ANTAYHUA DE LA CRUZ JUAN DE DIOS

por Juan De Dios Antayhua De La Cruz

Fecha de entrega: 08-dic-2024 08:52p.m. (UTC-0500)
Identificador de la entrega: 2545486212
Nombre del archivo: ANTAYHUA_DE_LA_CRUZ_JUAN_DE_DIOS.pdf (3.78M)
Total de palabras: 19330
Total de caracteres: 125065

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“OPTIMIZACIÓN EN LA GESTIÓN DE ALERTAS MEDIANTE CORTEX XSOAR EN UN CENTRO DE OPERACIÓN DE SEGURIDAD (SOC) PARA UNA ENTIDAD FINANCIERA - 2024”

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

ANTAYHUA DE LA CRUZ, JUAN DE DIOS
ORCID: 0009-0003-2371-0734

ASESOR
QUISPE AGUILAR, MAX FREDI
ORCID: 0000-0002-4199-0974

Villa El Salvador
2024

DEDICATORIA

Dedicado a mi querida madre Epifanía De La Cruz Carrasco cuyo apoyo incondicional me ha dado la fortaleza para superar cada desafío, a mi familia por su paciencia y comprensión, a todas las personas que me ayudaron a crecer personal y profesionalmente.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo se desarrolló en el SOC de la empresa NSEK en el distrito de Santiago de Surco, Lima, Perú donde brinda servicios a una entidad financiera y aborda desafíos significativos, como la gestión de enormes volúmenes de datos que no pueden gestionarse eficientemente. La falta de automatización y visibilidad del tiempo de atención de las alertas, afectan negativamente el rendimiento y efectividad.

Para abordar el problema, se trabajó con la solución Cortex XSOAR para mejorar la gestión de alertas en un SOC optimizando desde la recepción hasta la resolución del incidente, automatizando tareas repetitivas y acelerando la respuesta con playbooks personalizados, mientras se integra con diversas herramientas de seguridad para centralizar operaciones.

Se identificó un nuevo proceso y se implementó 4 playbooks personalizados con la finalidad de optimizar la gestión de alertas de seguridad de dominios similares. Esta optimización tuvo 2 fases de implementación. La primera fase fue la implementación de un proceso nuevo dentro de la gestión de alertas del SOC. La segunda fase buscó optimizar la volumetría de las alertas y el automatizado de acciones de contención (bloqueo de indicadores de compromiso) en base a las mejores prácticas establecidas en la entidad financiera.

Los resultados esperados son óptimos donde abarcan una mejora en tiempos de atención y respuesta en la gestión de alertas de un SOC. Siguiendo las directrices de la ISO y Framework NIST, se tomó las mejores prácticas para detectar, contener y erradicar amenazas que puedan desencadenar en incidentes de seguridad teniendo en cuenta siempre una mejora continua durante el periodo de servicio. La finalidad de este proyecto es proteger y responder rápidamente a los incidentes seguridad de la organización contra amenazas cibernéticas y reducir el impacto reputacional y posibles fraudes hacia la entidad financiera.

INTRODUCCIÓN

El aumento de amenazas cibernéticas y ataques informáticos más sofisticados ha convertido a los Centros de Operaciones de Seguridad (SOC) en componentes esenciales de las estrategias de ciberseguridad empresarial. Estos centros se han vuelto fundamentales para garantizar la continuidad operativa y proteger los activos de información en un entorno cada vez más complejo. Sin embargo, los SOC enfrentan desafíos significativos, como la gestión de enormes volúmenes de datos que no pueden procesarse eficientemente. La falta de automatización y la implementación de casos de uso deficientes dificultan la detección de ataques y anomalías en la red, afectando negativamente el rendimiento y efectividad de los SOC.

La implementación de Cortex XSOAR ayuda en la gestión de alertas de un SOC optimizando el proceso desde la recepción de la alerta hasta la resolución del incidente. Automatizando tareas repetitivas y acelerando la respuesta a incidentes mediante playbooks personalizados. Se integra con múltiples herramientas de seguridad, centralizando y orquestando operaciones desde una única plataforma. Además, reduce falsos positivos a través del análisis avanzado de datos, permitiendo que los analistas se concentren en amenazas reales. Sus capacidades de informes y análisis ayudan a evaluar y optimizar las operaciones de seguridad, mejorando la efectividad general del SOC.

Este trabajo tiene como objetivo optimizar la gestión de alertas en el SOC de una empresa de ciberseguridad mediante la automatización de procesos operativos con Cortex XSOAR. Se comenzará con un análisis detallado de los procesos actuales para identificar ineficiencias y puntos de mejora. Luego, se diseñarán y desarrollarán playbooks específicos para tareas rutinarias, mejorando la clasificación, priorización de alertas y agilizando la respuesta a incidentes. Estas automatizaciones se implementarán en el entorno del SOC y se evaluará su impacto en la eficiencia, utilizando métricas como la reducción de tiempos de respuesta y falsos positivos. Finalmente, se ofrecerán recomendaciones para la mejora continua, adaptando la solución a futuras necesidades y amenazas. Este enfoque integral busca mejorar significativamente la capacidad de la empresa para detectar y responder a amenazas de seguridad de manera más eficiente.

CAPÍTULO I. ASPECTOS GENERALES

1.1 Contexto

En un mundo cada vez más digital, el cibercrimen ha encontrado nuevas oportunidades para expandirse. Por ello, la ciberseguridad se ha convertido en una prioridad para las empresas. NSEK integra las tecnologías más avanzadas, servicios especializados y un equipo de expertos altamente capacitados, asiste a las organizaciones en el desafío de protegerse contra las amenazas digitales mediante el análisis, la detección y la prevención.

Empresa líder en ciberseguridad en América Latina, comprometida con la protección de los activos digitales y la gestión de riesgos cibernéticos para organizaciones de todos los tamaños. Con más de dos décadas de experiencia en el sector, NSEK ha construido una reputación sólida basada en su capacidad para enfrentar los desafíos más complejos de seguridad en un entorno digital en constante evolución.

NSEK tiene como visión aspirar a ser la empresa de referencia en ciberseguridad en América Latina, reconocida por su innovación, excelencia en el servicio y capacidad para ofrecer soluciones integrales que permitan a sus clientes operar de manera segura y confiable en un mundo digital.

La misión de NSEK es proteger a sus clientes contra las crecientes amenazas cibernéticas, asegurando la integridad, confidencialidad y disponibilidad de sus sistemas y datos.

La empresa busca lograr esto mediante la implementación de tecnologías avanzadas, la automatización de procesos de seguridad y un enfoque personalizado que se adapta a las necesidades específicas de cada cliente. NSEK se compromete a ser un socio estratégico en la continuidad operativa de sus clientes, ayudándolos a cumplir con normativas de seguridad, reducir riesgos y fortalecer su resiliencia frente a un entorno de amenazas cada vez más complejas.

1.2 Delimitación temporal y espacial del trabajo

1.2.1 Espacial

El presente proyecto de implementación está enfocado en optimizar la gestión de alertas del SOC, integrando tecnologías y herramientas disponibles en Cortex XSOAR, se desarrolló en la empresa NSEK ubicado en el distrito de Santiago de Surco, Lima.

1.2.2 Temporal

La implementación de optimización de la gestión de alertas del SOC mediante Cortex XSOAR, inició en 3 de enero y culminó el 31 de mayo del 2024.

1.2.3 Teórica

La delimitación teórica del proyecto se enfocó en analizar e identificar procesos de gestión de alertas en el SOC para implementar una optimización mediante automatizaciones personalizadas utilizando Cortex XSOAR.

1.3 Objetivos

1.3.1 Objetivo Principal

Optimizar la gestión de alertas mediante Cortex XSOAR en un Centro de Operaciones de Seguridad (SOC) para una entidad financiera - 2024.

1.3.2 Objetivos Específicos

- Identificar y diseñar los procesos de gestión de alertas para formular estrategias eficientes de automatización en el SOC.
- Implementar playbooks personalizados mediante Cortex XSOAR para optimizar la gestión de alertas de seguridad.
- Validar la optimización de la gestión de alertas en el SOC de acuerdo a las normas ISO y framework NIST.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Antecedentes Nacionales

Vasquez (2023) realizó el trabajo académico de nombre "*Implementación de servicio de centro de operaciones de ciberseguridad (CyberSoC) con plataformas open source a entidad financiera*", indica el creciente riesgo de ciberataques y la insuficiencia de los métodos convencionales de seguridad en muchas empresas en América Latina, especialmente en Perú, se encuentran vulnerables y no preparadas para enfrentar amenazas cibernéticas avanzadas. La falta de preparación, evidenciada por un informe de la OEA, ha llevado a las organizaciones a buscar proveedores y especialistas en ciberseguridad que dominen mecanismos informáticos más sofisticados, como los Centros de Operaciones de Ciberseguridad (SOC) con plataformas open source basado en el Framework NIST. El autor concluye con la implementación de un servicio CyberSoC en una entidad financiera que monitorea, detecta, analiza y previene eventos e incidentes de ciberseguridad en sus equipos e instalaciones utilizando herramientas de código abierto optimizando costos sin descuidar la seguridad y protección de los activos de la empresa. El uso de plataformas open source basado en el Framework NIST aporta a mi trabajo la toma de medidas y mitigación de daños durante un incidente de seguridad, así como la ejecución de planes y resiliencia postincidente.

Cisneros (2022) realizó el trabajo de investigación de nombre "*Implementación de un centro de operaciones de ciberseguridad (SOC) para mejorar la detección de ataques cibernéticos en empresas del sector tecnológico, Lima-2022*", aborda la necesidad de proteger una empresa contra incidentes de seguridad, pero se enfrentan dificultades para implementar un Centro de Operaciones de Ciberseguridad (SOC) debido a las limitaciones económicas. Esto pone en riesgo su capacidad para detectar y responder eficazmente a ciberataques, especialmente en un contexto donde las amenazas son cada vez más frecuentes y sofisticadas. Aunque existen herramientas open source que pueden mitigar estos riesgos, muchas empresas desconocen su existencia o no saben cómo integrarlas adecuadamente en sus operaciones de seguridad. El autor concluye con la

implementación de un SOC que mejora la detección de ciberataques utilizando herramientas open source y haciendo uso de las buenas prácticas de los estándares internacionales como ISO/IEC: 27035. El aporte de este trabajo hacia el mío son las buenas prácticas basadas en el estándar ISO/IEC:27035 para la identificación temprana de incidentes de seguridad como la respuesta rápida y eficiente para minimizar el impacto.

Hurtado (2021) realizó el trabajo académico de nombre "*Diseño de un sistema de gestión para mejorar el servicio de atención en la plataforma de seguridad de la información de la empresa SISCOTEC del Perú S.A.C.*", indica que la empresa en mención enfrentaba ineficiencias en la atención de incidencias y eventos críticos en su plataforma de seguridad de la información, lo que impacta negativamente en la satisfacción del cliente y la seguridad de la información. Identificaron que la implementación de un Centro de Operaciones de Seguridad (SOC) basado en Metodologías de Gestión de Riesgos y el estándar ISO 27001, mejora significativamente la eficiencia y la satisfacción del cliente, pero la empresa aún no cuenta con un sistema de gestión SOC formal. Esto generaba un desafío en la toma de decisiones sobre la inversión y la implementación gradual de un SOC que sea rentable y efectivo en mejorar los servicios de atención de incidencias. De la investigación se concluyó, que la implementación de un SOC basado en el estándar ISO 27001 y en etapas es posible y sostenible, donde el costo de implementación es recuperable en el tiempo. Así mismo, es importante tener en cuenta el estándar ISO/IEC 27001 debido a sus principales componentes de evaluación y mitigación de riesgos de seguridad, así como la mejora continua en una implementación.

2.1.2 Antecedentes Internacionales

Tilbury y Flowerday (2024) publicaron un artículo llamado "*Humanos y Automatización: Aumento de los Centros de Operaciones de Seguridad*" abordando el tema de la integración continua de herramientas automatizadas en los Centros de Operaciones de Seguridad (SOC) aumentando significativamente el volumen de alertas que los analistas de seguridad deben manejar, generando un riesgo creciente de sesgo y complacencia en la automatización, lo que ha llevado a que los analistas pasen por alto, ignoren o no actúen ante alertas críticas. Finalmente,

el autor concluye que la reducción de la eficacia en la respuesta a los incidentes de seguridad se da aplicando un enfoque técnico basado en la Matriz de Boston. Esta matriz, basada en un análisis exhaustivo de investigaciones existentes, proporciona un marco práctico para establecer una colaboración equilibrada y mutuamente beneficiosa, mejorando así la detección y respuesta a amenazas en los SOC. Para optimizar los procesos en los SOC, es crucial desarrollar una sinergia eficaz entre los analistas de seguridad y la automatización. La matriz de automatización aporta a mi trabajo la retroalimentación constante que debe tener el área o usuario final a donde la implementación de una automatización con el área de desarrollo o implementador, esto para crear un entorno de mejora constante en un servicio.

Forsberg y Frantti (2023) mediante una investigación llamado "*Métricas de rendimiento técnico de un centro de operaciones de seguridad*" indicaron que los Centros de Operaciones de Seguridad (SOC) enfrentan una limitación significativa en la evaluación precisa de su impacto en las capacidades de ciberdefensa debido a la falta de métricas adecuadas que midan su rendimiento técnico. La mayoría de las métricas existentes se centran en aspectos operativos, lo que dificulta la cuantificación del verdadero desempeño técnico de un SOC y, por ende, su eficacia en la detección y respuesta a amenazas. El autor concluye con desarrollar y aplicar un marco novedoso para la creación de métricas específicas que evalúen el rendimiento técnico de los SOC. Este marco, validado a través de la generación de cuatro métricas innovadoras, permitirá a los SOC medir de manera más precisa y objetiva su capacidad técnica, mejorando así su capacidad para detectar y responder a amenazas. Implementar este marco no solo ayudará a superar la deficiencia en las métricas actuales, sino que también ofrecerá un enfoque más completo para evaluar y optimizar el desempeño de un SOC. Las métricas se construyeron y presentaron mediante programación utilizando herramientas de código abierto y módulos de Python, incluyendo Jupyter Notebooks y la biblioteca de gráficos Plotly. También se empleó scikit-learn para el análisis de datos y el desarrollo de algoritmos de aprendizaje automático. Una métrica fundamental que aporta a mi trabajo es la “Precisión técnica del análisis” donde la clasificación detallada del evento o incidente de seguridad es importante para tener visibilidad histórica y planificar nuevos procedimientos de seguridad en el análisis de riesgos.

2.2 Bases teóricas

2.2.1 Normas y estándares de seguridad

2.2.1.1 ISO 27001

La ISO 27001 es una norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI). Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización (ISO, 2013).

Para una empresa de ciberseguridad la certificación ISO 27001 es fundamental por las siguientes razones:

a) Protección de la información sensible

Las empresas de ciberseguridad manejan datos extremadamente sensibles, tanto propios como de sus clientes, como vulnerabilidades, incidentes de seguridad y datos personales. La ISO 27001 establece un marco para proteger la confidencialidad, integridad y disponibilidad de esa información, lo cual es crítico para evitar filtraciones de datos o ciberataques (NormasISO, 2024).

b) Confianza y reputación

Contar con la certificación ISO 27001 demuestra a clientes y socios comerciales que la empresa tiene controles rigurosos para proteger su información. Esto genera confianza, mejora la reputación de la empresa y puede ser un diferenciador competitivo en el mercado (NormasISO, 2024).

c) Cumplimiento de regulaciones

En muchos sectores, incluidas las industrias financieras, gubernamentales y de salud, las empresas deben cumplir con normativas y leyes de protección de datos (como el GDPR en Europa o la Ley de Protección de Datos Personales en Perú). La ISO 27001 ayuda a cumplir con estos requisitos regulatorios al proporcionar un marco de buenas prácticas en la gestión de la seguridad de la información (NormasISO, 2024).

d) Mitigación de riesgos

La norma ISO 27001 ayuda a las empresas a identificar, evaluar y gestionar los riesgos de seguridad de la información de manera sistemática. Esto reduce la probabilidad de incidentes de seguridad y minimiza el impacto de posibles brechas (NormasISO, 2024).

e) Mejora continua

La certificación fomenta una cultura de mejora continua en los procesos de seguridad, ya que exige la evaluación regular de los controles y la implementación de acciones correctivas cuando sea necesario. Esto garantiza que la empresa se mantenga actualizada frente a nuevas amenazas y vulnerabilidades (NormasISO, 2024).

f) Requisitos contractuales

Muchas veces, los clientes y socios comerciales exigen que las empresas de ciberseguridad estén certificadas bajo ISO 27001 como un requisito para firmar contratos, especialmente en sectores altamente regulados. La certificación facilita el acceso a nuevos mercados y clientes (NormasISO, 2024).

2.2.1.2 ISO 27035

La ISO/IEC 27035 es una norma internacional que proporciona directrices y recomendaciones para la gestión de incidentes de seguridad de la información. Forma parte de la familia de normas ISO 27000, que se centra en la gestión de la seguridad de la información (ISO, 2023).

Se divide en varias partes y proporciona directrices detalladas para planificar, establecer, implementar, operar, monitorear, revisar y mejorar la respuesta a incidentes de seguridad:

a) Principios y conceptos

Proporciona una descripción general de los conceptos clave relacionados con los incidentes de seguridad de la información. Define qué es un incidente, la importancia de estar preparado y cómo identificar, analizar y responder a un incidente (Tenacy, 2024).

b) Directrices para la planificación y preparación

Enfoca la creación de un plan de gestión de incidentes que incluya políticas, procedimientos y responsabilidades. También sugiere cómo el personal debe estar capacitado para identificar y gestionar incidentes de manera eficaz (Tenacy, 2024).

c) Directrices para la respuesta a incidentes

Proporciona una guía para la detección, reporte, evaluación y análisis de incidentes. Describe las mejores prácticas para contener, erradicar y recuperarse de incidentes de seguridad, y cómo documentar el proceso (Tenacy, 2024).

d) Evaluación post-incidente

Después de gestionar un incidente, es crucial realizar una revisión exhaustiva para identificar las causas fundamentales y prevenir incidentes futuros. Se enfoca en el aprendizaje y la mejora continua del sistema de seguridad (Tenacy, 2024).

e) Monitoreo y mejora continua

Incluye el establecimiento de un ciclo de monitoreo y mejora de la gestión de incidentes, con base en las lecciones aprendidas y las tendencias observadas (Tenacy, 2024).

Objetivos:

- Identificación temprana de incidentes de seguridad de la información.
- Respuesta rápida y eficiente para minimizar el impacto.
- Comunicación clara entre los diferentes actores involucrados en la respuesta.
- Mejora continua basada en la experiencia y la retroalimentación de cada incidente.

2.2.1.3 NIST

El marco de ciberseguridad del NIST (NIST Cybersecurity Framework) es un conjunto de directrices, buenas prácticas y estándares desarrollados por el National Institute of Standards and Technology (NIST) de los Estados Unidos. Este marco tiene como objetivo ayudar a las organizaciones a gestionar y reducir los riesgos de ciberseguridad, mejorar la protección de sus sistemas y datos, y aumentar su capacidad para responder y recuperarse de ciberataques (NIST, 2024).

a) Principales características del Marco de Ciberseguridad NIST

El marco se basa en una estructura flexible y adaptable, lo que permite a organizaciones de cualquier tamaño o sector implementarlo según sus necesidades particulares. Se compone de cinco funciones principales, ver Tabla 1.

Tabla 1

Nombres de las Funciones y Categorías del NIST CSF 2.0 Core

Función	Descripción	Categorías
Identificar	Está orientada a entender el entorno organizativo para gestionar mejor los riesgos de ciberseguridad. Esto incluye la identificación de activos críticos, procesos comerciales, amenazas y vulnerabilidades, lo que permite establecer una base sólida para las siguientes acciones de ciberseguridad.	Identificación de activos y recursos. Comprensión de los riesgos y amenazas. Identificación de roles y responsabilidades. Evaluación de la infraestructura.
Proteger	Se centra en implementar medidas de protección para evitar o minimizar el impacto de posibles incidentes de ciberseguridad. Implica el desarrollo de controles que limiten el acceso no autorizado y fortalezcan las defensas del sistema.	Control de acceso. Conciencia y formación en ciberseguridad. Protección de la información y de los datos sensibles. Mantenimiento de la seguridad de infraestructuras.
Detectar	Identifica de manera oportuna los incidentes de ciberseguridad. Involucra la implementación de mecanismos de monitoreo continuo y sistemas de alerta que ayuden a detectar actividades anómalas o eventos sospechosos en la red.	Implementación de sistemas de detección. Monitoreo de redes y sistemas. Análisis de anomalías y eventos. Generación de alertas y notificaciones.
Responder	En esta función se desarrollan planes y procedimientos para reaccionar de manera efectiva ante incidentes de ciberseguridad. El enfoque está en minimizar el daño y restaurar las operaciones lo más rápido posible.	Gestión de incidentes de ciberseguridad. Comunicación interna y externa durante un incidente. Análisis del impacto del incidente. Ejecución de planes de respuesta y recuperación.
Recuperar	Se enfoca en restaurar las capacidades y servicios afectados después de un incidente de ciberseguridad. Incluye la planificación para la recuperación a largo plazo y la implementación de lecciones aprendidas para mejorar la resiliencia.	Planificación de la recuperación. Implementación de medidas correctivas. Comunicaciones durante la recuperación. Mejora continua del plan de recuperación.

