Protección integral al tráfico de datos en el data center Bancolombia ubicado en Niquía, Bello, Antioquia, habilitando un modelo de confianza cero por medio de la plataforma cisco Tetration

Daniel Alberto Cáceres Saavedra

Asesor

Freddy Mayo Rentería

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2023

Resumen

Este proyecto de grado aplicado tiene como objetivo implementar un modelo de confianza cero en el Data Center de Bancolombia utilizando la plataforma Cisco Tetration. Se busca mejorar la seguridad y protección de los datos de los clientes, así como fortalecer la infraestructura del centro de datos. Para lograrlo, se implementarán servidores y conmutadores de plataforma Cisco Nexus 9300, se instalará el software Cisco Tetration en una máquina virtual y se desplegará el Agente Tetration en servidores bancarios. Se verificará el correcto funcionamiento de la plataforma a través del servidor de Tetration y se realizarán mejoras a corto y mediano plazo, incluyendo la detección de vulnerabilidades de software y la inspección del proceso del servidor. Se establecerá un plan de mantenimiento preventivo y correctivo para garantizar el funcionamiento óptimo del sistema. Con la implementación exitosa de estas medidas de seguridad, Bancolombia podrá ofrecer servicios financieros de manera confiable, fortaleciendo la confianza de sus clientes y protegiendo sus datos confidenciales.

***Palabras clave**:* confianza cero, cisco Tetration, data center, protección integral, flujo de red, big data.

Abstract

This applied degree project aims to implement a zero trust model in the Bancolombia Data Center using the Cisco Tetration platform. It seeks to improve the security and protection of customer data, as well as strengthen the infrastructure of the data center. To achieve this, Cisco Nexus 9300 platform servers and switches will be implemented, Cisco Tetration software will be installed in a virtual machine and the Tetration Agent will be deployed in bank servers. The correct operation of the platform will be verified through the Tetration server and improvements will be made in the short and medium term, including detection of software vulnerabilities and inspection of the server process. A preventive and corrective maintenance plan will be established to ensure optimal system operation. With the successful implementation of these security measures, Bancolombia will be able to offer financial services in a reliable manner, strengthening the trust of its customers and protecting their confidential data.

Keywords: zero trust, cisco Tetration, data center, end-to-end protection, network flow, big data.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

El trabajo que se presenta tiene como tema la protección integral al tráfico de datos en el Data Center Bancolombia ubicado en Niquía, Bello, Antioquia, habilitando un modelo de confianza cero por medio de la plataforma Cisco Tetration. La razón detrás de este trabajo es la necesidad de proteger la información sensible que se maneja en el centro de datos, garantizando la seguridad y privacidad de los datos de los clientes. Para lograr esto, se ha implementado un modelo de confianza cero que establece que ningún usuario o dispositivo es confiable por defecto, y se requiere una autenticación y autorización rigurosa para permitir el acceso a los recursos del sistema. La plataforma Cisco Tetration permite una protección integral al tráfico de datos, lo que garantiza la seguridad de los datos y reduce el riesgo de amenazas cibernéticas. Este trabajo es importante porque el aumento de las amenazas cibernéticas y la importancia de la protección de datos hacen que la seguridad de la información sea una prioridad para las empresas y organizaciones en todo el mundo.

El trabajo ha sido planificado de manera detallada y rigurosa, en primer lugar, se llevará a cabo una revisión exhaustiva de la literatura existente en el tema de la seguridad informática y la protección de datos. A partir de esta revisión se definirán los conceptos clave que se tendrán en cuenta durante la investigación, lo que permitirá establecer una base teórica sólida para el trabajo.

En segundo lugar, se realizará una ficha de caracterización inicial que permitirá conocer en detalle las condiciones y requerimientos específicos del Data Center Bancolombia ubicado en Niquia, Bello, Antioquia.

Posteriormente, se identificarán las líneas y grupos de exploración de la cadena Electrónica, Telecomunicaciones y Redes (ETR) que se relacionan con los intereses en la

ingeniería e investigación, lo que permitirá definir con mayor precisión la idea para la investigación.

Una vez definida la idea para la investigación, se procederá a describir, analizar y definir el problema en cuestión, teniendo en cuenta aspectos como el ¿Dónde?, ¿Cuándo? y ¿Por qué? de la problemática.

Después, se establecerá un marco teórico que se cimentará en cinco concepciones claves sobre los temas involucrados en la problemática reconocida, y se analizarán los artículos más relevantes que servirán como guía para la implementación del proyecto.

Por último, se establecerá un cronograma de actividades que permitirá dar solución a los objetivos planteados, garantizando la calidad y eficacia del trabajo.

No obstante, del enfoque riguroso y detallado que se empleará en el trabajo es importante tener en cuenta que existen ciertas limitaciones en la investigación.

En particular, la implementación de un modelo de confianza cero puede presentar algunos desafíos técnicos y logísticos que podrían afectar la eficacia del sistema. Además, la aplicación específica de esta solución a las necesidades y requerimientos del Data Center Bancolombia puede requerir adaptaciones y ajustes adicionales que no hayan sido considerados inicialmente.

Por lo tanto, es importante reconocer estas limitaciones y estar abiertos a la posibilidad de enfrentar obstáculos y desafíos a lo largo del proceso de investigación y la implementación de la solución propuesta.

La protección de los datos y la seguridad informática son temas de gran importancia en el mundo actual, especialmente en el sector financiero. Por esta razón, el interés para hacer el trabajo de investigación sobre la protección integral al tráfico de datos en el Data Center de

Bancolombia surge de la necesidad de implementar soluciones efectivas y avanzadas para garantizar la seguridad de la información de los clientes del banco.

Este trabajo de investigación busca explorar y analizar las características de un modelo de confianza cero y cómo puede ser aplicado en el contexto específico del Data Center Bancolombia para mejorar la seguridad de la información. Encontrando soluciones innovadoras y efectivas para la protección de los datos, y proporcionar una metodología rigurosa para su implementación. Con esto, se espera contribuir a la protección de los datos financieros de los clientes del banco, así como a la confianza en la seguridad y la eficacia de los servicios que el banco ofrece.

La metodología utilizada involucró la identificación de las necesidades y vulnerabilidades en el manejo de datos en el Data Center Bancolombia, seguida del diseño de un modelo de seguridad basado en el concepto de confianza cero. Para lograr esto, se utilizó la plataforma Cisco Tetration, la cual permitió una protección integral al tráfico de datos. Además, se realizó un análisis exhaustivo de la literatura existente en el campo de la seguridad informática y la protección de datos para asegurar la validez y eficacia del modelo propuesto. La metodología empleada fue esencial para garantizar la calidad y la rigurosidad del trabajo de investigación

La metodología empleada en la implementación de la protección integral al tráfico de datos en el Data Center se basó en la habilitación de un modelo de confianza cero mediante la plataforma Cisco Tetration y el Marco conceptual. Cisco Tetration es una solución de protección integral para la carga de trabajo de Data Centers que permite identificar eventos de seguridad más rápidamente, frenar el movimiento lateral y reducir el plano de ataque, mientras que la seguridad de confianza cero se centra en eliminar la confianza de la arquitectura de red de una organización, estableciendo la familiaridad en cada solicitud de acceso. Además, se utilizaron

técnicas de monitoreo de flujo de red y Big Data para capturar, estudiar, gestionar y procesar los macrodatos que se generan en un Data Center. La implementación se basó en las últimas actualizaciones y capacidades de la plataforma Cisco Tetration, según lo reportado por diferentes publicaciones, y se enfocó en la defensa en profundidad para Tetration, que permitió a la organización impulsar una política a un servidor de aplicaciones, al perímetro de la red y a los controladores de Redes Definidas por Software o en ingle Software-Defined Networking (SDN), aplicando la carga de trabajo de forma nativa a través de agentes en contenedores y máquinas virtuales sin sistema operativo.

El propósito principal de este trabajo de investigación es adquirir nuevos conocimientos en relación con la búsqueda de soluciones a problemáticas específicas en este caso su objetivo es el estudio detallado de las medidas de seguridad necesarias para proteger la información en un Data Center de una entidad financiera.

Este trabajo se enfoca en implementar un modelo de seguridad en el Data Center utilizando la plataforma Cisco Tetration para monitorear y controlar el tráfico, de esta manera se busca no solo proteger los datos de la entidad financiera, sino también cumplir con las normativas y regulaciones establecidas en el sector financiero para garantizar la seguridad de la información.

Definiciones (Conceptos Clave)

Modelo de "Confianza Cero": Es un enfoque de seguridad informática que se basa en no confiar en ninguna entidad, usuario o dispositivo dentro o fuera de una red, y requiere una autenticación y verificación constantes antes de permitir el acceso a recursos. (Zero Trust Architecture: An AWS Perspective, 2022)

Plataforma Cisco Tetration: Es una solución de seguridad para centros de datos que proporciona una visibilidad completa de todo el tráfico de datos que fluye a través de la red, incluyendo el tráfico cifrado. También ofrece controles de seguridad avanzados para proteger las aplicaciones y los datos, y detectar y mitigar amenazas. (Cisco Tetration Analytics: A Platform for Comprehensive Data Center Security, 2017)

Data Center: Es un centro de datos que alberga los servidores y el almacenamiento de una organización, y proporciona servicios de procesamiento, almacenamiento y gestión de datos. (Data center, 2022)

Protección integral: Es un enfoque de seguridad que busca proteger los sistemas y datos de una organización de todas las amenazas posibles, incluyendo amenazas internas y externas. Esto implica la implementación de medidas de seguridad físicas y lógicas, la gestión de riesgos y la formación de los empleados en cuestiones de seguridad. (Protección integral de la información, 2021)

Normativas y regulaciones: Son las leyes, normas y directrices que rigen el comportamiento de las organizaciones en un sector determinado, y que pueden establecer requisitos específicos en materia de seguridad de la información. Algunas de las normativas y regulaciones aplicables en el sector financiero colombiano incluyen la Ley 1266 de 2008, la Ley 1581 de 2012 y la Circular Externa 052 de 2008 de la Superintendencia Financiera de Colombia. (Normatividad en seguridad de la información en Colombia, 2022)

Caracterización Inicial

Tabla 1

Ficha de caracterización inicial

Información solicitada	Respuesta
Nombres y Apellidos completos	Daniel Alberto Cáceres Saavedra
Programa	Ingeniería de Telecomunicaciones
Créditos aprobados	158
Intereses en ingeniería, e investigación	Sistemas avanzados de transmisión, administración de direccionamiento IP.
Experiencia en investigación (si/no) ¿cuál?:	Si, Redes avanzadas de acceso como HFC, DSL, GPON; Diseño en las redes de transmisión inalámbricas (5G NR y 4G LTE
Fortalezas en áreas de ingeniería:	Networking Cisco, IPAM, LAN, WLAN
Debilidades en áreas de ingeniería:	Microprocesadores.

Fuente. Cáceres Saavedra, D. A. (2023). *Ficha de caracterización* inicial [Fuente propia].

Relación de Intereses Investigativos

Tabla 2

Relación de interese investigativos, líneas y grupos de investigación

Intereses en ingeniería e investigación	Línea de investigación y áreas temáticas	Grupo de investigación
Gestión de direcciones de protocolo de internet o Internet Protocol Address Management (IP), Tetration aplicado en centro de datos.	Infraestructura tecnológica y seguridad en redes	Gestión de redes de telecomunicaciones

Fuente. Cáceres Saavedra, D. A. (2023). *Relación de interese investigativos, líneas y grupos de investigación.* [Fuente propia].

Idea Para la Investigación Aplicada

Protección integral para la carga de trabajo de Data Center Bancolombia ubicado en Niquia habilitando un modelo de "confianza cero" por medio de la plataforma Cisco Tetration.

El proyecto hace referencia a la implementación, configuración, administración y mantenimiento de servidores Cisco Tetration Analytics para red de Bancolombia S.A. en su Datacenter ubicado en Niquia, la cual es una plataforma diseñada que los ayudará a poseer una claridad compleja de todo el data center en tiempo real, teniendo toda la capacidad de analizar cientos de miles de datos por segundo, incorporando una composición de sensores de telemetría de software y hardware, posteriormente analiza la información, utilizando una mezcla de tecnologías modernas de big-data y machine Learning o aprendizaje automático basado en algoritmos, la cual entrega una información crítica para los especialistas de centro de datos,

como lo son: la observación de aplicaciones, Cisco Tetration Analytics, Análisis forense de flujo de red, Compliance Management, recomendaciones automáticas de políticas de listas blancas; Ganando una visibilidad más a fondo del Centro de Datos, automatizando el análisis de acciones, a través de la infraestructura de la compañía.

Descripción del Problema

Desde el área de TI en el Datacenter de Bancolombia S.A., no tengo claridad sobre los flujos de información, velocidad de transmisión y paquetes en tiempo real. No poseo un software o hardware que analice estos datos mediante analítica avanzada de Big Data, lo que limita la capacidad para realizar análisis más profundos sobre las aplicaciones y la automatización. Además, no dispongo de una herramienta que recopile la telemetría que atraviesa todo el Datacenter y que examine volúmenes altos de datos en tiempo real. Este es un problema importante que debo solucionar para mejorar la eficiencia y seguridad.

Como profesional en el área de ciberseguridad, veo cómo el apogeo del teletrabajo y trabajo en la nube ha transformado la forma de trabajar, enfrento la falta de claridad en cuanto al funcionamiento del Datacenter y la operación de las aplicaciones. Trabajando codo a codo con los especialistas e ingenieros de TI, me dedique a encontrar soluciones que permitan tener una mejor visibilidad y control sobre los flujos de información, la velocidad de transmisión y el análisis de datos en tiempo real. El acceso a los archivos desde la comodidad del hogar involucra cambios importantes en cuanto a la seguridad de los datos. Las organizaciones han tenido que adaptarse a este nuevo contexto, y en colaboración con los proveedores de ciberseguridad, se ha lanzado el concepto de confianza cero para hacer frente a los nuevos desafíos de seguridad. Sin embargo, este enfoque ha planteado un problema importante: no sé con certeza qué es lo que realmente está almacenado en la red, lo que aumenta el riesgo de violaciones de seguridad y brechas de datos.

El problema se presenta cuando una empresa no cuenta con una arquitectura de red de confianza cero, que está compuesta por una zona de datos resguardada, que contiene los recursos más valiosos de la empresa, como sus datos y aplicaciones, y por micro perímetros que protegen

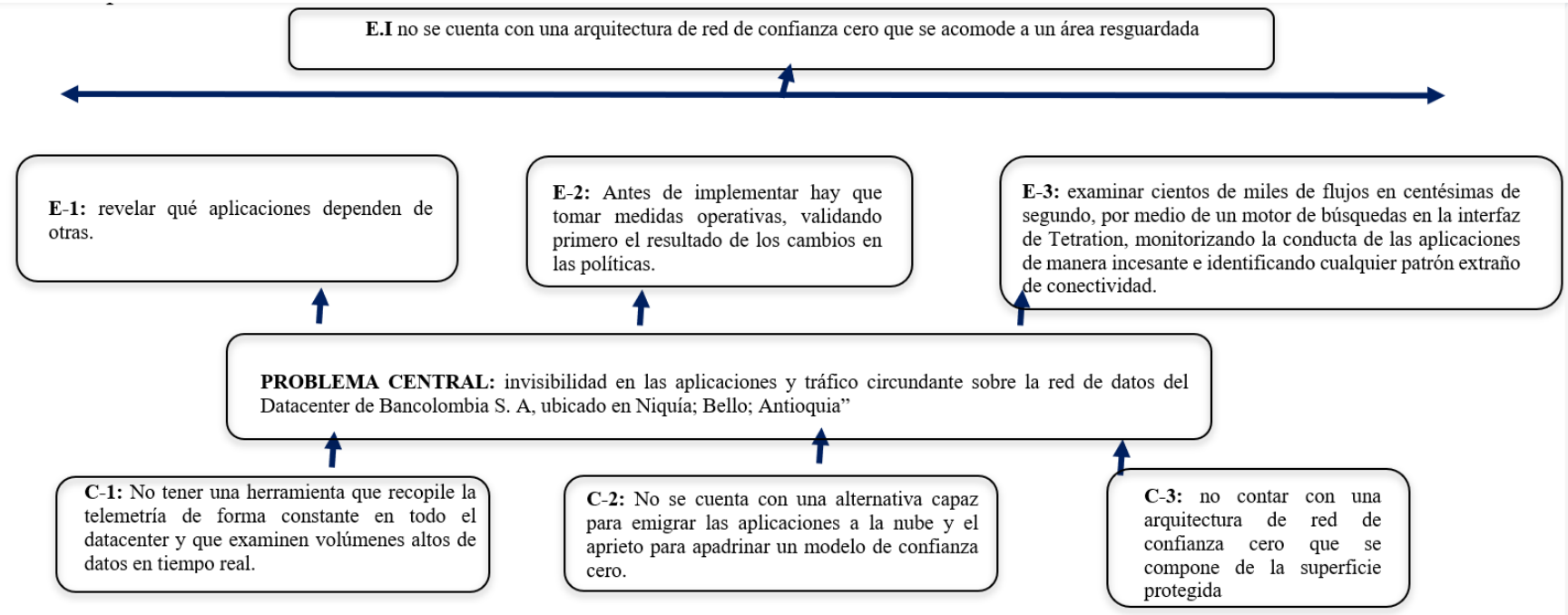
un recurso en lugar de un entorno de red completo. Este enfoque se hace fundamental para mejorar la eficiencia y seguridad de una empresa.

El problema ocurre porque no se cuenta con la capacidad de monitorización, análisis y generación de informes de manera efectiva y sostenible. En otras palabras, no se dispone de las herramientas y procesos necesarios para obtener una visibilidad completa de la red y de los datos que fluyen a través de ella, lo que aumenta el riesgo de vulnerabilidades y ataques cibernéticos. Es fundamental contar con una monitorización constante y un análisis de datos adecuado para poder detectar y responder rápidamente a cualquier anomalía o amenaza.

Árbol Causa – Efecto del Problema

Figura 1

Árbol del problema



Fuente. Caceres Saavedra, D. A. (2022). *Árbol de problema* [Fuente propia ed.]

Definición del Problema

El problema de falta de visibilidad y monitoreo efectivo de los flujos de información y datos en el Datacenter de Bancolombia es una situación real que ha sido reconocida por diversas fuentes en la industria de la tecnología y la ciberseguridad. Cisco, uno de los principales proveedores de soluciones de red y seguridad, ha destacado la importancia de contar con una arquitectura de seguridad de confianza cero y una visibilidad completa de la red para mitigar los riesgos de ataques cibernéticos y vulnerabilidades en la infraestructura de TI (Cisco, 2021).

Por su parte, Bancolombia ha reconocido públicamente la importancia de contar con una infraestructura de seguridad sólida y ha implementado diversas medidas y soluciones para fortalecer su posición en ciberseguridad (Bancolombia, 2022). Sin embargo, la falta de visibilidad y monitoreo efectivo de los flujos de información y datos en el Datacenter continúa siendo un desafío crítico que afecta la eficiencia y seguridad de la organización.

Posibles Soluciones

Implementar Arquitectura de Netflow Monitor, como características clave se tiene un monitoreo de ancho de banda que facilita la vista del uso de ancho de banda por aplicación, protocolo**,** grupo de direcciones IP, NTA permite que los administradores recopilen, monitoreen y analicen datos de flujo utilizando Cisco NetFlow, sFlow, J-Flow, IPFIX o NetStream. Usando NBAR2 ideas y monitoreo de WLC, SolarWinds NTA también se puede proporcionar una mejor visibilidad de las tendencias de tráfico de aplicaciones inalámbricas y su rendimiento en la red, se pueden obtener alertas en la red sobre el tráfico de la aplicación. (NetFlow Analyzer, 2022).

El Análisis del tráfico de red, el cual puede crear informes y alertas personalizables ayudando a detectar problemas en la primera señal de problemas. NTA informará sobre datos de tráficos de red actuales e históricos, incluidos datos de flujo y datos CBQoS, logrando detectar

tendencias en el uso máximo del ancho de banda con el fin de ajustar las políticas para una mejor gestión. Se puede establecer alertas para obtener información inmediata sobre cambios inusuales en el tráfico de la red, como cuando el uso del ancho de banda excede los umbrales establecidos. Siendo compatible con switches distribuidos de VMware vSphere. (*NetFlow Analyzer*, 2022).

Recopilador de Netflow, usa un monitoreo basado en flujo recopilando y analizando datos de flujo de múltiples proveedores de Cisco, incluidos NetFlow v5 y v9, Juniper J-Flow, sFlow, Huawei NetStream e IPFIX. El navegador de flujo de NTA permite crear y acceder a vistas de tráfico de red personalizadas, mientras que el sistema de informes le permite crear informes de tráfico de red detallados y programar la entrega semanal automática a su equipo con unos pocos clics. (*NetFlow Analyzer*, 2022).

Congestión de la red, identifica los problemas de congestión de la red rápidamente y muestra los puntos finales o aplicaciones específicos que consumen el mayor ancho de banda, cuenta con un panel de análisis de desempeño y reconocimiento de aplicaciones avanzadas. (*NetFlow Analyzer*, 2022).

Implementar Arquitectura de Cisco Tetration, como características clave: Cisco Secure Workload (Tetration) ofrece un enfoque de confianza cero para proteger las cargas de trabajo de su aplicación en cualquier entorno de centro de datos local y en la nube mediante la reducción de la superficie de ataque, la prevención del movimiento lateral, la identificación de anomalías en el comportamiento de la carga de trabajo y la corrección de amenazas rápidamente.

