ESPECIALIZACIÓN EN CIBERSEGURIDAD

GUÍA METODOLÓGICA PARA LA CREACIÓN Y GESION DE CDUs SIEM

JORGE MARIO QUECANO CLAVIJO

MIGUEL OCTAVIO CARO HERNÁNDEZ

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

GUÍA METODOLÓGICA PARA LA CREACIÓN Y GESTIÓN DE CDUs SIEM MITRE ATT&CK

Trabajo de grado presentado como requisito para optar al título de *Especialista en Ciberseguridad*

Modalidad de grado: Monografía

Asesor Msg. Héctor Roberto Gordon

Jorge Mario Quecano Clavijo y Miguel Octavio Caro Hernandez

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESPECIALIZACIÓN EN CIBERSEGURIDAD

MANIZALES, CALDAS

2023

Dedicatoria

A mi esposa Natalia, por su ánimo y apoyo dado durante todo el proceso de la especialización, por su paciencia y amor que es el motor que impulsa el ser cada día mejor.

A mi familia, por su amor incondicional, su apoyo constante en cada paso. Sin su respaldo, este logro no hubiera sido posible. Gracias por ser mi mayor motivación y mi inspiración diaria.

Tabla de contenido

Lista de figuras

Lista de tablas

Resumen

La Detección de ciberamenazas es de vital importancia en la actualidad, las organizaciones dependen cada día más de la tecnología y de la información para realizar su operación, pero el gran incremento de tecnologías e información hacen la tarea cada vez más difícil, siendo necesario la implementación de soluciones de última generación que permitan detectar de manera temprana estas amenazas. Una de estas soluciones es el correlacionador de eventos o SIEM (Security Information and Event Mangement) por sus siglas en inglés, la cual permite detectar amenazas de manera efectiva en una organización.

El SIEM puede ser el pilar para los centros de operaciones de seguridad SOC para realizar investigación de incidentes y análisis de eventos generados por comportamiento anómalo, pero presenta un reto para las organizaciones debido a que el SIEM puede tener sobrecarga de información, muchos falsos positivos o falta de contexto para realizar el análisis si no se definen: El uso de un marco de referencia, si no tienen identificados los actores maliciosos que pueden afectarlos, si no tienen claro que tácticas, técnicas y procedimientos son usados o si no tienen identificados los riesgos en ciberseguridad que tiene la organización.

Las organizaciones deben realizar una identificación de amenazas, riesgos, activos críticos, probabilidad de ocurrencia, prioridades y necesidades de cumplimiento normativo para determinar las necesidades de detección y centrar su atención en la definición de casos de uso de correlación SIEM adecuados.

Al definir los casos de uso SIEM, las organizaciones pueden enfocar su atención en las amenazas específicas y más críticas, y definir reglas de correlación para monitorear, detectar y responder a esas amenazas de manera efectiva, permitiendo una detección temprana y una

respuesta rápida. La definición de casos de uso simplifica la gestión de la solución, ya que los analistas de seguridad pueden enfocar sus esfuerzos en los eventos más críticos y específicos, y no en una gran cantidad de eventos irrelevantes. Además, permiten garantizar el cumplimiento de requisitos normativos y legales relacionados con seguridad de la información como PCI, SOX, HIPPA entre otros.

La guía metodológica presentada busca que las organizaciones que inician con una solución SIEM, puedan contar con una detección temprana de amenazas, una respuesta rápida y efectiva, y una gestión más eficiente al apoyarse en el uso de la guía metodológica desarrollada.

Palabras clave: marco MITRE AT&CK, SIEM, ciberamenazas

Abstract

The detection of cyber threats is of vital importance today, organizations depend more and more on technology and information to perform its operation, but the large increase in technology and information make the task increasingly difficult, being necessary to implement next-generation solutions that allow early detection of these threats. One of these solutions is the event correlator or SIEM (Security Information and Event Mangement), which allows to detect threats effectively in an organization.

SIEM can be the mainstay for SOCs to perform incident investigation and analysis of events generated by anomalous behavior, but it presents a challenge for organizations because SIEM can have information overload, many false positives or lack of context to perform the analysis if not defined: The use of a frame of reference, if they do not have identified the malicious actors that may affect them, if they are not clear what tactics, techniques and procedures are used or if they do not have identified the cybersecurity risks that the organization has.

Organizations should conduct an identification of threats, risks, critical assets, probability of occurrence, priorities and compliance needs to determine detection needs and focus their attention on defining appropriate SIEM correlation use cases.

By defining SIEM use cases, organizations can focus their attention on the specific, most critical threats and define correlation rules to effectively monitor, detect and respond to those threats, enabling early detection and rapid response. The definition of use cases simplifies solution management, as security analysts can focus their efforts on the most critical and specific events, rather than on a large number of irrelevant events. In addition, they help ensure compliance with

regulatory and legal requirements related to information security such as PCI, SOX, HIPPA and others.

The presented methodological guide aims for organizations that are starting with a SIEM solution, can count on an early detection of threats, a quick and effective response, and a more efficient management by relying on the use of the developed methodological guide.

Keywords: MITRE AT&CK framework, SIEM, cyber threats

1. Introducción

El aumento constante de las amenazas cibernéticas en los últimos años, apalancadas por el proceso de transformación digital realizado por las compañías y su constante evolución y adaptación de nuevas técnicas de ataque, presentan un gran reto para las compañías. Es necesaria la implementación de herramientas de seguridad cada vez más especializadas que permitan proteger los activos y la información frente a estas amenazas como (malware, phishing, ransomware, ataques de fuerza bruta, ataques de DDoS, entre otras).

Además, la superficie de ataque de las organizaciones crece de manera elevada debido al aumento en su infraestructura, equipos de escritorio, aplicaciones, virtualización, datos, servicios nube, internet de las cosas entre otras, implicando una administración de seguridad compleja debido a la gran cantidad de componentes a ser protegidos y monitoreados. Es necesario contar con una visibilidad completa de todos los dispositivos de usuarios, aplicaciones, servicios y toda la infraestructura de la organización en tiempo real para poder identificar la gran cantidad de amenazas a la cual se enfrentan todas la organizaciones, además de la necesidad de contar con personal profesional capacitado y un sólido conjunto de procesos para anticipar, prevenir, detectar y reaccionar ante estas amenazas, con el objetivo de asegurar la información.

Esa combinación de soluciones tecnológicas, personas y procesos se conoce como un centro de operaciones de seguridad SOC por sus siglas en inglés (Security Operation Center), el cual supervisa y analiza la actividad en las redes, equipos de escritorio, servidores, dispositivos IoT, terminales, aplicaciones, sitios web, bases de datos entre otros sistemas, en la búsqueda de actividad anómala la cual podría llegar a ser un incidente que comprometa la seguridad. El SOC

debe garantizar de manera efectiva la detección, el análisis, la investigación y la corrección de posibles incidentes de seguridad.

Debido a la gran cantidad de eventos totales de seguridad multiplicándose continuamente, la detección de eventos se convierte en tarea de frecuencia diaria cada vez más compleja. El uso de soluciones de seguridad basada en tecnologías digitales de vanguardia es un factor clave para poder administrar millones de eventos. Es por esto por lo que para lograr una seguridad efectiva se debe considerar la utilización de una solución dedicada con capacidad para monitorear, detectar, responder y neutralizar amenazas cibernéticas. La solución que cumple con estas características es conocida como SIEM (Security Information and Event Management) la cual permite tener una visión global de la seguridad y control total sobre los eventos que suceden en la organización detectando cualquier tendencia o patrón fuera de lo común y de esta manera actuar de forma inmediata.

La solución SIEM ayuda a centralizar la información útil sobre potenciales amenazas gracias a su sistema de correlación de eventos, recopilando datos de eventos y registros de flujo. Dado a que el SIEM es la base de una infraestructura de seguridad, debe contar con inteligencia la cual es dada por existen una gran variedad de casos de uso (CDUs) y reglas de correlación del SIEM, los cuales deben ser categorizados de acuerdo con los riesgos y prioridades de la organización.

Existen diferentes estándares y marcos en la industria que ayudan a enfrentar los desafíos de administrar los casos de uso.

Este documento proporciona un modelo general de gestión de creación de casos de uso SIEM basado en el marco de referencia MITRE ATT&CK.

2. Localización

La ciberseguridad en Latinoamérica es una preocupación permanente que va en crecimiento teniendo en cuenta el aumento de los ciberataques y las vulnerabilidades de las organizaciones en la región.

Según el informe de la CEPAL (Comisión Económica para América Latina y el Caribe), el costo anual de los en Latinoamérica se encuentra alrededor de los $90.000 millones de dólares.

Así mismo, el informe de ciberseguridad generado por Kaspersky, en 2020 los países de la región más afectados por ataques de malware fueron:

- Brasil
- México
- Colombia
- Perú
- Chile

Los sectores más afectados son el:

- Financiero
- Servicios públicos
- Infraestructura crítica
- Telecomunicaciones

Una consideración importante a tener en cuenta es la falta de inversión de las empresas de la región en ciberseguridad. Lo anterior de acuerdo con el informe de la empresa ESET de ciberseguridad, que afirma que el 43% de las empresas de la región no tienen un plan de ciberseguridad formal, y el 25% no tiene designado un responsable de seguridad de la información.

Es importante resaltar que cada país de la región cuenta con sus propias leyes y regulaciones en el marco legal de la ciberseguridad, pero se carece de una armonización y cooperación regional en este tema.

De acuerdo con lo expuesto anteriormente consideramos que una guía metodológica para la creación y gestión de casos de uso SIEM basado en el marco MITRE ATT&CK puede ser una herramienta muy útil para orientar a las organizaciones a fortalecer y mejorar las capacidades en ciberseguridad.

3. Objetivos

Objetivo general

Presentar una guía metodológica para la creación y gestión de casos de uso en una solución SIEM basada en el marco MITRE ATT&CK.

Objetivos específicos

- Elaborar un flujo de proceso sugerido para la gestión de casos de uso.
- Detallar las actividades a realizar en cada una de las fases de la guía propuesta.
- Presentar un modelo ejemplo de documentación de casos de uso.

4. Antecedentes

El 15 de noviembre de 2017 el sector financiero Holandes (FI-ISAC) en un esfuerzo conjunto desarrolló un marco de referencia y una herramienta en Excel para realizar la gestión de casos de uso. El marco se llama “MaGMa UCF” basado en el marco de casos de uso utilizado por ABN AMRO y desarrollado por Floris Ladan y Tony Trump.

La herramienta MaGMa UCF permite la implementación práctica del marco MaGMa y puede ser descargado de (*MaGMa*, 2023).

En abril del 2020 se publicó “SPEED Use Case Framework v1.1” el cual facilita la organización de las reglas de detección de seguridad. Puede ser descargado de (Visser, 2020)

IBM publicó el artículo “A Quick Guide to Effective SIEM Use Cases” en Noviembre 11 del 2020 («A Quick Guide to Effective SIEM Use Cases», 2020)

Estos trabajos desarrollados no contemplan todos los aspectos necesarios a tener en cuenta al momento de desarrollar un caso de uso SIEM descritos en la guía metodológica desarrollada, pero son la base para su creación.

Marco normativo

Es importante relacionar los marcos normativos más utilizados como referencia para la implementación de controles y buenas prácticas.

A continuación, se relacionan los más utilizados:

NIST Cybersecurity Framework:

Marco desarrollado por el instituto nacional de estándares y tecnología (NIST) de los Estados Unidos, el cual ofrece orientación para la gestión de la ciberseguridad en empresas de cualquier tamaño y sector.

ISO/IEC 27001:

Estándar internacional que proporciona una metodología para la gestión de la seguridad de la información, el cual orienta sobre los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) en una empresa.

PCI-DSS:

Es el conjunto de requisitos de seguridad para la protección de datos de tarjetas de crédito y débito, establecido por las principales compañías y entidades que prestan servicios con tarjetas de crédito.

GDPR (reglamento general de protección de datos de la unión europea):

Es el reglamento que establece las reglas para la protección de datos personales de los ciudadanos europeos.

Ley de protección de datos personales (LPDP):

Es la norma que regula el tratamiento de los datos personales en Colombia.

Dicha ley establece los principios, derechos y obligaciones para la protección de los datos personales y la privacidad de los ciudadanos colombianos.

Ley de Delitos Informáticos:

Esta ley establece los delitos informáticos y sus respectivas sanciones.

Resolución 3067 de 2019:

Esta resolución establece las directrices para la implementación de la Estrategia de Ciberseguridad Nacional en Colombia.

5. Marco teórico

Security operation center (SOC)

Un SOC (security operation center) por sus siglas en inglés, es un centro de operaciones de seguridad, cuya función principal es la realización de las actividades de seguridad analítica para contar con una detección proactiva y en tiempo real de todo tipo de amenazas. Un SOC debe aportar en la seguridad operativa, permitiendo gestión de vulnerabilidades y gestión de incidentes (Carlos Gomez, 2020).

El personal profesional y técnico del SOC está conformado principalmente por un grupo de analistas (1er y 2do nivel) y especialistas de ciberseguridad altamente experimentados y capacitados.

Los objetivos principales de un SOC son:

1. Tener capacidad de monitorear y detectar amenazas y actividades maliciosas
2. Analizar posibles ataques, vulnerabilidades y amenazas
3. Reducir tiempo de inactividad y garantizar la continuidad de negocio en caso de ataque.
4. Recuperar la información afectada por consecuencia de algún ataque
5. Mejorar la capacidad de respuesta en caso de un ciberataque o incidente
6. Ofrecer soporte de auditoría y cumplimiento.

Un SOC gestiona los eventos, lo cual consiste en la administración de soluciones de seguridad (regularmente), monitoreo de eventos, alertas y categorización de estos. Da respuesta a

incidentes, analiza y coteja la información de distintas fuentes, analiza y determina el estado de los activos críticos y entrega recomendaciones para remediación. Además, realiza cacería de amenazas complejas, anticipando posibles incidentes futuros.

Un SOC mejora la detección de incidentes de seguridad, realizando un monitoreo continuo y el análisis de la actividad de los datos permiten localizar cualquier amenaza o movimiento sospechoso al instante. Las organizaciones aumentan la capacidad de defenderse de cualquier ciberamenaza, minimizando el tiempo entre que el ataque es realizado y el tiempo de respuesta frente a la amenaza.

En el SOC cuenta con tres niveles de actuación:

Nivel 1: Dentro del nivel 1 de un SOC se encuentran los analistas de ciberseguridad, cuya principal función es la supervisión y monitorización de las alertas de seguridad procedentes de las soluciones de seguridad del SOC. Después del primer análisis, si es necesario dependiendo de la alerta o incidente esta se escalaría a los analistas nivel 2.

Nivel 2: Los analistas Senior nivel 2 realizan un primer mapeo del tipo de alerta y su afectación en los sistemas a proteger; si existe un impacto, los analistas nivel 2 tienen la facultad de dar respuesta y aplicar las primeras acciones correctivas.

Nivel 3: En el nivel 3 de un SOC se cuenta con profesionales con alta capacitación y experiencia en ciberseguridad. Estos expertos tienen la capacidad de realizar la resolución de incidentes de seguridad que han sido escalados desde el nivel 2.(Torres, 2022)

El SOC lidera la respuesta a incidentes en tiempo real e impulsa mejoras continuas de seguridad para defender a la organización de las ciberamenazas. Un SOC que funciona

correctamente brindará los siguientes beneficios al emplear una combinación complicada de las tecnologías y las personas adecuadas para monitorear y controlar toda la red:

El monitoreo continuo del comportamiento implica revisar el estado de todos los sistemas las veinticuatro horas del día, siete días a la semana, durante todo el año. Como resultado, los SOC pueden otorgar el mismo peso a los esfuerzos reactivos y proactivos porque la inactividad anómala se identifica de inmediato. Los modelos de comportamiento se pueden usar para educar a los sistemas de recopilación de datos sobre qué acciones son sospechosas y alterar los datos que pueden identificarse como falsos positivos.

Mantener los registros de eventos permite a los analistas del equipo SOC realizar búsquedas en el tiempo y descubrir actos pasados que pueden haber provocado una infracción. El SOC debe realizar un seguimiento de todas las comunicaciones y actividades dentro de una organización.

Capacidades de inteligencia y detección de amenazas que evalúan el origen, el efecto y la gravedad de cada evento cibernético

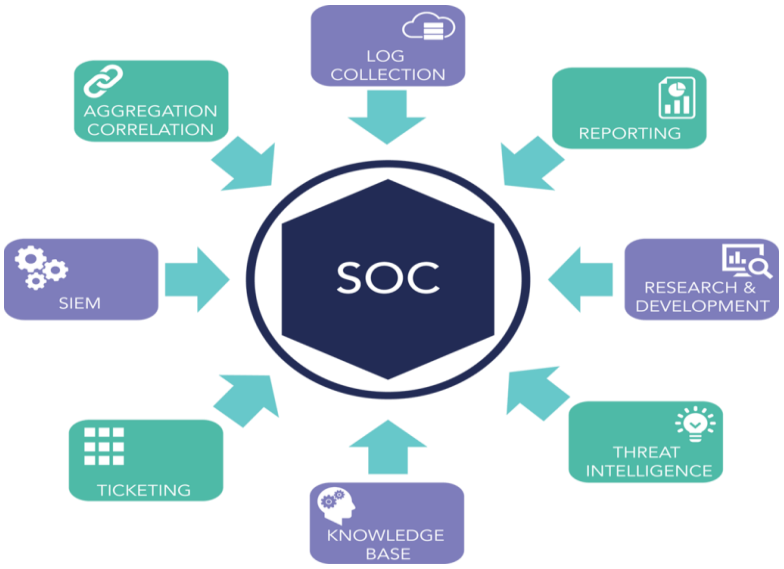
Informes para garantizar que todos los incidentes y amenazas se introduzcan en el repositorio de datos en el futuro, haciéndolo más preciso y receptivo.

La gestión del cumplimiento es esencial para garantizar que los miembros del equipo SOC y la organización se adhieran a los requisitos normativos y organizativos al ejecutar los objetivos comerciales. Por lo general, un miembro del equipo está a cargo de la educación y la aplicación del cumplimiento.

El equipo SOC también está a cargo de la operación, la administración y el mantenimiento del centro de seguridad como un recurso organizacional. Esta situación implica formular una

estrategia, un plan y procesos generales para respaldar las operaciones del centro. El grupo también evalúa, implementa y administra herramientas, dispositivos y aplicaciones y supervisa su integración, mantenimiento y actualizaciones.

Figura 1
Security Operation Center



Nota. Fuente: (Martínez, 2021)

Además de administrar incidentes específicos, el SOC recopila fuentes de datos de cada activo para crear una imagen de referencia de la actividad regular de la red. Luego, el SOC emplea esta información para detectar actividad inusual con una velocidad y precisión increíbles.

Una de las características más esenciales del SOC es que se ejecuta constantemente y ofrece capacidades de monitoreo, detección y respuesta las 24 horas del día, los siete días de la semana. Esto ayuda a las organizaciones a acortar su "tiempo de interrupción", la ventana crítica entre el momento en que un intruso compromete la primera máquina y cuando puede moverse lateralmente a otras secciones de la red, al garantizar que las amenazas se aíslen y se manejen rápidamente (Acanerler, 2022).

Una infraestructura típica en un SOC se compone de firewall, IPS o IDS, soluciones de detección de brechas, sondas y un SIEM el cual se detalla en el capítulo II.

SIEM (security information and event management)

El SIEM es una solución tecnológica con capacidad de detectar de forma rápida, contener y responder frente a amenazas informáticas. Su función principal es la de proporcionar una visión global de la seguridad tanto de la infraestructura tecnológica como de la información.

La solución SIEM surge de la combinación de las funciones de dos productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

Un SIEM permite tener una visibilidad completa de la seguridad informática y de la información de la organización. Al consolidar todos los eventos(logs) que suceden cada segundo de todas las plataformas de la organización, la plataforma puede detectar tendencias y centrar la atención de los analistas en los patrones fuera de lo común.

