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 MAGISTER

Título del artículo
Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Anchala Sanez Mauricio Rodolfo
Tutor:
Mg. Toasa Guachi Renato Mauricio Ph.D. Urdaneta Herrera Maryory

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.

Elaborado por: Mauricio Rodolfo Anchala Sanez, de C.I: 1717668691, estudiante de la Maestría: de 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 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Mg. Renato Mauricio Toasa Guachi

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.

Elaborado por: Mauricio Rodolfo Anchala Sanez, de C.I: 1717668691, estudiante de la Maestría: de 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 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

PhD. Maryory Urdaneta Herrera

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Mauricio Rodolfo Anchala Sanez con C.I: 1717668691, autor del proyecto de titulación denominado: Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos. 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 2024

Firmado electrónicamente por:
MAURICIO RODOLFO ANCHALA SANEZ

Firma

https://orcid.org/0009-0003-2965-7997

Tabla de contenidos

Índice de tablas

No se encuentran elementos de tabla de ilustraciones.

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

Debido al importante crecimiento tecnológico originado con el covid-19, la seguridad de la información ha venido tomando mucha fuerza debido a los ataques informáticos que cada día son más agresivos y sofisticados, agregándole a esto la reciente ley orgánica de protección de datos de Ecuador, misma que entró en vigor desde el año 2021, lo que ha motivado a las empresas a tomar acciones para proteger sus datos y la de sus clientes.

Las acciones para proteger los datos es una tarea que demanda inversión de recursos tecnológicos que día a día están en constante evolución, el uso de una solución antivirus ya no es suficiente para mantenerlos protegidos de amenazas que pueden atacar por cualquier medio que esté conectado a la red y tenga acceso al internet, el internet de las cosas es un punto clave que todavía está en desarrollo y genera muchos frentes de inseguridad para las empresas.

El teletrabajo promovido por el desarrollo de nuevas tendencias laborales y tecnológicas es otro de los puntos a controlar, debido a que los equipos corporativos empiezan a conectarse con otras redes fuera de las instalaciones empresariales, exponiéndose a ataques informáticos, sean desde sus casas o desde redes públicas.

En la sociedad existe una escaza cultura en temas de educación de seguridad informática, lo que expone a cualquier equipo a ser víctima de ataques que pueden estar fuera de la órbita del control tecnológico para las empresas, los firewalls o los mismos antivirus no garantizan una adecuada protección para la información de los equipos, las redes sociales, los correos electrónicos o cualquier sitio de internet puede ser un peligro si no se toman las adecuadas medidas de control.

La gestión de incidentes de seguridad es un aspecto fundamental para proteger los datos de las organizaciones. A medida que el panorama de amenazas se vuelve más complejo y sofisticado, las empresas buscan constantemente métodos que certifiquen la eficiencia y garantía de sus estrategias de respuesta, ya no solo dependiendo de los proveedores de servicios. En este escenario, la optimización de la gestión de incidentes se convierte en una prioridad para reducir el tiempo de descubrimiento y respuesta de los incidentes de seguridad, lo cual es crítico para mitigar el impacto de los ataques.

La optimización de la gestión de incidentes de seguridad con Lumu representa un cambio hacia una defensa más dinámica y adaptativa. Este enfoque proactivo no solo mejora la capacidad de una organización para enfrentar las amenazas cibernéticas actuales, sino que también la prepara para

los desafíos futuros, asegurando que pueda responder de forma efectiva en este entorno digital en constante cambio.

Problema de investigación

En el modelo convencional, las organizaciones a menudo adoptan una postura reactiva, enfrentando dificultades para detectar amenazas de manera temprana y responder a ellas de forma efectiva. Este enfoque retrasa la identificación de incidentes, lo que puede resultar en una afectación significativa y costosa para la infraestructura tecnológica y la reputación de la empresa. Además, la falta de integración y automatización en los procesos de respuesta a incidentes conduce a una gestión ineficiente y a una pérdida de tiempo valioso durante situaciones críticas para la continuidad del negocio provocando pérdida de confianza de sus clientes lo que relaciona con la afectación económica.

Ante este escenario, surge la necesidad de explorar soluciones como Lumu, que prometen una optimización mediante un enfoque proactivo. El problema radica en cómo implementar y adaptar esta herramienta dentro de los protocolos de seguridad existentes en las empresas para maximizar su eficacia.

Los resultados de este análisis e investigación permitirán difundir el conocimiento con personas involucradas en el mundo de la seguridad informática, ciberseguridad y todos los relacionados en el entorno tecnológico, para que sirva como referencia para adoptar nuevos modelos de automatizados de seguridad.

Bajo esta premisa, se puede plantear lo siguiente:

¿Cómo puede Lumu mejorar el descubrimiento temprano de amenazas y la réplica a incidentes para lograr obtener su infraestructura segura?

Objetivo general

Desarrollar una propuesta de seguridad para mejorar la detección y respuesta ante amenazas informáticas, mediante la integración de inteligencia de amenazas en tiempo real y análisis automatizado, para la contención de ataques informáticos con Lumu.

Objetivos específicos

- Contextualizar los fundamentos de los modelos de defensa que trabaja la solución Lumu.
- Evaluar la eficacia de Lumu en la detección de incidentes de seguridad, determinando qué tipos de amenazas se identifican más rápidamente.
- Diseñar un informe de gestión de respuesta a incidentes asistido por Lumu.

- Validar el impacto obtenido con Lumu en un caso estudio con criterio de especialistas.

Vinculación con la sociedad y beneficiarios directos:

Este documento de titulación puede contribuir directamente al ODS 9.1 como lo describe, Naciones Unidas (2015) “Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, incluidas infraestructuras regionales y transfronterizas, para apoyar el desarrollo económico y el bienestar humano, haciendo especial hincapié en el acceso asequible y equitativo para todos”, que intenta fomentar la innovación y la infraestructura resiliente, al mejorar la capacidad de las organizaciones para prevenir y responder a incidentes de seguridad cibernética, protegiendo así la infraestructura crítica y los datos personales.

Además, al asegurar la integridad de los sistemas de información, se apoya el ODS 16, que promueve sociedades pacíficas e inclusivas, facilitando el acceso a la justicia y la construcción de instituciones eficaces, responsables e inclusivas a todos los niveles. Los beneficiarios directos incluyen no solo a las entidades que adoptan Lumu, sino también a sus usuarios y clientes, quienes disfrutan de un entorno digital más seguro y confiable, lo que a su vez impulsa el crecimiento económico y la confianza en los servicios digitales.

El resultado de este trabajo se pretende difundir por medio de la red social LinkedIn enfocado a profesionales del entorno tecnológico, ciberseguridad, gerentes o cualquier persona involucrada en estas áreas por medio de los grupos de Seguridad y Tecnología.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1. Contextualización general del estado del arte

La nueva era tecnológica ha llevado a las empresas de distintos segmentos a implementar tecnologías que permitan la prevención, mitigación y protección de su infraestructura tecnológica a todo nivel, sin embargo, existe mucho por hacer, la falta de cultura en temas de seguridad de la información sumado a la Ley Orgánica de Protección de Datos Personales está dejando en evidencia que existe falta de conocimiento y poca inversión en las empresas.

Como se puede ver en la Figura 1, en el análisis del Observatorio de Ciberseguridad con corte al año 2020, se evidencia que a nivel país se han implementado políticas que han permitido la mejora en estos procesos en materia de seguridad informática, pero aún falta mucho por trabajar.

Figura 1

Políticas y Estrategia de Seguridad Cibernética

Nota. Adaptado de "*Políticas y Estrategia de Seguridad Cibernética"* (p. 94)*,* por Observatorio Ciberseguridad, 2020.

Según el Observatorio Ciberseguridad (2020) indica lo siguiente:

> Los desafíos significativos en el ámbito de la ciberseguridad, al igual que en el ámbito de Internet, tienen alcance global. Por consiguiente, es fundamental que los países de América Latina y el Caribe sigan promoviendo una cooperación más estrecha entre sí, implicando a todos los participantes pertinentes, y estableciendo sistemas de supervisión, análisis y evaluación de impacto en materia de ciberseguridad, tanto a nivel nacional como regional. (p. 17)

Según afirma Kaspersky (2023):

> Brasil encabeza el ranking de los países latinoamericanos más afectados, con 1.8 millones de intentos de infección durante el período analizado, lo que también lo posiciona como líder a nivel mundial. Le sigue México, con 271 mil intentos y en tercer lugar a nivel global. Colombia registra 72 mil intentos, seguido por Perú con 58 mil, Ecuador con 36 mil, Argentina con 29 mil y Chile con 21 mil. En Chile, el troyano brasileño Banbra es la familia de malware más activa. A nivel mundial, Rusia, India y China ocupan los puestos 2, 4 y 5 respectivamente en el ranking.

Ecuador está entre los países más afectados en intentos de infección, es por ello por lo que es importante analizar propuestas implementación de controles de respuesta y gestión a incidentes, dentro de las redes y equipos corporativos, en este preámbulo Lumu es una herramienta que permite gestionar los compromisos y acelerar las respuestas.

Según el sitio Lumu Technologies (2024):

> El propósito principal de la ciberseguridad es prevenir ataques y compromisos. A pesar de las enormes inversiones realizadas en este campo, las empresas continúan experimentando compromisos. Las estrategias actuales se centran en defensas y evaluaciones periódicas, dejando de lado el hecho de que el adversario puede ya haber penetrado en el sistema.
>
> La clave reside en la información, especialmente en los metadatos de la red. Lo que distingue al modelo Continuos Compromise Assessment de Lumu es su habilidad para recopilar, estandarizar y analizar una amplia gama de metadatos, que incluyen DNS, flujos de red, registros de acceso a proxys, firewalls y Spambox. La profundidad de visión que Lumu proporciona a través del análisis de estas fuentes de datos permite comprender el comportamiento de la red empresarial y detectar evidencia de compromisos de manera única.

> Según Ortega (2022) hoy en día, es común que todos los sistemas y redes enfrenten riesgos de seguridad debido a vulnerabilidades, lo que ha llevado a un aumento en la popularidad de la noción de seguridad informática en el último tiempo (p. 20).

> La mayoría de las pequeñas empresas dedican escasos recursos a la protección de sus sistemas y redes de comunicación, a menudo asumiendo que, al ser de tamaño reducido, no serán blanco de ataques. Sin embargo, en la actualidad, observamos cómo empresas de todo tipo y personas son blanco de hackers de diversas partes del mundo que buscan oportunidades en cualquier vulnerabilidad de seguridad para infiltrarse, robar información y exigir rescates (p.21).

> La solución SentinelOne, permite proteger los dispositivos según SentinelOne (2024) Singularity™XDR es una plataforma que fusiona funciones de prevención, detección, respuesta y búsqueda de amenazas, respaldadas por inteligencia artificial, en dispositivos finales de usuarios, contenedores, cargas de trabajo en la nube y dispositivos IoT. Nuestra solución capacita a las empresas contemporáneas para protegerse con mayor rapidez, alcance y precisión en todas sus áreas de vulnerabilidad.

