UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Trabajo de titulación previo a la obtención del título de Magíster en Ciberseguridad

AUTORES:

- Ricardo David Torres Sánchez
- David Geovanni Flores Millingalle
- Diego Elías Bajaña Noblecilla
- Andrés Alejandro Duque Andrade

TUTOR: Ing. Ronie Stalin Martínez Gordon, Mtr.

Optimización y creación de reglas en SIEM con Hacking Ético para un Centro de Operaciones de Seguridad (SOC)

Aprobación del tutor

Yo, Ronie Stalin Martínez Gordon, certifico que conozco los autores del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

_____

Ronie Stalin Martínez Gordon

Director de trabajo de titulación

Declaración de la autoría del trabajo de titulación

Nosotros, Ricardo David Torres Sánchez; David Geovanni Flores Millingalle; Diego Elías Bajaña Noblecilla y Andrés Alejandro Duque Andrade, declaramos solemnemente que el presente trabajo de titulación titulado 'Optimización y creación de reglas en SIEM con Hacking Ético para un Centro de Operaciones de Seguridad (SOC)' es el resultado de nuestra propia investigación y esfuerzo. Confirmamos que este trabajo es original y que todas las fuentes utilizadas han sido debidamente citadas y referenciadas según las normas académicas establecidas.

Asimismo, aseguramos que ninguna parte de este trabajo se presentó como trabajo de otro autor para obtener cualquier calificación académica. Este trabajo de titulación representa nuestra contribución al campo de la ciberseguridad y refleja nuestro compromiso con el rigor académico y la integridad intelectual.

D.M Quito, junio del 2024

Andrés Alejandro Duque Andrade

Autor de trabajo de titulación

Diego Elías Bajaña Noblecilla

Autor de trabajo de titulación

David Geovanni Flores Millingalle

Autor de trabajo de titulación

Ricardo David Torres Sánchez

Autor de trabajo de titulación

Autorización de derechos de propiedad intelectual

Por la presente, nosotros, Ricardo David Torres Sánchez; David Geovanni Flores Millingalle; Diego Elías Bajaña Noblecilla y Andrés Alejandro Duque Andrade, autores del trabajo de titulación titulado, 'Optimización y creación de reglas en SIEM con Hacking Ético para un Centro de Operaciones de Seguridad (SOC)' presentado para optar al grado de Magister en Ciberseguridad, en la Universidad Internacional del Ecuador, otorgo los siguientes derechos de propiedad intelectual asociados al mismo:

Autorizo la reproducción, distribución, comunicación pública y cualquier otro uso relacionado con mi trabajo de titulación, 'Optimización y creación de reglas en SIEM con Hacking Ético para un Centro de Operaciones de Seguridad (SOC)' con fines académicos y de divulgación, tanto dentro como fuera de la institución educativa, reconociendo que dichos derechos son no exclusivos.

D.M Quito, junio del 2024

Firmado electrónicamente por:
ANDRES ALEJANDRO DUQUE ANDRADE

Andrés Alejandro Duque Andrade

Autor de trabajo de titulación

Firmado electrónicamente por:
DIEGO ELIAS BAJANA NOBLECILLA

Diego Elías Bajaña Noblecilla

Autor de trabajo de titulación

Firmado electrónicamente por:
DAVID GEOVANNI FLORES MILLINGALLE

David Geovanni Flores Millingalle

Autor de trabajo de titulación

Firmado electrónicamente por:
RICARDO DAVID TORRES SANCHEZ

Ricardo David Torres Sánchez

Autor de trabajo de titulació

Dedicatoria

Queremos dedicar el presente trabajo de grado a nuestro estimado Tutor, el Ing. Ronie Stalin Martínez Gordón, cuya guía experta y apoyo inquebrantable fueron fundamentales en la culminación de este trabajo de titulación. Agradezco sinceramente su dedicación y conocimientos compartidos, los cuales han sido la piedra angular de este proyecto. También queramos expresar nuestra gratitud a nuestras familias y amigos por su constante aliento y comprensión durante este arduo proceso. Este logro es también suyo. Que este trabajo contribuya al avance del conocimiento en el campo de la seguridad de la información.

Agradecimiento

Queremos expresar nuestro agradecimiento a la Universidad Internacional del Ecuador por darnos la oportunidad de titular sobre 'Optimización y creación de reglas en SIEM con Hacking Ético para un Centro de Operaciones de Seguridad (SOC).

Agradecemos a los docentes de cada materia impartida en el proceso de aprendizaje de la maestría en ciberseguridad, así como su orientación y apoyo durante el proceso de investigación y desarrollo de este trabajo. Sus conocimientos y experiencias compartidas han sido fundamentales para nuestra formación académica y profesional.

Resumen

El proyecto se enfoca en mejorar la efectividad de las reglas y alertas de seguridad en los Sistemas de Información y Eventos de Seguridad (SIEM) en Centros de Operaciones de Seguridad (SOC), dado el contexto actual de amenazas cibernéticas complejas. Se destaca la importancia de optimizar el SIEM para evitar falsos positivos, retrasos en la respuesta a incidentes y garantizar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS - Acuerdos de Nivel de Servicio). El enfoque propuesto implica el uso de técnicas de Hacking Ético para evaluar y mejorar las reglas existentes, anticipando mejoras en la detección de amenazas y una reducción en la carga operativa de los analistas de seguridad. Además, se espera que este trabajo contribuya al fortalecimiento de la seguridad empresarial y al avance de la investigación en ciberseguridad, con posibles implicaciones para otras organizaciones.

Palabras clave: SIEM, SOC, ANS, Hacking Ético, Sistemas de información, Seguridad empresarial.

Abstract

The project focuses on improving the effectiveness of security rules and alerts in Security Information and Event Management (SIEM) Systems within Security Operations Centers (SOCs), given the current context of complex cyber threats. The importance of optimizing the SIEM to prevent false positives, delays in incident response, and ensure compliance with Service Level Agreements (SLAs) is highlighted. The proposed approach involves the use of Ethical Hacking techniques to assess and enhance existing rules, anticipating improvements in threat detection and a reduction in the operational burden on security analysts. Furthermore, it is expected that this work will contribute to strengthening corporate security and advancing cybersecurity research, with potential implications for other organizations.

Keywords: SIEM, SOC, ANS, Ethical Hacking, Information Systems, Business Security.

Tabla de contenidos

Lista de tablas

Lista de Figuras

CAPÍTULO I

Introducción

La evolución constante de las amenazas cibernéticas en el entorno empresarial ha posicionado la seguridad de la información como una prioridad ineludible. En este contexto, los Centros de Operaciones de Seguridad (SOC) enfrentan desafíos continuos en la protección de su infraestructura digital. Este proyecto se gesta como respuesta a la imperante necesidad de elevar la eficacia de las reglas y alertas en el Sistema de Información y Eventos de Seguridad (SIEM) del SOC a través de Hacking Ético.

Caso de estudio/ Problema de la investigación

En el marco contemporáneo, donde las amenazas cibernéticas adquieren una complejidad creciente, la seguridad de la información se posiciona como una imperativa prioridad para las empresas. Los Centros de Operaciones de Seguridad SOC, como otras organizaciones enfocadas en la ciberseguridad corporativa, se enfrentan con retos constantes en su afán de asegurar su infraestructura digital ante eventuales vulnerabilidades. Aunque los Sistemas de Información y Eventos de Seguridad (SIEM) son fundamentales en la detección y respuesta ante amenazas, su eficacia está ligada a la calidad y relevancia de las reglas y alertas implementadas.

En este contexto, emerge la necesidad imperante de elevar la eficacia de las reglas y alertas de seguridad en la estructura del SIEM del Centro de Operaciones de Seguridad (SOC). La carencia de una configuración óptima conlleva la potencial generación de falsos positivos, dilatando el tiempo de respuesta a incidentes, poniendo en riego el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) y menguando la capacidad de la organización para prevenir y mitigar amenazas cibernéticas.

El presente proyecto surge como una respuesta a esta problemática, proponiendo la ejecución de técnicas de Hacking Ético para evaluar y diagnosticar el funcionamiento de las reglas que están creadas e implementadas en el SIEM, que pueden ser imperceptibles al ataque. De esta manera, se puede identificar, perfeccionar, afinar y crear reglas y/o alertas en el SIEM del Centro de Operaciones de Seguridad (SOC). El desarrollo de destrezas en ciberseguridad con la optimización de la infraestructura de detección de amenazas aspira a robustecer la calidad y servicio de seguridad del SOC, disminuir los riesgos vinculados a potenciales ataques asegurando el cumplimiento de los ANS.

Se anticipa que la optimización de las reglas y alertas en el SIEM redundará en mejoras significativas. Primordialmente, se espera una mayor eficiencia en la detección de amenazas, reduciendo consiguientemente el tiempo de respuesta a incidentes. A la vez, la disminución de falsos positivos facultará a los operadores y analistas de seguridad en la creación de reglas robustas, optimización de los recursos, disminución de los falsos positivos y reducción de su carga operativa. Esto brinda el perfeccionando en los conocimientos y eficacia en detección de amenazas. Además, esta iniciativa contribuirá al fortalecimiento de la postura de seguridad de las empresas, generando confianza tanto a nivel interno como externo.

Este proyecto pretende favorecer los procesos de los Centros de Operaciones de Seguridad (SOC) y anhela aportar al ámbito de la ciberseguridad. La metodología propuesta, al incorporar técnicas de Hacking Ético, puede posicionarse como un referente para otras organizaciones que persiguen perfeccionar su SOC y sistemas de seguridad en general. En última instancia, los resultados obtenidos podrían propiciar el avance de la investigación en ciberseguridad, proporcionando un enfoque práctico y ético para la optimización de los sistemas de SIEM.

Objetivos

Objetivo general

Evaluar, diagnosticar y mejorar de manera efectiva las reglas y alertas implementadas en el Sistema de Información y Eventos de Seguridad (SIEM) del Centro de Operaciones de Seguridad (SOC) mediante la aplicación de metodología Global Información Assurance Certifications SANS (SysAdmin, Audit, Network, Security) de Hacking Ético.

Objetivos Específicos:

- Identificar y analizar el funcionamiento actual de las reglas personalizadas y definidas en el SIEM Alien Vault del SOC.
- Mediante la aplicación de técnicas SANS de Hacking Ético, documentar los hallazgos y debilidades detectadas en el sistema SIEM.
- Mejorar y afinar las reglas y alertas existentes en el SIEM para elevar su eficacia en la detección de amenazas.
- Crear reglas según los eventos generados por las pruebas de Hacking Ético que no se hayan detectado con las reglas existentes.

CAPÍTULO II

Marco Teórico

Con este marco teórico detallaremos las definiciones y características de las herramientas, técnicas y procesos que se aplicarán al desarrollar la optimización y creación de reglas en SIEM con Hacking Ético para un Centro de Operaciones de Seguridad (SOC).

Técnicas SANS

Según lo investigado en el trabajo de titulación (QUIROZ, 2020, pág. 18), “la técnica SANS (SysAdmin, Audit, Network, Security) es un enfoque integral utilizado en el ámbito del hacking ético para evaluar y mejorar la seguridad de los sistemas informáticos. Este enfoque se centra en cuatro áreas principales: administración de sistemas, auditoría, redes y seguridad. Al combinar conocimientos y habilidades en estas áreas, los profesionales de la seguridad pueden identificar vulnerabilidades y fortalecer la seguridad de una infraestructura de TI.”

Las principales técnicas más comunes incluyen:

Escaneo de Puertos y Servicios: Utilizado para identificar los puertos abiertos y los servicios que se ejecutan en un sistema o red. Herramientas como Nmap son comúnmente utilizadas para este propósito.

Enumeración de Sistemas y Usuarios: Implica recopilar información detallada sobre los sistemas y usuarios en una red, como nombres de hosts, nombres de usuarios, grupos, etc. Se pueden utilizar herramientas como enum4linux para sistemas basados en Windows y enum for Unix para sistemas basados en Unix.

Ataques de Fuerza Bruta y Diccionario: Utilizados para intentar adivinar contraseñas mediante la generación sistemática de combinaciones de caracteres o

mediante la prueba de palabras de un diccionario. Herramientas como Hydra y John the Ripper son ampliamente utilizadas para este propósito.

