NOMBRE DEL TRABAJO

DISEÑO E IMPLEMENTACIÓN DE UN CA SO DE USO MEDIANTE UN SIEM PARA M EJORAR LA CIBERSEGURIDAD DE UNA E NT

AUTOR

RENZO JOEL GASPAR HUAMANI

RECUENTO DE PALABRAS

18877 Words

RECUENTO DE CARACTERES

103464 Characters

RECUENTO DE PÁGINAS

109 Pages

TAMAÑO DEL ARCHIVO

4.8MB

FECHA DE ENTREGA

Apr 17, 2024 9:50 PM GMT-5

FECHA DEL INFORME

Apr 17, 2024 9:52 PM GMT-5

5% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 5% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45° de la ley N° 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (x)

DATOS PERSONALES

Apellidos y Nombres: GASPAR HUAMANI, RENZO JOEL
D.N.I.: 70243269
Otro Documento:
Nacionalidad: PERUANA
Teléfono: 922598449
e-mail: renzojoel_97@hotmail.com

DATOS ACADÉMICOS

Pregrado

Facultad: FACULTAD DE INGENIERÍA Y GESTIÓN
Programa Académico: TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado: INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Postgrado

Universidad de Procedencia:
País:
Grado Académico otorgado:

Datos de trabajo de investigación

Título: " DISEÑO E IMPLEMENTACIÓN DE UNA CASO DE USO MEDIANTE UN SIEM PARA MEJORAR LA CIBERSEGURIDAD DE UNA ENTIDAD FINANCIERA "
Fecha de Sustentación: 17 DE DICIEMBRE DE 2023
Calificación: APROBADO POR UNANIMIDAD
Año de Publicación: 2024

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo X No autorizo _____

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	(X)

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	( )
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

Motivos de la elección del acceso restringido:

Gaspar Huamani Renzo Joel

APELLIDOS Y NOMBRES

70243269

DNI

Firma y huella:

Lima, 04 de Junio del 2024

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

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

“DISEÑO E IMPLEMENTACIÓN DE UN CASO DE USO MEDIANTE UN SIEM PARA MEJORAR LA CIBERSEGURIDAD DE UNA ENTIDAD FINANCIERA”

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

GASPAR HUAMANI, RENZO JOEL
ORCID: 0009-0002-5960-0660

ASESOR
MORÁN MONTOYA ENRIQUE MANUEL
ORCID: 0009-0005-2964-746X

Villa El Salvador
2023

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

"Año de la unidad, la paz y el desarrollo"

VI Programa de Titulación por la Modalidad de Trabajo de SuficienciaProfesional
Decanato de la Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 15:08 horas del día 17 de diciembre de 2023, se reunieron en las instalaciones de la Universidad Nacional Tecnológica de Lima Sur, los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	:	DR. MARK DONNY CLEMENTE ARENAS	CIP Nº 181400
Secretario	:	MG. LUDWIG PASCUAL LÓPEZ HUAMAN	CIP Nº 310375
Vocal	:	MG. MARTHA ROXANA QUISPE AYALA	CIP Nº 124612

Designados con Resolución de Decanato de la Facultad de Ingeniería y Gestión N° 984-2023-UNTELS-R-D de fecha 13 de diciembre del 2023.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de **Ingeniero Electrónico y Telecomunicaciones**, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional (Resolución de Consejo Universitario Nº 065-2023-UNTELS-CU de fecha 08 de agosto del 2023), en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur" ; siendo que el Art. 4º del precitado Reglamento establece que:**"La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo deSuficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otrasmodalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar un mínimo de dos (02) años de experiencia laboral, de acuerdo a lo establecido en la Resolución Nº 174-2019- SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)…"**, en el cual;

El Bachiller **RENZO JOEL GASPAR HUAMANI**
Sustentó su Trabajo de Suficiencia Profesional: **DISEÑO E IMPLEMENTACIÓN DE UN CASO DE USO MEDIANTE UN SIEM PARA MEJORAR LA CIBERSEGURIDAD DE UNA ENTIDAD FINANCIERA**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición Aprobado por unanimidad Equivalencia Bueno de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las ..... horas del día 17 de diciembre de 2023 se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado.

PRESIDENTE
DR. MARK DONNY CLEMENTE ARENAS
CIP N° 181400

SECRETARIO
MG. LUDWIG PASCUAL LÓPEZ HUAMAN
CIP N° 310375

VOCAL
MG. MARTHA ROXANA QUISPE AYALA
CIP N° 124612

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia delpresidente del jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del jurado, la sustentación será reprogramada durante los 05 días siguientes.

DEDICATORIA

Expresar mi profundo agradecimiento a mi hermana Edith por su invaluable ayuda y correcciones en el proceso de la realización de este trabajo.

Mi gratitud hacia mis padres, quienes han sido mi mayor fuente de aliento y apoyo incondicional a lo largo de toda mi carrera profesional, guiándome hasta su culminación.

AGRADECIMIENTO

Agradezco al magister Enrique Morán por las recomendaciones brindadas durante las asesorías.

ÍNDICE

LISTADO DE FIGURAS

Listado de Tablas

RESUMEN

El presente trabajo de suficiencia profesional tuvo como finalidad diseñar e implementar el caso de uso fuerza bruta a cuenta VPN Citrix utilizando la plataforma SIEM RSA para proteger la confidencialidad, integridad y disponibilidad de la información de una Entidad Financiera, de esa manera, mitigar los riesgos ante posibles ataques cibernéticos. El diseño y la implementación del caso de uso se realizó en 4 etapas: diseño, configuración, validación y pase a producción.

La efectividad del funcionamiento del caso de uso implementado se demostró a través de la validación a la cual se sometió en un periodo de 6 semanas dando como resultado la activación de 16 alertas del caso de uso fuerza bruta a cuenta VPN Citrix en la plataforma SIEM RSA cumpliendo con las condiciones de la lógica que fueron establecidas en la etapa del diseño. También, la implementación exitosa del caso de uso ha facilitado la detección oportuna y respuesta eficiente ante amenazas de posibles ataques de fuerza bruta a cuentas de usuarios que utilizan VPN Citrix NetScaler para conectarse de manera remota hacia la Entidad Financiera.

Palabras claves: SIEM RSA, fuerza bruta, caso de uso

INTRODUCCIÓN

En la actualidad, las empresas buscan proteger la integridad, disponibilidad y confidencialidad de la información de las amenazas y vulnerabilidades externas, ya que constantemente están siendo atacados por los ciberdelincuentes que intentan robar su información confidencial y la de sus clientes. Estos ataques suelen aprovechar posibles fallas en las soluciones de seguridad, lo que puede resultar en considerables pérdidas económicas.

Por este motivo muchas empresas optan por implementar un SIEM o sistema de gestión de eventos e información de seguridad que les permitirá recolectar logs desde diferentes dispositivos de seguridad como firewall, antivirus, IPS, antispam, proxy, VPN entre otros y centralizar la información para luego realizar un análisis exhaustivo, correlacionando eventos en tiempo real mediante la creación de reglas o también denominados casos de uso con el propósito de buscar tendencias y patrones de comportamiento anómalo, facilitando así la identificación de eventos inusuales de aquellos que son comunes permitiendo prevenir, anticipar posibles amenazas y vulnerabilidades. También, emitiendo alertas oportunas para que se tomen acciones respectivas con la finalidad de ayudar a proteger los datos y reputación de la organización.

La Entidad Financiera solicitó la creación de un caso de uso proveniente del dispositivo VPN Citrix NetScaler. Esta medida se basa en la preocupación de que, si un atacante cibernético logra infectar y tomar el control de la computadora de un trabajador que se conecta remotamente a través de VPN a la red de la Entidad Financiera, podría intentar obtener las credenciales de la VPN utilizando software especializado. Este intento buscaría facilitar el acceso a la red de la Entidad Financiera con el objetivo de robar información confidencial.

El presente trabajo está estructurado de la siguiente manera:

El primer capítulo aborda los aspectos generales que contiene contexto, delimitación temporal y espacial del trabajo, así como los objetivos.

En el segundo capítulo se desarrolla el marco teórico que abarca antecedentes nacionales e internacionales, bases teóricas y definición de términos básicos.

En el tercer capítulo se describe el desarrollo del trabajo profesional que incluye la determinación y análisis del problema, el Modelo de solución propuesto que fue elaborado en 4 etapas.

Finalmente, se presenta los resultados, conclusiones, recomendaciones, referencias bibliográficas y Anexos.

CAPÍTULO I: ASPECTOS GENERALES

1.1. Contexto

1.1.1. Descripción de la actividad de la institución

SECURESOFT CORP S.A.C es una corporación regional especializada en ciberseguridad con presencia en Perú, Colombia y Ecuador que opera desde el 2004, se encuentra enfocada en brindar soluciones y consultorías a las empresas más importantes de los 3 países.

Además, cuenta con 3 Centro de Operaciones de Ciberseguridad (CyberSOC) ubicados en Lima-Perú, Quito-Ecuador, Bogotá-Colombia que son centros de monitoreo altamente especializados, tanto en su infraestructura como en los profesionales que lo dirigen. Este proyecto nació con el fin de responder a una necesidad del mercado contra las amenazas de ciberseguridad brindando un servicio 24x7, ayudando a las organizaciones a consolidar su transformación desde una postura tradicional reactiva a una postura proactiva que permita anticiparse a los ataques y reducir rápidamente los impactos que podrían generarse y de esa manera proteger sus datos y reputación (SecureSoft, 2023).

1.1.2. Misión

Apoyar a los clientes en su proceso de transformación digital mediante la oferta de productos y servicios en el ámbito de la ciberseguridad. Esto se llevará a cabo mediante una sólida base de consultoría, transparencia e innovación, con el compromiso de asegurar ingresos sostenibles y rentables para los accionistas y preocupándonos por el crecimiento y desarrollo profesional del personal (SecureSoft, 2023).

1.1.3. Visión

Ser líder de Ciberseguridad en Latinoamérica para el año 2025 (SecureSoft, 2023).

1.2. Delimitación temporal y espacial del trabajo

1.2.1. Delimitación temporal del trabajo

El periodo de duración de la actividad fue desde el 1 de mayo hasta 25 de mayo del 2023, el diseño e implementación contará con un cronograma de actividades donde se detallará cronológicamente, ver anexo 1.

1.2.2. Delimitación espacial del trabajo

El trabajo se realizó para una Entidad Financiera ubicado en Huancayo-Perú, pero el diseño y la implementación se realizó de manera remota desde las instalaciones de la empresa SecureSoft ubicada en distrito de surco en el área de ciberinteligencia.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

- Diseñar e Implementar un caso de uso utilizando un SIEM para proteger la confidencialidad, integridad y disponibilidad de la información de una Entidad Financiera con el fin de mitigar los riesgos ante posibles ataques cibernéticos.

1.3.2. OBJETIVOS ESPECÍFICOS

- Diseñar el caso de uso fuerza bruta a cuenta VPN Citrix para detectar y alertar a tiempo intentos de ataques de fuerza bruta hacia un usuario que tiene una cuenta de VPN Citrix.
- Implementar el caso de uso fuerza bruta a cuenta VPN Citrix para proteger los activos de la Entidad Financiera a través de la tecnología SIEM RSA.
- Validar el correcto funcionamiento del caso de uso de fuerza bruta a cuenta VPN Citrix

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

2.1.1 Antecedentes internacionales

Agudelo et al. (2022) realizaron una investigación cuyo propósito fue la creación de cinco casos de usos orientados a la mejora de ciberseguridad en el sector financiero con las plataformas SIEM que se utiliza en la empresa Securesoft. Para ello, se identificó las vulnerabilidades más frecuentes en el sector financiero que han sido reportadas por varias entidades financieras, de las cuales, se concentró en solucionar cinco problemas con mayor recurrencia en entidades financieras que dependan de sistemas informáticos que puedan ser vulnerados por ciberdelincuentes. Una vez definidos y limitados los requisitos para cada caso de uso se procedió a estructurar el flujo que se necesita para la implementación de cada uno. Asimismo, crear modelos de plantillas donde se describan el objetivo, alcance, fuentes de eventos, tipos de datos, flujo lógico, notificación, severidad y recomendaciones para abordar las amenazas y vulnerabilidades en el sector financiero.

En dicha investigación se llegó a las siguientes conclusiones: Una definición precisa de un caso de uso implica la creación de procedimientos de gestión de incidentes de ciberseguridad con el objetivo de reducir, eliminar y prevenir dichas situaciones. También, destaca el uso e implementación de un firewall a fin de mitigar de raíz las posibles amenazas de malware que vulneran la seguridad de las empresas, el cual considera como una opción viable para la protección de datos. Finalmente compara el uso de SIEM con UEBA donde el primer sistema engloba la gestión de eventos, patrones y tendencias que activan alarmas cuando detectan algo inusual mientras que UEBA opera de manera similar, pero se centra en los eventos inusuales basados en el comportamiento de los usuarios y el aprendizaje automático, la unión de estas dos tecnologías se considera en la actualidad como una de las mejores prácticas en ciberseguridad.

La investigación se asemeja a mi trabajo en que definen casos de uso basándose en el top de amenazas que afectan a las entidades financieras atacados por ciberdelincuentes y se diferencia en que los autores solo crean plantillas de 5 casos

de uso en el cual indican el flujo de la implementación de los casos de uso de manera general pero no realizan las configuraciones de dichos casos de uso como si se hará en este trabajo.

Sánchez (2019) en su tesis para optar título de magister: *"Implantación de Qradar en un entorno genérico multi-cliente para SOC"* implementó un SIEM QRadar para cada cliente que posteriormente gestionara el SOC con el fin de mejorar la capacidad de detección y respuesta a amenazas cibernéticas.

En dicha investigación se llegó a las siguientes conclusiones: se logró implementar el SIEM QRadar en cada uno de los clientes, adaptando las configuraciones de cada instalación según lo planificado y dentro del plazo previsto. Además, se adquirió nuevos conocimientos técnicos en el campo de la seguridad, así como habilidades generales como empatía, trabajo en equipo y liderazgo.

La relación que guarda con mi trabajo es que se implementa un SIEM en una entidad con la finalidad de mejorar la capacidad de detección y respuesta ante una posible amenaza o un ataque de ciberdelincuentes que quieran robar información.

Quintero y Tovar (2019) en el artículo *"Sistemas de Gestión de Información y Eventos de Seguridad (SIEM)"* menciona la importancia de que las empresas cuenten con un SIEM para que puedan proteger su infraestructura tecnológica ante posibles amenazas cibernéticas también da a conocer los diferentes SIEM que existen en la actualidad, sus funcionalidades, eficiencia y los aspectos que deben ser considerados al implementar un sistema de gestión de eventos y seguridad de la información (SIEM); Finalmente concluye que el SIEM no debe considerarse como una solución definitiva para eliminar problemas de seguridad, sino como un estímulo para iniciar procesos que los solucionen que pueden incluir la automatización, la intervención de administradores de los recursos o equipos de respuesta a incidentes para mejorar y optimizar los recursos tecnológicos.

La relación con mi trabajo es que nos indica la importancia de que las empresas cuenten con SIEM para que protejan su infraestructura antes posibles ataques cibernéticos, esto debido a que el SIEM centraliza todas las tecnologías de seguridad que pueda tener una entidad en una sola, y partir de ello pueda correlacionar, buscar amenazas y alertar mediante casos de uso cuando suceda

un ataque o un fallo en su seguridad para que puedan mitigarlo en el menor tiempo posible.

2.1.2 Antecedentes nacionales

Estela (2020) en su tesis de pregrado *"Implementación de un Security Information and Event Management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera"* propuso Implementar un Sistema de gestión de eventos y seguridad de la información (SIEM) con el propósito de identificar vulnerabilidades y amenazas que se encuentran expuestos en los sistemas informáticos y redes de una institución financiera. Para realizar la implementación utilizó programas de gestión de proyectos como Scrum, PMBOK y la guía de IBM para así disminuir las probabilidades de falla, su metodología compendió de 5 etapas: inicio, planificación, implementación, monitoreo y cierre del proyecto. Concluyendo que el empleo de la plataforma SIEM junto con controles de endpoints, redes y checkers, pueden mitigar los riesgos de forma más eficaz y evitar pérdidas económicas y de información. También, que el SIEM QRadar es una herramienta importante y eficaz que garantiza la disponibilidad y confidencialidad de los diferentes activos de la información ante un posible ataque cibernético. Finalmente, la entidad financiera que utilizó este sistema de monitoreo obtuvo resultados favorables.

La relación que guarda con mi trabajo es que ambas entidades financieras buscan protegerse de ataques informáticos con la finalidad de salvaguardar su información confidencial mediante el uso del SIEM, la diferencia seria que yo usé el SIEM RSA para crear un caso de uso y Estela utilizo el SIEM QRadar.

López (2019) en su tesis "*Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú"* propuso implementar un sistema que posibilite la integración de información relevante procedente de las herramientas de seguridad con el propósito de emitir alertas en tiempo real para detectar y mitigar cualquier tipo de amenaza que pueda infiltrarse en la red institucional naval puesto que anteriormente se monitoreaba independientemente cada herramienta el cual les dificultaba a la hora de detectar una posible amenaza

debido a que contaban con distintas soluciones de seguridad (firewall, Antivirus, IPS, Anti-Malware, etc).

Para llegar a su objetivo utilizó una serie de pasos como: Recopilación de datos, creación de informes, colaboración en equipo, diseño de gráficos de planificación temporal como el diagrama Gantt y ejecución de actividades programadas.

En dicha investigación se llegó a las siguientes conclusiones: el sistema de gestión de eventos y seguridad de la información (SIEM) es confiable ya que permite la visualización del flujo de la información de los intentos de ataques, permitiendo al analista de seguridad tomar acciones apropiadas para abordar cada tipo de amenaza usando casos de uso ya definidos, también se logró reducir en un 52% la cantidad de eventos en comparación con el monitoreo independiente de eventos a través de sensores de seguridad .Asimismo, se logró disminuir en un 13% en la detección de eventos clasificados como falsos positivos, permitiendo una mejora significativa en la eficiencia de los analistas de seguridad que monitoreaban el SIEM.

El trabajo de investigación del autor tiene relación con mi trabajo debido a que los SIEM indistintamente del fabricante son soluciones de seguridad que te ayudan a detectar, analizar, correlacionar eventos de seguridad y de acuerdo con la lógica del caso de uso activarse alertas en tiempo real para tomar las medidas correspondientes frente a un posible ataque informático.

Vasquez (2023) en su tesis "*Implementación de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera*" implementó un servicio de centro de operaciones de ciberseguridad (CyberSOC) utilizando herramientas de código abierto para una institución financiera que permitiría monitorear, detectar, analizar, prevenir y hacer seguimiento a eventos e incidentes de ciberseguridad en todos los dispositivos que cuenta la entidad financiera mediante el uso de herramientas tecnológicas, de esta manera se buscó disminuir las vulnerabilidades cibernéticas existentes en la red a las que están expuestas

Las conclusiones que obtuvo son las siguientes: Se logró implementar el servicio de CyberSOC en el tiempo establecido, se adquirió resultados favorables posterior

a la implementación, se crearon nuevos procedimientos para tratar un incidente de seguridad, informes de inteligencia sobre vulnerabilidades, análisis forense, monitoreo de vulnerabilidades tanto para cliente como para la entidad financiera. Finalmente, fomentó que las pequeñas empresas se inclinen hacia la inversión en plataformas de código abierto para elevar su nivel de madurez en ciberseguridad, lo que a su vez disminuiría las posibilidades de sufrir impactos en su negocio, como pérdidas económicas o daños a la reputación, entre otros.

La similitud con mi trabajo seria que ambos buscamos proteger los activos de la Entidad Financiera mediante un SIEM, la diferencia es que el autor implemento el servicio CyberSOC ya que la entidad financiera no contaba con ese servicio, mientras que, en mi caso, la Entidad Financiera ya contaba con el servicio de CyberSOC y también ya tenía implementado el SIEM.

2.2. Bases Teóricas

2.2.3. SIEM

Williams y Nicolett (2005) definieron el término SIEM como la tecnología que gestiona eventos en tiempo real y realiza un análisis histórico de los datos de seguridad que provienen de diferentes fuentes.

De la misma manera, los autores mencionados afirman que SIEM es la unión de dos tecnologías de seguridad que se complementan, pero cumplen diferentes funciones. A continuación, se describe las funciones de cada sistema:

- SIM: El Sistema de Gestión de Información de Seguridad recepciona, almacena todos los logs enviados de las diferentes fuentes de seguridad informática y los centraliza para analizar, interpretar datos históricos generando informes que brindan información valiosa el cual permitiría evaluarla y tomar mejores decisiones (Williams y Nicolett, 2005).
- SEM: El sistema de Gestión de eventos de Seguridad detecta, analiza patrones anormales y monitorea en tiempo real eventos de seguridad mediante logs enviados desde diferentes dispositivos de seguridad informática (firewall, IPS, EDR, antispam, etc), los correlaciona y es capaz de alertar, aunque solo de patrones predefinidos (Williams y Nicolett, 2005).

Por otro lado, según International Business Machines (IBM, s.f) definen al SIEM como una solución de seguridad que facilita a las organizaciones el reconocimiento inmediato de posibles amenazas y vulneraciones a la seguridad de las operaciones comerciales a fin de prevenir y conservar la información confidencial de las empresas.

El sistema SIEM recopila logs de diferentes fuentes y centraliza la información en una base de datos, donde realiza un análisis exhaustivo correlacionando eventos en tiempo real con el propósito de buscar tendencias y patrones de comportamiento anómalo, facilitando así la identificación de eventos inusuales de aquellos que son comunes garantizando una respuesta rápida y efectiva cuando suceda un ataque informático (Montesino et al, 2012).

Entonces se puede entender que el SIEM es un sistema de gestión de eventos de seguridad que recopila, analiza, correlaciona eventos e incidentes de seguridad provenientes de diversas fuentes de seguridad informática (IPS, Firewall, Antispam, Antivirus, EDR, etc) permitiendo prevenir, anticipar posibles amenazas cibernéticas al identificar patrones anómalos en tiempo real emitiendo alertas para que se tomen acciones respectivas en la cual ayuden a proteger los datos y reputación de la organización (Anumol, 2015).

2.2.4. Características del SIEM

Las características principales de un SIEM (sistema de gestión de eventos e información de seguridad) son las siguientes:

a) Capacidad para distinguir amenazas cibernéticas reales y no reales.
b) Almacenamiento de registros de eventos durante períodos prolongados.
c) Los registros se almacenan de manera segura en un concentrador para su posterior análisis.
d) Recopila registros de múltiples fuentes.
e) Análisis en tiempo real de eventos para detectar anomalías y amenazas potenciales.
f) Capacidad de generar alertas propias cuando hay indicios de posibles ciberataques o amenazas (Miller et al, 2010).

2.2.5 Estructura de SIEM

El SIEM es un sistema que generalmente está compuesto por 4 capas y 6 componentes, cada componente desempeña una tarea particular y puede funcionar independientemente; sin embargo, es crucial que todos operen de manera adecuada en conjunto, ya que, si alguno de ellos presenta fallos, el SIEM no funcionará correctamente (Miller et al, 2010).

Como se visualiza en la Figura 2 está compuesto por dispositivo fuente, colector de log, parseo/normalización de registros, motor de reglas/correlación, almacenamiento de registros y monitoreo.

2.2.5.1 Capas de SIEM

En la Figura 1 Capas del SIEM se observa que el sistema de gestión de eventos e información seguridad está compuesto por 4 capas, el número asignado a cada capa establece la secuencia en la que se configuran. Una vez completada la implementación del SIEM, estará listo para su uso.

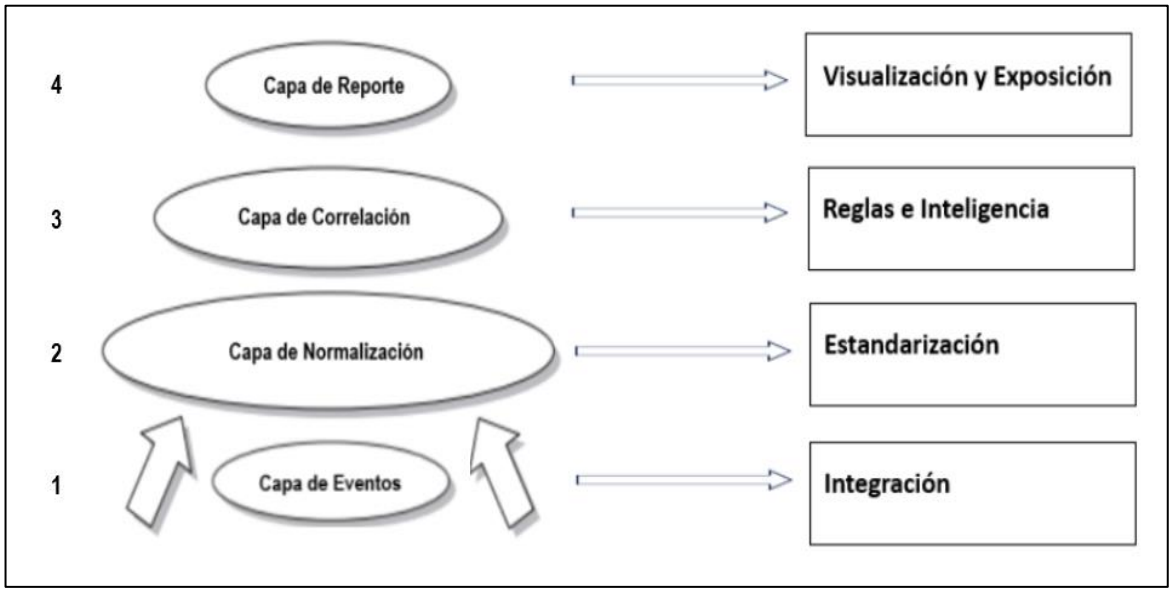


Figura 1. Capas del SIEM
Fuente: Miller et al (2010)

2.2.5.2 Componentes del SIEM

A continuación, se describe los 6 componentes que presenta el SIEM según la propuesta de Miller et al. (2010):

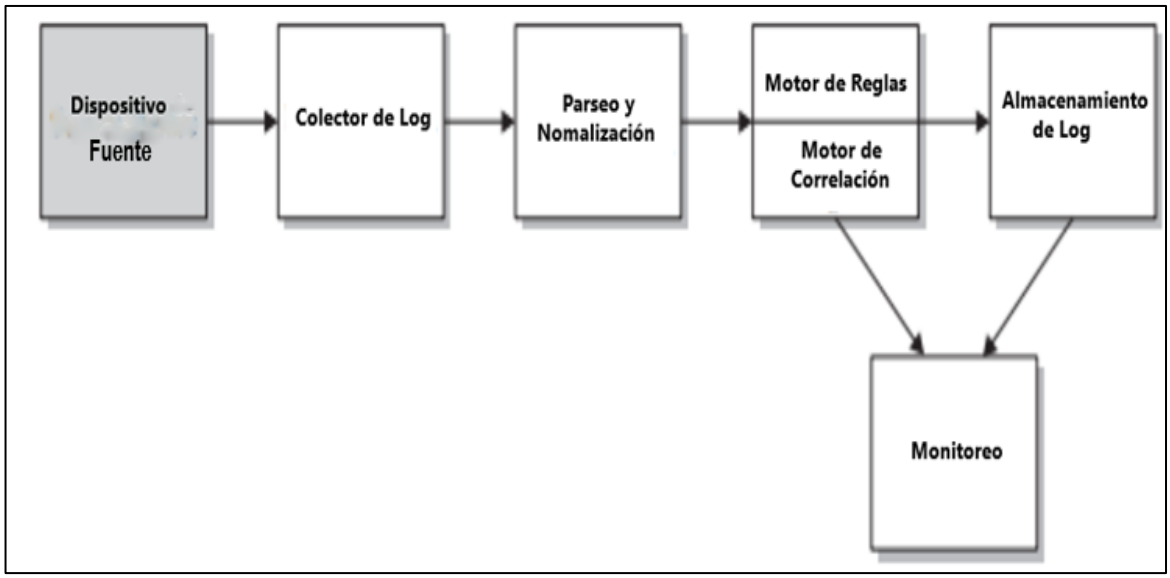


Figura 2. Componentes básicos de un SIEM
Fuente: Elaboración propia basada en Miller et al. (2010)

1. Dispositivo fuente

En la Figura 2 se observa que el dispositivo fuente es el primer elemento que alimenta de información al SIEM y pertenece a la primera capa.