La solución Netskope, según el sitio Netskope (2024) “es una plataforma de contenido de seguridad, basada en la nube que proporciona una visibilidad excepcional, datos en tiempo real y defensa contra amenazas al acceder a servicios en la nube, sitios web y aplicaciones privadas desde cualquier ubicación y dispositivo”.

El uso de herramientas complementarias para la protección de la infraestructura corporativa es vital, ya que estas permiten mantener una sinergia entre todas ellas, brindado solvencia al mitigar los riesgos que se detecten.

> Según afirma Logroño (2023) un elemento esencial en la ciberseguridad moderna es la inteligencia de amenazas, la cual resulta fundamental para que las organizaciones estén al tanto del cambiante panorama de amenazas. Al estar al día con las posibles amenazas, las organizaciones pueden tomar medidas proactivas para defenderse, reduciendo así el riesgo de ataques exitosos y resguardando sus activos valiosos (p.5).

Según Morales y otros (2020) “La estrategia de proteger la información mediante la implementación de firewall perimetral garantiza la seguridad de esta al salvaguardar su integridad, confidencialidad y disponibilidad, los cuales son los tres fundamentos principales de la seguridad de la información” (p.564).

1.2. Proceso investigativo metodológico

El método cualitativo por medio de entrevista, permitirá recolectar la información en base a las experiencias, así como lo afirma Álvarez (2014) “Una entrevista se define como un diálogo con una organización y objetivo específicos. En la investigación cualitativa, su propósito radica en comprender la visión del entrevistado sobre el mundo y analizar en detalle el significado de sus vivencias y experiencias” (p.109).

En el marco de este artículo, se empleará la técnica de entrevista como método que involucra la recolección de datos. La entrevista consta de diez preguntas diseñadas específicamente para el Gerente de Seguridades/Chief Information Security Officer (CISO) de la empresa de caso, conforme al proceso investigativo detallado en el Anexo 1: Entrevista al CISO.

Una vez ejecutada la entrevista se analizarán los datos para describir las impresiones de esta.

1.3. Análisis de resultados

Con base en las respuestas proporcionadas por el CISO durante la entrevista detallada en el Anexo 1, se puede concluir que la implementación de la herramienta Lumu ha tenido un impacto altamente positivo en la estrategia de ciberseguridad de la empresa objeto de estudio. Lumu ha sido eficazmente integrado como una solución central para mejorar la detección de amenazas en tiempo real, esta ha mejorado la capacidad de respuesta ante incidentes de seguridad. Su implementación ha permitido al equipo de seguridad enfocarse en actividades estratégicas al reducir la carga de trabajo manual a través de la automatización. Además, la adopción de Lumu fue fluida y se ajustó adecuadamente a las necesidades concretas de la organización, lo que resalta su flexibilidad y facilidad de configuración.

La gestión de falsos positivos y el proceso de verificación de alertas han demostrado ser eficaces, minimizando las interrupciones operativas. El apoyo y los recursos proporcionados por Lumu han facilitado la aceptación de la herramienta por parte del personal, lo que indica un compromiso con la educación continua en ciberseguridad. La integración de Lumu con otras soluciones de seguridad ha fortalecido la postura general de seguridad de la empresa, creando un entorno más sólido y cohesionado. Por último, existe un interés en futuras mejoras, como la capacidad de personalizar los paneles de control y el avance en inteligencia artificial para la predicción de amenazas, lo que podría orientar el desarrollo futuro de Lumu para satisfacer aún más las necesidades de la empresa.

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1. Resumen

Dentro del campo de la ciberseguridad, Lumu sobresale como una herramienta esencial que capacita a las organizaciones para enfrentar los ataques informáticos mediante una inteligencia avanzada en tiempo real. Al aprovechar las capacidades de Lumu, las empresas adquieren la habilidad de identificar y contrarrestar amenazas con una velocidad y precisión sin igual.

Los ataques informáticos están evolucionando rápidamente, lo que hace crucial que los equipos de seguridad tengan acceso a herramientas que proporcionen información en tiempo real sobre sus redes. Las capacidades de monitoreo y análisis continuo de Lumu aseguran que cualquier actividad inusual se identifique rápidamente, permitiendo tomar acciones inmediatas.

La gestión de incidentes de seguridad es una tarea compleja que requiere un enfoque integral. Lumu simplifica este proceso al ofrecer una plataforma optimizada para la respuesta ante incidentes. Su interfaz intuitiva y sistema de alertas automatizado permiten a los profesionales de seguridad priorizar y gestionar incidentes de manera efectiva.

Conforme las amenazas cibernéticas evolucionan hacia formas más complejas, resulta evidente la necesidad de soluciones avanzadas como Lumu. La incorporación de Lumu en la estrategia de ciberseguridad de una entidad fortalece su postura general de seguridad al añadir una capa de inteligencia en tiempo real, la cual es fundamental para una protección proactiva.

a. Palabras clave:

lumu, ataques informáticos, inteligencia en tiempo real, gestión de incidentes de seguridad, ciberseguridad

2.2. Abstract

In the field of cybersecurity, Lumu stands out as an essential tool that empowers organizations to combat cyberattacks through advanced real-time intelligence. By leveraging Lumu's capabilities, companies gain the ability to identify and counter threats with unprecedented speed and precision.

Cyberattacks are evolving rapidly, making it crucial for security teams to have access to tools that provide real-time insights into their networks. Lumu's monitoring and continuous analysis capabilities ensure that any unusual activity is quickly identified, enabling immediate action to be taken.

Managing security incidents is a complex task that requires a comprehensive approach. Lumu simplifies this process by offering a platform optimized for incident response. Its intuitive interface

and automated alert system allow security professionals to prioritize and manage incidents effectively.

As cyber threats evolve into more complex forms, the need for advanced solutions like Lumu becomes evident. Integrating Lumu into an entity's cybersecurity strategy strengthens its overall security posture by adding a layer of real-time intelligence, which is crucial for proactive protection.

a. Keywords

lumu, cyber-attacks, Real-time intelligence, security incident management, cybersecurity

2.3. Introducción

En el dinámico entorno tecnológico actual, la seguridad cibernética se ha vuelto una prioridad inevitable para organizaciones de todas las dimensiones. Ante la creciente amenaza de ataques informáticos, resulta crucial contar con herramientas que brinden inteligencia en tiempo real y una gestión eficaz de incidentes de seguridad. Lumu emerge como una solución avanzada, diseñada para abordar estos desafíos con notoria eficacia.

Esta innovadora herramienta redefine la seguridad en redes al posibilitar a las empresas detectar amenazas cibernéticas de forma proactiva y responder con agilidad. Lumu se destaca por su capacidad para analizar el tráfico de red e identificar comportamientos maliciosos, ofreciendo así una visión actualizada y clara de la seguridad informática.

La administración de incidentes de seguridad se simplifica con Lumu, al proporcionar un sistema estructurado y automatizado para atender las alertas de seguridad. Esto no solo mejora la capacidad de respuesta frente a incidentes, sino que también permite a los equipos de seguridad enfocarse en la prevención y en el perfeccionamiento continuo de las estrategias de protección.

Este artículo profundizará en cómo Lumu está transformando la ciberseguridad, proporcionando a las organizaciones una ventaja decisiva en la lucha contra los ataques informáticos y mejorando su capacidad para proteger sus activos digitales más valiosos.

1.1. Ciberseguridad y la Necesidad de Gestión de Incidentes

Según lo afirma Kaspersky (2024) la seguridad cibernética es un ámbito dinámico y en constante cambio que se enfoca en salvaguardar sistemas, redes y programas contra ataques digitales. Estos suelen buscar acceder, modificar o destruir información confidencial, extorsionar a usuarios o interrumpir las operaciones comerciales normales.

La gestión de incidentes en ciberseguridad es esencial, ya que permite a las organizaciones reaccionar de manera rápida y eficiente ante violaciones de seguridad o ataques cibernéticos. Una gestión efectiva minimiza el impacto negativo en las operaciones comerciales, protege la reputación de las empresas y garantiza la confiabilidad, integridad y disponibilidad de la información crítica. Al identificar y resolver incidentes de manera eficaz, las empresas pueden disminuir el tiempo de inactividad y los costos asociados con la recuperación de ataques.

Además, una gestión de incidentes sólida es crucial para el cumplimiento de normativas y regulaciones legales. Muchas regulaciones requieren que las organizaciones tengan planes de respuesta ante incidentes y notifiquen brechas de seguridad dentro de plazos específicos. Esto no solo contribuye a mantener la confianza de clientes y socios, sino que también evita sanciones legales y financieras que podrían derivarse de no seguir los procedimientos adecuados. Por lo que la gestión de incidentes es un mecanismo esencial de una estrategia integral de ciberseguridad.

Según Lumu Technologies (2024) Lumu es una plataforma de seguridad cibernética especializada en proporcionar inteligencia de amenazas en tiempo real, lo que permite a las organizaciones identificar y responder a incidentes de seguridad de manera más rápida y efectiva. Al utilizar la recopilación continua de datos de telemetría y la correlación de eventos de seguridad, ofrece una visión clara de las amenazas que enfrentan las infraestructuras de TI. Esto se traduce en una mayor capacidad para detectar compromisos y anomalías que podrían indicar una brecha de seguridad, lo que ayuda a las empresas a pasar de una postura reactiva a una proactiva en la gestión de la ciberseguridad.

Además, Lumu destaca por su simplicidad y facilidad de integración con los sistemas existentes, lo que significa que las organizaciones pueden empezar a obtener beneficios sin largos períodos de implementación o configuración compleja. La plataforma utiliza algoritmos avanzados y aprendizaje automático para analizar y clasificar amenazas, proporcionando a los equipos de seguridad información accionable. Esto no solo mejora la eficiencia de los equipos de seguridad al reducir los falsos positivos, sino que también permite una respuesta más rápida y precisa a los incidentes, minimizando así el impacto potencial de las amenazas cibernéticas en la organización.

