Universidad Cenfotec

Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

Casos de uso resilientes SIEM

Morales Morera Randy

Sanabria Echeverría Elio Andrés

Marzo 2020

DECLARATORIA DE DERECHOS DE AUTOR

Se autoriza a la Universidad Cenfotec hacer uso de todo el contenido o parte de lo que contiene esta tesis con fines estrictamente académicos, investigación o de consulta.

AGRADECIMIENTOS

Nos gustaría agradecer a todos nuestro familiares, amigos y profesores que nos han inspirado e impulsado a finalizar nuestra tesis. Además, a las personas que en este momento están leyendo esta tesis, por su tiempo y su retroalimentación para mejorar nuestros conocimientos. Esperamos que estén orgullosos de nuestro trabajo y aguardamos con ansias los demás retos.

¡Todos ustedes han sido y siempre serán la clave para nuestro éxito!

Nuestro pequeño aporte para nuestra gran meta: exponer a Costa Rica como un país lleno de expertos en ciberseguridad.

Lic. Randy Morales Morera

Ing. Elio A. Sanabria Echeverría

TABLA DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

RESUMEN EJECUTIVO

El objetivo de este proyecto es proveer un modelo para el ajuste y tuneo de las alertas de seguridad. Además, desarrollar una cultura de mejora continua para los equipos de seguridad de la información encargados de correlacionar los eventos, también conocidos como SIEM (Security Information and Event Management).

Para esto, se describieron las funciones, funcionamiento de los centros de operaciones de seguridad y su importancia para proteger el negocio de las amenazas, tanto externas como internas, en orden de salvaguardar los principios de confidencialidad, integridad y disponibilidad de la información. De igual forma, se explicó la visibilidad que provee un centro de operaciones de seguridad para comprender mejor el entorno y los riesgos a los que se enfrentan los negocios.

De acuerdo con el giro de negocio, las amenazas de seguridad son diferentes y su impacto varía según la industria. Por eso, se detallaron los diferentes incidentes de seguridad que puede enfrentar una organización, además se explicó el daño que estos pueden causar en las operaciones del negocio.

Se llevó a cabo una categorización y tipificación de los incidentes de seguridad más comunes, con el fin de facilitar la detección, el análisis y su contención, de una manera oportuna. Con esto, las organizaciones podrán prevenir varios incidentes con un mismo control y disminuirá el impacto que pueda casar la materialización de un riesgo.

Los equipos SIEM son el núcleo de un centro de operaciones de seguridad (SOC), en estos se monitorean las posibles amenazas, basados en el análisis de los datos obtenidos de los diferentes *logs sources*. En este documento se desarrolló una metodología de creación de casos de usos resilientes enfocados en una cultura de mejora continua, mediante la reducción de falsos positivos y al configurar correctamente los límites para evitar falsos negativos.

Capítulo I. Problema y propósito

1.1. Antecedentes del problema

En la actualidad, los ataques informáticos son más complejos y la constante innovación por parte de los cibercriminales obliga a las organizaciones a implantar nuevos dispositivos y técnicas para ser resilientes ante las amenazas emergentes. Debido a esto, era imperativo crear una unidad en la organización que permita monitorear y mitigar los riesgos que enfrenta.

Los centros de operaciones de seguridad (SOC) satisfacen esta necesidad y, con el paso de los años, se han convertido en la piedra angular de la división de seguridad de la información. Desde esta unidad se administran y monitorean todos los dispositivos encargados de ser líneas de defensa contra los cibercriminales y amenazas internas, esto brinda una radiografía digital de la postura de seguridad de la organización.

A pesar de esto, la gran cantidad de datos que generan estos dispositivos, la administración de múltiples plataformas y el monitoreo de sus registros, aumentan las cargas de trabajo a un departamento que usualmente esta corto de personal. El uso de una plataforma centralizada que permita integrar todos los *logs sources* posibles es imperativo. La implementación de soluciones SIEM ayudan a gestionar y monitorear los registros de múltiples plataformas en un único punto. Anudado a esto, las capacidades de correlación de estos equipos brindan una capa extra de visibilidad que permite llevar a cabo los análisis de posibles amenazas, de una forma más flexible y profunda, mediante el uso de filtros para búsquedas avanzadas.

No obstante, una solución SIEM sin el ajuste, actualización de las reglas o casos de uso configurados, se convierte únicamente en un repositorio de registros. La creación, actualización e incluso eliminación de reglas deben gestionarse, de manera periódica. Una solución SIEM sin ajuste de reglas puede generar miles de alertas por día, de las cuales un gran porcentaje estará relacionado con falsos positivos. Esto previene la visibilidad sobre eventos de seguridad más relevantes como los verdaderos

positivos.

1.2. Motivación e importancia del estudio

Herramientas como el SIEM solventan el problema que muchos ambientes empresariales presentan, es decir, la unificación de los registros de toda la empresa, sin importar de la marca que sea el dispositivo. La toma de esos registros permite correlacionarlos con una serie de reglas e inteligencia de amenazas para buscar patrones o posibles brechas de seguridad.

A pesar de ser una herramienta esencial para la visibilidad de eventos de seguridad informática por su complejidad, no existe una guía de buenas prácticas sobre el tuneo y entendimiento de esta. Ningún vendedor de este tipo de herramienta o universidad que tenga seguridad de la información entre su currículo de materias tiene una guía en la que se especifique la creación de casos de uso o tuneo de falsos. Estas actividades son esenciales para dar la visibilidad ideal de los eventos de seguridad en los ambientes que se monitorean. Esto ha provocado una demanda importante por parte de empresas que tienen estas herramientas de una guía que facilite esto o de personal calificado que los guie para optimizar su uso.

En la actualidad, el conocimiento es proveído por la experiencia del personal o por capacitaciones por parte de las empresas que venden estas herramientas. Esto genera una transferencia de conocimiento no estandarizada ni regulada por ningún marco de referencia de esta herramienta.

1.3. Planeamiento del problema

1.3.1. Problema general

Debido al déficit que ya existente de ingenieros capacitados sobre temas de ciberseguridad, surge una necesidad secundaria sobre una metodología para la mejora y el entendimiento de las reglas en un ambiente SIEM. En la actualidad, el personal encargado de estas actividades posee un conocimiento estandarizado sobre ciberseguridad, pero carecen de una guía especializada de buenas prácticas para maximizar el uso y visibilidad sobre los eventos de seguridad con esta herramienta.

La demanda de ingenieros especializados en manejo de herramientas SIEM se debe al crecimiento de los ambientes tecnológicos en los que existen miles de fuentes de *logs* desde computadoras, teléfonos, servidores, antivirus, *firewall*, IDS, IPS, etc. los cuales generan *gigabytes* de registros informacionales y de seguridad. Estos deben analizarse y correlacionarse para observar los eventos importantes que pueden ser una pista de un ambiente comprometido por un ataque cibernético. Desafortunadamente, esto no sucede con frecuencia porque las herramientas SIEM no han sido tuneadas para maximizar la detección de estas amenazas y no existe una metodología para optimizar los casos de uso.

Lo anterior, lleva a la gran interrogante de este proyecto: ¿De qué manera se podría incluir una metodología estándar que facilite la identificación de brechas sobre la cobertura de amenazas y la mejora continua de reglas en un ambiente SIEM?

1.3.2. Problemas específicos

A partir de esta cuestión se plasman preguntas más profundas en las cuales se busca responder la interrogante principal. Esto pretende brindar un alcance medible y extraer las áreas principales del problema que se busca responder en este proyecto.

- ¿Cuáles son las brechas de cobertura en un ambiente SIEM?
- ¿Cuáles son los problemas con las reglas que vienen por defecto en un dispositivo SIEM?
- ¿Cómo crear casos de usos resilientes en el ambiente SIEM de la manera óptima?
- ¿Cómo optimizar una regla en el ambiente SIEM?
- ¿Cómo se puede identificar las oportunidades de tuneo de un ambiente SIEM?

1.4. Objetivos

1.4.1. Objetivo general

Proponer un modelo para el mejoramiento continuo de reglas resilientes y entendimiento de una línea base en un ambiente SIEM.

1.4.2. Objetivos específicos

1. Describir el funcionamiento de un centro de operaciones de seguridad.
2. Comprender tendencias más recurrentes de patrones de ataque hacia una empresa.
3. Identificar brechas en la cobertura de la situación actual en el ambiente monitoreado.
4. Categorizar y tipificar los posibles incidentes de seguridad.
5. Desarrollar una guía para ajuste y mejoramiento de las reglas de seguridad.

1.5. Alcances y límites

1.5.1. Alcances

El proyecto tendrá como alcance la propuesta de un modelo que consta de buenas prácticas generales para el aprovechamiento de una herramienta SIEM. Además, se establecerá los requerimientos mínimos necesarios para optar por el nivel óptimo de utilización de los principios presentados. Se propondrán técnicas de identificación de brechas de cobertura, según las etapas de un ataque y creación de casos de uso con resiliencia.

Además, el proyecto no pretende dar un proceso paso a paso, sino una guía de buenas recomendaciones de lo que se puede aplicar a un SIEM para su aprovechamiento y dar mayor visibilidad a los eventos de seguridad importantes.

1.5.2. Limitaciones

Las limitantes de que marcaran el ámbito investigativo de este proyecto incluyen:

- Las recomendaciones se darán de una manera generalizada y pueden aplicarse a cualquier ambiente sin importar la marca del SIEM.
- El modelo se limitará únicamente al SIEM y dejará por fuera las recomendaciones de cada uno de los *logs sources*.
- Para el modelaje de una visión general del ambiente se ha elegido la metodología *cyber killchain*.
- Para la creación del modelo se cuenta con el tiempo establecido por el mentor asignado por la universidad. Cualquier extensión de este será notificada por los estudiantes, con justificación para la universidad.

Capítulo II. Marco teórico

2.1. Monitoreo de eventos

ITIL v3 define un servicio como “Un medio de entregar valor a los clientes facilitando los resultados que estos quieren lograr, sin asumir la propiedad de los costos y riesgos específicos” (s. f., s. p.). En la actualidad, los servicios ofrecidos por el Departamento de Tecnologías de la Información son cruciales para todas las empresas, estos son un habilitador efectivo, sin importar el giro de negocio. Por lo tanto, resulta evidente la necesidad de llevar a cabo una gestión y operación correcta de los servicios de TI.

En relación con este objetivo ITIL V3 indica que:

> El propósito de la operación de los servicios consiste en coordinar y realizar las actividades y procesos requeridos para entregar y gestionar servicios ofrecidos a los usuarios de negocio y clientes finales en los niveles acordados, siendo también responsable de la administración tecnológica que es usada para proveer y soportar dichos servicios (s. f., s. p.)

Para cumplir con esa responsabilidad, uno de los procesos fundamentales que soportan la correcta gestión de servicios de TI corresponde a la gestión de eventos. Este se encarga de monitorear todas las actividades que ocurren en la infraestructura de TI para permitir su operación correcta; salvaguardando la confidencialidad, integridad y disponibilidad de información, mediante la detección, análisis y escalación de condiciones anómalas. Un evento puede ser definido como cualquier ocurrencia detectable que sea significativa para la gestión de la infraestructura de TI y los servicios que esta soporta.

Por lo tanto, una gestión de eventos efectiva depende del conocimiento del estado de la infraestructura de TI, a través de la detección oportuna de cualquier desviación de la operación normal o esperada. Esto se logra mediante herramientas de monitoreo que permiten censar la infraestructura de TI para determinar su estado, disponibilidad y encontrar cualquier amenaza que puede causar una interrupción de los servicios.

Cualquier excepción al comportamiento normal de las operaciones, generará una alerta que deberá detectarse por el sistema de monitoreo y comunicada, de una manera, efectiva a los equipos correspondientes, así se podrán tomar las acciones necesarias para evitar o contener un incidente de seguridad.

2.2. Herramientas para la seguridad de redes

2.2.1. SIEM

SIEM o Security Information and Event Management (por sus siglas en inglés) es definido por Piggeé como “un conjunto complejo de tecnologías reunidas para proporcionar una visión holística dentro de la infraestructura técnica, el flujo de trabajo, cumplimiento y la gestión de registros” (s. f., s. p.). Según Jamil:

> Las siglas SEM, SIM y SIEM se han utilizado indistintamente, aunque hay diferencias en el significado y las capacidades del producto. El segmento de gestión de la seguridad que se ocupa del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola que comúnmente se conoce como Gestión de Eventos de Seguridad (SEM). La segunda área ofrece almacenamiento a largo plazo, el análisis y la comunicación de los datos de registro, y se conoce como Gestión de Seguridad de la Información (SIM) (s. f., s. p.).

Nicolett y Williams (2005), utilizan el término SIEM para describir las capacidades de los productos de la recopilación, análisis y presentación de datos de la red y los dispositivos de seguridad, las aplicaciones de gestión de identidades y accesos, gestión de vulnerabilidades y los instrumentos de política de cumplimiento, sistema operativo, base de datos y registros de aplicaciones. Un punto clave es monitorear y ayudar a controlar los privilegios de usuario y de servicio, servicios de AD y otros cambios de configuración del sistema, así como el abastecimiento de auditoría de registro, revisión y respuesta a incidentes.

Lane (s. f.), estratega de seguridad con más de 22 años de experiencia en la industria, define las siguientes capacidades de un SIEM:

- Agregación de datos: (administración de registros) soluciones para administración de registros desde muchas fuentes, incluyendo redes,

seguridad, servidores, bases de datos, aplicaciones, lo que da la capacidad de consolidar los datos monitoreados para evitar la pérdida de los acontecimientos cruciales.

- Correlación: busca los atributos comunes y relaciona eventos en paquetes o incidentes. Esta tecnología proporciona la capacidad de llevar a cabo una variedad de técnicas de correlación para integrar diferentes fuentes, con el fin de convertir los datos en información. La correlación es típicamente una función de la parte de gestión de la seguridad en una solución SIEM completa.
- Alerta: el análisis automatizado de eventos correlacionados y la producción de alertas, para notificar a los destinatarios de los problemas inmediatamente. Una alerta puede ser un tablero de instrumentos o enviarse a través de canales de terceros, como el correo electrónico.
- Dashboards: herramientas para tomar los datos del evento y convertirlo en tablas informativas para ayudar a ver patrones o identificar una actividad que no está siguiendo un patrón estándar.
- Cumplimiento: las aplicaciones SIEM se pueden emplear para automatizar la recopilación de datos y la elaboración de informes que se adapten a los procesos existentes de seguridad, gobernabilidad y auditoría.
- Retención: SIEM emplea soluciones a largo plazo de almacenamiento de datos para facilitar la correlación de estos con el tiempo y para proporcionar la retención necesaria para los requisitos de cumplimiento. Un largo plazo de retención de registros de datos es crítico en la investigación forense, ya que es poco probable que el descubrimiento de una violación de la red sea en el momento de que la infracción se produzca.