Ingeniería Social: Implica el uso de técnicas psicológicas para manipular a las personas y obtener acceso no autorizado a sistemas o información confidencial. Esto puede incluir el phishing, pretexting, tailgating, entre otros.

Análisis de Vulnerabilidades: Utilizado para identificar y evaluar las vulnerabilidades en sistemas y aplicaciones. Herramientas como Nessus y OpenVAS son comúnmente utilizadas para escanear sistemas en busca de vulnerabilidades conocidas.

Explotación de Vulnerabilidades: Implica aprovechar las vulnerabilidades identificadas para obtener acceso no autorizado a sistemas o redes. Herramientas como Metasploit se utilizan comúnmente para automatizar este proceso.

Análisis Forense Digital: Utilizado para recopilar, preservar y analizar evidencia digital relacionada con incidentes de seguridad. Esto puede incluir la recuperación de datos eliminados, el análisis de registros de eventos, la identificación de malware, entre otros.

SIEM de fabricante Alienvault

De acuerdo con la información (TT&T Cybersecurity, 2024), es una herramienta para detectar amenazas desde el primer día e impulse la eficiencia operativa con una plataforma unificada para la detección de amenazas, respuesta a incidentes y gestión del cumplimiento.

USM Anywhere centraliza el monitoreo de seguridad de redes y dispositivos en la nube, en las instalaciones y en ubicaciones remotas, ayudándolo a detectar amenazas prácticamente en cualquier lugar.

Características del SIEM:

Descubrimiento

- Descubrimiento de activos de red
- Descubrimiento de software y servicios
- Descubrimiento de activos de AWS
- Descubrimiento de activos de Azure
- Descubrimiento de activos de Google Cloud Platform

Análisis

- Correlación de eventos SIEM, alarmas con prioridad automática
- Monitoreo de la actividad del usuario
- Hasta 90 días de eventos en línea con capacidad de búsqueda

Detección

- Detección de intrusiones en la nube (AWS, Azure, GCP)
- Detección de intrusiones en la red (NIDS)
- Detección de intrusiones en el host (HIDS)
- Detección y respuesta de terminales (EDR)

Respuesta

- Consulta forense
- Automatizar y organizar la respuesta
- Notificaciones y emisión de billetes

Evaluación

- Escaneo de vulnerabilidades
- Evaluación de infraestructura en la nube
- Configuración de usuarios y activos

- Monitoreo de la web oscura

Informes

- Plantillas de informes de cumplimiento prediseñadas
- Plantillas de informes de eventos prediseñadas
- Vistas y paneles personalizables
- Almacenamiento de registros

Funcionamiento:

Detección automatizada de amenazas impulsada por Alien Labs

Con la inteligencia de amenazas proporcionada por Alien Labs, USM Anywhere se actualiza automáticamente para estar al tanto de las amenazas emergentes y en evolución, de modo que su equipo pueda concentrarse en responder a las alertas.

Orquestación de respuesta a incidentes con AlienApps

USM Anywhere admite un ecosistema en crecimiento de AlienApps, lo que le permite orquestar y automatizar acciones hacia otras tecnologías de seguridad para que pueda responder a incidentes de forma rápida y sencilla (TT&T Cybersecurity, 2024)

Implementación de un SIEM

Basados en el trabajo de grado de (DÍAZ, 2018, pág. 12) “al momento de implementar un SIEM es importante tener claro cuáles son las fuentes que se van a integrar y la capacidad de almacenamiento que se va a contratar y que políticas se debe priorizar como el cumplimiento normativo, activos que se implementaran, mejores prácticas y la creación de casos de uso más comunes”.

Para la implementación de un SIEM se debe tener en cuenta los siguientes puntos:

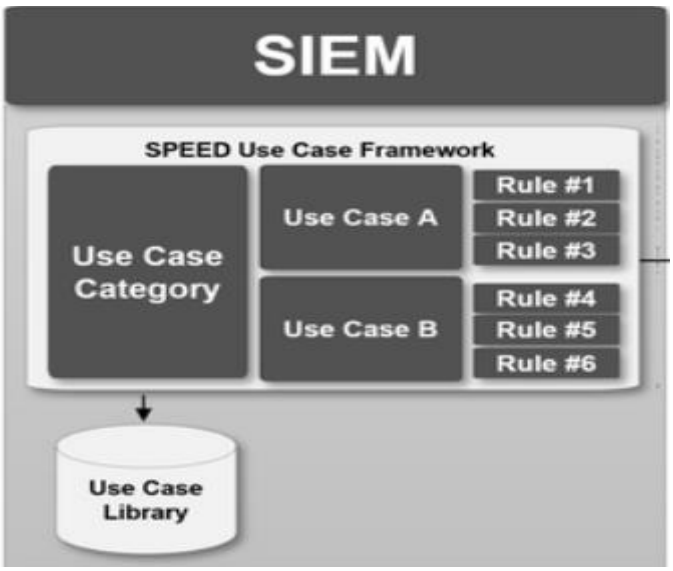
- El SIEM debe utilizarse como una base de datos de inventario de la información con su riesgo por activos.
- El inventario de las aplicaciones que tienen en cada activo para la correlación de eventos y actividades de estas.
- Los equipos deben habilitar los registros de auditoria para que se almacenen en el SIEM.
- Es importante que todos los eventos que es almacenen en el SIEM por lo menos un año son necesarios por auditoria y necesarios para una respuesta a incidentes.
- Se debe tener un conocimiento de los casos de uso que se van a implementar y las reglas que estén ligadas al negocio y a la estrategia de ciberseguridad.

Caso de uso.

Como menciana (Castro, 2022, pág. 19), “un caso de uso hace referencia a la configuración de reglas y alertas que permitan identificar y notificar ante un evento de seguridad o ataque cibernético. Estas reglas están configuradas en el SIEM de manera que permita responder a situaciones relacionadas a seguridad”.

Figura 1.

Casos de uso



Fuente: (Ramirez, 2021). Las mejores prácticas para implementar una estrategia SIEM [Por Rubén Ramírez]. https://ciberseguridad.blog/las-mejores-practicas-para-implementar-una-estrategia-siem/

Principales casos de uso usados en un SIEM

Detección de credenciales comprometidas. Se debe contar con casos de uso y un flujo de trabajo de investigación de los logs que se está recibiendo para detectar cualquier intento de comprometer las credenciales del usuario a través de ataques de fuerza bruta, Golden Ticket u otros métodos con el uso de diccionarios globales o personalizados. En caso de un compromiso exitoso, es crucial identificar a los usuarios y entidades afectados para investigar el impacto.

Detectar comportamientos inusuales en cuentas privilegiadas

Los usuarios privilegiados, como los administradores de sistemas o bases de datos, tienen derechos de acceso ampliados, lo que los convierte en un objetivo atractivo para los piratas informáticos. Con un SIEM, los analistas pueden vigilar de cerca cualquier acción que realicen estos usuarios privilegiados y buscar comportamientos inusuales que puedan indicar una amenaza.

Aplicaciones basadas en la nube

La computación en la nube tiene muchas ventajas, pero también conlleva varios desafíos: cumplir con nuevos requisitos de cumplimiento, mejorar la supervisión de los usuarios y el control de acceso, o prepararse contra posibles infecciones de malware y filtraciones de datos. Un SIEM debe admitir aplicaciones basadas en la nube como fuentes de registro, como Salesforce, Office365 o AWS, para extender el monitoreo del cumplimiento y la detección de amenazas a la nube.

Detección de Phishing

El phishing es un intento de obtener información confidencial utilizada para cometer fraude y suplantación de identidad. Esto incluye intentos de adquirir información personal, como números de seguro social, números de cuentas bancarias o códigos PIN y contraseñas. Es fundamental garantizar que estos tipos de datos estén protegidos en toda la organización. El phishing se utiliza a menudo para obtener acceso inicial dentro de una red. Al recibir un correo electrónico de phishing, los analistas pueden usar SIEM para rastrear quién los recibió, hizo clic en los enlaces que contiene o respondió, lo que les permite tomar medidas inmediatas para minimizar el daño (LOGPOINT, 2024).

RidgeBot

De acuerdo con (IT JETS, 2024), RidgeBot Automated Pentesting es un software con el enfoque de automatizar la frecuencia de pruebas de penetración en la infraestructura externa e interna. Bajo demanda y de manera programada se ejecutan pruebas ilimitadas de seguridad ofensiva (tal como haría un hacker o pentester) a sistemas IP y sitios web, con resultados y reportes desplegados en tiempo real para que el cliente esté un paso adelante en la remediación y no tenga que esperar días a semanas para saber cómo solucionar sus vulnerabilidades y riesgos. En general, RidgeBot permite evaluaciones diarias, semanales y mensuales a sistemas IP y sitios web con el propósito de mantener esa frecuencia de pruebas y presentando las vulnerabilidades más críticas que requieren una remediación urgente porque podrían ser explotadas por un hacker.

Ridgebot es un sistema de pruebas de penetración de seguridad continuo y totalmente automatizado. Combinas técnicas de Hacking Ético on algoritmos de toma de decisiones impulsados por IA para localizar objetivos vulnerables, luego explotarlos y priorizar los riesgos comerciales dentro de la empresa. RidgeBot encuentra y explota vulnerabilidades que residen en la infraestructura de red, servidores host, aplicaciones web, dispositivos de red, entornos DevOps, marcos de trabajo de terceros y API.

Descubrimiento automático de la superficie de ataque

Para los activos descubiertos, RidgeBot explora más a fondo los enlaces débiles o las superficies de unión asociadas. Las superficies de ataque pueden ser URL, subURL, carpetas, subcarpetas, etc. Los detalles de cada superficie de ataque se mostrarán en la "Superficie de ataque". El hallazgo de la superficie de ataque es la base para los siguientes pasos. Cuantas más superficies de ataque encuentre RidgeBot, mayores serán las posibilidades de que RidgeBot descubra vulnerabilidades y riesgos. Una prueba exitosa tendrá una tabla de "superficie de ataque" llena de detalles (Ridge Security Technology Inc., 2024).

Matriz MITRE ATT&CK

La matriz MITRE ATT&CK es una visualización de las tácticas y técnicas en el marco MITRE ATT&CK. Presenta la misma información en un formato condensado, utilizando una matriz que enumera las tácticas en la parte superior y las técnicas en el lateral. Cada celda de la Matriz ATT&CK representa una técnica específica dentro de una táctica específica. La matriz ATT&CK está codificada por colores para indicar la frecuencia y gravedad del uso de cada técnica en ataques cibernéticos del mundo real, así como los controles defensivos correspondientes que se pueden utilizar para mitigar el riesgo.

La matriz MITRE ATT&CK (Tácticas, técnicas y conocimientos comunes de confrontación) es un marco para comprender y categorizar las diversas tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes durante un ciberataque. MITRE, una organización sin fines de lucro que trabaja con el gobierno y la industria para mejorar la ciberseguridad, desarrolló ATT&CK Matrix.

Consta de dos componentes principales: tácticas y técnicas. Las tácticas representan los objetivos de un atacante, mientras que las técnicas representan los métodos específicos utilizados para lograr esos objetivos. La Matriz ATT&CK está organizada en varias categorías, cada una de las cuales representa una etapa diferente de un ciberataque.

Presenta la misma información en un formato condensado, utilizando una matriz que enumera las tácticas en la parte superior y las técnicas en el lateral. Cada celda de la Matriz ATT&CK representa una técnica específica dentro de una táctica específica. La matriz ATT&CK está codificada por colores para indicar la frecuencia y gravedad del uso de cada técnica en ataques cibernéticos del mundo real, así como los controles defensivos correspondientes que se pueden utilizar para mitigar el riesgo.