Modelo de confianza cero usando microsegmentación, hace referencia a la implementación en dicho entorno, dando un enfoque automatizado de Secure Workload ayudando a acelerar la protección de las cargas de trabajo de múltiples nubes híbridas y conteniendo el movimiento lateral.

Amplia las definiciones de políticas en función del contexto adicional, eliminando la creación manual de listas de recursos que consume mucho tiempo para segmentar aplicaciones, definiendo políticas predeterminadas y absolutas de microsegmentación mediante etiquetas de activos, desarrollando rápidamente políticas coherentes para aplicaciones mediante el etiquetado de activos en tiempo real, asociando un rico contexto empresarial con los servidores, definiendo las políticas basadas en usuarios y grupos de usuarios que necesitan acceso.

Aplicación de políticas con un solo clic en un centro de datos multinube, la cual hace cumplir el marco de seguridad mediante la segmentación de aplicaciones reduciendo la superficie vulnerable a los ataques, aplica políticas con un solo clic. Usando los mecanismos en entornos Linux y Microsoft Windows para hacer cumplir la política de seguridad la cual hace que se normalice la política para cada servidor, eliminando la necesidad de una intervención manual para identificar la política para cada uno de los servidores.

Defensa en profundidad, aplica políticas de segmentación y seguridad simultáneamente en Cisco Secure Firewalls a través de la integración con Cisco Secure Firewall Management Center

Detectar eventos de incumplimiento de políticas, realiza un seguimiento del cumplimiento de la política de aplicaciones en tiempo real, habilitando alertas para eventos de cumplimiento que luego se pueden integrar con los sistemas de Security Information and Event Management" en inglés (SIEM), que se refiere a un software de seguridad informática para investigación y corrección.

Identificación de desviaciones del comportamiento de la carga de trabajo, las líneas de base del comportamiento o las cargas de trabajo en función de las actividades y procesos de comunicación en las cargas de trabajo, detectan comportamientos anómalos de manera proactiva

e identificar indicadores de riesgo, habilitando las alertas para tales eventos para que se integren con sus sistemas SIEM para un mayor manejo de incidentes de seguridad, detectando las vulnerabilidades de software, obteniendo un inventario de software de referencia y la información de la versión instalada en los servidores, identificando rápidamente si alguna de las versiones del paquete tiene vulnerabilidades o exposiciones conocidas, junto con la gravedad, obteniendo un inventario preciso de todos los servidores que tienen el paquete vulnerable, vincula esta información a una política que designa una acción específica, como poner en cuarentena un servidor específico.

Opciones de recopilación de telemetría flexibles, agentes de software: capturan las actividades de comunicación y proceso junto con la información del paquete de software para establecer una referencia del comportamiento de la carga de trabajo, la cuales están diseñados para operar dentro de SLA de computación definidos por el administrador, por medio de Sensores ERSPAN, Sensores del controlador de entrega de aplicaciones ADC): F5, Citrix NetScaler, Sensores NetFlow, Registros de flujo de AWS VPC, Dispositivo de punto final y contexto de usuario, correlacionando los datos del usuario con el grupo de usuarios dentro de una organización, definiendo políticas específicas para la segmentación, utilizando información de usuarios y grupos de usuarios, las cuales se pueden aplicar en las cargas de trabajo. (Cisco, n.d.).

Tabla 3

Comparativa entre las tecnologías Netflow Monitor y Cisco Tetration

Características	**Netflow Monitor**	**Cisco Tetration**
Monitoreo de ancho de banda	Sí	No
Análisis del tráfico de red	Sí	Sí
Recopilador de Netflow	Sí	No
Identificación de congestión de red	Sí	No
Enfoque de confianza cero	No	Sí
Microsegmentación	No	Sí
Ampliación de políticas basadas en contexto	No	Sí
Aplicación de políticas con un solo clic	No	Sí
Defensa en profundidad	No	Sí
Detectar eventos de incumplimiento de políticas	No	Sí
Identificación de desviaciones del comportamiento de la carga de trabajo	No	Sí
Tipo de análisis	Análisis de flujo de red	Análisis de telemetría de red y de aplicación

Fuente de datos	Flujo de red capturado	Sensores de telemetría de red y de aplicación
Granularidad de datos	Flujo de paquetes individuales	Telemetría a nivel de paquete, proceso y usuario
Profundidad de análisis	Bajo a Medio	Alto
Aplicación de análisis	Monitorización de tráfico de red	Seguridad, cumplimiento, gestión de rendimiento y análisis de aplicaciones
Descripción general	Ofrece información sobre el tráfico de red y el uso de ancho de banda	Analiza el tráfico de red y de aplicaciones, procesos y usuarios para mejorar la seguridad, el cumplimiento y la eficiencia operativa
Propósito principal	Monitorización de la red	Análisis de telemetría para mejorar la seguridad, el cumplimiento y la eficiencia operativa
Tipo de empresa adecuada	Pequeñas a medianas	Medianas a grandes empresas

Fuente. Cáceres Saavedra, D. A. (2023). *Comparativa entre las tecnologías Netflow Monitor y Cisco Tetration* [Fuente propia].

Solución Seleccionada y Justificación

En la búsqueda por solucionar la problemática del Datacenter de Bancolombia S.A., seleccione la implementación de la arquitectura de Cisco Tetration, la cual se adapta perfectamente al tamaño del centro de datos. Esta solución ofrece un inventario completo de software y vulnerabilidades, con un análisis detallado del comportamiento de procesos y una segmentación de aplicaciones que me permite un control de comunicaciones mediante el uso de listas blancas. Para lograr esto, se requiere la implementación de seis servidores Tetration y dos conmutadores de la serie Cisco 9300, que son ideales para redes con menos de 5000 servidores.

En el análisis de datos y estadísticas de red, la analítica de red se convierte en una herramienta fundamental para el centro de Datos de Bancolombia S.A. Actualmente, no cuento con un software o hardware capaz de realizar un análisis más profundo en las aplicaciones y que recolecte la telemetría permanente de todo el datacenter, examinando grandes volúmenes de datos en tiempo real.

Con la instalación de los seis servidores y dos conmutadores de plataforma Cisco Nexus 9300, que es ideal para centros de datos de menos de 5,000 servidores, se podrán procesar hasta 500,000 eventos de flujo por segundo, permitiendo ver quién se comunica dentro de los servidores, qué puertos se utilizan, cuánto tráfico se genera y cuál es el retardo. Partimos de la no visibilidad de los datos que se transmiten en la red y se busca llegar a un análisis más detallado de cada uno de ellos, conociendo con qué equipos dentro y fuera de la red tienen más comunicación.

Actualmente, tengo 63 aplicaciones sin observación y alrededor de 2000 servidores sin supervisión, lo que resalta la necesidad de implementar una solución como Tetration. Con esto, puedo tener un análisis profundo de cada una de las aplicaciones y servidores en el centro de datos de Bancolombia S.A.

Justificación

Como responsable de TI en la empresa, desde mi punto de vista, la implementación de la analítica de datos en el Datacenter mediante la recopilación de metadatos de paquetes y flujos, junto con información del proceso, mediante un método de indexado exclusivo, sería una solución esencial para mejorar la eficiencia en el manejo de datos de las aplicaciones en el Datacenter. Además, como profesional de la Ingeniería de telecomunicaciones, tengo el compromiso social aplicar todos los conocimientos adquiridos en la formación para hacer el diseño, la implementación y planeación, controlando y gestionando los sistemas de telecomunicaciones de acuerdo con las necesidades actuales de la industria. Con esta implementación, se lograría mejorar la competitividad de la empresa y contribuir al progreso local, regional y nacional a nivel tecnológico, lo cual es una de las metas principales del programa.

Diseño Metodológico

Marco Referencial

Marco Conceptual

Cisco Tetration. Es una protección integral para la carga de trabajo de Data Centers habilita un modelo de confianza cero por medio del fraccionamiento de aplicaciones. Permitiendo identificar sucesos de seguridad más rápido, frenando el movimiento lateral y reduciendo el plano de ataque. (Cisco 2022).

Seguridad de Confianza Cero. Muestra un enfoque importante de la seguridad que se centraliza en el concepto de eliminar la confianza de la arquitectura de red de una organización, estableciendo la familiaridad en cada solicitud de acceso, sin importar de dónde provenga, asegurando el acceso a través de sus aplicaciones y una red amplía de confianza para dando soporte a una empresa moderna en toda la red distribuida. (Services, 2022)

Datacenter. El centro de procesamiento de datos es una instalación donde se alojan y conservan cuantiosos dispositivos electrónicos como servidores, Switches, Routers, conexiones y demás recursos necesarios los cuales son utilizados para la conectividad de una red y conexiones de datos de una o diversas empresas. (¿Qué es un Data Center?, 2022).

Flujo de Red. Serie de comunicaciones entre dos puntos finales que están restringidos por la apertura y el cierre de sesiones. (Network Flow Monitor, 2022).

Big Data. Son macrodatos en un conjunto de tamaño variable y cuya velocidad de crecimiento dificultan su captura, estudio, gestión y procesamiento, que, por medio de tecnologías y equipos convencionales como bases de datos relacionales y estadísticas convencionales, sean útiles dentro de un tiempo necesario (PowerData, 2022).

Estado del Arte

Tabla 4

Cisco Extends Tetration Analytics to Enable Workload Protection. (RAE)

RAE	
1. Titulo	Cisco Extends Tetration Analytics to Enable Workload Protection.
2. Autor	Kerner, Sean Michael
3. Edición	eWeek
4.Fecha	3/5/2018
5. Palabras clave	Workload protection, SDN, Cisco Tetration
6. Descripción	Publicación periódica, ofrece información sobre la nueva actualización de ayuda de carga de trabajo de la plataforma de análisis Cisco Tetration anunciada por Cisco, que ayuda a detectar vulnerabilidades de software, monitorear procesos en ejecución y detectar desviaciones de comportamiento de aplicaciones.
7. Fuentes	Sean Michael Kerner es editor sénior de eWEEK e InternetNews.com, consultor de Internet, estratega y colaborador de varios sitios web de empresas de TI líderes.
8. Contenidos	La publicación inicia, indicando la nueva actualización de cisco Tetration la cual, proporciona detección de vulnerabilidades y monitoreo del comportamiento del proceso, informando

	que Cisco anunció que está expandiendo la plataforma de análisis Tetration para brindar nuevas capacidades de protección de cargas de trabajo. Enfocando la defensa en profundidad para Tetration que permite a una organización impulsar una política a un host de aplicaciones, así como al perímetro de la red y a los controladores SDN, aplica la carga de trabajo de forma nativa a través de agentes en contenedores y máquinas virtuales sin sistema operativo.
9. Metodología	El escrito no se apoya en una metodología específica.
10. Conclusiones	El autor hace un énfasis claro en la expansión de la plataforma de análisis Tetration para brindar nuevas capacidades de protección de cargas de trabajo.
11. Autor del RAE	Daniel A. Cáceres Saavedra

Fuente. Cáceres Saavedra, D. A. (2023). *Cisco Extends Tetration Analytics to Enable Workload Protection. (RAE)* [Fuente propia].

Tabla 5

Cisco amps-up Tetration platform with better security, reduced footprint, AWS cloud option. (RAE)

RAE	
1. Titulo	Cisco amps-up Tetration platform with better security, reduced footprint, AWS cloud option
2. Autor	Cooney, Michael
3. Edición	Networks Asia
4.Fecha	2/9/2017
5. Palabras clave	Computer networks, devops
6. Descripción	El artículo ofrece información sobre Tetration Analytics de Cisco, que es un análisis de centro de datos en tiempo real que combina sensores de red y servidor para simplificar las redes definidas por software (SDN).
7. Fuentes	El texto no es consecuencia de una investigación determinada, se trata de la idea de que a medida que los clientes se mueven hacia un entorno más devops donde las aplicaciones se conectan y desconectan rápidamente, Tetration puede implementar políticas de seguridad rápidamente.
8. Contenidos	"A medida que las organizaciones se someten a la transformación digital y adoptan el modelo DevOps, están invirtiendo en nuevas tecnologías con una infraestructura que se está volviendo más

	dinámico y distribuido, y como resultado, la seguridad también debe ser más dinámica ", dijo Zeus Kerravala, analista principal de ZK Research and Network World blogger, en un comunicado. Los sensores de software Tetration admiten hosts de servidor Linux y Windows, mientras que los sensores de hardware están integrados en el conmutador de red Cisco Nexus 9200, Nexus 9300-EX y Nexus 9500-EX, para recopilar datos de flujo a la velocidad de línea de todos los puertos. Según Cisco, una vez implementada, la plataforma Tetration aprende su entorno empresarial y cualquier política que TI tenga implementada.
9. Metodología	El escrito no se apoya en una metodología específica.
	La adopción de las nuevas configuraciones de políticas y clientes se puede validar ejecutándose primero a través de Tetration para ver cuál sería su impacto en la empresa.
	La seguridad es una parte clave de Tetration y las nuevas versiones incorporan más opciones al sistema
10. Conclusiones	
11. Autor del RAE	Daniel A. Cáceres Saavedra

Fuente. Cáceres Saavedra, D. A. (2023). *Cisco amps-up Tetration platform with better security, reduced footprint, AWS cloud option. (RAE)* [Fuente propia].

Tabla 6

Cisco amps-up Tetration platform with better security, reduced footprint, AWS cloud option: Cisco Tetration helps users move toward Zero Trust data center. (RAE)

	RAE
1. Titulo	Cisco amps-up Tetration platform with better security, reduced footprint, AWS cloud option: Cisco Tetration helps users move toward Zero Trust data center.
2. Autor	Cooney, Michael
3. Edición	ARN: Australian Reseller News
4.Fecha	2/2/2017
5. Palabras clave	Tetration Analytics package, analytics package, cloud
6. Descripción	El artículo ofrece información sobre el lanzamiento del paquete Tetration Analytics de Cisco Systems Inc., que consta de funciones como una huella más pequeña y un sistema de servicio en la nube para atraer a más clientes de centros de datos
7. Fuentes	El texto no es consecuencia de una investigación determinada, indica un motor de aplicación y recomendación de

	políticas de Tetration Analytics la cual ahora puede tomar la microsegmentación, que es una técnica de seguridad que acepta la separación de la carga de trabajo, va un paso más allá al ofrecer la segmentación de aplicaciones Cisco ha lanzado una segunda versión de su paquete Tetration Analytics con características tales como una huella más pequeña y un servicio en la nube que contribuirá en gran medida a hacer que el sistema sea atractivo para más clientes de centros de datos. Jim Duffy, analista sénior del grupo de investigación 451, señaló que Cisco el verano pasado dijo en Cisco Live que reducirían Tetration, incluso al nivel del chip. “Por lo tanto, las huellas más pequeñas y el empaque y los precios más digeribles tienen mucho sentido”. Para la nube, Cisco también ha anunciado un dispositivo con software Tetration implementado en la nube
8. Contenidos	pública en Amazon Web Services

	(AWS). Tetration Cloud también admite hasta 1000 cargas de trabajo. Tetration puede monitorear cargas de trabajo en nubes privadas y públicas, afirmó Cisco.
9. Metodología	El escrito no se apoya en una metodología específica.
10. Conclusiones	Con cisco Tetration los usuarios podrán avanzar hacia la confianza cero en sus centros de datos. Se pueden enviar políticas al firewall de cualquier proveedor y también se pueden orquestar en la capa de red
11. Autor del RAE	Daniel A. Cáceres Saavedra

Fuente. Cáceres Saavedra, D. A. (2023). *Cisco amps-up Tetration platform with better security, reduced footprint, AWS cloud option: Cisco Tetration helps users move toward Zero Trust data center. (RAE)* [Fuente propia].

Tabla 7

Tetration. (RAE)

RAE	
1. Titulo	Tetration
2. Autor	Dunn, Katelyn
3. Edición	SC Magazine: For IT Security Professionals (15476693)
4.Fecha	Feb2019
5. Palabras clave	Security management, Cloud computing
6. Descripción	El artículo evalúa Cisco Tetration el cual ofrece protección de carga de trabajo y funcionalidad de Cisco Systems
7. Fuentes	El texto no es consecuencia de una investigación determinada, involucra las características clave y la intención de Cisco Tetration la cual proporciona un mecanismo dinámico que utiliza aprendizaje automático para generar y mantener las pólizas asignadas por las aplicaciones.
8. Contenidos	El artículo indica una política de línea de base la cual se genera a partir de espacios de trabajo de la aplicación mediante un modelo de comportamiento del proceso, a su vez los conocimientos de la aplicación y comunicaciones de red. Este plano se puede visualizar en un gráfico con la aplicación mapeo de dependencias. Los clientes pueden identificar diferentes

	clústeres y cuántos miembros contiene Este plano se puede utilizar para crear una política de lista blanca de referencia basada en comportamiento de comunicación de la aplicación observado. Hay tres elementos que componen la política de segmentación: el contexto de carga de trabajo y metadatos, integraciones de terceros y acceso a información personalizable para usuarios y grupos. Estos también se basan en autogeneración en el comportamiento de las aplicaciones y se pueden combinar para una política unificada. Tetration también se integra con sistemas CMDB y cualquier sistema de terceros que se pueden cargar en el Plataforma de Tetration vía API.
9. Metodología	El escrito no se apoya en una metodología específica.
10. Conclusiones	Las cargas de trabajo están protegidas contra desviaciones como escalada de privilegios, ejecución de código de shell, ataques de canal, creaciones de socket sin procesar y actividades de usuario de inicio de sesión.
11. Autor del RAE	Daniel A. Cáceres Saavedra

Fuente. Cáceres Saavedra, D. A. (2023). *Tetration. (RAE)* [Fuente propia].

Tabla 8

Cisco platform lets IT rein-in disruptive data center operations, security, applications. (RAE)

RAE	
1. Titulo	Cisco platform lets IT rein-in disruptive data center operations, security, applications
2. Autor	Cooney, Michael.
3. Edición	Network World (Online); Southborough
4.Fecha	Jun 15, 2016
5. Palabras clave	International Data Corp, zero-trust
6. Descripción	El artículo informa sobre la plataforma, Cisco Tetration Analytics, la cual compila información de sensores de software y hardware y que analiza la información utilizando análisis de big data y aprendizaje automático brindando a los administradores de TI una perspicacia más profunda de los recursos de su centro de datos. El sistema simplificará drásticamente la confiabilidad operativa, las migraciones de aplicaciones a SDN y la nube, así como el monitoreo de seguridad,
7. Fuentes	El contenido no es consecuencia de una investigación determinada, Después de dos años de desarrollo, Cisco lanza hoy un dispositivo de rack completo que promete hacer casi todo lo que se necesita para controlar un centro de datos, desde facilitar las operaciones de TI y controlar

8. Contenidos

la seguridad hasta el monitoreo de aplicaciones.

En general, las grandes empresas y los clientes de proveedores de servicios buscan una mayor visibilidad de sus redes de centros de datos. A un alto nivel, esto es lo que Cisco aborda con Tetration Analytics Platform. En varios escenarios: migración a la nube, migración a SDN, desastre la recuperación, la transición a un modelo de seguridad de confianza cero, la verificación del cumplimiento de políticas e incluso la integración de sistemas de TI después de fusiones y adquisiciones: la visibilidad generalizada es cada vez más crítica para el éxito", dijo Brad Casemore, director de investigación, redes de centros de datos de International Data Corp.

"Los clientes que enfrentan estos problemas y que sienten la necesidad aguda de una visibilidad generalizada probablemente no se desanimarán por el tamaño de la plataforma o por la inversión requerida para adquirirla, pero esta es una oferta que se adapta mejor a las organizaciones de tamaño suficiente y escalar para tener los casos de uso y los desafíos para los que se diseñó Tetration".

9. Metodología	El escrito no se apoya en una metodología específica.
10. Conclusiones	En el lado de la configuración de políticas, los clientes pueden validar nuevas políticas ejecutándolas primero a través de Tetration para ver cuál sería su impacto en la empresa. Los usuarios también pueden utilizar esta información para aplicaciones de cumplimiento normativo.
11. Autor del RAE	Daniel A. Cáceres Saavedra

Fuente. Cáceres Saavedra, D. A. (2023). *Cisco platform lets IT rein-in disruptive data center operations, security, applications. (RAE)* [Fuente propia].

Objetivos

Objetivo General

Implementar un modelo de confianza cero en el Data Center Bancolombia ubicado en Niquia, Bello, Antioquia, a través de la plataforma Cisco Tetration.

Objetivos Específicos

Implementar 6 servidores y 2 conmutadores de plataforma Cisco Nexus 9300 el cual es adecuado para centros de datos de menos de 5,000 servidores, solventando la solución y validando el número de eventos de flujo procesados por segundo.

Instalar el software cisco Tetration, por medio de todos los recursos que ofrece el proveedor el cual estará instalado en una máquina virtual en UCS, visualizando todos los datos, flujos y conexiones de cada servidor.

Instalar Agente Tetration en servidores bancarios mediante script ejecutado por administradores de plataformas Linux, AIX y Windows para establecer confianza en solicitudes de acceso de aplicaciones con modelo de confianza cero y lograr visibilidad en usuarios, dispositivos, contenedores, redes y aplicaciones.

Verificar el correcto funcionamiento de la plataforma, a través del servidor de Tetration, se validará el estado de cada agente instalado en cada servidor.