SEM únicamente centraliza el almacenamiento de logs, realiza la gestión de eventos de seguridad y permite realizar un análisis casi en tiempo real de lo que está sucediendo, detectando patrones anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad.

Mientras que SIM permite agrupar los datos (logs) a largo plazo en un repositorio central para luego ser analizados, suministrando la posibilidad de crear informes automatizados a los analistas para ser evaluados para toma de decisiones.

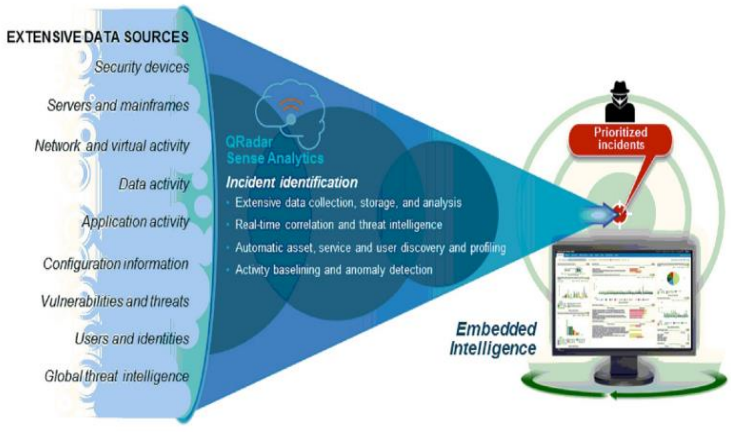
En las tecnologías de la información a nivel general el evento, registro o log es una información de bajo nivel generada y reportada por un sistema operativo, o una aplicación en concreto que permite conocer qué se está haciendo en los sistemas, que está ocurriendo, que se

está procesando, que se está guardando, que se está enviando, incluyendo además errores posibles, cualquier problema o avisos de alerta, y cuando ha sucedido esto, mostrando la hora, la fecha, el origen (direcciones IP, direcciones MAC), el usuario, y alguna otra información que sea posible registrar dependiendo del sistema, para determina que lo que ha sucedido.

Cada sistema, aplicación o solución y cada sistema operativo normalmente tienen un formato diferente de log; esto depende de cada fabricante de hecho y aunque existe un estándar de unificación de registros de log en la industria llamado syslog, la mayoría de soluciones, aplicaciones y todo aquello que pueda generar un log, tienen sus propios formatos («Sancho Lerena», s. f.)

El SIEM permite normalizar los eventos de diferentes plataformas para ser entendidos y utilizados para la creación de reglas de correlación, permitiendo que se pueda actuar de una forma ágil y rápida sobre los ataques, ya que por un lado ofrecen más visibilidad y por otro permiten utilizar los datos (logs) para la supervisión y el análisis de la seguridad en tiempo real, notificando de los ataques que se están produciendo, o incluso los que se van a producir (SOFECOM, 2023)

Figura 2
Fuentes de eventos SIEM



Nota. Fuente: (Virginia Fernandez, 2023)

Es imposible evitar un riesgo crítico en su totalidad en el panorama del entorno informático actual, por lo tanto, detectar y registrar las amenazas a tiempo puede reducir al mínimo el impacto ocasionado. El SIEM es la base fundamental para iniciar un proyecto de respuesta de incidentes en tiempo real de eventos de seguridad detectados en cualquier organización.(IONOS, Digital Guide, s. f.)

Correlación de eventos

La correlación de eventos consiente en descubrir y aplicar asociaciones lógicas entre eventos de diferentes fuentes, es posible que dichos pertenezcan a cualquier tipo de recolección o registro, como por ejemplo correlacionar eventos de una aplicación y eventos de acceso del usuario en el firewall interno.

La correlación de eventos permite no solo el organizar estos registros. A partir de ella, podemos tomar mejores decisiones con base en los datos recopilados. Esto se debe a que se tiene una visión más clara y amplia de los eventos ocurridos alrededor de los activos. Además, se pueden identificar las amenazas detectadas y responder eficientemente ante ellas. Una de las grandes ventajas de la correlación de eventos es la validación de la efectividad de los controles de seguridad.

Con la información recolectada y almacenada se puede entender donde existe un comportamiento anómalo y detectar ya sea fallas en las plataformas o eventos asociados a ataques cibernéticos.

Para visualizar mejor la correlación de eventos, podemos plantear el escenario donde se registran una alto número de eventos tentativos de iniciar sesión con la cuenta de un funcionario de la compañía que no había sido usada durante un periodo superior a dos años, por lo tanto dicha

cuenta e posible que inicie con la generación de dudosos comandos en poco tiempo, otro ejemplo puede ser la detección de inicio de sesión en de un usuario en Colombia y al paso de horas, la detección de inicio de sesión del mismo usuario desde una IP en China; por lo anterior realizando la correlación de eventos, un SIEM ayudaría en la determinación del evento y es posible que determinar si lo que se está analizando es una enumeración de cuentas y generar la alerta de que se está llevando a cabo un ataque.

Así las cosas, si después de varios intentos de inicio de sesión, uno tuvo éxito, en la correlación del evento se marcará cómo importante; por lo tanto, adicionalmente se detecta que 15 minutos antes, un puerto del sistema en cuestión fue escaneado; se determina que la dirección IP que sufrió el escaneo de puertos y los intentos de inicio de sesión son idénticos. Por lo anterior el SIEM cuenta con la capacidad de configurar alertas gracias a la correlación de los eventos descritos generando el evento y categorizarlo como crítico (esto dependerá de la organización de acuerdo con sus drivers de negocio), y dicha alerta debe recibir atención inmediata de acuerdo con los SLAs establecidos y ser marcado como incidente de seguridad.

Otro escenario de correlación de eventos en un SIEM podría ser la detección de múltiples intentos de acceso a una aplicación crítica desde direcciones IP sospechosas, seguidos de un gran volumen de tráfico de red saliente desde la misma dirección IP.

El SIEM tiene la capacidad de correlacionar estos eventos y generar una alerta de seguridad para indicar que hay una posible actividad malintencionada en la red. Esta alerta podría desencadenar medidas de seguridad adicionales, como el bloqueo de las direcciones IP sospechosas en los firewalls de la red, la notificación al equipo de respuesta a incidentes de seguridad, y la revisión de las políticas de seguridad en torno al acceso a la aplicación crítica y al monitoreo de tráfico de red.

Caso de uso en un SIEM

Un caso de uso puede ser una combinación de varias reglas técnicas dentro de una herramienta SIEM, o puede ser una combinación de acciones de varias reglas, según la necesidad. Convierte las amenazas en reglas técnicas SIEM, que luego detectan posibles amenazas y envían alertas al SOC. Construir y definir los casos de uso correctos ayuda a diferenciar los falsos positivos de los reales. También recomienda acciones basadas en la actividad actual o histórica que podría ser parte de un ataque en curso o futuro.

Es importante destacar que para que los casos de uso tengan mayor efectividad se pueden interrelacionar varios casos de uso. Normalmente, no funcionan tan bien solos. Su entrada combinada o cadena de acción determina la complejidad del tipo de ataque entrante.

Los casos de uso tienen tres componentes principales:

1. Reglas, que detectan y activan alertas basadas en eventos específicos
2. Lógica, que define cómo se considerarán los eventos o la reglas
3. Acción, que determina qué acción se requiere si se cumplen la lógica o las condiciones

Es de vital importancia definir qué marco de referencia se va a utilizar antes de iniciar la creación de los casos de uso y para esto IBM plantea los siguientes pasos:

1. Elija una herramienta en la que pueda diseñar y mapear el marco de casos de uso. Una vez que decida qué marco usar, comience a priorizar y centrarse en las amenazas y los riesgos comerciales que tienen un impacto financiero, de reputación y de datos para su grupo.

2. Piense en las categorías de ataque. Esto significa definir las amenazas comerciales que probablemente lo afecten, como el phishing, la extracción de datos, etc. Vincule cada tipo de

ataque que se aplique a usted con una o más amenazas comerciales. Al final de este paso, tendrá un mapa que muestra la relación entre los riesgos comerciales y los ataques.

3. Cree otra relación para especificar dónde y cómo deben abordarse estos ataques. Identifique los tipos de ataques enumerados y colóquelos dentro del marco seleccionado. Por ejemplo, un ataque de escaneo externo se incluirá en el reconocimiento/objetivo dentro del marco.

4. Conectar ambas relaciones: amenazas comerciales a ataques y ataques a framework.

Ahora, puede organizarlos en casos de uso de SIEM. Las amenazas comerciales identificadas serán casos de uso de alto nivel. Estos pueden dividirse aún más en casos de uso de bajo nivel. Dos o tres pueden anidar dentro de cada caso de uso de alto nivel. Siempre habrá cierta superposición en términos de cómo encajaría un caso de uso en múltiples amenazas comerciales/casos de uso de alto nivel. Por ejemplo, suponga que tiene un caso de uso de alto nivel: pérdida de datos. Los casos de uso de bajo nivel anidados dentro del caso de uso de pérdida de datos serían compromiso del servidor, exportación de datos desde el servidor y actividad de administrador no autorizada en el servidor.

Cada caso de uso de bajo nivel tendrá una conexión lógica con ciertos tipos de ataque, lo que ayudará cuando esté definiendo reglas técnicas. Cada caso de uso de bajo nivel puede encajar en varias reglas, y una regla puede estar relacionada con varios casos de uso de bajo nivel. Es importante definir esta estructura para mostrar esa conexión, ya que esto definirá aún más qué fuentes de registro necesita para que funcionen las reglas técnicas (Asheesh Kumar, IBM).

The cyber kill chain

El Marco Cyber Kill Chain, fue desarrollado por Lockheed Martin, hace parte del modelo intelligence driven defence el cual busca explicar los procedimientos que normalmente siguen los

ciberdelincuentes para realizar un ciberataque con éxito. Este marco tiene su origen en los modelos de ataque militares y acoplado al entorno digital con el objetivo de apoyar a los equipos a interpretar, prevenir y detectar las ciberamenazas. Es importante aclara que no ha todos los tipos de ciberataques se les aplicará los pasos del modelo Kill Chain, la mayor parte de los ataques utilizan todos los pasos, frecuentemente abarcar del paso 2 al paso 6 (Acanerler, 2022).

El Kill-Chain de Lockheed Martin consiste en siete fases diseñadas para representar los objetivos del atacante que deben lograrse para comprometer con éxito una red objetivo y realizar acciones maliciosas, como robo de datos, denegación de servicio o destrucción del sistema. Los investigadores de seguridad han podido identificar evidencia empírica para la mayoría de las fases dentro del Kill-Chain de Lockheed Martin y atribuir dicha evidencia a indicadores de intentos de lograr los objetivos del atacante definidos por sus respectivas fases. Sin embargo, estas fases a menudo se extienden más allá del alcance de la red de una sola organización y pueden requerir datos no disponibles para los equipos de seguridad internos para identificar amenazas.(Bryant & Saiedian, 2017)

El objetivo de los siete pasos de Kill Chain es ayudar a las organizaciones a entender mejor cómo funcionan los ataques cibernéticos y cómo pueden protegerse contra ellos. Al comprender cada paso de un ataque típico, las organizaciones pueden implementar medidas de seguridad adecuadas para prevenir, detectar y responder a los ataques.

Paso 1: Reconocimiento

Los ataques cibernéticos más efectivos comienzan con una amplia recopilación de información, como cualquier forma convencional de guerra. El reconocimiento es el primer paso en la cadena de eliminación de la seguridad cibernética y emplea una variedad de métodos, dispositivos y funciones estándar para navegar por Internet, incluidos:

- Archivos web
- Comando whois
- Motores de búsqueda
- Servicios públicos en la nube
- Servicios públicos en la nube
- Registro de nombres de dominio
- Escaneos de puertos
- Analizadores de protocolos de paquetes cómo wireshark, tcpdump, etc
- Rastreo de red con nmap

Los ciberdelincuentes utilizan una amplia gama de herramientas y tácticas para aprender sobre sus objetivos, cada una de las cuales revela segmentos únicos de información que podrían usar para encontrar puntos de entrada a las bases de datos, redes y aplicaciones más específicas que utiliza. Para evitar que los ciberdelincuentes descubran información comprometedora cuando navegan por los recursos que pone a disposición del público, incluidas las aplicaciones y los servicios en la nube, es crucial que proteger los datos confidenciales detrás de las defensas SASE en la nube, el cifrado y las páginas web seguras.

Paso 2: Preparación

Un atacante seleccionará uno o más vectores de ataque para iniciar la incursión en el área una vez que haya obtenido información adecuada sobre la víctima. Un vector de ataque es una técnica utilizada por los ciberdelincuentes para acceder a los sistemas y datos sin autorización. Los métodos de ataque van desde los más sencillos hasta los más sofisticado, pero es importante

recordar que los ciberdelincuentes con frecuencia seleccionan objetivos comparando los costos y los rendimientos de sus inversiones.

Los atacantes tienen en cuenta una variedad de factores, incluidos el poder de cómputo, el tiempo y el valor. Los ciberdelincuentes comunes a menudo elegirán la ruta más fácil, por lo tanto, es crucial pensar en todos los puntos de acceso potenciales a lo largo de la superficie de ataque (todas las ubicaciones en total donde es vulnerable al ataque) y reforzar su protección según sea necesario.

A continuación, relacionamos los algunos vectores de ataque:

- Cifrado deficiente o ausencia de cifrado
- Credenciales poco seguras
- Relaciones de confianza entre dispositivos y sistemas
- Phishing
- Ataques de inyección SQL
- Ataques de denegación de servicio (DoS)
- Ataques de intermediario (MITM)
- Troyanos, RAT

Paso 3: Distribución

En este paso el ciberdelincuente tendrá la libertad que necesita para repartir la carga de lo que sea que tenga reservado, en razón a que ya tiene acceso a las redes. Por lo tanto, puede inyectar cualquier carga maliciosa y configurarla para manejar cualquier ataque, ya sea inminente, planificado o provocado por un evento específico (ataque de bomba lógica). A veces, los

ciberdelincuentes pueden llevar a cabo estos ataques en un solo paso, o pueden crear un enlace remoto a la red.

Paso 4: Explotación

Según el método de ataque, el ciberdelincuente comienza a explotar el sistema una vez que ha entregado su carga útil. El término de "bomba lógica" se refiere a un asalto que está programado para una fecha posterior o que se activa cuando el objetivo realiza una acción en particular. Para evitar ser descubiertos, estos programas ocasionalmente tienen características de ofuscación que ocultan sus actividades y lugar de origen.

Paso 5: Instalación

El siguiente paso para un ciberdelincuente es instalar una puerta trasera para adquirir acceso continuo a los sistemas objetivo y de esta manera, puede entrar y salir de la red objetivo sin correr el peligro de ser descubierto al volver a entrar por diferentes rutas de ataque.

Estas puertas traseras se pueden instalar usando rootkits, y siempre que no muestren ningún comportamiento sospechoso (como tiempos de inicio de sesión irregulares o transferencias masivas de datos), pueden ser difíciles de encontrar.

Paso 6: Comando y control

El ciberdelincuente tomará el control de los sistemas después de instalar el malware y las puertas traseras y llevará a cabo cualquier ataque que haya planeado. Por lo tanto, cualquier acción que se tome aquí, solo se hará con la intención de mantener el objetivo bajo control. Dichas acciones pueden ser instalar ransomware, malware u otras herramientas que permitirán que los datos se filtren al exterior en el futuro.

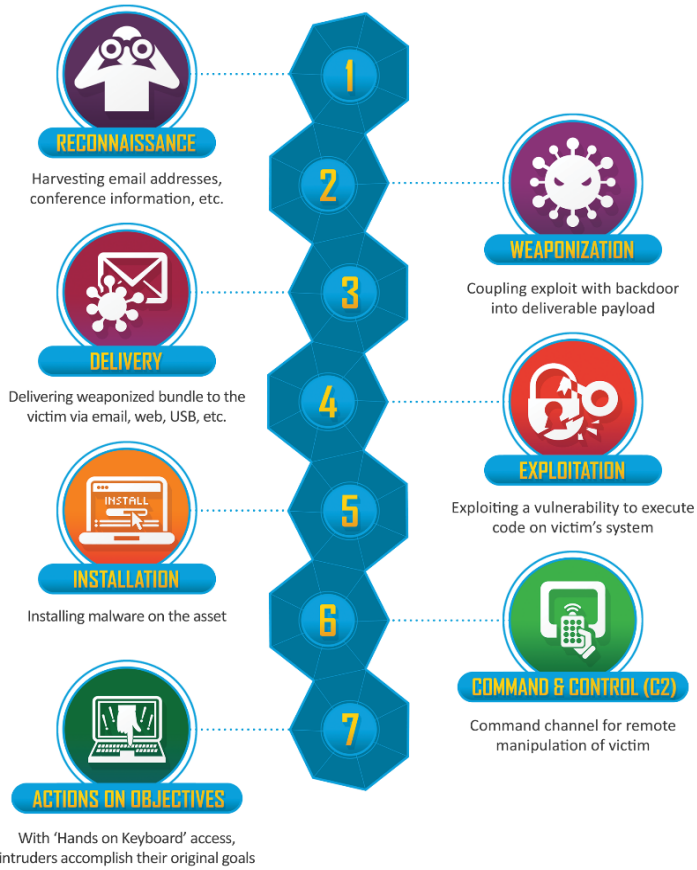
Paso 7: Acciones sobre los objetivos

En este paso un atacante actúa contra su objetivo y puede, entre otras cosas, encriptar sus datos a cambio de un rescate, filtrarlos al extranjero para obtener ganancias financieras, derribar su red a través de un ataque de denegación de servicio (DoS) o vigilar el sistema.

Las principales tácticas en esta etapa final de Kill Chain es la vigilancia permanente y el ciberespionaje, donde los atacantes mantienen un comportamiento encubierto y persistente

Figura 3

Pasos de Cyber Kill Chain



Nota. Fuente: (*Lockheed Martin Corporation*, 2023)

Att&ck de mitre

Con el fin de definir y categorizar las actividades de los adversarios en función de las observaciones reales, MITRE lanzó ATT&CK (adversaries tactics, techniques and common knowledge) en 2013. STIX y TAXII son solo dos de las matrices utilizadas para expresar los comportamientos conocidos de los atacantes que conforman la lista organizada. conocido como ATT&CK. Esta lista se puede utilizar para una serie de medidas ofensivas y defensivas, juegos de roles y otros métodos, ya que proporciona una descripción bastante completa de las acciones que realizan los ciberdelincuentes cuando se infiltran en las redes.

Enterprise, Mobile y PRE-ATT&CK son algunas de las empresas matrices de ATT&CK suministradas por MITRE. Cada una de estas matrices tiene diferentes estrategias y métodos relacionados con los contenidos de la matriz. Enterprise Matrix contiene métodos y estrategias que funcionan con computadoras Windows, Linux o Macintosh. Los dispositivos móviles se pueden utilizar con ciertas estrategias y procedimientos. PRE-ATT&CK incluye estrategias utilizadas por los atacantes para prepararse para un intento de infiltrarse en una red o sistema específico. (*MITRE,* 2023)

Al momento hay 14 tácticas en Enterprise ATT&CK Matrix:

Es importante que para mantener actualizada la información validen en la página oficial de Mitre ATT&CK la matriz actualizada, debido a que esta cambia regularmente al ser actualizada con nuevas tácticas y técnicas.