Componentes:

MITRE ha ampliado la Matriz ATT&CK original en tres matrices principales:

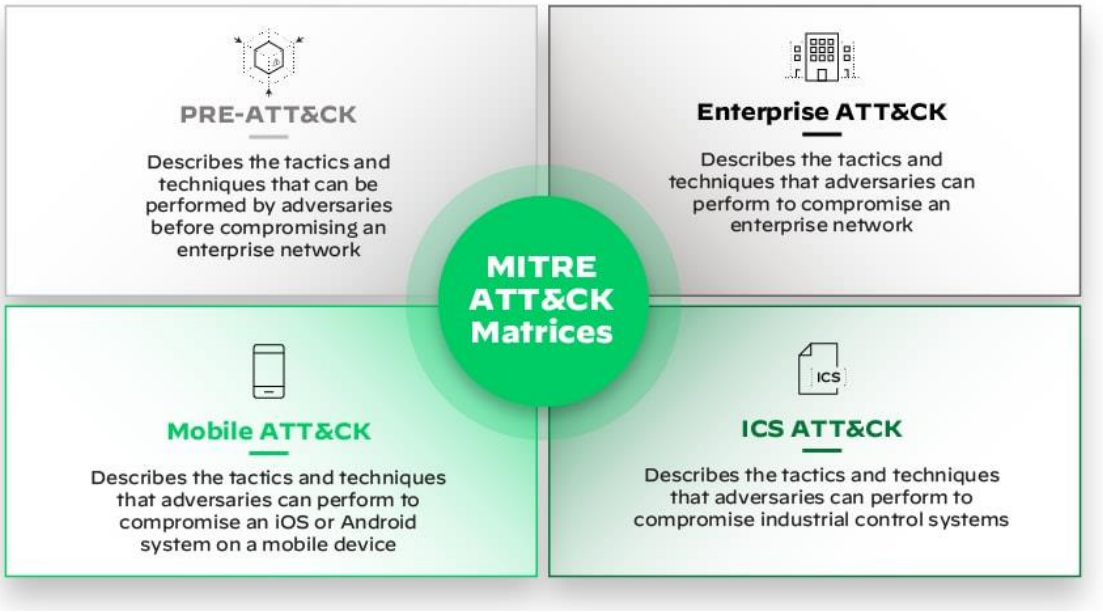
- Empresa
- Móvil
- ICS

Enterprise Matrix se desglosa por etapa y plataforma en:

- PRE-ATT&CK
- ventanas
- Mac OS
- Linux
- Nube (Incluido Microsoft 365, Google Workspace, Azure AD, SaaS e IaaS)
- Red
- Contenedores (Palo Alto Networks, 2024).

Figura 2.

Matrices MITRE ATT&CK



Nota: Adaptado de MITRE ATT&CK Matrix por PaloAlto *https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-matrix*

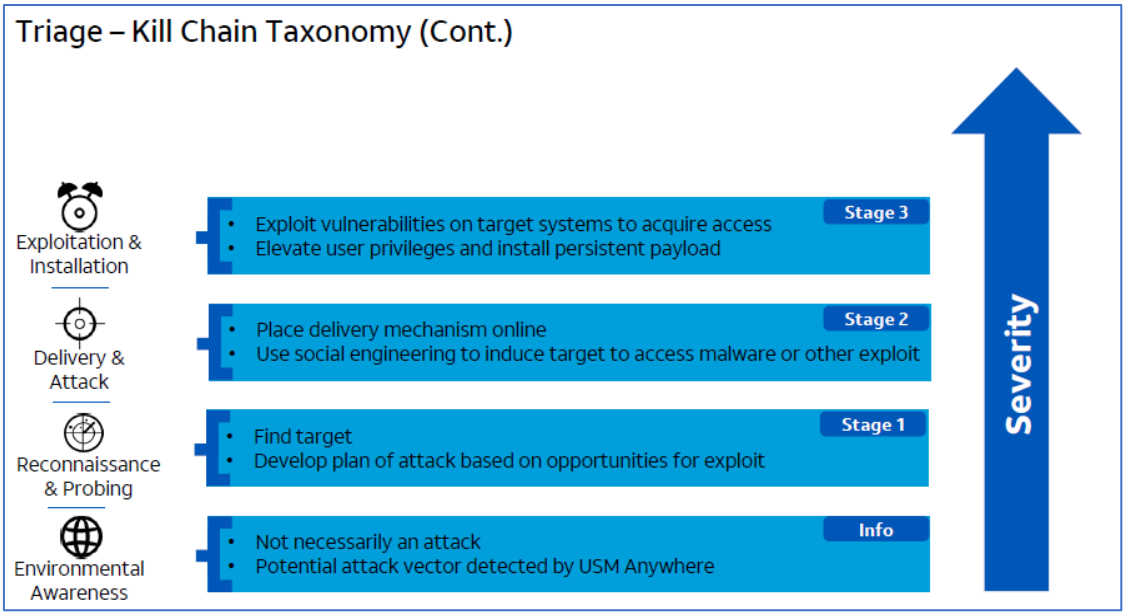
Triage – Kill Chain

Este marco conceptual en ciberseguridad que combina dos ideas principales: el triaje, que implica clasificar y priorizar amenazas, y la cadena de ataque, que describe las etapas secuenciales de un ataque cibernético. Este enfoque permite a las organizaciones entender y responder eficazmente a los ataques, categorizando las amenazas según su gravedad y alineándolas con las etapas de la cadena de ataque para una defensa más efectiva.

Para el cálculo de riesgos de las alertas nos basamos en la Taxonomia de Kill Chain de Alienvault, como lo indica la siguiente gráfica:

Figura 3

Triage – Kill Chain



Nota: Adaptado de *5 - Detection and Evaluation - ANYSAv2.7.0.PDF por https://cybersecurity.att.com/blogs/labs-research/adversary-simulation-with-usm-anywhere -*

El campo de prioridad en Alienvault puede mostrar Baja, Media o Alta. Este texto proviene de reglas de correlación y orquestación. Cuando crea una regla de orquestación, debe ingresar un valor de prioridad entre 0 y 100. AT&T Alien Labs™ crea las reglas de correlación e incluye un valor (Cybersecurity, 2024).

Metodología

La estrategia de investigación avanzada propuesta tiene como objetivo cumplir con los objetivos generales y específicos del proyecto, que se centran en evaluar, diagnosticar y mejorar las reglas y alertas del Sistema de Información y Eventos de Seguridad (SIEM) en el Centro de Operaciones de Seguridad (SOC) mediante la aplicación de técnicas de Hacking Ético. A continuación, se describe detalladamente la metodología a seguir:

1. Análisis Documental y Evaluación Preliminar:

Realizar una exhaustiva revisión de la documentación existente sobre las reglas y alertas actuales en el SIEM del SOC.

Llevar a cabo un análisis inicial de la arquitectura y configuración del SIEM para comprender su estructura.

2. Implementación de Pruebas Éticas:

Identificar y aplicar de manera ética y controlada técnicas de Hacking Ético para evaluar las reglas y alertas del SIEM.

Documentar cada prueba realizada, registrando los resultados obtenidos y las posibles áreas de mejora en el sistema.

3. Análisis de los Resultados:

Realizar un análisis detallado de los resultados de las pruebas de Hacking Ético.

Categorizar los hallazgos en áreas como vulnerabilidades críticas, aspectos a mejorar y puntos fuertes del SIEM.

4. **Diseño de Mejoras en Reglas y Alertas:**

Formular propuestas específicas de mejora para las reglas y alertas que se identificaron como deficientes durante las pruebas.

Garantizar que las mejoras propuestas estén alineadas con las mejores prácticas de seguridad y con los objetivos del SOC.

5. Implementación de Mejoras:

Aplicar las mejoras planificadas en el SIEM, minimizando cualquier impacto en la operatividad del SOC.

Realizar pruebas de validación para verificar la efectividad de las modificaciones implementadas.

6. **Evaluación Cuantitativa:**

Cuantificar la eficiencia de detección de amenazas antes y después de realizar las modificaciones en el SIEM.

Utilizar métricas de rendimiento, como la tasa de detección y la reducción de alertas falsas, para evaluar el progreso.

7. Documentación Completa y Presentación de Resultados:

Elaborar un informe detallado que documente todas las etapas de la investigación, desde la revisión inicial hasta las mejoras implementadas.

Presentar los resultados de manera clara y comprensible, destacando las mejoras realizadas y ofreciendo recomendaciones para futuras actualizaciones.

8. **Validación por el Equipo de Seguridad:**

Someter los resultados y las mejoras propuestas a revisión por parte del equipo de seguridad del SOC. Integrar comentarios y realizar ajustes en las mejoras según sea necesario.

Esta metodología busca asegurar una evaluación completa, un diagnóstico preciso y mejoras efectivas en el SIEM del SOC, contribuyendo a fortalecer la seguridad y la capacidad de respuesta frente a amenazas.

Desarrollo

Para el desarrollo de esta práctica se aplicarán técnicas SANS de Hacking Ético para poner a prueba la efectividad del SIEM en la detección de amenazas. Los hallazgos y debilidades detectadas durante estas pruebas se documentarán, proporcionando una visión clara de las áreas de mejora.

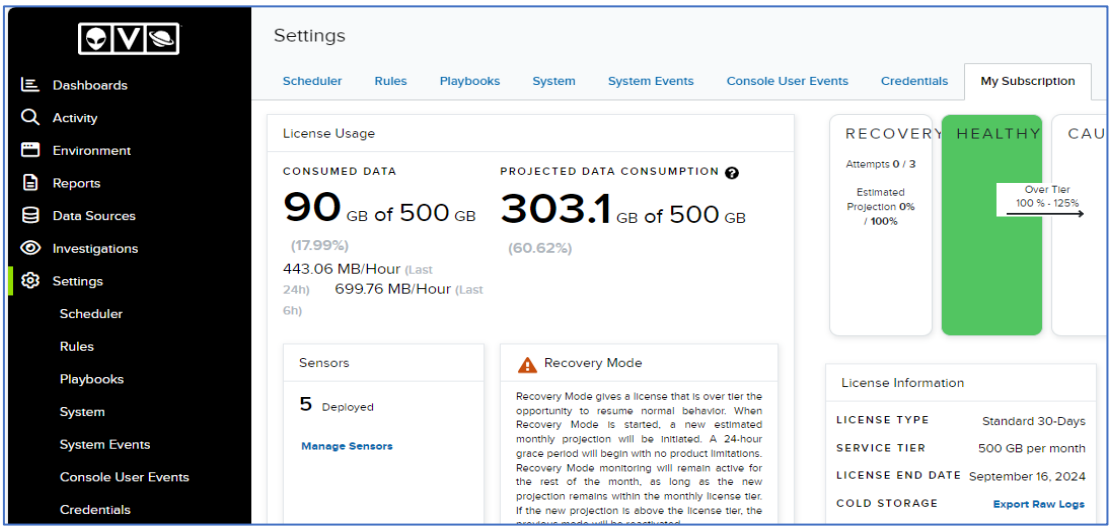
Al identificar y analizar el funcionamiento actual de las reglas customizadas y definidas en el SIEM Alien Vault del SOC se pretende entender cómo se están utilizando las reglas existentes y qué áreas pueden ser mejoradas.

Identificación del escenario actual

En el SOC se tiene instalado el SIEM de fabricante Alienvault que realiza correlación de los eventos, detección de las pruebas de intrusión, la cual se ira configurando y afinando según los casos de uso que se detecten basados en los resultados del Hacking ético.

Figura 4

SIEM de pruebas Alienvault



Fuentes de integración del SIEM

Las fuentes que tiene integrado el SIEM para la detección de amenazas son las siguientes:

Tabla 1

Tabla de fuentes integradas en el SIEM

Fuentes integradas
Sophos XG (Firewall)
Sophos Central (antivirus)

Office 365
Kaspersky Security Center
Cisco Router
NIDS
Alienvault Agent
Windows Nxlog

El resumen de las fuentes integradas y su porcentaje de eventos se encuentran en el Anexo1.

Activos definidos

Como alcance del proyecto se tiene los siguientes activos el pentesting realizado sobre estos activos es de Caja Gris.

Tabla 2

Activos definidos

CANTIDAD	ACTIVOS
1	Office 365
2	Un dominio
3	IP internas: 192.168.2.18, 192.168.2.20
4	IP publica: 34.211.179.77

Reglas personalizadas en el SIEM

En la siguiente tabla se evidencia las reglas que se encuentran en producción y ejecutándose en el SIEM del SOC forma normal las cuales serán sometidas a pruebas de funcionamiento y eficacia a través del Hacking ético. En el Anexo 2 están las reglas del SIEM.

Reglas de correlación del SIEM

En total se tiene presentes en la herramienta Alienvaut 2140 reglas de correlación de eventos. Las reglas de correlación son un componente fundamental de los sistemas de detección y prevención de intrusiones (IDS/IPS), así como de los sistemas de gestión de eventos e información de seguridad (SIEM). Estas reglas son utilizadas para identificar patrones de eventos que pueden indicar una posible actividad maliciosa o anómala en un entorno de red o sistema informático.