Nota: Muestra las funciones del Framework NIST. Adaptado de El Marco de Seguridad Cibernética (CSF) 2.0 del NIST. Fuente: NIST (2024)

b) Componentes del Marco de Ciberseguridad NIST

Según el Marco de Seguridad Cibernética (CSF) 2.0 del NIST, sus principales componentes son:

- Perfiles: Son una representación de los resultados que una organización desea alcanzar en términos de ciberseguridad. Permiten que las organizaciones alineen sus programas de ciberseguridad con sus requisitos de negocio y objetivos de gestión de riesgos (NIST, 2024).
- Niveles de implementación (Tiers): Estos niveles definen el grado de madurez de la gestión de riesgos de ciberseguridad dentro de una organización. Hay cuatro niveles, desde el Nivel 1: Parcial, hasta el Nivel 4: Adaptativo, donde las organizaciones implementan mejoras proactivas y automatizadas (NIST, 2024).
- Áreas de enfoque: Cada función y categoría del marco está vinculada a subcategorías específicas, que a su vez están relacionadas con estándares y controles técnicos (como los del NIST SP 800-53 o ISO/IEC 27001), lo que proporciona un enfoque coherente para la implementación (NIST, 2024).

c) Beneficios del Marco de Ciberseguridad NIST

La empresa de seguridad Fortinet, indica que el cumplimiento del Marco de Ciberseguridad NIST incluye distintos beneficios, como:

- Flexibilidad y escalabilidad: El marco puede adaptarse a cualquier tipo de organización, desde pequeñas empresas hasta grandes corporaciones, y permite a cada organización implementar medidas de acuerdo a sus capacidades y riesgos específicos (Fortinet, 2024).
- Gestión de riesgos: Ayuda a las organizaciones a adoptar un enfoque proactivo para gestionar el riesgo de ciberseguridad, al identificar activos críticos, evaluar amenazas y establecer controles apropiados (Fortinet, 2024).
- Cumplimiento normativo: Aunque no es una norma obligatoria, el marco es ampliamente reconocido y utilizado como base para cumplir con normativas y regulaciones sobre ciberseguridad, como el GDPR en Europa, o los requerimientos del gobierno de EE.UU (Fortinet, 2024).
- Comunicación mejorada: Facilita la comunicación tanto interna como externa sobre riesgos de ciberseguridad, permitiendo una colaboración más eficaz entre

los diferentes niveles de la organización y las partes interesadas (Fortinet, 2024).

- Mejora continua: El marco promueve la mejora continua en la seguridad cibernética mediante la evaluación constante de las amenazas, la implementación de controles actualizados y la revisión de incidentes para aprender de ellos (Fortinet, 2024).

2.2.2 Centro de Operaciones de Seguridad (SOC)

Un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés: Security Operations Center) es una unidad centralizada dentro de una organización dedicada a monitorear, detectar, analizar y responder a incidentes de seguridad cibernética de manera continua. El SOC actúa como el núcleo de la defensa cibernética de una organización, con un equipo especializado que utiliza tecnologías avanzadas para proteger la infraestructura tecnológica y la información sensible de la empresa contra amenazas y ataques (IBM, 2024).

a) Sus principales funciones son:

- Monitoreo 24/7: Realiza un monitoreo en tiempo real de la red, sistemas, aplicaciones y dispositivos de una organización para identificar comportamientos anómalos, posibles ataques o vulnerabilidades (IBM, 2024).
- Detección de amenazas: Identifica actividades maliciosas o sospechosas en la red como malware, phishing, intentos de acceso no autorizado, violaciones de políticas de seguridad, etc (IBM, 2024).
- Análisis de incidentes: Cuando se detecta una amenaza o un incidente, el equipo del SOC realiza un análisis detallado para entender el alcance, impacto y naturaleza del ataque (IBM, 2024).
- Respuesta a incidentes: Coordina la respuesta a los incidentes de seguridad, implementando medidas de contención, erradicación y recuperación (IBM, 2024).
- Gestión de vulnerabilidades: Identifica y gestiona vulnerabilidades en los sistemas y aplicaciones antes de que puedan ser explotadas por los atacantes. Esto se realiza a través de la evaluación continua de parches, pruebas de penetración y análisis de vulnerabilidades (IBM, 2024).

- Mejora continua y retroalimentación: Un SOC no solo se enfoca en la detección y respuesta de amenazas, sino también en la mejora continua de la postura de seguridad de la organización. Los análisis de los incidentes pasados ayudan a afinar las políticas de seguridad, actualizar las configuraciones de las herramientas de monitoreo y ajustar los controles de seguridad (IBM, 2024).
- Generación de informes y cumplimiento: Generar informes periódicos sobre incidentes de seguridad, métricas de rendimiento y otros indicadores clave. Estos informes son esenciales para cumplir con normativas de seguridad y regulaciones del sector, como GDPR, PCI DSS, ISO 27001, entre otras (IBM, 2024).

b) Componentes de un SOC:

i. Personal especializado:

Está compuesto por un equipo de profesionales en seguridad informática que desempeñan diferentes roles, entre ellos:

- Analistas de seguridad (Niveles 1, 2 y 3): Encargados de monitorear y analizar los eventos de seguridad (IBM, 2024).
- Ingenieros de seguridad: Especialistas que implementan y configuran las tecnologías y herramientas utilizadas en el SOC (IBM, 2024).
- Equipo de respuesta a incidentes: Responsables de coordinar y ejecutar las acciones de respuesta ante un incidente.
- Especialistas en inteligencia de amenazas: Analizan las tendencias y comportamientos de las amenazas emergentes (IBM, 2024).
- Líder o Supervisor: Responsable de orquestar el equipo de profesionales para cumplir con el objetivo de un SOC (IBM, 2024).

ii. Herramientas tecnológicas

Utiliza una amplia gama de tecnologías y herramientas para realizar sus funciones, tales como:

- SIEM (Security Information and Event Management): Plataforma que recopila y correlaciona datos de diferentes fuentes para detectar incidentes (IBM, 2024).

- SOAR (Security Orchestration, Automation, and Response): Plataforma que ayuda a los equipos de seguridad a gestionar y responder a incidentes de ciberseguridad de manera más eficiente y efectiva (IBM, 2024).
- IPS (Sistema de Prevención de Intrusiones): Monitorean el tráfico de red en busca de actividades sospechosas o no autorizadas (IBM, 2024).
- EDR (Endpoint Detection and Response): Detecta amenazas y responde en los dispositivos finales (IBM, 2024).
- Firewall y sistemas de control de acceso: Controlan y limitan el tráfico no autorizado en la red (IBM, 2024).
- Sistemas de inteligencia de amenazas: Herramientas que proporcionan información sobre las últimas amenazas y técnicas utilizadas por los atacantes (IBM, 2024).

iii. Procesos y procedimientos

Un SOC efectivo opera bajo un marco de procedimientos claramente definidos, que incluyen procesos estandarizados para la detección, análisis, clasificación y respuesta a incidentes. Estos procedimientos aseguran que cada incidente sea tratado de manera eficiente y con los pasos correctos para mitigar el riesgo (IBM, 2024).

2.2.3 CORTEX XSOAR

Cortex XSOAR (Extended Security Orchestration, Automation, and Response) de Palo Alto Networks es una plataforma avanzada diseñada para ayudar a los equipos de seguridad a gestionar, automatizar y orquestar las tareas o procesos relacionados con la ciberseguridad. Ofrece un conjunto de capacidades que mejoran la eficiencia y eficacia en la respuesta a incidentes, permitiendo a los equipos de seguridad enfrentar amenazas de manera más rápida y organizada (Palo Alto Networks, 2020).

2.2.3.1 Funciones

a) Orquestación

- Integración con herramientas de seguridad: Cortex XSOAR puede integrarse con una amplia variedad de herramientas de ciberseguridad, como sistemas SIEM, firewalls, soluciones de endpoint, y más. Esto permite centralizar y coordinar las operaciones desde una única plataforma (Palo Alto Networks, 2020).
- Automatización de flujos de trabajo: Cortex XSOAR automatiza tareas repetitivas y rutinarias a través de playbooks, lo que libera tiempo para que los analistas se enfoquen en problemas más complejos (Palo Alto Networks, 2020).

b) Automatización

- Playbooks automatizados: Cortex XSOAR utiliza playbooks predefinidos o personalizados que permiten automatizar respuestas a incidentes comunes, como la contención de malware, la investigación de alertas, o la gestión de vulnerabilidades (Palo Alto Networks, 2020).
- Reducción de tiempos de respuesta: La automatización reduce drásticamente el tiempo necesario para responder a incidentes, minimizando el impacto potencial de las amenazas (Palo Alto Networks, 2020).

c) Respuesta a Incidentes

- Gestión centralizada de incidentes: Ofrece una plataforma centralizada donde se pueden gestionar todos los incidentes de seguridad, proporcionando visibilidad completa y contexto detallado de cada incidente (Palo Alto Networks, 2020).
- Colaboración mejorada: Facilita la colaboración entre equipos de seguridad y otras partes interesadas, asegurando que todas las acciones y decisiones sean documentadas y accesibles en tiempo real (Palo Alto Networks, 2020).

d) Inteligencia de amenazas y Análisis

- Enriquecimiento del contexto: Cortex XSOAR puede agregar inteligencia sobre amenazas y otros datos relevantes al contexto de un incidente, mejorando la

capacidad de los analistas para tomar decisiones informadas (Palo Alto Networks, 2020).

- Dashboards y reportes personalizados: Ofrece capacidades de análisis y reportes que permiten a los equipos de seguridad evaluar su rendimiento y la eficacia de sus respuestas a incidentes (Palo Alto Networks, 2020).

e) Casos de uso extendidos

- Gestión de vulnerabilidades: Automatiza el proceso de identificación, priorización, y remediación de vulnerabilidades, alineando los esfuerzos de seguridad con las políticas de la organización (Palo Alto Networks, 2020).
- Respuesta a amenazas avanzadas: Integra inteligencia de amenazas para manejar de manera efectiva ataques avanzados, como ransomware o ataques dirigidos (Palo Alto Networks, 2020).

f) Escalabilidad y Flexibilidad

- Escalable para cualquier tamaño de organización: Diseñado para adaptarse tanto a pequeñas como grandes organizaciones, Cortex XSOAR puede escalar para manejar desde un número reducido de alertas hasta miles de incidentes diarios (Palo Alto Networks, 2020).
- Personalización y adaptabilidad: Los playbooks se pueden personalizar según las necesidades específicas de cada organización, permitiendo una adaptación precisa a diferentes entornos y procesos de seguridad (Palo Alto Networks, 2020).

g) Comunidad y Marketplace

- Marketplace de integraciones: Cortex XSOAR ofrece un marketplace donde se pueden descargar e integrar nuevas aplicaciones, playbooks, y conectores que expanden las capacidades de la plataforma (Palo Alto Networks, 2020).

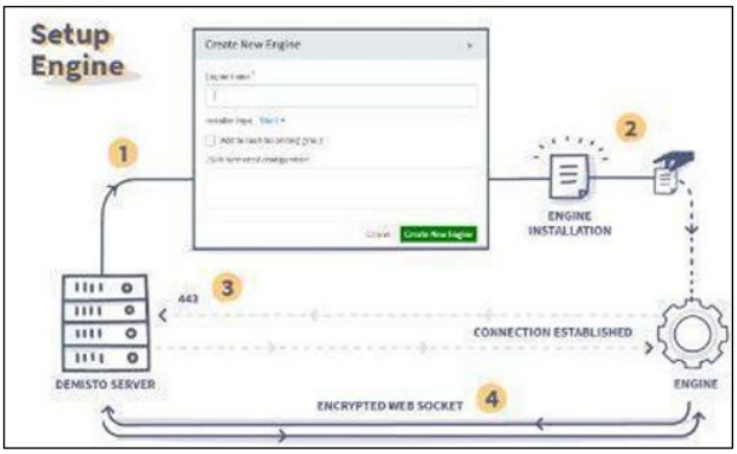
  La conexión de las integraciones y XSOAR se realiza a través del método de comunicación API mediante el protocolo HTTP (puerto 80).

  Para sus integraciones con redes On-premise, XSOAR utiliza un Proxy Engine que permite al servidor Cortex XSOAR acceder a servicios internos o externos

que de otra forma estarían bloqueados por un firewall, proxy u otro dispositivo de seguridad, ver Figura 1.

Figura 1

Configuración de Proxy Engine para comunicación XSOAR SaaS y entorno On-premise cliente



Nota: Obtenido de Palo Alto Networks Certified Security Automation Engineer (PCSAE) Study Guide. Fuente: Palo Alto Networks (2022).

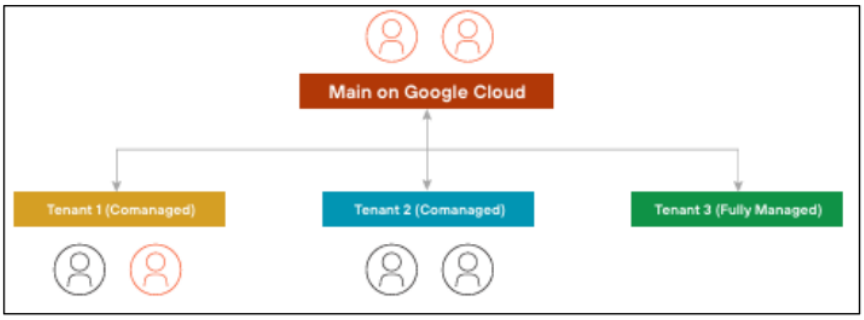
- Soporte de la comunidad: Existe una comunidad activa de usuarios y desarrolladores que contribuyen con nuevos playbooks, integraciones y buenas prácticas.

h) Multi-tenant

XSOAR ofrece una completa segmentación de datos entre clientes en una única implementación. Los datos de los clientes pueden separarse en hosts y tenants individuales mientras usted obtiene una vista de cada tenant en una única vista administrada. La separación completa de multi-tenant de datos como de procesos RBAC (control de accesos basado en roles) proporcionan un control granular sobre los datos de los clientes, garantizando una seguridad y privacidad férreas. XSOAR soporta implementaciones SaaS (Palo Alto Networks, 2024), ver Figura 2 y On-premise, ver Figura 3.

Figura 2

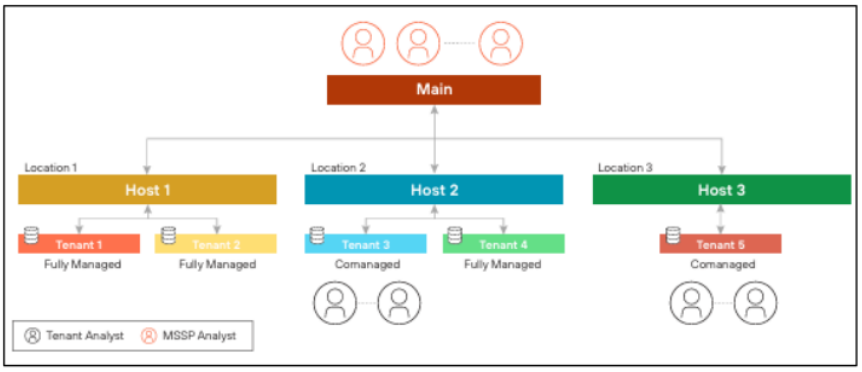
Cortex XSOAR SaaS arquitectura multi-tenant



Nota: Obtenido de Cortex XSOAR for Managed Security Service Providers. Fuente: Palo Alto Networks (2024).

Figura 3

Cortex XSOAR On-premise arquitectura multi-tenant



Nota: Obtenido de Cortex XSOAR for Managed Security Service Providers. Fuente: Palo Alto Networks (2024).

2.2.3.2 Arquitectura de Red

La arquitectura de red de Cortex XSOAR tiene los siguientes componentes:

a) Host principal:

"Es la instancia principal de la arquitectura desde la que accede, administra tenants (cuentas), crea y administra hosts" (Palo Alto Networks, 2022, p.56).

b) Host:

Es una instancia de Cortex XSOAR que actúa como proxy entre el host principal y los inquilinos. En un despliegue multitenant, los hosts no son necesarios, pero permiten escalar el despliegue gestionando una colección de tenants. Los datos no se almacenan en las máquinas host (Palo Alto Networks, 2022, p.56).

c) Tenant:

Es una instancia de Cortex XSOAR que atiende a un cliente o una cuenta y se puede ubicar en el host principal o en otros hosts. El tenant tiene datos específicos del cliente, como indicadores, incidencias, diseños, etc., que se almacenan en el índice del tenant de la base de datos. Los tenant comparten indicadores con el host principal mediante un índice de base de datos compartida. El tenant también puede heredar contenido como playbooks, indicadores, tipos de incidentes, etc., del host principal mediante etiquetas de propagación (Palo Alto Networks, 2022, p.57).

d) Engines:

Son instalaciones más pequeñas (agentes) de Cortex XSOAR que se utilizan para permitir la comunicación entre integraciones de terceros, que pueden estar en una parte diferente de la red o pueden estar bloqueadas a través de firewalls, y el host principal. Los engines se pueden instalar solos o como parte de un grupo de engines que distribuye la carga de una integración o de varias integraciones entre varios engines (Palo Alto Networks, 2022, p.57).

e) Segmentación de datos:

"El contenido de Cortex XSOAR, incluidos los playbooks, los scripts de automatización y los diseños de incidentes/indicadores entre otros, se administra en el host principal y se propaga a los tenants" (Palo Alto Networks, 2022, p.57).

f) Compartir indicadores:

Cada cuenta de tenant tiene un índice compartido dedicado en Elasticsearch, lo que permite a las cuentas de tenants compartir indicadores locales con un índice de Elasticsearch dedicado, desde el cual otros tenants pueden ingerir esos indicadores (tal como se configura en el host principal). El almacenamiento de indicadores locales en un índice compartido mantiene la segregación de datos entre los tenants, pero los tenants pueden beneficiarse de la información sobre amenazas detectada localmente (Palo Alto Networks, 2022, p.57).

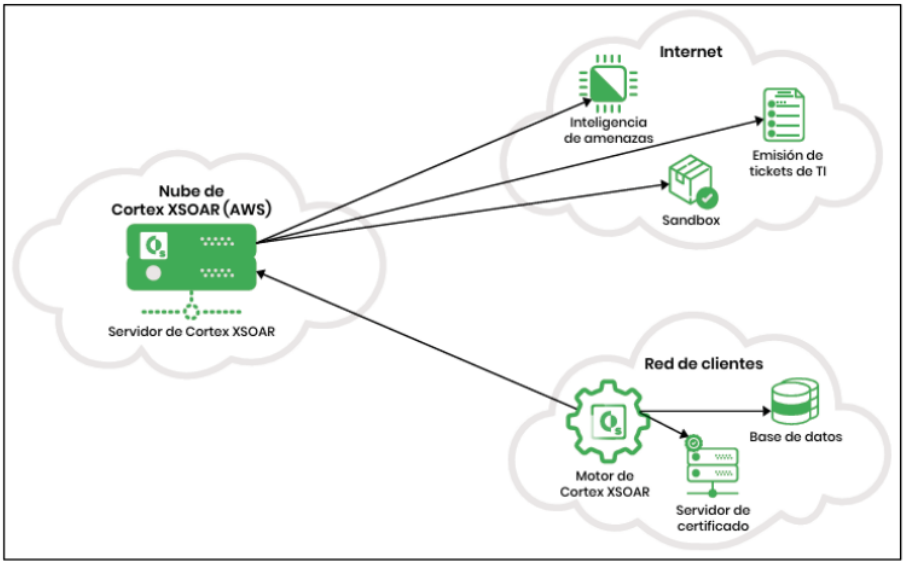
g) Comunicación:

El host principal y los hosts se comunican entre sí mediante TLS 2.1 a través del puerto 443 (este es el puerto predeterminado, pero se puede configurar). Además, todos los hosts que trabajan con Elasticsearch se comunican con la base de datos a través del puerto 9200. Las solicitudes a los tenants se envían a través de los hosts (principales u otros) en el puerto 443. Los hosts reenvían las solicitudes a los tenants, que escuchan en los puertos 18501 y posteriores (Palo Alto Networks, 2022, p.57).

La función de Orquestación en XSOAR es indispensable y es por ello que el servicio alojado en la nube de AWS, ver Figura 4, debe entablar comunicación con las herramientas de seguridad que se encuentran en la red de infraestructura onpremise.

Figura 4

Servicio AWS alojado de Cortex XSOAR



Nota: Arquitectura obtenido de Orquestación de seguridad, automatización y respuestas alojadas. Fuente: Palo Alto Networks (2020).

El servidor Cortex XSOAR tiene requisitos específicos de sistema operativo, solo es posible desplegar en sistemas operativos Red Hat, CentOS y Oracle Linux. En hardware también requiere un mínimo requisito para ser implementado, ver Tabla 2.

Tabla 2

Hardware requerido para servidor Cortex XSOAR

Componente	Entorno Desarrollo (Mínimo)	Entorno Producción (Mínimo)
CPU	8 núcleos de CPU	16 núcleos de CPU
Memoria	16 GB RAM	32 GB RAM
Disco	500 GB SSD	1TB SSD

Nota: Adaptado de Palo Alto Networks Certified Security Automation Engineer (PCSAE) Study Guide. Fuente: Palo Alto Networks (2022).

2.3 Definición de términos básicos

Ciberseguridad

Es la práctica de proteger sistemas informáticos, redes y datos contra accesos no autorizados, ataques y daños. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información (Cloudflare, 2024). Esto incluye la protección de datos sensibles, la seguridad de redes y sistemas, y la implementación de medidas de monitoreo y respuesta ante incidentes.

Context Data

Cada incidente y playbook tiene un lugar para almacenar datos llamado "context", que almacena los resultados de cada comando de integración y cada script de automatización que se ejecuta. El context es un diccionario de mapas o pares key-value, cuyos valores pueden anidar estructuras adicionales. Los objetos de context están en formato JSON y se crean para cada incidente (Palo Alto Networks, 2022).

EDR

Es una tecnología de ciberseguridad que monitorea constantemente dispositivos endpoint para identificar y mitigar amenazas de forma automática. Ayuda a los analistas a detectar problemas en endpoints antes de que se extiendan por la red registrando y analizando continuamente el comportamiento para identificar actividades sospechosas como ransomware, también puede contener amenazas y alertar para facilitar una investigación (Microsoft, 2024).

Endpoint

Es cualquier dispositivo informático conectado a una red que puede ser un punto de entrada a actores malintencionados a una organización. Estos dispositivos pueden ser teléfonos móviles, equipos de escritorio, portátiles, máquinas virtuales y tecnología del Internet de las cosas (IoT) entre otros (Microsoft, 2024).

Herramientas de código abierto

Las herramientas de código abierto son programas cuyo código fuente está disponible públicamente, permitiendo a cualquier persona ver, modificar y distribuir el software. Se distribuyen bajo licencias que especifican cómo se puede usar y

compartir el código. Generalmente, son gratuitas o de bajo costo, y permiten una alta flexibilidad y personalización (IBM, 2024).

IPS

Un software que protege los sistemas de ataques mediante un análisis preventivo en tiempo real de las conexiones y protocolos. Identifica amenazas basadas en patrones o comportamientos sospechosos y controla el acceso a la red. Además de generar alertas, puede bloquear paquetes y cerrar conexiones sospechosas (Incibe, 2020).