2.2.2. Log sources

Aunque no forman parte del sistema SIEM, las fuentes de eventos son una parte fundamental de la arquitectura, ya que sus capacidades, propiedades y ubicación en

la red son esenciales para el éxito de la operación de monitoreo de eventos de seguridad. Un *log sources* es el producto de cualquier dispositivo que genera algún tipo de notificación de un evento. Por ejemplo, en el caso de antivirus en un dispositivo, cuando un escaneo inicia y se encuentra algún tipo de amenaza en el sistema, genera una notificación de registro.

Otros ejemplos de dispositivos los *logs sources* pueden ser: computadoras de usuario final, una base de datos, *firewalls*, antivirus, servidores de autenticación, IDS, IPS, etc. Por lo general, hay varios sensores distribuidos por toda la infraestructura monitoreada, que cubren los diversos componentes. Esos sensores son responsables de generar los eventos de seguridad, representados generalmente como bloques de texto con un formato predeterminado. Los sensores de *hardware* son normalmente de naturaleza más simple, generalmente miden variables físicas y generan un solo valor que varía a través del tiempo. Por otro lado, los sensores de *software* pueden ser más complejos, con la capacidad de llevar a cabo procedimientos de autenticación para acceder a datos protegidos.

2.2.3. Firewall

Según Microsoft, “es un software o hardware que comprueba la información procedente de internet o de una red y bloqueo permite el paso de esta al equipo, en función de la configuración de esta” (2015, s. p.). Esto significa que es un dispositivo que se configura para que solo la información esperada llegue a la red en la que se encuentra el dispositivo. Existen múltiples capacidades de un firewall, ellos pueden configurarse para bloquear direcciones IP, puertos o hasta generar casos de usos muy específicos (por ejemplo, bloquear todo tráfico entrante que sea mayor a 500 bytes).

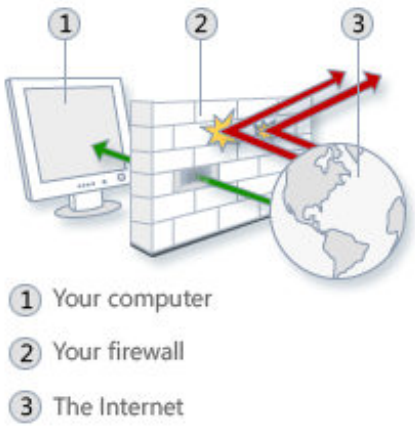

Ilustración 1. Funcionalidad de un firewall

Fuente: Microsoft, 2015.

Debido a sus capacidades, se puede afirmar que es una de las herramientas esenciales en tema de la ciberseguridad, además, puede brindar protección en todas las capas del modelo OSI. Es decir, es una pieza fundamental que imposibilita que atacantes externos logren penetrar un sistema o una red y roben información confidencial. Existen diferentes tipos de *firewall* de los cuales se categorizan entre un *firewall stateless* y uno *stateful*

2.2.3.1. Firewall stateless

Un *firewall* stateless es una versión más simple de un *firewall* normal, esto puede servir para una red de tamaño mediano o pequeño, según propósito de la seguridad que tenga. Según Mojidra:

> Ven el tráfico de red y restringen o bloquean paquetes basados en direcciones de origen y de destino u otros valores estáticos. No están 'conscientes' de los patrones de tráfico ni de los flujos de datos. Un *firewall* stateless utiliza conjuntos de reglas simples que no explican la posibilidad de que un paquete sea recibido por el *firewall* 'pretendiendo' que es algo que usted pidió (2016, s. p.).

En resumen, estos dispositivos cumplen meramente con los principios básicos de la seguridad.

2.2.3.2. Firewall stateful

A diferencia de los *firewalls stateless*, estos son un poco más complejos. Se caracterizan por ver el tráfico, a través de todas las capas del modelo OSI. Mojidra explica:

> Los *firewalls* stateful pueden ver flujos de tráfico de extremo a extremo. Son conscientes de las vías de comunicación y pueden implementar diversas funciones de seguridad IP, como túneles y cifrado. En términos técnicos, esto significa que los *firewalls* stateful pueden indicar en qué etapa está una conexión TCP (2016, s. p.).

Cabe destacar que uno no es superior al otro, son diferentes tipos de tecnologías que deben tomarse encuentra en el momento de implantar cualquiera de estas, según la necesidad del negocio.

2.2.4. Proxy

Un proxy es un representante o intermediario entre las comunicaciones de un dispositivo local hacia el mundo exterior, en este caso el Internet. Se puede afirmar que un proxy por su naturaleza ayuda a esconder una red interna del Internet, eso porque esta red no tiene contacto directo con ningún otro servidor aparte del proxy. En términos más técnicos un proxy "Un servidor proxy funciona interceptando las conexiones entre el remitente y el receptor. Todos los datos entrantes entran a través de un puerto y son reenviados al resto de la red a través de otro puerto" (Indiana University, 2015, s. p.)

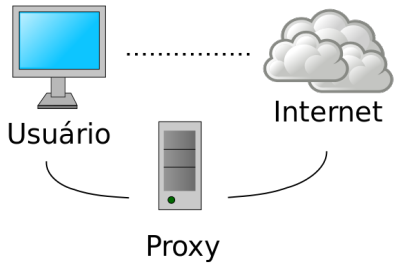

Ilustración 2. Esquema de un proxy

Fuente: Gobierno de España Seguridad Informática, 2010

2.2.5. Antivirus

Es un *software* que se aloja en un dispositivo que ayuda a la protección y detección de amenazas cibernéticas. Una definición de este es:

> Un *software* antivirus ayuda a proteger su computadora contra *malware* y ciberdelincuentes. El *software* antivirus analiza los datos (páginas *web*, archivos, *software*, aplicaciones) que viajan a través de la red a sus dispositivos. Busca amenazas conocidas y monitorea el comportamiento de todos los programas, marcando comportamientos sospechosos. Busca bloquear o eliminar el *malware* lo más rápido posible (Norton, s. f., s. p.).

2.2.6. IDS / IPS

Los sistemas de detección de intrusos (IDS, Intrusión Detection System) y los sistemas de protección de intrusos (IPS, Intrusión Prevention System) son una evolución de los sistemas de defensa basados en *firewall*. Estos sistemas ya no se basan únicamente en las comunicaciones con direcciones IP y puertos, sino que revisa el tráfico de red o el comportamiento de los equipos para encontrar actividad maliciosa.

> La principal característica que diferencia ambos sistemas es el comportamiento una vez detectado un posible comportamiento malicioso: los sistemas de detección, IDS, avisan a los administradores para que pueda analizar y actuar en consecuencia mientras que los de protección, IPS, aplican una serie de políticas que intentan detener las actividades maliciosas. Ambos sistemas pueden utilizarse en las mismas redes y utilizan las mismas técnicas si bien es el matiz de su actuación una vez detectada una amenaza el que los diferencia (Securizando, 2017, s. p.).

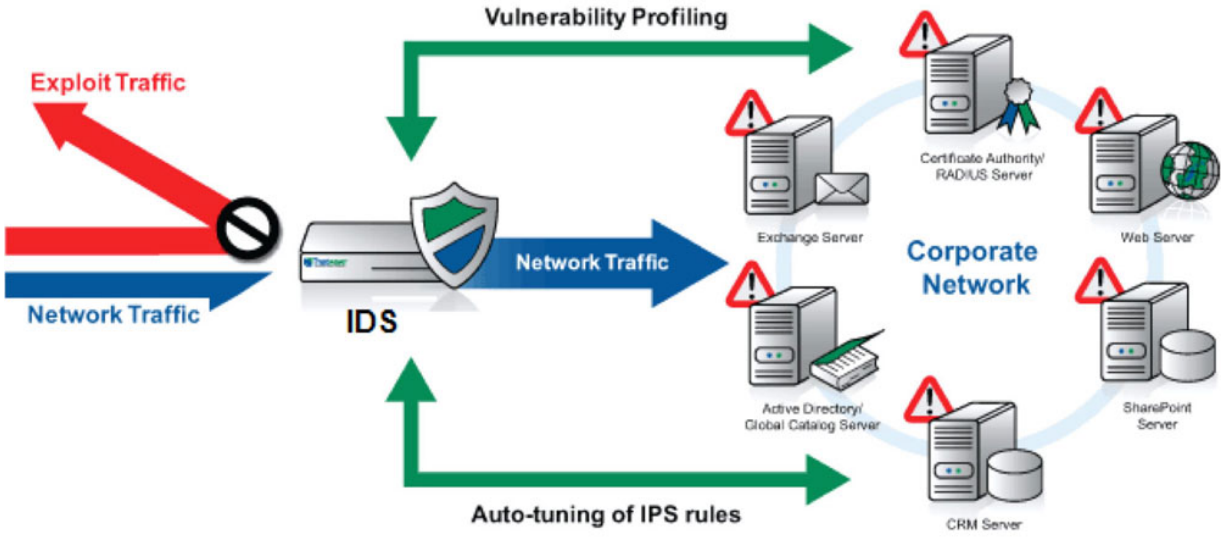

Ilustración 3. Esquema de funcionamiento IDS/IPS

Fuente: BringCom, s. p.

2.2.6.1. IPS e IDS por objetivo de monitorización

Estos sistemas pueden clasificarse en función del sistema que analizan en cuatro categorías. Los sistemas basados en red (NIPS, Network IPS) analizan el tráfico de una red en busca de intenciones maliciosas. Los sistemas de detección en redes inalámbricas (WIPS, Wireless IPS) hacen la misma función en redes Wi-Fi. Los sistemas basados en servidores (HIPS, Host IPS) monitorizan el comportamiento del propio servidor (uso de memoria, disco duro, conexiones, etc.) para encontrar *software* malintencionado.

2.2.6.2. Sistemas IPS e IDS por sistema de detección

Existen diferentes formas de intentar diferenciar un comportamiento anómalo o malicioso por lo que los desarrolladores de sistemas IDS han abordado el problema de diferentes formas. Aunque las soluciones en el mercado suelen incluir varias de estas formas de trabajo, tradicionalmente se han categorizado de la siguiente forma:

- Detección basada en firmas: este sistema intenta localizar una cadena de información, conocida previamente en una comunicación. El sistema analiza el tráfico http en busca de cadenas de peticiones que induzcan a un posible

ataque de SQL Injection. La principal ventaja de esta estrategia es su alta eficiencia para encontrar ataques ya conocidos, pero como contrapartida, es prácticamente inútil para encontrar ataques no conocidos por el sistema.

- Detección basada en políticas: este sistema requiere definir, de forma concienzuda, el tipo de comunicación (y no solo puertos y protocolo) entre los servidores o diferentes redes. Se trata de sistemas muy efectivos, pero que requieren de una configuración detallada.

- Detección basada en anomalías: estos sistemas buscan encontrar comportamientos anormales en nuestros sistemas. La principal dificultad es definir qué es normal. En la actualidad, se utilizan dos formas para intentar registrar cambios maliciosos.

- Detección estadística de anormalidades: los sistemas analizan el comportamiento de nuestra red o servidores durante un tiempo determinado. Con esta información generan un patrón. Cuando el comportamiento difiere del patrón normal calculado previamente las alarmas saltan y generan los avisos o actuaciones pertinentes.

- Detección no estadística de anormalidades: en estos equipos es un administrador quien define los patrones de comportamiento normal, por lo que pueden ser muy granulares y específicos, aunque es posible que con el tiempo se generen falsos positivos.

2.2.7. End-points

Deming (s. f.), define *endpoint* como:

Un dispositivo o nodo que está conectado a la LAN o WAN y acepta comunicaciones bidireccionales a través de la red. En su forma más tradicional, un *endpoint* puede ser un módem, un *hub*, un *router*, un *bridge*, o un *switch*. Además, este podría ser una terminal de datos como un teléfono IP, una impresora, o un computador. Hoy en día los *endpoints* más comunes son *laptops*, tabletas, teléfonos móviles, datáfonos y cajeros automáticos (s. p.).

2.2.8. SMTP servers

Pérez Porto y Gardey definen *SMTP servers* como:

> Un protocolo de red que se emplea para enviar y recibir correos electrónicos (*emails*). Cabe destacar que un protocolo de red es un conjunto de normativas y reglas que posibilitan la circulación de información en una red informática. En este caso, el SMTP forma parte de los llamados protocolos de Internet.
> La operación del SMTP se produce en el contexto de los servicios de correo electrónico. Debido a ciertas restricciones técnicas para recibir los correos, es habitual que el SMTP se emplee solo para el envío de mensajes y que para la recepción se apele a otros protocolos de Internet, como IMAP (Internet Message Access Protocol) o POP (Post Office Protocol).
> En el caso del SMTP, su función es permitir que un cliente se comunique con un servidor, posibilitando que el cliente envíe un correo a uno o más receptores. El SMTP trabaja con líneas de texto para brindar las instrucciones necesarias (s. f., s. p.).

2.2.9. Base de datos

Pérez Porto y Gardey definen las bases de datos como:

> Un conjunto de información que está organizado y estructurado de un modo específico para que su contenido pueda ser tratado y analizado de manera rápida y sencilla.
> Las bases de datos, por lo tanto, presentan datos estructurados de acuerdo con diferentes parámetros. Al disponer la información de una cierta forma, el usuario puede encontrar aquello que busca con facilidad, a diferencia de lo que le sucedería si todos los datos estuvieran mezclados y sin ningún tipo de orden (s. f., s. p.).

Todas las bases de datos de comerciales tienen un registro en el que se incluyen todas las transacciones y las modificaciones que se hacen en la base de datos. Además, permite auditar los intentos de acceso, usuarios, perfiles y roles asignados a los distintos componentes de la base de datos.

