UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

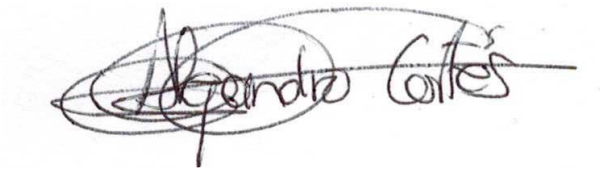
AUTOR: Ing. Bryan Adrián Agudelo Castro
Ing. Diego Javier Álvarez Yépez
Ing. Jennyfer Alexandra Andrade Valdez
Ing. Jorge Mentor Escobar Tucta

TUTOR: Alejandro Cortés López

Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft

Aprobación del Tutor

Yo, Alejandro Cortés López certifico que conozco a los autores del presente trabajo siendo los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.

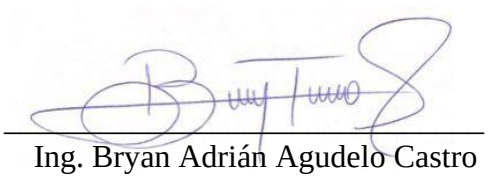


Alejandro Cortés López
DIRECTOR DE TESIS

Declaración de Autoría del Trabajo de Titulación

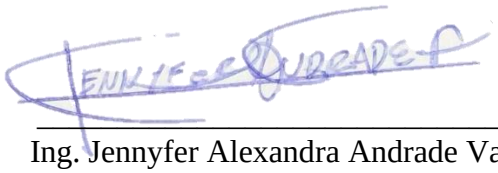
Nosotros, Bryan Adrián Agudelo Castro, Diego Javier Álvarez Yépez, Jennyfer Alexandra Andrade Valdez y Jorge Mentor Escobar Tucta, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Ing. Bryan Adrián Agudelo Castro

Ing. Diego Javier Álvarez Yépez



Ing. Jennyfer Alexandra Andrade Valdez

Ing. Jorge Mentor Escobar Tucta

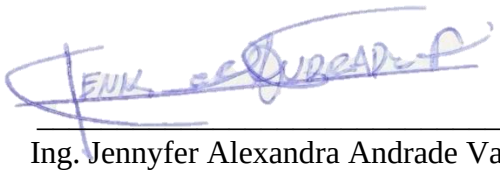
Autorización de Derechos de Propiedad Intelectual

Nosotros, Bryan Adrián Agudelo Castro, Diego Javier Álvarez Yépez, Jennyfer Alexandra Andrade Valdez y Jorge Mentor Escobar Tucta, en calidad de autores del trabajo de investigación titulado Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft, autorizo a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autor me corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Diciembre del 2022

Ing. Bryan Adrián Agudelo Castro

Ing. Diego Javier Álvarez Yépez



Ing. Jennyfer Alexandra Andrade Valdez

Ing. Jorge Mentor Escobar Tucta

Dedicatoria

Ante lo etéreo y la adecuada situación, es un honor rotundo dedicar este trabajo a las personas que me avivan la existencia. Papá, mamá, hermano, cuñada, sobrino y esposa mía, quienes han estado en las buenas, malas y peores.

Bryan Adrián Agudelo Castro

Dedicatoria

A mi abuela, quien me dió la confianza para llegar a este momento

Diego Javier Álvarez Yépez

Dedicatoria

Principalmente dedico este trabajo a mi familia, quienes siempre han creído en mí, dándome ejemplo de trabajo duro y constancia. También lo dedico a Denisse quien ha estado a mi lado apoyándome, siendo parte de cada decisión y por la paciencia durante este periodo académico.

Jennyfer Alexandra Andrade Valdez

Dedicatoria

A mis hermanos que me han inspirado profesionalmente mediante su gran ejemplo.

Jorge Mentor Escobar Tucta

Agradecimiento

Pertenecido al inmensurable agradecimiento hacia las personas que resaltan en mi mente e inspiran al regocijo de mi alma. Papá y mamá, gracias por la guía y el contagio oportuno de mis virtudes. Hermano y cuñada, gracias por el conveniente soporte con los ánimos y felicitaciones en cada paso planteado. Sobrino querido y amado, gracias por alumbrarme con tu hermosa existencia. Amor de mi vida, te agradezco por tu maravillosa incondicionalidad y amor sempiterno.

Bryan Adrián Agudelo Castro

Agradecimiento

A mis padres por sus valores, cariño y constancia que siempre me han inspirado y educado

Diego Javier Álvarez Yépez

Agradecimiento

Gracias a Diego, por no solo ser un buen compañero, sino que un gran amigo.

Jennyfer Alexandra Andrade Valdez

Agradecimiento

A mis padres que siempre han estado apoyándome en cualquier situación que se ha presentado.

Jorge Mentor Escobar Tucta

Resumen

El presente trabajo de titulación tiene como objeto la elaboración de cinco casos de usos orientados a la mejora de ciberseguridad en el sector financiero con las herramientas del SIEM que utiliza la empresa Secure Soft. Ante esto, se inició a la identificación de las vulnerabilidades más recurrentes dentro del sector financiero que han sido alertadas en las distintas instituciones financieras, mismas que fueron determinadas mediante un marco teórico, conceptualizando las vulnerabilidades más predominantes.

Además del marco teórico, se concretó la metodología del trabajo de titulación con la inserción del top de alertas más comunes, mediante la cual y con la identificación de vulnerabilidades permitió al equipo de trabajo concentrar las soluciones en los cinco problemas con mayor recurrencia en el área de finanzas dentro de las instituciones que dependan de sistemas informáticos que puedan ser vulnerados por ciberdelincuentes.

Finalmente, con el reconocimiento de vulnerabilidades, se estableció un modelo de plantilla para describir parámetros como: objetivo, alcance, fuentes de eventos, tipos de datos, flujo lógico, notificación, severidad y recomendación como respuesta de ciberseguridad ante la alerta o vulnerabilidad del sector financiero.

Abstract

The aim of this degree work is the development of five cases of uses aimed at improving cybersecurity in the financial sector with the tools of the SIEM used by the company Secure Soft with this, it began to identify the most recurrent vulnerabilities within the financial sector that have been alerted in the different financial institutions, which were determined by a theoretical framework, conceptualizing the most predominant vulnerabilities.

In addition to the theoretical framework, the methodology of the degree work was specified with the insertion of the most common alerts top, through which and with the identification of vulnerabilities allowed the task force to concentrate the solutions on the five problems with the greatest recurrence in the area of finance within the institutions that depend on computer systems that can be violated by cybercriminals.

Finally, with the recognition of vulnerabilities, a template model was established to describe parameters such as: objective, scope, event sources, data types, logical flow, notification, severity and recommendation as a cybersecurity response to the alert or vulnerability of the financial sector.

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

Capítulo 1

Introducción

El proyecto contempla el planteamiento de casos de uso sobre las herramientas SIEM administradas por la empresa de seguridad informática Secure Soft y su servicio a través de la unidad de Cyber SOC y con ello identificar de mejor manera las actividades y cargas de trabajo con el fin de encontrar actividades maliciosas enfocadas en grupos de clientes del sector financiero.

El servicio de Security Operations Center (SOC) de la empresa Secure Soft es un área de seguridad conformada por múltiples aplicaciones a diferentes niveles, acompañada de una infraestructura tecnológica y personal conformado por analistas y operadores encargados de detectar, analizar y gestionar los incidentes relacionados con la seguridad, con el objeto de minimizar riesgos. Uno de los sectores con mayor atención en la actualidad por parte del SOC es el financiero.

La transformación digital y el auge sobre la banca digital hacen que el mercado financiero en nuestro país crezca y sea más competitivo, sin embargo, esto conlleva a un cambio y crecimiento en la arquitectura tecnológica y, por ende, a nuevas posibles brechas de seguridad, lo que hace necesario centralizar el control de las diferentes fuentes de información de manejo y protección del tráfico de la infraestructura tecnológica.

Por ello es necesario que dentro del plan estratégico de las instituciones financieras deben ser contemplados, con alta prioridad, servicios que centralizan la

operatividad de seguridad como es el caso de CyberSOC, encargado principalmente en la automatización de la detección de eventos mediante tecnologías como el SIEM.

Las ventajas de contar con analistas y un CyberSOC externo permite optimizar el tiempo al equipo de tecnología de las instituciones quienes no requieren analizar o revisar información de logs o eventos, sino que lo realizan especialistas en la evaluación y análisis de los mismos, efectuando de esta manera el diseño de casos de uso específicos y personalizados basados en la evaluación de las principales fuentes de seguridad con las que cuenta cada empresa

Caso de Uso

Según (IBM, 2021), establece que un caso de uso es "un artefacto que define una secuencia de acciones que da lugar a un resultado de valor observable". Por lo que, para la necesidad del proyecto los casos de uso comprenden una estructura acertada para plasmar los requisitos funcionales e identificación de vulnerabilidades dentro del sector financiero.

Por otro lado, de acuerdo a (MADEJA), las características que deben tener los casos de uso son:

- Describir una tarea del negocio que sirva a una meta de negocio.
- Tener un nivel apropiado del detalle.
- Ser bastante sencillo como que un desarrollador lo elabore en un único lanzamiento.

Tipos de Caso de Uso. (Vega, 2010) establece que existen dos tipos de casos de uso según el nivel de detalle:

- Resumidos o de alto nivel, los cuales se elaboran en la fase inicial obteniendo el mayor detalle del requisito.
- Extensos, se elaboran en la fase de elaboración del proyecto.

Actores en los Casos de Uso. Acá puede ir otra idea del documento. De acuerdo a (Mediavilla) determina que un actor es “alguien o algo que interactúa con el sistema, pero que es externo al sistema”. Tomando como referencia este concepto y relacionándolo con el proyecto, es preciso identificar los distintos tipos de vulnerabilidades que atacan al sector financiero y de esta manera establecerlos como actores.

Por otro lado, para (Vega, 2010) nos menciona que existen tres tipos de actores principales, como lo son: Primarios, Secundarios e Iniciadores. Como actores primarios reconocemos que son todos los que interactúan con el sistema para explotar su funcionalidad, en cuanto a los secundarios son aquellos que ofrecen soporte del sistema para que los actores primarios desarrollen o trabajen en él. Y finalmente con los actores iniciadores nos referimos a aquellos que no hacen uso del sistema, pero liberan el trabajo de otro actor.

Por tanto, la implementación de casos de uso en un SIEM nos brinda la oportunidad de identificar, definir y relacionar las soluciones sostenibles a las vulnerabilidades más comunes y peligrosas en el sector financiero mediante la integración de la severidad y recomendación que el propio caso de uso pueda solucionar.

Objetivos

Objetivo General.

- Definir cinco casos de uso para la implementación de un SIEM que funciona a través de un SOC para las necesidades de ciberseguridad dentro de un ambiente de negocio del sector financiero.

Objetivos Específicos.

- Analizar la información por parte de la empresa Secure Soft sobre las vulnerabilidades más concurrentes en el área de clientes del sector financiero.
- Identificar el flujo necesario para el manejo de la información y la estructuración de casos de uso.
- Establecer un modelo de plantilla para la definición de los casos de uso.

