UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
ANÁLISIS COMPARATIVO DE PLATAFORMAS DE SIEM Y LAS SOLUCIONES DE DETECCIÓN Y RESPUESTA EXTENDIDA
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Paúl Fernando Nacimba Loachamín
Tutor:
MSc. Pablo Marcel Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varelacon C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: ANÁLISIS COMPARATIVO DE PLATAFORMAS DE SIEM Y LAS SOLUCIONES DE DETECCIÓN Y RESPUESTA EXTENDIDA.

Elaborado por: Paúl Fernando Nacimba Loachamín, de C.I: 1715893689, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Paúl Fernando Nacimba Loachamín con C.I: 1715893689, autor del proyecto de titulación denominado: Análisis comparativo de plataformas de SIEM y las soluciones de Detección y Respuesta Extendida. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023

Firma

Orcid: 0000-0001-5930-0241

Tabla de contenidos

Índice de tablas

Índice de figuras

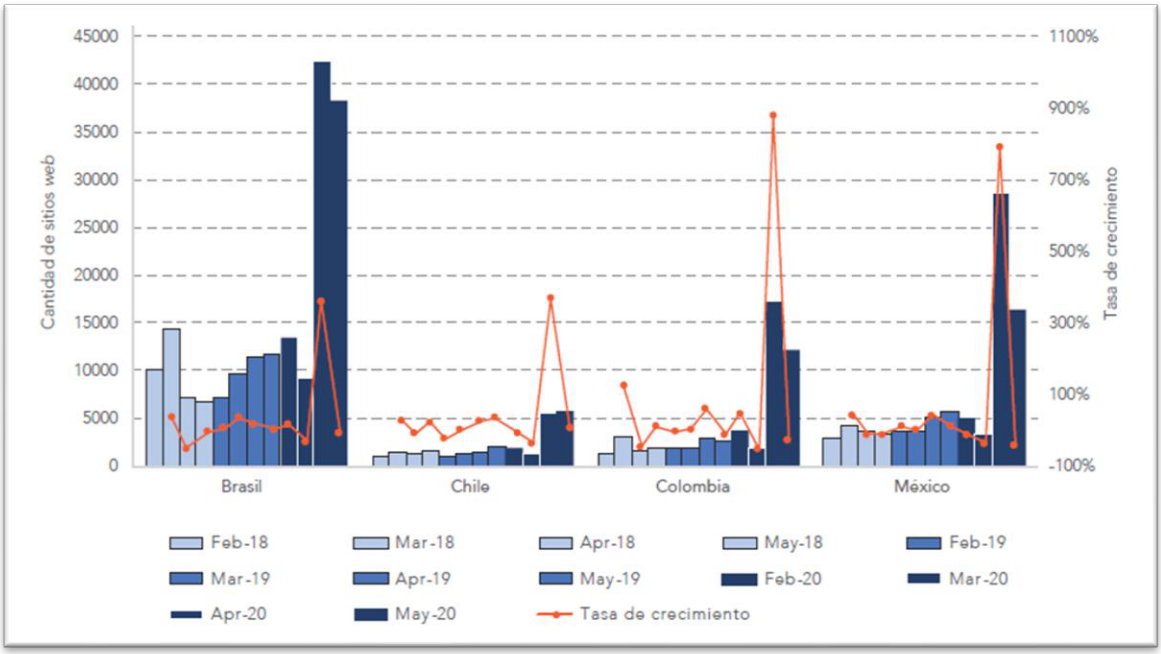
INFORMACIÓN GENERAL

Contextualización del tema

Según la CEPAL (2020), los datos son considerados uno de los activos más relevantes para todas las entidades sin importar la vertical de negocio o tamaño. Entre estos están incluidos datos personales, información de propiedad intelectual, datos sensibles, estadísticas del mercado, etc. A su vez estos son recopilados, normalizados, procesados, transmitidos y almacenados en medios tecnológicos. Por lo que es fundamental implementar medidas para proteger los datos y con esto evitar ataques y delitos informáticos que puedan afectar la normal operación y entrega de servicios de las empresas.

El crecimiento y diversificación de la infraestructura tecnológica empresarial impulsado por la transformación digital y la crisis del COVID-19, ha venido a ampliar la superficie de ataque que puede ser aprovechada por los ciberdelincuentes, mediante técnicas sofisticadas como los ataques persistentes avanzados, ataques dirigidos, ataques sin archivos, ataques de ingeniería social entre otros.

Figura 1.
Cantidad de sitios web empresariales creados al mes



Nota: CEPAL, 2020

Según Robalino (2018), en la actualidad existen diferentes recomendaciones y mejores prácticas para proteger las organizaciones ante dichas amenazas mediante la implementación de soluciones como firewalls de siguiente generación, sistemas de prevención de intrusiones, plataformas de protección de malware, firewalls de aplicaciones web, etc. Estas plataformas son efectivas en prevenir ataques informáticos en la capa de seguridad que protegen, sin embargo se presentan varios desafíos como: 1) Múltiples interfaces de administración de las plataformas de seguridad. 2) Miles de registros de eventos generados por las soluciones de seguridad, sistemas operativos y aplicaciones. 3) Almacenamiento limitado de registros que pueden tener información

muy valiosa sobre los eventos de seguridad. 4) Visibilidad limitada del ciclo del ataque, las plataformas de seguridad de forma independiente muestran información muy puntual en las alertas y no permiten tener un contexto más amplio de la amenaza. 5) Falta de personal capacitado.

Esto vuelve muy difícil el monitoreo, identificación y respuesta temprana ante amenazas avanzadas que usan múltiples vectores de ataque para llegar a su objetivo y no son detectadas por las soluciones tradicionales de seguridad.

Las plataformas se Security Information and Event Management (SIEM) mediante la recolección, normalización y correlación de eventos permiten descubrir y generar asociaciones entre estos registros, siendo que estos pueden ser de cualquier tipo de activo dentro de la organización. La correlación de eventos permite organizar y administrar los registros, pero también brindan información procesada para responder ante eventos de seguridad que afecten a las dimensiones de integridad, disponibilidad y confidencialidad de la información. Así como permiten medir el cumplimiento de estándares nacionales e internacionales como Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP) entre otros que pueden ser de importancia para la empresa.

Esta tecnología ha sido muy aceptada e implementada de forma directa, es decir administrada por la propia organización o en un modelo de servicio de servicio gestionado incluido en un Centro de Operaciones de Seguridad (SOC), sin embargo durante los últimos años soluciones emergentes como las de detección y respuesta extendida (XDR) las han venido a cubrir esta necesidad de una forma más específica en lo que ha seguridad informática se refiere.

Es decir que permiten recolectar, procesar y analizar los eventos identificados por diferentes plataformas de seguridad y adicionalmente incluyen capacidades de respuesta automática para la mitigación de amenazas (Quilachamín, 2020, pp 5-6).

El desarrollo de estas nuevas plataformas ha causado incertidumbre en los especialistas de seguridad sobre si una tecnología puede reemplazar a la otra o pueden ser complementarias. Por estos motivos es importante realizar el análisis de las características, casos de uso y escenarios en los que pueden ser implementadas.

Problema de investigación

Actualmente las organizaciones cuentan con una gran cantidad de plataformas de seguridad de diferentes fabricantes las cuales están generando de forma constante cientos de registros de eventos. Manejar estas alertas de forma independiente se vuelve cada vez más complicado ya que se debe contar con personal especializado y dedicado para estas actividades. La estrategia más utilizada en los últimos años ha sido la implementación de un SIEM, pero varios fabricantes han posicionado conceptos y plataformas como las denominadas de detección y respuesta extendida (XDR). Generando dudas en los departamentos de tecnologías de información sobre la mejor alternativa para cubrir los requerimientos de detección de amenazas.