Cronograma

Tabla 9

Establecer el cronograma de actividades para el diseño e implementación de la solución

Objetivos	Actividades	Mes 1	Mes 2	Mes 3	Mes 4
General	1. Realizar Topología Física General del Servicio	X			
	2.Validacion de las características de la plataforma	X			
Especifico 1	1. Instalación de cisco Tetration-M 8(RU)		X		
	2.Impletacion de servidores en clúster		X		
	3. Implementación Switches Nexus 9000		X		
Específico 2	1. Servidores UCS-C (ESXi) ERSPAN			X	
	2. VMware EsXI			X	
	3. Cableado Datacenter Clúster Tetration			X	
Específico 3	1. Especificación de servicios configurados			X	
	2. Enrutamiento L3			X	
	3. Detalles de sensores			X	

Especifico 4	1.Validar tipos de agentes Deep Visibility Agents, en plataformas Windows, AIX y Linux	X
	2. Configuración de sensores	X

Fuente. Cáceres Saavedra, D. A. (2022). *Establecer el cronograma de actividades para el diseño e implementación de la solución.* [Fuente propia].

Recursos

Tabla 10

Definir el presupuesto necesario para la implementación de la solución

Recurso	Descripción	Presupuesto en COP	Presupuesto en USD
Equipo Humano	Ingeniero de Telecomunicaciones para la implementación.	$7'500.000	
	Ingeniero Especialista Datacenter	$5'500.000	
	Ingeniero N2, conocimientos en Tetration, CCNA, Python	$3'700.000	
Equipos y Software	2x Switch Cisco 9300: (Optimización para acceso seguro de alta velocidad, agregación e implementaciones de sucursales ajustadas; 12 o 24 puertos de fibra 25G / 10G / 1G, 24 o 48 puertos de 1G / 2.5G / 5G / 10G multigigabit y Cisco 90W UPOE+ (nuevo); Uplinks modulares de doble tasa 100G/40G, multitasa 25G/10G/1G		USD 29.800

o multigigabit (Cisco Catalyst 9300 Series Switches, 2022).	
2x UCS C220 M5SX: las CPU escalables Intel Xeon más recientes (segunda generación) con hasta 28 núcleos por zócalo; Admite CPU escalables Intel Xeon de primera generación con hasta 28 núcleos por socket; Hasta 24 DIMM DDR4 para mejorar el rendimiento; Compatibilidad con la memoria persistente Intel Optane DC (128 G, 256 G, 512 G) [1]; Hasta 10 unidades de factor de forma pequeño (SFF) de 2,5 pulgadas o 4 unidades de factor de forma grande (LFF) de 3,5 pulgadas (capacidad de almacenamiento de 77 TB con todos los SSD PCIe NVMe); Soporte para el controlador RAID modular SAS de 12 Gbps en una ranura	USD 8.600

dedicada, dejando las ranuras PCIe Generation 3.0 restantes disponibles para otras tarjetas de expansión; Ranura modular LAN-On-Motherboard (mLOM) que se puede usar para instalar una tarjeta de interfaz virtual (VIC) Cisco UCS sin consumir una ranura PCIe; Dos puertos integrados Intel x550 10GBASE-T LAN-On-Motherboard (LOM). (Servicios, Computación, Servidores y Hojas, 2022)	
6 servidores UCS-C: 3rd Gen Intel® Xeon® Scalable CPUs, 2-socket; Up to 40 cores per socket; Up to 12 TB memory support with optional Intel Optane™ PMem; Up to 10 drives – SAS/SATA/NVMe; Up to 3 PCIe Gen 4.0	USD 7.866

	expansion slots. (Services and Computing, 2022).		
Viajes y Salidas de Campo	Transporte de Insumos al datacenter cada mercancía es asegurada.	$6'000.000	
Materiales y suministros	Cables de Stacking x 8	$2'000.000	
Total		$ 24.700.000	$ 46.266

Fuente. Cáceres Saavedra, D. A. (2022). *Definir el presupuesto necesario para la implementación de la solución.* [Fuente propia].

Services, P. and Computing, S., 2022. Cisco UCS C-Series Rack Servers. Services, P., Computing, S., Servers, C. and Sheets, D., 2022. Cisco UCS C220 M5 Rack Server Data Sheet.

Diseño de la Solución

Especificaciones Técnicas

Tetration-M 8(RU) consta de 6 servidores y 2 conmutadores de plataforma Cisco Nexus 9300 el cual es adecuado para centros de datos de menos de 5.000 servidores. La siguiente tabla muestra los requisitos de alimentación y refrigeración para la plataforma Secure Workload-M.

Tabla 11

Características de la plataforma

Item	Observación
Número de servidores (máquina virtual o bare metal)	Hasta 5000 cargas de trabajo con telemetría de flujo detallada Hasta 10 000 cargas de trabajo con telemetría de flujo solo de conversación
Número de eventos de flujo que se pueden procesar por segundo	Hasta 500,000 por segundo
Número de conmutadores Cisco Nexus serie 9000 habilitados para sensores de hardware	Hasta 100
Potencia máxima para Cisco Secure Workload-M (8RU)	5,5 kilovatios
Requisito máximo de enfriamiento para Cisco Secure Workload-M (8RU)	13,500 BTU por hora

Número de cargas de trabajo simultáneas (máquina virtual o bare metal o host de contenedor) desde las que se pueden analizar los datos de telemetría	Hasta 25 000 cargas de trabajo con telemetría de flujo detallada. Hasta 50 000 cargas de trabajo con telemetría de flujo solo de conversación
Número de eventos de flujo que se pueden procesar por segundo	Hasta 2 millones por segundo
Potencia máxima para Cisco Secure Workload: opción de un solo rack de 39 unidades de rack [39RU] *	22,5 kilovatios
Requisitos máximos de refrigeración para Cisco Secure Workload: opción de un solo rack de 39RU *	50,000 BTU por hora
Peso total para Cisco Secure Workload: opción de un solo rack de 39RU	1800 libras (800 kg)
Unidad de distribución de energía (PDU) y fuente de alimentación (opción de un solo rack de 39RU)	4 PDU trifásicas (las clasificaciones de corriente y voltaje varían según la geografía)

Potencia máxima para Cisco Secure Workload: opción de rack doble de 39RU	11,25 kW por rack (22,5 kW en total)
Requisito máximo de enfriamiento para Cisco Secure Workload: opción de rack doble de 39RU	25,000 BTU por hora por rack
Peso total para Cisco Secure Workload: opción de rack doble de 39RU	900 lb por estante (400 kg por estante)
PDU y fuente de alimentación: opción de rack doble de 39RU	4 PDU monofásicas por rack (las clasificaciones de corriente y voltaje varían según la geografía)

Fuente. Cáceres Saavedra, D. A. (2022). *Características de la plataforma de la solución.* [Fuente propia]. Cisco Secure Workload (2022).

Configuración de Red

Tabla 12

Configuración de acceso a la red administración

General	
Site Name	tetr-analitica
DNS Domain	bancoco.corp
DNS Resolver	10.9.35.11
External Network	10.9.196.0/24
Internal Network	1.1.1.0/17

Fuente. Cáceres Saavedra, D. A. (2022). *Configuración de acceso a la red administración*. [Fuente propia].

Ingreso Desde la Red de Bancolombia

Tabla 13

Configuración de acceso a la red banco

General	
IP	https://10.19.196.4/
DNS	https://te-analit.bancoco.corp/

Fuente. Cáceres Saavedra, D. A. (2022). *Configuración de acceso a la red banco.* [Fuente propia].

Especificaciones de Servicios Configurados, incluyen un servidor Syslog que puede utilizar Tetration para enviar mensajes de Syslog. Actualmente Se admite un único servidor Syslog. Los valores posibles para la gravedad de Syslog son: informational, notice, warning, error, critical, alert and emergency.

Inicialmente se realizará la instalación del clúster de Tetration versión 3.5.1.17 para este sistema se admiten las siguientes plataformas y versiones del sistema operativo.

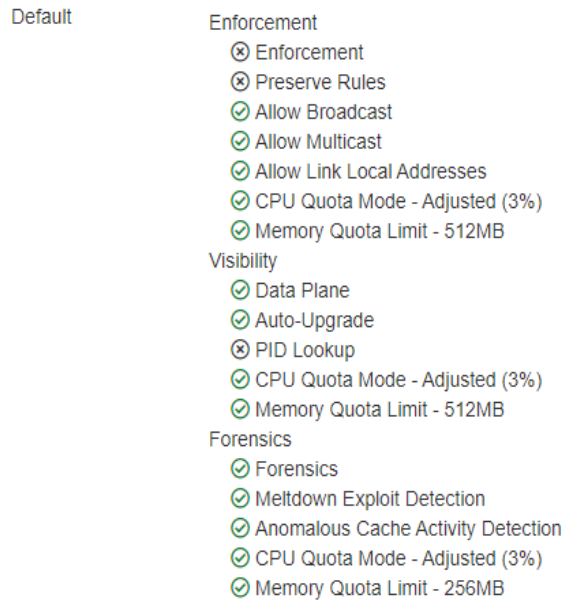
Tipo de Agentes**.** Deep Visibility Agents: Linux (RHEL, CentOS, Oracle, Ubuntu); Windows (Desktop, server); AIX (ALPHA).

La configuración de sensores para la instalación de agentes en los servidores de Bancolombia se estará instalando los agentes Deep Visibility con el perfil predeterminado que tiene los siguientes valores definidos de CPU y valores de memoria

Configuración Sensores

Figura 2

Configuración Sensores de agentes en servidores



Nota. Los agentes que coinciden con los criterios de filtro de inventario se actualizan automáticamente a la última versión de software disponible.

Cáceres Saavedra, D. A. (2022). *Configuración Sensores de agentes en servidores*. [Fuente propia].

Autenticación Tetration

Para ingresar a Tetration se puede ingresar de la siguiente manera:

Autenticación Local. Se crea usuarios locales para Administradores del sitio y usuarios de atención al cliente

Autenticación por LDAP. Se habilitó el componente de autenticación con el LDAP para los usuarios que ingresan del banco, los usuarios que inicien sesión utilizarán sus datos basados en la autenticación de LDAP de correo electrónico y contraseña para autenticarse con la plataforma.

Creación de ADMS

Se definió con el banco darle prioridad a 63 aplicaciones las cuales son críticas para el servicio de la operación, se definieron las siguientes aplicaciones para instalar agentes en los servidores crear annotations, scopes y ADMS de cada uno de sus ambientes.

Tabla 14

Creación de ADMs etapa1

Numero	Aplicación
1	Bizagi GF
2	Bizagi Go
3	Adminfo
4	Axiom Reporteria Legal
5	Balanza Cambiaria
6	Biometría Sucursales
7	Conocimiento del Cliente - MDM
8	Eureka
9	Gestión de Filas (Qflow)
10	HARVEST
11	Intermedia
12	Motor de Decision
13	Ordenes Web
14	OYD - Oferta y Demanda
15	Quality Center
16	Tesorería (Murex Colombia)
17	Unico
18	USD
19	USM
20	KOFAX
21	SIF Branch GOLF (WOLF)
22	Tarjetas Crédito
23	Emulacion iSeries
24	SAP CRM
25	SAP DM Disclosure Management
26	SAP ERP
27	SAP PORTAL

28	SAS GRID
29	SAS IFRS9
30	Nequi
31	POS y ATM Credibanco
32	POS y ATM Redeban
33	Swift Colombia
34	Conexión Empresarial Bancolombia (H2H)
35	Ahorro a la Mano (SMS)
36	APP Empresas Bancolombia
37	APP Personas Bancolombia
38	CB Credibanco
39	CB Redeban
40	CDT y BONOS
41	Compra y venta de Divisas por la SVE
42	Creditos Consufi
43	Cuentas AFC
44	Envío de Alertas Correo Electrónico
45	Envío de Alertas SMS
46	e-prepago APP
47	E-Trading (En linea)
48	Fondos de Inversión en Virtuales
49	Preordenes
50	PSE
51	Sucursal Telefónica Bancolombia
52	Sucursal Virtual Empresas Bancolombia
53	Sucursal Virtual Factoring
54	Sucursal Virtual Leasing
55	Sucursal Virtual Personas Bancolombia
56	Sucursal Virtual Sufi
57	Sucursal Virtual Valores Bancolombia
58	Ahorro a la Mano (APP)

59	APP Pyme Bancolombia
60	Billetera Móvil
61	Acceso Remoto Bancolombia
62	Biztrack
63	Portal de Contenidos Grupo Bancolombia

Fuente. Cáceres Saavedra, D. A. (2022). *Creación de ADMs etapa1*. [Fuente propia].

También se crearán las siguientes aplicaciones, las cuales entraron en la operación que son aparte de las 63 iniciales como parte de implementación.

Tabla 15

Creación de ADMs etapa2

Número	Aplicación
1	ControlM
2	Thanos
3	LZ
4	PasswordSafe
5	PKI
6	Antivirus
7	CASB
8	Power BI
9	Clave Dinámica
10	Tableros de Control
11	Panorámica del Cliente
12	BIOVOZ
13	IAM
14	BRM
15	SIA
16	CORONA

Fuente. Cáceres Saavedra, D. A. (2022). *Creación de ADMs etapa2.* [Fuente propia].

Se crearán 267 ADMs para las 79 aplicaciones, así como para otros componentes que forman parte de ellas, como balanceadores, brokers, MQ, iSeries, redes externas, Datapower, bus de integración, entre otros.

Para completar una aplicación al 100%, se tomaron en cuenta los siguientes valores, Data Aplicación; Sensores; ADM; Revisión Usuario Final

Data aplicación. Información de la aplicación que será enviada por usuarios.

Sensores: Instalación completa de agentes en los servidores de la aplicación.

ADM. creación del diagrama en base a la información enviada por el usuario.

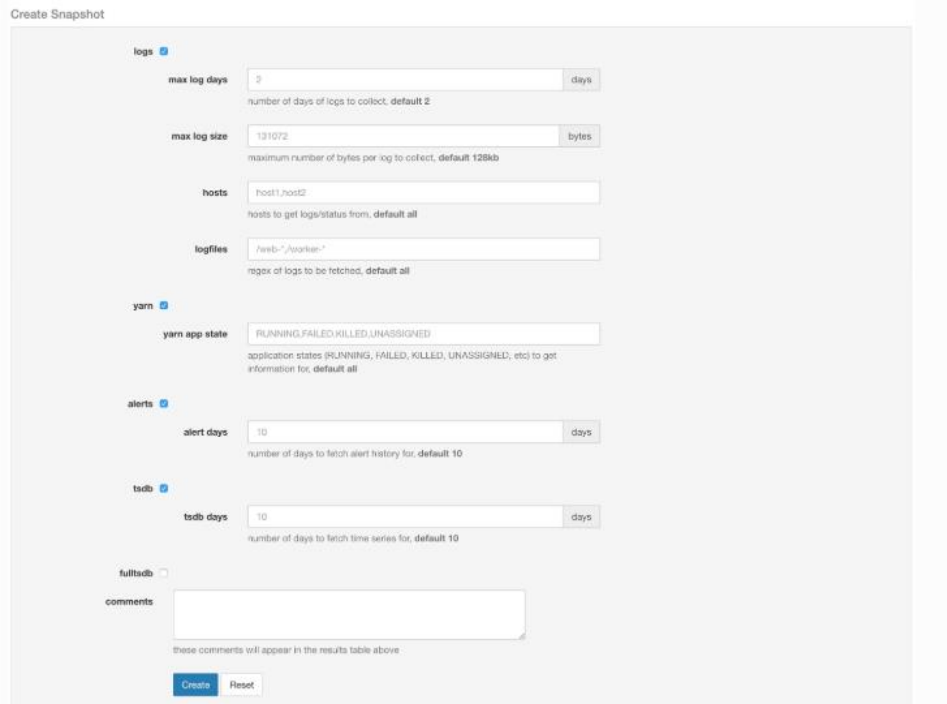
Revisión usuario: validación correcta de clúster y flujos

Backups

Tetration Snapshots, se ejecutará diariamente backups de la configuración del clúster de Tetration de acuerdo con los niveles de servicio estipulados, para guardar la configuración se realiza mediante un Snapshots el cual se descarga de la GUI de Tetration en la ruta Maintenance -> Snapshots, los snapshots serán almacenados en un servidor de Telefónica con (IP 10.19.192.136).

Figura 3

Proceso para generar snapshots en Tetration



Nota. Recopila la información de manera predeterminada de logs, alert history, numerous TSDB statistics. Cáceres Saavedra, D. A. (2022). *Proceso para generar snapshots en Tetration* [Fuente propia].

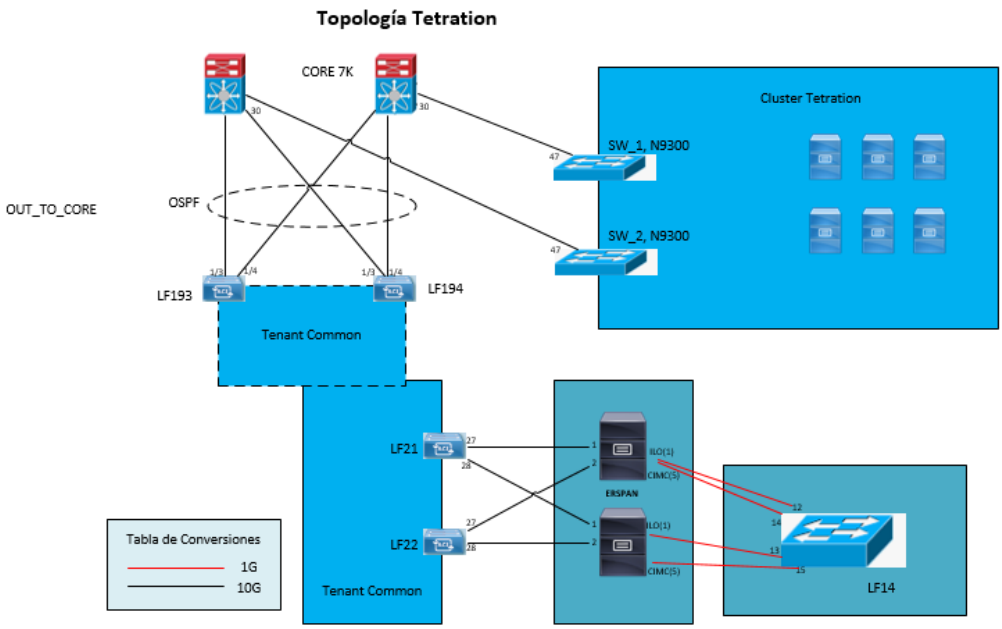
Backups ADMs, por medio de la API de Tetration se guardarán los detalles de los ADMs que ya están parametrizados en Tetration, se guardan las configuraciones de los clústeres y las políticas de cada ADM, el respaldo se generara por medio de un script realizado por python el cual se genera automáticamente todos los días y se almacenan en un servidor de Telefónica (IP 10.19.192.136).

Backups Annotation, los annotations son las etiquetas, atributos que se asignan a cada dirección de red, los annotations son el inventario principal para empezar a construir un ADM, por lo que el archivo principal de annotations se puede descargar de la GUI de Tetration para tenerlo como respaldo en caso de fallas del clúster y cambios no deseados, este archivo se guarda diariamente y se almacena en el servidor de Telefónica (IP 10.19.192.136). Ruta del archivo VISIBILITY -> Inventory Upload.

Planos

Figura 4

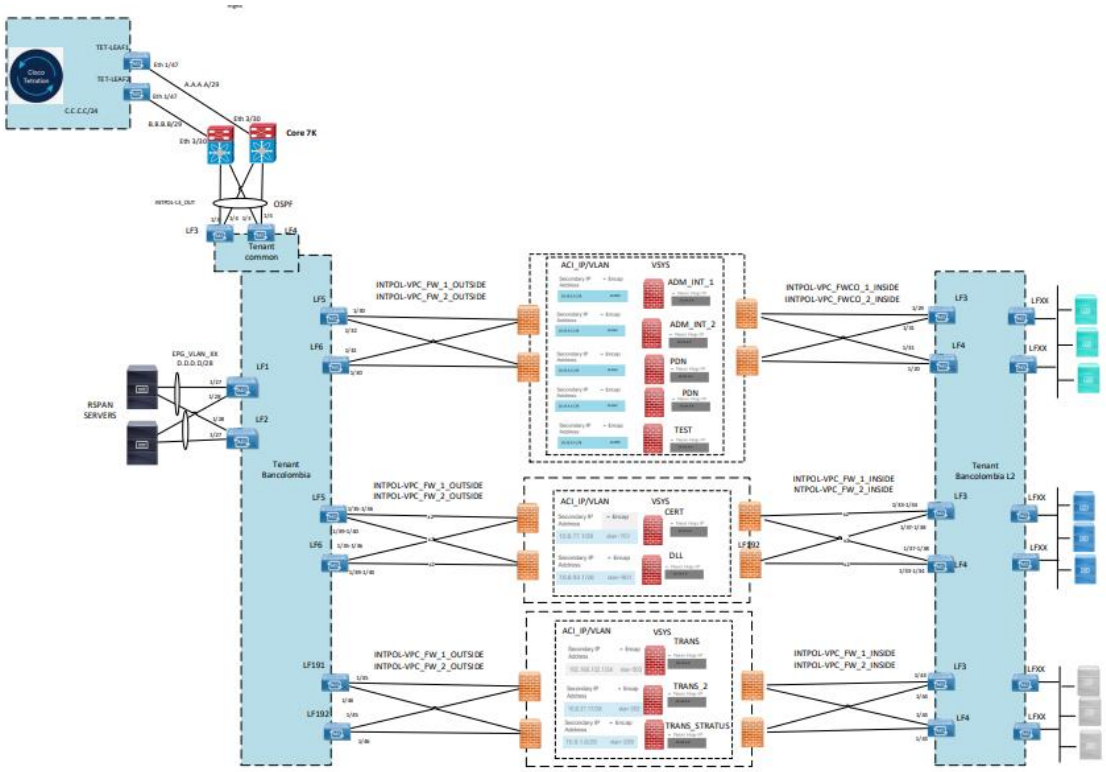
Detalles Físicos Datacenter ubicación de la arquitectura



Fuente. Cáceres Saavedra, D. A. (2022). *Detalles Físicos Datacenter ubicación de la arquitectura* [Fuente propia].

