ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TRABAJO DE TITULACIÓN

"IMPLEMENTACIÓN DE UNA HERRAMIENTA DE SEGURIDAD QUE PERMITA EVALUAR LA POSTURA DE SEGURIDAD DE LOS CLIENTES DE UN ISP BASADO EN INDICADORES DE COMPROMISO"

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. VALLE RODRIGUEZ CARLOS EDUARDO

ING. ADACHI CORDERO ANTHONY YOSHIHITO

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Quiero agradecer especialmente a mis padres, a mi esposa y a mis hijos. Su constante apoyo me dio ánimos y fuerzas para continuar en mi formación profesional. Sin su entusiasmo y apoyo este proyecto no habría sido posible

Ing. Carlos Eduardo Valle Rodriguez

Quisiera expresar mi más sincero agradecimiento a todas las personas que han sido fundamentales en la culminación de este proyecto académico.

En primer lugar, mi gratitud más profunda a mi familia, cuyo apoyo incondicional y comprensión han sido el pilar sobre el que se ha sostenido este esfuerzo. Su aliento constante, paciencia y amor inquebrantable han sido una fuente inestimable de fortaleza y motivación durante todo este proceso.

Asimismo, deseo reconocer a mis compañeros de trabajo y colegas, quienes han desempeñado un papel crucial en mi formación académica y profesional. Su guía experta, colaboración y consejos han enriquecido mi experiencia de aprendizaje y han contribuido de manera significativa a la calidad de este trabajo. Agradezco profundamente sus aportaciones y el ambiente de camaradería y apoyo mutuo que hemos compartido.

A todos ellos, mi más sincero agradecimiento.

Ing. Yoshihito Adachi

DEDICATORIA

Dedico este trabajo a mi familia en señal de agradecimiento por su constante amor y apoyo al momento de realizar esta tesis.

Ing. Carlos Eduardo Valle Rodriguez.

Dedico esta tesis a mi querida familia, cuyo amor y apoyo incondicional han sido el fundamento de cada logro alcanzado. Sin su comprensión y aliento constante, este proyecto no hubiera sido posible. Su presencia en cada etapa de mi vida ha sido una fuente de fortaleza y motivación, y por ello, estoy profundamente agradecido.

También dedico esta obra a mis compañeros de trabajo y colegas, quienes, con su sabiduría y colaboración, han enriquecido mi formación y contribuido significativamente al desarrollo de este proyecto. Su orientación y compañerismo han sido esenciales para mi crecimiento académico y profesional.

A todos ellos, mi más sincero agradecimiento y dedicación.

Ing. Yoshihito Adachi

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO
FREIRE COBO

M.SC. LENIN EDUARDO FREIRE COBO

TUTOR

Firmado electrónicamente por:
OMAR RODOLFO
MALDONADO DANIN

M.SC. OMAR RODOLFO MALDONADO DAÑIN

REVISOR

DECLARACIÓN EXPRESA

Nosotros VALLE RODIGUEZ CARLOS EDUARDO y ADACHI CORDERO ANTHONY YOSHIHITO acuerdo/acordamos y reconozco/reconocemos que: La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores. El o los estudiantes deberán procurar en cualquier caso de cesión de sus derechos patrimoniales incluir una cláusula en la cesión que proteja la vigencia de la licencia aquí concedida a la ESPOL.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, secreto empresarial, derechos patrimoniales de autor sobre software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al/los autor/es que existe una innovación potencialmente patentable sobre

los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 12 de noviembre del 2024

Firmado electrónicamente por:
CARLOS EDUARDO VALLE RODRIGUEZ

Ing. Carlos Valle

Firmado electrónicamente por:
ANTHONY YOSHIHITO ADACHI CORDERO

Ing. Anthony Adachi

Evaluadores

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Freire Cobo
PROFESOR TUTOR

Firmado electrónicamente por:
OMAR RODOLFO MALDONADO DANIN

Mgs. Omar Maldonado Dañin
PROFESOR EVALUADOR

RESUMEN

El presente trabajo de titulación se enfoca en la implementación de un sistema de monitoreo avanzado para el análisis del tráfico de red en un Proveedor de Servicios de Internet (ISP), con el propósito de identificar y mitigar amenazas informáticas. A diferencia de enfoques tradicionales dirigidos al sector empresarial, este estudio está orientado hacia el público general, buscando ofrecer soluciones accesibles y efectivas para usuarios no especializados en el ámbito de la ciberseguridad.

La investigación propone la creación de un sistema integral que contempla la instalación de zonas de limpieza en puntos estratégicos dentro de la red del ISP. Estas zonas de limpieza actúan como filtros y puntos de análisis que permiten una vigilancia continua y detallada del tráfico de datos. La ubicación estratégica de estas zonas está diseñada para maximizar la captura de información relevante y minimizar el impacto en el rendimiento general de la red.

Una parte crucial del sistema es el enriquecimiento de los datos recolectados a través de estas zonas de limpieza. La información obtenida se somete a un procesamiento exhaustivo, con el objetivo de extraer patrones y comportamientos que puedan indicar la presencia de amenazas potenciales. Este análisis detallado facilita la identificación de usuarios infectados y la detección temprana de actividades sospechosas.

El resultado de este proceso de enriquecimiento y análisis es la generación de un panel estratégico, una herramienta visual y funcional que permite a los operadores del sistema monitorizar el estado de la red de manera rápida y eficiente. El panel estratégico proporciona una vista integral del tráfico de red y resalta de forma destacada los incidentes de seguridad, facilitando la toma de decisiones y la implementación de medidas correctivas de manera oportuna.

ÍNDICE GENERAL

AGRADECIMIENTO II
DEDICATORIA IV
TRIBUNAL DE GRADUACIÓN VI
DECLARACIÓN EXPRESA VII
RESUMEN IX
ABREVIATURAS Y SÍMBOLOS XII
ÍNDICE DE FIGURAS XIV
ÍNDICE DE TABLAS XV
INTRODUCCION XVI
CAPÍTULO I: GENERALIDADES 1
1.1. ANTECEDENTES 1
1.2. DESCRIPCIÓN DEL PROBLEMA: 2
1.3. SOLUCIÓN PROPUESTA 5
1.4. OBJETIVO GENERAL 6
1.5. OBJETIVO ESPECÍFICOS: 6
1.6. METODOLOGÍA 6
CAPITULO II: MARCO TEORICO 9
2.1. HERRAMIENTAS DE SEGURIDAD 9
2.2. POSTURA DE SEGURIDAD 10
2.3. ISP 11
2.4. INDICADORES DE COMPROMISO 13
CAPÍTULO III: DISEÑO ZONAS DE LIMPIEZA DE TRÁFICO 16
3.1. ARQUITECTURA DEL SCRUBBING CENTER 16
3.2. PROCESO DE FILTRADO Y DEPURACIÓN 18
3.3. INTEGRACIÓN CON LA INFRAESTRUCTURA DE RED 20
3.4. CAPACIDADES DE ESCABILIDAD 21
CAPÍTULO IV: IMPLEMENTAR PANEL DE VISUALIZACIÓN DE AMENAZAS 22
4.1. SELECCIÓN DE LA PLATAFORMA DEL PANEL DE VISUALIZACIÓN 22
4.2. INTEGRACIÓN DE FUENTE DE DATOS 24
4.3. PROCESAMIENTO Y ANÁLISIS DE DATOS 26
4.4. VISUALIZACIÓN DE DATOS 29

4.5. CAPACIDAD DE REPORTES Y AUDITORIA PARA LA ALTA GERENCIA.....30
CAPÍTULO V: EVALUACIÓN DE LAS AMENAZAS.....32
5.1. TIPO DE AMENAZAS OBSERVADAS 32
5.2. ANÁLISIS DE TRAFICO DE RED.....34
5.3. TASA DE INCIDENTES.....38
5.4. FUENTE DE AMENAZAS.....45
5.5. ANÁLISIS DE VULNERABILIDADES EXPLOTADAS.....47
CONCLUSIONES 51
BIBLIOGRAFÍA.....56
ANEXO 58
A. Archivo de configuración para el filtrado y parsing de logstatsh con los eventos del scrubbing center. 58

ABREVIATURAS Y SÍMBOLOS

ACL Access Control List (Lista de Control de Acceso)

APT Advanced Persistent Threat (Amenaza Persistente Avanzada)

BAS Breach and Attack Simulation (Simulación de Brechas y Ataques)

BYOD Bring Your Own Device (Trae tu Propio Dispositivo)

CISO Chief Information Security Officer (Director de Seguridad de la Información)

CVE Common Vulnerabilities and Exposures (Vulnerabilidades y Exposiciones Comunes)

DDoS Distributed Denial of Service (Denegación de Servicio Distribuida)

DLP Data Loss Prevention (Prevención de Pérdida de Datos)

GRC Governance, Risk, and Compliance (Gobernanza, Riesgo y Cumplimiento)

HIDS Host-based Intrusion Detection System (Sistema de Detección de Intrusiones Basado en Host)

IaaS Infrastructure as a Service (Infraestructura como Servicio)

IDS Intrusion Detection System (Sistema de Detección de Intrusiones)

IoC Indicadores de Compromiso

IPS Intrusion Prevention System (Sistema de Prevención de Intrusiones)

ISO International Organization for Standardization (Organización Internacional de Normalización)

MFA Multi-Factor Authentication (Autenticación Multifactor)

NAC Network Access Control (Control de Acceso a la Red)

NIDS Network-based Intrusion Detection System (Sistema de Detección de Intrusiones Basado en Red)

OSINT Open Source Intelligence (Inteligencia de Código Abierto)

PaaS Platform as a Service (Plataforma como Servicio)

PKI Public Key Infrastructure (Infraestructura de Clave Pública)

RAT Remote Access Trojan (Troyano de Acceso Remoto)

RDP Remote Desktop Protocol (Protocolo de Escritorio Remoto)

SaaS Software as a Service (Software como Servicio)

SIEM Security Information and Event Management (Gestión de Información y Eventos de Seguridad)

SOC Security Operations Center (Centro de Operaciones de Seguridad)

TLS Transport Layer Security (Seguridad de Capa de Transporte)

VAPT Vulnerability Assessment and Penetration Testing (Evaluación de Vulnerabilidades y Pruebas de Penetración)

VPN Virtual Private Network (Red Privada Virtual)

WAF Web Application Firewall (Cortafuegos de Aplicaciones Web)

XSS Cross-Site Scripting (Scripting en Sitios Cruzados)

ÍNDICE DE FIGURAS

Ilustración 1 Diagrama de red para zona de limpieza de tráfico. (Autoría Propia)5Ilustración 2. Diagrama de alto nivel de la integración de los datos a un SIEM25Ilustración 3. Cantidad de eventos recolectados desde el scrubbing center al SIEM27Ilustración 4. Módulo de exploración de eventos del SIEM con la información del Scrubbing Center28Ilustración 5 Paneles de visualización del estado de tráfico analizado por el Scrubbing Center a nivel gerencial 30Ilustración 6. Reporte diseñado para la alta gerencia del estado actual de tráfico detectado como malicioso31Ilustración 7 Tráfico total y malicioso detectado por la herramienta de filtrado de paquetes en un periodo de 1 semana.34Ilustración 8 Porcentaje de tipo de ataques detectados en la red en el periodo de analisis.38Ilustración 9 Porcentaje de las severidades de alertas detectadas por la herramienta en el periodo de análisis41Ilustración 10 Porcentaje por categoría de tipo de ataque detectado por la herramienta en el periodo de análisis. 43Ilustración 11 Tabla de cantidad de usuarios, sesiones y tamaño de tráfico consumido por aplicación 48

ÍNDICE DE TABLAS

Tabla 1 Tipos de ataques por DDoS y sus metodos de mitigación 25

Tabla 2 Tipos de puertos asociados por su servicio estándar y las vulnerabilidades que frecuentemente son vigentes 38

INTRODUCCION

La seguridad informática se ha convertido en una prioridad para las empresas de todos los sectores, especialmente para los proveedores de servicios de Internet (ISP). A medida que la dependencia de la conectividad y los servicios digitales aumenta, también lo hacen las amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos. En este contexto, es esencial que los ISP no solo protejan sus propias infraestructuras, sino que también garanticen la seguridad de los datos de sus clientes. La evaluación continua de la postura de seguridad se presenta como un elemento crucial para identificar vulnerabilidades y mitigar riesgos.

El desarrollo e implementación de una herramienta de seguridad que permita evaluar la postura de seguridad de un ISP se fundamenta en la necesidad de establecer un marco robusto para la gestión de riesgos. Esta herramienta tiene como objetivo proporcionar a los ISP una evaluación integral de sus sistemas y procesos de seguridad, facilitando la identificación de debilidades y áreas de mejora. A través de análisis detallados y métricas específicas, los ISP podrán adoptar un enfoque proactivo hacia la seguridad, alineándose con las mejores prácticas y normativas del sector.

En un entorno donde las ciberamenazas son cada vez más sofisticadas y variadas, los ISP enfrentan desafíos únicos. Desde ataques DDoS hasta filtraciones de datos, la exposición a riesgos es constante y multifacética. Además, la creciente preocupación por la privacidad de los datos y el cumplimiento normativo, como el Reglamento General de Protección de Datos (GDPR) en Europa, exige que los ISP adopten prácticas de seguridad más estrictas. Por lo tanto, evaluar y mejorar continuamente la postura de seguridad se convierte en un imperativo estratégico.

La herramienta que se propone solo se centrará en la detección de vulnerabilidades, y amenazas de los clientes. Esto permitirá a los ISP tener una visión holística de su situación de seguridad y fomentar una cultura organizacional centrada en la seguridad. El desarrollo de esta herramienta se sustentará en metodologías reconocidas.

A medida que la tecnología avanza y las amenazas evolucionan, es crucial que los ISP estén preparados para adaptarse a estos cambios. La herramienta que se desarrollará no solo proporcionará una evaluación puntual, sino que también se convertirá en una parte integral del proceso de gestión de riesgos del ISP, permitiendo un enfoque más dinámico y adaptativo hacia la seguridad.