¿Como la identificación de las características a nivel de funcionalidades, inversión y cumplimiento normativo de las plataformas de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR) ayudan a las empresas a mejorar el proceso de evaluación, selección y adquisición de una plataforma que les

permita identificar amenazas mediante la correlación de eventos de plataformas de seguridad e infraestructura tecnológica?

Objetivo general

Analizar las características funcionales y no funcionales de plataformas de pago para Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR).

Objetivos específicos

Indagar sobre las soluciones de pago Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR) que actualmente están disponibles en el panorama de la seguridad de la información, para contextualizar las mismas a las necesidades de detección de amenazas.

Analizar las características técnicas y algunos casos de uso de las plataformas de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR) con el fin de establecer los criterios que permitan cubrir los requerimientos de funcionalidades, inversión y cumplimiento normativo en las organizaciones.

Proponer una guía con criterios que deben ser considerados para la evaluación y selección de las plataformas de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR).

Vinculación con la sociedad y beneficiarios directos:

En el panorama actual existen múltiples plataformas de seguridad informática las cuales están enfocadas en proteger diferentes puntos que pueden ser aprovechados por los ciberdelincuentes como el perímetro, estaciones de trabajo, servidores, bases de datos, aplicaciones web, etc. Pero al ser plataformas independientes no se puede tener el contexto completo sobre los ataques que pueden estar afectando a las organizaciones. Para cubrir esta problemática se tiene disponibles plataformas de correlación de eventos de seguridad y detección de amenazas con diferentes características. El presente estudio se centrará en el análisis de las plataformas de pago para Security Information and Event Management (SIEM) y las comparará con las de Detección y Respuesta Extendida (XDR). (Gb-advisors, 2020)

Con esto, se busca brindar una guía para que las organizaciones públicas y privadas puedan optimizar los procesos de evaluación y selección de plataformas de correlación de eventos y detección de amenazas de seguridad informática, con base en las funcionalidades técnicas, cumplimiento normativo e inversión económica.

Considerando los Objetivos de Desarrollo Sostenible, el análisis se centra en el objetivo número nueve que hace referencia a la Industria, Innovación e Infraestructuras. Ya que brinda asesoramiento sobre las tecnologías que pueden cubrir las necesidades de detección de amenazas mediante la correlación de eventos, garantizando que los usuarios puedan acceder de forma normal y eficiente a toda la información y servicios ofrecidos por las organizaciones.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La transformación digital ha llevado que la infraestructura tecnológica de las organizaciones este distribuida en sus premisas, proveedores de infraestructura como servicio, proveedores de plataformas como servicio y aplicaciones como servicio. Esto implica generar miles de eventos en diferentes ubicaciones haciendo que la gestión de estos sea una tarea muy compleja. (AWS, 2023).

1.1. Contextualización general del estado del arte

Según Kaspersky (2022), la protección de las infraestructuras tecnológicas corporativas frente a los ataques cibernéticos es una tarea que necesita cada vez más recursos tanto de plataformas de seguridad como de personal especializado. Esto debido a que la superficie de ataque se ha ampliado exponencialmente, generando que el riesgo digital aumente, para cubrir esto es mandatorio saber cómo gestionar las ciberamenazas de forma integral.

Las ciberamenazas actuales incluyen:

- Actores maliciosos que invierten tiempo para conocer a la potencial víctima, esto permite saber a quién exactamente atacarán, que procedimiento usarán y cuál es el mejor momento para ejecutar el ataque. Esta etapa de reconocimiento y planificación hace que los ataques sean más difíciles de detectar, más sofisticados y por lo tanto más efectivos.
- Trabajo en conjunto de atacantes para aprovechar sus diferentes habilidades. Algunos identifican vulnerabilidades, exfiltran información sensible, etc.
- Los ciberataques tratan de aprovecharse del eslabón más débil, el usuario final, para acceder a la red. Una vez que un equipo se encuentra comprometido, el atacante se puede mover de forma sigilosa por toda la organización hasta llegar a su objetivo, esto implica permanecer semanas, meses e incluso años en la red.
- Uso de herramientas propias del sistema operativo para ejecutar procesos maliciosos, estas actividades no pueden ser detectadas por herramientas tradicionales de seguridad.

Para responder de forma efectiva ante esta problemática se han generado múltiples plataformas de gestión y administración de eventos de seguridad, las cuales permiten tomar medidas proactivas y unificadas, es decir que los eventos detectados por las múltiples plataformas de seguridad ya no se manejen de forma independiente, sino de forma centralizada, esto conlleva tener un mayor contexto del incidente, investigación más precisa y respuesta efectiva. (Vielberth & Pernul, 2018)

La primera referencia de SIEM es atribuida al informe de la consultora Gartner y lo define como «La plataforma de gestión de información y eventos de seguridad (SIEM) permite la identificación de amenazas, cumplimiento normativo y administración de alertas de seguridad empleando la recopilación y análisis (cercano al tiempo real) de registros de seguridad, así como también una amplia cantidad de fuentes de datos importantes. Sus características principales incluyen un amplio alcance de ingesta y gestión de eventos, la capacidad de analizar eventos de registro y otra información a través de diversos orígenes y capacidades de administración (como análisis de incidentes, paneles e informes)». (Gartner Inc, 2023)

Con el paso de los años el SIEM ha evolucionado hasta llegar a ser algo más que una herramienta de administración de registros. En la actualidad las plataformas de SIEM incluyen capacidades de análisis avanzado en el que se incluye comportamiento de usuarios, inteligencia artificial y aprendizaje de máquina. Lo que permite que sea un

sistema de orquestación de eventos muy eficiente para gestionar las amenazas, así como el cumplimiento de las normativas y la elaboración de informes. (Patton, 2019)

Por otro lado, están las plataformas de detección y respuesta en los terminales (EDR) que fueron el primer tipo de sistema de detección y respuesta y, en comparación con las tecnologías de seguridad tradicionales, permiten una mayor visibilidad y respuesta más ágil ante las amenazas. Sin embargo están limitadas a la protección de los terminales de usuario y servidores.

La evolución natural de dichas plataformas son las soluciones de detección y respuesta extendida (XDR), las cuales permiten recolectar y correlacionar información en múltiples capas de seguridad como servidores, estaciones de trabajo, redes, cargas de trabajo en la nube, entre otros. Permitiendo tener una visión y trazabilidad más amplia sobre los eventos de seguridad. (Trendmicro, 2020)

Las plataformas de XDR ayudan a acelerar las investigaciones, pues entregan una imagen completa de cada evento de seguridad. Al consolidar distintos tipos de información y revelar la causa original y la cronología de las alertas, incluso permite a los analistas con menor experiencia clasificar las alertas. Por a la integración natural con los puntos de aplicación de las políticas, ayuda a responder a las amenazas en cualquier ubicación de la organización. Dichas plataformas, permiten usar las plataformas de seguridad existentes de la red, los *endpoints* y la nube como sensores y puntos de aplicación de políticas, esto evita tener que implementar nuevas soluciones. (Palo Alto Networks, 2021, pp 2).

1.2. Proceso investigativo metodológico

A continuación, se describe los procesos de investigación utilizados:

Investigación descriptiva

La investigación descriptiva se aplica cuando se necesita describir, en sus principales elementos, una realidad. Se refiere a estructuración de la investigación, generación de inquietudes y análisis de datos que se ejecutarán sobre un tema en particular. Es conocida como la metodología de investigación observacional ya que ninguno de los elementos que forman parte del análisis está sujeta a influencias. (Guevara, Verdesoto & Castro, 2020).