Escaneo de vulnerabilidades

Se realiza un escaneo de vulnerabilidades de los activos que son parte de este alcance de proyecto el escaneo de las IP se realiza usando Nessus y ZAP.

Tabla 3

Escaneo de IPs

Riesgo	Activo	Nombre	Descripción
Medio	192.168.2.20	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0030)	Un problema de corrupción de memoria que puede provocar un escape del entorno limitado de ESXi. (CVE-2022-31696)

Riesgo	Activo	Nombre	Descripción
Medio	192.168.2.20	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0030)	Un problema de corrupción de memoria que puede provocar un escape del entorno limitado de ESXi. (CVE-2022-31696)
Medio	192.168.2.20	Las vulnerabilidades de SMBv2 MS09-50	Error de índice de matriz en la implementación del protocolo SMBv2 en srv2.sys en Windows Vista versión Gold, SP1 y SP2, Windows Server 2008 versión Gold y SP2, y Windows 7 RC, de Microsoft, permite a los atacantes remotos ejecutar código arbitrario o causar una denegación de servicio
Medio	Dominio	La política de seguridad de contenido (CSP)	La Política de Seguridad de Contenido (CSP, por sus siglas en inglés Content Security Policy) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, como XSS (Cross-Site Scripting) y otros exploits que implican la ejecución de código malicioso en sitios web.
Bajo	Dominio	Encabezado de respuesta X-AspNet-Version	El servidor divulga información mediante

Riesgo	Activo	Nombre	Descripción
			campo(s) de encabezado de respuesta HTTP "X-AspNet-Version"/"X-AspNetMvc-Version".

Optimización de reglas

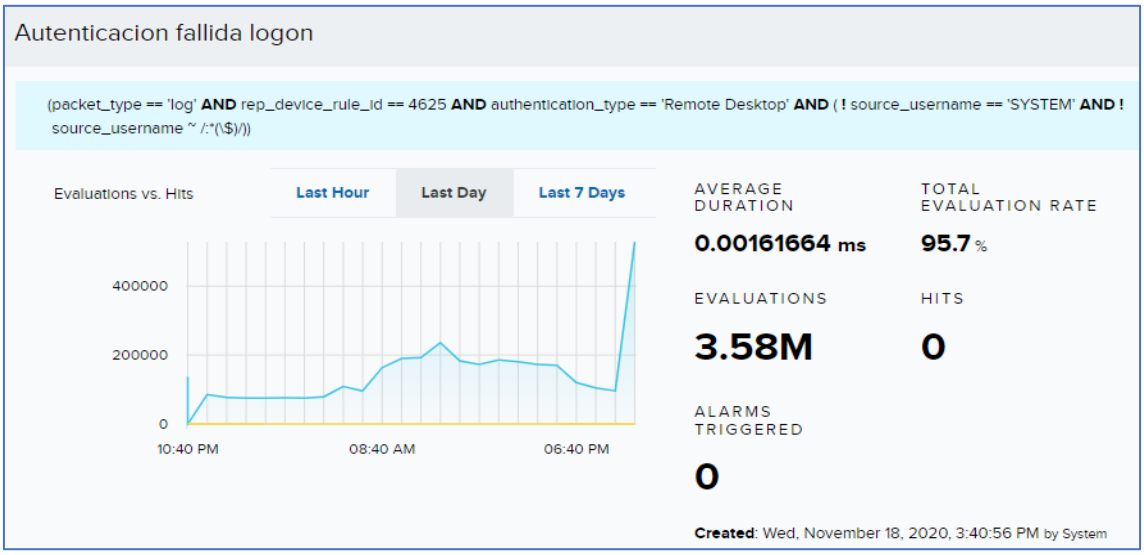
Para la detección de eventos nos basamos en los eventos que fueron detectados y no están siendo reportados ya que las reglas no están afinadas u optimizadas para un mejor alertamiento

Acceso fallido

La regla implementada tiene como parámetro para cuando se detecte el evento 4625 de Windows se alerte de un login fallido y sea de forma remota.

Figura 5:

Afinamiento de regla



Se revisa en el SIEM que la regla no está haciendo "*matching*" y no alerta los inicios de sesión fallidos, revisando los eventos del SIEM se detecta que el log de seguridad no tiene estos parámetros definidos cuando es detectado en el Office 365, el evento capturado durante la prueba es *UserLoginFiled*.

Detección del evento

En los logs de los eventos se detecta que cuando existe un inicio de sesión fallido la herramienta lo detecta como un InvalidUserorPassword, como se indica en la figura:

Figura 6:

Detección de evento

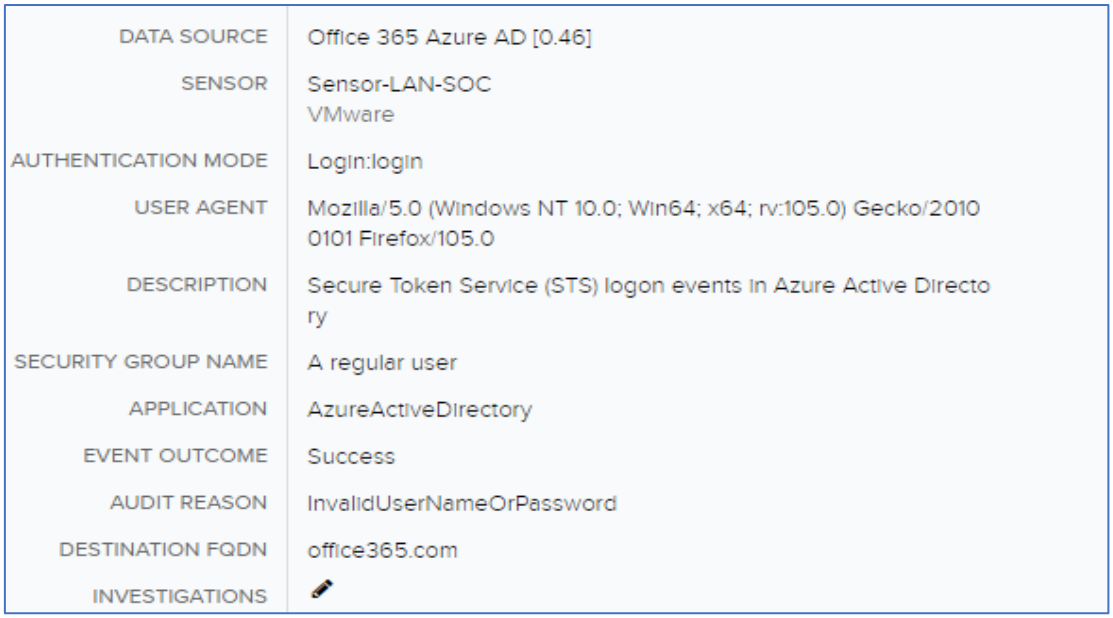


Tabla 4

Optimización de Regla de Login Failed Office 365

REGLA	**RIESGO**
Login failed OFFICE 365	BAJO
OBJETIVO	
Detectar un inicio de sesión fallido puede indicar que alguien está tratando de obtener acceso no autorizado a un sistema.	
MATRIZ MITRE ATT&CK	
Táctica: Credenciales de acceso	Técnica: Brute Force T1110
FUENTES DE INFORMACIÓN / DATASOURCES	

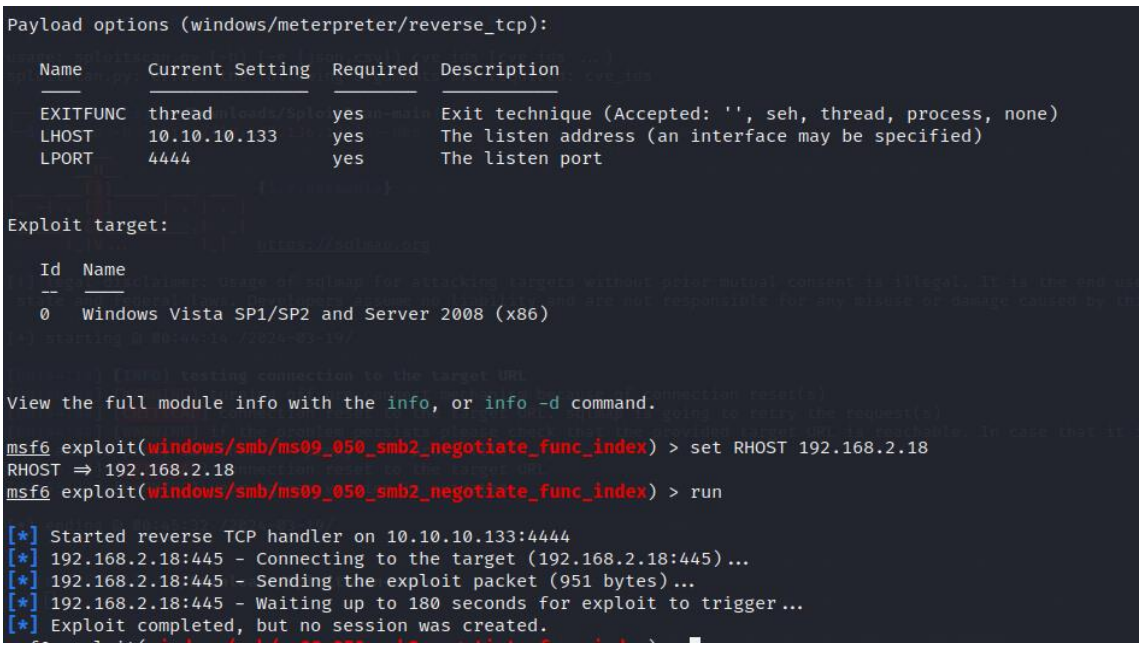
PLATAFORMA / SO	***Hostname / IP***	***Método de recolección***	***Observaciones***
OFFICE 365	OFFICE 365	SYSLOG	N/A
PARAMETROS DE EXCEPCIÓN			
N°	**Query**		
1	(packet_type == 'log' AND plugin == 'Office 365 Azure AD' AND event_description == 'Secure Token Service (STS) logon events in Azure Active Directory' AND security_group_name == 'A regular user' AND application == 'AzureActiveDirectory' AND event_outcome == 'Success' AND audit_reason == 'InvalidUserNameOrPassword' AND destination_fqdn == 'office365.com' AND destination_name == 'office365.com' AND event_name == 'UserLoginFailed')		

Pruebas de intrusión Metasploit

Mediante herramientas de hacking ético como un exploit se realiza la ejecución de pruebas de intrusión con el objetivo de explotar la vulnerabilidad ms09-050, donde se realiza la búsqueda del exploit y la ejecución.

Figura 7

Ejecución de exploit vulnerabilidad ms09_050 (CVE-2009-3103)

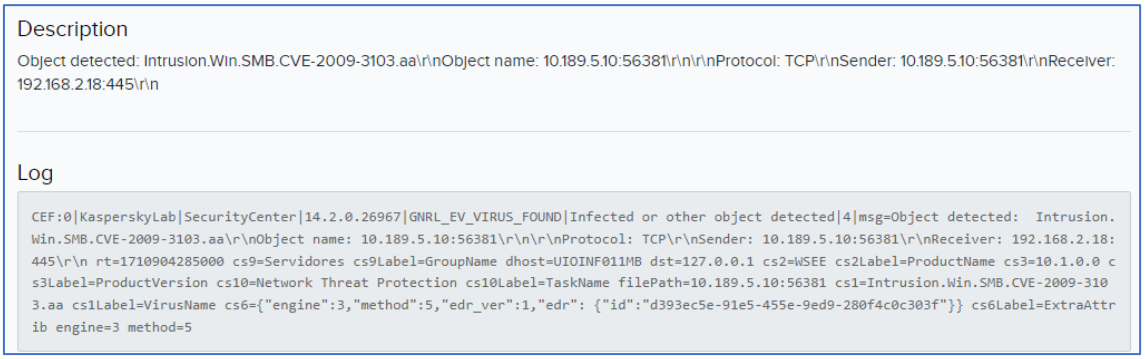


Evento detectado en el SIEM

En el SIEM se detecta los eventos de intrusión.WIN.SMB.CVE-2009-3103.