Tabla 1
Tácticas y atacantes MITRE ATT&CK

Táctica	Atacante(s) Objetivo
Reconocimiento	Recopilar información que puedan usar para planificar operaciones futuras.
Desarrollo de recursos	Establecer los recursos que pueden utilizar para apoyar las operaciones
Acceso inicial	Entra en tu red
Ejecución	Ejecutar código malicioso
Persistencia	Mantener su punto de apoyo
Escalada de privilegios	Obtener permisos de nivel superior
Evasión de defensa	Evita ser detectado
Credencial de Acceso	Robar nombres de cuenta y contraseñas
Descubrimiento	Descubre tu entorno
Movimiento lateral	Muévete por tu entorno
Colección	Recopilar datos de interés para su objetivo
Mando y Control	Comunicarse con sistemas comprometidos para controlarlos
Exfiltración	Robar datos
Impacto	Manipular, interrumpir o destruir sus sistemas y datos

Fuente. https://attack.mitre.org

Figura 4

Matriz de Cyber Kill Chain

Nota. Fuente: (*MITRE*, 2023)

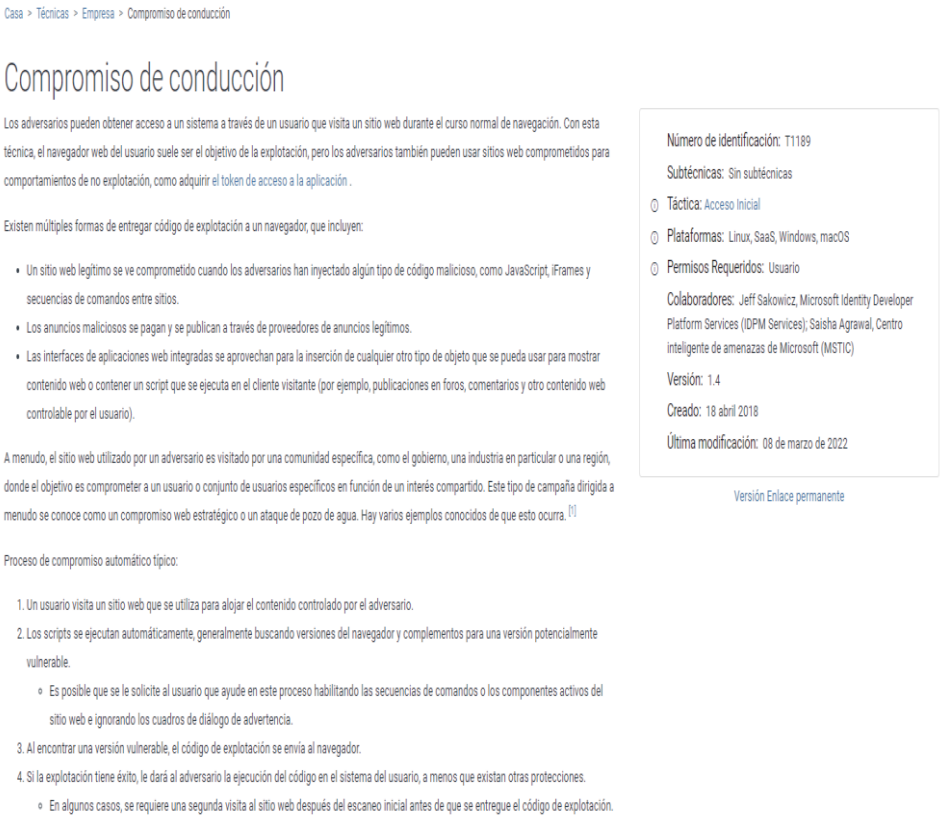
Los encabezados de columna en la parte superior de la matriz ATT&CK son tácticas y categorías de métodos. Las tácticas de los atacantes corresponden a las fases u objetivos que pretenden alcanzar, mientras que sus técnicas específicas hacen lo mismo

Una de las estrategias, por ejemplo, es el movimiento lateral. Un atacante deseará utilizar una o más de las estrategias descritas en la columna movimiento lateral de la matriz ATT & CK para lograr con éxito el movimiento lateral en una red.

Una técnica es un comportamiento específico utilizado para lograr un objetivo y, con frecuencia, es solo una de las muchas acciones que realiza un atacante para llevar a cabo todo su propósito.

Figura 5

Ejemplo descripción de técnica en ATT&CK MITRE



Casa > Técnicas > Empresa > Compromiso de conducción

Compromiso de conducción

Los adversarios pueden obtener acceso a un sistema a través de un usuario que visita un sitio web durante el curso normal de navegación. Con esta técnica, el navegador web del usuario suele ser el objetivo de la explotación, pero los adversarios también pueden usar sitios web comprometidos para comportamientos de no explotación, como adquirir el token de acceso a la aplicación .

Existen múltiples formas de entregar código de explotación a un navegador, que incluyen:

- Un sitio web legítimo se ve comprometido cuando los adversarios han inyectado algún tipo de código malicioso, como JavaScript, iFrames y secuencias de comandos entre sitios.
- Los anuncios maliciosos se pagan y se publican a través de proveedores de anuncios legítimos.
- Las interfaces de aplicaciones web integradas se aprovechan para la inserción de cualquier otro tipo de objeto que se pueda usar para mostrar contenido web o contener un script que se ejecuta en el cliente visitante (por ejemplo, publicaciones en foros, comentarios y otro contenido web controlable por el usuario).

A menudo, el sitio web utilizado por un adversario es visitado por una comunidad específica, como el gobierno, una industria en particular o una región, donde el objetivo es comprometer a un usuario o conjunto de usuarios específicos en función de un interés compartido. Este tipo de campaña dirigida a menudo se conoce como un compromiso web estratégico o un ataque de pozo de agua. Hay varios ejemplos conocidos de que esto ocurra. [1]

Proceso de compromiso automático típico:

1. Un usuario visita un sitio web que se utiliza para alojar el contenido controlado por el adversario.
2. Los scripts se ejecutan automáticamente, generalmente buscando versiones del navegador y complementos para una versión potencialmente vulnerable.
   - Es posible que se le solicite al usuario que ayude en este proceso habilitando las secuencias de comandos o los componentes activos del sitio web e ignorando los cuadros de diálogo de advertencia.
3. Al encontrar una versión vulnerable, el código de explotación se envía al navegador.
4. Si la explotación tiene éxito, le dará al adversario la ejecución del código en el sistema del usuario, a menos que existan otras protecciones.
   - En algunos casos, se requiere una segunda visita al sitio web después del escaneo inicial antes de que se entregue el código de explotación.

Número de identificación: T1189
Subtécnicas: Sin subtécnicas
Táctica: Acceso Inicial
Plataformas: Linux, SaaS, Windows, macOS
Permisos Requeridos: Usuario
Colaboradores: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Centro inteligente de amenazas de Microsoft (MSTIC)
Versión: 1.4
Creado: 18 abril 2018
Última modificación: 08 de marzo de 2022

Versión Enlace permanente

Fuente. (*MITRE*, 2023)

Un atacante podría querer obtener acceso a una red e instalar software de minería de criptomonedas en tantos sistemas como sea posible dentro de esa red, lo anterior como una ilustración de cómo funcionan las tácticas y técnicas en ATT&CK. El atacante debe completar efectivamente varios pasos intermedios para lograr este objetivo general.

Comenzará por obtener acceso a la red, tal vez utilizando un Spearphishing. Entonces, es posible que deba usar la inyección de procesos para escalar privilegios. Ahora puede usar el vertido

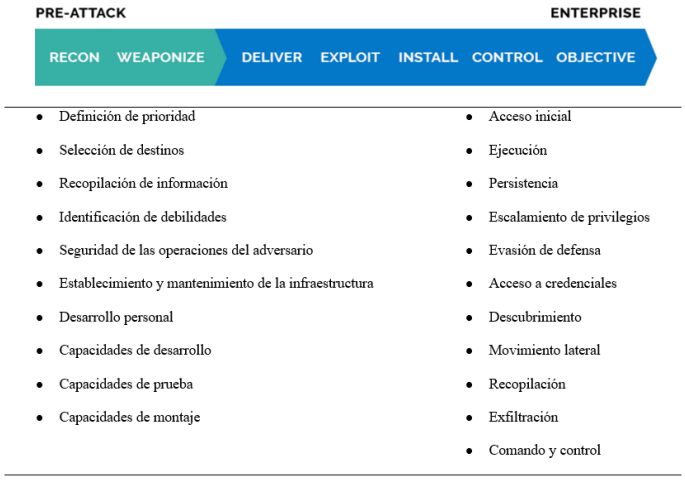
de credenciales para obtener credenciales adicionales del sistema y establecer la persistencia al programar un comando de extracción para que se ejecute de manera regular. Después de esto, el atacante podría usar Pass the Hash para moverse lateralmente a través de la red y distribuir su software de minado de criptomonedas a tantos sistemas como pueda.

En este caso, el atacante tuvo que completar con éxito cinco etapas, cada una de las cuales es una estrategia o fase de ataque distinta: acceso inicial, escalada de privilegios, acceso de credenciales, persistencia y movimiento lateral. Realizó cada fase de su ataque con un método particular dentro de estas tácticas.

Juntos, PRE-ATT&CK y ATT&CK Enterprise conforman el conjunto completo de estrategias que generalmente corresponden con la cadena de ataques cibernéticos. El reconocimiento, la armamentización y la entrega son las primeras tres etapas de la cadena de asalto a las que PRE-ATT&CK se parece más. Las acciones de explotación, instalación, comando y control son las cuatro etapas finales de la cadena de ataque, que se alinea bien con ATT&CK Enterprise. (*ANOMALI*, 2023).

Figura 6

PRE-ATT&CK y ATT&CK Enterprise



Fuente. (*ANOMALI*, 2023)

6. Metodología

La metodología aplicada para el desarrollo de la guía metodología para la creación y gestión de casos de uso de SIEM basado en marco Mitre ATT&CK es la siguiente:

Identificación del problema de investigación: El problema se centra en que no existe una guía que permita orientar a las organizaciones en la creación y gestión de casos de uso de SIEM basado en el marco Mitre ATT&CK.

Enfoque analítico sobre la situación de la ciberseguridad en relación con los casos de uso de SIEM

Diseño de la investigación: Se realizará análisis del contexto geográfico en Latinoamérica y Colombia y la documentación de normas y leyes existentes relacionadas con la ciberseguridad.

Técnicas de recolección de datos: La información recolectada por estudios realizados por grandes firmas de ciberseguridad en el mundo sobre la situación en Latinoamérica y Colombia.

Análisis de datos: Se utilizará análisis de contenido y análisis estadístico.

Limitaciones de la investigación: Se identifican las posibles limitaciones, como la falta de información del estado de la ciberseguridad en las organizaciones privadas en Latinoamérica y Colombia.

7. Cuerpo del trabajo

Guía metodológica propuesta

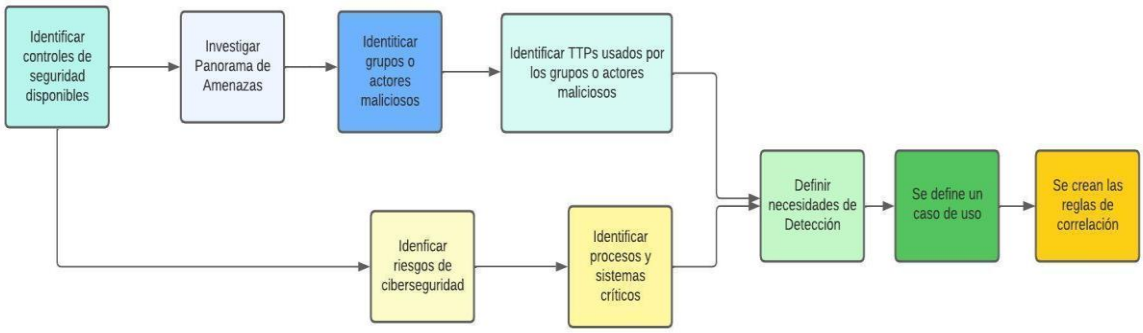
El proceso de gestión de casos de uso lo dividimos en tres partes principales:

1. Definir Casos de Uso
2. Documentar Casos de Uso
3. Mantener Casos de Uso
4. Usar herramienta de control y visibilidad de Casos de Uso

Definición Casos de Uso

Figura 7

Flujo creación de casos de uso SIEM



Fuente. Elaboración Propia

Identificar controles de seguridad

En el proceso de definición de caso de uso, el primer paso es realizar la identificación de controles de seguridad, es decir plataformas o soluciones de seguridad como, por ejemplo:

- Firewalls

- Sistemas de detección de intrusos (IDS)
- Antimalware

La identificación de los controles de seguridad brinda información sobre la capacidad de detección de la organización y es importante resaltar que “lo que no se ve no se puede controlar”.

A continuación, relacionamos los pasos básicos para la identificación de controles de seguridad:

1. Identificar los casos de uso relevantes para la organización, como por ejemplo:
    a. El acceso a datos confidenciales
    b. La autenticación de usuarios
    c. Monitoreo de la red
2. Realizar una evaluación de riesgos con el objetivo de identificar posibles amenazas y vulnerabilidades que puedan afectar a los casos de uso identificados.
3. Es necesario investigar los requisitos legales y normativos que se aplican a la organización, como:
    - La Ley de Protección de Datos Personales
    - ISO 27001
    - PCI - DSS (Payment Card Industry)

    Estos requisitos pueden incluir controles de seguridad específicos que deben ser implementados para cumplir con requisitos legales y normativos de un sector específico.
4. Una vez identificados los requisitos legales y normativos, el siguiente paso es identificar los estándares de la industria, como:
    - Marco NIST Cybersecurity Framework
    - CIS Controls

5. Revisar la documentación de seguridad de la información o ciberseguridad existente de la organización, como:

    - Políticas
    - Procedimientos
    - Planes de contingencia

La documentación permite identificar los controles de seguridad que deben ser implementados para los casos de uso relevantes.

A continuación, se relaciona un ejemplo para realizar una matriz con los controles o soluciones y sus capacidades de detección:

Tabla 2

Matriz de controles de seguridad

Solución	Ubicación	Visibilidad	Funcionalidades
Next Generation Firewall	Perímetro	• IP origen • IP destino • Puerto • Protocolo • HTTP • FTP • HTTPS • APLICACIONES • USUARIOS • CONTROL • URL	• IPS • URL • FILTERING

Fuente. Elaboración propia

Es importante que la organización cuente con un esquema de red donde se permita tener visibilidad de la arquitectura general. Lo anterior permitirá crear casos de uso y reglas de correlación con contexto.

Al identificar los controles de seguridad, se determinan las fuentes de datos que se utilizarán para recopilar información relevante para el caso de uso, como registros de eventos, logs de seguridad, alertas de sistemas, tráfico de red, entre otros.

Investigar el panorama de amenazas

Las ciberamenazas son una preocupación permanente para las organizaciones, por lo tanto, la identificación del panorama de amenazas se convierte en un factor importante y es prioridad la investigación de amenazas para la identificación de posibles riesgos, así mismo la definición de contramedidas adecuadas para proteger los sistemas y datos críticos de la organización, lo anterior implica que una organización debe tener en cuenta los siguientes factores:

- La identificación de fuentes de información relevantes
- El análisis de tendencias de amenazas
- La identificación de actores de amenazas
- La evaluación del nivel de riesgo
- La identificación de contramedidas recomendadas

A continuación, relacionamos las fases necesarias para investigar el panorama de amenazas para los casos de uso:

1. Identificar los casos de uso relevantes para la organización, como por ejemplo:
    - ❖ Acceso a los datos confidenciales
    - ❖ Monitoreo de red
    - ❖ Autenticación de usuarios

2. Investigar permanentemente fuentes de información relevantes para el panorama de amenazas, como por ejemplo:
    - ❖ Noticias y boletines de seguridad
    - ❖ Informes de ciber amenazas
    - ❖ Foros de ciberseguridad
    - ❖ Canales o redes sociales relevantes de ciberseguridad
3. Analizar las tendencias de ciber amenazas relevantes para los casos de uso identificados, como por ejemplo:
    - ❖ Vulnerabilidades más explotadas
    - ❖ Vectores de ataque más comunes
    - ❖ Patrones de comportamiento de los atacantes
4. Identificar los actores de amenazas relevantes para los casos de uso identificados así mismo la identificación de los motivos y objetivos de estos, cómo por ejemplo:
    - ❖ Ciberdelincuentes
    - ❖ Grupos de ciberdelincuencia organizada
    - ❖ Gobiernos hostiles

Así mismo un factor que complementa la identificación de actores de amenazas es la identificación de los motivos y objetivos de estos.

5. Evaluar el nivel de riesgo para los casos de uso identificados en función de la información recopilada en los 4 pasos anteriores. Es importante validar y determinar el impacto potencial de los ataques y la probabilidad de que se produzcan.
6. Identificar las contramedidas recomendadas para los casos de uso identificados teniendo en cuenta el nivel de riesgo evaluado. Algunas contramedidas pueden incluir lo siguiente:

- ❖ Controles de seguridad
- ❖ Capacitación de usuarios
- ❖ Políticas y procedimientos de seguridad

En la siguiente tabla se relaciona una guía que permite investigar el panorama de amenazas para casos de uso específico, donde se identifican los pasos necesarios para identificar y evaluar las amenazas relevantes y las contramedidas sugeridas.

Tabla 3
Pasos identificación Vectores de Amenazas

Paso	Actividades	Ejemplos de casos de uso	Vectores de amenazas
1	Identificar los casos de uso relevantes	● Sistema de gestión de nómina ● Aplicación de comercio electrónico ● Sistema de control de acceso físico	● Ataque de phishing dirigido a los empleados que manejan la información de la nómina ● Ataque de inyección de SQL en la aplicación de comercio electrónico ● Acceso no autorizado a la instalación física donde se encuentra el sistema de control de acceso
2	Investigar fuentes de información relevantes	● Boletines de seguridad de Microsoft ● Informes de amenazas de Symantec ● Blog de seguridad de KrebsOnSecurity	● Informe de vulnerabilidades de Microsoft relacionado con el sistema operativo utilizado por el sistema de gestión de nómina ● Informe de Symantec sobre una campaña de phishing dirigida a organizaciones de comercio electrónico ● Artículo de KrebsOnSecurity sobre un robo de identidad en una instalación física
3	Analizar las tendencias de amenazas relevantes	● El uso de malware como ransomware está en aumento ● Los ataques de phishing son cada vez más sofisticados	● El aumento del uso de ransomware para atacar sistemas de nómina ● El uso de correos electrónicos de phishing con contenido personalizado para atacar a empleados que trabajan en el comercio electrónico
4	Identificar los actores de amenazas relevantes	● Grupos de ciberdelincuentes que utilizan ransomware ● Empleados descontentos que tienen acceso a los sistemas de nómina	● Empleados malintencionados que realizan ataques internos en la aplicación de comercio electrónico ● Grupos de ciberdelincuentes que utilizan ataques de fuerza bruta para acceder a la instalación física donde se encuentra el sistema de control de acceso

5	Evaluar el nivel de riesgo	• El sistema de gestión de nómina presenta un riesgo alto debido a la posibilidad de un ataque interno • La aplicación de comercio electrónico presenta un riesgo moderado debido a la sofisticación de los ataques de phishing • El sistema de control de acceso presenta un riesgo bajo debido a las medidas de seguridad física implementadas	• En este campo se debe agregar: • La evaluación del nivel de riesgo • La justificación • Medidas recomendadas
6	Identificar las contramedidas recomendadas	• Capacitación de los empleados para prevenir ataques internos • Implementación de un sistema de detección de correo electrónico de phishing • Implementación de medidas de seguridad física adicionales	• En este campo se debe agregar: • Las contramedidas recomendadas • La justificación • El responsable de su implementación

Fuente. Elaboración Propia

Identificación de grupos o actores maliciosos

En el ciberespacio, identificar grupos o actores maliciosos es una tarea crítica para proteger las redes y los sistemas de una organización.