2.2.10. Prueba de concepto

Además, conocida por sus siglas PoC; son pruebas utilizadas para probar la idea de una determinada característica técnica o el diseño general de un plan. Estas demuestran que es posible aplicar esas ideas en las condiciones analizadas. Pueden

usarse para probar una característica de la estrategia antes de aplicarla en un ambiente de producción. Según Musienko, “explica cómo debería funcionar el proyecto sobre la base de una descripción detallada de los requisitos y especificaciones de este” (2019, s. p.).

2.2.11. Falso positivo

Un falso positivo es una expresión utilizada frecuentemente en ciberseguridad para expresar que un archivo, configuración o comportamiento se ha marcado como malicioso cuando no lo es. En contexto de un ambiente SIEM “los falsos positivos son alertas de seguridad mal etiquetadas, que indican que existe una amenaza cuando en realidad no existe” (Infocyte, 2019, s. p.).

Estas alertas, catalogadas como falsas o no maliciosas, aumentan el ruido para los equipos de seguridad que trabajan demasiado en entender que hay detrás de estos eventos en el SIEM. Estos pueden incluir errores de *software*, *software* mal escrito o tráfico de red no reconocido que no representa peligro a la seguridad de la información, además, afecta la visibilidad de eventos más relevantes en el ambiente.

2.3. Operaciones de un centro de seguridad

2.3.1. SOC

Un Centro de Operaciones de Seguridad (SOC) es un equipo organizado y calificado altamente cuya misión es monitorear y mejorar continuamente la postura de seguridad de una organización. Esto al mismo tiempo que previene, detecta, analiza y responde a incidentes ciberseguridad con la ayuda de tecnología, procesos y procedimientos definidos.

2.3.2. Tecnología

Se necesitan muchos componentes para construir un entorno tecnológico completo: *firewalls*, IPS / IDS, *data lost prevention systems* y un SIEM, solo por nombrar algunos. La recopilación de datos efectiva y eficiente es fundamental para un SOC exitoso. Los flujos de datos, telemetría, captura de paquetes, syslog y varios tipos

de eventos deben recopilarse, correlacionarse y analizarse desde una perspectiva de seguridad. El *threat intelligence* y la información sobre vulnerabilidades que afectan a todo el ecosistema por monitorear también es de gran importancia.

2.3.3. Roles

Además de la tecnología, las personas y los procesos son los pilares de un SOC exitoso. Aunque los requisitos técnicos son muy importantes, un centro de operaciones de seguridad con la tecnología más avanzada no valdría nada sin las personas correctas y los procedimientos necesarios para la gestión del monitoreo y respuesta a los incidentes de seguridad.

Se necesitará de un líder capaz de mantener a un equipo motivado y vigilante que trabaje 24/7, mientras que los roles de ingeniería, roles de analista y roles de administradores de seguridad tendrán que ser cubiertos. A continuación, se detallan cada uno de esos roles.

2.3.3.1. Analistas de seguridad

Estos deben llevar a cabo muchas funciones y serán asignados a dos o tres niveles. Las funciones principales de estos miembros del equipo serán el análisis con base en el monitoreo real de eventos; la detección de incidentes de seguridad o violaciones de datos, la respuesta a estos incidentes (después de la fase de triaje necesaria) y, por último, la remediación de las consecuencias de cada incidente detectado. La *Ilustración 4* resume las funciones de cada nivel.

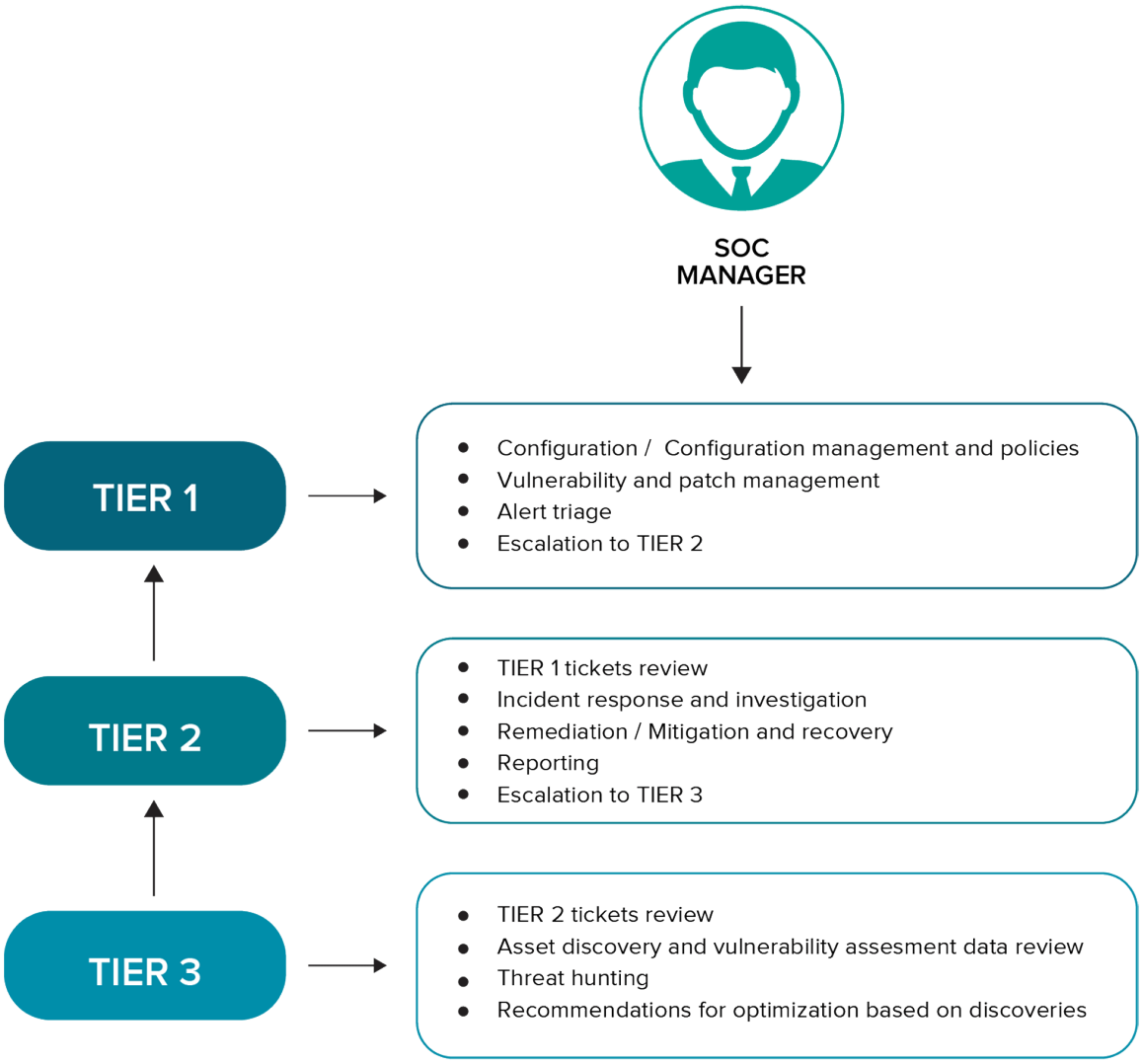

Ilustración 4. Niveles de analistas de seguridad

Fuente: Hashroot, s. f.

2.3.3.2. Ingenieros de seguridad

Estos serán responsables de la actualización de firmas, indicadores de compromiso, ajustar las reglas y políticas para aumentar la precisión de detección en los diferentes dispositivos de seguridad, especialmente en los equipos SIEM. En estos creará, modificará y ajustará las reglas del sistema de acuerdo con las especificaciones de alertas e incidentes.

Entre sus está funciones está la reducción de falsos positivos y mejor el

rendimiento creando una gestión de políticas y compilando informes de análisis de tendencias. Además, asignará la clasificación de las alertas de seguridad y dará recomendaciones de priorización, de acuerdo con el posible impacto de cada alerta.

2.3.3.3. Administradores de seguridad

El administrador de seguridad es responsable de mantener los diferentes dispositivos de seguridad en estado óptimo en relación con la configuración y los recursos necesarios para que funcionen correctamente, de manera eficiente y con el rendimiento deseado. Además, debe asegurarse que todas estas fuentes de *logs* estén enviando la información al dispositivo SIEM, de manera oportuna. Entre sus funciones se encuentran también la creación, modificación y eliminación de los conectores encargados de tomar los registros de las diversas fuentes de *logs* y enviarlos hasta el colector de eventos del equipo SIEM.

Todas las acciones entre los diferentes equipos deben coordinarse: la colaboración, comunicación, el tiempo y la eficiencia deben ser primordiales para la organización general de SOC.

2.3.4. Procesos y procedimientos

Un centro de operaciones de seguridad necesita tener documentada la información sobre los procesos y procedimientos necesarios para la atención de cualquier tipo de incidente de seguridad. Para esto, se hace la creación de Runbooks o Playbooks los cuales son una guía donde se detalla paso a paso de todas las actividades que se deben llevar a cabo para encontrar, contener y mitigar una amenaza específica. SANS ha creado un documento donde se detalla los 6 pasos para el proceso del manejo de incidentes de seguridad. De este se extrae la siguiente tabla:

Preparación	Esta fase implica la preparación de un equipo para estar listo para manejar un incidente en cualquier momento. Un incidente puede variar desde un corte de energía o una falla de hardware hasta los incidentes más extremos, como una violación de la política de la organización por parte de empleados descontentos o piratearse por piratas informáticos patrocinados por el estado (Bejtlich, 2005). Independientemente, de la causa del incidente, la preparación es la fase más crucial en comparación con todas las demás, ya que determinará cuál tan bien podrá responder su equipo en caso de una crisis.
Identificación	Esta fase se necesita de la detección y determinación de si una desviación de las operaciones normales dentro de una organización es un incidente. Este paso en particular requiere que se recopilen eventos de varias fuentes, como archivos de registro, mensajes de error y otros recursos, como sistemas de detección de intrusos y firewalls, que pueden producir evidencia para determinar si un evento es un incidente. Si se determina que el evento es un true positive, se debe informar lo antes posible para que el equipo de respuesta de incidentes tenga tiempo suficiente para recopilar pruebas y prepararse para los pasos posteriores (Bejtlich, 2005).
Contención	El propósito principal de esta fase es limitar el impacto y evitar que ocurra cualquier daño adicional (“Uf it security”, 2011). Hay varios

	pasos para esta fase; sin embargo, cada uno es necesario para mitigar completamente el incidente y evitar la destrucción de cualquier evidencia que pueda necesitarse más tarde para llevar el caso antes los tribunales.
Erradicación	Esta fase se necesita de la eliminación y restauración de los sistemas afectados. Al igual que con cada una de las fases anteriores, será necesaria la documentación continua de todas las acciones tomadas para determinar el costo de las horas hombre y otros recursos como un medio para determinar el impacto general para la organización. Además, es necesario asegurarse de que se tomaron las medidas adecuadas para eliminar archivos maliciosos y cualquier otro contenido ilícito de los sistemas afectados y garantizar que estén completamente limpios (Proceso de respuesta a incidentes, 2008).
Recuperación	El propósito de esta fase es devolver los sistemas afectados al entorno de producción, tomando las medidas necesarias para asegurar que no provocará otro incidente. Es esencial probar, monitorear y validar los sistemas que se vuelven a poner en producción para verificar que no estén siendo reinfectados por *malware* o comprometidos por algún otro medio.

Lecciones aprendidas	El propósito de esta fase es completar cualquier documentación que no se haya realizado durante el incidente, así como cualquier documentación adicional que pueda ser beneficiosa en futuros incidentes. El documento debe escribirse en forma de informe para proporcionar una revisión detallada de todo el incidente. Este informe debe ser capaz de responder a las preguntas sobre quién, qué, dónde, por qué y preguntas sobre cómo que puedan surgir durante la reunión de lecciones aprendidas. El objetivo general es aprender de los incidentes que ocurrieron dentro de una organización para mejorar el rendimiento del equipo y proporcionar materiales de referencia en caso de un incidente similar. La documentación también se puede usar como material de capacitación para los nuevos miembros del equipo o como un punto de referencia para comparar en futuras crisis (Bejtlich, 2005).

Cuadro 1. *Fases para el manejo de incidentes*

Fuente: Kral, 2011.

2.4. Tendencias de ataques

Cubrir todos los vectores de ataque que un actor malicioso puede utilizar para

comprometer la seguridad de una organización puede convertirse en una tarea titánica. Diariamente, recibimos boletines de seguridad donde se indica el descubrimiento de nuevas vulnerabilidades y amenazas que podría poner a cualquier organización en jaque. No obstante, los recursos son limitados y los presupuestos ajustado, lo cual genera la necesidad de priorizar los controles de seguridad a implantar.

Con el objetivo ayudar en esa priorización, en esta sección se detallarán cuáles son los 5 ataques más comunes a los cuales las empresas se enfrentan. Esta lista ayudará a priorizar la creación de reglas y caso de uso resilientes para estos comportamientos específicos.

2.4.1. Ataques de phishing

El recurso humano es eslabón más débil de la cadena y los ataques de phishing son una amenaza que han sido utilizada durante muchos años por los actores maliciosos. Esto se debe a su efectividad y facilidad de implementación. Sin embargo, las campañas de propagación recientes muestran nuevas características. Una de estas es el uso de certificados de seguridad en los sitios web utilizados para phishing.

De acuerdo con el Antiphishing Working (APWG, 2018), durante el segundo trimestre de 2018, alrededor del 35 % de los ataques de phishing registrados se alojaron en sitios web con el protocolo HTTPS. Esto representa un incremento en comparación con el casi 5 % de los casos de sitios falsificados con certificados SSL, reportados a finales de 2016.

Esta estrategia surge debido a recientes cambios en los navegadores *web* para marcar los sitos que utilicen HTTP como *No seguros*. Además, ciertas entidades certificadoras han empezado a emitir certificados de manera gratuita, lo que permite que más sitios puedan contar con certificados de seguridad, incluso los sitios fraudulentos.

Otra característica de las nuevas campañas de *phishing* es el uso de métodos de propagación no tradicionales. El correo electrónico ya no sería el único medio para engañar a los usuarios finales, sino que ahora se utilizan las aplicaciones de mensajería como SMS, WhatsApp, Facebook Messenger, entre otras. Además, el uso

de ataques homográficos añade una capa más dificultad a los usuarios finales para que puedan encontrar sitios *web* fraudulentos.