Figura 8

Pruebas de intrusión SMB.CVE-2009-3103

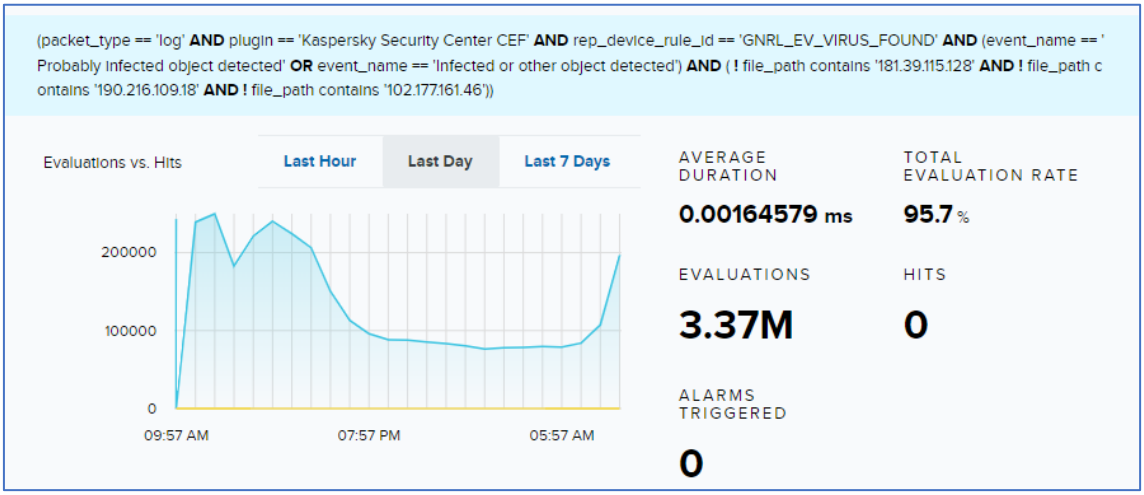


Alerta personalizada de Malicious File

La alerta que lo detecta es Malicious File, que hace referencia a un tipo de virus encontrado en el sistema y excluyendo algunas direcciones IP

Figura 9

Regla personalizada Malicious File



Optimización de regla de Explotación de Vulnerabilidades

Una de las amenazas más prevalentes de SOC es el ataque de explotación de vulnerabilidades CVE, que consiste en la utilización de debilidades o fallos en sistemas operativos, aplicaciones, redes o dispositivos para obtener acceso no autorizado. En respuesta a este hallazgo, se ha desarrolla una regla específica destinada a la detección de este tipo de ataques, con el propósito de contrarrestar dichas vulnerabilidades y salvaguardar la integridad de los sistemas. En la tabla siguiente se detalla los parámetros de configuración de la regla.

Tabla 5

Explotación de vulnerabilidades CVE

REGLA	RIESGO
Explotación de vulnerabilidades CVE	Medio
OBJETIVO	
Detectar un ataque de explotación de vulnerabilidades que se refiere al acto de aprovechar las debilidades o fallos en los sistemas operativos, aplicaciones, red o dispositivos para obtener accesos no autorizados.	

MATRIZ MITRE ATT&CK			
Táctica: Ejecución		Técnica: Explotación para la ejecución del cliente. T1203	
FUENTES DE INFORMACIÓN / DATASOURCES			
PLATAFORMA / SO	**Hostname / IP**	**Método de recolección**	**Observaciones**
Kaspersky	Kaspersky	SYSLOG	N/A
PARÁMETROS DE EXCEPCIÓN			
N°	**Query**		
1	(packet_type == 'log' AND plugin == 'Kaspersky Security Center CEF' AND malware_variant ~ /Intrusion\.Win\.[A-Za-z0-9_]+\.CVE-[0-9]+-[0-9]+/ AND event_name == 'Infected or other object detected')		

Para la optimización de la regla se usó regex en donde se indica que cuando se detecte una explotación de vulnerabilidad alerte con el nombre de Explotación de vulnerabilidades CVE.

Pruebas de Hacking ético

En esta sección detallaremos las pruebas de Hacking ético a las que fueron explotadas en la infraestructura de red del SOC, donde se encuentra implementado el SIEM.

Ejercicio 1- Ataque de Phishing

Se ejecuto un ataque de Phishing suplantando la identidad de Facebook, enviado desde una dirección IP sin reputación maliciosa.

Prueba ejecutada

Figura 10

Prueba de Phishing

Se consigue el acceso a suplantación de sitio de Facebook.

Figura 11

Suplantación de Facebook

Evento detectado en el SIEM

El evento es detectado por el antivirus como acceso denegado como lo muestra en los logs.

Figura 12

Evento de ataque de Phishing

Implementación de regla Phishing

La detección y prevención de ataques de phishing constituyen una preocupación primordial en el ámbito del SOC. En este contexto, se ha establecido una regla específica destinada a contrarrestar este tipo de fraude en línea, caracterizado por la suplantación de identidad de entidades legítimas con el propósito de obtener información confidencial. En la tabla siguiente, se argumentará la relevancia de esta regla en la corrección de vulnerabilidades asociadas con tales ataques, destacando su papel crucial en la protección de datos sensibles y la preservación de la integridad de los usuarios en el entorno digital.

Tabla 6

Regla de ataque de phishing

REGLA	**RIESGO**
Ataque Phishing	BAJO
OBJETIVO	
Detectar un ataque de phishing es una forma de fraude en línea en la que un atacante se hace pasar por una entidad legítima para engañar a las personas y obtener información confidencial, como contraseñas, números de tarjetas de crédito, información financiera o cualquier otro dato personal sensible.	

MATRIZ MITRE ATT&CK			
Táctica: Acceso Inicial		Técnica: Phishing T1566	
FUENTES DE INFORMACIÓN / DATASOURCES			
PLATAFORMA / SO	**Hostname / IP**	**Método de recolección**	**Observaciones**
Kaspersky	Kaspersky	SYSLOG	N/A
PARAMETROS DE EXCEPCIÓN			
N°	**Query**		
1	(packet_type == 'log' AND plugin == 'Kaspersky Security Center CEF' AND event_name == 'Acceso denegado' AND log ~ /\\/ajax\\/bz\?__a/)		

Ejercicio 2- Ataque de fuerza bruta VMWARE

Se realizó un ataque de fuerza bruta hacia el servidor de VMWARE que esta publicado en la IP 192.168.2.20.

Figura 13

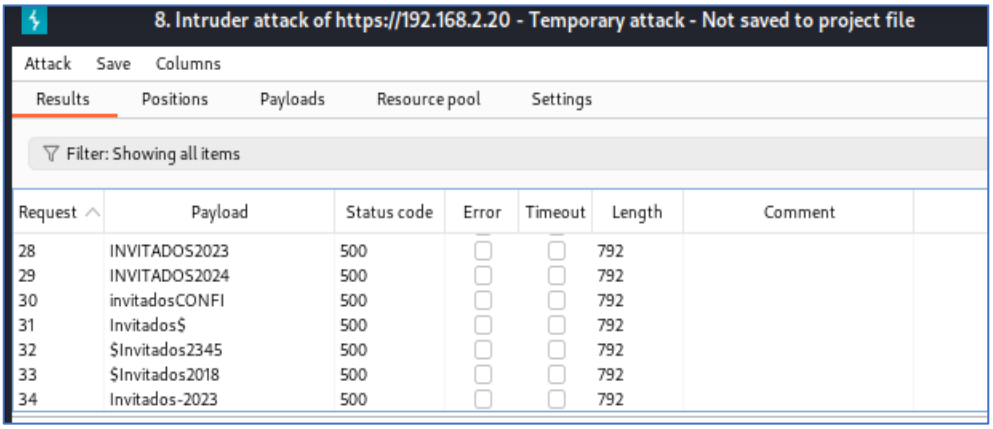
Interfaz gráfica del servidor WMWARE

Prueba de ejecutada

Por medio del Burp Suite, se ejecuta un ataque de fuerza bruta con un diccionario global para intentar acceder al sistema.

Figura 14

Ataque de fuerza bruta con Burp Suite

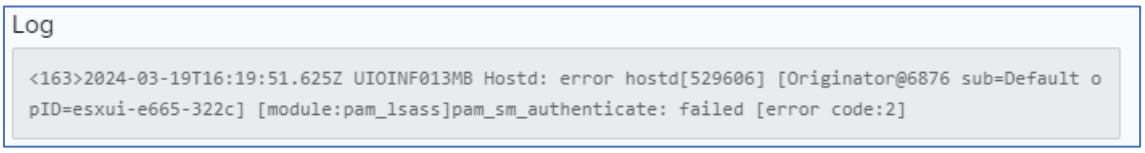


Evento detectado en el SIEM

Mediante la ejecución de ataque de fuerza bruta se detecta en el SIEM el evento que genera este tipo de pruebas que indica que el intento de autenticación fallo en el sistema.

Figura 15

Evento generado de autenticación



Implementación de regla Ataque de fuerza bruta VMWARE

Para el Centro de Operaciones de Seguridad (SOC) la protección de la información sensible son aspectos críticos en su entorno. Ante la amenaza constante de ataques de fuerza bruta, los cuales se caracterizan por su intento de acceso a sistemas o cuentas mediante la repetida adivinación de contraseñas, surgió la necesidad de crear o implementar una regla efectiva en la detección y prevención. Por lo tanto, se ha desarrollado una regla específica destinada a la detección de tales ataques, con el objetivo de contrarrestar esta técnica de intrusión y corregir las vulnerabilidades asociadas. Este la tabla siguiente se explorará la importancia de esta regla en la mitigación de riesgos de seguridad cibernética, subrayando su papel fundamental en la protección de la integridad de los sistemas y la salvaguardia de la información confidencial frente a las amenazas de fuerza bruta.

Tabla 7

Regla de ataque de fuerza bruta VMWARE

REGLA	**RIESGO**
Ataque de fuerza bruta VMWARE	BAJO
OBJETIVO	
Detectar un ataque de fuerza bruta es un método utilizado por los atacantes para intentar acceder a un sistema o cuenta adivinando repetidamente contraseñas o claves de acceso. La idea detrás de un ataque de fuerza bruta es probar todas las combinaciones posibles de contraseñas hasta encontrar la correcta.	

MATRIZ MITRE ATT&CK			
Táctica: Credenciales de acceso		Técnica: Brute Force T1110	
FUENTES DE INFORMACIÓN / DATASOURCES			
PLATAFORMA / SO	**Hostname / IP**	**Método de recolección**	**Observaciones**
VMWARE	VMWARE	SYSLOG	N/A
PARAMETROS DE EXCEPCIÓN			
N°	**Query**		
1	(packet_type == 'log' AND plugin == 'VMware Esxi' AND event_severity == 'error' AND source_process == 'hostd' AND event_name == 'ESXI Hostd event' AND log ~ /pam_sm_authenticate: failed/)]		

Ejercicio 3- Ejecución de NMAP

Con la herramienta Kali Linux a través de la ejecución de NMAP realizamos el descubrimiento de puertos y servicios que se puedan explotar, adicional se ejecuta con SCRIPT en busca de vulnerabilidades.

Figura 16

Ejecución de NMAP

Eventos detectados en el SIEM

Mediante el proceso de escaneo de NMAP se detecta el evento de listening_ports el cual es una vulnerabilidad significativa en la infraestructura del SOC. Basados en este hallazgo se procede a crear una regla la cual permita detectar un escaneo a través de la herramienta de NMAP para protegernos de un posible ataque, intrusión o prevenir el escaneo de vulnerabilidades.

Figura 17

Evento de NMAP


```
{
   "name": "listening_ports",
   "hostIdentifier": "8646804c-6e2e-469f-b455-066b80802d57",
   "calendarTime": "Tue Mar 26 03:26:03 2024 UTC",
   "unixTime": "1711423563",
   "epoch": 0,
   "counter": 60,
   "log_type": "result",
   "decorations": {
      "control_id": "606c399a-1e6b-48db-9369-0e8c187506f0",
      "optimized": "true",
      "source_asset_id": "8646804c-6e2e-469f-b455-066b80802d57"
   },
   "columns": {
      "family": "23",
      "file_path": "",
      "policy_address": "::1",
      "source_port": "49154",
      "source_process_commandline": "-1",
      "source_process_id": "4",
      "transport_protocol": "6"
   },
   "action": "added"
}
```

Implementación de regla de NMAP

Una preocupación recurrente de SOC y de todo el ámbito de la ciberseguridad, es la vulnerabilidad asociada al escaneo de puertos mediante herramientas como NMAP, que puede exponer los sistemas a riesgos de intrusión y explotación de vulnerabilidades. Por lo tanto y posterior al descubrimiento de esta vulnerabilidad en SOC se ha implementado una regla específica en SIEM con el objetivo de detectar y mitigar los escaneos realizados con NMAP, con el fin de prevenir posibles ataques y salvaguardar la integridad de la red. Este la siguiente tabla se detalla las características de esta regla en la protección proactiva de los sistemas contra amenazas de escaneo de puertos.