En conclusión, la implementación de una herramienta de evaluación de la postura de seguridad es un paso fundamental para que los ISP fortalezcan su defensa contra ciberamenazas, mejoren la confianza de sus clientes y cumplan con las expectativas normativas del sector. En las siguientes secciones se presentarán los detalles técnicos, metodológicos y operativos del desarrollo de esta herramienta, así como los beneficios esperados de su implementación.

CAPÍTULO I: GENERALIDADES

1.1. ANTECEDENTES

La creciente dependencia de la tecnología y la digitalización de servicios han transformado el paisaje de la seguridad cibernética. Los proveedores de servicios de Internet (ISP) se encuentran en una posición crítica, ya que son el punto de entrada y salida de datos para millones de usuarios. Esto los convierte en un objetivo atractivo para atacantes cibernéticos, quienes buscan explotar vulnerabilidades en sus infraestructuras.

En la última década, los ataques cibernéticos han aumentado de manera alarmante. Según informes de seguridad, las violaciones de datos y los ataques de ransomware se han convertido en eventos comunes, afectando tanto a empresas grandes como pequeñas. Los ISP, al gestionar grandes volúmenes de datos y mantener la conectividad de múltiples clientes, se ven especialmente amenazados.

En varios casos ISP que han sufrido brechas de seguridad significativas, lo que ha llevado a la pérdida de datos sensibles y a la desconfianza del cliente. Un caso notable fue el ataque a un importante ISP en 2020, donde se comprometieron millones de cuentas de usuarios. Este incidente no solo resultó en pérdidas financieras sustanciales, sino que también dañó la reputación de la empresa y provocó una disminución en la base de clientes. La falta de una evaluación adecuada de la postura de seguridad fue un factor determinante en la vulnerabilidad del ISP a este tipo de ataques.

La evidencia sugiere que muchos ISP carecen de las herramientas necesarias para llevar a cabo una evaluación integral y continua de su postura de seguridad. Aunque algunos han

implementado medidas básicas, la falta de un enfoque sistemático y proactivo ha dejado a muchos expuestos a riesgos significativos. Herramientas de evaluación automatizadas y enfoques integrales se han vuelto esenciales para que los ISP no solo identifiquen vulnerabilidades, sino que también implementen medidas correctivas de manera eficiente.

En resumen, los antecedentes revelan una necesidad crítica de desarrollar herramientas efectivas que permitan a los ISP evaluar y mejorar su postura de seguridad. La creciente amenaza de ciberataques, la presión regulatoria y los casos de brechas de seguridad han destacado la urgencia de establecer un marco robusto para la gestión de la seguridad. La herramienta que se propone busca llenar este vacío, proporcionando a los ISP los recursos necesarios para protegerse eficazmente en un entorno cibernético en constante evolución.

1.2. DESCRIPCIÓN DEL PROBLEMA:

Dada la complejidad y extensión de su infraestructura, los ISP se enfrentan a la carencia de un sistema de postura de seguridad sólido, lo que se traduce en la incapacidad para detectar y mitigar eficazmente las amenazas. Este problema es atribuible a una serie de factores, entre los que destacan: La falta de una infraestructura de seguridad robusta y actualizada, la insuficiente inversión en tecnologías de detección y mitigación de amenazas cibernéticas, la ausencia de un sistema eficiente para reportar y analizar incidentes de seguridad, la creciente complejidad en la gestión de la red, la cual se ve exacerbada por su constante expansión.

En consecuencia, se derivan las siguientes repercusiones: Existe un alto riesgo de brechas de seguridad y violaciones de datos, que a su vez pueden conllevar sanciones legales y erosionar la confianza de los clientes, la incapacidad para tomar decisiones fundamentadas por parte de la alta dirección, un impacto adverso en la reputación del ISP y su competitividad en el mercado,

un riesgo financiero derivado de posibles multas y costos asociados a la recuperación tras incidentes de seguridad, la pérdida de clientes y oportunidades de negocio debido a la percepción generalizada de inseguridad en la red.

El panorama presentado por las amenazas y el aumento de superficies de ataque que tienen las empresas/organizaciones han ido transformándose continuamente. La capacidad de los ciberdelincuentes en diseñar y adaptar nuevas técnicas para la explotación de entornos corporativos se mantiene en una evolución continua que conlleva al aumento de los riesgos para las empresas de todos los sectores independientemente de la industria o geografía.

Durante la primera mitad del 2023, varias organizaciones de delitos cibernéticos han adoptado nuevas tecnologías y con unas organizaciones similares a las empresas tradicionales con políticas definidas correctamente, responsabilidades, proyectos y objetivos. Estas estructuras operativas, combinadas con un fuerte apoyo económico resultante de exploits o naciones enteras, facilitan sus objetivos, permitiéndoles desarrollar y experimentar tecnologías que van cambiando radicalmente las técnicas y tácticas, como la nueva Inteligencia Artificial Generativa, que realizan ataques más complejos y difíciles de detectar.

La sofisticación de los actores malicioso ha ido aumentando las amenazas en frecuencias y complejidad, lo que ha conllevado en complejas campanas de ransomware que finaliza con violaciones de datos y cambios en la cadena de Kill Chain dentro de las tácticas de MITRE ATT&CK. [1]

Inicialmente, es esencial tener en cuenta que el núcleo del negocio de un ISP radica en la provisión de servicios de Internet a sus clientes. Los servicios de seguridad, por ende, no

constituyen un producto directamente dirigido al cliente, sino están centrados en la mejora de la calidad del servicio. En este contexto, es fundamental comprender que el financiamiento para iniciativas de seguridad proviene directamente del propio ISP. Desde la perspectiva de viabilidad técnica, es relevante destacar que el ISP ya dispone de la infraestructura técnica necesaria para la implementación del sistema. Esto incluye componentes esenciales como firewalls, sistemas de prevención de intrusiones (IPS), centros de limpieza de tráfico (scrubbing centers) y servidores donde se alojará la herramienta de correlación de eventos. Además, el sistema es altamente escalable y está diseñado para adaptarse al crecimiento continuo de la red, garantizando así su pertinencia para futuras necesidades.

En términos de competitividad, es imperativo comprender que la reputación de un ISP con relación a las amenazas tiene un impacto significativo en las comunicaciones con el exterior. Cuando una red figura en una lista de bloqueo de reputación, puede generar obstáculos en el acceso a sitios web o en el intercambio de correos electrónicos. Esto se debe a que numerosas herramientas de seguridad se basan en la reputación de una dirección IP para permitir o denegar el flujo de tráfico. La repercusión de esta situación se refleja en la experiencia del usuario final. Es decir, cuanto mayor sea la protección contra amenazas que se ofrece a los clientes, menor será la probabilidad de que una IP se incluya en una lista negra, lo que a largo plazo mejora la calidad del servicio en comparación con la competencia que no presta atención a su reputación en la red. [2]

1.3. SOLUCIÓN PROPUESTA

Se llevará a cabo un proceso de validación, recopilación y transformación de la información proveniente de diversas áreas de limpieza mediante el envío de eventos al Sistema de Gestión de Eventos e Información de Seguridad (SIEM). El objetivo del proceso es crear paneles de control que permitan visualizar de manera ágil y eficaz las amenazas y las vulnerabilidades de nuestros clientes, basándose en una puntuación que considera factores como la cantidad de direcciones IP, infecciones, medidas de mitigación y tráfico permitido.

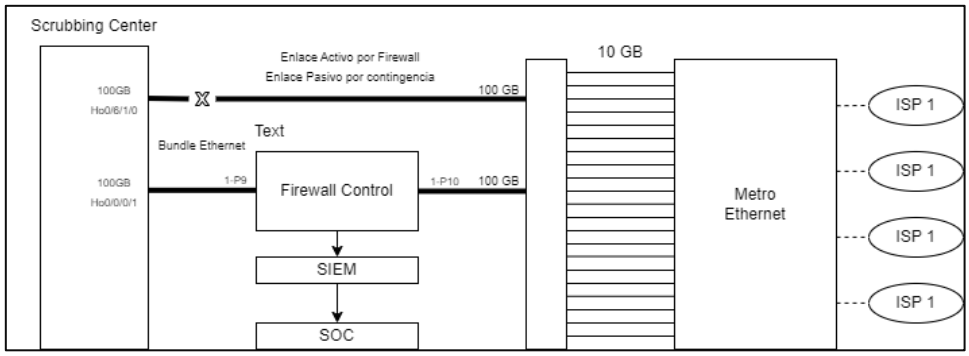

Ilustración 1 Diagrama de red para zona de limpieza de tráfico. (Autoría Propia)

El diagrama de red presentado en la figura 1 es óptimo para la infraestructura de la empresa de telecomunicaciones en la que se planea desplegar la solución, dada la gran cantidad de tráfico que gestiona de los clientes. Además, se han previsto contingencias adecuadas en caso de fallos en la herramienta de clasificación del tráfico, ya sea para determinar si es malicioso o no. Además, es importante destacar que la empresa ya dispone de los dispositivos necesarios para llevar a cabo la implementación. [3]

1.4. OBJETIVO GENERAL

Implementar un sistema que permita mostrar la postura de Seguridad de un ISP, utilizando tecnologías de Código abierto con la finalidad de reportar a la alta gerencia las amenazas relacionas al ecosistema.

1.5. OBJETIVO ESPECÍFICOS:

- Evaluar las amenazas que impactan a los usuarios finales de la red, utilizando fuentes de lista de reputación externas.
- Diseñar zonas de limpieza de tráfico para segmentar y controlar el flujo de datos en la red.
- Desarrollar un panel de control destinado a ser empleado por la alta dirección con el propósito de facilitar la toma de decisiones.

1.6. METODOLOGÍA

Este proyecto se enfoca en un alcance de tipo descriptivo que implica levantar y examinar el tráfico generado por los diversos clientes de las empresas telecomunicaciones lo que permitirá identificar las tácticas y técnicas de MITRE utilizadas por los ciberdelincuentes presentes en los flujos de comunicaciones, con el propósito de implementar medidas de filtrado de las conexiones optimas a través de centros de limpieza de tráfico (scrubbing centers). [4]

Además, se busca obtener perfiles del comportamiento de las organizaciones de alto nivel criminal (FIN o APT) que dirigen ataques hacia grandes proveedores de servicios de Internet (ISP). Esto se logrará mediante la identificación de Indicadores de Compromiso (IoC) e Indicadores de Ataque (IoA) que han sido reportados por destacadas empresas especializadas en ciber inteligencia en el tráfico de conexiones recolectada de los clientes. Para llevar a cabo este análisis, planeamos utilizar los datos clasificados por cuatro scrubbing centers, que generan un promedio aproximado de 100,000 eventos por segundo (EPS).

Un componente fundamental de este proyecto es la implementación de un panel de control que simplificará la evaluación del nivel de seguridad global del ISP con la ayuda de un Sistema de Información y Eventos de Seguridad (SIEM) de código abierto. Este panel permitirá identificar medidas de mitigación, tipos de ataques, sus fuentes y las áreas afectadas, todo ello en intervalos de tiempo específicos. El sistema mantendrá un registro de los datos durante 5 días en almacenamiento de acceso rápido y 10 días en almacenamiento de acceso lento.[5]

Las herramientas de seguridad perimetral son las encargadas de determinar si un flujo de datos contiene parámetros sospechosos o no, basándose en reglas de correlación previamente establecidas mediante análisis de firmas o comportamiento, dependiendo del escenario. Las herramientas que utilizaremos incluyen:

- Firewall Next Generation: Esta herramienta realiza la correlación a nivel de conexiones de sockets, lo que significa que analiza la dirección IP de origen, el puerto de origen, la dirección IP de destino y el puerto de destino. Además, ofrece funcionalidades adicionales como Web Protection o IPS.

- IPS/IDS: Estas herramientas analizan el tráfico a un nivel más profundo, examinando el contenido de los paquetes en busca de patrones previamente configurados mediante reglas de SNORT.
- Scrubbing Center: Similar al IPS/IDS, esta herramienta también analiza el tráfico a un nivel profundo. En vez de eliminar el paquete si encuentra un patrón malicioso, filtra el contenido y permite que la conexión continúe.

Adicionalmente, este proyecto mantiene un diseño no experimental de tipo transversal considerando que son necesarios varios parámetros esenciales en un tiempo específico con el propósito de recopilar de obtener una evaluación precisa de la postura de seguridad. [6]

Algunos de estos parámetros incluyen:

- ¿Cuántas direcciones IP han sido filtradas?
- ¿Se han registrado las cinco direcciones IP maliciosas principales por ataques en las últimas 24 horas?
- ¿Qué tipos de técnicas y tácticas de Mitre han sido identificadas?
- ¿Cuántas firmas de ataque han sido reportadas por el sistema de detección y prevención de intrusiones (IDS/IPS)?

Se empleará un enfoque de análisis prescriptivo. Esto implica que se utilizarán los datos existentes como base para orientar la toma de decisiones con el objetivo de fortalecer la postura de seguridad de una empresa de telecomunicaciones. En otras palabras, este enfoque proporcionará recomendaciones para guiar los próximos pasos a seguir.

Antes de conocer los resultados de la investigación, teniendo en cuenta el conocimiento de campo adquirido en los últimos años, se suele observar ataques de reconocimiento de diversas

direcciones IP en todo el mundo, dirigidos especialmente a empresas de renombre, en particular a grandes proveedores de servicios de Internet (ISP). Por lo tanto, es crucial mantener buenas prácticas de configuración en los dispositivos de protección perimetral. No obstante, en el área de los clientes, es más delicado aplicar restricciones, ya que muchos de ellos carecen de conocimientos básicos sobre las amenazas de los ciberdelincuentes. Como resultado, es probable que se filtre una gran cantidad de tráfico. [7]

CAPITULO II: MARCO TEORICO

2.1. HERRAMIENTAS DE SEGURIDAD

En el ámbito de la ciberseguridad defensiva, resulta imperativo implementar diversas herramientas especializadas en distintas capas de seguridad para proteger eficazmente los sistemas y datos sensibles frente a diversas amenazas. Entre estas herramientas destacan los sistemas de detección y prevención de intrusiones, conocidos como IDS e IPS, que desempeñan un papel fundamental al analizar patrones de tráfico, identificar comportamientos maliciosos y abordarlos de manera proactiva.