Un dispositivo fuente puede ser un dispositivo de red, servidores, dispositivos de seguridad perimetral entre otros que generan logs y que se necesitan procesar en el SIEM. Cabe recalcar que, el dispositivo fuente no forma parte de los componentes de un SIEM, sin embargo, se tiene en cuenta ya que constituye la fuente primaria que alimenta con información a los demás componentes para su posterior procesamiento de logs.

2. Colector de Logs

Este componente también forma parte de la primera capa de captura de eventos y se encarga de recopilar logs o registros que provienen de múltiples dispositivos fuente hacia el SIEM, como se observa en la Figura 3.

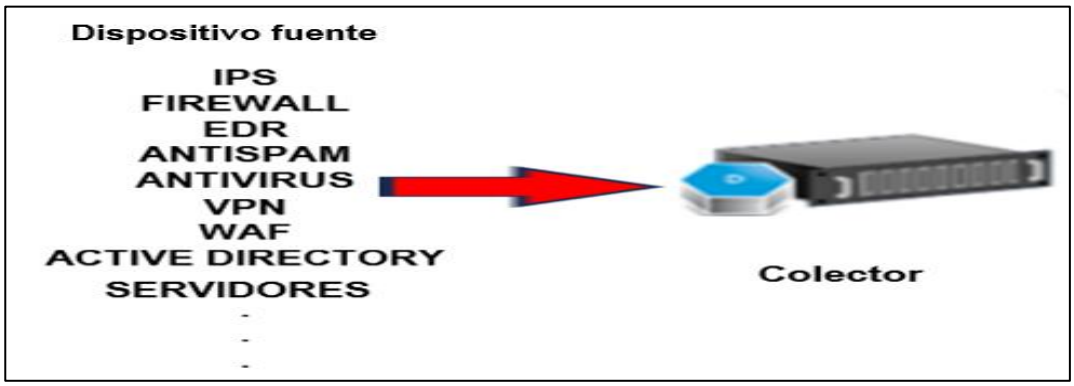


Figura 3. Recepción de logs de múltiples dispositivos fuente

Fuente: Elaboración propia

3. Parseo/normalización

La normalización o también denominado parseo se refiere a que los logs o registros provenientes de múltiples dispositivos enviados en diferentes formatos como CEF, LEF, Syslog y JSON deben estar en un formato estándar para que el SIEM lo pueda comprender y la información pueda ser procesada sin ningún problema, este componente pertenece a la segunda capa denominada normalización.

En la Figura 4 se observa una porción de log o registro en crudo enviado por la plataforma Check Point, este log está en formato CEF.

```
CEF:0|Check Point|VPN-1 & FireWall-1|Check Point|Decrypt|domain-udp|Unknown|act=Decrypt cs2Label=Pe
dhost=sscorppead02@securesoftcorp.com duser=jsusanibar@securesoftcorp.com  rt=1696257752000 shost=1
 cs2Label=Rule Name cs2=Servicio de AD para toda la Red VPN Cliente cs2=Acceso a nivel de Aplicacio
layer_uuid=2f248528-ce47-43f8-a9d2-8ba397d296e8 layer_uuid=fa418c2b-bdb4-47f2-9f72-2b3fc5d530b2 mat
rule_action=Accept rule_uid=f126a956-8b7f-4836-a36a-c6762eb1819c rule_uid=b9862a6f-f054-432a-85a1-6
{0x6b6601fd,0x7f097bf6,0x7052cab5,0xc6e1270f} origin=192.168.99.233 originsicname=CN\=SSPEFW,O\=SSP
fw_subproduct=VPN-1 hll_key=15150748115690241273 inzone=External lastupdatetime=1696257752 methods:
scheme:=IKE service_id=domain-udp session_uid={651AC787-0000-0000-C0A8-63E90A440000} src=172.16.250
log_link=https://192.168.99.232/smartview/#external-nav%3DOpenLogCard&domain-id%3D41e821a0-3720-11e
%3DbWFya2VyPUBBQEBCQDE2OTYyMjI4MDBAQ0A0MTEzMDY4Jm9yaWdfbG9nX3NlcnZlcl9pZD0wMDAwMDAwNS0wMDJkLTAwNGEt
```

Figura 4. Log crudo en formato CEF
Fuente: Elaboración propia

En la Figura 5 se observa el proceso de parseo del campo “user.src” para el SIEM RSA, el cual se conoce como “meta key”, es importante destacar que, este valor asignado no cambia mientras que, el “meta value” conformado por bferandez es un valor que puede cambiar. Cabe mencionar que, los campos de los “meta key” deben estar completos para generar las condiciones necesarias en el diseño de un caso de uso.

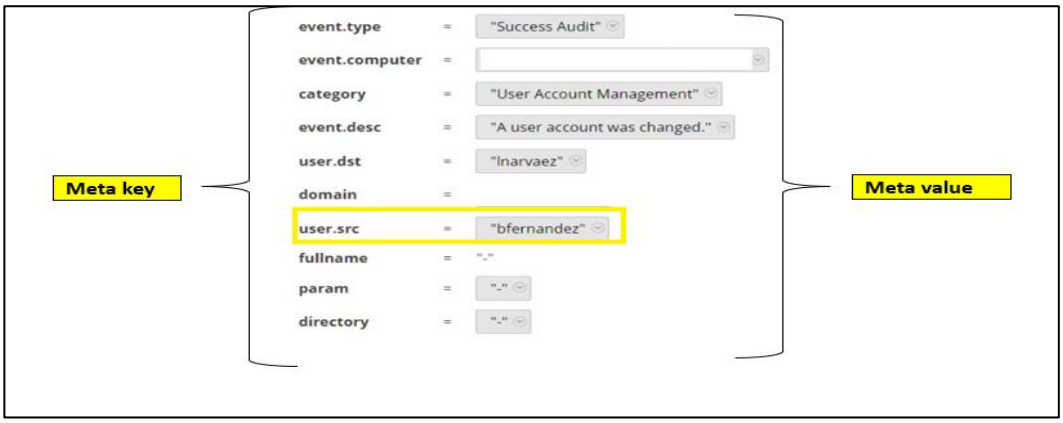


Figura 5. Campos parseados de un log
Fuente: Elaboración propia

4. Motor de reglas/motor de correlación

Este componente pertenece a la capa de correlación que se refiere al proceso de analizar y relacionar múltiples eventos o registros de datos provenientes de los diferentes dispositivos de origen para identificar patrones, tendencias o anomalías que puedan indicar posibles amenazas o incidentes de seguridad, es decir, busca detectar conexiones significativas entre eventos que, individualmente, podrían no parecer sospechosos, pero que cuando se analizan juntos pueden indicar una amenaza en curso**.** A continuación, se muestra la Tabla 1 que corresponde a los Eventos de un SIEM.

Tabla 1
Eventos de un SIEM

Tiempo	N° de evento	IP origen	IP destino	Evento
10:10:01	1035	192.168.1.200	10.10.10.25	Error al iniciar sesión en el servidor
10:10:02	1036	192.168.1.90	10.10.10.21	Inicio de sesión exitoso en el servidor
10:10:03	1037	192.168.1.200	10.10.10.25	Error al iniciar sesión en el servidor
10:10:04	1038	192.168.1.91	10.10.10.35	Error al iniciar sesión en el servidor
10:10:05	1039	192.168.1.10	10.10.10.2	Inicio de sesión exitoso en el servidor
10:10:06	1040	192.168.1.10	10.10.10.3	Inicio de sesión exitoso en el servidor
10:10:07	1041	192.168.1.200	10.10.10.25	Error al iniciar sesión en el servidor
10:10:08	1042	10.10.10.54	192.168.1.201	Error al iniciar sesión en el servidor
10:10:09	1043	10.10.10.34	192.168.1.10	Error al iniciar sesión en el servidor
10:10:10	1045	192.168.1.200	10.10.10.25	Inicio de sesión exitoso en el servidor

Fuente: Elaboración propia basado en Miller et al. (2010)

En la Tabla 1, se observa que en un periodo de 10 segundos hay 10 eventos de los cuales hay 4 eventos donde la IP 192.168.1.200 realiza tres intentos fallidos de inicio de sesión y un inicio de sesión exitoso hacia la IP 10.10.10.25, este comportamiento inusual probablemente podría ser de un intento de fuerza bruta contra el servidor de destino con IP 10.10.10.25.

Ahora, imaginemos que tenemos 1000 eventos en 10 segundos esto dificultará, ya que hay eventos relevantes e irrelevantes para ello es necesario filtrar la información y rastrear solo los eventos que puedan indicar un comportamiento malicioso en este caso de intentos de sesión satisfactorio e intentos de sesión fallida desde IP 192.168.1.200 hacia la IP 10.10.10.25.

Entonces, el motor de correlación en un SIEM se encarga de agrupar eventos individuales que forman parte de comportamientos maliciosos en un solo evento correlacionado que se visualiza en el interfaz del SIEM donde un analista ciberseguridad monitorea y el motor de reglas sería las condiciones o parámetros que se dan para que una alerta pueda activarse.

5. Almacenamiento de logs

Según, Miller et al. (2010) el almacenamiento de logs y el componente motor de correlación pertenecen a la capa 3 de correlación.

Almacenar logs generados por los distintos dispositivos demanda una base sólida de datos que posibilite la búsqueda eficiente de eventos históricos almacenados. Generalmente, se emplean para este proceso, las plataformas Oracle, MySQL, Microsoft SQL. Además, para llevar a cabo búsquedas de registros y generar informes, se requiere un hardware potente para asegurar un procesamiento efectivo de estas tareas, estos pueden ser almacenados durante periodos largos.

6. Monitoreo

Este componente pertenece a la capa de reportes y es el último componente en la arquitectura de un SIEM que involucra la interacción y la utilización de los registros almacenados. Esto se hace con el propósito de aprovechar al máximo las alertas generadas durante el proceso de correlación, monitoreo y generación de informes. Sin esta interacción, el SIEM simplemente funcionaría como un contenedor de registros.

La gestión de un SIEM se lleva a cabo a través de una interfaz o una aplicación, ambas permiten la interacción con los registros almacenados para crear nuevas reglas, realizar búsquedas, investigación, análisis forense, reportes de manera dinámica y eficiente por los expertos en ciberseguridad de manera continua los 365 días, así mismo se realiza el monitoreo y envió de alertas que se activaron hacia a los clientes para que puedan tomar acciones sobre posibles ataques cibernéticos a su infraestructura tecnológica.

En la Figura 6 observamos que la interfaz del SIEM RSA, tiene vistas como investigar, responder, usuarios, hospedadores, archivos, panel e informes en la cual cada una cumple una función específica.

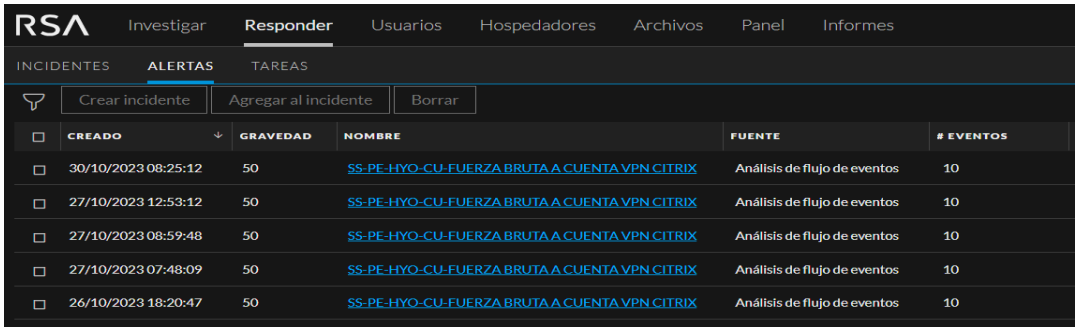


Figura 6. Vista general de la plataforma SIEM RSA
Fuente: Elaboración propia

2.2.6. Proveedores SIEM

Para obtener conocimiento sobre las soluciones SIEM más destacadas, nos apoyamos del Cuadrante Mágico de Gartner publicado en junio de 2022. En estos cuadrantes, se destacan como líderes los SIEM: Exabeam, QRadar (IBM), Securonix, Splunk y Microsoft como se detalla en la Figura 7.

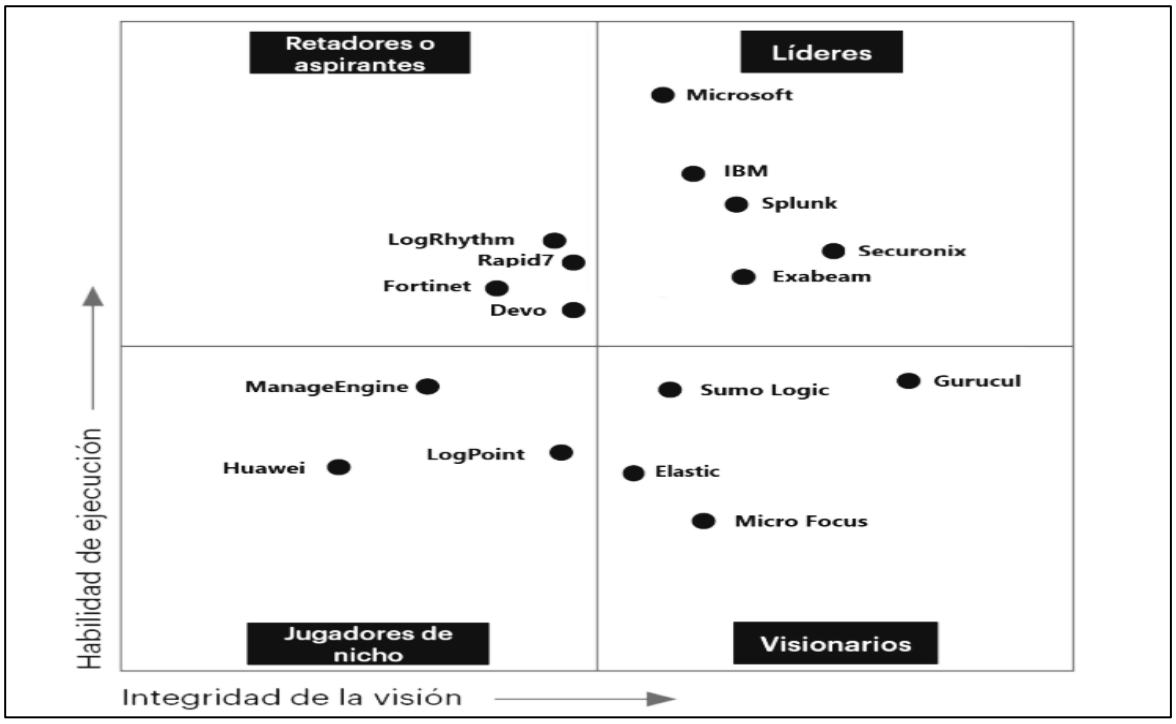


Figura 7. Cuadrante Mágico de Gartner de Sistemas SIEM
Fuente: Gartner (2022)

Como se observa en la Figura 7 el SIEM RSA ya no se encuentra en el cuadrante de Gartner publicado en año 2022 sin embargo hay organizaciones que lo siguen utilizando debido a su arquitectura flexible, escalable, fácil uso, capacidad de respuesta ante posibles ataques cibernéticos, etc. Después de exponer las ventajas y desventajas de los demás SIEM la Entidad Financiera decidió de acuerdo a sus necesidades e infraestructura tecnológica en implementar el SIEM RSA; a continuación, se profundizará ampliamente sobre el SIEM que utilizaremos para implementación del caso de uso.

2.2.7. SIEM RSA

RSA es una eficiente suite de detección de amenazas que agiliza las labores de búsqueda, priorización y clasificación de amenazas en los Centros de Operaciones de Seguridad (SOC). Esta plataforma le asiste en el aislamiento y solución de amenazas tanto conocidas como desconocidas, proporcionando una valiosa información detallada sobre paquetes, registros y dispositivos finales que le brinda una perspectiva única a una empresa. Su uso resulta más sencillo para los analistas de nivel 1, ya que automatiza la identificación y priorización de amenazas sospechosas. Los analistas de nivel 2 y nivel 3 tienen la capacidad de buscar y localizar amenazas mediante la exploración y filtrado de eventos (RSA, 2019).

2.2.7.1. Arquitectura

RSA brinda una considerable versatilidad en su implementación. La configuración de su estructura puede comprender la utilización de un solo equipo físico o múltiples equipos físicos, dependiendo de las necesidades particulares en cuanto a rendimiento y seguridad del cliente. Asimismo, la totalidad del sistema de RSA ha sido adecuadamente configurada para operar de manera eficaz en una infraestructura virtual.

Según RSA (2019) su arquitectura básica se compone de los siguientes componentes:

- Decoder (decodificador): Se encarga de recepcionar registros de múltiples dispositivos fuente y convertirlos a un formato comprensible para que el SIEM pueda interpretarlos adecuadamente.

- Concentrator (concentrador): Recibe data parseada (ordenada) del decoder, aquí se pueden realizar búsquedas con data actual o data histórica.
- Archaiver (archivador): Se encarga de almacenar a largo plazo registros que provienen de diferentes fuentes de seguridad informática como IPS, Firewall, Antispam, Antivirus, EDR, entre otros, para que pueda ser analizada posteriormente por el ESA. Es importante señalar que puede almacenar registros ordenados o sin ordenar.
- Esa (Event Stream Analysis): El servicio de Análisis de Flujos de Eventos ofrece capacidades analíticas relacionadas con la secuencia de eventos, tales como correlación y procesamiento de eventos complejos, a una velocidad elevada y con una latencia mínima identificando patrones anormales mediante reglas preestablecidas para posteriormente generar alertas.

En la Figura 8 se visualiza como está compuesto la arquitectura del SIEM RSA.

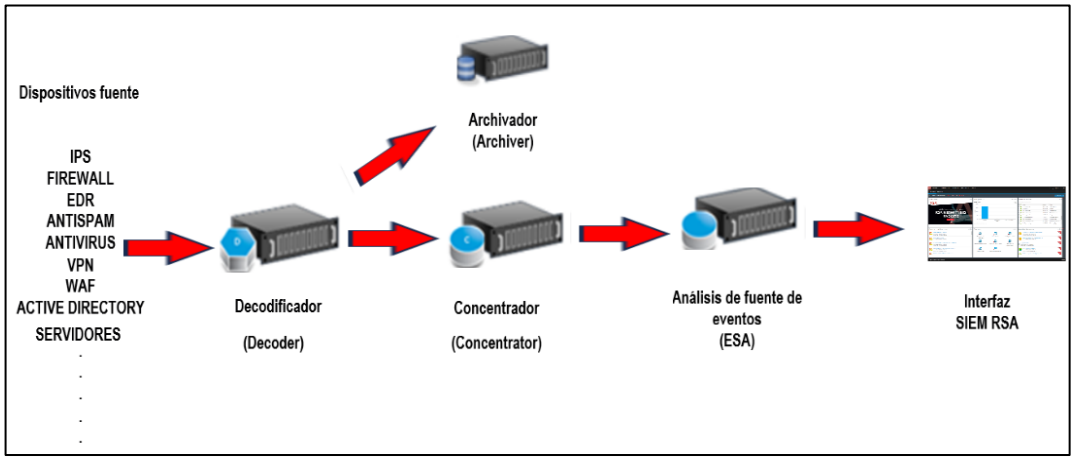


Figura 8. Arquitectura SIEM RSA

Fuente: Elaboracion propia basada en (RSA, 2019)

2.2.8. Gestión de datos de registro

Según Miller et al.(2010) se puede recopilar datos de cuatro formas distintas:

- Mediante la instalación de un agente en el dispositivo (el método más común).

- Estableciendo una conexión directa al dispositivo a través de un protocolo de red o una llamada API.
- Accediendo directamente a los archivos de registro almacenados, generalmente en formato Syslog.
- Utilizando un protocolo de transmisión de eventos como SNMP, IPFIX y Netflow.

2.2.9. Caso de Uso

Es un elemento que describe una serie de pasos y acciones que conduce a un resultado concreto y significativo IBM (2020).

Entonces podemos decir que los casos de uso son reglas de correlación cuya finalidad es detectar patrones y anomalías provenientes de distintas fuentes de eventos que llegan al SIEM basándose en reglas predefinidas o personalizadas que se configuran mediante condiciones o ciertos parámetros en base a ello poder generar alertas.

En la Figura 9 se observa varios casos de uso de diferentes clientes y la hora que se llegó a activar en un SIEM.

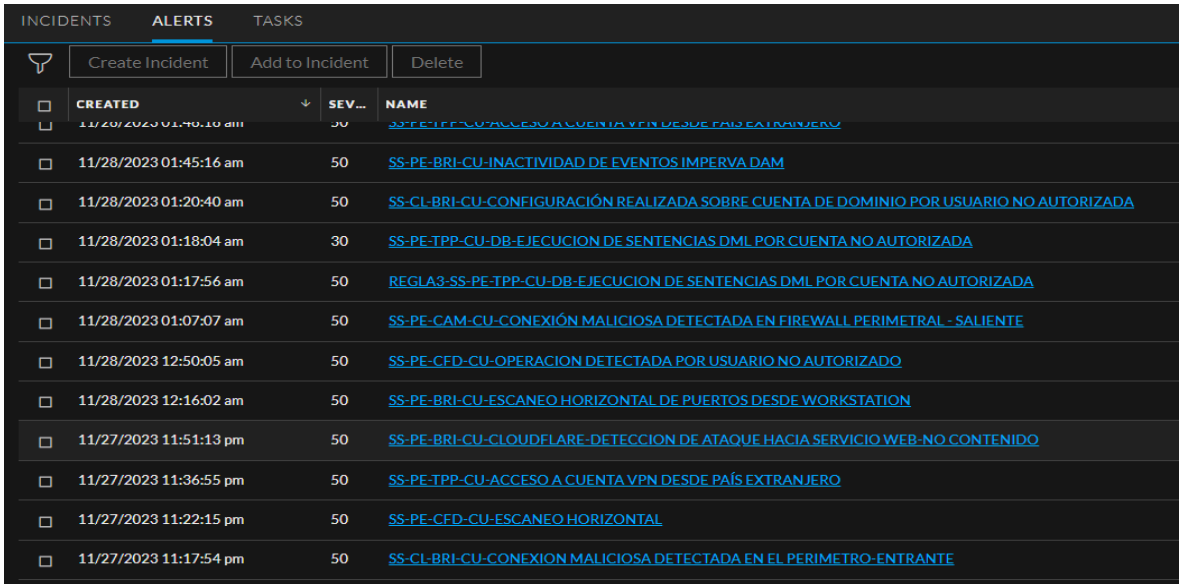


Figura 9. Visualización de casos de uso en un SIEM
Fuente: Elaboración propia

2.2.10. Logs

Logs o registros son archivos de texto que contienen información ocurrida después de un evento como actualizaciones, cambios, errores entre otros, en un sistema informático como servidor, aplicación o un programa. Los logs registran en una secuencia cronológica, donde se detallan los acontecimientos de cada evento ocurrido, no solo muestra lo que sucedió, sino cuando, donde y en qué orden (Miller et al, 2010).

En la Figura 10 se observa la recolección de eventos recepcionados de la VPN citrixns en orden cronológica, así mismo muestra información detallada de lo ocurrido en la vista de registros.

Hora de recolección	Tipo	Tipo de servicio	Clase de servicio	Registros
2023-10-29T10:47:06	Registro	citrixns	Cortafuegos de aplicaciones	29/10/2023:10:50:34 HYOMPX01 0-PPE-0: TCP CONN_TERMINATE 10425419 0 pre finalización 29/10/2023:10:50:34 - Total_bytes_send 1 - Total_bytes_recv 1
2023-10-29T10:47:07	Registro	citrixns	Cortafuegos de aplicaciones	29/10/2023:10:50:34 HYOMPX01 0-PPE-1: TCP CONN_TERMINATE 23180952 0 pre finalización 29/10/2023:10:50:34 - Total_bytes_send 0 - Total_bytes_recv 1
2023-10-29T10:47:07	Registro	citrixns	Cortafuegos de aplicaciones	29/10/2023:10:50:35 HYOMPX01 0-PPE-1: TCP CONN_TERMINATE 23180953 0 pre finalización 29/10/2023:10:50:35 - Total_bytes_send 0 - Total_bytes_recv 1
2023-10-29T10:47:07	Registro	citrixns	Cortafuegos de aplicaciones	29/10/2023:10:50:35 HYOMPX01 0-PPE-1: TCP CONN_TERMINATE 23180954 0 pre finalización 29/10/2023:10:50:35 - Total_bytes_send 0 - Total_bytes_recv 1
2023-10-29T10:47:07	Registro	citrixns	Cortafuegos de aplicaciones	29/10/2023:10:50:35 HYOMPX01 0-PPE-1: TCP CONN_TERMINATE 23180955 0 pre finalización 29/10/2023:10:50:35 - Total_bytes_send 0 - Total_bytes_recv 1
2023-10-29T10:47:08	Registro	citrixns	Cortafuegos de aplicaciones	29/10/2023:10:50:36 HYOMPX01 0-PPE-1: TCP CONN_TERMINATE 23180956 0 pre finalización 29/10/2023:10:50:36 - Total_bytes_send 0 - Total_bytes_recv 1

Figura 10. Secuencia cronológica de logs en el SIEM
Fuente: Elaboración propia

2.2.11. Seguridad Informática (Ciberseguridad)

Conjunto de tecnologías, procedimientos y métodos diseñados para salvaguardar sistemas, dispositivos de red, software, datos entre otros ante posibles ataques cibernéticos, hackeos o accesos no autorizados garantizando la integridad, confidencialidad y disponibilidad de la información de la organización (Roa, 2013).

2.2.12. Vulnerabilidades

Es una deficiencia que existe en un sistema informático ya sea hardware o software debido a un error de configuración, error de programación, retraso de los parches, descargas de programas de dudosa procedencia o un error en el diseño el cual es aprovechado por los ciber atacantes para comprometer y poner en riesgo la integridad y confidencialidad ya sea realizando actividades ilegales, sustraer

información sensible o interrumpiendo el funcionamiento del sistema informático (Roa, 2013).

En la Figura 11 se observa que el sistema operativo Windows 11 tiene una nueva versión y está solicitando que se actualice ya que tiene nuevas características, nuevo aspecto, así como también mejoras en la seguridad, debido a que probablemente existía errores en la versión antecesora con el cual los atacantes podrían vulnerar Windows 11.

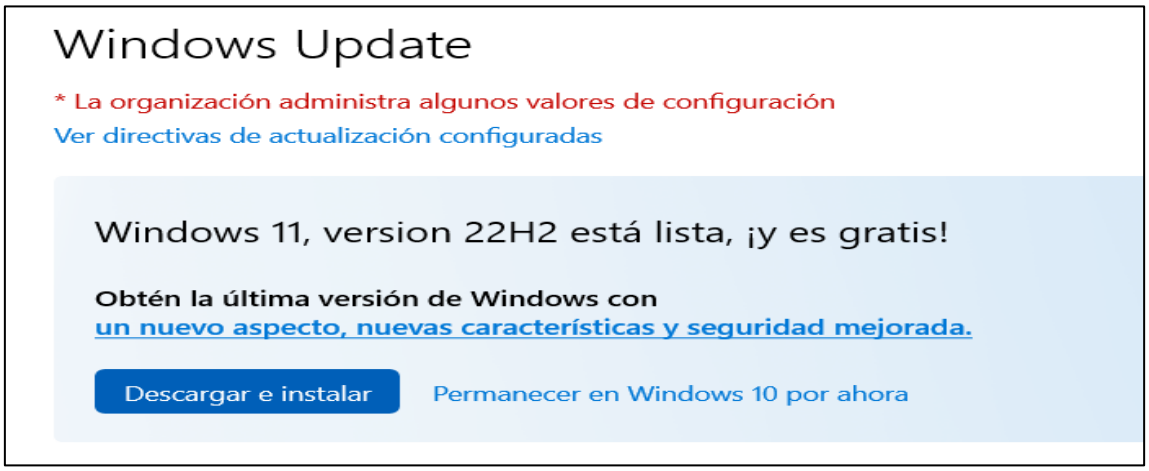


Figura 11. Actualización de sistema operativo Windows 11 - versión
Fuente: Elaboración propia

2.2.13. Amenazas Informáticas

Se debe a la explotación de una vulnerabilidad el cual es aprovechado para atacar un sistema informático, existen dos tipos de amenazas informáticas: las externas que provienen fuera de la organización realizados por ciberatacantes y las internas que se originan dentro de la organización por los propios trabajadores que tienen acceso a los activos de la organización y abusan deliberada o accidentalmente (Aguilera, 2010).