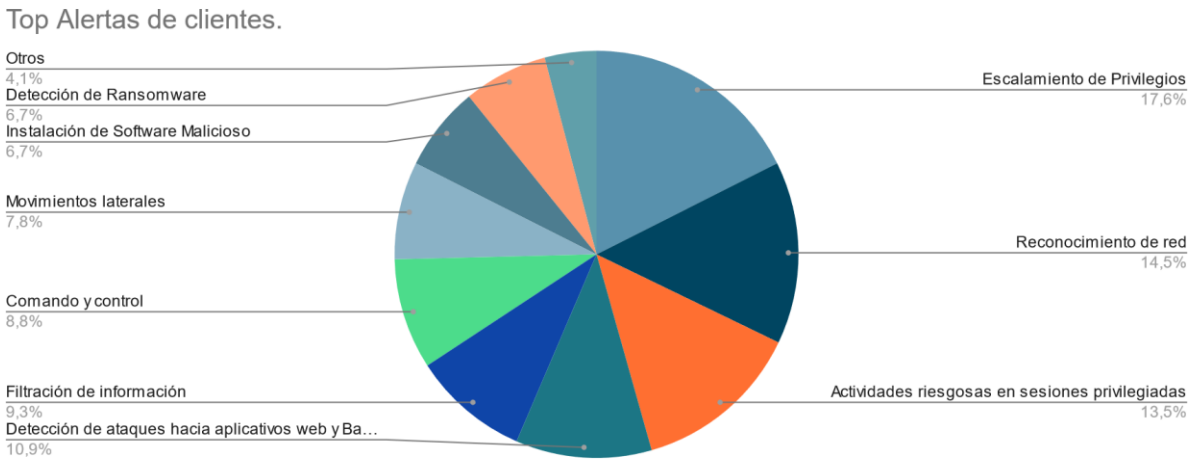
Capítulo 2

Metodología

Acorde al Foro Económico Mundial, los ciberataques forman ya parte del listado de riesgos globales, y esto conlleva a que las instituciones financieras y en general adopten medidas de seguridad y el manejo de buenas prácticas. Dentro de este contexto se forman los casos de uso los cuales serán regulados por el equipo de CyberSOC, enfocados principalmente en objetivos y cumplimientos. Desde este esquema, se ha generado una recolección de datos sobre los principales casos de uso enfocados a instituciones financieras, entre ellos se encuentran en modo general los siguientes:

Figura 1.

Top de alertas de seguridad detectado en clientes de SOC Secure Soft



Con la definición del flujo de trabajo que conlleva un caso de uso, uno de los componentes principales para centralizar la información receptora de fuentes y la

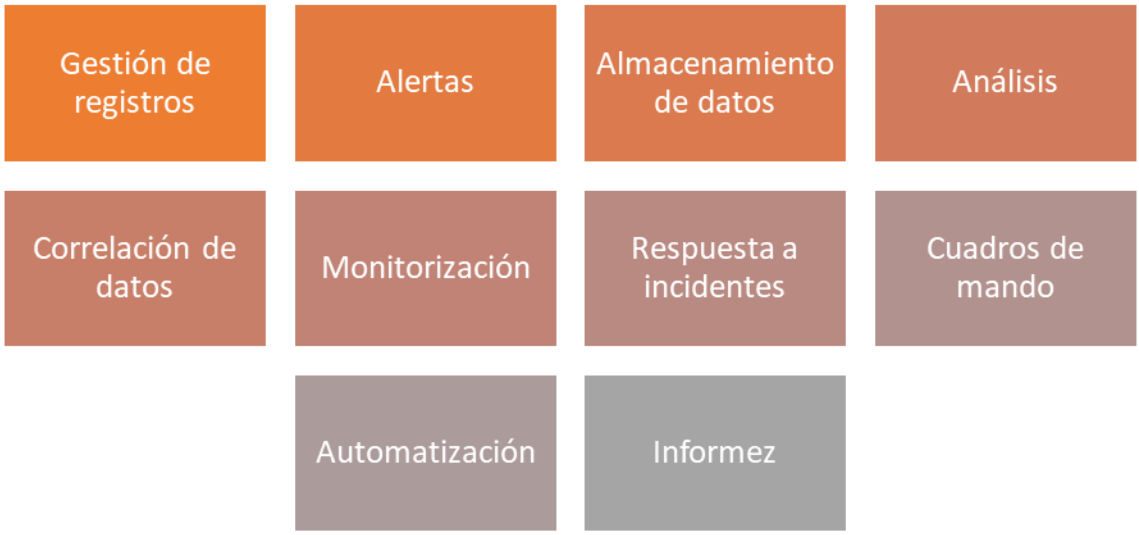
identificación de los casos de uso definidos son las plataformas de Gestión de Información y Eventos de Seguridad SIEM.

Security Information and Event Management (SIEM):

Podemos definir al gestor de eventos de información y eventos de seguridad (SIEM) como el conjunto de herramientas y servicios que permite tener una visión holística de la seguridad de la información dentro una empresa o institución. Arquitectura de un SIEM. Una solución de SIEM consta de varios componentes que permite al equipo de especialistas y analistas orquestar de mejor manera la detección y análisis de violaciones de datos, así como actividades maliciosas. Se detallan a modo general los siguientes componentes dentro de una arquitectura.

Figura 2.

Arquitectura de un SIEM



Gestión de registros. Los registros se encargan de registrar los eventos que se envían la información sobre varias fuentes de logs, tales como firewalls, EDR´s, herramientas de gestión de identidades, de networking, etc., lo cual conlleva en la gestión y manejo de un gran volumen de información, por lo que los especialistas deben dedicar mucho tiempo en garantizar que se recopilen los datos de manera correcta de cada fuente, previo agregarlos, normalizarlos y correlacionarlos.

El SIEM puede recopilar datos de cuatro maneras:

- A través de un agente instalado en el dispositivo (el método más común).
- Conectándose directamente al dispositivo mediante un protocolo de red o una llamada API.
- Accediendo a los archivos de registro directamente desde el almacenamiento, generalmente en formato Syslog.
- A través de un protocolo de transmisión de eventos como SNMP, Netflow o IPFIX.

El SIEM tiene la tarea de recopilar datos de los dispositivos, estandarizarlos y guardarlos en un formato que permita el análisis.

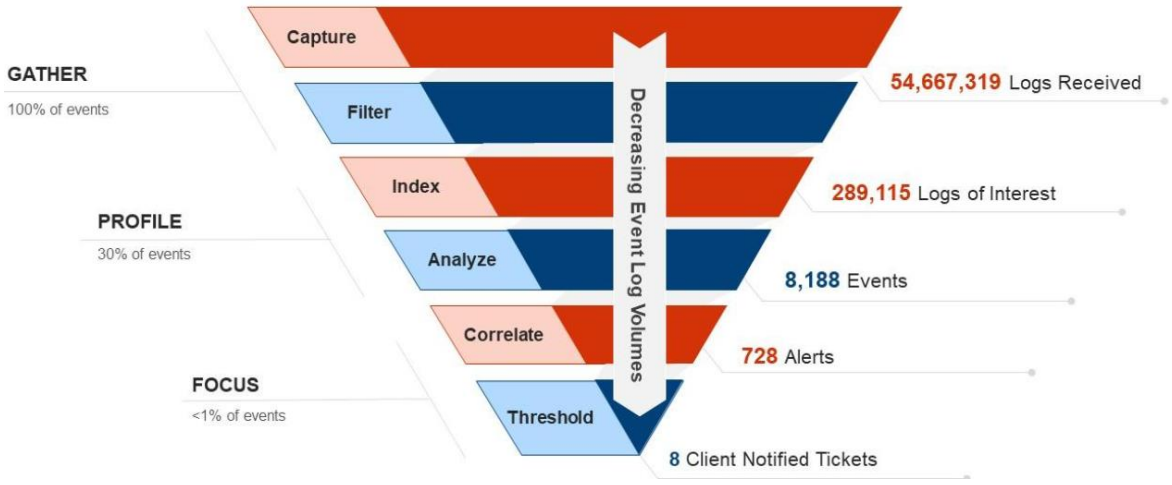
Los SIEM de próxima generación vienen pre integrados con sistemas en cloud y fuentes de datos comunes, lo cual le permite extraer datos de registro de manera directa.

Un SIEM captura el 100 % de los datos de todas las fuentes que se integren de la empresa. Posteriormente los datos empiezan a fluir por el embudo y cientos de millones de entradas pueden reducirse a sólo un puñado de alertas de seguridad procesables. Los SIEM filtran el ruido para mantener solo los datos pertinentes. Luego indexan y

optimizan los datos relevantes para permitir el análisis. Finalmente, alrededor del 1% de los datos, que es el más relevante para su postura de seguridad, se correlacionan y analizan con mayor profundidad. De esas correlaciones, las que superan los umbrales de seguridad se convierten en alertas de seguridad.

Figura 3.

Flujo de registros de un SIEM



Alertas Los registros que necesitan atención inmediata se envían a la empresa posterior al análisis de los eventos.

Almacenamiento de datos: En empresas grandes, los SIEM pueden almacenar un gran volumen de datos. Los datos deben ser:

- Almacenados: ya sea en las instalaciones, en la nube o en ambos principalmente si estos necesitan ser investigados posteriormente. Estos tipos de datos pueden ser datos históricos o métricas.

- Optimizado e indexado: Para permitir un análisis y una exploración eficientes
- En niveles: Los datos calientes necesarios para el monitoreo de seguridad en vivo deben estar en un almacenamiento de alto rendimiento, mientras que los datos fríos, que quizás desee investigar algún día, deben replegarse a medios de almacenamiento económicos de gran volumen.

Los SIEM de próxima generación se basan cada vez más en tecnologías como son data lake, Amazon S3, Hadoop o ElasticSearch, lo cual les permite un almacenamiento de datos ilimitado y con un costo bajo.

Los estándares de la industria como PCI DSS, HIPAA y SOX requieren que los registros se conserven entre 1 y 7 años. Las grandes empresas crean un volumen muy alto de registros todos los días desde los sistemas de TI.

La mayoría de los SIEM en la actualidad se implementan en las instalaciones. Esto requiere que las empresas consideren cuidadosamente el tamaño de los datos de eventos y registros que están generando, y los recursos del sistema necesarios para administrarlos.

Una medida común de velocidad son los eventos por segundo (EPS), definidos como:

 # de eventos de seguridad dividido por el período de tiempo en segundos = EPS

Los EPS pueden variar entre horas normales y pico. Podemos tomar como ejemplo, un router Cisco que puede generar 0,6 eventos por segundo en promedio, pero durante las horas pico, como durante un ataque, puede generar hasta 154 EPS.

De acuerdo con la Guía de evaluación comparativa SIEM del Instituto SANS, las organizaciones deben lograr un equilibrio entre las mediciones EPS normales y máximas. No es práctico, ni necesario, construir un SIEM para manejar EPS pico para todos los dispositivos de red, porque es poco probable que todos los dispositivos alcancen su punto máximo a la vez. Por otro lado, debe planificar para situaciones de crisis, en las que el SIEM será más necesario.

Un modelo simple para predecir EPS durante horas normales y pico:

- Medir el EPS normal y el EPS máximo, observando 90 días de datos para el sistema de destino
- Estimar el número de picos por día
- Calcular la duración en segundos de un pico y, por extensión, el total de segundos pico por día
- Calcular el total de eventos pico por día = (total de segundos pico por día) * EPS pico
- Calcular el total de eventos normales por día = (total de segundos – total de segundos pico por día) * EPS normal

La suma de estos dos números es la velocidad total estimada. Además, la guía SANS recomienda agregar:

- 10% por margen
- 10% para el crecimiento

De modo que el número final de eventos por día será:

(Total *de eventos pico por día + Total de eventos normales por día) * 110 % de espacio libre * 110 % de crecimiento*

Análisis: El SIEM interpreta los datos basándose en la categorización de los dispositivos. Debido a esta categorización de los dispositivos, el motor de análisis de SIEM es capaz de interpretar los datos en consecuencia. Se registra información como los registros de bitácora generados por un tipo de dispositivo en particular, los elementos de datos presentes, etc**.**

Correlación de ***datos:*** Dado que los datos se recogen de múltiples dispositivos, tienen que presentarse de una manera significativa y estructurada. La función de correlación ayuda a presentar una imagen más amplia de los datos recogidos desde múltiples puntos.

A través de esta actividad de correlación, un usuario puede acceder a información como qué usuario está conectado, qué dispositivo se está utilizando, qué errores se han generado, etc.

