



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Académico Profesional de Ingeniería Electrónica

**Diseño e implementación de una arquitectura SIEM y
despliegue de Cortex XDR para fortalecer la detección de
amenazas en UPAO**

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Daniel Arturo NAVEDA CASTILLO

ASESOR

Mg. Daniel DÍAZ ATAUCURI

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Naveda, D. (2026). *Diseño e implementación de una arquitectura SIEM y despliegue de Cortex XDR para fortalecer la detección de amenazas en UPAO*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Daniel Arturo Naveda Castillo
Tipo de documento de identidad	DNI
Número de documento de identidad	47324946
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Mg. Daniel Díaz Ataucuri
Tipo de documento de identidad	DNI
Número de documento de identidad	07139361
URL de ORCID	https://orcid.org/0000-0001-5747-2795
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Dr. Celso Ysidro Geronimo Huaman
Tipo de documento	DNI
Número de documento de identidad	09191500
Miembro del jurado 1	
Nombres y apellidos	Mg. Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Miembro del jurado 2	
Nombres y apellidos	Mg. Roberto Florentino Unsihuay Tovar
Tipo de documento	DNI
Número de documento de identidad	19944586
Datos de investigación	
Línea de investigación	C.0.3.28. Comunicación/redes y sistemas distribuidos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Lugar: Universidad Privada Antenor Orrego - UPAO País: Perú Departamento: La Libertad Provincia: Trujillo Distrito: Trujillo Centro poblado: Trujillo / Urb. Monserrate Latitud: -8.12811 Longitud: -79.03228
Año o rango de años en que se realizó la investigación	Enero 2025 – Julio 2025
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN
TRABAJO DE
SUFICIENCIA PROFESIONAL
ACTA N°26/FIEE-PPP/2026

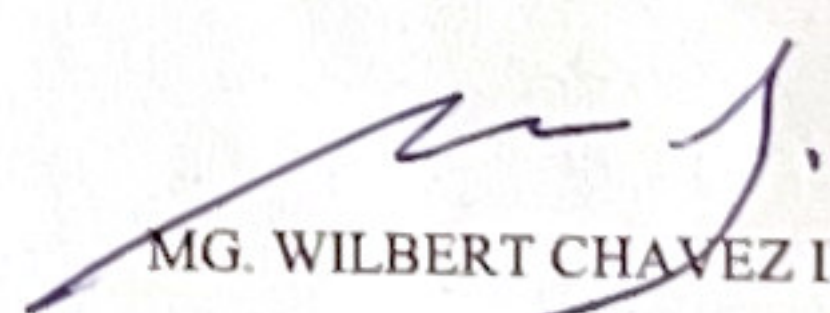
Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 08 de Mayo del 2026, como presidente de Jurado el **DR. CELSO YSIDRO GERONIMO HUAMAN**, integrado por el Miembro de Jurado el **MG. WILBERT CHAVEZ IRAZABAL**, el Miembro de Jurado el **MG. ROBERTO FLORENTINO UNSIHUAY TOVAR** y Miembro Asesor el **MG. DANIEL DÍAZ ATAUCURI**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **DANIEL ARTURO NAVEDA CASTILLO** con código 15190037 que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA SIEM Y DESPLIEGUE DE CORTEX XDR PARA FORTALECER LA DETECCIÓN DE AMENAZAS EN UPAO**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 18 (Dieciocho).

Ciudad Universitaria, 08 de mayo del 2026


DR. CELSO YSIDRO GERONIMO HUAMAN
Presidente Jurado


MG. WILBERT CHAVEZ IRAZABAL
Miembro Jurado


MG. ROBERTO FLORENTINO UNSIHUAY TOVAR
Miembro Jurado


MG. DANIEL DÍAZ ATAUCURI
Miembro Asesor



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo , **DANIEL DÍAZ ATAUCURI** en mi condición de asesor acreditado con el Dictamen N°29/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA SIEM Y DESPLIEGUE DE CORTEX XDR PARA FORTALECER LA DETECCIÓN DE AMENAZAS EN UPAO**, presentado por el bachiller DANIEL ARTURO NAVEDA CASTILLO, para optar el título profesional de Ingeniero Electrónico. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 15% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título profesional de Ingeniero Electrónico.

Lima, 08 de Mayo del 2026


Firma del Asesor

DNI: 07139361

Nombres y apellidos del asesor:
DANIEL DÍAZ ATAUCURI

DEDICATORIA

Este trabajo está dedicado a mis amorosos padres, Maribel y Jorge, por ser mi mayor fuente de fortaleza. Agradezco de todo corazón su amor incondicional, por enseñarme con su ejemplo el valor de la perseverancia y el esfuerzo. Este logro es tan suyo como mío.

AGRADECIMIENTOS

A mi familia en general, por sus ánimos y sus buenos deseos a lo largo de mi vida y mi carrera.

Y no menos importante a la familia de Smartglobal, por brindarme la oportunidad, el apoyo y los recursos necesarios para desarrollar este proyecto, y por confiar en mi capacidad para aportar valor a la organización.

RESUMEN

El presente trabajo es para aumentar el nivel de ciberseguridad en el entorno de red de la Universidad Privada Antenor Orrego (UPAO), y de esta forma preservar la información privada que circula al día a día. El objetivo general fue diseñar e implementar una arquitectura moderna de seguridad en la red, para que de esta forma se facilite el análisis y la respuesta eficaz a incidentes de seguridad.

La metodología que se usó fue la de un análisis inicial del estado de la tecnología de la UPAO. Para lo cual se realizó un diseño mediante las herramientas SIEM – ELA y el Cortex XDR con la finalidad de tener un mejor monitoreo, visualización de registros y una detección temprana de amenazas en la red interna y endpoints.

Los resultados muestran que la detección de incidentes se ha reducido a menos de 10 minutos, a su vez el 92 % de las alertas generadas en los endpoints se relacionan con amenazas reales y la tasa de falsos positivos permaneció por debajo del 5%. Se concluye que el nivel de seguridad implementado es eficiente y rápido, además de que puede ser mejorable mediante la correlación de la información.

Palabras clave: Ciberseguridad, SIEM, Cortex XDR, Firewall, Amenazas, Endpoints.

ABSTRACT

The purpose of this project is to enhance cybersecurity within the network environment of Antenor Orrego Private University (UPAO) and thereby protect the private information that circulates on a daily basis. The overall objective was to design and implement a modern network security architecture to facilitate the analysis of and effective response to security incidents.

The methodology employed involved an initial analysis of the state of UPAO's technology. To this end, a design was developed using SIEM – ELA and Cortex XDR tools to enable better monitoring, log visualization, and early threat detection on the internal network and endpoints.

The results show that incident detection time has been reduced to less than 10 minutes; furthermore, 92% of the alerts generated on endpoints are related to real threats, and the false positive rate remained below 5%. It is concluded that the implemented security level is efficient and fast, and that it can be improved through data correlation.

Keywords: Cybersecurity, SIEM, Cortex XDR, Firewall, Threats, Endpoints.

INDICE GENERAL

RESUMEN	iv
ABSTRACT	v
TABLA DE CONTENIDO	vi
LISTA DE FIGURAS	viii
LISTA DE TABLAS	xi
CAPITULO I: INTRODUCCIÓN	1
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	3
2.1. Institución – Actividad que desarrolla	3
2.2. Periodo de duración de la actividad	3
2.3. Finalidad y objetivos de la entidad	3
2.4. Razón social	3
2.5. Dirección postal	3
2.6. Nombre y correo electrónico del profesional a cargo.	3
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	4
3.1. Organización de la actividad	4
3.2. Finalidad y objetivos de la actividad	6
3.2.1. Finalidad	6
3.2.2. Objetivos	7
3.2.2.1. Objetivo general.	7
3.2.2.2. Objetivos específicos.	7
3.3. Problemática	8
3.3.1. Problema general	8
3.3.2. Problemas específicos	9
3.3.3. Justificación e importancia de la investigación	9

3.4.	Metodología	10
3.4.1.	Bases teóricas	11
3.4.1.1.	Fundamento teórico.	11
3.4.1.2.	Antecedentes.	12
3.4.1.3.	Arquitectura Siem.	14
3.4.1.4.	Seguridad con la VPN site to site.	18
3.4.2.	Marco conceptual	23
3.5.	Procedimiento	27
3.5.1.	Recolección de información	27
3.5.2.	Implementación del log360	28
3.5.3.	Configuración del SIEM – ELA	32
3.5.4.	Configuración VPN IPsec - Firewall PA-3410	37
3.5.5.	Integración ELA – PA-3410	39
3.5.6.	Configuración Cortex XDR	40
3.6.	Resultado de la actividad	43
3.6.1.	Análisis de las ventajas de las arquitecturas SIEM y Cortex XDR	43
3.6.2.	Diseño de la arquitectura de seguridad propuesta	47
3.6.3.	Análisis de tipos de ciberataques identificados por las arquitecturas SIEM y Cortex XDR	48
CAPITULO IV: DISCUSION DE RESULTADOS		57
4.1.	Descripción de la implementación	57
4.2.	EVALUACIÓN ECONÓMICA	58
CAPITULO V: CONCLUSIONES		61
CAPITULO VI: RECOMENDACIONES		63
CAPITULO VII: REFERENCIAS		64
CAPITULO VIII: ANEXOS		67

LISTA DE FIGURAS

Figura 1 Organigrama del flujo de la empresa.	4
Figura 2 Ubicación geográfica de la UPAO.	6
Figura 3 Tipos más comunes de amenazas	24
Figura 4 Túnel VPN Ipsec.	25
Figura 5 Análisis de datos de múltiples fuentes por Cortex XDR.	27
Figura 6 InstallShiel(R) Wizard de Log360.	29
Figura 7 Contrato de licencia.	30
Figura 8 Tipo de instalación Log360.	30
Figura 9 Ubicación de carpeta destino.	31
Figura 10 Registro para soporte.	31
Figura 11 Software instalado.	32
Figura 12 Log360 Integración.	33
Figura 13 ELA integración.	33
Figura 14 Verificación de estado del ELA.	34
Figura 15 Configuración ATA.	34
Figura 16 ATA Servidor.	35
Figura 17 Configuración ATA.	35
Figura 18 Configuración OTX.	36
Figura 19 Configuración del modo de autenticación.	36
Figura 20 Alertas.	36
Figura 21 Configuración interfaz de túnel.	37
Figura 22 Phase 1 - Ike Crypto Profile.	37
Figura 23 Phase 2 - IPsec Crypto Profile.	38
Figura 24 IKE Gateway.	38
Figura 25 Túnel IPsec.	39
Figura 26 Política de seguridad.	39
Figura 27 Integración – Equipos PA-3410.	39
Figura 28 Integración – SIEM-ELA.	40