Canvia (2023) indica que existen 10 amenazas más habituales que enfrentan las empresas en el ámbito cibernético, estos son:

- Malware: Hace referencia a cualquier software malicioso cuya finalidad es causar daño a un sistema informático accediendo de manera no autorizada donde puede realizar modificación en el funcionamiento o alterando la información que contiene, tal como se muestra en la Figura 12. La manera

en que un malware entra en un sistema varía según lo que la persona pretenda lograr, estos pueden ser: virus, gusanos, troyanos, spyware entre otros. (Escrivá et al, 2013).

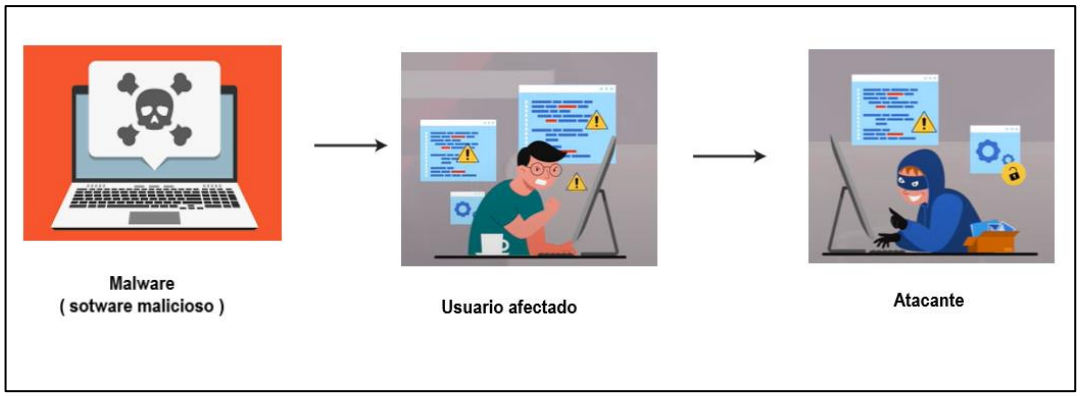


Figura 12. Atacante infecta una computadora con malware
Fuente: Elaboración propia

Phishing: consiste en la suplantación de la identidad, los atacantes mediante el envío de correos intentan engañar las personas haciéndose pasar por una organización confiable como bancos, empresas entre otros con la finalidad de adquirir información sensible como datos personales y claves de cuentas bancarias (Aguilera, 2010).

En la Figura 13 se observa que la víctima recibió un mensaje del bancoxyz en el cual le indica que entre al enlace para realizar lo que se indica en el mensaje. Sin embargo, al entrar te lleva a una página web creada por el atacante que es similar a la del bancoxyz que tiene como finalidad robar información de la víctima.


Incidencias@bancoxyz.com

Estimado cliente,

Sospechamos que en su cuenta se ha efectuado una transacción no autorizada. Para comprobar que la seguridad de su cuenta no está comprometida, por favor haga clic sobre el siguiente enlace para que podamos confirmar su identidad: www.bancoxyz.com.

Banco XYZ, 16 de marzo de 2013

Figura 13. Contenido de correo que contiene phishing
Fuente: Escrivá et al. (2013).

- Inyección SQL: El atacante explota las vulnerabilidades que existen en aplicaciones web basadas en SQL utilizando un código SQL, con este tipo de ataques se modifica el funcionamiento normal de la base de datos con el propósito de obtener información que podría ser valiosa (Escrivá et al, 2013).

- Denegación de servicio: Consiste en incapacitar temporalmente el acceso a un servidor provocando que un servicio o recurso este indisponible para los usuarios, esto sucede debido a que se generan grandes solicitudes al servicio desde una sola dirección IP, agotando los recursos disponibles en el servicio, llegando a un punto en el cual ya no puede responder y comienza a rechazar solicitudes, ocasionando generalmente la interrupción de la conectividad de la red debido a la congestión del ancho de banda o por la sobrecarga de los recursos del servidor (Costas, 2010).

  En la Figura 14 se observa que el ciberdelincuente mediante una computadora intento comprometer un servidor web, pero no tuvo éxito.

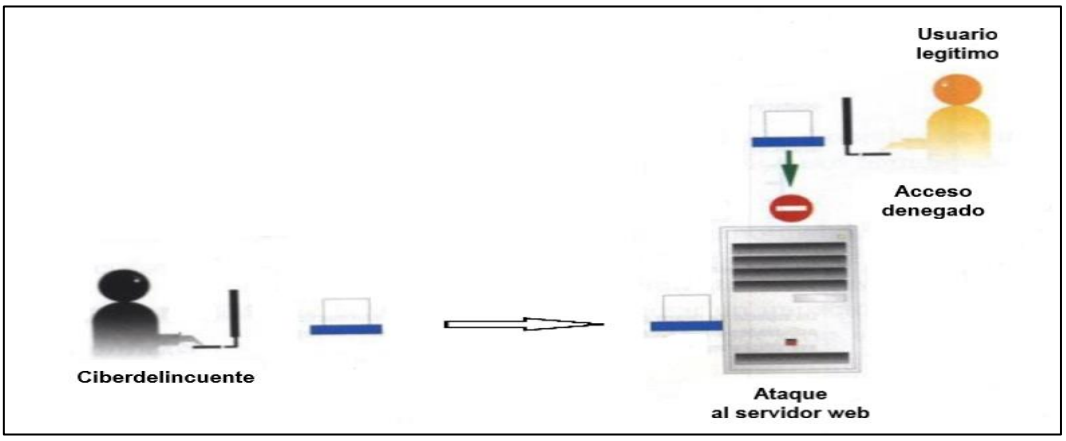


Figura 14. Denegación de servicio hacia un servidor web
Fuente: Elaboración propia basada en Aguilera (2010)

- Denegación de Servicio Distribuido (DDoS): Es un ataque similar a DoS, pero en este caso, no es una sola computadora la que crea las solicitudes falsas lo cual sería fácil de rastrear y abordar, sino que simultáneamente se utilizan numerosas computadoras distribuidas en diferentes ubicaciones del mundo, esto hace que su detección sea difícil. Estas computadoras que fueron comprometidas por un malware se convierten en computadoras zombis que están a la espera de recibir órdenes del atacante (Roa, 2013).

En la Figura 15 observamos que el ciberdelincuente dirige una red de bots o máquinas zombis para comprometer el servidor web con la finalidad que este indisponible por un tiempo determinado.

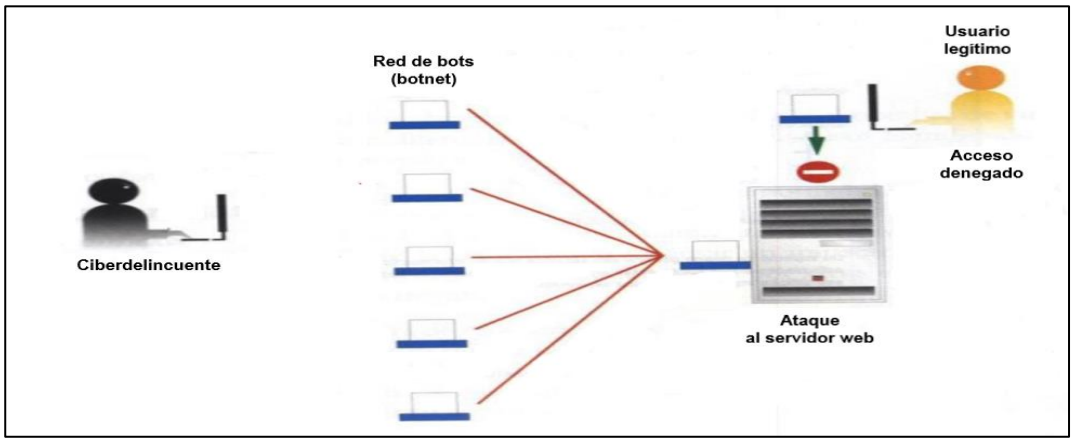


Figura 15. Denegación de servicios distribuido hacia un servidor web
Fuente: Aguilera (2010)

- Man in the middle (MITM): Esta amenaza implica la interceptación del atacante en una interacción en línea entre una página web o aplicación y un usuario. Su objetivo principal es obtener información del usuario al instalar un programa malicioso. Una de las formas para lograr su cometido seri creando una red Wi-Fi falsa sin contraseña en un lugar público. Si una persona se conecta a ella, el atacante puede acceder a cualquier tipo de información que la víctima comparta en línea (Canvia, 2023).

En la Figura 16 se observa que el atacante C intercepta el mensaje que el usuario A envía hacia el usuario B mediante la red, posteriormente lo reenvía hacia el usuario C sin que ambos usuarios legítimos se den cuenta. Esto se define como una amenaza Man in the middle.

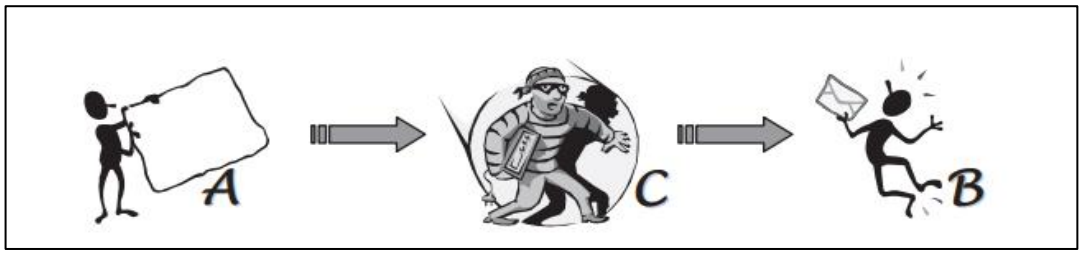


Figura 16. Amenaza Man in the middle
Fuente: Gómez (2011)

- Rootkit: Se trata de un tipo de malware que altera el sistema operativo del equipo infectado con el fin de ocultarse y permanecer en estado de espera

para recibir instrucciones del atacante. En muchas situaciones, los programas antivirus no son capaces de detectarlos (Escrivá et al, 2013).

- Emotet: Es un troyano conocido por su habilidad para burlar a los programas antivirus convencionales y mantenerse oculto ante ellos. Esto se debe a su capacidad de modificar ligeramente su código, es decir, es un malware polimórfico. Una vez que infecta un sistema, se expande como un gusano informático y busca infiltrarse en otros equipos informáticos de la misma red con la finalidad de sustraer información confidencial y personal. (Canvia, 2023).

  En la Figura 17 se observa que el atacante está actualizando el malware emotet en una computadora comprometida de un usuario, con el objetivo de evitar su detección por parte de los antivirus.

Figura 17. Actualización de malware emotet en computadora comprometida

Fuente: Elaboración propia

- Fuerza bruta: Consiste en intentar todas las posibles combinaciones de caracteres hasta descubrir la clave que permite acceder al sistema, Por lo tanto, entre más extensa sea la contraseña, más difícil resultará acceder, ya que lleva más tiempo adivinarla. Por ejemplo, la contraseña "e345Uj6R3L9834pS" es mucho más complicada de adivinar que simplemente "x4UM"(Escrivá et al, 2013).

En la Figura 18 se observa que el atacante después de varios intentos logró descifrar la contraseña del usuario.

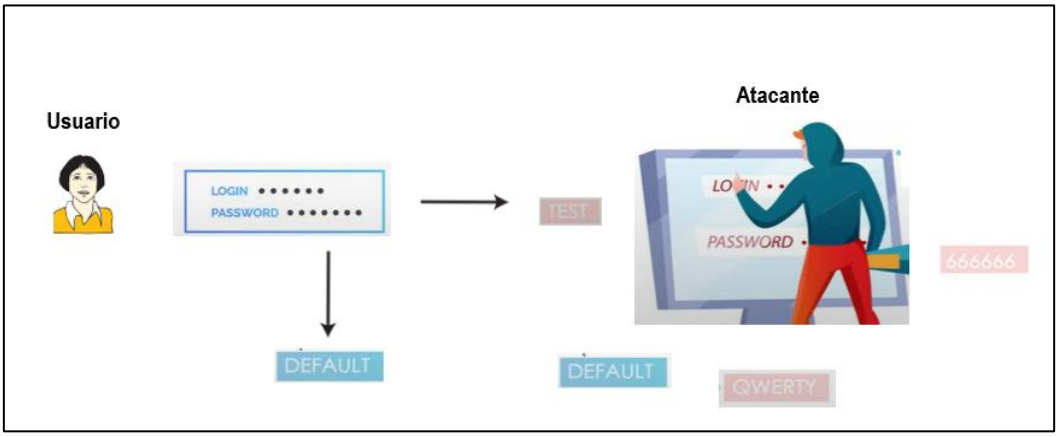


Figura 18. Atacante descifra la contraseña del usuario
Fuente: Elaboración propia

- Ransomware: sotware malicioso que evita que los usuarios accedan a sus equipos informáticos o a sus archivos personales, una vez que toma control puede cifrar los archivos importantes y solicitar un rescate como pago mediante bitcoin (Costas, 2010).

En la Figura 19 se muestra cómo un atacante infecta una computadora con un malware específico. Luego, el atacante recopila información valiosa y procede a cifrar los archivos críticos, bloqueando así el acceso a los mismos y exigiendo un rescate de 500 dólares a cambio de desbloquearlos.

Figura 19. Computadora de usuario infectado con ransomware a una computadora
Fuente: Elaboración propia

2.2.14. Ataques Informáticos

Se considera que ha ocurrido un ataque accidental o inesperado contra el sistema cuando se materializa una amenaza.

Según Roa (2013) Una vez que un atacante está determinado atacar una organización, tiene la opción de emplear las siguientes formas:

- Interrupción: El ataque busca interrumpir un servicio, lo que significa que el servidor web podría quedar inaccesible o el disco en red podría volverse inoperable, entre otras posibles consecuencias.
- Interceptación: El ciberdelincuente consiguió entrar en la red de una organización y duplico la información que se estaba enviando.
- Modificación: En lugar de simplemente copiar la información, el atacante la modifica para que llegue al destino de manera alterada, lo que podría desencadenar una reacción inusual. Por ejemplo, podría alterar los dígitos de una transacción bancaria.
- Fabricación o generación: El atacante finge ser el destinatario de la transmisión, con la finalidad de engañar a su víctima para obtener información valiosa, entre otras posibilidades.

En la Figura 20 se observan ejemplos de las formas en el cual un atacante puede atacar un determinado sistema para obtener información.

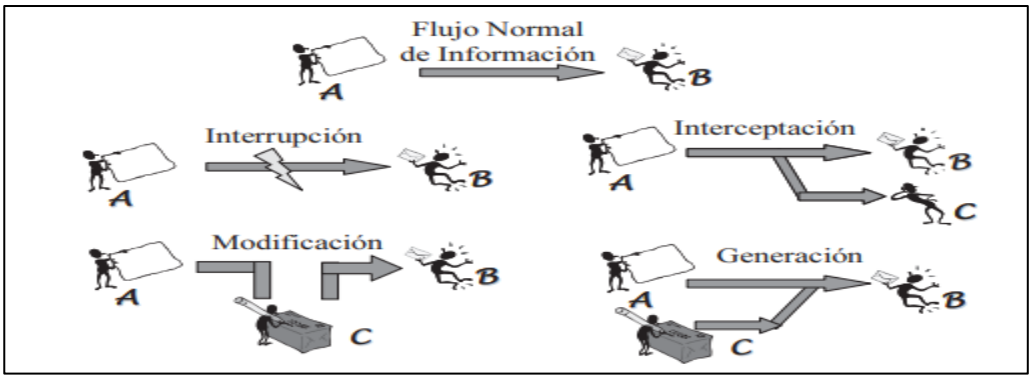


Figura 20. Formas de ataques informáticos
Fuente: Gómez (2011)

2.2.15. Solución de seguridad

- Antispam: Es un sotware de seguridad informática que se encarga de proteger a los dispositivos frente a algún malware que intenta acceder e infectar el equipo de un usuario mediante el envío de correos electrónicos no deseados denominados “SPAM” en el cual dentro del contenido podría contener un código malicioso, de ser así lo bloquea o los envía a la carpeta de cuarenta para su posterior eliminación.

  Algunos antispam utilizados por las diferentes organizaciones son FortiMail, Cisco Ironport AntiSpam, Barracuda Email Security Gateway, etc.

  En la Figura 21 se observa que el antispam FortiMail recibe un correo con un adjunto, entonces lo envía hacia el sandbox para que analice si es malicioso o no. Posterior a ello, se observa que el sandbox lo cataloga como malicioso por ende el correo no llegara al servidor del correo ni al destinario ya que fue eliminado.

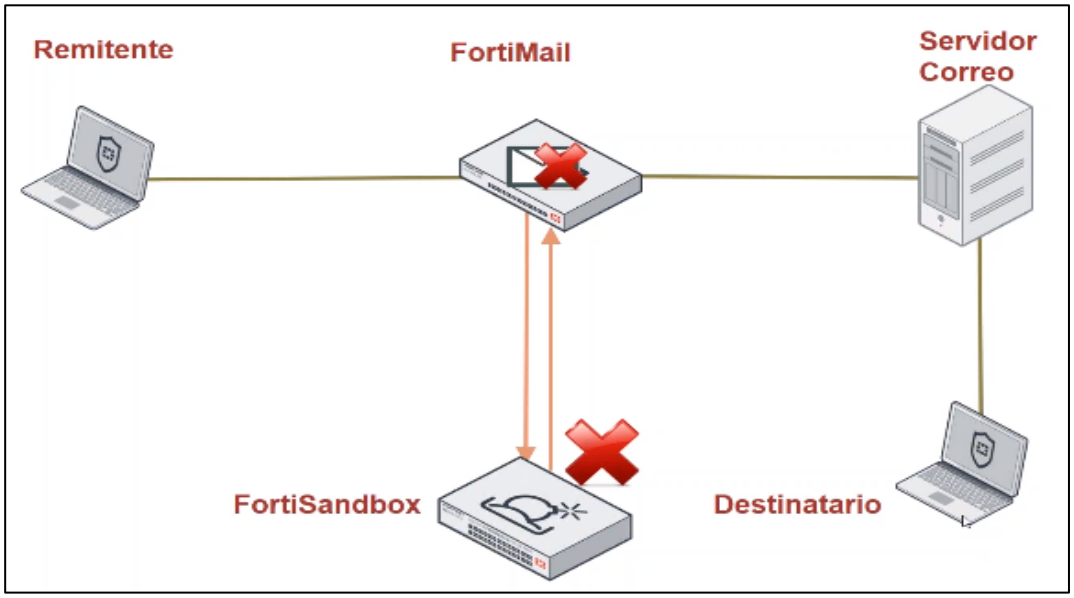
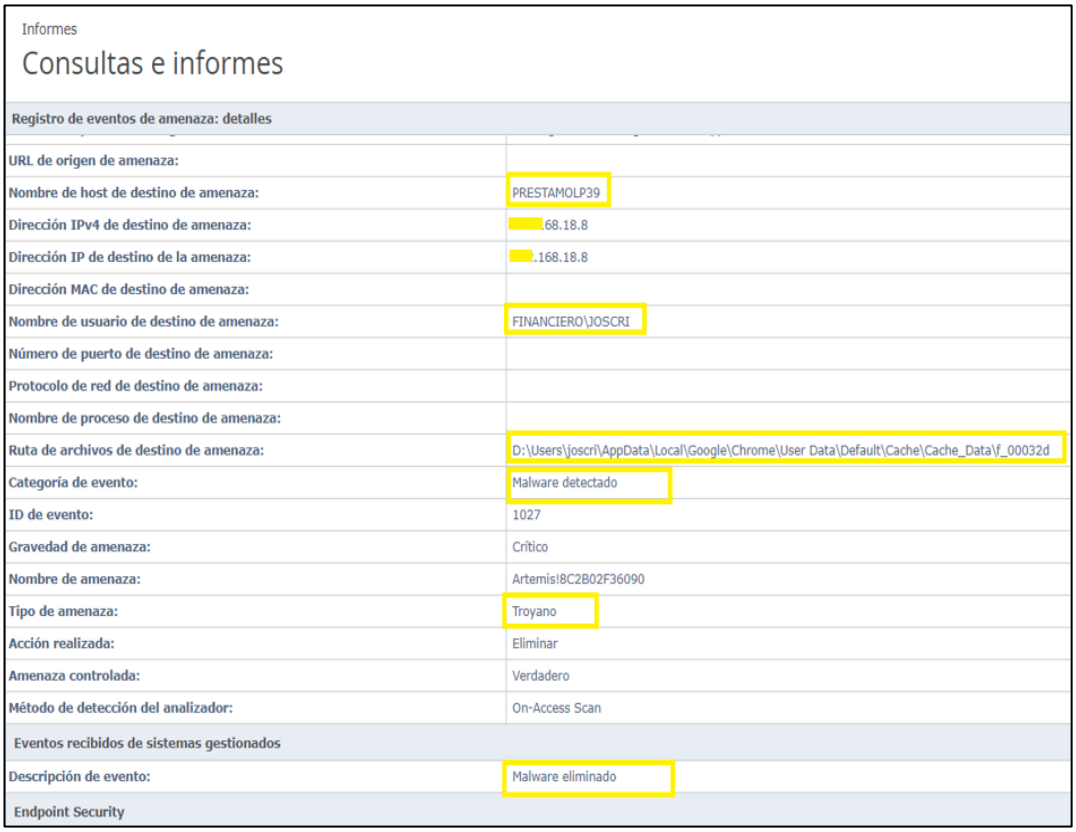


Figura 21. Funcionamiento de antispam FortiMail
Fuente: Elaboración propia

- Antivirus: Es un software que se encarga de analizar, detectar, bloquear y eliminar archivos maliciosos que contienen malware como: virus, troyanos, spyware, Ransomware y muchos más encontrados en un endpoint: computadora, laptop, impresora y servidor cuya finalidad es evitar que comprometa un endpoint y con ello vulnerar toda la red de una organización.

Algunos de los antivirus comúnmente utilizados son Symantec, McAfee, Kaspersky y ESET.

En la Figura 22 se aprecia que la computadora del usuario JOSCRI fue infectada con un troyano, sin embargo, el antivirus lo detectó y eliminó a tiempo.


Informes

Consultas e informes

Registro de eventos de amenaza: detalles	
URL de origen de amenaza:	
Nombre de host de destino de amenaza:	PRESTAMOLP39
Dirección IPv4 de destino de amenaza:	[redacted]68.18.8
Dirección IP de destino de la amenaza:	[redacted].168.18.8
Dirección MAC de destino de amenaza:	
Nombre de usuario de destino de amenaza:	FINANCIERO\JOSCRI
Número de puerto de destino de amenaza:	
Protocolo de red de destino de amenaza:	
Nombre de proceso de destino de amenaza:	
Ruta de archivos de destino de amenaza:	D:\Users\joscri\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00032d
Categoría de evento:	Malware detectado
ID de evento:	1027
Gravedad de amenaza:	Crítico
Nombre de amenaza:	Artemis!8C2B02F36090
Tipo de amenaza:	Troyano
Acción realizada:	Eliminar
Amenaza controlada:	Verdadero
Método de detección del analizador:	On-Access Scan
Eventos recibidos de sistemas gestionados	
Descripción de evento:	Malware eliminado
Endpoint Security	

Figura 22. Malware detectado por el Antivirus McAfee

Fuente: Elaboración propia

- Firewall: Es una solución de seguridad responsable de monitorear el tráfico de red que ingresa y sale de una red con el propósito de decidir si permite su paso hacia el destino previsto o debe ser bloqueado, en función de reglas predefinidas, de esta manera se busca prevenir y proteger a la red de la organización ante posibles intrusiones o ataques cibernéticos externos (Fortinet, 2023).

  Algunas marcas de firewall que existen son: Cisco, Palo Alto, Fortinet, Check Point.

En la Figura 23 se observa conexiones sospechosas que están siendo aceptadas por el firewall Fortinet desde la IP externa de Países Bajos hacia la IP interna de Perú por el puerto 80.

▼Fecha/Hora	ID del dispositivo	Acción	Origen	País Origen	IP Destino	Servicio	Puerto de Destino
19:43:36	FG6H0E5819905212	✓	37.0.10.12	Netherlands	200.	HTTP	80
19:43:33	FG6H0E5819905212	✓	37.0.10.12	Netherlands	200.	HTTP	80

Figura 23. Tráfico de firewall Fortinet
Fuente: Elaboración propia

- IPS: El sistema de prevención de intrusos es un dispositivo de seguridad de red que se diseñó para identificar prevenir y tomar acciones proactivas ante posibles amenazas cibernéticas que ocurren en tiempo real.

  Monitorea todo el tráfico de la red y compara patrones de tráfico con firmas de amenazas para posteriormente permitir o descartar paquetes protegiendo así contra vulnerabilidades nuevas y existentes en servidores (Fortinet, 2023).

- EDR: Es una solución de seguridad que proporciona monitoreo y análisis continuo del endpoint y la red, combina el antivirus convencional con herramientas de monitoreo e inteligencia artificial para proporcionar una respuesta ágil y efectiva ante un posible ataque cibernético en el cual puedan poner en riesgo a la organización (Trend Micro, 2023).

  En la Figura 24 se observa la interfaz del EDR Trend Micro como también la activación de 2 modelos con severidad media y alta en 2 equipos (laptops, computadora).

Workbench ID	Model name	Model severity	Impact scope	Data source / processor
WB-27026-20230609-00016	[Heuristic Attribute] Ransomware File Detecti...	Medium	1	Trend Micro Apex One as a Service
WB-27026-20230609-00015	[Heuristic Attribute] Possible Data Encrypted ...	High	1	Trend Micro Apex One as a Service

Figura 24. Interfaz del EDR Trend Micro
Fuente: Elaboración propia

- WAF: El firewall de aplicaciones web ayuda a resguardar las aplicaciones web de diversos ataques que apuntan al servidor de aplicaciones web. Su tarea fundamental es asegurar la integridad del servidor web al examinar

tanto las solicitudes HTTP/HTTPS como los patrones de tráfico (Cloudflare, 2023).

En la Figura 25 se observa que WAF examina las solicitudes HTTPS de A, B y C que intentan conectarse con el servidor web, ejecutando la regla de seguridad adecuada de entre todas las configuradas previamente. Posterior al análisis, en A y C no encontró ningún elemento sospechoso que pueda dañar al servidor, dejando completar la solicitud. Sin embargo, en B identifico una amenaza potencial, interrumpiendo de inmediato la conexión HTTPS para no permitir el acceso al servidor WEB.

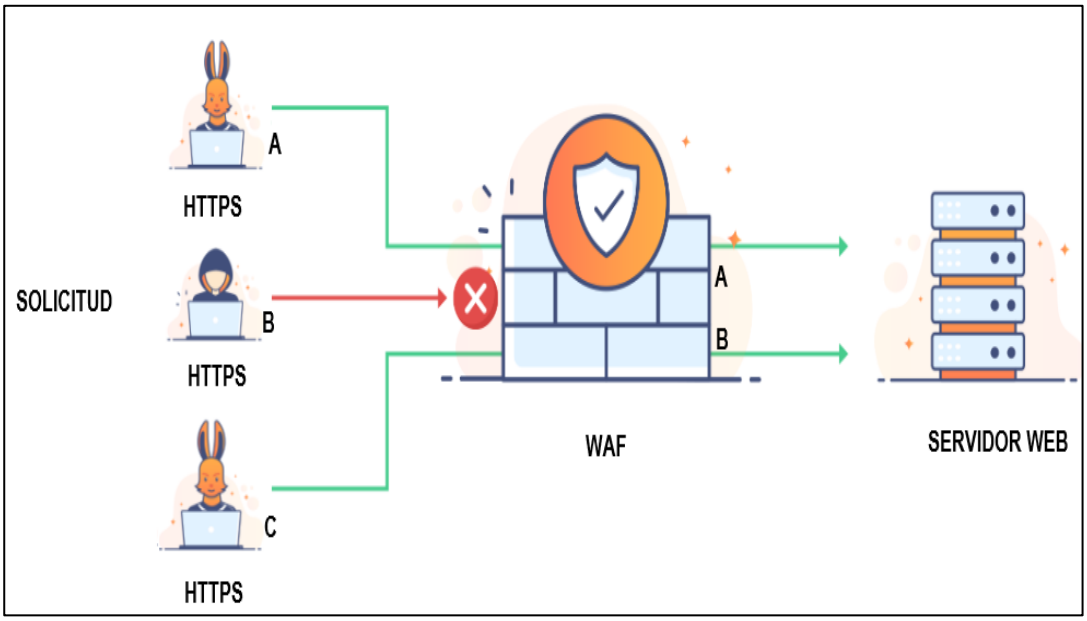


Figura 25. Funcionamiento de WAF
Fuente: Elaboración propia

- VPN: La red privada virtual es un sotware que permite a los usuarios establecer una conexión segura y encriptada entre dos dispositivos mediante internet, protegiendo la transmisión de la información confidencial y evitando posibles espionajes por parte de personas no autorizadas (Cisco, 2023).