Incidente de Seguridad

Ocurrencia de evento(s) que indique una posible violación de la seguridad de la información o falla de los controles que pueden dañar los activos de una organización o comprometer sus operaciones. En consecuencia, es un atentando contra la confidencialidad, la integridad y la disponibilidad de la organización (ISO, 2023).

Inteligencia de Amenazas

La Inteligencia de Amenazas se basa en recopilar y analizar información sobre ciberamenazas para ayudar a prevenir y mitigar posibles ataques. Proporciona datos sobre actores maliciosos, tácticas y vulnerabilidades explotadas. Su objetivo es anticipar riesgos y mejorar la capacidad de respuesta ante incidentes. Esto permite a las organizaciones tomar decisiones informadas en su estrategia de seguridad (Kaspersky, 2024).

Malware

El malware (software malicioso) es un tipo de software diseñado para dañar, interrumpir o obtener acceso no autorizado a sistemas y datos. Existen varios tipos de malware, incluyendo virus, gusanos, troyanos, ransomware y spyware (Cloudflare, 2024). Se propaga a menudo a través de correo electrónico malicioso, descargas de software no seguro o sitios web comprometidos.

On-premise

Se refiere a la infraestructura y software que se instalan y operan físicamente dentro de las instalaciones de una empresa u organización, en lugar de estar alojados en

la nube o gestionados por terceros. En este modelo, la empresa es responsable del mantenimiento, gestión y seguridad de los servidores y equipos donde se ejecutan las aplicaciones o servicios (Incentro, 2022).

Parches de Seguridad

Los parches de seguridad son actualizaciones que corrigen vulnerabilidades o fallos en software y sistemas, protegiéndolos de posibles ataques cibernéticos. Su objetivo es mejorar la seguridad y prevenir la explotación de brechas. Además, pueden optimizar el rendimiento y corregir otros errores. Son esenciales para mantener la integridad y protección de los sistemas (Xataca, 2020).

Phishing

Es una técnica de ingeniería social utilizada por delincuentes para obtener información confidencial como contraseñas, números de tarjetas de crédito y datos personales (Cloudflare, 2024).

Playbooks

Es un conjunto de tasks (tareas) con acciones predefinidas que guían a los equipos de seguridad en la respuesta a incidentes y amenazas. Estos tasks tienen la capacidad de llamar scritps para que ejecuten acciones, permitiendo automatizar muchos procesos de seguridad, incluidos el manejo de sus investigaciones y la administración de sus tickets (Palo Alto Networks, 2022).

Proxy

Es un servidor intermedio que procesa solicitudes entre un cliente y un servidor final (sitio web), mejorando el rendimiento mediante el almacenamiento en caché y proporcionando anonimato al ocultar la dirección IP del cliente. Además, controla el acceso a ciertos contenidos web y aumenta la seguridad al actuar como barrera entre la red interna y el tráfico externo (Palo Alto Networks, 2022).

Ransomware

Es un tipo de malware diseñado para cifrar los archivos de un usuario o sistema, impidiendo el acceso a los datos hasta que se pague un rescate, generalmente en criptomonedas. Este malware se propaga a menudo a través de tácticas como

correos electrónicos de phishing, descargas de software malicioso o aprovechamiento de vulnerabilidades en sistemas (Cloudflare, 2024).

Subplaybook

Un subplaybook es un playbook que está siendo utilizando dentro de otro. Esto con la finalidad de no hacer muy extenso el playbook principal o con el fin de crear un bucle de ejecución por cada input que se le configure (Palo Alto Networks, 2022).

SaaS

Software as a Service es un modelo de entrega de software en el cual las aplicaciones se alojan en la nube y se acceden a través de Internet. En lugar de instalar y mantener el software en computadoras locales o servidores, los usuarios pueden utilizar las aplicaciones directamente desde un navegador web, lo que elimina la necesidad de infraestructura local y la gestión de actualizaciones (Palo Alto Networks, 2022).

SIEM

Security Information and Event Management es una solución de ciberseguridad que recopila, analiza y gestiona datos de seguridad en tiempo real de diversas fuentes dentro de una organización. Combina la gestión de información de seguridad y la gestión de eventos de seguridad para detectar amenazas y comportamientos anómalos. Esto permite a las organizaciones identificar incidentes de seguridad, responder adecuadamente y cumplir con regulaciones de conformidad (Palo Alto Networks, 2022).

Vulnerabilidad

Es una debilidad o fallo en un sistema, aplicación o red que puede ser explotado por un atacante para comprometer la confidencialidad, integridad o disponibilidad de los datos y recursos. Estas vulnerabilidades pueden surgir de errores de programación, configuraciones inadecuadas, falta de actualizaciones de seguridad o incluso de procedimientos operativos deficientes (Palo Alto Networks, 2022).

CAPÍTULO III. DESARROLLO DEL TRABAJO PROFESIONAL

3.1 Determinación y análisis del problema

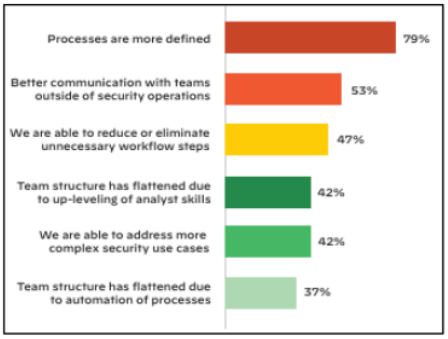
Los Centros de Operaciones de Seguridad (SOC) se han convertido en componentes esenciales de las estrategias de ciberseguridad empresarial debido al incremento en volumen y sofisticación de las ciberamenazas que son capaces de eludir los controles de seguridad más sofisticados, sin embargo, enfrentan retos significativos. En la actualidad, uno de los retos fundamentales que deben afrontar los SOC es la gestión de altas volumetrías de alertas que resultan falsos positivos junto con los procesos o tareas repetitivas que realizan diariamente.

En una publicación de Zafra (2022) indica que una misión claramente definida y un alcance bien delimitado son esenciales para el éxito de un Centro de Operaciones de Seguridad (SOC), para evitar sobrecargarlo de tareas y desviarlo de su función principal. Estas tareas que sobrecargan un SOC, como tareas de ingeniería, cumplimiento, integraciones o desarrollo de sistemas, no necesariamente son parte de su objetivo principal, pero terminan siendo gestionadas por el SOC.

Según Palo Alto Networks (2020) en su encuesta “The State of SOAR Report, 2020” donde los encuestados que han usado SOAR durante al menos dos años indicaron que: ayudó en la definición de los proceso en un 79%, permitió una mejor comunicación con los equipos fuera de las operaciones de seguridad en un 53%, hizo que los equipos de SOC pudieran reducir o eliminar pasos innecesarios en un 47%, la estructura de equipo aplanada debido a la mejora de las habilidades de los analistas en un 42%, hizo que el equipo aborde casos de uso de seguridad más complejos en un 42%, habilitó una estructura de equipo aplanada debido a la automatización de procesos en un 37%, ver Figura 5.

Figura 5

Estadística de información sobre cuánto mejoró SOAR el rendimiento del SOC



Nota: Imagen obtenido de "The State of SOAR Report, 2020". Fuente: Palo Alto Networks (2020).

La problemática del servicio SOC ofrecido por NSEK a la entidad financiera inicia identificando el proceso de detección de dominios similares existente en el equipo de Fraudes de la entidad financiera. La identificación temprana de dominios similares puede mitigar el riesgo de futuros casos de víctimas de phishing, que normalmente se materializan en operaciones fraudulentas o transacciones no reconocidas. Los tiempos de detección y respuesta del equipo de Fraudes no son óptimos debido al número de colaboradores y horario laboral (9x5) para esta área.

Durante el año 2021 al 2023 Indecopi informó que impusieron 1284 sanciones a bancos y entidades financieras por operaciones no reconocidas a nivel nacional. De dicha cantidad de sanciones impuestas, el 59.6% (765) se asocian a tarjetas de crédito y el 34.9% (448) a cuentas de ahorros (Indecopi, 2023).

Según el Decreto Supremo Nº 032-2021-PCM, las multas que Indecopi impone por operaciones no reconocidas en entidades financieras (grandes empresas) oscilan desde el 3.78 a 5.48 UITs dependiendo el tipo de afectación hacia el usuario (El Peruano, 2021).

Se estima que 100 usuarios anuales son víctimas de phishing de la entidad financiera donde brinda servicios NSEK, esto quiere decir que la entidad financiera

es propensa a recibir multas de Indecopi desde S/.1,946,700 a S/.2,822,200 anuales.

En tal sentido se plantea dar una solución alterna de implementación en el SOC sobre el proceso monitoreo de dominios similares junto con la optimización utilizando en la reducción volumétrica de alertas y toma de acciones utilizando Cortex XSOAR. Esto optimizará la gestión de alertas para prevenir posibles fraudes hacia la entidad financiera.

3.2 Modelo de solución propuesto

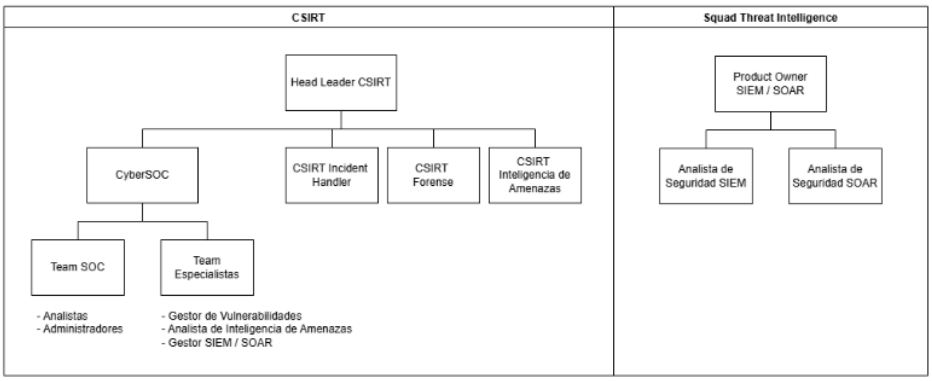
Para implementar esta optimización, es necesario conocer el organigrama de los equipos que interactúan en la implementación y el proceso de implementación.

3.2.1 Organigrama

El servicio CyberSOC (SOC más equipo de Especialistas) es liderado por el equipo de CSIRT (Equipo de Respuesta a Incidentes de Seguridad) de la entidad financiera, ver Figura 6. El Gestor de SOAR se encarga de gestionar requerimientos de automatizaciones en Cortex XSOAR, previa autorización o aprobación del Product Owner de SOAR, administrada por el Squad Threat Intelligence de la entidad financiera.

Figura 6

Organigrama de equipos de la entidad financiera



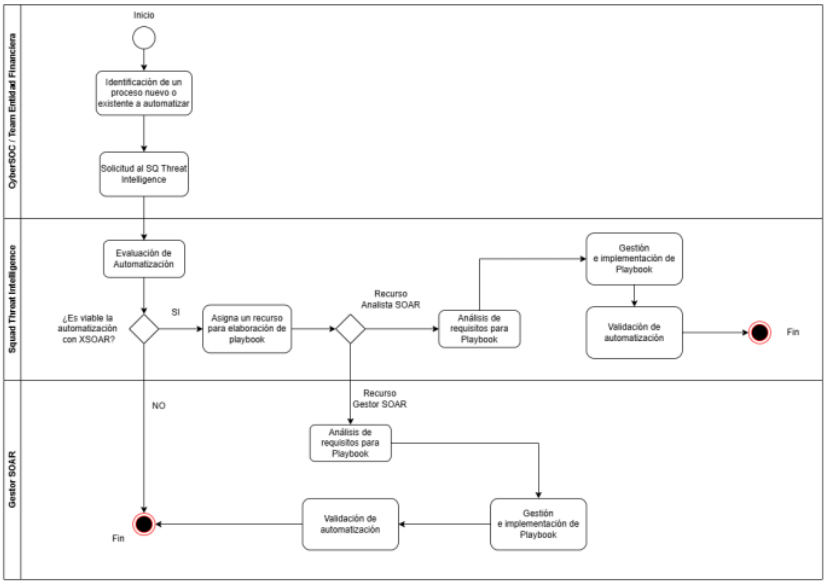
Nota: Organigrama referencial de los equipos que interactuarán en la implementación. Fuente: Propia

3.2.2 Proceso de implementación de un playbook con XSOAR

El proceso de implementación de un playbook en Cortex XSOAR en la entidad financiera requiere de una solicitud hacia Product Owner (dueño del producto) o Analista de Seguridad de la herramienta junto con la identificación del proceso que se desea automatizar para la evaluación y viabilidad de la automatización. En caso de ser aprobada, el Product Owner asigna un recurso para que la elaboración del playbook, ver Figura 7. El recurso asignado diseña e implementa el playbook previa solicitud de los requerimientos (documentos y socialización de la automatización) para el pase a producción.

Figura 7

Diagrama de flujo para implementación de un Playbook en Cortex XSOAR



Nota: Diagrama de flujo según lineamientos internos de la entidad financiera. Fuente: Propia

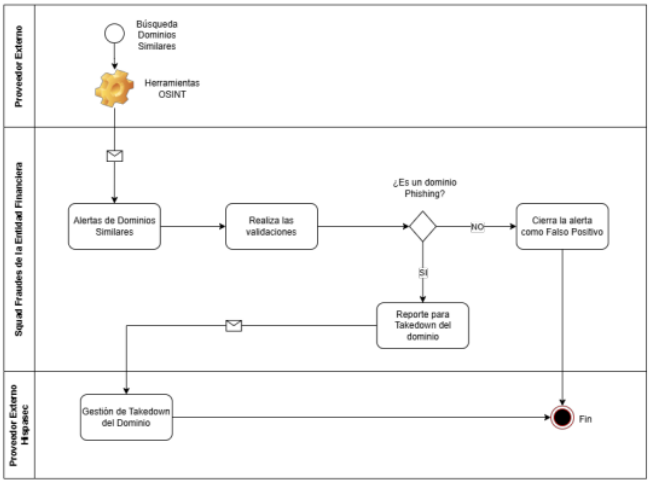
3.2.3 Identificación de Procesos

Proceso de gestión de alertas Dominios Similares: En base a las directrices para la planificación y preparación en la gestión de incidentes de seguridad de la información de la ISO 27035 y Framework NIST, se identificó que la financiera

cuenta con un sistema de monitoreo de dominios similares (gestionada por un proveedor externo) que alerta al equipo de Fraudes para su validación. Luego de realizar las validaciones respectivas, en caso de convertirse en un evento de phishing, Fraudes reporta a otro proveedor externo (Hispasec) para que pueda dar de baja (takedown) al dominio y mitigar riesgos, ver Figura 8. Los tiempos de detección y respuesta del equipo de Fraudes no son óptimos debido a la cantidad del personal y horario laboral (9x5).

Figura 8

Proceso de gestión de alertas de Dominios del Squad Fraudes

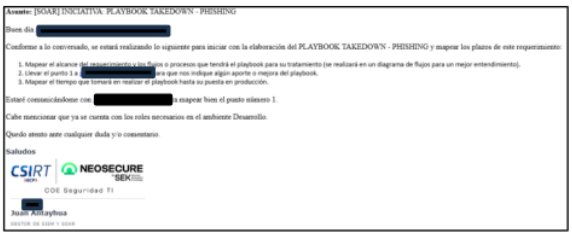


Nota: Flujo referencial de atención de alertas. Fuente: Propia

Dadas las directrices para la respuesta a incidentes de seguridad de la ISO 27035 y la característica fundamental de implementar medidas de protección del Framework NIST, el equipo de CSIRT solicitó implementar un proceso de monitoreo de dominios similares en el SOC con el objetivo complementar el monitoreo existente en otra área, ver Figura 9. Este proceso fue realizado con fuentes de código abierto y XSOAR con el objetivo de reducir el impacto reputacional y posibles fraudes hacia la entidad financiera, identificando dominios similares para la revisión, validación y toma de acción preventiva ante futuros fraudes y/o ataques. Posteriormente se optimizó la volumetría de las alertas y acciones de respuesta automatizada para contener posibles amenazas en la red interna.

Figura 9

Asignación de implementación de playbook



Asunto: [SOAR] INICIATIVA PLAYBOOK TAKEDOWN - PHISHING

Buen día [redacted]

Conforme a lo conversado, se estará realizando lo siguiente para iniciar con la elaboración del PLAYBOOK TAKEDOWN - PHISHING y mapear los plazos de este requerimiento:

1. Mapear el alcance del requerimiento y los flujos o procesos que tendrá el playbook para su tratamiento (se realizará en un diagrama de flujos para un mejor entendimiento).
2. Llevar el punto 1 a [redacted] para que nos indique algún aporte o mejora del playbook.
3. Mapear el tiempo que tomará en realizar el playbook hasta su puesta en producción.

Estaré comunicándome con [redacted] a mapear bien el punto número 1.

Cabe mencionar que ya se cuenta con los roles necesarios en el ambiente Desarrollo.

Quedo atento ante cualquier duda y/o comentario.

Saludos

CSIRT | NEOSECURE SEKTEC

COE Seguridad TI

[redacted]

Juan Antayhua

ANALISTA DE SEGURIDAD TI SENIOR

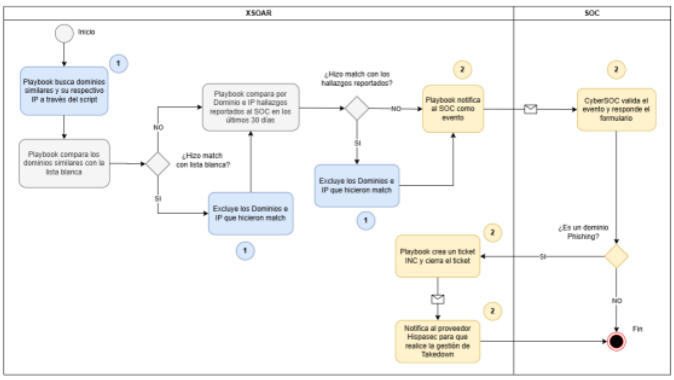
Nota: Correo de regularización de la designación de implementación. Fuente: Propia

3.2.4 Diseño de proceso de gestión de alertas de dominios similares

Para el diseño del playbook se elaboró un diagrama de flujo del nuevo proceso de la gestión de alertas de dominios similares, ver Figura 10. Este diagrama de flujo especifica las funciones principales que el playbook en XSOAR efectuará junto con las acciones realizadas por el SOC.

Figura 10

Diagrama de flujo del proceso de gestión de alertas de dominios similares en el SOC



Nota: Flujo resumido de implementación del proceso de gestión de alertas inicial de dominios similares. Los números 1 y 2 hacen referencia a los subplaybooks que ejecutaran dicha función. Fuente: Propia.

3.2.5 Requisitos para implementación de Playbooks en XSOAR

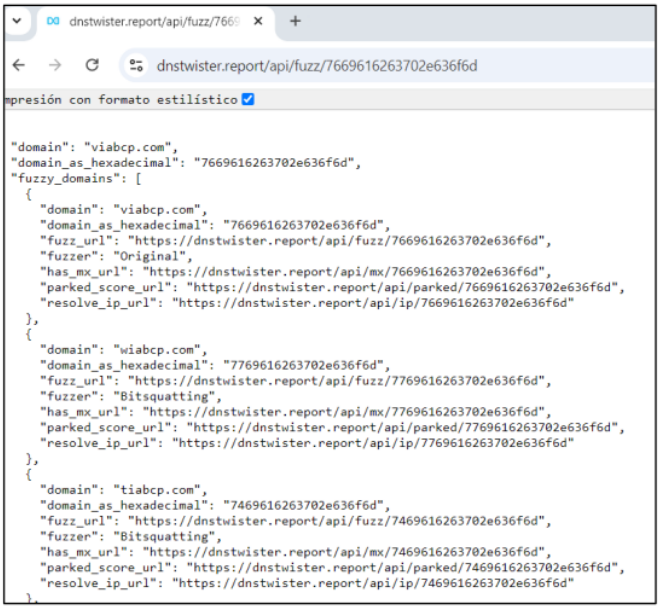
Para realizar el diseño del playbook, es importante tener mapeado nuestro alcance en el proceso que se requiere automatizar. Para ello, se debe precisar que acciones se puede realizar con las integraciones nativas que trae XSOAR y los artificios que se pueden realizar en el playbook para lograr el objetivo de la automatización. A continuación, se detalla los requisitos fundamentales que se utilizaron en el playbook.

3.2.5.1 DNStwist

DNStwist es herramienta OSINT que genera hashes (en sistema hexadecimal) similares al del nombre de un dominio web. De este modo, el programa usa algoritmos que generará una lista de dominios similares (en base al hash) que ha encontrado incluyendo dominios activos (con sus respectivas IPs) o inactivos, entre otros datos, ver Figura 11.

Figura 11

Programa DNStwist



Nota: Datos devueltos al insertar el dominio viabcp.com en la búsqueda. Fuente: Propia.

3.2.5.2 Script PhishingTakedown

Se elaboró un script en leguaje Python que funcionará como motor de búsqueda de los dominios similares utilizando el programa de código abierto DNStwist.
El script desarrollado en el entorno de XSOAR cumple la función de consultar el dominio original, insertado al final de la URL en formato hash vía API, en el programa DNStwister, ver Figura 12. Luego, solicita el estatus de la URL para determinar si encontró resultados. De encontrar resultados, solo almacena los datos de dominios similares e IPs (que contengan valores, es decir que se encuentran activos) para plasmarlo como salida en la key “Domains” y posteriormente reflejarse en el context data de un incidente en XSOAR. Para este desarrollo se colocó tres dominios como palabras clave que serán insertadas a través del playbook en la key “domainKey”.

Figura 12

Script desarrollado en XSOAR utilizando el programa DNStwister.

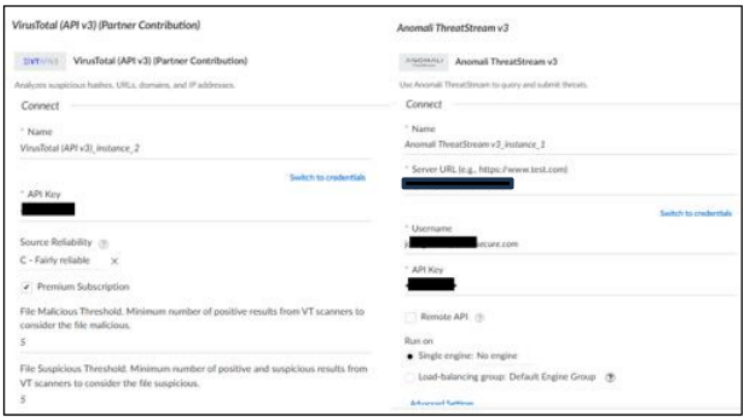
Nota: El script fue desarrollado en colaboración con el Analista de Seguridad de Inteligencia de Amenazas de CSIRT. Fuente: Propia

3.2.5.3 Feeds de Inteligencia

Para el análisis de un indicador de compromiso (IoC) sea IP, Dominio Hash o URL, se hace uso de los feeds de inteligencia. Se utilizó el feed Virus Total y Anomali Threat Stream, ver Figura 13, para enriquecer y dar un mejor contexto a las alertas.