Asimismo, los firewalls, o cortafuegos, constituyen elementos esenciales en cualquier entorno, al permitir el control del tráfico interno mediante reglas asociadas a direcciones IP y puertos. En los últimos años, ha ganado popularidad el empleo de firewalls de próxima generación que incorporan funcionalidades adicionales, aunque estas características pueden variar según el proveedor del servicio. [8]

Otra herramienta que destaca en los proveedores de internet (ISP) ha sido los "scrubbing centers" o centros de filtrado. Estos centros desempeñan un papel crucial en la mitigación de ataques distribuidos de denegación de servicio (DDoS), filtrando y limpiando el tráfico malicioso antes de que alcance los servidores de destino. Al implementar tecnologías avanzadas de filtrado, los "scrubbing centers" contribuyen significativamente a mantener la disponibilidad de los servicios en línea incluso en medio de ataques volumétricos masivos.

Adicionalmente, existen numerosas herramientas especializadas que ofrecen seguridad adaptada a las necesidades específicas de las empresas, como DLP, Proxy, Email Security Gateway, entre otras.

En última instancia, todas estas herramientas convergen en un enfoque integral destinado a preservar la integridad, confidencialidad y disponibilidad de los activos de información, proporcionando así una sólida defensa en el complejo panorama de la ciberseguridad. [9]

2.2. POSTURA DE SEGURIDAD

La postura de seguridad describe el estado actual de una empresa en relación con las diversas alertas de seguridad asociadas a las tácticas y técnicas de MITRE, con el objetivo de detectar de manera ágil cualquier actividad maliciosa. Este concepto se evidencia concretamente en la administración y respuesta del Centro de Operaciones de Seguridad (SOC).

La efectividad de un SOC para identificar y mitigar posibles riesgos constituye un indicador clave de la postura de seguridad de una organización. Esta no solo se enfoca en la cantidad de alertas,

sino también en la calidad de la detección y la capacidad de respuesta ante incidentes. Un SOC eficiente no solo cuantifica las amenazas, sino que las clasifica según su gravedad, las detecta, contiene, investiga, documenta, mitiga y restaura de manera rápida y precisa, con el objetivo de minimizar el tiempo de exposición a posibles vulnerabilidades.

La postura de seguridad del SOC se fortalece mediante la implementación de tecnologías avanzadas de detección, análisis de comportamiento y correlación de eventos. Además, la formación continua del personal del SOC, la optimización de los procesos de respuesta a incidentes y la integración de inteligencia de amenazas son elementos esenciales para mantener una postura de seguridad sólida y adaptable. [10]

En última instancia, la capacidad del SOC para gestionar de manera eficiente la cantidad y complejidad de alertas no solo refleja la madurez de la postura de seguridad de una organización, sino que también contribuye de manera significativa a la resiliencia cibernética y a la protección de activos digitales críticos.

2.3. ISP

El Proveedor de Servicios de Internet (ISP) desempeña un papel crucial en la infraestructura digital al ofrecer conectividad a Internet y garantizar la disponibilidad y estabilidad de la red. Sin embargo, las responsabilidades de un ISP van más allá de la mera provisión de acceso a la red; incluyen la implementación de una serie de medidas proactivas para proteger tanto a los usuarios individuales como a la red en su conjunto de amenazas cibernéticas. [11]

En el ámbito de la ciberseguridad, los ISP deben adoptar medidas proactivas para mitigar una variedad de riesgos y amenazas. Esto incluye la implementación de sistemas de filtrado para

bloquear contenido malicioso, como malware y phishing, antes de que llegue a los clientes. Los mecanismos de filtrado pueden basarse en listas negras de URLs maliciosas, análisis heurístico de tráfico y la identificación de patrones sospechosos en el tráfico de datos. Además, los ISP deben implementar protecciones contra ataques distribuidos de denegación de servicio (DDoS), que pueden inundar sus redes con tráfico no deseado, afectando la disponibilidad del servicio para todos los usuarios.

La capacidad para detectar y responder rápidamente a incidentes de seguridad es una función esencial para los ISP. Los sistemas de detección de intrusiones (IDS) y de prevención de intrusiones (IPS) desempeñan un papel crucial en la identificación de actividades anómalas y potencialmente maliciosas dentro de la red del ISP. Estos sistemas deben ser capaces de analizar grandes volúmenes de tráfico en tiempo real para identificar patrones que puedan indicar una brecha de seguridad. La respuesta efectiva a incidentes incluye la coordinación con equipos de respuesta a incidentes y la implementación de medidas correctivas para minimizar el impacto en los usuarios y en la integridad de la red.

La colaboración entre los ISP y las autoridades de ciberseguridad es fundamental para enfrentar amenazas que pueden afectar a múltiples redes y organizaciones. Los ISP deben participar en iniciativas de intercambio de información sobre amenazas, colaborando con organismos como CERT (Computer Emergency Response Teams) y otros grupos de respuesta a incidentes para compartir datos relevantes sobre ataques emergentes y vulnerabilidades. Este intercambio de información permite una respuesta más coordinada y eficaz a amenazas que trascienden las fronteras de una sola red. [12]

El compromiso de los ISP con la seguridad contribuye significativamente a la resiliencia y estabilidad de la infraestructura de Internet. La implementación de medidas preventivas y

reactivas ayuda a proteger no solo a los usuarios individuales, sino también a la integridad global de la red. Además, los ISP deben participar en la educación de los usuarios sobre buenas prácticas de seguridad, como la protección contra phishing y el uso de contraseñas seguras, para reforzar la defensa perimetral contra amenazas cibernéticas.

A pesar de los esfuerzos proactivos, los ISP enfrentan desafíos significativos en la protección de sus redes y clientes. La evolución continua de las amenazas cibernéticas y la sofisticación de los ataques requieren que los ISP mantengan sistemas de seguridad actualizados y que realicen inversiones continuas en tecnología y formación. Además, la gestión de la privacidad y el cumplimiento de las normativas de protección de datos son factores críticos que los ISP deben equilibrar con sus responsabilidades de seguridad. [13]

Los ISP tienen un papel esencial en la protección de la infraestructura digital y en la seguridad de sus clientes. La implementación de medidas de seguridad proactivas, la detección y respuesta a incidentes, la colaboración con autoridades de ciberseguridad y el fortalecimiento de la resiliencia de la red son componentes clave de sus responsabilidades. Al cumplir con estas obligaciones, los ISP contribuyen significativamente a un entorno digital más seguro y confiable.

2.4. INDICADORES DE COMPROMISO

Los Indicadores de Compromiso (IoCs) son esenciales para la detección y respuesta a amenazas cibernéticas, ya que permiten a los analistas identificar y mitigar actividades maliciosas basadas en patrones observables. Sin embargo, la efectividad de un IoC puede variar significativamente, y esta variabilidad se refleja en el concepto de la Pirámide de Dolor. Este modelo, desarrollado por el analista de seguridad David Bianco, clasifica los indicadores según el nivel de dificultad que representan para los atacantes en términos de evasión y adaptación. [14]

La Pirámide de Dolor se compone de varios niveles, comenzando con indicadores menos complejos como las direcciones IP y los nombres de dominio, y ascendiendo hacia indicadores más sofisticados como los patrones de tráfico y los artefactos de memoria. En la base de la pirámide, los IoCs como direcciones IP maliciosas y firmas de archivos proporcionan una visibilidad inmediata, pero pueden ser fácilmente cambiados por los atacantes. A medida que se asciende en la pirámide, los indicadores se vuelven más específicos y difíciles de alterar, incluyendo técnicas de fingerprinting de protocolos y patrones de comportamiento que ofrecen una visión más profunda de la actividad maliciosa. [18]

El fingerprinting de protocolos, como el método JA3, es una técnica avanzada para modelar y detectar comportamientos anómalos en el tráfico de red. JA3 es una técnica que se utiliza para crear un “fingerprint” único de las conexiones TLS/SSL basándose en los parámetros del handshake, como las versiones de protocolo, las suites de cifrado y las extensiones. Al capturar y analizar estos parámetros, JA3 permite a los analistas identificar patrones de comunicación específicos que pueden estar asociados con malware o actividades de comando y control (C&C). JA3 se centra en el tráfico de red al establecer un perfil único para cada cliente TLS/SSL basado en la combinación específica de parámetros que utiliza durante el handshake. Dado que muchos programas maliciosos utilizan implementaciones o configuraciones inusuales de TLS/SSL para evadir la detección, JA3 puede identificar patrones que no coinciden con las configuraciones estándar de clientes legítimos. Esta técnica proporciona una forma de identificar y bloquear tráfico malicioso antes de que pueda realizar actividades dañinas, incluso si el atacante cambia las direcciones IP o utiliza técnicas de evasión. [15]

La integración de IoCs como los fingerprints JA3 en las estrategias de seguridad cibernética mejora la capacidad de detección y respuesta. A diferencia de los indicadores más básicos, como

las direcciones IP, los fingerprints proporcionan una capa adicional de análisis que permite identificar amenazas que utilizan técnicas sofisticadas de evasión. Esta capacidad de modelar comportamientos específicos ayuda a los equipos de seguridad a detectar actividades maliciosas que pueden pasar desapercibidas mediante métodos tradicionales.

Los análisis de JA3 y otras técnicas avanzadas de fingerprinting se utilizan en combinación con otras herramientas de seguridad para proporcionar una visión más completa del tráfico de red y las posibles amenazas. Al correlacionar estos datos con otros IoCs y patrones de comportamiento, los profesionales de ciberseguridad pueden construir perfiles de amenaza más precisos y desarrollar estrategias de mitigación más efectivas. [16]

A pesar de su eficacia, la implementación de técnicas como JA3 presenta desafíos. La generación y el análisis de fingerprints requieren una comprensión profunda del tráfico de red y la configuración de los protocolos, así como la capacidad de integrar estos datos en sistemas de detección y respuesta en tiempo real. Además, los atacantes pueden adaptarse y modificar sus técnicas para evadir las técnicas de fingerprinting, lo que requiere una actualización constante de los métodos de detección y análisis.

La comprensión de los IoCs y la aplicación de técnicas avanzadas como el fingerprinting JA3 son fundamentales para mejorar la postura de seguridad cibernética. La Pirámide de Dolor proporciona un marco útil para evaluar la efectividad de los IoCs y guiar la implementación de estrategias de detección y respuesta. A medida que las amenazas evolucionan, la integración de múltiples técnicas y la colaboración entre organizaciones se vuelven esenciales para mantener una defensa efectiva y adaptativa contra las amenazas cibernéticas emergentes. [17]

CAPÍTULO III: DISEÑO ZONAS DE LIMPIEZA DE TRÁFICO

3.1. ARQUITECTURA DEL SCRUBBING CENTER

Los ataques DDoS representan uno de los desafíos más complejos de mitigar en el ámbito de la ciberseguridad. Es crucial que las organizaciones adopten modelos o arquitecturas óptimas para resguardarse eficazmente contra estos sofisticados vectores de ataque. Esta medida se vuelve esencial dado el creciente riesgo y la constante evolución de las tácticas empleadas por los perpetradores de ataques DDoS. Además, la implementación de estrategias sólidas y tecnologías avanzadas es fundamental para garantizar la continuidad operativa y la seguridad de los activos digitales de una organización en un entorno cada vez más hostil.

Un centro de filtrado DDoS cuenta con equipos de mitigación diseñados para enfrentar ataques de gran envergadura en redes. La mayoría de los proveedores ofrecen soluciones que consisten en múltiples centros de filtrado, generalmente distribuidos a nivel global. Durante un ataque, el tráfico se redirige al centro de filtrado más cercano, donde se analiza. Se eliminan los datos maliciosos y solo se permite el paso del tráfico legítimo a la red de la empresa. [19]

Los clientes pueden utilizar la protección del centro de filtrado de dos maneras: redirigir el tráfico según sea necesario cuando ocurre un ataque o redirigir el tráfico a través de los centros de filtrado en todo momento.

Un centro de filtrado puede detener cualquier tipo de ataque de red, ya sea web o no web (FTP, SMTP, etc.), así como ataques directos al origen. Sin embargo, no puede ofrecer protección contra ataques a nivel de aplicación. [18]

En comparación con la protección de Cloud WAF, la implementación de una solución de Scrubbing Center es más complicada debido a la desviación de tráfico BGP y el túnel GRE. Requiere que una organización posea un sistema autónomo y clases de red, pero, por otro lado, no se necesitan claves privadas, como en las soluciones Cloud WAF. Otro problema que puede surgir con un centro de filtrado es la latencia. Algunos de los proveedores que ofrecen soluciones de centro de filtrado incluyen Radware, Arbor, Akamai Prolexic, F5 Silverline y Cloudflare Magic Transit. Finalmente, se puede reducir que la arquitectura debe solventar los siguientes puntos:

- **Escalabilidad:** Los proveedores de servicios generalmente operan redes extensas con múltiples puntos de entrada. Esto plantea un desafío para identificar y mitigar ataques DDoS en toda la infraestructura.
- **Complejidad:** Los ataques DDoS pueden adoptar diversas formas, y diferentes tipos de ataques requieren técnicas de mitigación específicas. Por lo tanto, la implementación de una protección efectiva contra DDoS demanda experiencia y conocimientos especializados.
- **Costo:** Las soluciones de protección contra DDoS pueden resultar costosas, y los gastos asociados con la implementación y gestión de estas soluciones pueden acumularse rápidamente, especialmente para los proveedores de servicios que operan en redes extensas.