En la Figura 26 podemos observar que el usuario rjuan coloca sus credenciales para conectarse remotamente a través de Citrix NetScaler hacia la empresa en la que labora.

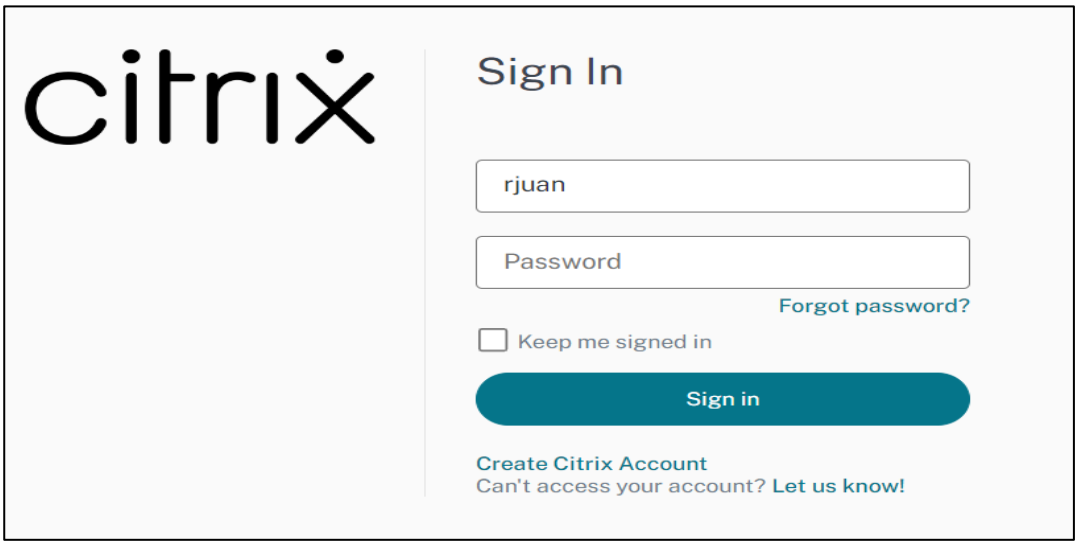


Figura 26. Conexión a través de VPN Citrix NetScaler
Fuente: Elaboración propia

2.2.16. SOC (Centro de Operaciones de Seguridad)

Es un grupo de expertos en seguridad informática que están encargados de vigilar sin interrupción la infraestructura tecnológica de una organización durante las 24 horas del día y los 7 días de la semana. Su objetivo primordial es identificar incidentes de seguridad cibernética en tiempo real y responder a ellos de la manera más rápida y efectiva posible para salvaguardar los activos y reputación de una organización utilizando distintas plataformas de seguridad y de monitoreo entre ellos el uso de SIEM (IBM, s.f).

Así mismo las funciones y obligaciones del SOC están conformadas por tres categorías:

1. Preparación, planificación y prevención
2. Supervisión, detección y respuesta
3. Recuperación, mejoras y conformidad

En la Figura 27 se observa a los especialistas de ciberseguridad del centro de monitoreo de operaciones (SOC) monitorear diversas plataformas de seguridad que tienen los clientes al cual se les brinda el servicio.

.

Figura 27. Centro de monitoreo (SOC)
Fuente: Elaboración propia

2.3 Definición de Términos

Device Type: Hace referencia al tipo específico de dispositivo que envía registros (logs) al SIEM RSA.

Confidencialidad: Su propósito es garantizar que solo las personas autorizadas pueden acceder a la información sensible y realizar cambios en ella (Escrivá et al, 2013).

Integridad: La finalidad de la integridad es que los datos permanezcan guardados de acuerdo con las expectativas del usuario, sin sufrir modificaciones sin su aprobación (Roa, 2013).

Disponibilidad: Hace referencia que los usuarios autorizados puedan acceder a la información en cualquier momento (Escrivá et al ,2013).

Activos: Se describe como un recurso dentro del sistema, ya sea informático o no, que resulta esencial para que la organización logre sus metas establecidas. En otras palabras, se refiere a cualquier cosa que tenga valor y deba ser resguardada en caso de posibles incidentes, tanto deliberados como accidentales, se pueden considerar como activos a los empleados, software, Información y hardware (Escrivá et al ,2013).

Interfaz SIEM RSA: Es un panel interactivo que está compuesto por varias vistas, aquí se pueden observar las alertas que se activan, podemos realizar informes, crear nuevos casos de uso, realizar investigaciones en el concentrador con data en tiempo real o con data histórica.

Volumetría: Cantidad de datos de eventos y registros que se recopilan y gestionan en un dispositivo, en un determinado tiempo.

Security Advisor: Encargado de diseñar y crear nuevos casos de uso en base a su investigación con el SIEM RSA, para ello utiliza varios logs de las distintas plataformas de seguridad que cuenta la Entidad Financiera; Con la finalidad de buscar amenazas el cual pueda afectar su infraestructura tecnológica.

Entidad Financiera: Así llamaremos a la empresa en el cual se implementó el caso de uso.

Evento: Suceso, ocurrencia o comportamiento anómalo identificado en el estado de un activo de información pudiendo generar una alerta o posible afectación.

Incidente: Violación o afectación inminente de la seguridad, generando impacto en el estado del activo de información.

Fuente: Nombre del dispositivo que envía registros (logs) al SIEM RSA.

Falso positivo: Se denomina a los eventos que son reconocidos por la Entidad Financiera, no afectan a los activos.

Formato 07: Documento que contiene información detallada sobre la configuración del caso de uso.

CAPITULO III: DESARROLLO DEL TRABAJO PROFESIONAL

3.1. Determinación y análisis del problema

En la actualidad, las empresas buscan proteger la integridad, disponibilidad y confidencialidad de la información de las amenazas y vulnerabilidades externas mediante dispositivos de seguridad informática como firewall, antivirus, IPS, antispam, proxy, VPN entre otros, ya que constantemente están siendo atacados por los ciberdelincuentes que intentan robar su información confidencial y la de sus clientes, aprovechando brechas abiertas en las soluciones de seguridad generando grandes pérdidas económicas.

Asimismo, si no se cuenta con un sistema sofisticado de monitoreo como la plataforma SIEM y ocurre un posible ataque hacia la infraestructura tecnológica, los especialistas de seguridad se tomarían mucho tiempo en identificar por dónde están siendo atacados, ya que disponen de varios dispositivos de seguridad informática como firewall, IPS, antivirus, antispam, EDR y otros que monitorean individualmente; mientras que los atacantes actúan en segundos, esto es una gran desventaja a la hora de responder y tratar de mitigar un ataque cibernético.

Por otro lado, Gartner (2022) presentó un cuadrante Mágico de Sistemas SIEM donde se puede apreciar que existen diferentes proveedores de SIEM como Microsoft, Exabeam, QRadar (IBM), Securonix, Splunk y Fortinet. Este informe demuestra que las empresas están invirtiendo en su seguridad para protegerse de ataques cibernéticos ayudándose del SIEM.

Por este motivo muchas empresas optan por implementar un SIEM o sistema de gestión de eventos e información de seguridad indistintamente del fabricante, que les permitirá recibir logs desde diferentes dispositivos y centralizar la información para luego realizar un análisis exhaustivo, correlacionando eventos en tiempo real mediante la creación de reglas o también denominados casos de uso con el propósito de buscar tendencias y patrones de comportamiento anómalo, facilitando así la identificación de eventos inusuales de aquellos que son comunes permitiendo prevenir, anticipar posibles amenazas y vulnerabilidades. Emitiendo alertas oportunas para que se tomen acciones respectivas con la finalidad de ayudar a proteger los datos y reputación de la organización.

También, Miller et al. (2010) afirman que el SIEM se concibe como una plataforma destinada a gestionar eventos e incidentes de seguridad. Esto implica normalizar datos, detectar comportamientos anómalos y maliciosos, emitiendo alertas sobre eventos relevantes, permitiendo una variedad de acciones como generar informes y gráficos para representar lo que sucede en la red de la organización en tiempo real o a lo largo del tiempo.

Según el Diario Gestión (2023) informó que el 36% de las empresas sufrieron vulneración de sus datos. También, se dio a conocer que los ciberdelincuentes atacan principalmente a la nube, vulneran los equipos de las empresas, realizan operaciones de pirateo y filtración. De la misma manera, el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, 2023) anunció el 23 de octubre que la empresa GTD de Chile sufrió un ataque de Ransomware lo cual afectó la indisponibilidad de los distintos servicios a nivel nacional e internacional siendo Perú y Chile los países más afectados.

Por ese motivo la Entidad Financiera años atrás había contratado el servicio de CyberSOC que ofrece la empresa SecureSoft, para proteger sus datos ante posibles amenazas cibernéticas, que incluía el monitoreo de todas sus plataformas de seguridad mediante el SIEM RSA, el cual presentó 2 etapas: de proyectos y servicio.

Durante la etapa de proyectos se configuraron los 20 casos de uso que fueron propuestos como base, relacionados a sus plataformas integradas en el SIEM RSA de acuerdo a su necesidad y, que toda empresa, debe tener para proteger su infraestructura tecnológica de los ataques cibernéticos, una vez configurados los 20 casos de uso, pasa a la etapa de servicio, en esta, los casos de uso restantes serán propuestos por el analista de ciberinteligencia en conjunto con el especialista de seguridad informática de la Entidad Financiera.

Actualmente, se encuentra en la etapa de servicio, por consiguiente, le quedan casos de uso extra que aún faltan implementar, por ello, el especialista de la Entidad Financiera solicitó la creación de un caso de uso proveniente del dispositivo VPN Citrix NetScaler.

Esta medida se basa en la preocupación de que, si un atacante cibernético logra infectar y tomar el control de la computadora de un trabajador que se conecta remotamente a través de VPN a la red de la Entidad Financiera, podría intentar obtener las credenciales de la VPN utilizando software especializado. Este intento buscaría facilitar el acceso a la red de la Entidad Financiera con el objetivo de robar información confidencial.

3.2. Modelo de solución propuesto

En relación con la problemática presentada, para proteger los activos de la Entidad Financiera se diseñó e implementó el caso uso fuerza bruta a cuenta VPN Citrix en 4 etapas: diseño, configuración, validación y pase a producción, como se observa en la Figura 28.

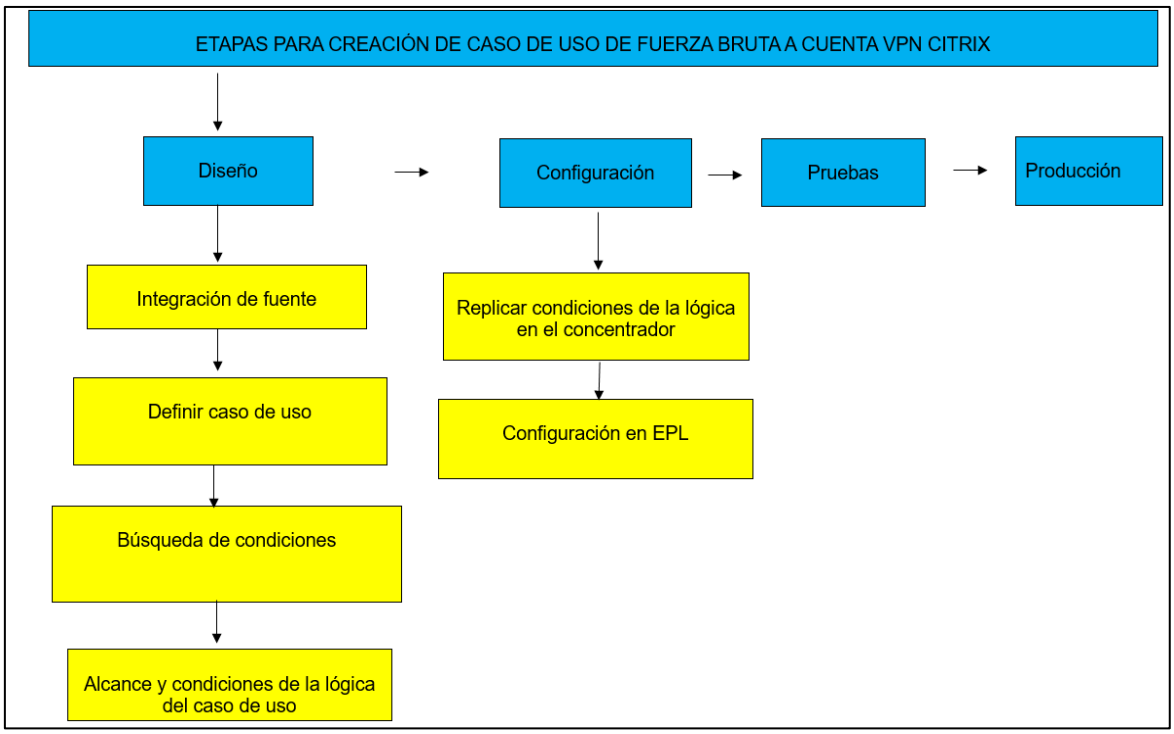


Figura 28. Etapas para la creación de caso de uso fuerza bruta a cuenta VPN CITRIX
Fuente: Elaboración propia

Para lograr el objetivo, se formó un equipo de trabajo donde el ingeniero de soporte SIEM se encargó de integrar la fuente VPN Citrix NetScaler en la plataforma SIEM RSA mediante citrixns. Por otro lado, el diseño, la configuración de las condiciones de la lógica en la plataforma SIEM RSA, realizar la validación y pasar el caso de

uso a producción estuvieron a cargo del analista de ciberinteligencia, cargo que actualmente desempeñó, como se visualiza en la Figura 29.

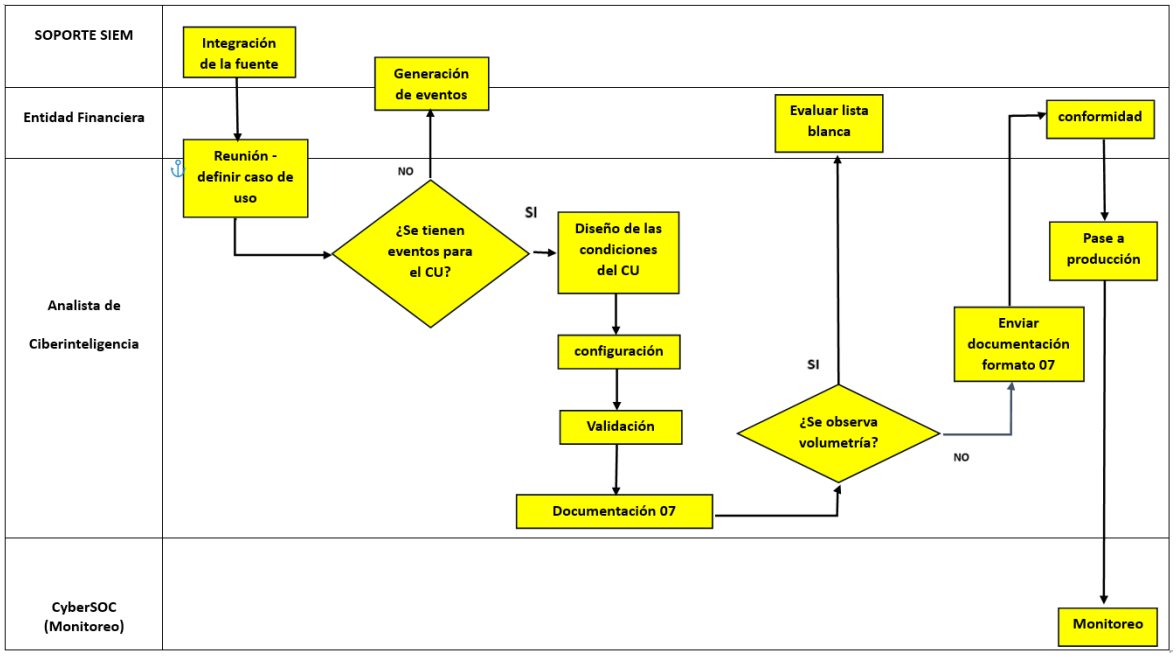


Figura 29. Proceso de la Implementación del Caso de uso
Fuente: Elaboración propia

El presupuesto invertido en la implementación del caso de uso fue de S/ 21693 soles. A continuación, se detallan los costos en la Tabla 2.

Tabla 2

Presupuesto de la creación del caso de uso

Recursos		Costo
Recursos humanos	✓ Analista de ciberinteligencia ✓ Ingeniero de soporte SIEM ✓ Supervisor de CyberSOC ✓ Analista de CyberSOC	S/ 933 S/ 1500 S/ 958 S/ 602
Materiales	✓ Laptop (4) ✓ Internet ✓ Uso de espacio ✓ Electricidad	S/ 500 S/ 300 S/ 700 S/ 200

Mantenimiento de plataforma	✓ SIEM RSA	S/ 1000
Diseño y configuración del Caso de uso	✓ fuerza bruta a cuenta VPN Citrix	S/ 15000
Total		S/ 21693

Fuente: Elaboración propia

3.2.1. Etapa de diseño

3.2.1.1 Integración de fuente - VPN Citrix NetScaler

Antes de diseñar y realizar la implementación del caso de uso, es indispensable que los distintos dispositivos que cuenta la Entidad Financiera tienen que estar integrados y enviar logs en tiempo real al SIEM RSA, esto es fundamental para crear los casos de uso debido a que si no envían logs no podrán correlacionar las condiciones de la lógica. Por consiguiente, el caso de uso no se activará.

Por ello, el ingeniero de soporte SIEM, encargado de realizar la integración de la fuente de eventos VPN Citrix NetScaler hacia el SIEM RSA tuvo que integrarlo con las buenas prácticas que recomienda el fabricante del dispositivo para que envíe correctamente logs hacia el SIEM RSA.

En la Figura 30 se observa el proceso de la integración de la fuente VPN CITRIX hacia el SIEM RSA.

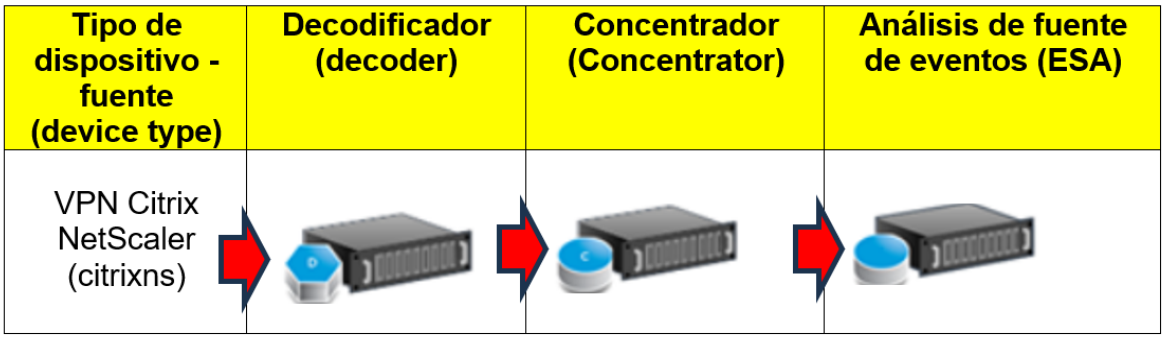


Figura 30. Proceso de la integración de la fuente VPN Citrix NetScaler
Fuente: Elaboración propia

Finalmente, el ingeniero de soporte SIEM validó que la fuente VPN Citrix NetScaler esté enviando logs en tiempo real al SIEM RSA, con ello quiere decir que está listo para diseñar el caso de uso de fuerza bruta a cuenta VPN Citrix.

En la Figura 31 se observa que la fuente de eventos VPN CITRIX NetScaler mediante citrixns está enviando logs en tiempo real hacia la plataforma SIEM RSA.

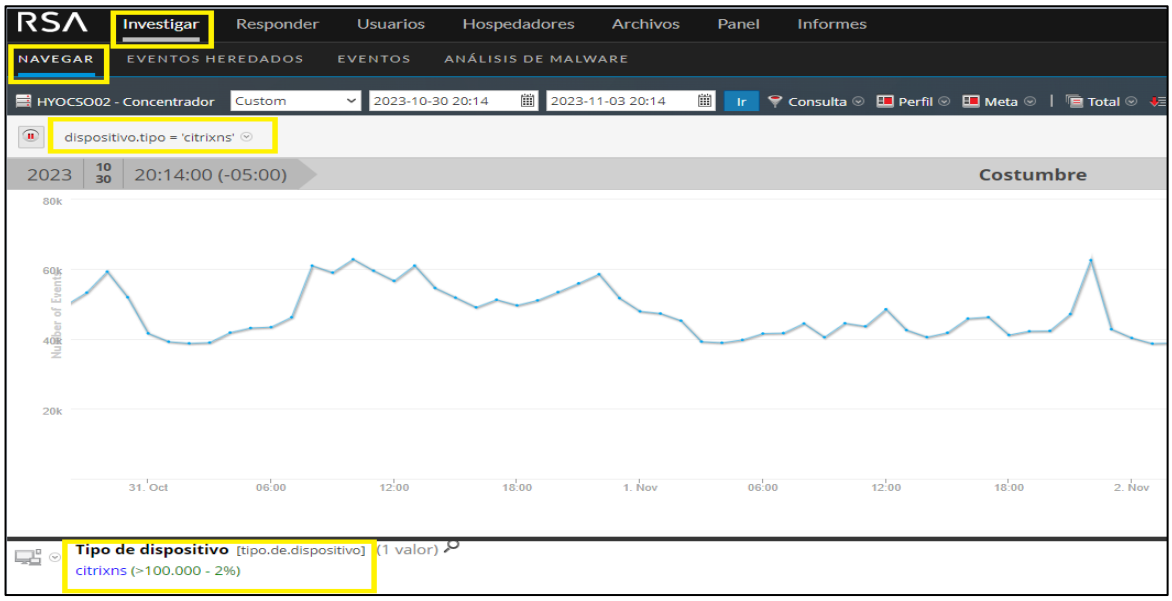


Figura 31. Recepción de eventos provenientes de VPN Citrix NetScaler hacia SIEM RSA
Fuente: Elaboración propia

3.2.1.2 Definir caso de uso

Después de la integración de la fuente de eventos VPN Citrix NetScaler al SIEM RSA a través de Citrixns, se llevó a cabo una sesión por Teams con el especialista de seguridad informática de la Entidad Financiera. Durante esta sesión, se discutió la problemática detectada y se colaboró para encontrar una solución.

Problema:

Los trabajadores de la Entidad Financiera utilizan VPN Citrix NetScaler para conectarse remotamente hacia la red de la Entidad Financiera. Entonces, si un ciberdelincuente llegase a infectar y tomar el control de sus computadoras, intentará conseguir las credenciales de la VPN utilizando un sotware especializado, para poder conectarse a la red de la Entidad Financiera y robar información confidencial.

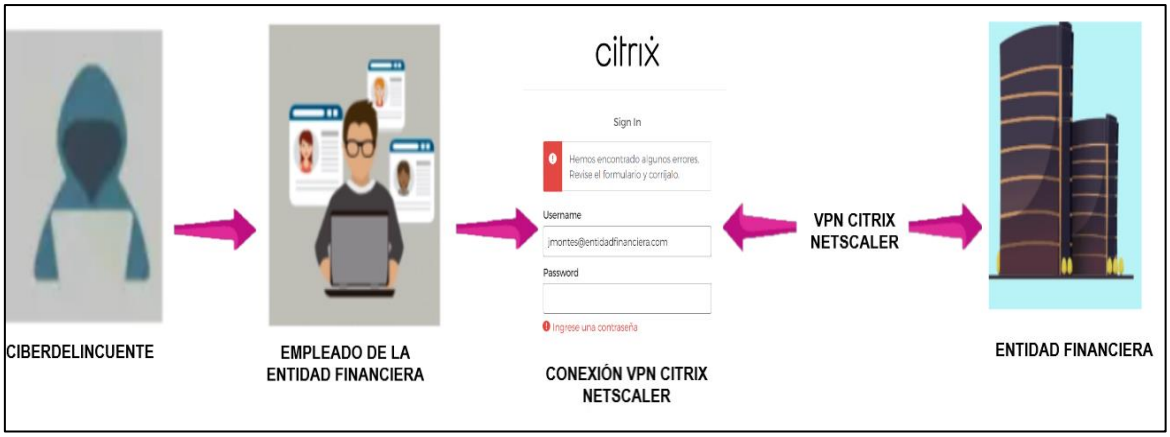


Figura 32. Ciberdelincuente intenta conectarse mediante VPN Citrix NetScaler hacia la Entidad Financiera

Fuente: Elaboración propia

En la Figura 32 se observa que el ciberdelincuente tomó el control de la computadora de un empleado de la Entidad Financiera, posteriormente intentó conectarse mediante VPN Citrix NetScaler colocando usuario y contraseña, al no tener la clave del usuario automáticamente saldrá error de conexión, lo intentará varias veces sin tener éxito; pero ¿Qué sucedería si el atacante lo intenta otro día y esta vez llega a tener éxito? el ciberdelincuente accedería a la información confidencial de la Entidad Financiera y de sus clientes.

Solución:

Crear un caso de uso que se active en la plataforma SIEM RSA cuando existen intentos de conexiones fallidas, por un usuario que utiliza VPN Citrix NetScaler para conectarse remotamente hacia la red de la Entidad Financiera, en un periodo determinado.

En la Figura 33 se observa interrogantes que suceden ante un problema y las soluciones.

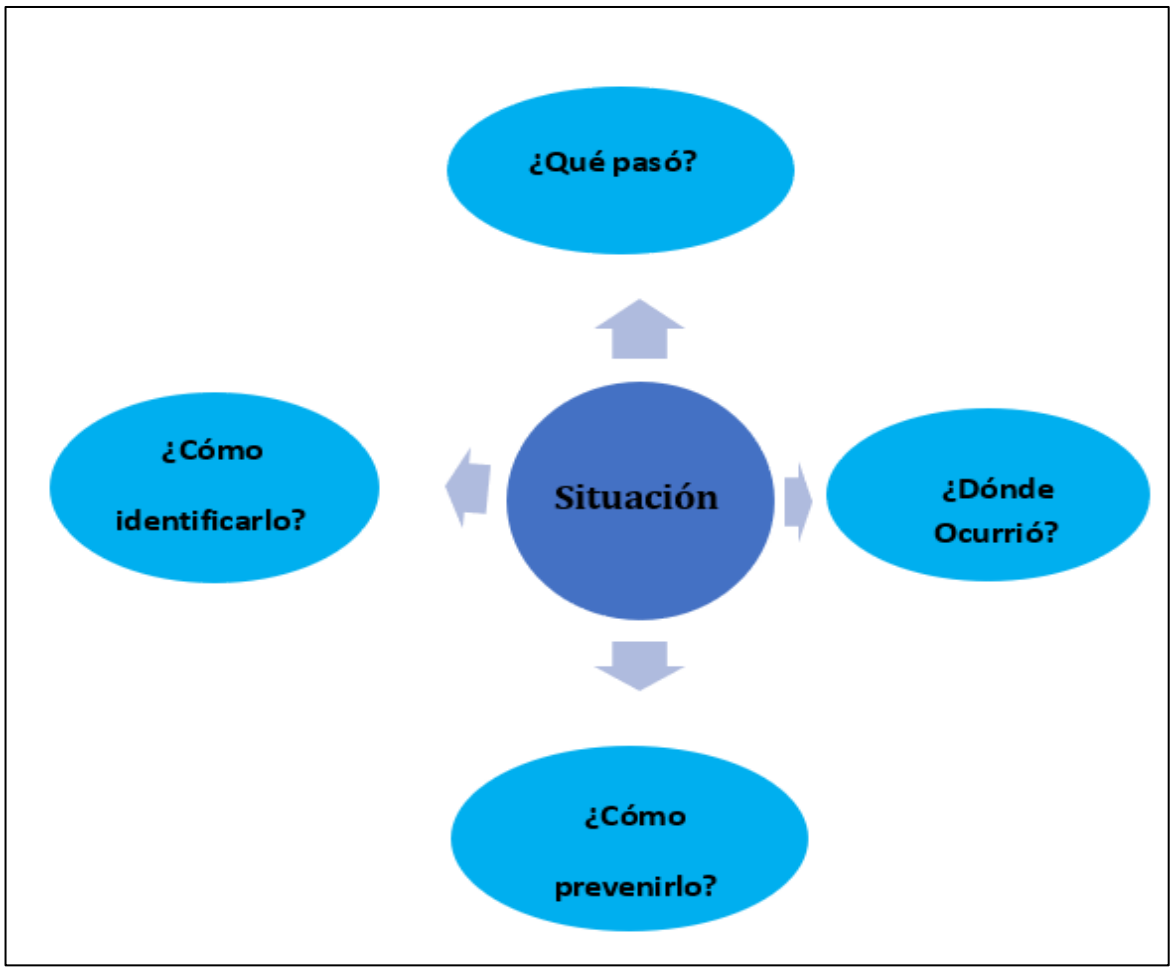


Figura 33. Interrogantes que suceden ante un problema

Fuente: Elaboración propia

3.2.1.3. Búsqueda de condiciones

Frente a esa posible amenaza se diseñó el caso de uso fuerza bruta a cuenta VPN Citrix, con la finalidad de saber qué usuarios tienen intentos fallidos constantes y si es que se debe a un error de contraseña porque ya caducó, intermitencia de internet, acceso no autorizado o si es un posible ataque de fuerza bruta en el cual los atacantes intentan descifrar la contraseña de los usuarios que trabajan en la Entidad Financiera.