Monitorización en tiempo real: Los usuarios reciben actualizaciones relacionadas con cualquier tipo de fallo de seguridad en tiempo real. Esto ayuda a realizar un seguimiento oportuno y eficiente y a eliminar la amenaza. La mayoría de los sistemas SIEM ofrecen paneles de control para los problemas de seguridad y otros métodos de notificación

directa permitiendo transmitir automáticamente los mensajes de notificación de alarmas de manera apropiada, así como programar, por parte de los especialistas, triggers para el envío de eventos en función del nivel de criticidad del evento.

Respuesta a incidentes: Si se ha producido un fallo de seguridad en una red, se tienen en cuenta todos los datos relevantes para proporcionar asistencia instantánea a la hora de hacer frente a dichas amenazas.

Cuadros de mando (Dashboards): Los dashboards del SIEM ayudan a los analistas de seguridad a comprender fácilmente los cambios en cualquier patrón de datos. Así, un analista de seguridad puede detectar fácil y rápidamente cualquier anomalía que se produzca en la red.

Automatización: Gracias a SOAR (Security, Orchestration, Automation, and Response), se puede responder automáticamente a cualquier incidente sin depender de los analistas de seguridad.

Elaboración de informes: La herramienta de generación de informes SIEM permite la generación de diferentes informes para otros administradores para minimizar cualquier confusión relacionada con su trabajo de informes. SIEM genera informes de forma eficiente ya que guarda toda la información de los registros en tablas de la base de datos.

Tipos de Integraciones de SIEM

- In-House: es el modelo tradicional de implementación de SIEM; en el que este se instala en un Datacenter, a menudo con un dispositivo SIEM dedicado, con este modelo se mantienen los sistemas de almacenamiento y administración on

premise. Dicho modelo se convirtió en una infraestructura compleja y costosa de mantener.

- MSSP: Modelo en la nube mediante un esquema de servicios gestionados en la recepción de eventos, recopilación y agregación o puede ser manejado directamente por la empresa y su personal de analistas.
- Modelo híbrido: Combina los esquemas in-house y MSSP

Desarrollo

El sistema financiero en el Ecuador lo componen principalmente instituciones financieras privadas, públicas, compañías de seguros, entre otras:

Figura 4.

Componentes del sistema financiero ecuatoriano.

La dependencia en el crecimiento de los servicios del sistema financiero en la infraestructura digital genera un incremento en la protección de esta, por ello el enfoque de la creación de casos de uso más modelados a las necesidades actuales, enfocadas en

ámbito de protección de cuentas, comportamiento de usuarios, control de protecciones de borde, entre otras. Por ello en la definición de los casos de uso se proponen lo siguientes:

- Caso de uso 1, Acceso a las cuentas privilegiadas protegidas en horas irregulares.
- Caso de uso 2, Exfiltración de Datos.
- Caso de uso 3, Ingreso a plataformas corporativas de manera irregular.
- Caso de uso 4, Detección de malware a través de un firewall perimetral.
- Caso de uso 5, Detección de Ransomware en ordenadores corporativos.

Caso de Uso 1. Acceso a las cuentas privilegiadas protegidas en horas irregulares.

El enfoque sobre la tecnología de aprendizaje automático permite un punto importante de ejecución del comportamiento de los usuarios y con ello definir un patrón de posibles amenazas que se pueden presentar, principalmente en el uso de cuentas de altos privilegios. El control del uso de cuentas que permiten la administración y control sobre diferentes servidores, bases de datos y aplicaciones de una institución, conlleva a que tomemos acción de protección sobre las mismas ya que un potencial ataque sobre movimiento lateral puede presentarse.

Las tecnologías que nos permiten dicho análisis de comportamiento y a la vez brindan protección de estas cuentas de altos privilegios son las denominadas Privileged Access Management (PAM).

Privileged Access Management (PAM): En un entorno empresarial, el término de acceso privilegiado define el acceso especial o las capacidades por encima de un

usuario estándar. Un acceso privilegiado permite a las empresas administrar su infraestructura y aplicaciones, así como de mantener la confidencialidad de los datos sensibles. Estos accesos privilegiados pueden asociarse a usuarios humanos y a usuarios no humanos.

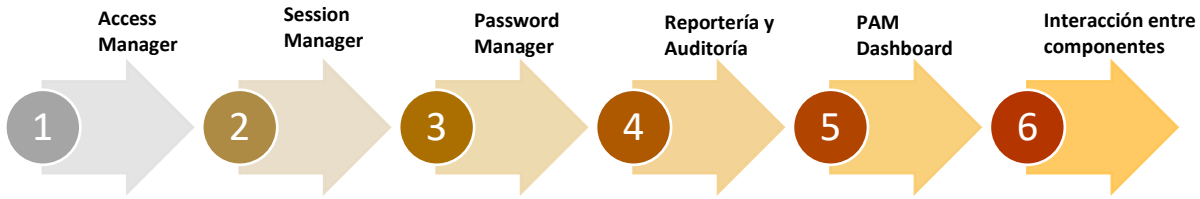
- Cuentas de usuarios humanos: Cuenta de super usuario, cuenta administrativa de dominio, cuenta administrativa local, secure socket shell (SSH) key, cuentas de emergencia, usuario de negocio privilegiado.
- Cuentas de usuarios no humanos: Cuenta de aplicación, cuenta de servicio, SSH key.

La gestión de accesos privilegiados (PAM) es una estrategia integral de ciberseguridad que comprende personas, procesos y tecnología cuyo objetivo es controlar, supervisar, asegurar y auditar todas las identidades y actividades privilegiadas humanas y no humanas en un entorno informático empresarial.

Componentes generales de Plataformas PAM:

Figura 5.

Flujo de registros de un SIEM



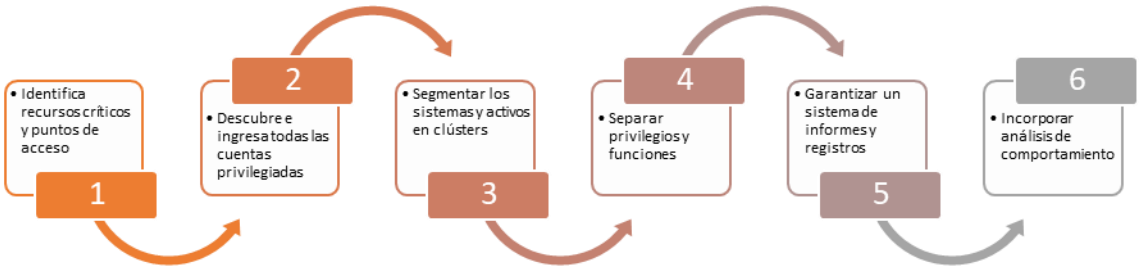
- **Access Manager:** Es el punto de entrada único que permite la interacción entre los usuarios y los recursos críticos. Almacena los permisos, los roles de los usuarios y la información de los usuarios privilegiados. Los gestores de políticas lo utilizan para crear políticas de acceso basadas en identidades o roles de usuarios individuales. El gestor de acceso también establece límites de privilegios a una lista predeterminada de aplicaciones y servicios.
- **Session Manager:** Este componente permite iniciar, supervisar y registrar las sesiones privilegiadas y el uso de las cuentas administrativas y privilegiadas.
- **Password Manager:** El componente del Password Manager administra y resguarda las credenciales de altos privilegios sobre una bóveda digital de manera encriptada, permitiendo de esta manera aplicar políticas sobre las cuentas sobre su estado, modificación o cambio acorde a políticas internas. El gestor de contraseñas reduce significativamente los errores humanos causados por una gestión inadecuada de las contraseñas.
- **Reportería y Auditoría:** Genera la correlación de logs y genera informes y acceso al registro de actividades que dan visibilidad sobre eventos relacionados a vulnerabilidades o actividades sospechosas realizadas en sesiones hacia los servicios target con cuentas privilegiadas controladas. Estos informes y el sistema de auditoría en el gestor de sesiones, juntos, proporcionan información forense que puede precisar cómo se produjeron

los intentos de violación de datos anteriores y qué técnicas de mitigación pueden prevenir futuros ataques.

- **PAM Dashboard**: Un dashboard de herramientas PAM proporciona una rápida visión general de las cuentas disponibles, las configuraciones de las mismas sobre los servidores target, los chequeos actuales, los escaneos recurrentes sobre las cuentas, su estatus y las actividades recientes. Permite además configurar las políticas de acceso, sesión y contraseña, descubrir las cuentas privilegiadas en todo el sistema y definir las identidades, los roles y los permisos de los usuarios.
- **Interacción entre componentes**: Todos los usuarios autorizados a utilizar las plataformas PAM pasan por el gestor de acceso, que accede a la bóveda digital de resguardo de cuentas de altos privilegios y permite una autenticación segura. Una vez autenticado, el control pasa al gestor de sesiones, que inicia, supervisa y finaliza las sesiones según sea necesario.

Figura 6.

Ciclo de gestión de cuentas sobre plataformas PAM



De las diferentes marcas que brindan este servicio hemos seleccionado la plataforma CyberArk, principalmente por ser una de las marcas más sólidas en el mercado de ciberseguridad en el ámbito de protección PAM:

Figura 7.

Cuadrante de Gartner 2022 marcas sobre herramientas PAM .

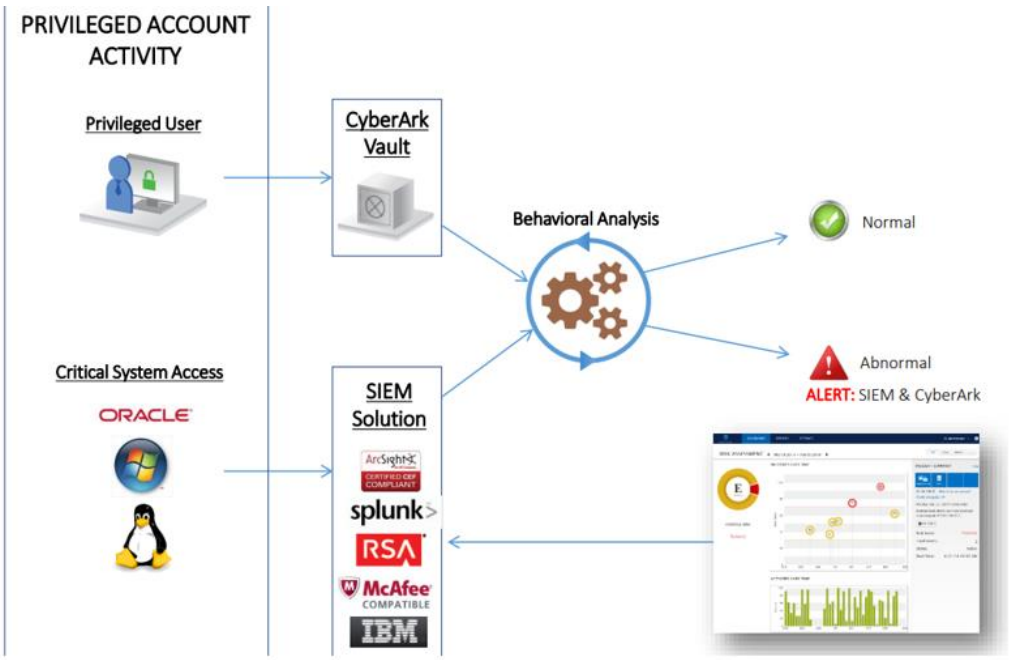
Las alertas a ser identificadas son las generadas mediante la herramienta Privileged Threat Analytics de CyberArk (PTA), una herramienta que componente la arquitectura de la plataforma CyberArk y que se encarga de recolectar y analizar la actividad de las cuentas privilegiadas, de igual manera permite la integración de fuentes de datos de soluciones SIEM, generando un envío de tráfico bidireccional de información como lo muestra la figura 9. La plataforma PTA de recolectar la información

proporcionada por la bóveda digital la cual es la fuente interna del componente y que se encarga de almacenar las cuentas privilegiadas, así como de herramientas externas como el SIEM.