Figura 29 Tenant activado.	40
Figura 30 Dashboard Cortex.	41
Figura 31 Endpoints Registrados.	41
Figura 32 Agentes.	42
Figura 33 Políticas.	42
Figura 34 Logs Threat.	43
Figura 35 ELA Dashboard.	44
Figura 36 Cortex XDR Dashboard.	44
Figura 37 Alertas - ELA.	45
Figura 38 Alertas – Correo.	45
Figura 39 Alertas – Cortex XDR.	46
Figura 40 Alertas bloqueadas – Cortex XDR.	46
Figura 41 Diagrama de integración.	48
Figura 42 Correo enviado desde el SIEM - ELA.	49
Figura 43 Información general de la amenaza.	50
Figura 44 Información geográfica de la amenaza.	50
Figura 45 Información de reputación de la amenaza.	51
Figura 46 Información de reputación de la amenaza.	51
Figura 47 Información recopilada por la función ATA.	52
Figura 48 Información recolectada de VirusTotal.	52
Figura 49 Logs Threat – Firewall PA-3410.	53
Figura 50 Logs Threat – Firewall PA-3410.	53
Figura 51 Conclusión de la información de la amenaza.	54
Figura 52 Address Group – Firewall PA-3410.	54
Figura 53 Policy security – Firewall PA-3410.	55
Figura 54 Alertas relacionadas al incidente ID-189.	55
Figura A1 Certificación ISO 27001:202.	67
Figura B1 Datasheet Palo alto PA-3410 – parte 1.	68
Figura B2 Datasheet Palo alto PA-3410 – parte 2.	69
Figura B3 Datasheet Palo alto PA-3410 – parte 3.	70
Figura B4 Datasheet Palo alto PA-3410 – parte 4.	71
Figura B5 Datasheet Palo alto PA-3410 – parte 5.	72
Figura B6 Datasheet Palo alto PA-3410 – parte 6.	73
Figura C1 Datasheet SIEM – ELA.	74
Figura D1 Reporte caso: ALERTA EXTERNAL THREAT SOURCE.	74

Figura D2 Reporte – Log360 Cloud Threat Analytics.	75
Figura D3 Reporte – Reputation Trends.	75
Figura D4 Reporte – Reputation Summary.	76
Figura D5 Reporte – Location Details.	76
Figura D6 Reporte – Related Indicators.	76
Figura D7 Reporte – Virus Total Info.	76
Figura D8 Security Vendors Analysis. Parte 1.	77
Figura D9 Security Vendors Analysis. Parte 2.	78
Figura D10 Security Vendors Analysis. Parte 3.	79
Figura D11 Security Vendors Analysis. Parte 4.	80

LISTA DE TABLAS

Tabla 1 Información Firewall	27
Tabla 2 Información SIEM	28
Tabla 3 Información Cortex XDR	28
Tabla 4 Recursos hardware LOG360 + ATA	28
Tabla 5 Detalles del incidente ID-189	56
Tabla 6 Presupuesto del proyecto – Firewalls & Cortex XDR – Marca: Palo Alto	59
Tabla 7 Presupuesto del proyecto – SIEM - ELA – Marca: Manage Engine	59
Tabla 8 Presupuesto del proyecto y servicio por 36 meses	60

1. CAPITULO I: INTRODUCCIÓN

El propósito de este Trabajo de Suficiencia Profesional (TSP) tiene como objetivo principal el diseño e implementación de una arquitectura de ciberseguridad enfocada en la protección avanzada de endpoints y el de un monitoreo de información eficaz en toda la red, con el fin identificar y gestionar amenazas en la infraestructura tecnológica de la Universidad Privada Antenor Orrego (UPAO).

El proyecto se llevó a cabo en un entorno en el que la institución, la cual estaba en proceso de mejora y expansión, reconoció la urgencia de reforzar su enfoque de ciberseguridad por medio de soluciones que ofrezcan una visión más panorámica y monitoreo sobre sus infraestructuras digitales.

Este trabajo se fundamenta en un proyecto desarrollado por la empresa SMARTGLOBAL S.A.C., del cual el autor del presente trabajo de suficiencia es miembro del equipo técnico. Este proyecto se centró en la integración de un sistema SIEM para la recolección y monitoreo de los eventos de seguridad, además del despliegue de Cortex XDR como solución para detectar y proteger los endpoints.

El tema fue elegido por la importancia, cada vez mayor, de la seguridad de la información en los ámbitos universitarios, donde la gran demanda de servicios digitales requiere que se ofrezcan soluciones que aseguren la confidencialidad, integridad y disponibilidad de la información.

En este contexto, se busca demostrar como una arquitectura de seguridad

moderna que integre capacidades de supervisión centralizada, como el SIEM, con protección avanzada en Endpoints, como el Cortex XDR, es capaz de adaptarse a las características específicas de una institución educativa sin poner en peligro su integridad ni escalabilidad.

El objetivo principal de este trabajo es presentar el diseño y el desarrollo de una estructura de ciberseguridad enfocada en detectar a tiempo y responder con eficacia ante amenazas. Se destaca como el SIEM permite el análisis de eventos que vienen del Firewall Palo Alto (protección perimetral), a su vez que el Cortex XDR ofrece un nivel de seguridad inteligente en los endpoints, lo cual ayuda a una defensa completa y proactiva del medio universitario.

2. CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1. Institución – Actividad que desarrolla

SMARTGLOBAL S.A.C. es una empresa peruana que brinda soluciones de ciberseguridad, infraestructura de redes y servicios TI.

2.2. Periodo de duración de la actividad

El proyecto se ejecutó entre abril del 2025 y julio del 2025, incluyendo el diseño, despliegue y validación de las soluciones implementadas.

2.3. Finalidad y objetivos de la entidad

SMARTGLOBAL S.A.C. tiene como finalidad brindar soluciones tecnológicas que fortalezcan la seguridad, operatividad y eficiencia de sus clientes.

2.4. Razón social

SMARTGLOBAL S.A.C

2.5. Dirección postal

Smart Global S.A.C. Calle Amador Merino Reyna 465 of. 701, San Isidro -
Lima Perú

2.6. Nombre y correo electrónico del profesional a cargo

Ing. Mariela Mamani – jefa del área de Operaciones.
Email: mariela.mamani@smartglobal.pe

3. CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1.Organización de la actividad

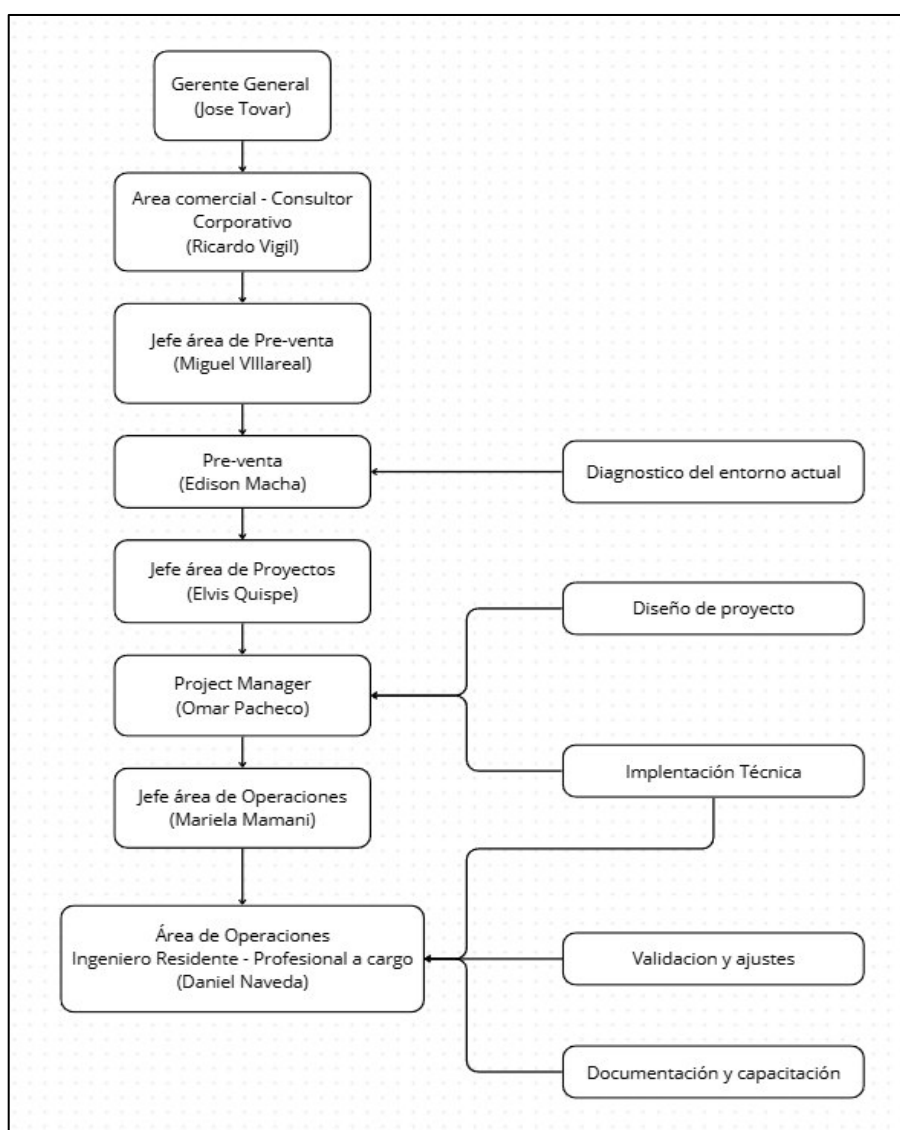


Figura 1 Organigrama del flujo de la empresa. Fuente. Elaboración propia.

Este trabajo que fue planeado y estructurado con cinco actividades, las cuales fueron:

- **Diagnóstico del entorno actual**

Se llevo a cabo un análisis del estado de la tecnología inicial, reconociendo la falta de visibilidad en relación con los incidentes de seguridad y la falta de alguna solución centralizadas de monitoreo y atención rápida.

- **Diseño del proyecto**

Con base en el diagnóstico, se diseñó una estructura de seguridad que incluye la incorporación de un sistema SIEM para la recolección y monitoreo de incidentes de seguridad, y la integración de Cortex XDR para la seguridad y una mejor detección en endpoints.

- **Implementación técnica**

Se realizó la comunicación del SIEM con el firewall PA-3410 mediante un túnel VPN Ipsec, a su vez de la instalación, ajustes y despliegue gradual de la solución Cortex XDR en los dispositivos de la UPAO.

- **Validación y ajustes**

Se realizó un seguimiento de la actividad del sistema y la emisión de alertas, mejorando las políticas y reglas de detección temprana de amenazas y disminuir los falsos positivos.

- **Documentación y capacitación**

Por último, se proporcionó asistencia y formación inicial al personal TI de la UPAO acerca de la utilización de las plataformas puestas en marcha, con un curso o programa de Certificación en Ciberseguridad y que incluye entornos simulados de un SOC registrando todo el procedimiento llevado a cabo de manera documentada.