Se uso de la investigación descriptiva para la recopilar la información más importante que apoye al desarrollo del presente trabajo.

Esta investigación pretende entregar una guía la cual permita identificar las características comunes, diferencias y aplicabilidad de las plataformas analizadas.

Investigación bibliográfica

En la actualidad existen muchos medios para tener acceso rápido a gran cantidad de información, sin embargo el principal desafío es poder encontrar información valida. La investigación bibliográfica consiste en buscar y recolectar información que tenga relación con el tema de la investigación. Usando medios tradicionales y también electrónicos (Ocampo, 2019).

En la presente investigación se aplicará un análisis cualitativo en el cual se identificarán los elementos que se van a analizar y se recopilara información de diferentes fuentes como tesis, artículos científicos, informes de analistas de seguridad y artículos de fabricantes. Para después realizar el análisis y estudio de las diferencias de

las plataformas de pago de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR), en este paso se validará que los datos recopilados sean entendibles y de importancia para la finalidad de la investigación.

1.3. Análisis de resultados

Acorde a Secureworks (2022), para realizar el análisis comparativo de las plataformas no gratuitas de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR), se han tomado en consideración las siguientes características:

Arquitectura

Describe las diferentes opciones de implementación disponibles en las plataformas de SIEM y XDR, pudiendo ser, mediante appliances virtuales o físicos en las premisas de la empresa, servicios Software as a Service (SaaS) o híbridos.

Funcionalidades

Características generales que se incluyen en las plataformas analizadas, considerando funcionalidades tradicionales como correlación de eventos, inventario de activos, análisis de integridad de archivos y análisis de vulnerabilidades. También se validarán las capacidades avanzadas como User and Entity Behavior Analytics (UEBA), aprendizaje de máquina e integración con fuentes de inteligencia de amenazas.

Personalización

Capacidades de personalización y creación de políticas, casos de uso personalizados, notificaciones, análisis de cumplimiento y reportería.

Capacidades de detección de amenazas y contexto

Características y técnicas empleadas para la detección de amenazas conocidas y de día cero, con base en los eventos correlacionados. Es importante indicar que también se tomaran en consideración la capacidad de dar contexto a las amenazas detectadas.

Capacidades de respuesta

Características y opciones disponibles en cada una de las plataformas sobre respuesta manual y automática para la mitigación de amenazas.

Análisis forense

Información de recursos disponibles para realizar el análisis forense de amenazas que pudieron evadir los controles de seguridad existentes y fueron detectadas durante el monitoreo de registros.

Almacenamiento de información

Opciones disponibles para la ubicación del almacenamiento de la información y también el tiempo de disponibilidad que ofrecen las plataformas de SIEM y XDR.

Cumplimiento de normativas y estándares

Capacidad para la generación de informes de cumplimiento de estándares y normativas relacionadas como PCI DSS, GDPR, Health Insurance Portability and Accountability Act of 1996 (HIPPA), SOX y otros.

CAPÍTULO II: PROPUESTA

El desafío más importante para los especialistas de seguridad no es la gran cantidad de amenazas existentes, si no el tratar de monitorear e identificar incidentes de seguridad en los miles de registros generados por los activos de la organización, considerando que la revisión y clasificación se debe hacer de forma manual y continua. (IBM, 2023)

2.1. Fundamentos teóricos aplicados

Security Information and Event Management (SIEM)

Es una plataforma de seguridad que apoya a las empresas a identificar vulnerabilidades y amenazas existente antes de que estas puedan a afectar la normal operación y entrega de servicios informáticos. A través de la recolección, normalización y correlación de registros de los activos de información. Permite identificar cualquier tendencia o comportamiento anómalo, en el tráfico de red, comportamiento de usuarios, navegación, correo electrónico, etc.

Con esta información identificada se pueden tomar acciones de investigación y respuesta. También viene a ser un componente esencial en los SOC para el monitoreo de seguridad y cumplimiento de estándares o normativas. (Quilachamín, 2020, pp 6)

Según Robalino (2018), las soluciones de SIEM tienen como base los siguientes componentes:

Security Event Management (SEM), enfocado en analizar los registros almacenados para detectar comportamiento anómalo, incluidas modificaciones sobre archivos o violaciones en los accesos de usuario. Está diseñado para comparar las anomalías detectadas con una base de inteligencia de amenazas.

Security Information Management (SIM), permite automatizar la recopilación y centralización de los registros de eventos de dispositivos como firewalls, servidores proxy, antimalware, etc. Para normalizarlos a un formato estándar.

Al integrar las tecnologías anteriormente descritas, las plataformas SIEM permiten recolectar, normalizar, procesar y correlacionar los registros de los activos tecnológicos de información de las organizaciones y con el apoyo de fuentes de inteligencia, detectar amenazas en las actividades diarias. Esto permite fortalecer e incrementar el nivel de madurez de seguridad entregando un panorama integral de seguridad del entorno de tecnológico de la empresa.

Tipos de SIEM

Según Coresecurity (2022), existen los siguientes tipos de SIEM:

SIEM de código abierto

Las plataformas SIEM de código abierto entregan capacidades de nivel inicial que puede ser aplicable para organizaciones que recién comienzan a tener registros y analizar los logs de seguridad. Estas soluciones son ideales para escenarios de prueba, permiten identificar lo que realmente se necesita monitorear y definir las medidas a tomar cuando identifique un comportamiento anómalo. El SIEM de código abierto necesita demasiada personalización para ser una alternativa viable en las empresas pequeñas.

SIEM gratuito

Las soluciones SIEM gratuitas, son sencillas y fáciles de usar. Sin embargo, no pueden garantizas suficiente estabilidad y funcionalidad. A medida que las organizaciones crecen, sus necesidades de seguridad crecen con ellas. Se necesita mayor capacidad para monitorear más activos de información y las características más avanzadas comienzan a ser más necesarias.

SIEM empresarial

Las características avanzadas, la facilidad de gestión y el soporte son los elementos básicos que hacen que las soluciones de grado empresarial se diferencien de sus contrapartes gratuitas o de código abierto. Sin embargo, las soluciones SIEM empresariales pueden tener características muy diferentes entre sí. Por ejemplo, la mayoría de las plataformas SIEM están destinadas a empresas u organizaciones grandes y serían demasiado complejas y costosas para organizaciones pequeñas. En su lugar, estas empresas buscarían una solución SIEM de rango medio que aún proporcione toda la funcionalidad crítica y sea más fácil de usar. Para garantizar que las prioridades y casos de uso de la organización sean cubiertas por la herramienta, siempre es necesario realizar una comparación de las funcionalidades del SIEM.

Capacidades generales de las plataformas SIEM

Según Gonzáles, Gonzáles & Díaz (2021, pp 1). Las soluciones SIEM pueden tener múltiples funcionalidades y características sin embargo en el nivel más básico, todas las soluciones incluyen las siguientes funcionalidades:

- Integraciones: El SIEM debe integrarse con múltiples fuentes de registros tanto de plataformas de seguridad así como también de plataformas no relacionadas con seguridad.
- Gestión de registros: mediante la recopilación y procesamiento de eventos generados en servidores, aplicaciones, plataformas de seguridad, equipos de comunicación, etc. Esto permite administrar de forma centralizada todo este flujo de datos.
- Correlación de eventos: constituye un componente esencial en cualquier plataforma SIEM y mediante el análisis avanzado puede identificar y descubrir asociaciones de entre registros de múltiples fuentes, brinda información precisa para identificar amenazas a la seguridad corporativa. Este seguimiento de la actividad es crucial en

la seguridad informática. También puede identificar errores operativos y defectos que pueden afectar el rendimiento de la computadora. En ocasiones, esto también se denomina gestión de incidentes.