Con la información obtenida genera análisis de patrones de comportamiento de los usuarios finales que utilizan dichas cuentas de altos privilegios mediante un modelo estadístico de autoaprendizaje basado en una combinación de algoritmos. Con la información sobre el evento generado el PTA alimenta al dashboard de eventos sobre la vulnerabilidad detectada, así como el envío de logs hacia el SIEM:

Figura 8.

Modelo de trabajo de plataforma Privileged Thread Analytics



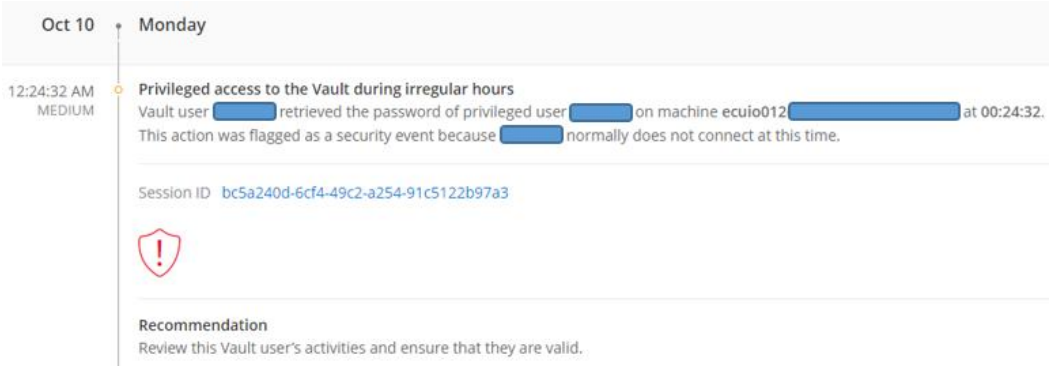
Dentro de las actividades sospechosas detectadas por la plataforma es la denominada “Privileged access to the Vault during irregular hours” (Acceso privilegiado

a la bóveda en horario irregular), la definición de la misma es cuando un usuario recupera la contraseña de una cuenta privilegiada a una hora que es irregular para ese usuario cuyo Event Type Id en la plataforma es 23.

La plataforma permite efectuar el control tanto de acceso con la cuenta privilegiada a un servidor target, así como la recuperación de la clave en horas irregulares del usuario, aquí se muestra en la Figura 9 un ejemplo del mensaje del evento:

Figura 9.

Visualización del evento en la plataforma CyberArk.



El log receptado por la plataforma PTA del evento de igual manera es enviado al SIEM mediante la conexión por el puerto 514 en TCP del syslog record con el siguiente ejemplo de formato:

CEF:0|CyberArk|PTA|12.6|1|Privileged access to the Vault during irregular hours|8|suser=mike2@prod1.domain.com shost=prod1.domain.com src=1.1.1.1 duser=andy@dev1.domain.com dhost=dev1.domain.com dst=2.2.2.2 cs1Label=ExtraData cs1=None cs2Label=EventID cs2=52b06812ec3500ed864c461e deviceCustomDate1Label=detectionDate deviceCustomDate1=1388577900000

cs3Label=PTAlink cs3=https://1.1.1.1/incidents/52b06812ec3500ed864c461e cs4Label=ExternalLink cs4=None

En ambos formatos de información los datos relevantes son principalmente:

- Nombre de usuario final que accede a CyberArk
- Servidor target al cual ingresa
- Fecha y hora del evento
- Session ID de la grabación de la sesión del usuario final

Caso de Uso 2. Exfiltración de Datos

Varias consecuencias se derivan de un hacking malicioso. Estas dependen de las intenciones del atacante y, también, de lo que permitan los diferentes tipos de vulnerabilidades informáticas que encuentre.

La exfiltración de datos es el robo, la eliminación o el movimiento no autorizado de cualquier dato de un dispositivo; suele implicar que un ciberdelincuente robe datos de dispositivos personales o corporativos, como ordenadores y teléfonos móviles, a través de diversos métodos de ciberataque.

También es la exportación y extrusión de datos, la fuga de datos o el robo de datos, que puede plantear graves problemas a las organizaciones. No controlar la seguridad de la información puede conducir a la pérdida de datos que podría causar daños tanto como imagen, así como a nivel económico a una organización.

Los tipos de exfiltración de datos y las técnicas de ciberataque más comunes son los que se detallan a continuación.

Ataques de ingeniería social y phishing

Los ataques de ingeniería social y phishing son un vector de ataque a la red muy popular que se utiliza para engañar a las víctimas para que descarguen malware y faciliten las credenciales de sus cuentas.

Los ataques de phishing consisten en correos electrónicos diseñados para parecer legítimos y que a menudo parecen proceder de remitentes de confianza. Contienen un archivo adjunto malicioso que inyecta malware en el dispositivo del usuario o un enlace a un sitio web que parece legítimo, pero que está falseado para robar las credenciales de acceso que el usuario introduce. Algunos atacantes también lanzan ataques de phishing dirigidos con el objetivo de robar datos de un usuario específico, como altos ejecutivos de empresas o personas de alto valor como celebridades o políticos.

Correos electrónicos salientes

Los ciberdelincuentes utilizan el correo electrónico para exfiltrar cualquier dato que se encuentre en los sistemas de correo electrónico saliente de las organizaciones, como calendarios, bases de datos, imágenes y documentos de planificación. Estos datos pueden ser robados de los sistemas de correo electrónico como mensajes de correo y de texto o a través de archivos adjuntos.

Descargas a dispositivos inseguros

Este método de exfiltración de datos es una forma común de amenaza interna accidental. El actor malicioso accede a información corporativa sensible en su dispositivo de confianza, y luego transfiere los datos a un dispositivo inseguro. Este dispositivo inseguro o no supervisado puede ser una cámara, un disco externo o un teléfono

inteligente que no está protegido por las soluciones o políticas de seguridad de la empresa, lo que supone un alto riesgo de que se filtren los datos.

Los smartphones también son susceptibles de sufrir una exfiltración de datos, siendo los dispositivos Android vulnerables a que se les instale un malware que tome el control del teléfono para descargar aplicaciones sin el consentimiento del usuario.

Subidas a dispositivos externos

Este tipo de exfiltración de datos suele provenir de atacantes internos malintencionados. El atacante interno puede exfiltrar datos descargando la información de un dispositivo seguro y luego cargándola en un dispositivo externo. Este dispositivo externo podría ser un ordenador portátil, un smartphone, una tableta o una unidad de memoria USB.

Error humano y comportamiento no seguro en la nube

La nube proporciona a los usuarios y a las empresas una multitud de beneficios, pero junto con ella hay importantes riesgos de exfiltración de datos. Por ejemplo, cuando un usuario autorizado accede a los servicios en la nube de forma insegura, permite a un actor malintencionado realizar cambios en las máquinas virtuales, desplegar e instalar código malicioso y enviar solicitudes maliciosas a los servicios en la nube. Los errores humanos y los problemas de procedimiento también desempeñan un papel en la exfiltración de datos, ya que es posible que no exista la protección adecuada.

Tomando en cuenta que el caso de uso es para una empresa del sector financiero, las alertas que se analizarán serán:

- Eventos de navegación asociados a las categorías de almacenamiento de información personal y Peer-to-Peer File Sharing.
- Eventos de correos salientes con archivos adjuntos dirigidos a un correo no relacionado con la organización.

Para obtener esta información los eventos se pueden tomar desde dos tipos de fuentes que son:

- **Proxy de navegación web**

Websense Content Gateway (Content Gateway) es un proxy web y caché de alto rendimiento basado en Linux que proporciona escaneo de contenido en tiempo real y clasificación de sitios web para proteger las computadoras de la red contra contenido web malicioso mientras controla el acceso de los empleados a sitios web dinámicos generados por usuarios. contenido 2.0. El contenido web ha evolucionado de una fuente de información estática a una plataforma sofisticada para comunicaciones bidireccionales, que puede ser una valiosa herramienta de productividad cuando se protege adecuadamente.

Content Gateway ofrece:

- Categorización automática de sitios Web 2.0 dinámicos
- Categorización automática de sitios nuevos y sin clasificar
- Inspección de contenido HTTPS
- Capacidades de almacenamiento en caché de proxy empresarial

Con Websense se obtienen las siguientes funciones:

- Escaneo de seguridad, que inspecciona las páginas web entrantes para bloquear inmediatamente el código malicioso, como el phishing, el malware y los virus
- Escaneo avanzado de archivos, que ofrece escaneo antivirus tradicional y técnicas de detección avanzadas para descubrir y bloquear archivos infectados y maliciosos que los usuarios intentan descargar
- Eliminación de contenido, que elimina el contenido activo (código escrito en lenguajes de secuencias de comandos seleccionados) de las páginas web entrantes.

- **Antispam**

El término antispam se utiliza para referirse a un software o procesos de detección y análisis que tienen como objetivo bloquear el spam (o mensajes no deseados). El problema detrás de los correos no deseados es que a menudo ocultan estafas y amenazas.

Entonces, lo que al principio sería un correo electrónico sin pretensiones puede estar ocultando una estafa de phishing o un malware destinado a robar información o secuestrar máquinas.

Cuando decimos que la palabra antispam puede hacer referencia a un proceso de detección y análisis, básicamente nos referimos a técnicas y estrategias para bloquear el spam.

Los softwares anti-spam hoy en día utilizan diferentes tecnologías, mecanismos, filtros, entre otras cosas. Se pueden implementar en la nube o mediante versiones locales,

e incluso pueden integrar otras soluciones. Lo importante a entender, en un principio, es que trabajan con técnicas de filtrado y análisis.

El análisis heurístico, por ejemplo, funciona con algoritmos para identificar qué es spam mediante un sistema de puntuación. El análisis bayesiano trabaja con estadísticas y ocurrencias.

Cisco Secure Email incluye capacidades avanzadas de filtrado y protección de correo contra amenazas para detectar, bloquear y remediar las amenazas, evitar la pérdida de datos y proteger la información importante en tránsito con cifrado de extremo a extremo.

Las amenazas actuales a la seguridad del correo electrónico consisten en Ransomware, malware avanzado, BEC, phishing y spam. La tecnología Cisco Secure Email bloquea las amenazas para que las empresas reciban únicamente mensajes legítimos. Cisco utiliza múltiples capas para proporcionar la máxima seguridad integral del correo electrónico, incorporando medidas preventivas y reactivas para reforzar su defensa, las cuales son

- Inteligencia global sobre amenazas
- Filtro de reputación
- Protección contra el spam
- Detección de correo electrónico falsificado
- Cisco Secure Email Phishing Defense
- Cisco Secure Email Domain Protection

Caso de Uso 3. Ingreso a plataformas corporativas de manera irregular.

Hay una necesidad en el sector financiero de monitorear las plataformas, el menester de saber que usuarios usan los datos y cómo los están usando

Hay una necesidad en el sector financiero de monitorear las plataformas, el menester de saber que usuarios usan los datos y cómo los están usando. En este caso en particular monitorear el horario en que los usuarios ingresan a las plataformas del banco.

Las alertas que se analizarán serán de anomalías de comportamiento, como son las de un usuario que está realizando algo no permitido o que normalmente no hace, como por ejemplo descargar más cantidad de archivos de gran volumen de lo que usualmente hace, etc.

Para podernos apoyar sobre la identificación de estos eventos nos apoyaremos en herramientas de seguridad de accesos. Hoy en día acordé a Netskope “la tecnología CASB se está transformando en algo de mucho mayor alcance. Si se combina con otras tecnologías como la prevención de pérdida de datos (DLP) y Next Generation Secure Web Gateway, el concepto de CASB se está convirtiendo en una pieza única”. Bajo este criterio seleccionamos como Fuente de este caso la herramienta CASB.

