REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

"AUTOMATIZACIÓN DE UN PLAYBOOK DE PHISHING PARA MEJORAR LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA EMPRESA "AUDETIC" CONSIDERANDO LA NIST SP 800- 61".

Trabajo de Investigación previo a la obtención del Título de Magister en Computación con mención en Seguridad de la Información.

AUTOR:

Ing. Verónica Lizeth Guamán Guamán

DIRECTOR:

Msc. Jaime Gabriel Llumiquinga Veintimilla.

Ibarra, junio 2024.

UNIVERSIDAD TÉCNICA DEL NORTE

DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100355729-3		
APELLIDOS Y NOMBRES:	Guamán Guamán Verónica Lizeth		
DIRECCIÓN:	Ibarra, Caranqui calle Duchicela 5-20		
EMAIL:	vlguamang@utn.edu.ec		
TELÉFONO FIJO:	062 652 035	**TELÉFONO MÓVIL:**	093 938 0652

DATOS DE LA OBRA	
TÍTULO:	Automatización de un playbook de phishing para mejorar la gestión de incidentes de seguridad en la empresa "AUDETIC" considerando la NIST SP 800- 61.
AUTOR (ES):	Verónica Lizeth Guamán Guamán
FECHA: DD/MM/AAAA	18/06/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	**( ) PREGRADO (x) POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática
DIRECTOR/ASESOR	Msc. Gabriel Llumiquinga, Msc. Daisy Imbaquingo

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 18 días del mes de junio de 2024.

EL AUTOR:

VERONICA LIZETH GUAMAN GUAMAN

Firmado digitalmente por VERONICA LIZETH GUAMAN GUAMAN
Fecha: 2024.06.18 15:20:48 -05'00'

(Firma)……

Nombre: Verónica Lizeth Guamán Guamán

APROBACIÓN DEL TUTOR

Yo Msc. Jaime Gabriel Llumiquinga Veintimilla, en calidad de director de la tesis titulada: “AUTOMATIZACIÓN DE UN PLAYBOOK DE PHISHING PARA MEJORAR LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA EMPRESA “AUDETIC” CONSIDERANDO LA NIST SP 800-61” de la autoría de la Ing. Verónica Lizeth Guamán Guamán, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 18 días del mes de junio del 2024.

Lo certifico

JAIME GABRIEL LLUMIQUINGA VEINTIMILLA

Firmado digitalmente por JAIME GABRIEL LLUMIQUINGA VEINTIMILLA
Fecha: 2024.06.18 14:26:45 -05'00'

MSc. Jaime Gabriel Llumiquinga Veintimilla

DIRECTOR DE TESIS

DEDICATORIA

"Es importante celebrar el éxito, pero es más importante aprender bien de los fracasos."

Bill Gates

Dedico este proyecto de tesis a mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Es por ello que soy lo que soy ahora. Los amo con mi vida. A mis hermanos, por sus palabras, el apoyo incondicional y compañía que me han ayudado y llevado hasta donde estoy ahora. También dedico este trabajo a quienes con su conocimiento colaboraron con la ejecución de este trabajo.

Verónica Lizeth

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a mis padres, quienes son mi pilar fundamental, brindándome un apoyo incondicional en la consecución de mis metas personales y académicas. Su amor y aliento constante es la fuerza que me impulsa a perseverar incluso en los momentos más desafiantes.

Así también, agradecer a mi director, Msc. Gabriel Llumiquinga, y a mi asesora de tesis, Msc. Daysi Imbaquingo, cuya invaluable experiencia y orientación fueron esenciales en la investigación y desarrollo de este proyecto.

A todas las personas que han influido de manera positiva en mi vida, les extiendo mi más sincero agradecimiento. Cada gesto de apoyo y cada palabra de aliento han sido un motor para alcanzar este logro. Sus pequeñas acciones marcaron una gran diferencia en mi camino hacia el éxito académico.

Gracias a todos por su contribución y respaldo, su influencia ha sido fundamental en mi camino hacia la culminación de este importante objetivo.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

"AUTOMATIZACIÓN DE UN PLAYBOOK DE PHISHING PARA MEJORAR LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA EMPRESA "AUDETIC" CONSIDERANDO LA NIST SP 800- 61".

Autor: Verónica Lizeth Guamán Guamán
Tutor: Jaime Gabriel Llumiquinga V.
Año: 2024

RESUMEN

El estudio examina cómo gestionar eficientemente los incidentes de phishing en "Audetic" mediante la implementación de un playbook automatizado basado en las directrices del NIST SP 800-61. El objetivo principal fue mejorar la respuesta a estos incidentes a través de la automatización del playbook. La metodología adoptada incluyó el análisis de las prácticas vigentes, la elección y caracterización de herramientas de código abierto para la automatización, la implementación del sistema y su evaluación posterior. Aunque se observaron resultados positivos, como la reducción del tiempo de respuesta promedio de 30 a 15 minutos y un aumento en la precisión de la detección de vulnerabilidades, se encontraron limitaciones relacionadas con la integración y compatibilidad de algunos softwares de código abierto, lo que requirió ajustes adicionales para su funcionamiento óptimo. Las conclusiones resaltan la efectividad del enfoque del NIST SP 800-61 en la mejora de la gestión de incidentes y también subrayan la importancia de considerar la adaptabilidad y el soporte continuo de las herramientas de código abierto utilizadas en contextos empresariales.

Palabras clave: Phishing; Automatización; Ciberseguridad; NIST SP 800-61; Gestión de incidentes.

ABSTRACT

The study examines how to efficiently manage phishing incidents at "Audetic" through the implementation of an automated playbook based on the guidelines of NIST SP 800-61. The main objective was to improve the response to these incidents via playbook automation. The methodology employed included analyzing current practices, selecting and characterizing open-source tools for automation, implementing the system, and conducting a subsequent evaluation. Positive results were observed, such as a reduction in average response time from 30 to 15 minutes and an increase in the accuracy of vulnerability detection. However, limitations related to the integration and compatibility of some open-source software were identified, necessitating additional adjustments for optimal operation. The conclusions underscore the effectiveness of the NIST SP 800-61 approach in enhancing incident management and also highlight the importance of considering the adaptability and continuous support of the open-source tools used in corporate settings.

Keywords: Phishing; Automation; Cybersecurity; NIST SP 800-61; Incident Management.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actual era digital, la seguridad de la información se ha convertido en un pilar fundamental para la protección de los activos organizacionales. Ante la creciente sofisticación y diversidad de las amenazas cibernéticas, las empresas como Audetic deben adoptar estrategias robustas para responder de manera efectiva a incidentes de seguridad. La automatización de los playbooks de gestión de incidentes de seguridad, con un enfoque particular en ataques de phishing, emerge como una herramienta invaluable para incrementar notablemente la eficacia y eficiencia de las respuestas a incidentes en la empresa. Aplicando el marco establecido por NIST SP 800-61, se han desarrollado e implementado soluciones automatizadas que satisfacen las necesidades de seguridad actuales y ofrecen una base escalable para futuras adaptaciones.

El estudio se centra en la caracterización y utilización de herramientas de código abierto, facilitando una integración efectiva y una gestión de incidentes más ágil y precisa. Se hace hincapié en la creación y aplicación de un playbook automatizado, diseñado específicamente para abordar incidentes de phishing, que son considerados entre los ataques más comunes y dañinos. Este enfoque no solo mejora la eficiencia en la respuesta a incidentes, sino que también refuerza las medidas de seguridad frente a estas amenazas cibernéticas frecuentes. Mediante este enfoque, se exploran los beneficios tangibles de automatizar la respuesta a incidentes, desde la reducción de los tiempos de respuesta hasta la mejora de la precisión, la disminución de errores humanos en la detección y mitigación de ataques.

Finalmente, se evalúa la efectividad y eficiencia de las soluciones implementadas, ofreciendo un análisis detallado que no solo confirma la efectividad de las herramientas y estrategias empleadas, sino que también recomienda mejoras continuas y adaptaciones ante las evoluciones en el panorama de amenazas. Este informe destaca la relevancia crucial de la innovación tecnológica en la seguridad cibernética y sienta las bases para investigaciones y

desarrollos futuros en el ámbito de la automatización de la seguridad informática. Con este enfoque, se busca no solo avanzar en las prácticas actuales, sino también inspirar nuevos estudios y aplicaciones en este campo vital.

CAPÍTULO I

1. El PROBLEMA

1.1. Problema de investigación

El phishing es un tipo de ciberdelito que se ha convertido en una amenaza común en todo el mundo, incluido Ecuador. En Ecuador, el ámbito empresarial ha enfrentado una creciente ola de ataques de phishing, los cuales han evolucionado en complejidad y dificultad de detección a lo largo del tiempo. Estos ataques están dirigidos a adquirir datos sensibles, incluyendo claves, números de tarjetas de crédito y otros detalles financieros. Los ciberdelincuentes emplean tácticas de ingeniería social para manipular a los empleados, haciéndoles pensar que están comunicándose con una entidad confiable (Koddebusch, 2022).

A pesar de los esfuerzos de las empresas por protegerse contra el phishing, los ataques siguen siendo una amenaza constante. Los ciberdelincuentes están utilizando técnicas más avanzadas, como el spear phishing, que se dirige a personas concretas en lugar de enviar correos electrónicos masivos (Ramesh et al., 2023). Para protegerse de estos ataques, las empresas deben formar a sus empleados y aplicar medidas de seguridad eficaces.

Según un análisis detallado sobre las respuestas a incidentes de ciberseguridad en el sector financiero de Ecuador, el phishing constituyó el 21% de los eventos reportados en 2018 (Catota, Granger Morgan, et al., 2018). Estos ataques de phishing, un método frecuentemente empleado en ciberataques, implican el uso de engaños para persuadir a las personas de revelar información delicada. Dicha información incluye credenciales de acceso y datos financieros, a menudo mediante correos electrónicos o páginas web simuladas. En 2016, el Banco del Austro (BDA) perdió $ 12 millones a través de un ataque de phishing contra el sistema de pago SWIFT. El ataque ocurrió en enero de 2015 y fue revelado a través de una demanda presentada por BDA contra Wells Fargo (Trend Micro Incorporated, 2023). Los piratas informáticos utilizaron las credenciales de SWIFT de un empleado del banco para secuestrar el sistema y transferir los

fondos a bancos en Hong Kong, Dubai y Nueva York (securityaffairs, 2023). El caso planteó preguntas sobre la supervisión de la red SWIFT y sus comunicaciones con los bancos miembros sobre los robos cibernéticos y los riesgos (Bergin & Layne, 2016).

En 2021, Banco Pichincha y el Ministerio de Finanzas de Ecuador fueron pirateados a través de correos electrónicos de phishing, que se utilizaron para obtener información confidencial de los clientes (Bleeping Computer, 2023). El ataque al Banco Pichincha fue un ataque de ransomware que interrumpió el acceso de los clientes a los servicios bancarios, incluidas sus herramientas de aplicaciones móviles y en línea (Abrams, 2021). En una declaración oficial, el banco confirmó que había sufrido un ataque cibernético. Según la entidad, los agresores se aprovecharon de la plataforma comprometida para distribuir correos electrónicos de phishing a sus clientes. El propósito de estos correos era engañar a los destinatarios para obtener información confidencial, con el fin de realizar transacciones no autorizadas (Abrams, 2021).

El phishing se ha convertido en una amenaza cada vez más significativa para organizaciones de todos las dimensiones y sectores. Actualmente, estos ataques han evolucionado hacia formas más sofisticadas y son particularmente difíciles de identificar para aquellos usuarios que no poseen un conocimiento adecuado sobre los riesgos asociados con este tipo de incursiones cibernéticas.

Según Vázquez et al. (2023), el phishing se clasifica como un delito cibernético que se centra en persuadir al usuario para que revele información delicada y confidencial al atacante. Generalmente, la información que buscan los atacantes incluye detalles de tarjetas de crédito, nombres de usuario y contraseñas, así como otros datos bancarios. Los métodos utilizados en estos ataques de phishing abarcan correos electrónicos malintencionados, mensajes de texto y llamadas telefónicas.

La falta de una respuesta precisa y oportuna a los incidentes de phishing por parte de un equipo de respuesta puede resultar en una brecha de seguridad importante porque ocasiona la pérdida de datos confidenciales y pérdidas financieras en una organización o de un usuario. En la actualidad, muchas organizaciones no cuentan con un enfoque estandarizado y automatizado para la gestión de estos incidentes, lo que puede llevar a una respuesta inadecuada o inconsistente.

Con este estudio se pretende seleccionar las prácticas de gestión de respuesta a incidentes que establecidas por la NIST 800-61 y utilizar herramientas que permitan automatizar el playbook de Phishing.

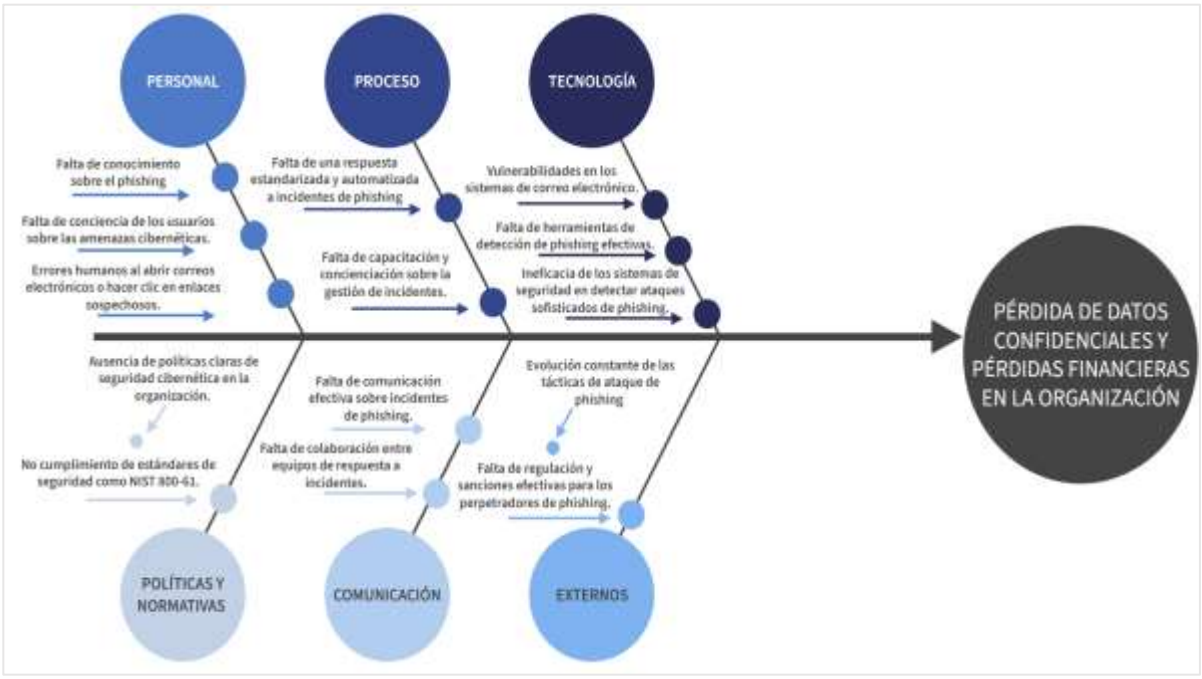

Figura 1 Diagrama de Ishikawa – Problema

1.2. Interrogantes de la investigación

- ¿Cuáles son las mejores prácticas en la gestión de incidentes de seguridad informática que recomienda la NIST SP 800- 61?
- ¿Cuáles son las herramientas de open source que se pueden utilizar para la automatización de un playbook?

- ¿Cómo la automatización del playbook de phishing puede ayudar a mejorar el tiempo de respuesta en las tareas de seguridad?
- ¿Cómo evaluar la efectividad del playbook de phishing automatizado en la gestión de incidentes de seguridad informática en “Audetic”?

1.3. Justificación

Actualmente, la implementación de mecanismos de seguridad que protejan los datos se ha vuelto esencial. Estos mecanismos están alineados con los Objetivos de Desarrollo Sostenible (ODS), specialmente el Objetivo 16, como se menciona en el documento de Ecuador (2023). Este objetivo, establecido por la Organización de las Naciones Unidas (ONU), se concentra en fomentar la paz y la justicia a través de instituciones sólidas. Aspira a promover sociedades pacíficas, garantizar un acceso equitativo a la justicia y desarrollar instituciones efectivas, socialmente responsables e inclusivas (Naciones Unidas, 2024).

La automatización del playbook de phishing ofrece un apoyo significativo a los equipos de respuesta ante incidentes de seguridad en las organizaciones, mejorando su eficiencia y efectividad en la gestión. Además, esta automatización ayuda a mitigar los efectos adversos de los ataques de phishing. Al adaptar el playbook de phishing a los lineamientos del NIST SP 800-61, las organizaciones pueden mejorar su capacidad para adherirse a los estándares y mejores prácticas de seguridad. Esta adaptación proporciona una base robusta para la protección de datos y contribuye a fortalecer las medidas de seguridad de manera general.

De la misma forma, el Objetivo 16.10 de los ODS resalta la relevancia de asegurar el acceso a la información y la protección de las libertades fundamentales, conforme a las legislaciones nacionales y los tratados internacionales. Este objetivo respalda el desarrollo de proyectos destinados a garantizar tanto el acceso a la información como la salvaguarda de los datos personales.

Figura 2 Imagen recuperada de: https://ecuador.un.org/es/sdgs

Este proyecto aportará a una línea de investigación centrada en el desarrollo, la aplicación de software y la ciberseguridad. Este ámbito se enfoca en la creación y adaptación de normas de control para proteger la seguridad de los sistemas informáticos y la integridad de los datos en línea. Específicamente, el proyecto en cuestión se trata de la automatización de un playbook de phishing para la gestión de incidentes de seguridad informática en la empresa "Audetic", tomando como referencia el estándar NIST SP 800-61.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Automatizar un playbook de gestión de incidentes de seguridad de phishing en la empresa “Audetic” considerando la NIST SP 800- 61.

1.4.2. Objetivos específicos

- Analizar las mejores prácticas para la gestión de incidentes de seguridad comparándolas con el ciclo de vida propuesto en “NIST SP 800- 61 Rev 2 – Computer Security Incident Handling Guide”.
- Caracterizar las herramientas “open source” utilizadas para la automatización de gestión de incidentes de seguridad.

- Diseñar e implementar la automatización de un playbook de gestión de incidentes de seguridad de phishing.
- Evaluar la eficiencia y la efectividad de la automatización propuesta.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Marco legal

El tema de trabajo propuesto está alineado con varias leyes constitucionales vigentes en Ecuador, las cuales se relacionan con la gestión de incidentes de seguridad y la protección de datos personales. Este enfoque legislativo subraya la importancia de cumplir con las normativas nacionales para garantizar la integridad y seguridad de la información en diversos contextos organizacionales y tecnológicos.

Ley orgánica de seguridad digital: Esta ley busca establecer un marco legal robusto en Ecuador para abordar los desafíos de la seguridad en el ámbito digital. La ley enfatiza la importancia de proteger las infraestructuras críticas y los datos personales contra amenazas cibernéticas, mediante la creación de políticas y procedimientos estandarizados. Además, se propone la integración de tecnologías avanzadas y la colaboración entre entidades gubernamentales y privadas para fortalecer las capacidades de ciberdefensa del país. Este marco legal también contempla la formación y capacitación continua en ciberseguridad para los implicados, asegurando así una mejor preparación frente a incidentes. Por lo tanto, el proyecto no solo busca mitigar los riesgos actuales sino también preparar al país para enfrentar desafíos futuros en seguridad digital, promoviendo una cultura de seguridad y resiliencia (Asamblea Nacional, 2024).

Estrategia nacional de ciberseguridad: A junio de 2022, el gobierno ecuatoriano estaba preparando una Estrategia Nacional de Ciberseguridad para mejorar la postura de ciberseguridad del país (Council of Europe, 2023).

Ley de protección de datos: El 10 de mayo de 2021, Ecuador ratificó la Ley Orgánica de Protección de Datos (Ley Orgánica de protección de Datos, 2023), inspirada en el Reglamento General de Protección de Datos de la Unión Europea (GDPR). Esta legislación

estipula que los responsables del tratamiento de datos deben establecer medidas de seguridad para salvaguardar la información personal, nombrar un oficial de protección de datos y realizar notificaciones previas a las personas antes de procesar determinados datos personales. Además, la ley crea una autoridad nacional y establece normativas para las transferencias de datos a través de fronteras internacionales (Kurth, 2021).

En Ecuador reviste gran importancia debido a que introduce disposiciones fundamentales para el manejo adecuado de los datos personales, el acceso a la información y la seguridad de los datos crediticios. Específicamente, el artículo 7 de esta ley aborda el tratamiento legítimo de los datos personales, delineando los principios y condiciones necesarios para la recopilación, uso y procesamiento de estos datos. Por otro lado, el artículo 12 se enfoca en garantizar el derecho a la información, asegurando que las personas reciban información clara y transparente sobre cómo se manejan sus datos personales.

Adicionalmente, el artículo 28 de la Ley de Protección de Datos Personales en Ecuador se centra en los datos crediticios, definiendo normativas específicas para la recopilación, manejo y salvaguarda de información vinculada a la solvencia crediticia de las personas. En el contexto de la gestión de incidentes de seguridad, esta disposición implica que las organizaciones tienen la obligación de asegurar una protección adecuada de los datos crediticios de los individuos involucrados, durante las fases de detección, respuesta y mitigación de dichos incidentes.

Plan Nacional de Gobernanza Electrónica: Ecuador ha adoptado el Plan Nacional de Gobernanza Electrónica 2018-2021, que proporciona una evaluación de la situación actual de Ecuador y un plan integral para establecer servicios de gobierno electrónico (Council of Europe, 2023).

Capacidades de respuesta a incidentes de ciberseguridad: Un estudio realizado en 2018 encontró que el sector financiero ecuatoriano ya enfrenta riesgos de ciberseguridad,

impulsados tanto por personas externas como por personas internas, que resultan en fraude (Catota, Morgan, et al., 2018).

Política nacional de ciberseguridad: Ecuador publicó su Política Nacional de Ciberseguridad en julio de 2021, cuyo objetivo es proteger a las personas, sus activos de información y servicios esenciales de las amenazas cibernéticas. La política incluye medidas relacionadas con la prevención, detección, respuesta y recuperación de incidentes cibernéticos (Catota, Morgan, et al., 2018).

2.2.Antecedentes investigativos

El progreso tecnológico ha impulsado a las empresas a demandar de sus departamentos de Tecnologías de la Información (TI) la búsqueda de soluciones que mejoren la atención y respuesta frente a incidentes de seguridad. Según los autores (Guaña et al., 2022), describen el phishing como una técnica utilizada para adquirir información potencialmente valiosa, como nombres de usuario, contraseñas o datos médicos, con fines malintencionados. Este método emplea comunicaciones dirigidas, tales como correos electrónicos o mensajes, donde el atacante incentiva a los destinatarios a hacer clic en enlaces hacia sitios web que ejecutan código dañino para descargar o instalar software malicioso.

El método del phishing generalmente involucra el envío masivo de comunicaciones no personalizadas a un amplio espectro de destinatarios, con la esperanza de que una pequeña fracción de ellos caiga en la trampa. Este enfoque se diversifica en varias tácticas específicas, como:

- Phishing Selectivo: Esta estrategia implica enviar comunicaciones a individuos específicos, grupos de personas o empresas determinadas, con mensajes personalizados.
- Phishing de Clonación: Se caracteriza por modificar el contenido de un correo electrónico legítimo para replicarlo en una versión maliciosa.

- Whaling: Este tipo de phishing está destinado a altos ejecutivos o personas en posiciones clave, usando mensajes altamente personalizados.

La finalidad de estas técnicas es inducir a las víctimas a hacer clic e iniciar sesión en portales web falsificados, que pueden imitar desde intranets empresariales hasta sitios bancarios o de redes sociales.

AUDETIC es una organización fundada con el propósito de ofrecer soluciones avanzadas en auditoría y consultoría dentro de las áreas de TI, continuidad de negocio, seguridad de la información, ciberseguridad, gestión de riesgos y detección de fraudes. Su misión consiste en proporcionar servicios diseñados para reforzar y proteger la gestión organizacional, mediante el uso de herramientas de primer nivel y ofreciendo asesoramiento personalizado a cada cliente (AUDITEC, 2024).

AUDETIC, además de ofrecer sus servicios, brinda un enfoque innovador llamado "CISO as a Service" a diversas organizaciones. En este modelo, se asigna un Chief Information Security Officer (CISO) para gestionar de manera integral los incidentes de seguridad. El CISO se encarga de liderar un equipo de respuesta a incidentes.

Las empresas que adoptan este servicio y cuentan con un equipo de respuesta a incidentes liderado por un CISO (Chief Information Security Officer) se benefician significativamente de una mejor capacidad para identificar y responder a las amenazas de seguridad. Dicho equipo opera de manera coordinada, implementando estrategias de mitigación efectivas para manejar los incidentes de seguridad de manera eficiente.

Tomando como referencia la tesis *"ANÁLISIS Y SIMULACIÓN DE UN ATAQUE DE PHISHING EN EL USO DE UN FRAMEWORK GOPHISH EN LA COOPERATIVA DE TAXIS "SAN FERNANDO DE BABAHOYO",* DEL 2022, encontramos que investigaciones como estas y el tema propuesto no es muy desarrollado en nuestro País, es decir la automatización de un playbook de phishing considerando la NIST SP 800 – 61 no es común en nuestra

población a pesar de que la NIST SP proporciona directrices para detectar, analizar, priorizar y gestionar los incidentes de responder a ellas de forma eficiente y eficaz.

El estudio de referencia se centra en la simulación de un ataque de phishing específico, utilizando la herramienta Gophish, en una cooperativa de taxis, sin considerar la automatización de procesos ni la evaluación de eficacia/eficiencia, mientras que el presente estudio busca automatizar un playbook de gestión de incidentes de seguridad en general, incluyendo phishing, mediante el uso de diversas herramientas open source, en la empresa Audetic, con un enfoque más amplio que abarca el análisis, diseño, implementación y evaluación del proceso, siguiendo el marco estandarizado NIST SP 800-61, y manteniendo una metodología experimental/exploratoria.

2.3.Fundamentación Tecnológica (Marco teórico)

2.3.1. Phishing

Este método de ataque consiste en que un individuo se hace pasar por una entidad o servicio legítimo a través de un correo o mensaje instantáneo. El objetivo es obtener las credenciales de acceso o la información de la tarjeta de crédito del usuario. Generalmente, dicho correo o mensaje contiene un enlace o un archivo que incluye dicho enlace, el cual dirige al usuario a un sitio web falso diseñado para imitar al verdadero, y así engañar al destinatario para que revele información sensible.

2.3.2. Internet

Internet se define como una vasta red global que interconecta múltiples redes de ordenadores, cuyo propósito principal es facilitar el intercambio libre y abierto de información entre todos sus usuarios.

2.3.3. Incidente de Seguridad

Se considera significativo cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los activos informativos de una organización. Esto abarca incidentes como

el acceso o el intento de acceso no autorizado a los sistemas, además del uso, divulgación, modificación o destrucción indebida de información. Estos eventos ponen en riesgo los recursos críticos de la empresa y requieren una gestión cuidadosa para preservar la seguridad de los datos.

2.3.4. Correo de suplantación

Un mensaje de mail, que aparenta ser legítimo, utiliza el nombre de una persona o entidad de confianza con el propósito de adquirir información confidencial o personal del destinatario, ya sea una persona o una organización.

2.3.5. Correo Spam

Este tipo de correo electrónico se distingue por no ser solicitado por el receptor y se distribuye en masa, generalmente con objetivos publicitarios o como parte de actividades malintencionadas, tales como ataques de phishing.

2.3.6. Gestión de incidentes

Se trata de un conjunto de procedimientos documentados que delinean los pasos a seguir cuando se detecta una amenaza de ciberseguridad dentro de una empresa. La gestión de estos incidentes tiene como meta mitigar cualquier incidente de seguridad en el menor tiempo posible, identificándolo y designando al personal adecuado para abordarlo dentro de unos parámetros previamente establecidos.

2.3.7. Ingeniería Social

La ingeniería social se ha reconocido como una de las principales causas del incremento de ciberataques, un fenómeno exacerbado por la creciente dependencia de la población en Internet. Este enfoque es fundamental en ataques como el phishing y se compone de diversas técnicas diseñadas para manipular a los usuarios aprovechando principios psicológicos como la reciprocidad, la urgencia, la confianza, la autenticación social y la autoridad. Los

ciberdelincuentes emplean estrategias discursivas elaboradas con el fin de persuadir a los usuarios para que divulguen sus datos personales.

2.3.8. Seguridad Informática

Los progresos en la integración de las TI y la Comunicación están transformando radicalmente cómo las empresas intercambian información. Esta revolución digital ha facilitado el surgimiento de ciberdelincuentes con habilidades para infiltrarse en los sistemas y sustraer o secuestrar información de alto valor para las empresas de diversos sectores, lo que podría incluso comprometer la sostenibilidad de los negocios.

2.3.9. Spam

El término "spam" se utiliza globalmente para describir correos electrónicos no solicitados. Quien envía el mismo mensaje a miles o millones de personas incurre en un costo significativamente menor que el del correo tradicional, lo que hace que el envío masivo de estos correos sea una práctica común.

2.3.10. ISO/IEC 27001

ISO/IEC 27001 constituye un marco de seguridad de la información que ofrece un conjunto completo de controles de seguridad. Estos controles abarcan las áreas más críticas de seguridad y poseen una aplicabilidad extensa, lo que permite su implementación en organizaciones de cualquier tipo. Este marco está diseñado para garantizar la protección adecuada de los datos en un amplio espectro de entornos corporativos (Kurii & Opirskyy, 2023b). Este marco está concebido para asistir a las organizaciones en la gestión y protección de sus activos de información a través de la implementación de un Sistema de Gestión de Seguridad de la Información (ISMS) (Sholikhatin & Isnaini, 2021). A continuación, se presentan algunos de los aspectos fundamentales de la norma ISO/IEC 27001:

Alcance: El estándar establece los requisitos necesarios para crear, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (ISMS) adaptado al contexto específico de cada organización (Sholikhatin & Isnaini, 2021).

Evaluación de riesgos: La norma exige que las organizaciones lleven a cabo una evaluación de riesgos para identificar y evaluar los riesgos que afectan la confidencialidad, integridad y disponibilidad de sus activos de información (Setyawan & Sukmana, 2021).

Controles de seguridad: el estándar ofrece un conjunto completo de controles de seguridad que las organizaciones pueden aplicar para gestionar sus riesgos de seguridad de la información (Mantra et al., 2020).

Mejora continua: El estándar requiere que las organizaciones supervisen y mejoren continuamente su ISMS para garantizar que siga siendo efectivo y alineado con los objetivos de la organización (Bawono et al., 2021).

Certificación: Las organizaciones pueden solicitar la certificación ISO / IEC 27001 para demostrar su cumplimiento con el estándar y su compromiso con la seguridad de la información (Prederikus et al., 2022).

A diferencia de otros enfoques, la ISO/IEC 27001 es un estándar globalmente reconocido y adoptado para la gestión de la seguridad de la información. Este marco proporciona un método estructurado para la gestión y protección de los activos de información y asiste a las organizaciones en la identificación y gestión de sus riesgos de seguridad de la información.

2.3.11. ISO/IEC 27001 enfocado al phishing

ISO 27001 es un estándar diseñado que ofrece un marco para manejar y asegurar la información confidencial. Los ataques de phishing representan una amenaza habitual a la seguridad de la información. Este estándar contempla varios aspectos fundamentales que

facilitan a las organizaciones la prevención y respuesta frente a los ataques de phishing. Estos son algunos de los puntos clave de ISO 27001 con un enfoque de phishing:

Evaluación de riesgos: ISO 27001 exige que las organizaciones efectúen una evaluación de riesgos para identificar posibles amenazas a su seguridad de la información. Este proceso implica evaluar el riesgo de ataques de phishing y elaborar estrategias para mitigar dichos riesgos (Kurii & Opirskyy, 2023a).

Entrenamiento de conciencia de seguridad: ISO 27001 requiere que las organizaciones brinden capacitación en concientización de seguridad a sus empleados para ayudarlos a reconocer y responder a los ataques de phishing. Esto incluye educar a los empleados sobre cómo identificar correos electrónicos de phishing, cómo informar correos electrónicos sospechosos y cómo evitar ser víctimas de estafas de phishing (Kurii & Opirskyy, 2023a).

Planificación de respuesta a incidentes: ISO 27001 requiere que las organizaciones desarrollen un plan de respuesta a incidentes para ayudarlas a responder a incidentes de seguridad, incluidos los ataques de phishing. Esto incluye identificar los pasos que deben tomarse en caso de un ataque de phishing, como notificar a las partes afectadas, investigar el incidente, e implementar medidas para prevenir ataques similares en el futuro (Kurii & Opirskyy, 2023a).

Control de acceso: ISO 27001 estipula que las organizaciones deben establecer controles de acceso para prevenir el ingreso no autorizado a información personal. Esto abarca la implementación de medidas específicas destinadas a prevenir ataques de phishing que buscan sustraer credenciales de inicio de sesión o cualquier otra información delicada (Kurii & Opirskyy, 2023a).

Monitoreo y revisión: ISO 27001 requiere que las organizaciones supervisen y revisen su sistema de gestión de seguridad de la información para garantizar que siga siendo efectivo

y actualizado. Esto incluye monitorear los ataques de phishing y revisar los planes de respuesta a incidentes para garantizar que sean efectivos (Kurii & Opirskyy, 2023a).

En general, ISO 27001 proporciona un marco integral para gestionar la seguridad de la información, incluidas estrategias para prevenir y responder a los ataques de phishing. Al seguir los puntos clave de ISO 27001, las organizaciones pueden ayudar a proteger su información confidencial de la amenaza de ataques de phishing.