Figura 2 Ubicación geográfica de la UPAO. Fuente. Imagen obtenida de Google Earth.

3.2. Finalidad y objetivos de la actividad

3.2.1. Finalidad

La finalidad principal de la actividad consistió en mejorar la estructura de ciberseguridad de la Universidad Privada Antenor Orrego (UPAO) para que tenga la capacidad de enfrentar las amenazas modernas en el ámbito digital, esto a través de la implementación de una arquitectura moderna de monitoreo y protección. Este proyecto tuvo como meta proporcionar a la institución recursos que le faciliten tener una perspectiva centralizada de los incidentes de seguridad, así como una defensa activa ante casos críticos que puedan amenazar la integridad, disponibilidad o privacidad de su información esencial. De igual manera, de acuerdo a la creciente necesidad de servicios digitales en el sector universitario, el presente proyecto favoreció al desarrollo de una infraestructura más robusta, siguiendo las mejores prácticas de seguridad.

Desde una perspectiva profesional, esta actividad brindó la oportunidad de poner en práctica conocimientos técnicos específicos en ciberseguridad, incorporando soluciones avanzadas como un sistema SIEM y Cortex XDR, en un escenario real y con un considerable impacto organizacional.

3.2.2. Objetivos

3.2.2.1. Objetivo general.

Reforzar la operatividad continua y la capacidad para identificar amenazas en la infraestructura tecnología de la UPAO, a través del diseño e implementación de una arquitectura SIEM que combine el monitoreo Firewall PA-3410 y los endpoints mediante Cortex XDR, lo que facilita el análisis y la respuesta eficaz a incidentes de seguridad ante el aumento constante de usuarios y equipos.

3.2.2.2. Objetivos específicos.

1. Analizar las ventajas funcionales de una arquitectura de seguridad basada en SIEM y protección de endpoints con Cortex XDR, frente a arquitecturas tradicionales sin monitoreo centralizado, en términos de detección, análisis y respuesta ante incidentes.
2. Diseñar una arquitectura de seguridad que combine un sistema SIEM con la solución de protección de endpoints Cortex XDR, aprovechando los registros del firewall Palo Alto y otros dispositivos críticos, adaptándose a las necesidades de red de la UPAO para mejorar la detección y respuesta ante amenazas.
3. Analizar los tipos de ciberataques y amenazas identificados mediante la integración del firewall Palo Alto y los endpoints con una arquitectura SIEM y Cortex XDR, así como evaluar su impacto y la efectividad de la respuesta dentro de la red de la UPAO.

3.3. Problemática

La Universidad Privada Antenor Orrego (UPAO) enfrentaba serias limitaciones en su capacidad de monitoreo, visibilidad y respuesta ante incidentes de ciberseguridad. Si bien contaba con un firewall Palo Alto en modo standalone, el crecimiento progresivo de alumnos, personal y dispositivos generaba una alta carga de sesiones, afectando el rendimiento y la continuidad de los servicios de red. Sin embargo, más allá de la saturación perimetral, la infraestructura carecía de una solución centralizada que permitiera recopilar, monitorear y analizar eventos de seguridad en tiempo real.

Esta carencia se reflejaba en la ausencia de una arquitectura SIEM (Security Information and Event Management), indispensable para una detección proactiva de amenazas y una gestión eficiente de logs y alertas. Asimismo, aunque se disponía de una solución básica de protección de endpoints con Cortex XDR, esta resultaba insuficiente frente al crecimiento del personal, la diversidad de dispositivos y la necesidad de configuraciones avanzadas para una respuesta más efectiva.

Como parte de una estrategia integral de mejora, se propuso la implementación de un sistema SIEM (Log360) interconectado mediante una VPN site to site con el firewall Palo Alto, acompañado de una nueva licencia y despliegue avanzado de Cortex XDR para ampliar la cobertura de monitoreo a nivel de endpoints. Estas soluciones, integradas a través de una arquitectura adecuada, permitirían mejorar la visibilidad, fortalecer la detección y respuesta ante incidentes, y garantizar la continuidad operativa de los servicios críticos de la universidad.

3.3.1. *Problema general*

¿Cómo reforzar la continuidad operativa y la capacidad de identificar y responder ante amenazas en la infraestructura tecnológica de la Universidad Privada Antenor Orrego (UPAO), mediante la implementación

de una arquitectura de monitoreo basada en SIEM y Cortex XDR, frente al aumento constante de usuarios, equipos e incidentes de seguridad en la red?

3.3.2. Problemas específicos

- ¿Qué ventajas ofrece una arquitectura de seguridad basada en SIEM y protección de endpoints con Cortex XDR, en comparación con arquitecturas tradicionales sin monitoreo centralizado?
- ¿Cómo se puede diseñar una arquitectura SIEM y protección de endpoints con Cortex XDR que se adapte al entorno de red de la UPAO e integre eficientemente el firewall Palo Alto para detectar y responder a incidentes de ciberseguridad?
- ¿Qué tipos de ciberataques y amenazas pueden ser identificados mediante la integración del firewall Palo Alto y los endpoints con una arquitectura SIEM y Cortex XDR, y cómo se analiza su impacto y la efectividad de la respuesta dentro de la red de la UPAO?

3.3.3. Justificación e importancia de la investigación

En un ambiente académico con alta necesidad tecnológica como el de la Universidad Privada Antenor Orrego (UPAO), tener servicios digitales seguros y accesibles se ha vuelto en un aspecto fundamental para asegurar la continuidad tanto en lo académico como en lo administrativo.

En este contexto, la institución educativa presentaba una infraestructura limitada, sin una gestión centralizada que pueda realizar un monitoreo, análisis y relacionar eventos en tiempo real. De acuerdo con lo antes mencionado, esto representaba un riesgo tanto para continuidad de las operaciones como para la seguridad de los sistemas, al no contar de herramientas eficaces para la detección rápida de amenazas o el análisis

forense luego de un incidente.

La implementación de una arquitectura SIEM (Security Information and Event Management) se muestra como una estrategia que ayuda a la integración, consolidación y análisis de los eventos de seguridad que ha generado el Firewall Palo Alto. También se agregó una solución avanzada para la protección de los dispositivos finales en el entorno de la Institución educativa, a través del uso de Cortex XDR, lo cual complementa la función del SIEM al brindar la capacidad de monitoreo, detección y respuesta ante amenazas para los dispositivos finales. Con esto se tiene un control general en toda la institución educativa para detectar ataques en sus primeras fases y responder de manera efectiva ante incidentes.

La contribución de este trabajo de suficiencia profesional está en dar solución técnica a los problemas de ciberataques en el sector educativo, donde es importante tener una infraestructura eficiente que pueda asegurar que la información que maneja esté segura al igual que los servicios que emplea. Se diseña e implementa la arquitectura SIEM, junto con el despliegue de Cortex XDR en la institución educativa, con soluciones modernas, escalables y en sintonía con las buenas prácticas internacionales de ciberseguridad.

3.4. Metodología

La presente actividad profesional se desarrolló bajo un enfoque técnico-aplicado, orientado a resolver una necesidad real identificada en la infraestructura tecnológica de la Universidad Privada Antenor Orrego (UPAO). El objetivo fue diseñar e implementar una arquitectura de ciberseguridad que permita la detección temprana, monitoreo continuo y respuesta eficiente frente a amenazas mediante el uso de herramientas especializadas como un sistema SIEM y la solución Cortex XDR.

3.4.1. Bases teóricas

3.4.1.1. Fundamento teórico.

La ciberseguridad ha evolucionado significativamente desde sus inicios en la década de 1970, consolidándose como un pilar fundamental para la protección de los sistemas informáticos modernos. Uno de los primeros hitos registrados fue el gusano Creeper en 1971, considerado como el primer software malicioso, el cual dio origen a la necesidad de mecanismos de defensa digital (Cyber Magazine, 2023).

En este contexto, (Saltzer y Schroeder, 1975), sentaron las bases teóricas con su artículo *The Protection of Information in Computer Systems*, donde propusieron principios como el de mínimo privilegio, defensa en profundidad y separación de privilegios, los cuales aún sustentan las arquitecturas de seguridad actuales.

Desde entonces, diversos eventos como la creación del Morris Worm en 1988, los ataques de denegación de servicio en los años 2000 y la creciente sofisticación del malware han impulsado el desarrollo continuo de soluciones de ciberseguridad (Certauro, 2024).

Décadas más tarde, (Warner, 2012) aportó una revisión histórica crítica que permitió comprender cómo, incluso antes del auge de Internet, las primeras amenazas y ataques informáticos impulsaron el desarrollo progresivo de mecanismos de protección en entornos gubernamentales y militares, destacando que la seguridad informática nació como una respuesta táctica a riesgos reales.

Más recientemente, (Seeley, 2024) realizó un análisis retrospectivo de trabajos fundacionales, rescatando cómo modelos como Bell-LaPadula y Biba no solo influyeron en el control de acceso, sino que además marcaron un enfoque formal en la protección de la confidencialidad e integridad, el cual aún guía el diseño de soluciones modernas como los sistemas SIEM y plataformas XDR.

3.4.1.2. Antecedentes.

Obi, et al (2024) realizaron un análisis de las amenazas más actuales, la implementación de estrategias y mecanismos de defensa avanzadas para su mitigación de forma más proactiva.

Los puntos más importantes del artículo en donde hacen más énfasis son los siguientes:

- Se introducen en los avances en inteligencia artificial (IA), aprendizaje automático y análisis del comportamiento, dándole importancia en el crecimiento de las defensas de ciberseguridad.
- Entendemos que el intercambio de información sobre amenazas y cooperación mundial es fundamental para el fortalecimiento de un ecosistema global de ciberdefensa. Además de la concienciación del factor humano sobre ciberseguridad, y de esta forma tener una organización más segura.
- Analiza los marcos regulatorios y los estándares de cumplimiento que son fundamentales para establecer buenas prácticas y directrices en dirección de la ciberseguridad.

En el presente artículo, los autores plantean que es crucial la anticipación de las amenazas modernas con estrategias de ciberseguridad avanzadas. Por ello es importante que las organizaciones deben tener un enfoque proactivo y adaptativo en materia de ciberseguridad. Debido a que el panorama cibernético tiene una naturaleza dinámica es necesario una estrategia integral que abarque personas, procesos y tecnologías. A medida que las organizaciones navegan por las complejidades de la era digital, un enfoque estratégico y con visión de futuro en materia de ciberseguridad es fundamental para asegurar el futuro digital.

Sleem (2022) realizó un estudio de los diferentes tipos de protección de ciberseguridad contra las amenazas.