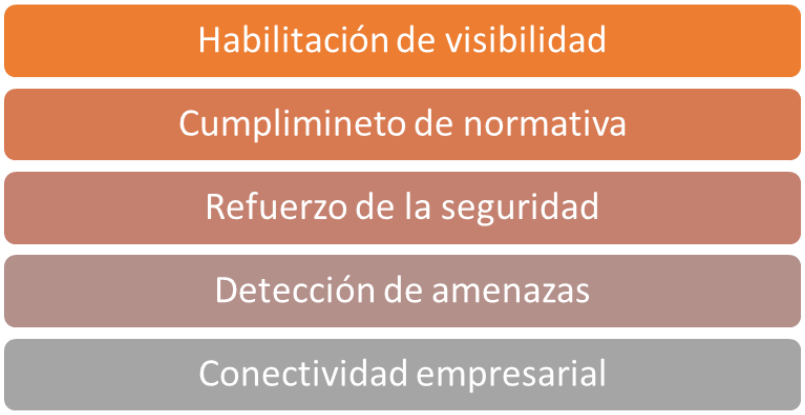
Acorde a la definición de Gartner, un agente de seguridad de acceso a la nube (CASB) es un punto de imposición de políticas de seguridad, ya sea en las instalaciones físicas o en la nube, situado entre los consumidores de servicios en la nube y los proveedores de servicios en la nube, cuyo propósito es combinar e interponer políticas de seguridad corporativas cuando se acceda a los recursos en la nube. El CASB es como un

policía que obliga a cumplir las leyes establecidas por los administradores del servicio en la nube.

- **Fundamentos de CASB:** Se pueden definir como los fundamentos principales de las plataformas CASB como los siguientes:

Figura 10.

Visualización del evento en la plataforma CyberArk.



Un CASB permite realizar un inventario exhaustivo del entorno de cloud y revelar los componentes que hasta ahora no se habían mapeado. De igual manera permite aplicar un conjunto estandarizado de normas de cumplimiento en todos sus componentes de la nube, refuerza la seguridad enfocada principalmente en el mapeo del uso de servicios en la nube, identificando anomalías y signos de vulnerabilidades, temas como límite de exposición de datos y de igual manera gestión de privilegios de usuarios. Finalmente permite la integración de las instituciones financieras al conectar los distintos elementos del core y de las instalaciones con los componentes circundantes de la nube. El tráfico puede pasar hacia y desde la nube, ya que el broker de seguridad de acceso a la nube permite la integración bidireccional con el core.

- **Arquitectura de CASB:** La implementación del agente de seguridad de acceso a la nube se basa en 10 componentes:
    - Core empresarial inmediato: Todos los componentes de la infraestructura informática en el campus principal de la institución
    - Core empresarial secundario: Los componentes que técnicamente son propiedad de la institución pero que operan desde una ubicación remota
    - Platform as a service (PaaS): Permite a las instituciones desarrollar y ejecutar aplicaciones sin interactuar con las instalaciones de la empresa.
    - Infrastructure as a Service (IaaS): Se refiere a los componentes de la nube que replican los equipos locales, como los dispositivos de almacenamiento y los aparatos de red, en la nube.
    - Software as a service (Saas): Se refiere a todas las aplicaciones basadas en la nube desplegadas por los usuarios de la institución, que podrían estar alojadas en muchos entornos de nube.
    - Gateway de conectividad: Permite a los usuarios establecer conexiones entre el núcleo de la institución y los diferentes componentes de la nube.
    - Normas de seguridad y cumplimiento: Puede tener reglas preconfiguradas, como un conjunto de usuarios en la lista negra y en la lista blanca que pueden acceder a un determinado servicio en la nube. De igual forma puede tener reglas dinámicas que se refieren a las reglas empresariales que utilizan datos contextuales para permitir o denegar el acceso

- Integración bidireccional: Permite el flujo de datos bidireccional y seguro entre la institución y la nube
- Tráfico: Es el componente que el broker de seguridad de acceso a la nube pretende mediar.
- Análisis de uso de la nube: Las perspectivas analíticas están disponibles a través de la interfaz de administración del agente de seguridad de acceso a la nube, y mantienen a los administradores de TI informados sobre el estado del panorama de la nube.

Para la selección de la marca que proporcione la fuente de información hemos revisado de igual manera el cuadrante de Gartner del 2002 de Security Service Edge (SSE), ya que, según la definición de Gartner, el SSE es una pila en evolución de diferentes herramientas de seguridad basadas en la nube, que incluyen CASB, Web Security Gateway, Zero Trust Network Access, etc.:

Figura 11.

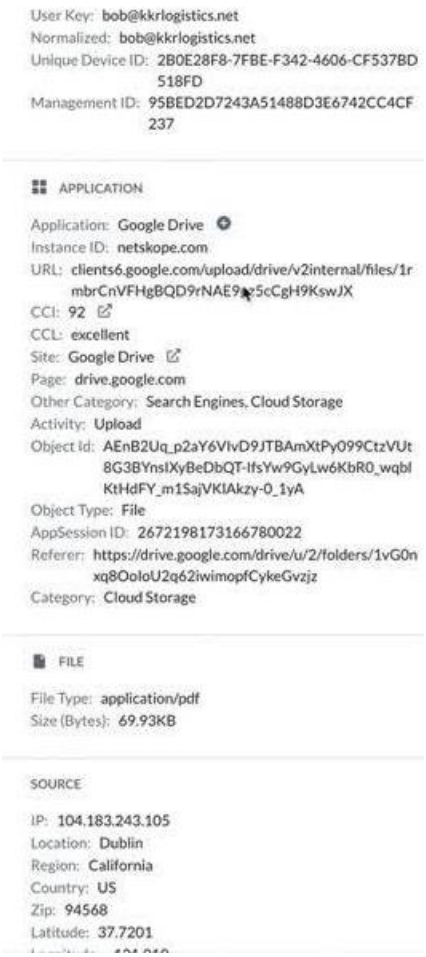
Cuadrante de Gartner 2022 marcas sobre herramientas SSE.

Con ello hemos definido para la obtención de fuentes como mejor opción a Netskope y su solución de CASB. Con Netskope CASB, ya que es un componente central de Netskope Intelligent Security Service (SSE), adoptando aplicaciones y servicios en la nube, sin sacrificar la seguridad. Gestiona el movimiento involuntario o no aprobado de datos sensibles entre instancias de aplicaciones en la nube y en el contexto del riesgo de las aplicaciones y del usuario con la solución de seguridad en la nube.

Con este contexto podemos controlar el acceso de usuarios a componentes de la plataforma de las instituciones en base al registro de control y acceso.

Figura 12.

Ejemplo de logs sobre Netskope CASB.



Caso de Uso 4. Detección de malware a través de un firewall perimetral

Conceptualización de Firewall o Cortafuegos

"Los cortafuegos (firewalls) son sistemas de seguridad que controlan el tráfico de red mediante reglas preestablecidas" (Neupane, Haddad & Chen, 2018). De este modo para la detección de malware, el uso de firewall o cortafuegos representa una solución óptima al momento de utilizar las prestaciones de herramientas SIEM, pues lo ideal es incrementar la seguridad dentro de las redes institucionales para afianzar la integridad de los datos de la empresa.

Tipos de Firewall

De acuerdo a (Forcepoint), determina a cuatro tipos de firewalls: Next-generation firewalls (NGFW), Proxy Firewalls, Network address translation (NAT) y Stateful multilayer inspection (SMLI). Para el primer tipo se definen como aquellos cortafuegos que combinan la tecnología de firewall tradicional con funciones adicionales, como inspección de tráfico encriptado, sistemas de prevención de intrusiones, antivirus y más. Para el segundo grupo, en cuanto a proxy firewalls son aquellos que ayudan a filtrar el tráfico de red a nivel de aplicación.

A diferencia de los firewalls básicos, el proxy actúa como intermediario entre dos sistemas finales. Como tercer grupo, tenemos a los cortafuegos NAT, mismos que se conceptualizan como sistemas que permiten a múltiples dispositivos con direcciones de red independientes se conecten a Internet usando una sola dirección IP, manteniendo ocultas las direcciones IP individuales. Como punto final disponemos de los cortafuegos SMLI los cuales filtran paquetes en las capas de red, transporte y aplicación, comparándolos con paquetes confiables conocidos.

Cuadrante de Gartner en Firewalls año vigente

Según lo establecido por (Gartner, 2022), definió a Palo Alto como el mejor puntuado para los casos de Nube Pública y Perímetro Empresarial. Por tanto, tomando de referencia lo comunicado por Gartner, las recomendaciones se orientarán al uso de este firewall perimetral.

De modo que, uno de los casos de uso presentado con mayor resistencia en el sector financiero es la detección de vulnerabilidad que intente comprometer a la

información empresarial con la posible inserción de un tipo de malware de la empresa como, por ejemplo: Ransomware, spyware, gusanos, adware, troyanos o botnets.

De acuerdo a (Belcic, 2022) menciona que, en la mayoría de los casos de infección detectados en dispositivos, el malware es muy complicado de observar debido a que trabajan en segundo plano, por lo que para detectarlo en máquinas infectadas se necesita de un software especializado. Además, el incentivo con mayor predominancia para los cibercriminales es provocar frustración y contratiempos a sus víctimas.

Al tratarse de una vulnerabilidad empresarial, se sujeta la opción de configuración de firewall desde una seguridad informática perimetral. (Accensit, 2017) detalla a la seguridad informática perimetral como una primera línea de defensa parecidas a las alarmas de una oficina o establecimiento en las que si detectan un movimiento sospechoso activa los medios de contingencia. Por tanto, las prestaciones de un sistema de defensa perimetral ofrecen al sector financiero una menor probabilidad de infección con los distintos tipos de malware mencionados anteriormente en este apartado.

De acuerdo al portal web (Nunsys), describe los beneficios de configurar un firewall de seguridad perimetral como lo son: Protección ante ataques de denegación de servicio (DoS), Seguridad ante intrusión y sustracción de credenciales, Accesos seguros desde equipos externos, entre otros. No obstante, las habilidades de los cibercriminales ponen en alerta a todo sistema de información, puesto a que los intentos por vulnerar las protecciones de seguridad informática generan un peligro para la empresa.

Como recomendación ante la configuración de un firewall perimetral de frente a una vulnerabilidad se encuentran las siguientes opciones: bloqueo de puertos, antispam en correos institucionales, servicios de detección y prevención (IDP).

Caso de Uso 5. Detección de Ransomware en ordenadores corporativos.

El Ransomware es un tipo de software malicioso (malware) que amenaza con publicar o bloquear el acceso a los datos o a un sistema informático, generalmente cifrándolos, hasta que la víctima paga una tarifa de rescate al atacante. En muchos casos, la demanda de rescate viene con una fecha límite. Si la víctima no paga a tiempo, los datos desaparecen para siempre o el rescate aumenta.

Los ataques de Ransomware son muy comunes en estos días. Las principales empresas de del mundo han sido víctimas de ello, entre ellas varias del sector financiero. Los ciberdelincuentes atacarán a cualquier consumidor o cualquier negocio y las víctimas provienen de todas las industrias.

Cualquier dispositivo conectado a Internet corre el riesgo de convertirse en la próxima víctima de Ransomware. El Ransomware escanea un dispositivo local y cualquier almacenamiento conectado a la red, lo que significa que un dispositivo vulnerable también convierte a la red local en una víctima potencial. Si la red local es una empresa, el Ransomware podría cifrar documentos importantes y archivos del sistema que podrían detener los servicios y la productividad.

Si un dispositivo se conecta a Internet, debe actualizarse con los parches de seguridad de software más recientes y debe tener instalado un antimalware que detecte y

detenga el Ransomware. Los sistemas operativos obsoletos, que ya no reciben mantenimiento, corren un riesgo mucho mayor.

Varias agencias gubernamentales, incluido el FBI, desaconsejan pagar el rescate para evitar fomentar el ciclo del Ransomware. Además, es probable que la mitad de las víctimas que pagan el rescate sufran ataques repetidos de Ransomware, especialmente si no se limpia del sistema.