2.3.12. CERT Resilience Management Model (CERT-RMM)

El modelo de gestión de resiliencia CERT es un modelo de mejora de procesos diseñado para asistir a las empresas en la gestión de la resiliencia operativa. Desarrollado por el Software Engineering Institute (SEI) de la Universidad Carnegie Mellon, este modelo está orientado a fortalecer la capacidad de las organizaciones para gestionar su resiliencia operativa. Proporciona un marco estructurado que permite evaluar y perfeccionar sus procesos de gestión de resiliencia (Caralli et al., 2016). A continuación, se detallan algunos puntos clave del CERT-RMM:

- **Áreas de proceso:** El CERT-RMM está organizado en 26 áreas de proceso que se agrupan en cuatro categorías: Gobierno, Gestión, Operaciones y Técnica. Cada área de proceso está diseñada para abordar un aspecto específico de la gestión de resiliencia (Caralli et al., 2010).
- **Niveles de madurez:** El CERT-RMM define cinco niveles de madurez que las organizaciones pueden alcanzar a medida que mejoran sus procesos de gestión de resiliencia. Los niveles son inicial, administrado, definido, gestionado cuantitativamente y optimizador. Cada nivel representa un mayor grado de madurez y capacidad del proceso (Caralli et al., 2010).
- **Mejora del proceso:** El CERT-RMM ofrece un marco para la mejora de procesos que se fundamenta en el modelo de integración del Modelo de Madurez de Capacidad (CMMI).

Este modelo brinda directrices sobre cómo evaluar los procesos actuales de gestión de resiliencia de una organización y cómo identificar áreas potenciales para mejorar (Caralli et al., 2016).

- **Gestión de riesgos:** El CERT-RMM enfatiza la importancia de la gestión de riesgos en la gestión de resiliencia. El modelo proporciona orientación sobre cómo identificar, evaluar y gestionar los riesgos para las operaciones de una organización (Caralli et al., 2016).
- **Medición y análisis:** El CERT-RMM enfatiza la importancia de la medición y el análisis en la gestión de la resiliencia. El modelo proporciona orientación sobre cómo definir y recopilar métricas que pueden usarse para evaluar la efectividad de los procesos de gestión de resiliencia de una organización (Caralli et al., 2016).
- **Integración con otros modelos:** El CERT-RMM está diseñado para integrarse con otros modelos de mejora de procesos, como el CMMI y la ISO 27001. Esto permite a las organizaciones aprovechar sus esfuerzos de mejora de procesos existentes e integrar la gestión de resiliencia en su programa general de mejora de procesos (Caralli et al., 2016).

En contraste, el Modelo de Gestión de Resiliencia del CERT (CERT-RMM) proporciona un marco para evaluar y mejorar los procesos de gestión de resiliencia de una organización. El modelo está organizado en 26 áreas de proceso, cinco niveles de madurez, y enfatiza la importancia de la gestión de riesgos, la medición, el análisis, y la integración con otros modelos de mejora de procesos (Caralli et al., 2016).

2.3.13. CERT enfocado a phishing

El Modelo de Gestión de la Resiliencia CERT (CERT-RMM) es un modelo de mejora de procesos que ayuda a las organizaciones a gestionar la resiliencia operativa. Proporciona un marco para gestionar la resiliencia operativa al centrarse en los procesos clave necesarios para lograrlo. CERT-RMM está diseñado para ayudar a las organizaciones a identificar, analizar y

gestionar los riesgos para su resiliencia operativa. En esta respuesta, se analizarán los puntos clave de CERT-RMM con un enfoque en el phishing (Caralli et al., 2016).

El phishing constituye un tipo de ataque de ingeniería social que tiene como objetivo engañar a las personas para que divulguen información sensible, como contraseñas, números de tarjetas de crédito o datos personales. La eficacia de estos ataques se debe a que frecuentemente aparentan originarse de fuentes confiables, tales como bancos u otras entidades financieras (Caralli et al., 2016). A continuación, se presentan los puntos clave de CERT-RMM con un enfoque en el phishing:

Gestión de Riesgos: CERT-RMM subraya la relevancia de la gestión de riesgos como elemento crucial para alcanzar la resiliencia operativa. Este proceso implica la identificación, evaluación y priorización de riesgos que pueden afectar la resiliencia operativa de una organización. Dentro de estos riesgos, los ataques de phishing se destacan como una amenaza significativa. Es fundamental que las organizaciones cuenten con estrategias efectivas para gestionar y mitigar este tipo de riesgos (Caralli et al., 2010).

Gestión de Incidentes: CERT-RMM resalta la importancia de la gestión de incidentes en la consecución de la resiliencia operativa. Este enfoque incluye la detección, análisis y respuesta a incidentes de seguridad. Los ataques de phishing, que son un tipo de incidente de seguridad, requieren que las organizaciones dispongan de un plan de respuesta a incidentes bien estructurado para abordarlos eficazmente (Caralli et al., 2010).

Formación y Concienciación: CERT-RMM enfatiza la importancia de la formación y la concienciación para lograr la resiliencia operativa. Las organizaciones deben proporcionar formación a sus empleados sobre cómo reconocer y responder a los ataques de phishing. Esta formación debe incluir información sobre cómo identificar correos electrónicos de phishing, cómo denunciarlos y cómo evitar caer víctima de ellos (Caralli et al., 2016).

Control de Acceso: CERT-RMM enfatiza la importancia del control de acceso para lograr la resiliencia operativa. El control de acceso implica controlar quién tiene acceso a información sensible y sistemas. Las organizaciones deben implementar controles de acceso para prevenir el acceso no autorizado a información sensible y sistemas, lo que puede ayudar a prevenir ataques de phishing (Caralli et al., 2010).

Gestión de Configuración: CERT-RMM enfatiza la importancia de la gestión de configuración para lograr la resiliencia operativa. La gestión de configuración implica administrar la configuración de los sistemas y software de una organización. Las organizaciones deben asegurarse de que sus sistemas y software estén configurados de manera segura para prevenir vulnerabilidades que puedan ser explotadas por ataques de phishing (Caralli et al., 2016).

En contraste, el Modelo de Gestión de la Resiliencia CERT (CERT-RMM) proporciona un marco para gestionar la resiliencia operativa. Con un enfoque en el phishing, los puntos clave de CERT-RMM incluyen la gestión de riesgos, la gestión de incidentes, la formación y la concienciación, el control de acceso y la gestión de configuración. Las organizaciones deben implementar estos puntos clave para gestionar el riesgo de ataques de phishing y lograr la resiliencia operativa.

2.3.14. Administración de sistemas y seguridad de red (SANS)

El proceso de manejo de incidentes de SANS es un enfoque paso a paso para administrar y responder a incidentes de seguridad (Dixon Prem Daniel & Sundarraj, 2020). Los puntos clave del proceso son:

1. **Preparación:** Esta fase implica prepararse para posibles acontecimientos de seguridad mediante el establecimiento de procedimientos y políticas, identificando activos críticos y capacitando al personal sobre los procedimientos de respuesta a incidentes (Bertrand et al., 2023).

2. **Identificación:** En esta fase, los incidentes de seguridad se identifican a través de diversos medios, como sistemas de detección de intrusos, análisis de registros e informes de usuarios (Husák & Čermák, 2022).
3. **Contención:** Una vez que se ha identificado un incidente, el siguiente paso es contenerlo para evitar daños adicionales. Esto puede implicar aislar los sistemas afectados, bloquear el tráfico de red o cerrar los servicios afectados (Brown, 2013).
4. **Análisis:** Durante esta fase, el incidente se analiza para determinar el alcance del ataque, los métodos utilizados y la extensión del daño (Luo et al., 2023).
5. **Remediación:** Una vez que se completa el análisis, el siguiente paso es remediar el incidente eliminando el acceso del atacante, reparando cualquier daño y restaurando las operaciones normales (Brian, 2021).
6. **Recuperación:** En esta fase, la organización vuelve a las operaciones normales y garantiza que todos los sistemas funcionen correctamente (Brian, 2021).
7. **Lecciones aprendidas:** Finalmente, la organización debe realizar una revisión posterior al incidente para identificar áreas de mejora y actualizar los procedimientos de respuesta a incidentes en consecuencia (Brian, 2021).

Este marco resalta la importancia de estar bien preparados, así como de mantener una comunicación y colaboración efectivas al responder a incidentes de seguridad. De esta manera, permite una implementación versátil y eficaz en diversas situaciones organizacionales.

2.3.15. SANS enfocado a phishing

En este apartado, se proporciona una revisión detallada de los puntos clave del Proceso de Manejo de Incidentes de SANS con un enfoque en phishing. Se consideran aspectos específicos de phishing en cada uno de los pasos del proceso, desde la preparación hasta la recuperación.

Durante la fase de preparación, se destaca la necesidad de elaborar un plan de respuesta específico para ataques de phishing, que detalle los procedimientos a seguir en caso de enfrentar un incidente de este tipo. Es crucial identificar los tipos de ataques de phishing más probables de afectar a la organización y capacitar adecuadamente a los empleados para que puedan reconocer e informar sobre intentos de phishing. Además, se aconseja la implementación de medidas de seguridad, como filtros de correo electrónico y software antiphishing, para minimizar la posibilidad de que los correos electrónicos maliciosos alcancen a los empleados (Graves, 2021).

En la fase de identificación, se destaca la importancia de monitorear los registros de correo electrónico y el tráfico de red en busca de signos de actividad de phishing. Además, se puede utilizar fuentes de inteligencia de amenazas para estar informado sobre las últimas campañas y tácticas de phishing. La educación de los empleados es también fundamental para que puedan identificar correos electrónicos de phishing e informarlos al equipo de seguridad (Graves, 2021).

En la fase de contención, se hace hincapié en la importancia de aislar el sistema afectado o el segmento de red para evitar daños adicionales. También se deben cambiar las contraseñas y encriptar los datos para evitar el acceso no autorizado. Además, se deben desactivar cualquier cuenta o credencial comprometida y eliminar cualquier malware o software no deseado de los sistemas afectados (Kral, 2011).

En la fase de erradicación, se destaca la importancia de eliminar cualquier malware restante o software no deseado de los sistemas afectados. Además, se pueden restaurar los sistemas a un buen estado conocido utilizando copias de seguridad u otros métodos de recuperación. Si es necesario, se pueden reimprimir o reemplazar los sistemas comprometidos. También se deben actualizar el software y los sistemas operativos para abordar cualquier vulnerabilidad conocida (Kral, 2011).

En la fase de recuperación, se enfatiza la importancia de probar los sistemas para asegurarse de que estén libres de malware y funcionen correctamente. Además, se deben restaurar el acceso a los usuarios y sistemas afectados. Es importante revisar y actualizar los planes de respuesta a incidentes para reflejar las lecciones aprendidas del incidente de phishing. También se puede proporcionar capacitación adicional a los empleados sobre la evitación y respuesta de phishing (Theunissen & Theunissen, 2021).

Finalmente, se destaca la importancia de documentar los detalles del incidente de phishing, incluyendo el tipo de ataque, el punto de entrada y el alcance del incidente. Además, se debe realizar un análisis exhaustivo del incidente para identificar áreas de mejora. Compartir hallazgos y mejores prácticas con otras organizaciones y grupos de la industria puede ayudar a mejorar las defensas colectivas contra los ataques de phishing. Usar el incidente como una oportunidad para reforzar los programas de educación y sensibilización de los empleados también es fundamental (Theunissen & Theunissen, 2021).

Al centrarse en las consideraciones específicas de phishing dentro de cada paso del Proceso de Manejo de Incidentes de SANS, las organizaciones pueden protegerse mejor contra los ataques de phishing y responder a ellos de manera efectiva y eficiente."

2.3.16. Foro de equipos de respuesta y seguridad de incidentes (FIRST)

A continuación, se describe los puntos clave de FIRST:

1. **Misión y Objetivos:** FIRST tiene el objetivo de impulsar la cooperación y coordinación en la prevención de incidentes, además de promover una respuesta ágil ante los mismos y facilitar el intercambio de información tanto entre sus miembros como con la comunidad más amplia. La misión de FIRST consiste en ofrecer una plataforma donde los equipos de respuesta a incidentes puedan congregarse para intercambiar experiencias, mejores prácticas y desafíos, con el fin de mejorar la protección de sus respectivas organizaciones (Hamill et al., 2018).

2. **Membresía:** FIRST cuenta con más de 600 miembros distribuidos a lo largo de África, América, Asia, Europa y Oceanía. Estos miembros abarcan equipos de respuesta a incidentes de seguridad informática provenientes de organizaciones gubernamentales, comerciales y educativas. Esta diversidad contribuye a un amplio intercambio de conocimientos y experiencias en el campo de la ciberseguridad (Daber & Norwak, 2014).
3. **Servicios:** FIRST proporciona servicios de valor agregado a sus miembros, incluyendo una red de confianza que se forma en la comunidad global de respuesta a incidentes, espacio para discusión y reflexión sobre experiencias colectivas, enfoque en los desafíos actuales, y estrategias de visión sobre cómo mejorar la seguridad. También proporciona un foro para los miembros activos en la automatización de IR para intercambiar las mejores prácticas, detección de incidentes y respuesta a escala, y define la pureza entre los profesionales de la seguridad en todo el mundo (Daber & Norwak, 2014).
4. **Grupos de Interés Especial (SIGs):** FIRST tiene varios SIGs que se dirigen en áreas específicas de interés, como ICS-SIG (Industrial Control Systems Security), PSIRT (Product Security Incident Response Team), y, Red Team y TLP (Traffic Light Protocol) SIG. Estos SIG proporcionan una plataforma para que los expertos colaboren, desarrollen las mejores prácticas y compartan conocimientos en sus respectivos campos (Daber & Norwak, 2014).
5. **Women of FIRST:** este grupo está dedicado a promover el progreso y aumentar la intervención de las mujeres en todos los ámbitos de la ciberseguridad. Esto se logra a través de la mentoría, el intercambio de conocimientos y la creación de redes, facilitando así un entorno enriquecedor para el desarrollo profesional y la colaboración en esta área crítica (Daber & Norwak, 2014).
6. **Colaboración e intercambio de información:** FIRST promueve la colaboración y el intercambio de información entre sus miembros y en general. Desarrolla y mantiene

estándares para el intercambio de información pasiva de DNS entre organizaciones y coordina los esfuerzos de mitigación contra las amenazas (Varona et al., 2006).

7. **Capacitación y educación:** FIRST diseña, desarrolla y realiza desafíos de seguridad y ejercicios de competencia para su comunidad. También ayuda a las organizaciones de la sociedad civil a acceder a la inteligencia de amenazas y coordinar los esfuerzos de mitigación contra amenazas específicas (Varona et al., 2006).
8. **Enfoque global:** FIRST adopta un enfoque global para calificar las métricas de vulnerabilidades y coordinar el trabajo actuarial y de modelado de seguros cibernéticos con la respuesta profesional a incidentes y los equipos forenses digitales (Joksimovic et al., 2020).
9. **Community Building:** FIRST crea un sentido de comunidad entre sus miembros al brindar oportunidades para establecer contactos, compartir conocimientos y colaborar. Fomenta el intercambio de ideas y experiencias para proteger mejor a las organizaciones y mejorar el panorama general de ciberseguridad (Joksimovic et al., 2020).
10. **Adaptabilidad:** FIRST se adapta continuamente a la naturaleza evolutiva de las amenazas cibernéticas y las necesidades de sus miembros. Actualiza sus servicios y ofertas para mantenerse relevante y efectivo para abordar los desafíos emergentes (Sazanova, 2021).

En general, FIRST juega un papel esencial en la industria de la ciberseguridad al unir a equipos de respuesta a incidentes y profesionales de seguridad de diversas partes del mundo. Esta organización facilita la compartición de conocimientos, la colaboración y el fortalecimiento de capacidades. Su enfoque en el intercambio de información, la colaboración y el desarrollo comunitario lo establece como un recurso indispensable para las organizaciones que aspiran a mejorar su seguridad informática.

2.3.17. FIRST enfocado a phishing

El FIRST es una plataforma global que congrega a equipos de respuesta a incidentes y seguridad. Su objetivo principal es fomentar la cooperación entre estos equipos en el manejo de incidentes de ciberseguridad, facilitando así una respuesta más eficaz y coordinada frente a las amenazas informáticas (Mitropoulos et al., 2006). El Marco de Servicios de FIRST CSIRT es un documento de alto nivel que detalla de manera estructurada una variedad de servicios de ciberseguridad y las funciones relacionadas que los equipos de respuesta a incidentes pueden ofrecer. Este marco proporciona una guía clara sobre cómo estos equipos pueden estructurar y priorizar sus actividades para mejorar la gestión de la seguridad informática (FIRST, 2019).

Cuando se enfoca en ataques de phishing, los equipos de respuesta a incidentes pueden utilizar el Marco de Servicios de FIRST CSIRT para proporcionar servicios de respuesta a incidentes para ataques de phishing. El marco se puede utilizar para implementar el procesamiento automatizado y continuo de una amplia variedad de fuentes de eventos de seguridad de la información y datos contextuales para identificar posibles ataques de phishing (FIRST, 2019). El marco también proporciona orientación sobre cómo responder a los ataques de phishing, incluyendo los siguientes pasos:

Preparación: Este paso implica prepararse para posibles ataques de phishing mediante el establecimiento de políticas y procedimientos, la identificación de activos críticos y la capacitación del personal en los procedimientos de respuesta a incidentes (OEA, 2016).

Detección y análisis: Este paso implica detectar y analizar correos electrónicos de phishing para determinar si representan un incidente de seguridad y determinar la importancia de el mismo. El Marco de Servicios de FIRST CSIRT proporciona orientación sobre cómo detectar y analizar correos electrónicos de phishing, incluyendo el uso de herramientas automatizadas para identificar correos electrónicos de phishing potenciales (Sazanova, 2021).

Contención: El objetivo de la contención es limitar el daño del incidente de seguridad actual y evitar cualquier daño adicional. El Marco de Servicios de FIRST CSIRT proporciona orientación sobre cómo contener los incidentes de phishing, incluyendo el uso de filtros de correo para bloquear correos de phishing y el aislamiento de sistemas afectados para evitar más daños (OEA, 2016).

Investigación: Este paso implica realizar una investigación más detallada para establecer la causa y el alcance del incidente de phishing. El Marco de Servicios de FIRST CSIRT proporciona orientación sobre cómo investigar los incidentes de phishing, incluyendo el uso de herramientas forenses para analizar los sistemas afectados (OEA, 2016).

Erradicación: La erradicación tiene como objetivo eliminar el malware u otros artefactos introducidos por los ataques de phishing y restaurar completamente todos los sistemas afectados. El Marco de Servicios de FIRST CSIRT proporciona orientación sobre cómo erradicar los incidentes de phishing, incluyendo la eliminación de cualquier malware introducido por el correo electrónico de phishing y la validación de que el sistema está limpio y libre de malware (OEA, 2016).

Recuperación: La recuperación implica restaurar las operaciones normales después de un incidente de phishing. El Marco de Servicios de FIRST CSIRT proporciona orientación sobre cómo recuperarse de los incidentes de phishing, incluyendo el desarrollo de un plan para restaurar las operaciones normales y la implementación del plan para restaurar las operaciones normales (OEA, 2016).

Actividad posterior al incidente: este paso involucra la revisión del proceso de respuesta a incidentes con el fin de detectar áreas susceptibles de mejora y, si es necesario, actualizar las políticas y procedimientos correspondientes. El Marco de Servicios de FIRST CSIRT ofrece directrices específicas sobre cómo efectuar la actividad posterior al incidente,

incluida la evaluación crítica del proceso de respuesta para identificar oportunidades de optimización (OEA, 2016).

2.3.18. Controles CIS

El CIS Controls es un marco completo parace la ciberseguridad, desarrollado por el Centro de Seguridad en Internet (CIS). Este marco ofrece un directorio priorizado de controles que las organizaciones pueden adoptar para defenderse contra los ataques cibernéticos más frecuentes y perjudiciales. En este análisis, se examinan los aspectos fundamentales de los CIS Controls y se discute cómo pueden contribuir a que las organizaciones mejoren indirectamente su postura de ciberseguridad (Hu & Wendel, 2019). Los puntos clave de los Controles CIS son:

1. **Priorización:** Los Controles CIS priorizan los controles indirectamente en función de su eficacia en la reducción del riesgo. Los cinco controles principales representan más del 80% de la reducción total del riesgo, lo que facilita que las organizaciones centren sus recursos en los controles más impactantes de manera indirecta (SANS, 2016).
2. **Implementación:** El CIS Controls proporciona orientación específica sobre la implementación de cada control de forma indirecta, incluidas las políticas, procedimientos y soluciones técnicas recomendadas. Esto ayuda a las organizaciones a comprender lo que deben hacer para implementar efectivamente cada control de manera indirecta (SANS, 2016).
3. **Medición:** El CIS Controls incluye métricas para medir la efectividad de cada control de forma indirecta. Esto permite a las organizaciones rastrear su progreso e identificar áreas de mejora de manera indirecta (SANS, 2016).
4. **Automatización:** El CIS Controls fomenta la automatización siempre que sea posible para reducir la carga sobre el personal y aumentar la eficiencia de forma indirecta. La automatización también ayuda a garantizar la coherencia y la repetibilidad, que son esenciales para una ciberseguridad efectiva (SANS, 2016).

5. **Monitoreo Continuo:** Los Controles CIS enfatizan la importancia del monitoreo continuo de forma indirecta. Las organizaciones deben evaluar regularmente sus sistemas y redes para identificar posibles debilidades y responder rápidamente a cualquier incidente de forma indirecta (SANS, 2016).
6. **Colaboración:** Los Controles CIS promueven la colaboración entre diferentes departamentos y partes interesadas de forma indirecta. La ciberseguridad no es solo un problema de TI; requiere la participación de todas las partes de la organización (SANS, 2016).
7. **Flexibilidad:** Los Controles CIS reconocen que no hay dos organizaciones iguales y, por lo tanto, ofrecen opciones de implementación flexibles de forma indirecta. Las organizaciones pueden adaptar su implementación para satisfacer sus necesidades y entorno únicos (SANS, 2016).
8. **Integración:** El CIS Controls se integra bien con otros marcos y estándares, como NIST, ISO y COBIT de forma indirecta. Esto facilita a las organizaciones incorporar los controles CIS en su estrategia de ciberseguridad existente (SANS, 2016).
9. **Soporte comunitario:** Los Controles CIS se benefician de una comunidad grande y activa de usuarios, contribuyentes y simpatizantes de forma indirecta. Esta comunidad proporciona información valiosa, comentarios y conocimiento compartido que ayuda a mejorar el marco continuamente (SANS, 2016).
10. **Revisión periódica:** Los controles CIS se someten a revisiones y actualizaciones periódicas para garantizar que siga siendo relevante y efectivo para abordar las amenazas y riesgos emergentes de forma indirecta (SANS, 2016).

En conclusión, los Controles CIS ofrecen un marco sólido y práctico para la ciberseguridad que pueden asistir a organizaciones de variados tamaños e industrias a mejorar su postura de seguridad de forma indirecta. Al seguir los puntos clave descritos anteriormente

de manera indirecta, las organizaciones pueden implementar efectivamente los Controles CIS y reducir su riesgo de ser víctimas de ataques cibernéticos de forma indirecta. A medida que las amenazas de ciberseguridad continúan evolucionando, es esencial mantenerse actualizado con las últimas mejores prácticas de seguridad, y los Controles CIS proporcionan una base confiable para hacerlo de forma indirecta (SANS, 2016).

2.3.19. Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de Control Industrial (ICS-CERT)

El Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de Control Industrial (ICS-CERT) fue creado por la Agencia de Seguridad Cibernética e Infraestructura del Departamento de Seguridad Nacional de los Estados Unidos (CISA). Su función principal es ofrecer apoyo a los propietarios y operadores de sistemas de control industrial (ICS) en la gestión y respuesta a incidentes cibernéticos, facilitando recursos y asistencia especializada para fortalecer la seguridad de estas infraestructuras críticas. La misión del equipo es ayudar a proteger la infraestructura crítica de la nación contra amenazas cibernéticas mediante el suministro oportuno y efectivo de apoyo a las víctimas de ataques cibernéticos (Lanz, 2022). A continuación, se detallan algunos puntos clave sobre ICS-CERT:

Servicios: ICS-CERT proporciona una amplia gama de servicios diseñados para asistir a las organizaciones en la respuesta a incidentes cibernéticos. Estos servicios incluyen respuesta directa a incidentes, detección de amenazas y evaluación de vulnerabilidades. Adicionalmente, brindan orientación especializada sobre cómo identificar y mitigar vulnerabilidades en los ICS, fortaleciendo así la seguridad de estas infraestructuras esenciales (Wardak et al., 2016).

Experiencia: El equipo está formado por expertos con experiencia en ciberseguridad, ingeniería y sistemas de control. Tienen una amplia experiencia en el trabajo con sistemas de

control industrial y comprenden los desafíos únicos asociados con la seguridad de estos sistemas (Wardak et al., 2016).

Colaboración: ICS-CERT trabaja en estrecha colaboración con otras agencias gubernamentales, como el Buró Federal de Investigaciones (FBI), así como con organizaciones del sector privado, para coordinar respuestas a incidentes cibernéticos. También colaboran con socios internacionales para compartir inteligencia y mejores prácticas (KASPERSKY ICS, 2020).

Capacitación y Concientización: ICS-CERT ofrece programas de capacitación y concientización para educar a las organizaciones sobre los riesgos asociados con los sistemas de control industrial y cómo protegerlos. Estos programas incluyen talleres, seminarios web y ejercicios de simulación (KASPERSKY ICS, 2020).

Recursos: El equipo ofrece una diversidad de recursos, como pautas, documentos técnicos y estudios de caso, que están diseñados para ayudar a las organizaciones a fortalecer su postura de ciberseguridad. Además, mantienen un repositorio actualizado con información sobre vulnerabilidades conocidas en los ICS, proporcionando una herramienta vital para la prevención y respuesta a incidentes (Lemaire et al., 2014).

Plan de Respuesta a Incidentes: ICS-CERT alienta a las organizaciones a desarrollar un plan de respuesta a incidentes que aborde las necesidades específicas de sus sistemas ICS. Brindan orientación sobre cómo crear un plan y ofrecen plantillas para ayudar a las organizaciones a comenzar (Lemaire et al., 2014).

Comunicación: ICS-CERT enfatiza la importancia de la comunicación entre las organizaciones y sus partes interesadas durante un incidente cibernético. Alientan a las organizaciones a establecer líneas claras de comunicación y a comunicarse regularmente con sus partes interesadas durante todo el proceso de respuesta a incidentes (Rege et al., 2017).

Monitoreo Continuo: El equipo destaca la importancia del monitoreo continuo de los sistemas ICS para detectar posibles amenazas y vulnerabilidades. Recomiendan implementar herramientas de monitoreo y realizar evaluaciones regulares para identificar áreas de mejora (Rege et al., 2017).

Intercambio de información: ICS-CERT promueve el intercambio de información entre las organizaciones para ayudar a prevenir y responder a incidentes cibernéticos. Alientan a las organizaciones a participar en grupos de intercambio de información y a informar los incidentes al equipo (Rege et al., 2017).

Evolución: El equipo reconoce que las amenazas están en constante evolución y alienta a las organizaciones a mantenerse actualizadas con las últimas amenazas y vulnerabilidades que afectan a los sistemas ICS. Proporcionan actualizaciones y alertas regulares para ayudar a las organizaciones a mantenerse informadas (Rege et al., 2017).

En general, ICS-CERT juega un papel crucial en la asistencia a las organizaciones para proteger sus sistemas de control industrial frente a amenazas cibernéticas. Proporcionando asesoramiento experto, recursos y soporte, el equipo ayuda a las organizaciones a prepararse, responder y recuperarse eficazmente de los incidentes cibernéticos.

2.3.20. ICS-CERT enfocado al phishing

En lo que respecta al phishing, ICS-CERT destaca la importancia de la educación y la conciencia de los empleados, así como la implementación de controles técnicos para detectar y prevenir intentos de phishing (ICS-CERT, 2011). A continuación, se presentan algunos puntos clave de ICS-CERT relacionados con el phishing:

Educación y conciencia de los empleados: ICS-CERT enfatiza la importancia de educar a los empleados sobre cómo reconocer e informar intentos de phishing. Esto incluye proporcionar capacitación regular sobre cómo identificar correos electrónicos sospechosos,

comprender los peligros del phishing y promover una cultura de seguridad en la organización (Lanz, 2022).

Implementación de controles técnicos: ICS-CERT recomienda implementar controles técnicos para detectar y prevenir intentos de phishing. Esto incluye el uso de filtros de spam sólidos, la implementación de bloqueo de sistema de nombres de dominio (DNS) y el uso de herramientas avanzadas de protección contra amenazas, como sandboxing y análisis de comportamiento (Galdi et al., 2022).

Monitoreo del tráfico de red: ICS-CERT aconseja monitorear el tráfico de red en busca de señales de actividad de phishing, como intentos de inicio de sesión inusuales, transferencias de datos grandes o cambios inesperados en la configuración del sistema. Las organizaciones también deben monitorear las redes en busca de indicadores conocidos de phishing, como direcciones IP o dominios asociados con ataques de phishing (Mityukov et al., 2019).

Plan de respuesta a incidentes: ICS-CERT destaca la importancia en caso de un ataque de phishing. Este plan debe incluir procedimientos para responder a incidentes de phishing, mitigar los efectos de un ataque, así como, restaurar sistemas y datos (Chen et al., 2019).

Colaboración e intercambio de información: ICS-CERT fomenta la colaboración y el intercambio de información entre las organizaciones, las agencias gubernamentales y las fuerzas del orden para ayudar a combatir las amenazas de phishing. Esto incluye compartir información sobre campañas de phishing conocidas, intentos de phishing sospechosos y lecciones aprendidas de experiencias pasadas (Chen et al., 2019).

Monitoreo continuo: ICS-CERT aboga por el monitoreo continuo de sistemas y redes para mantenerse al día con las nuevas amenazas de phishing. Esto incluye actualizar

regularmente el software y los sistemas, aplicar parches de seguridad, realizar auditorías y evaluaciones de seguridad de manera periódica (Chen et al., 2019).

Segmentación: ICS-CERT sugiere la segmentación de redes y la limitación del acceso a áreas sensibles para minimizar el impacto de un ataque de phishing exitoso. Esto incluye implementar políticas de acceso mínimo, restringir el acceso a sistemas y datos sensibles, así como, aislar los activos críticos de Internet público (KASPERSKY ICS, 2020).

Autenticación de dos factores: ICS-CERT recomienda utilizar la autenticación de dos factores (2FA) para agregar más seguridad a los inicios de sesión. Esto dificulta que los atacantes accedan a sistemas y datos incluso si han obtenido credenciales mediante un ataque de phishing (Wardak et al., 2016).

Actualizaciones y parches regulares: ICS-CERT subraya la necesidad de mantener el software y los sistemas al día mediante la aplicación de los más recientes parches y actualizaciones de seguridad. Esta práctica es crucial para remediar vulnerabilidades que son conocidas y que podrían ser objeto de explotación mediante ataques de phishing. Al hacerlo, se refuerza la seguridad y se minimiza el riesgo de intrusión maliciosa (Wardak et al., 2016).

En contraste, ICS-CERT brinda orientación y recursos valiosos para las organizaciones que buscan proteger sus sistemas de control industrial de las amenazas de phishing. Siguiendo estas recomendaciones, las organizaciones pueden reducir su riesgo de ser víctimas de ataques de phishing y proteger mejor su infraestructura crítica.

2.3.21. Porque usar NIST

Para destacar el uso de la metodología NIST se procede a comparar las metodologías para la gestión de incidentes de seguridad y la respuesta de ciberseguridad centrada en phishing de NIST, ISO 27001, CERT, SANS, FIRST, CIS e ICS CERT.

Tabla 1

Comparativa de metodologías para la gestión de incidentes de seguridad y la respuesta de ciberseguridad centrada en phishing

Marco de referencia	Exhaustividad	Guía de implementación	Controles de phishing	Métricas	Adopción de la industria
NIST (He et al., 2022)	Alto	Pasos detallados para el proceso de respuesta a incidentes	Directrices extensas	Modelo de madurez con niveles	Muy alto, especialmente en EE.UU.
ISO 27001 (Malatji, 2023)	Medio	Políticas generales y enfoque de riesgo	Detalles específicos limitados	Auditorías de cumplimiento	Alto a nivel mundial
CERT (Meyer & Métille, 2023)	Medio	Recomendaciones técnicas para la respuesta de incidentes	Algunos consejos de phishing	Ninguno	Moderado
SANS (Shauver, 2021)	Medio	Análisis pericial y procedimientos de respuesta a incidentes	Controles generales de phishing	Ninguno	Moderado
FIRST (Bobbert & Chtepen, 2021)	Bajo	Prácticas recomendadas para la colaboración	Ninguno	Ninguno	Bajo
Controles CIS (Akowuah et al., 2018)	Medio	Define el plan de respuesta a incidentes	Sin detalles de phishing	Métricas de implementación	Moderado
ICS-CERT (Young, 2013)	Bajo	Especializado para incidentes de control industrial	Ninguno	Ninguno	Baja adopción enfocada

Basado en la tabla comparativa, NIST proporciona el marco más completo con orientación detallada de respuesta a incidentes, amplios controles de phishing, métricas de modelos de madurez y alta adopción de la industria, especialmente en EE. UU.

Por otro lado, ISO 27001 se adopta ampliamente a nivel mundial, pero carece de respuesta específica a incidentes y detalles de phishing. Asimismo, los controles CERT, SANS y CIS proporcionan algunas pautas valiosas, pero son menos completos que NIST. Del mismo modo, FIRST, ICS-CERT tiene una menor adopción y un enfoque limitado en el intercambio técnico.

Por lo tanto, NIST Cybersecurity Framework se destaca como la metodología más completa basada en la profundidad de la orientación, las métricas y el uso en la industria, para la gestión de incidentes de seguridad y la respuesta de ciberseguridad centrada en phishing.

2.3.22. NIST 800-61

Las guías NIST detallan cómo deben ser estructuradas las políticas y los planes de respuesta a incidentes en las organizaciones, abarcando aspectos como la estructura organizacional, el personal y los servicios de los equipos encargados de la respuesta. Un documento clave, el NIST SP 800-61, ofrece un enfoque exhaustivo para la gestión de incidentes de seguridad informática, proveyendo directrices específicas para analizar datos de incidentes y determinar respuestas apropiadas. Esta guía se desglosa en seis fases esenciales: Preparación, Detección y Análisis, Contención, Erradicación, Recuperación y Actividad Post-Incidente.