Para ello, se contó con 7 días para diseñar el caso de uso en el cual se tuvo que hacer una investigación previa, ya sea buscando información relevante en la documentación del fabricante o filtrando la fuente VPN Citrix NetScaler (citrixns) en

el concentrador del SIEM RSA perteneciente al cliente para buscar logs que contengan atributos como cuenta de usuario, cantidad de conexiones, actividad de usuario (logueos fallidos), tiempo, plataforma de detección, IP's participantes, en base a ello crear las condiciones para que cumpla la lógica del caso de uso propuesto.

En la Figura 34 se observa que los logueos fallidos "user.activity.failed logins" de los usuarios se encuentran en el atributo "nombre de categoría de evento" con 431 eventos.

Figura 34. Buscando condiciones para la lógica del caso de uso

Fuente: Elaboración propia

En la Figura 35 podemos observar un log proveniente de la fuente VPN Citrix NetScaler(citrixns) donde se observa la fecha, inicio de sesión fallida del usuario scastillof, su IP y la acción que tomo VPN Citrix NetScaler, de ese modo, es como va buscando información para crear las condiciones de la lógica del caso de uso.

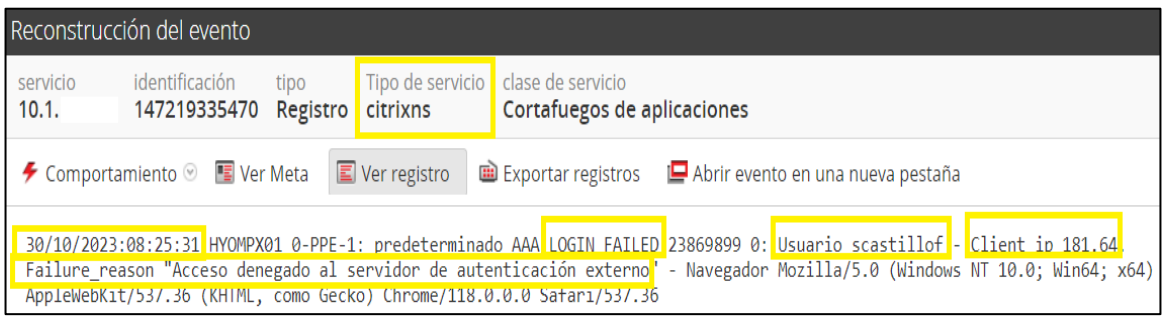


Figura 35. Logs fallidos de VPN Citrix NetScaler (citrixns)

Fuente: Elaboración propia

Asimismo, si existen atributos que no están parseados en el concentrador y se necesita para crear la lógica del caso de uso, entonces se realiza el parseo del atributo, generalmente mediante el sotware LPT, pero para este caso no se tuvo que recurrir, ya que los atributos que se necesitó (usuario de destino, nombre de categoria de evento actividad, IP's y hora) se encontraban parseados, como se observa en la Figura 36.

Figura 36. Atributos necesarios para el caso de uso

Fuente: Elaboración propia

3.2.1.4. Alcance y condiciones de la lógica del caso de uso

Una vez realizado se definió el alcance y las condiciones que contemplaría la lógica del caso de uso fuerza bruta a cuenta VPN Citrix, que posteriormente se usó para configurar, estos fueron:

Nombre del caso uso:

SS-PE-Entidad Financiera-CU-FUERZA BRUTA A CUENTA VPN CITRIX

Descripción del caso de uso:

Este caso de uso se activa cuando existen 10 intentos de login fallidos hacia un usuario de Citrix, en un periodo de 5 minutos.

Condiciones del caso de uso:

Tipo de dispositivo:

- Cuando el campo device.type es igual a 'citrixns'

Actividad del usuario de destino:

- Cuando el campo event.cat.name es igual a 'user. activity.failed logins'

Agrupación:

- Agrupación de 10 a más eventos user.dst en 5 minutos.

Supresión:

- Supresión por user.dst por un periodo de 8 horas.

Funcionamiento:

Si en la fuente de eventos 'citrixns', se registran 10 o más eventos de intentos fallidos de inicio de sesión hacia usuarios de destino (user.dst), dentro de un lapso de 5 minutos y agrupados por usuarios de destino (user.dst), se activará el caso de uso fuerza bruta a cuenta VPN Citrix. Sin embargo, se activará solo una vez cada 8 horas si se trata del mismo usuario de destino(user.dst), debido a la supresión configurada.

Es preciso mencionar que, la cantidad asignada de 10 intentos de inicio de sesiones fallidas de usuarios y el tiempo de duración de 5 minutos para activarse la alerta, se ha considerado siguiendo los estándares del fabricante SIEM RSA y, de acuerdo a ello, la empresa de SecureSoft adapta y adecúa el caso de uso en coordinación con el cliente. Asimismo, para definir la cantidad y el tiempo se recurre a los logs que envía la fuente de eventos citrixns.

3.2.1.5. Diagrama de flujo del caso de uso

Para un mejor entendimiento del caso uso se realizó un diagrama de flujo de las condiciones de la lógica del caso de uso fuerza bruta a cuenta VPN Citrix, como se observa en la Figura 37.

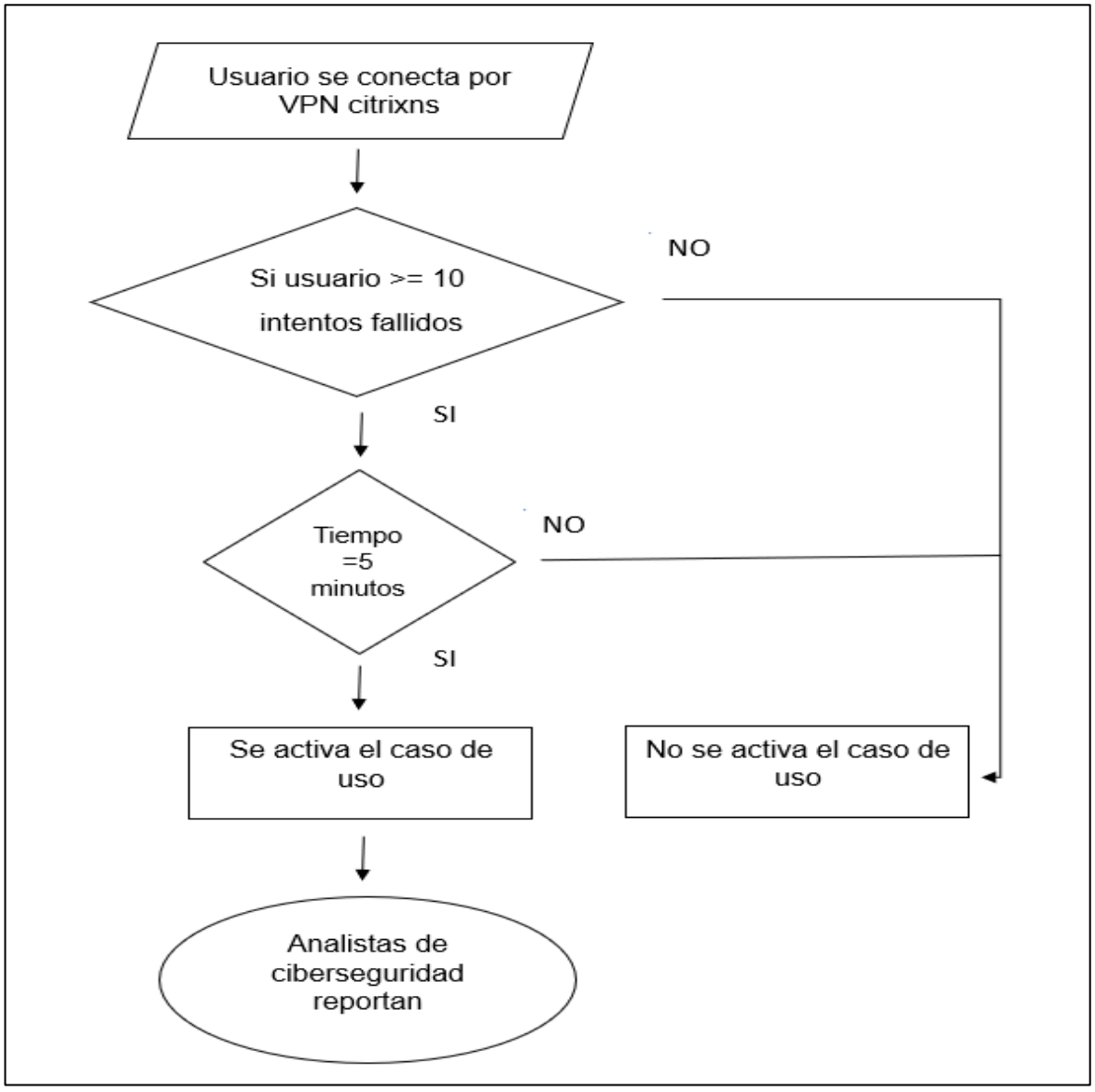


Figura 37. Diagrama de flujo del caso de uso fuerza bruta a cuenta VPN CITRIX
Fuente: Elaboración propia

3.2.2. Etapa de configuración

En esta etapa, se tuvo 3 días hábiles para realizar la configuración con las condiciones de la lógica del caso de uso fuerza bruta a cuenta VPN Citrix.

3.2.2.1. Replicar condiciones de la lógica en el concentrador

Antes de configurar se tuvo que replicar las condiciones del caso uso en la plataforma SIEM RSA para validar que haya eventos que cumplan con la lógica del caso de uso descrito:

Paso 1:

Nos dirigimos a la pestaña investigar > navegar > concentrador de la Entidad Financiera y el primer filtro que se colocó fue que el tipo de dispositivo (device. type) sea igual a citrixns.

En la Figura 38 podemos observar que en 6 minutos la fuente de eventos citrixns envió 5766 eventos y por cada segundo estuvo enviando un promedio de 900 eventos.

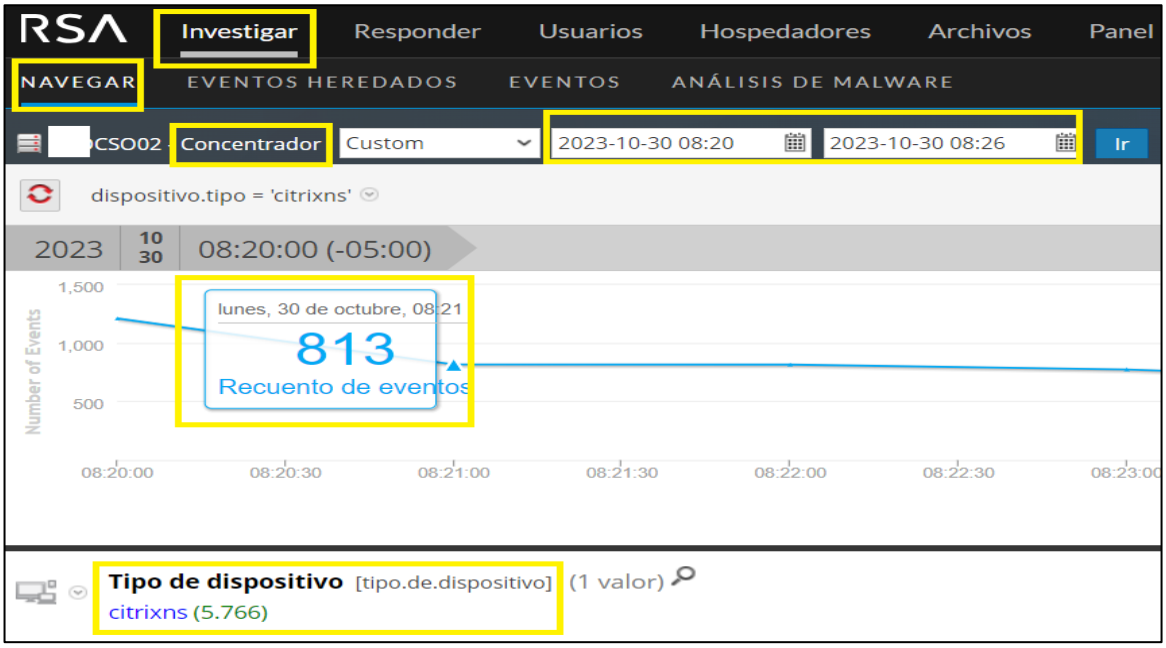


Figura 38. Búsqueda de eventos de VPN Citrix NetScaler en SIEM RSA
Fuente: Elaboración propia

PASO 2:

Como se observa en la Figura 39, el segundo filtro que se colocó fue que el nombre de categoria de evento (event.cat.name) sea igual a usuario.actividad.inicios de sesión fallidos (user.activity.failed logins), validando que también hay eventos.

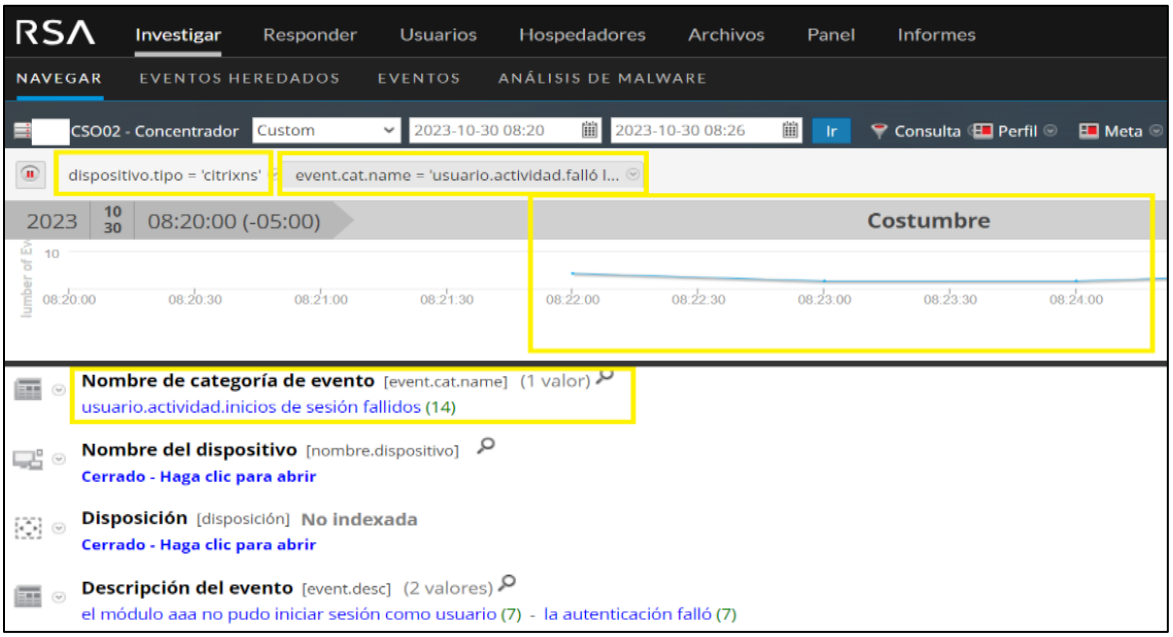


Figura 39. Eventos de logueos fallidos
Fuente: Elaboración propia

PASO 3:

La tercera condición es que en 5 minutos haya 10 o más eventos por usuario de destino (user.dst); así mismo, que se encuentre agrupado con la finalidad de que el caso de uso pueda funcionar y llegue a activarse, caso contrario el caso de uso no se activará.

En la Figura 40 se observa que el 30/10/23 entre las 8:22 AM - 8:26 AM, el usuario destino scastillof tuvo 14 intentos de conexión fallida.

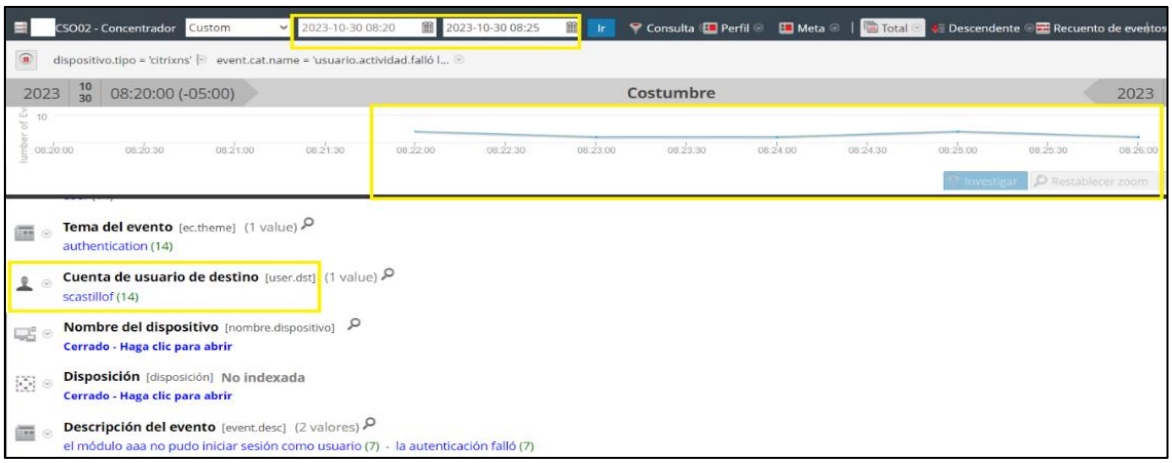


Figura 40. Usuario con intentos de logueos fallidos mayores a 10 eventos

Fuente: Elaboración propia

PASO 4:

La cuarta condición es que haya supresión por usuario de destino (user.dst), con la finalidad de activar el caso de uso una vez cada 8 horas para un mismo usuario de destino; caso contrario, podría estar activándose varias veces durante el día, por lo que reduciría la visibilidad de los demás casos de uso que se encuentran en producción cuando se activan. Esta supresión se configura durante la configuración del caso de uso, y los detalles se proporcionarán más adelante.

3.2.2.2. Configuración en EPL

SIEM RSA para la configuración de casos de uso utiliza el lenguaje de procesamiento de eventos (EPL) que es similar a SQL, puesto que se utilizan parámetros.

La siguiente Tabla describe los parámetros que se utiliza para configurar un caso de uso en SIEM RSA.

Tabla 3

Parámetros que se utiliza para configurar un caso de uso

Parámetro	Descripción
Operador	Es, no es, o, y, no es nulo, es mayor que (>), es mayor o igual a (>=), es menor que (<), es menor o igual a (<=), es uno de, no es uno de, contiene, no contiene, empieza con, termina con.
¿Ignorar caso?	Cuando se elige la opción 'Ignorar mayúsculas y minúsculas', la consulta interpreta todo el texto de la cadena como minúsculas. Esto garantiza que una regla destinada a encontrar al usuario 'Johnson' se activará si el evento contiene 'johnson', 'JOHNSON' o 'JoHnSoN.

Fuente: Elaboración propia

Paso 1:

Para configurar el caso de uso nos dirigimos a la pestaña configurar > reglas de la ESA > normas > biblioteca de reglas >EPL avanzado como se muestra en la Figura 41.

Figura 41. Vista de reglas de la ESA

Fuente: Elaboración propia

Paso 2:

Después de presionar en EPL avanzado, se abrió la pestaña “nueva regla EPL avanzada” y se completó los siguientes campos, como se observa en la Figura 42.

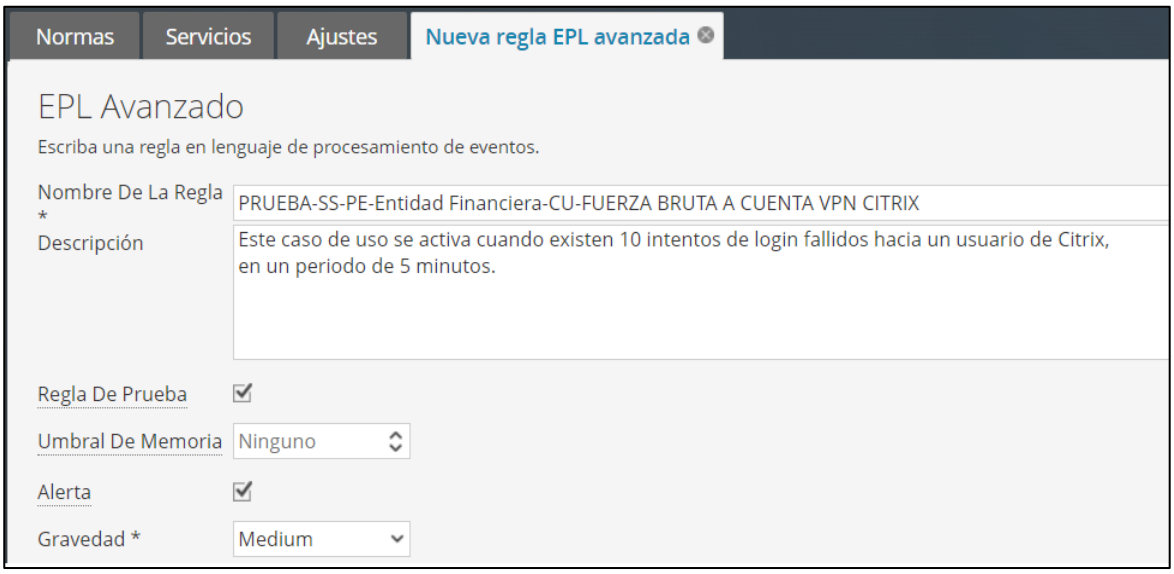


Figura 42. Llenado de campos en EPL avanzado

Fuente: Elaboración propia

- En nombre de la regla se colocó el nombre del caso de uso FUERZA BRUTA A CUENTA VPN CITRIX, acompañado de ciertos parámetros establecidos en conjunto con la Entidad Financiera, como se observa en la Figura 43.

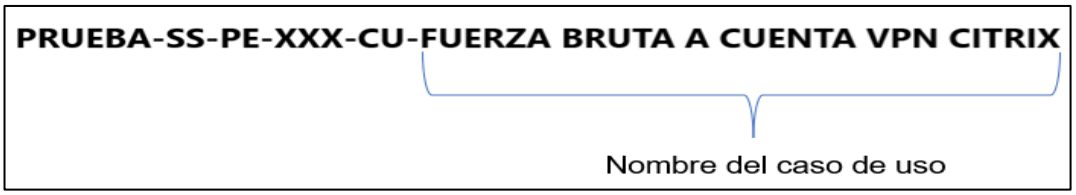


Figura 43. Nombre del caso de uso y parámetros
Fuente: Elaboración Propia

SS= Empresa que realiza la configuración del caso de uso (SecureSoft)

PE=País que se encuentra la Entidad Financiera

XXX=Nombre de la Entidad Financiera

CU=Abreviación del caso de uso

PRUEBA=Cuando el caso de uso aún no está en producción se coloca prueba

- En descripción se colocó una pequeña descripción referente al caso de uso.
- En regla de prueba seleccionamos con sheft.
- En umbral de memoria se colocó ninguno, para que su memoria nunca llegue al máximo y el caso de uso pueda funcionar sin ningún problema.
- En Alerta se marcó un sheft, siempre tiene que estar marcado, caso contrario el caso de uso no se activará cuando cumpla las condiciones de la lógica.
- En gravedad existen 4 niveles: bajo, medio, alto y crítico; para este caso de uso se seleccionó medio, tras acordarse conjuntamente con la Entidad Financiera como la opción más adecuada.

Paso 3:

Después de llenar los campos nos dirigimos a consulta como se muestra en la Figura 44, donde se colocaron las condiciones de la lógica del caso de uso fuerza bruta a cuenta VPN Citrix:

1. Cuando el campo device.type es igual a citrixns
2. Cuando el campo event.cat.name es igual a user.activity.failed logins
3. Agrupación de 10 a más eventos user.dst en 5 minutos.
4. Supresión por user.dst por un periodo de 8 horas.

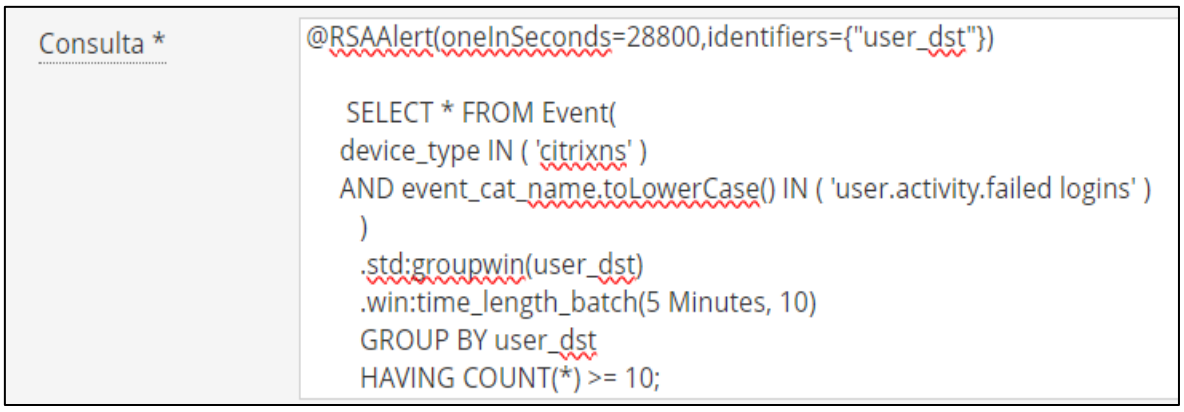


Figura 44. Configuración del caso de uso mediante condiciones

Fuente: Elaboración propia

En la Tabla 4 se detalla el significado de cada condición configurada en el lenguaje EPL (Lenguaje de procesamiento de eventos).

Tabla 4

Explicación del caso de uso

CONDICIONES	SIGNIFICADO
@RSAAlert(oneInSeconds=28800,identifiers={"user_dst"})	El caso de uso se activará cada 8 horas (28800/3600), porque tiene una supresión por usuario destino (user.dst).
SELECT * FROM Event (device_type IN ('citrixns')	Indica que la fuente de eventos citrixns (VPN Citrix NetScaler), será el encargado de suministrar eventos al caso de uso.
AND event_cat_name.toLowerCase() IN ('user.activity.failed logins'))	Indica la actividad que realizaron los usuarios (Intentos de conexiones fallidas) al conectarse mediante VPN Citrix NetScaler.
std:groupwin(user_dst)	Indica la agrupación
win:time_length_batch(5 Minutes, 10)	Indica que en 5 minutos debería haber 10 eventos por usuario destino.
GROUP BY user_dst	agrupación por usuario destino

HAVING COUNT(*) >= 10;	Indica la cantidad de eventos que necesita el caso de uso para activarse

Fuente: Elaboración propia

Paso 4:

Después, nos dirigimos a la sección de notificaciones para añadir la dirección de correo electrónico de monitoreo de SecureSoft. Esto permitirá recibir una notificación inmediata cuando el caso de uso se active, agilizando así su análisis y facilitando el envío rápido hacia el cliente para su revisión, como se visualiza en la Figura 45.