2.4.2. Criptojacking

Esta amenaza surgió en 2017 y tiene como objetivo usar la capacidad de procesamiento de equipos ajenos para ganar dinero mediante la minería de criptomonedas. Existen diversas formas de infectar a los dispositivos, una de ellas es mediante scripts que se ejecutan en el navegador de los usuarios finales. En otras palabras, basta con que el usuario visite un sitio web que contenga el código para que su procesador sea utilizado para minar alguna criptodivisa.

De acuerdo con un estudio de ESET (2018), en la región latinoamericana, casi la mitad de las detecciones de minería de criptomonedas se concentraron en dos países: Perú (30,72 %) y México (17,41 %), seguidos por Ecuador (8,89 %), Brasil (7,73 %) y Argentina (7,08 %). Esta misma firma no categoriza esta amenaza como *malware*, sino como aplicación no deseada. Esto se debe a que la minería de criptomoneda es una actividad legítima, sin embargo, la ilegalidad del *criptojacking* se da cuando los recursos de procesamiento del usuario son utilizados sin su consentimiento y sin su conocimiento.

2.4.3. Malware

El código malicioso es una de las principales amenazas que enfrentan las organizaciones. La aparición de nuevas familias de malware hace que esta amenaza crezca en cantidad, complejidad y técnicas de evasión año con año, convirtiéndose en la principal causa de incidentes de seguridad de las empresas latinoamericanas de acuerdo con el ESET Security Report 2018. (ESET, 2018). De acuerdo con este reporte, esta firma recibe diariamente más de 300 000 muestras únicas de malware, lo que muestra la gravedad del problema. Además, los actores maliciosos se han mutado de la creación de malware para Windows hacia un alcance más amplio en el que actualmente se desarrolla código malicioso para prácticamente todos los sistemas operativos de la actualidad.

Adicionalmente, se identifican mensualmente, en promedio, 300 muestras de malware para Android. Además, ha aumentado la creación de malware para dispositivos de IoT los cuales, después de ser comprometidos, son utilizados para llevar a cabo otros ataques (Stefanko, 2018). Sin embargo, la mayor preocupación relacionada con el malware son las infecciones de ransomware. En solo un año se encontraron 1190 nuevas familias, lo que representa un incremento del 60 % en comparación con el año anterior. El *ransomware* ha evolucionado gracias a la rentabilidad que les ofrece a los atacantes, debido a la disposición de los afectados estos de pagar el rescate para recuperar su información.

2.4.4. Explotación de vulnerabilidades

Este es un método utilizado por los atacantes y el cual ha crecido significativamente en los últimos 3 años. Un ejemplo de vulnerabilidad es una falla en la programación de una aplicación que permite ser abusada y explotada por actores maliciosos para ejecutar su propio código.

De acuerdo con la base de datos de vulnerabilidades CVE Details (CVE Details, 2019), el 2017 fue el año en el que se registraban el mayor número de vulnerabilidades reportadas, exactamente 14 714. Esto superó, por mucho, los registros de años anteriores, sin embargo, en 2018, esta cifra llegó a un total de 16 556. En lo que va de 2019 este número ha decrecido, no obstante, es la tercera más alta en toda la historia con un total de 12 174 a la fecha.

2.4.5. Ataques web

Desde un punto de vista de negocio, es obligatorio que toda empresa tenga presencia en Internet y que este medio sea su principal canal para promocionar sus productos y llevar a cabo transacciones. Sin embargo, si no se aplican las medidas de seguridad correspondientes, este habilitador se convertirá en una puerta de entrada para que actores maliciosos puedan ingresar dentro de la organización.

Galobardes (s. f.), investigador de seguridad, llevó a cabo una prueba en la que conectó un honeypot (servidor intencionalmente vulnerable) a Internet y durante la

primera hora obtuvo los siguientes datos:

- 30 000 conexiones.
- Desde 116 direcciones IP maliciosas.
- Origen del tráfico: 65 % generado desde China, 15 % Estados Unidos, 5 % Rusia, 15 % otros países.
- 27 534 intentos de conexión en el puerto 22 SSH, 24 822 intentos en el puerto 80 HTTP y 24 034 para el puerto 443 HTTPS.
- 74 archivos maliciosos descargados los cuales estaban relacionados con la minería de criptomonedas y la inclusión del servidor dentro de diversas botnets para ataques de DDOS.

Los números dan una imagen clara de los riesgos a los que se exponen las organizaciones diariamente por el simple hecho de tener presencia en Internet. Debido a la falta de controles de seguridad, los ataques *web* se han convertido en el principal método de los atacantes.

Esto ha creado una reacción en la comunidad de profesionales de la seguridad y se han creado organizaciones encargadas de promover el desarrollo seguro de las aplicaciones *web*. Una de estas organizaciones es OWASP (*The Open Web Application Security Project*) la cual detallaremos en el próximo capítulo.

Capítulo III. Estado de la cuestión

3.1. Planificación

En este apartado analizaremos los diferentes proyectos existentes que establezcan una metodología para la efectiva detección y respuesta de los incidentes de seguridad, de una forma oportuna y eficiente. Se buscará un *framework* de seguridad que permita encontrar el ciclo de un ataque en cualquiera de sus fases siguiendo la misma línea de pensamiento del concepto de defensa en profundidad. Además, la metodología deberá ser capaz de encontrar cualquier tipo de ataque, sin importar su naturaleza y que cumpla con los criterios de elección detallados en el apartado siguiente

3.1.1. Criterio de elección del framework

Para efectuar la búsqueda de los elementos utilizados en el desarrollo de la investigación se utilizaron una serie de parámetros para la escogencia del *framework* por utilizar. Estas se presentan a continuación:

- Escalabilidad: la capacidad del modelo para adaptarse para las necesidades del negocio, sin necesidad de perder la visibilidad o calidad de eventos de seguridad, según el crecimiento que se dé en el ambiente.
- Complejidad: la complejidad para entender y aplicar el *framework* en un ambiente sin importar el nivel de madurez del ambiente. Además, se tomará en cuenta el si es requerido de un equipo o personal especializado para comprender la aplicación de los modelos expuestos.
- Alcance: el objetivo es de encontrar un modelo que se puede aplicar en un ambiente sin importar su nivel de madurez o tamaño.
- Costo: existe algún tipo de coste por la aplicación o acceso a la información del *framework* elegido en un ambiente doméstico o empresarial.
- Comunidad: al basarnos en un *framework* especializado estos en su mayoría

cuenta con una comunidad activa de expertos detrás de ella la cual expande la capacidad de soporte o documentación que se pueda encontrar.

- Documentación: que tanta información existe indexada adecuadamente, enumera y de acceso público para entender el *framework*.

3.1.2. Frameworks relacionados

3.1.2.1. Owasp

Es una organización internacional sin fines de lucro dedicada a la seguridad de aplicaciones web. Uno de los principios centrales de OWASP es que todos sus materiales estén disponibles gratuitamente y sean fácilmente accesibles en su sitio web, lo que hace posible que cualquiera pueda mejorar la seguridad de sus propias aplicaciones web. Los materiales que ofrecen incluyen documentación, herramientas, videos, foros y entrenamientos. Cabe destacar que su proyecto más conocido es el framework del OWASP Top. 10.

El OWASP Top. 10 es un informe actualizado regularmente que describe las tendencias de ataques para la seguridad de las aplicaciones web, centrándose en los 10 riesgos más críticos. El informe lo elaboran un equipo de expertos en seguridad de todo el mundo. OWASP se refiere al Top. 10 como un documento de conciencia y recomiendan que todas las compañías incorporen el informe en sus procesos para minimizar o mitigar los riesgos de seguridad. En su publicación más reciente OWASP 2017 la organización enlista las siguientes amenazas como parte de su *framework*:

- Injection.
- Broken Authentication.
- Sensitive Data Exposure.
- XML External Entities.
- Broken Access Control.
- Security Misconfiguration.

- CrossSite Scripting.
- Insecure Deserialization.
- Using Components with Known Vulnerabilities.
- Insufficient Logging and Monitoring.

3.1.2.2. MITRE ATT&CK

Es conocido por ser una base de conocimiento accesible en el ámbito mundial de tácticas y técnicas adversas basadas en observaciones ataques cibernéticos. La información se muestra en matrices organizadas por etapas de ataque, desde el acceso inicial al sistema hasta el robo de datos o el control de la máquina. Es tan granular que existen matrices con recomendaciones para tecnologías específicas como computadoras con sistema operativo Windows o servidores Unix.

El objetivo de MITRE ATT&CK es crear una lista completa de tácticas y técnicas conocidas utilizadas durante un ataque cibernético. El *framework* es destinado a crear una taxonomía estándar para hacer que las comunicaciones entre organizaciones sean específicas y fluidas. A continuación, se enlistan las etapas incluidas en el *framework*:

- Initial Access.
- Execution.
- Persistence.
- Privilege Escalation.
- Defense Evasion.
- Credential Access.
- Discovery.
- Lateral Movement.
- Collection.

- Exfiltration.

3.1.2.3. Cyber Kill-chain

Es una metodología que consta en una serie de pasos para identificar las etapas de un ciberataque desde las primeras etapas de reconocimiento hasta la exfiltración de la información. Esta ayuda a comprender y combatir las amenazas de seguridad en los ambientes en los que se aplica. Fue diseñada en 2011 y se ha vuelto un estándar para identificar un ataque y aplicar medidas defensivas para detener la amenaza. Además, consta de siete etapas:

- Recon.
- Weaponize.
- Deliver.
- Exploit.
- Control.
- Execute.
- Maintain.

3.1.3. Cuadro comparativo de *frameworks*

	OWASP	**MITRE ATT&CK**	**Cyber Kill-chain**
Escalabilidad	Media – Cada caso de uso es personalizado por aplicación *web*.	Alta – la metodología se presta para ser tan genérico o granular, según las necesidades del ambiente.	Alta –permite la generalización de casos de uso a un alto nivel.
Complejidad	Media – Se requiere de conocimiento avanzado en patrones de ataque hacia aplicaciones *web*	Alta – el *framework* es tan detallado que se requiere de un equipo de seguridad especializado para	Baja – cuenta con 7 asociadas con los patrones de ataques sin importar la tecnología.

	OWASP	MITRE ATT&CK	Cyber Kill-chain
		entender cada una de las categorías y subcategorías	
Alcance	Enfocado en el top. 10 de ataques hacia aplicaciones *web*	Cuenta con 13 categorías que contiene un sinnúmero de casos de uso por cada una	Enfocado en las 7 etapas de un ataque
Coste	Libre de acceso a la información, aplicación y uso dentro de ambientes empresariales	Libre de acceso a la información, aplicación y uso dentro de ambientes empresariales	Libre de acceso a la información, aplicación y uso dentro de ambientes empresariales
Comunidad	Comunidad activa con varios proyectos presentes dentro de la organización	Comunidad activa su mayoría asesores con un costo	Comunidad activa con entusiastas de la seguridad dispuestos a ayudar
Documentación	Documentación indexada y enumerada en la página del proyecto	Documentación centralizada y actualizada en su sitio *web*.	Documentación centralizada y actualizada en su sitio *web*.

Cuadro 2*. Comparación de frameworks*

Fuente: elaboración propia.

3.1.4. Framework escogido

Después de analizar las distintas capacidades ofrecidas por los frameworks mencionados, se llegó a la conclusión de que Cyber Kill Chain es el marco que mejor se adhiere al alcance de este proyecto, debido a sus características y baja complejidad de implementación en relación con los otros frameworks. El modelo identifica las fases que los actores maliciosos deben completar, con el fin de alcanzar sus objetivos.

Desde las primeras etapas de reconocimiento hasta la exfiltración de la información, los atacantes deben completar cada una de estas fases para tener éxito. Ser capaz de detener a los adversarios en cualquiera de estas etapas irrumpiría la

cadena del ataque, con esto se puede bloquear por completo la ofensiva en proceso. A continuación, se detallarán cada una de esas 7 etapas y se brindarán 2 enfoques, el primero está relacionado con las acciones específicas que llevará a cabo el atacante y el segundo con las acciones que puede llevar a cabo los defensores para encontrar las actividades realizadas por el atacante:

3.1.4.1. Reconnaissance

Identificación de objetivos.

3.1.4.2. Táctica del atacante

En esta etapa los atacantes planean la operación en la que hacen investigaciones para entender el entorno del objetivo e identificar cuáles son los recursos que podrían ayudarlos a cumplir su meta. Algunas de las actividades de esta etapa son:

- Obtener direcciones de correo de la organización por atacar.
- Identificar y crear perfiles de los empleados de la organización con información extraída de las redes sociales.
- Descubrir servidores que se encuentren expuestos a Internet.

3.1.4.3. Táctica defensiva

Encontrar las actividades de reconocimiento en tiempo real puede ser algo difícil. Sin embargo, cuando los analistas de seguridad las detectan, incluso cuando finalizaron, estas pueden revelar las intenciones de los atacantes. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Obtener los *logs* de las visitas al sitio *web* para generar alertas y llevar a cabo búsquedas históricas.
- Colaborar con los administradores *web* para utilizar sus herramientas de análisis existentes.

- Crear alertas para búsquedas *web* relacionadas con actividades de Reconocimiento.
- Priorizar las defensas alrededor de tecnologías particulares o personas basadas en las actividades de reconocimiento detectadas.

3.1.4.4. Weaponization

Se elige el programa maligno para el acceso remoto, como un virus, *malware* o *worm*, modificado para explotar una o más vulnerabilidades.

3.1.4.5. Táctica del atacante

Los atacantes están en la fase de preparación y puesta en marcha de su operación. Es probable que la generación de *malware* no se haga de forma manual, se utilizan herramientas automatizadas que permiten ahorrar tiempo. Algunas de las actividades realizadas durante esta etapa son:

- Obtener la herramienta (arma), desarrollada por ellos u obtenida a través de canales públicos o privados.
- Para los *exploits* basados en archivos, en esta etapa se selecciona el documento que será utilizado como señuelo y que se presentará a la víctima.
- Se seleccionará el código que será utilizado como puerta trasera (*backdoor*) y la infraestructura de comando apropiada y control para la operación.
- Se designará un identificador de la misión específico que se incrustará en el *malware.*
- Se compila el *backdoor* y el *payload*, para que queden listos para el ataque.