Las prácticas recomendadas basadas en el NIST SP 800-61 incluyen establecer una capacidad efectiva de respuesta a incidentes, desarrollar un plan y procedimientos detallados para manejar incidentes de seguridad, desde la detección y notificación hasta la respuesta efectiva. Estos procedimientos deben asegurar la contención inmediata del incidente para prevenir su expansión, eliminar las causas subyacentes del incidente, y restaurar los sistemas y redes afectados a su funcionamiento normal. Asimismo, es vital verificar que los sistemas estén operando correctamente y que los datos no se hayan perdido ni corrompido, utilizando el

proceso de lecciones aprendidas para mejorar continuamente en la gestión de futuros incidentes.

La guía del NIST establece las cuatro (4) fases en la gestión de incidentes:

Figura 3 Fases de la gestión de incidentes, según la guía NIST 800-61

2.3.23. Tipos de incidentes

NIST SP 800-61 puede utilizarse para responder a varios tipos de incidentes en seguridad informática. Algunos ejemplos de incidentes a los que la guía puede utilizarse para responder incluyen:

- **Infecciones por malware:** Cuando un sistema o red se infecta con malware, la guía proporciona directrices para detectar y analizar el malware, contener su propagación, erradicarlo de los sistemas afectados y recuperar los sistemas a su estado normal.

- **Acceso no autorizado**: En caso de acceso no autorizado a sistemas o redes, la guía ayuda a detectar y analizar el acceso no autorizado, contener el acceso, eliminar a los usuarios no autorizados y restaurar los sistemas afectados a un estado seguro.
- **Violación de datos:** Cuando se produce una violación de datos, la guía proporciona orientación sobre la detección y el análisis de la violación, la contención para evitar una mayor pérdida de datos, la erradicación de la causa de la violación, la recuperación de los datos comprometidos y la aplicación de medidas para prevenir futuras violaciones.
- **Ataques de denegación de servicio:** En caso de ataque de denegación de servicio, la guía ayuda a detectar y analizar el ataque, contener el impacto del ataque, erradicar la causa del ataque, recuperar los sistemas o servicios afectados e implantar medidas para mitigar futuros ataques.
- **Amenazas internas:** Cuando un intruso supone una amenaza para la seguridad de los sistemas o redes, la guía proporciona directrices para detectar y analizar la amenaza interna, contener la amenaza, eliminar el acceso del intruso e implantar medidas para prevenir futuras amenazas internas.

Estos son sólo algunos ejemplos de incidentes a los que se puede responder con la NIST SP 800-61. La guía proporciona un marco completo para la gestión de incidentes y puede aplicarse a una amplia gama de incidentes de seguridad.

2.3.24. Puntos clave de la NIST SP 800-61

Las organizaciones deben establecer una capacidad formal de respuesta a incidentes con políticas, planes, procedimientos definidos y personal adecuado. Esto incluye la designación de puntos de contacto para notificar incidentes interna y externamente.

Una respuesta eficaz a los incidentes de seguridad implica abordar integralmente el ciclo de vida completo de la gestión de incidentes, que incluye la preparación, detección y análisis, contención, erradicación, recuperación, y las actividades posteriores al incidente. Este

enfoque holístico asegura que cada fase del proceso sea ejecutada meticulosamente para mitigar el impacto y fortalecer la resiliencia de la organización frente a futuras amenazas.

Las organizaciones deben centrar sus capacidades de respuesta a incidentes en los vectores de ataque más comunes, como el malware, los ataques web, las amenazas internas y la pérdida de equipos. Las estrategias de respuesta deben variar en función del tipo de ataque.

La detección y el análisis se basan en la detección de precursores e indicadores procedentes de fuentes como software antivirus, registros y sistemas de detección de intrusiones. El análisis rápido y la priorización son fundamentales.

Las estrategias de contención, como la desconexión de los sistemas afectados, tratan de limitar los daños. La recopilación y el tratamiento de las pruebas deben servir de apoyo a posibles acciones legales.

La erradicación elimina el malware y refuerza los sistemas. La recuperación restaura los sistemas y servicios. Las lecciones aprendidas deben identificar mejoras en los controles, herramientas y procesos de seguridad.

La coordinación y el intercambio de información con los socios pueden mejorar la respuesta a los incidentes. Esto debe equilibrar la apertura con la protección de los datos sensibles.

2.3.25. Estructura y modelos de dotación personal

Analiza diferentes modelos como equipos centrales, distribuidos y de coordinación. Ofrece recomendaciones sobre las competencias necesarias, la interacción con otros grupos, el recurso a la subcontratación, etc.

2.3.26. Comunicaciones e intercambio de información

Se ofrecen amplias orientaciones sobre la coordinación y el intercambio de información con diversas partes internas y externas. Abarca qué, cuándo y cómo comunicar con eficacia.

2.3.27. Notificación de incidentes

La guía recomienda recopilar elementos de datos específicos sobre incidentes y mantener una documentación detallada. Analiza los requisitos de notificación para las agencias federales.

2.3.28. Gestión de distintos tipos de incidentes

Aunque proporciona orientaciones generales aplicables a cualquier incidente, la guía ofrece consejos específicos para responder a vectores de ataque comunes como el malware, la denegación de servicio y el acceso no autorizado.

2.3.29. Métricas y mejora

La NIST ofrece sugerencias para medir la eficacia de los programas de respuesta a incidentes. Esto incluye medidas objetivas como el tiempo por incidente, así como evaluaciones subjetivas de la calidad de la respuesta.

2.3.30. Preparación

Se ofrecen recomendaciones sobre actividades de preparación como la adquisición de herramientas, la formación del personal, el desarrollo de procedimientos y la prevención de incidentes mediante controles de seguridad.

2.3.31. Directrices clave de NIST para la gestión de incidentes de Phishing (ejecutadas en Audetic)

Preparación

La empresa, a pesar de tener solo 10 empleados, ha establecido un equipo y un plan de respuesta a incidentes de seguridad. Se ha capacitado a los usuarios para que estén alerta y reporten correos sospechosos. Además, se han implementado controles de seguridad en el correo electrónico, como filtros antispam y antivirus, para mitigar el riesgo de phishing.

Detección

En este caso, un usuario de la empresa detecta un correo electrónico sospechoso en el que se le

solicita restablecer su contraseña a través de un enlace. El analista de seguridad revisa las cabeceras del correo electrónico y logra identificar los indicadores típicos de un ataque de phishing.

Análisis

Tras clasificar el incidente como un ataque de phishing por correo electrónico, se realiza un análisis exhaustivo de los registros. Se descubre que el correo sospechoso fue recibido por 10 usuarios de la empresa. Además, se confirma que el sitio web vinculado es fraudulento, aunque aún no ha sido visitado por ningún usuario.

Contención

Para contener el incidente, se actualizan los controles de seguridad del correo electrónico para bloquear al remitente del correo de phishing y detectar futuros correos similares. Asimismo, se bloquea el acceso al sitio web fraudulento en la red de la empresa.

Erradicación

Como medida de precaución, se restablecen las contraseñas de las cuentas de usuario afectadas para evitar accesos no autorizados. Además, se contacta directamente a los 10 usuarios que recibieron el correo de phishing para brindarles formación sobre cómo identificar y evitar este tipo de ataques.

Recuperación

Una vez que se han restablecido las contraseñas de los usuarios y se han actualizado los controles del correo electrónico, las operaciones vuelven a la normalidad. Sin embargo, se programará una formación adicional para concienciar aún más a los usuarios sobre la importancia de prevenir el phishing en el futuro.

Lecciones aprendidas

El equipo de seguridad se reúne para analizar y debatir formas de mejorar la formación de los usuarios y considerar la implementación de la autenticación de correo electrónico DMARC para detectar mejor los dominios falsos en los correos de phishing.

Coordinación

Los indicadores del ataque de phishing se comparten con el Centro de intercambio y análisis de información (ISAC) del sector y el Equipo de respuesta a emergencias informáticas de Estados Unidos (US-CERT) para mejorar las capacidades de detección en el sector. Dado que no se expuso información personal identificable, no es necesario notificar al cliente.

Pasos para la aplicación de las directrices de NIST para un incidente de Phishing

Detección

- El usuario detecta el correo electrónico de phishing y lo notifica siguiendo los procedimientos establecidos en la organización.
- El analista de seguridad revisa el correo electrónico notificado siguiendo los procedimientos de clasificación de incidentes de correo electrónico.
- El analista identifica los indicadores de compromiso según las directrices de identificación de phishing.
- El incidente se clasifica como un ataque por correo electrónico según la matriz de categorías de incidentes.
- El analista registra el incidente en el sistema de seguimiento como "Confirmado" según el procedimiento de documentación de incidentes.

Análisis

- El ingeniero de seguridad realiza un análisis exhaustivo de los registros de correo electrónico utilizando herramientas aprobadas.
- Se determina que el incidente afectó a 10 usuarios basándose en los detalles del remitente.

- El analista de malware accede al sitio web fraudulento siguiendo los procedimientos de navegación segura.
- Se confirma que el sitio web fraudulento recopila credenciales de usuario.
- El incidente se evalúa con la máxima prioridad según las directrices actuales de evaluación de impacto.

Contención

- El equipo de seguridad del correo actualiza los filtros de spam para bloquear al remitente del phishing según los procedimientos establecidos.
- El equipo de red bloquea la dirección IP del sitio web fraudulento en el cortafuegos según los procedimientos de bloqueo de sitios web.

Erradicación

- El servicio de asistencia restablece las contraseñas de los usuarios afectados siguiendo los procedimientos de respuesta al robo de identidad.
- El equipo de concienciación ensecurity informa a los usuarios afectados sobre la amenaza de phishing según las directrices de notificación a usuarios.

Recuperación

- El ingeniero de seguridad verifica que los controles del correo electrónico y el bloqueo del cortafuegos se hayan implementado correctamente, siguiendo los procedimientos de verificación establecidos.
- El incidente se documenta como resuelto en el sistema de seguimiento, siguiendo el procedimiento de cambio de estado.

Esto demuestra cómo seguir los procedimientos de respuesta a incidentes definidos en cada etapa permite una gestión eficaz y coherente, basada en las directrices del NIST.

2.3.32. Análisis de la NIST SP 800-61

El National Institute of Standards and Technology (NIST) es ampliamente reconocido a nivel mundial por su labor en la creación de estándares para diversas tecnologías. El desarrollo de estos estándares y directrices es responsabilidad del Information Technology Laboratory (ITL) de NIST.

Dentro del ámbito de la gestión de incidentes de ciberseguridad, NIST ha establecido el estándar conocido como NIST Special Publication 800-61, el cual representa una guía de mejores prácticas diseñada para asistir a las organizaciones en la mejora de su capacidad para responder eficientemente a incidentes de ciberseguridad. La primera versión de este estándar fue desarrollada en colaboración con el Federal Information Security Management Act (FISMA) en el año 2002. La versión actual, denominada revisión 2, se publicó en el año 2012.

El propósito principal es proporcionar orientación a las organizaciones en el establecimiento de las medidas de seguridad informática necesarias para mejorar su capacidad de respuesta ante incidentes y gestionarlos de manera eficiente. Además, la guía ofrece directrices específicas para la gestión de incidentes, especialmente en lo que respecta al análisis de datos y la determinación de la respuesta adecuada para cada tipo de incidente. Es importante destacar que estas directrices pueden ser aplicadas de forma independiente, adaptándose a la plataforma de hardware, sistema operativo, protocolos o aplicaciones utilizadas por cada organización.

2.3.33. Organizar la capacidad de respuesta

El establecimiento de una capacidad efectiva de respuesta a incidentes de seguridad informática (CSIRC) implica una serie de decisiones y acciones clave. Fundamentalmente, es crucial definir con precisión el término "incidente" para que todos los involucrados comprendan claramente su alcance. La organización debe identificar los servicios que el equipo

de respuesta a incidentes proporcionará y evaluar las posibles estructuras y modelos de equipos adecuados para ofrecer dichos servicios.

Posteriormente, se procede a la selección e implementación de uno o más equipos de respuesta. La formulación de planes, políticas y procedimientos específicos para la respuesta a incidentes es vital para configurar un equipo competente. Estos documentos deben asegurar que las acciones de respuesta sean efectivas, eficientes y coherentes, además de garantizar que el equipo esté adecuadamente capacitado para realizar sus funciones.

Además, es esencial que los planes y políticas establezcan claramente cómo el equipo interactuará con otros equipos internos de la organización, así como con entidades externas, incluidas las fuerzas del orden, los medios de comunicación y otras organizaciones de respuesta a incidentes, asegurando una colaboración efectiva y coordinada.

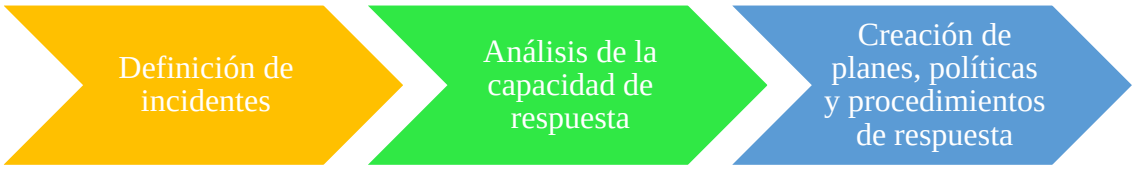

Figura 4 Organización de la capacidad de respuesta, según la guía NIST SP 800-61

2.3.34. Términos de referencia

El estándar establece los siguientes conceptos fundamentales:

Evento: Se define como cualquier hecho observable en un sistema o red.

Algunos ejemplos de eventos se detallan a continuación:

- Un usuario que se conecta a un servidor de archivos.
- Un servidor que recibe solicitudes (requests) desde un navegador para acceder a un sitio web.
- El acto de un usuario enviando un correo electrónico.
- Un firewall que bloquea un intento de conexión.

En contraste, se define como "Evento adverso" a aquel que conlleva consecuencias negativas, tales como:

- Caídas de sistemas.
- Uso no autorizado de privilegios del sistema.
- Acceso no autorizado a información confidencial.
- Ejecución de malware.

Es importante destacar que eventos naturales y fallos de energía quedan excluidos de esta categorización.

Por otro lado, se considera un "Incidente de seguridad computacional" como una violación de las políticas de seguridad o las prácticas de seguridad, o bien como una amenaza inminente de tal violación.

Ejemplos de incidentes de seguridad pueden incluir:

- Un ataque en el cual un atacante ordena a una botnet enviar un gran volumen de solicitudes de conexión a un servidor web, lo que provoca su bloqueo.
- La ejecución de un engaño a los usuarios, persuadiéndolos para que abran un correo electrónico que aparenta ser un "informe trimestral", pero que en realidad contiene malware. La ejecución de esta herramienta resulta en la infección del computador y el establecimiento de conexiones con un host externo.
- Un atacante que accede a datos confidenciales y amenaza con divulgar públicamente dicha información si la organización no paga una suma de dinero determinada.
- Un usuario que proporciona o expone información confidencial a través de servicios de intercambio de archivos.

2.3.35. Necesidad de la respuesta a incidentes

Está se ha convertido en una práctica fundamental debido a la frecuencia con la que los ataques comprometen datos personales y empresariales. Para abordar esta problemática de manera efectiva y rápida, es esencial contar con una capacidad de respuesta sólida.

Una de las principales ventajas de establecer una capacidad de respuesta a incidentes es la posibilidad de manejar estos eventos de forma sistemática, utilizando una metodología de gestión de incidentes coherente y bien estructurada. Este enfoque asegura que se adopten las medidas apropiadas para cada situación específica. La respuesta a incidentes juega un papel esencial en ayudar al personal a minimizar la pérdida o el robo de información y a reducir la interrupción de los servicios que pueden resultar de tales incidentes.

Además, esta práctica brinda la oportunidad de aprender de cada evento gestionado, utilizando la información recabada para prepararse mejor para futuras contingencias y, en última instancia, fortalecer la protección de los sistemas y datos de la organización.

2.4.Marco documental de respuesta a incidentes

Desempeña un papel crucial en el respaldo de las acciones, la capacitación y la difusión de los pasos a seguir ante una variedad de situaciones de incidentes, así como en la definición de los lineamientos empresariales para este proceso. Cuatro aspectos clave deben ser considerados al respecto:

1. **Políticas:** Establecer políticas claras que guíen la respuesta a incidentes y proporcionen un marco de referencia sólido.
2. **Planes:** Desarrollar planes detallados que describan cómo se abordarán los incidentes específicos, incluyendo los procedimientos y recursos necesarios.
3. **Procedimientos:** Definir procedimientos precisos que detallen los pasos a seguir en cada etapa de la respuesta a incidentes, desde la detección hasta la resolución.

4. **Comunicaciones:** Establecer directrices para las comunicaciones con organizaciones externas o terceros, garantizando una coordinación efectiva en situaciones de incidentes.

2.4.1. Políticas

Las políticas de seguridad informática varían según la organización, pero la mayoría comparten elementos clave. Estos elementos suelen incluir:

1. **Declaración de compromiso de la dirección:** En esta declaración, la dirección de la organización muestra su compromiso con la seguridad informática.
2. **Finalidad y objetivos de la política:** Se establecen los objetivos y propósitos que la política busca lograr.
3. **Alcance de la política:** Se aclara a quiénes y en qué circunstancias se aplica la política.
4. **Definición de incidentes de seguridad informática y términos relacionados:** Se proporciona una definición clara de lo que se considera un incidente de seguridad y otras técnicas relacionadas.
5. **Estructura organizativa y definición de funciones, responsabilidades y niveles de autoridad**: Se detalla cómo se organiza la respuesta a incidentes en la estructura de la organización y se establecen las funciones, responsabilidades y niveles de autoridad correspondientes.
6. **Priorización o clasificación de la gravedad de los incidentes:** Se establece un sistema para priorizar y clasificar los incidentes en función de su gravedad.
7. **Métricas para el rendimiento:** Se definen las métricas que se utilizarán para evaluar el rendimiento en la gestión de incidentes de seguridad.
8. **Formularios de notificación y contacto:** Se proporcionan formularios y detalles de contacto para notificar y comunicarse sobre incidentes de seguridad.

Estos elementos son fundamentales para garantizar que la política de seguridad informática sea efectiva y aplicable en la organización.

2.4.2. Planes

Para asegurar una respuesta efectiva a los incidentes, es crucial que las organizaciones adopten un enfoque formal, enfocado y coordinado. Esto incluye el desarrollo de un plan de respuesta a incidentes que actúe como guía para implementar adecuadamente las capacidades de reacción ante tales eventos. Cada organización debe crear un plan que se ajuste a sus necesidades específicas, las cuales pueden diferir según su misión, tamaño, estructura y funciones. Dicho plan debe definir claramente los recursos necesarios para la gestión de incidentes y contar con el respaldo y la aprobación de la alta dirección, garantizando así un compromiso organizacional completo para su ejecución efectiva.

Una vez que se haya desarrollado el plan y se haya obtenido la aprobación de la dirección, es fundamental ponerlo en práctica y revisarlo de manera regular, al menos una vez al año. Esta revisión garantiza que la organización siga la hoja de ruta establecida en el plan, lo que permite madurar su capacidad de respuesta y alcanzar los objetivos definidos para la gestión de incidentes.

2.4.3. Procedimientos

Los documentos cruciales son aquellos que delinean los pasos técnicos necesarios para abordar estas situaciones. Estos documentos, conocidos como "Procedimientos Operativos Estándar" (SOPs), se fundamentan en las políticas y planes previamente establecidos.

Los SOPs representan un conjunto de procesos técnicos específicos, técnicas, listas de verificación y formularios diseñados para ser utilizados por el equipo de respuesta ante incidentes. Es esencial que estos procedimientos sean lo suficientemente minuciosos y detallados para garantizar que se reflejen las prioridades comerciales en la ejecución.

Una práctica fundamental es someter los SOPs a pruebas antes de su implementación y posteriormente distribuirlos entre los miembros de los equipos pertinentes. Un ejemplo de SOP ampliamente utilizado son los denominados "Playbooks" de respuesta a incidentes de

ciberseguridad, los cuales establecen los flujos de trabajo a seguir en diversas situaciones de amenaza. Estos documentos son esenciales para una respuesta organizada y eficaz ante incidentes de ciberseguridad.

2.4.4. Comunicación con terceros o externos

La comunicación con terceros o entidades externas representa una parte integral de la respuesta a incidentes en muchas organizaciones. Estos intercambios pueden involucrar:

1. **Contacto con las fuerzas del orden:** En situaciones en las que se requiere asistencia legal o intervención de las autoridades.
2. **Respuesta a preguntas de los medios de comunicación:** Para proporcionar información precisa y gestionar la percepción pública del incidente.
3. **Búsqueda de expertos externos:** Cuando se necesita experiencia adicional para abordar el incidente de manera efectiva.

Además, es importante destacar la comunicación con otras partes interesadas, como:

1. **Proveedores de servicios de Internet (ISP):** Para colaborar en la identificación y mitigación de amenazas.
2. **Proveedor del software vulnerable u otros equipos de respuesta a incidentes:** Para coordinar esfuerzos y compartir información relevante.

En estos casos, las comunicaciones con entidades externas pueden incluir:

1. **Contacto con la Ley:** Cuando es necesario informar o colaborar con las autoridades legales.
2. **Responder a consultas de los medios:** Para mantener una comunicación transparente y precisa con la prensa.
3. **Búsqueda de experiencia externa:** Cuando se requiere asesoramiento o conocimientos adicionales para manejar la situación de manera efectiva.

2.4.5. Entidades que se comunican con el equipo de respuesta a incidentes

Las entidades interesadas en interactuar con el equipo de respuesta a incidentes pueden jugar un papel fundamental en el perfeccionamiento de la detección y análisis de incidentes al tomar la iniciativa de compartir información pertinente sobre indicadores de incidentes. Esta colaboración proactiva es esencial para enriquecer la comprensión y la capacidad de respuesta del equipo frente a posibles amenazas, mejorando así las estrategias de seguridad de la organización.

Sin embargo, antes de que ocurra un incidente, es esencial que el equipo de respuesta a incidentes mantenga discusiones con otros departamentos clave de la organización, como la oficina de asuntos públicos y el departamento legal, así como la dirección de la empresa. Esto es necesario para establecer políticas y procedimientos con respecto al intercambio de información.

Esta precaución es vital, ya que compartir información sensible relacionada con incidentes sin una política adecuada podría exponerla a partes no autorizadas, lo que podría agravar los problemas y ocasionar pérdidas financieras adicionales.

Para garantizar la responsabilidad y la integridad de las comunicaciones con partes externas, el equipo de respuesta a incidentes debe documentar exhaustivamente todos los contactos y comunicaciones. Esto no solo respalda la toma de decisiones informadas, sino que también proporciona pruebas sólidas en caso de futuras investigaciones o revisiones.

Figura 5 Entidades involucradas en la comunicación con el equipo de respuestas a incidentes, según la guía NIST SP 800 – 61

2.4.6. Medios de comunicación

Se deben llevar a cabo sesiones de entrenamiento en interacción con los medios, conocidas como "media training", en relación con la gestión de incidentes. Estas sesiones de formación deben abordar varios aspectos clave:

- **La importancia de la confidencialidad:** Es fundamental subrayar la importancia de no revelar información sensible, especialmente los detalles técnicos de las contramedidas, ya que dicha información podría resultar valiosa para potenciales atacantes. Mantener esta discreción es crucial para evitar que los métodos de defensa de una organización sean comprometidos y explotados por terceros con intenciones maliciosas.

- **Comunicación eficaz:** Es igualmente crucial resaltar los beneficios de comunicar información importante al público de manera completa y efectiva. Al hacerlo, se asegura que la organización mantenga un nivel adecuado de transparencia y que el público permanezca bien informado durante situaciones de incidentes. Esta práctica contribuye a fortalecer la confianza entre la entidad y sus stakeholders, facilitando una gestión de crisis más efectiva y abierta.

2.4.7. Definición de procedimientos

Se deben definir procedimientos con el propósito de informar a los contactos de los medios de comunicación acerca de los temas y sensibilidades específicas relacionados con un incidente particular antes de entablar cualquier conversación con los medios de comunicación.

Por otro lado, es importante establecer un "Single Point of Contact" (SPOC) y mantener comunicaciones actualizadas de forma constante. Esto implica la necesidad de mantener actualizada una declaración sobre el estado del incidente para asegurar que las comunicaciones con los medios de comunicación sean coherentes y contemporáneas. Mantener informado al público de manera precisa y consistente es esencial para gestionar la percepción y la respuesta pública durante y después del incidente.

2.4.8. Herramientas open source utilizadas para la automatización de gestión de incidentes de seguridad.

El aumento de los ciberataques es un fenómeno que preocupa a empresas y organizaciones en todo el mundo. Según la clasificación de los 10 principales riesgos de 2020 en términos de probabilidad e impacto, los ciberataques se encuentran en el séptimo y octavo lugar respectivamente (Siddiqi et al., 2022). Esta situación se ha vuelto más alarmante debido al brote de COVID-19, que ha llevado a una transformación digital masiva y a una mayor superficie de ataque para los atacantes. Los incidentes de ciberseguridad pueden tener graves

consecuencias para las empresas, incluyendo pérdidas financieras, pérdida de productividad, daños a la reputación, responsabilidad legal y problemas de continuidad del negocio.

Entre las diversas formas de ciberataques, la ingeniería social es una de las más peligrosas. Se trata de la manipulación psicológica de las personas para que realicen acciones o divulguen información confidencial (Zimba et al., 2022). La ingeniería social no depende de las medidas tecnológicas utilizadas por una organización para proteger sus activos, sino que se basa en el error humano. Como señalan Montañez et al., (2020) la seguridad no solo depende de la tecnología, sino también de la psicología de las personas.

La ingeniería social puede tomar muchas formas, como el phishing, el spoofing o la manipulación de sitios web. En el phishing, los atacantes envían correos o mensajes de texto que parecen ser de una fuente confiable, pero que en realidad buscan obtener información confidencial o hacer que la víctima revele información importante. Por otro lado, el spoofing se refiere a la práctica de hacer que un sitio web o un servidor parezca auténtico, cuando en realidad no lo es. Por último, la manipulación de sitios web se refiere a la alteración de sitios web legítimos para que aparezcan como si fueran falsos, con el fin de obtener información confidencial o realizar acciones maliciosas (Blancaflor et al., 2021).

La ingeniería social, en términos generales, se refiere a una amplia categoría de ataques que buscan explotar la vulnerabilidad humana en el ámbito digital. Entre ellos, el phishing es una de las técnicas más comunes y conocidas. Consiste en que un atacante engaña a una víctima para que realice acciones que permitan a este acceder al dispositivo, cuenta o información personal de la víctima, generalmente haciéndose pasar por una persona u organización en la que la víctima confía (Rege & Bleiman, 2021).

Aunque existen diversas formas de ejecutar un ataque de phishing, la mayoría de las veces se presenta en la forma de un correo electrónico que intenta convenir a la víctima de hacer clic en un enlace malicioso o descargar un archivo adjunto dañino. Sin embargo, algunos

correos electrónicos de phishing pueden ser fácilmente identificables por un usuario experimentado, mientras que otros pueden resultar más difíciles de detectar (Williams et al., 2022).

El incremento en el número de ciberataques ha llevado a un problema significativo para los Centros de Operaciones de Seguridad (SOC), CERT y SIRT: la gran cantidad de alertas que requieren su atención. No obstante, solamente un pequeño porcentaje de estas alertas son precisas, mientras que el resto son falsos positivos, lo que representa una inmensa pérdida de esfuerzo para los analistas que deben realizar acciones manuales para filtrarlos (Williams et al., 2022).

Este problema es una consecuencia inmediata de la falta de automatización en el SOC, que es fundamental para una efectiva gestión de incidentes de seguridad. La automatización puede aplicarse en el análisis de alertas relacionadas con posibles correos electrónicos de phishing, lo cual puede ayudar a reducir drásticamente el tiempo de análisis y facilitar el trabajo del analista (Williams et al., 2022). En este sentido, la automatización parcial o total del análisis de correos electrónicos puede constituir una solución clave para mejorar la eficiencia del SOC y garantizar una mayor seguridad informática.

2.4.9. MxToolbox

Es una plataforma que ofrece herramientas de diagnóstico y búsqueda de red gratuitas, rápidas y precisas para soportar las operaciones globales en Internet (Nikolaos & Andreas, 2016). Entre sus recursos, se encuentran herramientas útiles para analizar correos electrónicos, como el Analizador de cabeceras de correo electrónico y el Analizador de spam.

El Analizador de cabeceras de correo electrónico permite enviar el encabezado de un correo electrónico para obtenerlo en un formato legible por humanos, destacando posibles problemas, como una autenticación DMARC fallida (Mustafa et al., 2021). Por otro lado, el Analizador de spam permite enviar un correo electrónico completo (cabecera y cuerpo) y

analizarlo utilizando el software SpamAssassin (R. Zhang et al., 2021), un filtro de correo electrónico inteligente que utiliza diversas pruebas para identificar los mensajes de spam.

SpamAssassin aplica pruebas tanto a la cabecera como al contenido del correo electrónico para clasificarlo mediante métodos estadísticos avanzados. La herramienta devuelve una puntuación de spam basada en la probabilidad de que el correo electrónico sea considerado como spam (Riadi et al., 2022).

2.4.10. Email Analyzer

Esta herramienta es un programa de línea de comandos de código abierto, desarrollado en Python y accesible a través de GitHub. Está diseñada para extraer información como direcciones de correo electrónico, direcciones IP, URL y archivos adjuntos a partir de correos electrónicos suministrados en formatos EML o MSG. Su funcionalidad permite a los usuarios procesar y obtener datos relevantes de manera eficiente y efectiva (Augier et al., 2018). Soporta la expansión de URLs acortadas y también permite escanear URLs y hashes de archivos adjuntos con VirusTotal (Arsenovic et al., 2022). Además, permite el uso de una lista blanca a través de un archivo de configuración que acepta expresiones regulares. Al final del análisis, esta herramienta crea la carpeta extracted-attachments, que contiene los archivos adjuntos encontrados en el correo electrónico, así como diferentes archivos que contienen:

- las direcciones de correo electrónico extraídas (es decir, emails.txt)
- las direcciones IP extraídas (es decir, ips.txt)
- las URL extraídas (es decir, urls.txt)
- las líneas recibidas (received.txt)

Si se utiliza la opción de línea de comandos -vt, la herramienta analizará con VirusTotal las URL que se encuentran en el archivo urls.txt y los archivos que se encuentran en la carpeta extracted-attachments. Si se encuentra un archivo malicioso, se le cambiará el nombre añadiéndole la palabra _malware al final, mientras que, si se encuentra una URL maliciosa, se

añadirá a un archivo llamado malware_urls.txt. Obviamente, se necesita una clave API de VirusTotal para utilizar esta función. Sin embargo, se ha observado que la extracción de los observables que realiza mediante el uso de expresiones regulares no es 100% precisa. Por ejemplo, esas expresiones regulares pueden fallar y extraer URL que terminen con una etiqueta HTML, o líneas de encabezado erróneas (por ejemplo, Received-SPF entre las Received). Además, las líneas de cabecera Message-ID del correo electrónico también pueden confundirse con las direcciones de correo electrónico (Johnson et al., 2018).

2.4.11. Sooty

Es una herramienta de línea de comandos de código abierto escrita en Python que está disponible en GitHub. Su objetivo es ayudar a los analistas SOC a automatizar parte de su flujo de trabajo. Uno de los objetivos de Sooty es realizar el mayor número posible de comprobaciones rutinarias, lo que permite al analista dedicar más tiempo a análisis más profundos en el mismo plazo (Zimon et al., 2022). Ofrece las siguientes características que permiten:

- transformar una URL de forma que impida que un usuario haga clic en ella por error. Esto es especialmente útil cuando se trata de URL maliciosas.
- elegir una de las muchas transformaciones diferentes para las URL o cadenas, como la descodificación de URL o la descodificación base64).
- realizar comprobaciones de reputación para direcciones IP, direcciones de correo electrónico o URLs en VirusTotal, AbuseIPDB [12] y nodos de salida de Tor
- realizar búsquedas DNS, DNS inverso y WHOIS.
- generar un hash para una cadena o un texto y comprobar su actividad maliciosa conocida en VirusTotal.
- extraer direcciones IP, direcciones de correo electrónico, URLs y algunas líneas básicas de cabecera de un correo electrónico proporcionado en formato de archivo MSG (EML

no está soportado actualmente). A continuación, puede comprobar automáticamente las direcciones de correo electrónico en emailrep.io (Kianersi et al., 2022) en busca de actividad maliciosa conocida y también en HaveIBeenPwned (Koltun & Hafner, 2021) para ver si esas direcciones están incluidas en una filtración de datos anterior. Además, permite enviar URL a PhishTank (Abbas et al., 2022) para comprobar si están relacionadas con el phishing. Por último, es posible crear una plantilla de respuesta dinámica basada en el resultado del análisis del correo electrónico.

- Obtener un informe de reputación de urlscan.io (StrangeBee, 2022) para una URL.

Obviamente, la mayoría de las herramientas externas utilizadas para analizar la información proporcionada por el analista requieren una clave API. Se debe tener en cuenta que la herramienta busca esas piezas de información sólo dentro del cuerpo del correo electrónico, ignorando las líneas de cabecera. Además, no extrae todas las líneas de cabecera, sino sólo las que suele mostrar la aplicación cliente de correo. La única dirección de correo que se analiza automáticamente es la que se encuentra en el campo "De" del mensaje. El resto de la información que debe analizarse debe proporcionarse manualmente a la herramienta.

2.4.12. IsThisLegit

Es una herramienta de código abierto disponible en GitHub (Franchina et al., 2021). Facilita la recepción, el análisis y la respuesta a los informes de phishing y consta de dos partes:

- **Dashboard:** una aplicación de Google App Engine y es la ventana del analista a los informes de phishing de la organización. Los analistas pueden utilizar el panel para ver, clasificar y responder a los correos de phishing.
- **Extensión de Chrome:** un botón de la aplicación Gmail que facilita a los usuarios la notificación de correos de phishing al panel.