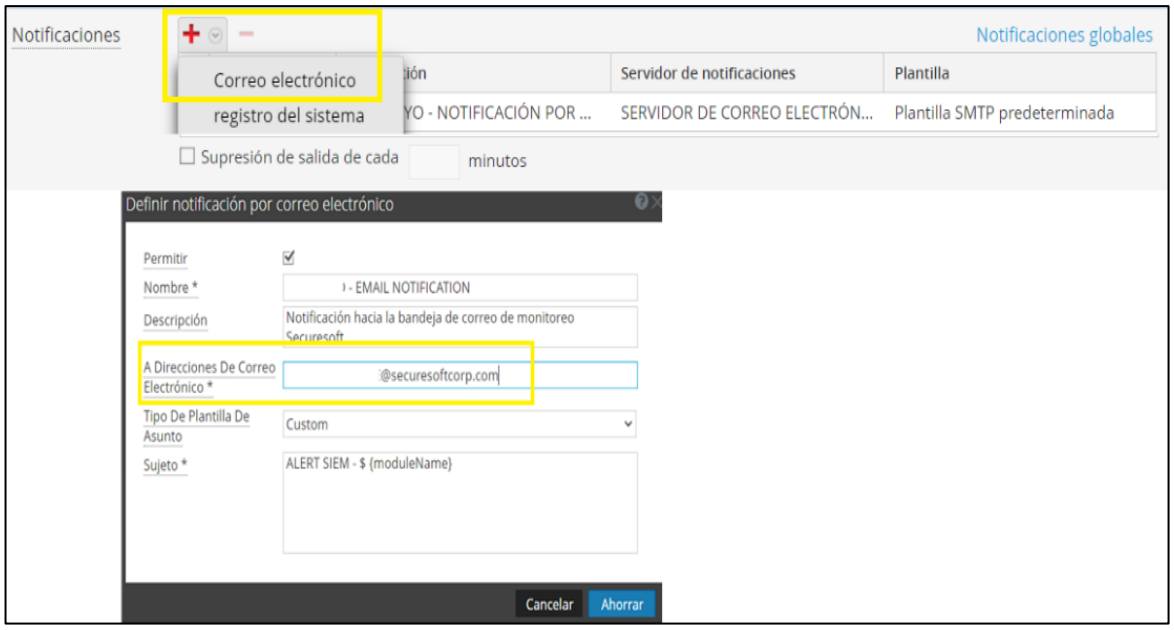


Figura 45. Notificación de alertas mediante correo

Fuente: Elaboración propia

Paso 5:

Después de haber completado todos los campos se procedió a guardar presionando “ahorrar”, como se observa en la Figura 46.

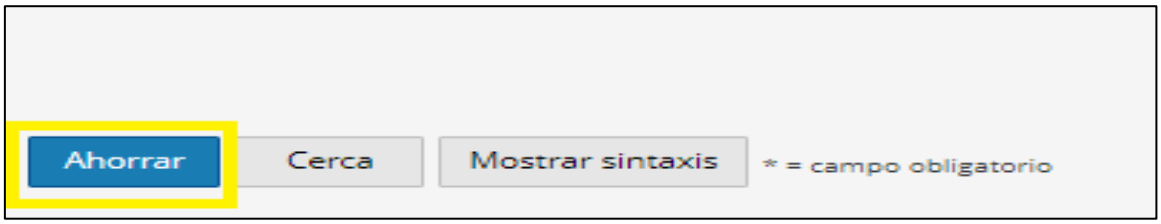


Figura 46. Guardando la configuración realizada

Fuente: Elaboración propia

Paso 6:

Una vez finalizada la configuración, el caso de uso se almacenó en la biblioteca de reglas, procediendo agregar a la ubicación donde se encuentran los demás casos de uso de la Entidad Financiera, tal como se ilustra en la Figura 47.

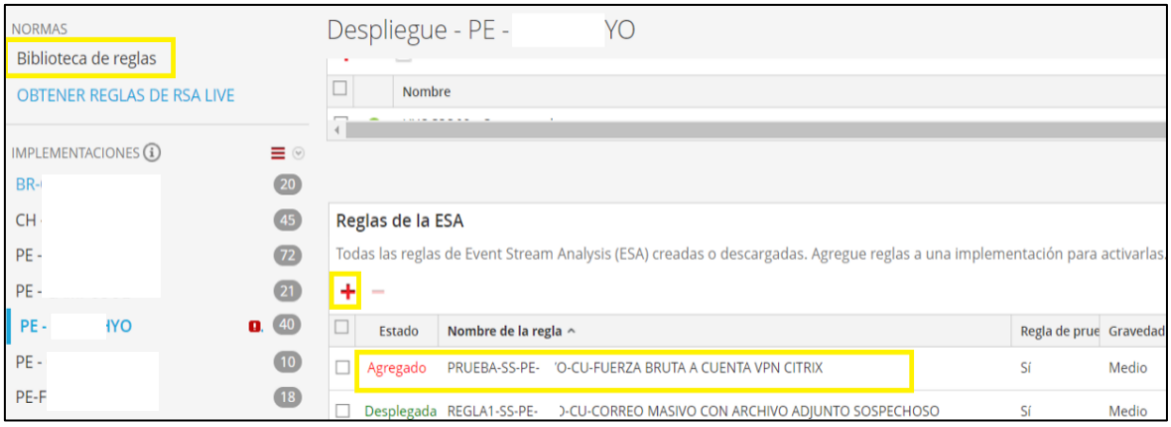


Figura 47. Habilitación del caso de uso en el ESA

Fuente: Elaboración propia

PASO 7:

Posteriormente se presionó en “implementar ahora”, este paso implica habilitar el caso de uso, como se observa en la Figura 48.

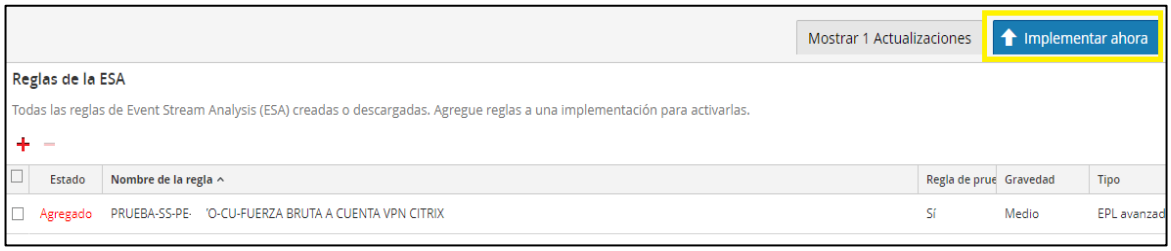


Figura 48. Agregando nuevo caso de uso de la Entidad Financiera

Fuente: Elaboración propia

PASO 8:

Finalmente, como se observa en la Figura 49 el caso de uso se encuentra desplegado y habilitado para que cuando cumpla las condiciones de la lógica pueda activarse.

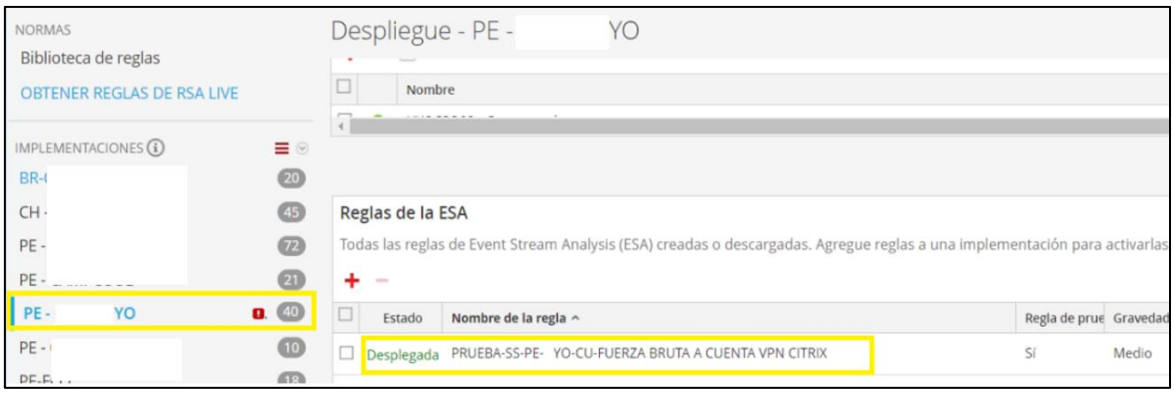


Figura 49. Despliegue del caso de uso

Fuente: Elaboración propia

3.2.3. Etapa de validación

Una vez que el caso de uso fue desplegado, las pruebas se realizaron durante 5 días hábiles, es decir, que la prueba del caso de uso denominada PRUEBA-SS-PE-Entidad Financiera-CU-FUERZA BRUTA A CUENTA VPN CITRIX se podrá visualizar en el tablero de alertas del SIEM RSA y también por correo electrónico a la empresa de SecureSoft, sin embargo, aún no se podrá reportar, debido a que en

estos días se verá si hay mucha volumetría con respecto a algún usuario, o si se necesita mejorar en algo, con el fin de que el caso de uso no genere falsos positivos.

Posteriormente, se envió un correo hacia el cliente solicitando aprobación para pasar el caso de uso a producción, debido a que las pruebas fueron satisfactorias y no se tiene ninguna observación, adjuntando el informe de configuración del caso de uso en formato 07.

3.2.4. Etapa de pase a producción

Después de recibir la aprobación del cliente, se procedió a pasar el caso de uso a producción, procediendo a realizar los siguientes pasos en la plataforma SIEM RSA:

PASO 1:

Como se observa en la Figura 50, nos dirigimos a la ruta: configurar>reglas de la esa>normas(reglas)>implementaciones>Entidad Financiera y presionamos el caso de uso PRUEBA-SS-PE-Entidad Financiera-CU-FUERZA BRUTA A CUENTA VPN CITRIX donde se abrirá una pestaña.

Figura 50. Buscar el caso de uso fuerza bruta a cuenta VPN Citrix en SIEM RSA
Fuente: Elaboración propia

Paso 2:

se retiró la palabra PRUEBA, quedándose el caso de uso como: SS-PE-Entidad Financiera-CU-FUERZA BRUTA A CUENTA VPN CITRIX y se guardó los cambios, como se observa en la Figura 51.

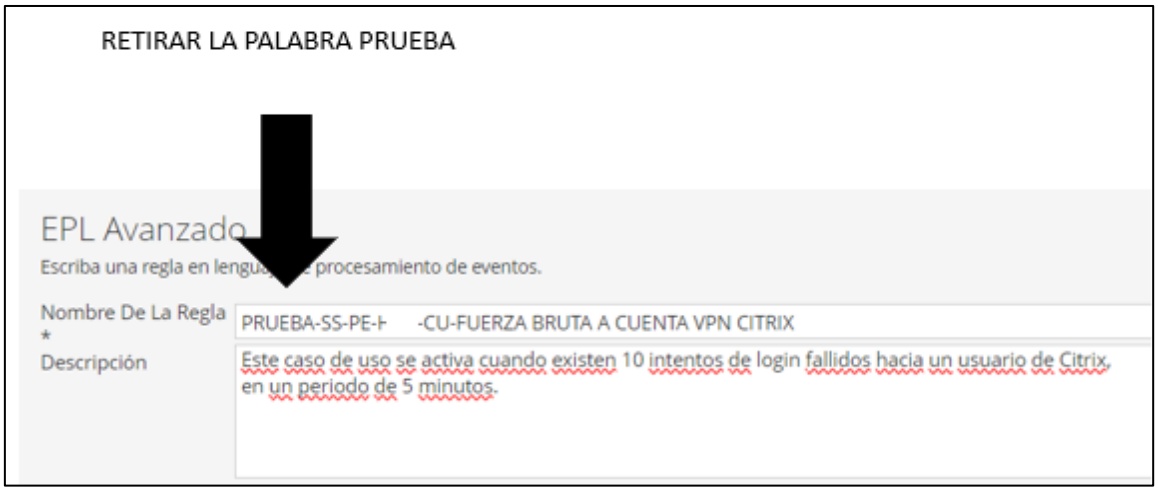


Figura 51. Retiro del caso de uso prueba
Fuente: Elaboración propia

Paso 3:

Después, se tuvo que presionar en implementar ahora, para que se actualicen los cambios realizados en el caso de uso SS-PE-Entidad Financiera-CU-FUERZA BRUTA A CUENTA VPN CITRIX, como se visualiza en la Figura 52.

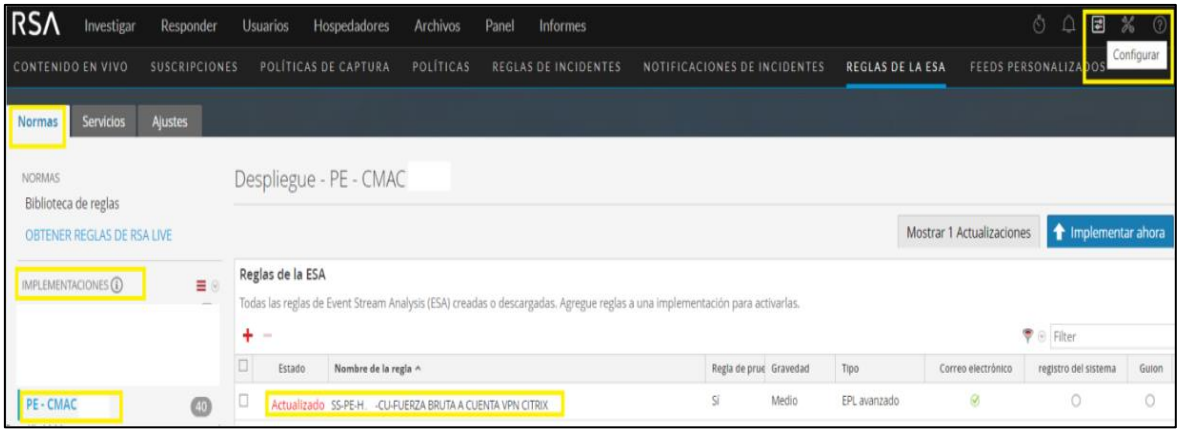


Figura 52. Cambio realizado en el caso de uso
Fuente: Elaboración propia

Paso 4:

Luego de realizar el despliegue, el caso de uso SS-PE-Entidad Financiera-CU-FUERZA BRUTA A CUENTA VPN CITRIX se encuentra en producción, listo para que sea monitoreado por los analistas de ciberseguridad, como se observa en Figura 53; asimismo, se brindó el traspaso de información acerca del caso de uso.

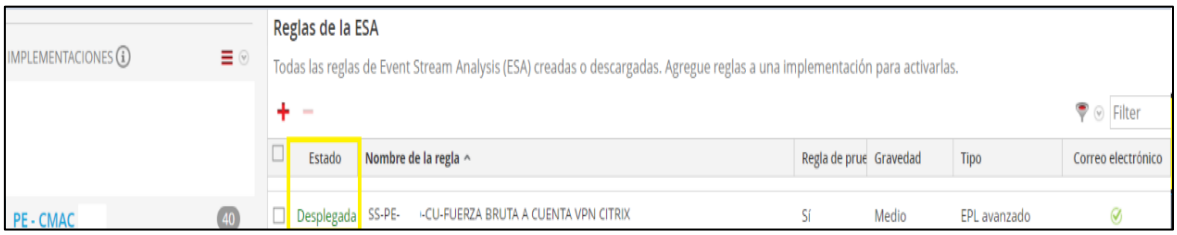


Figura 53. Caso de uso se encuentra desplegado
Fuente: Elaboración propia

3.3. Resultados

Después de realizar la implementación del caso de uso de fuerza bruta a cuenta VPN CITRIX y haber pasado a producción, los analistas de ciberseguridad del área del SOC de Securesoft encargados de monitorear la plataforma SIEM RSA de la Entidad Financiera, lograron detectar a tiempo cuando el caso de uso se activaba reportando inmediatamente al cliente para que revise lo antes posible debido a que puede ser un ataque de fuerza bruta y la Entidad Financiera podría verse afectada.

Como muestra de que funciona correctamente el caso de uso, se ha seleccionado el período comprendido durante el 26 y el 30 de octubre entre las 18:00 pm y 08:30 am de 2023 para verificar la cantidad de veces que se activó el caso de uso y, en caso de no activarse, identificar las posibles razones detrás de ello.

A. ALERTAS ACTIVADAS

En la Figura 54 se observa que durante el 26 y el 30 de octubre entre las 18:00 pm y 08:30 am de 2023 se registraron 431 intentos fallidos de inicio de sesión por parte de usuarios que se querían conectar mediante VPN Citrix NetScaler hacia la Entidad Financiera. Sin embargo, el caso de uso solo se activó 5 veces, debido que cumplieron con las condiciones de la lógica, siendo los usuarios afectados

Mhuamaniy, uextsistemas04, uextsistemas36 y scastillof. A continuación, se detallará cada alerta activada.

Figura 54. Cantidad de eventos entre el 26 y 30 de octubre de 2023

Fuente: Elaboración propia

ALERTA 1:

INC80632-PE-XXX-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

Activación del caso de uso

En la Figura 55 se observa que el caso de uso se activó el 26 de octubre a las 6:20:47 pm en el SIEM RSA de la Entidad Financiera.

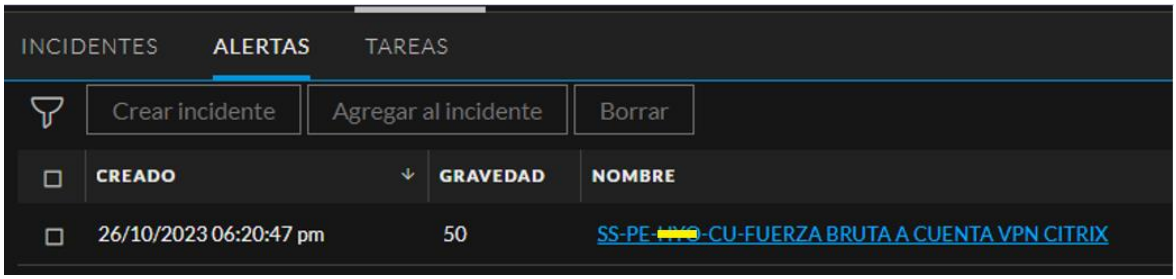


Figura 55. INC80632-PE-XXX-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

Fuente: Elaboración propia

Validación de la alerta

En la Figura 56 se observa que el usuario Mhuamaniy realizo 11 intentos fallidos de inicios de sesión en un rango de 7 minutos.

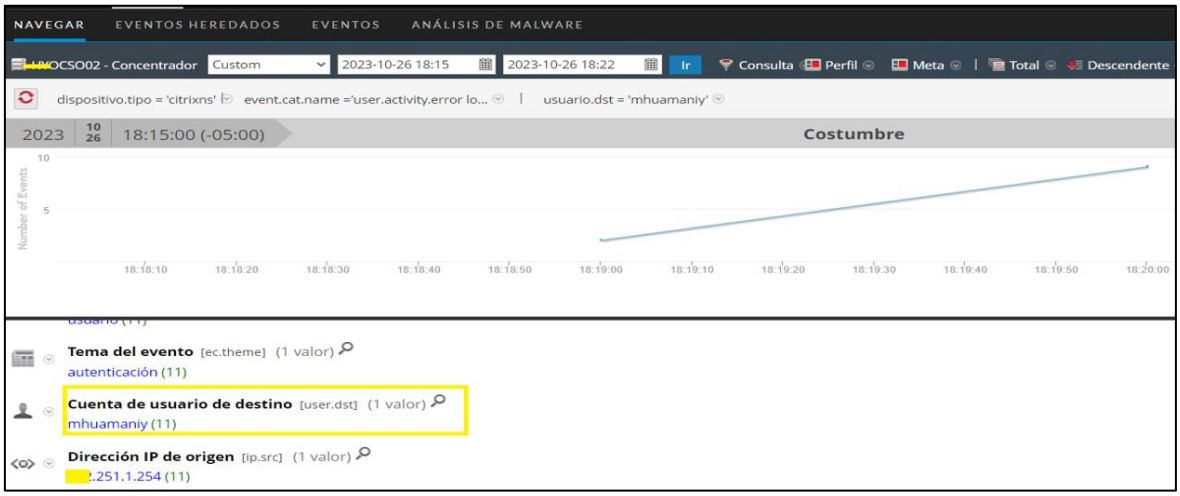


Figura 56. Replicación de la lógica del caso uso para el usuario Mhuamaniy
Fuente: Elaboración propia

En la Tabla 5, se observa que el usuario Mhuamaniy intentó conectarse 11 veces entre las 18:19:54 pm y 18:20:52 pm, en un rango de 58 segundos. Las condiciones de la lógica para activar el caso de uso (10 intentos o más por inicio de sesión fallida de un usuario destino en un rango de 5 minutos) se cumplieron a los 50 segundos (18:19:54-18:20:44), activándose el caso de uso a las 6:20:47 pm, 3 segundos después de cumplir la lógica del caso de uso.

Tabla 5

Eventos de logueos fallidos del usuario Mhuamaniy-26/10/2023

HORA	IP	USUARIO	ACTIVIDAD
18:19:54	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:19:59	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:09	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:17	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:22	X.251.1.254	Mhuamaniy	inicio de sesión fallida

18:20:28	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:33	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:37	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:40	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:44	X.251.1.254	Mhuamaniy	inicio de sesión fallida
18:20:52	X.251.1.254	Mhuamaniy	inicio de sesión fallida

Fuente: Elaboración propia

Respuesta del cliente:

Posterior a la activación del caso de uso, el analista de ciberseguridad reportó hacia la Entidad Financiera mediante el ticket INC80632. El cliente respondió el 27 de octubre indicando que se trató de una actividad legítima realizado por el usuario Mhuamaniy, esta alerta se considera falso positivo debido a que no afecta a la Entidad Financiera, como se visualiza en la Figura 57.

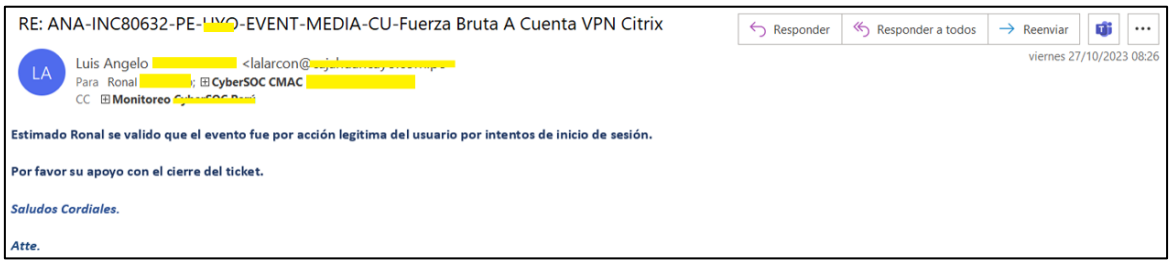


Figura 57. Respuesta del cliente a la alerta reportada- INC80632
Fuente: Elaboración propia

Alerta 2. INC80695-PE-XXX-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

En la Figura 58 se observa que el caso de uso se activó el 27 de octubre a las 07:48:09 am en el SIEM RSA de la Entidad Financiera.

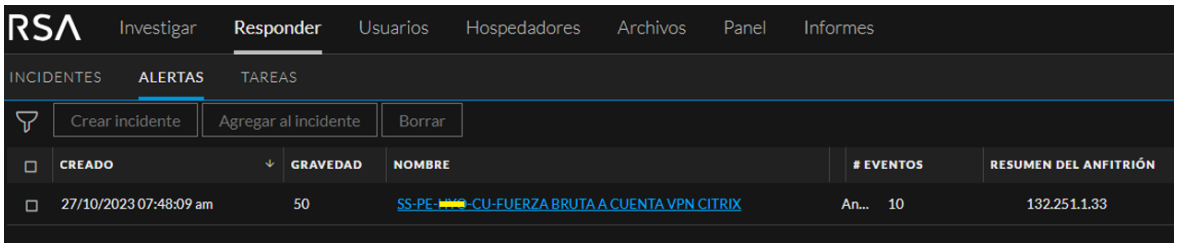


Figura 58. Activación del caso de uso - 27/10/2023

Fuente: Elaboración Propia

Validación de la alerta

En la Figura 59, se observa que el usuario Mhuamaniy realizó 13 intentos fallidos de inicio de sesión al intentar conectarse a la Entidad Financiera a través de VPN Citrix NetScaler.

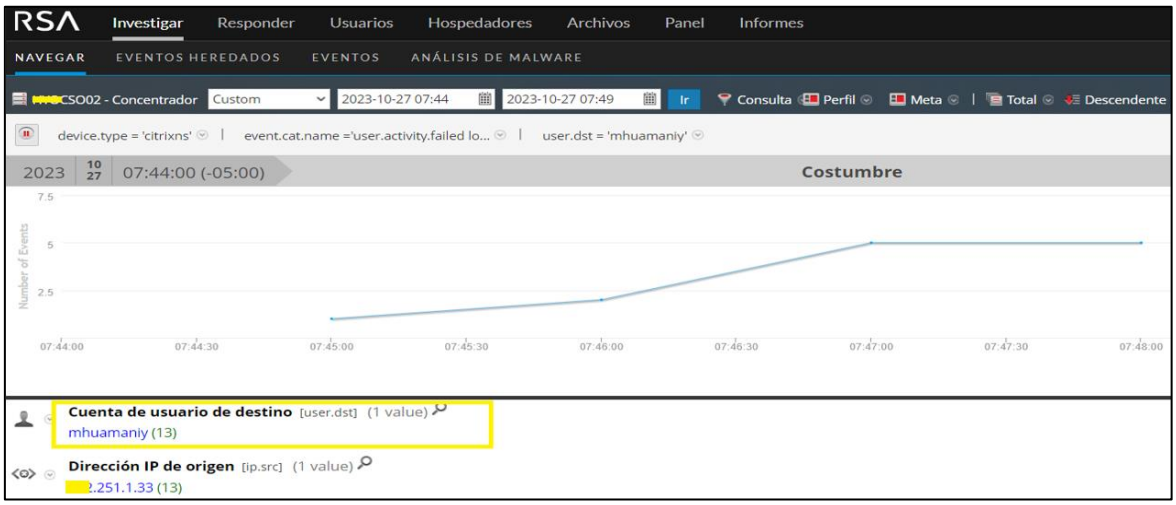


Figura 59. Replicación de la lógica del caso uso para el usuario Mhuamaniy

Fuente: Elaboración Propia

En la Tabla 6, se observa que el usuario Mhuamaniy intentó conectarse 13 veces entre las 07:45:05 am y 07:48:22 am, en un rango de 3 minutos con 17 segundos. Las condiciones de la lógica para activar el caso de uso (10 intentos o más por

inicio de sesión fallida de un usuario destino en un rango de 5 minutos) se cumplieron a los 3 minutos con 2 segundos (07:45:05-07:48:07), activándose el caso de uso a las 07:48:09 am, 2 segundos después de cumplir la lógica del caso de uso.

Tabla 6

Eventos de logueos fallidos del usuario Mhuamaniy-27/10/2023

HORA	IP	USUARIO	ACTIVIDAD
07:45:05	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:46:18	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:46:53	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:47:12	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:47:27	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:47:41	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:47:47	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:47:54	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:48:00	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:48:07	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:48:11	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:48:17	X.251.1.33	Mhuamaniy	inicio de sesión fallida
07:48:22	X.251.1.33	Mhuamaniy	inicio de sesión fallida

Fuente: Elaboración propia

Respuesta del cliente:

Posterior a la activación del caso de uso, el analista de ciberseguridad reportó hacia la Entidad Financiera mediante el ticket INC80695. El cliente respondió el 27 de octubre indicando que se trató de una actividad legítima realizado por el usuario Mhuamaniy, esta alerta se considera falso positivo debido a que no afecta a la Entidad Financiera, como se visualiza en la Figura 60.