- Monitoreo de alertas e incidentes de seguridad: al recopilar, procesar y correlacionar los registros de múltiples fuentes de información en las organizaciones, las plataformas SIEM pueden monitorear, identificar y brindar un mayor nivel de información sobre los incidentes de seguridad en todos los dispositivos, usuarios y aplicaciones. Con la configuración de casos de uso, los administradores pueden ser notificados de inmediato y tomar las acciones necesarias para impedir que la amenaza se llegue a convertir en un problema de seguridad más crítico.
- Uso de fuentes de inteligencia de amenazas que pueden ser de código abierto o bajo suscripción, es un componente esencial para identificar los ataques conocidos.
- Cumplimiento: por la gran cantidad de datos procesados que manejan las soluciones de SIEM, pueden generar informes de cumplimiento en tiempo real de estándares como PCI-DSS, SOC, HIPPA, GDPR, entre otros. Reduciendo de forma significativa la carga en la gestión de seguridad. (Fortra, 2018)

Arquitectura del SIEM

Las plataformas de Security Information and Event Management (SIEM), tienen los siguientes componentes básicos en su arquitectura:

Figura 2.
Arquitectura básica de un SIEM

Nota: Desarrollo propio basado en Gonzáles, Gonzáles & Díaz (2021)

Acorde a Robalino (2018), las características de cada componente del SIEM son:

- Dispositivo fuente: son las plataformas de seguridad, dispositivos de red, servidores, estaciones de trabajo, etc. Desde los cuales se recolectan los eventos.
- Recopilación de registros: Una vez listos los eventos de los dispositivos, el SIEM puede recopilar y procesar de forma autónoma los registros de seguridad generados en los dispositivos origen, la recolección se puede hacer mediante sensores de red, agentes, conectores, protocolos, etc.
- Normalización y parseo: El proceso de estandarización es una pieza muy importante en la arquitectura del SIEM, el cual necesita que para el análisis, todos los logs de seguridad recopilados de varios dispositivos estén en un formato estándar.
- Motor de correlación de eventos: En este componente se incluye una cantidad de reglas predeterminadas y aplicadas para que el procedimiento de correlación de eventos consiga analizar e identificar un potencial incidente de seguridad. Estas

reglas incluidas en el proceso permitirán descubrir interrelaciones asociadas con ataques complejos e identificar falsos positivos.

- Almacenamiento: Se refiere al aprovisionamiento de los logs de seguridad generados en los dispositivos origen y los registros que procese el SIEM.
- Interface de Monitoreo: Es la plataforma que permite a los analistas de seguridad monitorear de forma constante (24/7/365) las alarmas generadas durante el proceso de correlación, mediante esta se realiza el proceso de investigación, análisis forense y si es posible la respuesta.

Beneficios de SIEM

De acuerdo con Watchguard (2022), sin importar el tamaño de una organización es imprescindible tomar medidas proactivas para monitorear, identificar y mitigar riesgos de seguridad TI. Las plataformas de SIEM brindan diversos beneficios y se han convertido en elementos importantes para cumplir con este objetivo, los principales beneficios que aporta un SIEM en las organizaciones son:

- Identificación de amenazas en tiempo real: al realizar el monitoreo activo de la red, se reduce de manera considerable el tiempo de identificación y reacción ante posibles vulnerabilidades, violaciones de seguridad, identificación de comportamientos sospechosos y amenazas en la infraestructura.
- Base de conocimientos: una característica principal de la plataforma es la documentación continua de los incidentes y acciones tomadas. Con esto se crea una base de conocimientos centralizada la cual permite tener información procesada para identificar y solucionar problemas futuros de una forma más ágil y eficiente.
- Investigación forense: cuando las organizaciones han sufrido un incidente de seguridad, las plataformas de SIEM son una herramienta ideal para ejecutar investigaciones forenses, al disponer de toda la información de los registros de los activos digitales se tiene la posibilidad de recrear incidentes o analizar nuevos para investigar comportamientos sospechosos y con esto implementar mejoras en los procesos de seguridad informática.
- Reducción de costos: por su alto grado de optimización en la recolección, procesamiento y correlación de registros, las plataformas de SIEM permiten optimizar los recursos de TI, tanto tecnológicos como humanos. Permitiendo que las actividades se enfoquen en labores de análisis y respuesta ante amenazas detectadas.

Plataformas de SIEM de suscripción

Por otro lado Gonzáles, Gonzáles & Diaz (2021, pp 3-4), indican que las principales plataformas de SIEM de pago dentro del ámbito empresarial son:

IBM Security QRadar

Es una de las plataformas de SIEM más robustos que existen. Incluye más de 400 módulos, tienen la capacidad de soportar una pesada carga de eventos, alcanzando los millones de eventos al día. Esta solución brinda información importante para que los equipos de seguridad puedan actuar de forma oportuna y reducir o evitar el impacto de los incidentes.

McAfee Enterprise Security Manager

Es la herramienta de la corporación de ciberseguridad McAfee, puede monitorizar la infraestructura de TI de las organizaciones para poder recolectar, analizar y correlacionar eventos de seguridad TI con una amplia base de datos de logs, y así llegar a identificar comportamiento sospechoso de manera temprana y proactiva.

LogRhythm

Proporciona una plataforma de SIEM de próxima generación para problemas como flujos de trabajo fragmentados, fatiga de alarmas, detección de amenazas segmentadas, falta de automatización, falta de métricas para comprender la madurez y falta de visibilidad centralizada. Tiene opciones de almacenamiento de datos flexibles.

USM Anywhere

La plataforma de gestión unificada de seguridad (USM) de AlienVault entrega una solución integrada, simple y accesible para el cumplimiento normativo y detección de amenazas conocidas y de día cero. Es robustecida por las fuentes de inteligencia de amenazas Labs Threat Intelligence y el Open Threat Exchange de AlienVault, siendo uno de los mayores intercambios de inteligencia de amenazas, USM está enfocado para que las organizaciones pequeñas y medianas puedan defenderse contra los ataques actuales.

Tabla 1.
Posicionamiento de las plataformas de SIEM según Gartner

Fabricante de SIEM	2016	2017	2018	2020	2021
ArgSigth	Leader	Challenger			Niche Player
RSA	Challenger	Challenger	Leader	Leader	
IBM	Leader	Leader	Leader	Leader	Leader
LogRhythm	Leader	Leader	Leader	Leader	Leader
AlienVault/ AT&T	Visionary	Visionary	Niche Player	Niche Player	
Rapid7		Visionary	Visionary	Leader	Leader
Trellix		Niche Player		Niche Player	Niche Player
Splunk	Leader	Leader	Leader	Leader	Leader

Nota: Gonzales, Gonzales & Diaz (2021)

XDR (Extended Detection and response)

Según Palo Alto Network (2021, pp1), los equipos de seguridad tienen que dar la cara a una creciente variedad de amenazas, iniciando con el ransomware y espionaje hasta los ataques que no usan archivos y la exfiltración de datos. Sin embargo, el mayor desafío para la gran cantidad de analistas de seguridad no es la gran cantidad de riesgos que dominan el panorama actual, si no las actividades repetitivas que deben ejecutar cada día tras día para categorizar los incidentes e intentar disminuir la creciente acumulación de alertas.