Figura 13

Configuración de integración de feeds de inteligencia Virus Total y Anomali Threat Stream en XSOAR



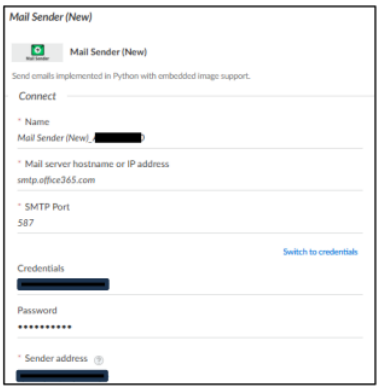
Fuente: Propia

3.2.5.4 Envío de Correo Electrónico

Se utilizó la integración Mail Sender (New) que es un desarrollo en Python para enviar correos electrónicos desde el host de correos smtp de un buzón administrado, ver Figura 14.

Figura 14

Configuración de integración Mail Sender (New) en XSOAR



Fuente: Propia

3.2.5.5 JiraITSM

Es una solución de gestión de servicios TI, que ayuda a gestionar y resolver las solicitudes en un entorno laboral mediante su sistema de tickets, ver Figura 15.

Figura 15

Configuración de integración JiraITSM en XSOAR

Fuente: Propia

3.2.5.6 Rasterize

Es un desarrollo en Python que convierte el contenido de una URL, archivos PDF o correos electrónicos en una imagen o pdf. Es una integración que XSOAR ofrece nativamente en su Marketplace, ver Figura 16.

Figura 16

Configuración de integración Rasterize en XSOAR

Fuente: Propia

3.2.5.7 Script Set

Se utiliza para establecer un valor en el context data bajo una key introducida. Estos valores solo pueden ser visualizados dentro de la ejecución de un playbook, mas no en reportes. Utilizando transformadores, puede parsear datos para almacenar y ser usados posteriormente.

3.2.5.8 Script SetIncident

Se utiliza para establecer o modificar un valor de incidente en el context data. Al igual que el script Set, este script puede modificar datos de un incidente y almacenarlos. La diferencia es que los datos almacenados si pueden visualizarse en reportes o dashboards.

3.2.6 Fase 1: Implementación de Playbooks

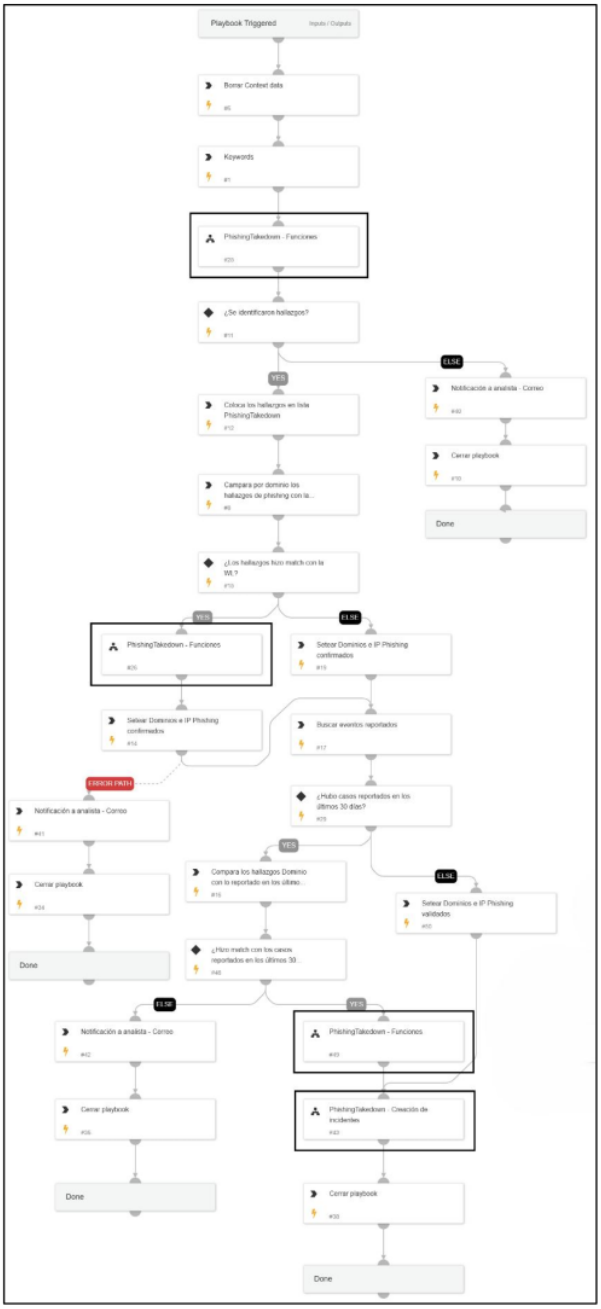
Para ser posible la automatización del proceso de gestión de alertas de dominios similares de la Figura 10, se elaboraron dos playbooks principales y dos subplaybooks:

3.2.6.1 Playbook Principal: PhishingTakedown

Este playbook tiene como objetivo buscar los dominios similares con su respectiva IP a través de la herramienta DNStwister, compara con una lista blanca y excluye los hallazgos distintos, compara y excluye los hallazgos notificados al SOC en los últimos 30 días, ver diseño en la Figura 17.

Figura 17

Diseño del playbook PhishingTakedown



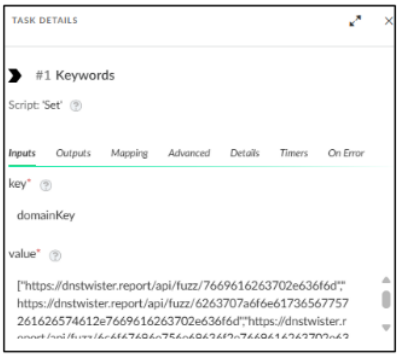
Nota: Los cuadros resaltados en negro hacen referencia a los subplaybooks utilizados dentro del playbook PhishingTakedown. Fuente: Propia

A continuación, se brinda los pasos configurados en el desarrollo del playbook:

i. Se configuró el task #1 de nombre “Keywords” que llama al script “Set” para almacenar en el context data el key “domainKey” y como valor se colocó la lista de keywords “viabcp.com, bcpzonasegurabeta.viabcp.com, loginunico.viabcp.com” en formato hash hexadecimal, ver Figura 18.

Figura 18

Configuración task #1

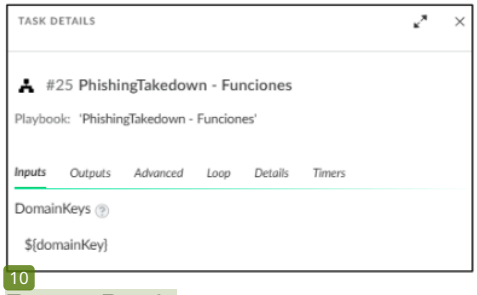


Fuente: Propia

ii. Se configuró el input “DomainKeys” del subplaybook 'PhishingTakedown - Funciones' para buscar los posibles dominios e ip similares haciendo un loop con cada input domainKey almacenado en el paso (i), ver Figura 19.

Figura 19

Configuración de input “DomainKeys” en el subplaybook 'PhishingTakedown - Funciones'

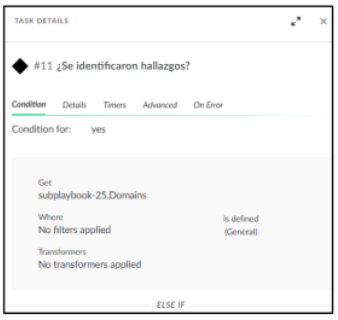


Fuente: Propia

iii. Luego se configuró el task #11 condicional de nombre “¿Se identificaron hallazgos?” para identificar si presentó hallazgos en la búsqueda del paso (ii), ver Figura 20.

Figura 20

Configuración task #11

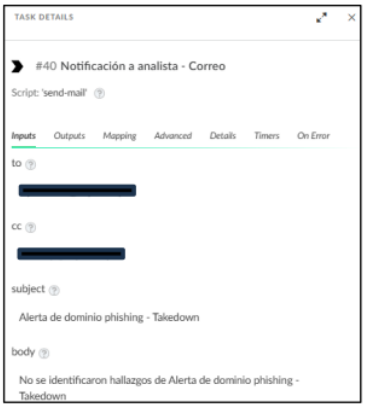


Fuente: Propia

iv. En caso no identifique hallazgos en el paso (iii), se configuró el task #40 de nombre “Notificación a analista - Correo”, llamando al script “send-mail” (de la integración Mail Sender (New)) para que envié un correo de respuesta al SOC indicando “No se ide notificaron hallazgos de Alerta de dominio phishing - Takedown” y posteriormente cierra el playbook, ver Figura 21.

Figura 21

Configuración task #40

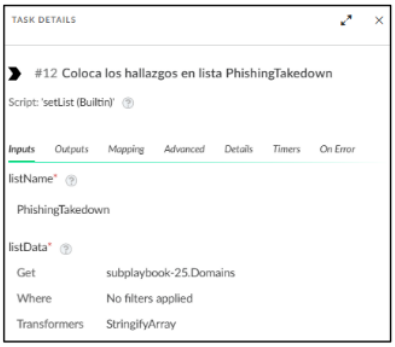


Fuente: Propia

v. En caso identifique hallazgos en el paso iii, se configuró el task #12 de nombre “Coloca los hallazgos en lista PhishingTakedown” llamando al script “setList” para almacenar los hallazgos del paso (ii) en la lista “PhishingTakedown” de XSOAR, ver Figura 22.

Figura 22

Configuración task #12

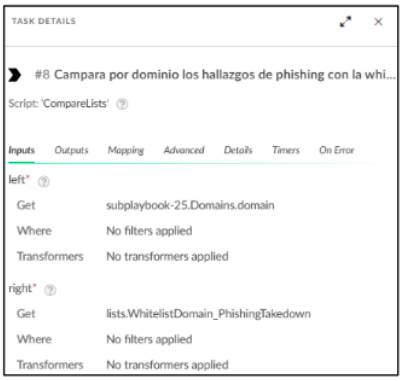


Fuente: Propia

vi. Luego se configuró el task #8 de nombre “Campara por dominio los hallazgos de phishing con la whitelist” llamando al script “CompareLists” para realizar una comparación de los hallazgos en el paso (ii) con la lista blanca de dominios “WhitelistDomain_PhishingTakedown”, ver Figura 23.

Figura 23

Configuración task #8



Fuente: Propia

vii. Luego se configuró un task #15 condicional, de nombre “¿Los hallazgos hizo match con la WL?” para identificar si hubo match en el paso (vi), ver Figura 24.

Figura 24

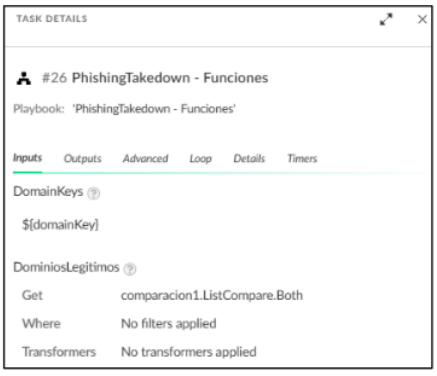
Configuración task #15

Fuente: Propia

viii. En caso si identifique match en el paso (vii), se configuró subplaybook 'PhishingTakedown - Funciones' para almacenar en el context data los hallazgos que hicieron match con la whitelist y retirarlos de la lista PhishingTakedown, ver Figura 25.

Figura 25

Configuración de input “DominiosLegitimos” en el subplaybook 'PhishingTakedown - Funciones'

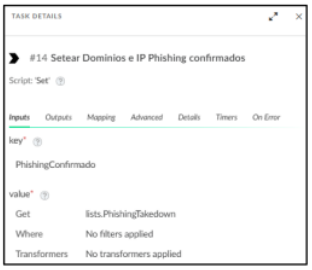


Fuente: Propia

ix. Luego se configuró un task #14 de nombre “Setear Dominios e IP Phishing confirmados” que llama al script “Set” para almacenar en el context data el key “PhishingConfirmado” y como valor se colocó los hallazgos que hicieron match en el paso (viii), ver Figura 26.

Figura 26

Configuración de task #14

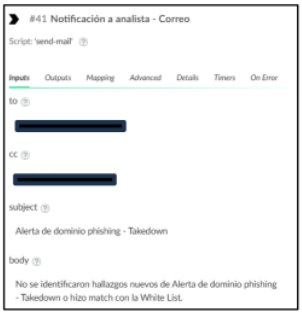


Fuente: Propia

x. En caso el paso (ix) devuelve error, significa que se retiró todos hallazgos de la lista “PhishingTakedown” en el paso (viii) y no quedaron hallazgos nuevos. Por ello se configuró el task #41 de nombre “Notificación a analista - Correo” llamando al script “send-mail” (de la integración Mail Sender (New)) para que envié un correo de respuesta al SOC indicando “No se ide notificaron hallazgos nuevos de Alerta de dominio phishing - Takedown” y posteriormente cierra el playbook, ver Figura 27.

Figura 27

Configuración de task #41

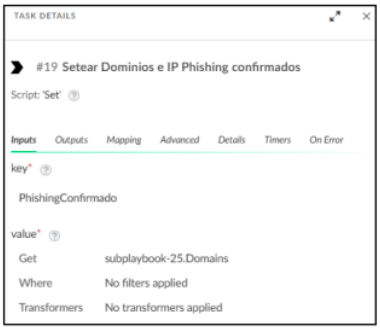


Fuente: Propia

xi. En caso no identifique match en el paso (vii), se configuró el task #19 de nombre “Setear Dominios e IP Phishing confirmados” que llama al script “Set” para almacenar en el context data el key “PhishingConfirmado” y como valor se colocó los hallazgos identificados en el paso (ii), ver Figura 28.

Figura 28

Configuración de task #19

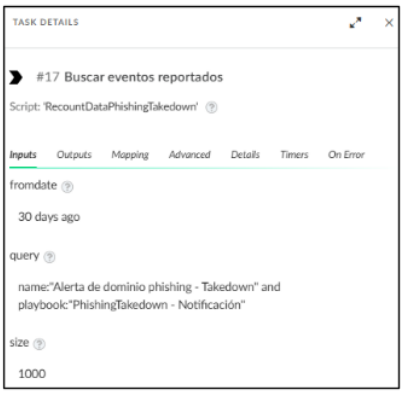


Fuente: Propia

xii. En caso el paso (ix) no devuelve error o continuando con el paso (xi), se configuró el task #17 de nombre “Buscar eventos reportados” que llama al script “RecountDataPhishingTakedown” para realizar una búsqueda de los eventos notificados al SOC en los últimos 30 días, ver Figura 29.

Figura 29

Configuración de task #17



Fuente: Propia

xiii. Luego se configuró un task #29 condicional de nombre "¿Hubo casos reportados en los últimos 30 días?" para identificar eventos notificados al SOC del paso (xii), ver Figura 30.

Figura 30

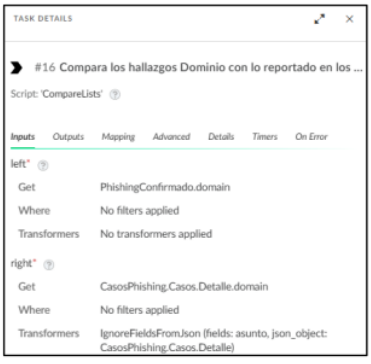
Configuración de task #29

Fuente: Propia

xiv. En caso si identifique eventos notificados en el paso (xiii), se configuró el task #16 de nombre "Compara los hallazgos Dominio con lo reportado en los últimos 30 días" llamando al script "CompareLists" para realizar una comparación de los dominios del hallazgo en el paso (ix) o (xi) con los hallazgos del paso (xii), ver Figura 31.

Figura 31

Configuración de task #16



Fuente: Propia

xv. Luego se configuró un task #48 condicional de nombre “¿Hizo match con los casos reportados en los últimos 30 días?” para identificar si hubo match en el paso (xiv), ver Figura 32.

Figura 32

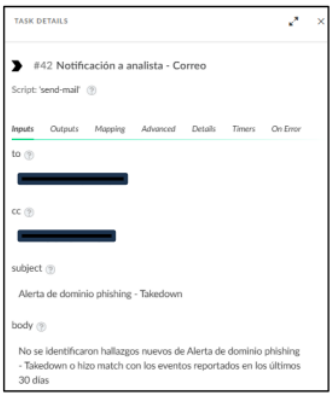
Configuración de task #48

Fuente: Propia

xvi. En caso si se identifique match en el paso (xv), se configuró el task #42 de nombre “Notificación a analista - Correo”, llamando al script “send-mail” (de la integración Mail Sender (New)) para que envié un correo de respuesta al SOC indicando “No se identificaron hallazgos nuevos de Alerta de dominio phishing - Takedown” y posteriormente cierra el playbook, ver Figura 33.

Figura 33

Configuración de task #42

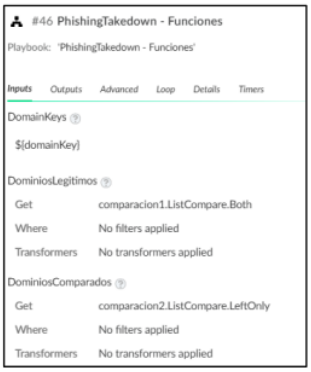


Fuente: Propia

xvii. En caso no identifique match en el paso (xv), se configuró subplaybook 'PhishingTakedown - Funciones' para almacenar en el context data los hallazgos nuevos excluyendo los dominios e ips que fueron reportados al SOC en los últimos 30 días, ver Figura 34.

Figura 34

Configuración de input "DominiosComparados" en el subplaybook 'PhishingTakedown - Funciones'

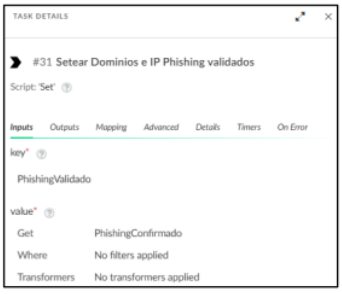


Fuente: Propia

xviii. En caso no identifique eventos notificados al SOC en el paso (xiii), se configuró el task #31 de nombre "Setear Dominios e IP Phishing validados" para almacenar en el context data el key "PhishingValidado" y como valor se colocó los hallazgos del paso (ix) o (xi), ver Figura 35.

Figura 35

Configuración de task #31

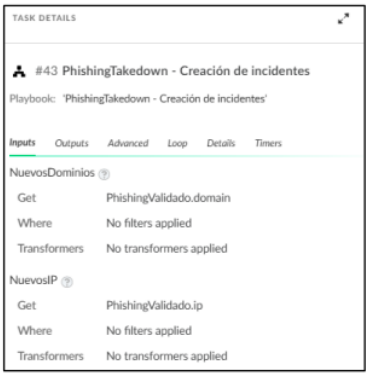


Fuente: Propia

xix. A continuación del paso (xvii) o (xviii), se configuró el subplaybook “PhishingTakedown - Creación de incidentes” para crear un incidente en XSOAR por cada hallazgo identificado y notificarlo al SOC. Posteriormente cierra el playbook y culmina, ver Figura 36.

Figura 36

Configuración de inputs “NuevosDominios” y “NuevosIP” en el subplaybook 'PhishingTakedown - Creación de Incidentes”



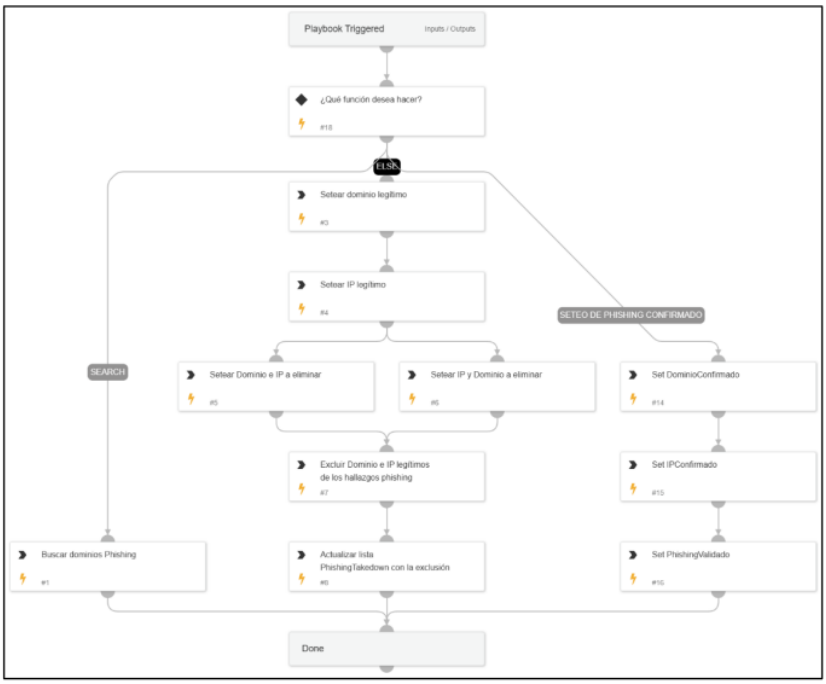
Fuente: Propia

a) Subplaybook: PhishingTakedown - Funciones

Este subplaybook es utilizado dentro del playbook “PhishingTakedown” para realizar funciones como la búsqueda de dominios similares o actualizar la lista PhishingTakedown excluyendo los dominios permitidos o también el almacenamiento de los dominios confirmados, excluyendo los eventos reportados al SOC en los últimos 30 días, ver Figura 37.