Los actores maliciosos pueden incluir desde individuos, grupos de piratas informáticos, hasta organizaciones criminales y agencias gubernamentales. Por lo tanto, la identificación de estos actores de amenazas implica una variedad de técnicas, incluyendo el análisis de registros de seguridad, el seguimiento de patrones de tráfico de red y la recopilación de inteligencia de amenazas.

A continuación, profundizaremos en cómo se puede identificar grupos o actores malicioso teniendo en cuenta los siguientes aspectos:

1. Recopilar datos es el primer paso para identificar a los grupos o actores maliciosos. Dichos datos se pueden recopilar a través de diversas fuentes como por ejemplo:

- Registros de seguridad
- Informes de inteligencia de amenazas
- Análisis de vulnerabilidades

Es importante asegurarse de que la información recopilada sea precisa, relevante, esté actualizada y que venga de fuentes confiables.

1. Realizar análisis de patrones que implica la identificación de comportamientos o acciones sospechosas. Este análisis se realiza utilizando técnicas de correlación y análisis de datos, para establecer un perfil de comportamiento para los grupos o actores maliciosos, como por ejemplo, el análisis de patrones puede ayudar a identificar cuándo se lleva a cabo un ataque y cómo se lleva a cabo, lo que puede ser útil para prevenir futuros ataques.
2. Realizar análisis de inteligencia el cual implica la recopilación y análisis de información sobre grupos o actores maliciosos, sus motivaciones, tácticas y técnicas utilizadas en sus ataques. Dicho análisis puede incluir la recopilación de información de fuentes abiertas y cerradas, como por ejemplo:

- ❖ Foros de discusión
- ❖ Redes sociales
- ❖ Sitios web

3. Realizar análisis de redes, para la identificación de las conexiones entre diferentes actores y cómo trabajan juntos, lo cual ayudará a identificar la estructura de los grupos o actores maliciosos, lo que puede ser útil para prevenir ataques futuros.
4. Usar herramientas de seguridad, como, por ejemplo:

- Sistemas de detección de intrusiones (IDS)
- Sistemas de prevención de intrusiones (IPS)
- Sistemas de gestión de eventos de seguridad (SIEM)

Lo anterior puede ser útil para identificar comportamientos maliciosos y para alertar sobre posibles amenazas; dichas herramientas también pueden ayudar a bloquear y prevenir ataques.

A continuación, se relaciona una guía para la identificación de grupos o actores maliciosos:

Tabla 4
Identificación de patrones de ataque

Identificación de patrones de ataque

Patrón de ataque	Descripción	Ejemplo
Fuerza bruta	Intentos repetidos y automatizados para adivinar credenciales o contraseñas	Ataque de fuerza bruta a la cuenta de administrador de un sistema
Ingeniería social	Utilización de la manipulación psicológica para obtener información confidencial	Phishing por correo electrónico que lleva a la víctima a revelar información personal
Inyección de código	Inserción de código malicioso en sistemas o aplicaciones para obtener acceso no autorizado	Ataque de inyección SQL para obtener información de la base de datos
Exploración de vulnerabilidades	Escaneo de sistemas en busca de vulnerabilidades que puedan ser explotadas	Escaneo de puertos en busca de vulnerabilidades

Identificación de herramientas y tácticas de ataque

Herramienta o táctica de ataque	Descripción	Ejemplo
Botnets	Redes de dispositivos infectados controlados por un atacante	Ataque DDoS utilizando una botnet
Ransomware	Malware que cifra los archivos de la víctima y exige un rescate para su recuperación	Ataque de ransomware WannaCry

Malware de acceso remoto	Malware diseñado para proporcionar acceso remoto no autorizado a sistemas	Ataque de troyano de acceso remoto (RAT)
Phishing	Ataque que utiliza correos electrónicos, mensajes de texto u otros medios para engañar a los usuarios para que revelen información confidencial	Ataque de phishing para obtener credenciales de inicio de sesión

Identificación de los objetivos de los atacantes

Objetivo de los atacantes	**Descripción**	**Ejemplo**
Robo de información	Obtención de información confidencial, como datos personales o secretos comerciales	Ataque a la base de datos de clientes de una organización
Sabotaje	Intención de causar daño a un sistema o red, interrumpiendo sus operaciones	Ataque de denegación de servicio (DoS) que deja fuera de servicio un sitio web
Extorsión	Amenaza de dañar o filtrar información a menos que se pague un rescate	Ataque de ransomware que exige un pago en criptomonedas
Espionaje	Obtención de información confidencial de una organización o país por parte de otra organización o país	Ataque de espionaje cibernético patrocinado por un estado

Identificación de la motivación de los atacantes

Motivación de los atacantes	**Descripción**	**Ejemplo**
Financiera	Obtención de beneficios económicos, como robo de datos o rescates	Ataque de phishing para robo de información bancaria
Política	Ataques contra organizaciones o gobiernos con fines políticos	Ataque de denegación de servicio a un sitio

Fuente. Elaboración Propia

Identificar TTPs usados por los grupos o actores maliciosos

Los actores maliciosos están en constante evolución y suelen utilizar técnicas cada vez más sofisticadas para llevar a cabo sus ataques. Por lo tanto es importante estar al tanto de las tácticas, técnicas y procedimientos (TTPs) utilizados por estos grupos para poder anticiparse a sus movimientos y detectar posibles amenazas.

La identificación de los TTPs puede ser un proceso complejo, ya que los grupos maliciosos suelen utilizar diferentes técnicas para lograr sus objetivos, pero es esencial para entender cómo operan.

A continuación, explicamos cómo identificar los TTPs utilizados por los grupos o actores maliciosos.

1. Recopilar información de diferentes fuentes, como por ejemplo:
   - ❖ Informes de seguridad
   - ❖ Blogs especializados
   - ❖ Investigaciones previas

   Esta información puede ser utilizada para obtener una comprensión más profunda de los grupos o actores maliciosos.

   1. Analizar la información, en búsqueda de patrones o similitudes en las técnicas utilizadas por los grupos o actores maliciosos, así mismo es necesario considerar la frecuencia de uso y la gravedad de los ataques.
   2. Utilizar herramientas de análisis puede a revisar y comparar los diferentes TTPs utilizados por los grupos o actores maliciosos. Algunas de estas herramientas incluyen ATT&CK de MITRE, Cyber Kill Chain de Lockheed Martin, y Diamond Model.

3. Actualizar y mejorar continuamente sobre las últimas tendencias y TTPs utilizados por los grupos o actores maliciosos; así mismo la información recopilada y analizada debe ser revisada y actualizada regularmente para asegurar que se tengan las medidas de seguridad adecuadas en su lugar.

A continuación, se relaciona un ejemplo de cómo se puede llevar a cabo el registro para la identificación de TTPs utilizados por grupos o actores maliciosos:

Tabla 5
Identificación Tácticas, Técnicas y Procedimientos

TTP	Descripción	Ejemplo
Spear Phishing	Ataque de phishing dirigido a un individuo o grupo específico	Un correo electrónico que parece provenir de una fuente confiable, solicitando información confidencial
Malware	Software malicioso diseñado para dañar o controlar un sistema	Un troyano que permite el control remoto de un sistema infectado
Ingeniería Social	Manipulación psicológica para obtener información confidencial	Un atacante que se hace pasar por un empleado de una organización y solicita información confidencial a un empleado desprevenido
Ataques de fuerza bruta	Ataque de prueba y error para adivinar contraseñas o claves	Un atacante que intenta adivinar la contraseña de un usuario mediante la fuerza bruta
Explotación de vulnerabilidades	Aprovechamiento de vulnerabilidades en sistemas o software	Un atacante que utiliza una vulnerabilidad en el software para obtener acceso no autorizado a un sistema

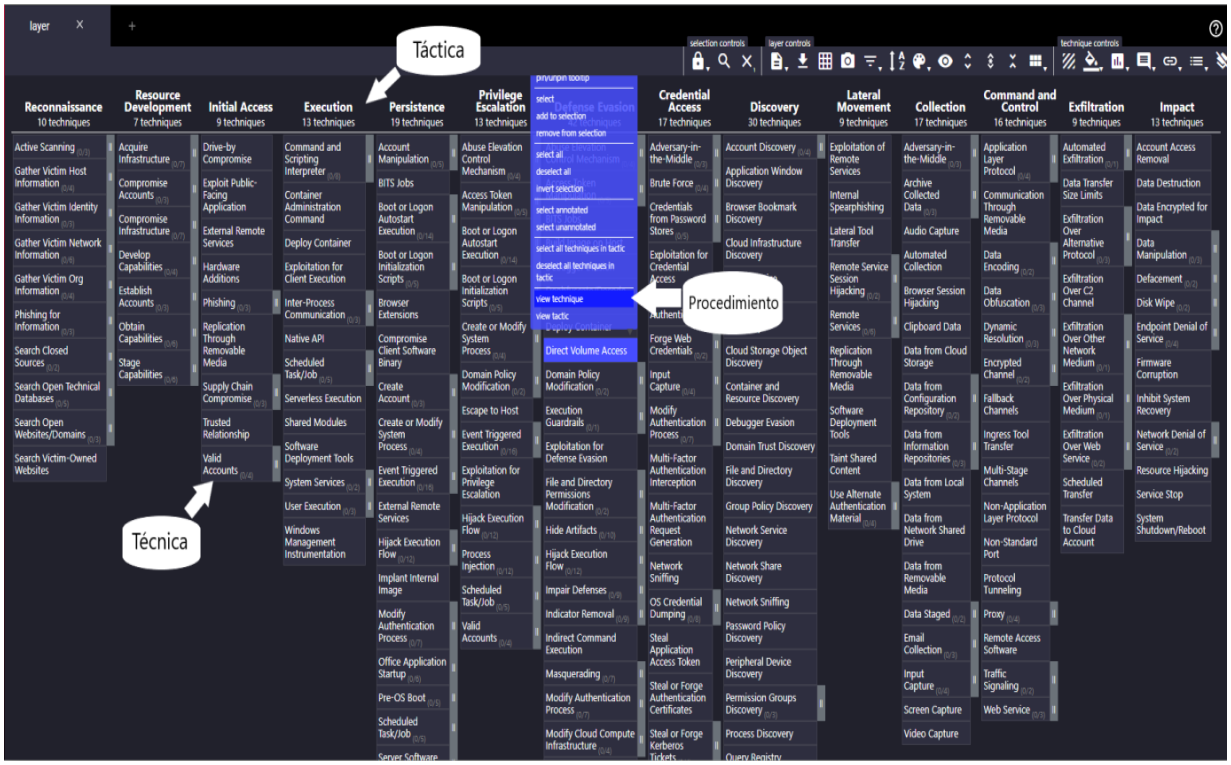
Fuente. Elaboración Propia

Identificar TTPs Utilizadas con MITRE ATT&CK Navigator

Mitre ATT&CK Navigator es una base de datos de conocimiento del comportamiento de los adversarios, TTPS creada y mantenida por MITRE (*ATT&CK® Navigator*, s. f.).

MITRE ATT&CK Navigator proporciona una navegación básica en la ATT&CK Matrix.

Figura 8
Matriz MITRE ATT&CK Navigator

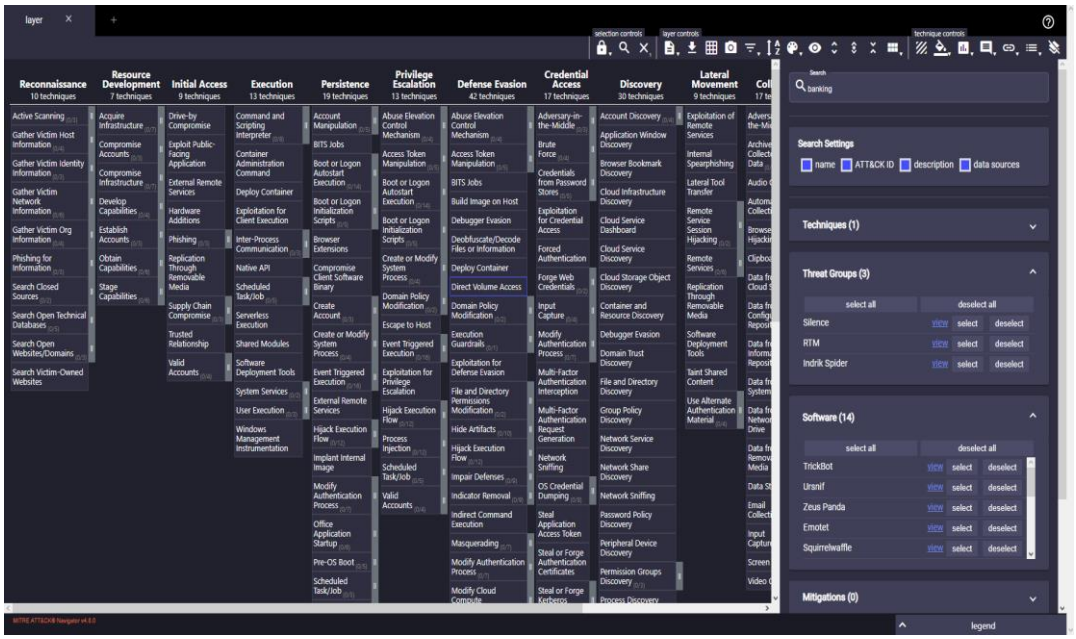


Nota. Fuente Elaboración Propia

Podrá encontrar la matriz completa de MITRE ATT&CK y realizar búsquedas personalizadas como por ejemplo identificar los grupos de actores maliciosos que atacan el sector al que pertenece su organización, por ejemplo: Banking

Figura 9

Búsqueda Banking

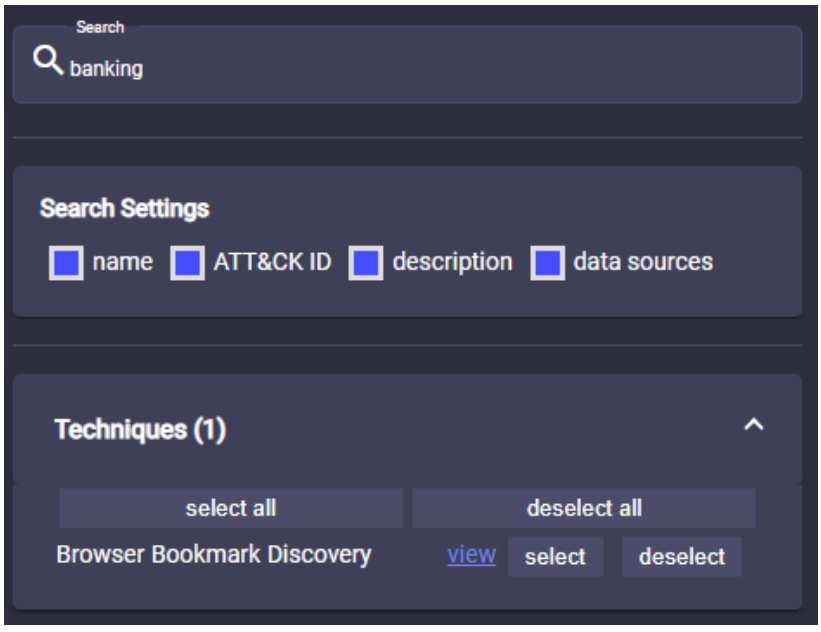


Nota. Fuente Elaboración Propia

Al digitar el sector en búsqueda, ésta mostrará las técnicas utilizadas

Figura 10

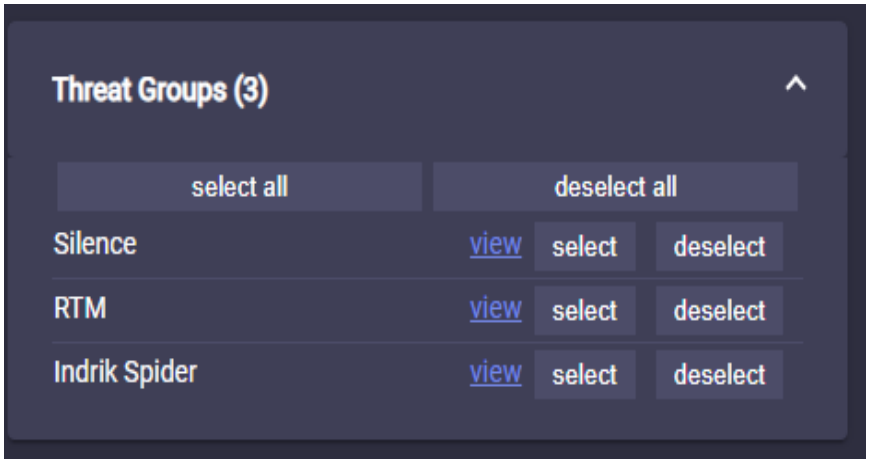
Técnicas búsqueda Banking MITRE Navigator



Nota. Fuente Elaboración Propia

Figura 11

Grupos búsqueda Banking MITRE Navigator

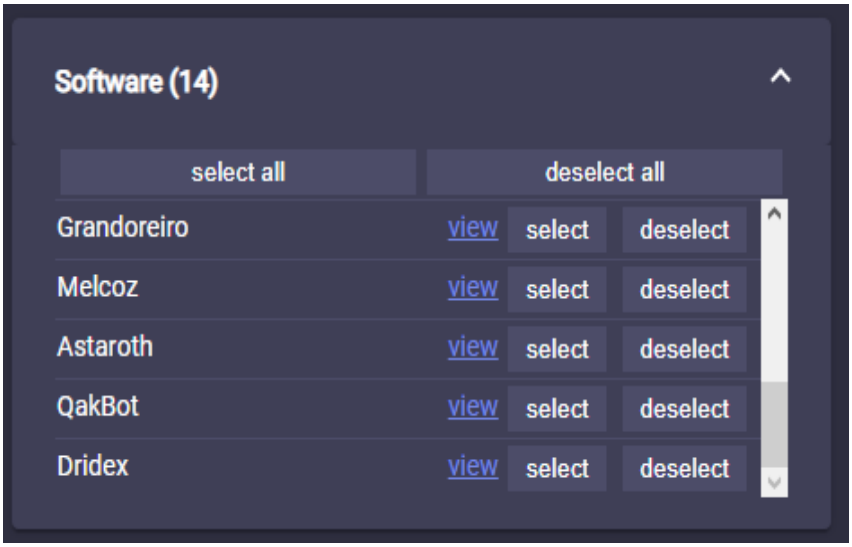


Nota. Fuente Elaboración Propia

Podrá identificar el software utilizado para realizar los ataques

Figura 12

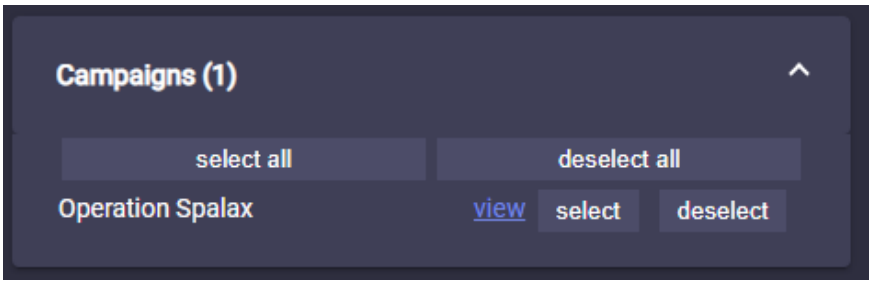
Software búsqueda Banking MITRE Navigator



Nota. Fuente Elaboración Propia

Se listarán las campañas existentes

Figura 13
Campañas búsqueda Banking MITRE Navigator

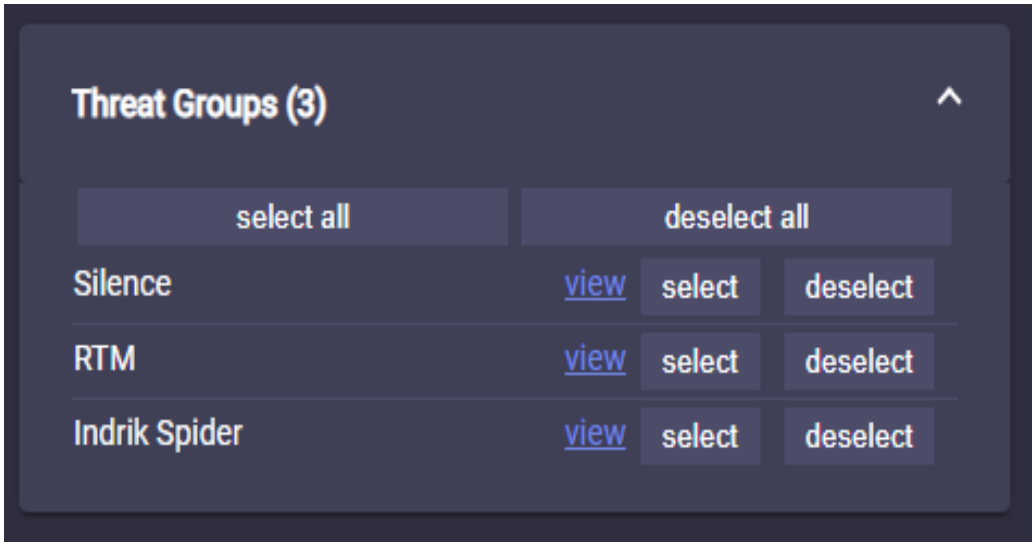


Nota. Fuente Elaboración Propia

MITRE ATT&CK Navigator permite en este caso conocer que grupos de actores maliciosos atacan al sector organizacional relevante para cada uno.