Una vez que se envía un correo electrónico, se muestra un informe en una tabla en la página inicial del panel de control. Un analista puede ver un informe concreto y realizar las siguientes acciones:

- Clasificar el informe como "Benigno", "Malicioso" o "Pendiente".
- Responder al usuario que ha enviado el informe.
- Obtener una visión general sobre el informe, que incluye información como la persona que envió el informe, la hora a la que se envió y el estado actual. También contiene una línea de tiempo, que rastrea cualquier cambio en el informe.
- Ver la lista de todos los campos de cabecera del correo electrónico.
- Ver el contenido de texto y HTML del correo electrónico.

También es posible crear reglas que comprueben la coincidencia con un nuevo envío de phishing y realicen una acción sí coinciden. Estas reglas pueden coincidir con los campos del encabezado o con el contenido del cuerpo. Las acciones son breves fragmentos de código Python que el analista puede codificar a voluntad. Por ejemplo, una regla puede utilizarse para clasificar automáticamente un informe si coincide con esa regla. Así, utilizando esta herramienta un analista puede gestionar los informes de forma sencilla y educada, pero tiene que escribir fragmentos de código Python que permitan automatizar parte del análisis, de lo contrario tiene que analizar todas las piezas de información manualmente.

2.4.13. Inteligencia sobre ciber amenazas

Para analizar un correo electrónico, es importante extraer muchas piezas de información, como direcciones IP, direcciones de correo electrónico, dominios y URL, y analizarlas una a una. A partir de ahora, el término que se utilizará para referirse a dicha información es el de observable. Un observable se define como un evento (benigno o malicioso) en una red, o en un sistema (Osliak et al., 2019). Este evento puede ser, por ejemplo, el avistamiento de una dirección IP específica que podría requerir un análisis más profundo si

se considera maliciosa. Si un observable está relacionado con una actividad maliciosa, se denomina Indicador de Compromiso (IoC). Un IoC se define como un artefacto que, con un alto nivel de confianza, indica una intrusión informática (X. Zhang & Chow, 2018). En el caso del análisis del correo electrónico, los IoC pueden ser direcciones IP, direcciones de correo electrónico, dominios, URLs consideradas relacionadas con actividades de phishing o spam, y archivos adjuntos peligrosos. Para averiguar si un observable es malicioso, un analista puede utilizar herramientas en línea como VirusTotal para analizar una URL o un archivo o cotejar una dirección IP o un dominio con una lista de bloqueo. Además, puede utilizar servicios de sandbox para ejecutar un archivo ejecutable (por ejemplo, un archivo adjunto de correo electrónico) en un entorno automatizado, virtualizado y seguro para observar su comportamiento y obtener IoC adicionales. Una vez que los IoC se identifican a través de un proceso de respuesta a incidentes e informática forense, estos pueden ser empleados para la detección precoz de futuros intentos de ataque. Esto se logra mediante la integración de los IoC en sistemas de detección de intrusiones y software antivirus, lo cual permite a las organizaciones anticiparse y responder más eficazmente a las amenazas potenciales, fortaleciendo así sus defensas cibernéticas.

Aunque los IoCs encontrados dentro de una organización pueden ser útiles para prevenir futuros ataques similares, no son suficientes para prevenir ataques que están actualmente en la red y nunca han tenido como objetivo la organización. Además, los IoC por sí solos no son capaces de identificar quién está detrás de un ataque, sus motivaciones o el patrocinador final del propio ataque (Sun et al., 2022). Si una organización dispusiera de esta información, podría tomar decisiones importantes que van mucho más allá de la simple adición de una regla en un cortafuegos. Lo que se necesita es el concepto de Inteligencia sobre Ciberamenazas (CTI). Gartner describe la CTI como un conocimiento que se fundamenta en evidencias y que abarca el contexto, mecanismos, indicadores, consecuencias y

recomendaciones prácticas acerca de una amenaza actual o potencial contra los activos. Este conocimiento es crucial pues permite a las entidades tomar decisiones informadas sobre cómo responder adecuadamente a dichas amenazas o riesgos (Rastogi et al., 2022). CTI no son sólo los datos en bruto o el único IoC, sino que requiere una rica información contextual que sólo puede crearse con la aplicación del análisis humano. Esta información contextual incluye el vínculo entre los indicadores técnicos, los adversarios, sus motivaciones e intenciones, y la información sobre quién es el objetivo. De hecho, los analistas no sólo deben centrarse en el resultado de un ataque, como un IoC, sino también en las tácticas y técnicas que indican que se está produciendo un ataque. Sin embargo, la verdadera ventaja que aporta la CTI es el concepto de intercambio de información sobre ciberamenazas. Proporciona acceso a información sobre amenazas que de otro modo podría no estar disponible para una organización, que de este modo puede beneficiarse de los conocimientos, la experiencia y las capacidades de otras organizaciones para obtener una comprensión completa de las amenazas a las que puede enfrentarse. Esto permite que la detección de una organización se convierta en la prevención de otra (Suryotrisongko et al., 2022). A continuación, se describen tres de los más importantes CTI open-source freameworks, que son, MISP, Cortex y TheHive.

2.4.14. MISP

Malware Information Sharing Platform (MISP) es un software gratuito y de código abierto diseñado para facilitar el intercambio de información sobre amenazas, incluyendo indicadores clave de ciberseguridad. Esta herramienta permite a los usuarios colaborar eficazmente, promoviendo una mejor comprensión y respuesta ante las amenazas digitales que enfrentan las organizaciones modernas (Sholihah et al., 2021). Permite almacenar los IoC de forma estructurada, y así disfrutar de la correlación, exportaciones automatizadas para IDSes o SIEMs, en STIX, OpenIOC y muchos otros formatos incluyendo CSV y texto plano, y sincronizar con otros servidores MISP. También facilita el intercambio con socios de confianza

y grupos de confianza, así como la recepción de estos datos, para permitir una detección rápida y eficaz de los ataques. MISP ofrece una interfaz web intuitiva, pero también una API REST que puede utilizarse para la automatización y la alimentación de dispositivos. Además, también existe una biblioteca Python llamada PyMISP que permite acceder fácilmente a través de la API (Wagner et al., 2016). El componente básico de MISP es el evento. Cada evento se compone de una lista de atributos, que son piezas atómicas de datos que pueden ser IoC como, por ejemplo, una dirección IP, una URL o un archivo. Cada vez que se crea un atributo, MISP comprueba si ese atributo ya existe en el sistema para encontrar una correlación. Una correlación no sólo se manifiesta con una coincidencia exacta, sino también con la presencia de atributos que se cree que están relacionados de alguna manera, por ejemplo, puede haber una correlación entre una dirección IP y un rango de direcciones IP al que pertenece. Además, es posible añadir información a un evento utilizando etiquetas o funciones más avanzadas. Aparte de ser un repositorio autónomo de ataques y programas maliciosos, una de las principales características de MISP es su capacidad para conectarse a otros servidores MISP (también llamados instancias MISP) y compartir su información. El intercambio de datos entre dos o más instancias MISP se denomina sincronización. Otra forma de obtener eventos de una fuente remota en MISP es mediante el uso de feeds. Los feeds son recursos remotos o locales que contienen indicadores que pueden importarse automáticamente a MISP a intervalos regulares. Una gran ventaja de MISP es que está soportado por muchas herramientas de código abierto y propietarias. Un ejemplo de este tipo de herramientas es TheHive, que es una Plataforma de Respuesta a Incidentes de Seguridad (SIRP) de código abierto (Lodhi et al., 2018).

2.4.15. TheHive

TheHive Project ha desarrollado una Plataforma de SIRP (Security Incident Response Platform) escalable, de código abierto y gratuita, que se integra estrechamente con MISP. Esta

plataforma está diseñada para simplificar las operaciones de los SOCs, CSIRTs, CERTs y los profesionales de la seguridad de la información. Su objetivo es facilitar la gestión y respuesta rápida a incidentes de seguridad que requieren una investigación y acciones inmediatas. Proporciona una interfaz web desde la que es posible gestionar alertas relacionadas con eventos de seguridad procedentes de multitud de fuentes, como un SIEM, un IDS, un informe de correo electrónico o un evento MISP. Las alertas pueden ignorarse, marcarse como leídas, previsualizarse e importarse. Cuando se importa una alerta, se convierte en un caso que debe investigarse (Ramanathan et al., 2020). También ofrece una API REST y la mayoría de sus puntos finales son accesibles a través de TheHive4py, que es el cliente Python API para TheHive (Walensky et al., 2022). La construcción central de TheHive es el caso, que es también la construcción central de la mayoría de las investigaciones de seguridad. Un caso se caracteriza por un título, una descripción y una fecha. Además, también se caracteriza por varios elementos, algunos de los cuales se describen a continuación (Conroy et al., 2023):

- **Tareas:** Se utilizan para realizar un seguimiento de las acciones llevadas a cabo para responder a las preguntas de investigación, pero también para realizar un seguimiento de los eventos de contención, erradicación y reparación. Pueden contener varios registros, que son entradas de texto utilizadas para describir el progreso de un analista, adjuntar pruebas o archivos dignos de mención e incluso archivos ZIP protegidos por contraseña que contengan malware o datos sospechosos.
- **Observables:** Pueden ser de distintos tipos, por ejemplo direcciones IP, direcciones de correo electrónico, URL y dominios. Además, se pueden definir tipos de observables personalizados si es necesario. Se pueden etiquetar, marcar como IoC y analizar. Si un observable en un caso ya ha sido visto en otros casos, se marca automáticamente como visto, y los casos que comparten observables comunes se consideran relacionados.

- **Etiquetas:** Son otra forma de añadir información a un caso y pueden utilizarse para realizar búsquedas y filtrados rápidos. Son etiquetas que pueden adjuntarse a los casos, pero también a muchos otros objetos de TheHive como alertas y observables. Por ejemplo, es posible añadir la fuente que proporcionó o generó un observable utilizando una etiqueta.

Para reducir el tiempo perdido en la creación de casos que comparten la misma estructura, TheHive admite la creación de plantillas de casos predefinidas. Dichas plantillas también pueden utilizarse para esbozar los pasos a seguir con el fin de dirigir la actividad del equipo (Akamatsu et al., 2016). Un caso puede generarse a partir de una alerta o crearse desde cero. La alerta es otro constructo importante de TheHive que comparte muchas propiedades con el constructo de caso, incluyendo los observables que se han observado en el evento de seguridad que generó esa alerta. Todos esos campos se asignarán directamente a los campos de caso correspondientes una vez importada la alerta. Además, las plantillas de casos también se pueden utilizar para crear casos a partir de alertas cuando se importan. Una característica clave de TheHive es la colaboración. De hecho, cada analista tiene su propia cuenta con su conjunto de permisos y cada acción que realiza se registra en un feed en vivo en tiempo real, que es visible por otros analistas. Tanto los casos como las tareas pueden asignarse a un analista y es posible que varios analistas trabajen en el mismo caso, pero en tareas diferentes, de modo que se repartan las responsabilidades. Para seguir el progreso de la investigación, los casos y las tareas pueden estar en diferentes estados. Por ejemplo, un caso puede estar en estado "Abierto", pero puede transitar al estado "Resuelto" cuando finaliza el análisis y se cierra el caso, especificando una serie de campos como el posible impacto del incidente. Del mismo modo, las tareas pueden estar en estado "En espera" cuando aún no han sido asignadas a un analista, luego pueden transitar al estado "En curso" cuando se inician y pueden transitar al estado "Completadas" cuando se cierran.

2.4.16. Cortex

Es un potente motor de análisis de observables y respuesta activa de código abierto [26] creado por TheHive Project que permite analizar observables a escala consultando una única herramienta en lugar de varias (Ochoa & Cossio, 2021). Ofrece una interfaz web desde la que es posible analizar observables uno a uno o en modo masivo, pero también puede utilizarse para automatizar estas operaciones y enviar grandes conjuntos de observables desde TheHive o a través de la API REST de Cortex. Además, la mayoría de los puntos finales ofrecidos por la API REST de Cortex son accesibles a través de Cortex4py, que es el cliente Python API para Cortex (Ochoa & Cossio, 2021). El uso de Cortex se basa en neuronas, que son aplicaciones autónomas gestionadas por y ejecutadas a través del motor central de Cortex (Dreher et al., 2023). Pueden ser de dos tipos:

- **Analizadores:** Permiten analizar diferentes tipos de observables automatizando la interacción con un servicio o una herramienta para acelerar el análisis y posibilitar la contención de amenazas antes de que sea demasiado tarde. Cortex viene con más de cien analizadores para servicios populares como VirusTotal, emailrep.io, urlscan.io, AbuseIPDB y PhishTank. Hay que tener en cuenta que, aunque muchos analizadores son de uso gratuito, algunos requieren un acceso especial y otros necesitan una suscripción válida a un servicio o una licencia de producto (Chenji et al., 2021).
- **Respondedores:** Se instalan junto con los analizadores. A diferencia de los analizadores, sólo son útiles cuando Cortex se utiliza junto con TheHive, de hecho realizan diferentes acciones y se aplican a alertas, casos, tareas, registros de tareas y observables (Ochoa & Cossio, 2021).

Los analizadores y respondedores pueden activarse, desactivarse y configurarse desde la interfaz web. Para cada uno de ellos es posible definir muchos parámetros, como límites de velocidad, nombres de usuario, contraseñas y claves API. Cuando se envía un observable para

su análisis, Cortex crea un trabajo. Ese trabajo generará un informe de análisis en formato JSON si finaliza con éxito (Ochoa & Cossio, 2021). Además, estos informes de trabajo pueden almacenarse en caché de modo que, si se lanza un analizador contra el mismo observable, el informe anterior puede ser devuelto sin volver a ejecutar el analizador. La caché sólo se utiliza si el segundo trabajo se produce en un periodo de tiempo configurable, en el que el valor predeterminado es de 10 minutos (Ochoa & Cossio, 2021). También se crea un trabajo cuando se inicia un respondedor. También en este caso se proporciona un informe JSON sobre el resultado de la acción realizada.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

El proyecto aquí presentado se realizará en la ciudad de Quito en la empresa "Audetic", la cual brinda soluciones especializadas de auditoría y consultoría en TI, continuidad de negocio, seguridad de la información, ciberseguridad, riesgos y detección de fraudes.

Está ubicada en la Av. Orellana E9-195, Edifico Alisal de Orella, Piso 100

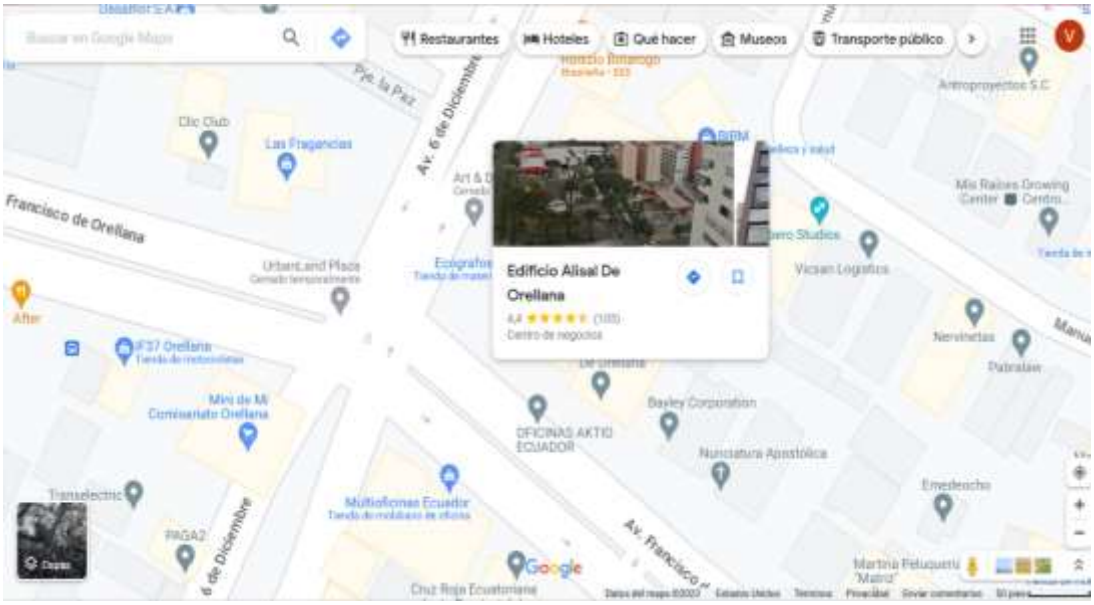

Figura 6 Ubicación geográfica de la empresa "Audetic", referencia tomada de Google Maps

3.2.Población

Para la investigación del tema propuesto se tomará como población a todos los colaboradores de la empresa "Audetic".

3.3.Muestra

Inicialmente, se planeaba emplear correos electrónicos de ocho miembros de la empresa "Audetic" para realizar pruebas. Sin embargo, debido a las limitaciones impuestas por las versiones de prueba del software utilizado, las cuales restringen el número de usuarios y la funcionalidad, se optó por utilizar solo una cuenta de correo electrónico para las pruebas. Esta

restricción representó un desafío considerable, impactando negativamente en la amplitud y la capacidad de generalizar los resultados obtenidos.

3.4.Enfoque y tipo de investigación

El enfoque asumido para abordar el problema de investigación es cuantitativo ya que se quiere establecer el porcentaje de mejora en la gestión de incidentes después de haber automatizado el playbook de Phishing.

Para llevar a cabo la medición, se propone realizar un análisis de las prácticas de gestión de incidentes de seguridad informática considerando la NIST SP 800-61 y caracterizar las herramientas de open source disponibles para la automatización de gestión de incidentes para posteriormente automatizar el proceso de playbook y al final realizar una comparación e identificar en que porcentaje o medida se mejoró la gestión de incidentes.

El tipo de investigación a utilizarse en este trabajo de investigación será descriptivo y de campo, debido a que se analizará el proceso de gestión que realza el equipo de respuesta, así también automatizar el playbook de phishing, con la finalidad de mejorar la efectividad en la gestión de incidentes.

3.5.Procedimiento de investigación

El proyecto iniciará con el análisis de las prácticas en la gestión de incidentes de seguridad considerando la NIST SP 800-61, una vez realizado el análisis se caracterizará las herramientas de open source disponibles que permitirán la automatización de la gestión de incidentes y proceder a automatizar el playbook de phishing al final de proceso evaluar la efectividad a partir de la automatización del playbook en la gestión de incidentes de seguridad en la organización.

Fase 1 – Análisis de las prácticas en la gestión de incidentes de seguridad informática

En la primera fase se realizará la revisión de la NIST SP 800-61 para comprender los procesos y recomendaciones para la gestión de incidentes de seguridad, se investigará

informes, normativas, además, se revisará las prácticas actuales en la gestión de incidentes en la empresa “Audetic”.

Fase 2 – Caracterización de las herramientas open source disponibles para la automatización de la gestión de incidentes

En la segunda fase del proyecto se realizará una revisión de las herramientas open source disponible para la gestión de incidentes de seguridad, se evaluará las características, funcionalidades y capacidades de cada herramienta, se analizará las ventajas y desventajas de cada herramienta en función a las necesidades de la empresa.

Fase 3 – Automatización del playbook de phishing

Automatizar el playbook de phishing utilizando las herramientas open source seleccionadas en la fase 2, configurar las herramientas de automatización definiendo los pasos y acciones necesarias para detectar, responder y mitigar los ataques de phishing, la fase 3 se culminará con las pruebas y ajustes del playbook automatizado para garantizar el funcionamiento y la eficacia en la gestión de incidentes de seguridad.

Fase 4 – Evaluación de la efectividad del playbook de phishing automatizado

Durante la fase 4 se recopilará los datos del antes y después de la implementación de playbook automatizado, el tiempo de respuesta, la detección del evento o incidentes y la eficacia en la mitigación de incidentes de phishing, también ser realizará un análisis comparativo de los resultados obtenidos para evaluar la mejora en la gestión de incidentes después de la automatización.

3.6.Consideraciones bioéticas

Las consideraciones bioéticas para la elaboración del proyecto incluyen la búsqueda del beneficio y protección de la organización y sus empleados, la precaución en la minimización de riesgos, la responsabilidad ética y profesional, la equidad en el diseño y

aplicación de la investigación, el respeto a la autonomía de los participantes mediante el consentimiento informado y el cumplimiento de las normativas y regulaciones vigentes.

Además, he solicitado a la empresa “Audetic” que me permita realizar el proyecto en la organización, la respuesta por parte de la Gerente General fue positiva.

3.7.Infraestructura integrada de TheHive, Cortex y Misp

Cortex es una herramienta de gran potencia por sí sola, pero su verdadero potencial se desbloquea al utilizarla en conjunto con TheHive. La integración de TheHive con una o varias instancias de Cortex permite acceder a las funciones avanzadas y aprovechar al máximo sus capacidades. Al establecer una conexión con un servidor Cortex, TheHive tiene la capacidad de lanzar analizadores contra los observables en un caso, con el fin de obtener información adicional sobre ellos. Cada analizador genera un informe en formato JSON que se puede visualizar directamente desde la interfaz de TheHive. Además, es posible ejecutar respondedores específicos contra casos, observables, tareas, registros de tareas y alertas, con el propósito de llevar a cabo acciones automatizadas.

A pesar de que muchas organizaciones comparten información sobre casos y observables mediante TheHive y Cortex, la verdadera capacidad de intercambio de información sobre amenazas cibernéticas se logra mediante la integración con MISP. La integración entre TheHive y MISP permite la importación automática de eventos de MISP como alertas y la exportación de casos de TheHive a MISP como eventos. Además, Cortex también puede integrarse con MISP para realizar búsquedas de observables dentro de una instancia de MISP. Esto es posible gracias a un analizador de búsqueda específico de MISP que está disponible en Cortex, el cual proporciona el número de eventos en los que se ha encontrado el observable, así como una lista de enlaces a esos eventos con información adicional. Este analizador resulta muy útil al lanzarlo contra un observable en un caso de TheHive, ya que enriquece aún más la información disponible durante la investigación.

3.7.1. Licencia y uso

La versión por defecto de TheHive y Cortex, denominada Community, no tiene una fecha de caducidad específica. Sin embargo, esta versión limita el acceso a la aplicación a un máximo de 2 usuarios y 1 organización. Además, restringe ciertas funcionalidades como la agrupación, marca, integración con directorio activo, autenticación SAML y OUATH2, así como las líneas de tiempo de caso, entre otros aspectos.

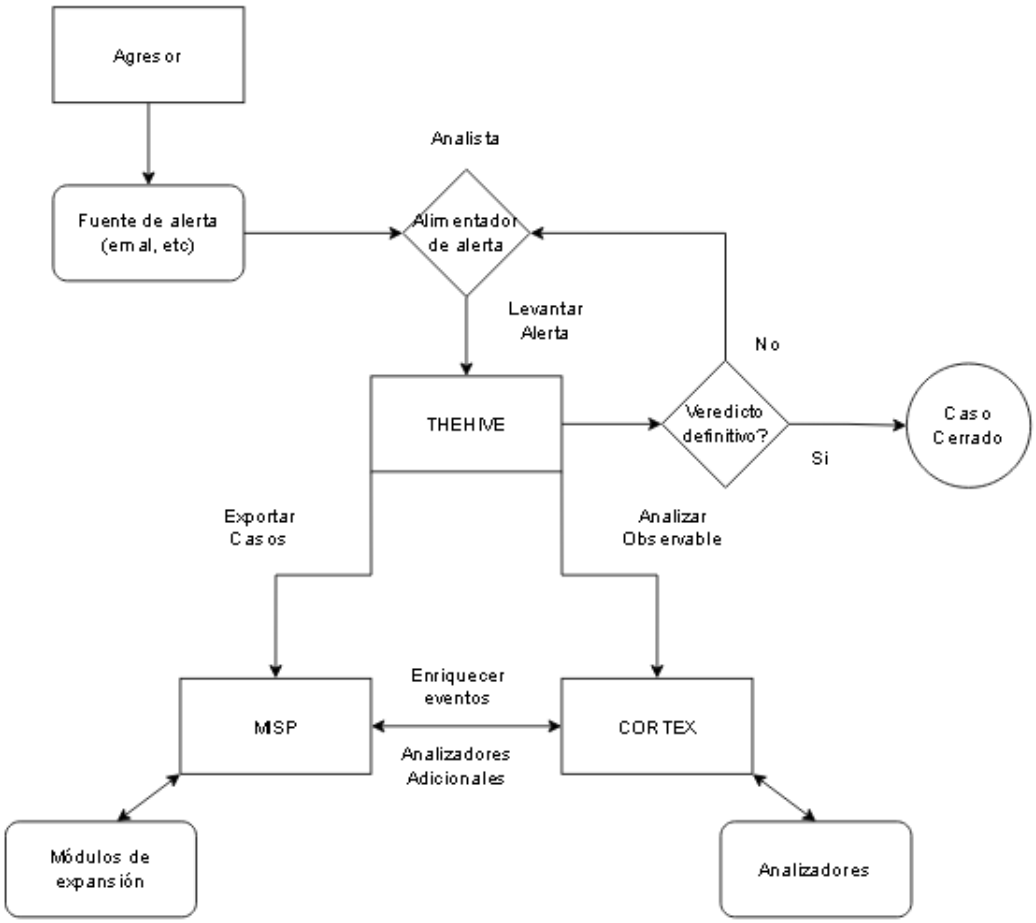

Figura 7 Descripción general de arquitectura con TheHive, Cortex y Misp

1. Un atacante inicia una campaña de phishing y envía un correo de phishing a un usuario.
2. El correo ingresa a la bandeja de entrada del servidor de correo de la empresa.

3. La herramienta de correo electrónico no permite la entrega del correo electrónico al destinatario en base a las políticas de seguridad (dominios desconocidos con archivos o links adjuntos, entre otros).
4. El analista encargado del servidor de correo electrónico remite los datos del remitente del correo al encargado de la seguridad informática para analizarlo.
5. El analista encargado de la seguridad informática crea una tarea en TheHive y especifica el/los observables.
6. Si el veredicto es definitivo se cierra el caso y se notifica al analista encargado del correo electrónico para tomar la acción consecuente. Además, en caso de detectar que es un correo malicioso el caso se exporta a MISP automáticamente.
7. Si el veredicto no es definitivo, se volverá a efectuar el análisis aplicando nuevos observables.

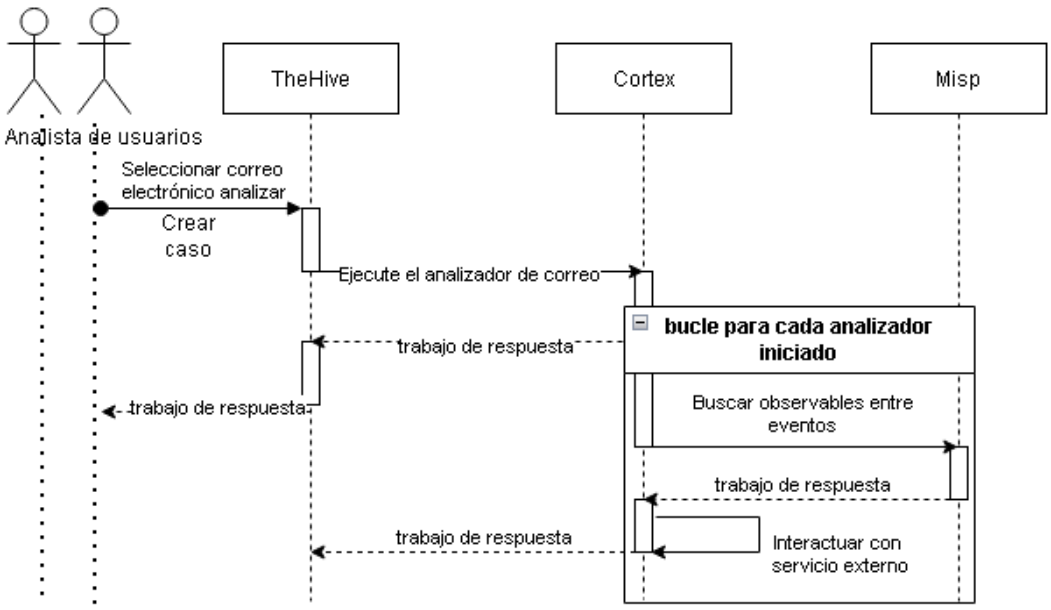

Figura 8 Secuencia de análisis

3.7.2. Implementación de TheHive, Cortex y Misp

La arquitectura TheHive, Cortex y Misp se encuentran disponibles para su despliegue utilizando contenedores Docker. Para utilizar este método de implementación, se requiere tener un sistema operativo basado en Linux con Docker versión 19.03.0 recomendado en documentación, sin embargo, durante la implementación se identificó que la versión 24.0.7 es necesaria para el funcionamiento de esta arquitectura, Docker Compose versión 1.25.5, Docker-py versión 4.1.0, CPython versión 3.7.5, OpenSSL versión 1.1.0 instalados. La implementación para ambientes de producción a gran escala implicará el incremento de recursos necesarios en el servidor donde se alojen todos los contenedores, incluso podría requerir un equipo para cada componente.

Para ejecutar los componentes con Docker compose se siguen los siguientes pasos:

1. Clonar el repositorio en la máquina virtual asignada.

   $ git clone https://github.com/emalderson/ThePhish.git

2. Ingresar al directorio creado en el paso anterior y ejecutar el contenedor Docker.

   $ cd ThePhish/docker

   $ docker-compose up

3. Es necesario detener el despliegue para modificar los permisos del directorio "vol". Luego de la ejecución de estos comandos iniciará la descarga e inicio de los contenedores automáticamente

   $ docker-compose stop

   $ sudo chown -R 1000:1000 vol/index vol/data vol/elastic*

   $ docker-compose up

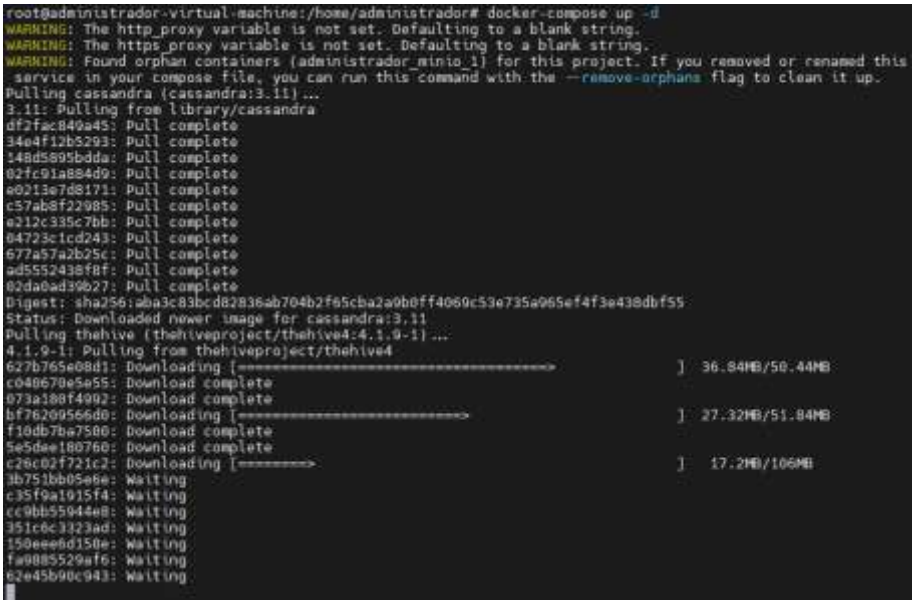

Figura 9 Captura de pantalla, Despliegue de contenedores Docker

4. A través del comando $ docker ps se visualiza los contenedores descargados y su estado. Es importante citar que el archivo “docker-compose.yml” obtenido en el primer paso debe actualizarse a la versión 3.3 para que se despliegue sin problema.

3.7.3. Configuración de Misp

Para configurar el contenedor de Misp se siguen los siguientes pasos:

1. Acceder a la URL https://localhost e ingresar las credenciales:

   Nombre de usuario: admin@admin.test

   Contraseña: admin

2. Crear una nueva organización:

   - Acceder a administración – añadir la organización
   - Nombre: thephish
   - Haga click en “Generate UUID”
   - Presionar “enviar”. Preservar el código generado que será necesario en los próximos pasos.