3.1.4.6. Táctica defensiva

Esta es una etapa esencial para que los analistas de seguridad comprendan el *modus operandi* de los atacantes analizando los indicadores de compromiso del *malware* utilizado. Las detecciones contra estos indicadores de compromiso (IoC's)

son a menudo las defensas más duraderas y resistentes. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Llevar a cabo un análisis de *malware* completo, no solo lo determinar lo que ejecuta el *payload*, sino entender como este fue creado.
- Crear detecciones para los indicadores de compromiso. Es una práctica común entre los atacantes reutilizar sus artefactos, por ejemplo, *exploits*, *malware*, servidores de comando y control, etc. Identificar estos indicadores de compromiso permitirá encontrar fácilmente nuevas campañas, nuevos *payloads* y relacionarlos con un grupo de atacantes específico.
- Analizar la línea de tiempo de cuándo se creó el *malware* en relación con cuándo se usó. El *malware* antiguo está listo para usar, pero el nuevo puede significar operaciones activas y personalizadas.
- Recopilar archivos y metadatos para futuros análisis.

3.1.4.7. Delivery

Lanzar la operación.

3.1.4.8. Táctica del atacante

Los atacantes transmiten el *malware* al objetivo. En este punto han lanzado su operación, algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Hacer una entrega controlada del *malware*, de forma directa, contra los servidores *web.*
- Entregar el *malware*, de forma remota, ya sea por un correo electrónico malicioso, en una memoria USB, mediante redes sociales o al infectar sitios *web* frecuentados por la víctima.

3.1.4.9. Táctica defensiva

Esta es la primera y más importante oportunidad para que los analistas de seguridad puedan bloquear la operación. Una medida clave de efectividad es la fracción de intentos de intrusión que se bloquean en esta etapa. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Analizar el medio de entrega, esto permitirá comprender los pasos previos que debieron llevar a cabo los atacantes.
- Comprender los servidores objetivo y a las personas, sus roles y responsabilidades, así como la información disponible.
- Inferir la intención del adversario en función de los objetivos atacados.
- Analizar la hora del día en que comenzó la operación.
- Recopilar los *logs* de correo electrónico y *web* para la reconstrucción forense. Incluso si se detecta una intrusión de forma tardía, los analistas de seguridad deben determinar cuándo y cómo comenzó el ataque.

3.1.4.10. Exploitation

Se sintetiza en el estado que el atacante obtiene acceso al dispositivo de la víctima.

3.1.4.11. Táctica del atacante

Los atacantes deben explotar la vulnerabilidad para ganar acceso. La frase *zero day* se refiere al código de explotación usado en este paso. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Se podrá atacar *software*, *hardware* o una vulnerabilidad humana.
- Adquirir o desarrollar zero day *exploits.*
- Lanzar *exploits* basados en las vulnerabilidades de los servidores que se encuentren expuestos a Internet.

- Los archivos adjuntos de correos maliciosos son abiertos por la víctima.
- La víctima da clic en un enlace malicioso.

3.1.4.12. Táctica defensiva

Esta es la primera y más importante oportunidad para que los analistas de seguridad puedan bloquear la operación. Una medida clave de efectividad es la fracción de intentos de intrusión que se bloquean en esta etapa. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Las medidas de *hardening* tradicionales agregan resistencia, pero las capacidades personalizadas son necesarias para detener las vulnerabilidades zero day en esta etapa.
- Capacitaciones de concientización en ciberseguridad y pruebas de *phishing* para empleados.
- Entrenamiento en codificación segura para desarrolladores *web.*
- Se deben llevar a cabo análisis de vulnerabilidades y pruebas de penetración regulares.
- Medidas de *hardening* para los equipos de los usuarios finales, por ejemplo:
    - Restringir los privilegios de administrador.
    - Utilizar Microsoft EMET (Enhanced Mitigation Experience Toolkit).
    - Reglas para bloquear la ejecución de *shellcode*.
    - Habilitar los *logs* de auditoría para que los analistas forenses puedan determinar el origen del *exploit*.

3.1.4.13. Control

Tomar posesión de los procesos del dispositivo y atrincherarse en la víctima.

3.1.4.14. Tácticas del atacante

Por lo general, los atacantes instalan una puerta trasera (*backdoor*) persistente en el entorno de la víctima para mantener el acceso durante un periodo prolongado de tiempo. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Instalar *web shell* en el servidor *web.*
- Instalar *backdoor* en la víctima.
- Cree un punto de persistencia agregando servicios, claves de ejecución automática en el registro, etc.
- Algunos atacantes modifican el tiempo del archivo para hacer parecer que el *malware* es parte de la instalación estándar del sistema operativo.

3.1.4.15. Táctica defensiva

Instrumentación de los *endpoints* para encontrar y registrar la actividad de instalación. Durante el análisis del *malware* se debe examinar la fase de instalación, con el fin de crear nuevas mitigaciones para los *endpoints*. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Configurar un sistema de prevención de intrusiones con base en *host* (HIPS) para alertar o bloquear rutas de instalación comunes utilizadas por los códigos maliciosos.
- Comprender si el *malware* requiere privilegios de administrador o solo usuario.
- Habilitar los *logs* de auditoría en los *endpoints* para descubrir creaciones de archivos anormales.
- Extraer certificados de cualquier ejecutable firmado.
- Comprender el tiempo de compilación del *malware*, para determinar si es antiguo o nuevo.

3.1.4.16. Execute

Ejecutar códigos maliciosos, de forma remota, en los dispositivos de las víctimas, comprometidos previamente.

3.1.4.17. Táctica del atacante

El malware abre un canal de comando que le permite al atacante manipular a la víctima, de manera remota. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Abrir un canal de comunicación bidireccional a la infraestructura comando y control (C2).
- Los canales C2 más comunes son los protocolos web, DNS y de correo electrónico.
- La infraestructura C2 puede ser propiedad de un atacante u otra red de víctimas.

3.1.4.18. Táctica defensiva

La última oportunidad de los analistas de seguridad para bloquear la operación, esto mediante el bloqueo del canal de comando y control. Durante el análisis del malware se debe examinar la fase de instalación, con el fin de crear nuevas mitigaciones para los endpoints. Si los atacantes no pueden emitir órdenes, los defensores pueden evitar el impacto. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Descubrir la infraestructura C2, a través de análisis de malware.
- Requerir proxies para todos los tipos de tráfico (HTTP, DNS).
- Configurar los bloqueos de protocolos C2 en servidores proxy web.
- Llevar a cabo bloqueos en el proxy basados en la categoría, incluidos los dominios ninguno o sin clasificar.

- Crear un DNS Sink Hole.
- Llevar a cabo una investigación de inteligencia de amenazas, con el objetivo de descubrir nuevas infraestructuras de C2.

3.1.4.19. Maintain

Alcanzar el objetivo de la misión.

3.1.4.20. Tácticas del atacante

En este punto los atacantes tienen acceso remoto al sistema, de esta forma, cumplen con su objetivo, lo que pase después dependerá de su habilidad e intenciones. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Recopilar credenciales de usuario.
- Escalar privilegios.
- Reconocimiento interno.
- Movimiento lateral a través del entorno.
- Recopilar y extraer datos.
- Destruir los sistemas.
- Sobrescribir o corromper datos.

3.1.4.21. Táctica defensiva

Cuanto más tiempo tenga acceso al sistema un atacante, mayor será el impacto. Los analistas de seguridad deben encontrar esta etapa lo más rápido posible, mediante el uso de evidencia forense y capturas de paquetes de red, para la evaluación de daños. Algunas de las actividades que se podrían llevar a cabo durante esta etapa son:

- Establecer un *playbook* de respuesta a incidentes que incluya el plan de

comunicaciones.

- Encontrar exfiltración de datos, movimiento lateral y uso de credenciales no autorizadas.
- Respuesta inmediata del analista a todas las alertas de seguridad.
- Agentes forenses desplegados previamente en los *endpoints* para un triaje rápido.
- Captura de paquetes de red para recrear la actividad.
- Llevar a cabo una evaluación de daños con expertos en la materia.

Capítulo IV. Propuesta

4.1. Propuesta

En este capítulo se presentan las técnicas para mejorar la resiliencia de las reglas en el ambiente SIEM. Mejorar la resiliencia de las reglas de correlación es crucial para que se recopile toda la información relevante y se mantenga su integridad. Esto es clave para tener una operación exitosa sobre el análisis de los eventos de seguridad por los equipos de analistas. Para lograr este objetivo es esencial llevar a cabo la correlación y sacar provecho de los miles de millones de eventos procesados en el ambiente.

Las reglas del SIEM son el núcleo de este dispositivo, el objetivo es mejorar las implementaciones de las reglas para expandir su rango de detección y disminuir la cantidad de falsos positivos en el ambiente. Esto tendrá un efecto secundario directo de una mejor operación de análisis por los equipos de seguridad. A continuación se presentan ejemplos reglas que pueden ser traducidas a cualquier tecnología SIEM.

4.1.1. Identificando brechas de casos de uso

Antes de llevar a cabo la optimización de cualquier regla primero se deben identificar las brechas en los casos de uso, como se propuso inicialmente se usa el *cyber killchain* para este proceso. La manera más rápida y oportuna de hacer este ejercicio es identificar todos los casos de uso en el SIEM, estos se van a identificar y catalogar cada una de las categorías del *framework*. Este evidenciará en qué parte de la cadena no existen casos de usos habilitados.

4.1.2. Reglas usando un único log *source* y límite de tiempo

Cada regla de correlación inicia con los parámetros de frecuencia que deberían activar una alarma. En la regla se muestra una violación de la política que debería activar una alarma para el equipo de seguridad, incluso si ocurre solo una vez. La política establece que todos los cambios en las cuentas de usuario deben hacerse con el sistema de gestión de identidad como un domain controller. Si existe algún cambio

que no se origine en ese sistema se debe activar una alarma y crear una ofensa.

En la línea 1, se define una restricción de tiempo para activar la regla y establecer que debe activarse por el primer evento que cumpla los criterios en las líneas restantes. El criterio para activar la regla es una conjunción de tres condiciones. La línea 2 expresa que el nombre de usuario del atacante es diferente de la cuenta utilizada por el domain controller, la línea 3 hace coincidir el tipo de evento con la categoría conocida de autenticación y, por último, la línea 4 indica que el resultado del evento fue exitoso.

1. where 1 event within 60 seconds with
2. and where user different username.dc
3. and event category Authentication
4. and event category equals Authentication Success

La regla se basa en la detección de una sola fuente y el directorio de la empresa es el *log source*. Este tipo de regla es efectiva siempre y cuando el usuario que ejecute el cambio no sepa el nombre del administrador.

4.1.3. Limitaciones de correlación de reglas básicas

Los equipos de seguridad están altamente expuestos a posibles fallas de confiar en las detecciones de reglas de un único *log source*. Tan pronto como un atacante es consciente sobre cómo se construyen las reglas de detecciones puede dirigir el ataque con mucho más inteligencia y probabilidades de éxito. Como se ha expuesto en el caso anterior, este tipo de reglas configuradas por defecto en muchos dispositivos SIEM, son fáciles de eludir con solo conocer parcialmente información del evento o al agregar una variable de tiempo. La única manera de evitar este tipo de vulnerabilidad es diseñar reglas robustas que saquen provecho de los miles de eventos, que incluyan información única y se puedan correlacionar entre sí.

4.2. Optimizando las reglas de correlación

Como se ha confirmado, las reglas de correlación estándar pueden ser

ineficaces, incluso costosas de ejecutar. El objetivo es eliminar las debilidades en los casos de uso propuestos para aumentar su resistencia y complejidad para su eficacia ante un atacante. Al igual que cualquier otro sistema, el primer paso debería ser entender mejor la raíz del problema, para esto se pueden incluir casos de uso no directo de la actividad anómala. Esto permite enriquecer la regla de correlación con más datos, propiedad y tipos de eventos.

En lugar de considerar solo una parte de la información que constituye un evento, se aprovecha la mayor cantidad de información posible para encontrar comportamientos maliciosos, incluso si el atacante toma algunas precauciones para no ser notado. Además, al ampliar el alcance de las propiedades consideradas al definir las reglas, se aumenta la dificultad de adulterar la información de los eventos. Comprender las propiedades adjuntas de los eventos es clave para diseñar reglas de correlación más resistentes. Al reconocer las especificaciones de cada evento es posible amplificar las capacidades de detección de anomalías y profundizar en estas.

Aunque el entendimiento de las propiedades de los eventos permite crear casos de usos más complejos, no sirve de mucho si se basan en la detección con el uso de un único *log source*. Esto permite que un atacante pueda comprometer un *log source* y tener control de los eventos, asó como volver inefectivas las reglas por medio de una única fuente de datos comprometida. La idea de utilizar la correlación de múltiples fuentes es que todos los dispositivos viven interconectados en un mismo ambiente, por lo que una acción resulta en una cadena de eventos asociados con más de uno. Todo eso puede utilizarse como redundancia a la hora que los eventos se procesen en el motor del SIEM.

La importancia de la redundancia es encontrar desde anomalías hasta atacantes con habilidades avanzadas, por ejemplo, si un atacante logra comprometer un servidor sin ser detectados y, posteriormente, deshabilita el registro de eventos de esa fuente. Si el atacante usa ese servidor como pivote para lanzar un nuevo ataque hacia otros sectores de la red, el destino de esos ataques genera los eventos, así como los componentes que los conectan. Por lo tanto, incluso cuando una fuente está comprometida, es posible de encontrar esta actividad por medio de otras fuentes, al

usar los eventos asociados con las comunicaciones del ambiente. La resiliencia, redundancia y autonomía de las reglas de detección son claves para esto.

4.2.1. Método de mejora continua para reglas de correlación

Un método de mejora continua sobre las reglas de correlación se puede llevar a cabo de acuerdo con la Ilustración. La metodología se expone de una manera genérica para aplicarla en cualquier ambiente SIEM, sin importar su tamaño y cuyo diseño lo hace fácilmente escalable para adaptarse a las necesidades del centro de seguridad. Según el tipo de regla y los *log sources* existirán excepciones en las que pasos pueden ser omitidos en situaciones específicas.

El primer paso de esta metodología es identificar a cuál de las siete categorías del *cyber killchain* pertenece el caso de uso. El propósito de esto es tener una visión global de ambiente e identificar una brecha en cualquier de las categorías y eliminar cualquier punto ciego en las etapas de un ataque. Una vez identificado y categorizado el caso de uso se entiende el proceso desde el inicio hasta el final, para agregar todos los dispositivos que se encuentren y agregar redundancia de detección desde diferentes puntos de red. Los datos como el nombre de *host*, el puerto o el agente que recopiló el evento, pueden presentar información valiosa para el análisis.