- **Urgencia temporal:** Los ataques DDoS pueden ocurrir en cualquier momento y sin previo aviso. Por lo tanto, los proveedores de servicios deben contar con tiempos de respuesta rápidos para mitigar el ataque antes de que cause daños significativos.

3.2. PROCESO DE FILTRADO Y DEPURACIÓN

Una vez que el tráfico es redirigido a la zona que según corresponda el firewall aplica políticas de protección basadas en una lista de reputación del fabricante Fortinet conocida como Fortiguard la misma que nos provee información relevante sobre la reputación basados en IOC a nivel de IP, Sitios Web y contenido malicioso dentro de un paquete IP. Dependiendo del tipo de tráfico que se inspecciona y del contenido en ciertos casos es posible realizar una depuración o filtrado de la información que se solicita hacia el internet mientras que en otros casos el tráfico únicamente es bloqueado. [11]

Aunque los ataques distribuidos de degradación de servicios están constantemente evolucionando, se considera que existen 4 grupos de características principales de ataques.

- **Ataques Volumétricos:** Son ataques basados en inundaciones que pueden ocurrir en las capas 3, 4 o 7. Los ataques en las capas 3–4 suelen involucrar tráfico UDP falsificado.
- **Asimétricos:** Se refieren a tráfico UDP unidireccional o sin estado
- **Computacionales:** Son ataques diseñados para consumir recursos de CPU y memoria, generalmente en la capa 7 a través de TCP.
- **Basados en Vulnerabilidades:** Son ataques que explotan vulnerabilidades de software.

Por lo que suele usarse los siguientes métodos de defensa para los tipos de ataques anteriormente mencionados. [2]

Tabla 1 Tipos de ataques por DDoS y sus metodos de mitigación

Categoría de ataque	**Método de mitigación**
Ataques Volumétricos	Scrubbing Center Lista Negra por reputación de IP Blackhole Flowspec
Asimétricos	Scrubbing Center Lista Negra por reputación de IP Blackhole Flowspec
Computacionales	Firewall de red WAF
Basados en vulnerabilidades	IPS/IDS WAF Lista Negra por reputación de IP

La lista negra por reputación de IP se refiere a la clasificación llevada a cabo por entidades externas para etiquetar direcciones IP como benignas o maliciosas, utilizando indicadores de compromiso. Sin embargo, esta práctica presenta varios desafíos, especialmente en términos de la confiabilidad de las etiquetas y la velocidad de clasificación. [2]

La rapidez de esta clasificación es crucial, ya que etiquetar erróneamente una IP como maliciosa puede resultar en la afectación del servicio para los clientes finales, especialmente si la IP en cuestión no es de naturaleza maliciosa. Por lo tanto, es esencial abordar estos desafíos de

manera cautelosa y considerar la precisión y agilidad en la toma de decisiones al utilizar este enfoque de lista negra por reputación de IP. [1]

El "blackholing" es una técnica utilizada para mitigar el impacto de un ataque de Denegación de Servicio Distribuido (DDoS). En esta técnica, el tráfico de red dirigido a la dirección IP objetivo se redirige a un "agujero negro" ("blackhole"), esencialmente un vacío virtual que elimina todo el tráfico entrante sin entregárselo al destinatario previsto. Cuando ocurre un ataque DDoS, el administrador puede identificar rápidamente la dirección IP objetivo y redirigir todo el tráfico hacia esa dirección a un agujero negro.

Sin embargo, es importante tener en cuenta que el blackholing también puede tener consecuencias no deseadas, como la eliminación de tráfico legítimo. Por lo tanto, se debe usar con precaución y solo como último recurso cuando otras técnicas de mitigación no sean efectivas. [14]

3.3. INTEGRACIÓN CON LA INFRAESTRUCTURA DE RED

Para implementar la derivación de tráfico de lo malicioso conocido, se emplea una Lista de Control de Acceso (ACL) en cada router distribuido a lo largo de las distintas zonas de servicio. Esta ACL direcciona el tráfico hacia una VRF (Routing and Forwarding Table) específica que contiene una ruta predeterminada dirigida hacia el firewall encargado de llevar a cabo la limpieza. Este firewall se encuentra ubicado en el datacenter principal y cuenta con una contingencia correspondiente en el datacenter alterno para garantizar la continuidad operativa. [25]

En la segunda zona de limpieza, donde todo el tráfico se deriva, se sitúa el firewall estratégicamente en uno de los trayectos de comunicación entre el router principal y la red de transporte óptico. Aquí, el firewall opera en modo capa 2, simulando únicamente una conexión directa y evitando la adición de saltos en la comunicación a nivel de capa 3. Esta configuración permite una eficiente filtración del tráfico malicioso, contribuyendo a la seguridad de la red y minimizando el impacto en el rendimiento del sistema. Además, se asegura la redundancia mediante la presencia de contingencias en el datacenter alterno, fortaleciendo la resiliencia del sistema ante posibles interrupciones. [16]

3.4. CAPACIDADES DE ESCABILIDAD

En la actualidad, el proceso de scrubbing con derivación de tráfico malicioso conocido presenta un rendimiento notable, con un promedio de 200 Mbps de tráfico, y su equipamiento está dimensionado para manejar una capacidad de hasta 15 Gbps. Este enfoque ha demostrado ser eficiente en la detección y mitigación de amenazas conocidas, proporcionando una sólida defensa para la infraestructura de red. [17]

Por otro lado, la modalidad de scrubbing que implica la derivación de todo el tráfico se destaca por su capacidad de manejar volúmenes significativamente mayores. Actualmente, este sistema opera con un tráfico promedio de 100 Gbps, y su equipamiento está diseñado para soportar hasta 1.5 Tbps. Esta mejora en la capacidad de procesamiento permite gestionar eficazmente grandes flujos de datos, asegurando una protección integral contra diversas amenazas, incluyendo aquellas de naturaleza desconocida.

Estas capacidades diferenciadas ofrecen una respuesta adaptativa a las cambiantes dinámicas del panorama de seguridad cibernética, permitiendo una gestión efectiva de los riesgos y la garantía de un entorno de red seguro y eficiente. Es esencial destacar que la continua evolución y optimización de estos enfoques son fundamentales para mantenerse a la vanguardia en la protección contra amenazas emergentes. [13]

CAPÍTULO IV: IMPLEMENTAR PANEL DE VISUALIZACIÓN DE AMENAZAS

4.1. SELECCIÓN DE LA PLATAFORMA DEL PANEL DE VISUALIZACIÓN

Existen diversas plataformas destinadas a monitorear y dar seguimiento a la visualización de eventos, no obstante, es esencial destacar que las herramientas preeminentes para la correlación de datos son los SIEMs. Un SIEM (Security Information and Event Management) representa una solución integral que fusiona la gestión de información de seguridad (SIM) y la gestión de eventos de seguridad (SEM), ofreciendo así una perspectiva centralizada y analítica de los datos asociados con la seguridad de una organización. [11]

Un SIEM (Security Information and Event Management) desempeña funciones clave para fortalecer la postura de seguridad de una organización. En primer lugar, se encarga de la recopilación de datos, agregando registros y eventos de seguridad provenientes de diversas fuentes, como firewalls, antivirus, sistemas de detección de intrusiones, servidores y otros

dispositivos de red. A continuación, mediante la normalización y correlación de datos, el SIEM garantiza que la información se presente en un formato consistente, identificando patrones que podrían sugerir amenazas al correlacionar eventos aparentemente no relacionados. [9]

La seguridad de la información también se ve reforzada a través del almacenamiento seguro proporcionado por el SIEM, que no solo almacena los datos de manera segura, sino que también facilita la recuperación de información histórica para análisis y para cumplir con las normativas vigentes. Además, el SIEM emplea técnicas avanzadas de análisis de datos y reglas predefinidas para detectar posibles amenazas, generando alertas y, en ciertos casos, llevando a cabo acciones automáticas o brindando recomendaciones para la respuesta.

En términos de rendición de cuentas y cumplimiento normativo, el SIEM facilita la generación de informes personalizados y proporciona evidencia concreta de la aplicación efectiva de medidas de seguridad adecuadas. Finalmente, a través de la integración con otras herramientas de seguridad, como firewalls, sistemas de prevención de intrusiones y antivirus, el SIEM mejora la eficiencia y la capacidad de respuesta, creando un ecosistema de seguridad integral para la organización. [10]

Basándome en mi experiencia personal, opto por el uso de Kibana como el mejor SIEM. Esta elección se fundamenta en la notable versatilidad que ofrece en cuanto a la integración de diversas fuentes de datos y la estructura gestionada por la comunidad. Kibana, al ser parte del stack ELK (Elasticsearch, Logstash, Kibana), proporciona una plataforma sólida y flexible para la visualización y análisis de eventos de seguridad.

La fortaleza de Kibana radica en su capacidad para trabajar con conjuntos de datos heterogéneos, facilitando la correlación de información desde diferentes fuentes de seguridad. Además, su estructura gestionada por la comunidad significa que se beneficia constantemente de las contribuciones y mejoras de una amplia base de usuarios, lo que garantiza una evolución continua y adaptabilidad a las necesidades cambiantes en el ámbito de la seguridad de la información. [11]

Al elegir Kibana, no solo se accede a una herramienta potente para la gestión de eventos de seguridad, sino que también se aprovecha la experiencia colectiva de una comunidad activa, lo que contribuye a la eficacia y robustez del enfoque de seguridad implementado. [5]

4.2. INTEGRACIÓN DE FUENTE DE DATOS

A continuación, se presenta un diagrama de alto nivel (ilustración 4.1) que ilustra la integración y visualización de datos en nuestro sistema. Este diagrama proporciona una visión general de cómo se conectan las diferentes componentes para recopilar, procesar y presentar información de manera efectiva. Cada bloque en el diagrama representa un componente clave en el flujo de datos, desde la ingestión inicial hasta la visualización final en la interfaz de usuario. [12]

Este enfoque integral facilita la comprensión de la arquitectura subyacente y cómo los datos fluyen a lo largo del proceso. Además, destaca la interacción entre los diversos elementos para lograr una integración eficiente y una presentación significativa de la información recopilada.

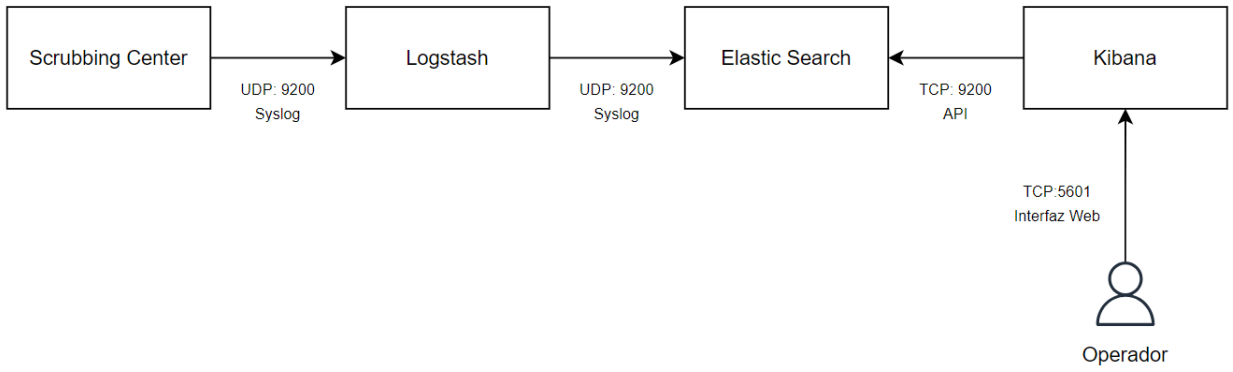

Ilustración 2. Diagrama de alto nivel de la integración de los datos a un SIEM

En este escenario, los eventos generados por el scrubbing center son enviados al puerto 9200 UDP (utilizando el protocolo syslog), marcando el inicio del proceso de recolección y análisis de datos.

El primer componente clave en esta cadena de integración es Logstash, una herramienta de procesamiento y filtrado de logs. Logstash recibe los datos syslog del scrubbing center y realiza operaciones de parsing y normalización para asegurar que la información se encuentre en un formato coherente y estructurado. Esta etapa es crucial para la correlación efectiva de eventos y para garantizar que la información sea interpretada de manera consistente por las fases subsiguientes del sistema. [15]

A continuación, los datos procesados por Logstash son transmitidos hacia Elasticsearch, que actúa como el motor de búsqueda central. Elasticsearch indexa y almacena los eventos de manera eficiente, permitiendo búsquedas rápidas y análisis avanzado. Este componente es fundamental para mantener una base de datos de eventos robusta y escalable, lo que facilita la gestión y recuperación de información histórica de manera efectiva.

Finalmente, para la visualización y análisis de los datos almacenados en Elasticsearch, se implementa Kibana como la plataforma para el usuario final. Kibana ofrece una interfaz intuitiva

y potente que permite a los usuarios explorar, visualizar y comprender los eventos recopilados. Desde la creación de dashboards personalizados hasta la ejecución de consultas específicas, Kibana proporciona las herramientas necesarias para una comprensión detallada y una respuesta efectiva a los eventos de seguridad. [16]

En conjunto, esta integración técnica del scrubbing center con Logstash, Elasticsearch y Kibana constituye un sistema integral que mejora la visibilidad, la capacidad de respuesta y la eficiencia en la gestión de eventos de seguridad. La implementación de este flujo de trabajo proporciona una base sólida para la monitorización y protección proactiva contra amenazas. [7]

4.3. PROCESAMIENTO Y ANÁLISIS DE DATOS

Dado que los eventos son transmitidos en formato syslog, lo cual es posible gracias a la tecnología empleada en el proyecto actual, se opta por utilizar los nombres de los campos proporcionados por la herramienta de seguridad. Como parte del proceso, se lleva a cabo la extracción de los nombres y valores asociados a dichos campos.