Figura 37

Diseño del subplaybook PhishingTakedown - Funciones



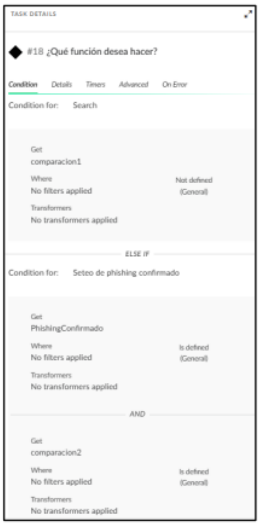
Nota: Este subplaybook tiene como finalidad ejecutar un bucle por cada input configurado. Fuente: Propia

El subplaybook “PhishingTakedown - Funciones” tiene como inputs “DomainKeys”, “DominiosLegitimos” y “DominiosComparados” que almacenan valores del paso (i), output del paso (vi) y output del paso (xiv) respectivamente del playbook “PhishingTakedown”. A continuación, se brinda los pasos configurados en el desarrollo del subplaybook.

i. Se configuró el task #18 condicional de nombre “¿Qué función desea hacer?” para identificar que función realizará la ejecución en automático, ver Figura 38.

Figura 38

Configuración de task #18

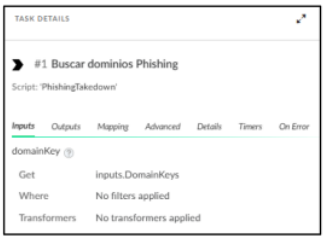


Fuente: Propia

ii. En caso identifique el paso (i) solo valores en el input DomainKeys (significa que se ejecutó el paso (ii) del playbook principal PhishingTakedown), se configuró el task #1 de nombre “Buscar dominios Phishing” llamando al script “PhishingTakedown” para que realice busque dominios similares en bucle por cada input y termina la ejecución del subplaybook, ver Figura 39.

Figura 39

Configuración de task #1

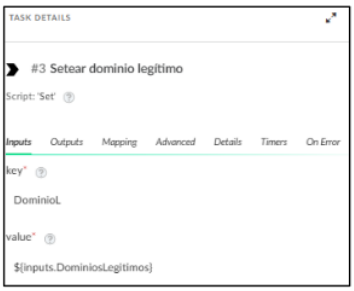


Fuente: Propia

iii. En caso identifique el paso (i) solo valores en los inputs “DomainKeys” y “DominiosLegitimos” (significa que se ejecutó el paso (viii) del playbook principal PhishingTakedown), se configuró el task #3 de nombre “Setear dominio legítimo” llamando al script “Set” para almacenar en el context data el key “DominioL” y como valor se colocó los dominios en bucle de cada input “DominiosLegitimos”, esto con la finalidad de almacenar los dominios legítimos, ver Figura 40.

Figura 40

Configuración de task #3

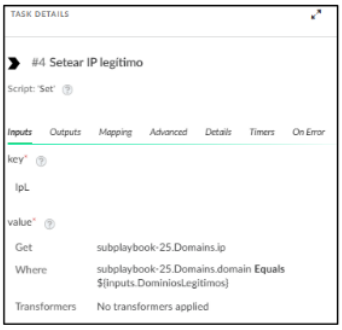


Fuente: Propia

iv. Luego se configuró un task #4 de nombre “Setear IP legítimo” que llama al script “Set” para almacenar en el context data el key “IpL” y como valor se colocó las IP en bucle de cada input “DominiosLegitimos”, esto con la finalidad de almacenar las IPs legítimas, ver Figura 41.

Figura 41

Configuración de task #4

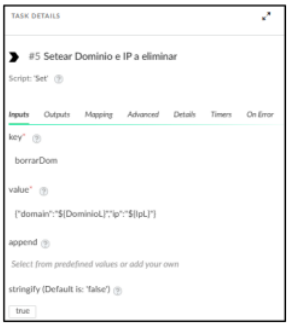


Fuente: Propia

v. Luego se configuró un artificio en el task #5 de nombre “Setear Dominio e IP a eliminar” que llama al script “Set” para almacenar en el context data el key “borrarDom” y como valor se colocó en formato JSON el valor de “DominioL” almacenado en el paso (iii) y el valor de “IpL” almacenado en el paso (iv) respectivamente, ver Figura 42.

Figura 42

Configuración de task #5

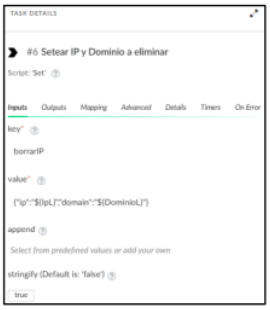


Fuente: Propia

vi. Luego se configuró un artificio en el task #6 de nombre “Setear IP y Dominio a eliminar” que llama al script “Set” para almacenar en el context data el key “borrarIP” y como valor se colocó en formato JSON el valor de “IpL” almacenado en el paso (iv) y el valor de “DominioL” almacenado en el paso (iii) respectivamente, ver Figura 43.

Figura 43

Configuración de task #6

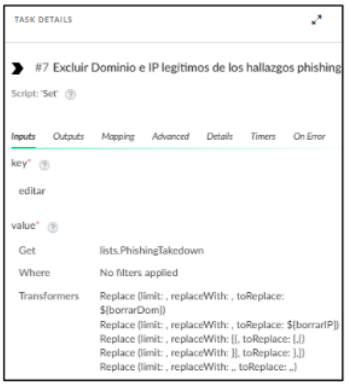


Fuente: Propia

vii. Posteriormente, se configuró el task #7 de nombre “Excluir Dominio e IP legítimos de los hallazgos phishing” que llama al script “Set” para almacenar en el context data el key “editar” y como valor se excluyó los datos del paso (v) y (vii) de la lista PhishingTakedown, es decir, se excluyó los dominios e ips legítimos de la lista almacenándolo en el key “editar”, ver Figura 44.

Figura 44

Configuración de task #7

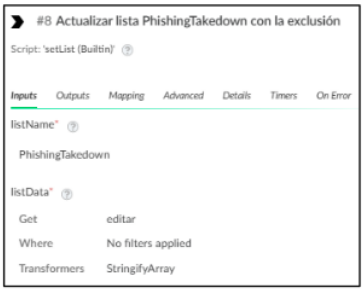


Fuente: Propia

viii. Luego se configuró el task #8 de nombre “Actualizar lista PhishingTakedown con la exclusión” que llama al script “setList” para actualizar la lista “PhishingTakedown” y sobrescribir el contenido con la data del paso (vii) y termina la ejecución del subplaybook, ver Figura 45.

Figura 45

Configuración de task #8

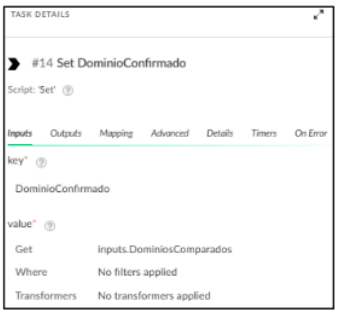


Fuente: Propia

ix. En caso identifique el paso (i) los tres inputs “DomainKeys”, “DominiosLegitimos” y “DominiosComparados” (significa que se ejecutó el paso (xvii) del playbook principal PhishingTakedown), se configuró el task #14 de nombre “Set DominioConfirmado” llamando al script “Set” para almacenar en el context data el key “DominioConfirmado” y como valor se colocó los dominios en bucle de cada input “DominiosComparados”, ver Figura 46.

Figura 46

Configuración de task #14

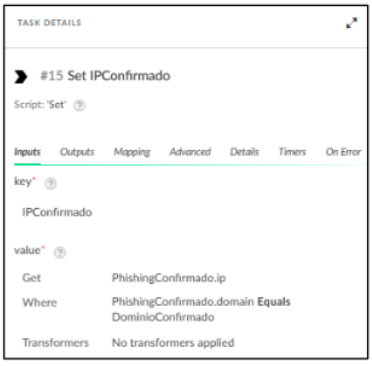


Fuente: Propia

x. Luego se configuró el task #15 de nombre “Set IPConfirmado” llamando al script “Set” para almacenar en el context data el key “IPConfirmado” y como valor se colocó las IP en bucle de cada input “DominiosComparados”, ver Figura 47.

Figura 47

Configuración de task #15



Fuente: Propia

xi. Por último, se configuró el task #16 de nombre “Set PhishingValidado” llamando al script “Set” para almacenar en el context data el key “PhishingValidado” y como valor se colocó en formato JSON los dominios e ips las almacenados en los pasos (ix) y (x). Posteriormente cierra la ejecución del subplaybook, ver Figura 48.

Figura 48

Configuración de task #16

Fuente: Propia

b) Subplaybook: PhishingTakedown - Creación de incidentes

Este subplaybook es utilizado dentro del playbook “PhishingTakedown” para crear un incidente por cada hallazgo nuevo identificado en el paso (xi) del subplaybook PhishingTakedown - Funciones o el paso (xviii) del playbook PhishingTakedown. Tiene como inputs “NuevosDominios” y “NuevosIP”, ver Figura 49.

Figura 49

Diseño del subplaybook PhishingTakedown - Creación de incidentes

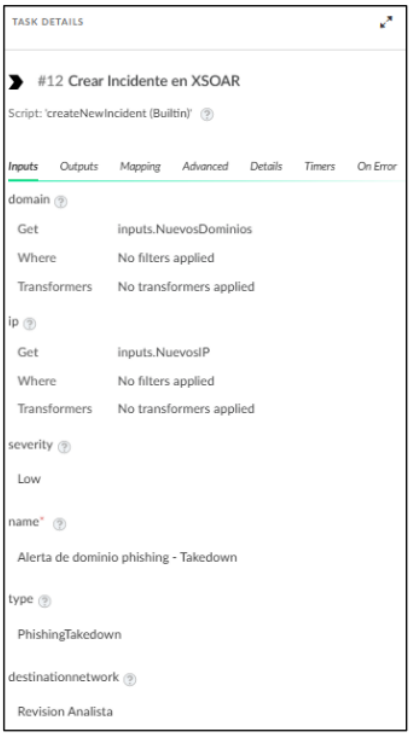
Nota: Tiene como finalidad ejecutar un bucle por cada input configurado. Fuente: Propia

A continuación, se brinda los pasos configurados en el desarrollo del subplaybook.

i. Se configuró el task #12 de nombre “Crear Incidente en XSOAR” llamando al script “createNewIncident” para establecer los parámetros del incidente que creará por cada hallazgo identificado con un entre tiempo de 90 segundos (task #17), es decir por cada input “NuevosDominios” y “NuevosIP”. Posteriormente cierra la ejecución del subplaybook, ver Figura 50.

Figura 50

Configuración task #12



Fuente: Propia

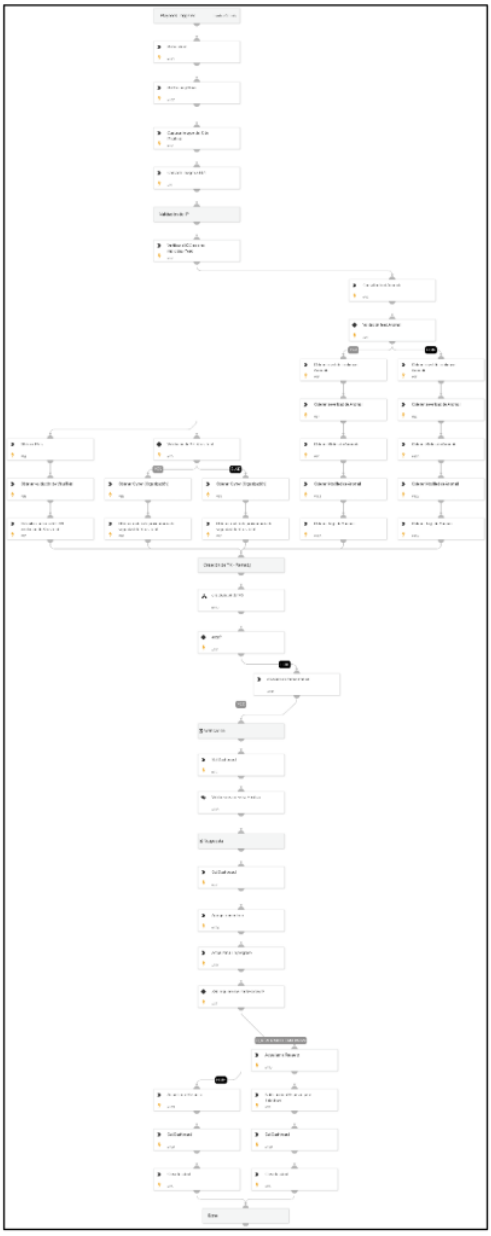
3.2.6.2 Playbook Principal: PhishingTakedown - Notificación

Este playbook se ejecuta a raíz del “Playbook PhishingTakedown - Creación de incidentes”, para cada hallazgo de dominio similar y su respectiva ip, posteriormente notifica el evento al SOC para que se realice el triaje donde tiene

un formulario con la opción de elegir dar de baja al dominio o cerrarlo en automático, ver Figura 51.

Figura 51

Diseño del playbook PhishingTakedown - Notificación



Fuente: Propia

A continuación, se brinda los pasos configurados en el desarrollo del playbook:

i. Se configuró el task #79 de nombre “Capturar imagen del Sitio Phishing” llamando al script “rasterize” para navegar en el dominio almacenado en la key “incident.domain” creado en el paso (i) del subplaybook PhishingTakedown - Creación de incidentes. Esto con el fin de obtener una imagen del contenido del sitio web, ver Figura 52.

Figura 52

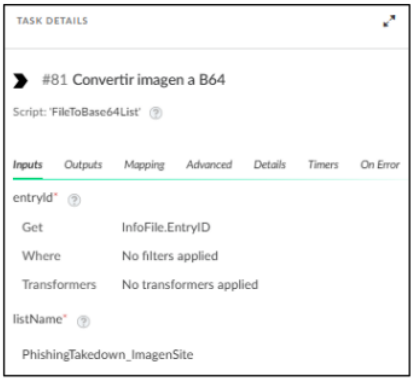
Configuración task #79

Fuente: Propia

ii. Luego se configuró el task #81 de nombre “Convertir imagen a B64” llamando al script “FileToBase64List” para convertir la imagen del paso (i) en código base 64 y almacenarlo en la lista “PhishingTakedown_ImagenSite”, ver Figura 53.

Figura 53

Configuración task #82

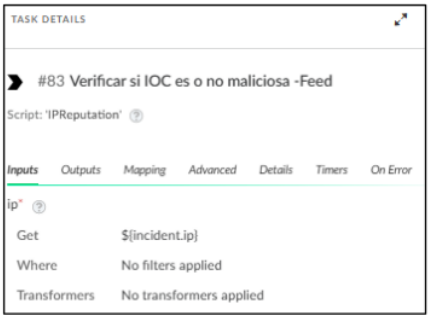


Fuente: Propia

iii. Luego se configuró el task #83 de nombre “Verificar si IOC es o no maliciosa - Feed” llamando al script “IPReputation” para consultar en los feeds de inteligencia la reputación de la IP, ver Figura 54.

Figura 54

Configuración task #83



Fuente: Propia

iv. Luego se configuró múltiples task para almacenar información de la IP del dominio similar (país, owner, numero de vendors, severidad, tags, etc) consultadas en los feeds de inteligencia de Virus Total y Anomali Threat Stream, ver Figura 55.

Figura 55

Configuraciones múltiples task para enriquecimiento de la alerta

Nota: Este enriquecimiento brinda más contexto de la alerta. Fuente: Propia

v. Luego se configuró el task #113 de nombre “Jira creacion tk INC” llamando al subplaybook nativo “Jira creacion tk INC” para crear un ticket INC en el sistema de JiraITSM, junto con los detalles de la alerta, ver Figura 56.

Figura 56

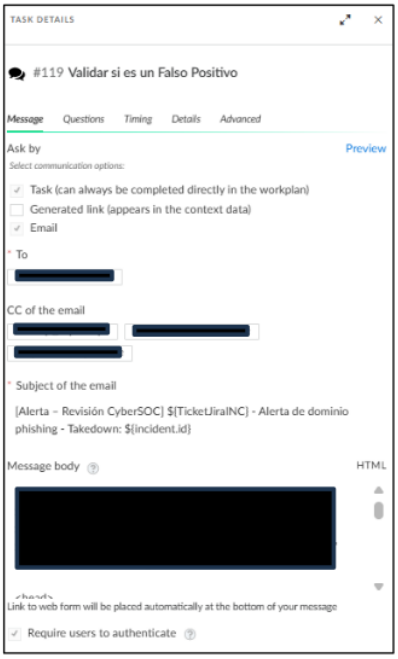
Configuración de inputs del subplaybook “Jira creacion tk INC”

Nota: Detalle de parámetros necesarios para la creación de ticket. Fuente: Propia

vi. Se configura el task #119 tipo data collection de nombre “Validar si es un Falso Positivo” donde alerta al SOC por correo electrónico el evento de dominios similares. Este task recoleta información a través del formulario que contiene en el correo del evento. Con esto, el analista del SOC interactúa con el formulario (previa autenticación) para responder a la pregunta “¿Es un dominio phishing activo?” las opciones “Si, notificar a Hispasec para el takedown.” y “No, es un falso positivo.”. Se elaboró una plantilla de correo en formato html para la notificación al SOC, esto con la finalidad customizar la alerta y enriquecer con varios datos, ver Figura 57.

Figura 57

Configuración task #119

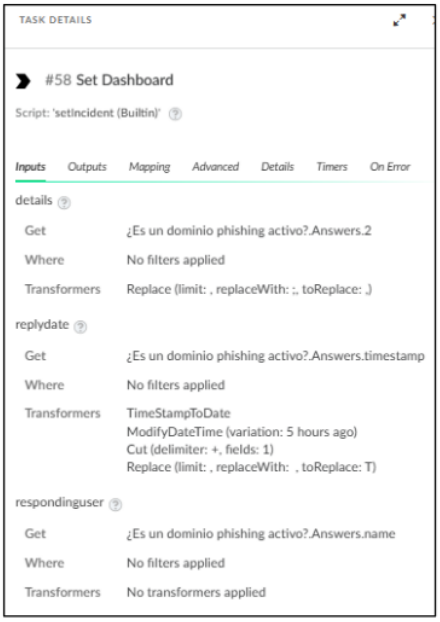


Fuente: Propia

vii. Luego se configuró el task #58 tipo data collection de nombre “Set Dashboard” llamando al script “setIncident” para almacenar la fecha de respuesta del formulario, el detalle de la respuesta del formulario y el usuario quien respondió el formulario; esto en los campos replydate, details y respondinguser, ver Figura 58.

Figura 58

Configuración task #58

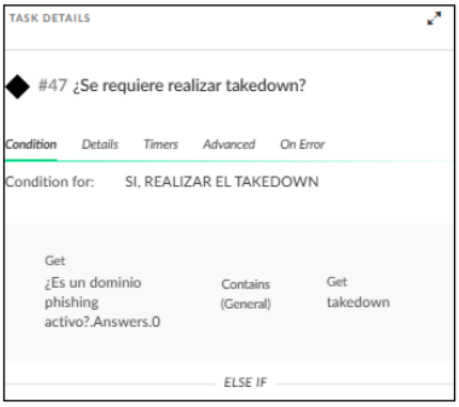


Fuente: Propia

viii. Luego se configuró un task #47 de tipo condicional con el nombre "¿Se requiere realizar takedown?" para decidir una acción en el evento, ver Figura 59.

Figura 59

Configuración task #47



Fuente: Propia

ix. En caso se identifique en el paso (viii) que el analista del SOC respondió el formulario con la opción “Si, notificar a Hispasec para el takedown”, se configuró el task #118 con el nombre “Actualizar a Resuelto” llamando al script “jira-update-status” para cambiar el estado del ticket a Resuelto y cerrándolo como Verdadero Positivo, ver Figura 60.

Figura 60

Configuración task #118

Fuente: Propia

x. Luego se configuró el task #52 de nombre “Notificación a Hispasec para Takedown” llamando al script “send-mail” (de la integración Mail Sender (New)) para que envié un correo al proveedor Hispasec indicando que gestione el takedown del dominio phishing identificado. Posteriormente cierra la ejecución de playbook, ver Figura 61.

Figura 61

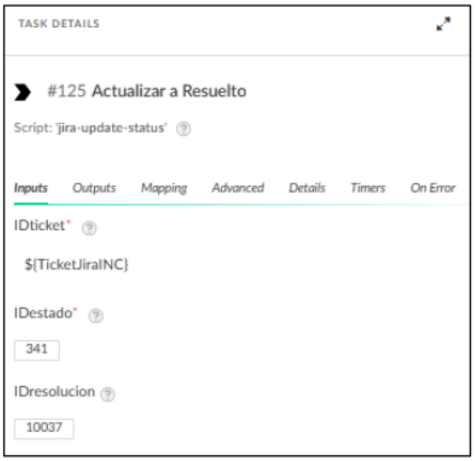
Configuración task #52

Fuente: Propia

xi. En caso se identifique en el paso (viii) que el analista del SOC respondió el formulario con la opción “No, es un falso positivo”, se configuró el task #125 con el nombre “Actualizar a Resuelto” llamando al script “jira-update-status” para cambiar el estado del ticket a Resuelto y cerrándolo como Falso Positivo, ver Figura 62.

Figura 62

Configuración task #125



Fuente: Propia

3.2.7 Gestión de implementación de Playbooks

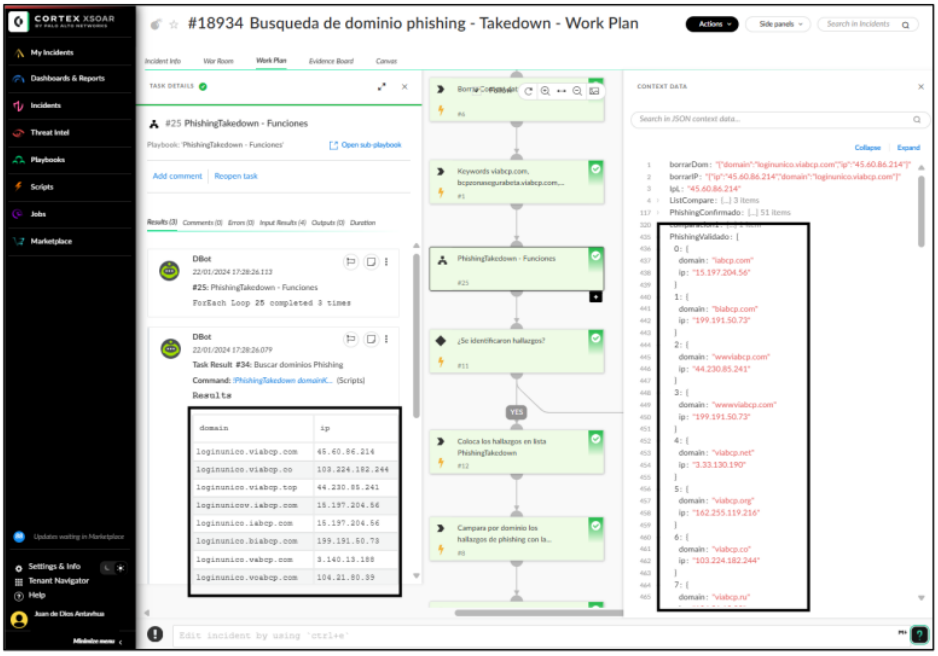
Antes de puesta a marcha blanca o pase a entornos productivos, se ejecutan pruebas en entorno de desarrollo para identificar posibles errores en su ejecución o algún ajuste que se deba realizar.