El tercer paso sería incorporar información de la red y modelos de activos, con las ventajas que se mencionaron anteriormente. Como se verifica la integridad de la información en estos modelos y solo un administrador de SIEM puede actualizar sus contenidos, estos se pueden usar como líneas de base para comparar con los datos del evento.

La mayoría de las reglas de correlación en ambientes SIEM se basan en lapsos entre eventos o número de eventos similares en una ventana de tiempo. Esta limitación se debe ajustar para que coincidan en la detección de anomalías. Este parámetro es uno de los más críticos porque pueden causar falsos positivos o falsos negativos que disminuyen las capacidades de notificación de un SIEM y saturan las pantallas para los analistas. Se deben tomar en cuenta ambos escenarios al construir o enriquecer reglas, ya que dan como resultado la pérdida de información vital. La solución ante

este problema se debe basar en un proceso de aprendizaje diseñado cuidadosamente para el ajuste de estos parámetros, de acuerdo con el funcionamiento normal de la infraestructura y resultados en pruebas de concepto.

A partir de lo expuesto en los capítulos anteriores se puede afirmar que los pasos de esta metodología permiten disminuir el riesgo ante la creación, modificación o enriquecimiento de casos de uso en ambientes SIEM. Los pasos están dirigidos a la personalización de cada uno de los casos de usos, lo que dificulta que las acciones del atacante pasen desapercibidas. Los últimos dos pasos tienen como objetivo interponer restricciones de tiempo y llevar a cabo pruebas de concepto para asegurar el rendimiento adecuado de las reglas en el ambiente SIEM.

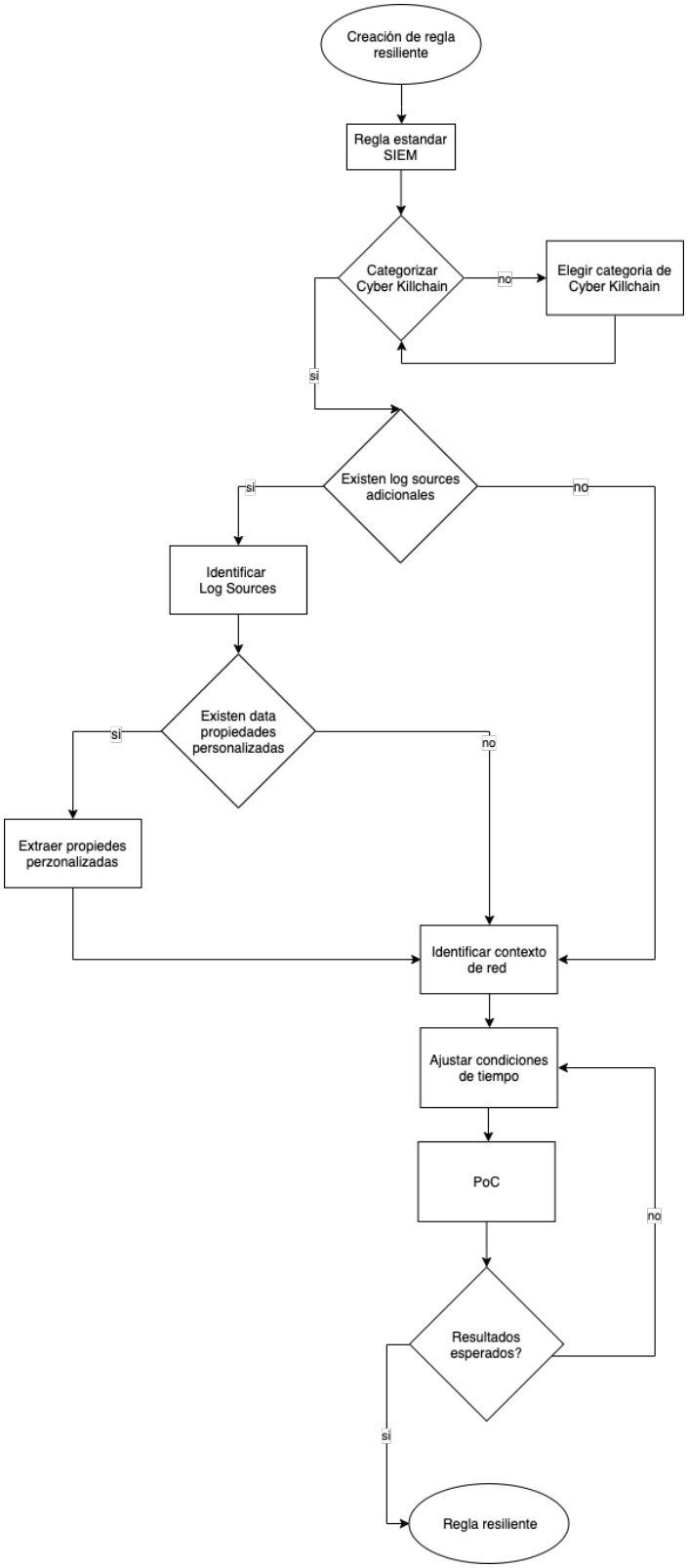

Ilustración 5. Diagrama de metodología propuesta

Fuente: elaboración propia.

4.2.2. Enriquecimiento de reglas SIEM con resiliencia

En esta sección se aplicará la metodología propuesta en apartados anteriores para agregar resiliencia a las reglas de un ambiente SIEM. Se ha mencionado que en la regla presentada es vulnerable a múltiples ataques por las condiciones en las que fue construida. Por ejemplo, se podría presentar suplantación de identidad del administrador porque la regla solo hace una verificación de la cuenta origen sin considerar ningún otro tipo de *log source* para verificar esta acción. Por lo tanto, puede mejorarse al agregar información de otras propiedades de diferentes eventos. Estas propiedades se pueden usar para incluir más detalles de ese sistema, lo que obliga a un posible atacante a comprometer más información y vuelve el ataque más complejo.

Definición	Descripción
Requerimiento	▪ Identificar cualquier cambio en la cuenta de los usuarios por un actor no autorizado
Caso de uso SIEM	▪ Violación de política ○ Cambio no autorizado en cuenta de usuario
Cyber Killchain	Execute
Log *sources*	▪ Sistemas Operativos: HP UX, IBM AIX, Microsoft Windows, Linux, Sun Solaris ▪ Identidad: Microsoft Domain Controller, LDAP, TACACS, RADIUS ▪ Bases de datos: IBM DB2, Microsoft SQL Server, Oracle Database ▪ *Web* Proxy: Bluecoat SG Appliance, McAfee *Web* Gateway, Microsoft ISA, Sophos *Web* Security Appliance, Squid *Web* Proxy ▪ Firewalls: Check Point *Firewall*-1, Cisco ASA, Fortinet Fortigate, Linux iptables *Firewall*, Palo Alto *Firewall* ▪ Intrusión Prevention System (IPS): Check Point IPS, Cisco SourceFire, IBM Proventia Network IPS, IBM Security Network

Definición	Descripción
	Protection (XGS), McAfee IntruShield, McAfee Network Security Platform, Trend Micro TippingPoint ▪ *Web* Application *Firewall* (WAF): F5 BIG-IP ASM, Imperva SecureSphere, NetScaler AppFirewall

Cuadro 3. *Caso de uso resilente*

Fuente: elaboración propia.

La regla que se presenta es una versión mejorada con resiliencia para adaptarse a los cambios del ambiente, se agregaron las condiciones en negrita para forzar verificaciones adicionales. En la línea 3, al usar la dirección del atacante y la firma del sistema operativo, es posible hacer que la regla sea más robusta. Esto obliga a un posible atacante a suplantar no solo el nombre de la cuenta, sino también la dirección y la huella digital del sistema operativo del *domain controller*.

1. where 1 event within 60 with (
2. and **not** from ***domain_controller*** where **user** equals **username_admin**
3. and ***source*_ip** equals ***domain_controller*_authorization_server**
4. and **operative_system** equals **windows_server**)
5. and from ***domain_controller*** event category equals Authentication Success
6. and event category equals Authentication Success

Para hacer posibles estas condiciones se tendría que configurar un gran conjunto de propiedades en el SIEM para aumentar los esfuerzos operativos y la complejidad de la configuración. Afortunadamente, el sistema SIEM incluye estas propiedades por defecto, la metodología propone el uso de estos modelos de activos y redes, para facilitar la gestión de las reglas de correlación al agregar información y actualizarla en el SIEM para identificar mejor los sistemas de origen o de destino.

Capítulo V. Implementación y resultados

5.1. Panorama inicial de implementación

Cuando se asumió el reto de mejorar las reglas de detección de un ambiente SIEM, se hizo el esfuerzo de hacerlo de una manera genérica posible, para lograr la implementación del concepto en cualquier ambiente sin importar la tecnología. En este caso fue implementado en un ambiente de producción real, con un promedio de 50 millones de eventos mensuales de una empresa Fortune 500.

El primer reto fue la identificación de todos los eventos centralizados en el SIEM. Durante esta implementación se experimentaron problemas con la verificación del nivel de registro por cada uno de los *logs sources* configurados, también se identificaron algunos con un nivel de registro inferior, porque afectan el rendimiento de la red o eran administrados por un tercero. Por esto, se optó por iniciar la implementación en un ambiente en el que estas variables podían controlarse, es decir, el área más crítica en la que se resguarda la información de investigación y desarrollo.

5.2. Ambiente de pruebas

Para evaluar la efectividad de la metodología propuesta y obtener la mayor información valiosa para aumentar la resistencia de los sistemas SIEM, se hizo uso de un ambiente de pruebas que era una simétrica del de producción. Después de llevar a cabo una investigación del ambiente de producción, se decidió implantar una consola destinada para las pruebas con QRadar. Este ambiente contaba con tres tipos de hardware distribuidos estratégicamente en los centros de datos: event collectors, event processors y consola de QRadar, las especificaciones técnicas se presentan en el Cuadro *4*. Además de los requisitos de la operación de *hardware*, también se tiene que cumplir con los requisitos de ley, por lo tanto, se requiere almacenamiento a largo plazo.

	Event Collector	**Event Processor**	**Consola**
Sistema Operativo	Red Hat Enterprise Linux 6.2 64-bit	Red Hat Enterprise Linux 6.2 64-bit	Red Hat Enterprise Linux 6.2 64-bit

	Event Collector	Event Processor	Consola
CPU	1 x Intel Xeon 2620 6-Core 2.0 GHz	2 x Intel Xeon 2620 6-Core 2.0 GHz	1 x Intel Xeon 2620 6-Core 2.0 GHz
RAM	128 GB	128 GB	64 GB
Eventos por segundo	15000	15000	15000
Almacenamiento	6 x 500 GB (RAID 5)	4 x 500 GB (RAID 5)	4 x 500 GB (RAID 5)

Cuadro 4. *Especificaciones técnicas*

Fuente: elaboración propia.

Un ambiente SIEM incluye una gran cantidad de reglas de correlación por defecto. Se asume que el equipo de seguridad se basa en este conjunto de reglas predeterminadas, para adaptarlas a las necesidades de monitoreo de la operación. Se inició con la clasificación de *log source* para determinar los parámetros de la creación de reglas resilientes.

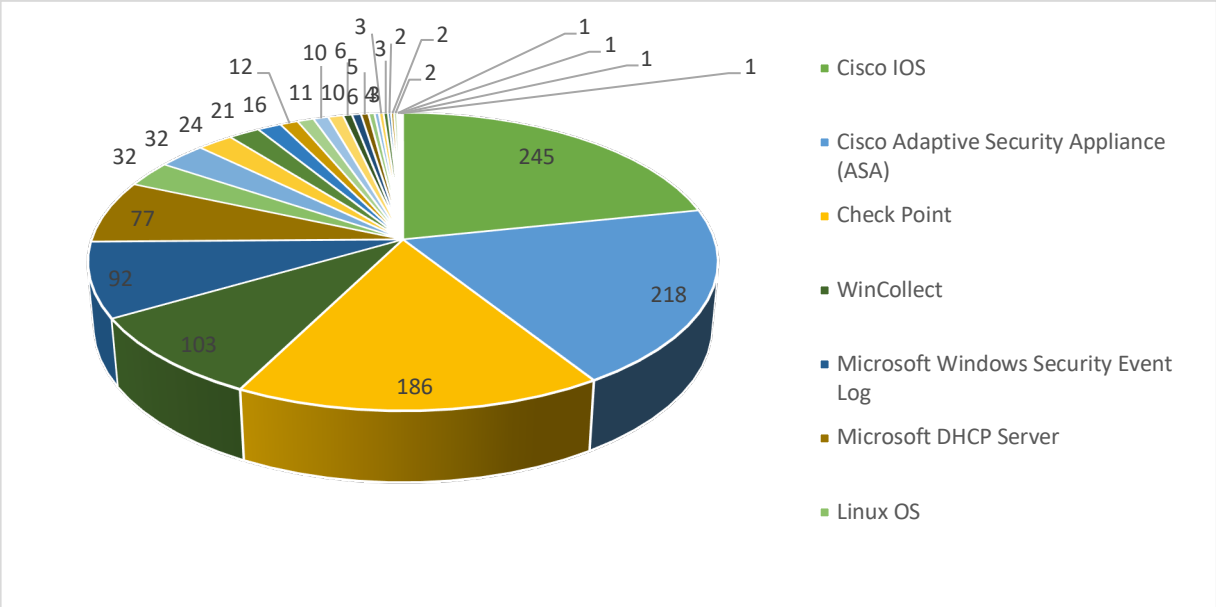

Gráfico 1. Clasificación tipo de log source

Fuente: elaboración propia.

Además, separamos el conjunto de reglas predeterminado de las reglas de correlación desarrolladas internamente para permitir un mayor control de los resultados. Se identificaron un total de 531 reglas, de las cuales únicamente 255 estaban habilitadas para la creación de alertas en el sistema con su configuración *default*.