Este enfoque se basa en la eficiente estructura del formato syslog, permitiendo la identificación y utilización directa de los campos de interés establecidos por la herramienta de seguridad. Al emplear esta estrategia, se facilita la integración y el manejo de los datos, asegurando coherencia en la interpretación de la información contenida en los eventos.

La extracción de los nombres y valores de los campos es un paso crítico para la posterior fase de procesamiento y análisis de datos. Este procedimiento es esencial para garantizar la coherencia y precisión en la interpretación de la información, lo que contribuye significativamente a la validez y relevancia de los resultados obtenidos en el marco del proyecto.

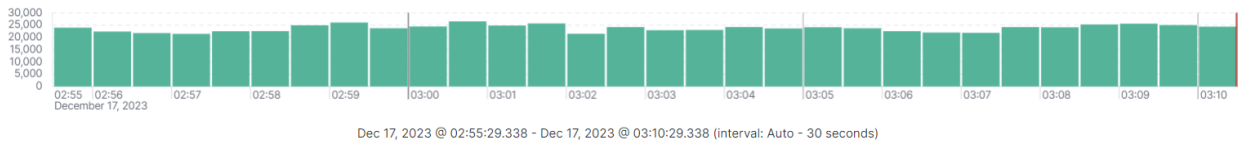

Ilustración 3. Cantidad de eventos recolectados desde el scrubbing center al SIEM

Actualmente, según se evidencia en la ilustración 2, se registra una tasa promedio de alrededor de 25,000 eventos cada 30 segundos. Extrapolando este ritmo, se estima que diariamente se procesarán alrededor de 72,000,000 de eventos, lo que equivale aproximadamente a 50 GB de datos por día. Esta magnitud de información resulta prácticamente imposible de ser analizada operativamente por el personal del Centro de Operaciones de Seguridad (SOC) con el propósito de identificar y descartar comportamientos maliciosos. [8]

La ingente cantidad de datos generados diariamente presenta un desafío significativo para la operatividad del SOC, ya que la capacidad de procesamiento humano se ve claramente superada. En consecuencia, resulta imperativo implementar soluciones tecnológicas y estrategias automatizadas para la detección temprana de comportamientos sospechosos, permitiendo así una respuesta más eficiente ante posibles amenazas a la seguridad. Este enfoque estratégico es esencial para garantizar la integridad y eficacia de las operaciones de seguridad en el entorno operativo actual.

Gracias a la correcta realización del proceso de parseo de la información, se confirma la existencia de un total de 74 campos que han sido extraídos de manera integral de los eventos de seguridad. Este procedimiento de parseo, fundamental para la estructuración y organización de los datos, ha permitido validar la presencia y correcta interpretación de estos campos en los eventos recibidos. La identificación de estos 74 campos es esencial para la posterior fase de análisis, ya que proporciona una visión detallada y exhaustiva de la información contenida en los

eventos de seguridad, facilitando así interpretaciones precisas y una comprensión más profunda de los datos registrados. [9]

A continuación, en la ilustración 3, se presenta la exploración de datos en la plataforma de SIEM mediante Kibana. Esta visualización ofrece una interfaz gráfica que permite analizar y comprender de manera efectiva la información recopilada. La herramienta Kibana facilita la interpretación de datos a través de diversos gráficos, tablas y paneles, brindando una visión intuitiva y detallada de los eventos de seguridad. Este enfoque visual resulta esencial para el monitoreo y la detección de patrones, contribuyendo así a una gestión más eficiente de la seguridad de la información.

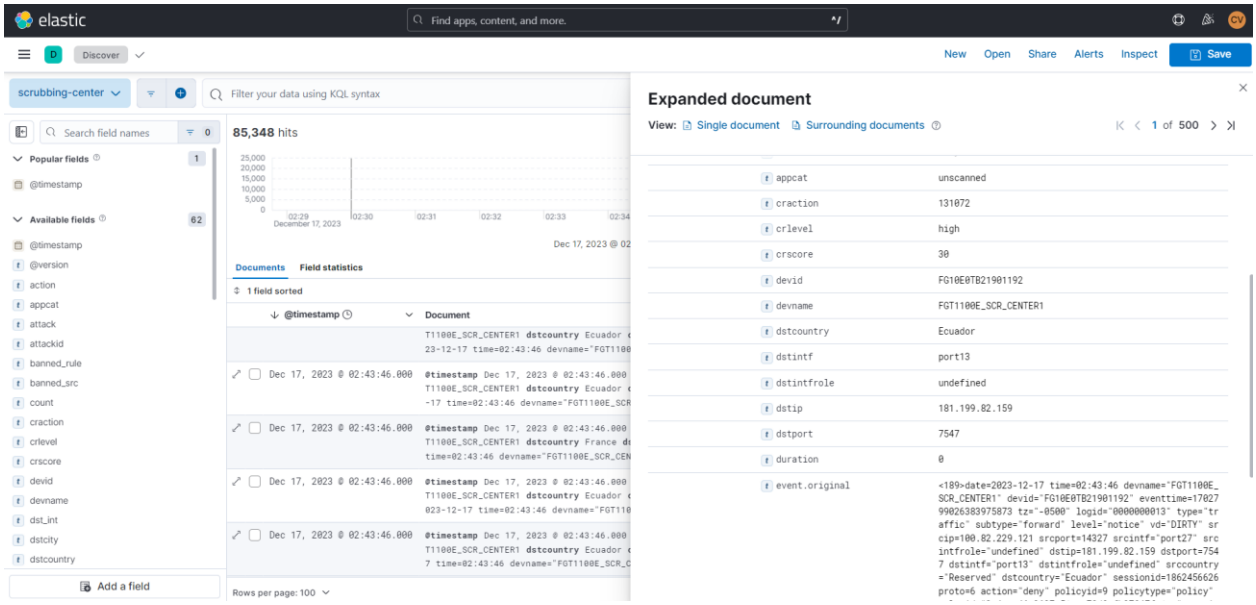

Ilustración 4. Módulo de exploración de eventos del SIEM con la información del Scrubbing Center

4.4. VISUALIZACIÓN DE DATOS

A continuación, tal como se aprecia en la ilustración 4, se presenta el módulo de paneles de visualización de los datos de la herramienta de seguridad de Scrubbing Center. Esta sección es esencial para monitorear y analizar diversos aspectos críticos del entorno de seguridad. Al utilizar estos paneles, se puede realizar un seguimiento minucioso de la cantidad de eventos recibidos por minuto, examinar las acciones llevadas a cabo por Scrubbing Center, evaluar la clasificación y la cantidad de severidad de conexiones, identificar los principales 10 ataques detectados, comprender las 5 políticas de seguridad más activadas, analizar las principales 10 direcciones IP de origen y destino, explorar los 5 puertos de destino más relevantes, revisar la cantidad de eventos relacionados con acciones y países destino, y evaluar el volumen de tráfico entre países de origen y destino. [4]

La importancia de esta visualización radica en la capacidad que brinda para realizar un seguimiento en tiempo real y de manera intuitiva de las métricas críticas relacionadas con la seguridad de la red. Estos paneles proporcionan información clave que permite a los responsables de seguridad identificar patrones, tomar decisiones informadas y responder eficazmente a eventos de seguridad. Asimismo, facilitan la comprensión integral del panorama de amenazas y la evaluación del rendimiento del sistema, contribuyendo así a fortalecer la postura de seguridad de la organización. [1]

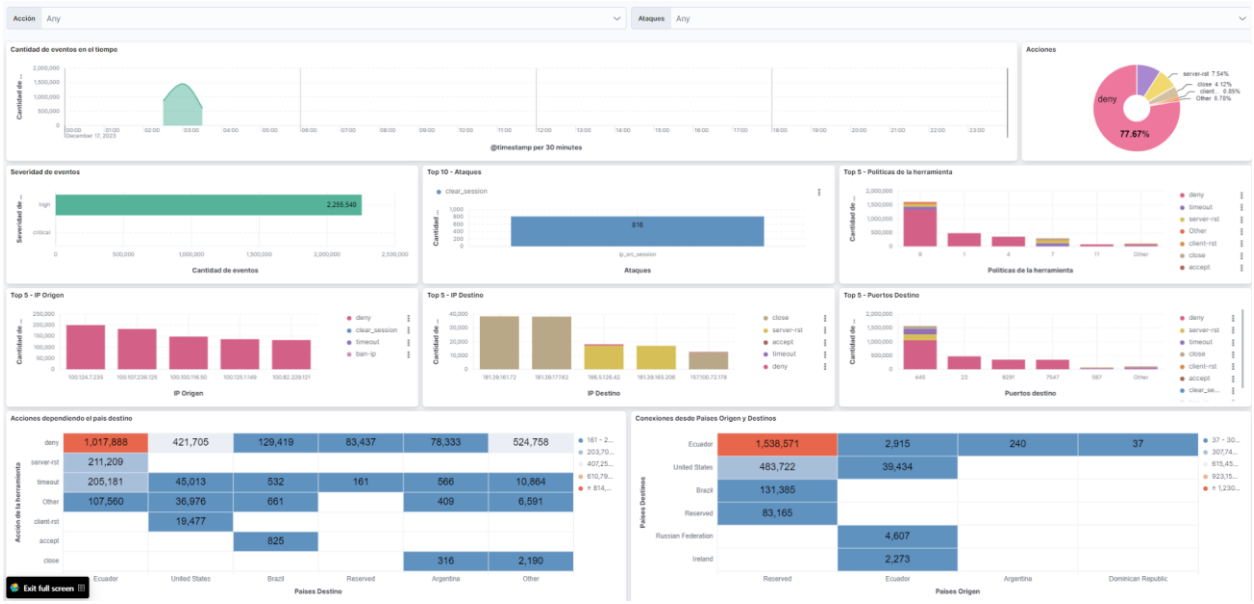

Ilustración 5 Paneles de visualización del estado de tráfico analizado por el Scrubbing Center a nivel gerencial

4.5. CAPACIDAD DE REPORTES Y AUDITORIA PARA LA ALTA GERENCIA

Dentro de la herramienta del Sistema de Gestión de Eventos e Información de Seguridad (SIEM), se cuenta con la capacidad de configurar y automatizar el envío de informes a los operadores del Centro de Operaciones de Seguridad (SOC). Estos profesionales llevan a cabo una revisión previa y realizan los ajustes necesarios antes de que los informes sean autorizados por las jefaturas correspondientes. Una vez autorizados, los informes son remitidos a la gerencia técnica, quienes tienen la responsabilidad de tomar decisiones a nivel ejecutivo. Esta estructura de revisión y autorización asegura la precisión y relevancia de la información antes de llegar a la gerencia técnica. Además, proporciona a la alta dirección una visión global y detallada de los eventos y actividades en la red, permitiéndoles tomar decisiones estratégicas fundamentadas en un panorama integral de la seguridad informática. Este proceso contribuye de manera significativa a la toma de decisiones a alto nivel en la organización.

Tal como se aprecia en la ilustración 5, se presenta un resumen de los paneles de visualización previamente detallados, acompañado por la descripción de las observaciones realizadas. Este análisis de alto nivel es llevado a cabo por especialistas en seguridad y profesionales expertos en las operaciones de la empresa. Su tarea principal consiste en descartar falsos positivos, proporcionando así una evaluación precisa y enfocada en las amenazas reales. Este proceso de revisión y análisis experto se lleva a cabo con el objetivo claro de mantener la precisión en la identificación y erradicación de amenazas genuinas. La combinación de la tecnología de visualización avanzada y la experiencia humana especializada se traduce en una estrategia efectiva para asegurar la integridad y la eficacia de las operaciones de seguridad de la organización. [12]

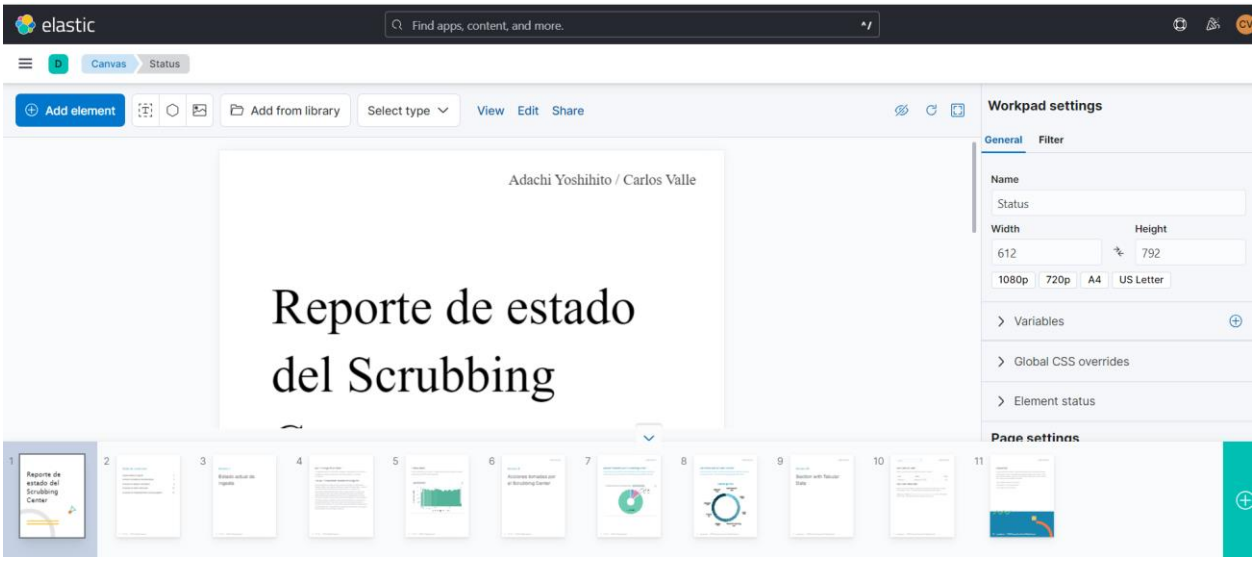

Ilustración 6. Reporte diseñado para la alta gerencia del estado actual de tráfico detectado como malicioso

El informe se envía a través de correo electrónico en formato PDF y cuenta con la flexibilidad de ser personalizado según las necesidades y requisitos de las jefaturas. Además, se adapta a los

puntos de auditoría identificados en la empresa para satisfacer las demandas específicas de monitoreo y visualización. Este enfoque permite cumplir con las normativas establecidas dentro de las políticas de seguridad e información de la organización. La capacidad de personalización y ajuste a los estándares de auditoría proporciona a las jefaturas una herramienta adaptada a sus necesidades específicas, facilitando una comprensión detallada de la situación de seguridad y contribuyendo a una gestión más efectiva y alineada con las políticas corporativas. [16]

CAPÍTULO V: EVALUACIÓN DE LAS AMENAZAS

5.1. TIPO DE AMENAZAS OBSERVADAS

A partir del análisis del tráfico dirigido hacia el Scrubbing Center, se han identificado cinco amenazas que requieren una evaluación más detallada. Este análisis adicional permitirá confirmar la naturaleza de las amenazas y determinar las acciones correctivas necesarias para mitigar los riesgos asociados, adaptándolas según el tipo específico de amenaza.