Tabla 8

Regla de escaneo de puertos NMAP

REGLA			**RIESGO**
Ejecución de NMAP			Bajo
OBJETIVO			
Detectar un escaneo a través de la herramienta de NMAP para protegernos de un posible ataque, intrusión o prevenir el escaneo de vulnerabilidades			
MATRIZ MITRE ATT&CK			
Táctica: Descubrimiento		Técnica: Descubrimiento de servicios de red. T1046	
FUENTES DE INFORMACIÓN / DATASOURCES			
PLATAFORMA / SO	**Hostname / IP**	**Método de recolección**	**Observaciones**
Aliennvault Agent	EC	Agente	N/A

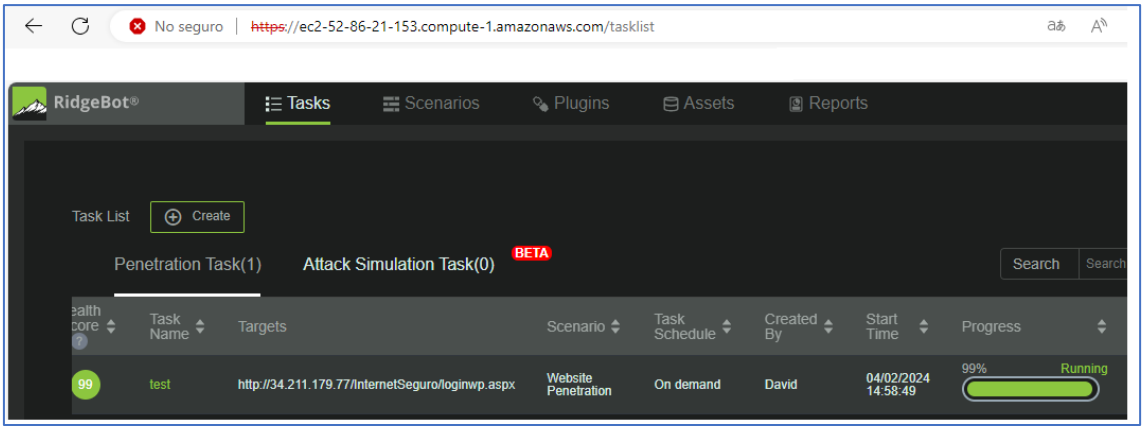
PARAMETROS DE EXCEPCIÓN	
N°	**Query**
1	packet_type == 'log' and plugin == 'AlienVault Agent' and event_action == 'added' and source_process_commandline == '-1' and policy_address == '::1' and event_name == 'Listening Port')

Ejercicio 4 Pruebas con Herramientas de automatización RidgeBot

A través de la herramienta de Hacking Ético automatizado que nos permite detectar las vulnerabilidades y realizar la explotación de estas.

Figura 18

Pruebas de hacking con RidgeBot



Mediante la ejecución de pruebas de automatización se revisa, en el SIEM que el datasource que lo detecta es los agentes de Alienvault, que clasifica la información como Windows Process Outbount Connections, que indica que un proceso del sistema se está comunicando con una IP de destino que es la IP de ataque.

Figura 19

Evento generado por RidgeBot


```
{
   "name": "windows_process_outbound_connections",
   "hostIdentifier": "8646804c-6e2e-469f-b455-066b80802d57",
   "calendarTime": "Tue Apr  2 20:24:53 2024 UTC",
   "unixTime": "1712089493",
   "epoch": 0,
   "counter": 2468,
   "log_type": "result",
   "decorations": {
      "control_id": "606c399a-1e6b-48db-9369-0e8c187506f0",
      "optimized": "true",
      "source_asset_id": "8646804c-6e2e-469f-b455-066b80802d57"
   },
   "columns": {
      "destination_address": "52.86.21.153",
      "destination_port": "59464",
      "family": "2",
      "file_path": "",
      "source_address": "172.31.25.81",
      "source_port": "443",
      "source_process": "System",
      "source_process_commandline": "-1",
      "source_process_id": "4",
      "transport_protocol": "6"
   },
   "action": "added"
}
```


Implementación de la regla

La regla que se configura cuando se detecta un proceso que en un sistema operativo Windows que está estableciendo conexiones salientes.

Tabla 9

Regla de procesamiento de conexiones Windows

REGLA	RIESGO
windows_process_outbound_connections	Medio
OBJETIVO	
Que un proceso en un sistema operativo Windows está estableciendo conexiones salientes. Esto significa que un programa en ejecución en el sistema está intentando comunicarse con otros dispositivos, servicios o servidores a través de la red.	
MATRIZ MITRE ATT&CK	

Táctica: Ejecución		Técnica: Servicio de sistema T1569.001	
FUENTES DE INFORMACIÓN / DATASOURCES			
PLATAFORMA / SO	**Hostname / IP**	**Método de recolección**	**Observaciones**
Alienvault Agent	EC	SYSLOG	N/A
PARAMETROS DE EXCEPCIÓN			
N°	**Query**		
1	(packet_type == 'log' AND plugin == 'AlienVault Agent' AND event_action == 'added' AND source_process == 'System' AND transport_protocol == 'TCP' AND event_name == 'Outbound connection' AND source_process_commandline == '-1' AND log ~ /windows_process_outbound_connections/)		

En la creación de la regla se toma como referencia el datasource que lo detecta, el nombre del evento que lo genera y dentro del Raw log se identifica el evento windows_process_outbound_connections

CAPÍTULO III

Análisis de resultados

A continuación, se validan las reglas implementadas por medio de la ejecución de los diferentes ataques:

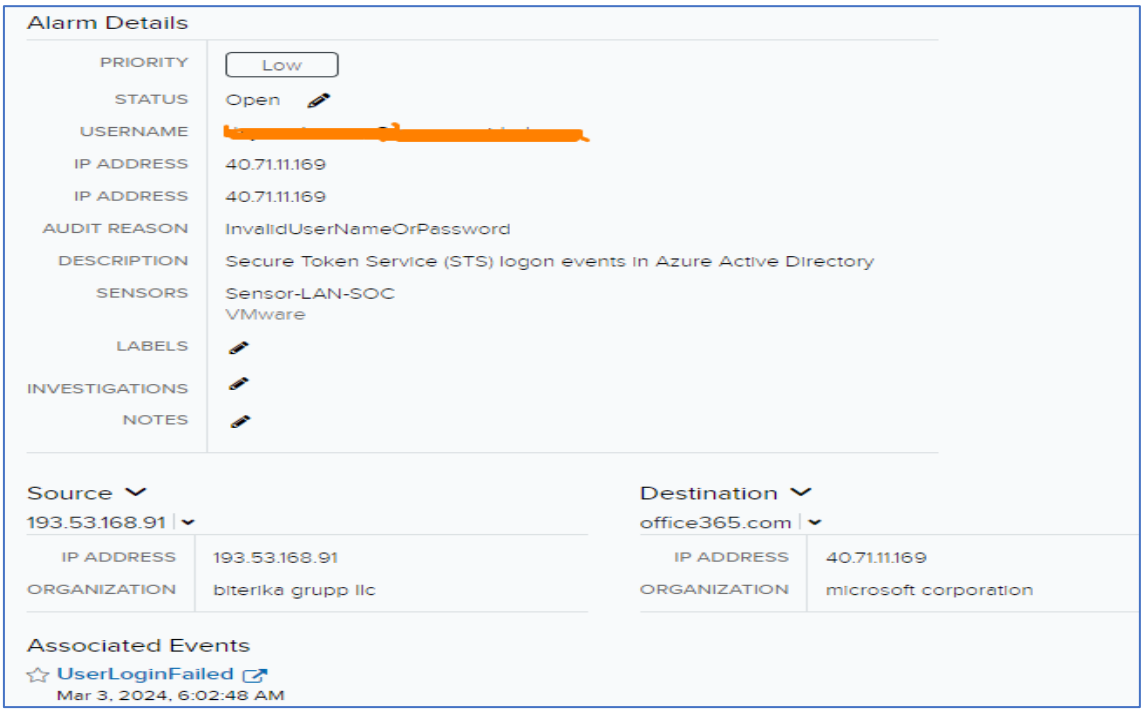
Optimización de reglas

Regla optimizada Login failed OFICE 365

La optimización de la regla de Login Failed nos permite ajustar y mejorar su detección en este caso se validó que solo se monitorea los eventos de Windows 4625 y no los eventos que genera el Office 365 de UserLoginFailed.

Figura 20

Evento de UserLoginFailed



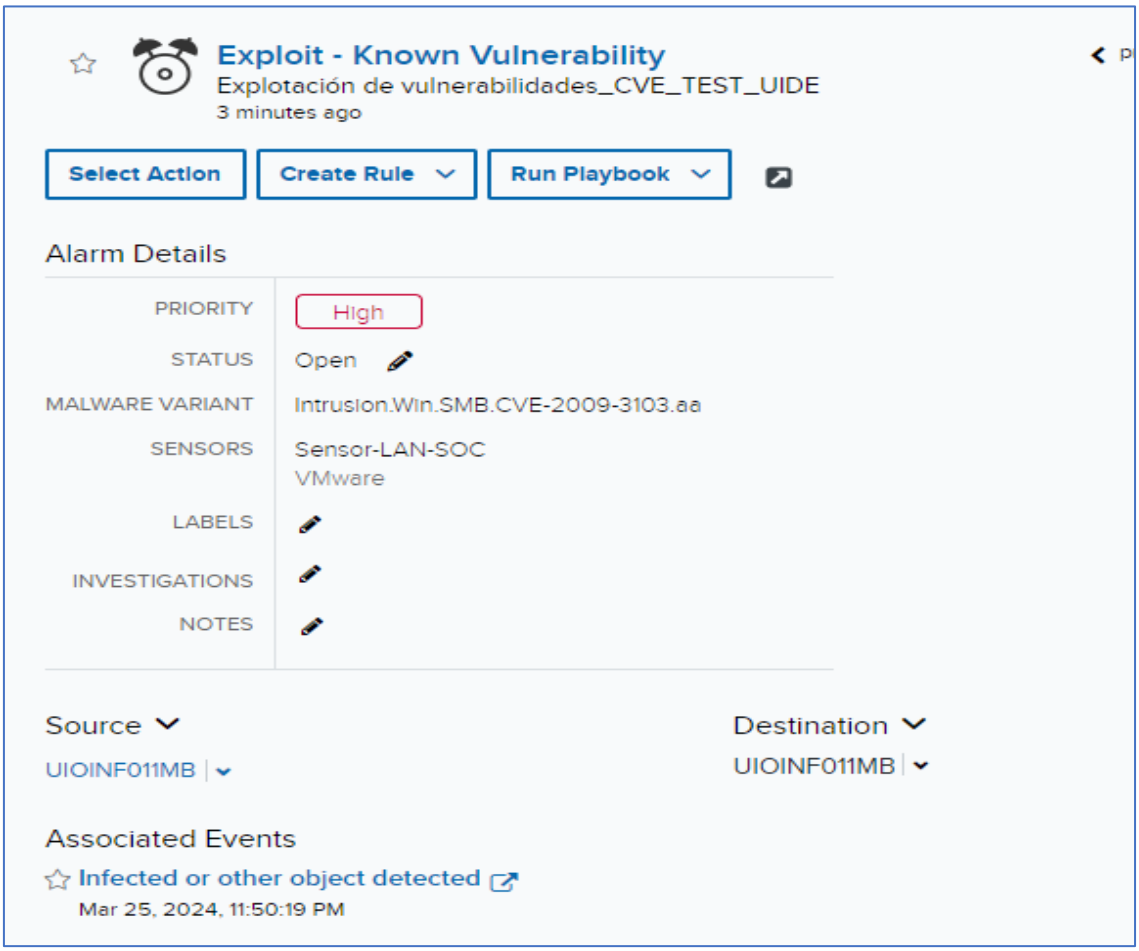
El evento demostró que el intento de sesión no tuvo éxito debido a que el nombre de usuario o la contraseña proporcionados son incorrectos o no coinciden con los registros del sistema.