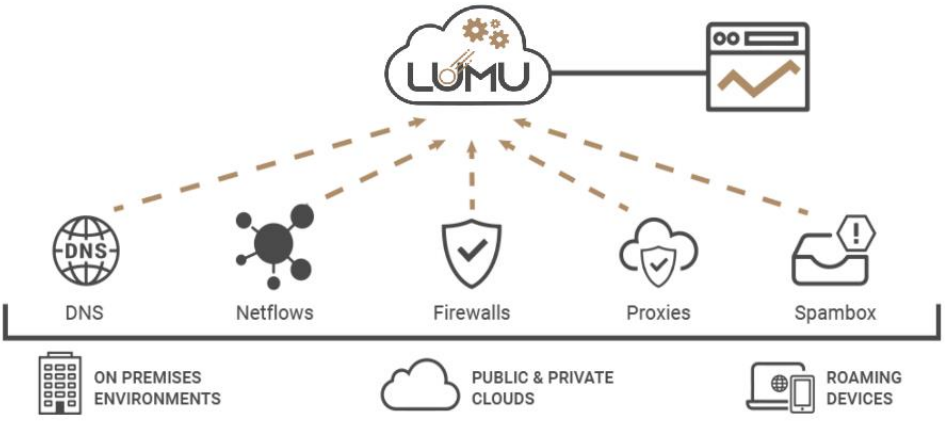
Según Lumu Technologies (2024) la ciberseguridad tiene un objetivo claro: prevenir compromisos. A pesar de las inversiones considerables realizadas en este ámbito, las empresas continúan experimentando compromisos. Las estrategias actuales se concentran en defensas y evaluaciones periódicas, olvidando que el adversario puede ya estar dentro. Solo se puede encontrar lo que se busca. Lumu ofrece la capacidad de buscar compromisos de manera deliberada y constante.

1.2. Análisis de la detección de Lumu en los comportamientos anómalos en la red.

Lumu proporciona una solución basada en la nube que recopila y estandariza metadatos en toda su infraestructura de red, incluidas consultas de DNS, tráfico de red, registros de acceso a proxy y firewall, y filtros de spam. Luego utiliza inteligencia artificial para conectar inteligencia sobre amenazas de estas fuentes dispares para detectar y aislar puntos de compromiso confirmado.

Figura 2

Interacción de Lumu en la red



Nota. Adaptado de "*La Necesidad de un Nuevo Avance en Ciberseguridad",* por Lumu, 2024.

Lumu Defender proporciona integraciones flexibles y preconfiguradas que simplifican el enrutamiento de casos de compromiso confirmados por Lumu a cualquier herramienta externa a través de API, lo que facilita la automatización de la reparación y la reparación. Además, las integraciones personalizadas brindan varias opciones de integración con listas de bloqueo, firewalls, SIEM y otras herramientas.

Figura 3

Integraciones con Lumu

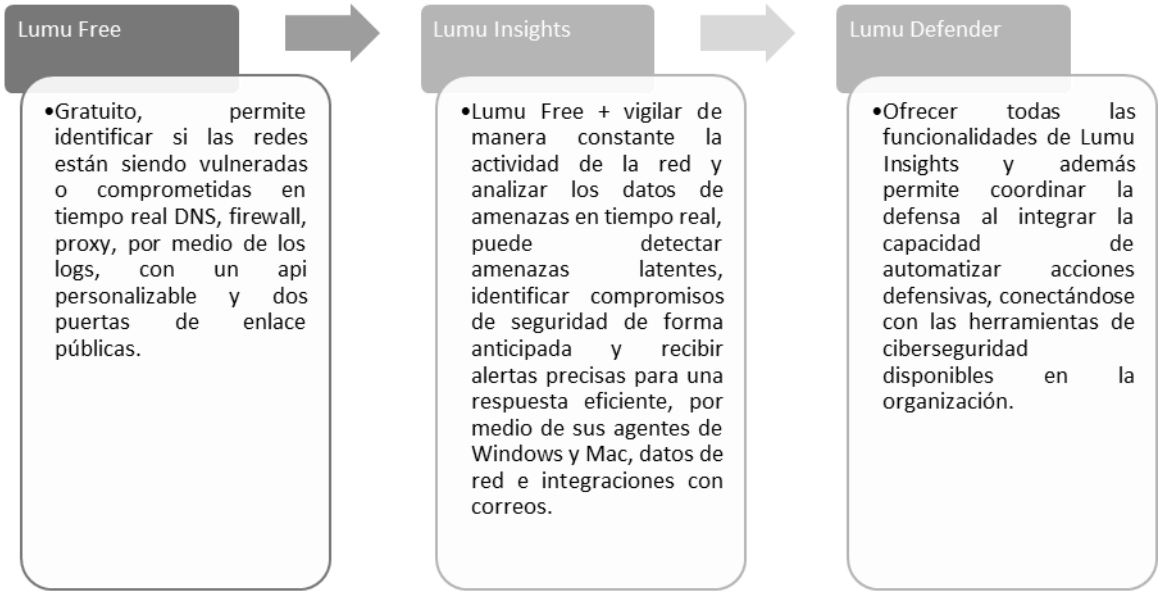
Nota. Adaptado de "*La Necesidad de un Nuevo Avance en Ciberseguridad",* por Lumu, 2024.

Las soluciones de Lumu se destacan por su enfoque en la inteligencia de amenazas en tiempo real, brindando una visión clara del panorama de amenazas a nivel global. Sus soluciones identifican amenazas ocultas y priorizan los incidentes más relevantes, lo que ayuda a las organizaciones a optimizar sus recursos de seguridad. Además, Lumu ofrece detección temprana de compromisos y genera alertas precisas, permitiendo una respuesta rápida y eficiente a las amenazas.

Lumu presenta tres soluciones principales como se muestra en la Figura 4: Lumu Free, Lumu Insights y Lumu Defender.

Figura 4

Soluciones de Lumu



1.3. Gestión de Incidentes de Seguridad con Lumu

El proceso de gestión de incidentes se basa en tres pilares detección, investigación y resolución como se muestra en la Figura 5.

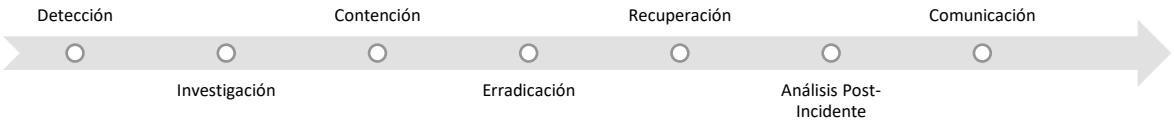
Figura 5

Proceso de gestión de incidencias con Lumu

Dentro del proceso de gestión de incidentes de seguridad se desarrollan los siguientes pasos mostrados en la Figura 6:

Figura 6

Línea de tiempo gestión de incidentes



Detección: Lumu supervisa el tráfico de red para identificar comportamientos anómalos o indicadores de compromiso. Las alertas se generan cuando se detecta actividad sospechosa en los dispositivos conectados a la red.

Investigación: Después de recibir una alerta, se lleva a cabo una investigación interna para identificar la naturaleza y el alcance del incidente utilizando los recursos disponibles. Esto puede implicar la revisión de registros y la correlación de eventos con los metadatos proporcionados en la base de conocimientos de Lumu.

Contención: Se implementan acciones para controlar el incidente, como el aislamiento de los sistemas afectados o la restricción del acceso a los recursos comprometidos, teniendo en cuenta la presencia de un agente instalado en todos los dispositivos informáticos conectados a la red, incluyendo los servidores.

Erradicación: Se elimina la fuente del incidente, lo que puede incluir la limpieza de malware, el cierre de vulnerabilidades y el fortalecimiento de las defensas, con los demás equipos de seguridad, incluyendo software antivirus, antispam u otro software de protección.

Recuperación: Se restauran los sistemas y servicios a su funcionamiento normal, asegurándose de que la amenaza se ha eliminado por completo y que el entorno es seguro, no solo a nivel del servicio afectado, sino de cada elemento que interactúa con el mismo.

Análisis Post-Incidente: Se analiza el incidente para comprender qué sucedió, cómo se manejó y cómo se puede mejorar la respuesta en el futuro, esto se trabaja a nivel operativo con área de seguridades, Lumu como tal recolecta toda información de la trazabilidad del caso para poner a disposición de los expertos. De ser necesario se deben actualizar las políticas y se refuerza la capacitación según amerite.

Comunicación: Se mantiene informados a los equipos internos y si es necesario, a los clientes y partes interesadas externas durante todo el proceso. Este se comunica con todos los equipos de la red, siendo estos los firewalls, routers, endpoints, software antivirus para replicar la regla o política para contener futuros ataques.

Este proceso debe adaptarse a las políticas y procedimientos específicos de cada organización. Lumu proporciona las herramientas e inteligencia necesarias para facilitar este proceso y mejorar la postura de seguridad general, cada organización deberá adaptar a su arquitectura y su realidad.

1.4. Inteligencia en Tiempo Real

La capacidad de respuesta durante la gestión de incidentes de seguridad se ve mejorada de múltiples formas por la inteligencia en tiempo real de Lumu, teniendo en cuenta cada uno de los aspectos cruciales sobre la relevancia de la visibilidad de la red en la prevención de ataques.

Detección a tiempo: Permite obtener una visión completa de toda la red identificando señales de alerta tempranas de posibles ataques. Esto incluye tráfico inusual, intentos de acceso no autorizados y patrones de comunicación sospechosos. Al detectar estos signos tempranamente, se pueden tomar medidas antes de que se materialice un ataque completo.

Análisis del Tráfico: Examinar todo el tráfico de la red es fundamental para comprender qué datos se están transmitiendo y si se ajustan a un comportamiento habitual de la red. La inteligencia en tiempo real puede desglosar este tráfico para detectar posibles contenidos maliciosos, comunicaciones con servidores de comando y control, o transferencias de datos no autorizadas.

Gestión de Vulnerabilidades: La visibilidad permite a las organizaciones mapear su superficie de ataque y entender dónde pueden existir debilidades. Esto es crucial para implementar parches, actualizar sistemas y fortalecer las configuraciones de seguridad para prevenir ataques que exploten estas vulnerabilidades.

Cumplimiento de Normativas: Las normativas de seguridad y privacidad requieren que las empresas salvaguarden la información confidencial, con énfasis especial en Ecuador, donde se debe cumplir con la Ley Orgánica de Protección de Datos. La visibilidad de la red contribuye a asegurar el cumplimiento de estas regulaciones al proporcionar pruebas de que los datos están siendo gestionados y protegidos de manera adecuada.

Respuesta a los Incidentes: Ante un incidente, una comprensión nítida de la red permite a los equipos de seguridad identificar con rapidez el origen del ataque, comprender su alcance y comportamiento utilizando la matriz de MITRE, y adoptar medidas para contener y eliminar la amenaza, minimizando de este modo su impacto.

Optimización de Recursos: Con una visión clara de la red, los equipos de seguridad pueden asignar sus recursos de manera más efectiva, enfocándose en las áreas y procesos de mayor riesgo, asegurando que las medidas de protección sean proporcionales a la amenaza, cada organización por su naturaleza del negocio es menos o más vulnerable por los atacantes informáticos.

Educación y Concienciación: La visibilidad de la red también sirve como una herramienta educativa, proporcionando ejemplos reales de intentos de ataque y cómo la red los maneja. Esto puede ayudar a fomentar una mayor conciencia de seguridad entre los empleados y promover mejores prácticas incluyendo adoptar otras tecnologías complementarias.