Intrusiones y Escaneos de Puertos: Un análisis exhaustivo del tráfico puede identificar intentos de escaneo de puertos, los cuales se utilizan para buscar vulnerabilidades en la red. Los escaneos de puertos suelen generar un elevado volumen de tráfico dirigido a diversos puertos con el objetivo de descubrir posibles puntos de entrada que podrían ser explotados para comprometer la seguridad.

Malware y Comunicaciones de Comando y Control (C2): El tráfico dirigido hacia y desde servidores de comando y control (C2) puede ser indicativo de la presencia de malware en la red. Este tipo de tráfico incluye comunicaciones cifradas o encubiertas, que podrían señalar la existencia de un botnet u otras formas de software malicioso, el cual utiliza estos servidores para recibir instrucciones y exfiltrar datos.

Exfiltración de Datos: La detección de tráfico que muestra grandes volúmenes de datos siendo transferidos fuera de la red puede ser un signo de intentos de exfiltración de información confidencial o robada. Este comportamiento sospechoso sugiere posibles intentos de fuga de datos que podrían comprometer la integridad y la seguridad de la información.

Uso No Autorizado de Protocolos o Servicios: La aparición de tráfico inusual relacionado con protocolos o servicios no autorizados en la red puede ser una señal de que se están utilizando recursos de la red para fines no aprobados. Este uso indebido de protocolos o servicios puede indicar actividades maliciosas o no permitidas que podrían poner en riesgo la seguridad de la infraestructura de red. [13]

Vulnerabilidades en Protocolos: El tráfico en la red puede revelar intentos de explotar vulnerabilidades conocidas en protocolos de comunicación. Esto incluye el envío de paquetes maliciosos diseñados para aprovechar debilidades específicas en los protocolos, lo que puede comprometer la integridad y la confidencialidad de los datos transmitidos.

5.2. ANÁLISIS DE TRAFICO DE RED

En el presente análisis de red, se limita la recopilación de datos a nivel de dirección IP y protocolo (Capa 3 - Capa 4 del modelo OSI). Esta metodología permite la correlación de información basada en Indicadores de Compromiso (IoCs) asociados a direcciones IP, sin comprometer la privacidad ni la integridad de los datos del usuario final. [4]

Las alertas se generan en respuesta a conexiones dirigidas a destinos clasificados como maliciosos. Estas alertas pueden surgir debido a la detección de tráfico que utiliza protocolos específicos para comunicarse con servidores identificados como potencialmente peligrosos, o por la observación de patrones de tráfico que indican escaneos de red, tales como conexiones excesivas a múltiples destinatarios. Este tipo de actividad puede ser indicativo de intentos de exploración o escaneo (scanning) para identificar vulnerabilidades en la red.

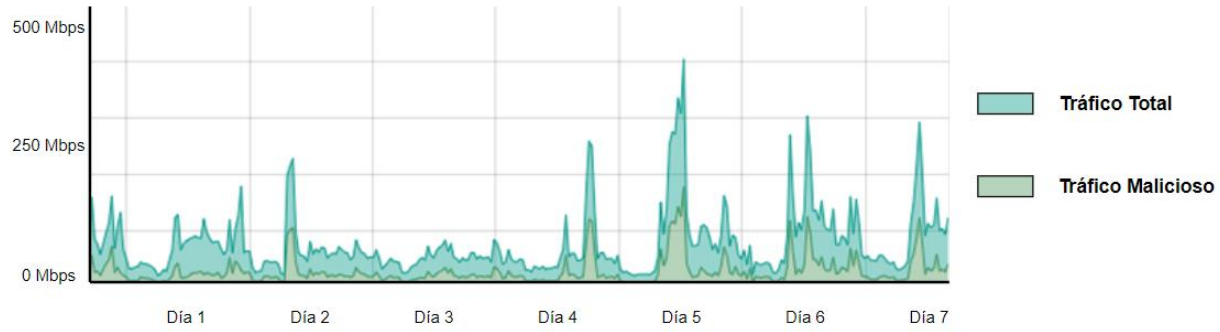

Ilustración 7 Tráfico total y malicioso detectado por la herramienta de filtrado de paquetes en un periodo de 1 semana.

La ilustración 6 se presenta un análisis del consumo promedio semanal de tráfico clasificado como malicioso, el cual es dirigido hacia el Scrubbing Center.

Además, se puede observar en la gráfica que el tráfico malicioso exhibe un comportamiento que se asemeja al tráfico total, representando aproximadamente el 30% del volumen global de tráfico.

La tabla proporciona un resumen del tráfico que es redirigido al Scrubbing Center para su posterior análisis. Este tráfico es evaluado para identificar y mitigar posibles amenazas, asegurando que solo el tráfico legítimo continúe hacia su destino final. [5]

Tabla 2 Tipos de puertos asociados por su servicio estándar y las vulnerabilidades que frecuentemente son vigentes

PROTOCOLO	**SERVICIO**	**VULNERABILIDAD**
TCP/25	SMTP	SPAM
TCP/587	SMTP	SPAM
TCP/22	SSH	C&C
TCP/23	TELNET	BRUTEFORCE
TCP/445	SAMBA	MALWARE

Para un mayor contexto de la tabla anteriormente obtenida, se detalla lo siguiente:

TCP/25 (SMTP - Simple Mail Transfer Protocol) - Spam:

El puerto 25 se utiliza para el envío de correos electrónicos mediante el protocolo SMTP. Es uno de los puertos más comúnmente explotados para enviar spam debido a su función primordial en la transferencia de correos electrónicos.

El spam, o correo electrónico no deseado, puede ser enviado masivamente desde servidores comprometidos o mal configurados. La literatura de seguridad resalta que el spam puede ser

utilizado para distribuir malware, phishing, o simplemente inundar la bandeja de entrada de los usuarios con mensajes no deseados.

TCP/587 (SMTP - Submission) - Spam:

El puerto 587 es utilizado para el envío de correos electrónicos a través de SMTP con autenticación. Aunque este puerto está diseñado para mejorar la seguridad mediante la autenticación, también puede ser usado para el envío de spam si el servidor está comprometido.

El uso de autenticación para el envío de correos electrónicos no siempre previene el abuso si el servidor es mal configurado o comprometido. Symantec y otras fuentes de seguridad destacan que la autenticación en el puerto 587 puede ser insuficiente si el servidor es utilizado por atacantes para enviar spam. [17]

TCP/22 (SSH - Secure Shell) - C&C (Command and Control):

El puerto 22 se utiliza para el protocolo SSH, que proporciona una manera segura de acceder a sistemas remotos. Sin embargo, cuando es explotado, puede servir para las comunicaciones de comando y control (C&C) entre un atacante y una red comprometida.

Los servidores SSH comprometidos pueden ser utilizados para controlar remotamente sistemas infectados, facilitando la ejecución de comandos maliciosos. FireEye y otros informes de seguridad indican que los puertos SSH son a menudo utilizados para mantener el acceso no autorizado a sistemas comprometidos. [15]

TCP/23 (Telnet) - Bruteforce:

Telnet, que opera en el puerto 23, es un protocolo de red que permite la comunicación en modo texto. Es conocido por su falta de cifrado, lo que lo hace vulnerable a ataques de fuerza bruta, en los cuales los atacantes intentan múltiples combinaciones de contraseñas para acceder al sistema.

Debido a su falta de cifrado y autenticación básica, Telnet es un objetivo frecuente para ataques de fuerza bruta. CVE Details y otras bases de datos de vulnerabilidades indican que Telnet ha sido sustituido en muchas aplicaciones modernas por protocolos más seguros como SSH debido a estos problemas.

TCP/445 (SMB - Server Message Block) - Malware:

El puerto 445 se utiliza para el protocolo SMB, que es usado para compartir archivos e impresoras en redes Windows. La explotación de SMB puede resultar en la distribución de malware.

SMB ha sido el objetivo de varios ataques significativos, incluyendo ransomware como WannaCry. Microsoft y otras organizaciones de seguridad han documentado múltiples vulnerabilidades en SMB que pueden ser explotadas para distribuir malware y comprometer sistemas en una red.

Por lo tanto, el análisis de estas vulnerabilidades se alinea con la primera etapa del modelo MITRE ATT&CK, que se centra en la Reconnaissance y la Initial Access. En esta fase inicial, los atacantes realizan escaneos y buscan debilidades en los sistemas para identificar puntos vulnerables que puedan explotar. La observación de servicios comunes y puertos abiertos proporciona a los atacantes pistas sobre posibles vulnerabilidades. [14]

En el contexto de la Seguridad en Capas (Modelo de Cebolla), este análisis representa solo una capa del enfoque integral de seguridad. El modelo de seguridad en capas implica la

implementación de múltiples niveles de protección para mitigar los riesgos. En este caso, se está analizando la primera capa de defensa, donde los atacantes y escaneadores de Internet intentan descubrir vulnerabilidades mediante la observación de la huella digital expuesta de una empresa.

La identificación de estas vulnerabilidades en esta etapa es una práctica normal y esencial para desarrollar una estrategia de defensa robusta. La protección adecuada en cada capa ayuda a minimizar el riesgo y a proteger la red contra posibles ataques.

5.3. TASA DE INCIDENTES

Se registra un promedio de 3,000 incidentes diarios, los cuales se pueden clasificar de la siguiente manera:

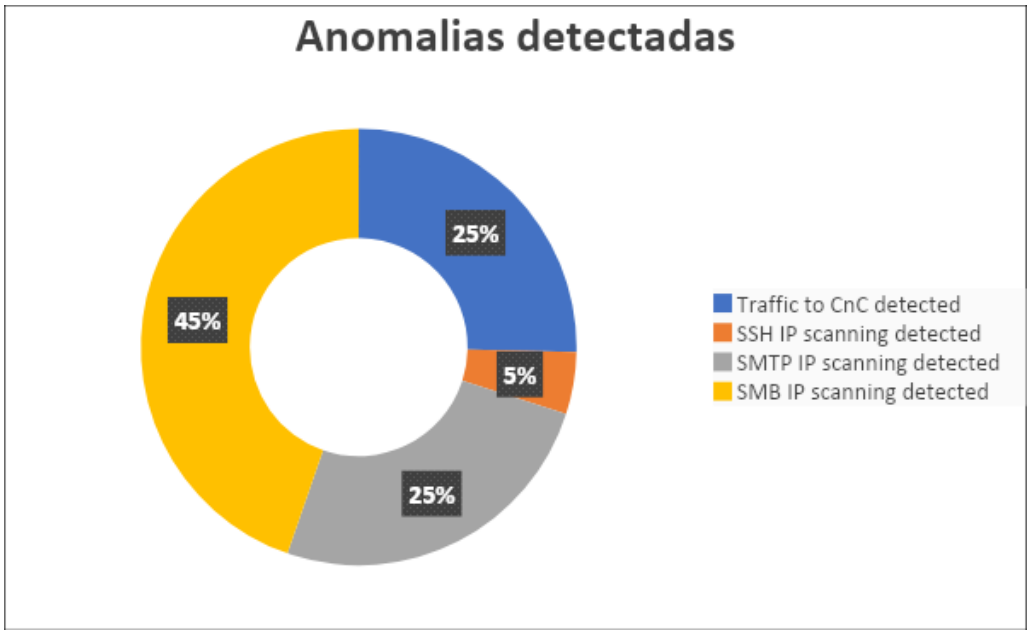

Ilustración 8 Porcentaje de tipo de ataques detectados en la red en el periodo de analisis.

Traffic to CnC Detected (25%)

El tráfico dirigido a servidores de Comando y Control (CnC) representa el 25% de las anomalías detectadas. Este tráfico indica la comunicación entre sistemas comprometidos y servidores externos utilizados por los atacantes para controlar y gestionar malware o redes botnet. [12]

La presencia de tráfico hacia servidores CnC es una señal clara de que la red puede estar comprometida por malware o software malicioso que intenta comunicarse con un servidor externo para recibir instrucciones, enviar datos robados o realizar otras acciones maliciosas. Identificar y bloquear este tráfico es crítico para la contención y eliminación de amenazas dentro de la red.

Si no se aborda adecuadamente, el tráfico hacia CnC puede facilitar la expansión de una intrusión, comprometer la integridad de los datos y permitir el control remoto de sistemas afectados, lo que puede llevar a un daño significativo a la infraestructura de TI. [2]

SSH IP Scanning (5%)

El escaneo de IP en el puerto SSH (TCP/22) representa el 5% de las anomalías detectadas. Esta actividad involucra el intento de conectar con múltiples direcciones IP utilizando el protocolo SSH para identificar sistemas vulnerables o acceder a ellos sin autorización.