Explotación de vulnerabilidades CVE

En respuesta a la explotación de vulnerabilidades CVE, se ha desarrolla una regla específica destinada a la detección de este tipo de ataques, con el propósito de contrarrestar dichas vulnerabilidades y salvaguardar la integridad de los sistemas. En la siguiente gráfica se detalla los parámetros de configuración de la regla.

Figura 21

Generación de alerta de vulnerabilidad Meta-exploit



Resultado

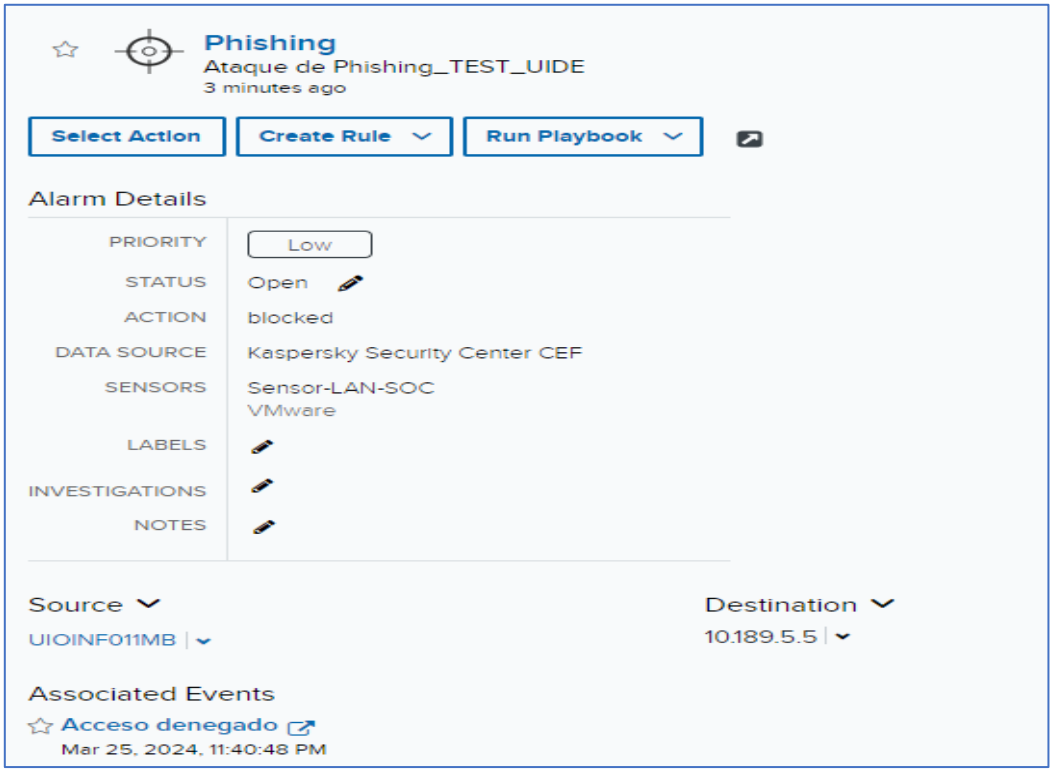
Luego de la implementación de la regla se ejecuta la prueba de validación con los resultados obtenidos muestra la ejecución de un Exploit.

Resultados de Ataque de Phishing

Se ha establecido una regla específica destinada a contrarrestar este tipo de fraude en línea, caracterizado por la suplantación de identidad de entidades legítimas con el propósito de obtener información confidencial. En la figura siguiente, se argumentará la relevancia de esta regla en la corrección de vulnerabilidades asociadas con tales ataques, destacando su papel crucial en la protección de datos sensibles y la preservación de la integridad de los usuarios en el entorno digital. En la imagen siguiente se cuenta con parámetros y características de la regla creada en el SIEM de SOC.

Figura 22

Generación de alerta Phishing



Resultado

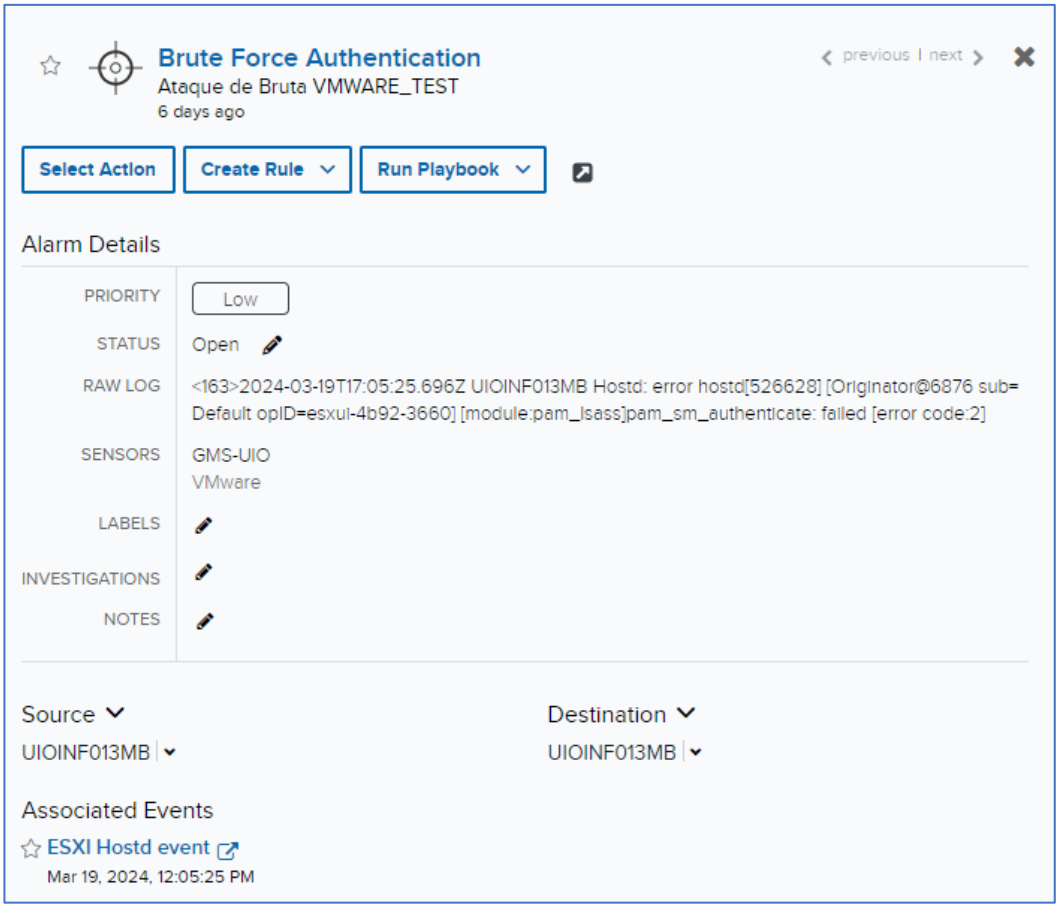
Tras la implementación de la regla, se lleva a cabo una evaluación de su desempeño mediante la realización de pruebas, cuyos resultados se analizan detenidamente y se corrige la vulnerabilidad.

Resultados de Ataque de fuerza bruta VMWARE

Posterior al descubrimiento de esta vulnerabilidad en SOC se ha implementado una regla específica en SIEM con el objetivo de detectar y mitigar los escaneos realizados con NMAP, con el fin de prevenir posibles ataques y salvaguardar la integridad de la red. Este la siguiente gráfica se detalla las características de esta regla en la protección proactiva de los sistemas contra amenazas de escaneo de puertos.

Figura 23

Generación de alerta de ataques de fuerza bruta



Resultado

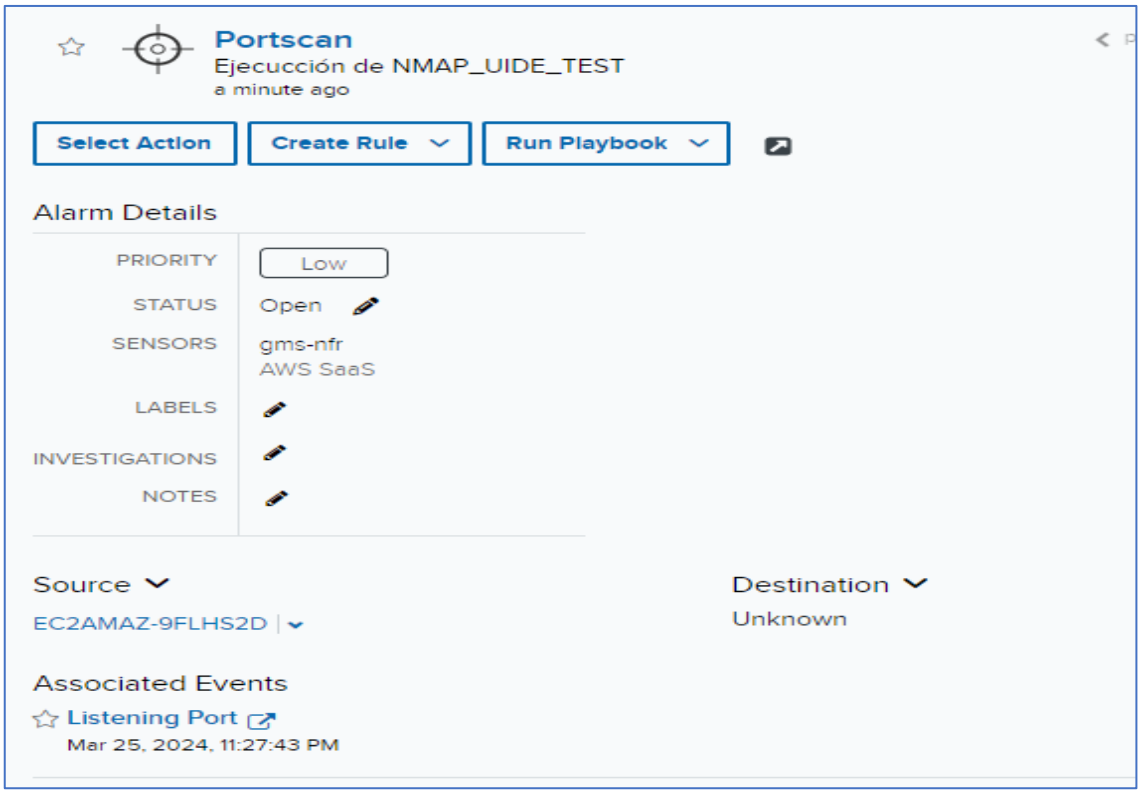
Luego de la implementación de la regla se realiza la prueba de ejecución y se valida que la regla funciona correctamente.

Resultados Escaneo de puertos NMAP

Basados en el análisis y resultados de pruebas de escaneo de puertos NMAP se ha implementado una regla específica en SIEM con el objetivo de detectar y mitigar los escaneos realizados con NMAP, con el fin de prevenir posibles ataques y salvaguardar la integridad de la red. Este la siguiente tabla se detalla las características de esta regla en la protección proactiva de los sistemas contra amenazas de escaneo de puertos. En la siguiente grafica se puede observar cada uno de los parámetros de configuración de esta.

Figura 24

Alerta de Portscan NMAP



Resultado

Una vez generada la regla se realiza la prueba de funcionamiento generando nuevamente el ataque NMAP.