3.2.7.1 Ejecución de pruebas de Playbooks

Se ejecutó el playbook principal “PhishingTakedown” y se identificó el correcto funcionamiento del script “PhishingTakedown” que hace uso de la herramienta DNStwist para obtener dominios similares, así mismo se identificó que se estaba excluyendo correctamente los hallazgos reportados al SOC en los últimos 30 días y la exclusión de dominios legítimos, ver Figura 63.

Figura 63

Prueba de playbook principal PhishingTakedown

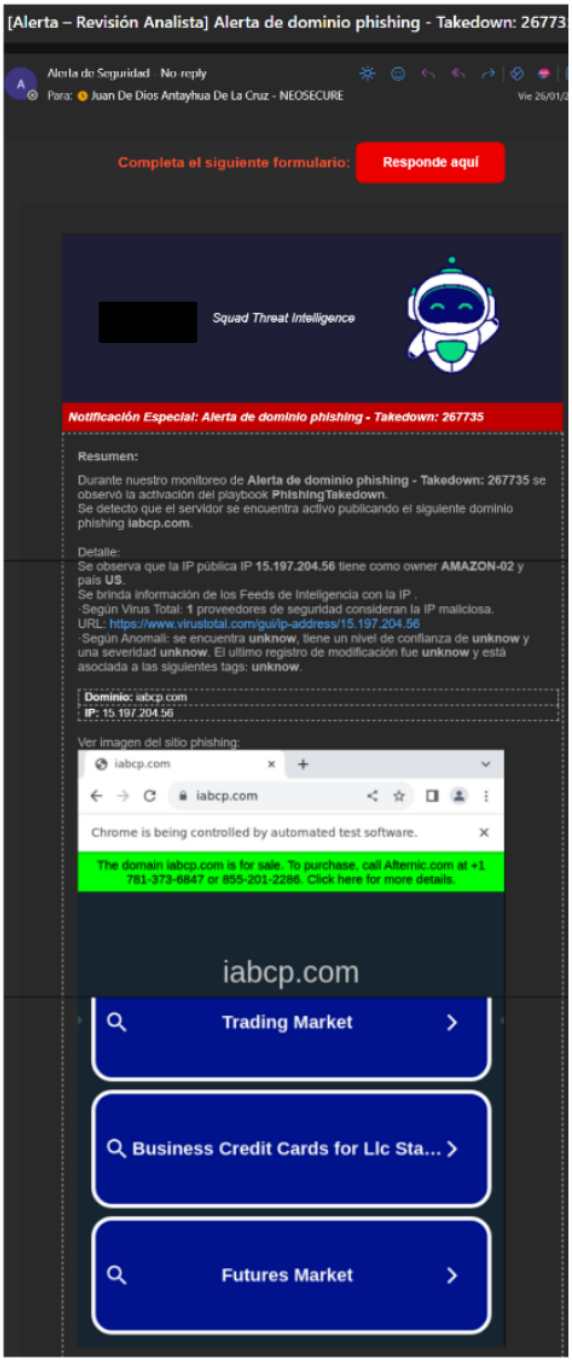


Nota: Los cuadros resaltados evidencia de la data que está procesando el playbook para la identificación de dominios similares. Fuente: Propia

También, se realizó pruebas del playbook principal “PhishingTakedown - Notificación” donde se observó el alertamiento por correo del evento junto con el contenido de la plantilla diseñada. Esta plantilla trae consigo datos del enriquecimiento de contexto de la IP, captura de pantalla del sitio de dominio similar y el formulario para respuesta del evento, ver Figura 64.

Figura 64

Prueba de plantilla de notificación del evento.



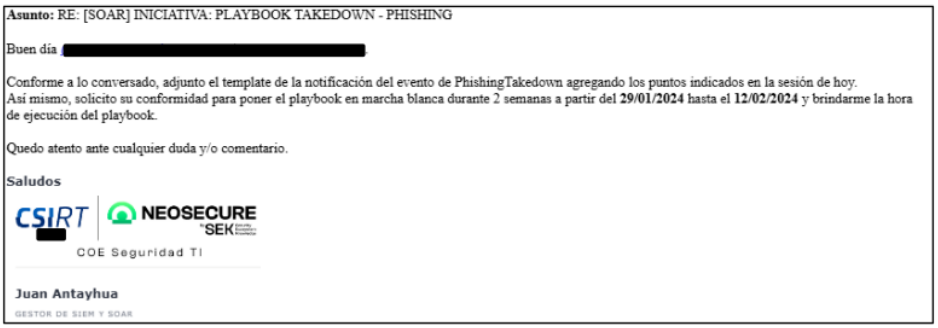
Fuente: Propia

3.2.7.2 Solicitud de conformidades para periodo de marcha blanca

Luego de haber diseñado el playbook y realizado las configuraciones y pruebas necesarias, se solicitó al cliente (Lider de CSIRT) su aprobación para ejecutar la fase de marcha blanca (entorno desarrollo) de las alertas por un periodo de dos semanas, ver Figura 65. Esta marcha blanca fue llevada de manera interna, es decir, las alertas no fueron enviadas al SOC sino al Analista de Seguridad de Inteligencia de Amenazas quien se ocupó de tratarlas.

Figura 65

Correo de solicitud para ingreso a fase de marcha blanca



Asunto: RE: [SOAR] INICIATIVA: PLAYBOOK TAKEDOWN - PHISHING

Buen día [redacted].

Conforme a lo conversado, adjunto el template de la notificación del evento de PhishingTakedown agregando los puntos indicados en la sesión de hoy.
Así mismo, solicito su conformidad para poner el playbook en marcha blanca durante 2 semanas a partir del **29/01/2024** hasta el **12/02/2024** y brindarme la hora de ejecución del playbook.

Quedo atento ante cualquier duda y/o comentario.

Saludos

CSIRT [redacted] | NEOSECURE SEK

COE Seguridad TI

Juan Antayhua

GESTOR DE SIEM Y SOAR

Fuente: Propia

Luego de recibir el conforme del cliente (Lider de CSIRT), se solicita el conforme del Product Owner de XSOAR, ver Figura 66, y con ello se procede con la implementación (activación) de los playbooks y demás desarrollos elaborados para la automatización en entorno de desarrollo, ver Figura 67.

Figura 66

Correo de conformidad de Líder de CSIRT

Nota: Se evidencia la solicitud de conformidad hacía el Product Owner. Fuente: Propia

Figura 67

Correo de conformidad de Product Owner de XSOAR

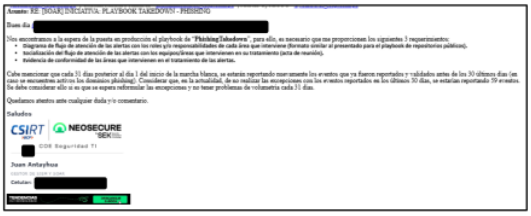
Nota: También se evidencia la implementación en entornos productivos y puesta en fase de marcha blanca. Fuente: Propia

3.2.7.3 Solicitud de requerimientos de pase a entornos productivos

Culminada la fase de marcha blanca y de no encontrar errores en la ejecución de la implementación, se solicitó al cliente los requerimientos de diagrama de flujo del tratamiento de la alerta, socialización con los equipos que interactúan en el proceso de gestión de alertas de dominios similares y la conformidad de los equipos que participan, ver Figura 68.

Figura 68

Correo de solicitud de requerimientos de pase a producción



Fuente: Propia

Luego de obtener los requerimientos de pase a producción junto con las conformidades necesarias, ver Figura 69, se procedió a implementar (activar) en entornos productivos los playbooks y automatizaciones desarrolladas el 20 de marzo del 2024, ver Figura 70.

Figura 69

Correo de respuesta con requerimientos de pase a producción

Fuente: Propia

Figura 70

Correo implementación en entorno de producción

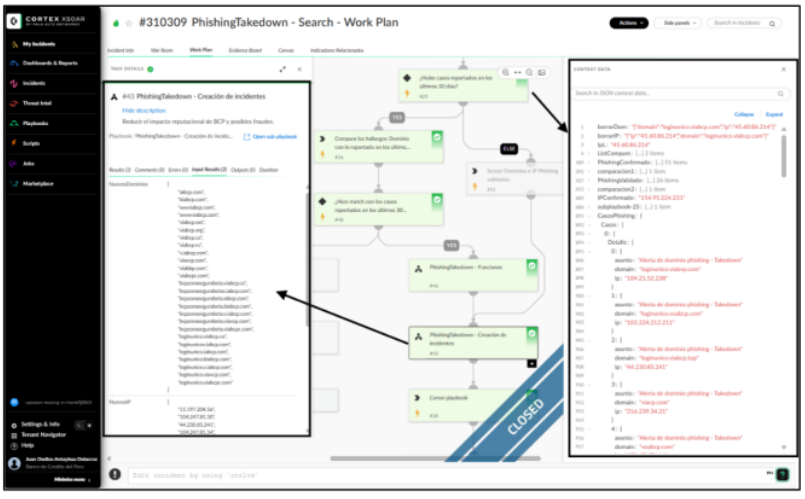
Fuente: Propia

3.2.8 Validación de implementación de Playbooks

Puesto en producción el proceso de gestión de alertas de dominios similares e implementado el playbook “PhishingTakedown” para esta gestión, se procedió a validar el correcto funcionamiento de las alertas, obtención de métricas y análisis de datos obtenidos. Se validó el correcto funcionamiento del job que ejecuta diariamente a las 9 am el playbook “Phishingtakedown - Search” en Cortex XSOAR, donde no se observó eventos nuevos dentro de los 10 primeros días. El día 11, se observó la correcta creación de incidentes de dominios similares junto con sus IPs activos y visualizándose en el context data, ver Figura 71.

Figura 71

Recolección de dominios similares

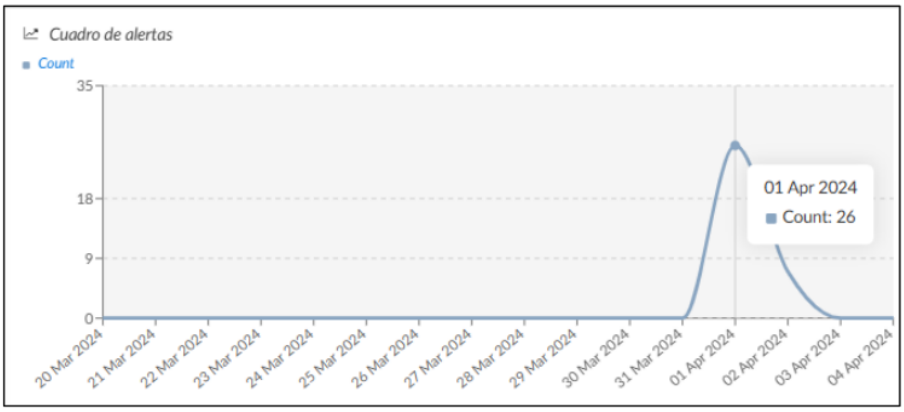


Fuente: Propia

Se validó el correcto alertamiento del playbook “PhishingTakedown - Notificación”, sin embargo, el día 11 posterior a la puesta en producción, se visualizó el alertamiento de manera masiva de dominios similares en simultáneo. El día 11 se alertó 26 eventos de dominios similares en menos de 20 minutos y de manera similar el día 12 se alertó 7 eventos de dominios similares, ver Figura 72. De las 33 alertas presentadas, el SOC llegó a la conclusión luego de la validación que 30 fueron verdaderos positivos (se derivaron para la gestión correspondiente de takedown) y 3 fueron falsos positivos en un tiempo promedio de atención de 8 horas.

Figura 72

Volumetría de alertas de dominio phishing

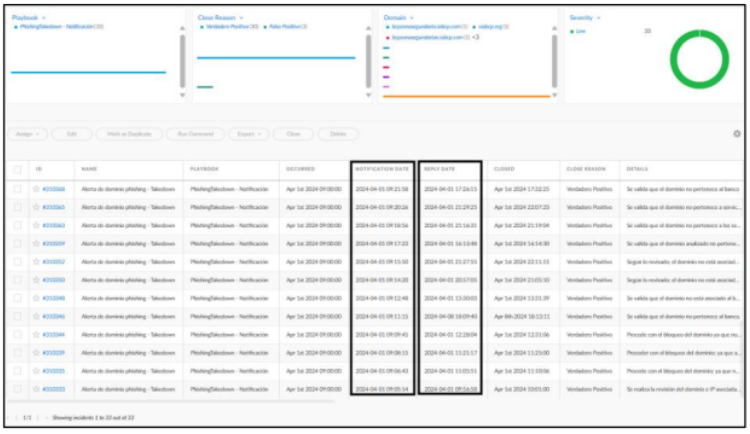


Fuente: Propia

Esta volumetría de alertas ocasionó que se incumpliera con los tiempos esperados para responder los eventos de dominios similares, ver Figura 73, donde el tiempo esperado es de 2 horas según acuerdo contractual para alertas de severidad Baja. Para más detalles de los 33 eventos gatillados en la fase 1, ver Anexo 1.

Figura 73

Alertamiento masivo en un corto periodo de tiempo

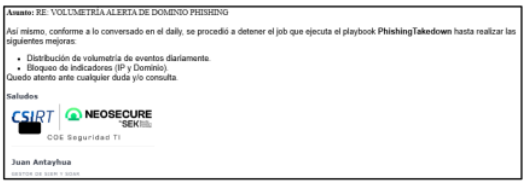


Nota: La columna “Notification Date” y “Reply Date” indican los tiempos en que fue notificado la alerta y el tiempo en que fue respondido el formulario de la alerta respectivamente. Así mismo, la columna Close Reason indica el veredicto final del evento. Fuente: Propia

Esta volumetría fue alertada por el SOC, donde a raíz de ello se planteó optimizar las alertas distribuyendo la volumetría y agregar el bloqueo de indicadores de forma automatizada a través del formulario del evento, mientras tanto se detuvo el alertamiento de los eventos de dominios similares, ver Figura 74. Realizando un análisis de los comentarios colocados en los formularios de los eventos (columna Details de la Figura 73), se observó que el SOC no tenía bien definido el criterio para considerar una alerta como verdadero positivo, y se solicitó el reforzamiento de atención de la alerta.

Figura 74

Correo de evidencia de puntos a optimizar en las alertas de dominios similares



Asunto: RE: VOLUMETRIA ALERTA DE DOMINIO PHISHING

Así mismo, conforme a lo conversado en el daily, se procedió a detener el job que ejecuta el playbook **PhishingTakedown** hasta realizar las siguientes mejoras:

- Distribución de volumetría de eventos diariamente.
- Bloqueo de indicadores (IP y Dominio).

Quedo atento ante cualquier duda y/o consulta.

Saludos

CSIRT | NEOSECURE SEK

COE Seguridad TI

Juan Antayhua

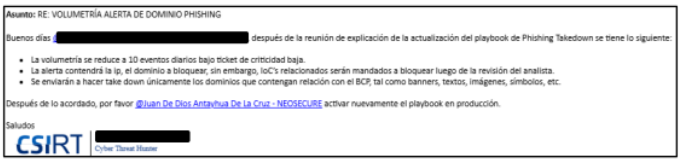
Fuente: Propia

3.2.9 Optimización de alertas de dominios similares

La mejora continua dispuesta por la norma ISO 27001 está presente en el servicio brindado a la entidad financiera. Para optimizar los puntos observados en la gestión de alertas de dominios similares, se distribuyó la volumetría a 10 eventos por día como máximo, teniendo un entre tiempo de 90 minutos. Además, se agregó el bloqueo en los sistemas de seguridad del dominio similar e ip del evento a través del formulario y de forma automatizada, ver Figura 75.

Figura 75

Correo de socialización de la optimización



Fuente: Propia

3.2.10 Fase 2: Implementación de Optimización

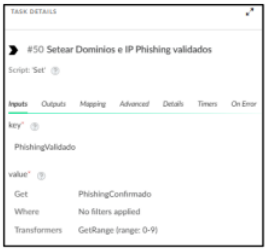
Se realizó la implementación de la optimización el 22 de mayo del 2024 en los siguientes playbooks:

3.2.10.1 Playbook Principal: PhishingTakedown

i. Se configuró el task #50 de nombre “Setear Dominios e IP Phishing validados” para almacenar en el context data el key “PhishingValidado” donde se agregó la configuración de obtener solo los 10 primeros eventos de los hallazgos del paso (ix) o (xi) de la configuración del playbook “PhishingTakedown” inicial, aplicando el Transformers GetRange(range:0-9) todo ello en reemplazo del task #31, ver Figura 76.

Figura 76

Configuración de task #50

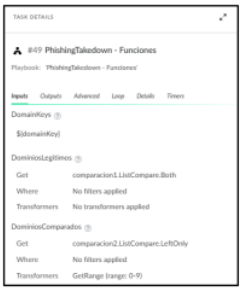


Fuente: Propia

ii. Se configuró subplaybook 'PhishingTakedown - Funciones' para almacenar en el context data solo los primeros10 hallazgos nuevos excluyendo los dominios e ips que fueron reportados al SOC en los últimos 30 días. Aplicando el Transformers GetRange(range:0-9) todo ello en reemplazo del paso (xvii) del playbook "PhishingTakedown" inicial, ver Figura 77.

Figura 77

Configuración de input "DominiosComparados" con aplicación de Transformers en el subplaybook 'PhishingTakedown - Funciones'



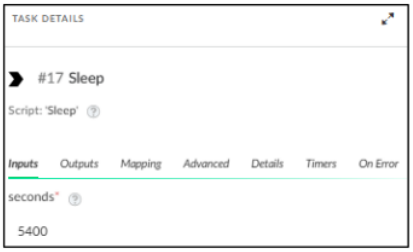
Fuente: Propia

3.2.10.2 Subplaybook: PhishingTakedown - Creación de incidentes

i. Se reconfiguró el task #17 de nombre "Sleep" llamando al script "Sleep" para detener la ejecución del subplaybook por un tiempo de 90 minutos. Esto con el objetivo que cada creación de un incidente tenga como entre tiempo de 90 minutos, ver Figura 78.

Figura 78

Configuración task #17



Fuente: Propia

3.2.10.3 Playbook Principal: PhishingTakedown - Notificación

i. Se reconfiguró el task #119 tipo data collection de nombre “Validar si es un Falso Positivo” donde alerta al SOC por correo electrónico el evento de dominios similares. Se agregó la pregunta “¿Desea que se realice el bloqueo de la IP y/o Dominio?” en el formulario junto con las opciones “Bloqueo de IP y Dominio”, “Solo bloqueo de IP”, “Solo bloqueo de Dominio” y “No bloquear”, ver Figura 79.

Figura 79

Configuración task #119

Fuente: Propia

ii. Posterior al task #119, se agregó la funcionabilidad de bloquear IP y/o Dominio del evento según se marque en el formulario. Para ello, se agregó el subplaybook "BCP - Bloquear Indicador - Produccion" donde cumple la funcionalidad de bloquear IP en la Lista Externa Dinámica del Next Generation Firewall de Palo Alto y también en el WAF Imperva Incapsula. Así mismo, los dominios se bloquearán en lista de bloqueo del Proxy Netskope, ver Figura 80.

Figura 80

Configuración del subplaybook "Bloquear Indicador - Produccion"

Nota: Este subplaybook fue elaborado por la entidad financiera para agilizar el bloqueo de indicadores de compromiso. Fuente: Propia

3.2.11 Validación de la optimización

3.2.11.1 Validación de alertamiento de dominios similares

En base a la función principal de detección del Framework NIST, se puede observar en la Figura 81 el alertamiento por correo del evento de dominios similares, junto con sus tres componentes clave.

El componente número 1 de la alerta de dominios similares, contiene el link para responder el formulario del evento, este link se encuentra como hipervínculo en el texto "Responde aquí". El Analista de Seguridad del SOC luego de realizar el análisis del evento, responderá la pregunta del formulario "¿Es un dominio phishing activo?" con las opciones "Si, notificar a Hispasec para el takedown." o "No, es un falso positivo.". Así mismo responderá a la siguiente pregunta "¿Desea que se

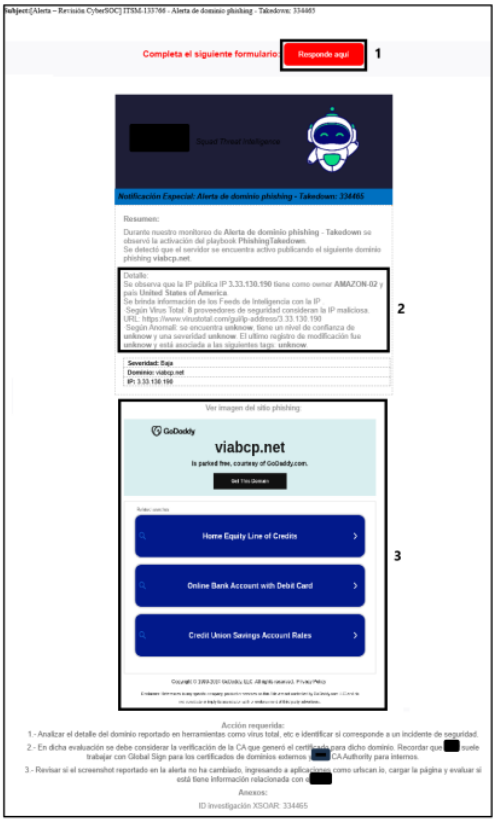
realice el bloqueo de la IP y/o Dominio?" con las opciones "Bloqueo de IP y Dominio", "Solo bloqueo de IP", "Solo bloqueo de Dominio" o "No bloquear".