En el ejemplo al realizar la búsqueda de los actores de banking nos muestra:

Figura 14
Grupos de actores Maliciosos búsqueda Banking MITRE Navigator



Nota. Fuente Elaboración Propia

Como se puede ver en la imagen anterior, identifica 3 grupos:

Silence, RTM e Indrik Spider. Si ponemos el apuntador del mouse sobre cada grupo mostrará las diferentes técnicas usadas por cada uno de los grupos.

Figura 15

Técnicas usada por grupos de actores maliciosos en Banking MITRE Navigator

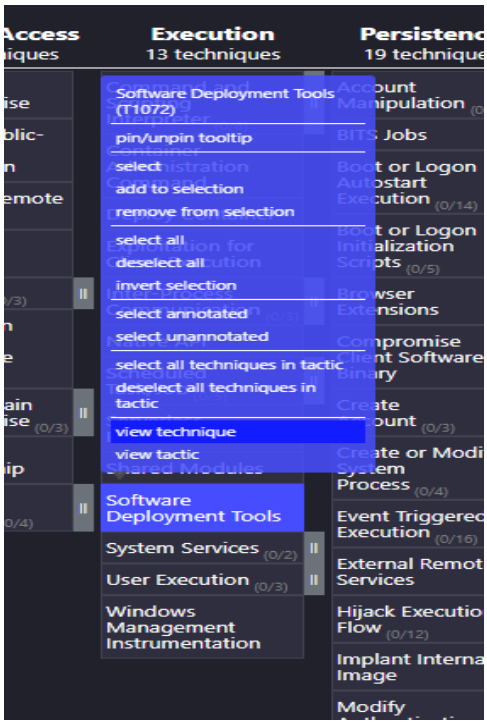
Nota. Fuente Elaboración Propia

La herramienta MITRE ATT&CK Navigator permite realizar búsquedas rápidamente, centrar la atención en las tácticas, técnicas y procedimientos que son relevantes para la organización.

Se puede dar clic en view technique en cada una de las técnicas usadas para ser dirigido a la página con el detalle de cada una de estas.

En la imagen de la siguiente página se muestra como ingresar a ver el detalle de cada técnica.

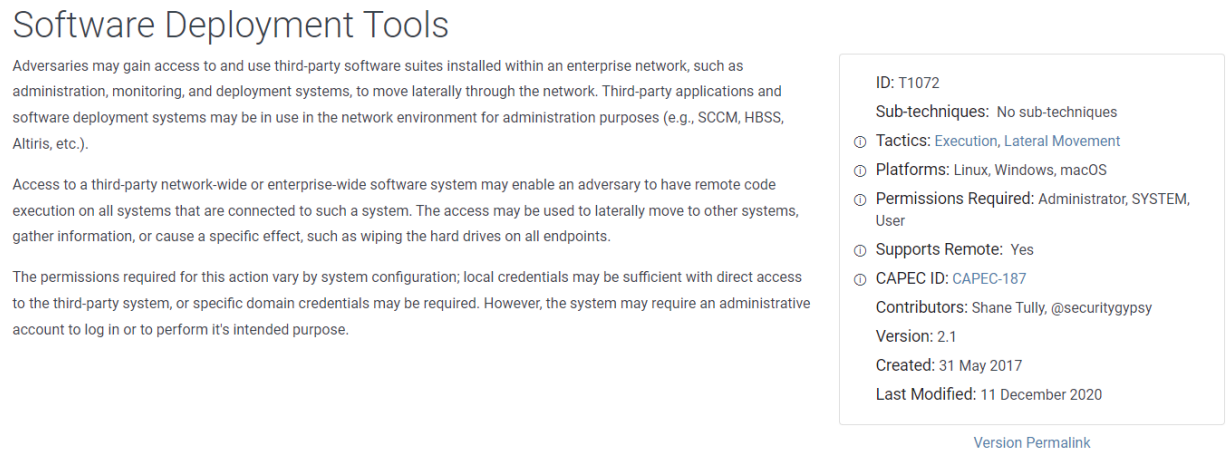
Figura 16
Selección View MITRE Navigator



Nota. Fuente Elaboración Propia

Al seleccionar view technique lo dirigirá a la página con información detallada como la de la imagen a continuación:

Figura 17
Descripción Técnica Software Deploymet Tool



Software Deployment Tools

Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network. Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, HBSS, Altiris, etc.).

Access to a third-party network-wide or enterprise-wide software system may enable an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform it's intended purpose.

ID: T1072
Sub-techniques: No sub-techniques
Tactics: Execution, Lateral Movement
Platforms: Linux, Windows, macOS
Permissions Required: Administrator, SYSTEM, User
Supports Remote: Yes
CAPEC ID: CAPEC-187
Contributors: Shane Tully, @securitygypsy
Version: 2.1
Created: 31 May 2017
Last Modified: 11 December 2020

Version Permalink

Nota. Fuente Elaboración Propia

En esa página también podrá ver información sobre otros Grupos de actores con procedimientos que usan esa técnica que se está analizando.

Figura 18

Lista de grupos de actores con procedimientos con misma técnica

Version Permalink

Procedure Examples

ID	Name	Description
G0050	APT32	APT32 compromised McAfee ePO to move laterally by distributing malware as a software deployment task.[1]
G0091	Silence	Silence has used RAdmin, a remote software tool used to remotely control workstations and ATMs.[2]
G0028	Threat Group-1314	Threat Group-1314 actors used a victim's endpoint management platform, Altiris, for lateral movement.[3]
S0041	Wiper	It is believed that a patch management system for an anti-virus product commonly installed among targeted companies was used to distribute the Wiper malware.[4]

Nota. Fuente Elaboración Propia

Por último, se pueden encontrar las recomendaciones para la mitigación.

Figura 19

Tabla de mitigaciones recomendadas MITRE ATT&CK

Mitigations

ID	Mitigation	Description
M1015	Active Directory Configuration	Ensure proper system and access isolation for critical network systems through use of group policy.
M1032	Multi-factor Authentication	Ensure proper system and access isolation for critical network systems through use of multi-factor authentication.
M1030	Network Segmentation	Ensure proper system isolation for critical network systems through use of firewalls.
M1027	Password Policies	Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network.
M1026	Privileged Account Management	Grant access to application deployment systems only to a limited number of authorized administrators.
M1029	Remote Data Storage	If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.
M1051	Update Software	Patch deployment systems regularly to prevent potential remote access through Exploitation for Privilege Escalation.
M1018	User Account Management	Ensure that any accounts used by third-party providers to access these systems are traceable to the third-party and are not used throughout the network or used by other third-party providers in the same environment. Ensure there are regular reviews of accounts provisioned to these systems to verify continued business need, and ensure there is governance to trace de-provisioning of access that is no longer required. Ensure proper system and access isolation for critical network systems through use of account privilege separation.
M1017	User Training	Have a strict approval policy for use of deployment systems.

Nota. Fuente Elaboración Propia

Además, muestra detalles de la tecnología que puede ayudar a detectar el comportamiento de los adversarios que hacen uso de la técnica, así como referencias para realizar una investigación más profunda.

Figura 20
Técnologia recomendada de detección técnica MITRE ATT&CK

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Often these third-party applications will have logs of their own that can be collected and correlated with other data from the environment. Ensure that third-party application logs are on-boarded to the enterprise logging system and the logs are regularly reviewed. Audit software deployment logs and look for suspicious or unauthorized activity. A system not typically used to push software to clients that suddenly is used for such a task outside of a known admin function may be suspicious. Monitor account login activity on these applications to detect suspicious/abnormal usage.Perform application deployment at regular times so that irregular deployment activity stands out.
DS0009	Process	Process Creation	Monitor for newly executed processes that does not correlate to known good software. Analyze the process execution trees, historical activities from the third-party application (such as what types of files are usually pushed), and the resulting activities or events from the file/binary/script pushed to systems.

Nota. Fuente Elaboración Propia

Identificar riesgos de ciberseguridad

La identificación de riesgos de ciberseguridad es un proceso necesario para mantener la seguridad de una organización. Los riesgos pueden provenir de diversas fuentes, como, por ejemplo:

- Amenazas internas y externas
- Vulnerabilidades en sistemas y aplicaciones
- Errores humanos

Para identificar los riesgos de ciberseguridad, es importante seguir un proceso estructurado que permita identificar, evaluar y priorizar los riesgos.

El proceso de identificación de riesgos de ciberseguridad se divide en los siguientes pasos:

1. **Identificación de activos:** es prioritario tener una lista detallada de los activos de información que posee la organización, como, por ejemplo:
    - Sistemas, aplicaciones
    - Documentos
    - Bases de datos
2. **Identificación de amenazas:** es necesario identificar las posibles amenazas a los activos de información, tanto internas como externas, como, por ejemplo:
    - Malware
    - Phishing
    - Ingeniería social
    - Vulnerabilidades de seguridad
3. **Identificación de vulnerabilidades:** identificar las vulnerabilidades en los sistemas, aplicaciones y otros activos de información.
4. Evaluación de riesgos identificados para determinar la probabilidad de que ocurran y el impacto que tendrían en la organización.
5. **Priorización de riesgos:** es importante priorizar los riesgos identificados según su impacto potencial y la probabilidad de ocurrencia. Lo anterior ayudará a enfocar los recursos de la organización en las áreas más críticas.

Identificar activos

Es importante identificar todos los activos para poder evaluar los riesgos y diseñar controles de seguridad adecuados. A continuación, se relaciona el ejemplo para la identificación de activos:

Tabla 6
Identificación de activos

Fase	Objetivo	Actividades
Planificación	Identificar el alcance del análisis de activos	1. Definir los objetivos del análisis de activos 2. Establecer los límites del análisis de activos 3. Identificar las personas involucradas en el análisis de activos
Recopilación de datos	Identificar y recopilar información sobre los activos	1. Crear una lista de posibles activos 2. Identificar la ubicación de los activos 3. Identificar el valor de los activos 4. Identificar los propietarios de los activos
Análisis	Evaluar la importancia de los activos para la organización	1. Analizar los datos recopilados para evaluar la importancia de los activos 2. Identificar la criticidad de los activos para la organización 3. Evaluar la vulnerabilidad de los activos a las amenazas
Documentación	Documentar los resultados del análisis de activos	1. Crear un inventario de activos 2. Documentar los resultados del análisis de activos 3. Identificar las posibles medidas de protección para los activos

Nota. Fuente Elaboración Propia

Identificar amenazas

Es importante tener en cuenta que no todas las amenazas son relevantes para una organización y es necesario enfocarse en aquellas que pueden tener un mayor impacto en los activos críticos.

A continuación, describimos la metodología general para la identificación de amenazas:

Identificación de activos críticos: similar a la identificación de activos, es importante tener una lista de los activos críticos de la organización para poder enfocarse en las amenazas que podrían afectarlos.

Identificación de vectores de ataque: es fundamental identificar los posibles vectores de ataque que podrían ser utilizados para acceder a los activos críticos.

Identificación de amenazas: una vez identificados los vectores de ataque, se deben identificar las amenazas específicas que podrían aprovecharlos.

Evaluación de riesgos: una vez identificadas las amenazas, es importante evaluar la probabilidad de que se materialicen y el impacto potencial que podrían tener los activos críticos. Dicha evaluación puede basarse en la historia previa de ataques similares, la existencia de medidas de seguridad adecuadas.

Priorización de amenazas: finalmente, se deben priorizar las amenazas identificadas de acuerdo con su probabilidad e impacto potencial, lo que permitirá enfocarse en las más críticas y asignar recursos adecuados para su mitigación.

Identificar vulnerabilidades

Es válido aclarar que una vulnerabilidad es una debilidad en un sistema o aplicación que puede ser explotada por un atacante para comprometer la confidencialidad, integridad o disponibilidad de la información.

A continuación, se relaciona un ejemplo para identificar vulnerabilidades en un sistema o aplicación:

Tabla 7
Identificación de vulnerabilidades

Fase	Actividad	Herramientas	Resultados
1	Identificación de activos	• Inventarios de hardware y software • Escaneo de red • Entrevistas con el equipo de TI	Lista de activos identificados
2	Evaluación de vulnerabilidades	• Escaneo de vulnerabilidades • Pruebas de penetración • Revisión de configuraciones • Análisis de código fuente	Lista de vulnerabilidades identificadas
3	Priorización de vulnerabilidades	• Análisis de impacto • Análisis de probabilidad • Evaluación de amenazas • Análisis de riesgos	Lista de vulnerabilidades priorizadas
4	Mitigación de vulnerabilidades	• Aplicación de parches o actualizaciones • Configuraciones seguras • Medidas de seguridad adicionales • Solución de problemas de software • Actualización de hardware	Lista de vulnerabilidades mitigadas

Fuente. Elaboración Propia

Evaluar Riesgos

Una de las fases más importantes en el proceso de identificación de riesgos es la evaluación de riesgos, lo cual permite identificar los posibles riesgos y amenazas que pueden afectar la integridad, confidencialidad y disponibilidad de los datos y sistemas de una organización. Es importante resaltar que, con una evaluación adecuada de riesgos, se pueden establecer medidas de seguridad efectivas y estrategias de mitigación para minimizar los riesgos y prevenir ataques. En dicha evaluación se toman en cuenta factores como, por ejemplo:

- La probabilidad de ocurrencia
- El impacto potencial
- La criticidad de los activos y las medidas de seguridad existentes

A continuación, se relaciona un ejemplo de cómo se puede realizar la evaluación de riesgos:

Tabla 8
Evaluación de riesgos

Fase	Actividad	Descripción
1	Identificación de activos	Identificación y documentación de los activos de información que posee la organización, incluyendo datos, sistemas, redes, aplicaciones, hardware y software.
2	Identificación de amenazas	Identificación y documentación de las posibles amenazas que podrían afectar los activos de información de la organización, incluyendo ataques cibernéticos, desastres naturales, errores humanos.
3	Identificación de vulnerabilidades	Identificación y documentación de las vulnerabilidades que podrían ser explotadas por las amenazas identificadas.
4	Evaluación de riesgos	Evaluación de la probabilidad de ocurrencia y el impacto potencial de las amenazas identificadas, teniendo en cuenta las vulnerabilidades existentes y las medidas de seguridad implementadas.
5	Priorización de riesgos	Priorización de los riesgos identificados según su nivel de criticidad y su impacto potencial en la organización.
6	Plan de mitigación	Desarrollo de un plan de mitigación de riesgos que incluya medidas de seguridad para reducir la probabilidad de ocurrencia de los riesgos identificados y minimizar su impacto en caso de que ocurran.
7	Implementación y seguimiento	Implementación del plan de mitigación de riesgos y seguimiento continuo para asegurarse de que las medidas de seguridad están funcionando de manera efectiva y para realizar ajustes según sea necesario.

Fuente. Elaboración Propia

Priorizar Riesgos

Una vez que se han identificado y evaluados los riesgos, es necesario determinar qué riesgos son los más críticos y cuáles deben abordarse primero.

La priorización de riesgos se basa en la probabilidad de que ocurra una amenaza y el impacto que tendría si se materializa.

Existen muchas metodologías para la priorización de riesgos, pero la mayoría se basan en una matriz de riesgos que clasifica los riesgos según su probabilidad e impacto. Una matriz de riesgos típica tiene cuatro cuadrantes:

1. Alto riesgo/alta prioridad
2. Alto riesgo/baja prioridad
3. Bajo riesgo/alta prioridad
4. Bajo riesgo/baja prioridad

Los riesgos que se encuentran en el cuadrante de alto riesgo/alta prioridad son los que se deben abordar primero.

Además de la probabilidad e impacto, otros factores que pueden influir en la priorización de riesgos son:

- La criticidad del activo
- La madurez de los controles de seguridad existentes
- La capacidad de la organización para responder a los riesgos
- La tolerancia al riesgo de la organización
- Capacidad para asumir ciertos riesgos

Identificar procesos y sistemas críticos

Es importante realizar una evaluación exhaustiva de los procesos y sistemas que manejan información sensible o crítica para la organización.

A continuación, se relaciona un ejemplo de una buena práctica para la identificación de procesos y sistemas críticos:

Realizar un inventario de activos: Es necesario conocer todos los activos de la organización, tanto hardware como software, para poder identificar los procesos y sistemas críticos que requieren una protección especial.

Identificar los sistemas críticos: Una vez que se ha realizado el inventario de activos, se deben identificar los sistemas críticos que son esenciales para el funcionamiento de la organización. Estos sistemas pueden ser identificados mediante la realización de análisis de impacto en el negocio y en la continuidad del servicio.

Analizar la interdependencia de los sistemas: Los sistemas críticos a menudo están interconectados y dependen unos de otros para su funcionamiento. Es importante comprender la interdependencia de los sistemas críticos y cómo se ven afectados unos a otros en caso de un ataque.

Realizar evaluaciones de riesgos: Con el fin de identificar los procesos y sistemas críticos, se deben realizar evaluaciones de riesgos continuamente, para identificar las amenazas que podrían afectar los sistemas críticos, las vulnerabilidades que pueden ser explotadas por los atacantes y el impacto que tendrían en la organización.

Definir los niveles de protección: Una vez que se han identificado los sistemas críticos y se han evaluado los riesgos, es importante definir los niveles de protección necesarios para cada uno.

A continuación, relacionamos algunas de las metodologías que se pueden utilizar para identificar los procesos y sistemas críticos en una organización:

- **Análisis de impacto en el negocio (BIA):** esta metodología se enfoca en identificar los procesos y sistemas críticos que son necesarios para mantener las operaciones de la organización y cumplir con sus objetivos.

El **BIA** considera las interdependencias entre los procesos y sistemas críticos y evalúa el impacto que tendría su interrupción en la organización.

- **Análisis de riesgos:** esta metodología se enfoca en identificar los procesos y sistemas críticos que son más vulnerables a amenazas y riesgos de ciberseguridad.

El análisis de riesgos considera las amenazas y vulnerabilidades existentes en los procesos y sistemas y evalúa la probabilidad y el impacto de un incidente de ciberseguridad.

- **Análisis de vulnerabilidades:** esta metodología se enfoca en identificar los sistemas y aplicaciones que presentan las mayores vulnerabilidades de ciberseguridad.

El análisis de vulnerabilidades evalúa los sistemas y aplicaciones para identificar las vulnerabilidades conocidas y desconocidas, y evalúa la probabilidad y el impacto de una explotación exitosa.