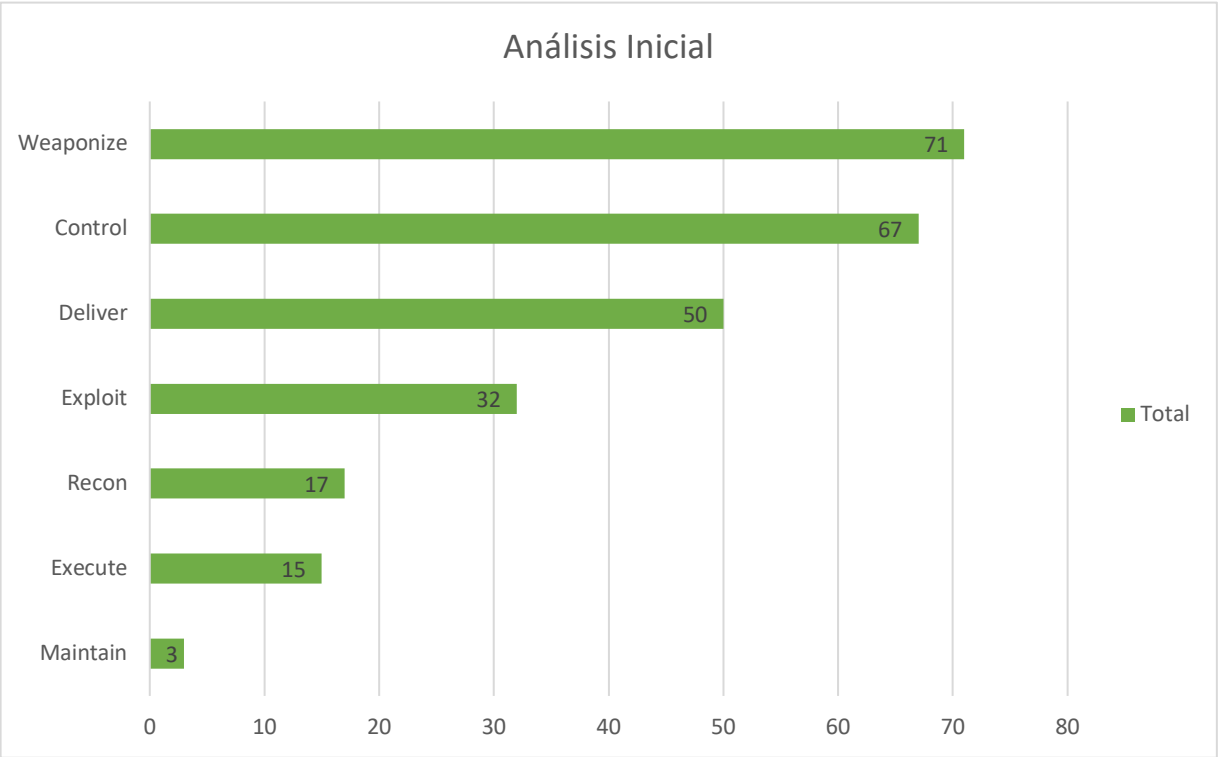

Gráfico 2. Análisis inicial

Fuente: elaboración propia.

5.3. Implementando la metodología propuesta

La validación de nuestra propuesta se basa en mejorar las reglas de correlación existentes y ajustar su resistencia ante los ataques haciéndolas más resilientes al cambio. Con este objetivo plasmamos la implementación de la metodología expuesta en este documento. Se inició con la identificación de los casos de uso, tomando en cuenta toda la cadena de eventos de los logs sources y su extracción de las propiedades de cada uno. La información sobre el inventario como aplicaciones, servidores, bases de datos y dispositivos de red fue actualizada en el ambiente SIEM previo la implementación de la metodología. Como se ha mencionado, es fundamental entender la infraestructura para aumentar la resiliencia y eficacia de las reglas de correlación.

El enfoque durante esta etapa fue probar las reglas de correlación identificadas en la sección 5.2, además de proponer nuevos casos de uso para tener una cobertura más balanceada en cada una de las etapas del cyber killchain. La información de

alarmas generadas se monitoreó durante un mes, para determinar una línea base de eventos e identificar las reglas que generaban más ruido en el ambiente. Concluir la aplicación de la metodología tomó un total de 8 meses.

El *Gráfico 3* muestra el número total de ofensas creadas en el ambiente durante 4 semanas, con un aproximado de 50 millones de eventos. Es un promedio de 1049 alertas por semana las cuales representaban ruido sobre las etapas de *execute* y *control*. Estas categorías, por su naturaleza, proveían poco valor agregado a los analistas del SOC o su remediación era muy costosa al encontrarse en las últimas etapas del *cyber killchain*.

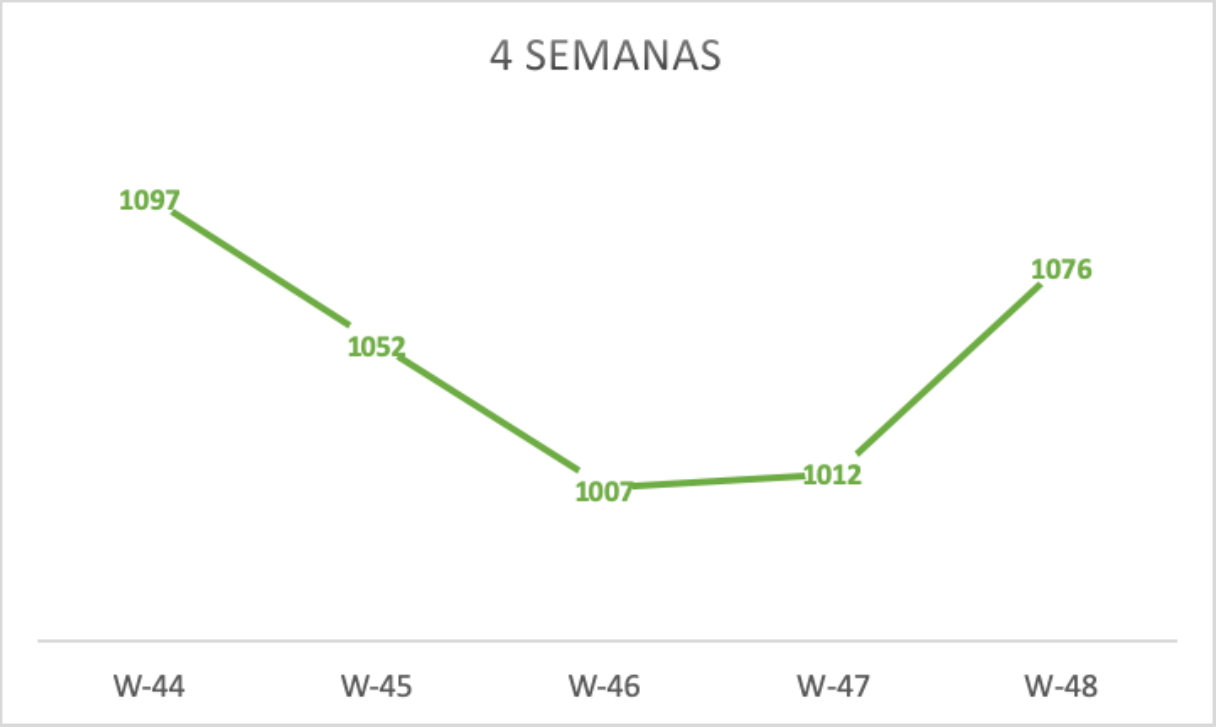

Gráfico 3. Total de alertas mensuales

Fuente: elaboración propia.

5.4. Resultados

Tener acceso a un ambiente con eventos reales en un entorno de producción tiene beneficios y desventajas. Por un lado, es posible observar cómo se pueden aplicar las reglas de correlación en un escenario del mundo real y ver los patrones de ataque mientras suceden. Por otro lado, el hecho de que este es un ambiente de

pruebas limita las posibilidades de que las alarmas generadas sean valoradas en ese momento por un analista de seguridad.

Como parte de la metodología, en la primera etapa se logró identificar brechas en la cobertura sobre el cyber killchain y balancear el número de reglas habilitadas para las etapas de cobertura con los casos de uso propuestos. Además, se reforzaron las etapas más críticas de un ataque como recon y exploit, sumando un total de 337 reglas habilitadas.

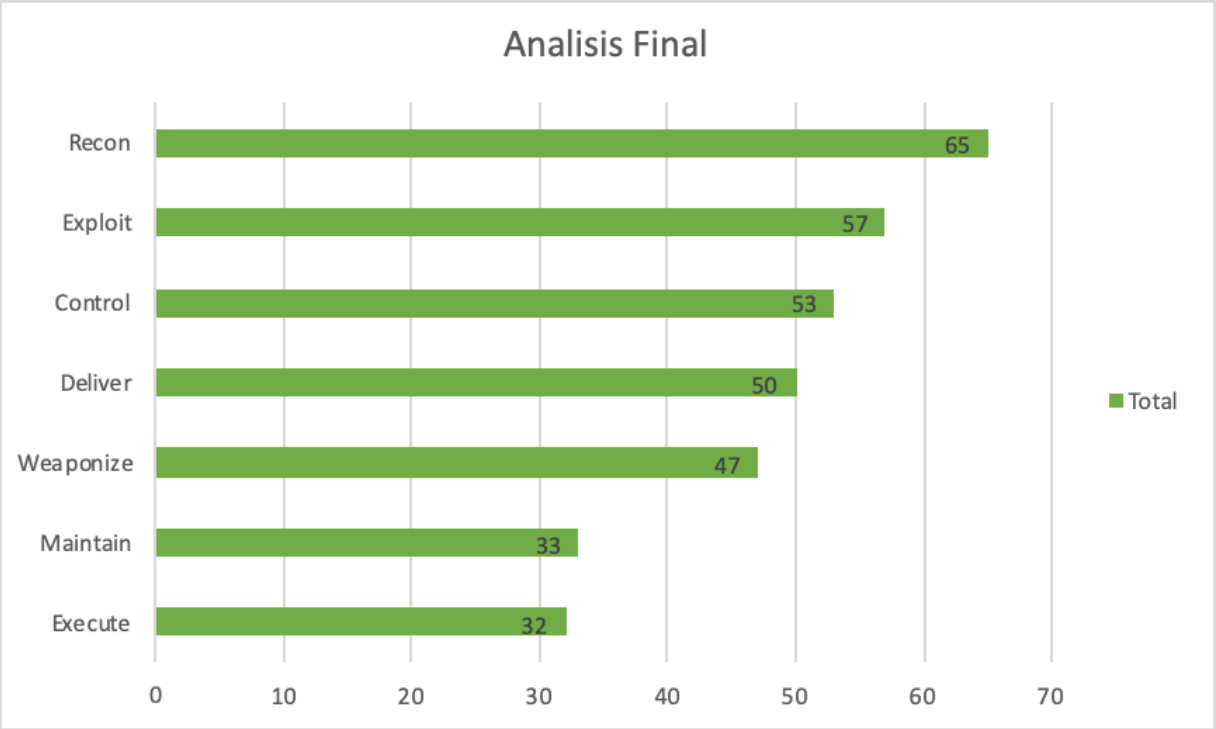

Gráfico 4. Análisis final

Fuente: elaboración propia.

Cubrir en las primeras etapas del *cyber killchain* da un valor agregado a que la remediación de los ataques durante estas etapas no es tan compleja o costosa como el resto. En el momento de identificar un actor de malicioso en la red con un escaneo o un ataque de fuerza bruta, la remediación puede ser tan sencilla como bloquear el tráfico desde la fuente. Sin embargo, cuando este actor se encuentra dentro de la red la remediación es ejecutar una investigación forense o formatear todos los dispositivos de red donde se cree que el actor malicioso pudo haber estado.

Al eliminar las debilidades en las reglas de correlación y las brechas de detección, por medio de la metodología propuesta, fue posible aumentar el número de patrones de comportamiento detectados y las alarmas activadas con mayor valor para los analistas. El uso de la versión mejorada de cada regla de correlación significa que los equipos de seguridad pueden beneficiarse de datos adicionales. El uso de múltiples fuentes de eventos contribuye, de manera positiva, a la detección de acciones maliciosas e incluso o en el monitoreo de la infraestructura.

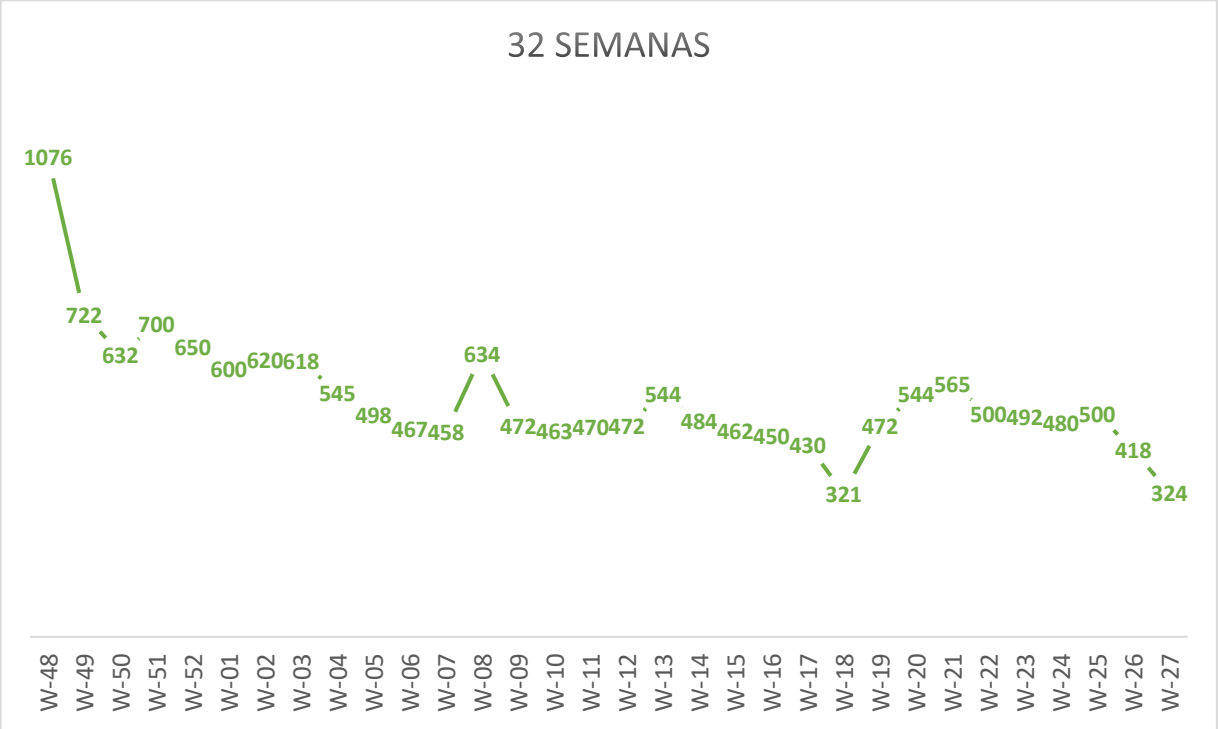

Gráfico 5. Total de alertas 8 Meses

Fuente: elaboración propia.