Para obtener esta información los eventos se pueden tomar desde un XDR.

XDR: Acorde a (Gartner) define a XDR como "una herramienta de detección de amenazas de seguridad y respuesta a incidentes basada en SaaS y específica para cada proveedor, que integra de forma nativa varios productos de seguridad en un sistema de operaciones de seguridad cohesionado"

La definición de XDR de (Forrester Research) es un poco más amplia: "La evolución de EDR, que optimiza la detección, investigación, respuesta y caza de amenazas en tiempo real. La XDR unifica las detecciones de puntos finales relevantes para la seguridad con la telemetría de las herramientas de seguridad y empresariales, como el análisis y la visibilidad de la red (NAV), la seguridad del correo electrónico, la gestión de la identidad y el acceso, la seguridad en la nube, etc.

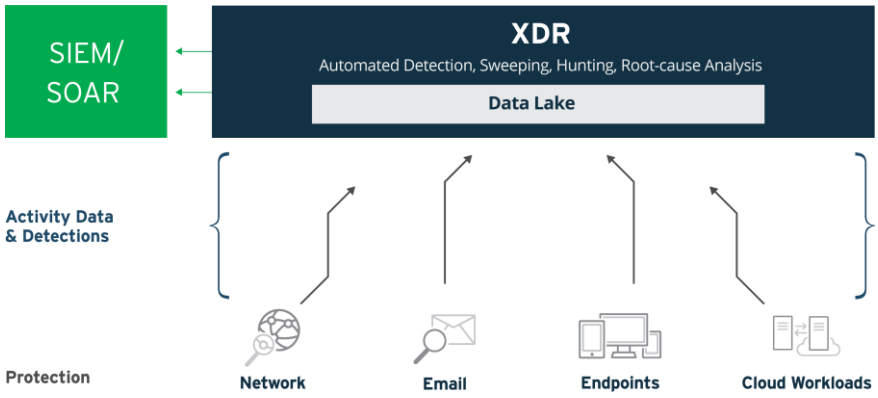
Es una plataforma nativa de la nube construida sobre una infraestructura de big data para proporcionar a los equipos de seguridad flexibilidad, escalabilidad y oportunidades de automatización."

- **Arquitectura General XDR:**

Los equipos de TI y de seguridad se ven a menudo desbordados por las alertas procedentes de diferentes soluciones. Una empresa con una media de 1.000 empleados puede ver cómo entran en su sistema de gestión de eventos e información de seguridad (SIEM) un pico de hasta 22.000 eventos por segundo. Esto supone casi 2 millones de eventos en un día. XDR vincula automáticamente una serie de actividades de menor confianza en un evento de mayor confianza, haciendo aflorar menos alertas y más prioritarias para la acción. Esto ayuda significativamente para no genera ruido sobre cualquier caso de uso seleccionado.

Figura 13.

Ejemplo de Arquitectura General XDR.



Ante los numerosos registros y alertas, pero sin indicadores claros, es difícil saber qué buscar. Si se encuentra un problema o una amenaza, es difícil trazar su trayectoria y su impacto en toda la organización. Las plataformas Extended detection and response automatizan las investigaciones de las amenazas eliminando los pasos manuales y proporcionando datos y herramientas para el análisis que de otro modo sería demasiado complicado.

Un analista puede ver claramente la línea de tiempo y la ruta de ataque que puede atravesar el correo electrónico, los puntos finales, los servidores, las cargas de trabajo en la nube y las redes. El analista puede ahora evaluar cada paso del ataque para poner en marcha la respuesta necesaria.

El esquema de trabajo de un XDR se puede detallar de la siguiente manera:

1. XDR recopila datos de varios puntos de seguridad, como endpoints, redes, servidores y la nube. Tras la agregación de datos, realiza un análisis de los mismos para correlacionar el contexto de las distintas alertas que se generan. Esto evita que los equipos de seguridad tengan que lidiar con grandes volúmenes de alertas de seguridad y les permite concentrarse en las señales o alertas de alta prioridad.
2. Genera visibilidad de la infraestructura de TI de la institución. Esto permite al sistema examinar las señales de cualquier amenaza detectada e informar de las críticas que requieren una respuesta. El factor de visibilidad también permite a las empresas profundizar en el comportamiento anormal de las amenazas e investigar sus orígenes antes de que afecten a otras partes del sistema.
3. XDR contiene y elimina principalmente las amenazas detectadas, posteriormente, actualiza las políticas de seguridad para garantizar que no vuelva a producirse un incidente similar en un futuro próximo.

Figura 14.

Ejemplo de Proceso XDR

Para la selección de la marca que proporcione la fuente de logs hemos seleccionado una de las líderes actuales que es TrendMicro.

Acorde a (TrendMicro) “XDR recopila datos de actividad profunda y suministra esa información a un data lake para lograr un rastreo, búsqueda e investigación extendidas a través de las capas de seguridad.

La aplicación de IA y análisis especializados para enriquecer el conjunto de datos produce menos alertas y con más contexto, lo que se puede enviar a una solución SIEM de la empresa. XDR no reemplaza la SIEM, sino que la mejora reduciendo el tiempo que los analistas de seguridad necesitan para evaluar alertas y registros relevantes y decidir qué es lo que necesita atención y merece mayor investigación.”

Figura 15.

Ejemplo de Logs XDR TrendMicro

Capítulo 3

Análisis de resultados

Una vez definidos y limitados los requisitos para cada caso de uso, se identifican las siguientes tareas a seguir dentro del proceso de manejo de casos de uso:

Flujo de Implementación de Casos de Uso:

Secure Soft emplea dentro de su departamento de Consultoría de Seguridad el siguiente flujo para implementar diferentes casos de uso para el análisis de eventos a sus plataformas SIEM administradas:

- Se recepta la solicitud del cliente sobre el caso de uso requerido, con ello se valida el alcance del mismo.
- Se valida si dicho caso se encuentra dentro de los pre definidos, en este punto es donde se proponen los casos de uso desarrollados, principalmente si el cliente es una institución financiera, si el caso se acopla al requerimiento pasa a su diseño y propuesta directo.
- Si el caso requerido no se acopla a los pre definidos se procede al análisis de las fuentes, documentación y reportes de eventos proporcionados para su revisión. Esto además permite en el proceso de validación identificar si existe una cantidad excesiva de logs, se solicita al cliente efectuar un afinamiento en su fuente para que llegue menor información de logs y más específica.
- Con esto afinado puede ser enviado al procedo de diseño del caso de uso.
- En este punto sea con caso de uso pre existente o nuevo, pasa a la aprobación del cliente o cambios en el diseño de ser necesario

- Una vez aprobado el caso en su totalidad este pasa a producción en el SIEM y queda en proceso para generar alertas al equipo de análisis y monitoreo de eventos, efectuando la retroalimentación correspondiente del proceso e implementación, así como de alertas de seguridad que emita el caso
- Con el envío de eventos y la retroalimentación por parte del cliente, se valida o no el afinamiento respectivo, esto principalmente para los casos de uso pre definidos que entran en el diseño e implementación de manera directa. Con ello se re configuran las reglas del caso de ser necesario y el proceso finaliza con el caso de uso implementado.

Caso de uso 1, Acceso a las cuentas privilegiadas protegidas en horas irregulares.

- **Objetivo**

Detectar los relacionados a las actividades efectuadas con cuentas privilegiadas protegidas sobre una bóveda digital realizadas en horas irregulares.

- **Alcance**

Detección de recuperación y utilización de cuentas privilegiadas a equipos en horas irregulares de usuarios finales.

- **Fuentes de Eventos**
    - CyberArk Privileged Threat Analytics (PTA)

- **Tipos de datos**

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Tabla 1
Tipos de Datos

Plataforma	***Tipo de Log***
PTA	Eventos sobre actividades sospechosas relacionadas con la recuperación de cuentas privilegiadas en horas irregulares de dicho usuario

- **Flujo Lógico**

Se arrojará una alerta cuando se detecte el event type ID 23 sobre el control de uso o recuperación de credenciales de cuentas privilegiadas en horas irregulares de un usuario específico.

- **Notificación**

Las notificaciones de las alertas serán enviadas a la cuenta operador@cliente.com.

La notificación se realizará de acuerdo con el formato estándar definido por cliente.

- **Severidad**

Tabla 2
Severidad

Alerta/Reporte	***Severidad***
Privileged access to the Vault during irregular hours	Media

- **Recomendación**

Implementar sobre la plataforma PAM de CyberArk un flujo de control y aprobación de accesos y utilización de cuentas para el control correspondiente de su uso en tiempos de uso reportados por los usuarios finales.

Caso de uso 2. Exfiltración de Datos.

- **Objetivo**

Detectar actividad potencialmente asociada a exfiltración de Datos en navegación web, activación de firmas y correos salientes. Entendemos como exfiltración a la fuga de información de la red tecnológica del cliente.

- **Alcance**

Este caso de uso tiene el siguiente alcance:

  - Navegación web categorizada como Bandwidth y Peer to Peer.
  - Correos salientes con adjuntos asociados a palabras clave de exfiltración.

- **Fuentes de Eventos**
  - Proxy Websense
  - Antispam

- **Tipos de datos**

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Tabla 3
Tipos de Datos

Plataforma	***Tipo de Log***
Proxy Websense	Eventos de navegación asociados a las categorías de Almacenamiento de red personal y Peer-to-Peer File Sharing
Antispam	Eventos de correos salientes con archivos adjuntos dirigidos a un correo no relacionado con la organización

- **Flujo Lógico**
    - Se arrojará una alerta cuando se detecte que un usuario se conectó una página potencialmente asociada a exfiltración de Datos y su consumo total durante la conexión de la sesión sea mayor a 20 MB.
    - Se generará un reporte semanal con el top 20 de usuarios que se conectaron a páginas potencialmente asociadas a exfiltración de Datos con el respectivo consumo de Datos.
    - Se arrojará un reporte cuando se detecte un correo saliente a un correo no relacionado con el banco y que el nombre del adjunto haga match con las palabras: “cliente”, “cuenta corriente”, “Cuenta de ahorro” o “Nomina Contraseña”.

- **Notificación**

Las notificaciones de las alertas serán enviadas a la cuenta operador@cliente.com

La notificación se realizará de acuerdo con el formato estándar definido por cliente.

- **Severidad**

Tabla 4
Severidad

Alerta/Reporte	***Severidad***
Almacenamiento de red personal	Media
Peer-to-Peer File Sharing	Media
Correo con contenido de la organización	Media

- **Recomendación**

Implementar una herramienta de análisis de comportamiento de usuarios, lo cual hará que los falsos positivos disminuyan y que únicamente se alerten los casos inusuales o sospechosos.

Caso de Uso 3. Ingreso a plataformas corporativas de manera irregular.

- **Objetivo**

Detectar las conexiones inusuales mediante el monitoreo a través de componentes de control de acceso en la nube.

- **Alcance**

Este caso de uso tiene el siguiente alcance:

- Identificar patrones de logueo de usuarios para determinar actividades sospechosas.
- Identificar cambios en permisos y creación de superusuarios.

- **Fuentes de Eventos**
    - Netskope Cloud Log Shipper
- **Tipos de datos**

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Tabla 5
Tipos de Datos

Plataforma	***Tipo de Log***
Log Shipper	Eventos hora, cantidad y patrón en cuanto a logueos de los usuarios del sistema
Log Shipper	Eventos de interacción o eliminación de archivos que normalmente no usa y/o a deshoras

- **Flujo Lógico**
    - Se generan reportes diarios automáticos que originados por el logueo de una cuenta en el sistema. donde se encuentra toda la descripción de las anomalías con los siguientes detalles: usuario, Host remoto, IP remota, dominio, host name, tipo de logueo, ID del evento, hora y la descripción del caso anormal.
    - Se disparará una alerta al mail del operador@cliente.com cuando la herramienta detecte que se realizó un logueo de una cuenta que ingrese al sistema en un horario inusual en comparación a lo que CASB tiene

registrado como normal según su historial personal o la configuración de horario realizada por el cliente.