Detección y Respuesta Extendida, es una de las tecnologías más avanzada y prometedoras de ciberseguridad, desarrollada bajo un modelo Software as a Service (SaaS). Las soluciones de monitoreo se centraban en una sola capa de seguridad o solo se limitaban a realizar la correlación de eventos y notificación de estos. El XDR permite la detección y respuesta a incidentes de seguridad informática en múltiples capas de la infraestructura de TI. La tecnología XDR recolecta y vincula automáticamente los eventos de múltiples fuentes, que pueden incluir puntos finales, servidores, redes y usuarios. Esto apoya a identificar más amenazas y entrega a los analistas una visión completa del comportamiento y datos necesarios para responder de manera más ágil, eficaz y sobre todo proactiva.

El XDR es el siguiente paso en la evolución de soluciones como la de análisis de tráfico de red (NTA) y la de detección y respuesta de puntos finales y servidores (EDR). Aún siguen siendo útiles, sin embargo, generan mayor número de alertas, necesitan más tiempo para la investigación y respuesta para los eventos, y es necesario más administración y afinamiento.

Según Sophos (2022), XDR sirve ayuda a los equipos de seguridad a:

- Identificar amenazas avanzadas que son difíciles de identificar por medios tradicionales.
- Ejecutar un seguimiento de las amenazas a través de varios elementos de la infraestructura.
- Mejorar la velocidad de detección y respuesta.
- Analizar todo tipo de amenaza de forma eficaz y eficiente.

Acorde a FireEye (2021), Las principales características de las soluciones de XDR según son:

Capacidad de prevención: incluir fuentes de inteligencia de amenazas y aprendizaje de maquina puede ayudar a asegurar que las soluciones puedan ejecutar protecciones contra la gran cantidad de ataques. Adicionalmente, el monitoreo continuo junto con la respuesta automática bloquea amenazas de cualquier tipo tan pronto como sea identificada para evitar daños.

Visibilidad granular: entrega datos completos del usuario en las estaciones de trabajo en conjunto con comunicación de red y aplicaciones empresariales. Esto incluye información sobre autorización de acceso, aplicaciones en uso y archivos a los que se ingresa. Tener completa visibilidad en todos los sistemas, incluso en el data center físico y en la nube, le permite detectar y bloquear ataques de manera oportuna.

Respuesta eficaz: la recolección y análisis de eventos permite rastrear el camino de un ataque y reconstruir las acciones del ciberdelincuente. Esto entrega la información necesaria para ubicar al atacante donde quiera que se ubique y formar un perfil del comportamiento del atacante para evitar futuras amenazas y robustecer las defensas.

Control: capacidad de agregar en la lista blanca y lista negra el tráfico y los procesos permitidos. Esto garantiza que solo las acciones aprobadas y los usuarios verificados puedan ingresar a los sistemas empresariales.

Alta productividad: la unificación reduce la cantidad de alertas e incrementa la precisión de las alertas. Esto implica menos falsos positivos por depurar y analizar. Asimismo, dado que el XDR es una plataforma integrada y no una mezcla de soluciones de múltiples puntos, es más fácil de administrar y mantener, reduciendo la cantidad de interfaces a las que los analistas deben ingresar durante un el proceso de investigación y respuesta.

Machine Learning

Datascientes (2023) indica que, el Machine Learning o aprendizaje de maquina es un área científica y más específicamente, una ramificación de la inteligencia artificial. Se fundamenta en permitir que los algoritmos identifiquen patrones o comportamientos frecuentes, en los datos recolectados (palabras, frases, imágenes, números, etc.).

Todo lo que pueda recolectar y almacenar en formato digital puede ser usado como insumo para el aprendizaje de máquina. Al detectar dichos patrones en la información, los algoritmos van aprendiendo y optimizan su productividad. En resumen, los algoritmos de Machine Learning aprenden automáticamente al ejecutar una actividad, hacen predicciones tomando como base los datos y mejoran su rendimiento con el paso del tiempo. Una vez preparado, el algoritmo tiene la capacidad de detectar los patrones en nueva información.

Indicadores de compromiso

Los indicadores de compromiso (IDC), son toda información de valor que describe un evento de ciberseguridad o actividad, mediante el análisis de los modelos de comportamiento. El objetivo de un IDC es graficar la información que se recibe o se recolecta durante el proceso de investigación de un incidente, de tal forma que pueda reusarse por otros investigadores o víctimas, para descubrir los mismos patrones en sus sistemas de TI y llegar a constatar si han sido o no afectados ya sea desde la perspectiva de monitoreo de anomalías o por investigación forense (Ponce, 2021).

2.2. Descripción de la propuesta

En las siguientes tablas se pueden ver las principales ventajas y desventajas generales de las plataformas de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR), no enfocadas a fabricantes específicos.

Tabla 2.
Ventajas entre SIEM y XDR

Ventajas	
SIEM	**XDR**
Reducen considerablemente el tiempo necesario para identificar y reaccionar ante posibles amenazas de la red, lo que ayuda a reforzar la posición de seguridad a medida que la organización crece.	Dispone de capacidades de prevención avanzadas con la inclusión de inteligencia de amenazas y aprendizaje automático adaptativo ayuda a asegurar que las soluciones puedan implementar protección contra la mayor cantidad y variedad de ataques.
Auditoría de cumplimiento normativo, permiten centralizar las auditorías de cumplimiento normativo y la elaboración de informes en toda la infraestructura empresarial.	Entrega datos de equipos de usuario final, información de red y aplicaciones. Esto incluye información de accesos y archivos accedidos. Tener completa visibilidad de los sistemas, ya sea en la nube o en las premisas, le permite detectar y responder más rápido a los ataques.
Las plataformas de SIEM de última generación se pueden integrar con plataformas de automatización, orquestación y respuesta de seguridad (SOAR), lo que optimiza el tiempo y esfuerzo del equipo de TI usado en la administración de la seguridad organizacional.	Incluye capacidades nativas y automáticas de respuesta.
Mejora en la eficiencia de la organización proporcionando mayor visibilidad de los entornos de TI. Con una vista única y unificada de los datos.	Reduce la cantidad y aumenta la precisión de las alertas. Esto significa menos falsos positivos que procesar.
Permite la detección de amenazas avanzadas y desconocidas	El XDR es una plataforma unificada por lo que reduce la cantidad de consolas de administración que gestionar.
Mediante auditoría y la elaboración de informes sobre el cumplimiento, reducen significativamente el costo para gestionar este proceso al brindar auditorías cercanas al tiempo real y elaboración de informes bajo demanda y personalizados sobre el cumplimiento de las normativas siempre que sea necesario.	

Fuente: Desarrollo propio basado en varios autores

Tabla 3.
Desventajas entre SIEM y XDR

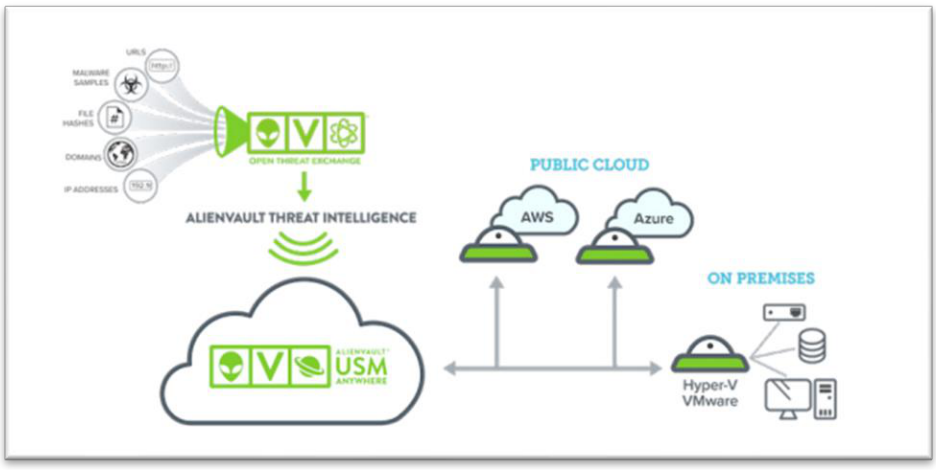
Desventajas	
SIEM	**XDR**
Concentran tanta información para analizar, que los equipos de TI se enfrentan al problema de saturación de alertas haciendo ineficaz la identificación de comportamiento sospechoso.	Plataformas 100% SaaS, puede tener limitantes por almacenamiento de información fuera del territorio nacional.
Gran cantidad de datos irrelevantes recolectados, los mismos que posteriormente disparan falsos positivos.	Integración limitada a plataformas de seguridad.
Integración con plataformas de terceros muy complicada	Limitados casos de uso
Definición de casos de uso personalizados incluye un proceso completo de implementación	Almacenamiento en línea e históricos por tiempo limitado.
Limitada integración con fuentes de inteligencia de terceros	No permite generar reportes e informes de cumplimiento.
Necesidad de personal altamente calificado para monitoreo y análisis de eventos de seguridad.	