- **Identificación de activos críticos:** esta metodología se enfoca en identificar los activos críticos de la organización, que pueden ser procesos, sistemas, aplicaciones, datos, infraestructura, etc. Una vez identificados los activos críticos, se puede evaluar su importancia en relación con los objetivos de la organización y su impacto en caso de interrupción.

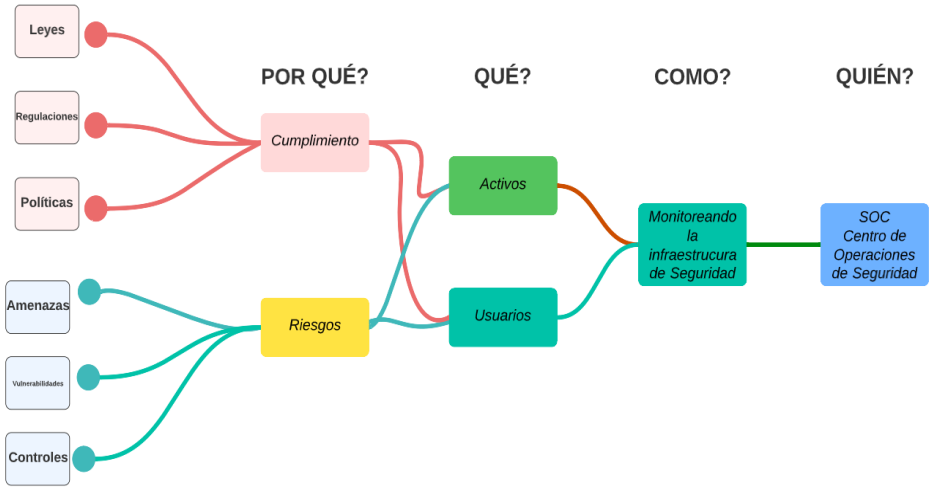
Cada una de estas metodologías puede ser adaptada y combinada según las necesidades y objetivos específicos de la organización. Lo importante es tener un enfoque sistemático y estructurado para identificar los procesos y sistemas críticos en la organización.

Definir necesidades de detección.

Al definir las necesidades de detección no solo se puede tener en cuenta las amenazas, varios factores se deben considerar del entorno organizacional.

Usando el modelo de Lasswell para realizar el monitoreo de seguridad del entorno se debe considerar:

Figura 21
Entorno de monitoreo de seguridad



Nota. Elaboración propia según (*MaGMa,* 2023)

Al identificar los grupos de actores maliciosos, las tácticas, técnicas y procedimientos usados por estos grupos, los riesgos asociados a estas amenazas, las vulnerabilidades y los controles con lo que cuenta actualmente la organización, además de tener claridad de qué leyes, regulaciones o políticas de se deben cumplir, las organizaciones tendrán claridad en las necesidades de detección en las cuales se debe centrar la atención.

Por ejemplo:

Si al realizar el análisis se identifica:

1. Que se debe cumplir con la ley de protección de datos personales en Colombia, Ley 1581 de 2012.
2. Que no existen políticas estrictas al interior de la organización en el uso de correo electrónico
3. Que el sector al que pertenece la organización está siendo atacado con técnicas de phishing
4. Que la organización cuenta con una solución de protección de correo electrónico, pero no tiene activo todas sus funcionalidades.

Se puede establecer una necesidad puntual de mejorar la detección de correos maliciosos y mejorar los controles de seguridad para el correo electrónico.

Al definir las necesidades de detección las organizaciones podrán centrar su atención en la definición de casos de uso que permitan tener visibilidad y cerrar de algún modo los puntos ciegos si es que existen, o disminuir el riesgo de que una amenaza sea explotada.

Pueden determinar por ejemplo las siguientes necesidades:

- Detectar cuando las credenciales de un usuario son comprometidas
- Detectar escalamiento anómalo de privilegios
- Detectar Comunicaciones de comando y control
- Detectar infracción de manejo de información personal
- Detectar cifrado rápido

- Detectar movimiento lateral

Definir Casos de uso

Según IBM "Un caso de uso es un artefacto que define una secuencia de acciones que da lugar a un resultado de valor observable. Los casos de uso proporcionan una estructura para expresar requisitos funcionales en el contexto de procesos empresariales y de sistema. Los casos de uso pueden representarse como un elemento gráfico en un diagrama y como una especificación de caso de uso en un documento textual.

Un caso de uso empresarial define una secuencia de acciones que una empresa lleva a cabo y que da lugar a un resultado de valor observable (una salida de trabajo) para un actor empresarial particular o que muestra el modo en que la empresa responde a un evento empresarial (Engineering Lifecycle Management, 2023).

Entonces, un Caso de Uso se refiere a un escenario o situación específica que puede ocurrir en un entorno de seguridad de la información. Este escenario describe una actividad o evento que puede ser detectado y analizado por una solución de SIEM, con el objetivo de mejorar la seguridad y la visibilidad en la infraestructura de una organización.

Al definir las necesidades de detección se podrá identificar que casos de uso son necesarios desarrollar, algunos ejemplos de casos de uso SIEM incluyen la detección de intentos de intrusión en la red, la monitorización de usuarios sospechosos o de actividades maliciosas, la identificación de anomalías en el tráfico de red o en los registros de eventos, la gestión de incidentes de seguridad, el cumplimiento de normativas y regulaciones, de seguridad IoT, Amenazas Internas, Phishing, entre otros. La clasificación de estos dependerá de las necesidades de cada organización. A continuación, presentaremos algunos ejemplos de casos de uso comunes:

Caso de uso para el cumplimiento de PCI

PCI es el estándar de seguridad de datos de la industria de tarjetas de pago PCI DSS y fue creado para proteger los datos del titular de la tarjeta de crédito contra el rogo y e uso indebido. Todo Banco en el mundo debe cumplir el estándar PCI.

Caso de uso para el cumplimiento de GDPR

Ley de protección de datos reconoce y protege el derecho que tienen todas las personas a conocer, actualizar, y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

La GDPR aplica a cualquier entidad legal que almacene, controle o procese datos personales de ciudadanos.

Caso de uso para el abuso de acceso de privilegios

Los usuarios con accesos privilegiados a los sistemas de TI pueden realizar acciones no deseadas debido a que tienen más derechos de acceso de los que necesitan para realizar su trabajo.

Al definir un caso de uso, este debe contar con al menos lo siguiente:

Tabla 9
Especificación caso de uso

Nombre del caso de uso	Indica el nombre del caso de uso. Normalmente, el nombre expresa el resultado objetivo y observable del caso de uso, como por ejemplo "Retirar efectivo" en el caso de un cajero automático.
Breve descripción	Describe el rol y el objetivo del caso de uso.
Flujo de eventos	Presenta el flujo básico y flujos alternativos. El flujo de eventos describe el comportamiento del sistema; no describe cómo el sistema funciona, los detalles de la presentación ni los detalles de la interfaz de usuario. Si se intercambia información, el caso de uso debe ser específico sobre lo que ha transmitido. Por ejemplo, en lugar de describir una acción como "el actor especifica información de cliente", indica que "el actor especifica el nombre y la dirección del cliente".

Flujo básico	Describe el comportamiento ideal y principal del sistema.
Requisitos especiales	Requisitos no funcionales que son específicos de un caso de uso pero que no se especifican en el texto del flujo de sucesos del caso de uso. Ejemplos de requisitos especiales incluyen los factores siguientes: requisitos legales y reguladores; estándares de aplicación; atributos de calidad del sistema, incluidos la usabilidad, la fiabilidad, el rendimiento y la capacidad de soporte; sistemas operativos y entornos; requisitos de compatibilidad y limitaciones de diseño.
Condiciones previas	Estado del sistema que debe estar presente antes del inicio del caso de uso.
Puntos de ampliación	Punto del flujo de eventos de caso de uso en el que se hace referencia a otro caso de uso.

Fuente. (Engineering Lifecycle Management, 2023)

Crear reglas de correlación

Para crear la regla de correlación debe basarse en la información recolectada anteriormente y tener claridad de a qué caso de uso o que casos de uso aplicaría esta regla de correlación.

Identificar el objetivo: Determine qué eventos o actividades desea correlacionar y por qué. Por ejemplo, puede querer correlacionar eventos de inicio de sesión fallidos con eventos de intentos de inicio de sesión exitosos desde la misma dirección IP.

Identificar los eventos: Determine los eventos que desea correlacionar. Puede hacerlo buscando eventos en el registro de eventos o en los flujos de datos.

Definir los criterios de correlación: Defina los criterios que se utilizarán para correlacionar los eventos. Esto puede incluir información como la dirección IP, la fecha y la hora del evento, el usuario o el tipo de evento.

Establecer los umbrales: Establezca los umbrales para los eventos correlacionados. Esto significa determinar cuántos eventos correlacionados se necesitan antes de que se active la regla de correlación.

Configurar las acciones de respuesta: Configure las acciones que se tomarán cuando se active la regla de correlación. Esto puede incluir la generación de alertas, la ejecución de scripts o la creación de tareas.

Definir criticidad: Defina el nivel de criticidad de las alertas asociadas a la regla de correlación, esto permitirá a los analistas tener prioridades de atención.

Documentar la regla: Importante que, al crear la regla de correlación, se documente la información del motivo de creación de la regla, fecha de creación, casos de uso asociado y muy relevante definir una estructura de nombre regla de correlación. Aconsejamos nombrar las reglas de correlación que permitan identificar y agrupar las reglas de forma ordenada.

Ejemplo: EX:EC:Malware:Cortex: Explotacion de Código remoto Drupal

EX: técnica Explotación

EC: Técnica Explotación para la ejecución del cliente

Malware: Caso de Uso

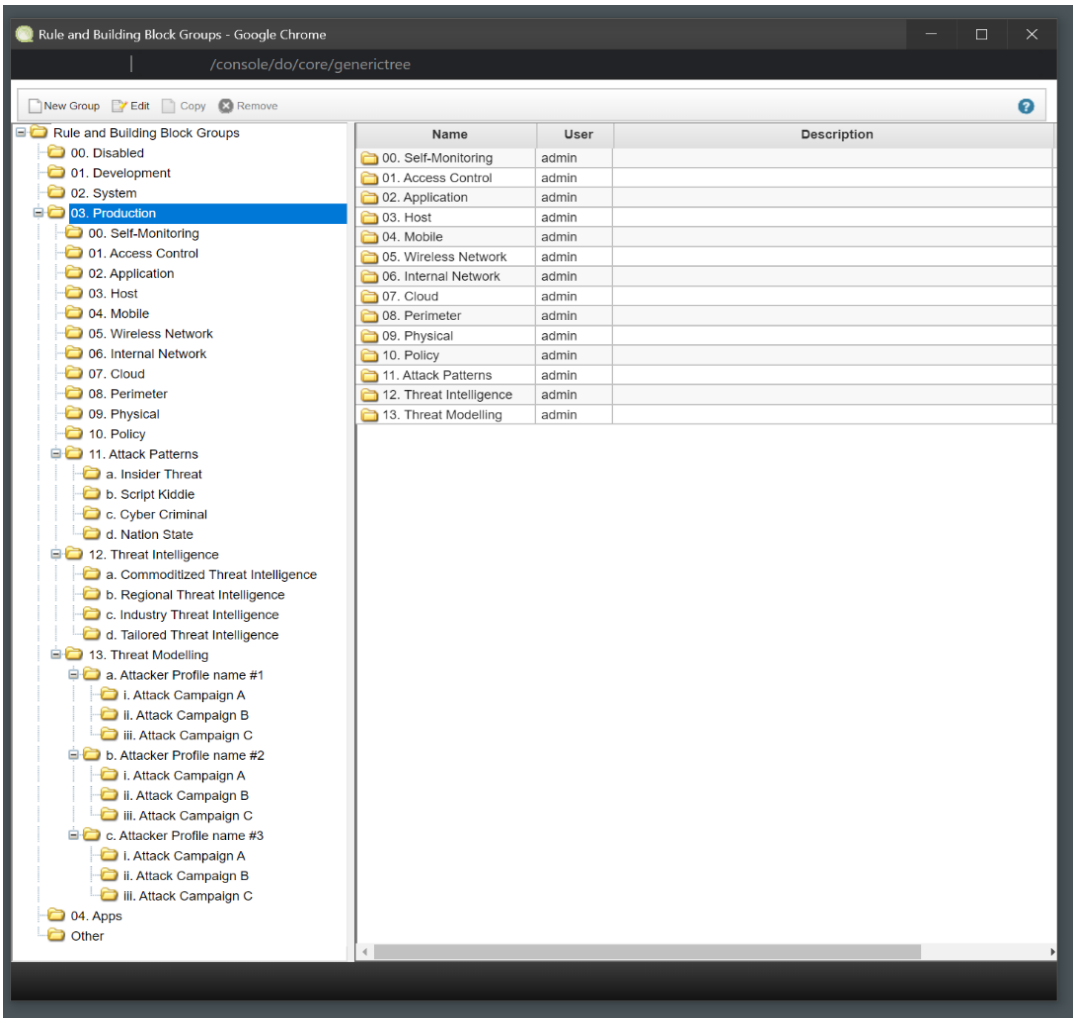
Cortex: Fuente de datos o eventos

Explotación de código remoto drupal: Nombre que describe brevemente lo alertado.

Se pueden nombrar de tal forma que permita identificar la táctica y técnica MITRE ATT&CK como en el ejemplo anterior y agruparlas de acuerdo la necesidad de cada organización. A continuación, mostramos un ejemplo de los directorios de reglas creados en (Acanerler, 2022).

Figura 22

Ejemplo de estructura de directorios



Nota. Fuente (Jurgen, 2020)

Documentar caso de uso

La documentación de un caso de uso SIEM es importante para tener una referencia clara y detallada de los pasos que se siguen en el proceso de detección, análisis y respuesta a eventos de

seguridad en la red de una organización. A continuación, se presentan algunas pautas generales que pueden ayudar a documentar un caso de uso SIEM:

- Título del caso de uso: Proporcione un título claro y conciso para el caso de uso. El título debe describir el objetivo general del caso de uso.
- Objetivo: Escriba una descripción detallada del objetivo del caso de uso. El objetivo debe explicar el problema de seguridad que se está abordando y cómo el caso de uso aborda ese problema.
- Fuentes de datos: Enumere las fuentes de datos que se utilizarán para el caso de uso. Esto puede incluir registros de eventos, tráfico de red, bases de datos, entre otros.
- Reglas: Defina las reglas que se utilizarán para detectar el comportamiento sospechoso o malicioso en las fuentes de datos seleccionadas. Esto puede incluir patrones de comportamiento, firmas de ataques conocidas y otros criterios específicos.
- Alertas: Determine las alertas que se generarán cuando se detecte actividad sospechosa o maliciosa en los datos. Especifique los detalles de la alerta, como el destinatario, el nivel de gravedad y la información que se incluirá en la alerta.
- Definición de reglas: Especifique las reglas que se han definido para la detección de eventos de seguridad. Esto incluye reglas de correlación, reglas de detección de anomalías y reglas de detección de ataques conocidos.

- Configuración de alertas: Especifique las alertas que se generarán cuando se detecten eventos de seguridad. Incluya información como la gravedad de la alerta, el destinatario de la alerta y el formato de la alerta.
- Procedimientos de análisis: Documente los procedimientos que se seguirán para analizar los eventos de seguridad detectados. Esto puede incluir la definición de perfiles de usuarios, la correlación de eventos y la investigación de eventos sospechosos.
- Acciones de respuesta: Escriba las acciones que se tomarán en respuesta a las alertas generadas por el caso de uso. Esto puede incluir el bloqueo de una dirección IP, la eliminación de un archivo malicioso o la desconexión de una cuenta de usuario.
- Validación: Especifique los pasos que se tomarán para validar la efectividad del caso de uso. Esto puede incluir pruebas en entornos de prueba, monitoreo continuo y ajustes del caso de uso en función de los resultados de la validación.
- Actualizaciones: Establezca un proceso para actualizar y mantener el caso de uso a medida que evoluciona la amenaza cibernética y cambian las necesidades de seguridad de la organización

Al documentar un caso de uso SIEM, es importante que la documentación sea clara y concisa. También se debe asegurar que la documentación se mantenga actualizada y esté disponible para todos los miembros del equipo de seguridad y TI de la organización.

Mantener caso de uso

Mantener actualizado el caso de uso es de gran importancia para garantizar que es efectivo y relevante. Sugerimos unos pasos a seguir para realizar la actualización de casos de uso SIEM:

Realizar monitoreo constante: Es importante monitorear constantemente el entorno de la organización para detectar cualquier cambio en las amenazas de seguridad o en los patrones de actividad de los usuarios. Esto puede incluir la revisión de registros de eventos, el monitoreo de alertas y la realización de análisis de vulnerabilidades.

Realizar revisión periódica: Es importante revisar regularmente los casos de uso SIEM existentes para asegurarse de que sigan siendo relevantes y efectivos. Esto puede incluir la revisión de los criterios de detección, la evaluación de la eficacia de las reglas de correlación y la identificación de nuevos casos de uso.

Actualizar las reglas de correlación: Las reglas de correlación son una parte importante de un caso de uso SIEM, por lo que es importante revisarlas y actualizarlas periódicamente para garantizar que estén alineadas con las últimas amenazas y patrones de ataque. Validar cantidad de veces que se han gatillado en determinado tiempo puede indicar si es relevante o si existio algún cambio en la plataforma fuente de los eventos de la regla de correlación.

Evaluar nuevos dispositivos: Cuando se agregan nuevos dispositivos o sistemas a la infraestructura de la organización, es importante evaluar cómo se integrarán con el sistema SIEM y actualizar los casos de uso y reglas de correlación en consecuencia. El agregar dispositivos de seguridad e integrarlos al SIEM aumenta la inteligencia en la detección, permitiendo ser más exactos al momento de generar una alerta para un caso de uso particular.

Capacitar y educar: Es importante proporcionar capacitación y educación a los miembros del equipo de seguridad para asegurarse de que estén alineados con los últimos patrones de amenazas y de actividad de los usuarios. Esto puede incluir la realización de sesiones de capacitación sobre la identificación de amenazas y la respuesta a incidentes.

Actualizar la solución SIEM: Es importante mantener actualizado el software del sistema SIEM y sus componentes para garantizar que estén protegidos contra las últimas amenazas de seguridad y vulnerabilidades. Las actualizaciones del sistema también pueden incluir nuevas funciones y características que puedan mejorar la capacidad de detección y respuesta del sistema SIEM.

En resumen, mantener actualizado un caso de uso SIEM es un proceso continuo que requiere monitoreo constante, revisión periódica, actualización de reglas de correlación, evaluación de nuevos dispositivos, capacitación y educación, y actualizaciones del sistema SIEM. Al seguir estos pasos, un equipo de seguridad puede garantizar que su sistema SIEM siga siendo efectivo y relevante para proteger su organización contra las últimas amenazas de seguridad. Pero, para garantizar esto es muy importante poder contar con una herramienta que permita tener visibilidad general de los casos de uso implementados e integre toda la información relevante.

Algunos fabricantes como IBM en su plataforma de correlación de eventos SIEM QRADAR ofrece QRadar Use Case Manager que incluye un explorador de casos de uso que ofrece informes flexibles relacionados con sus reglas.QRadar Use Case Manager también expone asignaciones predefinidas a las reglas del sistema y lo ayuda a asignar sus propias reglas personalizadas a las tácticas y técnicas de MITRE ATT&CK.

A continuación, presentamos la forma de usar una herramienta que permite tener visibilidad general de las reglas de correlación, casos de uso y además visualizar la cobertura de amenazas según Marco MITRE ATT&CK.

Usar herramienta de control y visibilidad de Casos de Uso

A continuación, se presenta la forma de usar una herramienta en Excel basada en la desarrollada por la comunidad financiera holandesa MaGMa para la gestión y administración de casos de uso SIEM.