- **Notificación**

Las notificaciones de las alertas serán enviadas a una cuenta que incluye todos los mails de los administradores y personal de IT.

Los reportes diarios llegarán a la cuenta de correo operador@cliente.com o también se podrán revisar dentro de la herramienta.

La notificación se realizará de acuerdo con el formato estándar definido por cliente.

- **Severidad**

Tabla 6
Severidad

Alerta/Reporte	***Severidad***
Logueo a FTP	Media
Logueo a SSH Unix	Crítica
Logueo SU Unix	Crítica
Logueo FTP SFTP Unix	Media
Logueo a Windows	Media

- **Recomendación**

Entender que UEBA empieza a trabajar mejor alrededor de quince días a un mes después de haber sido instalada ya que por su tecnología de machine learning tarda un tiempo en aprender el comportamiento de los perfiles de usuarios y sus diferentes características y horarios.

Aprovechar lo amigable de la herramienta y realizar alertas personalizadas de login, según plataformas, aplicaciones, dispositivos y/o perfiles conforme vayan apareciendo las necesidades de seguridad de la empresa.

Caso de Uso 4. Detección de malware a través de un firewall perimetral

- **Objetivo**

Detectar los tipos de malware a través del firewall perimetral

- **Alcance**

Este caso de uso tiene el siguiente alcance:

- Protección ante ataques de denegación de servicios (DoS)
- Accesos seguros desde equipos externos e internos
- Seguridad ante intrusión y sustracción de credenciales
- Bloqueo de puertos ante actividad sospechosa

- **Fuentes de Eventos**
    - IDP (Servicio de Detección y Prevención)
    - Antispam

- **Tipos de datos**

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Tabla 7
Tipos de Datos

Plataforma	***Tipo de Log***
Bloqueo de puertos	Eventos de bloqueo de puertos ante una actividad sospechosa.
Antispam	Eventos de correos entrantes con archivos adjuntos mediante phishing.

- **Flujo Lógico**
    - Se activará una alerta cuando se detecte que un tráfico o trama de red pretenda vulnerar un puerto.
    - Se activará una alerta cuando se detecte un evento con una firma asociados a las categorías de Ataques hacia aplicativos del sector financiero

- **Notificación**

Las notificaciones de las alertas serán enviadas a la cuenta operador@cliente.com.

La notificación se realizará de acuerdo con el formato estándar definido por cliente.

- **Severidad**

Tabla 8
Severidad

Alerta/Reporte	***Severidad***
Intrusión de puertos	Alta
Denegación de servicios (DoS)	Alta
Correo con malware	Alta

- **Recomendación**

Implementar un firewall perimetral para la protección de puertos, denegación de servicios y ataques phishing.

Caso de Uso 5. Detección de Ransomware en ordenadores corporativos.

- **Objetivo**

Detectar los ataques de tipo Ransomware en ordenadores identificados como parte de la empresa.

- **Alcance**

Este caso de uso tiene el siguiente alcance:

- Protección ante ataques de Ransomware.

- **Fuentes de Eventos**
    - Antispam
    - Trend Micro Vision One
- **Tipos de datos**

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Tabla 9
Tipos de Datos

Plataforma	***Tipo de Log***
Vision One	Eventos de prevención de intrusiones
Vision One	Eventos Antimalware
Vision One	Logs de monitoreo de comportamiento

- **Flujo Lógico**

Se activará una alerta cuando se detecte un evento de IPS y antimalware

- **Notificación**

Las notificaciones de las alertas serán enviadas a la cuenta operador@cliente.com.

La notificación se realizará de acuerdo con el formato estándar definido por cliente.

- **Severidad**

Tabla 10
Severidad

Alerta/Reporte	***Severidad***
IPS	Alta
Antmalware	Alta

- **Recomendación**

Implementación de plataforma XDR para una gestión de detección y respuesta extendida efectiva.

Capítulo 4

Conclusiones

- La definición correcta de un caso de uso desarrolla procesos de gestión de incidentes de ciberseguridad para mitigarlos, eliminarlos y prevenirlos.
- Para concluir en cuanto a la implementación de firewall perimetral, es evidente el hecho de que la información empresarial siempre se encontrará en riesgo por la cantidad evolutiva e incremental de los malware, que si bien pueden introducirse a los distintos sistemas de información con técnicas de ciberdelincuencia. Por lo que, el uso e implementación de firewall para bloquear de raíz esta problemática se considera como una opción viable de protección de datos.
- Podemos comparar el uso del SIEM contra UEBA, pero mientras el primero es un gran sistema que incluye gestión de eventos, patrones y tendencias que gatillan las alarmas cuando encuentran algo anómalo, UEBA tiene el mismo comportamiento, pero refleja sus eventos anómalos en función del comportamiento del usuario y el machine learning. El uso combinado de estos dos grupos de tecnologías viene a ser una de las mejores prácticas en la ciberseguridad actual.

Recomendaciones

- Se recomienda que para la implementación de firewall perimetral dentro del sector financiero se considere el cuadrante de Gartner del año vigente especificado al cortafuegos mejor puntuado a la categoría de perímetro empresarial.
- Se debe considerar todas las alternativas de configuración que presenta la tecnología UEBA para personalizar alarmas de acuerdo al comportamiento aprendido a través del machine learning de UEBA.

Lista de referencias

Abrisqueta Sánchez, U. (2021). Diseño, despliegue e inteligencia de una herramienta SIEM. Obtenido de https://addi.ehu.es/bitstream/handle/10810/53944/Abrisqueta_TFM.pdf?sequence=2&isAllowed=y

Accensit.com. (2017). Seguridad perimetral informática: Información necesaria. Obtenido de https://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/

Belcic, I. (2022). Avast. Obtenido de https://www.avast.com/es-es/c-phishing

Blokdyk, G. (2018). SIEM and UEBA A Clear and Concise Reference. 5STARCooks.

Forcepoint. (s.f.). What is a Firewall? Obtenido de https://www.forcepoint.com/cyber-edu/firewall

Gartner. (2022). Network Firewalls Reviews and Ratings. Obtenido de https://www.gartner.com/reviews/market/network-firewalls

IBM. (09 de 03 de 2021). Engineering Lifecycle Management. Obtenido de https://www.ibm.com/docs/es/elm/6.0.3?topic=requirements-defining-use-cases

Khanna, S. (2021). Using Color To Identify Insider Threats Obtenido de https://arxiv.org/pdf/2111.13176.pdf

Lukashin, A., Popov, M., Bolshakov, A., & Nikolashin, Y. (2019, October). Scalable data processing approach and anomaly detection method for user and entity behavior analytics platform. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-32258-8_40

Navarro, T. S., & Guerrero, A. G. (2022). El SOC “Autónomo”: Inteligencia Artificial para la nueva ciberseguridad. Obtenido de https://revista.uclm.es/index.php/ruiderae/article/view/3088

Netskope (s.f.). Netskope Cloud Access Security Broker (CASB). Obtenido de https://www.netskope.com/resources/data-sheets/netskope-cloud-access-security-broker-casb

Neupane, K., Haddad, R., & Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. SoutheastCon, 1-6.

Nunsys. (s.f.). FIREWALL DE SEGURIDAD PERIMETRAL. Obtenido de https://www.nunsys.com/producto-seguridad-perimetral-firewall/

MADEJA. (2009). Guía para la redacción de casos de uso. Obtenido de https://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/416

Mediavilla, E. (s.f.). II MODELOS y HERRAMIENTAS. Obtenido de II.2 UML: Modelado de casos de uso: https://www.ctr.unican.es/asignaturas/mc_oo/doc/casos_de_uso.pdf

Mohanakrishnan, Ramya. (30 de agosto de 2021). What Is Privileged Access Management (PAM)? Definition, Components, and Best Practices. Obtenido de https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-privileged-acces-management/

Pérez Robles, Á. (2022). Gestión de incidentes de ciberseguridad. Aplicaciones prácticas en un SOC. Obtenido de https://oa.upm.es/cgi/users/login?target=https%3A%2F%2Foa.upm.es%2F71115%2F1%2FTFG_ALVARO_PEREZ_ROBLES.pdf

Schwab, C. (2016). User and Entity Behavior Analytics for Enterprise Security. Obtenido de http://shashanka.net/stuff/shashanka_BigData2016.pdf

Trend Micro (s.f). Qué es XDR? Obtenido de https://www.trendmicro.com/es_es/what-is/xdr.html

Vega, M. (2010). Casos de uso UML. Obtenido de https://lsi2.ugr.es/~mvega/docis/casos%20de%20uso.pdf

Vilcarromero Zubiate, L. L., & Vilchez Linares, E. (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. Obtenido de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624832/VilcarromeroZ_L.pdf?sequence=11&isAllowed=y

Apéndice

Plantilla de Caso de Uso 1

Acceso a las cuentas privilegiadas protegidas en horas irregulares

Control de cambios

Fecha Actualización	Realizado por	Autorizado por	Naturaleza del Cambio
Corresponde a la fecha de elaboración / fecha de modificación del documento	Oficial responsable de la elaboración / personal del proveedor encargado de la elaboración cuando aplique	Línea de supervisión de ROT, la autorización se adjunta vía mail	Breve descripción del cambio ejecutado, en el caso en que el documento sea nuevo no se requiere descripción

CONTENIDO

OBJETIVO

Detectar los relacionados a las actividades efectuadas con cuentas privilegiadas protegidas sobre una bóveda digital realizadas en horas irregulares.

ALCANCE

Este caso de uso tiene el siguiente alcance:

- Detección de recuperación y utilización de cuentas privilegiadas a equipos en horas irregulares de usuarios finales.

FUENTES DE EVENTOS

- CyberArk Privileged Threat Analytics (PTA)

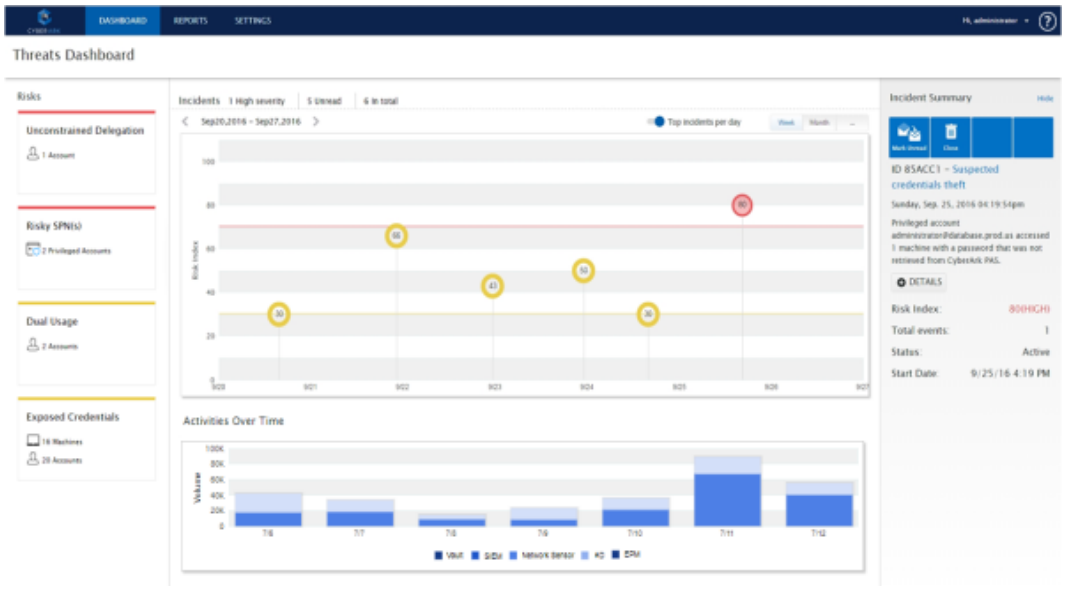


Imagen 1: Eventos recolectados de la **fuente de eventos** PTA de CyberArk.

