RESUMEN ANALÍTICO ESPECIALIZADO -RAE

Fecha de Realización:	17/10/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Gestión de sistemas
Título:	Análisis De Soluciones Para El Monitoreo De Seguridad Activa Y Pasiva De Infraestructuras Tecnológicas Apoyado En Un Servicio De SOC
Autor(es):	Mora Montoya Julian David
Palabras Claves:	Correlación, CSOC, Detección de amenazas, Monitoreo, SIEM, SOAR, SOC.
Descripción:	El presente documento encontrara documentación relacionada con lo que se debe tener en cuenta para llevar a cabo un diseño de un servicio de monitoreo de ciber seguridad en una organización, factores clave a tener en cuenta, contemplando diversas opciones de recolección de los datos, tipos de logs, servicio SOC, acciones de respuesta automatizada para garantizar una pronta reacción ante un posible incidente de ciberseguridad, con base a las recomendaciones que puedan existir en los marcos de referencia como NIST, circular externa 007 de 2018 de la super intendencia financiera de Colombia, para que con base a esta información se logre comprender las necesidades y fortalecer un esquema de monitoreo que pueda alimentar al equipo de

	respuesta a incidentes de ciberseguridad de las organizaciones.

Fuentes bibliográficas destacadas:

Biggeri, Patricio Hernán. Centro de operaciones de seguridad: estrategia, diseño y gestión. [En línea] Trabajo Final de Maestría. Universidad de Buenos Aires Facultad de Ciencias Económicas Escuela deEstudios de Posgrado. Buenos Aires, 2018. [Consultado 1 de junio 2021] Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1202_BiggeriPH.pdf

Ceballos Lopez, Adriana, Equipo TicTac. Evaluación retos y amenazas a la ciberseguridad. Bogota D.C. 2021. p. 33.

Centro Cibernetico Policial de Colombia. Balance Cibercrimen BLSC20335DS1. Bogotá D.C. 2020. p. 2

Crooks, David, y Liviu Vâlsan. «Building a Minimum Viable Security Operations Centre for the Modern Grid Environment». Proceedings of International Symposium on Grids & Clouds 2019 — PoS (ISGC2019), Sissa Medialab, 2019, p. 010.

Fusion SIEM [En línea] Exabeam. Consultado el 2 de octubre de 2021. Disponible en: https://www.exabeam.com/product/fusion-siem/.

Gartner Reprint.[en línea] Consultado el 2 de octubre de 2021. Disponible en: https://www.gartner.com/doc/reprints?id=1-26Q3T88Y&ct=210706&st=sb.

Mendez Fonseca, Victor Julio. Marco Tecnológico de un SOC de Nueva Generación. Universidad Piloto de Colombia. Especialización en seguridad informática. 2019. p.12.

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST CSWP 04162018, National Institute of Standards and Technology, 16 de abril de 2018, p. NIST CSWP 04162018. DOI.org (Crossref), doi: 10.6028/NIST.CSWP.04162018.	
Contenido del documento:	El presente documento tiene como objetivo analizar soluciones para que las organizaciones establezcan una estrategia de monitoreo activo y pasivo de la seguridad de la información y de la infraestructura tecnológica mediante la incorporación de un servicio de SOC. dentro de este se podrá encontrar información relevante con la identificación de información del marco de trabajo de NIST relevante para ser aplicada en un servicio de monitoreo, principales ataques cibernéticos identificados en Colombia a los cuales están expuestas las organizaciones, diferentes herramientas de SIEM para la implementación de un SOC y estrategias que ayudaran a fortalecer los sistemas de monitoreo de ciberseguridad para las organizaciones con alternativas que permitan llevar a cabo la respuesta oportuna ante amenazas de seguridad buscando reducir los tiempos.
Conceptos adquiridos:	En el contenido del documento, se adquieren conceptos como:

	Reconocer y comprender que es un SOC, que es un SOC de nueva generación, Framework NIST y cada una de sus funciones, identificar, proteger, detectar, responder, recuperar, SOAR SIEM y sus principales ventajas, UEBA, Playbooks, Inteligencia de amenazas, entre otros elementos importantes para establecer servicio de monitoreo de seguridad.
Conclusiones:	Con base a las validaciones realizadas sobre el marco de trabajo de NIST, se cuenta con una herramienta potencial que brinda diversas opciones para la mejora de la ciberseguridad en cualquier tipo de organización, este puede servir como referencia decidiendo cuales de sus elementos pueden ser aplicados, no es necesario trabajar con todas sus funciones, cada organización está en la libertad de acogerse a alguna de ellas con base a sus necesidades. Adicionalmente, en Colombia las organizaciones reguladas por la super intendencia financiera, según lo establecido en el numeral 3 de la circular externa 007 de 2018, deben realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de SOC. En Colombia se ha definido un CSIRT liderado por la policía nacional, el cual se encarga de gestionar las denuncias interpuestas por la

	ciudadanía, bien sea personas naturales o empresas, con base a esto se identifican los principales ataques que se presentan en el país con base a lo identificado, los principales ataques son; phishing, suplantación de identidad, envío de malware, fraudes en medios de pago en línea, así mismo se argumenta cuáles son las estadísticas de crecimiento, se comparten de manera periódica y pueden ser consultadas de manera libre, con base a esta información se puede deducir que los ataques cibernéticos están en constante evolución y crecimiento, los ciber delincuentes cada día encuentran nuevas alternativas para evadir los controles. Existen en el mercado diferentes tipos de soluciones SIEM, de las cuales se realiza un análisis con base a la información suministrada por el cuadrante de Gartner, entre ellas; LogRhythm, InsightIDR, Splunk, QRADAR, Exabeam Fusion SIEM, Securonix Next-Gen SIEM, Elastic Security;las cuales son la base para establecer un centro de operaciones de seguridad, estas herramientas cuentan con diferencias tanto en las prestaciones como en los costos, se pueden encontrar en el mercado soluciones con diferentes tipos de licenciamiento, de acuerdo a las necesidades

	de la organización, así mismo también se puede optar por la implementación de herramientas de uso libre como: OSSIM, OSSEC, Apache Metron, SIEMonster, Prelude SIEM. Security Onion, las cuales pueden ser de utilidad para establecer un sistema de monitoreo en una organización de bajos recursos. Las estrategias de ataques cibernéticos han ido evolucionando con el paso del tiempo, con base a esto se ha venido trabajando en la definición de nuevas estrategias para fortalecer el monitoreo, la detección y respuesta oportuna de amenazas, con base a esto se debe garantizar que una estrategia de monitoreo no debe basarse en una simple recolección de logs, sino que debe ir más allá de lo convencional apoyándose en nuevas alternativas como las propuestas. SOAR, UEBA, implementación de Playbooks, inteligencia de amenazas, lo cual permitirá estar un paso delante de los atacantes.