El escaneo SSH puede ser un indicativo de ataques de fuerza bruta o intentos de explotar vulnerabilidades en el protocolo SSH. Aunque representa una proporción menor de las anomalías detectadas, es esencial monitorear y responder a estos escaneos para prevenir accesos no autorizados y proteger la administración remota de sistemas.

El escaneo SSH puede resultar en compromisos si los atacantes logran encontrar contraseñas débiles o configuraciones inseguras. La protección adecuada y la implementación de autenticación robusta son necesarias para mitigar estos riesgos.

SMTP IP Scanning (25%)

El escaneo de IP en el puerto SMTP (TCP/25) representa el 25% de las anomalías detectadas. Este escaneo se dirige a identificar servidores de correo electrónico que podrían estar mal configurados o vulnerables a abusos como el envío de spam o malware.

El escaneo SMTP puede ser utilizado por los atacantes para buscar servidores que puedan ser explotados para el envío de correos electrónicos maliciosos o para realizar campañas de spam. Este tipo de actividad puede estar asociado con intentos de comprometer la infraestructura de correo electrónico o utilizarla para ataques adicionales. [3]

Si se compromete un servidor SMTP, los atacantes podrían utilizarlo para distribuir spam o malware, afectando la reputación de la organización y comprometiendo la seguridad de los usuarios finales.

SMB IP Scanning (45%)

El escaneo de IP en el puerto SMB (TCP/445) representa el 45% de las anomalías detectadas. Esta actividad implica la búsqueda de sistemas que utilizan el protocolo SMB para compartir archivos e impresoras en una red. [7]

El escaneo SMB es significativo debido a la prominencia de SMB como objetivo en ataques recientes, incluyendo ransomware y otras formas de malware. Dado que SMB puede exponer

vulnerabilidades críticas, como las encontradas en los ataques WannaCry y NotPetya, un alto porcentaje de escaneos en este puerto puede indicar intentos de explotar estas vulnerabilidades.

Un alto volumen de escaneos SMB puede preceder a ataques más graves, como la propagación de ransomware o la explotación de vulnerabilidades para la escalada de privilegios. Es crucial implementar medidas de seguridad robustas y mantener el protocolo SMB actualizado para protegerse contra estas amenazas.

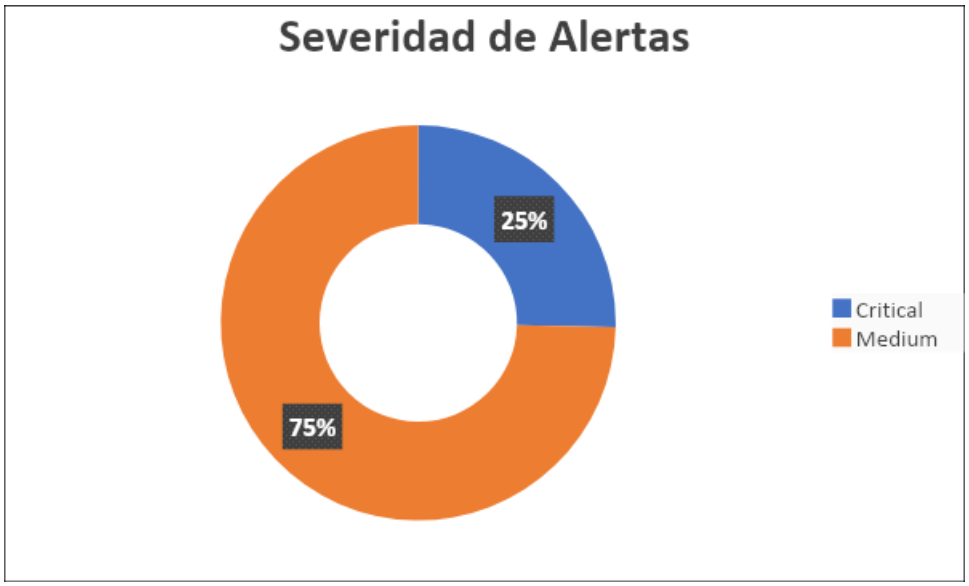

Ilustración 9 Porcentaje de las severidades de alertas detectadas por la herramienta en el periodo de análisis

El análisis de las alertas de seguridad ha revelado que el 25% de las alertas son clasificadas como críticas, mientras que el 75% restante se considera de nivel medio. Esta distribución proporciona una visión clara sobre la gravedad y la frecuencia de los incidentes detectados, y su interpretación es fundamental para priorizar las respuestas y fortalecer la postura de seguridad. [16]

Alertas Críticas (25%)

Las alertas críticas representan un cuarto del total de las alertas y están asociadas con eventos que indican una amenaza grave e inmediata para la seguridad de la red. Estas alertas suelen estar vinculadas a actividades que pueden comprometer significativamente la integridad, confidencialidad o disponibilidad de los sistemas afectados. [2]

Las alertas críticas requieren una respuesta rápida y efectiva debido a su potencial para causar daño inmediato. Los eventos clasificados como críticos pueden incluir intentos de acceso no autorizado, ataques de ransomware, tráfico hacia servidores de comando y control (CnC), y otras acciones que podrían llevar a una brecha de seguridad severa. La atención prioritaria a estas alertas es esencial para prevenir daños graves y contener posibles incidentes de seguridad antes de que se conviertan en crisis.

La omisión o retraso en la respuesta a alertas críticas puede resultar en compromisos significativos, pérdida de datos, interrupción de servicios y daño a la reputación de la organización. Es crucial contar con un plan de respuesta a incidentes bien definido y recursos adecuados para abordar estas amenazas de manera efectiva. [18]

Alertas Medias (75%)

Las alertas medias constituyen el 75% del total y están asociadas con eventos que, aunque no son inminentemente peligrosos, aún representan riesgos que deben ser gestionados adecuadamente. Estas alertas pueden incluir actividades sospechosas, patrones inusuales de tráfico, y vulnerabilidades que requieren atención pero no representan una amenaza inmediata.

Las alertas medias, aunque menos urgentes que las críticas, son fundamentales para mantener la seguridad de la red a largo plazo. La gestión efectiva de estas alertas implica monitorear y

analizar actividades que podrían indicar problemas potenciales antes de que escalen a situaciones críticas. Las alertas medias a menudo proporcionan información valiosa para la identificación temprana de tendencias y patrones que podrían señalar problemas de seguridad futuros.

Si no se abordan adecuadamente, las alertas medias pueden evolucionar hacia problemas más serios, como brechas de seguridad o vulnerabilidades explotables. La capacidad de gestionar y priorizar estas alertas asegura que se mantenga una vigilancia continua y se mitiguen los riesgos antes de que se conviertan en amenazas críticas. [19]

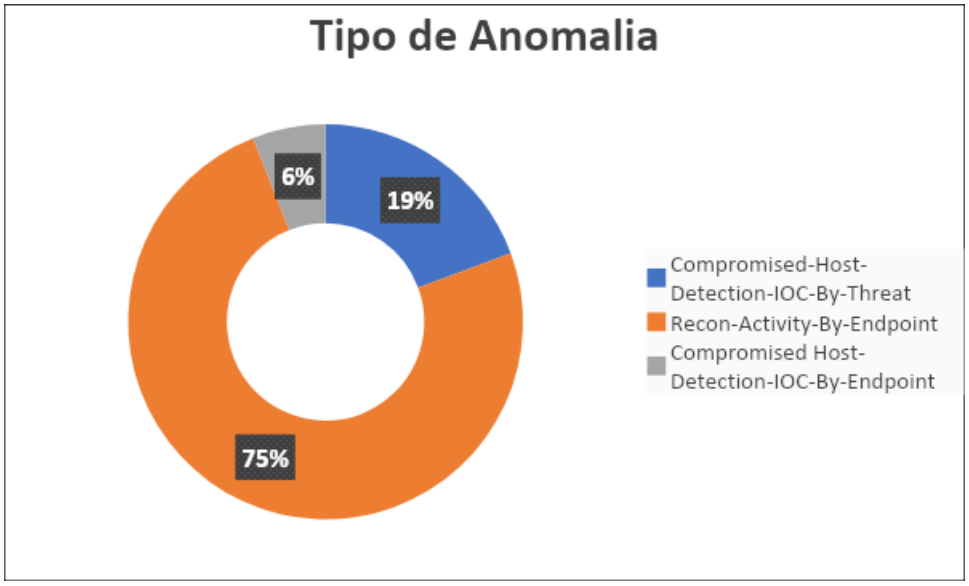

Ilustración 10 Porcentaje por categoría de tipo de ataque detectado por la herramienta en el periodo de análisis.

Compromised Host Detection IoC by Threat (19%)

La detección de indicadores de compromiso (IoC) relacionados con hosts comprometidos por amenazas representa el 19% de las anomalías. Esta categoría se refiere a la identificación de

hosts dentro de la red que han sido comprometidos por amenazas específicas, basadas en IoCs asociados con actividad maliciosa.

La detección de hosts comprometidos es crucial para contener y mitigar brechas de seguridad. Estos indicadores suelen incluir firmas de malware, patrones de comportamiento inusuales, o comunicación con servidores de comando y control (CnC). La identificación de estos IoCs permite a los equipos de seguridad focalizarse en los sistemas afectados y tomar medidas correctivas para restaurar la seguridad y evitar la propagación de la amenaza.

Un alto porcentaje de hosts comprometidos puede indicar una brecha de seguridad significativa, con riesgos asociados como la pérdida de datos, la interrupción de servicios, o el acceso no autorizado a información sensible. La respuesta rápida y efectiva a estos indicadores es esencial para minimizar el daño y prevenir futuras intrusiones.

Recon Activity by Endpoint (75%)

La actividad de reconocimiento detectada por endpoint representa el 75% de las anomalías. Esta actividad incluye escaneos y recopilación de información por parte de actores maliciosos que buscan identificar vulnerabilidades y preparar el terreno para posibles ataques. [18]

El reconocimiento por parte de endpoints es una etapa preliminar en el ciclo de vida de un ataque cibernético. Durante esta fase, los atacantes recopilan información sobre los sistemas de la red, identifican servicios expuestos y evalúan posibles vectores de ataque. La alta proporción de actividad de reconocimiento indica un interés activo en la exploración y potencial explotación de la infraestructura de red.

Una elevada actividad de reconocimiento puede señalar una preparación para ataques futuros y la posible identificación de vulnerabilidades en la red. Aunque no necesariamente indica una

intrusión actual, la detección temprana de esta actividad permite a los equipos de seguridad reforzar las defensas y abordar las vulnerabilidades antes de que sean explotadas.

Compromised Host Detection IoC by Endpoint (6%)

La detección de indicadores de compromiso (IoC) relacionados con hosts comprometidos, específica por endpoint, constituye el 6% de las anomalías detectadas. Esta categoría se enfoca en la identificación de compromisos en endpoints individuales dentro de la red, utilizando IoCs específicos para cada dispositivo.

La detección de compromisos en endpoints es esencial para la gestión de la seguridad a nivel de dispositivo. Identificar y abordar compromisos en endpoints individuales ayuda a contener las amenazas localizadas y prevenir que se propaguen a otros sistemas dentro de la red. Este enfoque granular es clave para mantener una postura de seguridad robusta y minimizar el impacto de incidentes de seguridad.

Aunque el porcentaje de detección en esta categoría es relativamente bajo, la identificación de compromisos específicos por endpoint es crucial para la contención de amenazas y la mitigación de riesgos. La respuesta oportuna a estos IoCs puede prevenir la escalada de compromisos y proteger la integridad de la red. [1]

5.4. FUENTE DE AMENAZAS

La fuente de amenazas son entidades, actividades, o condiciones que pueden causar daño a un sistema, red o información. Identificar estas fuentes es crucial para la gestión efectiva de la seguridad dentro del ISP.

Basados en los servicios o riesgos que se pueden atribuir a la publicación o acceso a recursos expuestos al internet, a continuación, se detalla las principales fuentes de amenazas que pueden afectar a sistemas y redes: [13]

Amenazas Externas

- **Hackers y Cibercriminales:** Individuos o grupos que buscan explotar vulnerabilidades para obtener acceso no autorizado, robar datos o causar daño.
- **Organizaciones de Amenazas Avanzadas:** Grupos de cibercriminales bien financiados y organizados que realizan ataques sofisticados, como APT (Amenazas Persistentes Avanzadas).
- **Hacktivistas:** Personas o grupos que realizan ataques para promover causas políticas o sociales.

Malware

- **Virus:** Programas que se replican y se propagan a través de archivos o sistemas, causando daño.
- **Troyanos:** Software malicioso que aparenta ser legítimo pero que permite a los atacantes tomar control del sistema.
- **Ransomware:** Software que cifra los archivos de un sistema y exige un rescate para liberarlos.
- **Spyware:** Programas diseñados para recopilar información del usuario sin su conocimiento.

Vulnerabilidades del Sistema

- **Software Desactualizado:** Programas que no han sido actualizados con los últimos parches de seguridad, lo que puede dejar expuestas vulnerabilidades conocidas.
- **Configuraciones Incorrectas:** Configuraciones inadecuadas de software o hardware que pueden ser explotadas por atacantes.
- **Fallos de Seguridad en Protocolos:** Deficiencias en los protocolos de comunicación que pueden ser aprovechadas para realizar ataques.