El componente número 2 de la alerta de dominios similares contiene el enriquecimiento de los feeds de inteligencia Virus Total y Anomali Threat Stream. Este enriquecimiento brinda un mejor contexto a la alerta referente a las amenazas se encuentra relacionada el evento a través de sus indocares (Dominio o IP).

El componente número 3 de la alerta de dominios similares contiene una imagen del contenido de la URL, esto con el fin de mitigar el riesgo de descargar un posible contenido malicioso al intentar acceder, cumpliendo así con el requisito de la ISO 27001, reduciendo también el tiempo de validación al ingresar a la página web.

Figura 81

Alerta por correo de dominios similares

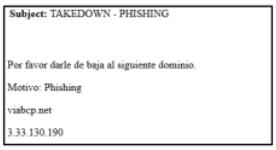


Nota: Plantilla de notificación de eventos de dominios similares. Fuente: Propia

Luego de responder el formulario con la opción “Si, notificar a Hispasec para el takedown.”, Cortex XSOAR enviará un correo de notificación al proveedor Hispasec para que realice la gestión de takedown del dominio alertado, ver Figura 82.

Figura 82

Alertamiento a Hispasec para gestión de takedown del dominio



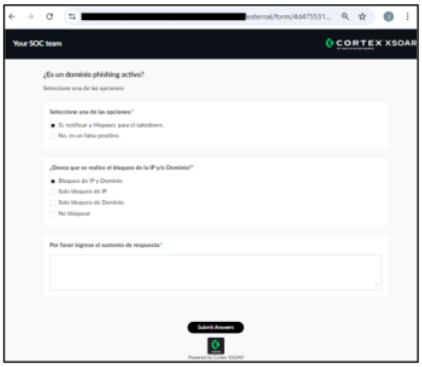
Fuente: Propia

3.2.11.2 Validación del bloqueo automatizado de indicadores de compromiso

Luego de abrir el formulario y responder a la pregunta “¿Desea que se realice el bloqueo de la IP y/o Dominio?” con la opción “Bloqueo de IP y Dominio”, ver Figura 83, el playbook ejecutó las tareas correspondientes de bloqueo para agregar los indicadores en las listas de bloqueo de las herramientas de seguridad de forma automatizada (Proxy, WAF y Firewall). Esta función alineada a la ISO 27035 y el Framework NIST permite responder y prevenir futuros incidentes hacia la entidad financiera.

Figura 83

Contenido del formulario del evento

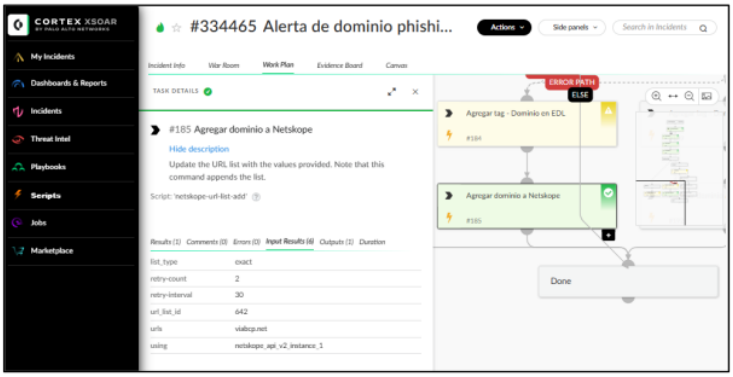


Fuente: Propia

Se validó a nivel de XSOAR el correcto funcionamiento del playbook para el bloqueo de Dominio en el Proxy. En la Figura 84 se evidencia el envío correcto de datos al Proxy para añadir a su lista negra.

Figura 84

Task ejecutado correctamente para el envío de datos al Proxy - Netskope

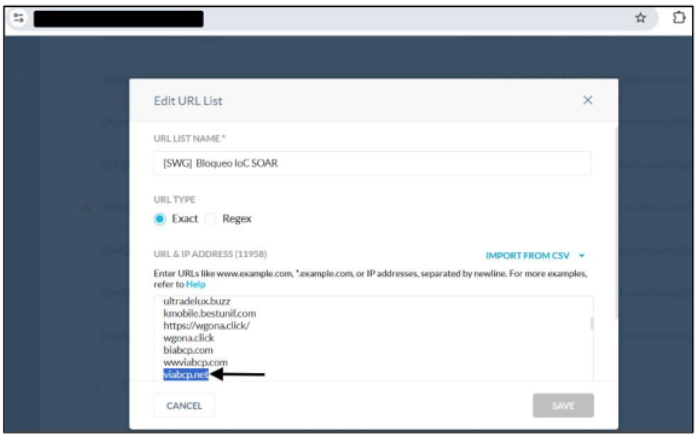


Fuente: Propia

A nivel Proxy - Netskope, se validó que el dominio reportado en el evento fue agregado correctamente a la lista negra mediante la integración con XSOAR, ver Figura 85.

Figura 85

Lista negra de Proxy - Netskope para eventos de XSOAR



Fuente: Propia

Así mismo, se validó a nivel de XSOAR el correcto funcionamiento del playbook para el bloqueo de la IP en el WAF. En la Figura 86 se evidencia el envío correcto de datos al WAF para añadir a su lista negra.

Figura 86

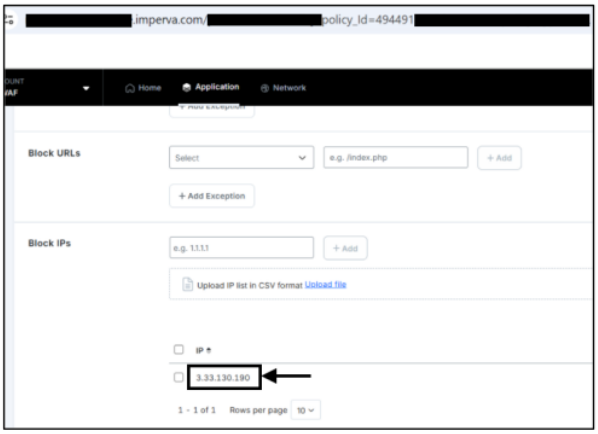
Task ejecutado correctamente para el envío de datos al WAF - Imperva

Fuente: Propia

A nivel WAF - Imperva, se validó que la IP reportada en el evento fue agregado correctamente a la lista negra mediante la integración con XSOAR, ver Figura 87.

Figura 87

Lista negra de WAF - Imperva para eventos de XSOAR

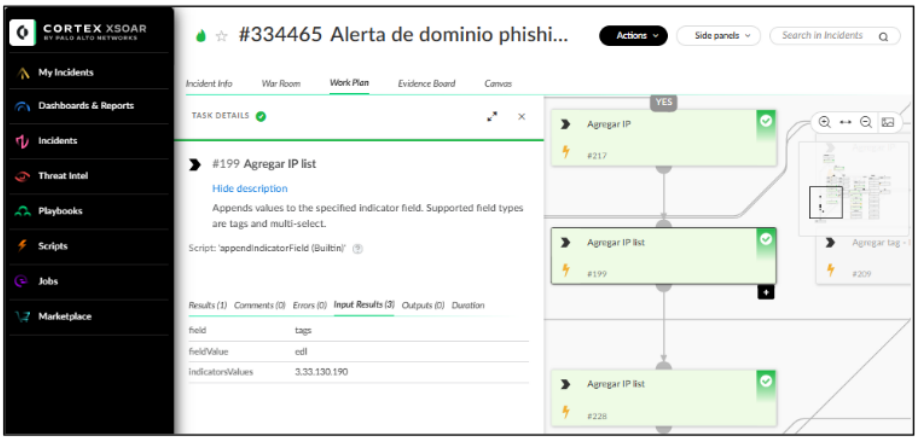


Fuente: Propia

También se validó a nivel de XSOAR el correcto funcionamiento del playbook para el bloqueo de la IP en el Firewall (a través de la EDL). En la Figura 88 se evidencia el envío correcto de datos al WAF para añadir a su lista negra.

Figura 88

Task ejecutado correctamente para el envío de datos al EDL



Fuente: Propia

A nivel de EDL, se validó que la IP reportada en el evento fue agregado correctamente a la lista negra mediante la integración con XSOAR, ver Figura 89. Esta EDL está configurada en el Firewall para que sea consumido cada 5 minutos y pueda agregarse a su política de bloqueo del Firewall.

Figura 89

Lista negra de EDL

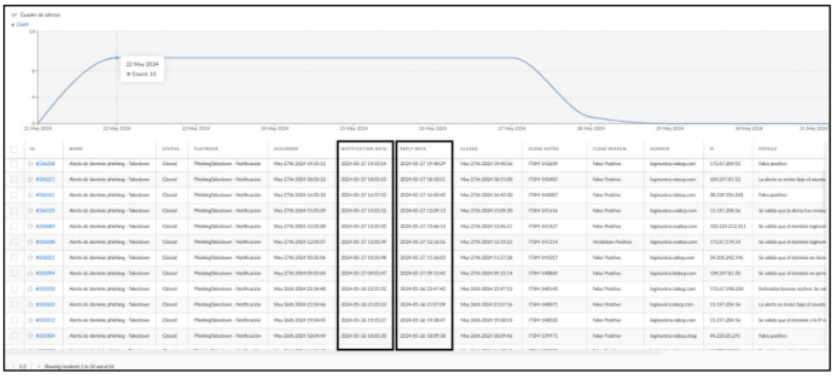
Fuente: Propia

3.2.11.3 Validación de la volumetría de alertas

En base a los lineamientos de la ISO 27001 e ISO 27035 de fomentar mejora continua y buenas prácticas en los procesos de seguridad, los resultados respecto a la volumetría de las alertas fueron los esperados. Se distribuyó el alertamiento a 10 notificaciones por día con un lapso de 90 minutos entre cada alertamiento para que el SOC tenga cobertura de revisar otras alertas entre ese tiempo, ver Figura 90. Para más detalles de los 61 (VP: 14, FP: 47) eventos gatillados en la fase 2, ver Anexo 2.

Figura 90

Volumetría de alertas de dominios similares



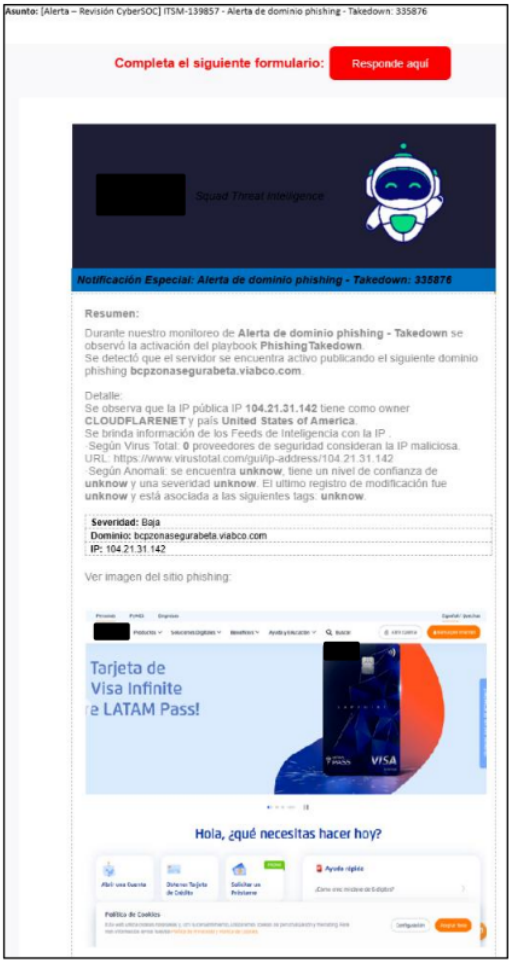
Nota: Esta volumetría optimizó los tiempos de respuesta, dando un promedio de 30 minutos la atención de los eventos de dominios similares. Fuente: Propia

3.2.11.4 Hallazgo identificado

Durante el alertamiento de dominios similares en el mes de mayo, se identificó que el dominio “bcpzonasegurabeta[.]viabco[.]com” e IP “104[.]21[.]31[.]142” cargaba un contenido clonado de la página oficial de la entidad financiera, ver Figura 91. Este evento fue analizado por el SOC y se determinó que no era un dominio legítimo de la entidad financiera. El evento fue catalogado como Phishing (Verdadero Positivo) y reportado al proveedor Hispasec para que procediera con la gestión correspondiente de takedown y con ello reducir el riesgo de fraudes a los usuarios. Así mismo, el dominio e ip fueron bloqueados en las plataformas de seguridad para prevenir futuros ataques hacia la entidad financiera.

Figura 91

Alertamiento de un evento de dominio similar "bcpzonasegurabeta[.]viabco[.]com"



Fuente: Propia

3.2.12 Competencias adquiridas durante formación profesional

Durante mi formación profesional en la Universidad Nacional Tecnológica de Lima Sur cursé asignaturas de gestión empresarial, programación para la ingeniería hasta arquitectura de redes y protocolos, contribuyendo en mi aprendizaje de la carrera profesional Ingeniería Electrónica y Telecomunicaciones. Dichas asignaturas aportaron conocimientos fundamentales para mi formación profesional, ver Tabla 3.

Tabla 3

Asignaturas que aportaron conocimientos fundamentales en mi formación profesional

Curso	Aporte
Liderazgo Personal	Este curso formó las bases para liderar con éxito mi entorno personal y profesional. Ayudándome a conocer mis fortalezas, debilidades, valores y motivaciones esto con el fin de aprender a manejar mis emociones y definir mis objetivos en la implementación de este proyecto.
Liderazgo Estratégico	Este curso me ayudó a desarrollar un pensamiento estratégico en entornos cambiantes tomando decisiones informadas. Además, me ayudó a gestionar recursos y prioridades de manera eficiente, alinear y motivar equipos, fomentando la colaboración hacia los objetivos estratégicos comunes que impulsen el éxito organizacional en mi entorno laboral.
Programación para Ingeniería	Este curso fue fundamental ya que me ayudó a aplicar conceptos de programación para resolver problemas específicos en el ámbito de la ingeniería. Aprendí lenguajes fundamentales de programación como C++ y Python utilizados para crear herramientas de programación que optimizó tareas repetitivas y mejoró la eficiencia de procesos en la entidad financiera.
Arquitectura del Computador	Este curso aportó el entendimiento de los elementos fundamentales de un computador o sistema, como CPU, memoria y dispositivos de entrada/salida. Además, aprendí como interactúan entre hardware y el software y cómo los diseños de hardware afectan la programación y el rendimiento de aplicaciones en un sistema.
Teoría de Redes	Este curso sentó las bases teóricas de Networking para comprender las arquitecturas de redes (LAN, WAN, Internet) y sus componentes, así como el entendimiento de modelos como OSI y TCP/IP, para entender cómo se organiza y opera la comunicación en redes para asegurar una transmisión eficiente y segura.
Transmisión de Datos	Este curso me ayudó a comprender las técnicas y tecnologías que permiten el envío de datos entre dispositivos en redes de comunicación; cómo se aplican los conceptos de señales, modulación, codificación y tipos de medios de transmisión en diferentes entornos de red como Ethernet, Wi-Fi y redes celulares.
Gestión Empresarial	Este curso me ayudo a explorar conceptos de marketing y como impulsar mi trabajo, así como el desarrollo de estrategias para posicionar y promover mi producto o servicio en mi entorno laboral. Estableciendo métricas y herramientas para medir el rendimiento de mi equipo, realizando análisis de costo/tiempo y evaluando la efectividad de mis estrategias implementadas.
Arquitectura de Redes y Protocolos	Este curso aportó en mi formación como profesional a diseñar redes seguras y escalables manteniendo las normas y estándares de seguridad del mercado. Así mismo contribuyó con el análisis de protocolos TCP/IP, UDP, HTTP, DNS, etc, para ser capaz de diagnosticar, solucionar problemas de red dentro de mi entorno laboral.

Nota: Habilidades adquiridas de las asignaturas en mi etapa educativa y como aportaron en mi desarrollo laboral. Fuente: Propia

3.3 Resultados

- Se identificó un proceso existente de gestión de alertas de dominios similares en el Squad de Fraudes y se implementó un proceso similar en el SOC para complementar el monitoreo existente. Para ello se diseñó un proceso de gestión más robusto de acorde a los lineamientos establecidos por la norma ISO 27035 y Framework NIST.

- Se implementó 4 playbooks personalizados, 2 principales y 2 subplaybooks, con la finalidad de optimizar la gestión de alertas de seguridad de dominios similares. Esta optimización tuvo 2 fases de implementación.
  La primera fase fue la implementación de un proceso nuevo dentro de la gestión de alertas del SOC que alineados a la norma ISO 27001, ISO 27035 y Framework NIST identifica, protege, detecta y responde las posibles amenazas hacia la entidad financiera.
  La segunda fase se realizó dentro del marco de mejora continua de la ISO 27001, donde se buscó optimizar la volumetría de las alertas y el automatizado de acciones de contención (bloqueo de indicadores de compromiso) en base a las mejores prácticas establecidas en la entidad financiera, también optimizó los tiempos de atención en un 90% respecto a la fase 1. Esta gestión de alertas tiene un 80% de acciones automatizadas y un 20% de acciones manuales realizadas por el SOC.

- Se validó el alertamiento de eventos de dominios similares en base a la función principal de detección del Framework NIST. Así mismo siguiendo las directrices para la respuesta ante incidentes que indica la ISO 27035 se tomó las mejores prácticas para contener y erradicar amenazas que pueden desencadenar en incidentes de seguridad.
  Se validó el correcto funcionamiento del bloqueo automatizado de indicadores de compromiso del evento de dominios similares. Esta función alineada a la ISO 27035 y el Framework NIST permite responder y prevenir futuros incidentes hacia la entidad financiera. Así mismo, se validó la reducción de tiempos de atención de los eventos de dominios similares respecto a la fase 1 y fase 2 de implementación.

En la segunda fase se validó la reducción de volumetría de eventos diarios de dominios similares, gatillando 10 eventos diarios con rango de tiempo de 90 minutos entre cada evento. Se identificaron 14 dominios e IPs sospechosos donde se realizó la gestión de takedown y fueron bloqueados en las plataformas de seguridad de la entidad financiera.

- Se complementó el monitoreo de dominios similares utilizando recursos existentes de la entidad financiera y herramientas open source, realizando así una implementación de costo cero en adquisición de materiales o herramientas. Se redujo el impacto reputacional y posibles fraudes hacia la entidad financiera, así como posibles multas desde S/.1,946,700 a S/.2,822,200 anuales de Indecopi. Se automatizó la contención de indicadores de compromiso para prevenir futuros ataques de phishing hacia la red interna de la entidad financiera.

CONCLUSIONES

- El diseño de un nuevo proceso en un SOC para complementar un monitoreo existente en la entidad financiera, amplía la cobertura de atención de las alertas de dominios similares debido al horario 24x7 y capacidad de 15 analistas de seguridad que tiene el SOC. El proceso implementado en el SOC es mas robusto debido que cuenta con acciones automatizadas en un 40% mas del proceso original en el área de Fraudes.

- De los resultados se concluye, la implementación de los playbooks personalizados ayudó automatizar el 80% de la gestión de alerta de dominios similares, dejando el 20% como actividad manual de validación para el SOC. La optimización del playbook en la segunda fase redujo tiempos de atención en un 90% respecto a la primera fase, así como la reducción de la volumetría diaria de alertas en un 40%.

- La optimización en la gestión de alertas de dominios similares en el SOC mediante Cortex XSOAR cumple con las normas ISO 27001, ISO 27035 y Framework NIST. Dado que identifica y gestiona la mitigación de riesgos, planifica y prepara una gestión de incidentes, responde de manera eficaz y mantiene la cultura de mejora continua en los procesos de seguridad de la entidad financiera.

RECOMENDACIONES

- De acuerdo a lo presentado en la implementación, se recomienda mantener una mejora continua en un servicio de SOC para optimizar los procesos de gestión de alertas.

- Implementar subplaybooks de procesos de gestión de alertas que automatice la contención de un incidente en múltiples plataformas de seguridad para ser reutilizados en playbooks de procesos nuevos.

- Implementar una estrategia para el monitoreo de clonación de páginas web a través del contenido HTML hasheado para la ampliación de búsqueda en dominios no similares.

REFERENCIAS BIBLIOGRÁFICAS

Cisneros, P. (2022). Implementación de un centro de operaciones de ciberseguridad (SOC) para mejorar la detección de ataques cibernéticos en empresas del sector tecnológico, Lima-2022. Obtenido de http://repositorio.ulasamericas.edu.pe/handle/upa/1990

Cloudflare. (2024). ¿Qué es ciberseguridad? Obtenido de https://www.cloudflare.com/es-es/learning/security/what-is-cyber-security/

El Peruano. (2021). DECRETO SUPREMO Nº 032-2021-PCM. Obtenido de https://cdn.www.gob.pe/uploads/document/file/1692068/DECRETO%20SUPREMO%20N%C2%BA%20032-2021-PCM.pdf.pdf?v=1614268947

Forsberg, J., & Frantti, T. (2023). Technical performance metrics of a security operations center. Computers & Security, 135(103529), 0167-4048. Obtenido de https://doi.org/10.1016/j.cose.2023.103529

Fortinet. (2024). Cumplimiento del NIST. Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/nist-compliance

Hurtado, C. (2021). Diseño de un sistema de gestión para mejorar el servicio de atención en la plataforma de seguridad de la información de la empresa SISCOTEC del Perú S.A.C. Obtenido de https://repositorio.uss.edu.pe//handle/20.500.12802/7894

IBM. (2024). ¿Qué es el software de código abierto? Obtenido de https://www.ibm.com/mx-es/topics/open-source#:~:text=El%20software%20de%20c%C3%B3digo%20abierto%20es%20software%20desarrollado,lo%20use%2C%20examine%2C%20altere%20y%20redistribuya%20como%20quiera.¿Qué es el software de código abierto?