Figura 5

Topología Lógica Tetration

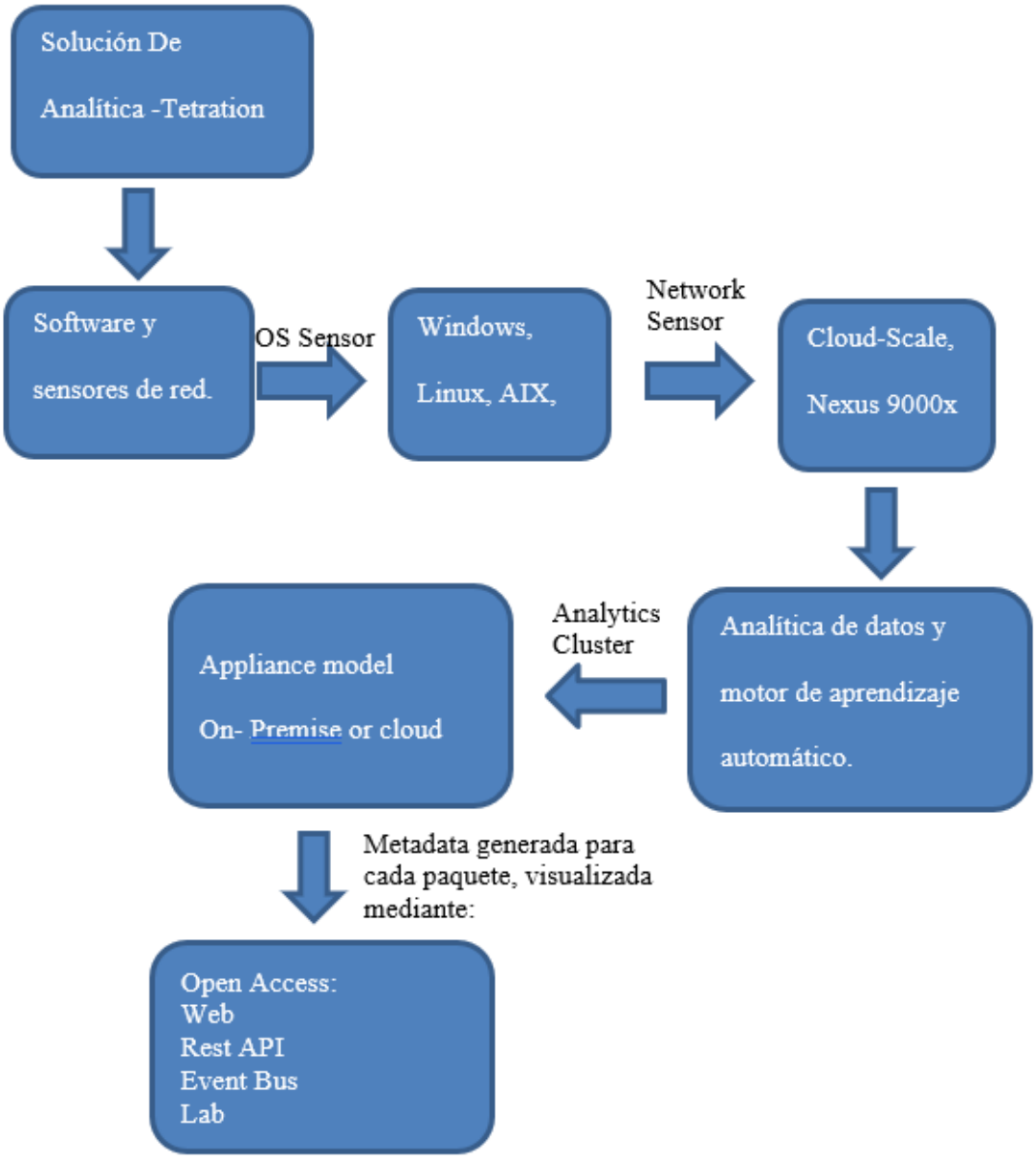


Nota. Con esta solución, los hosts no necesitan ejecutar agentes de software, porque los conmutadores Cisco retransmitirán el tráfico de los hosts al dispositivo ERSPAN para su procesamiento. Cáceres Saavedra, D. A. (2022). *Topología Lógica Tetration* [Fuente propia].

Algoritmos

Figura 6

Solución De Analítica -Cisco Tetration



Nota. El algoritmo presentado aquí describe los componentes esenciales del sistema de analítica de datos Cisco Tetration. Cáceres Saavedra, D. A. (2022). Solución De Analítica -Cisco Tetration [Fuente propia].

Con esta solución de analítica, se puede monitorear y analizar el tráfico de red y aplicaciones en tiempo real, lo que permite a los usuarios tener una mayor visibilidad y control sobre su infraestructura de TI.

En primer lugar, se destaca la importancia de la solución de analítica Tetration, que es el primer paso en la implementación de esta tecnología. A continuación, se mencionan los componentes del software y los sensores de red necesarios para recopilar y analizar los datos de la red. Se hace hincapié en la necesidad de sensores para los sistemas operativos Windows, Linux y AIX, así como en los sensores de red de escala en la nube. La analítica de datos y el motor de aprendizaje automático en la solución de analítica de Tetration. Con estos componentes, se pueden identificar patrones y anomalías en el tráfico de red, lo que permite una respuesta más rápida a los problemas.

El algoritmo menciona la posibilidad de utilizar un cluster de analítica o un appliance model en local o en la nube. Por último, se hace referencia a la generación de metadatos para cada paquete, que se pueden visualizar mediante diferentes métodos, como el open access, la web, la API Rest y el bus de eventos.

Explicación Detallada del Funcionamiento de la Solución Implementada

Figura 7

Instalación Cluster Tetration

Nota. En la foto se puede apreciar el Cluster Tetration-M 8(RU) compuesto por seis servidores y dos conmutadores de plataforma Cisco Nexus 9300. Cáceres Saavedra, D. A. (2022). Instalación Cluster Tetration [Fuente propia].

Cisco Tetration Analytics fue implementado para el datacenter de Bancolombia, ubicado en Niquia para unos 2500 servidores ingresa por la IP 10.19.196.4 o por el DNS te-analit.bancoco.corp, su integración se realizó con el LDAP del banco, para los usuarios locales o que no son de banco y son de otro proveedor se genera un usuario local para que puedan acceder esta implementación nace principalmente por el crecimiento exponencial a nivel de servidores y aplicaciones las cuales no se tenía control de cómo funcionaban, con quien se comunica, como disminuir el crecimiento en datacenter y comenzarlo a publicar en la nube, Tetration usa unos agentes que se instalan en los servidores, los cuales envían la metadata y el clúster de Tetration en Niquia consume toda la metada y analiza los flujos usando algoritmos de

inteligencia artificial, bigdata con el fin de conocer esos flujos prediciendo comportamiento de usuarios y aplicaciones.

La arquitectura de Cisco Tetration se basa en: la recopilación de datos a través de agentes, que se dividen en tres clases: software, hardware y RSPAN Netflow, y envían información al clúster. La infraestructura de Tetration cuenta con el Analytics Engine, encargado del análisis de big data y del establecimiento de comportamientos de flujos. Para acceder a la información recopilada, se dispone de un mecanismo de acceso que permite a los usuarios utilizar la interfaz web GUI y REST API para exportar información. Por último, la plataforma de GUI de Cisco Tetration Apps utiliza Python y Scala para determinar la información recopilada.

El modelo implementado fue Cisco Tetration 8RU-M5 el cual admite hasta 5000 servidores y su clúster está compuesto por 6 servidores y 2 Switches Nexus 9300

Tetration ofrece varios casos de uso: gracias a la metadata enviada por los agentes. Esta metadata permite establecer políticas de comunicación, definir con qué aplicaciones se puede hablar y establecer el comportamiento de tráfico. Además, Tetration es capaz de generar políticas automáticamente y detectar vulnerabilidades de software en el servidor. También proporciona información sobre el rendimiento de la red y retiene datos históricos durante más de 3 meses. Por último, Tetration es útil en el proceso de inventario.

Tipos de agentes, actualmente Bancolombia tiene los siguientes servidores: Windows, Linux, AIX-ALPHA, ERSPAN, Netflow, los agentes que se usaron en la implementación son Deep Visibility un software se descarga de la misma herramienta de Tetration, un paquete MSI que se instala en los servidores y levanta un servicio llamado TNG, el cual da la información de vulnerabilidades, metadatos , procesamiento, memoria, es el mayor agente en Tetration, esta para

Windows Linux y AIX, por script también se puede instalar, el agente está restringido para que solo use un 3% de la CPU en los servidores

Implementados: W**i**ndows (server, 2012, 2008, 2016,2019) (datacenter, essential, R2standard, Enterprise); Linux (RedHat, Oracle); AIX (7.1, 7.2)

Anottation: es la base de datos de información de cliente y Tetration cuando se creó la implementación se definieron ciertas capas: ambiente (certificación, producción desarrollo o preproductivo), ámbito (son los scopes o árboles que se definen en Tetration para agrupar cierta información), aplicación, (bizagi, SUCVP, SUCVE), bloque de red, capa de aplicación, DNS, Hostname, Interfaz de red, ubicación, inactive.

Scopes: sirven para un filtro de inventario, lo que hace como tal es agrupar todos los dispositivos de la misma familia, agrupa las IPs

ADM: ver cómo está la aplicación, por ejemplo, si te piden alguna ayuda de cómo está la aplicación Wolf,

Tetration tiene visibilidad dentro y fuera del punto final como del tráfico que fluye a través de la red, nos brinda algunas capacidades de análisis forense; Tetration puede alarmar cuando ve un comando que nunca había visto, ataques de canal lateral, fusiones, etc. Puedo crear alertas específicas para ciertos eventos o alertas más amplias en la configuración forense, iniciar un análisis para un día, hora o rango determinado también filtrar en función de una selección de tipos de eventos.

En las siguientes imágenes se puede observar la Interfaz Gráfica de Usuario (por sus siglas en inglés Graphical User Interface (GUI), de la solución de Cisco Tetration. Al explorar los distintos módulos de la plataforma, pudimos realizar una validación detallada y obtener información valiosa sobre el comportamiento de la red. Gracias a esta herramienta, logre identificar vulnerabilidades y riesgos potenciales en el datacenter, lo que nos permitió mejorar la seguridad y protección de la red. Los diferentes módulos nos ayudaron a obtener información clara y precisa, lo que facilitó la toma de decisiones y la implementación de soluciones efectivas:

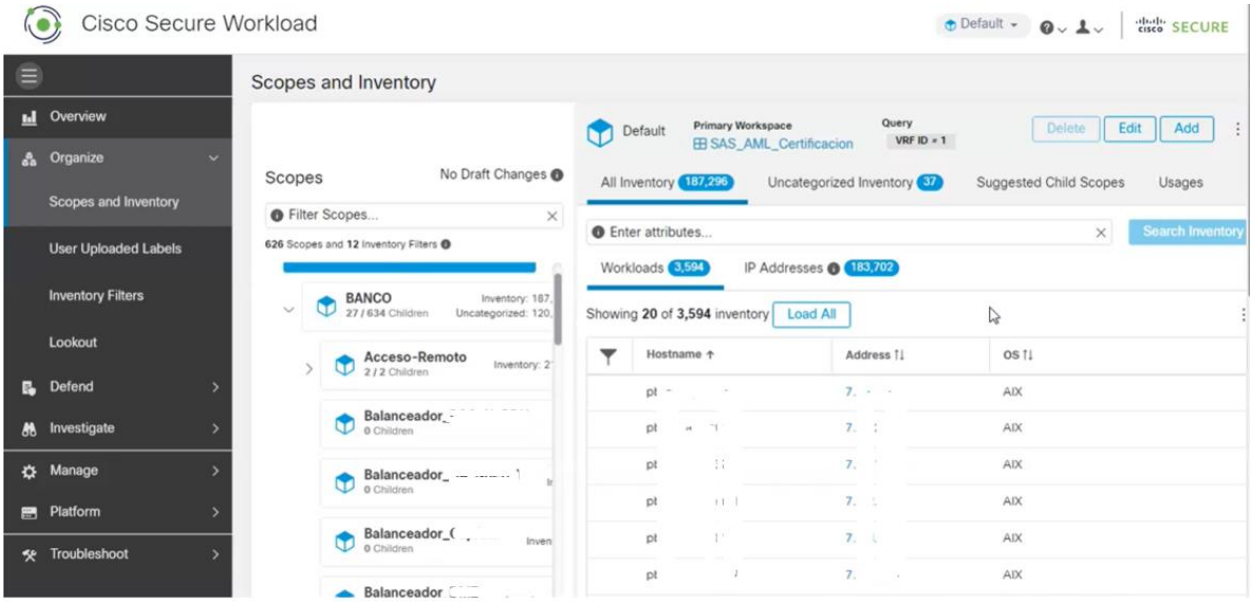
Figura 8

Scope Security Score

Nota. Scope Security Score es una métrica que mide la seguridad de un alcance específico en una organización. Cáceres Saavedra, D. A. (2023). *Scope Security Score* [Fuente propia].

Figura 9

Scope and Inventory

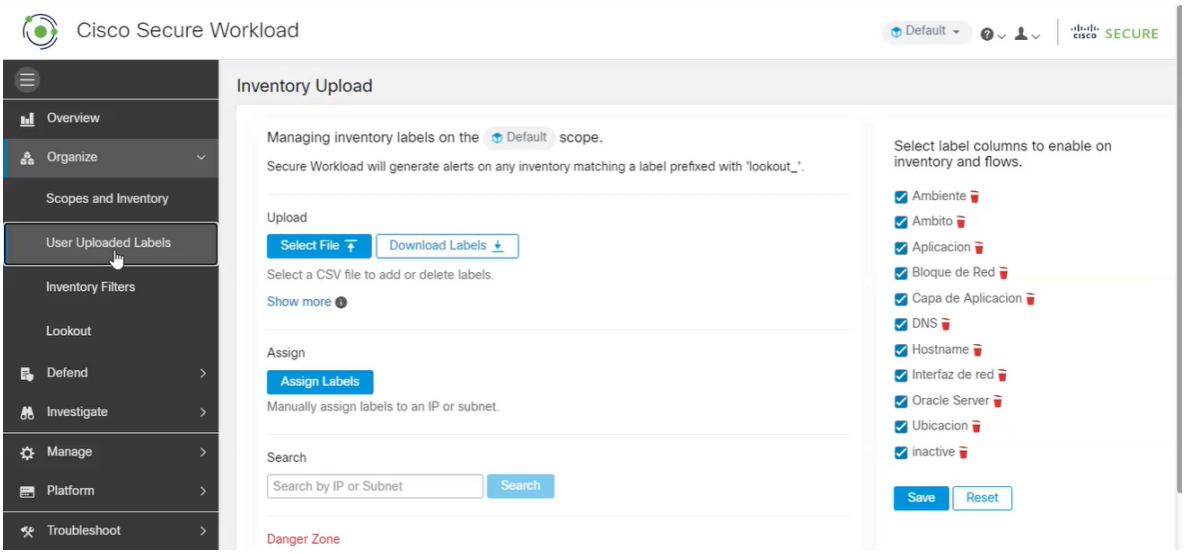


Nota. Scopes and inventory se refiere a la capacidad de la solución de crear y mantener un inventario detallado de los componentes de la infraestructura de TI de una organización.

Cáceres Saavedra, D. A. (2023). *Scope and Inventory* [Fuente propia].

Figura 10

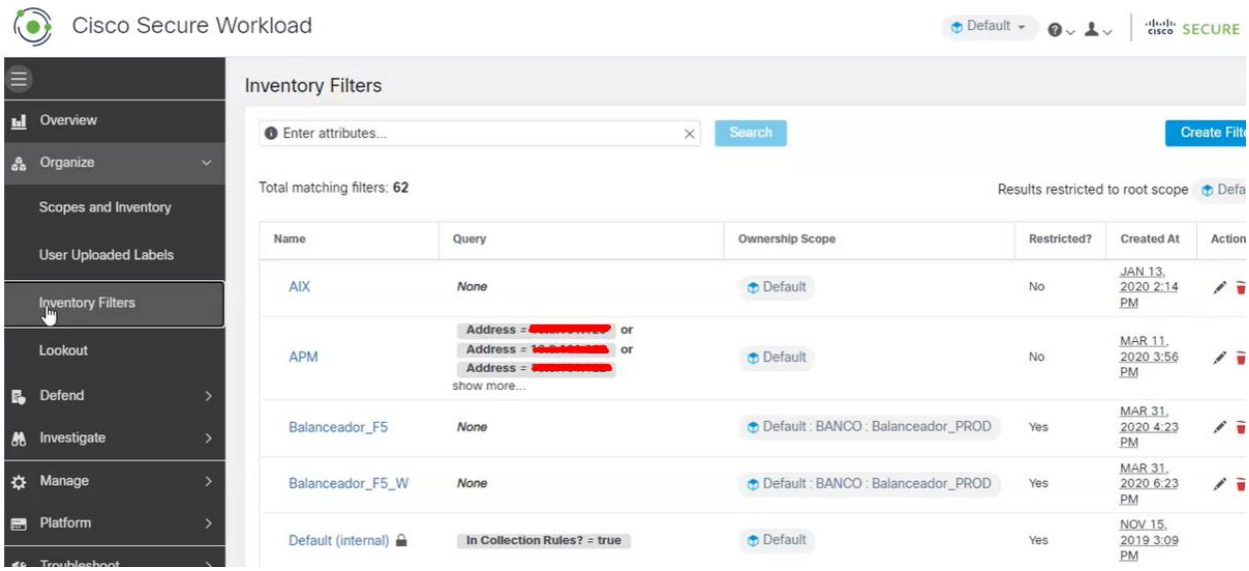
Inventory Upload



Nota. Inventory upload carga o sube un inventario de los recursos de la infraestructura de TI en la plataforma para su gestión y monitoreo. Cáceres Saavedra, D. A. (2023). *Inventory Upload* [Fuente propia].

Figura 11

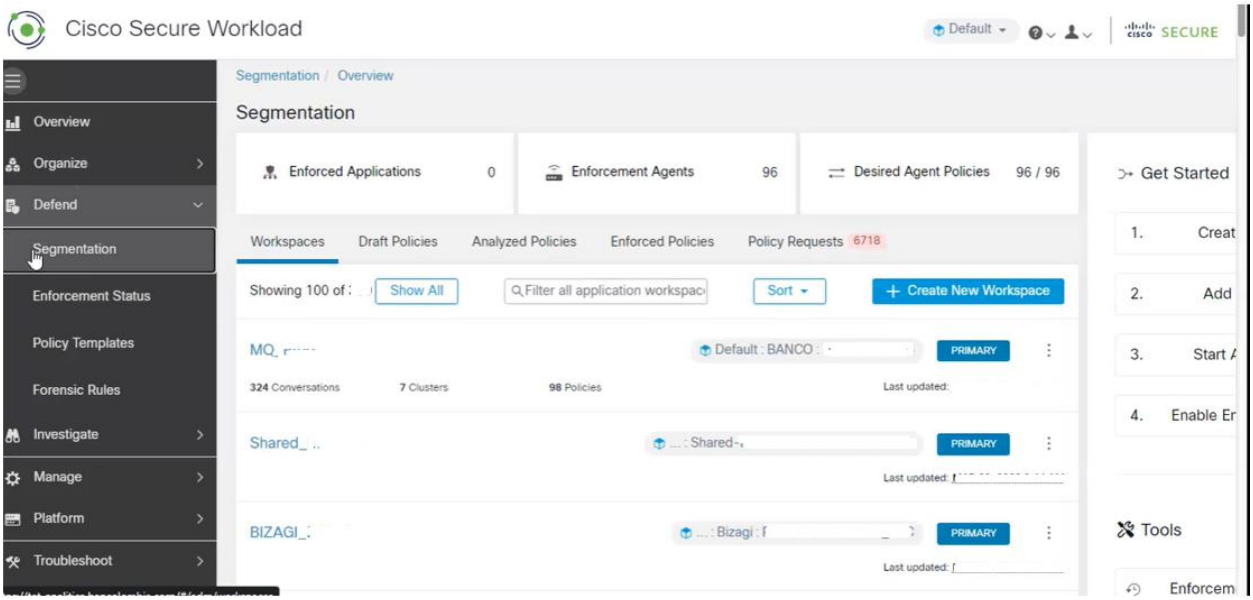
Inventory Filters



Nota. Inventory Filters se refiere a la capacidad de filtrar la información de inventario de recursos de la red en función de ciertos criterios. Cáceres Saavedra, D. A. (2023). *Inventory Filters* [Fuente propia].