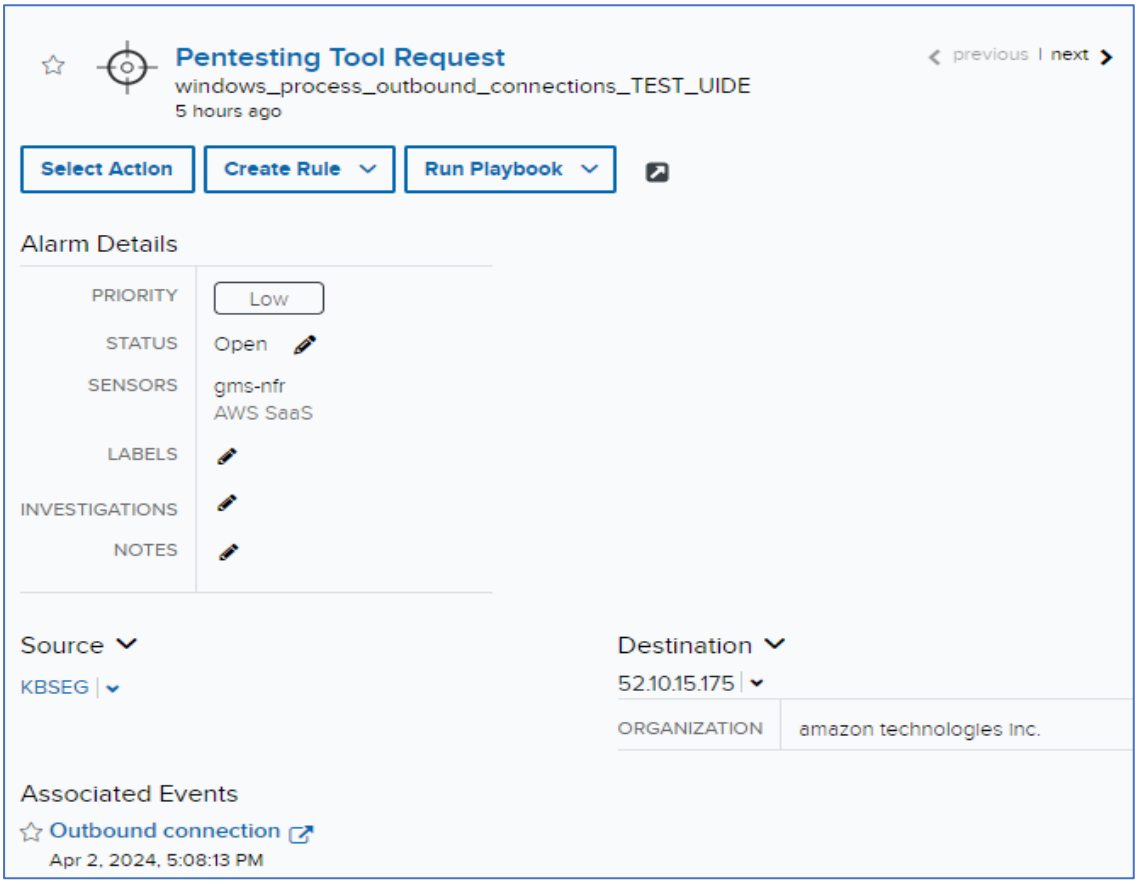
Pruebas con Herramientas de automatización RidgeBot

A realizar pruebas de automatizadas se generan dos eventos el primero es sobre un objeto infectado y el segundo sobre un proceso de Windows que se está comunicando con una IP saliente.

El resultado que se tiene luego de implementar la regla es la detención de esta actividad que se está ejecutando.

Figura 25

Pruebas con RidgeBot



Dentro de los eventos que se generaron cuando se aplicó un pentesting fue cuando un proceso se está comunicando con una IP, en este caso la IP es Amazon en donde se encuentra instalado RidgeBot que es 52.10.15.175.

CAPÍTULO IV

Conclusiones

- Se logró optimizar reglas de login fallidos, añadiendo el valor Invaliduser, en la regla de login fallido, la regla queda configurada de esta manera cuando detecte un login fallido valida el identificador 4625 o invaliduser.
- Con la ejecución de un exploit SMB.CVE-2009-3103, y no existía una regla que detecte este tipo de ejecuciones a partir de los eventos se creó una regla donde se utiliza Regex para la captura de CVE dentro de los eventos.
- Se hizo un ataque de fuerza bruta hacia la plataforma de VMWARE, y pruebas de NMAP que ayudaron a detectar eventos en el SIEM. Con estos datos se han creado nuevas reglas de detección.
- Usando una herramienta automatizada de RidgeBot, permitió detectar dos eventos el primero es sobre un objeto infectado y el segundo sobre un proceso de Windows que se está comunicando con una IP saliente, para este tipo de pruebas se creó una regla.
- La aplicación de técnicas SANS de Hacking Ético permitió documentar de manera detallada los hallazgos y debilidades detectadas en el sistema SIEM, proporcionando una base sólida para la mejora y afinación de las reglas y alertas existentes.
- La mejora y afinación de las reglas y alertas en el SIEM demostraron ser fundamentales para elevar su eficacia en la detección de amenazas. Esto se tradujo en una respuesta más rápida y precisa ante posibles incidentes de seguridad, mejorando así la capacidad de defensa del SOC frente a ataques cibernéticos.
- En las pruebas realizadas de escaneo se usaron herramientas como Nessus, NMAP, ZAP, entre otras. Cuando los eventos son dropeados o eliminados por las herramientas de seguridad no son visibles estos datos en el

SIEM, esto es debido que estos eventos son filtrados en el sensor del Alienvault con el fin de no sobre pasar la capacidad de almacenamiento.

Recomendaciones

- Se recomienda realizar evaluaciones periódicas del SIEM utilizando metodologías de Hacking Ético reconocidas, como la de Global Information Assurance Certifications SANS, para mantener un nivel óptimo de seguridad en el SOC.
- Es importante establecer un proceso de revisión continua de las reglas y alertas del SIEM para identificar y corregir cualquier debilidad o deficiencia en el sistema.
- Se sugiere la implementación de nuevas reglas y realizar pruebas de pentesting en conjunto con el cliente para detectar eventos que no se estén alertando ante un ataque o pruebas de Hacking Ético.
- Se recomienda mantenerse al tanto de las últimas tendencias y desarrollos en ciberseguridad y adaptar las reglas del SIEM en consecuencia, asegurando así una protección efectiva contra las amenazas emergentes.
- Se recomendable para este tipo de pruebas de pentesting que los clientes realizan, revisar que las fuentes que están integradas estén enviando este tipo de información o desarrollar sesiones para validar que tipos de eventos se generaron dentro del servidor y no fue detectada por el SIEM.

Referencias Bibliográficas

BV, E. (5 de 07 de 2021). *Science Direct*. Obtenido de SPEAR SIEM: Un sistema de gestión de eventos e información de seguridad para Smart Grid: https://www.sciencedirect.com/science/article/pii/S1389128621001237

Castro, B. A. (Diciembre de 2022). *Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft* . Obtenido de UIDE.

Cybersecurity, A. (21 de 03 de 2024). *Priority Field for Alarms*. Obtenido de https://cybersecurity.att.com/documentation/usm-anywhere/user-guide/alarms/alarms-list-priority-field.htm

DÍAZ, J. W. (01 de 07 de 2018). *PROPUESTA METODOLÓGICA Y SIMULACIÓN DE LA IMPLEMENTACIÓN DE UN SIEM BASADO EN LA NORMA ISO 27001 Y/O 27002* . Obtenido de TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN CONECTIVIDAD Y REDES DE TELECOMUNICACIONES .

Granadillo, G. G. (12 de 07 de 2021). *MDPI*. Obtenido de Gestión de eventos e información de seguridad (SIEM): análisis, tendencias y uso en infraestructuras críticas: https://www.mdpi.com/1424-8220/21/14/4759

Horalek, J., Neradova, S., & Marik, O. (22 de 06 de 2015). *IEEE XPLORE*. Obtenido de El despliegue de la gestión de eventos e información de seguridad en la infraestructura de la nube: https://ieeexplore.ieee.org/abstract/document/7128982

IT JETS. (23 de 04 de 2024). *RidgeBot Automated Pentesting*. Obtenido de https://itjets.com/ridgebot-automated-pentesting.html

LOGPOINT. (07 de 05 de 2024). *Top 10 SIEM use cases to implement*. Obtenido de https://www.logpoint.com/en/top-10-use-cases-implement/#

Palo Alto Networks. (23 de 04 de 2024). *Cyberpedia*. Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-matrix

QUIROZ, M. A. (9 de Agosto de 2020). *DISEÑO DE UN SECURITY OPERATIONS CENTER (SOC), MEDIANTE LA IMPLEMENTACIÓN DE ROLES DEFINIDOS POR EL INSTITUTO SANS PROPORCIONANDO LAS FUNCIONES DE RECOPILAR Y FILTRAR DATOS, DETECTAR Y CLASIFICAR AMENAZAS, ANALIZAR E INVESTIGAR AMENAZAS Y LA IMPLEMENTACIÓ*.

(U. P. QUITO, Ed.) Obtenido de Trabajo de titulación previo a la obtención del título de: Ingeniera e Ingeniero de Sistemas .

Ramirez, R. (07 de 05 de 2021). *Ciberseguridad.blog*. Obtenido de Las mejores prácticas para implementar una estrategia SIEM: https://ciberseguridad.blog/las-mejores-practicas-para-implementar-una-estrategia-siem/

Ridge Security Technology Inc. (07 de 05 de 2024). *RidgeBot Automated Penetration Testing Acceptance Criteria*. Obtenido de RidgeBot Test Acceptance Criteria: https://portal.ridgesecurity.ai/dashboard

TT&T Cybersecurity. (23 de 04 de 2024). *USM Anywhere*. Obtenido de https://cybersecurity.att.com/products/usm-anywhere

Apéndice A.

Fuentes integradas y porcentaje de eventos

Tabla A1

Fuentes integradas y porcentaje de eventos

Data Source	Events	Total
Sophos XG	14.089.445	61.4 GB
Sophos XG	7.410.094	23.8 GB
AlienVault Agent - Windows EventLog	1.449.163	5.6 GB
AlienVault Agent	1.401.652	4.4 GB
Office 365 Exchange	577.925	3.1 GB
Sophos Central JSON	977.154	2.1 GB
Office 365 Azure AD	52.721	241.5 MB
Office 365 Audit	42.752	122.1 MB
User Entity and Behavior Analytics	43	136.4 kB
Sophos XG	1.564.503	4.6 GB
Sophos XG	1.076.776	3.5 GB
AlienVault Generic Data Source	2	2.6 kB

Apéndice B.

Tabla B1

Reglas personalizadas

Fuente	Caso de uso	Descripción
Firewall	Malicious Network Activity — Conexiones desde IP maliciosas	Detección de conexiones desde IP que poseen indicadores de compromiso.
Firewall	Malicious Network Activity — Conexiones hacia IP maliciosas	Detección de conexiones Hacia IP que poseen indicadores de compromiso.
Windows Nxlog	Account Manipulation — User account was deleted	Detección de eliminación de cuentas por personal de no autorizado.
Windows Nxlog	Account Manipulation — A User Account was Disabled	Detección de deshabilitación de cuentas por personal no autorizado
Windows Nxlog	Account Manipulation — A user account was created	Detección de habilitación y creación de cuentas de usuarios por personal no autorizado

Windows Nxlog	Account Manipulation — A user account was changed	Modificación de cuentas de usuario por personal no autorizado
Firewall	Malicious Network Activity — comunicaciones no autorizadas	Detectar comunicaciones no autorizadas desde Países atacantes
Firewall	C&C Communication — Malware Command and Control IPs	Alertar cuando se detecta comando y control desde una IP interna hacia una publica con Indicadores de compromiso
Firewall	Configuration Modification — Configuration Changed by Administrator	Modificación o cambio realizados en el firewall
Firewall	Suspicious Behavior —User Connects to VPN_Fuera de horario laboral	Conexiones a la VPN luego de un horario laboral
WAF	Web Server Attack — Ataque desde IP maliciosa	Conexiones desde IP maliciosas desde WAF
Kaspersky	Malware Infection — Se detectó un objeto malicioso	Objeto malicioso detectado por Kaspersky
Kaspersky	Malware Infection — Ataque de red detectado	Ataque de red detectado por Kaspersky

Kaspersky	Malware Infection— Objeto Probablemente Infectado	Se ha detectado un objeto que probablemente esté infectado, por Kaspersky
Kaspersky	Malware Infection — No se puede desinfectar	Un objeto no se puede desinfectar por Kaspersky
Kaspersky	System Error — Faltan las bases de datos o están dañadas	Faltan las bases de datos o están dañadas, evento que muestra la actualización de la base de datos fallo.
Kaspersky	System Error — Las bases de datos están desactualizadas	Las bases de datos están desactualizadas, las tareas de actualización no se han completado
Windows Nxlog	Software - Remote Desktop — Autenticacion exitosa logon RDP	Autenticación exitosa por conexión remota