TIPO DE DATOS

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Plataforma	Tipo de log
PTA	Eventos sobre actividades sospechosas relacionadas con la recuperación de cuentas privilegiadas en horas irregulares de dicho usuario

FLUJO LÓGICO

- Se gatillará una alerta cuando se detecte el event type ID 23 sobre el control de uso o recuperación de credenciales de cuentas privilegiadas en horas irregulares de un usuario específico.

NOTIFICACIÓN

- Las notificaciones de las alertas serán enviadas a la cuenta xxxxx@domain.com.
- La notificación se realizará de acuerdo con el formato estándar definido por cliente (Ver sección de anexos).

SEVERIDAD

Alerta/Reporte	Severidad
Por definir en taller	Alta/Media/Baja

RECOMENDACIÓN

- Implementar sobre la plataforma PAM de CyberArk un flujo de control y aprobación de accesos y utilización de cuentas para el control correspondiente de su uso en tiempos de uso reportados por los usuarios finales.

Plantilla de Caso de Uso 2

Exfiltración de Datos

Control de Cambios

Fecha Actualización	Realizado por	Autorizado por	Naturaleza del Cambio
Corresponde a la fecha de elaboración / fecha de modificación del documento	Oficial responsable de la elaboración / personal del proveedor encargado de la elaboración cuando aplique	Línea de supervisión de ROT, la autorización se adjunta vía mail	Breve descripción del cambio ejecutado, en el caso en que el documento sea nuevo no se requiere descripción

CONTENIDO

OBJETIVO

Detectar actividad potencialmente asociada a exfiltración de Datos en navegación web, activación de firmas y correos salientes. Entendemos como exfiltración a la fuga de información de la red tecnológica del Cliente

ALCANCE

Este caso de uso tiene el siguiente alcance:

- Navegación web categorizada como Bandwidth y Peer to Peer.
- Correos salientes con adjuntos asociados a palabras clave de exfiltración.

FUENTES DE EVENTOS

- Proxy Websense
- Antispam

TIPO DE DATOS

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Plataforma	Tipo de log
Proxy Websense	Eventos de navegación asociados a las categorías de Almacenamiento de red personal y Peer-to-Peer File Sharing
Antispam	Eventos de correos salientes con archivos adjuntos dirigidos a un correo no relacionado con la organización

FLUJO LÓGICO

- Se arrojará una alerta cuando se detecte que un usuario se conectó una página potencialmente asociada a exfiltración de Datos y su consumo total durante la conexión de la sesión sea mayor a 20 MB.

- Se generará un reporte semanal con el top 20 de usuarios que se conectan a páginas potencialmente asociadas a exfiltración de Datos con el respectivo consumo de Datos.
- Se arrojará un reporte cuando se detecte un correo saliente a un correo no relacionado con el banco y que el nombre del adjunto haga match con las palabras: “cliente”, “cuenta corriente”, “Cuenta de ahorro” o “Nómina Contraseña”.

NOTIFICACIÓN

- Las notificaciones de las alertas serán enviadas a la cuenta xxxxx@domain.com.
- La notificación se realizará de acuerdo con el formato estándar definido por cliente
-

SEVERIDAD

Alerta/Reporte	**Severidad**
Almacenamiento de red personal	Media
Peer-to-Peer File Sharing	Media
Correo con contenido de la organización	Media

RECOMENDACIÓN

- Implementar una herramienta de análisis de comportamiento de usuarios, lo cual hará que los falsos positivos disminuyan y que únicamente se alerten los casos inusuales o sospechosos.

Plantilla de Caso de Uso 3

Ingreso a plataformas corporativas de manera irregular

Control de Cambios

Fecha Actualización	Realizado por	Autorizado por	Naturaleza del Cambio
Corresponde a la fecha de elaboración / fecha de modificación del documento	Oficial responsable de la elaboración / personal del proveedor encargado de la elaboración cuando aplique	Línea de supervisión de ROT, la autorización se adjunta vía mail	Breve descripción del cambio ejecutado, en el caso en que el documento sea nuevo no se requiere descripción

CONTENIDO

OBJETIVO

Detectar logueos usuales e inusuales mediante el monitoreo de redes y dispositivos en la nube.

ALCANCE

Este caso de uso tiene el siguiente alcance:

- Identificar patrones de logueo de usuarios para determinar actividades sospechosas.

- Identificar cambios en permisos y creación de superusuarios.

FUENTES DE EVENTOS

- Netskope Cloud Log Shipper

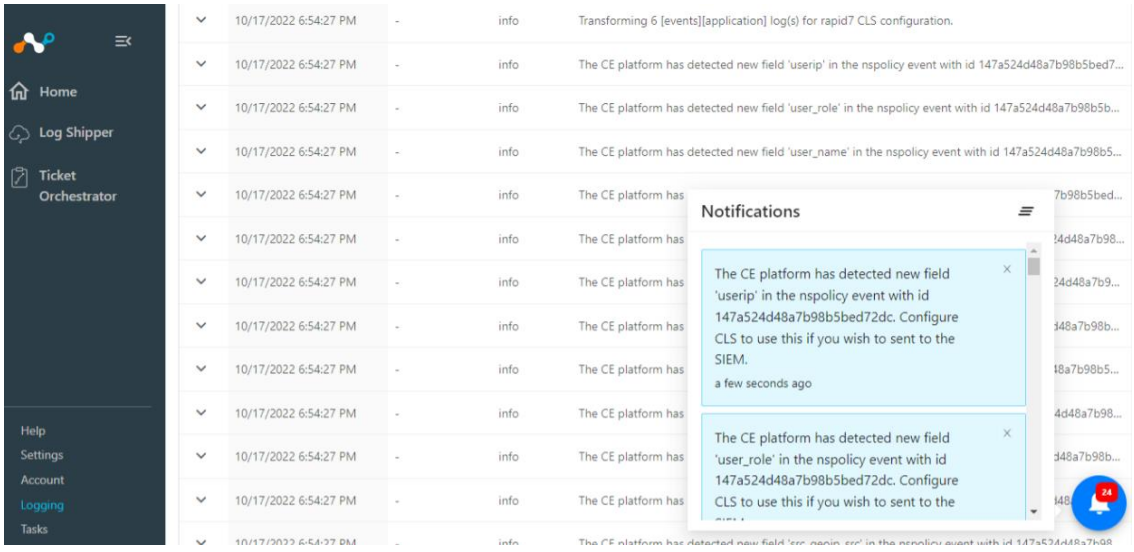


Imagen 1: Eventos recolectados de la herramienta

TIPO DE DATOS

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Plataforma	Tipo de log
Log Shipper	Eventos hora, cantidad y patrón en cuanto a logueos de los usuarios del sistema
Log Shipper	Eventos de interacción o eliminación de archivos que normalmente no usa y/o a deshoras.

FLUJO LÓGICO

- Se generan reportes diarios automáticos que originados por el logueo de una cuenta en el sistema. donde se encuentra toda la descripción de las anomalías con los siguientes detalles: usuario, Host remoto, IP remota, dominio, host name, tipo de logueo, ID del evento, hora y la descripción del caso anormal.
- Se disparará una alerta al mail del operador@cliente.com cuando la herramienta detecte que se realizó un logueo de una cuenta que ingrese al sistema en un horario inusual en comparación a lo que CASB tiene registrado como normal según su historial personal o la configuración de horario realizada por el cliente.

NOTIFICACIÓN

- Las notificaciones de las alertas serán enviadas a una cuenta que incluye todos los mails de los administradores y personal de IT.
- La notificación se realizará de acuerdo con el formato estándar definido por CLIENTE.
- Los reportes diarios llegarán a la cuenta de correo operador@cliente.com o también se podrán revisar dentro de la herramienta.

- Las notificaciones de las alertas serán enviadas a la cuenta operador@cliente.com

- La notificación se realizará de acuerdo con el formato estándar definido por cliente.

SEVERIDAD

Alerta/Reporte	**Severidad**
Logueo a FTP	Media
Logueo a SSH Unix	Crítica
Logueo SU Unix	Crítica
Logueo FTP SFTP Unix	Media
Logueo a Windows	Media

RECOMENDACIÓN

- Entender que CASB empieza a trabajar mejor alrededor de un mes después de haber sido instalada ya que por su tecnología de machine learning tarda un tiempo en aprender el comportamiento de los perfiles de usuarios y sus diferentes características y horarios.

- Aprovechar lo amigable de la herramienta y realizar alertas personalizadas de login, según plataformas, aplicaciones, dispositivos y/o perfiles conforme vayan apareciendo las necesidades de seguridad de la empresa.

Plantilla de Caso de Uso 4

Detección de malware en firewall perimetral

Control de Cambios

Fecha Actualización	Realizado por	Autorizado por	Naturaleza del Cambio
Corresponde a la fecha de elaboración / fecha de modificación del documento	Oficial responsable de la elaboración / personal del proveedor encargado de la elaboración cuando aplique	Línea de supervisión de ROT, la autorización se adjunta vía mail	Breve descripción del cambio ejecutado, en el caso en que el documento sea nuevo no se requiere descripción

CONTENIDO

OBJETIVO

Detectar los tipos de malware, a través del firewall perimetral

ALCANCE

Este caso de uso tiene el siguiente alcance:

- Protección ante ataques de denegación de servicio (DoS).
- Accesos seguros desde equipos externos e internos
- Seguridad ante intrusión y sustracción de credenciales
- Bloqueo de puertos ante actividad sospechosa

FUENTES DE EVENTOS

- IDP
- Antispam

TIPO DE DATOS

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Plataforma	Tipo de log
Bloqueo de puertos	Eventos de actividad sospechosa
Antispam	Eventos de correos entrantes con archivos adjuntos mediante phishing.

FLUJO LÓGICO

- Se activará una alerta cuando se detecte un evento con una firma asociados a las categorías de Ataques hacia aplicativos del sector financiero

NOTIFICACIÓN

- Las notificaciones de las alertas serán enviadas a la cuenta xxxxx@domain.com.
- La notificación se realizará de acuerdo con el formato estándar definido por CLIENTE

SEVERIDAD

Alerta/Reporte	**Severidad**
Intrusión de puertos	Alta
Denegación de servicios (DoS)	Alta
Correo con malware	Alta

RECOMENDACIÓN

- Implementar un firewall perimetral.

Plantilla de Caso de Uso 5

Detección de Ransomware en ordenadores corporativos

Control de Cambios

Fecha Actualización	Realizado por	Autorizado por	Naturaleza del Cambio
Corresponde a la fecha de elaboración / fecha de modificación del documento	Oficial responsable de la elaboración / personal del proveedor encargado de la elaboración cuando aplique	Línea de supervisión de ROT, la autorización se adjunta vía mail	Breve descripción del cambio ejecutado, en el caso en que el documento sea nuevo no se requiere descripción

CONTENIDO

OBJETIVO

Detectar los ataques de tipo ransomware en ordenadores identificados como parte de la empresa.

ALCANCE

Este caso de uso tiene el siguiente alcance:

- Protección ante ataques de ransomware.

FUENTES DE EVENTOS

- Trend Micro Vision One

TIPO DE DATOS

Para la creación de este caso de uso, se requiere el análisis de los siguientes tipos de información:

Plataforma	Tipo de log
Vision One	Eventos de prevención de intrusiones
Vision One	Eventos Antimalware
Vision One	Logs de monitoreo de comportamiento

FLUJO LÓGICO

- Se activará una alerta cuando se detecte un evento de IPS y antimalware

NOTIFICACIÓN

- Las notificaciones de las alertas serán enviadas a la cuenta xxxxx@domain.com.
- La notificación se realizará de acuerdo con el formato estándar definido por CLIENTE

SEVERIDAD

Alerta/Reporte	Severidad
IPS	Alta
Antimalware	Alta

RECOMENDACIÓN

- Implementación de plataforma XDR para una gestión de detección y respuesta extendida efectiva.