Cada uno de estos puntos es crucial para una estrategia de seguridad integral. La visibilidad de la red no es solo una herramienta de prevención, sino también un componente esencial para una respuesta rápida y efectiva ante incidentes de seguridad.

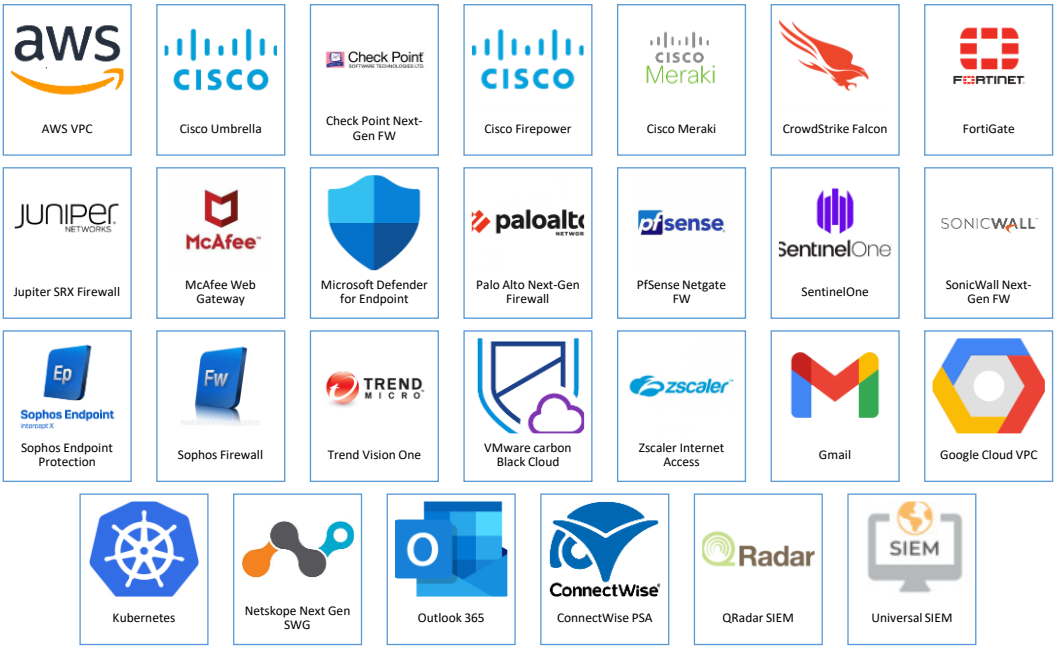
1.5. Integración de Lumu con otras herramientas

La integración de Lumu con otras aplicaciones de ciberseguridad es una estrategia que fortalece la postura de seguridad de una organización, proporcionando una defensa en capas más efectiva y una gestión de incidentes más ágil y precisa.

Lumu puede integrar con Data Collection, Response y SecOps como se muestra en la siguiente Figura 7:

Figura 7

Data Collection, Response y SecOps compatibles con Lumu



Para considerar el análisis de estas herramientas se las agrupado de acuerdo a su funcionalidad

Herramientas de Seguridad en la Nube (Netskope, Zscaler Internet Access)

Visibilidad Mejorada: Permite un monitoreo detallado del uso de aplicaciones en la nube y su tráfico.

Control de Acceso Dinámico: Facilita la implementación de políticas de seguridad informadas por la inteligencia de amenazas en tiempo real.

Soluciones de Protección de Endpoints (Sentinel One, CrowdStrike Falcon)

Respuesta Automatizada: Automatiza la respuesta a incidentes, como el aislamiento de endpoints comprometidos.

Detección de Comportamientos Anómalos: Mejora la capacidad de detectar comportamientos sospechosos en los dispositivos.

Orquestación de Contenedores (Kubernetes)

Seguridad en Contenedores: Aumenta la seguridad en entornos de contenedores al monitorear el tráfico y detectar anomalías.

Cumplimiento de Políticas de Seguridad: Ayuda a cumplir con regulaciones mediante la visibilidad y control de las comunicaciones.

Firewalls y Gateways (Sophos Firewall, Fortigate firewall)

Defensa Perimetral Reforzada: Integra inteligencia de amenazas para fortalecer la defensa perimetral.

Análisis de Tráfico Enriquecido: Proporciona un análisis más profundo del tráfico para identificar amenazas ocultas.

Plataformas de Correo Electrónico (Outlook 365, Gmail)

Protección contra Phishing: Ayuda a identificar intentos de phishing y otras amenazas que se relacionan con el correo electrónico.

Educación de Usuarios: Informa y educa a los usuarios sobre las amenazas detectadas.

Infraestructura de la Nube (AWS VPC, Google Cloud VPC)

Visibilidad en la Nube: Ofrece visibilidad adicional en el tráfico de red dentro de las VPCs.

Identificación de Configuraciones Inseguras: Detecta configuraciones de red potencialmente vulnerables.

Sistemas de Información y Eventos de Seguridad (QRadar SIEM, Universal SIEM)

Correlación de Eventos: Permite una visión holística de la seguridad al correlacionar eventos de múltiples fuentes.

Alertas Inteligentes: Enriquece el SIEM con inteligencia de amenazas actualizada para mejorar la calidad de las alertas.

Al integrarse con estas herramientas tecnológicas, Lumu fortalece la capacidad de detectar y responder a incidentes de ciberseguridad, mejora la administración de la seguridad y la eficiencia operativa, y ofrece una perspectiva más exhaustiva y contextualizada de las amenazas en tiempo real.

1.6. Beneficios de integrar Lumu en la estrategia de ciberseguridad de una organización con herramientas complementarias.

La integración de Lumu con otras aplicaciones de gestión de incidentes de ciberseguridad proporciona varios beneficios que mejoran la capacidad de una organización en la detección, respuesta y recuperación de incidentes de seguridad.

Mejora en la Detección de Amenazas: Al integrar Lumu con otras aplicaciones de seguridad, como sistemas de prevención de intrusiones o soluciones de seguridad de endpoints, se puede lograr una detección de amenazas más rápida y precisa. Lumu aporta su inteligencia de amenazas para identificar comportamientos sospechosos o maliciosos que podrían pasar desapercibidos por una sola aplicación.

Automatización de la Respuesta a Incidentes: La integración permite la automatización de la respuesta a incidentes. Por ejemplo, si Lumu detecta una comunicación maliciosa, puede activar automáticamente una respuesta en otras aplicaciones, como el aislamiento de un endpoint infectado o el bloqueo de una dirección IP maliciosa en un firewall.

Correlación de Datos y Contextualización: Lumu puede enriquecer los datos recopilados por otras aplicaciones con su contexto de amenazas, lo que favorece a los analistas de ciberseguridad comprender mejor la naturaleza y el alcance de un incidente. Esto es crucial para una evaluación precisa del impacto y la planificación que se puede tener en sus respuestas.

Eficiencia Operativa: La integración de Lumu con herramientas de gestión de incidentes y plataformas SIEM (Security Information and Event Management) puede mejorar la eficiencia operativa al reducir la cantidad de falsos positivos y centralizar la visión de la seguridad, lo que permite a los equipos de seguridad concentrarse en las amenazas reales.

Cumplimiento y Reportes: Lumu puede ayudar a generar informes más completos y detallados para cumplir con regulaciones y estándares de la industria. La integración facilita la colección y el análisis de datos necesarios para los informes de cumplimiento.

Educación y Concienciación: La integración de Lumu con plataformas de comunicación y formación puede ayudar a difundir información sobre amenazas y buenas prácticas de seguridad entre los empleados, aumentando la conciencia de seguridad en toda la organización.

Mejora Continua: La retroalimentación constante entre Lumu y otras aplicaciones permite refinar continuamente los procesos de seguridad y las políticas de respuesta a incidentes, adaptándose a las amenazas emergentes y cambiando las condiciones de seguridad.

2.4. Metodología

2.1. Metodología de investigación

La metodología de investigación aplicada en este artículo se centró en métodos mixtos, combinando análisis y colección de información de múltiples fuentes con la realización de una entrevista estructurada. Este enfoque permitió una comprensión amplia y detallada del tema de investigación. La recopilación de información se llevó a cabo por medio de la revisión de la literatura relevante, la exploración de sitios web especializados y el análisis de documentos existentes, lo que proporcionó una base sólida de conocimiento previo y permitió la identificación de tendencias y patrones actuales relevantes para el tema de investigación.

Por otro lado, la entrevista estructurada fue un método adicional para obtener información específica y profunda sobre el estudio. Esta técnica consta de un conjunto de preguntas predefinidas para garantizar la coherencia y entendimiento del tema tratado con sus respuestas. La entrevista brinda acceso a perspectivas personales y experiencias de primera mano, enriquecieron el análisis y agregó una dimensión cualitativa al estudio. La combinación de estos métodos proporciona un enfoque de investigación integral y sólido que garantiza la eficacia y seguridad de los resultados obtenidos.

Metodología de Evaluación de Amenazas Cibernéticas

Lumu utiliza una combinación de técnicas y herramientas para la identificación de amenazas en la ciberseguridad.

Como lo expresado por Marco Brando en reciente webinar “Product Training | Cacería de amenazas inteligente, sin complicaciones” (Canal Lumu Technologies, 2023, 27:10) se detallan las siguientes características de la metodología de Lumu:

Colección de Metadatos: Lumu recopila metadatos de tráfico de red, como direcciones IP, URLs, y hashes de archivos, para obtener una visión amplia de la actividad de la red sin comprometer la privacidad.

Análisis de Compromiso: Utiliza algoritmos avanzados para analizar los metadatos y detectar indicadores de compromiso (IoCs) que señalan la presencia de amenazas.

Inteligencia de Amenazas: Se integra con bases de datos de inteligencia de amenazas para comparar los IoCs detectados con patrones conocidos de malware, phishing y otras ciberamenazas.

Aprendizaje Automático: Emplea modelos de aprendizaje automático para identificar patrones anómalos y predecir posibles ataques basándose en el comportamiento del tráfico de red.

Sandboxing: Para los archivos sospechosos, Lumu puede utilizar entornos de pruebas seguros (sandboxes) donde los archivos se ejecutan y observan para identificar comportamientos maliciosos.

DNS Analytics: Analiza las consultas DNS para identificar solicitudes a dominios maliciosos o de comando y control utilizados por atacantes.

Retroalimentación Continua: Lumu mejora continuamente su capacidad de detección al aprender de las interacciones y retroalimentación de los usuarios, ajustando sus modelos y heurísticas.

Integración con Otras Herramientas: Lumu tiene la capacidad de conectarse con otras soluciones de seguridad, como firewall y varios sistemas de prevención de intrusos, con el fin de mejorar el análisis y la respuesta ante incidentes.