Nota: Desarrollo propio basado en varios autores

a. Estructura general

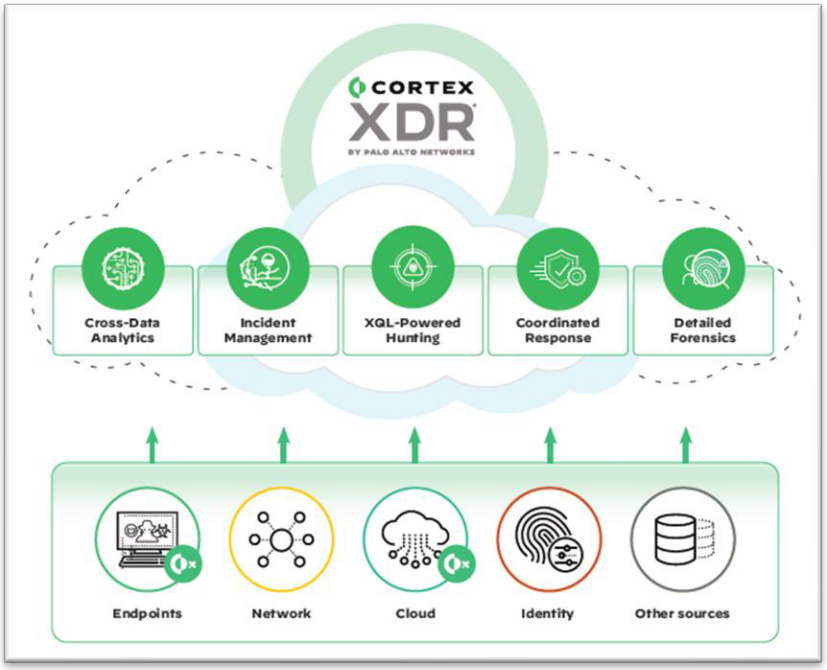
En la actualidad las plataformas de SIEM están disponibles como Software as a Service (SaaS) o también en las premisas de la organización, es importante indicar que algunas funcionalidades y capacidades de integración con los activos pueden varias de un ambiente a otro, por otro lado las plataformas de XDR están disponibles únicamente como como SaaS, con algunos componentes en las premisas de la organización, pero toda la correlación se realiza en la nube.

Figura 3.
Estructura de un SIEM SaaS



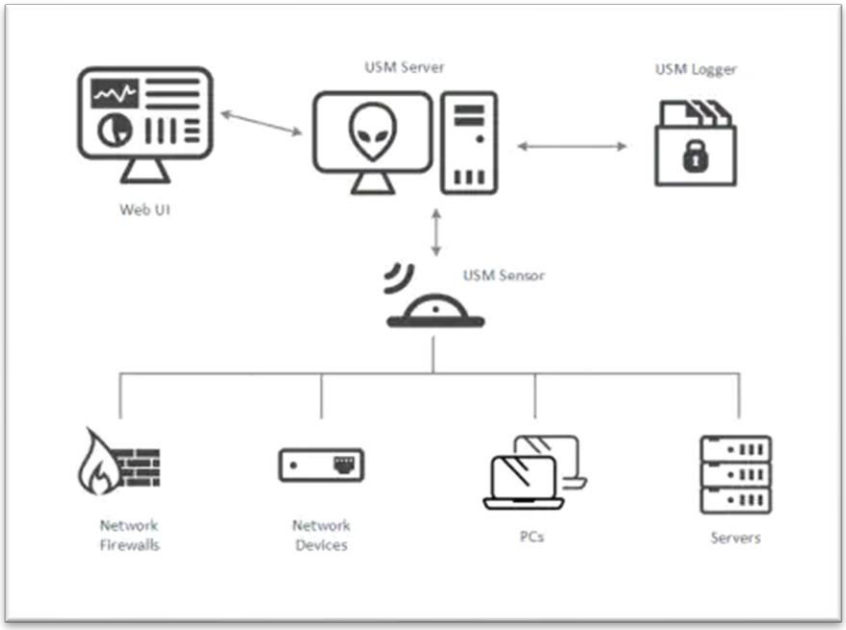
Nota: AlienVault® USM Anywhere (2021)

Figura 4.
Estructura de un XDR



Nota: Palo Alto Networks (2021).

Figura 5.
Estructura de un SIEM en premisas



Nota: AT&T Cybersecurity (2022).

b. Explicación del aporte

En los resultados se muestran las principales diferencias que existen entre las plataformas de pago de Security Information and Event Management (SIEM) y Detección y Respuesta Extendida (XDR), tomado en consideración las funcionalidades más comunes que entregan los diferentes fabricantes.

Tabla 4.
Comparación general de plataformas SIEM Y XDR

Característica	SIEM	XDR
Descripción general	Recopila, agrega, analiza y almacena grandes volúmenes de datos de registro de toda la empresa.	Gartner define al XDR como, una plataforma que integra correlaciona y contextualiza datos para identificar amenazas.
Alcance	Proporciona visibilidad de la actividad sospechosa y maliciosa. Recopilando datos de todos los activos de información, incluyendo las aplicaciones de red y el hardware. Concentra todos los datos en una única plataforma centralizada. Aprovecha los datos para generar alertas, crear informes y garantizar la respuesta a incidentes.	Recolecta, correlaciona y analiza datos de estaciones de trabajo, servidores, cargas de trabajo en la nube, redes y plataformas de correo electrónico a través de herramientas avanzadas de automatización e inteligencia artificial (IA). Analiza los datos y brinda información a los equipos de seguridad en un formato normalizado a través de una única consola. Gestiona las herramientas de seguridad, unificando y automatizando el análisis, la investigación y remediación de la seguridad.

Nota: Desarrollo propio basado en varios autores

Tabla 5.
Comparación de arquitectura de plataformas SIEM Y XDR

Característica	SIEM	XDR
Opciones de implementación	En las premisas de la organización (sensores, motor de correlación y almacenamiento). Servicio SaaS (Sensores y agentes en las premisas, motor de correlación y almacenamiento en la nube)	Servicio SaaS (Sensores y agentes en las premisas, motor de correlación y almacenamiento en la nube)
Integraciones	Cualquier dispositivo que genere logs: Plataformas de seguridad Servidores (aplicaciones, bases de datos, archivos, etc). Estaciones de trabaja Dispositivos de red Nube Aplicaciones como servicios	Plataformas de seguridad Redes Nube Servidores Estaciones de trabajo
Recolección de log	Se realiza la recolección de logs mediante: Syslog Agente API NIDS	Se realiza la recolección de logs mediante: Agente Sensores de red API
Estandarización de logs	Requiere estandarizar a un solo formato los logs recolectados de los múltiples dispositivos. Es necesario realizar actividades de normalización de logs.	Los eventos recolectados ya se encuentran estandarizados.