Figura 12

Modulo Defend Segmentation

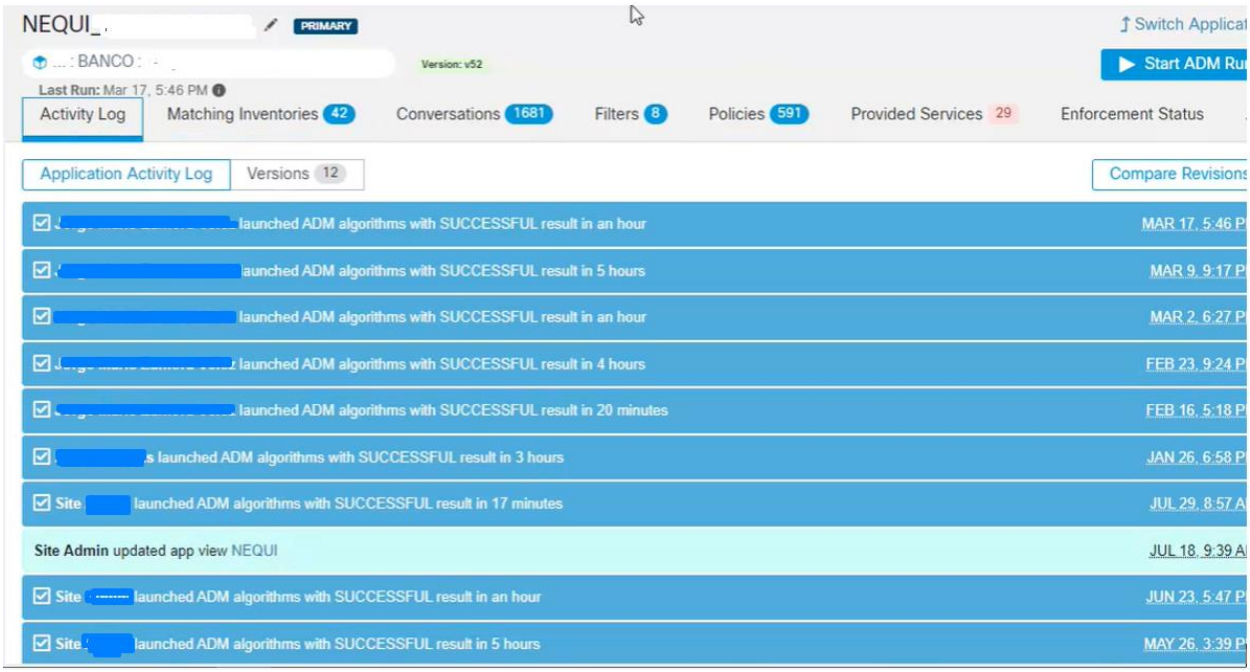


Nota. El módulo Defend tiene la funcionalidad de Segmentación, permite definir y aplicar políticas de seguridad basadas en etiquetas de aplicaciones y microsegmentación. Cáceres Saavedra, D. A. (2023). *Modulo Defend Segmentation* [Fuente propia].

Se toma como ejemplo una de las aplicaciones monitoreadas en este caso Nequi, Dentro del submódulo de segmentación, se pueden crear espacios de trabajo (workspaces. Figura 11) específicos para diferentes aplicaciones o entornos de producción, las aplicaciones están indicadas en la Tabla 14 y Tabla 15. Por ejemplo, en este caso, el workspace "Nequi producción" puede ser utilizado para definir políticas de seguridad específicas para la aplicación Nequi en el entorno de producción.

Figura 13

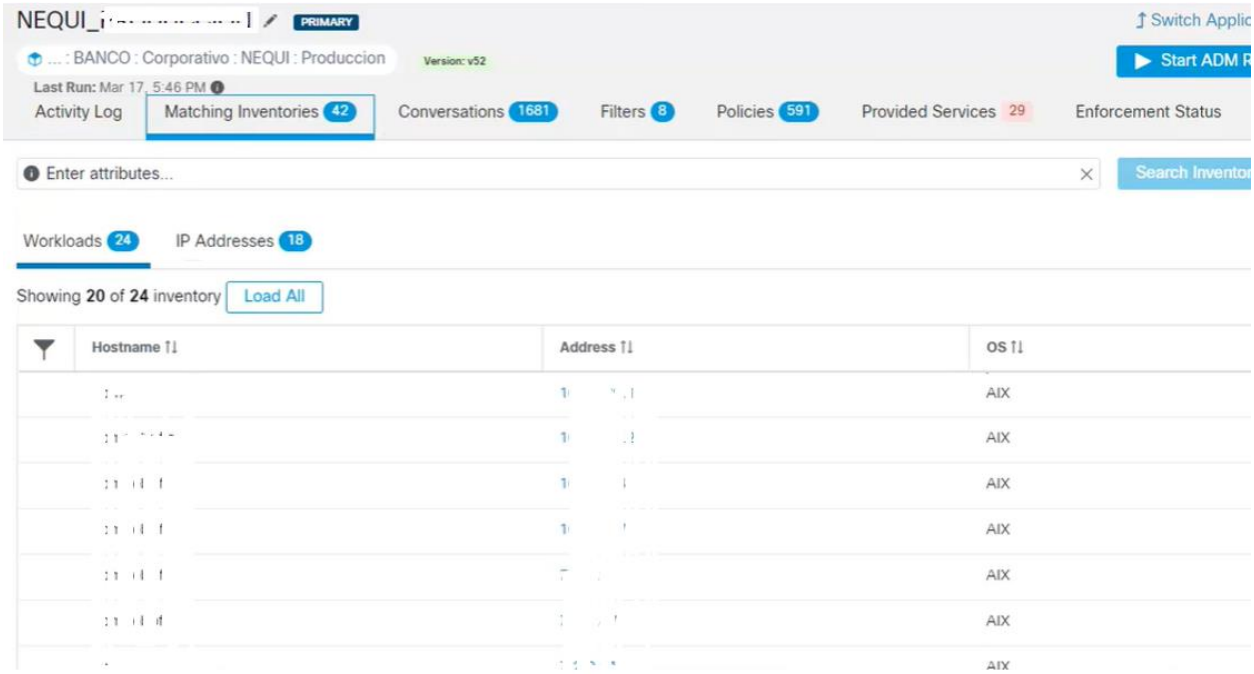
Modulo Defend Segmentation; Aplicación Nequi, Activity Log



Nota. Activity Log se refiere a un registro de actividades en la plataforma que proporciona información sobre las operaciones y eventos que ocurren en el sistema. Cáceres Saavedra, D. A. (2023). *Modulo Defend Segmentation; Aplicación Nequi, Activity Log* [Fuente propia].

Figura 14

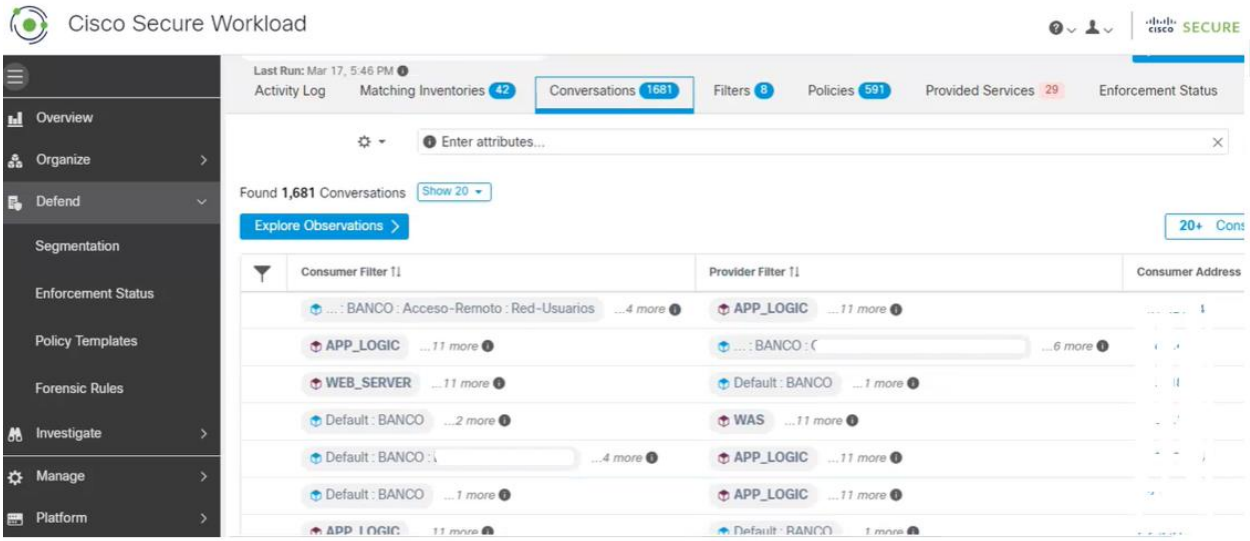
Modulo Defend Segmentation; Aplicación Nequi, Matching Inventories



Nota. Matching Inventories se refiere a la función de comparar y contrastar los inventarios de la red con las políticas de segmentación implementadas. Cáceres Saavedra, D. A. (2023). *Modulo Defend Segmentation; Aplicación Nequi, Matching Inventories* [Fuente propia].

Figura 15

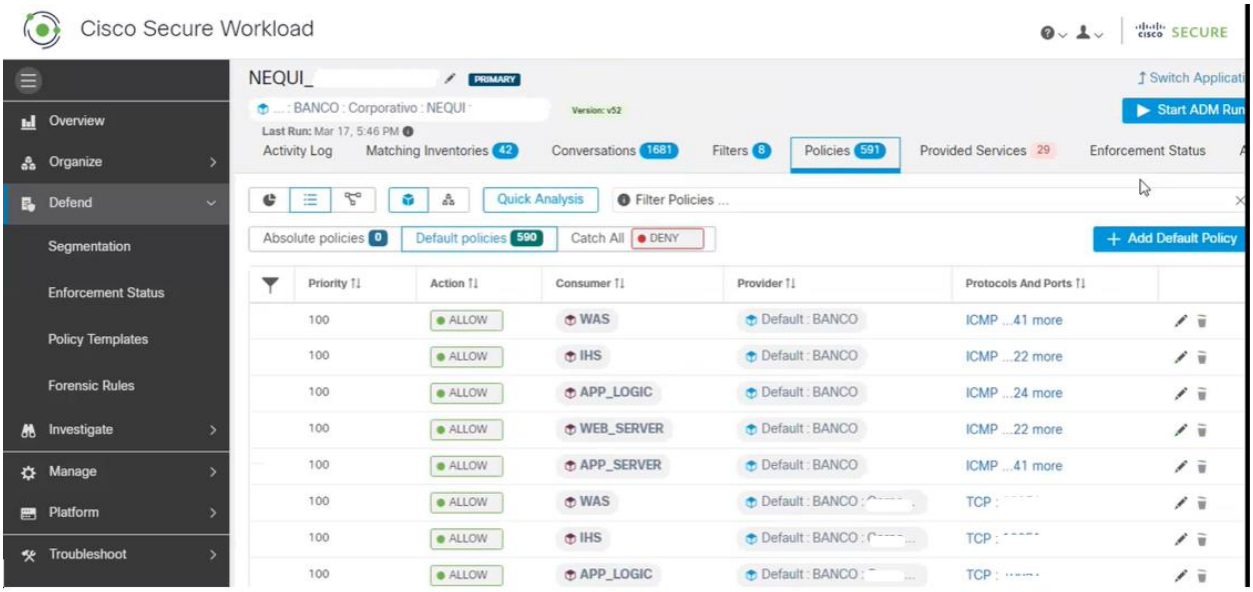
Modulo Defend Segmentation; Aplicación Nequi, Conversations



Nota. Conversations se refiere a los flujos de tráfico entre diferentes dispositivos en una red y cómo se comunican entre sí. Cáceres Saavedra, D. A. (2023). *Modulo Defend Segmentation; Aplicación Nequi, Conversations* [Fuente propia].

Figura 16

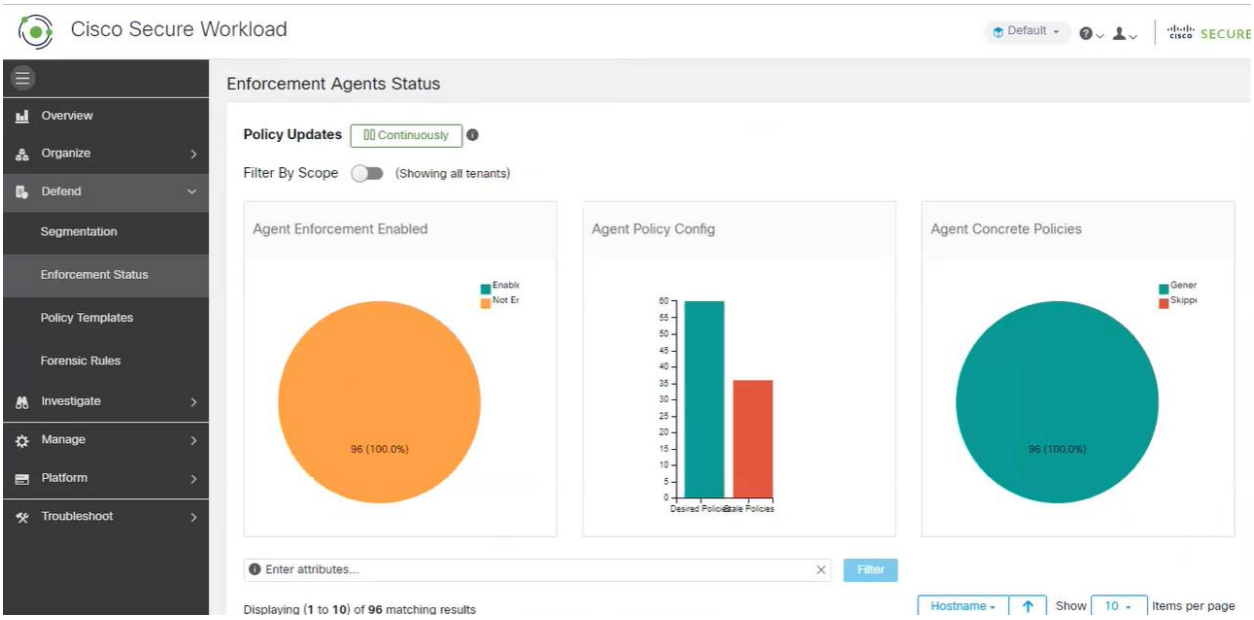
Modulo Defend Segmentation; Aplicación Nequi, policies



Nota. Se pueden establecer políticas de seguridad en la pestaña de "policies" para definir las reglas de acceso permitidas y restringidas para diferentes componentes de la aplicación. Cáceres Saavedra, D. A. (2023). *Modulo Defend Segmentation; Aplicación Nequi, policies* [Fuente propia].

Figura 17

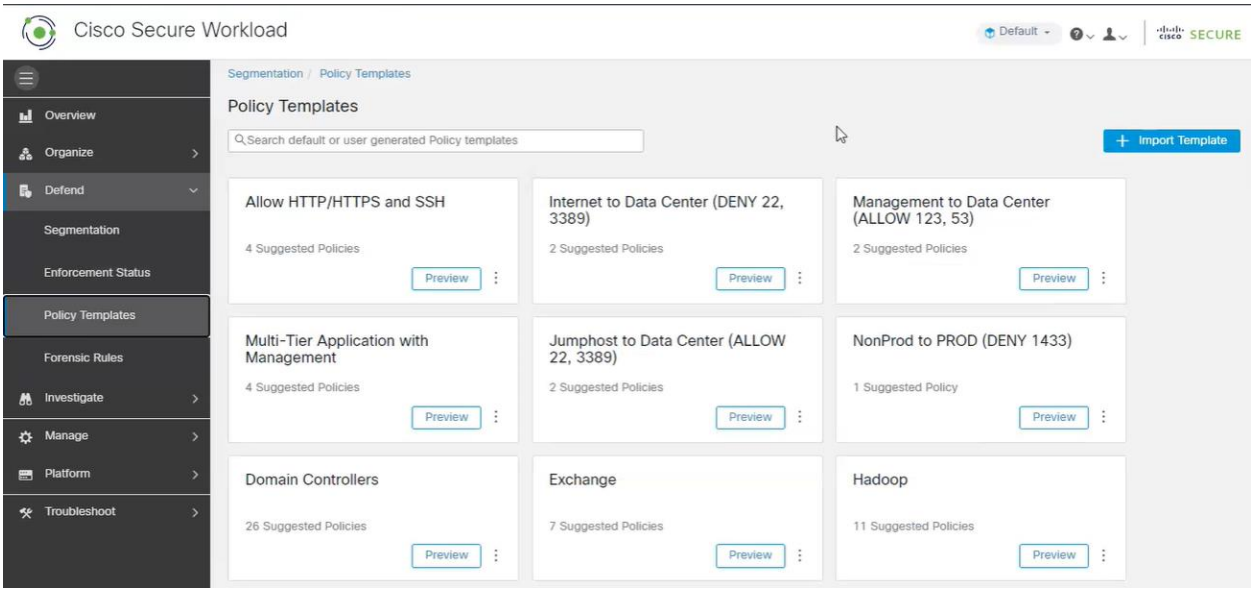
Modulo Defend Enforcement status



Nota. Enforcement Agents Status se refiere al estado de los agentes de cumplimiento de Tetration en la red. Cáceres Saavedra, D. A. (2023). *Modulo Defend Enforcement status* [Fuente propia].

Figura 18

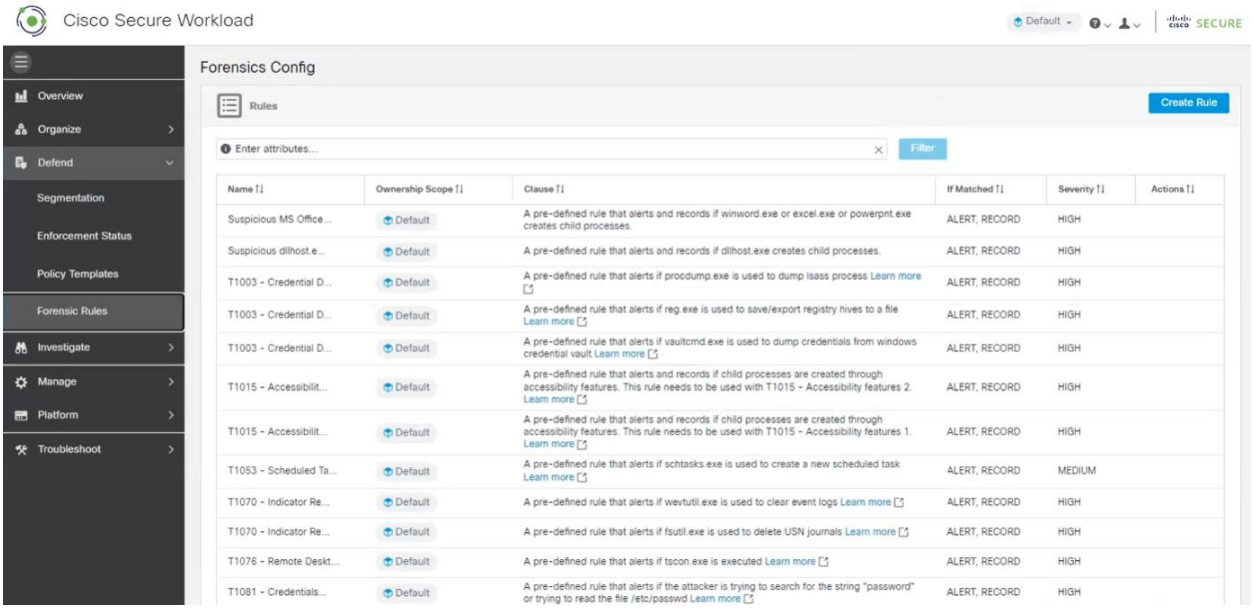
Modulo Policy Templates



Nota. El módulo de Policy templates permite crear plantillas predefinidas de políticas de seguridad para aplicarlas de manera consistente en diferentes workspaces. Cáceres Saavedra, D. A. (2023). *Modulo Policy Templates* [Fuente propia].