Estas técnicas y herramientas permiten a Lumu proporcionar una detección de amenazas precisa y en tiempo real, ayudando a las organizaciones a responder de manera proactiva a las ciberamenazas.

2.2. Criterios para la clasificación y priorización de las amenazas detectadas con Lumu

Lumu clasifica y prioriza las amenazas detectadas utilizando varios criterios detallados:

Severidad de la Amenaza: Se evalúa el potencial de daño que una amenaza puede causar. Las amenazas se clasifican como críticas, altas, medias o bajas, basándose en la severidad del impacto que podrían tener en los activos de la organización.

Confianza en la Detección: Se considera la fiabilidad de los indicadores de compromiso (IoCs) utilizados para detectar la amenaza. Las amenazas detectadas con IoCs de alta confianza se priorizan sobre aquellas con IoCs menos fiables.

Contexto de la Amenaza: Se analiza el contexto en el que se detecta la amenaza, incluyendo el tipo de sistema afectado, los datos comprometidos y la posición de la amenaza dentro de la red. Esto ayuda a entender la urgencia y la prioridad de la respuesta.

Inteligencia de Amenazas Externa: Se integra información de fuentes externas de inteligencia de amenazas para evaluar la amenaza en un contexto más amplio. Esto incluye detalles sobre tácticas, técnicas y procedimientos (TTPs) de atacantes conocidos y campañas de amenazas actuales.

Comportamiento Anómalo: Se priorizan las amenazas que muestran un comportamiento anómalo significativo en comparación con el comportamiento normal de la red.

Tendencias y Evolución de la Amenaza: Se tiene en cuenta cómo ha evolucionado la amenaza a lo largo del tiempo y si muestra signos de escalada o propagación dentro de la red.

Impacto en la Continuidad del Negocio: Se evalúa cómo la amenaza podría afectar las operaciones del negocio. Las amenazas que podrían causar interrupciones significativas o pérdida de ingresos se priorizan más alto.

Capacidad de Respuesta: Se evalúa la destreza de la organización cara a la amenaza. Aquellas amenazas que necesitan una respuesta rápida o que pueden ser contrarrestadas de manera pronta se priorizan para garantizar una utilización eficaz de los recursos de seguridad.

Estos criterios permiten a Lumu proporcionar una clasificación y priorización precisa de las amenazas, asegurando que los equipos de seguridad puedan enfocarse en las amenazas más críticas y responder de manera efectiva.

2.3. Datos empresa caso estudio

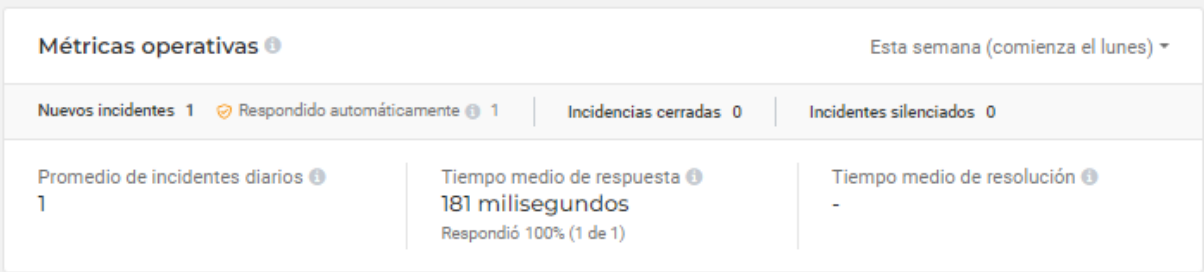
Para este caso se analizará una empresa multinacional que tiene presencia en varias ciudades del Ecuador, esta ha implementado la solución de Lumu en sus operaciones de ciberseguridad, de lo cual ha obtenido los siguientes resultados:

Detección de Amenazas:

La Figura 18 muestra el tiempo de duración media entre la notificación del incidente y el inicio de acciones para abordarlo es de 181 milisegundos de acuerdo con Lumu.

Figura 8

Métricas operativas Lumu

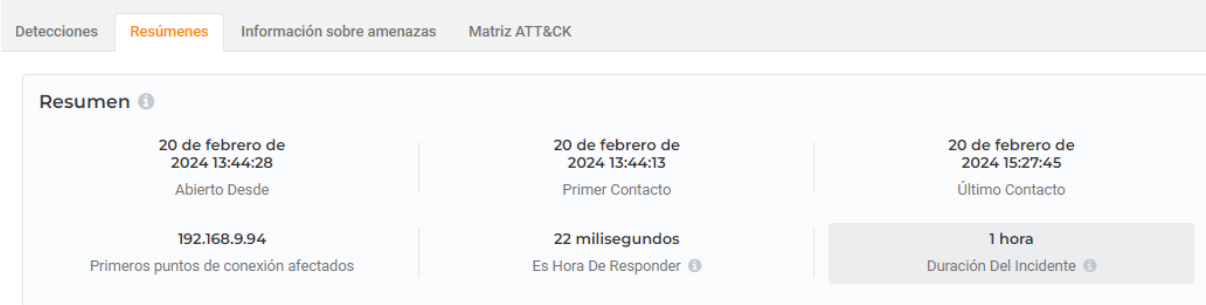


Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Para este caso en particular, para el inicio de respuesta es de 22 milisegundos como se evidencia en la Figura 9.

Figura 9

Resumen tiempos de respuesta



Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

El tiempo para aplicar remediación es de 1 hora considerando que replica las acciones hacia todos los equipos que conforman la red como son: Firewalls, Antivirus, etc.

Para el análisis del último trimestre, el tiempo de respuesta para 133 casos fue de 631.5 milisegundos como muestra la Figura 10.

Figura 10

Métricas operativas

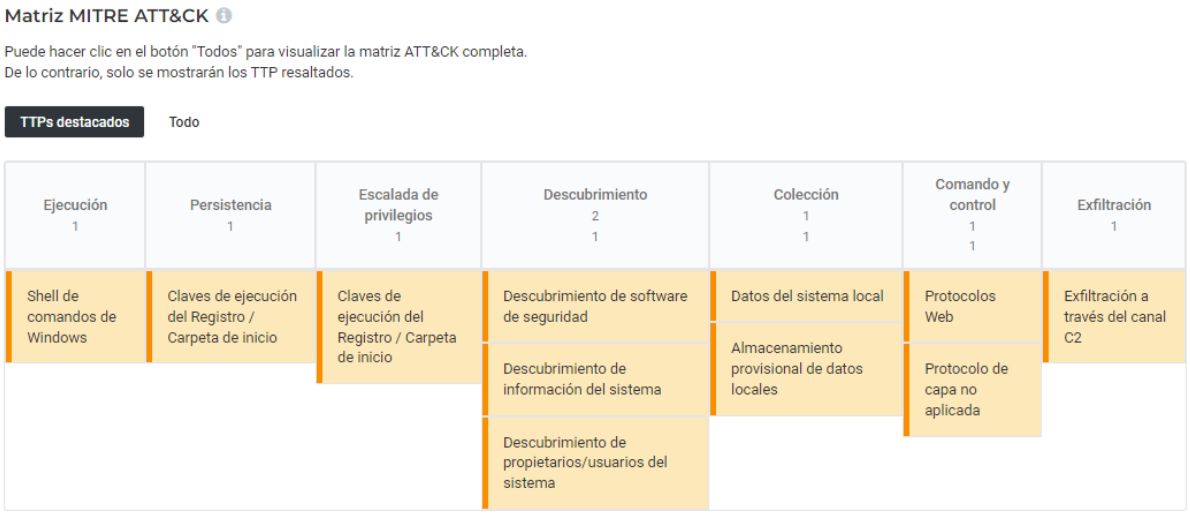
Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Respuesta a Incidentes:

Mediante la Matriz Mitre, se evalúa los TTPs destacados, lo que contribuye a la gestión de incidentes, específicamente en la clasificación automática de alertas y en la agilización de los procesos de respuesta como se visualiza en la Figura 11.

Figura 11

Matriz MITRE

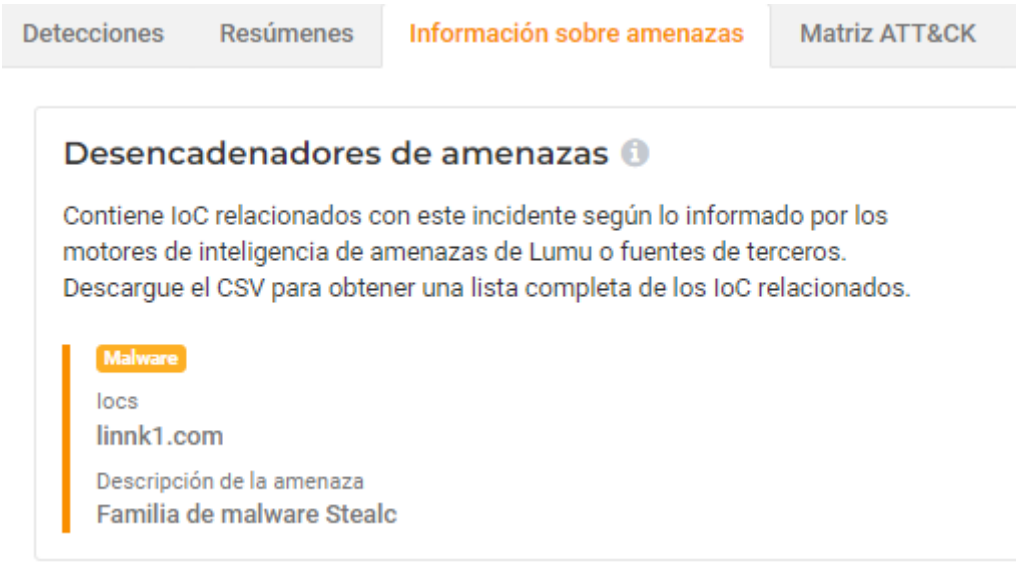


Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Lumu consulta sobre sus motores de inteligencia de amenazas o fuentes de terceros para obtener la información relacionada al incidente mostrado en la Figura 12.