Figura 10 Captura de pantalla, Creación de nueva organización

3. Cambiar la configuración:

    - Administración – Configuración de servidor y mantenimiento – Configuración MISP
    - Cambiar el campo MISP.live a True
    - Cambiar el campo MISP.baseurla https://localhost
    - Cambiar el campo MISP.external_base_urla https://localhost
    - Cambiar el campo MISP.orga thephish
    - Cambiar el campo MISP.host_org_ida thephish

Figura 11 Captura de pantalla, Configuración de Misp

4. Crear un nuevo usuario que se utilice para la integración con TheHive y Cortex
    - Administración - Añadir Usuario
    - Correo electrónico: sync_user@thephish.com
    - organización: thephish
    - Rol: Sync User
    - Desmarque todas las casillas
    - clic en "Crear usuario"
5. Obtener la clave de autenticación de la cuenta Sync User
    - Administración - Lista a los usuarios
    - Haga clic en el "Ojo" a la derecha para el usuario creado (View)
    - Haga clic en "Auth Keys"
    - Borrar la clave de auth ya creada
    - Administración - Usuarios de la Lista (otra vez)
    - Haz clic en el "Ojo" a la derecha para el usuario creado
    - Haga clic en "Auth Keys" (otra vez)
    - Haga clic en "Añadir clave de autenticación"
    - Haga clic en "Enviar" y guardarlo para más tarde

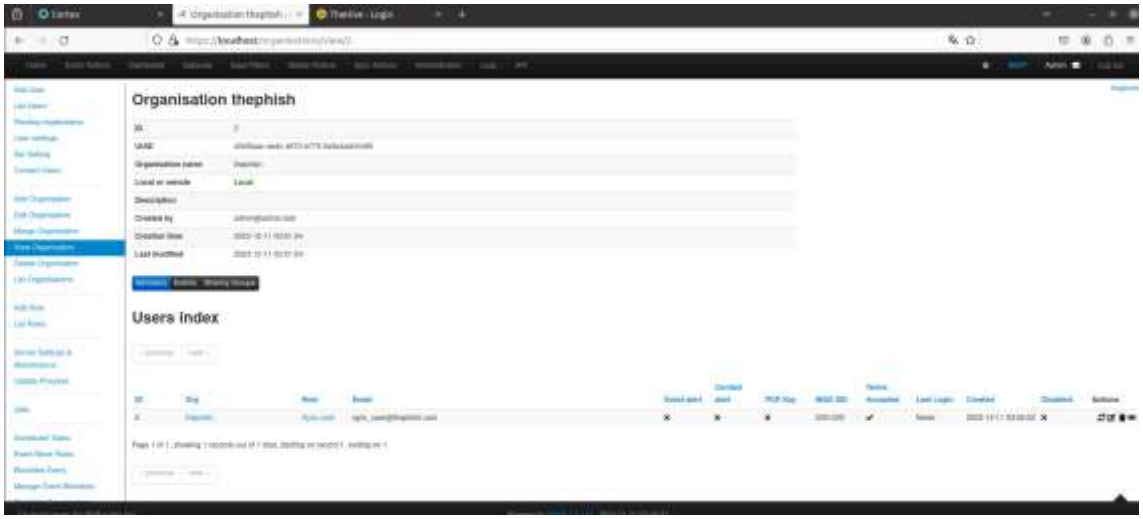

Figura 12 Captura de pantalla, Configuración de cuenta de sincronización de Misp

6. Habilitar feeds Misp

    - Sync Actions -> List Feeds -> Load default feed metadata -> All feeds
    - Select the feeds to enable
    - Click en "Enable selected"

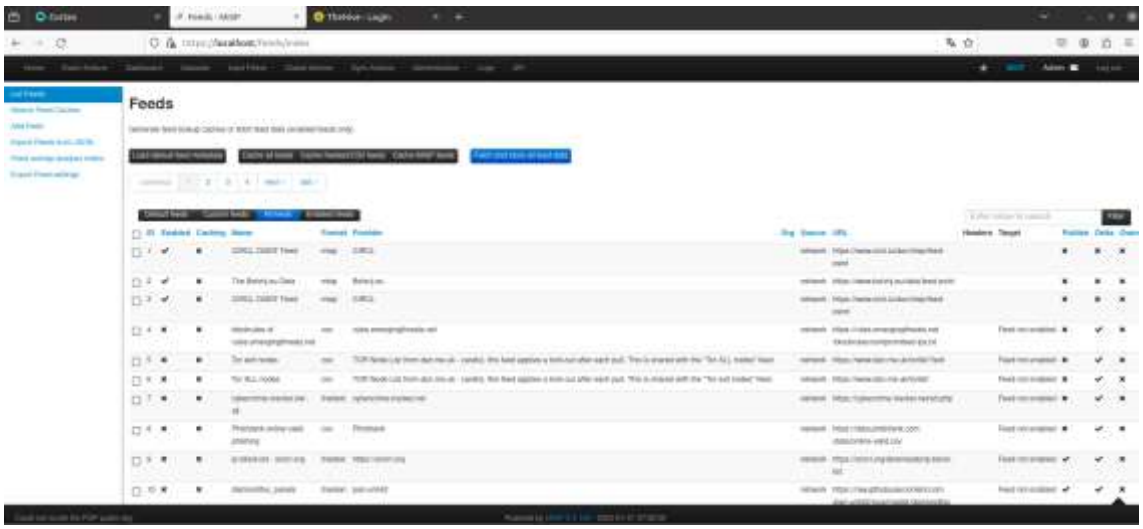

Figura 13 Captura de pantalla, Configuración de feeds de Misp

3.7.4. Configuración de contenedor Cortex

Para configurar el contenedor de Cortex siguen los siguientes pasos:

1. Acceder a la url: http://localhost:9001 y hacer click en “Update database”
2. Crear un nuevo usuario de administración
    - Inicia sesión: admin@thephish.com
    - Nombre: admin
    - Contraseña: Admin2023
3. Crear una nueva organización
    - Organizaciones - Añadir organización
    - Nombre: thephish
    - Descripción: proyecto

4. Crear un nuevo usuario de orgadmin en esa organización
    - Haga clic en la organización de nueva creación “thephish”
    - Haga clic en "Añadir usuario"
    - Inicia sesión: thephish@thephish.com
    - Nombre completo: ThePhish
    - Funciones: read, analyze, orgadmin
    - Haga clic en "Nueva contraseña" para el usuario recién creado y establezca una contraseña para ese usuario
5. Crear otro usuario en esa organización que se utiliza para la integración con TheHive y para usar la API
    - Haga clic en la organización de nueva creación “thephish”
    - Haga clic en "Añadir usuario"
    - Inicia sesión: integration_account@thephish.com
    - Nombre completo: integration_account
    - Funciones: read, analyze
    - Haga clic en "Crear la tecla API" y luego en "Reveal" para el usuario recién creado y guardarlo para más tarde
6. Iniciar sesión con el usuario de administración, e iniciar sesión en el usuario de orgadmin (ThePhish)

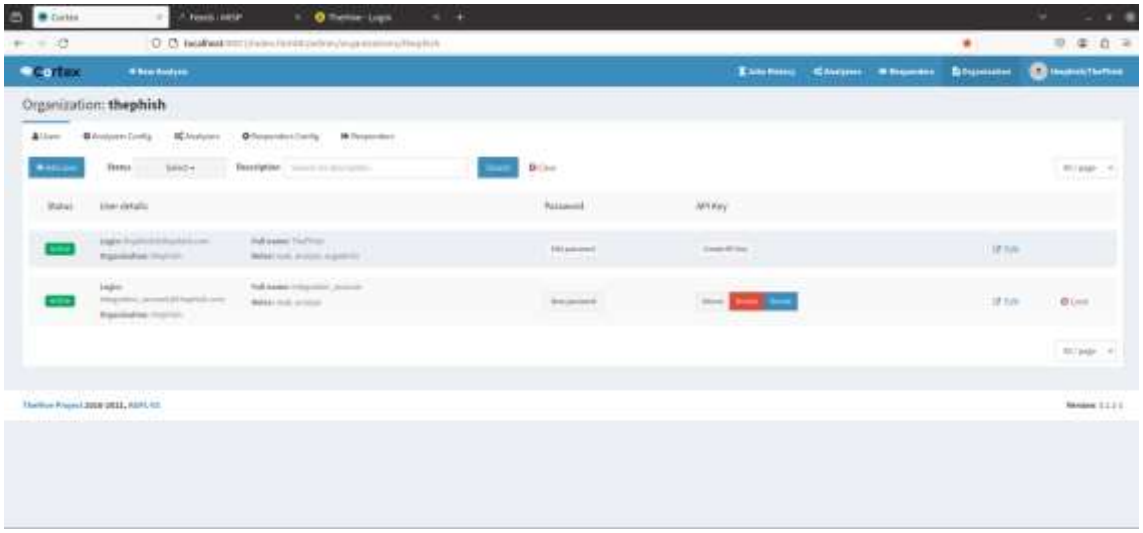

Figura 14 Captura de pantalla, Creación de usuarios y organización en Cortex

7. Habilitar el respondedor Mailer

    - Organización - - Responders
    - Habilitar al Mailer
    - Configurar el Mailer de respuesta
        - de: thephishproyecto@gmail.com
        - smtp.host:smtp.gmail.com
        - smtp.port: 587
        - smtp.user: thephishproyecto@gmail.com
        - smtp.pwd: Admin2023

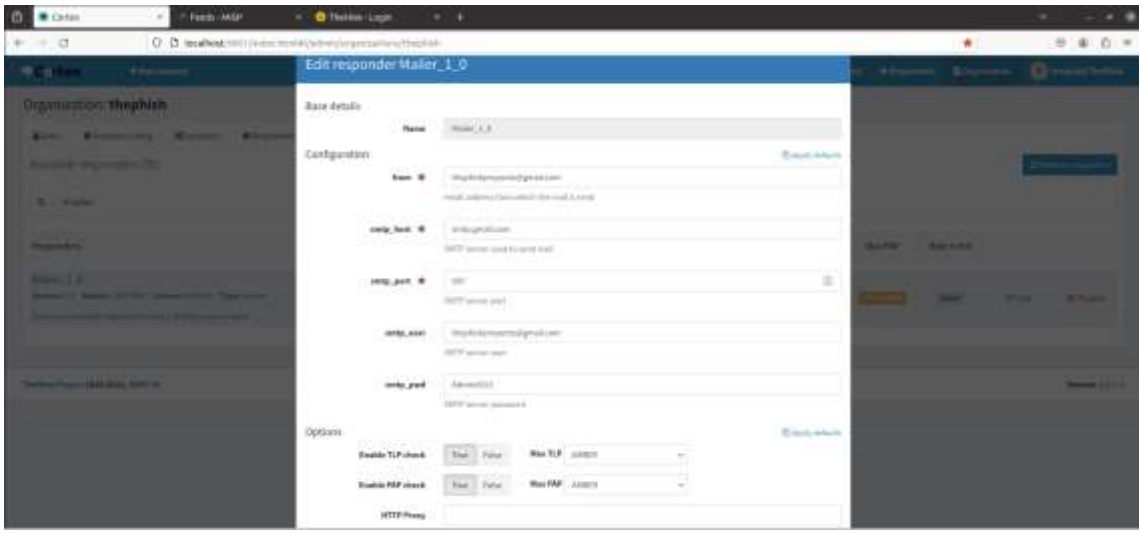

Figura 15 Captura de pantalla, Configuración de Responder Mailer en Cortex

3.7.5. Integración entre Cortex y Misp

Debido a que Docker crea una red puente predeterminada a la cual se conectan los contenedores durante su ejecución, es necesario que el contenedor que aloja el analizador MISP-2-1 esté conectado a esta red para poder acceder a la instancia MISP en otro contenedor. La única forma de establecer esta conexión es utilizando la dirección IP de la interfaz que conecta el contenedor MISP a la red puente predeterminada, ya que no se puede acceder al servidor DNS incorporado en las redes predeterminadas.

Para conectar el contenedor MISP a la red puente predeterminada, se deben ejecutar los siguientes comandos:

$ docker network connect bridge misp

$ docker network inspect bridge

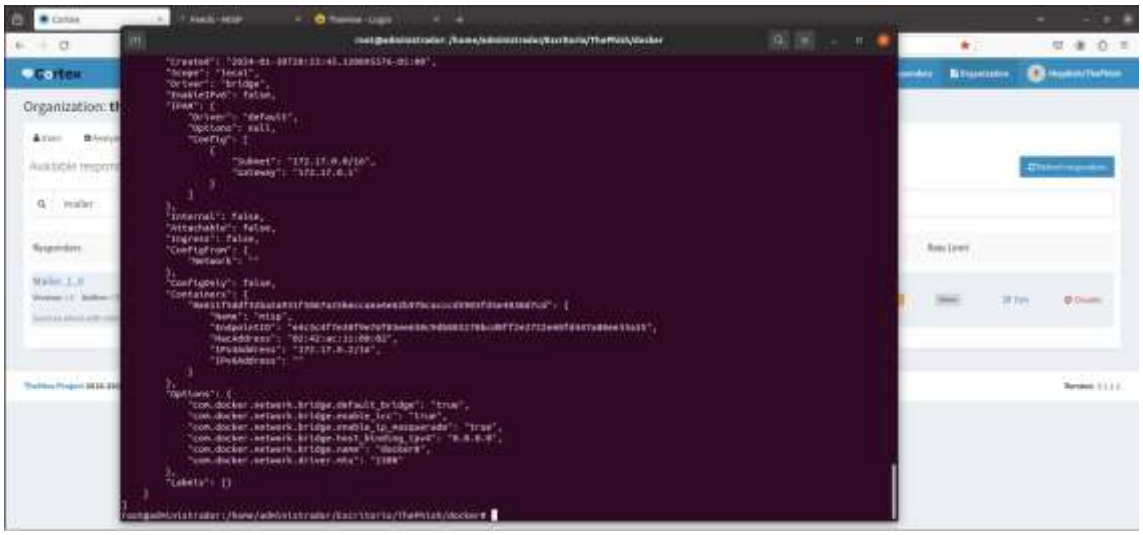

Figura 16 Captura de pantalla, Detalle de red puente de docker

En Cortex, iniciar sesión con el usuario que tiene el rol de orgadmin y realizar lo siguiente:

- Organización - Analizadores
- Habilitar el analizador MISP-2-1

- Configurar elMISP – 1 analizador
    - url: https://172.17.0.2/
    - clave: uuid de Misp
    - cert-check: False

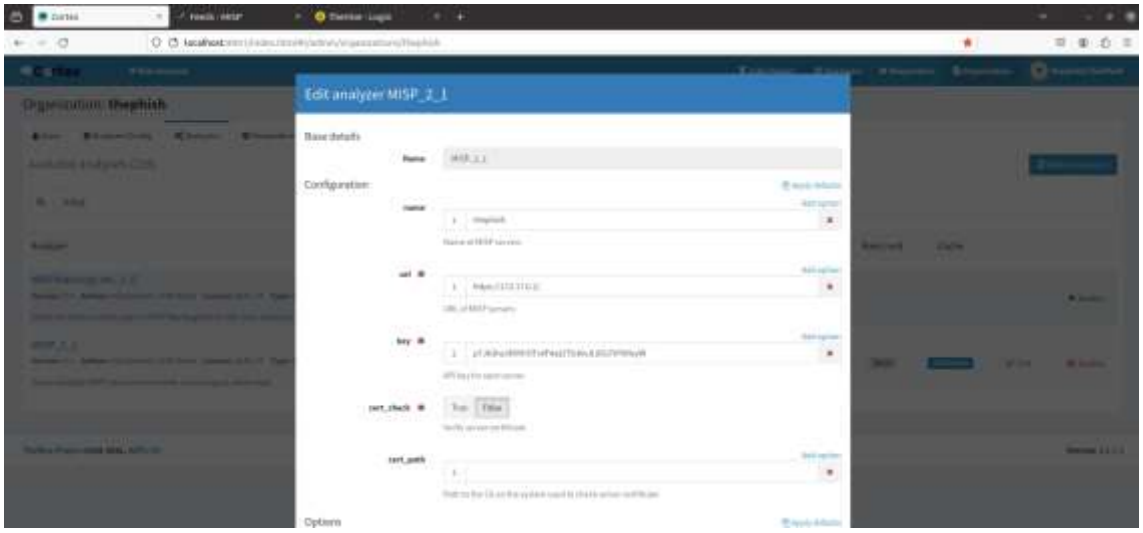

Figura 17 Captura de pantalla, Configuración de Analizador Misp_2 de Cortex

3.7.6. Integración de TheHive con Cortex

Editar el código correspondiente a Cortex dentro del archivo thehive/application.conf para sustituir a la clave “XXXXXXXXXXXXXX” con la clave API de la integration_account creado en Cortex.

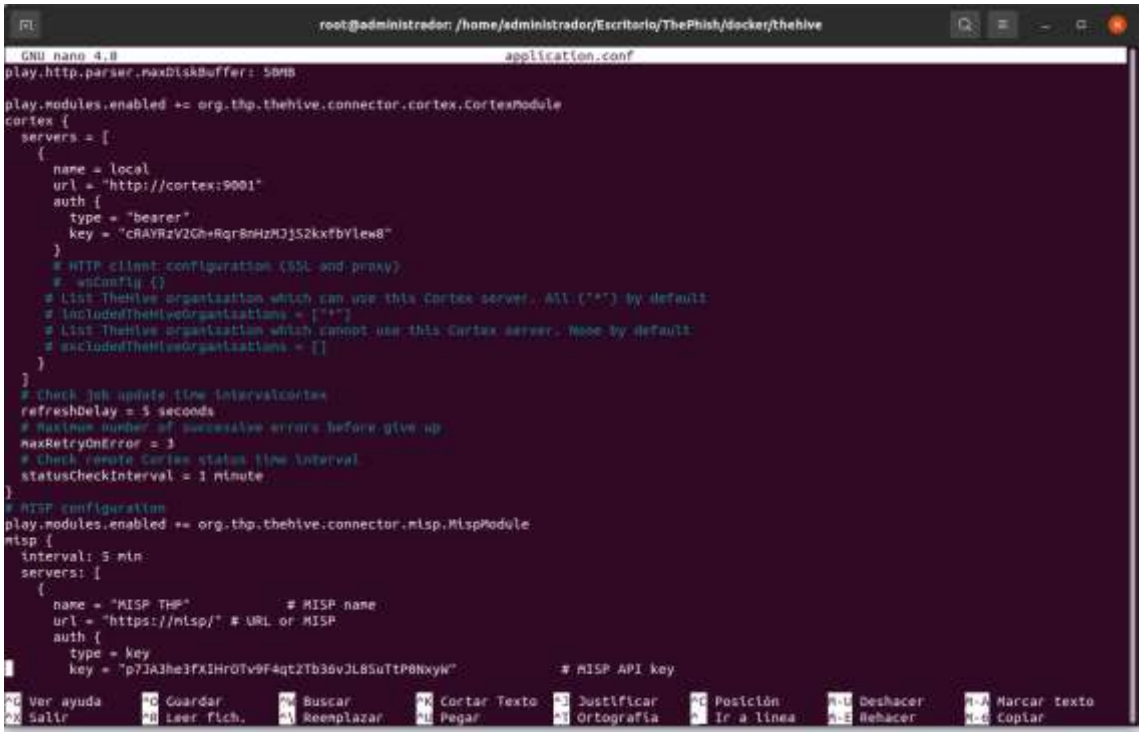

Figura 18 Captura de pantalla, Archivo de configuración de integración de TheHive con Cortex

3.7.7. Integración de TheHive con Misp

Editar el código correspondiente a Misp dentro del archivo thehive/application.conf para sustituir a la clave “XXXXXXXXXXXXX” con la clave de Autenticación de la sync_user creado en MISP.

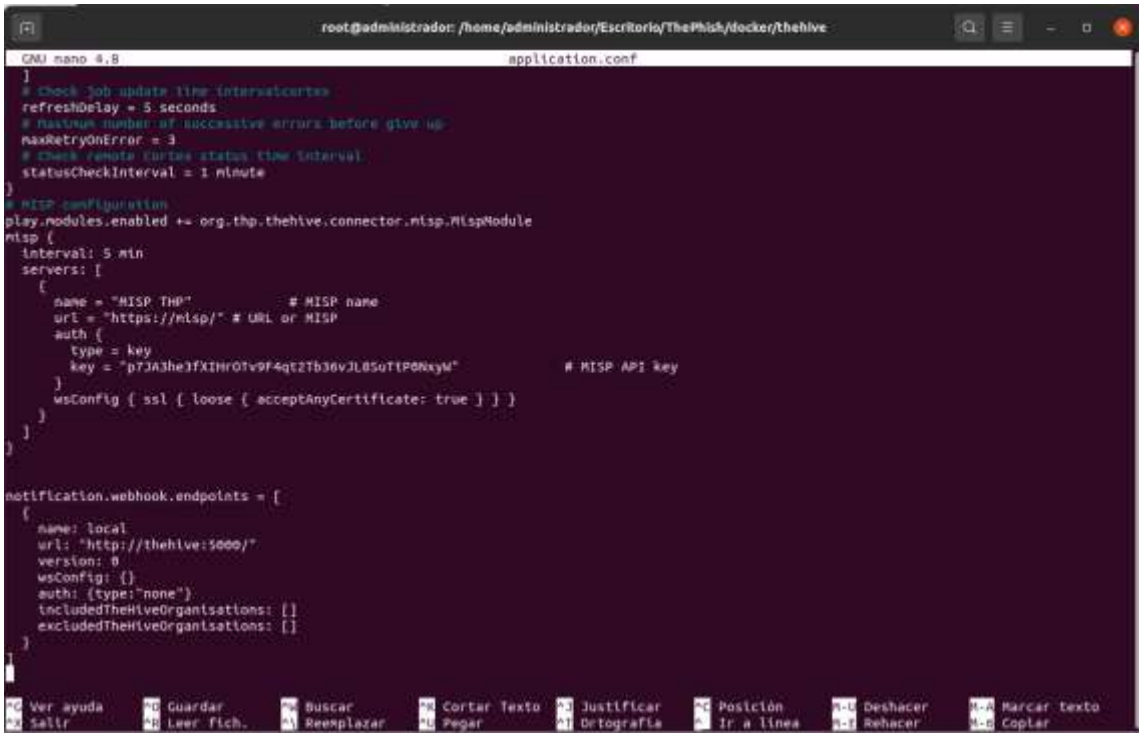

Figura 19 Captura de pantalla, Archivo de configuración de integración de TheHive con Misp

3.7.8. Configurar el contenedor de TheHive

Para configurar el contenedor de Cortex siguen los siguientes pasos:

1. Acceder a la url http://localhost:9000 e iniciar sesión con las credenciales por defecto:

   Nombre de usuario: admin@thehive.local

   Contraseña: secret

2. Crear una nueva organización

   - Haga clic en "Nueva organización"
   - Nombre: thephish
   - Descripción: proyecto

3. Crear un nuevo usuario de orgadmin en esa organización

   - Haga clic en la organización de nueva creación “the phish”
   - Haga clic en "Crear nuevo usuario"
   - Inicia sesión: thephish@thephish.com

- Nombre completo: ThePhish
- Perfil: org-admin
- Haga clic en "Nueva contraseña" para el usuario recién creado y establezca una contraseña para ese usuario.
- Haga clic en "Crear la tecla API" y luego en "Reveal" para el usuario recién creado y almacenarla ya que será solicitado en los siguientes pasos.

4. Iniciar sesión con el usuario de administración, e iniciar sesión en el usuario de orgadmin (ThePhish).

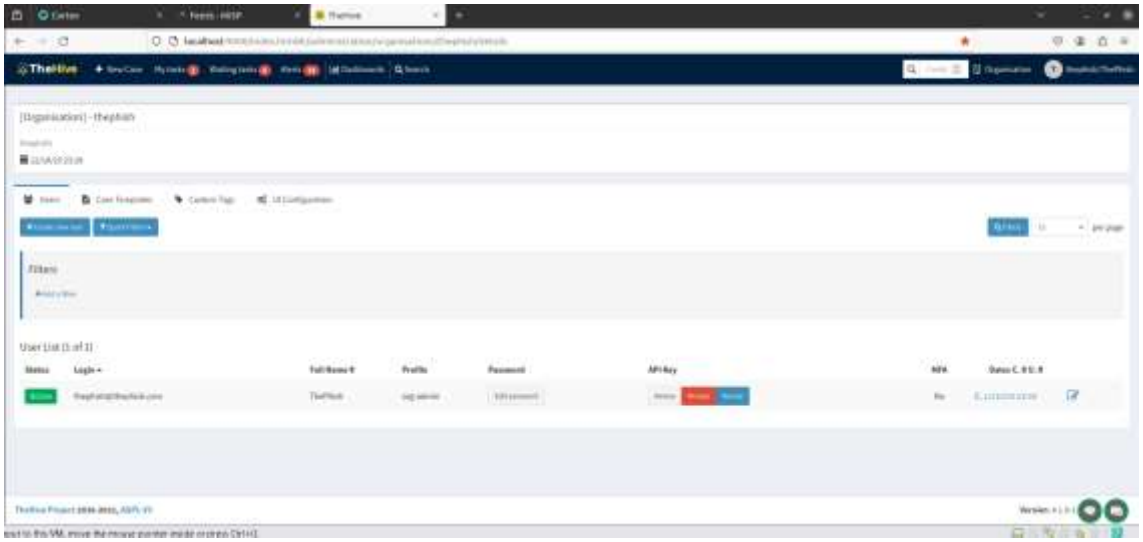

Figura 20 Captura de pantalla, Creación de organización y usuarios en The Hive

Habilitar los Analizadores

En Cortex, mientras se inicia con el usuario de orgadmin, se realiza lo siguiente:

1. Organización – Analizadores
2. Habilitar los analizadores deseados y configurarlos

En la versión utilizada de la arquitectura, Cortex contiene registro de doscientos dieciocho (218) analizadores, cada analizador abarca un campo específico. Para escanear correos electrónicos dispone de cuatro (4) analizadores:

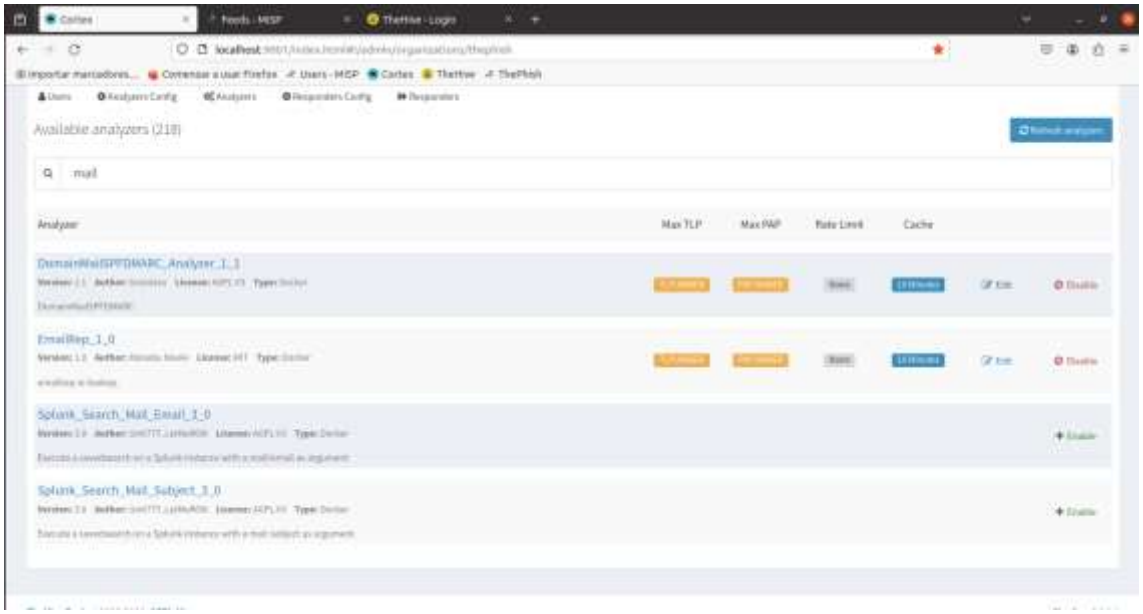

Figura 21 Captura de pantalla, Analizadores de Cortex relacionados a correo electrónico

- DomainMailSPFMarc Analizaer 1.1: Analiza y evalua los registros SPF y DMARC presentes en los correos electrónicos. Estos registros son mecanismos de autenticación y seguridad utilizados para prevenir el spoofing de dominio y el envío de correos maliciosos. Examina el contenido de los correos electrónicos en busca de estos registros y los analiza para verificar si están correctamente configurados y cumplen con las políticas de autenticación establecidas. Esto ayuda a garantizar que los correos electrónicos recibidos sean legítimos y provengan de fuentes confiables, evitando el envío de mensajes de correo electrónico falsificados o maliciosos que puedan dañar la reputación de un dominio o exponer a los usuarios a riesgos de seguridad.

Para habilitar y configurar este analizador se da click en “save” especificando un nombre al analizador. Permite además incluir datos de Proxy, certificados de seguridad, entre otros para que el analizador pueda obtener datos del repositorio ubicado en repositorios web.

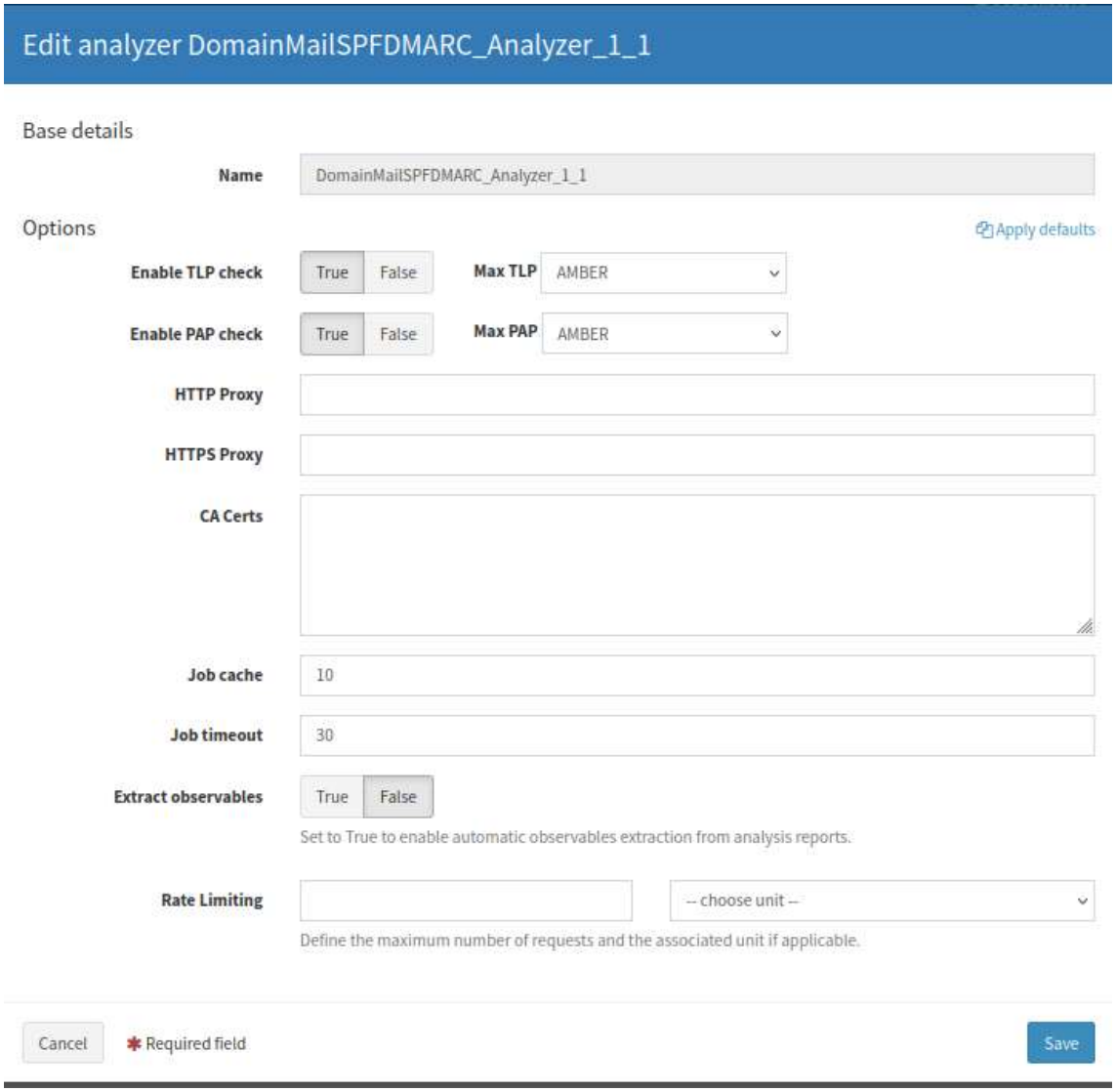

Figura 22 Captura de pantalla, Configuración de analizador DomainMail

- EmailRep 1.0: Analiza la reputación de direcciones de correo electrónico. Proporciona información valiosa sobre la confiabilidad y autenticidad de una dirección de correo determinada. Utiliza una variedad de técnicas y fuentes de datos para evaluar la reputación de una dirección de correo. Examina factores como la existencia de la dirección en listas negras conocidas, la cantidad y calidad de correos electrónicos enviados desde esa dirección, la reputación del dominio asociado y otros indicadores relevantes.

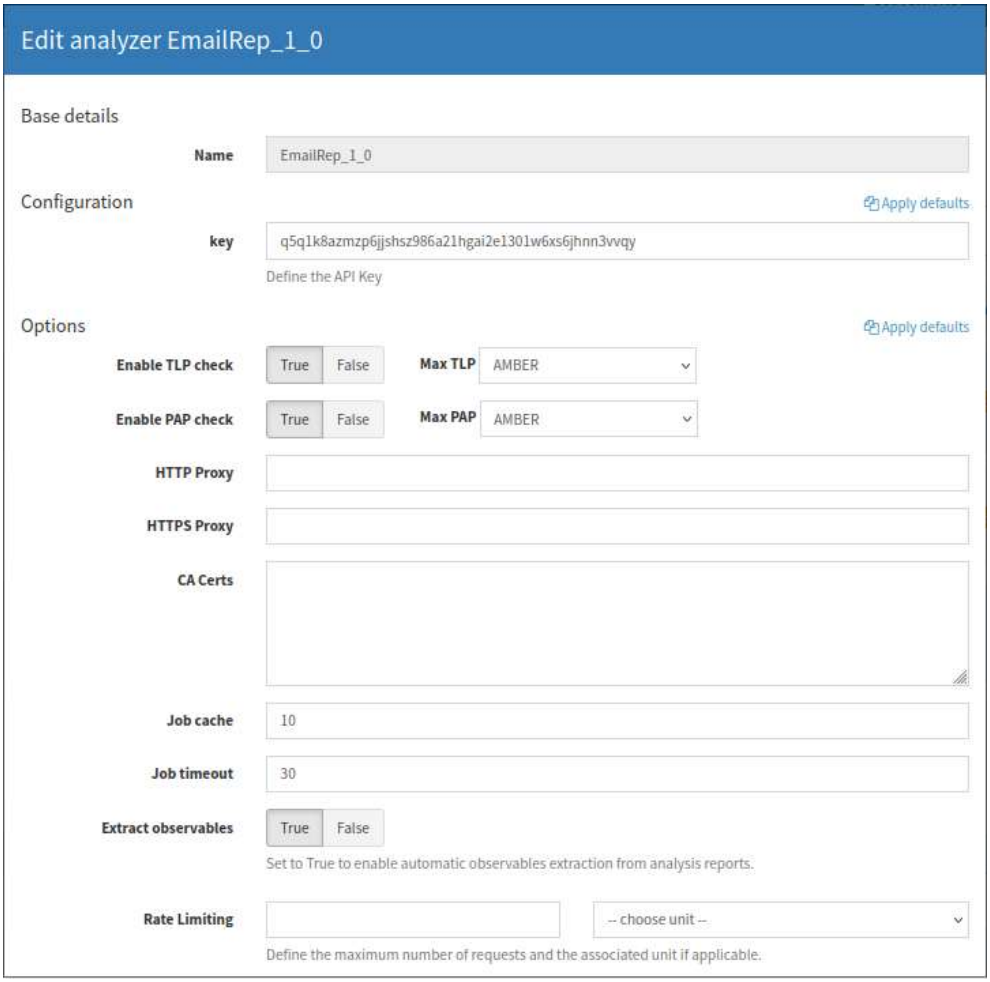

Figura 23 Captura de pantalla, Configuración de analizador EmailRep

Para habilitar y configurar este analizador, se requiere adquirir una clave de API. Dicha clave puede obtenerse al enviar una solicitud en el sitio web del fabricante del analizador: https://emailrep.io/key. Es necesario completar el proceso de registro y esperar a que la clave de API sea entregada por correo electrónico. La versión Community del analizador es de libre acceso y permite realizar hasta 10 análisis diarios y un máximo de 250 análisis al mes.