Figura 19

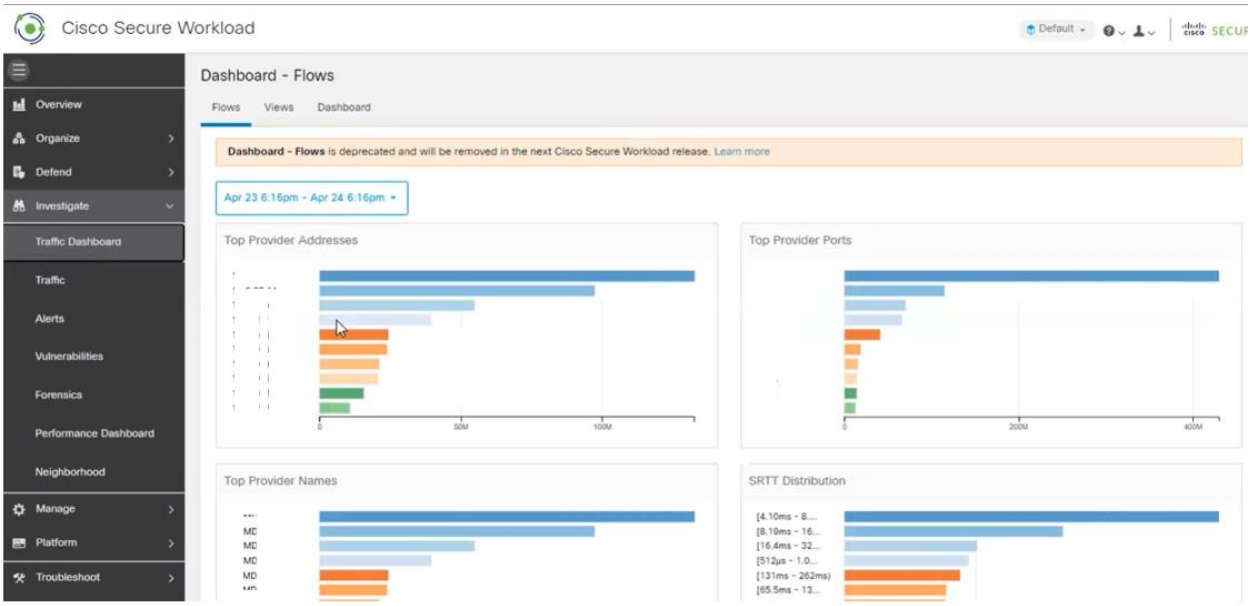
Modulo Forensic Rules



Nota. El módulo Forensic Rules se refiere a las reglas que se pueden aplicar para recopilar datos y llevar a cabo investigaciones forenses en caso de que se produzca un incidente de seguridad. C. (s. (s/f). security-policy-enforcement-forensics. https://www.cisco.com/c/en/us/products/security/tetration-analytics/security-policy-enforcement-forensics.html

Figura 20

Modulo Investigate Traffic Dashboard



Nota. El módulo investigate en la plataforma de Cisco Tetration Analytics permite analizar el tráfico de red detalladamente para obtener información importante acerca del comportamiento de las aplicaciones y los usuarios en la red. Cisco. (s.f.). Investigate: Traffic Dashboard. https://www.cisco.com/c/en/us/td/docs/security/tetration-analytics/investigate-user-guide/traffic-dashboard.html

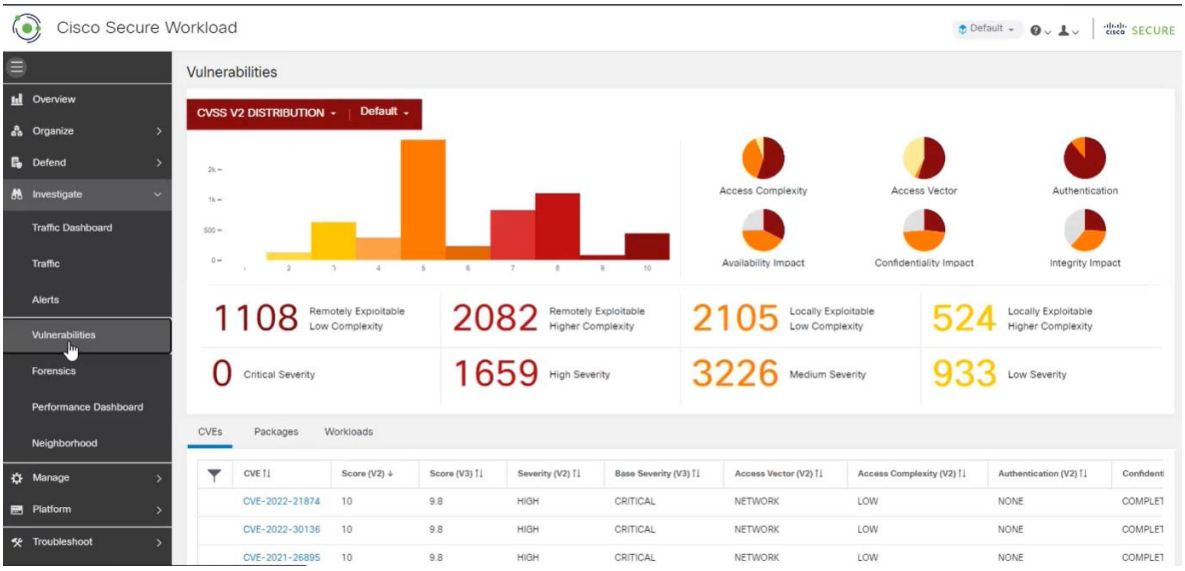
Figura 21

Modulo Investigate; Traffic, Flow Search

Nota. El módulo flow search permite realizar búsquedas de tráfico específicas en la red, filtrando por diferentes criterios como la dirección IP de origen y destino, el puerto utilizado, el protocolo, el tiempo, entre otros. Cáceres Saavedra, D. A. (2023). *Modulo Investigate; Traffic, Flow Search* [Fuente propia].

Figura 22

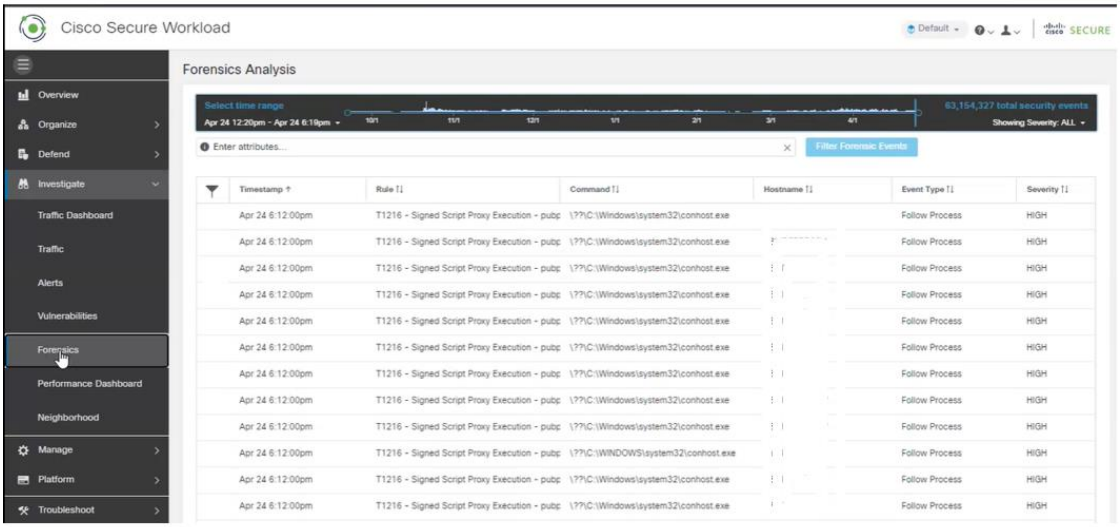
Modulo Investigate; Vulnerabilities



Nota. El módulo Vulnerabilities detecta y analiza las vulnerabilidades en la infraestructura de la red. Cáceres Saavedra, D. A. (2023). *Modulo Investigate; Vulnerabilities* [Fuente propia].

Figura 23

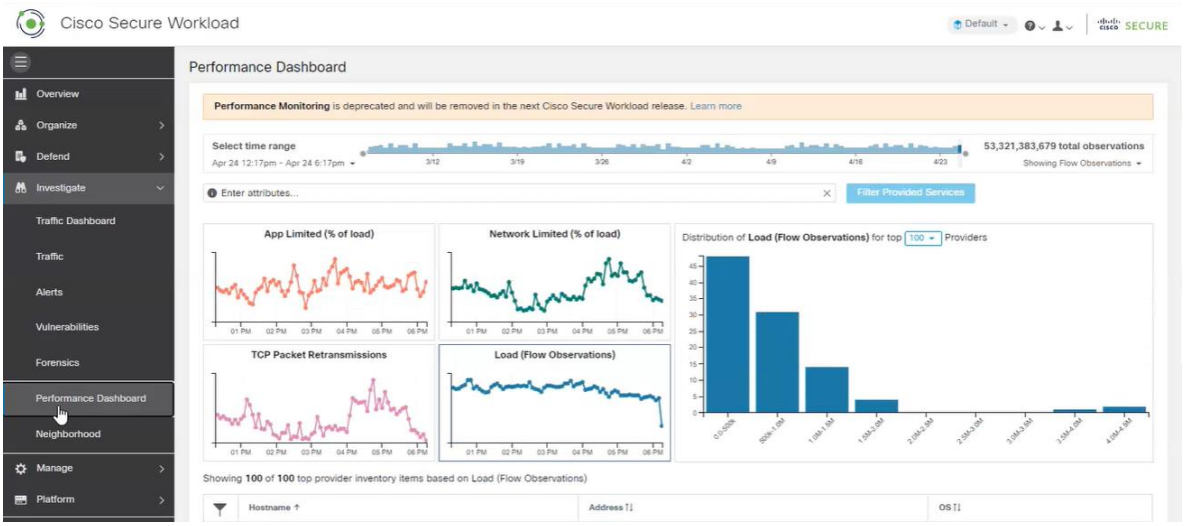
Modulo Investigate; Forensics



Nota. El módulo Forensics permite la identificación y el análisis de incidentes de seguridad en la red mediante la recopilación y correlación de información de diferentes fuentes. Cisco. (s.f.). Security and Policy Enforcement: Forensics. https://www.cisco.com/c/en/us/products/security/tetration-analytics/security-policy-enforcement-forensics.html

Figura 24

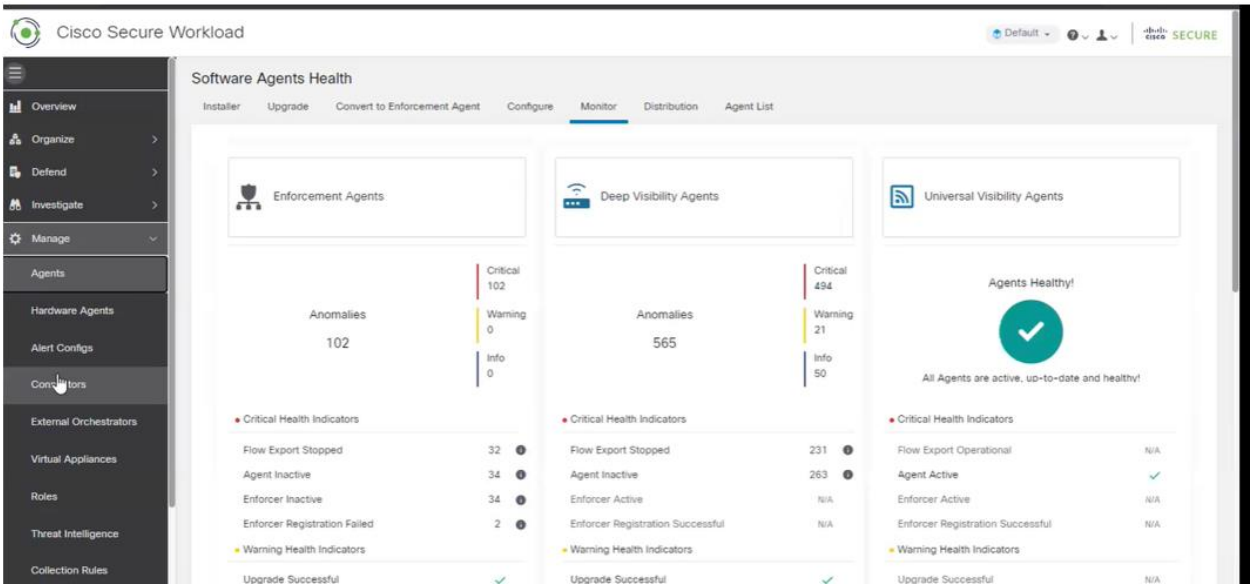
Modulo Investigate; Performance Dashboard



Nota. Performance Dashboard en la plataforma es una herramienta de visualización de datos que proporciona información detallada sobre el rendimiento de las aplicaciones en la red. Cáceres Saavedra, D. A. (2023). *Modulo Investigate; Performance Dashboard* [Fuente propia].

Figura 25

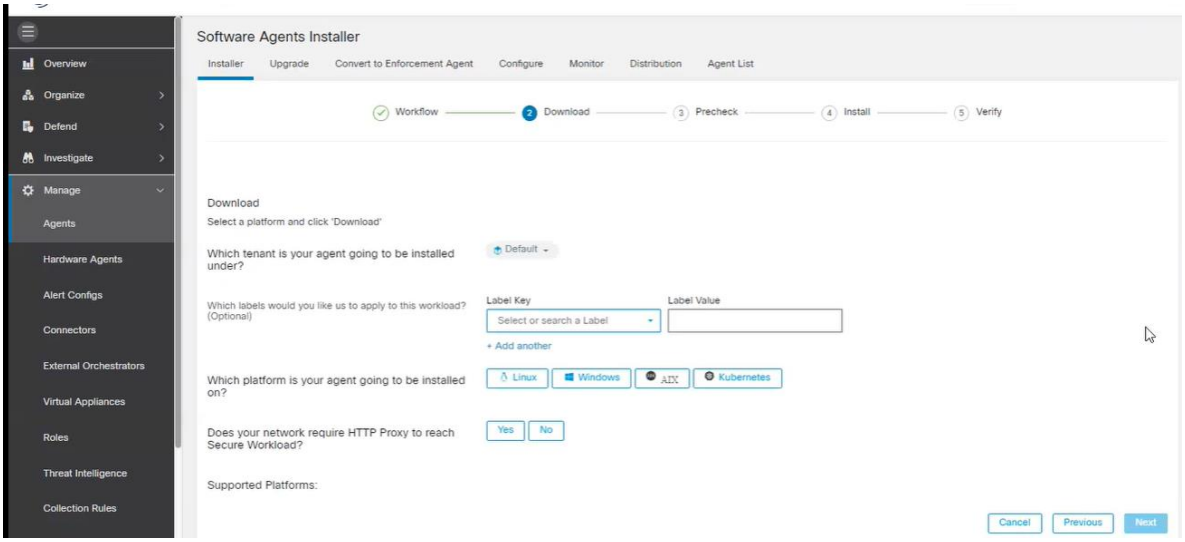
Modulo Manage; Software Agents Health



Nota. El módulo Software Agents Health se encarga de monitorear el estado y la salud de los agentes de software que se han instalado en los servidores de la red. Cáceres Saavedra, D. A. (2023). *Modulo Manage; Software Agents Health* [Fuente propia].

Figura 26

Modulo Manage; Software Agents Installer

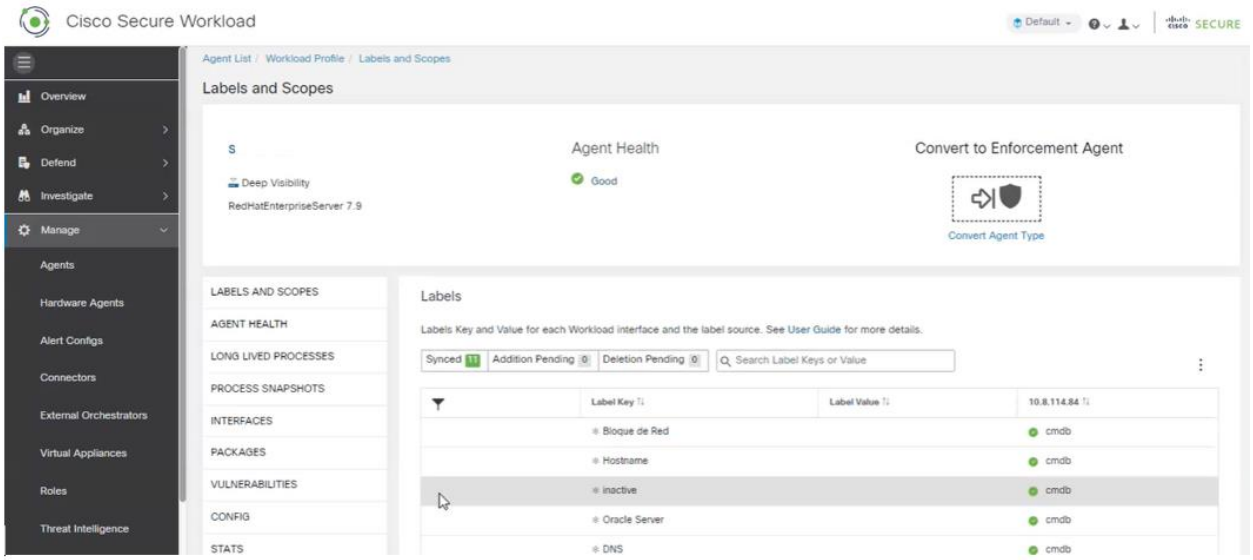


Nota. El módulo software agents installer permite instalar los agentes de software en los dispositivos de la red para recopilar información y enviarla al sistema de Tetration. Cisco. (s.f.). Software Agent Installation. https://www.cisco.com/c/en/us/td/docs/security/tetration/tetration-analytics/sw-install.html

Después de explorar los módulos de la plataforma, se identificaron vulnerabilidades y riesgos en la red y se tomaron medidas para mejorar la seguridad, como la implementación de políticas de acceso, configuración de firewalls y actualización de software. Se establecieron protocolos de monitoreo proactivo y seguimiento de alarmas para detectar y solucionar posibles fallas o intrusiones en tiempo real. Todo esto permitió mejorar la seguridad de la red significativamente. Las figuras ilustran cómo se utilizan los módulos para llevar a cabo estas mejoras y obtener información valiosa del comportamiento de la red. Se utiliza un servidor con el agente Tetration instalado como ejemplo para obtener información precisa del comportamiento.

Figura 27

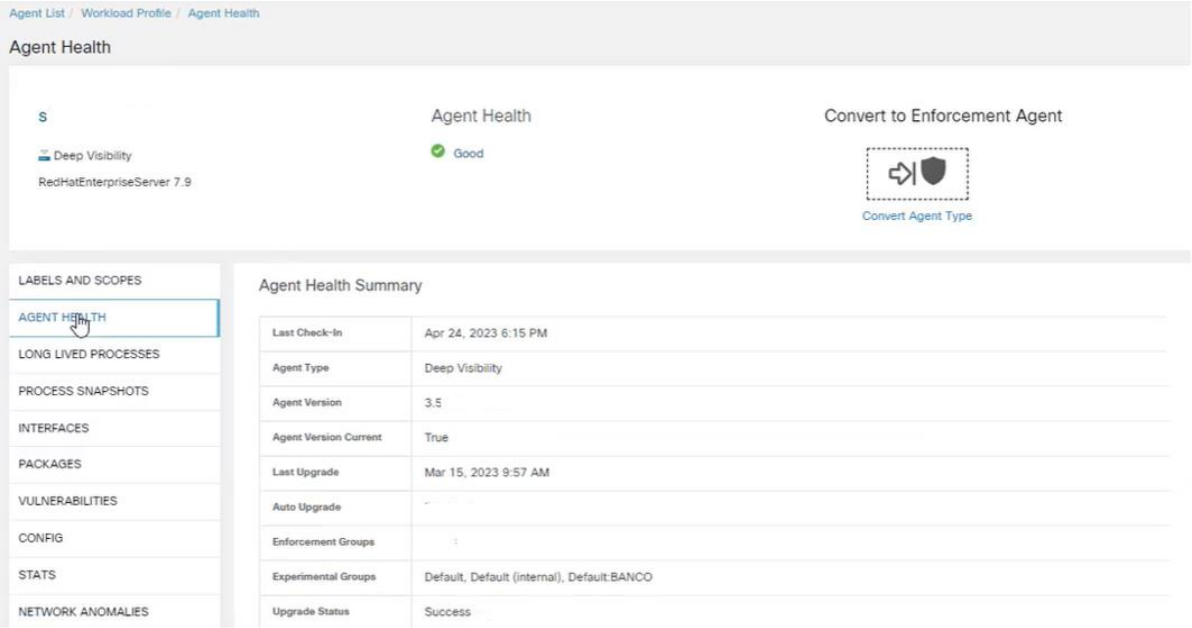
Modulo Agent list, Wordload Profile; Labels and Scopes



Nota. Labels and Scopes permite asignar etiquetas (labels) a los diferentes recursos de la red y agruparlos en conjuntos llamados scopes. Cáceres Saavedra, D. A. (2023). *Modulo Agent list, Wordload Profile; Labels and Scopes* [Fuente propia].