Durante la segunda fase de la propuesta se trabajó en las reglas para agregar resiliencia, esto tomó 32 semanas. La investigación resultó en la identificación de la regla Recon: Excessive Firewall Denies from Local Host más sólida, que se activó en 1430 ocasiones durante las primeras 4 semanas de monitoreo con una mejora de un 47,55 % a lo largo del estudio, esto ayudó a la reducción de falsos positivos. La regla original detectaba únicamente comportamiento sobre cualquier dispositivo sin enlistar más log sources o entendimiento sobre actividades esperadas de la red. Al investigar más a fondo una muestra de las alertas generadas por esta regla, concluimos que

existían una gran cantidad falsos positivos, ya que la mayoría de las ofensas correspondían a intentos de autenticación por medio de scripts de cuentas de servicio inactivas.

En el periodo de 4 semanas, la regla Recon: Potential Local Port Scan Detected se activó 1004 veces, lo que indica intentos escaneo de puertos de la red. El primer paso consistió en el mapeo del log sources para identificar este patrón de ataque. Un análisis detallado de la mayor cantidad de alarmas mostró que muchos sistemas tienen procesos y scripts incorporados de mantenimiento sobre aplicaciones ya no utilizadas en el sistema. Además, se encontraron escaneos de vulnerabilidades que cumplían con el mismo patrón.

Para este caso se agregaron listas de fuentes de confianza que pueden llevar a cabo los escaneos en el ambiente la misma es revisada cada trimestre para asegurarse de tener la información más actualizada en el sistema. Además, se agregaron más log sources para la identificación con la extracción de propiedades personalizadas para hacer una triangulación de los eventos y descartar servicios que, por su naturaleza, requieren descubrir los puertos habilitados en un dispositivo.

Por último, para la regla Execute: Honeyfile movement, durante el periodo de 4 meses se activó un total de 950 veces, cada vez que se aplicaba un parche en el ambiente sobrescribía sobre la base de datos en la que el documento se encontraba. Para este caso se agregaron más fuentes de datos para descartar las actividades de mantenimiento, además, se complementó con un horario de mantenimiento para descartar los falsos positivos en el ambiente. El Cuadro *5* resume las mejoras realizadas del top. 3 de las reglas con un porcentaje de mejora durante lo largo de la implementación.

Regla	Original	Resiliente	Mejora
Recon: Excessive *Firewall* Denies from Local Host	1430	680	47,55 %
Recon: Scanner Account Policy Removal	1004	400	39,15 %
Execute: Honeyfile movement	950	10	95 %

Cuadro 5. *Top. 3 Mejoras realizadas*

Fuente: elaboración propia.

El ambiente de pruebas permitió demostrar la efectividad de todas las mejoras a las reglas de correlación frente a ataques maliciosos, además, proporcionó un valioso escenario del mundo real para implantar los casos en el ambiente de producción al reducir el impacto negativo. Por esta medida se facilitó la implementación de las nuevas reglas en el ambiente de producción.

Capítulo VI. Conclusiones y recomendaciones

6.1. Conclusiones

Esta investigación abordó un trasfondo relevante sobre la evolución del panorama de la recolección de datos, el reconocimiento creciente de la gestión de eventos y un enfoque multidimensional para la seguridad de la información. La metodología propuesta utiliza métodos tradicionales de detección de actores maliciosos en un ambiente con técnicas de enriquecimiento para la creación de casos de uso resilientes. La propuesta muestra cómo el SIEM es el centro de operaciones para monitoreo de eventos, pero sin su mejora continua o reglas que se adapten a cambios se puede volver irrelevante para la operación.

La metodología propuesta también se enfocó en presentar principios que puedan aplicarse en cualquier ambiente SIEM, sin importar la tecnología, para que sirva como una guía que sea incorporada fácilmente a las operaciones de un equipo seguridad. Los efectos de aplicación de la metodología propuesta se verán reflejados en las tareas de los equipos de analistas, ya que existirá una reducción de falsos positivos y se enfocarán en alertas con eventos de seguridad más relevantes o de mayor impacto global en el ambiente.

Cabe mencionar que existe la posibilidad que la cantidad de alertas generadas incremente por el simple hecho de la modificación de los casos de uso en el ambiente, porque se remueven las condiciones restrictivas y excepciones estáticas implementadas. Por lo tanto, se concluye que si la metodología se aplica correctamente en el ambiente SIEM, esto puede ayudar en la identificación de patrones de actores maliciosos más puntuales y brechas en la cobertura de protección.

6.2. Trabajo futuro

Se planea seguir trabajando en la afinación de la metodología para agregar un algoritmo que de un promedio aritmético para relacionar la criticidad de una regla, con base en su posición en el *cyber killchain*, cantidad de *log sources* y su importancia en la estrategia de seguridad. La idea es dar un valor cuantitativo para facilitar la toma de

decisiones en el proceso de mejora continua del ambiente.

Además, se planea llevar a cabo el desarrollo de un sistema que automaticé las labores expuestas en esta investigación. La meta es publicar o patentar ese sistema automatizado para la mejora continua de los ambientes SIEM. Por lo anterior, se pone a disposición de la comunidad este documento para que se utilice como referencia y pueda adaptarse. según la retroalimentación.

6.3. Recomendaciones

- Una regla de oro es nunca trabajar sobre la lógica de una regla de correlación original, se sugiere la creación de una copia, deshabilitar la regla del ambiente y trabajar con esta copia para evitar cambios irreversibles al caso de uso.
- Para enriquecer las reglas se recomienda el uso de inteligencia de amenazas, esto consta de una lista de indicadores de compromiso de actores maliciosos y sus campañas. Los indicadores pueden variar entre IPs, hashes, nombre de dominios hasta firmas de dispositivos de seguridad como antivirus o IPS/IDS. La idea es aprovechar un máximo esta inteligencia, más allá de solo aplicarla en los dispositivos perimetrales. Se sugieren los siguientes tiempos de revisión de cada uno:
    a. IPs y dominios cada 7 días o menos
    b. Hashes cada 90 días.
    c. Firmas de detección cada 180 días.
- La clave de esta investigación fue el acceso a un ambiente de pruebas para llevar a cabo la revisión de la modificación de los casos de uso, se sugiere tener un ambiente de pruebas lo más similar al ambiente de producción. De no ser así, por lo menos tener un ambiente que no afecte los dispositivos, más críticos para las pruebas de concepto.
- Evitar el uso de *whitelists* u otro mecanismo de excepción, a menos que sea

requerido, ya que permite que un atacante pueda evitar la detección al hacerse pasar por un actor de confianza en esta lista. Existen situaciones en las que el uso de *whitelists* es justificable y necesario, por ejemplo, cuando se consideran sistemas específicos que hacen tareas prohibidas, como los escáneres de vulnerabilidades. Sin embargo, en esas situaciones, es vital definir cuidadosamente las excepciones, a través de información completa, no limitada a direcciones IP o nombres de *host*.

Bibliografía

Aidemark, J. y Karlsson, J. (2019). Using Massive Time Redundancy to AchieveNode-level Transient Fault Tolerance. Recuperado de: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.8464&rep=rep.1&type=pdf

APWG. (2018). Phishing Activity Trends Report. Recuperado de: https://docs.apwg.org//reports/apwg_trends_report_q2_2018.pdf

Arbor Networks. (2015). Security Beyond the SIEM. Recuperado de: https://pages.arbornetworks.com/BeyondtheSIEMOnDemand-View.html

BringCom. (s. f.). Network security. Recuperado de: http://www.bringcom.com/services/network-security/

Burnham, J. D. (2015). A Simple Definition: What is an 'Endpoint'? Recuperado de: Druva: https://www.druva.com/blog/simple-definition-endpoint/

Chuvakin, A. (2012). Marcus Ranum chat: Next-generation SIEM. Recuperado de: Search Security: https://searchsecurity.techtarget.com/opinion/Marcus-Ranum-chat-Next-generation-SIEM

CVE Details. (2019). The Ultimate Security Vulnerability Source. Recuperado de: CVE Details: https://www.cvedetails.com/browse-by-date.php

EC-Council. (2019). What Is Security Incident and Event Management (SIEM)? Recuperado de: https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/

ESET. (2018). ESET Security Report. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Gartner. (2019). Gartner Glossary. Recuperado de:

https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Gobierno de España Seguridad Informática. (2010). UD 7 Servidores proxy. Recuperado de: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/usted_7_servidores_proxy.html

Hashroot. (s. f.). White Paper: SOC y State of Art SIEM Workflow. Recuperado de: https://www.hashroot.com/whitepaper/soc-siem

IBM. (2019). System requirements for virtual appliances. Recuperado de: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_ha_vrt_ap_reqs.html

Indiana University. (2015). What is a proxy server? Recuperado de: https://kb.iu.edu/d/ahoo

Infocyte. (2019). Cybersecurity 101: What You Need To Know About False Positives and False Negatives. Recuperado de: https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-and-false-negatives/

Jamil, A. (2010). The difference between SEM, SIM and SIEM. Recuperado de: http://www.gmdit.com/NewsView.aspx?ID=9IfB2Axzeew=

Kral, P. (2011). Incident Handler's Handbook. Recuperado de: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Lane, A. (2010). Understanding and Selecting SIEM/LM. Recuperado de: http://securosis.com/blog/understanding-and-selecting-siem-lm-use-cases-part-1

Lockheed, M. (2019). The Cyber Kill Chain. Recuperado de:

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Luotonen, A. y Altis, K. (1994). World-Wide Web Proxies. Recuperado de: http://courses.cs.vt.edu/~cs4244/spring.09/documents/Proxies.pdf

Microsoft. (2015). Safety y Security Center. Recuperado de: https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx

Microsoft. (2017). Conceptos básicos sobre bases de datos. Recuperado de: https://support.office.com/es-es/article/Conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204

MITRE. (2019). MITRE. Recuperado de: https://attack.mitre.org/

Mojidra, N. (2016). Stateful vs. Stateless Firewalls. Recuperado de: Cybrary: https://www.cybrary.it/0p. 3n/stateful-vs.-stateless-firewalls/

Musienko, Y. (2019). What is Proof of Concept (POC) in Software Development. Recuperado de: https://merehead.com/blog/proof-concept-software-development/

Norton. (s. f.). What is antivirus software? Antivirus definition. Recuperado de: https://us.norton.com/internetsecurity-*malware*-what-is-antivirus.html

OWASP. (2017). OWASP. Recuperado de: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Pérez Porto, J. y Gardey, A. (2016). SMTP. Recuperado de: https://definicion.de/smtp/

Rothman, M. (2013). SIEM best practices for advanced attack detection. Recuperado de: https://searchsecurity.techtarget.com/tip/SIEM-best-practices-for-advanced-attack-detection

Securizando. (2017). IPS e IDS. Recuperado de:

https://securizando.com/definiciones/ips-e-ids/

Sr, J. P. (2016). What Is a SIEM? Recuperado de: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/

Stefanko, L. (2018). Descubrieron 29 troyanos bancarios en Google Play simulando ser apps reales. Recuperado de: https://www.welivesecurity.com/la-es/2018/10/24/troyanos-bancarios-descubiertos-google-play-simulando-apps-reales/

Swift, D. (2006). A Practical Application of SIM/SEM/SIEM Automating. Recuperado de: https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781

UpGuard. (2019). Top. 6 Free Network Intrusion Detection Systems (NIDS) Software in 2019. Recuperado de: https://www.upguard.com/articles/top-free-network-based-intrusión-detection-systems-ids-for-the-enterprise

Williams, A. T. y Nicolett, M. (2005). Improve IT Security With Vulnerability Management. Recuperado de: https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management

Anexos

Anexo 1. Mapeo de caso de uso

Definición	Descripción
Requerimiento	▪ <Descripción del requerimiento para el caso de uso>
Caso de uso SIEM	▪ <Descripción del caso del uso>
Cyber Killchain	▪ <Categoría del *cyber killchain*>
Log *sources*	▪ <Log *sources* identificados en la línea de eventos del caso de uso>

Cuadro 6. *Mapeo de casos de uso*

Fuente: elaboración propia.

Anexo 2. Glosario

Backdoor – es un medio para acceder a un dispositivo o datos cifrados que omiten los mecanismos de seguridad habituales de un dispositivo.

CIRT – por sus siglas en inglés, equipo informático de respuesta a incidentes.

Command and Control – conocido como C2 es una computadora controlada por un atacante o un *hacker* que se utiliza para enviar comandos a sistemas comprometidos por *malware* y recibir datos robados de una red objetivo.

Correlation Engine – es el procesador del sistema SIEM, capaz de analizar continuamente miles de eventos por segundo, comparándolos con un conjunto de reglas predefinidas.

Endpoint – dispositivo remoto que se comunica de ida y vuelta con una red a la que está conectado como una computadora, servidor, *router*, teléfono, etc.

Exploit – software diseñado para aprovechar una vulnerabilidad en un dispositivo, generalmente con fines maliciosos, como la instalación de *malware*.

Hardening – proceso de asegurar un sistema al reducir su superficie de vulnerabilidad, que es mayor cuando un sistema realiza más funciones. Usualmente, se hace al aplicar parches, cerrar puertos o agregar controles complementarios.

Payload – es el contenido de un *malware*, *worm* o virus que hacen la acción maliciosa.

Playbook – es un documento que proporciona a todos los miembros de una organización una comprensión clara de sus responsabilidades en los estándares de seguridad y las prácticas aceptadas antes, durante y después de un incidente de seguridad.

Resiliencia – propiedad de ser capaz de resistir o recuperarse rápidamente de condiciones cambiantes.

SIEM – por sus siglas en inglés (*Security Information and Event Management*) es un sistema de centralización de eventos de seguridad.

Threat Intelligence – es el conocimiento que le permite prevenir o mitigar ataques cibernéticos.

Whitelist – una lista de personas, dispositivos, actividades o cosas consideradas aceptables o confiables.

Zero Day – es una vulnerabilidad desconocida por aquellos que deberían estar interesados en mitigarla.