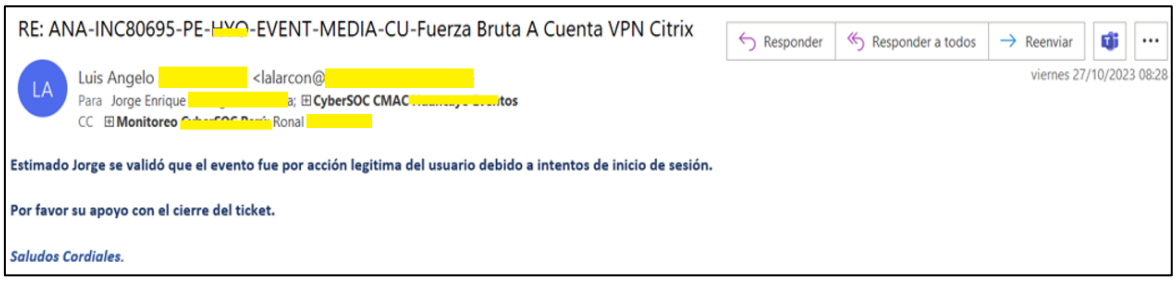


Figura 60. Respuesta del cliente a la alerta reportada- INC80695
Fuente: Elaboración propia

Alerta 3. INC80688-PE-XXX-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

En la Figura 61 se observa que el caso de uso se activó el 27 de octubre a las 08:59:48 am en el SIEM RSA de la Entidad Financiera.

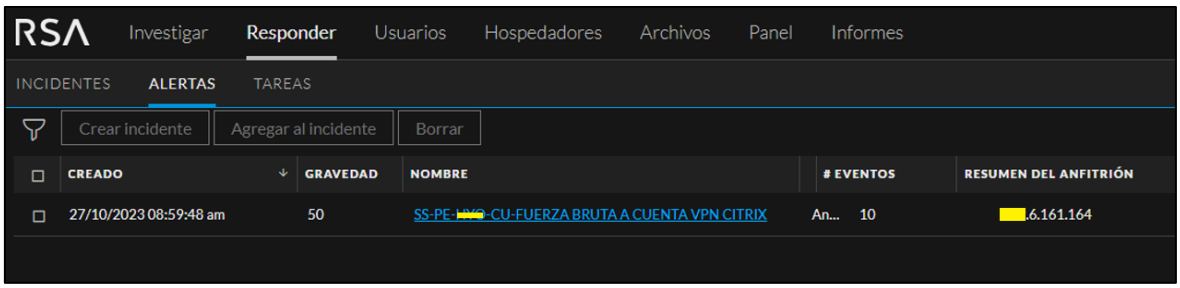


Figura 61. Activación del caso de uso - 27/10/2023 - 08:59:48 AM

Fuente: Elaboración propia

Validación de la alerta

En la Figura 62 se observa que el usuario uextsistemas04 intentó conectarse a la Entidad Financiera mediante VPN Citrix NetScaler realizando 10 intentos de inicio de sesión.

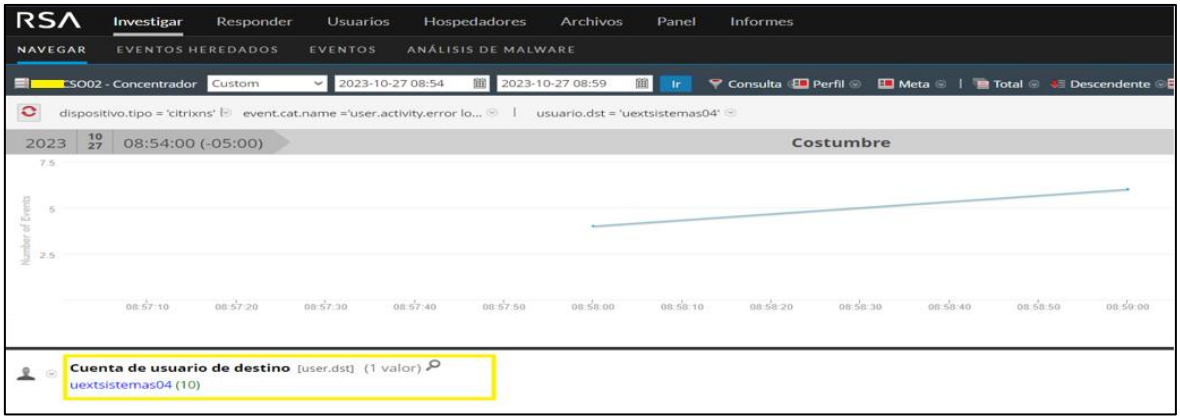


Figura 62. Replicación de la lógica del caso uso para el usuario uextsistemas04
Fuente: Elaboración propia

En la Tabla 7, se observa que el usuario uextsistemas04 intentó conectarse 10 veces entre las 08:58:42 am y 08:59:46 am. Las condiciones de la lógica para activar el caso de uso (10 intentos o más por inicio de sesión fallida de un usuario destino en un rango de 5 minutos) se cumplieron en un minuto con 4 segundos

(08:58:42-08:59:46), activándose el caso de uso a las 08:59:48 am, 2 segundos después de cumplir la lógica del caso de uso.

Tabla 7

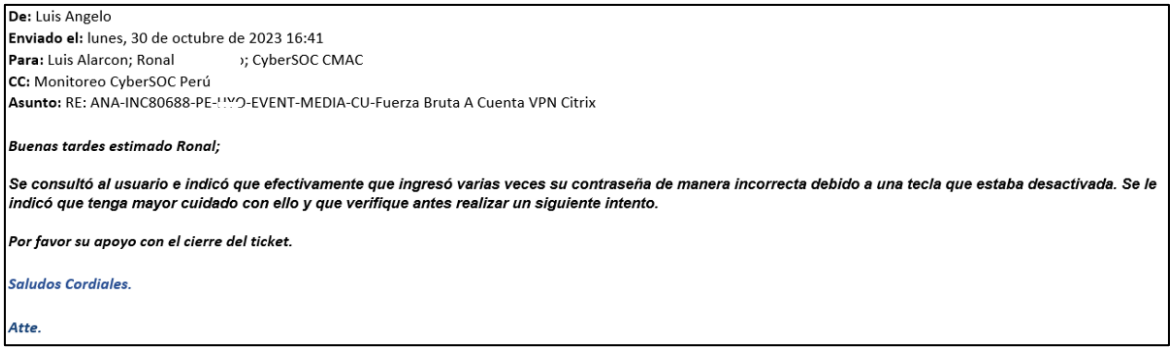
Eventos de logueos fallidos del usuario uextsistemas04

HORA	IP	USUARIO	ACTIVIDAD
08:58:42	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:58:42	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:58:51	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:58:51	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:59:05	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:59:05	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:59:20	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:59:20	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:59:46	X.6.161.164	uextsistemas04	inicio de sesión fallida
08:59:46	X.6.161.164	uextsistemas04	inicio de sesión fallida

Fuente: Elaboración propia

Respuesta del cliente:

Posterior a la activación del caso de uso, el analista de ciberseguridad reportó hacia la Entidad Financiera mediante el ticket INC80688, El cliente respondió el 30 de octubre indicando que el usuario uextsistemas04 había ingresado varias veces su contraseña de manera incorrecta debido a una tecla que estaba desactivada. Asimismo, se le indicó que tenga mayor cuidado con ello y que verifique antes de realizar un siguiente intento, como se observa en la Figura 63.



De: Luis Angelo
Enviado el: lunes, 30 de octubre de 2023 16:41
Para: Luis Alarcon; Ronal ›; CyberSOC CMAC
CC: Monitoreo CyberSOC Perú
Asunto: RE: ANA-INC80688-PE-[illegible]-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

Buenas tardes estimado Ronal;

Se consultó al usuario e indicó que efectivamente que ingresó varias veces su contraseña de manera incorrecta debido a una tecla que estaba desactivada. Se le indicó que tenga mayor cuidado con ello y que verifique antes realizar un siguiente intento.

Por favor su apoyo con el cierre del ticket.

Saludos Cordiales.

Atte.

Figura 63. Respuesta del cliente a la alerta reportada- INC80688

Fuente: Elaboración propia

Alerta 4. INC80779-PE-XXX-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

En la Figura 64 se observa que el caso de uso se activó el 27 de octubre a las 12:53:12 pm en el SIEM RSA de la Entidad Financiera.

Figura 64. Activación del caso de uso - 27/10/2023 - 12:53:12 PM

Fuente: Elaboración propia

Validación de la alerta

En la Figura 65 se observa que el usuario uextsistemas36 intentó conectarse 13 veces a la Entidad Financiera mediante VPN Citrix NetScaler.

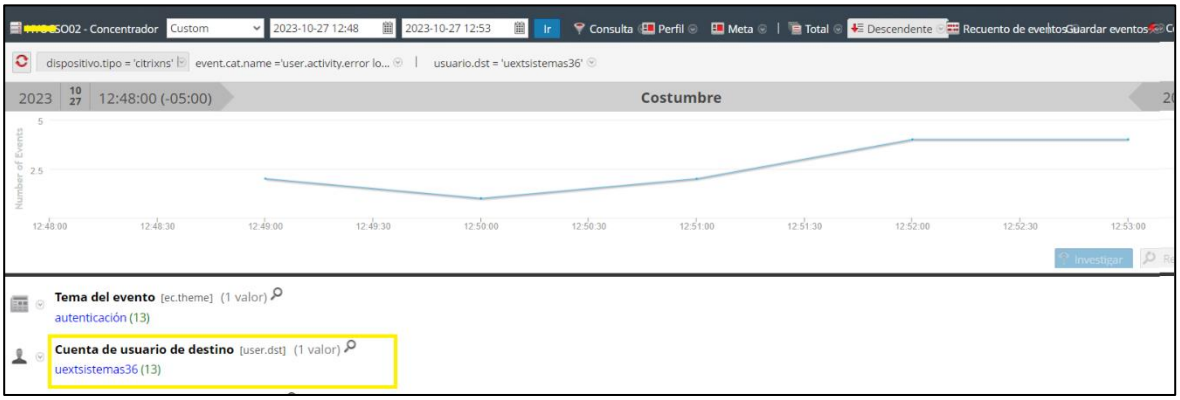


Figura 65. Replicación de la lógica del caso uso para el usuario uextsistemas36

Fuente: Elaboración propia

En la Tabla 8, se observa que el usuario uextsistemas36 intentó conectarse 13 veces entre las 12:49:09 pm y 12:53:22 pm, en un rango de 4 minutos con 13 segundos. Las condiciones de la lógica para activar el caso de uso (10 intentos o más por inicio de sesión fallida de un usuario destino en un rango de 5 minutos) se cumplieron a los cuatro minutos (12:49:09-12:53:09), activándose el caso de uso a las 12:53:12 pm, 3 segundos después de cumplir la lógica del caso de uso.

Tabla 8

Eventos de logueos fallidos del usuario uextsistemas36

HORA	IP	USUARIO	ACTIVIDAD
12:49:09	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:49:29	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:50:12	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:51:49	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:51:49	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:52:10	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:52:10	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:52:50	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:52:50	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:53:09	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:53:09	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:53:22	X.5.56.241	uextsistemas36	inicio de sesión fallida
12:53:22	X.5.56.241	uextsistemas36	inicio de sesión fallida

Fuente: Elaboración propia

Respuesta del cliente:

Posterior a la activación del caso de uso, el analista de ciberseguridad reportó hacia la Entidad Financiera mediante el ticket INC80779. El cliente respondió el 27 de octubre indicando que la IP origen x.5.56.241 fue detectado como maliciosa. Por consiguiente, se tomó la decisión de bloquear preventivamente dicha IP para conexiones entrantes y salientes a nivel del Firewall Perimetral, como se observa en la Figura 66.

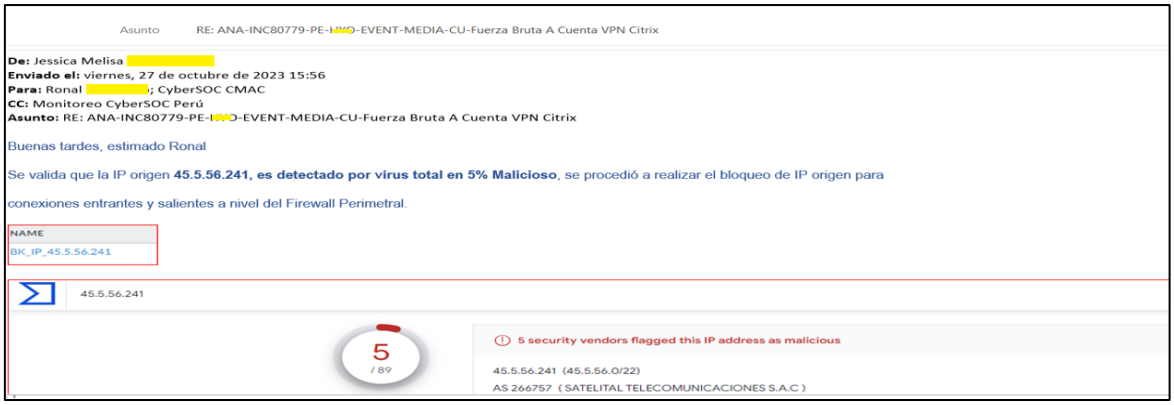


Figura 66. Respuesta del cliente a la alerta reportada- INC80779
Fuente: Elaboración propia

Alerta 5: INC81158-PE-XXX-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

En la Figura 67 se observa que el caso de uso se activó el 30 de octubre a las 08:25:12 am en el SIEM RSA de la Entidad Financiera.

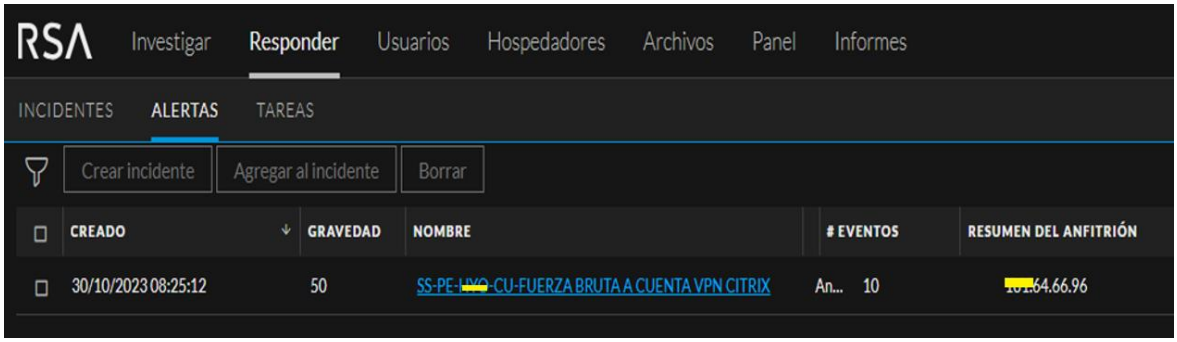


Figura 67. Activación del caso de uso - 30/10/2023 - 08:25:12 AM
Fuente: Elaboración propia

Validación de la alerta

En la Figura 68 se observa que el usuario scastillof intentó conectarse a la Entidad Financiera mediante VPN Citrix NetScaler realizando 12 intentos de inicio de sesión.

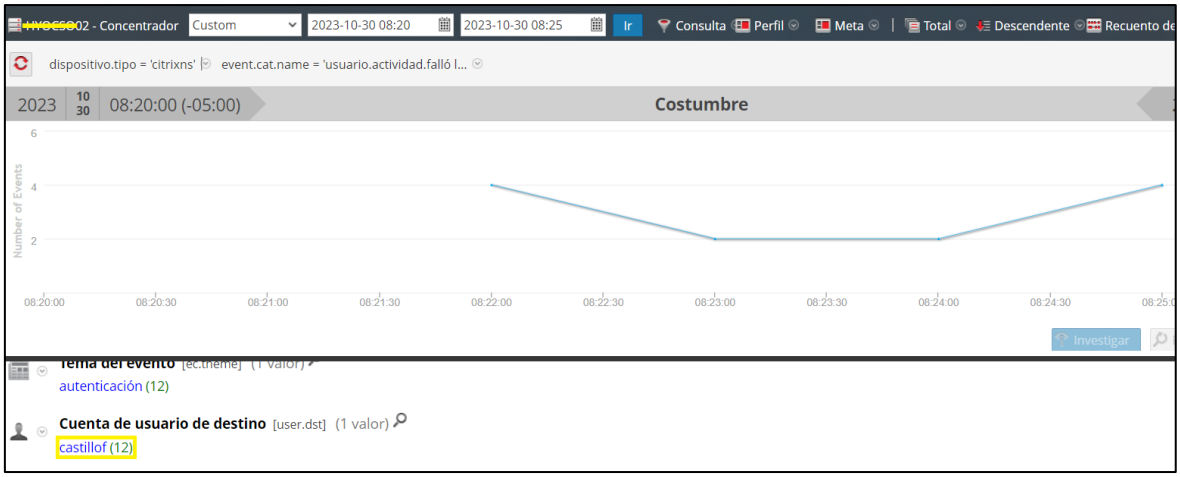


Figura 68. Replicación de la lógica del caso uso para el usuario scastillof
Fuente: Elaboración propia

En la Tabla 9, se observa que el usuario scastillof intentó conectarse 12 veces entre las 08:22:01 am y 08:25:44 am, en un rango de 3 minutos con 43 segundos. Las condiciones de la lógica para activar el caso de uso (10 intentos o más por inicio de sesión fallida de un usuario destino en un rango de 5 minutos) se cumplieron a los tres minutos con ocho segundos (08:22:01-08:25:09), activándose el caso de uso a las 08:25:12 am, 3 segundos después de cumplir la lógica del caso de uso.

Tabla 9

Eventos de logueos fallidos del usuario scastillof

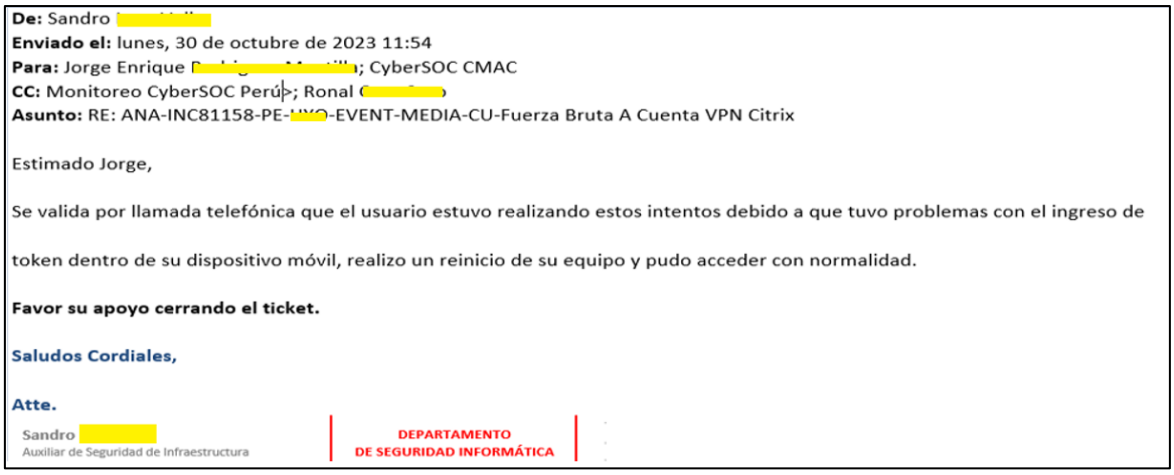
HORA	IP	USUARIO	ACTIVIDAD
08:22:01	X.64.66.96	scastillof	inicio de sesión fallida
08:22:01	X.64.66.96	scastillof	inicio de sesión fallida
08:22:08	X.64.66.96	scastillof	inicio de sesión fallida
08:22:08	X.64.66.96	scastillof	inicio de sesión fallida
08:23:04	X.64.66.96	scastillof	inicio de sesión fallida
08:23:04	X.64.66.96	scastillof	inicio de sesión fallida
08:24:53	X.64.66.96	scastillof	inicio de sesión fallida
08:24:53	X.64.66.96	scastillof	inicio de sesión fallida
08:25:09	X.64.66.96	scastillof	inicio de sesión fallida

08:25:09	X.64.66.96	scastillof	inicio de sesión fallida
08:25:44	X.64.66.96	scastillof	inicio de sesión fallida
08:25:44	X.64.66.96	scastillof	inicio de sesión fallida

Fuente: Elaboración propia

Respuesta del cliente:

Posterior a la activación del caso de uso, el analista de ciberseguridad reportó hacia la Entidad Financiera mediante el ticket INC81158. El cliente respondió el 30 de octubre indicando que el usuario estuvo realizando los intentos debido a que tuvo problemas con el ingreso del token dentro de su dispositivo móvil, posteriormente realizó un reinicio de su equipo y pudo acceder con normalidad, como se observa en la Figura 69.



De: Sandro
Enviado el: lunes, 30 de octubre de 2023 11:54
Para: Jorge Enrique ; CyberSOC CMAC
CC: Monitoreo CyberSOC Perú; Ronal
Asunto: RE: ANA-INC81158-PE- -EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

Estimado Jorge,

Se valida por llamada telefónica que el usuario estuvo realizando estos intentos debido a que tuvo problemas con el ingreso de token dentro de su dispositivo móvil, realizo un reinicio de su equipo y pudo acceder con normalidad.

Favor su apoyo cerrando el ticket.

Saludos Cordiales,

Atte.

Sandro
Auxiliar de Seguridad de Infraestructura

DEPARTAMENTO
DE SEGURIDAD INFORMÁTICA

Figura 69. Respuesta del cliente a la alerta reportada- INC81158

Fuente: Elaboración propia

En la Figura 70 se observa las 5 alertas que se activaron durante el 26 y 30 de octubre entre las 06:20:47 pm y 08:25:12 am de 2023.

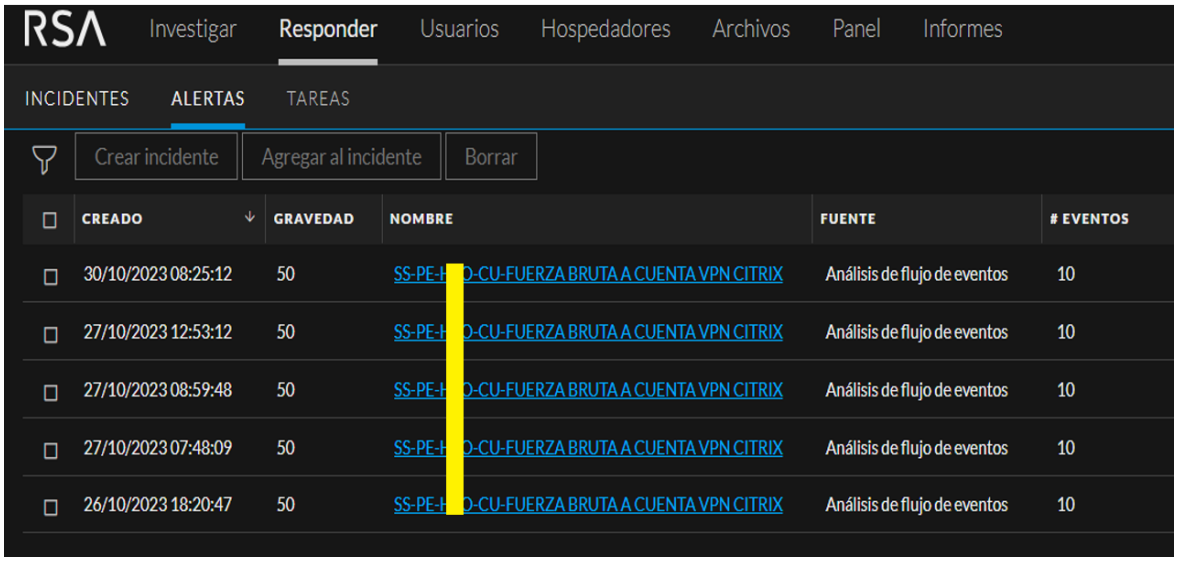


Figura 70. Alertas activadas durante el 26 y 30 de octubre entre las 06:20:47 pm - 08:25:12 am de 2023

Fuente: Elaboración Propia

B. Alerta no activada

Para demostrar cómo el caso de uso fuerza bruta a cuenta VPN Citrix no se activa si no cumple con las condiciones establecidas, las cuales requieren 10 o más intentos de inicio de sesión fallida hacia un usuario que utilice VPN Citrix NetScaler para conectarse hacia la Entidad Financiera en un intervalo de 5 minutos, se examinaron los registros del usuario mcoronel entre el 26 y el 30 de octubre. A continuación, se detalla lo ocurrido con el usuario mcoronel al que se ha tomado como ejemplo.

En la Figura 71 se observa que el usuario mcoronel entre el 26 y 30 de octubre realizó 5 intentos de conexiones fallidas desde 2 IP's diferentes.

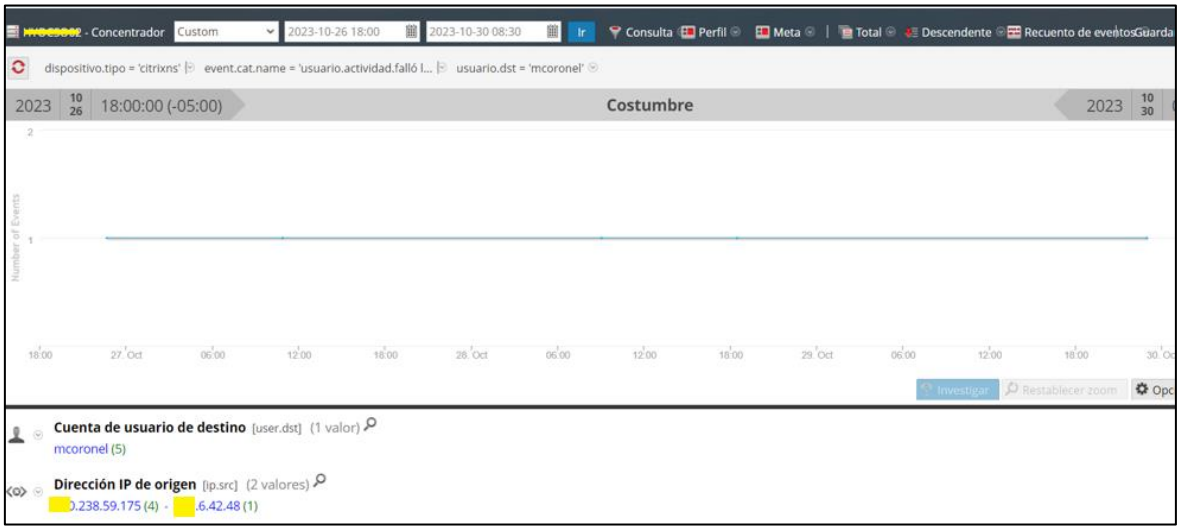


Figura 71. Eventos de mcoronel
Fuente: Elaboración propia

En la Tabla 10 se registra que el usuario mcoronel tuvo una conexión fallida el día 26 y otra el día 27. El día 28 hubo dos intentos fallidos en momentos distintos, mientras que el día 29 se registró una conexión fallida. Sin embargo, el caso no se activó, ya que no cumplió con las condiciones de la lógica estipulada en el caso de uso, la cual requería 10 eventos o más de inicio de sesión fallida por usuario destino en un intervalo de 5 minutos.

Tabla 10

Eventos de logueos fallidos del usuario mcoronel

FECHA	HORA	IP	USUARIO	ACTIVIDAD
26/10/2023	22:38:27	X.238.59.175	mcoronel	inicio de sesión fallida
27/10/2023	10:51:05	X.238.59.175	mcoronel	inicio de sesión fallida
28/10/2023	09:01:39	X.238.59.175	mcoronel	inicio de sesión fallida
28/10/2023	18:27:16	X.238.59.175	mcoronel	inicio de sesión fallida
29/10/2023	22:56:19	X.6.42.48	mcoronel	inicio de sesión fallida

Fuente: Elaboración propia

El análisis anterior fue de un periodo corto, por ello, se ha extendido la investigación para conocer con mayor precisión lo que ocurre en 6 semanas con la implementación del caso de uso en la plataforma SIEM RSA.

A continuación, se detalla la cantidad de alertas activadas y las que no cumplen con las condiciones establecidas (no activadas) a través del caso de uso fuerza bruta a cuenta vpn citrix desde el 21 de setiembre hasta el 31 de octubre para evaluar si se logró cumplir con los objetivos del presente proyecto.

Tabla 11

Resumen de alertas activadas y no activadas desde el 21 de setiembre hasta el 31 de octubre en la plataforma SIEM RSA

FECHA	N° DE USUARIOS	ALERTAS ACTIVADAS	ALERTAS NO ACTIVADAS	TICKET	USUARIO AFECTADO	COMENTARIO
21-Set	54	1	53	INC686511	cmendoza	Actividad legítima del usuario
22-Set	64	0	64	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
23-Set	61	0	61	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.