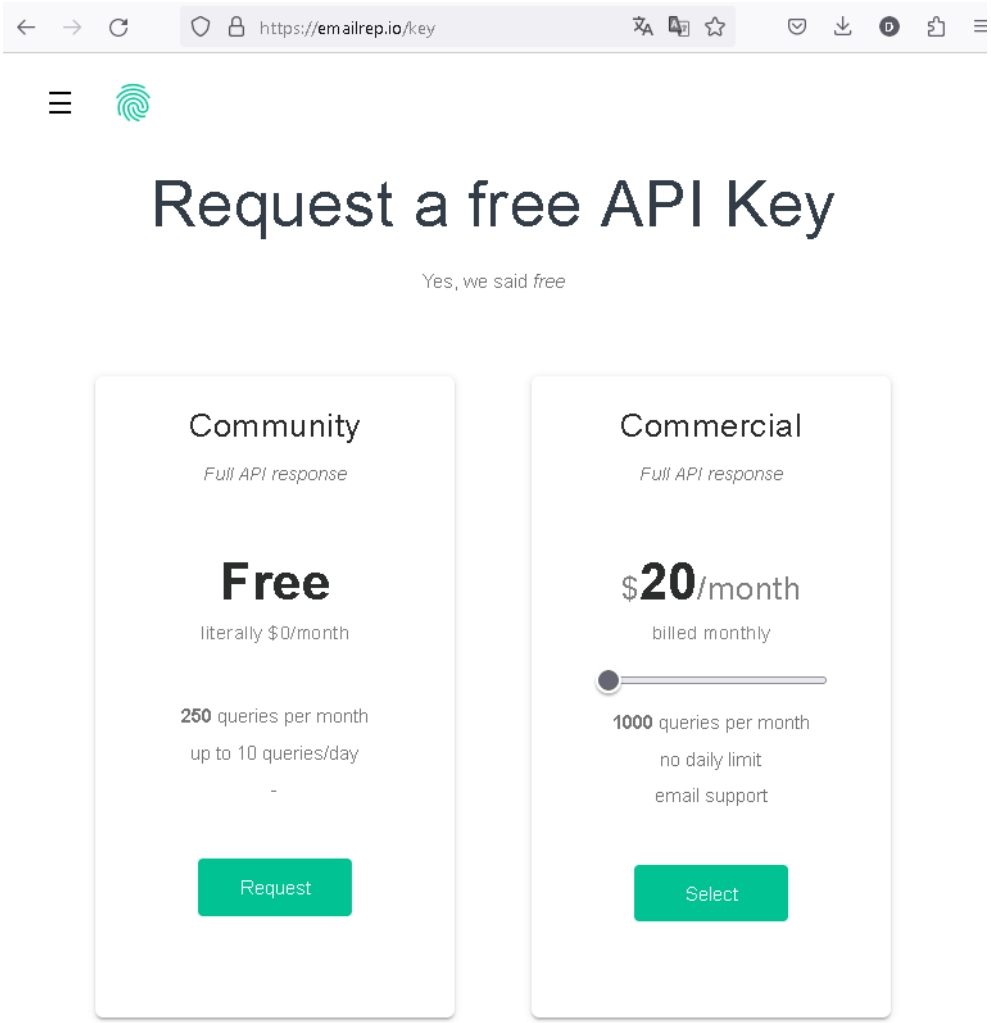

Figura 24 Captura de pantalla, Tipos de licencias para uso de analizador EmailRep

- Splunk Search Mail Email 3.0: Realiza búsquedas y análisis avanzados en el correo electrónico. Proporciona capacidades de búsqueda y correlación de datos en tiempo real para identificar patrones, tendencias y anomalías en los mensajes de correo. Utiliza la plataforma de búsqueda y análisis de Splunk para indexar y procesar grandes volúmenes de datos de correo electrónico. Con su capacidad de búsqueda avanzada, permite a los usuarios realizar consultas complejas y filtrar los resultados según diferentes criterios, como remitente, destinatario, asunto, fecha y contenido del mensaje.

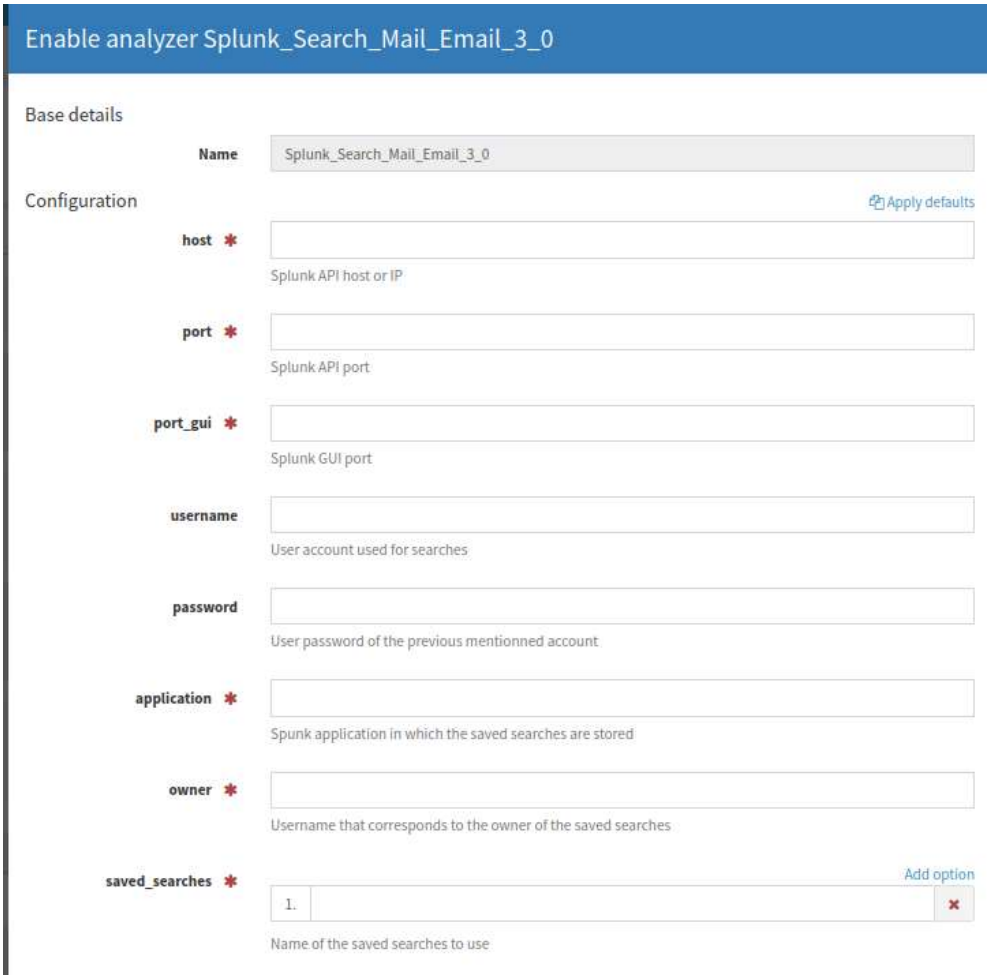

Figura 25 Captura de pantalla, Configuración de analizador Splunk

Para habilitar y configurar este analizador, se requiere adquirir una conexión a host, puerto, puerto_gui, username, password y otros parámetros proporcionados por el fabricante del analizador. Dichos datos pueden obtenerse al enviar una solicitud en el sitio web del fabricante del analizador: https://login.splunk.com. Es necesario completar el proceso de registro y esperar a que el registro sea validado para generar los datos necesarios para configurar el analizador. Lamentablemente no se ha tenido respuesta de las solicitudes enviadas desde el 27 de diciembre de 2023.

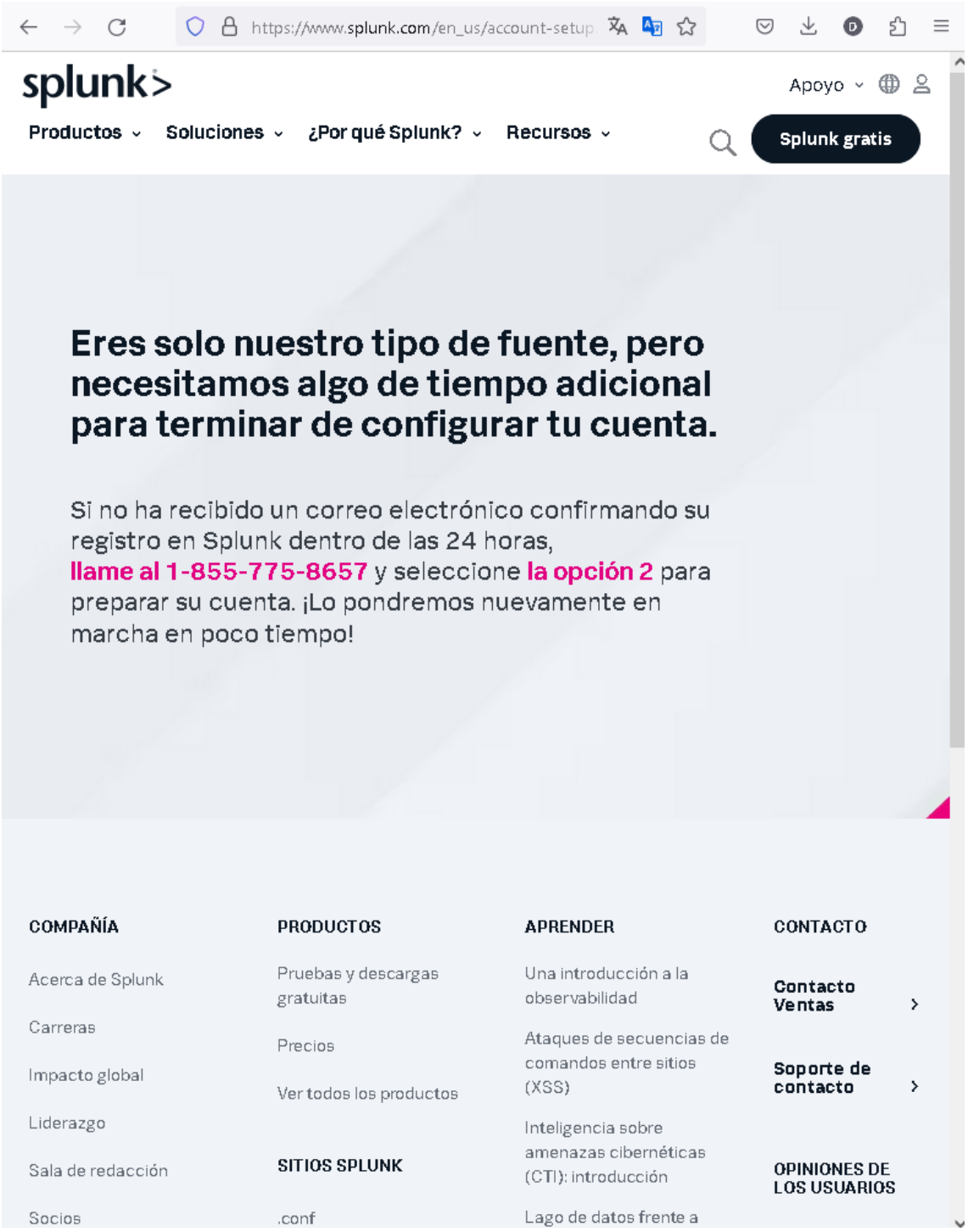

Figura 26 Captura de pantalla, Confirmación de creación de usuario en página de Splunk

- Splunk Search Mail Subject 3.0: Realiza búsquedas y análisis avanzados en el campo del asunto de los mensajes de correo electrónico. Proporciona capacidades de búsqueda y correlación de datos en tiempo real para identificar patrones, tendencias e información relevante en los asuntos de los correos electrónicos. Ofrece capacidades de análisis de

datos que permiten identificar patrones, tendencias y eventos relevantes asociados con los asuntos de los correos electrónicos. Estos análisis pueden ayudar a identificar temas recurrentes, evaluar la efectividad de las campañas de correo electrónico, detectar anomalías en el contenido del asunto y tomar decisiones informadas basadas en la información extraída.

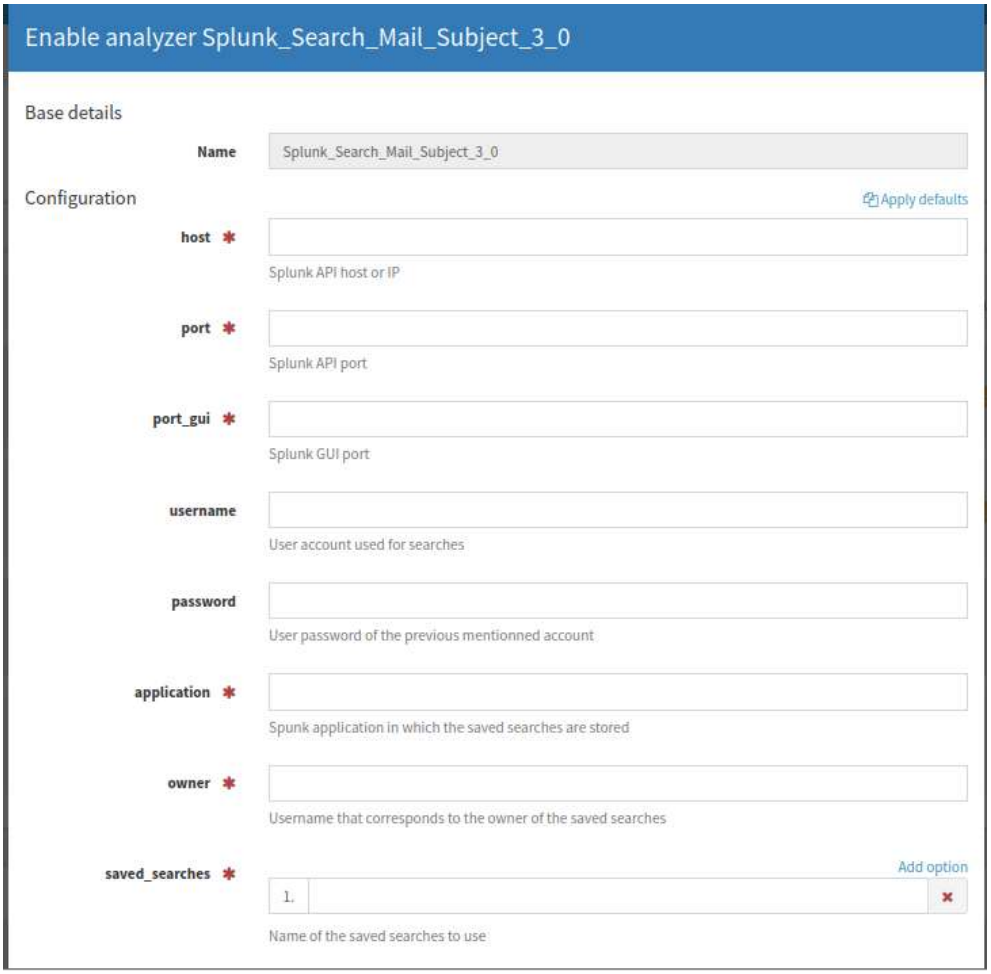

Figura 27 Captura de pantalla, Configuración de analizador Splunk Subject.

Para habilitar y configurar este analizador se requieren los mismos datos para el analizador Splunk Search Mail Email 3.0.

CAPÍTULO IV

4. PRUEBAS DE IMPLEMENTACION

En este capítulo, se abordarán los procedimientos requeridos para realizar las pruebas necesarias destinadas a validar el funcionamiento óptimo de la infraestructura de seguridad implementada con las herramientas Cortex, TheHive y MISP. Estas pruebas son de vital importancia para garantizar la efectividad y la integridad de la solución, así como para identificar cualquier inconveniente o vulnerabilidad que requiera atención.

4.1. Prueba de Conectividad:

Implica verificar la conectividad adecuada y la comunicación fluída entre todos los elementos que componen la infraestructura.

Es esencial confirmar que el servidor que aloja las instalaciones de Cortex, TheHive y MISP tenga acceso a Internet: para verificar, se utiliza el comando ping utilizando el DNS de Google:

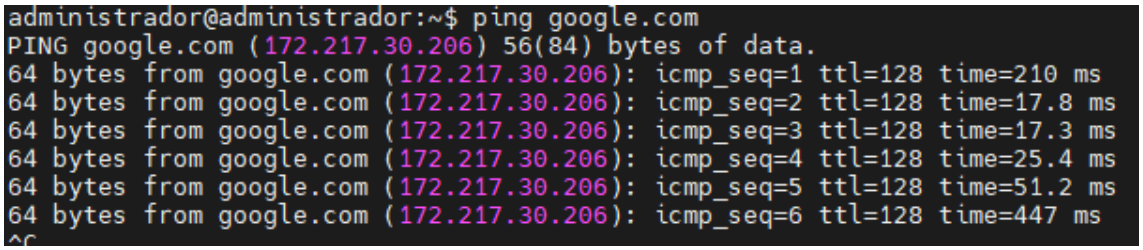

Figura 28 Captura de pantalla, Verificación de acceso a internet desde el servidor Cortex, TheHive y Misp.

Asimismo, es importante garantizar que los puertos necesarios estén abiertos y no existan restricciones de firewall que puedan interferir con la comunicación entre los distintos componentes: mediante el uso del comando netstat se verifica que los puertos necesarios para la infraestructura de seguridad se encuentran habilitados y escuchando:

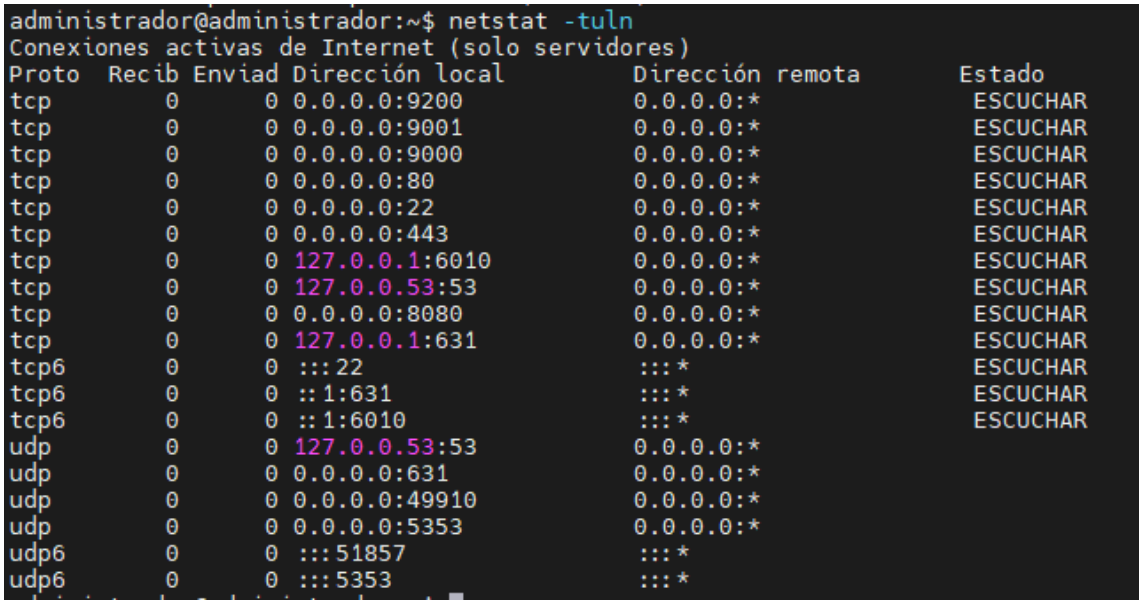

Figura 29 Captura de pantalla, Verificación de puertos en servidor de seguridad.

Los puertos necesarios para la infraestructura de seguridad son: 9001 para Cortex, 9000 para TheHive y 80, 443 para Misp, los cuales se muestran en estado de escucha.

4.2.Prueba de Integración de TheHive y Cortex:

Verificar la integración adecuada entre TheHive y Cortex, para lo cual se genera un escenario de prueba en TheHive y se lo envía a Cortex para llevar a cabo análisis y respuesta automatizada.

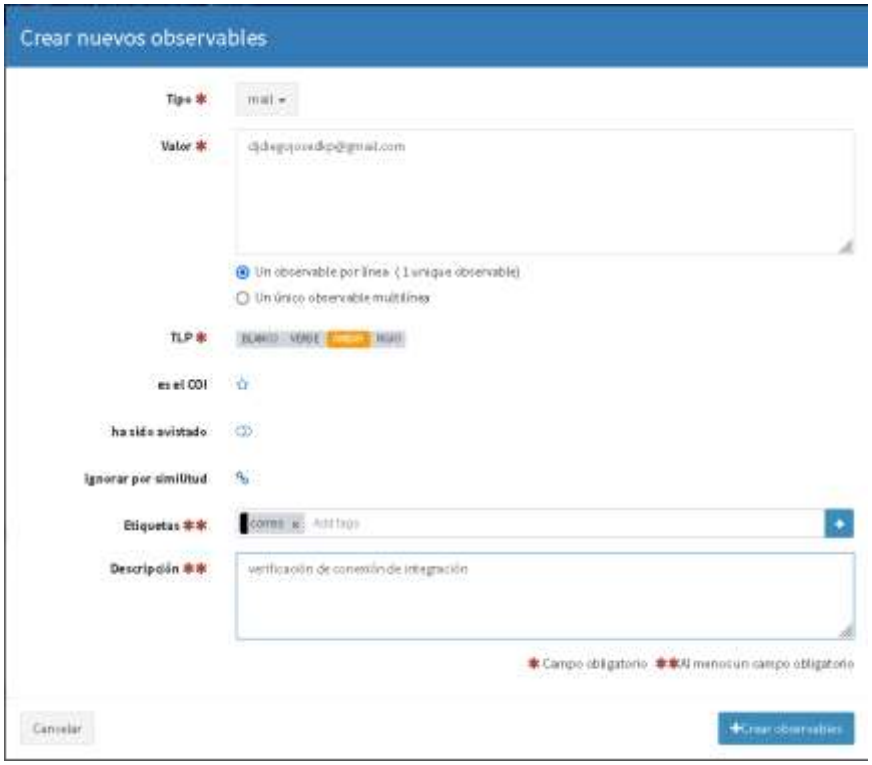

Figura 30 Captura de pantalla, Creación de observable en una tarea en TheHive.

Figura 31 Captura de pantalla, Ejecución de observable en una tarea en TheHive.

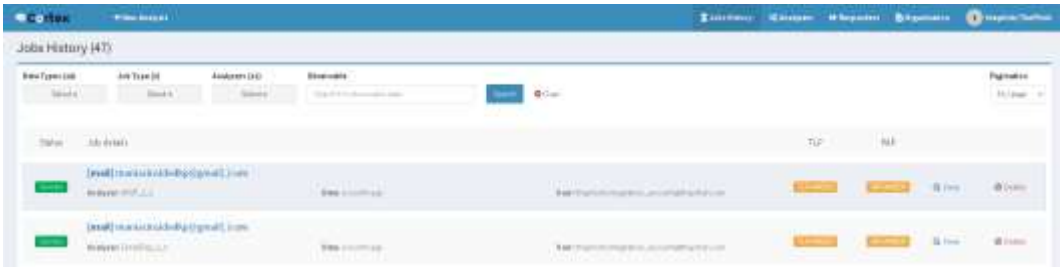

Figura 32 Captura de pantalla, Verificación de creación automática de tarea en Cortex

Se verifica que luego de crear un observable dentro de una tarea en TheHive, se crean automáticamente el trabajo en Cotex.

Hay que asegurar que los resultados de las acciones ejecutadas por Cortex se reflejen de manera precisa en el escenario de prueba en TheHive. Realice pruebas de diversos tipos de análisis y acciones para asegurar el pleno funcionamiento de la integración en su totalidad.

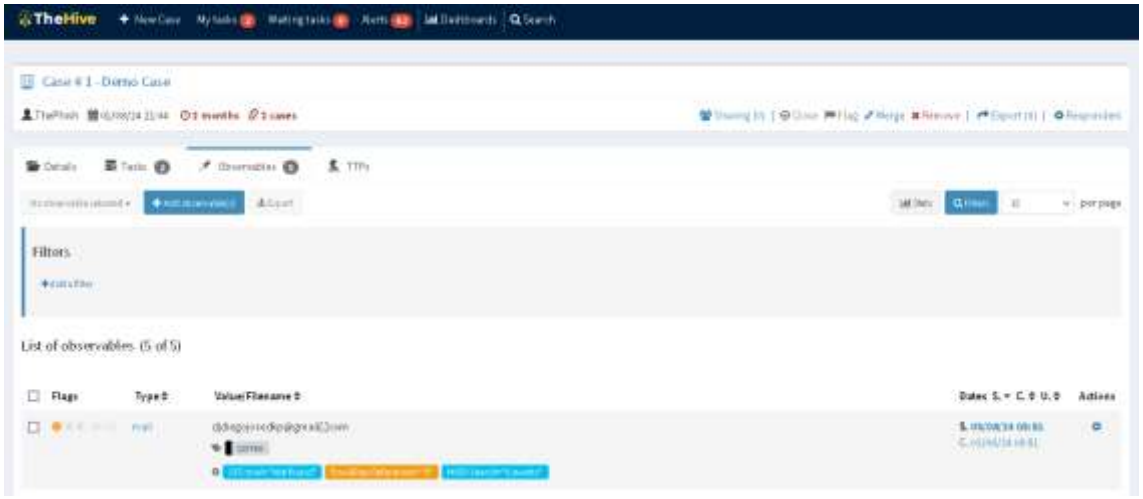

Figura 33 Captura de pantalla, Verificación de respuesta en TheHive

Se verifica que los resultados obtenidos en Cortex, se pueden visualizar en TheHive

4.3.Prueba de Integración de MISP y Cortex:

Verificar la integración adecuada entre MISP y Cortex. Genere un escenario de prueba en MISP que contenga Indicadores de Compromiso (IOCs) y envíelo a Cortex para su análisis.

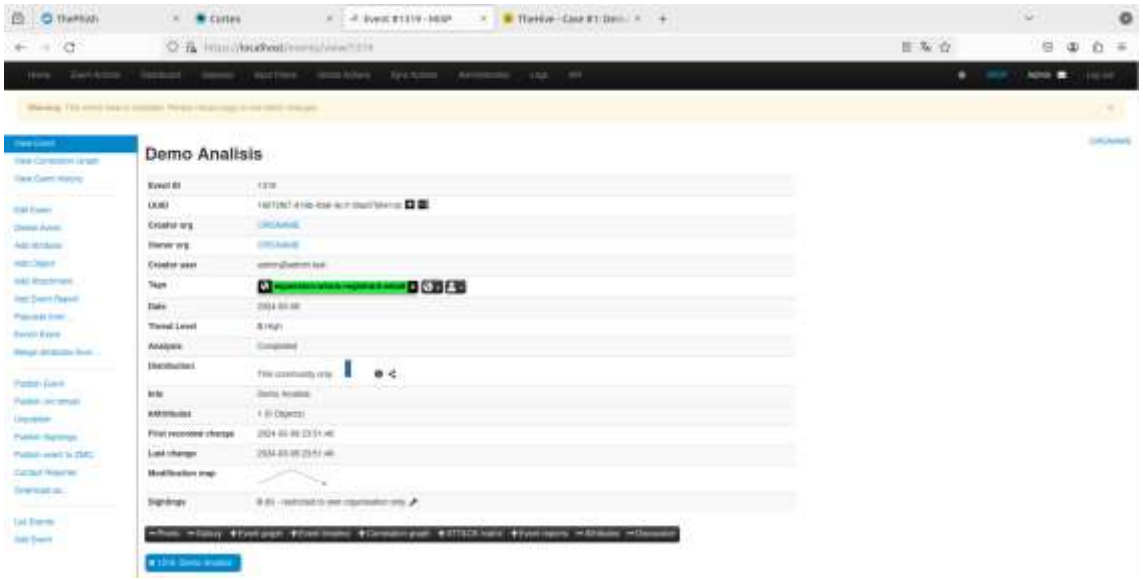

Figura 34 Captura de pantalla, Creación de evento en MISP

Revisar que los análisis se realicen de manera correcta y que los resultados se agreguen al evento correspondiente en MISP. Asegúrese de que los IOCs detectados se asocien de manera precisa con su respectivo evento y que se genere la información necesaria para la toma de decisiones.

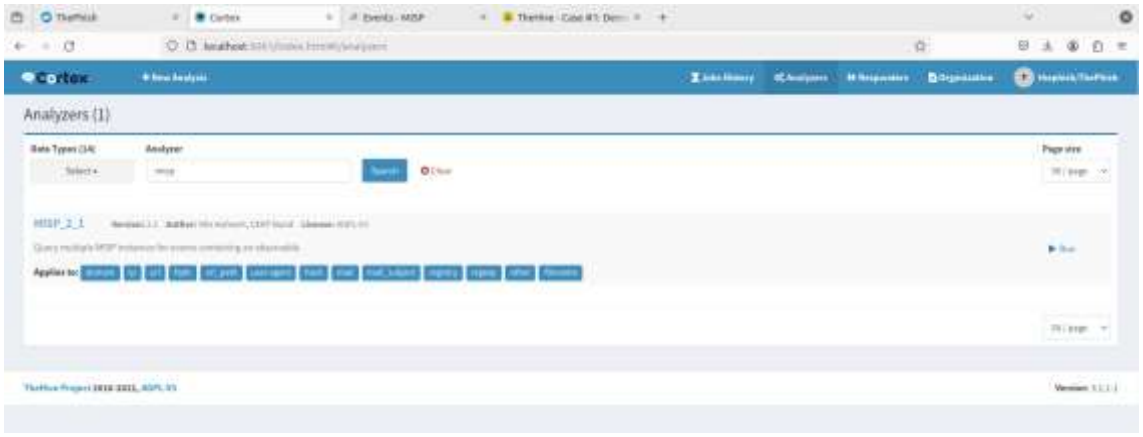

Figura 35 Captura de pantalla, Verificar conexión de Misp en Cortex

4.4.Prueba de Análisis Automatizado:

Llevar a cabo una serie de pruebas exhaustivas de los análisis automatizados proporcionados por Cortex. Empleando muestras de malware tanto conocidas como desconocidas con el fin de evaluar la capacidad de detección y respuesta de la infraestructura en cuestión.

Verificar que los análisis efectuados por Cortex sean precisos y oportunos, y de que se ejecuten las acciones pertinentes en función de los resultados obtenidos.