5.5. ANÁLISIS DE VULNERABILIDADES EXPLOTADAS

Considerando que el tráfico analizado proviene de un Proveedor de Servicios de Internet (ISP) que atiende exclusivamente a usuarios residenciales (Home) y que estos usuarios no exponen servicios, sino que únicamente consumen servicios de Internet, se pueden extraer las siguientes conclusiones. El análisis del tráfico revela que las aplicaciones más destacadas son SMTP (en los puertos TCP/25 y TCP/587) y SMB (en el puerto TCP/445). [16]

Application	# of Clients	Sessions	Bytes (Sent/Received)
tcp/587	10275	434,383	55.8 GB/1.0 GB
SMB	6687	3,972,018	1.2 GB/5.3 GB
tcp/5555	6481	5,222,384	992.3 MB/4.4 GB
TCP/587	3697	195,522	80.8 GB/508.0 MB
Google-Gmail	3438	302,270	7.3 GB/175.6 MB
Cloudflare-CDN	2962	136,798	758.0 MB/4.9 MB
SSH	2712	292,486	45.5 GB/134.0 GB
HTTPS	2179	14,786	27.4 MB/19.9 MB
Microsoft-Outbound_Email	1980	366,520	4.2 GB/174.0 MB
Amazon-AWS	1372	86,185	2.1 GB/609.2 MB
Apple-Outbound_Email	1241	16,496	4.7 GB/71.0 MB
Google-Outbound_Email	1192	39,313	758.3 MB/17.2 MB
SMTP	861	672,960,702	12.2 GB/10.6 MB
Akamai-CDN	819	19,775	1.1 GB/6.5 MB

Ilustración 11 Tabla de cantidad de usuarios, sesiones y tamaño de tráfico consumido por aplicación

Este patrón de tráfico es indicativo de las actividades comunes de los usuarios residenciales, quienes suelen interactuar principalmente con servicios de correo electrónico y de compartición de archivos. La prominencia de SMTP en el tráfico analizado sugiere una alta utilización de servicios de correo electrónico, mientras que la presencia significativa de SMB refleja el uso de protocolos de compartición de archivos y recursos en red.

En resumen, el tráfico predominante observado en los puertos SMTP y SMB es consistente con el comportamiento esperado de usuarios residenciales, quienes se enfocan en la utilización de servicios de comunicación y colaboración en línea.

Debido a esto existen vulnerabilidades que pudieron ser explotadas de varias maneras, pero las más relevantes se detallan a continuación:

Vulnerabilidades en el Sistema Operativo

- **Sistemas Operativos Desactualizados:** Los sistemas operativos que no se mantienen actualizados con los últimos parches de seguridad son susceptibles a vulnerabilidades conocidas. Los atacantes pueden aprovechar estas debilidades para obtener acceso no autorizado, tomar control total de la máquina o realizar otras actividades maliciosas. [9]

- **Fallas en la Configuración de Seguridad:** Las configuraciones de seguridad incorrectas o innecesarias, tales como el uso de cuentas con privilegios elevados sin justificación, pueden ser objetivos ideales para los atacantes. La falta de una configuración adecuada expone los sistemas a riesgos innecesarios, facilitando posibles intrusiones. [17]

Aplicaciones y Software Desactualizado

- **Aplicaciones Vulnerables:** Las aplicaciones y programas que no se actualizan regularmente pueden contener vulnerabilidades que los atacantes explotan para ejecutar código malicioso o comprometer el sistema. Las versiones obsoletas de software suelen tener fallos de seguridad que han sido corregidos en versiones más recientes.
- **Plug-ins y Extensiones Inseguras:** Las extensiones del navegador y los complementos de software que no se mantienen actualizados con frecuencia pueden ser vectores para malware o ataques. Los atacantes pueden aprovechar estos componentes desactualizados para infiltrarse en el sistema o realizar actividades no autorizadas.

Phishing e Ingeniería Social

- Correos Electrónicos de Phishing: Los ataques de phishing, a través de correos electrónicos fraudulentos, buscan engañar a los usuarios para que divulguen información confidencial o descarguen software malicioso. Estos correos electrónicos se diseñan para parecer legítimos y así obtener acceso a datos sensibles.
- Técnicas de Ingeniería Social: Los atacantes pueden emplear técnicas de ingeniería social para manipular a los usuarios, llevándolos a revelar información confidencial o a conceder acceso a sus sistemas y cuentas. Estas técnicas se basan en el engaño y la explotación de la confianza del usuario. [14]

CONCLUSIONES

El objetivo principal de esta investigación fue implementar un sistema que permita mostrar la postura de seguridad de un Proveedor de Servicios de Internet (ISP), utilizando tecnologías de código abierto para reportar a la alta gerencia sobre las amenazas relacionadas con el ecosistema. El desarrollo y despliegue del sistema han logrado cumplir este objetivo de manera efectiva, proporcionando herramientas esenciales para la toma de decisiones en materia de seguridad.

El sistema implementado ha integrado de manera exitosa diversas fuentes para analizar el tráfico que ingresa a la red del ISP, permitiendo la identificación y catalogación de tráfico malicioso. A través de este análisis, se ha desarrollado un dashboard que proporciona indicativos claros para la toma de decisiones. Este dashboard facilita la visualización de amenazas, permitiendo la intervención precisa, como el corte de ciertos canales o el parcheo de vulnerabilidades específicas. La capacidad de clasificar y gestionar el tráfico de manera eficaz es fundamental para mantener la integridad y seguridad de la infraestructura de red del ISP.

En relación con el primer objetivo específico, se ha llevado a cabo una evaluación exhaustiva de las amenazas que impactan a los usuarios finales de la red, utilizando fuentes de lista de reputación externas. Este análisis ha permitido detectar patrones y tipos de ataques en concordancia con la primera cadena del marco MITRE ATT&CK, así como identificar vulnerabilidades y tipos de ataques relevantes. Los resultados obtenidos reflejan un entendimiento profundo de las amenazas actuales y proporcionan una base sólida para la implementación de medidas de mitigación efectivas.

Para el segundo objetivo específico, se diseñaron e implementaron zonas de limpieza de tráfico para segmentar y controlar el flujo de datos en la red. Este diseño ha demostrado su funcionalidad en el entorno del ISP, permitiendo una gestión más eficiente del tráfico y una protección mejorada contra posibles amenazas. La segmentación y el control del flujo de datos son esenciales para limitar el impacto de ataques y para asegurar la eficiencia operativa de la red.

En cumplimiento con el tercer objetivo específico, se desarrolló un panel de control destinado a la alta dirección con el propósito de facilitar la toma de decisiones. Este panel proporciona una visión macro de la situación de seguridad del ISP, permitiendo a la alta dirección acceder a información clave de manera rápida y eficiente. La implementación del panel de control ha optimizado el proceso de toma de decisiones, ofreciendo una herramienta visual y analítica que mejora la capacidad de respuesta ante incidentes de seguridad.

El proyecto ha logrado implementar un sistema integral que mejora significativamente la postura de seguridad del ISP. La integración de tecnologías de código abierto, junto con la creación de un dashboard y un panel de control eficientes, ha permitido una gestión proactiva y reactiva de la seguridad. La evaluación de amenazas y la implementación de zonas de limpieza de tráfico refuerzan la capacidad del ISP para proteger su red y mantener la confianza de sus usuarios. Los resultados obtenidos demuestran la efectividad del sistema y su contribución a la mejora continua de las prácticas de seguridad en el entorno del ISP.

RECOMENDACIONES

A partir de los resultados obtenidos y el análisis realizado en el proyecto, se proponen las siguientes recomendaciones para fortalecer la postura de seguridad del ISP y mejorar la eficacia del sistema implementado:

Es crucial mantener el sistema operativo y el software actualizado para mitigar riesgos asociados con vulnerabilidades conocidas. Las actualizaciones periódicas y la aplicación de parches son fundamentales para proteger los sistemas contra nuevas amenazas y exploits. Además, se recomienda establecer un proceso automatizado para la gestión de actualizaciones y parches, minimizando el riesgo de exposición a vulnerabilidades.

Para mejorar la precisión y el alcance del análisis de tráfico, se recomienda ampliar la integración de fuentes de datos adicionales, como servicios de inteligencia de amenazas y listas de reputación más amplias. La incorporación de múltiples fuentes puede enriquecer el análisis y proporcionar una visión más completa de las amenazas emergentes y las tácticas utilizadas por los atacantes.

El dashboard y el panel de control desarrollados han demostrado ser herramientas efectivas para la toma de decisiones. Sin embargo, se recomienda realizar evaluaciones periódicas y obtener retroalimentación de los usuarios para optimizar estas herramientas. La incorporación de características adicionales, como alertas en tiempo real y capacidades avanzadas de análisis, puede mejorar la capacidad de respuesta y la eficiencia en la gestión de incidentes.

Desarrollar e implementar estrategias de respuesta a incidentes específicas basadas en las amenazas identificadas y las vulnerabilidades detectadas. Estas estrategias deben incluir procedimientos claros para la contención, erradicación y recuperación de incidentes, así como la formación continua del personal en las mejores prácticas de respuesta a incidentes.

Se recomienda llevar a cabo evaluaciones de seguridad periódicas, incluidas pruebas de penetración y auditorías de seguridad, para identificar nuevas vulnerabilidades y validar la eficacia de las medidas de seguridad existentes. Estas evaluaciones ayudarán a adaptar y mejorar continuamente las estrategias de seguridad en función de las amenazas y vulnerabilidades emergentes.

Es fundamental promover la conciencia y formación en seguridad entre todos los empleados del ISP. Programas de capacitación continua en temas de ciberseguridad, como phishing, ingeniería social y prácticas seguras en el uso de sistemas, pueden reducir el riesgo de errores humanos y mejorar la capacidad de respuesta ante incidentes.

Fomentar la colaboración con otras organizaciones y autoridades en el campo de la ciberseguridad. La cooperación y el intercambio de información sobre amenazas y vulnerabilidades con entidades externas pueden proporcionar valiosas perspectivas y recursos adicionales para mejorar la postura de seguridad del ISP.

Continuar evaluando y ajustando las zonas de limpieza de tráfico para asegurar que se mantengan efectivas frente a las amenazas. La segmentación adecuada del tráfico no solo ayuda

a controlar el flujo de datos, sino que también puede limitar el impacto de ataques y mejorar la capacidad de respuesta.

BIBLIOGRAFÍA

[1] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

[2] Zhou, Z., & Wang, D. (2018). A survey of intrusion detection systems. Journal of Computer Networks and Communications, 2018, 1-10. https://doi.org/10.1155/2018/3482564

[3] McMillan, R. (2019). The Rise of Next-Generation Firewalls. Computerworld. https://www.computerworld.com/article/3277304/the-rise-of-next-generation-firewalls.html

[4] Cole, E., & Ring, S. (2019). Advanced Persistent Threats: How to Defend Against Them. Information Security Journal: A Global Perspective, 28(2), 63-73. https://doi.org/10.1080/19393555.2019.1567483

[5] Karasek, R., & Kolb, D. (2020). Evaluating Security Posture: Metrics and Measurements. Information Systems Research, 31(1), 100-115. https://doi.org/10.1287/isre.2019.0905

[6] Zhang, K., & Wang, J. (2016). Incident Response and Management. Computer Communications, 79, 86-98. https://doi.org/10.1016/j.comcom.2016.01.014

[7] Forcht, K. A. (2017). Cybersecurity Risk Management. Journal of Strategic and International Studies, 13(1), 45-56. https://www.jstor.org/stable/26474836

[8] Stallings, W. (2017). Computer Security: Principles and Practice (4th ed.). Pearson.

[9] Case, A., & Kark, S. (2015). DDoS Protection: A Practical Guide. SANS Institute. https://www.sans.org/white-papers/37135/

[10] Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals. Syngress.

[11] Chou, D. (2015). Next-Generation Security Operations Centers. Journal of Cybersecurity, 2(4), 22-29. https://doi.org/10.1093/cysec/tgw026

[12] Tan, Y., & Dinev, T. (2017). Mitigating DDoS Attacks. Network Security, 2017(9), 10-13. https://doi.org/10.1016/j.netsec.2017.07.002

[13] Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (7th ed.). Cengage Learning.

[14] Gollmann, D. (2011). Computer Security. Wiley.

[15] Hall, B., & D'Antonio, T. (2018). Managing Security in Information Technology. CRC Press.

[16] Bianco, A. (2014). The Role of Security Operations Centers in Modern Security Strategies. Journal of Information Security, 5(3), 183-197. https://doi.org/10.4236/jis.2014.53020

[17] Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Pearson.

[18] Carna, C. M., & Anderson, J. (2020). JA3 Fingerprinting for TLS/SSL Traffic. Information Security Journal: A Global Perspective, 29(2), 100-110. https://doi.org/10.1080/19393555.2020.1720294

[19] Anderson, J., & Carna, C. M. (2020). JA3: Identifying Malicious Activity in TLS/SSL Traffic. Computer Security, 95, 101848. https://doi.org/10.1016/j.cose.2020.101848

ANEXO

A. Archivo de configuración para el filtrado y parsing de logstatsh con los eventos del scrubbing center.

```
input {
   udp {
     port => 9200
     type => "forti_log"
     tags => ["fortigate-valle-adachi"]
  }
}


filter {
if [type] == "forti_log" {
        grok {
                match => ["message",
"%{SYSLOG5424PRI:syslog_index}%{GREEDYDATA:message}"]
                overwrite => [ "message" ]
                tag_on_failure => [ "forti_grok_failure" ]
              }
        kv {
    source => "message"
    value_split => "="
    field_split => " "
}
```

```
    mutate {
    add_field => { "temp_time" => "%{date} %{time}" }
    rename => { "type" => "ftg_type" }
    rename => { "subtype" => "ftg_subtype" }
    add_field => { "type" => "forti_log" }
    convert => { "rcvdbyte" => "integer" }
    convert => { "sentbyte" => "integer" }
}
date {
    match => [ "temp_time", "yyyy-MM-dd HH:mm:ss" ]
    timezone => "America/Bogota"
    target => "@timestamp"
    }
    mutate {
    remove_field                                                                    =>
["syslog_index","syslog5424_pri","path","temp_time","service","date","time","sentpkt","rcvdpkt","l
og_id","message","poluuid"]
}
}
}
output {
if [type] == "forti_log" {
elasticsearch {
hosts => "localhost:9200"
        ssl => true
        ssl_certificate_verification => false
        user => "usuario"
```

```
        password => "password"
http_compression => "true"
index => "forti-scrubbing"
}
}
}
```