24-Set	49	0	49	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
25-Set	43	0	43	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
26-Set	24	0	24	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
27-Set	63	1	62	INC690544	uextsistemas19	actividad legítima del usuario uextsistemas19, es una cuenta asignada a un proveedor el cual tuvo problemas para conectarse.

28-Set	45	1	44	INC691523	77429265	Se realizó la validación de la IP X.218.150.25 lo cual no corresponde a ningún proveedor de la Entidad Financiera, de manera preventiva se procedió con el bloqueo de ingreso y salida a nivel del Firewall perimetral.
29-Set	46	1	45	INC691894	uextsistemas08	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.

30-Set	68	0	68	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
1-Oct	34	1	33	INC693003	harmas	Se valida que es una actividad legitima del mismo usuario, quien estuvo realizando varios intentos de acceder a su cuenta CITRIX el día domingo, al no poder acceder reiniciaba el explorador para seguir intentando, sin lograr el acceso.

2-Oct	52	0	52	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
3-Oct	41	0	41	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
4-Oct	29	0	29	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
5-Oct	32	0	32	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.

6-Oct	61	0	61	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
7-Oct	53	0	53	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
8-Oct	57	0	57	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
9-Oct	55	0	55	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.

10-Oct	41	0	41	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
11-Oct	41	1	40	INC700475	sgarciar	Actividad legítima del usuario.
12-Oct	31	0	31	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
13-Oct	58	2	56	INC702284	UDelta_Jpaz	Se originó debido a que la contraseña del usuario expiró.
				INC702497	sgarciar	Realizó intentos de conexión incorrectos por cambio reciente de contraseña.

14-Oct	51	1	50	INC703094	MSOLANOH	Usuario no podía acceder, debido a que su contraseña había expirado un día antes.
15-Oct	55	1	54	INC703606	EVEGA	Actividad legítima del usuario.
16-Oct	48	1	47	INC704134	sgarciar	Logueos fallidos del usuario, debido al bloqueo de su cuenta.
17-Oct	18	0	18	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
18-Oct	54	0	54	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.

19-Oct	71	0	71	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
20-Oct	58	0	58	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
21-Oct	43	0	43	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
22-Oct	29	0	29	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.

23-Oct	58	0	58	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
24-Oct	60	0	60	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
25-Oct	47	0	47	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
26-Oct	36	1	35	INC80632	Mhuamaniy	Acción legítima del usuario por intentos de inicio de sesión.
27-Oct	61	3	58	INC80688	uextsistemas04	Usuario ingresó varias veces su contraseña de manera incorrecta

						debido a una tecla que estaba desactivada. Se le indicó que tenga mayor cuidado con ello y que verifique antes de realizar un siguiente intento.
				INC80695	Mhuamaniy	Acción legítima del usuario debido a intentos de inicio de sesión.
				INC80779	uextsistemas36	Se valida que la IP origen x.5.56.241, es detectado por virus total en 5% como malicioso, se procedió a realizar el bloqueo de IP origen para conexiones entrantes y salientes a nivel del Firewall Perimetral.

28-Oct	37	0	37	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
29-Oct	28	0	28	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
30-Oct	38	1	37	INC81158	scastillof	Usuario estuvo realizando intentos fallidos debido a que tuvo problemas con el ingreso de token dentro de su dispositivo móvil, realizó un reinicio de su equipo y pudo acceder con normalidad.

31-Oct	36	0	36	0	0	No superaron los 10 intentos de inicio de sesión fallida en un lapso de 5 minutos.
Total	1930	16	1914	16 tickets	16 usuarios	16 repuestas por parte del cliente

Fuente: Elaboración propia

En la Tabla 11, se aprecia que de un total de 1930 usuarios que intentaron acceder a la red de la Entidad Financiera mediante VPN Citrix NetScaler desde el 21 setiembre hasta el 31 de octubre, solo 16 usuarios cumplieron con las condiciones de la lógica del caso de uso, alcanzando 10 o más intentos de inicio de sesión fallida en un intervalo de 5 minutos, activando la alerta correspondiente. Los restantes 1914 usuarios no lograron superar los 10 intentos de inicio de sesión fallida en dicho lapso, por lo que no cumplieron con las condiciones establecidas y no se activaron.

Esto quiere decir que el caso de uso implementado funciona y es efectivo, ya que permite detectar a tiempo las intromisiones realizadas por los ciberdelincuentes que intentan conectarse hacia la red de la Entidad Financiera, este hecho hace que el analista de ciberseguridad reporte al cliente la alerta activada para que pueda revisarlo e indicar si son acciones permitidas por los usuarios que trabajan en la Entidad Financiera o si es un ataque de fuerza bruta, de esa manera, se actúa inmediatamente para tomar las medidas respectivas.

Asimismo, de las 16 alertas activadas el cliente indico que todos fueron falsos positivos, sin embargo, el caso de uso implementado evidencia cualquier situación anómala cuando cumple con las condiciones de la lógica del caso de uso. Por otro lado, se evidencia que la infraestructura tecnológica de la Entidad Financiera se encuentra protegida para evitar posibles robos de información confidencial.

Conclusiones

1. Se diseñó adecuadamente un caso de uso de acuerdo a las necesidades y exigencias de la Entidad Financiera, previamente se realizó una investigación en el SIEM RSA donde se encuentra integrado el dispositivo Citrix NetScaler con el nombre citrixns para encontrar en los logs las condiciones de la lógica del caso de uso que cumpla los criterios asignados en su implementación a fin de detectar, proteger y mitigar los ataques cibernéticos.

2. Se logró diseñar con éxito el caso de uso fuerza bruta a cuenta VPN Citrix a través del hallazgo pertinente de las condiciones necesarias de la lógica que comprende la actividad del usuario (intentos fallidos de inicio de sesión), el tipo de dispositivo (citrixns) así como el tiempo y la agrupación del usuario.

3. La implementación exitosa del caso de uso en la plataforma SIEM RSA ha permitido una detección oportuna y una respuesta eficiente ante amenazas de posibles ataques de fuerza bruta a cuentas de usuarios que utilizan VPN Citrix NetScaler para conectarse de manera remota hacia la Entidad Financiera.

4. Se validó la efectividad del caso de uso diseñado realizando pruebas en un periodo corto del 26 al 30 de octubre, de 06:00 pm a 08:30 am, donde el caso de uso se activó 5 veces, en un intervalo de 2 a 3 segundos después de cumplir con las condiciones de la lógica. Así mismo, se verificó que no se activó cuando eran menos de 10 intentos de inicio de sesión por usuario. Posteriormente, se amplió el periodo de validación desde el 21 de setiembre hasta el 31 de octubre, a fin de observar y detectar las alertas que se activaron siendo 16 las que cumplieron la lógica del caso de uso en diferentes días. Esto demuestra que el caso de uso fuerza bruta a cuenta VPN Citrix funciona adecuadamente en el SIEM RSA, ya que detecta oportunamente las intromisiones sospechosas.

5. El funcionamiento del caso de uso implementado en la plataforma SIEM RSA depende de una adecuada configuración, de lo contrario no se activará a pesar de que cumpla con las condiciones de la lógica.

Recomendaciones

1. Se recomienda a la Entidad Financiera continuar invirtiendo en nuevas soluciones de seguridad cibernética para una protección más efectiva. Esto se debe a la constante evolución de las amenazas cibernéticas y la creciente sofisticación de los ciberdelincuentes.

2. Es necesario adecuar los casos de uso de acuerdo con las necesidades específicas de la situación de la empresa, teniendo en cuenta la infraestructura tecnológica y los activos críticos, ya que existen diferentes tipos de SIEM, por ello, es importante evaluar el que mejor se adapta a los requerimientos de la empresa. Esta adaptación permitirá aprovechar al máximo las capacidades del SIEM y garantizar una efectiva seguridad.

3. Realizar un mantenimiento del caso de uso implementado cada cierto tiempo para evaluar su correcto funcionamiento o detectar cambios imprevistos.

4. Se sugiere capacitar al personal que realiza la configuración en la plataforma SIEM RSA para que pueda brindar un óptimo servicio a la Entidad Financiera.

Referencias bibliográficas

Anumol, E. T. (2015). Use of machine learning algorithms with SIEM for attack prediction. en *Intelligent Computing, Communication and Devices: Proceedings of ICCD 2014, Volume 1* (pp. 231-235). Springer India.

Agudelo Castro, B. A., Álvarez Yépez, D. J., Andrade Valdez, J. A., & Escobar Tucta, J. M. (2022). Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft. *(tesis de maestría)*. Universidad Internacional del Ecuador, Quito, Ecuador.

Aguilera López , p. (2010). *Seguridad informática.* Editex.

Canvia. (2023). *Estas son las 10 amenazas cibernéticas más comunes en empresas*. Recuperado el 24 de setiembre de 2023, de Canvia: https://www.canvia.com/amenazas-ciberneticas/

Cisco. (2023). *¿Qué es una VPN? - Red privada virtual*. Recuperado el 27 de setiembre de 2023, de Cisco: https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Cloudflare. (2023). *¿Qué es un WAF?* | *Explicación de Web Application Firewall*. Recuperado el 30 de setiembre de 2023, de Cloudflare: https://www.cloudflare.com/es-es/learning/ddos/glossary/web-application-firewall-waf/

Costas Santos, J. (2010). *Seguridad informática.* RA-MA.

CSIRT. (2023). *Alerta de seguridad de la información.IOC de ransomware en GTD*. Recuperado el 28 de octubre de 2023, de https://www.csirt.gob.cl/noticias/10cnd23-00115-02/

Diario Gestión. (2023). *Ciberataques: 36% de empresas han sufrido vulneración de sus datos*. Recuperado el 27 de octubre de 2023, de https://gestion.pe/tecnologia/ciberataques-36-de-empresas-han-sufrido-

vulneracion-de-sus-datos-ciberataques-vulneracion-de-datos-ia-generativa-noticia/

Escrivá Gascó, G., Romero Serrano, R., Ramada, D., & Onrubia Pérez, R. (2013). *Seguridad Informática.* Macmillan profesional.

Estela Campos, M. A. (2020). Implementación de un security information and event management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera. *(Tesis de Pregrado)*. Univerdidad Tecnologíca del Perú, Lima, Perú.

Fortinet. (2023). *¿Qué es un cortafuegos o firewall de red?* Recuperado el 25 de setiembre de 2023, de https://www.fortinet.com/lat/resources/cyberglossary/firewall#:~:text=Un%20firewall%20es%20una%20soluci%C3%B3n,conjunto%20de%20reglas%20previamente%20programadas.

Fortinet. (2023). *Servicio de seguridad de FortiGuard IPS*. Recuperado el 26 de setiembre de 2023, de https://www.fortinet.com/lat/products/ips#:~:text=Un%20sistema%20de%20prevenci%C3%B3n%20de,existentes%20en%20dispositivos%20y%20servidores.

Gartner. (2022). *Cuadrante Mágico de Gartner para la gestión de eventos e información de seguridad*. Recuperado el 27 de setiembre de 2023, de Gartner: https://www.gartner.es/es/metodologias/magic-quadrant

Gómez Vieites , Á. (2011). *Gestión de incidentes de desguridad infórmatica.* STARBOOK .

IBM. (2020). *Definición de casos de uso*. Recuperado el 28 de setiembre de 2023, de https://www.ibm.com/docs/es/engineering-lifecycle-management-suite/lifecycle-management/7.0.0?topic=requirements-defining-use-cases

IBM. (s.f). *¿Qué es SIEM?* Recuperado el 20 de setiembre de 2023, de https://www.ibm.com/mx-es/topics/siem?mhsrc=ibmsearch_a&mhq=que%20es%20un%20siem

IBM. (s.f). *Centro de operaciones de seguridad (SOC)*. Recuperado el 29 de setiembre de 2023, de https://www.ibm.com/es-es/topics/security-operations-center

López Torres Herrera, L. R. (2019). Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú. *(Tesis de Pregrado)*. Piura, Perú.

Miller , D., Harris , S., Harper, A., VanDyke, S., & Blask, C. (2010). *Security Information and Event Management (SIEM) Implementation.* McGraw Hill Professional.

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Emerald, 20*(4), 248-263. doi:10.1108/09685221211267639

Quintero Martínez, M. I., & Tovar Balderas, S. A. (2019). artículo . *Sistemas de Gestión de Información y Eventos de Seguridad (SIEM)* , 1-9.

Roa Buendía, J. F. (2013). *Seguridad informática.* McGraw-Hill.

RSA NetWitness. (junio de 2019). *Guía de introducción para RSA NetWitness Platform 11.3*. Recuperado el 23 de setiembre de 2023, de RSA Community.

Sánchez Sanz, A. (2019). Implantación de Qradar en un entorno genérico multi-cliente para SOC. *(tesis de maestría)*. Universidad Politécnica de Valencia, Valencia, España.

SecureSoft. (2023). Obtenido de https://www.securesoftcorp.com/

Trend Micro. (2023). *¿Qué es EDR?* Recuperado el 29 de setiembre de 2013, de https://www.trendmicro.com/es_es/what-is/xdr/edr.html

Vasquez Barzola, W. F. (2023). Implementación de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera. *(Tesis de Pregrado)*. Universidad Nacional Mayor de San Marcos, Lima, Perú.

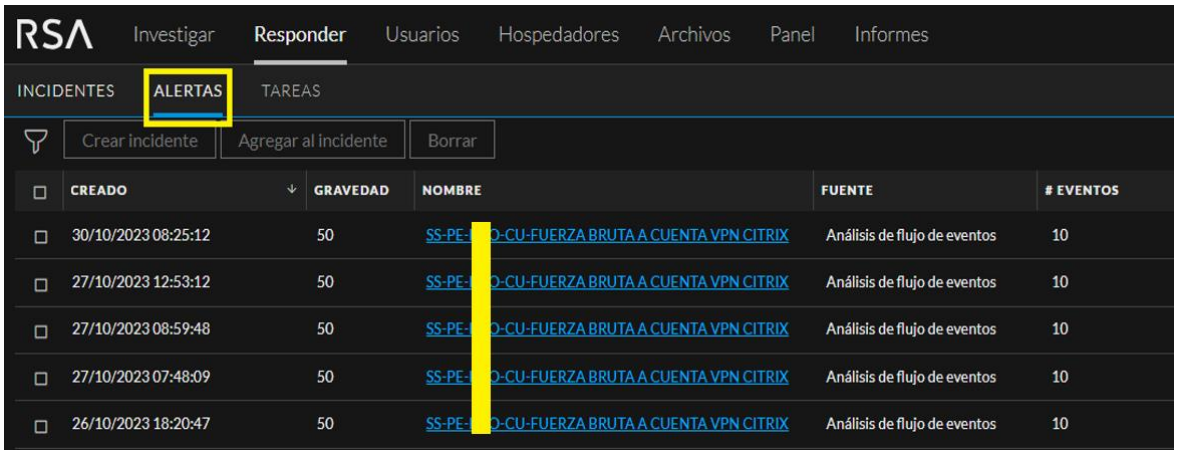
Williams, A., & Nicolett, M. (2005). *Improve IT Security with Vulnerability Management.* Gartner ID, (G00127481).

ANEXOS

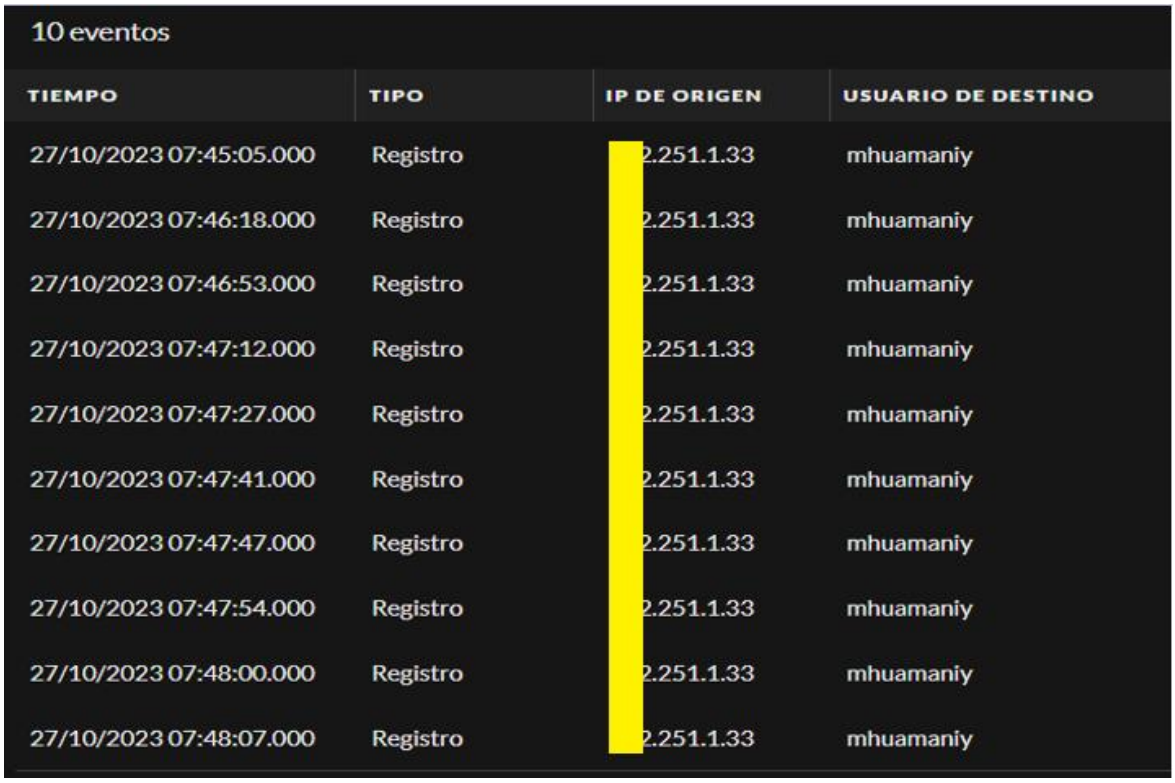
Anexo 1. Cronograma del diseño e implementación del caso de uso fuerza bruta a cuenta VPN Citrix

Cronograma																										
ACTIVIDAD	Fecha		Mayo																							
	INICIO	FIN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Integración de fuente	1/05/2023	10/05/2023																									
Diseño	11/05/2023	17/05/2023																									
Configuración	17/05/2023	19/05/2023																									
Validación	20/05/2023	24/05/2023																									
Pase a producción	25/05/2023	25/05/2023																									

Anexo 2. Activación de alertas del caso de uso fuerza bruta a cuenta VPN Citrix en la vista de alertas



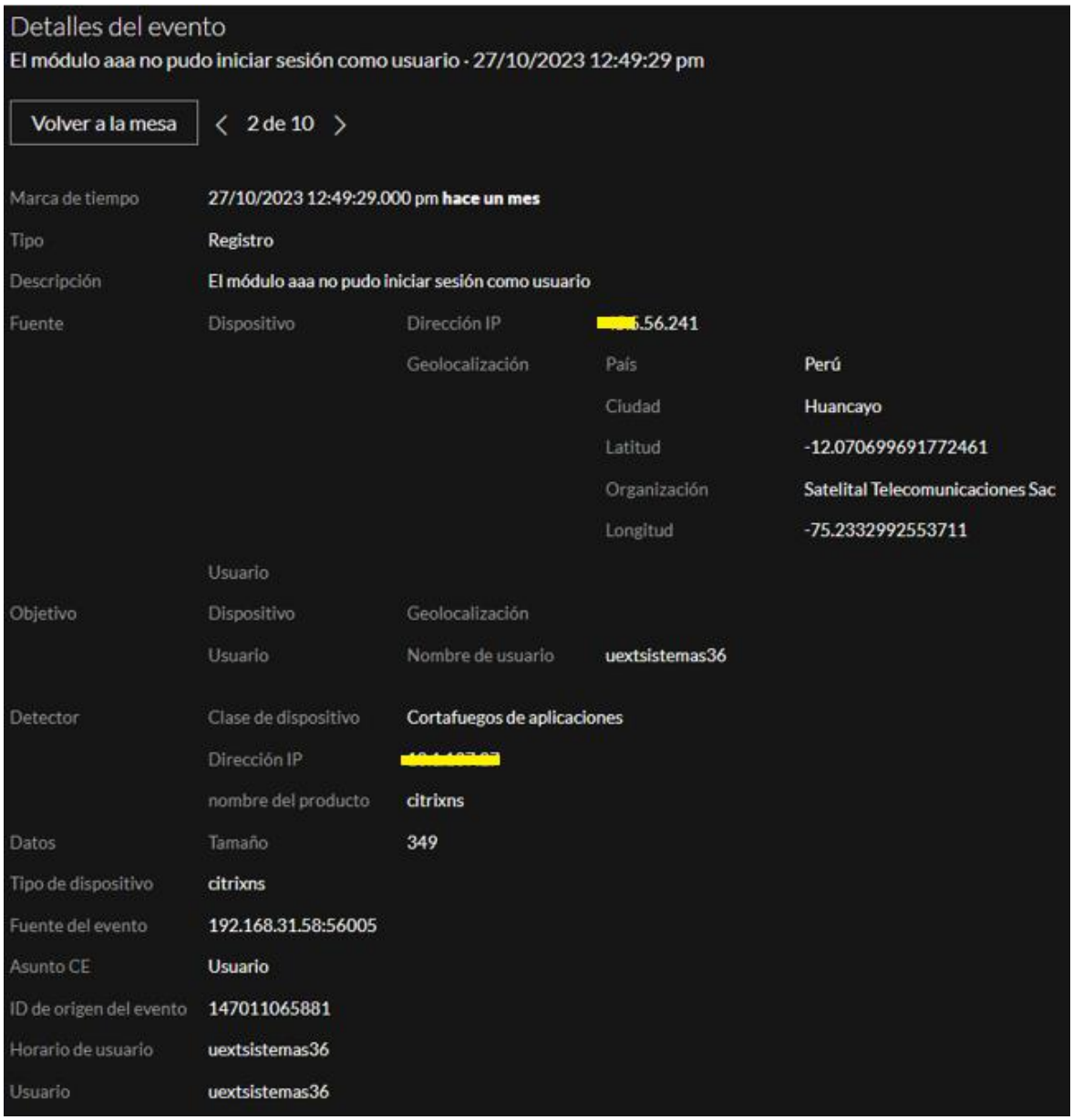
Anexo 3. Información de la alerta activada del usuario mhuamaniy



10 eventos

TIEMPO	TIPO	IP DE ORIGEN	USUARIO DE DESTINO
27/10/2023 07:45:05.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:46:18.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:46:53.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:47:12.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:47:27.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:47:41.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:47:47.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:47:54.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:48:00.000	Registro	[redacted]2.251.1.33	mhuamaniy
27/10/2023 07:48:07.000	Registro	[redacted]2.251.1.33	mhuamaniy

Anexo 4. Detalle con más información del usuario afectado uextsistemas36



Anexo 5. Acciones a realizar por parte de la Entidad Financiera

RV: ANA-INC80779-PE-LVO-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

RC Ronal [redacted]
Para Renzo Joel Gaspar Huamaní

Responder | Responder a todos | Reenviar
lunes 6/11/2023 15:51

CC: Monitoreo CyberSOC Perú <monitoreo_pe@[redacted]>
Asunto: RE: ANA-INC80779-PE-LVO-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

Buenas tardes, estimado Ronal

Se valida que la IP origen **45.5.56.241, es detectado por virus total en 5% Malicioso**, se procedió a realizar el bloqueo de IP origen para conexiones entrantes y salientes a nivel del Firewall Perimetral.

NAME
BK_IP45.5.56.241

45.5.56.241

5 / 89

5 security vendors flagged this IP address as malicious

Similar | Graph | API

45.5.56.241 (45.5.56.0/22)
AS 266757 (SATELITAL TELECOMUNICACIONES S.A.C)

PE
Last Analysis Date
3 months ago

Proceder con el cierre del ticket.

Saludos cordiales.

Anexo 6. Evento reportado hacia la Entidad Financiera

RV: ANA-INC80779-PE-LVO-EVENT-MEDIA-CU-Fuerza Bruta A Cuenta VPN Citrix

RC Ronal [redacted]
Para Renzo Joel Gaspar Huamaní

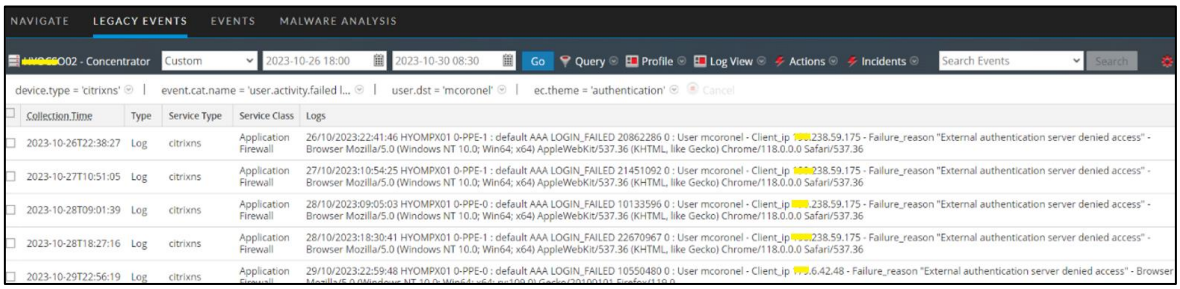
Categoría	Reconnaissance
Fecha y hora	27/10/2023 12:53:12
Origen	Perú
Vector de ataque	Brute Force
	Durante el monitoreo se observó la activación del caso de uso **FUERZA BRUTA A CUENTA VPN CITRIX.** **Descripción:** Este caso de uso se activa cuando existen 10 intentos de login fallidos hacia un usuario de Citrix, en ur **Detalle:** Se observa que se presento múltiples login fallidos por una cuenta en un tiempo de 5 minutos a nivel Citrix.

Equipo (Fuente)	IP del Equipo (Fuente)	Usuario	IP Origen	País Origen	Owner de IP Ori
NetScaler Citrix	[redacted]107.27	**uextsistemas36**	**[redacted].5.56.241**	**Perú**	**SATELITAL TELECOMUN S.A.C**

Validación de la IP (origen) por las siguientes fuentes de Threat Intelligence:

- Virus Total (**BlackList 05**)

Anexo 7. Registro del usuario mcoronel - alerta no activada



NAVIGATE | LEGACY EVENTS | EVENTS | MALWARE ANALYSIS

[redacted]002 - Concentrator | Custom | 2023-10-26 18:00 | 2023-10-30 08:30 | Go | Query | Profile | Log View | Actions | Incidents | Search Events | Search

device.type = 'citrixns' | event.cat.name = 'user.activity.failed l... | user.dst = 'mcoronel' | ec.theme = 'authentication' | Cancel

Collection Time	Type	Service Type	Service Class	Logs
2023-10-26T22:38:27	Log	citrixns	Application Firewall	26/10/2023:22:41:46 HYOMPX01 0-PPE-1 : default AAA LOGIN_FAILED 20862286 0 : User mcoronel - Client_ip [redacted].238.59.175 - Failure_reason "External authentication server denied access" - Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
2023-10-27T10:51:05	Log	citrixns	Application Firewall	27/10/2023:10:54:25 HYOMPX01 0-PPE-1 : default AAA LOGIN_FAILED 21451092 0 : User mcoronel - Client_ip [redacted]238.59.175 - Failure_reason "External authentication server denied access" - Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
2023-10-28T09:01:39	Log	citrixns	Application Firewall	28/10/2023:09:05:03 HYOMPX01 0-PPE-0 : default AAA LOGIN_FAILED 10133596 0 : User mcoronel - Client_ip [redacted].238.59.175 - Failure_reason "External authentication server denied access" - Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
2023-10-28T18:27:16	Log	citrixns	Application Firewall	28/10/2023:18:30:41 HYOMPX01 0-PPE-1 : default AAA LOGIN_FAILED 22670967 0 : User mcoronel - Client_ip [redacted]238.59.175 - Failure_reason "External authentication server denied access" - Browser Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
2023-10-29T22:56:19	Log	citrixns	Application Firewall	29/10/2023:22:59:48 HYOMPX01 0-PPE-0 : default AAA LOGIN_FAILED 10550480 0 : User mcoronel - Client_ip [redacted].6.42.48 - Failure_reason "External authentication server denied access" - Browser