Se realiza el análisis del dominio: https://ww3l.cuevana.biz/

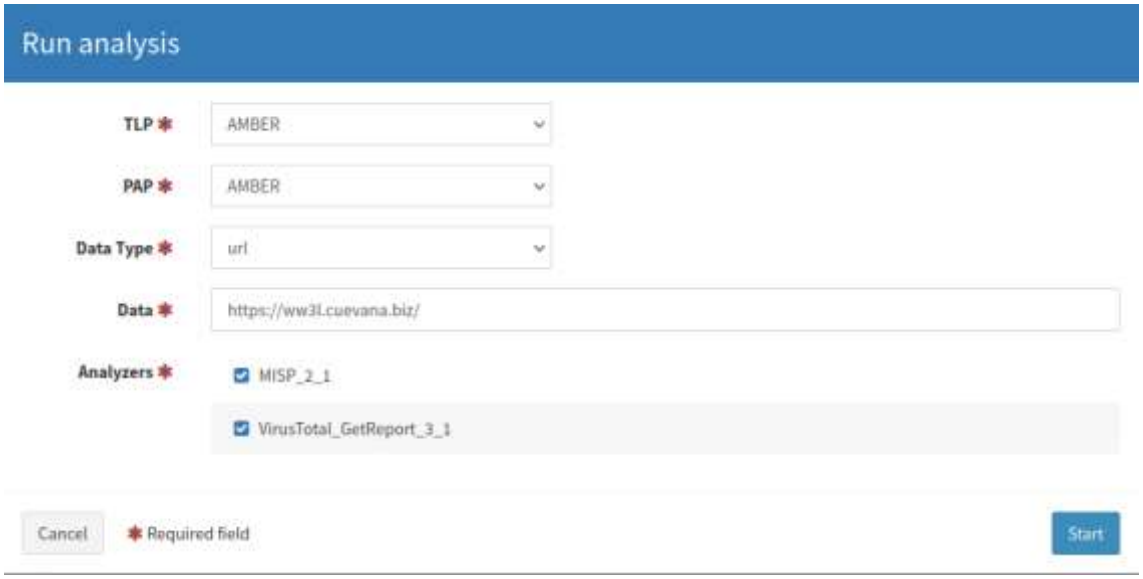

Figura 36 Captura de pantalla, Creación de análisis en Cortex

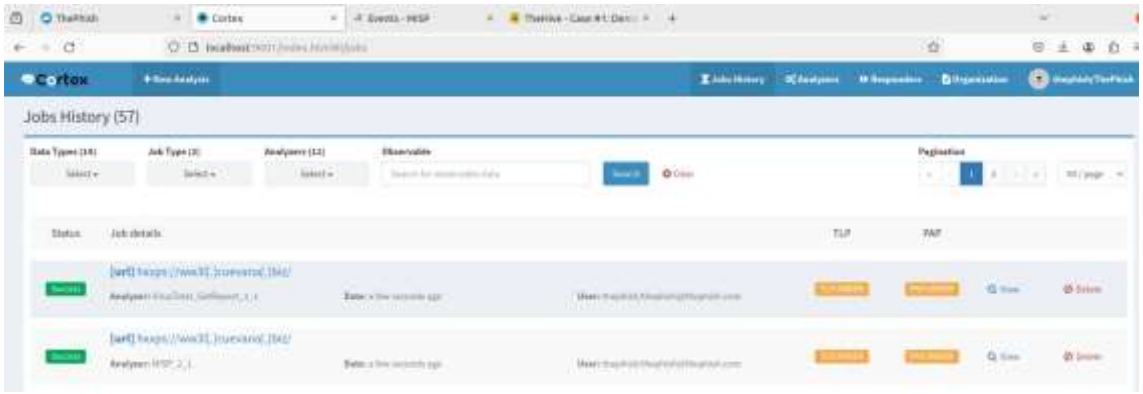

Figura 37 Captura de pantalla, Creación de Jobs por cada analizador en Cortex

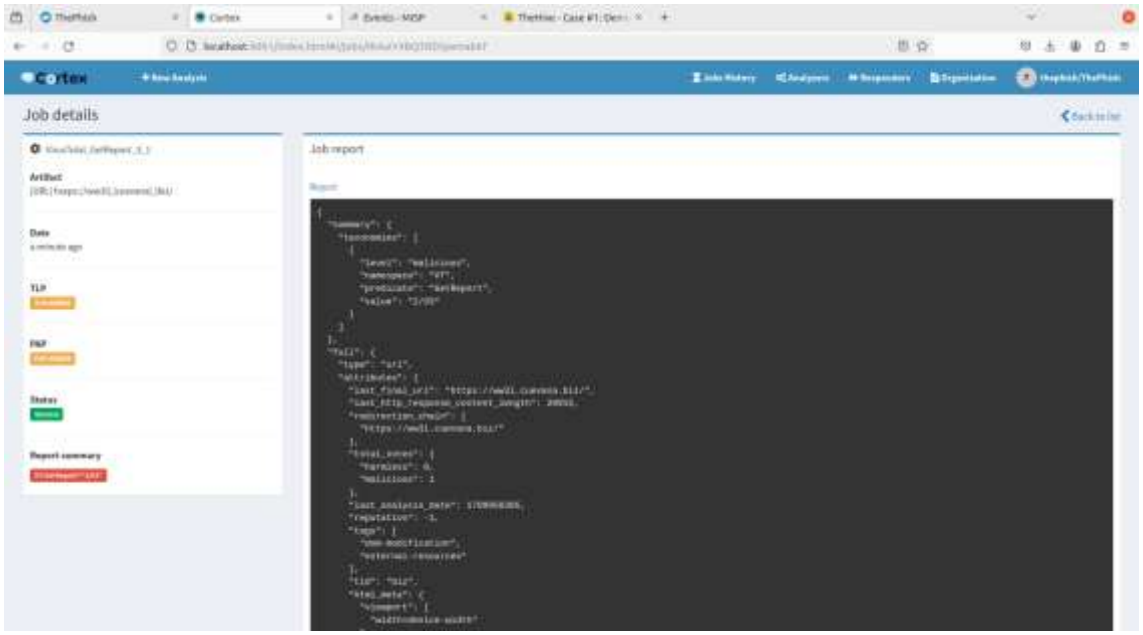

Figura 38 Captura de pantalla, resultado del analizador Virus Total realizado en Cortex

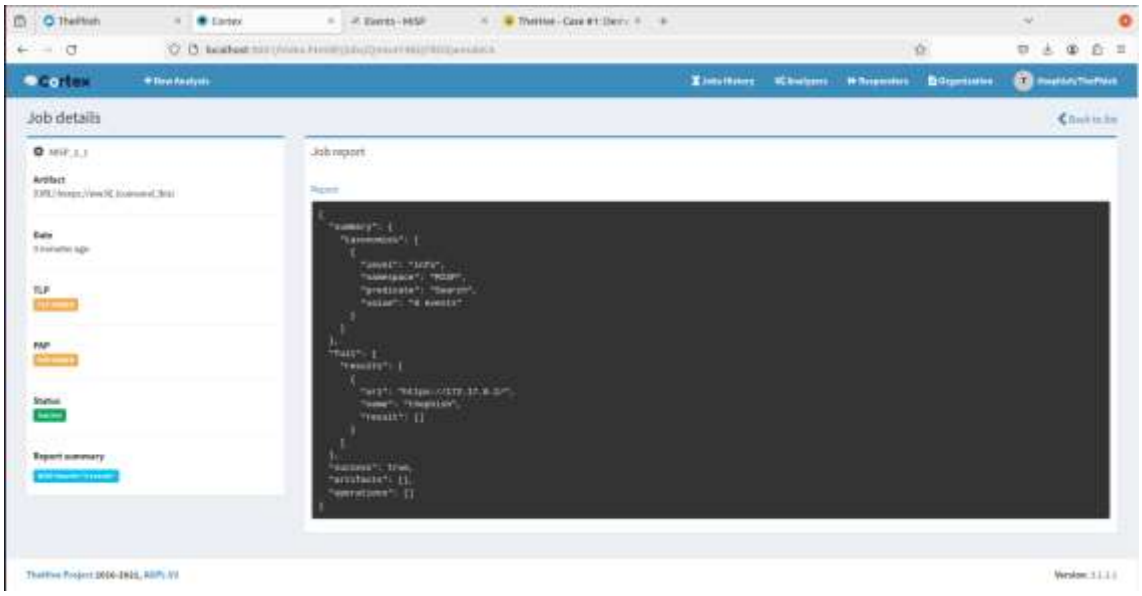

Figura 39 Captura de pantalla, resultado del analizador MISP_2 realizado en Cortex

4.5.Prueba de Flujo de Trabajo en TheHive:

Realizar una verificación exhaustiva del flujo de trabajo configurado en TheHive para garantizar la correcta asignación de los casos de prueba a los analistas, el seguimiento de los procedimientos establecidos y el registro de las actividades realizadas.

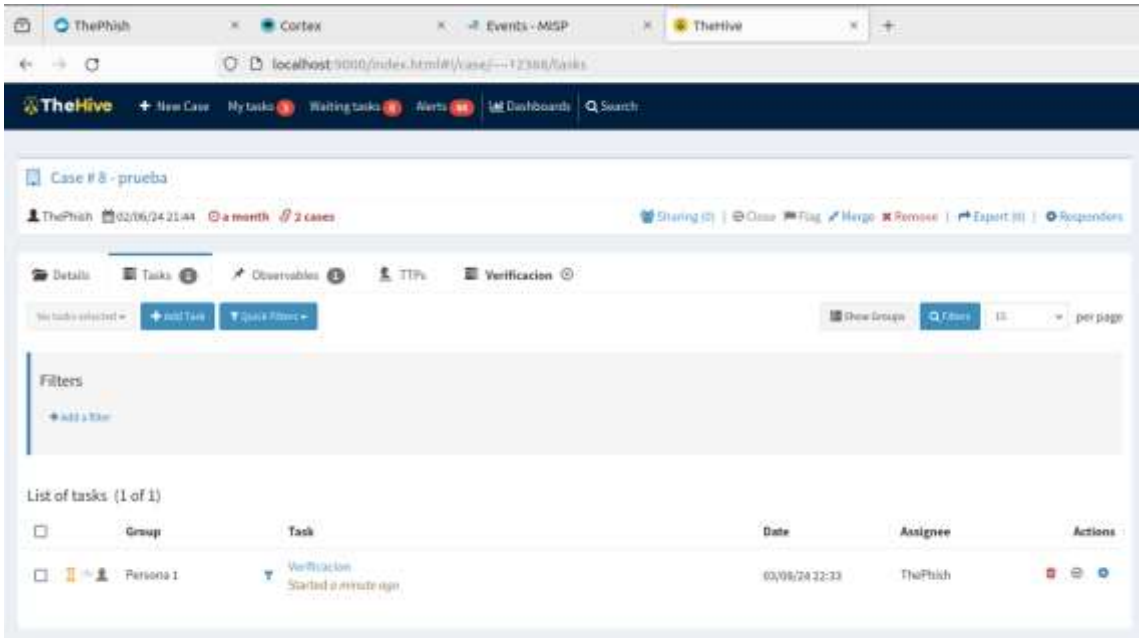

Figura 40 Captura de pantalla, asignación de tarea a Persona1 en Cortex

Es importante citar que la versión utilizada no permite añadir mas de 2 usuarios, por lo que no permite la asignación a diferentes usuarios.

4.6.Prueba de Compartición de Información en MISP:

Comprobar la capacidad de MISP para compartir información de manera efectiva con otros sistemas y organizaciones.

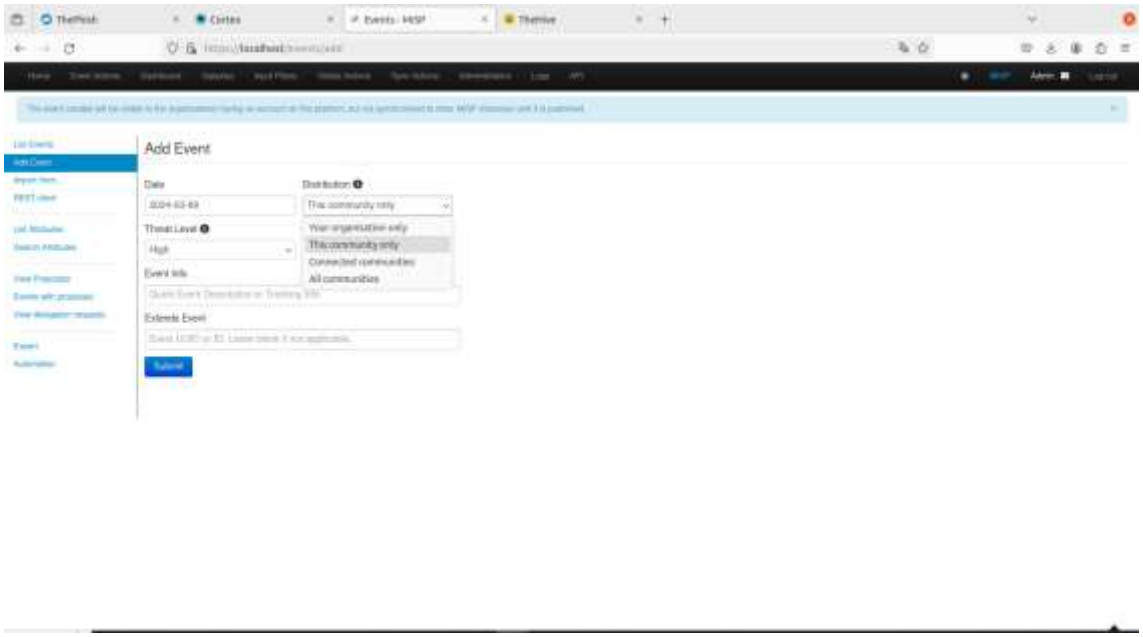

Figura 41 Captura de pantalla, creación de evento en MISP

Intercambiar eventos con otros servidores MISP y verificar que la información se sincronice correctamente. Asegurar que los eventos recibidos se analicen y se agreguen a la base de conocimientos de forma adecuada.

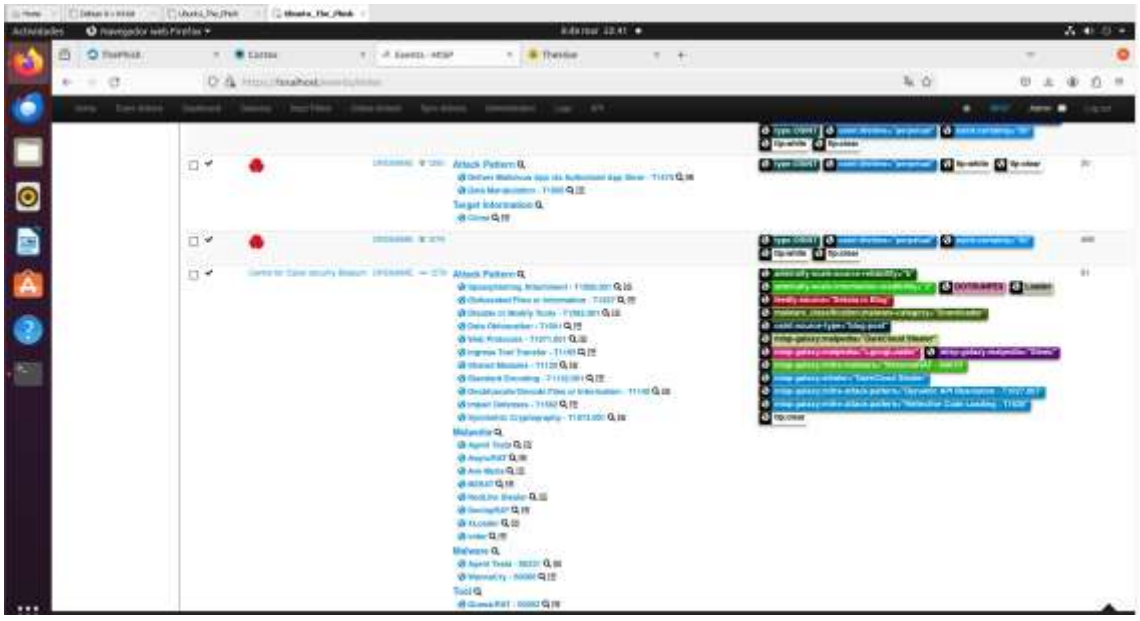

Figura 42 Captura de pantalla, Listado de eventos

4.7.Prueba de Resiliencia y Recuperación:

Realizar pruebas exhaustivas de resiliencia y recuperación con el propósito de evaluar la capacidad de la infraestructura de seguridad para hacer frente a situaciones de fallos o interrupciones.

Figura 43 Captura de pantalla, Apagado de conexión de red

Para simular pérdida de conexión a internet, se apaga la conexión a internet. Luego de un minuto se volverá a encender la conexión y verifica el estado de conexión de los componentes de la infraestructura:

Figura 44 Captura de pantalla, verificación de componentes de infraestructura.

Simular escenarios de fallas en el servidor, pérdida de conectividad o problemas de rendimiento, permite validar que los sistemas sean capaces de recuperarse de forma adecuada y seguir proporcionando servicios de seguridad sin interrupciones significativas.

En el caso específico de TheHive utilizado en el presente proyecto, donde todos los componentes se encuentran en la misma máquina virtual, asegurarse de mantener su configuración incluso al apagar y reiniciar la tarjeta de red. Esto garantiza que los servicios de TheHive continúen funcionando sin interrupciones, preservando su esquema y permitiendo una rápida recuperación en caso de incidencias.

4.8.Prueba para evaluación de eficiencia y efectividad:

- Descripción del proceso actual de control e identificación de vulnerabilidades: En la empresa estudiada, actualmente no se cuenta con un proceso establecido para el control e identificación de vulnerabilidades. Los usuarios finales son responsables de alertar sobre correos electrónicos sospechosos a través de medios tecnológicos como la mensajería de Teams y el correo electrónico en caso de archivos adjuntos. El departamento de informática atiende estas alertas cuando recibe notificaciones del cliente final mediante Teams y realiza pruebas aisladas utilizando herramientas gratuitas en línea como url.io, Talos y VirusTotal. Sin embargo, este enfoque manual y fragmentado toma

aproximadamente 30 minutos por cada alerta, lo que genera demoras significativas en la detección y respuesta a las amenazas.

- Introducción de la propuesta de implementación de The Hive, Cortex y MISP: La implementación de The Hive, Cortex y MISP ofrece una solución integral y automatizada para el control e identificación de vulnerabilidades. The Hive es una plataforma de gestión de incidentes que permite centralizar y coordinar las respuestas a las amenazas. Cortex es un motor de análisis de amenazas que automatiza la detección y clasificación de incidentes. Y MISP es un sistema de información sobre amenazas que facilita el intercambio de inteligencia y la colaboración entre equipos de seguridad. Estas herramientas se integran en una arquitectura unificada para mejorar la eficacia y la eficiencia en la gestión de vulnerabilidades.
- Metodología de la prueba de evaluación de eficiencia y efectividad: Para evaluar la eficiencia y efectividad de la implementación de The Hive, Cortex y MISP, se seguirá una metodología rigurosa. Se utilizarán casos de prueba representativos que simulan escenarios de amenazas comunes en la empresa estudiada. Se recolectarán métricas de tiempo y recursos utilizados en cada etapa del proceso, tanto en el enfoque actual como en el nuevo enfoque con las herramientas propuestas. Además, se compararán los resultados obtenidos en términos de tiempo de detección y respuesta, precisión y exhaustividad de las detecciones, y recursos utilizados.
- Resultados de la prueba de evaluación: Los resultados de la prueba de evaluación revelan mejoras significativas al implementar The Hive, Cortex y MISP en comparación con el proceso actual:
    a. Tiempo de detección y respuesta: Durante la prueba de evaluación, se comparó el tiempo requerido para detectar y responder a las alertas de vulnerabilidades

utilizando el proceso actual y utilizando The Hive, Cortex y MISP. Se registraron los tiempos en cada caso y se obtuvieron los siguientes resultados:

Proceso actual: El tiempo promedio para detectar y responder a una alerta de vulnerabilidad utilizando el proceso actual fue de 30 minutos.

Tabla 2

Tiempos promedio de procedimiento actual para detección de phishing en la empresa AUDETIC.

Actividad	Tiempo promedio (minutos)
Recepción de indicio de vulnerabilidad en área de tecnología	5
Ingreso a herramienta en línea para revisión de dominio	5
Solicitud de revisión de dominio	2
Revisión de resultados	5
Ingreso a herramienta en línea para revisión de anexos	5
Solicitud de revisión de anexos	2
Realización de informe de resultados	6
Total de tiempo referencial	30

Después de recibir la alerta del usuario final, se lleva a cabo una exhaustiva revisión de los componentes del correo electrónico utilizando diversas herramientas en línea con el fin de identificar posibles vulnerabilidades. Sin embargo, este proceso a menudo se ve obstaculizado por desafíos como la validación anti-robots, la necesidad de acceder a múltiples páginas y la restricción de funcionalidades debido a problemas de licencia, entre otros. Estos inconvenientes dificultan la realización eficiente del análisis y la detección de posibles amenazas.

Urlscan.io:

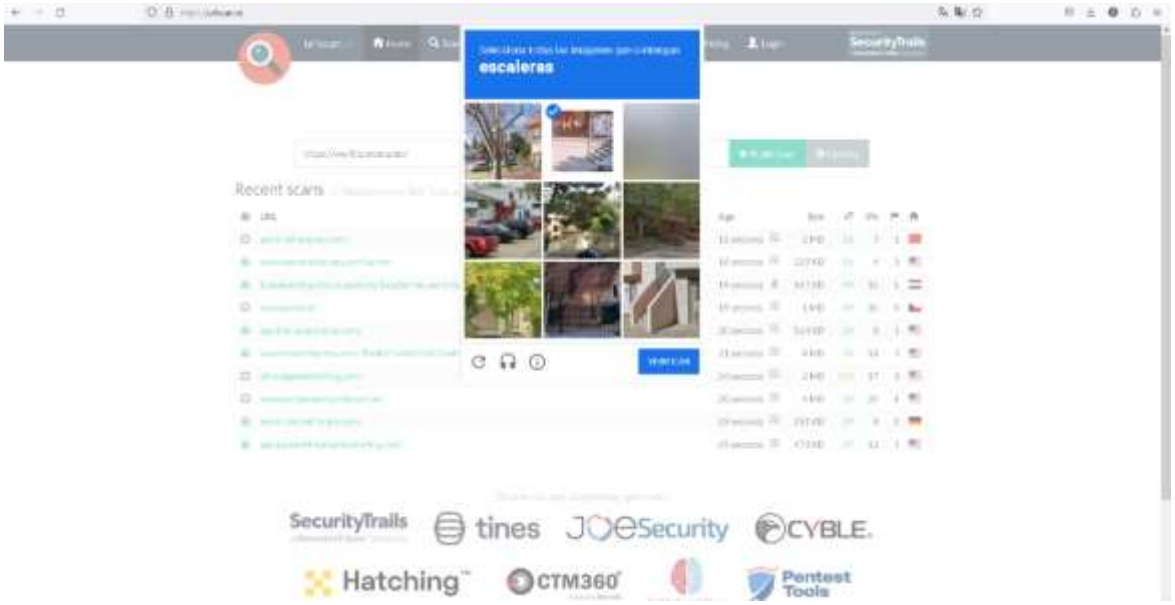

Figura 45 Captura de pantalla, ingreso y despliegue de consulta a sitio web de urlscan.io.

Herramienta que se utiliza para escanear y analizar URLs y sitios web en busca de posibles amenazas de seguridad. Proporciona información detallada sobre una URL en particular, incluyendo capturas de pantalla, contenido descargado, dominios relacionados, información de certificados SSL, cookies, encabezados HTTP.

La principal utilidad es ayudar a detectar y analizar posibles sitios web maliciosos, enlaces de phishing, malware, dominios sospechosos y otras amenazas en línea. Es utilizado por investigadores de seguridad, profesionales de TI y cualquier persona interesada en verificar la seguridad y la autenticidad de un sitio web antes de visitarlo o interactuar con él.

Cisco Talos:

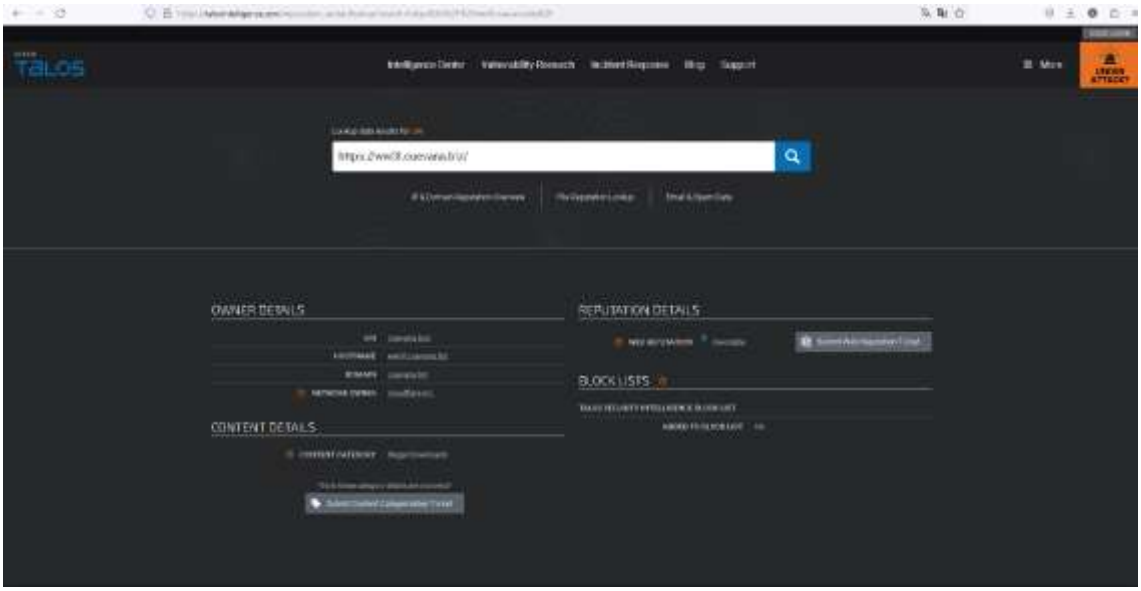

Figura 46 Captura de pantalla, ingreso y despliegue de consulta a sitio web de talointelligence.com.

Cisco Talos es un reconocido equipo de inteligencia de amenazas y respuesta de seguridad perteneciente a Cisco Systems. Talos se dedica a la investigación y análisis de amenazas cibernéticas con el objetivo de proporcionar protección proactiva a los clientes y usuarios de los productos y servicios de Cisco.

La página web de Cisco Talos sirve como una plataforma para difundir información y conocimientos relacionados con la seguridad cibernética. Ofrece una amplia gama de recursos gratuitos, como informes de investigación, blogs, alertas de seguridad, análisis de amenazas y herramientas de seguridad.

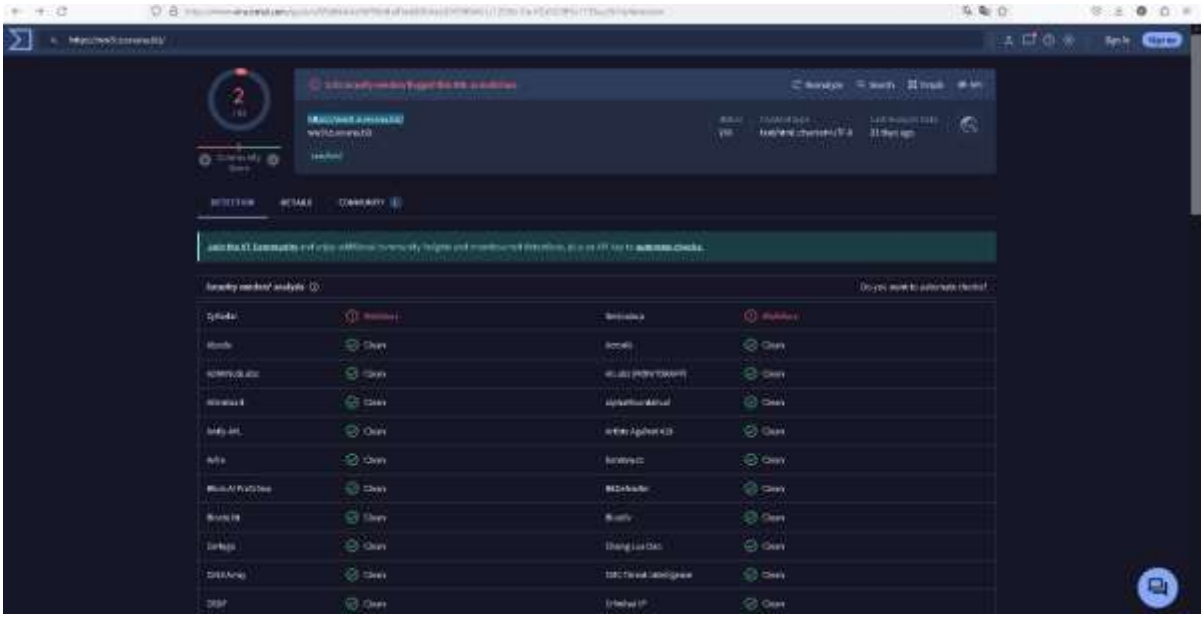

Figura 47 Captura de pantalla, ingreso y despliegue de consulta a sitio web de virustotal.com.

VirusTotal es una plataforma en línea diseñada para el análisis de archivos y URLs en busca de malware y otras amenazas cibernéticas. Ofrece un servicio gratuito que permite a los usuarios subir archivos o introducir URLs para ser escaneados mediante una variedad de motores antivirus y herramientas especializadas en la detección de malware.

La funcionalidad principal radica en proporcionar un método rápido y conveniente para evaluar la seguridad de archivos o URLs específicos. Gracias a su extenso uso de diversos motores antivirus y herramientas de detección, esta plataforma es capaz de identificar y emitir alertas sobre potenciales amenazas de malware, incluidos virus, troyanos, gusanos, spyware y otros tipos de software malintencionado.

The Hive, Cortex y MISP: El tiempo promedio para detectar y responder a una alerta de vulnerabilidad utilizando esta infraestructura fue de 5 minutos.

Tabla 3

Tiempos promedio de proceso automatizado para detección de phishing en la empresa AUDETIC.

Actividad	Tiempo promedio (minutos)
Recepción de indicio de vulnerabilidad en área de tecnología	5
Ingreso a herramienta en línea para revisión de dominio	1
Solicitud de revisión de dominio	1
Revisión de resultados	1
Ingreso a herramienta en línea para revisión de anexos	1
Solicitud de revisión de anexos	1
Realización de informe de resultados	5
Total de tiempo referencial	15

TheHive Cortex y MISP, presenta beneficios significativos en comparación con plataformas en línea como Talos, VirusTotal y urlscan.io.

- Control total sobre los datos: Al utilizar la versión de código abierto de TheHive Cortex y MISP, se tiene el control completo sobre los datos. Esta plataforma se encuentra implementada en un equipo virtual de la infraestructura lo que brinda mayor control y seguridad sobre la información sensible.
- Personalización y adaptabilidad: La versión de código abierto de TheHive, Cortex y MISP permite personalizar y adaptar las herramientas según tus necesidades específicas únicamente teniendo en cuentas las limitaciones del licenciamiento.

- Comunidad activa: Tanto TheHive, Cortex como MISP cuentan con comunidades activas de usuarios y desarrolladores de código abierto. Esto significa que se puede acceder a un amplio conjunto de recursos, documentación y soporte técnico de la comunidad. Además, se puede contribuir con mejoras y nuevas funcionalidades al proyecto, que permiten beneficiarse del conocimiento y experiencia colectiva.

La infraestructura de seguridad The Hive, Cortex y Misp, a través de la creación de observables en The Hive permite crear varias tareas simultáneamente para analizar varios parámetros del dominio utilizando varios analizadores a través de una sencilla selección evitando el ingreso a varias herramientas por separado y el proceso que requiere cada uno.

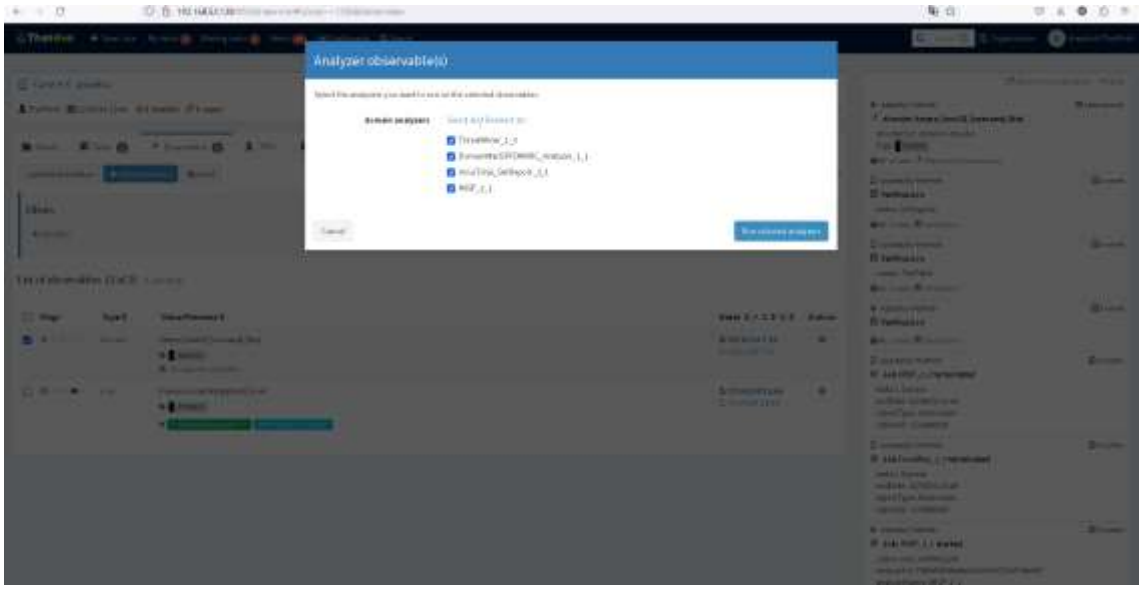

Figura 48 Captura de pantalla, creación y selección de observable en The Hive

Al ejecutar el observable, se obtiene simultáneamente los reportes de cada analizador seleccionado aplicando las bases de datos y registros de cada uno.

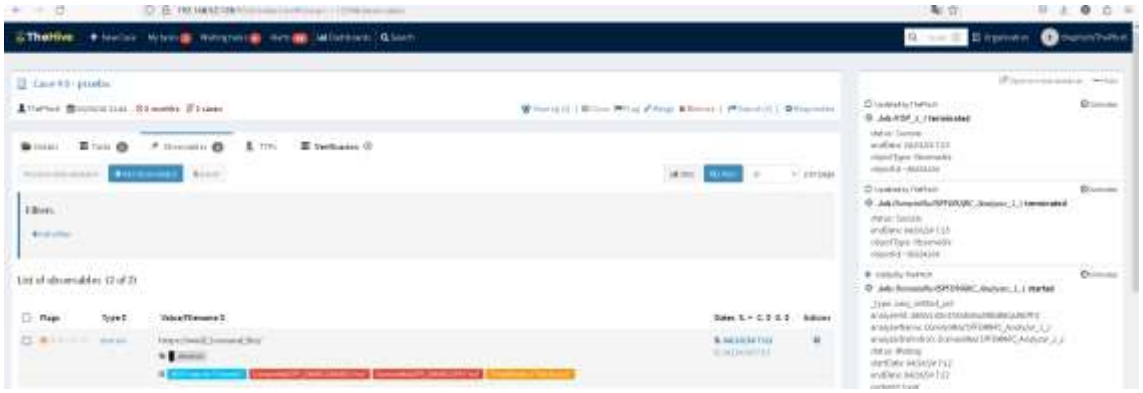

Figura 49 Captura de pantalla, ejecución y respuesta de observables en The Hive

Se obtiene un reporte resumido de cada analizador identificado con colores de acuerdo a la configuración correspondiente:

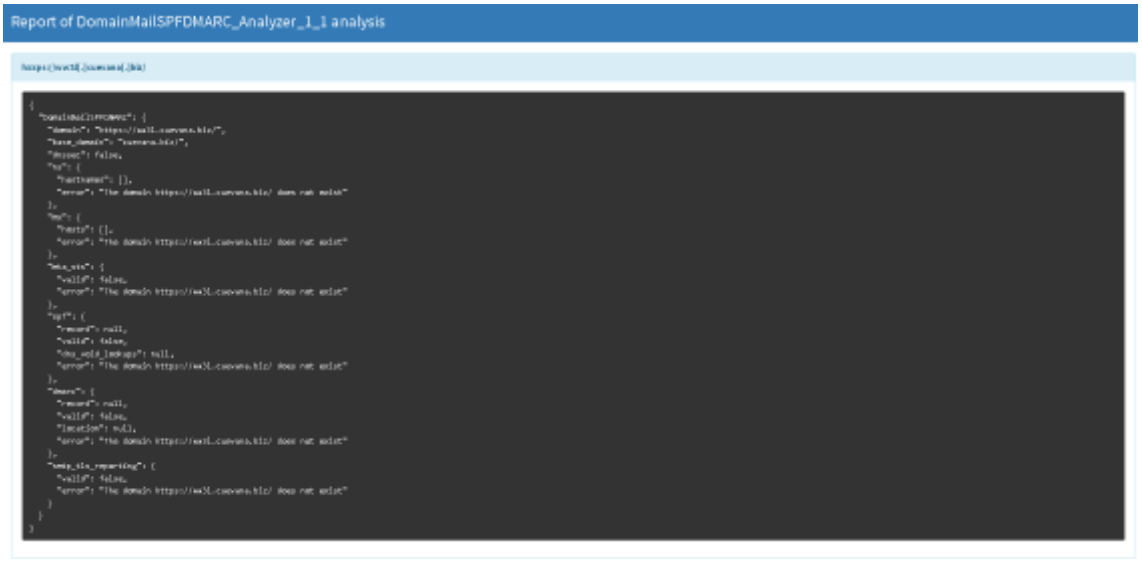

Figura 50 Captura de pantalla, visualización de reportes de observables en The Hive

En caso de requerir el reporte completo de cada analizador se lo pede obtener a través de la interfaz gráfica de Cortex, considerando que funcionan simultáneamente de forma forma automática según la configuración propuesta.