Figura 28

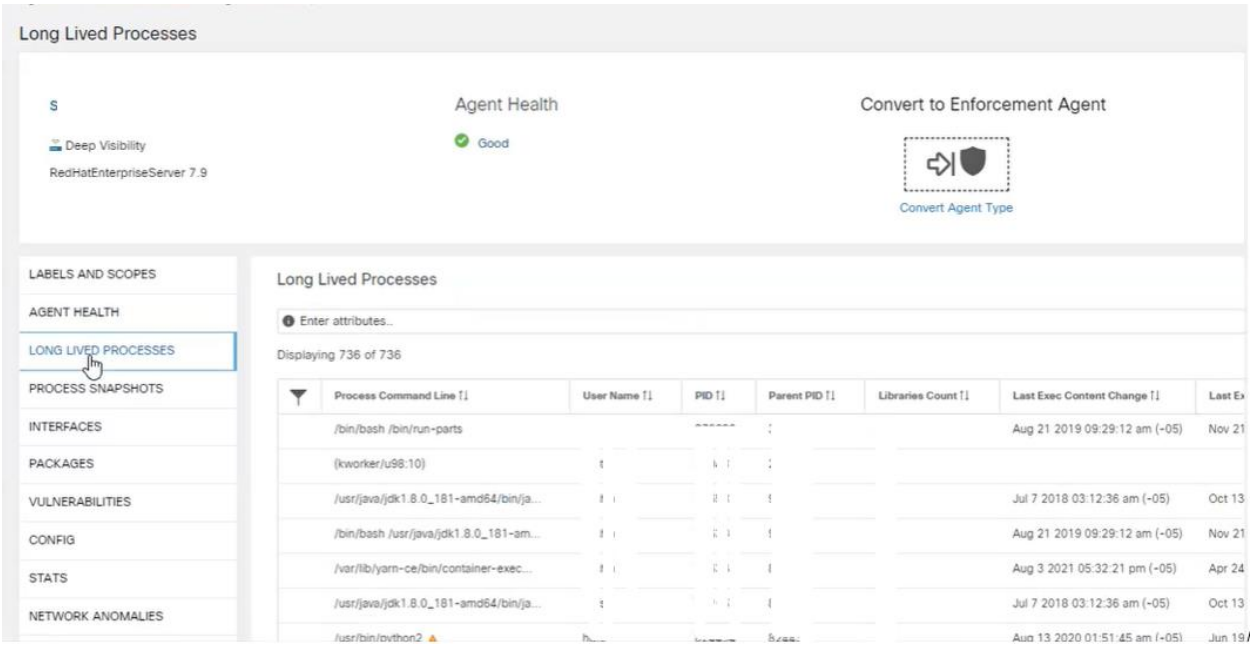
Modulo Agent list, Wordload Profile; Agent Health



Nota. Agent health monitorea el estado de los agentes instalados en los servidores para asegurarse de que estén funcionando correctamente. Cáceres Saavedra, D. A. (2023). *Modulo Agent list, Wordload Profile; Agent Health* [Fuente propia].

Figura 29

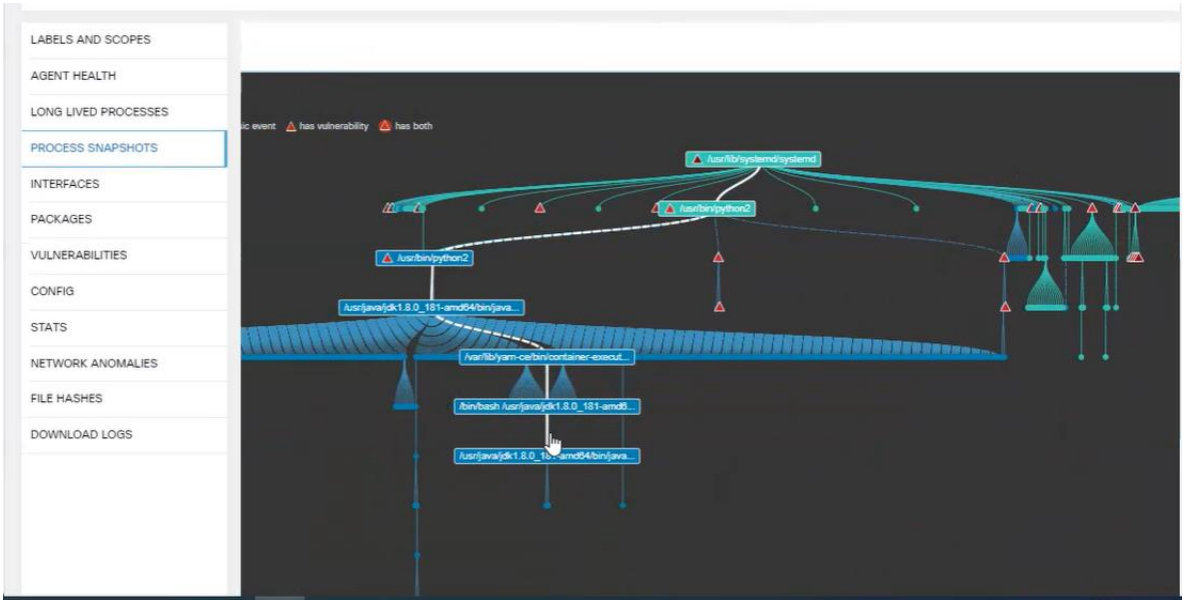
Modulo Agent list, Wordload Profile; Long Lives Processes



Nota. Long Lived Processes permite identificar y monitorear los procesos de larga duración en los servidores y su comportamiento. Cáceres Saavedra, D. A. (2023). *Modulo Agent list, Wordload Profile; Long Lives Processes* [Fuente propia].

Figura 30

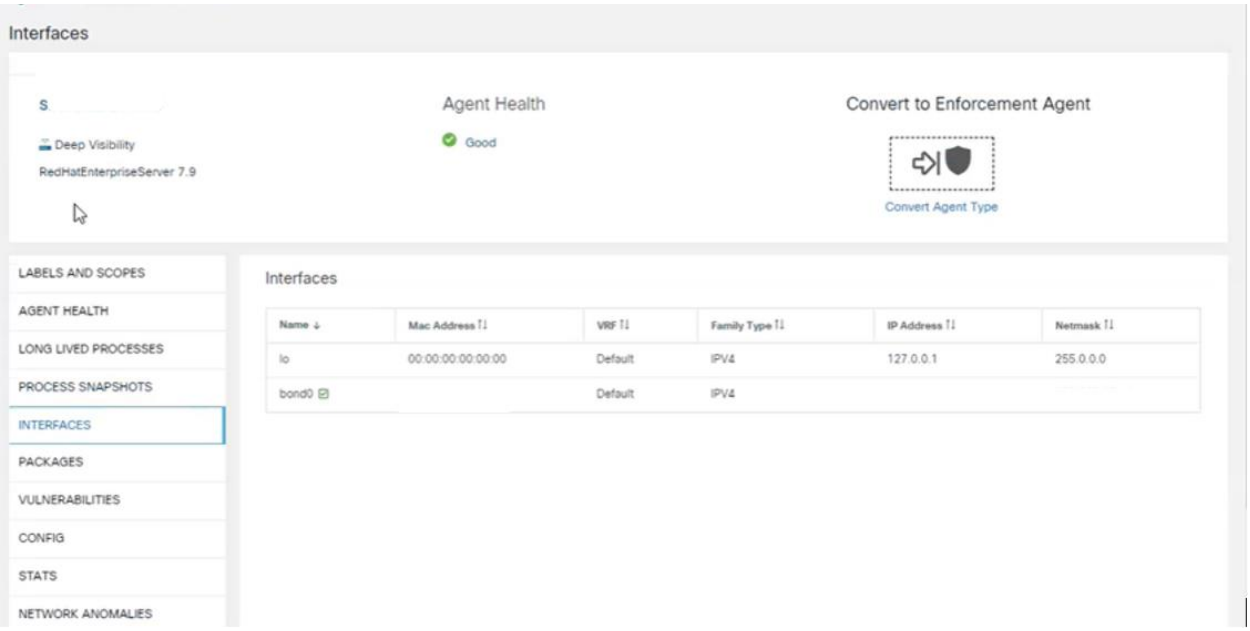
Modulo Agent list, Wordload Profile; Process snapshots



Nota. Process Snapshots permite obtener información detallada sobre los procesos que se están ejecutando en un servidor en tiempo real. Cisco. (s.f.). Cisco Tetration Analytics - Solution Overview. https://www.cisco.com/c/en/us/products/security/tetration-analytics/index.html#~why-choose-tetration-analytics.

Figura 31

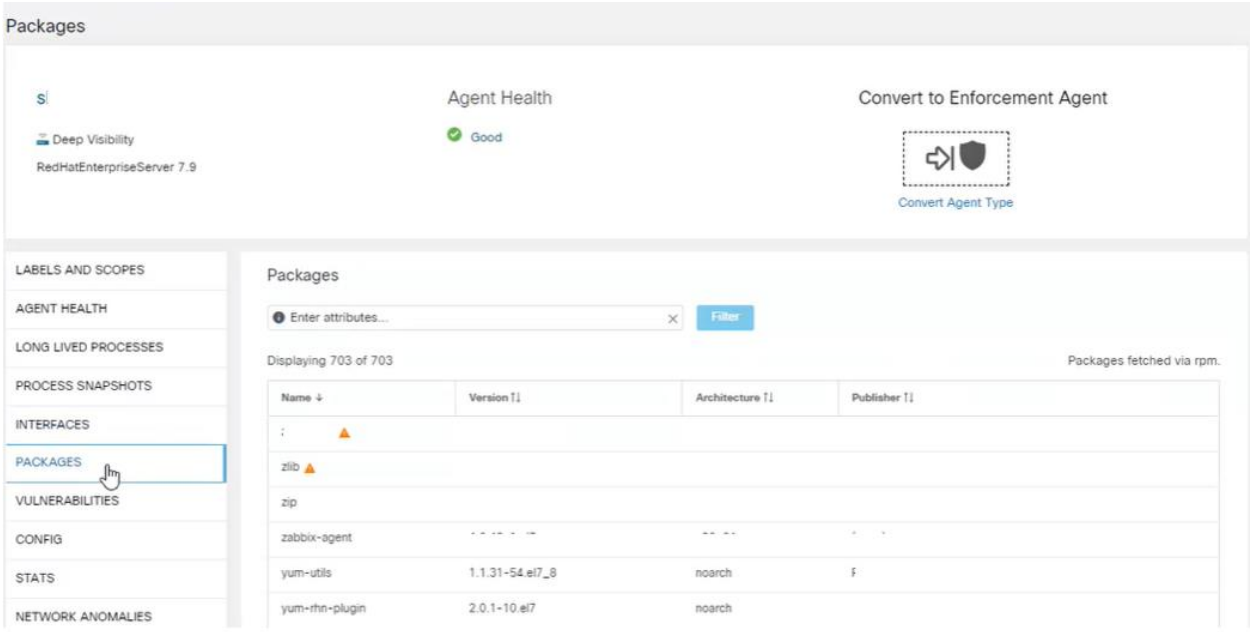
Modulo Agent list, Wordload Profile; Interfaces



Nota. El módulo Interfaces proporciona información detallada sobre los interfaces de red de los dispositivos de la red. Cáceres Saavedra, D. A. (2023). *Modulo Agent list, Wordload Profile; Interfaces* [Fuente propia].

Figura 32

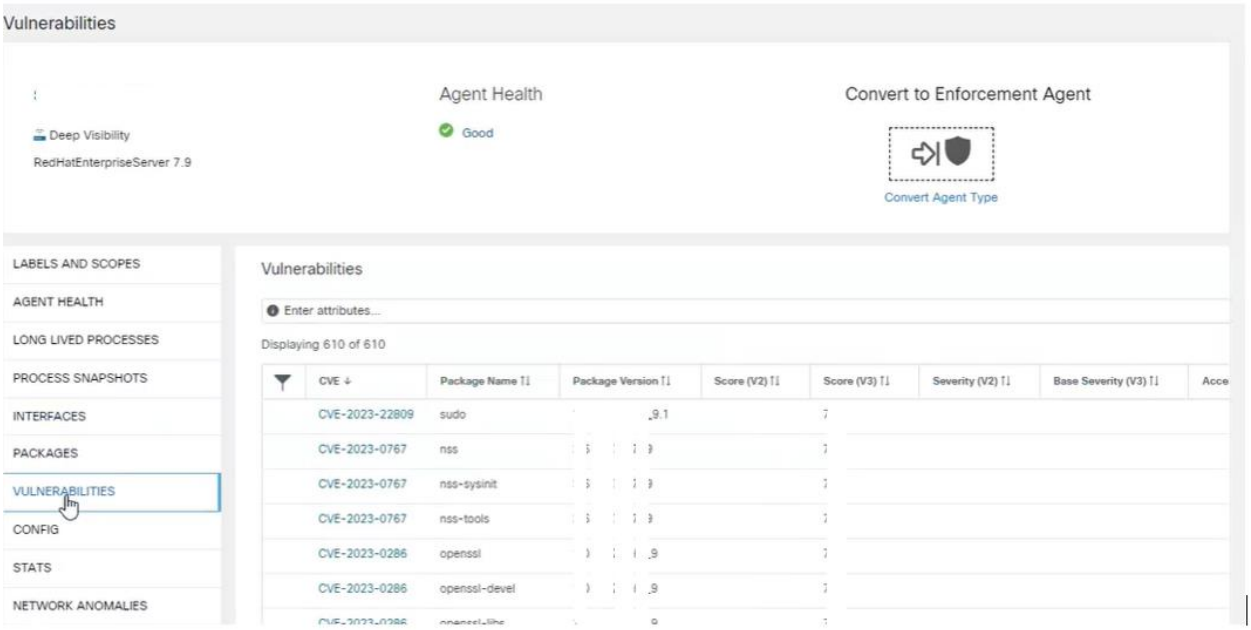
Modulo Agent list, Wordload Profile; Packages



Nota. Packages se refiere a la gestión de paquetes de software en la red. Este módulo permite realizar un seguimiento de los paquetes de software que están instalados en los servidores y dispositivos de red en tiempo real. Cisco. (s.f.). Cisco Tetration Analytics. https://www.cisco.com/c/en/us/products/security/tetration-analytics/index.html

Figura 33

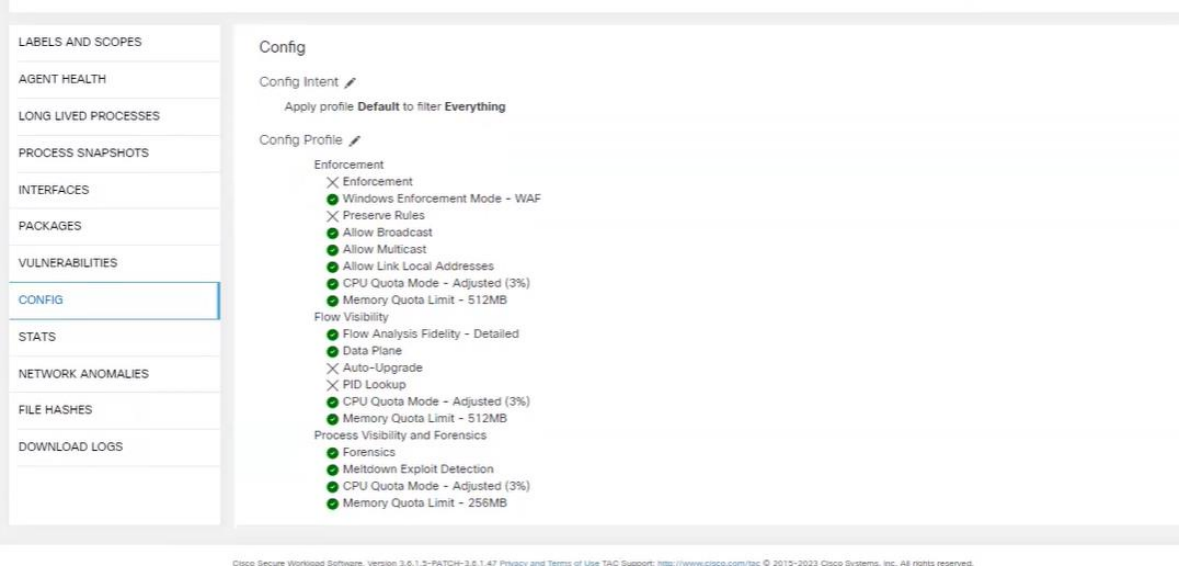
Modulo Agent list, Wordload Profile; Vulnerabilities



Nota. Vulnerabilities se encarga de realizar análisis de vulnerabilidades en los paquetes de software instalados en el servidor monitoreado. Cáceres Saavedra, D. A. (2023). *Modulo Agent list, Wordload Profile; Vulnerabilities* [Fuente propia].

Figura 34

Modulo Agent list; Wordload Profile; Config



Nota. Config permite visualizar la configuración de los dispositivos de red en la red. Con este módulo se puede tener una visión general de la configuración de los dispositivos. Cáceres Saavedra, D. A. (2023). *Modulo Agent list; Wordload Profile; Config* [Fuente propia].

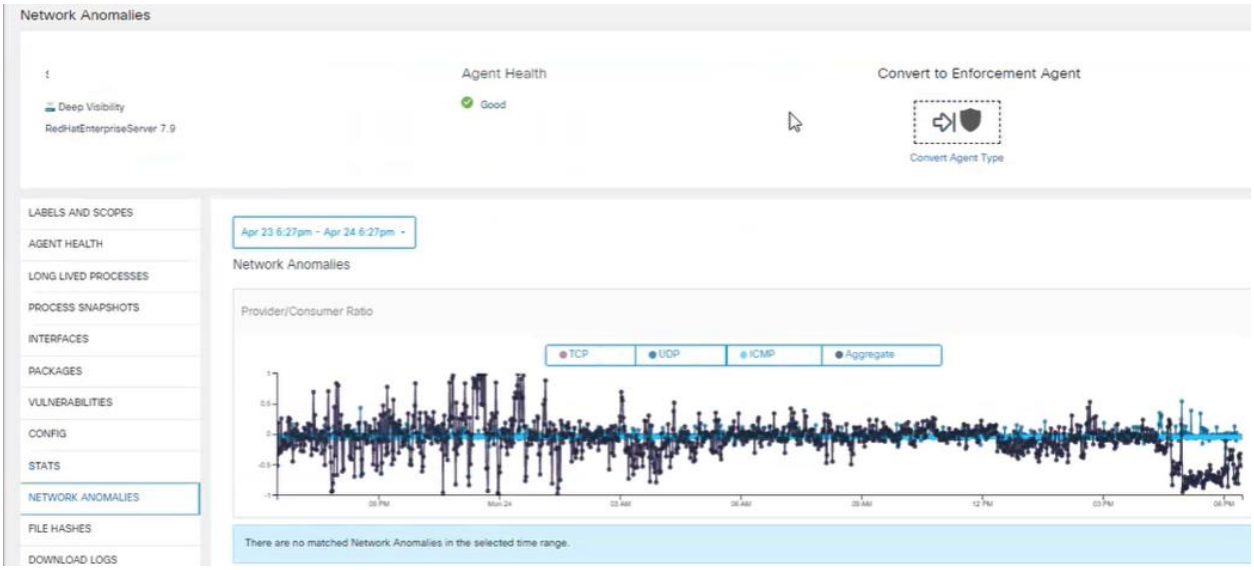
Figura 35

Modulo Agent list; Wordload Profile; Stats

Nota. Stats realiza la recopilación y análisis de datos estadísticos en tiempo real para proporcionar información sobre el rendimiento de los sistemas y la red. Cisco. (2019). Cisco Tetration Analytics - Data Sheet. https://www.cisco.com/c/en/us/products/collateral/security/tetration-analytics/datasheet-c78-741076.html

Figura 36

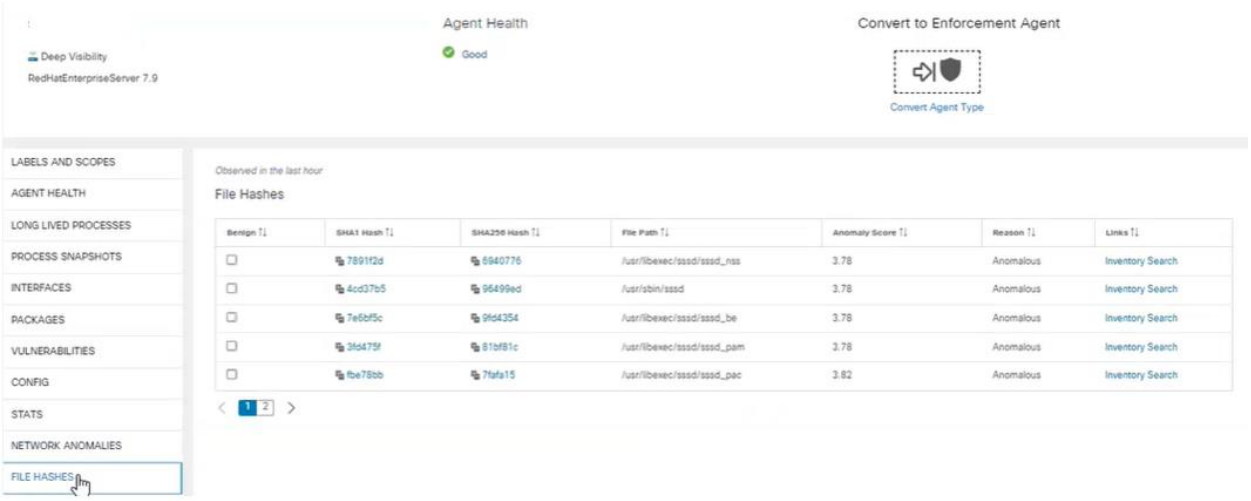
Modulo Agent list; Wordload Profile; Network Anomalies



Nota. Network Anomalies se utiliza para detectar comportamientos anormales en la red. El sistema monitorea el tráfico de la red y genera alertas cuando detecta patrones de tráfico que son inusuales o indican una posible amenaza. Cisco. (2020). Cisco Tetration Analytics: Network Anomalies Module, https://www.cisco.com/c/en/us/products/security/tetration-analytics/network-anomalies.html

Figura 37

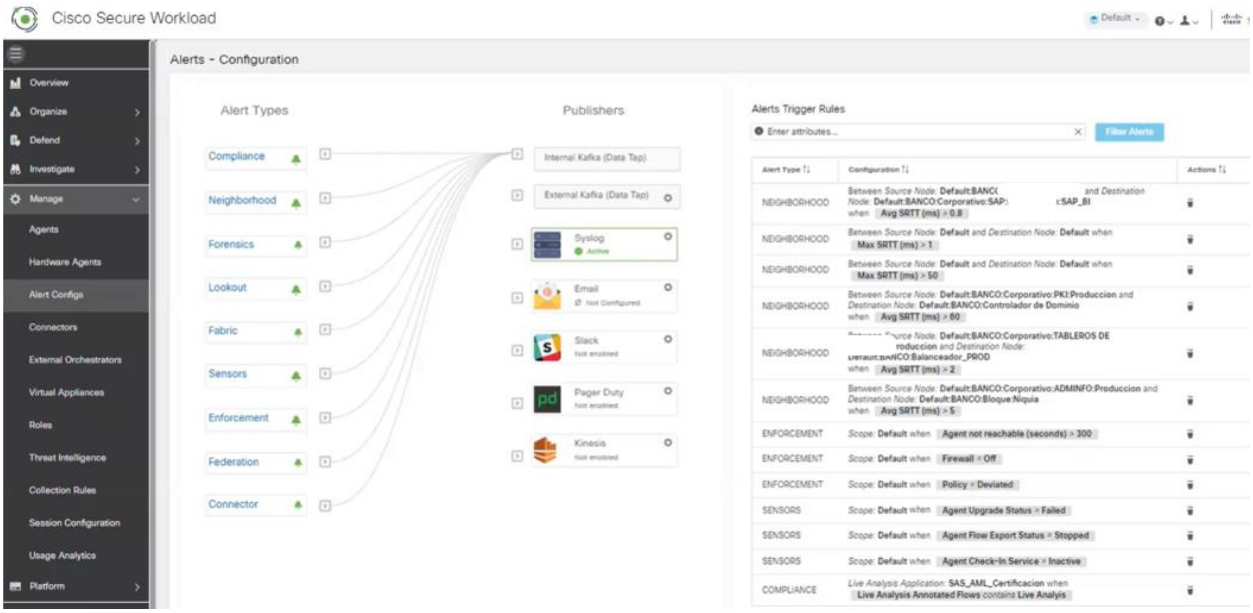
Modulo Agent list; Wordload Profile; File Hashes



Nota. File Hashes realiza la recopilación y análisis de hash de archivos. Este módulo permite detectar la existencia de archivos maliciosos o sospechosos en los sistemas monitoreados y proporciona información detallada sobre ellos. Cáceres Saavedra, D. A. (2023 *Modulo Agent list; Wordload Profile; File Hashes* [Fuente propia].