La herramienta fue modificada y actualizada, ajustada de acuerdo con el macro MITRE ATT&CK.

El uso de la herramienta permitirá a las organizaciones tener la capacidad de control y monitoreo de seguridad basada en las necesidades de detección de amenazas emergentes y las necesidades de cumplimiento.

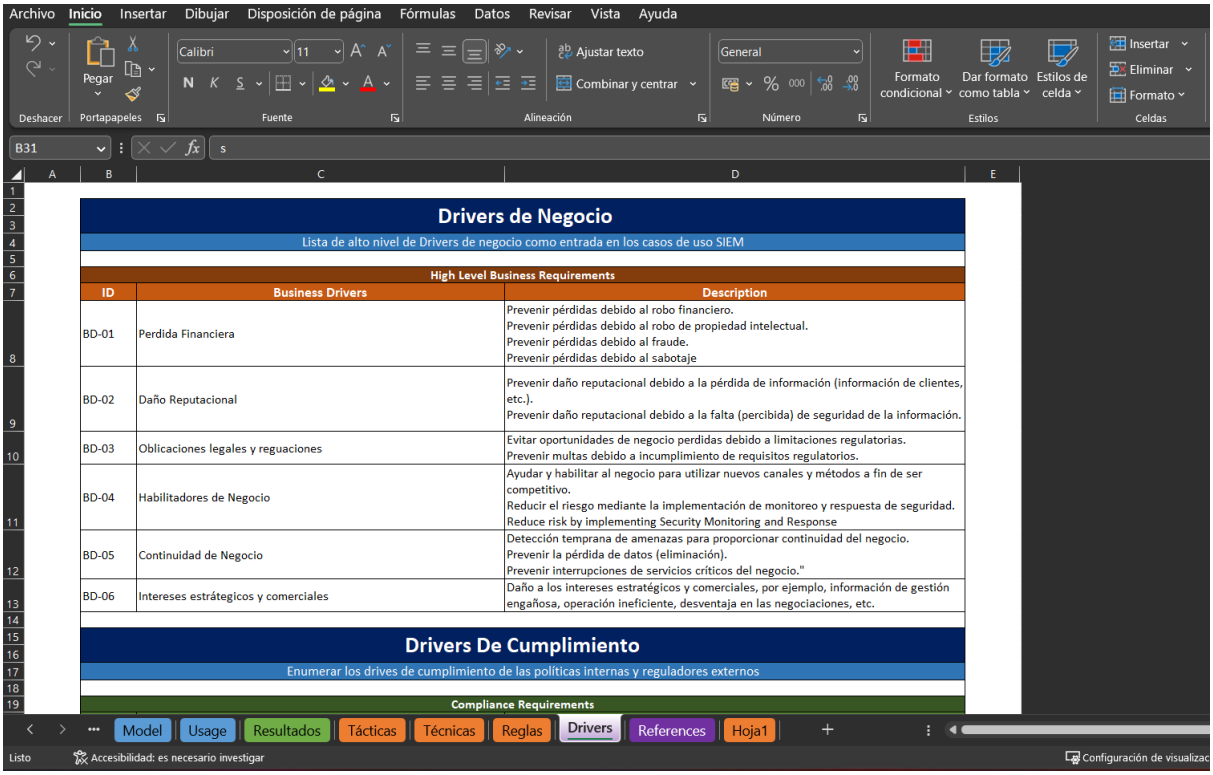
El archivo original puede ser descargado y utilizado de forma libre y está disponible en línea en el siguiente link:

https://www.betaalvereniging.nl/wp-content/uploads/Magma-UCF-Tool.xlsx

Para usar la herramienta se debe seguir los siguientes pasos:

Diligencie la información en la pestaña DRIVERS

Figura 23
Pestaña Tácticas MITRE ATT&CK



Drivers de Negocio

Lista de alto nivel de Drivers de negocio como entrada en los casos de uso SIEM

High Level Business Requirements		
ID	**Business Drivers**	**Description**
BD-01	Perdida Financiera	Prevenir pérdidas debido al robo financiero. Prevenir pérdidas debido al robo de propiedad intelectual. Prevenir pérdidas debido al fraude. Prevenir pérdidas debido al sabotaje
BD-02	Daño Reputacional	Prevenir daño reputacional debido a la pérdida de información (información de clientes, etc.). Prevenir daño reputacional debido a la falta (percibida) de seguridad de la información.
BD-03	Oblicaciones legales y reguaciones	Evitar oportunidades de negocio perdidas debido a limitaciones regulatorias. Prevenir multas debido a incumplimiento de requisitos regulatorios.
BD-04	Habilitadores de Negocio	Ayudar y habilitar al negocio para utilizar nuevos canales y métodos a fin de ser competitivo. Reducir el riesgo mediante la implementación de monitoreo y respuesta de seguridad. Reduce risk by implementing Security Monitoring and Response
BD-05	Continuidad de Negocio	Detección temprana de amenazas para proporcionar continuidad del negocio. Prevenir la pérdida de datos (eliminación). Prevenir interrupciones de servicios críticos del negocio."
BD-06	Intereses estrátegicos y comerciales	Daño a los intereses estratégicos y comerciales, por ejemplo, información de gestión engañosa, operación ineficiente, desventaja en las negociaciones, etc.

Drivers De Cumplimiento

Enumerar los drives de cumplimiento de las políticas internas y reguladores externos

Compliance Requirements

Nota. Fuente Elaboración Propia

En esta tabla se debe listar todos los drivers de negocio y los drivers de cumplimiento de la compañía. Estos son los factores que impulsan la necesidad de proteger la información de la organización. Son la base en la definición de los casos de uso.

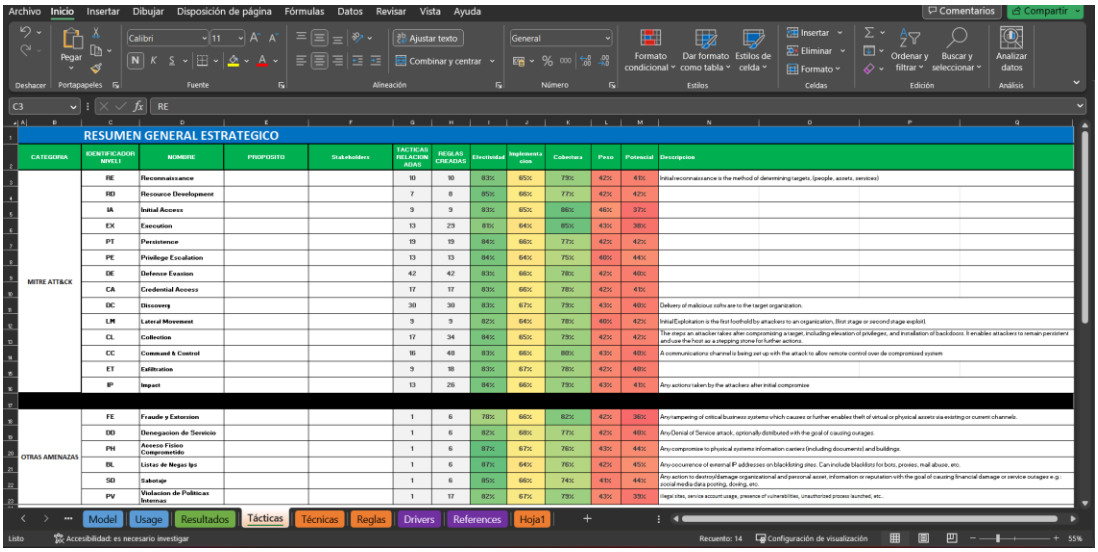
Esta información hace parte de la recolectada en la metodología propuesta en los puntos iniciales.

En la Pestaña Tácticas recomendamos incluir todas las tácticas de la Matriz de MITRE ATT&CK y otras amenazas propias del segmento de la organización.

Asigne un identificador de dos letras único, que permita identificar la táctica.

Figura 24

Pestaña Tácticas



Nota. Fuente Elaboración Propia

Tabla 10

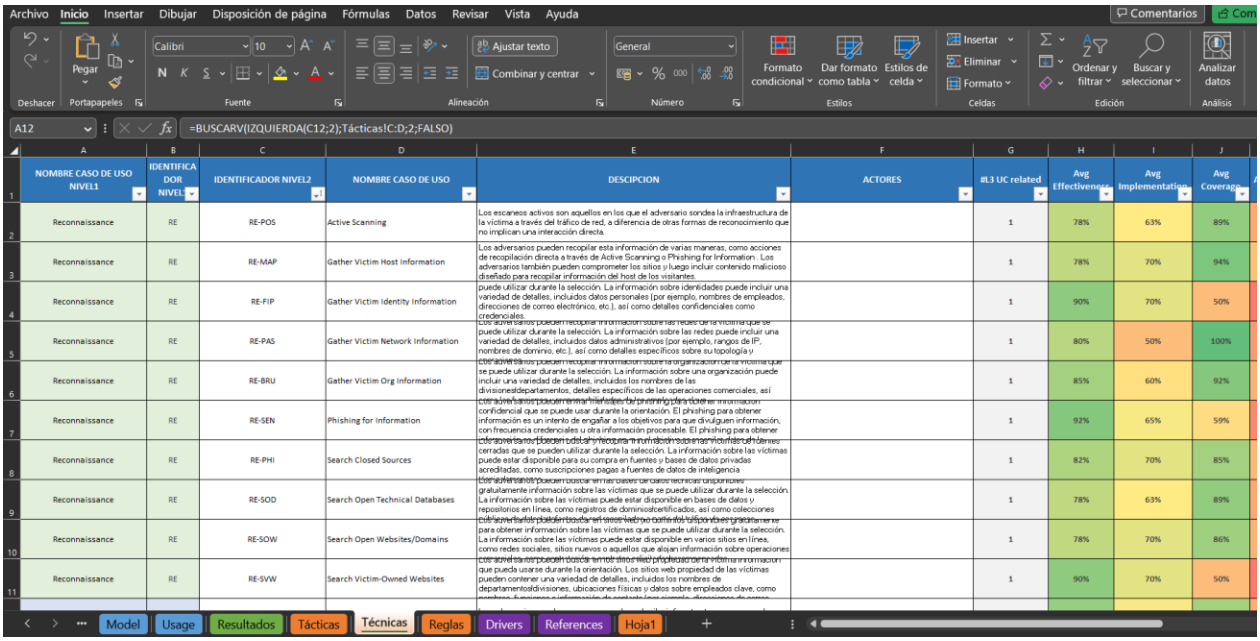
Identificadores Tácticas

Identificador	Táctica
RE	Reconnaisssance
RD	Resource Development
IA	Initial Access
EX	Execution
PT	Persistence
PE	Privilege Escalation
DE	Deense Evation
CA	Credential Access
DC	Discovery
LM	Lateral Movement
CL	Collection
CC	Command & Control
ET	Exfiltration
IP	Impact

Fuente. Elaboración Propia

En la pestaña Técnicas, recomendamos listas cada una de las técnicas usadas por cada una de las tácticas de MITRE ATT&CK y las técnicas usadas de las otras amenazas.

Figura 25
Pestaña Técnicas



Nota. Fuente Elaboración Propia

Al igual que el identificador de la táctica, en la pestaña Nivel 2 Caso de Uso, debe crear un identificador de la técnica asociada a la táctica. Para este caso debe usar las dos primeras letras de la táctica y luego tres letras que identifiquen la técnica separada por un guion como se muestra en la siguiente tabla.

Tabla 11
Identificador técnicas

Táctica	Identificador Táctica	Identificador Técnica	Nombre de la técnica
Resource Development	RD	RD-CAC	Compromise Accounts

Resource Development	RD	RD-CIT	Compromise Infrastructure
Resource Development	RD	RD-DCB	Develop Capabilities

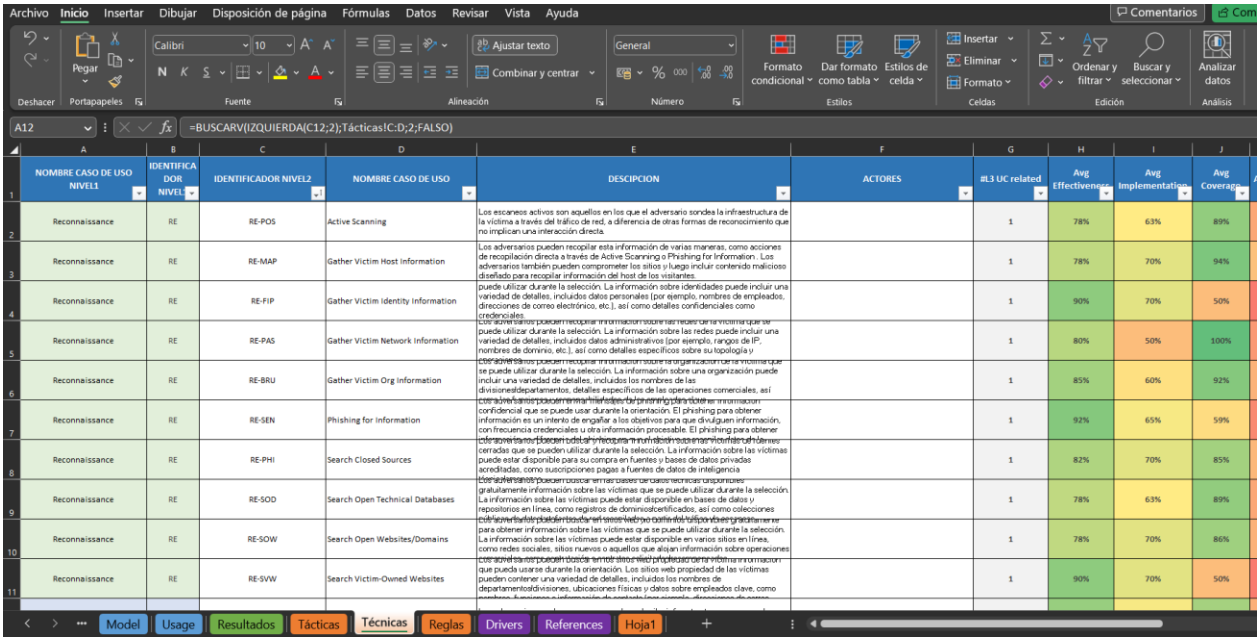
Fuente. Elaboración Propia

De esta manera se relacionarán las técnicas a sus tácticas.

En la pestaña Reglas, ingrese todos los nombres de las reglas de correlación que tienen implementadas en la actualidad.

Importante que las reglas cuenten con una estandarización para que la herramienta pueda contabilizar y generar graficas de uso por cada tácticas y técnica.

Figura 26
Pestaña Reglas



Nota. Fuente Elaboración Propia

Ejemplo de estandarización nombre de reglas

Tabla 12
Identificadores Reglas de correlación

IDENTIFICADOR REGLA	NOMBRE DE LA REGLA
PE-AEC-258	Detect Modifications of Startup Items
PE-ATM-259	Detect Abuse of Setuid and Setgid Files
PE-BLA-260	Detect Securityd Memory Access Attempt
PE-BLS-261	Detect Presence of Unauthorized Cron Job

Fuente. Elaboración Propia

Identificador de la regla: PE-AEC-258

PE identifica la Táctica, la cual en este caso es Persistence

AEC identifica la Técnica, la cual en este caso es Abuse Elevation Control Mechanism

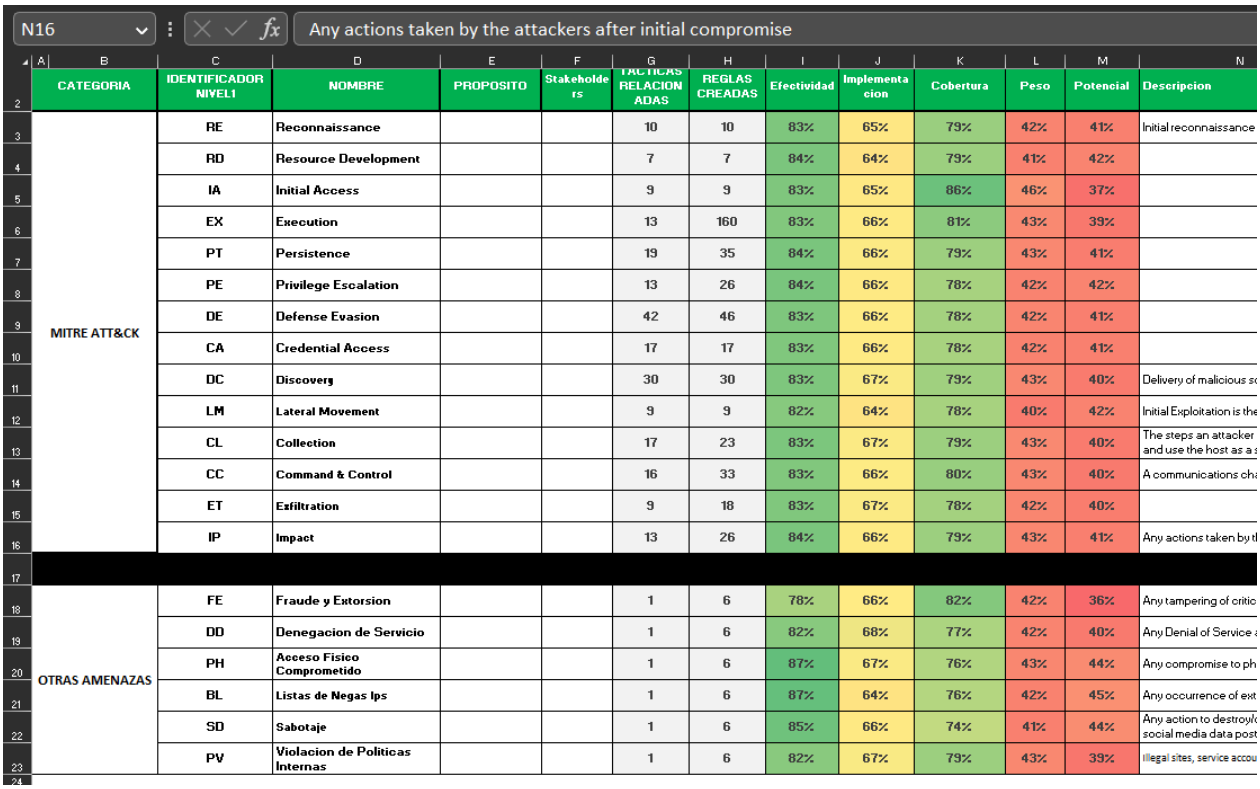
258 número de la regla de correlación

De esta manera todas las reglas contaran con un único identificador y podrá ser identificada la táctica y técnica a la cual pertenece cada una de las reglas, dando una visión general del cubrimiento de protección con el que cuenta la organización basada en MITRE ATT&CK.

En la columna H de la pestaña Tácticas, podrán ver la cantidad de reglas asociadas a cada táctica.