IBM. (2024). ¿Qué es un centro de operaciones de seguridad (SOC)? Obtenido de https://www.ibm.com/es-es/topics/security-operations-center

Incentro. (2022). ¿Qué es on premise y en qué se diferencia del cloud? Obtenido de https://www.incentro.com/es-ES/blog/que-es-on-premise-y-en-que-se-diferencia-del-cloud

Incibe. (2020). ¿Qué son y para qué sirven los SIEM, IDS e IPS? Obtenido de https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

Indecopi. (2023). El Indecopi impuso más de mil sanciones a bancos y financieras por operaciones no reconocidas por sus usuarios. Obtenido de https://www.gob.pe/institucion/indecopi/noticias/825526-el-indecopi-

impuso-mas-de-mil-sanciones-a-bancos-y-financieras-por-operaciones-no-reconocidas-por-sus-usuarios

ISO. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO. (2023). ISO/IEC 27035-1:2023 Information technology — Information security incident management. Obtenido de https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27035:-1:ed-2:v1:en

Kaspersky. (2024). ¿Qué es la inteligencia de amenazas? Definición y explicación. Obtenido de https://latam.kaspersky.com/resource-center/definitions/threat-intelligence

Microsoft. (2024). ¿Qué es la detección y respuesta de puntos de conexión (EDR)? Obtenido de https://www.microsoft.com/es-es/security/business/security-101/what-is-edr-endpoint-detection-response?msockid=301b99e9cb4c6fa627348d05caa16e88

NIST. (26 de Febrero de 2024). El Marco de Seguridad Cibernética (CSF) 2.0 del NIST. 29, 16. Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

NormasISO. (2024). Norma ISO 27001. Obtenido de https://normasiso.org/norma-iso-27001/

Palo Alto Networks. (2020). Cortex XSOAR Administración de casos. Obtenido de https://www.paloaltonetworks.lat/apps/pan/public/downloadResource?pagePath=/content/pan/es_LA/resources/datasheets/cortex-xsoar-case-management

Palo Alto Networks. (2020). Orquestación de seguridad, automatización y respuestas alojadas. Obtenido de https://www.paloaltonetworks.lat/apps/pan/public/downloadResource?pagePath=/content/pan/es_LA/resources/datasheets/cortex-xsoar-hosted-solution

Palo Alto Networks. (2020). Redefinición de la orquestación de seguridad y automatización. Obtenido de https://www.paloaltonetworks.lat/apps/pan/public/downloadResource?pagePath=/content/pan/es_LA/resources/datasheets/cortex-xsoar-overview

Palo Alto Networks. (2020). The State of SOAR Report, 2020. Obtenido de https://media.bitpipe.com/io_15x/io_154375/item_2268964/the-state-of-soar-report-2020.pdf

Palo Alto Networks. (Julio de 2022). Palo Alto Networks Certified Security Automation Engineer (PCSAE) Study Guide. Obtenido de https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcsae-study-guide.pdf

Palo Alto Networks. (2024). Cortex XSOAR for Managed Security Service Providers. Obtenido de https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-xsoar-for-mssps

Tenacy. (2024). ISO 27035. Obtenido de https://www.tenacy.io/es/resources/iso-27035/

Tilbury, J., & Flowerday, S. (2024). Humans and Automation: Augmenting Security Operation Centers. Cybersecurity and Privacy, 4(3), 388-409. Obtenido de https://doi.org/10.3390/jcp4030020

Vasquez, W. (2023). Implementación de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera. Obtenido de https://cybertesis.unmsm.edu.pe/backend/api/core/bitstreams/7e3bac47-f219-4c12-94fc-5dab1667120d/content

Xataca. (2020). Parches de seguridad de Windows: qué son y cómo instalarlos. Obtenido de https://www.xataka.com/basics/parches-seguridad-windows-que-como-instalarlos

Zafra, L. (2022). Los seis desafíos clave de un SOC que pueden provocar un 'daltonismo de seguridad'. Obtenido de https://es.linkedin.com/pulse/los-seis-desaf%C3%ADos-clave-de-un-soc-que-pueden-provocar-zafra-labrador-ggclc

ANEXOS

Anexo 1. Detalles de eventos gatillados en la fase 1 de implementación

ID	Playbook ID	Notification Date	Reply Date	Close Notes	Close Reason	Domain
310862	PhishingTakedown - Notificación	2/04/2024 09:14	9/04/2024 11:32	ITSM-83383	Verdadero Positivo	bcpzonasegurabeta.viabvp.com
310860	PhishingTakedown - Notificación	2/04/2024 09:12	9/04/2024 10:59	ITSM-83343	Verdadero Positivo	bcpzonasegurabeta.vizbcp.com
310859	PhishingTakedown - Notificación	2/04/2024 09:11	9/04/2024 10:58	ITSM-83342	Verdadero Positivo	bcpzonasegurabeta.voabcp.com
310855	PhishingTakedown - Notificación	2/04/2024 09:09	9/04/2024 11:00	ITSM-83344	Verdadero Positivo	bcpzonasegurabeta.viabcp.top
310852	PhishingTakedown - Notificación	2/04/2024 09:08	9/04/2024 11:01	ITSM-83347	Verdadero Positivo	vizbcp.com
310849	PhishingTakedown - Notificación	2/04/2024 09:06	9/04/2024 11:01	ITSM-83348	Verdadero Positivo	viqbcp.com
310848	PhishingTakedown - Notificación	2/04/2024 09:05	9/04/2024 11:00	ITSM-83346	Verdadero Positivo	viabcp.top
310415	PhishingTakedown - Notificación	1/04/2024 09:43	9/04/2024 10:57	INC000003971878	Verdadero Positivo	loginunico.viabcpc.com
310412	PhishingTakedown - Notificación	1/04/2024 09:41	9/04/2024 10:56	INC000003971877	Verdadero Positivo	loginunico.viavcp.com
310409	PhishingTakedown - Notificación	1/04/2024 09:40	9/04/2024 10:55	INC000003971876	Verdadero Positivo	loginunico.v.iabcp.com
310404	PhishingTakedown - Notificación	1/04/2024 09:38	9/04/2024 10:55	INC000003971875	Verdadero Positivo	loginunico.biabcp.com
310401	PhishingTakedown - Notificación	1/04/2024 09:37	9/04/2024 10:54	INC000003971874	Verdadero Positivo	loginunico.iabcp.com
310399	PhishingTakedown - Notificación	1/04/2024 09:35	9/04/2024 10:53	INC000003971873	Verdadero Positivo	loginunicov.iabcp.com
310394	PhishingTakedown - Notificación	1/04/2024 09:34	9/04/2024 04:09	INC000003971561	Verdadero Positivo	loginunico.viabcp.co
310389	PhishingTakedown - Notificación	1/04/2024 09:32	9/04/2024 04:06	INC000003971559	Verdadero Positivo	bcpzonasegurabeta.viabcpc.com
310386	PhishingTakedown - Notificación	1/04/2024 09:31	9/04/2024 04:02	INC000003971558	Verdadero Positivo	bcpzonasegurabeta.viavcp.com
310382	PhishingTakedown - Notificación	1/04/2024 09:29	9/04/2024 03:59	INC000003971557	Verdadero Positivo	bcpzonasegurabeta.v.iabcp.com
310381	PhishingTakedown - Notificación	1/04/2024 09:28	9/04/2024 03:56		Falso Positivo	bcpzonasegurabeta.biabcp.com
310375	PhishingTakedown - Notificación	1/04/2024 09:26	9/04/2024 03:53		Falso Positivo	bcpzonasegurabeta.iabcp.com
310371	PhishingTakedown - Notificación	1/04/2024 09:24	2/04/2024 06:14		Falso Positivo	bcpzonasegurabetav.iabcp.com
310370	PhishingTakedown - Notificación	1/04/2024 09:23	1/04/2024 17:57	INC000003963451	Verdadero Positivo	bcpzonasegurabeta.viabcp.co
310368	PhishingTakedown - Notificación	1/04/2024 09:21	1/04/2024 17:26	INC000003963432	Verdadero Positivo	viabcpc.com
310365	PhishingTakedown - Notificación	1/04/2024 09:20	1/04/2024 21:29	INC000003963840	Verdadero Positivo	viabbp.com

310363	PhishingTakedown - Notificación	1/04/2024 09:18	1/04/2024 21:16	INC000003963831	Verdadero Positivo	viavcp.com
310359	PhishingTakedown - Notificación	1/04/2024 09:17	1/04/2024 16:13	INC000003963291	Verdadero Positivo	v.iabcp.com
310352	PhishingTakedown - Notificación	1/04/2024 09:15	1/04/2024 21:27	INC000003963838	Verdadero Positivo	viabcp.ru
310350	PhishingTakedown - Notificación	1/04/2024 09:14	1/04/2024 20:57	INC000003963800	Verdadero Positivo	viabcp.co
310348	PhishingTakedown - Notificación	1/04/2024 09:12	1/04/2024 13:30	INC000003963057	Verdadero Positivo	viabcp.org
310346	PhishingTakedown - Notificación	1/04/2024 09:11	8/04/2024 18:09	INC000003970990	Verdadero Positivo	viabcp.net
310344	PhishingTakedown - Notificación	1/04/2024 09:09	1/04/2024 12:28	INC000003963007	Verdadero Positivo	wwwviabcp.com
310339	PhishingTakedown - Notificación	1/04/2024 09:08	1/04/2024 11:21	INC000003962840	Verdadero Positivo	wwviabcp.com
310335	PhishingTakedown - Notificación	1/04/2024 09:06	1/04/2024 11:05	INC000003962828	Verdadero Positivo	biabcp.com
310333	PhishingTakedown - Notificación	1/04/2024 09:05	1/04/2024 09:56	INC000003962630	Verdadero Positivo	iabcp.com

Anexo 2. Detalles de eventos gatillados en la fase 2 de implementación

ID	Playbook ID	Notification Date	Reply Date	Close Notes	Close Reason	Domain
336394	PhishingTakedown - Notificación	28/05/2024 09:05	28/05/2024 09:13	ITSM-143242	Falso Positivo	loginunico.vialbcp.com
336288	PhishingTakedown - Notificación	27/05/2024 22:35	27/05/2024 23:31	ITSM-142812	Verdadero Positivo	loginunico.viabc.com
336269	PhishingTakedown - Notificación	27/05/2024 21:05	27/05/2024 21:13	ITSM-142676	Falso Positivo	loginunico.viabcpc.com
336258	PhishingTakedown - Notificación	27/05/2024 19:35	27/05/2024 19:40	ITSM-142609	Falso Positivo	loginunico.viabxp.com
336211	PhishingTakedown - Notificación	27/05/2024 18:05	27/05/2024 18:10	ITSM-142487	Falso Positivo	loginunico.viavcp.com
336161	PhishingTakedown - Notificación	27/05/2024 16:37	27/05/2024 16:43	ITSM-142007	Falso Positivo	loginunico.visbcp.com
336125	PhishingTakedown - Notificación	27/05/2024 15:05	27/05/2024 15:09	ITSM-141616	Falso Positivo	loginunico.v.iabcp.com
336083	PhishingTakedown - Notificación	27/05/2024 13:35	27/05/2024 13:46	ITSM-141427	Falso Positivo	loginunico.vuabcp.com
336048	PhishingTakedown - Notificación	27/05/2024 12:05	27/05/2024 12:16	ITSM-141214	Verdadero Positivo	loginunico.voabcp.com
336021	PhishingTakedown - Notificación	27/05/2024 10:35	27/05/2024 11:36	ITSM-141017	Falso Positivo	loginunico.vabcp.com
335994	PhishingTakedown - Notificación	27/05/2024 09:05	27/05/2024 09:13	ITSM-140860	Falso Positivo	loginunico.biabcp.com
335933	PhishingTakedown - Notificación	26/05/2024 22:35	26/05/2024 23:47	ITSM-140143	Falso Positivo	loginunico.ciabcp.com
335922	PhishingTakedown - Notificación	26/05/2024 21:05	26/05/2024 21:07	ITSM-140071	Falso Positivo	loginunico.iabcp.com
335912	PhishingTakedown - Notificación	26/05/2024 19:35	26/05/2024 19:38	ITSM-140020	Falso Positivo	loginunicov.iabcp.com
335904	PhishingTakedown - Notificación	26/05/2024 18:05	26/05/2024 18:09	ITSM-139971	Falso Positivo	loginunico.viabcp.shop
335895	PhishingTakedown - Notificación	26/05/2024 16:35	26/05/2024 16:47	ITSM-139935	Falso Positivo	loginunico.viabcp.top
335886	PhishingTakedown - Notificación	26/05/2024 15:05	26/05/2024 15:08	ITSM-139885	Falso Positivo	loginunico.viabcp.co
335876	PhishingTakedown - Notificación	26/05/2024 13:35	26/05/2024 13:57	ITSM-139857	Verdadero Positivo	bcpzonasegurabeta.viabco.com
335862	PhishingTakedown - Notificación	26/05/2024 12:05	26/05/2024 12:11	ITSM-139824	Falso Positivo	bcpzonasegurabeta.viabc.com
335850	PhishingTakedown - Notificación	26/05/2024 10:35	26/05/2024 10:43	ITSM-139781	Falso Positivo	bcpzonasegurabeta.viabcpc.com
335832	PhishingTakedown - Notificación	26/05/2024 09:05	26/05/2024 09:12	ITSM-139743	Falso Positivo	bcpzonasegurabeta.viabxp.com
335759	PhishingTakedown - Notificación	25/05/2024 22:35	25/05/2024 22:39	ITSM-139370	Falso Positivo	bcpzonasegurabeta.viavcp.com
335746	PhishingTakedown - Notificación	25/05/2024 21:05	25/05/2024 21:16	ITSM-139175	Falso Positivo	bcpzonasegurabeta.vialbcp.com
335735	PhishingTakedown - Notificación	25/05/2024 19:36	25/05/2024 19:51	ITSM-139104	Falso Positivo	bcpzonasegurabeta.visbcp.com
335718	PhishingTakedown - Notificación	25/05/2024 18:05	25/05/2024 18:36	ITSM-139048	Falso Positivo	bcpzonasegurabeta.v.iabcp.com
335699	PhishingTakedown - Notificación	25/05/2024 16:35	25/05/2024 17:07	ITSM-139017	Falso Positivo	bcpzonasegurabeta.vuabcp.com

335683	PhishingTakedown - Notificación	25/05/2024 15:05	25/05/2024 16:05	ITSM-138965	Verdadero Positivo	bcpzonasegurabeta.voabcp.com
335666	PhishingTakedown - Notificación	25/05/2024 13:35	25/05/2024 14:51	ITSM-138929	Falso Positivo	bcpzonasegurabeta.vabcp.com
335647	PhishingTakedown - Notificación	25/05/2024 12:05	25/05/2024 14:45	ITSM-138873	Falso Positivo	bcpzonasegurabeta.biabcp.com
335632	PhishingTakedown - Notificación	25/05/2024 10:35	25/05/2024 11:45	ITSM-138822	Verdadero Positivo	bcpzonasegurabeta.ciabcp.com
335618	PhishingTakedown - Notificación	25/05/2024 09:05	25/05/2024 09:52	ITSM-138772	Falso Positivo	bcpzonasegurabeta.iabcp.com
335511	PhishingTakedown - Notificación	24/05/2024 22:36	24/05/2024 23:01	ITSM-138179	Falso Positivo	bcpzonasegurabetav.iabcp.com
335502	PhishingTakedown - Notificación	24/05/2024 21:06	24/05/2024 21:24	ITSM-138119	Falso Positivo	bcpzonasegurabeta.viabcp.shop
335492	PhishingTakedown - Notificación	24/05/2024 19:36	24/05/2024 19:52	ITSM-138046	Falso Positivo	bcpzonasegurabeta.viabcp.top
335479	PhishingTakedown - Notificación	24/05/2024 18:06	24/05/2024 18:17	ITSM-137915	Falso Positivo	bcpzonasegurabeta.viabcp.co
335441	PhishingTakedown - Notificación	24/05/2024 16:36	24/05/2024 17:03	ITSM-137722	Falso Positivo	viabco.com
335400	PhishingTakedown - Notificación	24/05/2024 15:06	24/05/2024 15:11	ITSM-137197	Falso Positivo	viabc.com
335368	PhishingTakedown - Notificación	24/05/2024 13:36	24/05/2024 14:39	ITSM-137067	Falso Positivo	viabcpe.com
335333	PhishingTakedown - Notificación	24/05/2024 12:06	24/05/2024 12:43	ITSM-136933	Falso Positivo	viabcpc.com
335284	PhishingTakedown - Notificación	24/05/2024 10:36	24/05/2024 10:43	ITSM-136770	Falso Positivo	viabxp.com
335244	PhishingTakedown - Notificación	24/05/2024 09:06	24/05/2024 09:45	ITSM-136558	Falso Positivo	viabbp.com
335060	PhishingTakedown - Notificación	23/05/2024 22:35	23/05/2024 22:40	ITSM-136010	Falso Positivo	viavcp.com
335032	PhishingTakedown - Notificación	23/05/2024 21:05	23/05/2024 22:03	ITSM-135943	Verdadero Positivo	viacp.com
335008	PhishingTakedown - Notificación	23/05/2024 19:35	23/05/2024 21:01	ITSM-135873	Verdadero Positivo	vialbcp.com
334983	PhishingTakedown - Notificación	23/05/2024 18:05	23/05/2024 20:29	ITSM-135766	Verdadero Positivo	visbcp.com
334930	PhishingTakedown - Notificación	23/05/2024 16:35	23/05/2024 17:20	ITSM-135603	Falso Positivo	v.iabcp.com
334877	PhishingTakedown - Notificación	23/05/2024 15:05	23/05/2024 17:07	ITSM-135474	Verdadero Positivo	vuabcp.com
334824	PhishingTakedown - Notificación	23/05/2024 13:35	23/05/2024 13:55	ITSM-135338	Falso Positivo	voabcp.com
334769	PhishingTakedown - Notificación	23/05/2024 12:05	23/05/2024 12:20	ITSM-135145	Falso Positivo	vabcp.com
334710	PhishingTakedown - Notificación	23/05/2024 10:35	23/05/2024 10:54	ITSM-134950	Falso Positivo	viabcp.shop
334625	PhishingTakedown - Notificación	23/05/2024 09:05	23/05/2024 09:14	ITSM-134795	Falso Positivo	viabcp.online
334546	PhishingTakedown - Notificación	22/05/2024 23:49	22/05/2024 23:54	ITSM-134338	Falso Positivo	viabcp.top
334533	PhishingTakedown - Notificación	22/05/2024 22:19	22/05/2024 22:32	ITSM-134215	Falso Positivo	viabcp.ru
334524	PhishingTakedown - Notificación	22/05/2024 20:49	22/05/2024 21:49	ITSM-134095	Verdadero Positivo	viabcp.co
334505	PhishingTakedown - Notificación	22/05/2024 23:47	22/05/2024 23:52	ITSM-134336	Falso Positivo	viabcp.org
334465	PhishingTakedown - Notificación	22/05/2024 17:49	22/05/2024 18:53	ITSM-133766	Verdadero Positivo	viabcp.net

334414	PhishingTakedown - Notificación	22/05/2024 16:19	22/05/2024 18:53	ITSM-133358	Verdadero Positivo	wwwviabcp.com
334353	PhishingTakedown - Notificación	22/05/2024 14:49	22/05/2024 15:59	ITSM-132785	Verdadero Positivo	wwviabcp.com
334303	PhishingTakedown - Notificación	22/05/2024 13:19	22/05/2024 13:28	ITSM-132576	Verdadero Positivo	biabcp.com
334222	PhishingTakedown - Notificación	22/05/2024 11:49	22/05/2024 12:37	ITSM-132254	Falso Positivo	ciabcp.com
334169	PhishingTakedown - Notificación	22/05/2024 10:19	22/05/2024 10:28	ITSM-131418	Falso Positivo	iabcp.com

Anexo 3. Autorización de proyecto

NEOSECURE SAC
Av. del Pinar Nro. 152 Int. 1101, Surco, Lima, Perú
info@sek.io

Lima, 22 de Noviembre de 2024

Señores

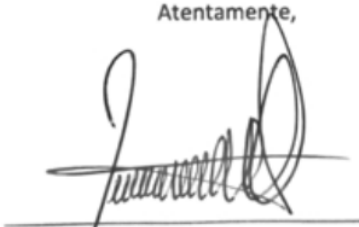
UNIVERSIDAD NACIONAL TECNOLOGICA DE LIMA SUR - UNTELS

Presente.

De mi consideración:

Es grato dirigirme a ustedes en mi calidad de **Service Manager** identificado con DNI N° 46191638 o / Carnet de Extranjería de la empresa o institución, para comunicar que el Señor **Juan de Dios Antayhua de la Cruz** identificado con DNI N° **75132733**, ha desempeñado el cargo **Gestor de SIEM y SOAR**, por ello otorgamos la autorización de presentar y desarrollar el proyecto de suficiencia profesional titulado: **"OPTIMIZACIÓN EN LA GESTIÓN DE ALERTAS MEDIANTE CORTEX XSOAR EN UN CENTRO DE OPERACION DE SEGURIDAD (SOC) PARA UNA ENTIDAD FINANCIERA - 2024"** en el VII Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional 2024 de su institución.

Atentamente,



Firma y sello del Representante Legal
o Cargo que desempeña
N° DNI: 46191638
N° COLEGIATURA: 349782

ANTAYHUA DE LA CRUZ JUAN DE DIOS

INFORME DE ORIGINALIDAD

5%	%	%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
2	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
3	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	1%
4	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	1%
5	Submitted to Universidad Tecnológica Centroamericana UNITEC Trabajo del estudiante	<1%
6	Submitted to Universidad San Marcos Trabajo del estudiante	<1%
7	Submitted to Universidad del Istmo de Panamá Trabajo del estudiante	<1%

8	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	<1 %
9	Submitted to Instituto Tecnologico de Costa Rica Trabajo del estudiante	<1 %
10	Submitted to Universidad Americana Trabajo del estudiante	<1 %
11	Submitted to Universidad Abierta para Adultos Trabajo del estudiante	<1 %
12	Submitted to Universidad Continental Trabajo del estudiante	<1 %
13	Submitted to Corporación Universitaria Minuto de Dios,UNIMINUTO Trabajo del estudiante	<1 %
14	Submitted to Universidad Católica Boliviana "San Pablo" Trabajo del estudiante	<1 %
15	Submitted to Universidad TecMilenio Trabajo del estudiante	<1 %
16	Submitted to ITESM: Instituto Tecnologico y de Estudios Superiores de Monterrey Trabajo del estudiante	<1 %
17	Submitted to Universidad Argentina John F. Kennedy	<1 %

Trabajo del estudiante

18	Submitted to Universidad Dr. José Matías Delgado Trabajo del estudiante	<1 %
19	Submitted to Universidad Nacional de Trujillo Trabajo del estudiante	<1 %
20	Submitted to ulacit Trabajo del estudiante	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 12 words
Excluir bibliografía	Activo		