Los puntos más importantes del artículo en donde hacen más énfasis son los siguientes:

- Para contrarrestar estas amenazas, las organizaciones y las personas deben adoptar medidas robustas de ciberseguridad. Esto incluye la implementación de contraseñas seguras, autenticación de dos factores y cifrado para proteger los datos.
- Las actualizaciones periódicas de software, la segmentación de la red y los firewalls pueden ayudar a prevenir el malware y el acceso no autorizado.
- La investigación sobre amenazas de ciberseguridad es un área de estudio crucial, dada la creciente dependencia de la tecnología digital y el consiguiente aumento de las amenazas de ciberseguridad.

En el presente artículo, el autor ofrece una visión general de las amenazas de ciberseguridad y las estrategias para mitigar los riesgos en la era digital actual. Enfatiza en la importancia de mejorar la cultura de seguridad organizacional, adoptar protocolos de autenticación robustos, implementar cifrado, realizar evaluaciones de seguridad periódicas, monitorear redes y sistemas, y contar con un plan de respuesta a incidentes bien definido.

González, et al (2021) realizó un estudio de la evolución de las soluciones SIEM hasta convertirse en sistemas integrales que ofrecen una amplia visibilidad para identificar áreas de alto riesgo.

Los puntos más importantes del artículo en donde hacen más énfasis son los siguientes:

- Los SIEM tienen la capacidad de recopilar, agregar, almacenar y correlacionar eventos generados por una infraestructura gestionada.
- Realiza un análisis profundo de las características y capacidades de los SIEM actuales, centrando sus limitaciones para proponer posibles mejoras que se integren en la plataforma SIEM en el año de la publicación del artículo.
- Se proporciona una visión general de las soluciones SIEM en infraestructuras críticas para identificar el uso potencial de estas herramientas.

Este artículo presenta un análisis comercial y técnico de algunas de las principales soluciones SIEM disponibles en el mercado. En cuanto al análisis de comportamiento, el análisis de riesgos y su implementación, es necesario desarrollar técnicas y herramientas para analizar, evaluar y guiar la implementación óptima de diversos mecanismos de seguridad en la infraestructura gestionada.

3.4.1.3. Arquitectura Siem.

Ban, et al (2023) realizó un estudio sobre la arquitectura SIEM, la cual la define como una herramienta que tiene como objetivo recopilar, integrar y analizar datos relacionados con la seguridad de múltiples fuentes.

Como resultado, las soluciones SIEM proporcionan una visión integral de las actividades que ocurren en la infraestructura de TI y pueden detectar posibles incidentes de seguridad antes de que causen daños significativos.

La arquitectura de un SIEM comprende una serie de componentes que desarrollan una función importante en el proceso de una visión general de la seguridad y la respuesta a incidentes.

Recopilación y agregación de datos

La base de cualquier sistema SIEM es la recopilación y agregación de datos, obteniendo información de seguridad de una amplia variedad de fuentes: dispositivos de red, incluidos firewalls y routers; servidores; endpoints; y aplicaciones, incluidas las alojadas en la nube. Los sistemas SIEM modernos están diseñados para admitir grandes volúmenes de datos, agregando registros en tiempo real, desde cientos hasta miles de fuentes (SentinelOne, 2025).

Normalización y análisis

Cuando se recopilan datos de diversas fuentes, suelen estar en muchos formatos. Esta diversidad de formatos de registro crea un problema para el análisis y la correlación de la información. Durante el proceso de normalización, este formato de registro diverso se transforma en un formato estandarizado, mucho más fácil de procesar para el SIEM (SentinelOne, 2025).

Motor de correlación

El motor de correlación es probablemente la parte más crítica de un sistema SIEM, donde se lleva a cabo el núcleo analítico de dicho sistema. Este motor procesa los datos normalizados con el fin de identificar patrones y relaciones que, de otro modo, apuntarían hacia una amenaza para la seguridad. Podría ejecutar un motor de correlación capaz de detectar varios intentos fallidos de inicio de sesión en diferentes puntos finales en un breve periodo de tiempo, lo que podría indicar un ataque de fuerza bruta. Las soluciones SIEM modernas utilizan diversas técnicas de correlación para mejorar la detección de amenazas (SentinelOne, 2025).

Gestión y retención de registros

Algunas de las principales preocupaciones de la arquitectura SIEM tienen que ver con la gestión y la retención de registros en lo que respecta al cumplimiento normativo y las investigaciones forenses. A tal efecto, los sistemas SIEM deben almacenar los registros de forma segura y hacerlos accesibles siempre que sea necesario para auditorías o investigaciones. Una buena gestión de registros implica organizar y mantener los registros de tal manera que sean fáciles de recuperar y analizar durante un incidente o una auditoría (SentinelOne, 2025).

Alertas e informes

Es aquí donde las alertas generadas a través del sistema SIEM cobran gran importancia, ya que cuando el motor de correlación identifica un posible incidente de seguridad, la rápida mitigación de la amenaza depende en gran medida de las alertas. Estas suelen enviarse a los analistas de seguridad, que investigan más a fondo y responden a las amenazas.

En algunos casos, también pueden integrarse con plataformas de respuesta a incidentes, o incluso con respuestas automatizadas, lo que facilita una reacción más rápida ante amenazas críticas. Otras características críticas del sistema SIEM son los informes que profundizan en los detalles minuciosos sobre las tendencias de seguridad, el estado de cumplimiento de la organización y la eficacia general de la seguridad. (SentinelOne, 2025).

Las principales funciones y ventajas de implementar un SIEM en un entorno de centro de operaciones de seguridad (SOC) es la de mantener soluciones de seguridad completas y resistentes.

Supervisión en tiempo real

Supervisar regularmente el tráfico de la red y el comportamiento de los usuarios ayuda a las organizaciones a identificar rápidamente actividades inusuales que puedan ser señal de un ataque o de un acceso no autorizado. Este enfoque permite a los equipos de seguridad responder con rapidez y evitar las filtraciones de datos (Palo Alto Networks, s.f.).

Detección de amenazas

Las herramientas SIEM ayudan a las organizaciones a analizar los registros de seguridad para detectar indicios de ciberataques, amenazas de personas internas o infracciones de las normas. Revisan grandes cantidades de datos de seguridad para detectar actividades inusuales que puedan indicar una infracción, centrándose en pequeños problemas como cambios en el comportamiento de los usuarios (Palo Alto Networks, s.f.).

Respuesta ante incidentes

Los sistemas SIEM ayudan a responder a las amenazas de la seguridad, ya sea de forma automática o manual. Se encarga de tareas repetitivas como notificar a los usuarios y contener las amenazas con rapidez, reduciendo los tiempos de respuesta y limitando la propagación de los ataques. Las respuestas manuales permiten a los analistas de seguridad investigar incidentes de pensamiento único o necesario, garantizando que las respuestas se ajustan a cada amenaza específica (Palo Alto Networks, s.f.).

Informes de cumplimiento

Las soluciones SIEM recopilan y normalizan continuamente grandes conjuntos de datos, garantizando que la información sea precisa y fácilmente accesible para las auditorías de cumplimiento. En última

instancia, los procesos racionalizados que hacen posibles las soluciones SIEM mejoran el cumplimiento y liberan valiosos recursos, lo que permite a los equipos de seguridad centrarse en tareas de seguridad más estratégicas (Palo Alto Networks, s.f.).

Actualmente los SIEM, como toda herramienta, también presentan ciertas limitaciones, a pesar de que ofrece potentes funcionalidades en cuanto a correlación, almacenamiento, visualización y rendimiento, así como la capacidad de automatizar el proceso de respuesta mediante la selección e implementación de contramedidas, los sistemas de respuesta actuales son muy limitados y las contramedidas se seleccionan e implementan sin realizar un análisis exhaustivo del impacto de los ataques y los escenarios de respuesta (González-Granadillo, et al, 2021).

El futuro de los SIEM al estar en una naturaleza cambiante debido a las amenazas a la seguridad, la proliferación de dispositivos móviles, la globalización, el auge de las redes sociales y los rápidos cambios en la normativa están acelerando la evolución de la Gestión de Información y Eventos de Seguridad (SIEM). Los factores externos que podrían afectar el futuro de los sistemas SIEM y sus tecnologías relacionadas a mediano y largo plazo, son considerando los factores políticos, económicos, sociales, tecnológicos, legales y ambientales (González-Granadillo, et al, 2021).

3.4.1.4. Seguridad con la VPN site to site.

Zohaib (2024) realizó un estudio sobre la tecnología de VPN como una conexión segura y cifrada.

La conexión de la tecnología de VPN permite a los usuarios enviar y recibir datos a través de redes compartidas o públicas como si sus dispositivos informáticos estuvieran conectados directamente a la red privada. El cifrado garantiza que, incluso si los datos son interceptados, no se pueden leer. Al enmascarar su dirección IP, una VPN ayuda a proteger su privacidad en línea.

Una VPN site to site es una red privada que oculta las intranets privadas y permite a los usuarios de estas redes seguras acceder a los recursos de otras redes. Las VPN site to site mejoran la seguridad y la eficiencia de las redes organizacionales (Palo Alto Networks, s.f.).

La elección de utilizar una VPN site to site para la seguridad de la transmisión de información se basa en las siguientes propiedades de seguridad criptográfica que ofrecen:

Confidencialidad

Las VPNs utilizan criptografía simétrica para cifrar y descifrar sus canales de comandos y datos. La criptografía simétrica suele ser más eficiente y requiere menos potencia de procesamiento que la criptografía asimétrica, por lo que normalmente se utiliza para cifrar la mayor parte de los datos que se transmiten a través de una VPN. Entre los algoritmos aprobados por el Instituto Nacional de Estándares y Tecnología (NIST) que implementan la criptografía simétrica se incluyen el Estándar de Cifrado Avanzado (AES) y el Estándar de Cifrado de Datos Triple (3DES). Uno de los modos aprobados por el NIST para los algoritmos de criptografía simétrica es el Modo de Contador de Galois AES (AES-GCM) (NIST, 2020).

Integridad

La integridad se garantiza mediante un algoritmo de autenticación de mensajes. Este algoritmo toma los datos de entrada y una clave secreta de integridad, y genera un código de autenticación de mensajes (MAC). Los datos y el MAC se envían a través de la red. El receptor calcula el MAC de los datos recibidos utilizando la misma clave secreta de integridad (previamente establecida entre el emisor y el receptor). Si se produce algún cambio en el mensaje o en su MAC, la verificación del MAC fallará y el mensaje deberá descartarse (NIST, 2020).

Autenticación

Un algoritmo de firma digital se utiliza para la autenticación entre pares. Utiliza dos claves distintas: una clave pública y una clave privada. Las VPN suelen utilizar criptografía asimétrica para la autenticación de identidad. Este par de claves pública/privada puede utilizarse de forma independiente o estar incluido en un certificado X.509. Un método menos seguro de autenticación de identidad es el uso de una clave precompartida (PSK). Las partes autentican la identidad de la otra basándose en que nadie más posee esta clave compartida, la cual debe establecerse entre el origen y el destino. Las PSK deben ser altamente aleatorias (proporcionando al menos 112 bits de seguridad) y no deben basarse en palabras o frases simples (NIST, 2020).