Figura 27

Contador de reglas por táctica



N16 | Any actions taken by the attackers after initial compromise

CATEGORIA	IDENTIFICADOR NIVEL1	NOMBRE	PROPOSITO	Stakeholders	TACTICAS RELACIONADAS	REGLAS CREADAS	Efectividad	Implementacion	Cobertura	Peso	Potencial	Descripcion
MITRE ATT&CK	RE	Reconnaissance			10	10	83%	65%	79%	42%	41%	Initial reconnaissance
	RD	Resource Development			7	7	84%	64%	79%	41%	42%	
	IA	Initial Access			9	9	83%	65%	86%	46%	37%	
	EX	Execution			13	160	83%	66%	81%	43%	39%	
	PT	Persistence			19	35	84%	66%	79%	43%	41%	
	PE	Privilege Escalation			13	26	84%	66%	78%	42%	42%	
	DE	Defense Evasion			42	46	83%	66%	78%	42%	41%	
	CA	Credential Access			17	17	83%	66%	78%	42%	41%	
	DC	Discovery			30	30	83%	67%	79%	43%	40%	Delivery of malicious sc
	LM	Lateral Movement			9	9	82%	64%	78%	40%	42%	Initial Exploitation is the
	CL	Collection			17	23	83%	67%	79%	43%	40%	The steps an attacker and use the host as a s
	CC	Command & Control			16	33	83%	66%	80%	43%	40%	A communications cha
	ET	Exfiltration			9	18	83%	67%	78%	42%	40%	
	IP	Impact			13	26	84%	66%	79%	43%	41%	Any actions taken by t
OTRAS AMENAZAS	FE	Fraude y Extorsion			1	6	78%	66%	82%	42%	36%	Any tampering of critic
	DD	Denegacion de Servicio			1	6	82%	68%	77%	42%	40%	Any Denial of Service a
	PH	Acceso Fisico Comprometido			1	6	87%	67%	76%	43%	44%	Any compromise to ph
	BL	Listas de Negas Ips			1	6	87%	64%	76%	42%	45%	Any occurrence of ext
	SD	Sabotaje			1	6	85%	66%	74%	41%	44%	Any action to destroy/c social media data post
	PV	Violacion de Politicas Internas			1	6	82%	67%	79%	43%	39%	Illegal sites, service accou

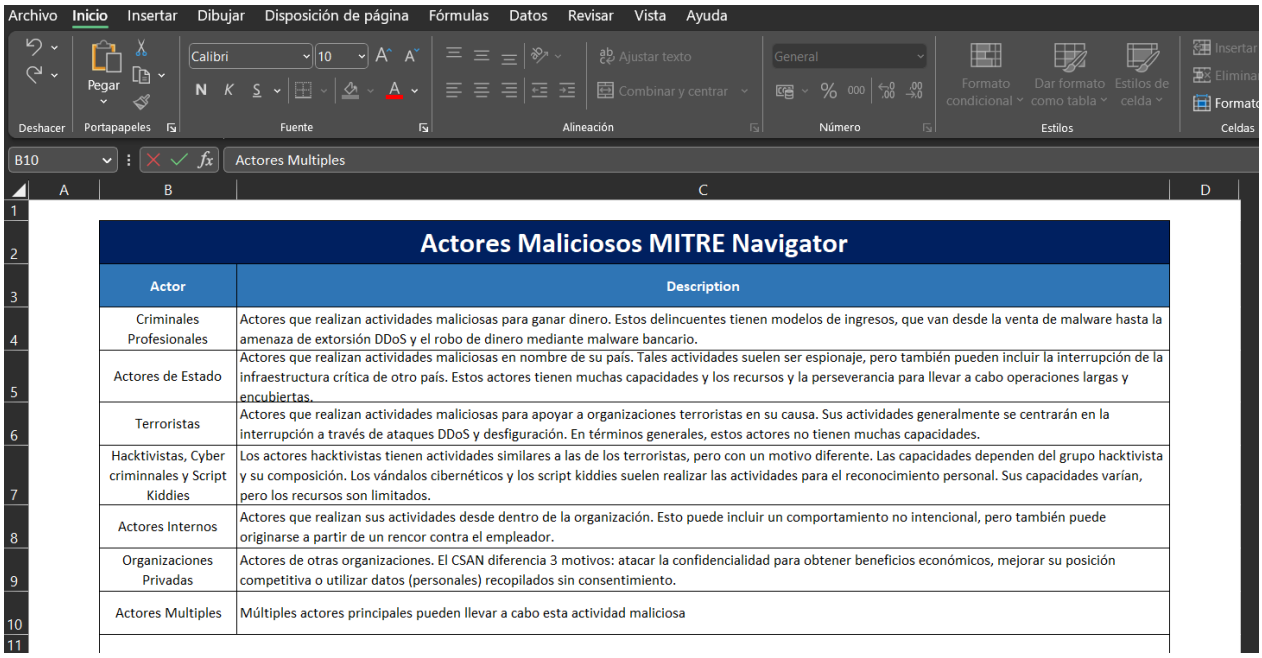
Nota. Fuente Elaboración Propia

En la pestaña “Referencias”, agreguen detalle sobre:

Los actores maliciosos identificados durante el proceso de investigación en las etapas iniciales de la guía propuesta. Esta tabla debe ser actualizada regularmente ya que pueden identificarse nuevos actores o por el contrario ser eliminados de la lista.

Figura 28

Actores Maliciosos

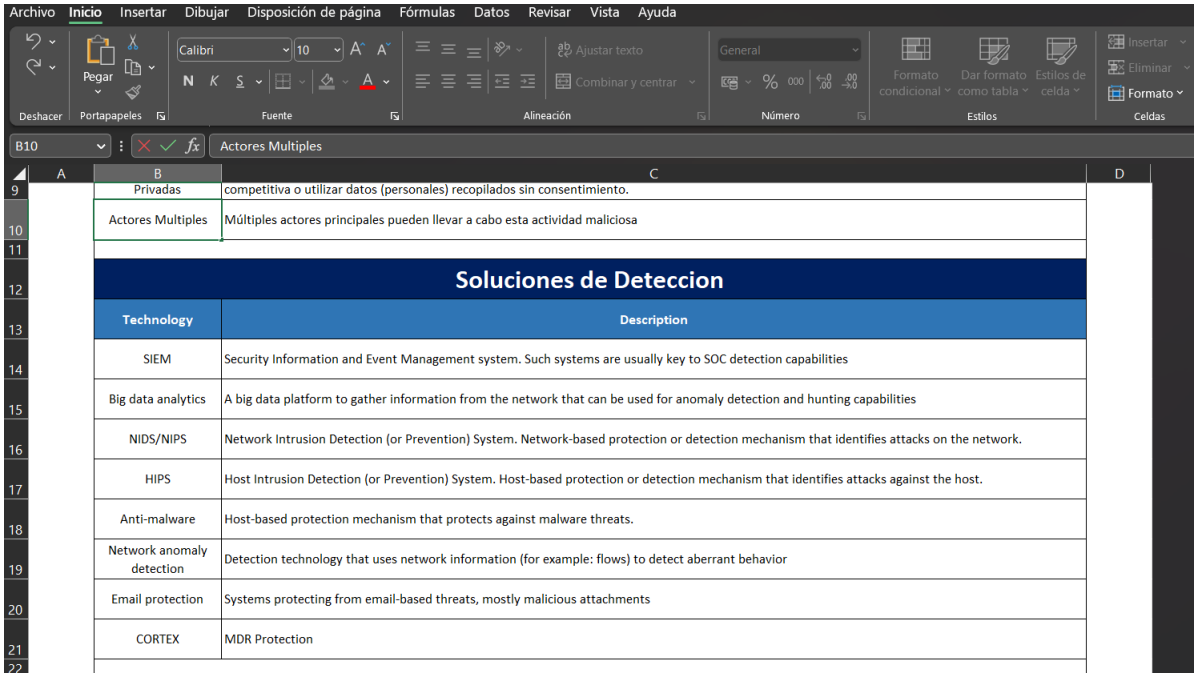


Actores Maliciosos MITRE Navigator	
Actor	**Description**
Criminales Profesionales	Actores que realizan actividades maliciosas para ganar dinero. Estos delincuentes tienen modelos de ingresos, que van desde la venta de malware hasta la amenaza de extorsión DDoS y el robo de dinero mediante malware bancario.
Actores de Estado	Actores que realizan actividades maliciosas en nombre de su país. Tales actividades suelen ser espionaje, pero también pueden incluir la interrupción de la infraestructura crítica de otro país. Estos actores tienen muchas capacidades y los recursos y la perseverancia para llevar a cabo operaciones largas y encubiertas.
Terroristas	Actores que realizan actividades maliciosas para apoyar a organizaciones terroristas en su causa. Sus actividades generalmente se centrarán en la interrupción a través de ataques DDoS y desfiguración. En términos generales, estos actores no tienen muchas capacidades.
Hacktivistas, Cyber criminnales y Script Kiddies	Los actores hacktivistas tienen actividades similares a las de los terroristas, pero con un motivo diferente. Las capacidades dependen del grupo hacktivista y su composición. Los vándalos cibernéticos y los script kiddies suelen realizar las actividades para el reconocimiento personal. Sus capacidades varían, pero los recursos son limitados.
Actores Internos	Actores que realizan sus actividades desde dentro de la organización. Esto puede incluir un comportamiento no intencional, pero también puede originarse a partir de un rencor contra el empleador.
Organizaciones Privadas	Actores de otras organizaciones. El CSAN diferencia 3 motivos: atacar la confidencialidad para obtener beneficios económicos, mejorar su posición competitiva o utilizar datos (personales) recopilados sin consentimiento.
Actores Multiples	Múltiples actores principales pueden llevar a cabo esta actividad maliciosa

Nota. Fuente Elaboración Propia

Figura 29

Soluciones de Detección de la Organización



Privadas	competitiva o utilizar datos (personales) recopilados sin consentimiento.
Actores Multiples	Múltiples actores principales pueden llevar a cabo esta actividad maliciosa

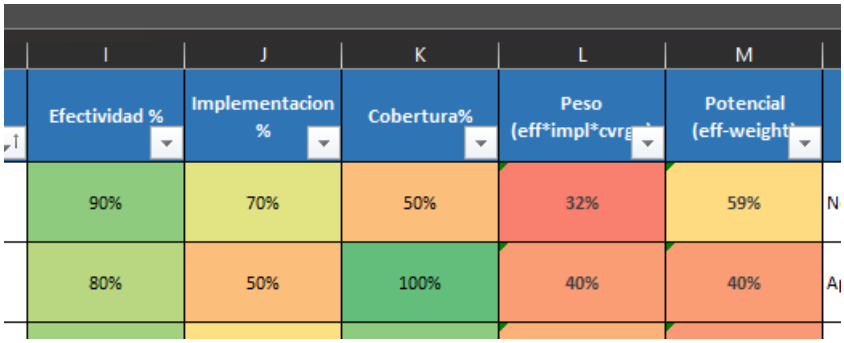
Soluciones de Deteccion	
Technology	**Description**
SIEM	Security Information and Event Management system. Such systems are usually key to SOC detection capabilities
Big data analytics	A big data platform to gather information from the network that can be used for anomaly detection and hunting capabilities
NIDS/NIPS	Network Intrusion Detection (or Prevention) System. Network-based protection or detection mechanism that identifies attacks on the network.
HIPS	Host Intrusion Detection (or Prevention) System. Host-based protection or detection mechanism that identifies attacks against the host.
Anti-malware	Host-based protection mechanism that protects against malware threats.
Network anomaly detection	Detection technology that uses network information (for example: flows) to detect aberrant behavior
Email protection	Systems protecting from email-based threats, mostly malicious attachments
CORTEX	MDR Protection

Nota. Fuente Elaboración Propia

En la pestaña “Reglas” encuentran las columnas con las métricas “Efectividad”, Implementación “Cobertura” , “Peso” y “Potencial”

Figura 30

Metricas de Efectividad, Implementación y Cobertura



I	J	K	L	M
Efectividad %	Implementacion %	Cobertura%	Peso (eff*impl*cvrg	Potencial (eff-weight
90%	70%	50%	32%	59%
80%	50%	100%	40%	40%

Nota. Fuente Elaboración Propia

A continuación se explica a que hace referencia cada una de las métricas:

Efectividad: Esta métrica se utiliza para determinar la efectividad del mecanismo de detección de la regla.

Implementación: Esta métrica se utiliza para determinar el nivel en el que se implementa el mecanismo de detección de la regla

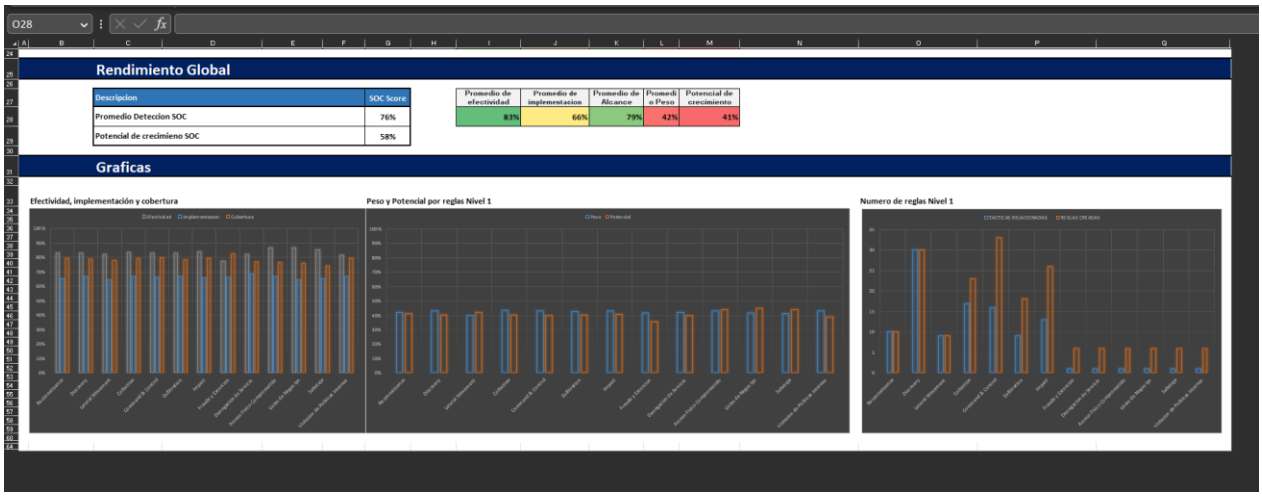
Cobertura: Esta métrica se utiliza para determinar el nivel en el que el mecanismo de detección la regla cubre el caso de uso

Peso: Esta métrica es un puntaje general calculado de efectividad, implementación y cobertura

Potencial: Esta métrica es un valor calculado que indica cuánta mejora se puede lograr al invertir en cobertura e implementación.

En la parte inferior de la pestaña “Tácticas” podrán ver un resumen del Rendimiento Global con algunas graficas de ejemplo. Estas pueden ser ajustadas y creadas a necesidad.

Figura 31
Rendimiento Global



Nota. Fuente Elaboración Propia

Al diligenciar toda la información en la herramienta, permitirá tener una visión más clara de la efectividad de detección y potencial de crecimiento.

Identificaran fácilmente que tipo de reglas según las tácticas y técnicas de MITRE ATT&CK deben centrarse en crear, cuales modificar, cuales eliminar.

8. Análisis de resultados

La guía metodológica proporciona una estructura clara para la creación de casos de uso SIEM basados en el marco MITRE ATT&CK, la cual se basa en un enfoque centrado en los activos críticos y los datos relevantes para la organización, lo que aumenta significativamente la eficacia de la ciberseguridad; así mismo se destaca la importancia de la monitorización y actualización regular de los casos de uso SIEM para asegurarse de que sean efectivos en la detección y prevención de amenazas de ciberseguridad.

9. Conclusiones

Destacamos la importancia de la gestión de casos de uso en la ciberseguridad y lo fundamental que puede llegar a ser en el proceso de identificación y mitigación de las amenazas y riesgo a los que está expuesta una organización.

La postura de una organización frente a la adopción de un marco de referencia como MITRE ATT&CK debe ser clara y concisa para que permita una articulación en cuanto a la gestión de incidentes y la respuesta a ciberataques.

Al contar con una guía metodológica para la creación y gestión de casos de uso SIEM permite identificar, precisar y priorizar los casos de uso más críticos y a establecer una respuesta rápida y efectiva frente a las amenazas.

Es importante y prioritario la identificación de procesos y sistemas críticos en la gestión de la ciberseguridad de una organización en razón a que permite enfocar los recursos en aquellos elementos que son fundamentales para la continuidad del negocio.

La evaluación de riesgos es un proceso continuo que debe formar parte de la cultura de ciberseguridad de una organización, en razón a que permite identificar las amenazas y vulnerabilidades más críticas y establecer medidas de mitigación efectivas para prevenir y mitigar los riesgos.

10. Referencias bibliográficas

A Quick Guide to Effective SIEM Use Cases. (2020, noviembre 12). *Security Intelligence*. https://securityintelligence.com/posts/quick-guide-to-siem-use-cases/

Acanerler, A. (2022, enero 17). *What is a Security Operations Center (SOC)? (Ultimate Guide)*. SOCRadar® Cyber Intelligence Inc. https://socradar.io/what-is-a-security-operations-center-soc-ultimate-guide/

ANOMALI. (2023). https://www.anomali.com/es/resources/what-mitre-attck-is-and-how-it-is-useful

ATT&CK® Navigator. (s. f.). Recuperado 26 de marzo de 2023, de https://mitre-attack.github.io/attack-navigator/

Bryant, B. D., & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. *Computers & Security*, *67*, 198-210. https://doi.org/10.1016/j.cose.2017.03.003

Engineering Lifecycle Management. (2023). *Definición de casos de uso — Documentación de IBM*. https://www.ibm.com/docs/es/elm/6.0.3?topic=requirements-defining-use-cases

IONOS, Digital Guide. (s. f.). *SIEM: ¿Qué es el Security Information and Event Management?* Recuperado 30 de marzo de 2023, de https://www.ionos.es/digitalguide/servidores/seguridad/que-es-siem/

Jurgen. (2020). *Introducing: SPEED Use Case Framework for SIEM*. http://correlatedsecurity.com/introducing-speed-use-case-framework-v1-0/

Lockheed Martin Corporation. (2023). https://lockheedmartin.com/

MaGMa. (2023, febrero 24). Betaalvereniging Nederland. https://www.betaalvereniging.nl/en/safety/magma/

Martínez, M. G. (2021, abril 22). ¿Qué es y cómo funciona un SOC frente a los ciberataques? *Nuestros Datos Seguros*. https://nuestrosdatosseguros.es/que-es-y-como-funciona-un-soc-frente-a-los-ciberataques/

MITRE. (2023). https://www.anomali.com/es/resources/what-mitre-attck-is-and-how-it-is-useful

Sancho Lerena. (s. f.). *Pandora FMS - The Monitoring Blog*. Recuperado 26 de marzo de 2023, de https://pandorafms.com/blog/fr/author/slerena/

SIEM Use Cases: Implementation and Best Practices. (s. f.). Recuperado 26 de marzo de 2023, de https://blog.netwrix.com/2021/05/05/siem-use-cases/

SOFECOM. (2023). SOFECOM. *SOFECOM, Servicios Integrales En IT*. https://sofecom.com/category/articulos/

Torres, P. (2022, agosto 3). ¿Cómo es la organización de un SOC para proteger tu organización? *Sothis*. https://www.sothis.tech/como-es-la-organizacion-de-un-soc-para-proteger-tu-organizacion/

Virginia Fernandez. (2023). *IBM Security QRadar*. https://www.slideshare.net/VirginiaFernandez11/ibm-security-qradar

Visser, J. (2020). *The "SPEED" SIEM Use Case Framework*.

11. Anexos

1. Archivo en Excel guía para la gestión de casos de uso SIEM.

   Herramienta Administración CASOS DE USO_-UCM-JQ_MC.xlsx

La herramienta ha sido subida a un repositorio público en GitHub, lo que permite su acceso y disponibilidad para el público en general. Puedes encontrar la herramienta y su código fuente en el siguiente enlace:

https://github.com/MigCHZ/Herramienta-Administracion-CASOS-DE-USO.git.

2. Inventario de activos de información_.xlsx

La herramienta ha sido subida a un repositorio público en GitHub, lo que permite su acceso y disponibilidad para el público en general. Puedes encontrar la herramienta y su código fuente en el siguiente enlace:

https://github.com/MigCHZ/Inventario_de_activos_de_informacion.git

Desde allí, cualquier persona interesada puede explorar, clonar y contribuir al desarrollo de la herramienta. Esta iniciativa busca fomentar la transparencia, la colaboración y el aprendizaje compartido en la comunidad, invitando a los usuarios a participar y mejorar la herramienta según sus necesidades y conocimientos.

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co