Figura 12

Información sobre amenazas



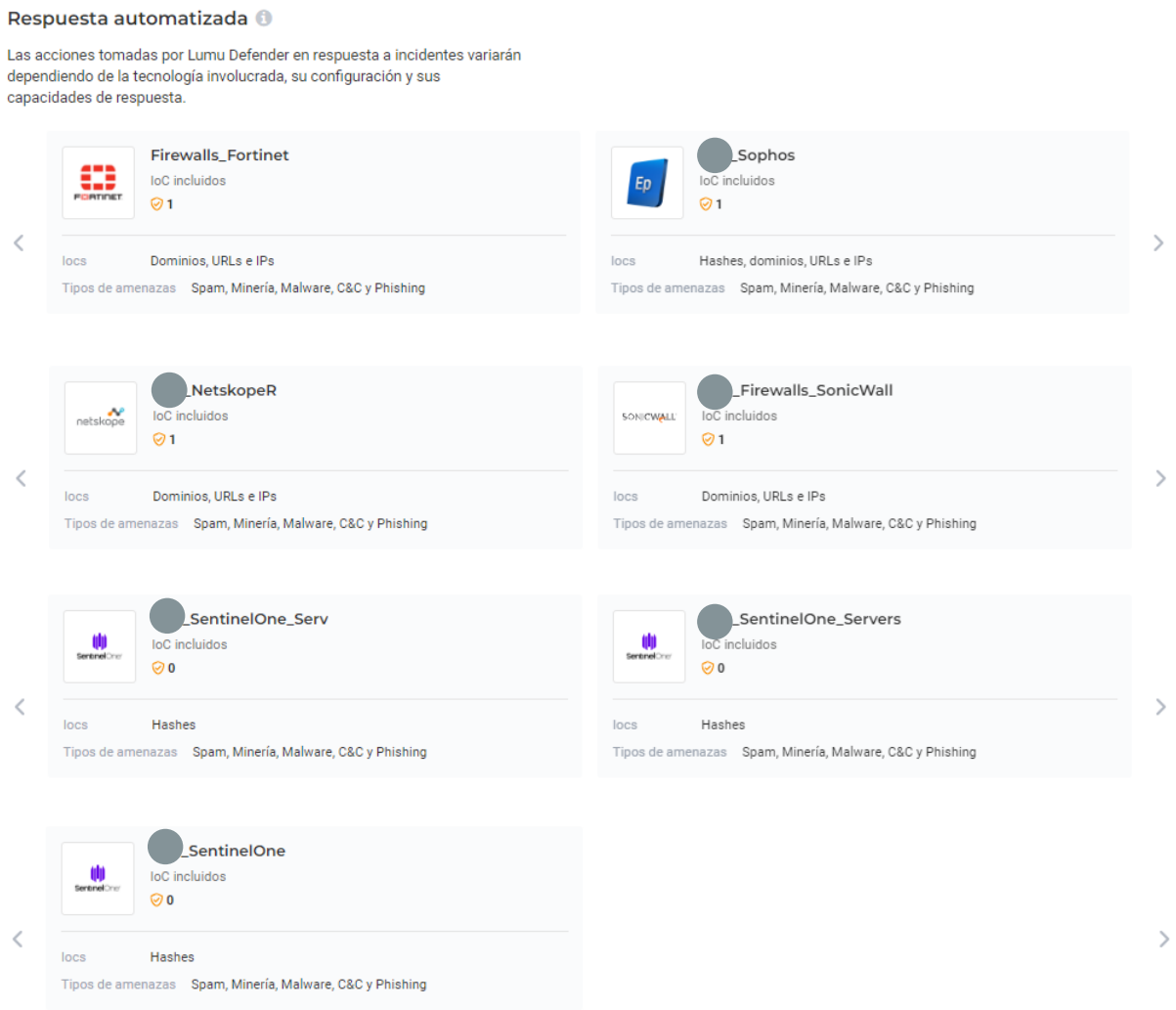
Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Integración con Herramientas Existentes:

Para el caso de la trazabilidad al caso de la Figura 8, se evidencia la respuesta automática replicando la remediación hacia todos los equipos que intervienen en la red como lo muestra la Figura 13, se evidencia la replicación de la solución al incidente.

Figura 13

Respuestas automatizadas



Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Lumu para este caso se integra con otras herramientas de seguridad como Netskope, SentinelOne, Fortinet, Sophos Firewall y SonicWall Firewall, esta integración ahorra considerablemente el tiempo de replicación de la solución a la amenaza, de esta manera mejora la postura de seguridad general.

La siguiente Figura 14, se muestra la línea de tiempo de Lumu para erradicar la amenaza, desde su primer contacto y la respuesta automatizada replicando la solución en todos los equipos de la red, hasta la notificación al responsable y su cierre de caso.

Figura 14

Operación línea de tiempo

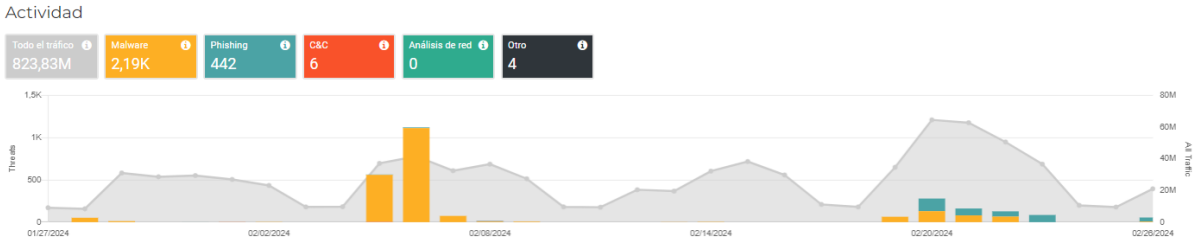
Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Impacto en la Operatividad: Es crucial examinar cómo Lumu afecta la operatividad diaria de la empresa, incluyendo la reducción del tiempo de inactividad y la eficiencia operativa mejorada gracias a una respuesta más rápida a incidentes.

La siguiente Figura 15 muestra la actividad clasificada por tipo de amenazas en el rango del 27/01/2024 al 26/02/2024, si los ataques fueran exitosos se generarían complicaciones en la operatividad de la compañía, en la imagen se visualiza 2.19K de intentos de afectación por malware, 422 intentos de phishing, 6 intentos de C&C y 4 clasificados como otros, que pueden estar relacionados con el comportamiento de las otras amenazas, estos datos del total de 823.83 millones de registros.

Figura 15

Actividad tráfico de red

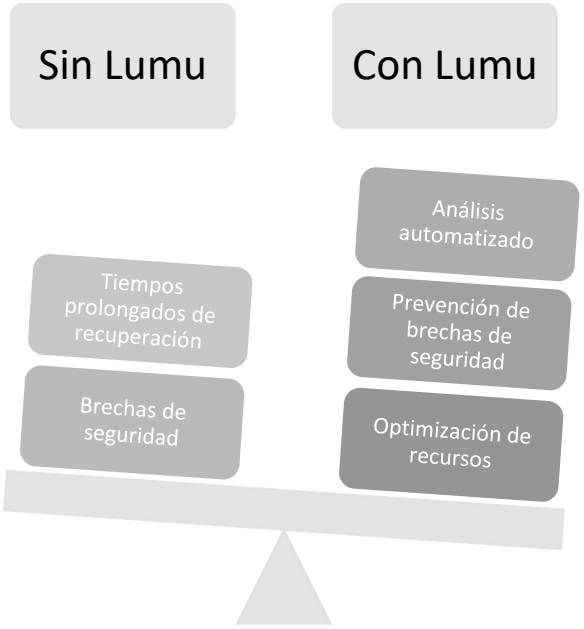


Nota. Adaptado de "*Portal administración Lumu",* por Lumu, 2024.

Reducción de Costos: Se debe considerar la reducción de costos asociados con la recuperación de ataques y el mantenimiento de la seguridad, como resultado de la implementación de Lumu, cada empresa tendrá su propia realidad o impacto, con o sin la herramienta como muestra la Figura 16.

Figura 16

Impacto de Lumu



Análisis General de Resultados: Desde la incorporación de Lumu, la empresa ha experimentado una notable mejora en la detección y respuesta, esta plataforma ha permitido identificar ataques en sus etapas iniciales, reduciendo significativamente el tiempo de respuesta ante incidentes. Esto

se ha traducido en una disminución del tiempo de inactividad que se relaciona con la reducción de los costos asociados a la recuperación de ataques.

Netskope proporciona una capa adicional de protección, especialmente para aplicaciones en la nube y tráfico web, lo que permite políticas de seguridad consistentes y efectivas. A su vez, SentinelOne refuerza la protección contra ataques de malware y ransomware gracias a su avanzado motor de inteligencia artificial que previene, detecta y responde automáticamente a las amenazas a los endpoints.

La sinergia entre estas soluciones y los equipos firewall ha mejorado la capacidad de la empresa para mitigar ataques proactivamente. La visibilidad mejorada y la inteligencia de amenazas proporcionada por Lumu han permitido ajustar las configuraciones de seguridad de manera más precisa y eficiente, fortaleciendo la seguridad de la empresa.

La implementación de Lumu, así como de Netskope y SentinelOne y su integración con dispositivos de firewall ha sido transformadora para la empresa. proporcionando una poderosa plataforma para la gestión de la seguridad, que mejora la protección de los activos digitales y la continuidad del negocio.

2.5. Resultados – Discusión

3.1 Propuesta de gestión de incidentes de seguridad con Lumu

En el contexto actual de amenazas cibernéticas en constante evolución, es imperativo que las empresas adopten una estrategia integral de gestión de incidentes de seguridad. Esta propuesta detalla la integración de inteligencia de amenazas con herramientas de seguridad avanzadas para una contención efectiva de ataques informáticos.

Objetivos:

- Establecer un sistema de gestión de incidentes de seguridad robusto y eficiente.
- Describir la inteligencia de amenazas para una detección y respuesta rápida ante ataques informáticos.
- Aprovechar las capacidades de Lumu, Netskope, SentinelOne, firewalls, y Outlook 365 para proteger la infraestructura de TI.

Establecer un sistema de gestión de incidentes de seguridad robusto y eficiente es crucial para cualquier organización que dependa de la tecnología para sus operaciones diarias. Un sistema de este tipo se encarga de identificar, analizar y responder a incidentes de seguridad de manera oportuna. Esto es esencial para proteger la información sensible y los activos digitales de la

empresa contra amenazas cibernéticas que evolucionan constantemente. Al contar con un sistema bien estructurado, las organizaciones pueden detectar rápidamente actividades sospechosas o maliciosas, responder de manera efectiva para mitigar el daño y recuperarse de los incidentes con el menor impacto posible en sus operaciones comerciales.

La eficiencia de un sistema de gestión de incidentes de seguridad se refleja en su capacidad para minimizar el tiempo de respuesta y la gravedad de los incidentes. Esto se puede logra a través de la integración de herramientas avanzadas como Lumu, que proporciona inteligencia de amenazas en tiempo real y monitoreo constante del tráfico de red. Además, un sistema robusto incluye procedimientos claros y bien practicados, capacitación regular del personal y una cultura de seguridad que involucra a todos los niveles de la organización. Al mantener un enfoque proactivo y estar preparados para enfrentar incidentes de seguridad, las empresas pueden asegurar la continuidad de sus operaciones y mantener la confianza de sus clientes y socios comerciales.