Protección del tráfico en redes públicas

Cuando se utiliza el modo túnel de IPsec, quien monitoriza el tráfico de red desconoce qué participantes se comunican, con qué frecuencia se producen las comunicaciones y la cantidad de datos que se intercambian. Si bien se puede contabilizar el número y el tamaño de los paquetes cifrados que se intercambian, esto genera una reducción de riesgo en la interceptación de paquetes o de espionaje. Se pueden enviar paquetes ficticios para ocultar aún más la cronología de la comunicación real (NIST, 2020).

IPsec es un conjunto de protocolos para proteger las conexiones entre dispositivos. IPsec ayuda a mantener seguros los datos enviados a través de redes públicas. Se utiliza frecuentemente para configurar VPN site to site y funciona cifrando los paquetes, además de autenticar su origen. El cifrado es el proceso de ocultar información alterando matemáticamente los datos para que parezcan aleatorios. En términos más sencillos, el cifrado consiste en el uso de un "código secreto" que solo las partes autorizadas pueden interpretar (Cloudflare, s. f.).

En una arquitectura de una VPN site to site, esta configuración une dos redes, la cual establece un canal lógico protegido. Este canal es establecido por un conjunto de componentes, protocolos y procesos. Esta arquitectura se basa en el protocolo Ipsec que tiene los siguientes pasos:

Intercambio de claves

Las claves son necesarias para el cifrado; una clave es una cadena de caracteres aleatorios que se utiliza para cifrar y descifrar mensajes. IPsec establece claves mediante un intercambio entre los dispositivos conectados, de modo que cada dispositivo pueda descifrar los mensajes del otro (Cloudflare, s. f.).

Encabezados y pies de página de los paquetes

Todos los datos que se envían a través de una red se dividen en fragmentos más pequeños llamados paquetes. Los paquetes contienen tanto la carga útil (los datos que se envían) como los encabezados (información sobre esos datos) para que los ordenadores que los reciben sepan qué hacer con ellos. IPsec añade varios encabezados a los paquetes de datos que contienen información de autenticación y cifrado. IPsec también añade pies de página, que se colocan después de la carga útil de cada paquete, en lugar de antes (Cloudflare, s. f.).

Autenticación

IPsec proporciona autenticación para cada paquete, como un sello de autenticidad en un objeto de colección. Esto garantiza que los paquetes provienen de una fuente confiable y no de un atacante (Cloudflare, s. f.).

Cifrado

IPsec cifra la carga útil de cada paquete y su encabezado IP (a menos que

se utilice el modo de transporte en lugar del modo túnel). Esto garantiza la seguridad y privacidad de los datos enviados a través de Ipsec (Cloudflare, s. f.).

Transmisión

Los paquetes IPsec cifrados viajan a través de una o más redes hasta su destino mediante un protocolo de transporte. En esta etapa, el tráfico IPsec se diferencia del tráfico IP convencional en que suele utilizar UDP como protocolo de transporte, en lugar de TCP. TCP (Protocolo de Control de Transmisión) establece conexiones dedicadas entre dispositivos y garantiza la llegada de todos los paquetes. UDP (Protocolo de Datagramas de Usuario) no establece estas conexiones dedicadas. IPsec utiliza UDP porque permite que los paquetes IPsec atraviesen los firewalls (Cloudflare, s. f.).

Descifrado

En el otro extremo de la comunicación, los paquetes se descifran y las aplicaciones (por ejemplo, un navegador) pueden utilizar los datos recibidos (Cloudflare, s. f.).

La implementación de una VPN site to site si bien realiza encriptación y autenticación de la información que pasa por el canal, es bien sabido que también tiene sus riesgos y limitaciones. El Gateway VPN es uno de los principales riesgos, debido a la exposición que tiene hacia la internet. Este factor lo hace objetivo si se tiene configuraciones erróneas o vulnerabilidades. Con respecto a sus limitaciones, la saturación en un ambiente concurrente puede generar lentitud y hasta la caída del canal, depende de una configuración correcta y tener problemas por temas de cifrado en la traslación de la información. Debido a lo antes mencionado, Este tipo de configuración de VPN site to site no tiene una solución completa y se debe apoyar de otras configuraciones que puedan aportar a una protección más eficaz.

3.4.2. Marco conceptual

Ciberseguridad

En el artículo (Palo Alto Networks, s. f.), define la ciberseguridad como la práctica de proteger computadoras, servidores, redes, dispositivos y datos confidenciales contra ataques digitales maliciosos y accesos no autorizados. Abarca un conjunto integral de medidas de seguridad, herramientas y mejores prácticas para proteger a usuarios y organizaciones de las ciberamenazas en constante evolución.

ISO/IEC 27001

Esta norma ISO/IEC 27001 tiene un enfoque sistemático para la gestión de la información sensible de la empresa, garantizando su confidencialidad, integridad y disponibilidad. Es una norma internacional que proporciona orientación para el establecimiento, la implementación y el mantenimiento de un sistema de gestión de la seguridad de la información (TechTarget, 2024).

Amenazas cibernéticas

ORSYS Le Mag (2025), define una ciberamenaza como cualquier circunstancia o acontecimiento susceptible de causar daños a través del ciberespacio a los sistemas de información. Tales como robar datos, dañar sistemas o interrumpir la vida digital, afectando la confidencialidad, integridad o disponibilidad de la información.

Una ciberamenaza utiliza vectores para alcanzar su objetivo. Los vectores más comunes son:

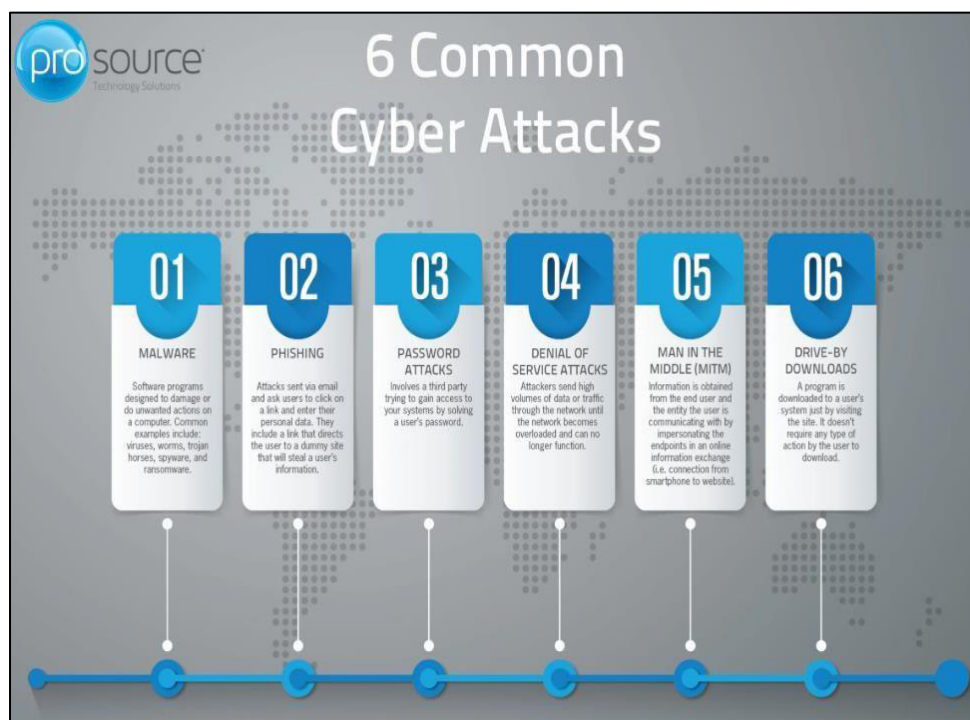


Figura 3 Tipos más comunes de amenazas. Fuente. Información tomada de Hoverman (2017).

Firewall PA-3410

El Palo Alto Networks PA-3410 es un firewall de próxima generación orientado a organizaciones que requieren alto rendimiento, seguridad avanzada y continuidad operativa. Está diseñado para inspeccionar, filtrar y controlar el tráfico de red en tiempo real, aplicando políticas de seguridad que previenen intrusiones, malware y accesos no autorizados.

En el contexto de conectividad segura, el PA-3410 soporta VPN IPsec de hasta 6,8 Gbps, permitiendo la creación de túneles cifrados y confiables entre sedes, sucursales o hacia infraestructuras en la nube. Esto garantiza que los datos transmitidos mantengan su confidencialidad e integridad, incluso a través de redes públicas. Su capacidad de alta disponibilidad lo convierten en un componente esencial para empresas que buscan un esquema seguro y eficiente (Palo Alto Networks, s. f.).

Túnel VPN IPsec

De acuerdo a (Cloudflare, 2025), es una comunicación basada en un conjunto de protocolos creados para asegurar el intercambio de información en redes IP. Son túneles cifrados de extremo a extremo, evitando que intermediarios intercepten la información durante su tránsito. Realizan intercambio de cifrado con integridad (ESP), claves mediante IKE y autenticación (AH).

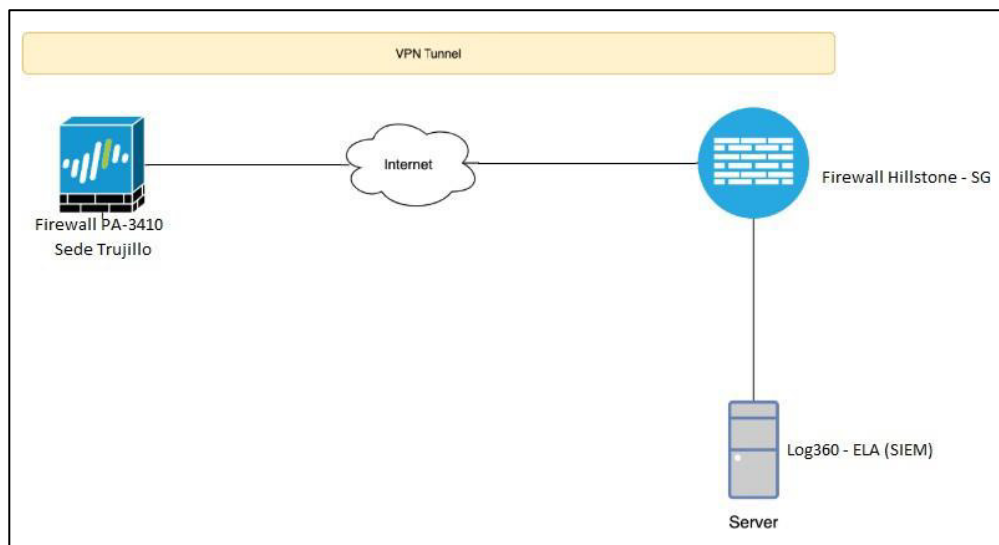


Figura 4 Túnel VPN Ipsec. Fuente. Elaboración propia.