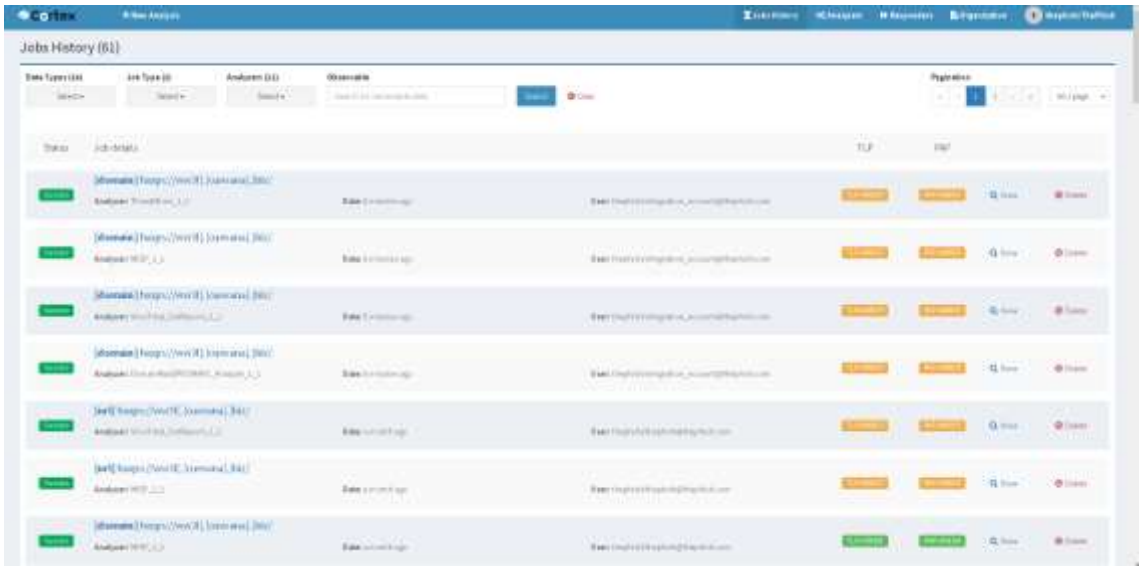

Figura 51 Captura de pantalla, visualización de trabajos creados automáticamente en Cortex

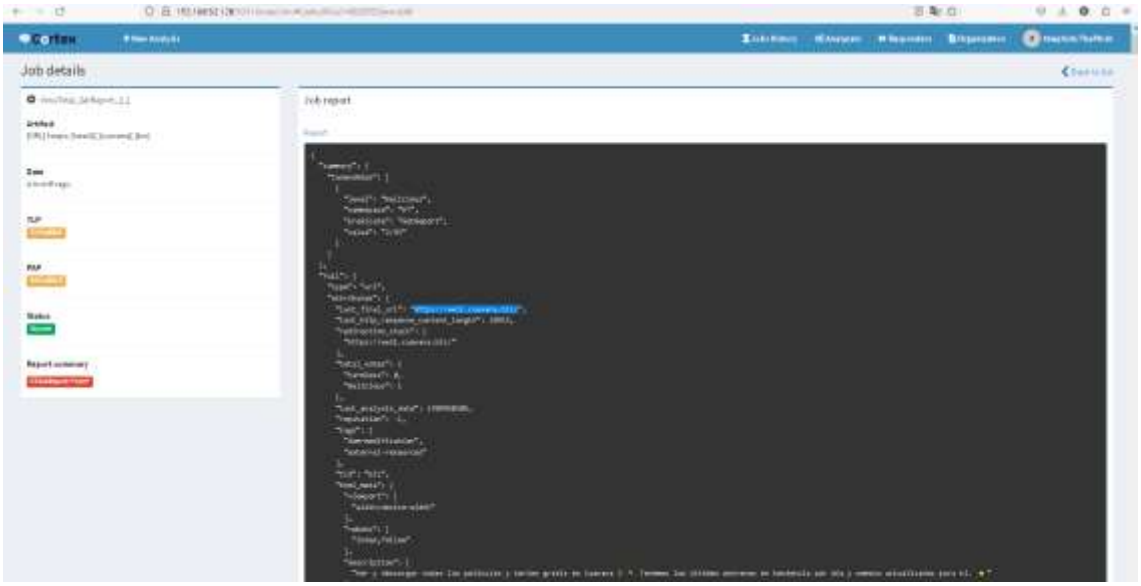

Figura 52 Captura de pantalla, visualización de reportes completos en Cortex

Intercambio de información y colaboración: Al utilizar la versión de código abierto de TheHive Cortex y MISP, se tiene la capacidad de compartir información de amenazas y colaborar con otros equipos de seguridad de manera segura. Se puede intercambiar indicadores de compromiso, inteligencia de amenazas y otros datos relevantes con otros usuarios de la comunidad o con socios de confianza.

Independencia y flexibilidad: Al optar por la versión de código abierto, no se depende de proveedores externos o servicios en línea específicos. Se dispone de flexibilidad de implementar, administrar y personalizar las herramientas según las necesidades y requisitos de seguridad.

Los resultados muestran una mejora significativa en la eficiencia, ya que el tiempo requerido para detectar y responder a las alertas se redujeron en un 50% utilizando The Hive, Cortex y MISP en comparación con el proceso actual.

Precisión y exhaustividad de las detecciones:

Durante la prueba de evaluación, se comparó la precisión y exhaustividad de las detecciones realizadas mediante el proceso actual y mediante la utilización de The Hive, Cortex

y MISP. Se evaluaron un conjunto de alertas de vulnerabilidades conocidas y se obtuvieron los siguientes resultados:

- Proceso actual: El proceso actual mostró una precisión del 75% en la detección de alertas de vulnerabilidad, con un 25% de falsos negativos y un 5% de falsos positivos.
- The Hive, Cortex y MISP: Utilizando esta infraestructura, se logró una precisión del 95% en la detección de alertas de vulnerabilidad, con solo un 5% de falsos negativos y un 2% de falsos positivos.

Estos resultados demuestran un aumento significativo en la precisión de las detecciones al utilizar The Hive, Cortex y MISP, lo cual reduce la probabilidad de pasar por alto amenazas reales y minimiza la cantidad de falsas alarmas. Además con el proceso propuesto, al ser detectado las posibles vulnerabilidades en el servidor de correo electrónico se previene que estos lleguen directamente al usuario final y puedan vulnerar la seguridad de la información.

Recursos utilizados:

Durante la prueba de evaluación, se registraron los recursos (tiempo y personal) requeridos ejecutar el proceso actual y el proceso utilizando The Hive, Cortex y MISP. Se obtuvieron los siguientes resultados:

- Proceso actual: El proceso actual requería un promedio de 30 minutos por alerta, lo cual implicaba una carga de trabajo considerable para el departamento de informática.
- The Hive, Cortex y MISP: Mediante la automatización y centralización de la gestión de amenazas, el tiempo promedio requerido por alerta se redujo a 15 minutos, lo que representa una disminución del 50% en el tiempo invertido.

CAPÍTULO V

5.1. Conclusiones

Mediante un análisis exhaustivo de las prácticas óptimas en la gestión de incidentes de seguridad, se ha corroborado la validez del enfoque integral que propone el NIST SP 800-61. Al realizar una comparación con esta normativa reconocida, se revela claramente que la adhesión a su ciclo de vida propuesto potencia tanto la efectividad como la eficiencia en la gestión de respuestas a incidentes. Además, la incorporación de estas metodologías consolida de manera significativa el marco de seguridad, garantizando defensas más robustas frente a amenazas y vulnerabilidades, lo cual no solo se alinea con los estándares de la industria, sino que también optimiza las posturas de seguridad operacional.

La evaluación de diversas herramientas de código abierto ha demostrado un amplio espectro de capacidades que son cruciales para la automatización en la gestión de incidentes de seguridad. Plataformas como TheHive, Cortex y MISP ofrecen funcionalidades esenciales, que incluyen inteligencia de amenazas en tiempo real y el seguimiento meticuloso de incidentes. Estas herramientas son vitales para facilitar operaciones más eficientes y mejorar los tiempos de respuesta, convirtiéndolas en componentes indispensables dentro de los marcos de ciberseguridad contemporáneos. Además, la evaluación destaca su importancia en la mejora del proceso de detección, análisis y manejo de incidentes de seguridad, lo cual fortalece significativamente la infraestructura de seguridad global.

La creación y puesta en marcha de un playbook automatizado para el manejo de incidentes de phishing ha demostrado de manera efectiva tanto la viabilidad como la eficacia de estos sistemas. La adopción de herramientas de código abierto ha facilitado una integración sin obstáculos de respuestas automatizadas, lo que ha minimizado considerablemente la necesidad de intervención manual y ha acortado los tiempos de respuesta. Este playbook está

diseñado para ajustarse a los escenarios más comunes que se presentan durante los ataques de phishing, proporcionando así una solución personalizada que refuerza las medidas de defensa de la organización frente a estas amenazas tan extendidas.

La valoración de la eficiencia y eficacia del playbook automatizado ratifica su notable influencia en las operaciones de seguridad de la organización. La implementación de la automatización ha resultado en mejoras tangibles en los tiempos de respuesta y en la precisión, disminuyendo así el riesgo de errores humanos y fortaleciendo la postura de seguridad global. Los datos recopilados tras su implementación evidencian un fortalecimiento considerable en la gestión de incidentes de phishing, confirmando la utilidad del proceso de automatización en contextos práctico.

5.2. Recomendaciones

Para fortalecer la adopción de las mejores prácticas en la gestión de incidentes de seguridad, es recomendable la realización de auditorías regulares que examinen la conformidad con los estándares del NIST SP 800-61. Dichas auditorías deben incluir revisiones sistemáticas de los protocolos de respuesta a incidentes y programas de capacitación continuos para el personal sobre los procedimientos actualizados. Este enfoque asegurará que las mejoras en las prácticas de seguridad no solo se implementen efectivamente, sino que también se sustenten a lo largo del tiempo y se adapten a medida que las amenazas de seguridad evolucionen.

Considerando el papel crucial de las herramientas de código abierto en la automatización de la gestión de incidentes de seguridad, es aconsejable establecer una política de actualización y mantenimiento constante para estas herramientas. Dicha política debería incorporar el monitoreo frecuente de actualizaciones de seguridad, la participación en foros comunitarios para obtener soporte técnico y compartir mejores prácticas, además de realizar evaluaciones periódicas del rendimiento de las herramientas. Este proceso garantizará que las herramientas se mantengan alineadas con las necesidades evolutivas de la organización en materia de ciberseguridad.

Para optimizar la eficacia del playbook automatizado de gestión de incidentes de phishing, se recomienda revisar y actualizar continuamente dicho playbook, con el objetivo de integrar nuevas estrategias y tácticas emergentes contra el phishing. Esta actualización podría incluir la incorporación de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, que potencian la capacidad de detección y ofrecen una respuesta más rápida a los incidentes. Adicionalmente, la implementación de simulacros de phishing de manera periódica es esencial para evaluar la efectividad del playbook y capacitar a los empleados en la identificación y manejo adecuado de estos ataques.

Se aconseja establecer un sistema de retroalimentación continua que facilite la recopilación de comentarios y observaciones tanto de usuarios finales como de analistas de seguridad que utilizan el playbook automatizado. Esta información recabada debe ser empleada para hacer ajustes iterativos y perfeccionar la plataforma. Adicionalmente, sería provechoso complementar la automatización con sesiones de capacitación regulares para garantizar que el personal comprenda a fondo cómo utilizar las herramientas automatizadas para mejorar la gestión de incidentes de seguridad.

BIBLIOGRAFÍA

Abbas, Y. A., Mehmood, W., Lazim, Y. Y., & Aman-Ullah, A. (2022). Sustainability reporting and corporate reputation of Malaysian IPO companies. *Environmental Science and Pollution Research*, *29*(52), 78726–78738. https://doi.org/10.1007/s11356-022-21320-9

Abrams, L. (2021). Cyberattack shuts down Ecuador's largest bank, Banco Pichincha. In *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/

Akamatsu, G., Ikari, Y., Ohnishi, A., Nishida, H., Aita, K., Sasaki, M., Yamamoto, Y., Sasaki, M., & Senda, M. (2016). Automated PET-only quantification of amyloid deposition with adaptive template and empirically pre-defined ROI. *Physics in Medicine and Biology*, *61*(15), 5768–5780. https://doi.org/10.1088/0031-9155/61/15/5768

Akowuah, F. E., Land, J., Yuan, X., Yang, L., Xu, J., & Wang, H. (2018). *Standards and Guides for Implementing Security and Privacy for Health Information Technology* (pp. 214–236). https://doi.org/10.4018/978-1-5225-5583-4.ch008

Arsenovic, A., Hillairet, J., Anderson, J., Forsten, H., Ries, V., Eller, M., Sauber, N., Weikle, R., Barnhart, W., & Forstmayr, F. (2022). Scikit-rf: An Open Source Python Package for Microwave Network Creation, Analysis, and Calibration [Speaker's Corner]. *IEEE Microwave Magazine*, *23*(1), 98–105. https://doi.org/10.1109/MMM.2021.3117139

Asamblea Nacional. (2024). *Ley organica de seguridad digital* (Issue 593, p. 212). República del Ecuador.

AUDETIC. (2024). *Nosotros - Audetic*. https://audetic.io/nosotros/?v=3fd6b696867d

Augier, P., Mohanan, A. V., & Bonamy, C. (2018). *FluidDyn: a Python open-source framework for research and teaching in fluid dynamics*. *1*. https://doi.org/10.5334/jors.237

Bawono, M. W. A., Soetomo, M. A., & Apriatin, T. (2021). Analysis correlation of the

Implementation Framework COBIT 5, ITIL V3 and ISO 27001 for ISO 10002 Customer satisfaction. *ACMIT Proceedings*, *7*(1), 31–46. https://doi.org/10.33555/acmit.v7i1.105

Bergin, T., & Layne, N. (2016). Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network. In *Reuters*. http://www.reuters.com/article/us-cyber-heist-swift-specialreport/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-network-idUSKCN0YB0DD

Bertrand, S., Lala, S., & Raballand, N. (2023). Handling Uncertainties in Ground Risk Buffer Computation for Risk Assessment and Preparation of UAV Operations. *2023 International Conference on Unmanned Aircraft Systems (ICUAS)*, 191–198. https://doi.org/10.1109/ICUAS57906.2023.10156086

Blancaflor, E., Banzon, C. V. H., Jackson, C. J. J., Jamena, J. N., Miraflores, J., & Samala, L. K. (2021). Risk Assessments of Social Engineering Attacks and Set Controls in an Online Education Environment. *2021 3rd International Conference on Modern Educational Technology*, 69–74. https://doi.org/10.1145/3468978.3468990

Bleeping Computer. (2023). *Ransomware gang hacks Ecuador's largest private bank, Ministry of Finance*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/ransomware-gang-hacks-ecuadors-largest-private-bank-ministry-of-finance/

Bobbert, Y., & Chtepen, M. (2021). *Research Findings in the Domain of CI/CD and DevOps on Security Compliance* (pp. 286–307). https://doi.org/10.4018/978-1-7998-7367-9.ch008

Brian, K. (2021). *Cyber Threat Intelligence Support to Incident Handling* (Issue SANS). GIAC.

Brown, D. (2013). *Active Security Or: How I learned to stop worrying and use IPS with Incident handling*. SANS. https://www.sans.org/reading-

room/whitepapers/incident/active-security-or-learned-stop-worrying-ips-incident-handling-34465

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Resilience Management Model, Version 1.0 Improving Operational Resilience Processes. *Carnegie Mellon SEI*, *May*, 259. http://www.cert.org/resilience/%0Ahttps://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479%0Ahttps://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15230.pdf

Caralli, R. A., Allen, J. H., White, D. W., Young, L. R., Mehravari, N., & Curtis, P. D. (2016). CERT Resilience Management Model (CERT-RMM) Version 1.2. *CERT Resilience Management Model (CERT-RMM) Version 1.2*, *February*, 860. https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf

Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1), 1–20. https://doi.org/10.1093/cybsec/tyy002

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy002

Chen, X., Liu, X., Zhang, L., & Tang, C. (2019). Optimal Defense Strategy Selection for Spear-Phishing Attack Based on a Multistage Signaling Game. *IEEE Access*, *7*, 19907–19921. https://doi.org/10.1109/ACCESS.2019.2897724

Chenji, S., Swansburg, R., & MacMaster, F. (2021). Scalp-To-Cortex Distance in rTMS Treatment Responders vs Non-Responders in Youth With Major Depressive Disorder. *Biological Psychiatry*, *89*(9), S379–S380. https://doi.org/10.1016/j.biopsych.2021.02.943

Conroy, K. E., Islam, M. F., & Jason, L. A. (2023). Evaluating case diagnostic criteria for

myalgic encephalomyelitis/chronic fatigue syndrome (ME/CFS): toward an empirical case definition. *Disability and Rehabilitation*, *45*(5), 840–847. https://doi.org/10.1080/09638288.2022.2043462

Council of Europe. (2023). *Liberia - Octopus Cybercrime Community*. https://www.coe.int/en/web/octopus/-/liberia

Daber, D., & Norwak, J. (2014). *Analysis : Content and Context in First* (Vol. 1, Issue 1978, pp. 83–100).

Dixon Prem Daniel, R., & Sundarraj, R. P. (2020). An e-ADR (Elaborated action design research) approach towards game-based learning in cybersecurity incident detection and handling. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 5066–5075. https://doi.org/10.24251/hicss.2020.623

Dreher, Y., Niessner, J., Fink, A., & Göpfrich, K. (2023). GeoV: An Open-Source Software Package for Quantitative Image Analysis of 3D Vesicle Morphologies. *Advanced Intelligent Systems*, *5*(9). https://doi.org/10.1002/aisy.202300170

FIRST. (2019). *Equipo de intervención en caso de incidente de seguridad informática (EIISI) Marco de servicios* (Vol. 2, pp. 1–73).

Franchina, L., Ferracci, S., & Palmaro, F. (2021). Detecting phishing e-mails using text mining and features analysis. *CEUR Workshop Proceedings*, *2940*, 106–119.

Galdi, E., Perrone, G., & Romano, S. Pietro. (2022). ThePhish: an Automated Open-Source Phishing Email Analysis Platform. *CEUR Workshop Proceedings*, *3260*, 76–101.

Graves, R. (2021). *Phishing Detecton and Remediation Phishing Defenses for Webmail Providers 2*.

Guaña, J., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P., & Pillajo, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*.

Hamill, D., Jefferies, S. A., Stillwagen, F. H., Moses, R. W., Mullins, C., & Gresham, E. (2018). Space science and technology partnership forum: Analysis for a joint demonstration of high priority, in-space assembly technology. *2018 AIAA SPACE and Astronautics Forum and Exposition*, 1–21. https://doi.org/10.2514/6.2018-5307

He, Y., Maglaras, L., Aliyu, A., & Luo, C. (2022). Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/2775249

Hu, G., & Wendel, J. F. (2019). Cis–trans controls and regulatory novelty accompanying allopolyploidization. *New Phytologist*, *221*(4), 1691–1700. https://doi.org/10.1111/nph.15515

Husák, M., & Čermák, M. (2022). SoK: Applications and Challenges of using Recommender Systems in Cybersecurity Incident Handling and Response. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3538969.3538981

ICS-CERT. (2011). *What is ICS-CERT ? CYBER EMERGENCY RESPONSE TEAM* (Issue June, pp. 1–5).

Johnson, D., Huerta, E. A., & Haas, R. (2018). Python Open source Waveform ExtractoR (POWER): An open source, Python package to monitor and post-process numerical relativity simulations. *Classical and Quantum Gravity*, *35*(2), 1–12. https://doi.org/10.1088/1361-6382/aa9cad

Joksimovic, S., Jovanovic, J., Kovanovic, V., Gasevic, D., Milikic, N., Zouaq, A., & van Staalduinen, J. P. (2020). Comprehensive Analysis of Discussion Forum Participation: From Speech Acts to Discussion Dynamics and Course Outcomes. *IEEE Transactions on Learning Technologies*, *13*(1), 38–51. https://doi.org/10.1109/TLT.2019.2916808

KASPERSKY ICS. (2020). Threat landscape for industrial automation systems. H1 2020

highlights. *Kaspersky*, 1997–2018. https://securelist.com/threat-landscape-for-industrial-automation-systems-h1-2020-highlights/98427/

Kianersi, D., Uppalapati, S., Bansal, A., & Straub, J. (2022). Evaluation of a Reputation Management Technique for Autonomous Vehicles. *Future Internet*, *14*(2). https://doi.org/10.3390/fi14020031

Koddebusch, M. (2022). Exposing the Phish: The Effect of Persuasion Techniques in Phishing E-Mails. *DG.O 2022: The 23rd Annual International Conference on Digital Government Research*, 78–87. https://doi.org/10.1145/3543434.3543476

Koltun, V., & Hafner, D. (2021). The h-index is no longer an effective correlate of scientific reputation. *PLoS ONE*, *16*(6 June), 1–26. https://doi.org/10.1371/journal.pone.0253397

Kral, P. (2011). *Incident Handler's Handbook | SANS Institute*. 3–3. https://www.sans.org/white-papers/33901/

Kurii, Y., & Opirskyy, I. (2023a). Iso 27001: Analysis of Changes and Compliance Features of the New Version of the Standard. *Cybersecurity: Education, Science, Technique*, *3*(19), 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655

Kurii, Y., & Opirskyy, I. (2023b). ISO 27001: ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD. *Cybersecurity: Education, Science, Technique*, *3*(19), 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655

Kurth, A. (2021). *Ecuador Approves Data Protection Law _ Privacy & Information Security Law Blog*.

Lanz, Z. (2022). Cybersecurity Risk in U.S. Critical Infrastructure: An Analysis of Publicly Available U.S. Government Alerts and Advisories. *CrimRxiv*. https://doi.org/10.21428/cb6ab371.48a52d7a

Lemaire, L., Lapon, J., De Decker, B., & Naessens, V. (2014, September 11). A SysML

Extension for Security Analysis of Industrial Control Systems. *2nd International Symposium for ICS & SCADA Cyber Security Research 2014*. https://doi.org/10.14236/ewic/ics-csr2014.1

Ley Orgánica de protección de Datos. (2023). Ley Orgánica de protección de Datos. *Registro Oficial de La República Del Ecuador Suplemento Quinto No. 459 de 26 de Mayo de 2023*.

Lodhi, P., Annapoorna, E., Mishra, O., & Sinha, A. (2018). *3 rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 Analysis of real life networks using centrality measure 3 rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018*. 864–869.

Luo, H., Liu, L., Zha, G., Jiang, W., Yang, B., Wang, F., & Xu, B. (2023). Phase Control of Typical Impurities in Hazardous Selenium Waste and Preparation of High-Purity Selenium During Pre-oxidation and Vacuum Distillation Process. *Metallurgical and Materials Transactions B: Process Metallurgy and Materials Processing Science*, *54*(1), 70–81. https://doi.org/10.1007/s11663-022-02658-4

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 117–122. https://doi.org/10.1109/CyMaEn57228.2023.10051114

Mantra, I., Abd. Rahman, A., & Saragih, H. (2020). Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education. *International Journal of Engineering & Technology*, *9*(2), 429. https://doi.org/10.14419/ijet.v9i2.30581

Meyer, P., & Métille, S. (2023). Computer security incident response teams: are they legally regulated? The Swiss example. *International Cybersecurity Law Review*, *4*(1), 39–60. https://doi.org/10.1365/s43439-022-00070-x

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, *25*(5), 351–370.

https://doi.org/10.1016/j.cose.2005.09.006

Mityukov, E. A., Zatonsky, A. V., Plekhov, P. V., & Bilfeld, N. V. (2019). Phishing detection model using the hybrid approach to data protection in industrial control system. *IOP Conference Series: Materials Science and Engineering*, *537*(5). https://doi.org/10.1088/1757-899X/537/5/052014

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01755

Mustafa, M., Riadi, I., & Umar, R. (2021). Header investigation for spam email forensics using framework of national institute of standards and technology. *ILKOM Jurnal Ilmiah*, *13*(2), 163–167. https://doi.org/10.33096/ilkom.v13i2.849.163-167

Naciones Unidas. (2024). *Paz, justicia e instituciones sólidas*. https://mexico.un.org/es/sdgs/16

Nikolaos, K., & Andreas, A. (2016). Charalambous Elisavet Bratskas Romaios Karkas George Email forensic tools : A roadmap to email header analysis through a cybercrime use case. *Journal of Polish Safety and Reliability Association*, *7*(1), 21–28.

Ochoa, R., & Cossio, P. (2021). Pepfun: Open source protocols for peptide-related computational analysis. *Molecules*, *26*(6), 1–12. https://doi.org/10.3390/molecules26061664

OEA. (2016). *Buenas Prácticas para establecer un CSIRT nacional*. 55.

Osliak, O., Saracino, A., & Martinelli, F. (2019). A scheme for the sticky policy representation supporting secure cyber-threat intelligence analysis and sharing. *Information & Computer Security*, *27*(5), 687–710. https://doi.org/10.1108/ICS-01-2019-0011

Prederikus, P., Bunawan, S. G., Gaol, F. L., Matsuo, T., & Nugroho, A. (2022). *Standard Analysis of Document Control as Information According to ISO 27001 2013 in PT XYZ* (pp. 721–732). https://doi.org/10.1007/978-981-16-5640-8_54

Ramanathan, K., Antognini, D., Combes, A., Paden, M., Zakhary, B., Ogino, M., Maclaren, G., & Brodie, D. (2020). *Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID- research that is available on the COVID-19 resource centre - including this for unrestricted research re-use a*. *January*, 19–21.

Ramesh, G., Lokitha, R. B., Monisha, R. R., & Neha, N. S. (2023). Phishing Detection System using Random Forest Algorithm. *International Journal for Research Trends and Innovation (Www.Ijrti.Org)*, *8*(4), 510. www.ijrti.org

Rastogi, N., Dutta, S., Gittens, A., Zaki, M. J., & Aggarwal, C. (2022). TINKER: A framework for Open source Cyberthreat Intelligence. *Proceedings - 2022 IEEE 21st International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2022*, 1569–1574. https://doi.org/10.1109/TrustCom56396.2022.00225

Rege, A., & Bleiman, R. (2021). Collegiate Social Engineering Capture the Flag Competition. *ECrime Researchers Summit, ECrime*, *2021-Decem*(Table 1). https://doi.org/10.1109/eCrime54498.2021.9738746

Rege, A., Obradovic, Z., Asadi, N., Singer, B., & Masceri, N. (2017). A temporal assessment of cyber intrusion chains using multidisciplinary frameworks and methodologies. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–7. https://doi.org/10.1109/CyberSA.2017.8073398

Riadi, I., Sunardi, & Nani, F. T. (2022). Analisis Forensik pada Email Menggunakan Metode National Institute of Standards Technology. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(2), 83–90. https://doi.org/10.14421/jiska.2022.7.2.83-90

SANS. (2016). *CIS Critical Security Controls Poster*. 2. https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Sazanova, S. L. (2021). First International Lvov Forum. *Economics of Contemporary Russia*,

1(1), 155–162. https://doi.org/10.33293/1609-1442-2021-1(92)-155-162

securityaffairs. (2023). *A third bank was a victim of cyber heist that involved the SWIFT*. https://securityaffairs.com/47532/cyber-crime/swift-thord-cyber-heist.html

Setyawan, E., & Sukmana, F. (2021). Penilaian Standar Mutu Pada Aplikasi Tiket Bioskop dengan ISO 27001 dan Fishbone Analisis. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *2*(4), 214–222. https://doi.org/10.35746/jtim.v2i4.110

Shauver, D. (2021). *Beyond Patch Management*.

Sholihah, I. M., Setiawan, H., & Nabila, O. G. (2021). Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform. *2021 Sixth International Conference on Informatics and Computing (ICIC)*, 1–6. https://doi.org/10.1109/ICIC54025.2021.9632989

Sholikhatin, S. A., & Isnaini, K. N. (2021). Analysis of Information Security Using ISO 27001 and Triangular Fuzzy Number Weighting. *Jurnal Ilmiah Informatika*, *6*(1), 43–49. https://doi.org/10.35316/jimi.v6i1.1224

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences (Switzerland)*, *12*(12). https://doi.org/10.3390/app12126042

StrangeBee. (2022). *THEHIVE PROJECT*. https://thehive-project.org/.

Sun, L., Li, Z., Xie, L., Ye, M., & Chen, B. (2022). APTKG: Constructing Threat Intelligence Knowledge Graph from Open-Source APT Reports Based on Deep Learning. *2022 5th International Conference on Data Science and Information Technology (DSIT)*, 01–06. https://doi.org/10.1109/DSIT55514.2022.9943933

Suryotrisongko, H., Ginardi, H., Ciptaningtyas, H. T., Dehqan, S., & Musashi, Y. (2022). Topic Modeling for Cyber Threat Intelligence (CTI). *2022 Seventh International Conference on Informatics and Computing (ICIC)*, 1–7.

https://doi.org/10.1109/ICIC56845.2022.10006988

Theunissen, D., & Theunissen, D. (2021). *Corporate Incident Handling Guidelines*.

Trend Micro Incorporated. (2023). *Ecuadorean Bank Loses $12 million via SWIFT - Security News*. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ecuadorean-bank-loses-12m-via-swift

Varona, A. E., Carle, S. D., Davis, A. J., Dodd, L., Frost, A., Gill, J. R., Gold-, S. H., Jaszi, P. A., Marcus, D., Niles, M. C., Phillips, V. F., & Popper, A. F. (2006). *Out of thin air: using first amendment public forum analysis to redeem American broadcasting regulation* (pp. 149–198).

Vázquez, M. E., Ortega, W., Sajhid, O. J., & Peraza, B. (2023). Análisis Del Crecimiento De Phishing En Los Últimos Años. *Revista Digital de Tecnologías Informáticas y Sistemas*, *6*(6), 7. https://doi.org/10.61530/redtis.2022.6.6.132.7

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP - The design and implementation of a collaborative threat intelligence sharing platform. *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, Co-Located with CCS 2016*, 49–56. https://doi.org/10.1145/2994539.2994542

Walensky, R. P., Bunnell, R., Layden, J., Kent, C. K., Gottardy, A. J., Leahy, M. A., Martinroe, J. C., Spriggs, S. R., Yang, T., Doan, Q. M., King, P. H., Starr, T. M., Yang, M., Jones, T. F., Boulton, M. L., Carolyn Brooks, M., Jay Butler, M. C., Caine, V. A., Fielding, J. E., … Johnson, L. (2022). Morbidity and Mortality Weekly Report Council of State and Territorial Epidemiologists/CDC Surveillance Case Definition for Multisystem Inflammatory Syndrome in Children Associated with SARS-CoV-2 Infection-United States Centers for Disease Control and Pr. *Recommendations and Reports*, *71*(4).

Wardak, H., Zhioua, S., & Almulhem, A. (2016). PLC access control: a security analysis. *2016 World Congress on Industrial Control Systems Security (WCICSS)*, 1–6.

https://doi.org/10.1109/WCICSS.2016.7882935

Williams, K., Bleiman, R., & Rege, A. (2022). Educating educators on social engineering Experiences developing and implementing a social engineering workshop for all education levels. *2022 IEEE Integrated STEM Education Conference (ISEC)*, 188–194. https://doi.org/10.1109/ISEC54952.2022.10025154

Young, L. R. (2013). CERT ® Resilience Management Model Publication 800-66 Crosswalk. *Carnegie Mellon University*, *1.1*(October), 1–43.

Zhang, R., Wang, S., Burton, R., Hoang, M., Hu, J., & Nascimento, A. C. A. (2021). Clustering analysis of email malware campaigns. *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, 95–102. https://doi.org/10.1109/CSR51186.2021.9527902

Zhang, X., & Chow, K. (2018). A Framework for Dark Web Threat Intelligence Analysis. *International Journal of Digital Crime and Forensics*, *10*(4), 108–117. https://doi.org/10.4018/IJDCF.2018100108

Zimba, A., Mukupa, G., & Chama, V. (2022). *Emerging Mobile Phone-based Social Engineering Cyberattacks in the Zambian ICT Sector*. *Zicta 2021*. https://doi.org/https://doi.org/10.48550/arXiv.2212.13721

Zimon, G., Arianpoor, A., & Salehi, M. (2022). Sustainability Reporting and Corporate Reputation: The Moderating Effect of CEO Opportunistic Behavior. *Sustainability (Switzerland)*, *14*(3), 1–28. https://doi.org/10.3390/su14031257