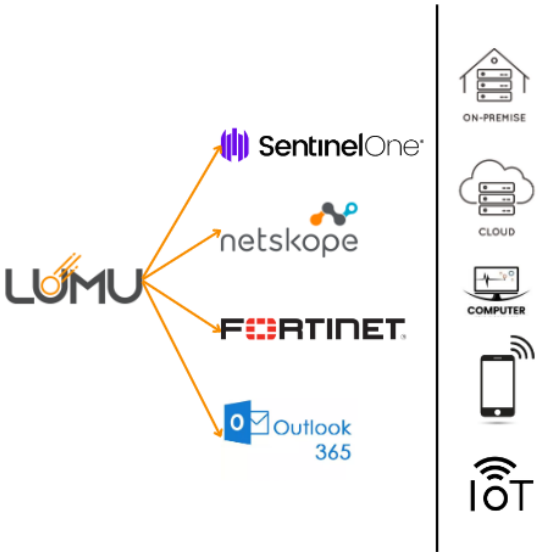
Modelo de gestión de incidentes de seguridad con Lumu

La inteligencia de amenazas es un componente crítico en la detección y respuesta rápida ante ataques informáticos, con la recolección, análisis y aplicación de conocimientos sobre amenazas cibernéticas existentes y emergentes. Este proceso permite a las organizaciones anticiparse a los ataques, identificando patrones y tácticas que los adversarios podrían utilizar. Al integrar la inteligencia de amenazas en los sistemas de seguridad, las empresas pueden mejorar su capacidad para detectar intrusiones de manera temprana y responder de manera efectiva.

Como lo muestra la siguiente Figura 17, el modelo de gestión propuesto como base para implementar con los controles mínimos recomendados en este estudio, consta de herramientas como SentinelOne, Netskope, Fortinet y Outlook 365.

Figura 17

Modelo de gestión con Lumu



Lumu: Se implementará para el monitoreo continuo del tráfico de red, el que permitirá identificar comportamientos anómalos y alertar sobre posibles incidentes de seguridad en tiempo real.

Netskope: Proporcionará visibilidad y control sobre el uso de aplicaciones en la nube y servicios SaaS, asegurando que los datos corporativos estén protegidos en todos los entornos.

SentinelOne: Se utilizará para la protección de endpoints, aplicando su tecnología de inteligencia artificial para detectar y responder automáticamente a amenazas avanzadas.

Firewall Fortinet: Se configurarán para asegurar la periferia de la red, controlando el acceso y filtrando tráfico potencialmente peligroso.

Outlook 365: Se integrarán soluciones de seguridad para proteger contra amenazas transmitidas por correo electrónico, como phishing y malware.

Plan de Implementación:

El despliegue de esta propuesta se recomienda realizarla en fases, comenzando con la evaluación de la infraestructura actual y la planificación detallada de la integración. Se debe asignar responsables para cada etapa y se establecerán protocolos de prueba para garantizar la correcta implementación de las soluciones.

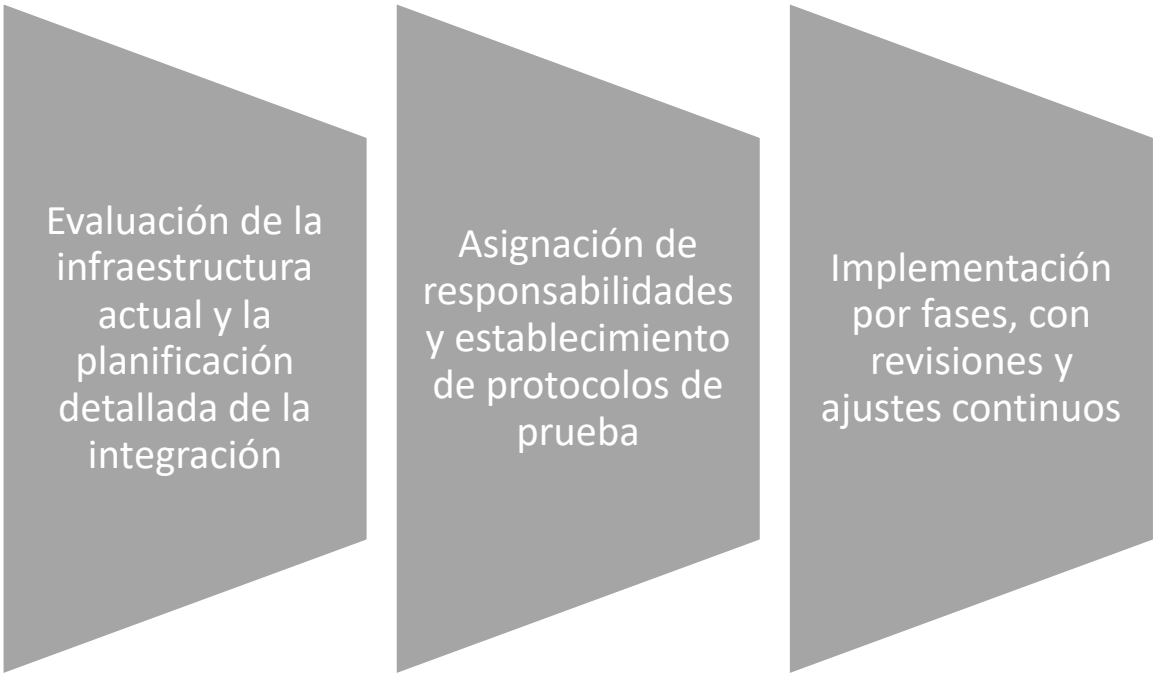
La implementación como tal es asesorada por los consultores técnicos que la firma que represente la marca en cada localidad, sin embargo, dentro de Lumu existen varias API's que permiten

interconectar con varios dispositivos y marcas, si la realidad de la empresa es diferente al esquema propuesto con las soluciones mencionadas se puede validar la compatibilidad de los mismos, considerando que se basen en este esquema como mínimo.

En la siguiente Figura 18, se detalla las etapas que se debería seguir para una correcta implementación

Figura 18

Etapas de la implementación



Capacitación y Concienciación:

Desarrollar un programa de capacitación para el personal, enfocado en el uso efectivo de las nuevas herramientas y en la importancia de seguir los protocolos de seguridad apegados a la política de seguridad de la compañía. Se debe fomentar una cultura en materia de seguridad informática en toda la organización, con contenidos interactivos que permitan medir el impacto que estas generan en los usuarios.

Monitoreo y Mejora Continua:

Implementar un sistema de monitoreo para evaluar la efectividad de la gestión de incidentes y establecer un proceso de revisión y actualización constante de las herramientas y estrategias de seguridad. Ayudará a las empresas a medir y justificar la inversión que se debe realizar para esta implementación.

Medición de Resultados:

Definir indicadores clave de rendimiento (KPIs) para medir la eficacia de la gestión de incidentes de seguridad y realizar un seguimiento continuo para informar a la dirección sobre los resultados obtenidos.

Esta propuesta busca crear un entorno de seguridad informática más seguro y resiliente, aprovechando la integración de tecnologías avanzadas y la colaboración entre herramientas especializadas. Con un enfoque proactivo y una estrategia bien definida, la empresa estará mejor equipada para enfrentar y mitigar los riesgos de seguridad cibernética.

Al adoptar Lumu como una solución de ciberseguridad, las organizaciones pueden experimentar una serie de resultados positivos y discusiones relevantes en torno a la mejora de su postura de seguridad como son:

Mejora en la Detección de Amenazas: Lumu ofrece una identificación más ágil y precisa de amenazas al examinar metadatos del tráfico de red y emplear inteligencia de amenazas en tiempo real. De esta manera, las organizaciones pueden detectar y abordar los incidentes de seguridad de forma preventiva.

Reducción de Falsos Positivos: La capacidad de Lumu para clasificar y priorizar alertas de seguridad reduce significativamente el número de falsos positivos. Esto optimiza los recursos del equipo de seguridad, permitiéndoles concentrarse en amenazas reales y críticas.

Cumplimiento Normativo: Lumu asiste a las organizaciones en su cumplimiento de regulaciones sobre seguridad de datos al ofrecer una visión exhaustiva de la red y simplificar la administración de vulnerabilidades y la salvaguarda de información confidencial.

Eficiencia Operativa: La incorporación de Lumu a los sistemas ya establecidos aumenta la eficacia operativa al automatizar la detección y respuesta a incidentes, lo que conlleva a una disminución en el tiempo y esfuerzo requeridos para administrar la seguridad de la red.

Mejora Continua: Lumu aprende continuamente de la retroalimentación y los datos de incidentes, lo que permite a las organizaciones adaptar y mejorar sus estrategias de seguridad frente a amenazas emergentes.

Discusión Estratégica: La implementación de Lumu puede desencadenar conversaciones estratégicas sobre la seguridad de la información, dado que suministra datos y métricas que podrían impactar en la toma de decisiones a nivel ejecutivo.

Retorno de la Inversión (ROI): Al mejorar la detección de amenazas y reducir los tiempos de respuesta, Lumu puede ayudar a disminuir los costos asociados con los incidentes de seguridad, lo que se traduce en un ROI positivo para la organización.

Colaboración y Compartición de Inteligencia: Lumu facilita la colaboración entre equipos al compartir inteligencia de amenazas y mejores prácticas, lo que fortalece la seguridad en toda la organización.

Cada uno de estos aspectos requiere un análisis minucioso y una discusión interna dentro de las organizaciones sobre los datos concretos y las estadísticas que respaldan los resultados alcanzados después de la implementación de Lumu. Además, es esencial examinar las lecciones aprendidas y definir los pasos a seguir para lograr una mejora continua en materia de ciberseguridad. Este proceso de reflexión y evaluación permitirá a las organizaciones fortalecer su postura de seguridad y adaptarse eficazmente a las amenazas emergentes en el panorama digital.

Validaciones de especialistas

La validación realizada por especialista del área de Infraestructura y Ciberseguridad, han calificado esta propuesta como muy adecuada por su contenido investigativo, considerando que esta herramienta es nueva en el entorno tecnológico e innovadora, que permite a las empresas ajustar sus soluciones de protección, optimizando tiempo y recursos económicos, generando un retorno de inversión asegurado.

Recomiendan este trabajo a la comunidad tecnológica para analizar la posible implementación y puesta en marca en todo tipo de empresa, haciendo hincapié en la facilidad de interacción de la plataforma con los especialistas de área de seguridad, como se muestra en el Anexo 2.

CONCLUSIONES

La solución Lumu se basa en modelos de defensa cibernética que se centran en la recolección y análisis de metadatos de tráfico de red para identificar amenazas, utiliza técnicas como el análisis de compromiso, inteligencia de amenazas, aprendizaje automático y sandboxing para detectar y responder a incidentes de seguridad. La contextualización de estos fundamentos es esencial para comprender cómo Lumu se integra y mejora las estrategias de seguridad existentes, proporcionando una capa adicional de protección basada en la visibilidad y el análisis continuo del tráfico de red.