LOG360

(ManageEngine, s. f.), la define como una solución completa de gestión de eventos y datos de seguridad. Log360 puede monitorear toda su red, ayuda a detectar y mitigar las amenazas de seguridad en una etapa temprana. Log360 tiene los siguientes componentes:

- ✓ **EventLog Analyzer (ELA):** monitoreo de registros para el perímetro de la red, servidores, aplicaciones y soluciones de seguridad.
- ✓ **ADAudit Plus:** auditoría de Active Directory en tiempo real.
- ✓ **Cloud Security Plus:** auditoría de infraestructura de nube pública.

- ✓ Exchange Reporter Plus: supervisión dedicada de servidores Exchange.
- ✓ O365 Manager Plus: monitoreo dedicado para Office 365.
- ✓ ADManager Plus: informes sobre los riesgos de Active Directory.
- ✓ DataSecurity Plus: visibilidad, auditoría y protección de datos.
- ✓ Log360 UEBA: análisis basado en aprendizaje automático y puntuación de riesgo.

EventLog Analyzer (ELA)

Es una solución web, en tiempo real, de monitorización de registros y gestión del cumplimiento normativo para la Gestión de Eventos e Información de Seguridad (SIEM). Esta herramienta es perfecta para cumplir con los requisitos de auditorías de TI. EventLog Analyzer es una solución perfecta para la recolección, análisis, generación de reportes y archivar registros recibidos de dispositivos como, por ejemplo, Firewalls de la marca Palo Alto (ManageEngine s. f.).

- ✓ Función de Advance Threat Analytics (ATA):

Esta función extrae información valiosa sobre la gravedad de las amenazas utilizando el puntaje de reputación para URL, dominios y direcciones IP potencialmente maliciosos. Para activar la funcionalidad de inteligencia de amenazas, se debe adquirir un complemento en la licencia de Log360 (ManageEngine s. f.).

- ✓ Plataforma Open Threat Exchange (OTX):

Es una fuente de inteligencia, la cual recopila información de indicadores de compromiso extraídos de diversas fuentes, entre ellas redes sociales como Twitter/X (ManageEngine s. f.).

Cortex XDR

Es una plataforma extendida de detección y respuesta, que integra de forma nativa datos de red, endpoints, la nube y de terceros para detener ataques sofisticados. Mediante análisis de comportamiento, identifica amenazas desconocidas y altamente evasivas que atacan la red (Palo Alto Networks, s. f.).

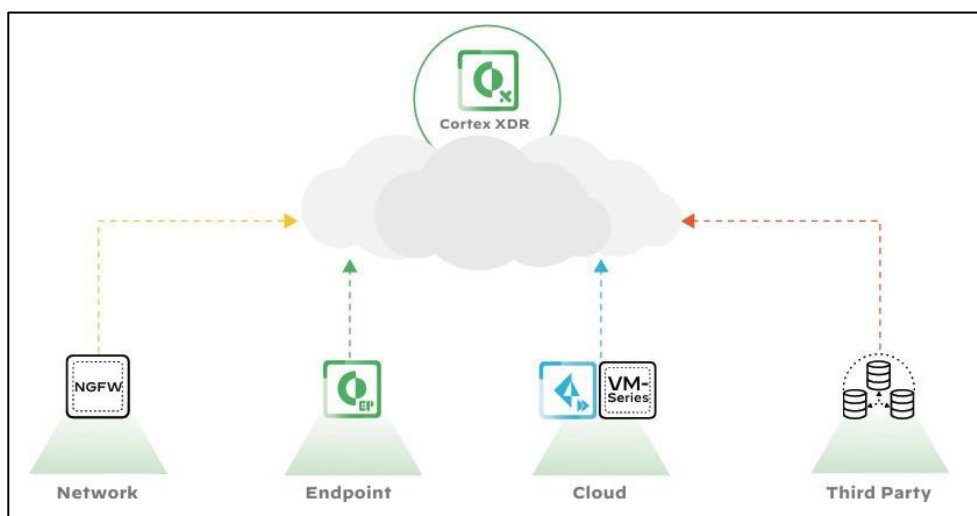


Figura 5 Análisis de datos de múltiples fuentes por Cortex XDR. Fuente. Información tomada de la página web de Palo Alto Networks.

3.5. Procedimiento

3.5.1. Recolección de información

Se muestra la información correspondiente a los equipos físicos y virtuales a considerar en el presente trabajo.

Tabla 1 Información Firewall

MARCA	MODELO	SITE
PALO ALTO	PA-3410	Datacenter Cliente - Trujillo
PALO ALTO	PA-3410	Datacenter Cliente - Trujillo

Fuente. Información obtenida de los equipos Firewalls de la UPAO.

Tabla 2 Información SIEM

MARCA	MODELO
MANAGE ENGINE	Log 360 - ELA

Fuente. Información obtenida de la herramienta SIEM de SmartGlobal.

Tabla 3 Información Cortex XDR

MARCA	MODELO
PALO ALTO	Cortex 250 Agents

Fuente. Información obtenida de la herramienta Cortex XDR de la UPAO.

3.5.2. Implementación del log360

Consideración de la solución:

1. Puertos necesarios para Log360: el puerto 9322 (TCP) debe estar abierto para la comunicación con el servidor y 8095 (TCP) para la conexión de la interfaz gráfica (web).
2. Puertos requeridos para EventLog Analyzer: Se necesita que los puertos mencionados a continuación estén abiertos en el servidor:
 - ✓ 8400 (TCP): Puerto del servidor web.
 - ✓ 513 (UDP), 514 (TCP y UDP): Puerto de escucha de syslog.
3. En la solución LOG360 se instalará un ELA, pero se deberá tener en cuenta los recursos necesarios.

Requisitos de hardware:

Debido a que se va a instalar un LOG360 + ELA y Advance Threat Analality (ATA), se consideró la siguiente información de recursos del sistema.

Tabla 4 Recursos hardware LOG360 + ATA

HARDWARE	MINIMUM	RECOMMENDED
Processor	2.4Ghz	3Ghz
Core	12 Core	16 Core
RAM	48 GB	64 GB
Disk Space	1.5 TB	2 TB
Disk Type	SSD	SSD

Fuente. Información obtenida del manual del Manage Engine.

Requisitos de software:

Para el ManageEngine Log360 que se ha implementado se ha optado por la siguiente versión del sistema operativo Microsoft Windows: Microsoft Windows Server 2016 Standard (v.10.0.14393).

Navegadores compatibles:

ManageEngine Log360 requiere que uno de los siguientes navegadores esté instalado en el sistema para acceder al cliente web de Log360.

- ✓ Internet Explorer 9 y superior
- ✓ Firefox 4 y superior
- ✓ Chrome 10 y superior
- ✓ Safari 5 y superior

Instalación del LOG360:

- ✓ Se descarga el archivo del software desde la siguiente URL <https://www.manageengine.com/log-management/download.html>.
- ✓ Seleccionar el archivo descargado *ManageEngine_Log360_64bit* para iniciar la instalación.



Figura 6 InstallShield(R) Wizard de Log360. Fuente. Información obtenida de la instalación del ManageEngine Log360.

- ✓ Seleccionar el acuerdo de contrato de licencia.



Figura 7 Contrato de licencia. Fuente. Información obtenida de la instalación del ManageEngine Log360.

- ✓ Seleccionar el tipo de instalación, ya sea estándar, mínimo y personalizado. Además, seleccionar la ubicación de la carpeta destino donde se alojará el software.

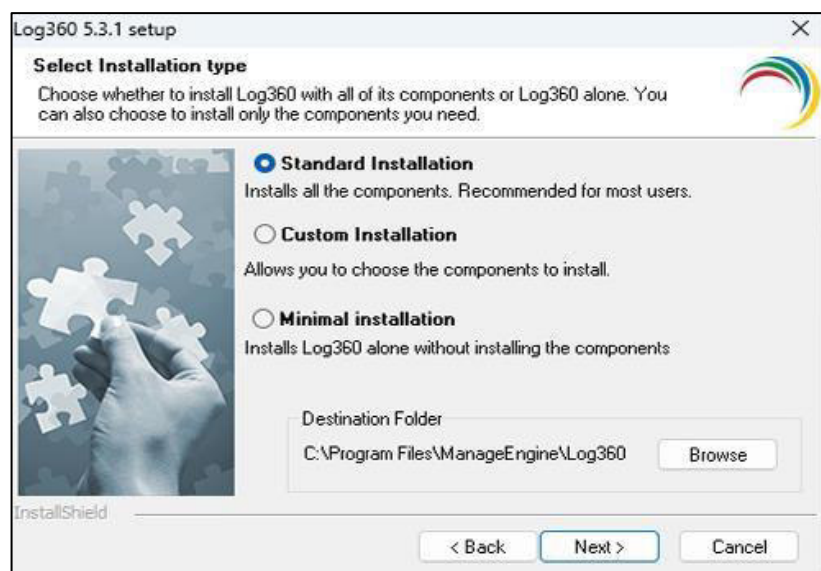


Figura 8 Tipo de instalación Log360. Fuente. Información obtenida de la instalación del ManageEngine Log360.

- ✓ Iniciar con la copia de archivos para la instalación.

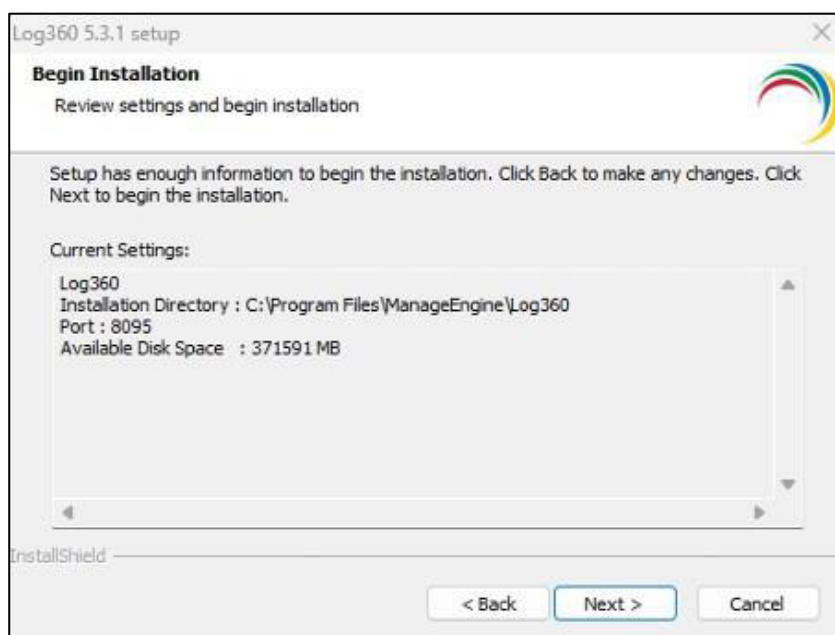


Figura 9 Ubicación de carpeta destino. Fuente. Información obtenida de la instalación del ManageEngine Log360.