Nota: Desarrollo propio basado en varios autores

Tabla 6.

Comparación funcionalidades SIEM Y XDR

Característica	SIEM	XDR
Casos de uso	Casos de uso complejos de almacenamiento de registros o gobernanza, gestión de riesgos y cumplimiento (GRC)	No permite
Retención de datos	Retención de datos a largo plazo para cumplimiento y auditoría	Tiempo de almacenamiento limitado
Enfoque de detección	Se enfoca en el análisis basado en la correlación	Ofrece análisis avanzados basados en aprendizaje automático
Automatización de respuesta	Entrega alertas de los eventos de seguridad detectados, la respuesta depende de integraciones con soluciones adicionales y compatibles.	Ofrece casos de usos predefinidos para Detección, investigación y respuesta de amenazas con orquestación prescriptiva, automatización y playbooks.
Licenciamiento	El licenciamiento se lo establece por: Volumen de datos Tiempo de almacenamiento de registros	El licenciamiento se lo establece por: Volumen de datos Tiempo de almacenamiento de registros

Nota: Desarrollo propio basado en varios autores

c. Estrategias o técnicas

En el proceso se realizó el análisis de conceptos ya definidos en otros trabajos de investigación y consultoras internacionales, sin embargo, al hacer referencia a plataformas de seguridad desarrolladas por fabricantes privados, se han tomado como referencia las características descritas en las hojas de datos, manuales de administración, *whitepapers,* entre otras.

2.3. Validación de la propuesta

Acorde a lo descrito por Motadata (2017), para una empresa es vital la recolección, gestión, correlación y análisis de datos de registro en un entorno de tecnologías de la información. Ya sea para detección de amenazas, registro interno o incluso para fines de cumplimiento.

El principal reto es identificar los registros que son relevantes, correlacionarlos e identificar de forma temprana los posibles ataques, para esto es necesario contar con plataformas de SIEM o XDR, siendo que cada organización puede seleccionar una de las dos opciones dependiendo de su vertical de negocio, casos de uso a implementar y arquitectura.

Tabla 7.
Comparativo general SIEM y XDR

Característica	SIEM	XDR
Arquitectura	Cloud En la premisa del cliente	Cloud
Integraciones	Cualquier dispositivo que genere logs	Limitado
Correlación de eventos	Si	Si
Recolección de eventos	Si	Si
Uso de automatización e inteligencia artificial	No	Si
Uso de inteligencia de amenazas	Si	Si
Visibilidad de actividad maliciosa	Si	Si
Gestión	Necesita personalización manual	Automática
Políticas	Personalizadas	Limitado
Casos de uso	Personalizados	Limitado
Conectores	Permite la creación de conectores personalizados	Limitado
Procesamiento de datos	Normalización después del almacenamiento	Normalización antes de ser almacenados en el lago de datos
Notificaciones	Si	Si
Reportes personalizados	Si	Si
Capacidades de detección de amenazas y contexto	Limitado	Si
Capacidades de respuesta	Limitado (depende de la integración con otras soluciones)	Si (nativo)
Análisis forense	Limitado	Si
Almacenamiento de información	A medida	Tiempo limitado
Cumplimiento de normativas y estándares	Apalanca el cumplimento en almacenamiento y operaciones de tecnologías de la información	Su enfoque es de seguridad no en cumplimiento.

Nota: Desarrollo propio basado en varios autores

Tabla 8.
Consideraciones para la selección de una plataforma de SIEM o XDR

Requerimientos de la organización	Plataforma
Recolección, procesamiento y correlación de eventos	SIEM/XDR
Identificación de amenazas basado en firmas	SIEM/XDR
Identificación de amenazas basado en inteligencia artificial	XDR
Integración con múltiples fuentes de eventos	SIEM
Casos de uso personalizados	SIEM
Reglas personalizadas	SIEM
Capacidades avanzadas de análisis forense	XDR
Almacenamiento de información para cumplimiento	SIEM
Validación de cumplimiento de normativas	SIEM
Capacidades de respuesta inmediata	XDR
Notificaciones automáticas	SIEM/XDR
Reportes personalizados	SIEM/XDR
Limitaciones de envío de información a la nube	SIEM
Facilidad de gestión de eventos	XDR

Nota: Desarrollo propio basado en varios autores

Para corroborar el análisis realizado en la propuesta se realizó una revisión por parte del Msc. Jonathan Quezada quien se desempeña como Ingeniero Regional Preventa de soluciones y servicios de ciberseguridad en la empresa GMS y confirmo la validez del análisis realizado. El detalle de la experiencia se describe en el Anexo 1.

Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 9.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
SIEM	Es una plataforma de seguridad que recolecta, normaliza y correlaciona eventos de múltiples activos de información de la infraestructura te de las organizaciones.	La metodología de investigación fue bibliográfica que permitió tener los conceptos del SIEM	Fuente bibliográfica	Permitió identificar las características generales y específicas de la plataforma de seguridad	Resúmenes digitales
XDR	Dispone de las mismas características de correlación que el SIEM, sin embargo se enfoca en detección de amenazas de seguridad	La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre el XDR	Fuente bibliográfica	Permitió identificar las características generales y específicas de la plataforma de seguridad	Resúmenes digitales

	y usa tecnologías como inteligencia artificial y aprendizaje de máquina.

Fuente: Elaboración propia

CONCLUSIONES

Se realizó la búsqueda de información en múltiples repositorios de información para completar el análisis comparativo de las principales características y funcionalidades de las plataformas de SIEM Y XDR, en donde se pudo confirmar el alcance que cada una de estas tiene de forma general y específica.

Se ha llegado a contextualizar las características, funcionalidades y aplicabilidad de las plataformas de SIEM y XDR de pago, disponibles en la actualidad.

El análisis comparativo ha permitido definir que ambas plataformas tienen como enfoque principal la detección de amenazas mediante la recopilación, procesamiento y correlación de eventos de seguridad, en términos generales las soluciones de SIEM y XDR tienen la misma finalidad.

Se elaboró una tabla comparativa que muestra las principales diferencias entre las plataformas desde el punto de vista de arquitectura, integración, funcionalidades y cumplimiento.

La principal diferencia entre las plataformas analizadas está en el tipo de tecnología usada para la correlación e identificación de amenazas, opciones de respuesta y tipos de integración que cada una soporta.

Las plataformas de XDR incluyen tecnologías como inteligencia artificial lo que optimiza los tiempos de detección, investigación y respuesta. La tecnología está siendo implementada en las plataformas de SIEM de siguiente generación sin embargo aun necesitan personal altamente especializado para su optimización.

Se pudo confirmar que las plataformas de SIEM apoyan a las organizaciones en la detección de amenazas y cumplimiento normativo, por otro lado el XDR se enfoca por completo a la ciberseguridad.

En una estrategia de ciberseguridad lo ideal sería trabajar con las plataformas de SIEM y XDR ya que según lo identificado en el análisis, estas se pueden complementar entre sí, permitiendo tener un correlación y detección de amenazas más efectiva, sin embargo, si se quiere optar por una de estas se debe validar si la organización está bajo el cumplimento de alguna normativa o monitoreo de casos de usos específicos, con esta información se puede definir el mejor camino a seguir desde el punto de vista funcional.

Varios fabricantes de plataformas de SIEM han adoptado una estrategia en la cual han incluido funcionalidades de XDR en su portafolio de soluciones, permitiendo que pueda existir una integración más natural entre ambas plataformas.