Lumu demuestra ser efectivo en la rápida detección de una amplia variedad de amenazas, especialmente aquellas vinculadas a comunicaciones de comando y control, malware y phishing, gracias a su capacidad de análisis en tiempo real y su amplia base de datos de inteligencia de amenazas, Lumu puede identificar tanto amenazas emergentes como conocidas con gran velocidad.

Un informe de gestión de respuesta a incidentes asistido por Lumu permite detallar cómo la solución contribuye a la respuesta y mitigación de incidentes de seguridad, la cual incluye la clasificación y priorización de las amenazas, las acciones tomadas para contener y erradicar las amenazas, y cómo Lumu facilita la comunicación y colaboración entre los equipos de seguridad.

Al presentar el impacto de Lumu en una empresa caso estudio se pudo evidenciar como Lumu ha mejorado la detección de amenazas, automatizando la gestión de los incidentes, remediando los ataques con todos los equipos involucrados en la red, por medio de las herramientas paralelas de control, al existir compatibilidad con varios fabricantes se abre un abanico de posibilidades para mantener controlada la infraestructura frente a las amenazas cibernéticas.

RECOMENDACIONES

En relación con la efectividad de Lumu en la detección de incidentes de seguridad, se sugiere explorar cómo la integración de Lumu con otras soluciones de seguridad puede potenciar aún más la detección y respuesta ante amenazas. Esto puede implicar el análisis de casos de uso particulares donde Lumu colabora con sistemas de prevención de intrusiones o plataformas de seguridad de endpoints.

Respecto al diseño de un informe de gestión de respuesta a incidentes asistido por Lumu, se identifica la necesidad de mejorar la personalización de los informes para diferentes audiencias. Se recomienda desarrollar plantillas de informes que se adapten a los roles específicos dentro de la organización, desde técnicos hasta ejecutivos, para comunicar la información de manera más efectiva.

Con respecto a los resultados alcanzados con Lumu en una empresa caso estudio, se propone desarrollar un programa de estudios de casos que registre diversas experiencias de implementación de Lumu. Este programa podría abarcar webinars, entradas de blog y estudios de casos detallados que se compartan en diferentes plataformas para fomentar la educación y promover las mejores prácticas en ciberseguridad.

Para la contextualización de los modelos de defensa que trabaja la solución Lumu, se recomienda realizar talleres y seminarios que expliquen estos modelos a profesionales de la ciberseguridad. Estos eventos podrían incluir demostraciones prácticas de Lumu y discusiones sobre cómo adaptar los modelos de defensa a diferentes entornos de red y amenazas emergentes.

BIBLIOGRAFÍA

Álvarez, J. (2014). *La entrevista como técnica de investigación cualitativa*. Universidad Autónoma del Estado de Hidalgo: https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n7/r1.html

Canal Lumu Technologies. (2023). Product Training | Cacería de amenazas inteligente, sin complicaciones [Archivo de Video]. Youtube: https://www.youtube.com/watch?v=DN08rTnq2Ig

Kaspersky. (2023). Kaspersky Daily: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

Logroño, E. (2023). *Open Source Intelligence para inteligencia de amenazas de seguridad informática.* Repositorio Universidad Israel: https://repositorio.uisrael.edu.ec/bitstream/47000/3955/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-021.pdf

Lumu. (2024). Hoja de datos de Lumu: https://lumu.io/resources/lumu-datasheet/

Lumu Technologies. (2024). Hoja de datos de Lumu: https://lumu.io/resources/lumu-datasheet/

Morales, F., Topanta, S., & Toasa, R. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Iberica de sistemas e tecnologías de informacao*(E27), pp. 553-565. https://www.researchgate.net/profile/Renato-Mauricio-Toasa-G/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Implementacion-de-un-sistema-de-seguridad

Netskope. (2024). Plataforma Netskope: https://www.netskope.com/es/platform

Observatorio Ciberseguridad. (2020). *Reporte Ciberseguridad 2020*. https://observatoriociberseguridad.org/#/final-report

Ortega, S. (2022). *Análisis de sistemas de detección de intrusos con herramientas open source.* Repositorio Digital Universidad Israel: https://repositorio.uisrael.edu.ec/handle/47000/3364

SentinelOne. (2024). Qué es SentinelOne: https://es.sentinelone.com/why-sentinelone/

ANEXOS

ANEXO 1

ENTREVISTA AL CISO

UNIVERSIDAD TECNOLÓGICA ISRAEL

Nombre del entrevistador: Mauricio Anchala

Lugar donde se realiza la entrevista: Oficinas de la empresa caso estudio

Ciudad: Quito

Fecha: 22 de enero del 2024

Objetivo: Conocer sobre cómo la herramienta Lumu ha impactado la estrategia de ciberseguridad en la empresa caso estudio, esta información será usada exclusivamente para fines académicos.

1. ¿Cómo integra Lumu en la estrategia general de ciberseguridad de la organización?

CISO: Lumu es una parte central de nuestra estrategia de ciberseguridad. Nos ha permitido tener una visión detallada de las amenazas en tiempo real y nos ayuda a responder de manera más efectiva todos los ataques e incidentes de seguridad que se presentan.

2. ¿Qué desafíos específicos de seguridad de la información esperan mitigar con Lumu?

CISO: Principalmente, el phishing y los ataques de malware avanzados. Lumu nos ayuda a identificar estos ataques rápidamente y a mitigarlos antes de que causen daño significativo, considerando que tenemos otras herramientas que ayudan a controlar las amenazas, una vez que ellas no pueden solventarlas es donde entra a participar Lumu.

3. ¿Cómo ha mejorado Lumu la visibilidad de las amenazas en tiempo real en su infraestructura de TI?

CISO: Antes de Lumu, teníamos ciertas lagunas en nuestra visibilidad. Ahora, con Lumu, podemos detectar anomalías y patrones sospechosos casi de inmediato con la facilidad de la integración de inteligencia de amenazas en tiempo real a toda nuestra infraestructura.

4. ¿Podría describir el proceso de implementación de Lumu y cómo se adaptó a las necesidades específicas de su organización?

CISO: La implementación fue bastante ágil. Trabajamos con los consultores de Lumu para configurar la herramienta de acuerdo con nuestras necesidades y estructura de red, integrando el resto de las soluciones como los Firewall, Antivirus y la solución inteligente de Netskope, con el fin de proteger cada uno de los equipos que interactúan y se interconectan a nuestras redes.

5. ¿Cómo maneja Lumu los falsos positivos y qué procedimientos siguen para investigar las alertas?

CISO: Lumu tiene un buen equilibrio en la gestión de falsos positivos. Cuando surge una alerta, mi equipo de seguridades sigue un protocolo de verificación antes de tomar cualquier acción, estas llegan por correo electrónico e ingresando a la interfaz de Lumu podemos ver la trazabilidad y tomar las acciones recomendadas por el fabricante de la solución o por nuestra investigación.

6. ¿De qué manera Lumu ha afectado la carga de trabajo de su equipo de seguridad de la información?

CISO: Ha sido positivo. Lumu ha automatizado muchas tareas que antes consumían mucho tiempo, permitiendo que el equipo se concentre en asuntos más estratégicos, nosotros tenemos varias sucursales en diferentes países, cada uno con su cultura y las amenazas son diversas, es en eso que nos dedicamos más tiempo gracias a Lumu.

7. ¿Cómo evalúa la efectividad de Lumu en el proceso de detección y sus respuestas a los incidentes de seguridad?

CISO: La efectividad ha sido notable. Hemos reducido significativamente el tiempo de detección y respuesta desde que implementamos Lumu. Considerando que cuando se detecta alguna amenaza, la herramienta autogestiona y sincroniza con las demás soluciones la remediación, permitiendo mantener nuestra infraestructura protegida todo el tiempo.

8. ¿Qué tipo de formación o capacitación se proporcionó al personal para el uso eficiente de Lumu?

CISO: Proporcionamos sesiones de formación interna con el proveedor y también aprovechamos los recursos de capacitación que Lumu ofrece dentro de su plataforma, es importante e indispensable tener los conocimientos del entorno de red y hay situaciones en las que trabajamos con el equipo de infraestructura e incluso con los desarrolladores de las aplicaciones en donde el trabajo en equipo ayuda a generar más conocimiento.

9. ¿Cómo se integra Lumu con otras herramientas de seguridad que ya están en uso en su organización?

CISO: Lumu se integra bien con nuestras otras herramientas, creando un ecosistema de seguridad más robusto y cohesivo, por medio de los conectores ha sido muy fácil de integrar, tuvimos un pequeño inconveniente con la solución antivirus y siguiendo las recomendaciones del fabricante optamos por cambiarla por otra que nos brindaba mejores prestaciones.

10. ¿Qué mejoras o características adicionales considera que podrían ser beneficiosas para Lumu en futuras actualizaciones?

CISO: Nos gustaría ver mejoras en la personalización de los paneles de control y en la inteligencia artificial para predecir amenazas, con esto talvez podríamos desistir de una de las herramientas adicionales que tenemos y no está demás que tenga conectores con otros fabricantes para disponer de diversidad de opciones para proteger nuestra red.

Gracias por su tiempo a esta entrevista.

ANEXO 2

VALIDACIÓN ESPECIALISTAS

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Oscar Mera

Título obtenido
MBA, Ingeniero en Sistemas y Telecomunicaciones
Cédula de Identidad
1600392375
E- mail
omera@bmicos.com
Institución de Trabajo
BMI Companies Ecuador
Cargo
Jefe Corporativo de Infraestructura
Años de experiencia en el área
16

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		X			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	X				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		X			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		*25*	*8*			

Observaciones:

El proceso de implementación es sencillo y brinda una gran perspectiva de los ataques y se evidencia que se necesita menos recursos para el análisis de esta información gracias a la Inteligencia Artificial.

Recomendaciones

La seguridad es uno de los factores críticos para mantener una operación estable y este trabajo aporta a la comunidad tecnológica como una base de conocimiento para optar por herramientas que optimicen la carga laboral asignada a un equipo de IT, utilizando herramientas tecnológicas con IA que facilita la correlación de eventos y mejora los tiempos de respuesta ante ataques

Lugar, fecha de validación: Quito, 07 de marzo 2024

Firma del especialista

2

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Geovanny Torres

Título obtenido
Ingeniero en Sistema e Informática
Cédula de Identidad
1708032790
E- mail
gtorres@bmicos.com
Institución de Trabajo
BMI Companies
Cargo
CISO
Años de experiencia en el área
10

1

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	X				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	X				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		X			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	X				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	X				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		X			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	X				
Total		*25*	*8*			

Observaciones:

El análisis e investigación de la propuesta es un gran aporte para la comunidad.

Recomendaciones

Considerar la propuesta como fuente de consulta para que las organizaciones puedan considerar este modelo de gestión.

Lugar, fecha de validación: Quito, 07 de Marzo 2024

Firma del especialista

2