- ✓ Colocar datos de registros para el soporte.

The screenshot shows the 'Log360 5.3.1 setup' window at the 'Registration for Technical Support (Optional)' screen. The title bar includes the text 'Log360 5.3.1 setup' and a close button. The main window has a header 'Registration for Technical Support (Optional)' with a sub-header 'Enter Your Details below'. Below this, there are five input fields: 'Name', 'E-mail Id', 'Phone', 'Company Name', and 'Country'. The 'Country' field is a dropdown menu with '-Select-' as the current selection. Below the input fields, a message states: 'By clicking "Next", you agree to our [Privacy Policy](#).' At the bottom, there are three buttons: '< Back', 'Next >', and 'Skip'. The 'Next >' button is highlighted with a blue border.

Figura 10 Registro para soporte. Fuente. Información obtenida de la instalación del ManageEngine Log360.

- ✓ Programa de instalación finalizado.



Figura 11 Software instalado. Fuente. Información obtenida de la instalación del ManageEngine Log360.

3.5.3. Configuración del SIEM – ELA

1. Se descargó el componente ELA desde la página web <https://www.manageengine.com/log-management/download.html> y luego proceda con la instalación.
2. Para poder integrar este componente, debemos realizar la siguiente configuración en la plataforma:
 - ✓ Dirigirse a la ruta Admin→ LOG360 Integration.
 - ✓ Seleccionar EventLog Analyze

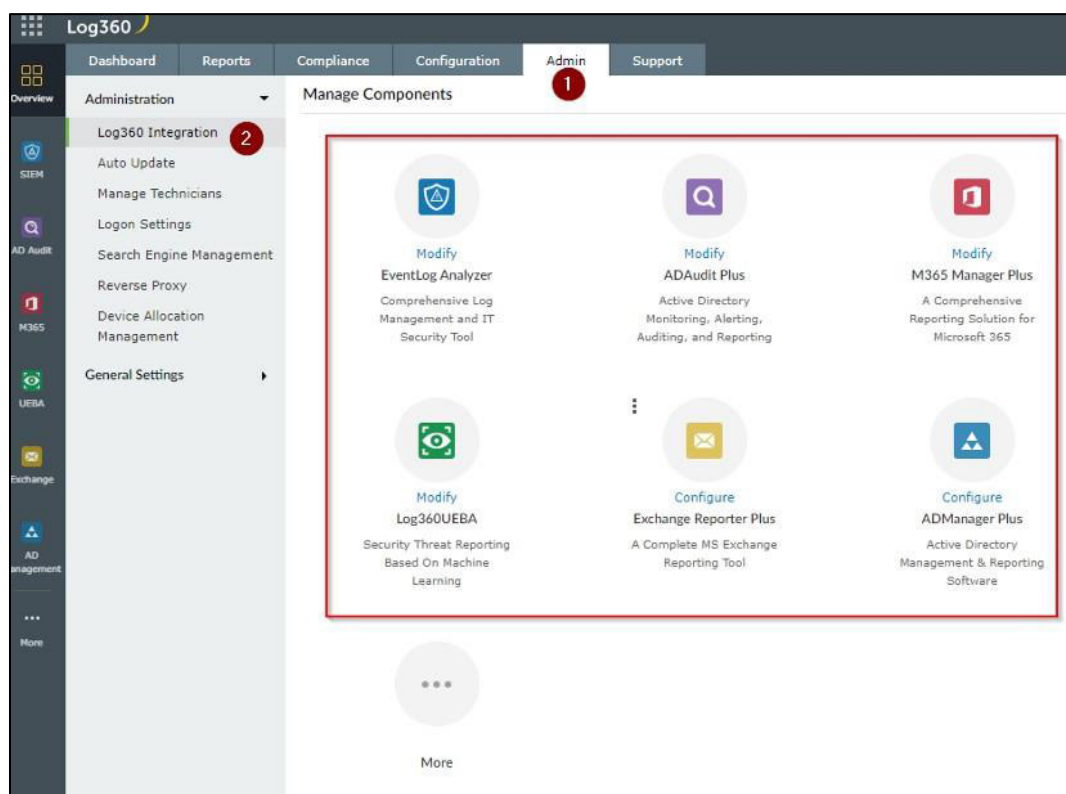


Figura 12 Log360 Integración. Fuente. Información obtenida de la plataforma LOG360.

- ✓ Introducir el nombre o la dirección IP y el número de puerto del servidor para el componente seleccionado.
- ✓ Seleccionar la opción de “Integrate Now”. Estos pasos se pueden repetir para los demás componentes.

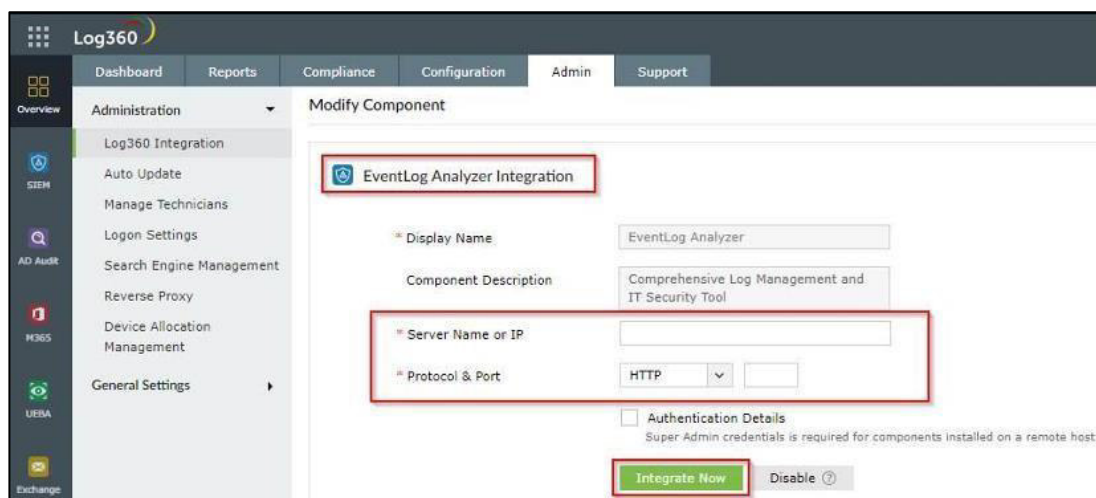


Figura 13 ELA integración. Fuente. Información obtenida de la plataforma LOG360.

- ✓ Una vez que se haya integrado los diferentes componentes de Log360, desde la opción Manage Components se puede validar el estado de sincronización o que el servidor se está ejecutando en cada componente.

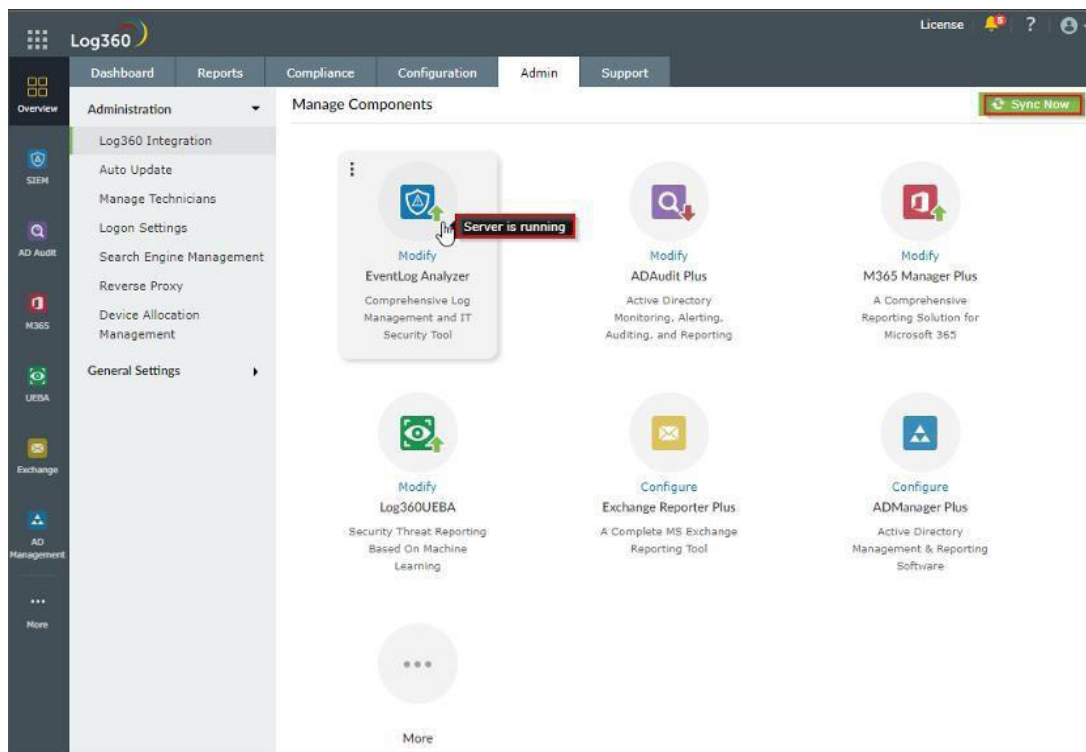


Figura 14 Verificación de estado del ELA. Fuente. Información obtenida de la plataforma LOG360.

3. Configuración del Advance Threat Analytics (ATA)

- ✓ Seleccionar la opción Setting→Threat Feeds→Threat Management→Advanced Threat Anality.

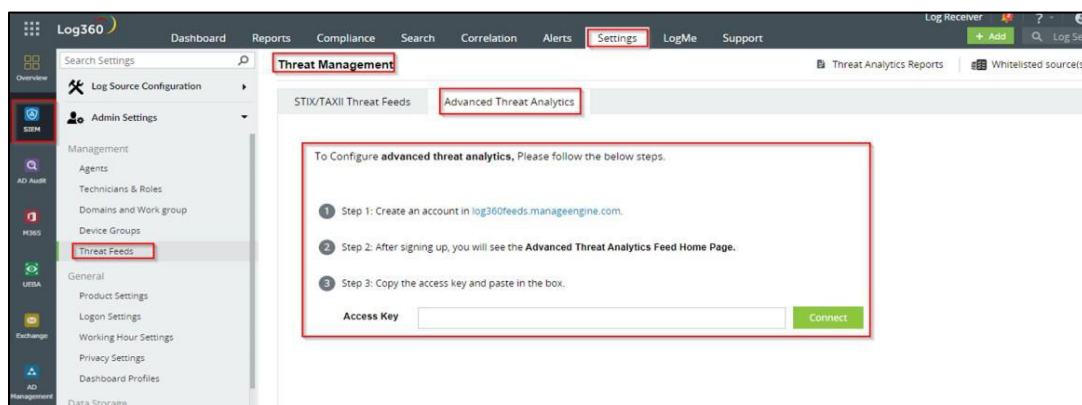


Figura 15 Configuración ATA. Fuente. Información obtenida de la plataforma SIEM – ELA.

