad de que una vulnerabilidad específica sea explotada en el futuro cercano. Se basa en análisis de datos históricos y factores técnicos, ayudando a las organizaciones a priorizar parches y estrategias de mitigación de manera más eficiente.

Exploit

Código o técnica utilizada para aprovechar una vulnerabilidad en un sistema o aplicación con el objetivo de ejecutar acciones no autorizadas.

Explotación de Vulnerabilidades

Proceso mediante el cual se intenta aprovechar una debilidad identificada para comprobar su impacto real en un sistema o aplicación.

Firma de Malware

Patrón identificable dentro del código o comportamiento de un programa malicioso que permite a las herramientas de seguridad detectar su presencia.

Gartner

Empresa de investigación y consultoría tecnológica que desarrolla análisis, marcos conceptuales y tendencias relacionadas con la gestión de tecnologías de la información y la seguridad informática.

Gray Hat

Persona que puede explotar vulnerabilidades sin autorización previa, aunque generalmente sin intención directa de causar daño o beneficio económico.

Hash Criptográfico

Valor alfanumérico generado mediante una función matemática que transforma datos de cualquier tamaño en una cadena de longitud fija, utilizada frecuentemente para verificar la integridad de archivos.

IBM X-Force Exchange

Plataforma de inteligencia de amenazas que proporciona información sobre vulnerabilidades, malware e indicadores de compromiso recopilados a partir de investigaciones globales.

Indicador de Ataque (IOA)

Evidencia basada en patrones de comportamiento que permite detectar la ejecución de actividades maliciosas durante el desarrollo de un ataque.

Indicador de Compromiso (IOC)

Evidencia técnica observable que indica que un sistema o red ha sido comprometido o ha sido objeto de una actividad maliciosa.

Indicador de Riesgo (IOR)

Condición o situación que aumenta la probabilidad de que una organización sea vulnerable a un ataque, como configuraciones inseguras o sistemas sin actualizaciones.

IOC Basado en Dominio

Dominio utilizado para realizar ataques de phishing o para mantener comunicación con sistemas comprometidos.

IOC Basado en Hash

Identificador único de un archivo utilizado para detectar muestras de malware conocidas.

IOC Basado en IP

Dirección IP asociada a actividades maliciosas como servidores de comando y control o distribución de malware.

IOC Basado en URL

Dirección web utilizada para distribuir contenido malicioso o redirigir a víctimas hacia sitios fraudulentos.

KEV (Known Exploited Vulnerabilities)

Lista pública de vulnerabilidades que se sabe están siendo activamente explotadas en entornos reales. Esta información permite a las organizaciones priorizar la mitigación de riesgos y aplicar parches de manera más efectiva para proteger sus sistemas.

Malware

Software malicioso diseñado para infiltrarse, dañar o tomar control de sistemas informáticos sin el consentimiento del usuario.

MITRE ATT&CK

Marco de conocimiento que documenta tácticas y técnicas utilizadas por atacantes en entornos reales y que se utiliza ampliamente para el análisis y la defensa frente a amenazas cibernéticas.

MISP (Malware Information Sharing Platform)

Plataforma de código abierto diseñada para compartir, almacenar y correlacionar información sobre amenazas entre organizaciones.

Modelado de Amenazas

Proceso de identificación y análisis de posibles amenazas que podrían afectar un sistema, con el fin de diseñar controles de seguridad adecuados.

Nuclei

Herramienta automatizada utilizada para la detección rápida de vulnerabilidades mediante plantillas que identifican configuraciones inseguras en aplicaciones y servicios.

OpenVAS

Escáner de vulnerabilidades de código abierto utilizado para identificar fallas de seguridad en sistemas, redes y aplicaciones.

OSINT (Open Source Intelligence)

Técnica de recopilación de información a partir de fuentes públicas y abiertas, utilizada para análisis de seguridad, investigación y generación de inteligencia.

OWASP (Open Web Application Security Project)

Proyecto comunitario que desarrolla guías, herramientas y estándares para mejorar la seguridad de aplicaciones web. Su recurso más conocido, el *OWASP Top Ten*, identifica las principales vulnerabilidades web críticas y ofrece recomendaciones para prevenirlas.

Pentesting (Pruebas de Penetración)

Proceso controlado de simulación de ataques contra un sistema informático con el fin de descubrir vulnerabilidades que podrían ser explotadas por atacantes reales.

Phishing

Técnica de ingeniería social que busca engañar a las víctimas para que revelen información sensible, como contraseñas o datos financieros.

Pirámide del Dolor

Modelo conceptual que clasifica los diferentes tipos de indicadores de amenazas según el nivel de dificultad que representan para los atacantes al ser detectados o bloqueados.

Proof of Concept (POC)

Demostración práctica que valida que una vulnerabilidad puede ser explotada en condiciones reales.

Purple Team

Enfoque colaborativo que integra las actividades de los equipos Red Team y Blue Team con el objetivo de mejorar la capacidad de detección y respuesta de una organización.

Red Team

Equipo de seguridad encargado de simular ataques reales contra una organización con el objetivo de evaluar la efectividad de sus controles de seguridad.

STIX (Structured Threat Information eXpression)

Lenguaje estandarizado utilizado para representar y compartir información estructurada sobre amenazas cibernéticas.

Superficie de Ataque

Conjunto de todos los puntos potenciales que un atacante podría utilizar para interactuar con un sistema o red.

TAXII (Trusted Automated Exchange of Intelligence Information)

Protocolo diseñado para facilitar el intercambio automatizado de información de inteligencia de amenazas entre diferentes sistemas.

Threat Actor

Individuo, grupo u organización responsable de realizar actividades maliciosas contra sistemas informáticos.

Threat Feed

Flujo continuo de datos que contiene información actualizada sobre amenazas, indicadores de compromiso y vulnerabilidades emergentes.

Threat Hunting

Actividad proactiva de búsqueda de amenazas dentro de una red o sistema con el objetivo de identificar ataques que no han sido detectados por mecanismos automáticos.

Threat Landscape

Panorama general de amenazas que describe los riesgos y tendencias actuales que afectan a un entorno tecnológico determinado.

TLP (Traffic Light Protocol)

Protocolo utilizado para clasificar y controlar la difusión de información sensible dentro de comunidades de seguridad.

TTP (Tácticas, Técnicas y Procedimientos)

Conjunto de métodos y estrategias utilizados por los atacantes para ejecutar y mantener operaciones maliciosas.

URL Maliciosa

Dirección web creada para distribuir malware o redirigir a usuarios hacia páginas fraudulentas.

Vulnerabilidad

Debilidad en un sistema, aplicación o infraestructura que puede ser explotada por un atacante para comprometer su seguridad.

White Hat

Hacker ético que realiza actividades de seguridad de forma legal y autorizada con el objetivo de mejorar la protección de sistemas informáticos.