Figura 38

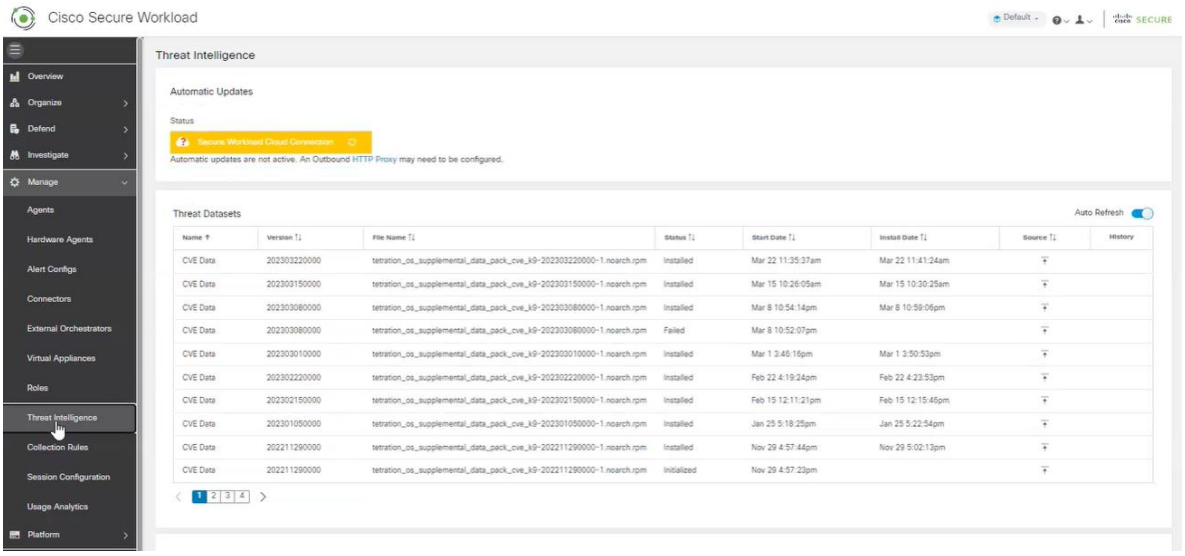
Modulo Manage; Alerts - Configuration



Nota. Alerts - Configuration se refiere a la configuración de las alertas que se generan en la plataforma. Cáceres Saavedra, D. A. (2023). *Modulo Manage; Alerts – Configuration* [Fuente propia].

Figura 39

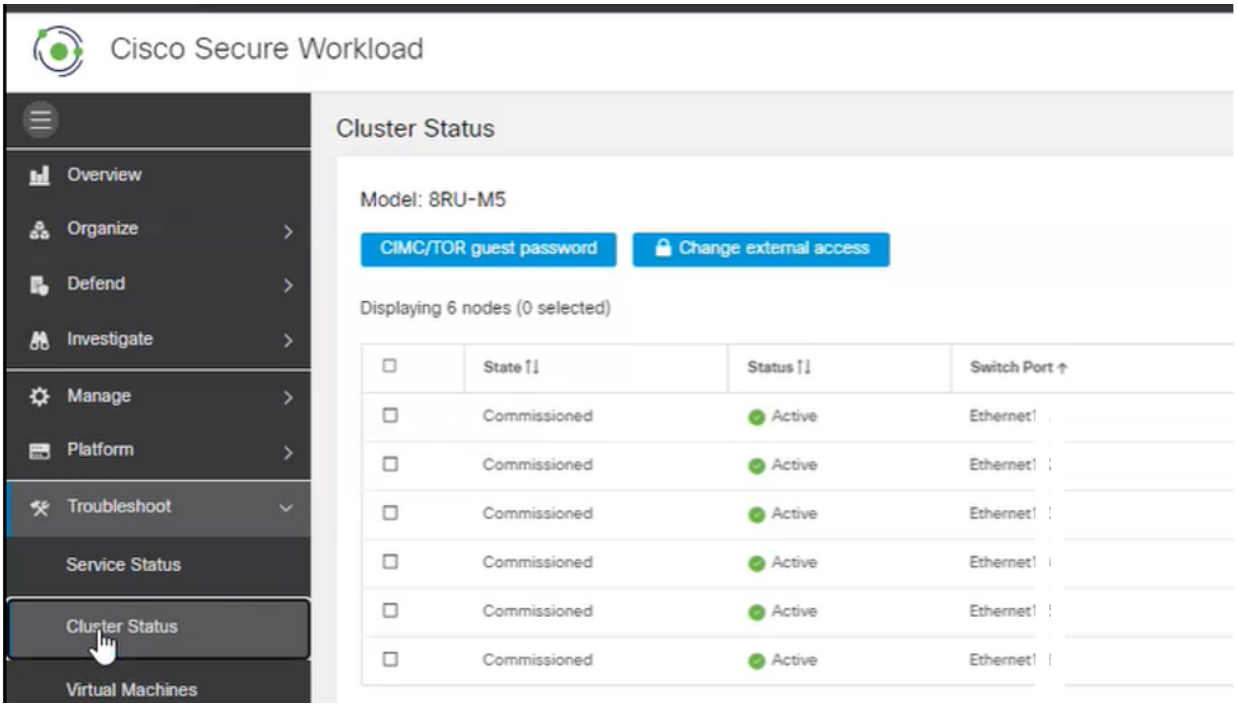
Modulo Manage; Threat intelligence



Nota. Threat Intelligence proporciona una lista de amenazas conocidas y desconocidas para ayudar en la detección y respuesta de amenazas. Cisco. (2021). Cisco Tetration Analytics. https://www.cisco.com/c/en/us/products/security/tetration-analytics/index.html

Figura 40

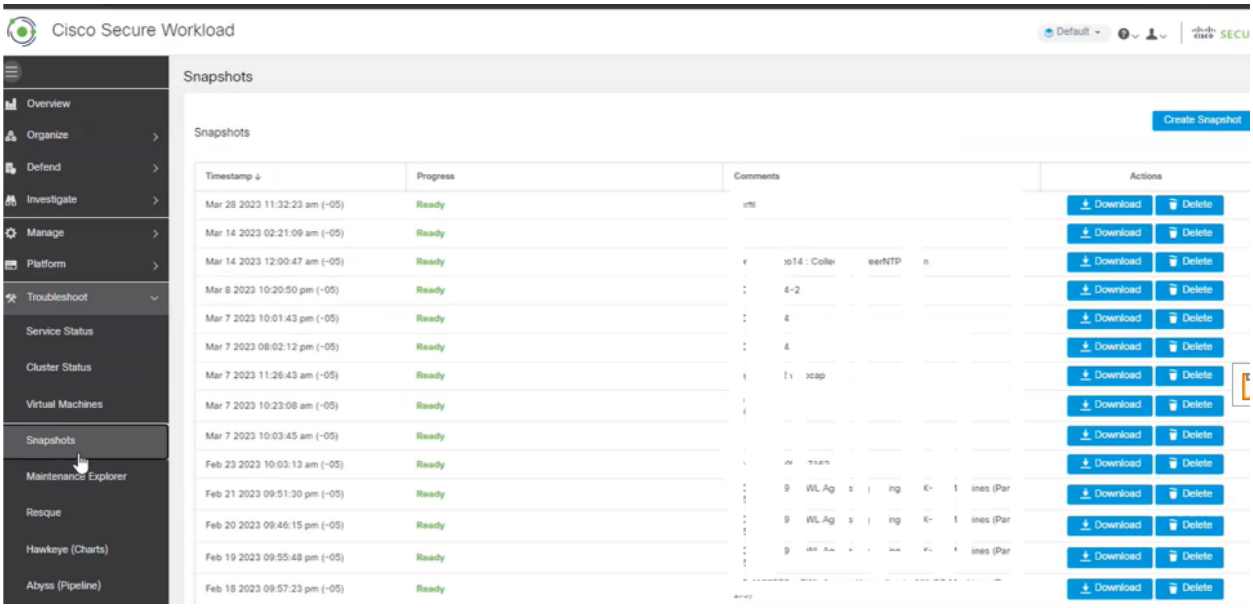
Modulo Troubleshoot; Cluster Status



Nota. Cluster Status proporciona información sobre el estado del clúster, incluyendo información sobre los nodos del clúster, la salud de los servicios del clúster y el uso de recursos. Cáceres Saavedra, D. A. (2023). *Modulo Troubleshoot; Cluster Status* [Fuente propia].

Figura 41

Modulo Troubleshoot; Snapshots



Nota. Snapshots se refiere a la capacidad de la herramienta de capturar información detallada en tiempo real del estado actual de los servidores y aplicaciones que están siendo monitoreados. Cisco. (2019). Cisco Tetration Analytics Data Sheet. https://www.cisco.com/c/en/us/products/collateral/security/tetration-analytics/datasheet-c78-739753.html

Operar la Implementación

Plan de Mejoras

Tetration ofrece transparencia en el entorno de una nube híbrida y puede conectarse con AWS, Microsoft Azure y VMware, Service Now. En cuanto a los métodos de seguridad, Tetration añade lo siguiente:

Localización de vulnerabilidades de software por medio de la combinación de un catálogo de cada uno de los paquetes de software, la versión y la información del editor, y la base de datos de exposición y vulnerabilidades comunes. Tetration detecta paquetes de software con CVE conocidos y desarrolla una puntuación.

Inspección del proceso del servidor. Tetration compila y conserva un catálogo de los métodos que se ejecutan en los servidores por minuto. La información del proceso (ID, parámetros, usuarios, duración y firma) es clave para la seguridad.

Inspección de desvío de referencia. Tetration puede descubrir patrones de conducta que se desvían de la línea de base. Esta conducta desviada puede sobresalir en el aumento de privilegios y ataques en canales secundarios.

Plan de Mejoras a Corto Plazo

Las mejoras vienen por medio de las versiones de software y parches que el proveedor Cisco aprueba una vez se revisan con el TAC. Se comprueban y realizan pruebas para ver que sean las mejores para implementar antes de la instalación, teniendo en cuenta el gran número de servidores que se manejan actualmente.

Plan de Mejoras a Mediano Plazo

Se realizará un monitoreo proactivo de todos los elementos de Tetration, incluyendo los elementos del clúster, y se verificarán las alarmas que se presenten a través de E-solution y Service status de Tetration. En caso de detectar una alarma, se realizará el seguimiento y escalamiento correspondiente. Este plan de mejoras incluirá un soporte directo con el fabricante y atención inmediata en caso de ser necesario, así como el tema de soporte en sitio y mantenimiento programado de los servidores.

Plan de Mantenimiento

Durante esta etapa se realiza todo el tema concerniente a la ejecución de rutinas de Backup, ejecución de carga de software, actualización de agentes, mantenimiento físico del clúster y reinicios programados si se llega a requerir.

Plan de Mantenimiento Correctivo

El equipo de monitoreo está a cargo de verificar cada una de las alarmas que se presenten en el clúster. A su vez, informa al ingeniero encargado de la plataforma, quien dictamina el paso a seguir. En caso de que falle algún componente de hardware, se reemplaza en el menor tiempo posible, ya que se cuenta con una línea directa con el proveedor. Posteriormente, después de la validación técnica, se realiza la instalación.

Plan de Mantenimiento Predictivo

Nuestro equipo de monitoreo realiza la inspección visual de todo el clúster de Tetration, lo que nos permite identificar variables físicas como la CPU, RAM, temperatura, estado de interfaces y cambios de software generados. El NOC central está capacitado en la solución de Tetration Analytics y conoce cada uno de sus componentes, lo que nos permite evaluar posibles

riesgos y mitigarlos. Después de validar con el ingeniero especializado de la empresa y en conjunto con el TAC de Cisco, se toma una decisión predictiva del asunto.

Plan de Mantenimiento Preventivo

Ejecución de rutina de Backups: Durante esta etapa, se procede a efectuar la configuración del clúster descargando el Snapshot que se encuentra en la parte de mantenimiento. Se guarda la configuración de los ADMs actualmente implementados y también se guarda el último annotation registrado en el clúster.

Ejecución de carga de software: Este proceso comprende la carga del software propiamente dicho. Se descarga el patch install RPM desde la página de cisco.com y se carga desde la opción de mantenimiento > upgrade.

Conclusiones

A través de diversas formaciones ya obtenidas a lo largo de la carrera. Se conoce la importancia de aplicar la investigación en varios escenarios reales en donde coexiste la necesidad de dar solución empleando conocimientos adecuados de la disciplina,

Se consultó los conceptos básicos que se tendrán en el proyecto durante su implementación dando un espectro más amplio de cada Ítem indicado.

Se procede con la documentación de la ficha de caracterización inicial donde se ven nuestra experiencia en investigación, fortalezas y debilidades.

Se relacionaron los intereses en ingeniería e investigación identificaron las líneas y los grupos de investigación de la cadena ETR;

Se propuso la idea para la investigación aplicada la cual es una Protección integral para la carga de trabajo de Data Center Bancolombia habilitando un modelo de "confianza cero” por medio de la plataforma Cisco Tetration.

Se identifica el problema central el cual es la invisibilidad en las aplicaciones y tráfico circundante sobre la red de datos del Datacenter de Bancolombia S. A, ubicado en Niquía; Bello; Antioquia.

La expansión de la plataforma de análisis Tetration brinda nuevas capacidades de protección de cargas de trabajo, avanzando hacia la confianza cero en sus centros de datos, también se pueden enviar políticas al firewall de cualquier proveedor y orquestar en la capa de red, siendo la seguridad es una parte clave de Tetration y con las nuevas versiones se incorporan más opciones al sistema.

Por medio de Estado del arte logre validar el contenido de cada una de las publicaciones realizadas, dando un espectro más amplio de la implantación que se va a realizar unificando varios conceptos evidenciados en cada artículo.

Evidencie como cisco Tetration me ayuda a observar por medio de su agente Deep visibility, temas de vulnerabilidades, ancho de banda, estado de interfaces, programas instalados etc.

Antes de implementar la protección integral y adoptar la confianza cero, Bancolombia enfrentaba desafíos relacionados con la seguridad y privacidad de los datos de sus clientes. La falta de un enfoque integral de protección y la confianza implícita en las redes internas podrían haber dejado a la organización vulnerable a ataques cibernéticos y brechas de seguridad. Sin embargo, con la implementación de la protección integral y la adopción de la confianza cero, Bancolombia ha logrado abordar estos problemas de manera efectiva. La protección integral ha permitido a la organización establecer un conjunto de medidas de seguridad y políticas que abarcan todos los aspectos de su infraestructura, desde la red hasta los dispositivos y las aplicaciones utilizadas. La confianza cero ha sido fundamental para garantizar la seguridad de los datos. Al eliminar la confianza implícita en las redes internas y requerir una autenticación y autorización estrictas para cada acceso, Bancolombia ha reducido significativamente el riesgo de intrusiones no autorizadas y ha fortalecido la protección de los datos confidenciales de sus clientes. Al tener controles rigurosos en su entorno tecnológico, la organización puede mitigar las amenazas y los riesgos, lo que se traduce en una mayor confianza de los clientes y en la capacidad de ofrecer servicios financieros de manera confiable.

Referencias

Bancolombia. (2022). Ciberseguridad la seguridad es lo primero. https://www.grupobancolombia.com/wps/portal/personas/nosotros/sostenibilidad/lineamientos-sostenibilidad/seguridad-informacion

Cisco. (2021). Trusted Zero Trust: The Role of Visibility in Cybersecurity. https://www.cisco.com/c/dam/m/en_us/security/cisco-zero-trust-importance-of-visibility-0621.pdf

Cisco. (n.d.). Cisco Secure Workload (Tetration) Platform Data Sheet. Cisco. https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html

Cisco. (2022). *Cisco Catalyst 9300 Series Switches*. https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/index.html#~models

Cisco.com. (2022).https://www.cisco.com/c/dam/global/es_mx/products/data-center-analytics/pdfs/c45-737257-00_tetration_analytics_aag_v4a_es-xl.pdf

Computerworld.es. (2022). Cisco lanza Tetration Analytics para mejorar la visibilidad de los datacenters. https://www.computerworld.es/centro-de-datos/cisco-lanza-tetration-analytics-para-mejorar-la-visibilidad-de-los-datacenters

Concepto. (2022). ¿Qué es una Idea? Concepto, para qué sirven y tipos de ideas. https://concepto.de/idea/

Concepto. (2022). ¿Qué son los objetivos generales y específicos? https://concepto.de/objetivos-generales-y-especificos/

Concepto. (2022). Alcance y Limitaciones de un Proyecto - Cuáles son y ejemplos. https://concepto.de/alcance-y-limitaciones-de-un-proyecto/

Concepto. (2022). Conclusión de un Proyecto - Concepto, cómo hacerla y ejemplos. [online] Available at: https://concepto.de/conclusion-de-un-proyecto/

Concepto. (2022). Justificación de una Investigación - Qué es, ejemplos. https://concepto.de/justificacion-de-una-investigacion/.

Concepto. (2022). Marco Teórico - Qué es, objetivos, estructura y ejemplo. https://concepto.de/marco-teorico/

Cooney, M. (2016). Cisco platform lets IT rein-in disruptive data center operations, security, applications. Network World (Online), https://bibliotecavirtual.unad.edu.co/trade-journals/cisco-platform-lets-rein-disruptive-data-center/docview/1797419329/se-2?accountid=48784

Dunn, K. (2019). Tetration. SC Magazine: For IT Security Professionals (15476693), 30(1), 36.

Kerner, Sean Michael. (2018). "Cisco Extends Tetration Analytics to Enable Workload Protection." EWeek, March, 1. https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=bsu&AN=128334688&lang=es&site=eds-live&scope=site.

Kionetworks.com. (2022). ¿Qué es un Data Center? https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center

Molina Montoya, N., (2022). ¿Qué es el estado del arte? Ciencia y Tecnología para la Salud Visual y Ocular. https://ciencia.lasalle.edu.co/svo/vol3/iss5/10/.

NetFlow Analyzer. (2022). SolarWinds. https://www.solarwinds.com/es/netflow-traffic-analyzer

PowerData, G., (2022). Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad. [online] Powerdata.es. https://www.powerdata.es/big-data

RedesZone. (2022). Confianza cero: ¿es una buena solución contra el ransomware? [online] https://www.redeszone.net/noticias/seguridad/confianza-cero-solucion-contra-ransomware/

Ruiz L. J (2019). Investigación experimental. https://www.scientific-european-federation-osteopaths.org/wp-content/uploads/2019/01/Investigaci%C3%B3n-experimental.pdf

Services, P. and Computing, S., (2022). *Cisco UCS C-Series Rack Servers*. [online] Cisco. https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html#~models

Services, P., (2022). Zero Trust Security. [online] Cisco. https://www.cisco.com/c/en/us/products/security/zero-trust.html

Services, P., Computing, S., Servers, C. and Sheets, D., (2022). *Cisco UCS C220 M5 Rack Server Data Sheet*. [online] Cisco. https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/datasheet-c78-739281.html

Servicios, P., (2022). Plataforma Cisco Tetration. [online] Cisco. https://www.cisco.com/c/es_es/products/data-center-analytics/tetration-analytics/index.html

Tesis y Masters Colombia. (2022). ¿Cómo hacer el Diseño Metodológico de una Tesis? [online] https://tesisymasters.com.co/como-hacer-el-diseno-metodologico-de-una-tesis/