RECOMENDACIONES

Se recomienda revisar todas las características y funcionalidades que se han encontrado de las plataformas de SIEM y XDR.

El uso de nuevas técnicas, tácticas y procedimientos por parte los ciberdelincuentes obligan a que las plataformas de SIEM y XDR estén en constante actualización e innovación, por lo que es recomendable hacer la revisión de las nuevas funcionalidades que son liberadas por los fabricantes de forma constante.

Es válido que antes de iniciar el proyecto de adquisición de una plataforma de seguridad como el SIEM o XDR se tenga bien identificada el tipo de organización (vertical de negocio y estrategia comercial), normativa o legislación aplicable y requerimientos de seguridad, esto permitirá identificar la mejor opción a implementar.

Se recomienda que para sacar el máximo provecho a las inversiones realizadas en plataformas de SIEM o XDR es necesario que las organizaciones cuenten con personal especializado que pueda hacer el análisis, investigación y dar respuesta a los eventos de seguridad detectados por las plataformas.

En el escenario de que las organizaciones que busquen implementar soluciones de monitoreo de eventos de seguridad no cuenten con personal especializado y necesario para la óptima gestión de las plataformas es recomendable optar por servicios gestionados por los fabricantes o servicios como los de Centro de Operaciones de Seguridad (SOC), los cuales cuentan con todos los recursos humanos y tecnológicos y procesos para la administración de las soluciones.

BIBLIOGRAFÍA

AWS (2023). *¿Qué es la transformación digital?* https://aws.amazon.com/es/what-is/digital-transformation/#:~:text=La%20transformaci%C3%B3n%20digital%20es%20el,ofrece%20valor%20a%20los%20clientes.

CEPAL (2022). *Séptima Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe.* https://www.cepal.org/es/organos-subsidiarios/conferencia-ministerial-la-sociedad-la-informacion-america-latina-caribe.

Carrión, J. Jumbo, P (2019). *Implementación de un siem para el comando de ciberdefensa utilizando herramientas de código abierto bajo el estándar iso 27032.* https://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf

Coresecurity (2023). *What is SIEM.* https://www.coresecurity.com/siem

Datascientest (2023). *Machine Learning: definición, funcionamiento, usos.* https://datascientest.com/es/machine-learning-definicion-funcionamiento-usos

FireEye (2021). *The Future of XDR is Now!.* https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/xdr/wp-esg-fireeye-xdr.pdf

Fortra (2018). *Que es un SIEM*. https://www.fortra.com/es/blog/que-es-un-siem

Gartner Inc. (2023). *Security Information And Event Management (SIEM).* https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Gb-advisors (2020). *Correlación de Eventos y su importancia en la recolección de datos.* https://www.gb-advisors.com/es/correlacion-de-eventos-y-su-importancia-en-la-recoleccion-de-datos/

Gonzáles-Granadillo, G. González-Zarzoza, S. Díaz, R (2021). *Security Information and Event Management (SIEM): Analysis, Trends and Usage in Critical Infrastructures [Paper, University of Regensburg].* https://stop-it-project.eu/download/publication-security-information-and-event-management-siem-analysis-trends-and-usage-in-critical-infrastructures/

Guevara, G. Verdesoto, A. Castro, N. (2020). *Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción).* https://recimundo.com/index.php/es/article/view/860/1363

IBM (2023). *Qué es la gestión de información y eventos de seguridad.* https://www.ibm.com/es-es/topics/siem

Kaspersky (2023). *Kaspersky predice cambios en el panorama de amenazas para el sector industrial.* https://latam.kaspersky.com/about/press-releases/2023_kaspersky-predice-cambios-en-el-panorama-de-amenazas-para-el-sector-industrial

Motadata (2017). *Correlación de registro: una tendencia o una necesidad.* https://www.motadata.com/es/blog/log-correlation-trend-need/

Ocampo, D. (2019). *Investigación bibliográfica.* https://investigaliacr.com/investigacion/investigacion-bibliografica/

Palo Alto Networks (2021). *Cortex XDR: Rompa los silos de seguridad para las tareas de detección y respuesta.* https://www.paloaltonetworks.es/resources/whitepapers/cortex-xdr.html

Patton, B. (2019) *SIEM Integration Best Practices: Making the Most of Your Security Event Logs.* https://www.quest.com/docs/siem-integration-best-practices-making-the-most-of-your-security-event-logs-white-paper-27113.pdf

Ponce, J. (2021). *Un indicador de compromiso o IDC, es toda aquella información relevante que describe cualquier incidente de ciberseguridad, actividad o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.* https://dspace.ups.edu.ec/bitstream/123456789/20937/1/UPS-GT003378.pdf

Quilachamin, A (2020). *Despliegue de un sistema de gestión de eventos e información de seguridad de código abierto.* https://bibdigital.epn.edu.ec/handle/15000/20870

Robalino, J (2018) *Propuesta Metodológica y Simulación de la Implementación de un SIEM basado en la Norma ISO 27001 y/o 27002.* http://bibdigital.epn.edu.ec/handle/15000/19672

Secureworks (2022). *XDR vs. SIEM: A cybersecurity leader's guide.* https://content.secureworks.com/-/media/Files/US/White%20Papers/Secureworks_ECO_XDRvsSIEM.ashx?modified=20220617194746

Sophos (2021). *Detección y respuesta ampliadas (XDR): Guía para principiantes.* https://assets.sophos.com/X24WTUEQ/at/2cjqbbwcmhhnk89v8qhx49/sophos-xdr-beginner-guide-es.pdf

Trendmicro (2020). *The XDR Payoff: Better Security Posture.* https://www.trendmicro.com/explore/amea_knowledge_hub/00435-xdr-en-rpt?lx=qUmYMe

Vielberth, M. Pernul, G. (2018). *A Security Information and Event Management Pattern*. https://www.researchgate.net/publication/337946451_A_Security_Information_and_Event_Management_Pattern

Watchguard (2022). *5 beneficios de integrar sistemas corporativos SIEM.* https://www.watchguard.com/es/wgrd-news/blog/5-beneficios-de-integrar-sistemas-corporativos-siem#:~:text=El%20sistema%20SIEM%20garantiza%20que,procedente%20de%20tantas%20fuentes%20diferentes

ANEXOS

ANEXO 1

A continuación se describe la experiencia y conocimiento del especialista encargado de validar la propuesta:

- Nombre:

Jonathan Fernando Quezada Haro

- Perfil profesional:

Consultor, auditor, docente y Magister en Ciberseguridad con más de 6 años de experiencia en el ámbito de la Seguridad de la Información, Ciberseguridad y Seguridad informática.

- Estudios realizados y certificaciones:
    - Escuela Superior Politécnica de Chimborazo (Riobamba – Ecuador)
    - Ingeniero en Electrónica en Telecomunicaciones y Redes.
    - Pontificia Universidad Católica del Ecuador (Ambato – Ecuador) _Máster en Ciberseguridad.
    - Universidad Internacional de la Rioja – UNIR_Máster en Liderazgo y Desarrollo Personal
    - Perito Informático acreditado por el Consejo de la Judicatura.
    - Certificado de Gestión y Gobierno de la Privacidad como DPO según el RGPD.
    - ISO/IEC 27001:2013 Internal Auditor I27001IA.
    - Diplomado en Auditoría Informática y Forense.
    - PSE Cortex Associate: Cortex XDR.
    - Palo Alto Networks Certified Network Security Engineer (PCNSE).
    - AT80FT - SG UTM to XG Firewall 18.0 - Certified Architect FastTrack.
    - Cloud One Channel Technical Campaingn Tren Micro.
    - 002.104 Kaspersky Endpoint Security and Management. Fundamentals

Ing. Jonathan Quezada