- ✓ Registrar una cuenta en la nube de Log360 mediante la URL <https://log360feeds.manageengine.com>.
- ✓ Después de registrarse e iniciar sesión, se observará la página de inicio de servidor de Advanced Threat Anality Feed Server.

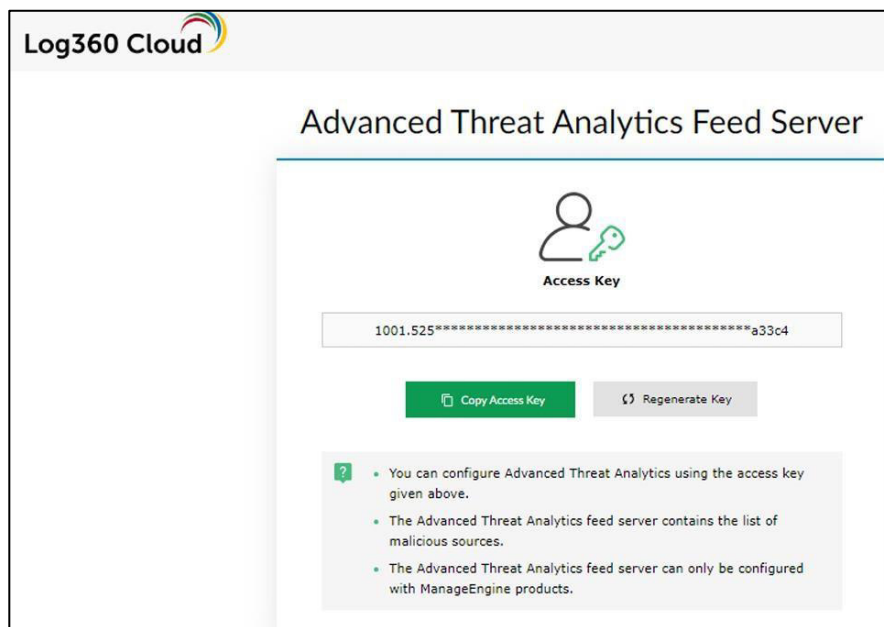


Figura 16 ATA Servidor. Fuente. Información obtenida de la plataforma SIEM – ELA.

- ✓ Copiar el Key de acceso y pegar en la opción Connect para culminar la activación.

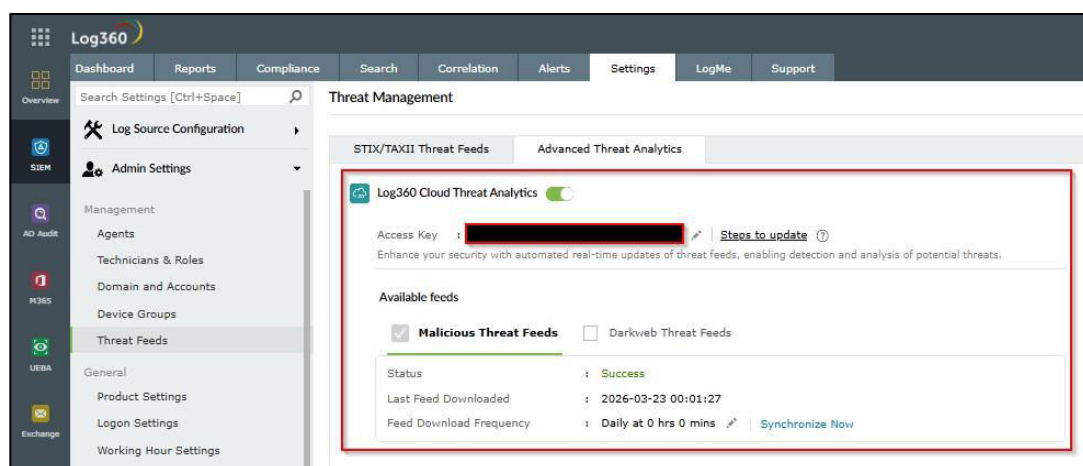


Figura 17 Configuración ATA. Fuente. Información obtenida de la plataforma SIEM – ELA.

4. Configuración del Open Threat Exchange (OTX)

- ✓ Seleccionar la opción Setting → Threat Feeds → Threat Management → STIX/TAXII THREAT Feeds.



Figura 18 Configuración OTX. Fuente. Información obtenida de la plataforma SIEM – ELA.

5. Configuración de la autenticación de Google para los usuarios

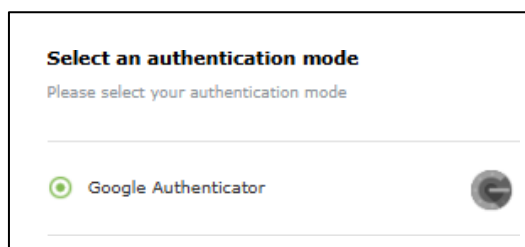


Figura 19 Configuración del modo de autenticación. Fuente. Información obtenida de la plataforma LOG360.

6. Configuración de las alertas

- ✓ Alertas configuradas para la detección y visualización de las amenazas con más detalle, estas alertas son enviadas por correo para una rápida acción.

Dashboard Reports Compliance Search Correlation Alerts Settings LogMe Support						
Manage Profiles						
Alert Profile Type All Alert Profiles						
Alert Name	Type	Severity	Device(s) / Group(s) Configured	Notification Type		
☐ ALERT WILDFIRE SIGNATURE FEED_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT VULNERABILITY EXPLOIT DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT VIRUS DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT URL FILTERING_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT THREAR SOURCE_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT SPYWARE DOWNLOAD DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT SCAN DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT INTERFACE UP DETECTION_UPAO	Custom	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT INTERFACE DOWN DETECTION_UPAO	Custom	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT FLOOD DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT FILETYPE DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT FAILED LOGONS_UPAO	Custom	Attention	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT FAILED LOGONS ADMIN_UPAO	Custom	Attention	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT DNS BOTNET SIGNATURES_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT DATA FILTERING DETECTION_UPAO	Predefined	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT CRITICAL ATTACK_UPAO	Custom	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT CONFIG CHANGED_UPAO	Custom	Attention	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		
☐ ALERT CHASSIS ALARM_UPAO	Custom	Critical	FW-PRINCIPAL-TRUJILLO, FW-SECUNDARI...	Email		

Figura 20 Alertas. Fuente. Información obtenida de la plataforma SIEM – ELA.

3.5.4. Configuración VPN IPsec - Firewall PA-3410

- ✓ Se realizó la configuración en base a las interfaces y redes configuradas en el equipo Firewall PA-3410 del cliente.
- ✓ Esta configuración es fundamental para el envío de la información de eventos y amenazas al SIEM, el cual se encuentra en el Datacenter de Smartglobal.
- ✓ Se configuró la interfaz de túnel:

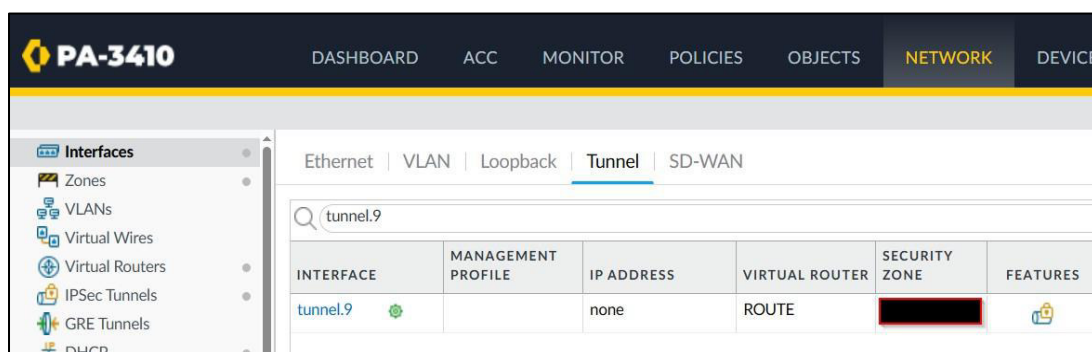


Figura 21 Configuración interfaz de túnel. Fuente. Información obtenida de la GUI del firewall PA-3410.

- ✓ Para la Phase 1 se creó el IKE Crypto Profile, en base a los parámetros establecidos con el otro Peer:

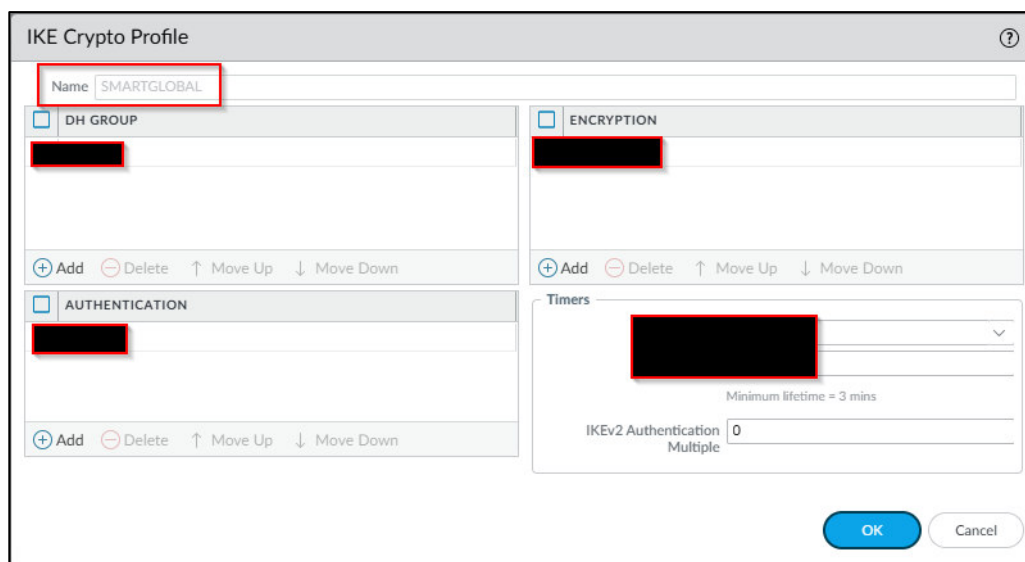


Figura 22 Phase 1 - Ike Crypto Profile. Fuente. Información obtenida de la GUI del firewall PA-3410.

- ✓ Para la Phase 2 se creó el IPsec Crypto Profile, en base a los parámetros establecidos con el otro Peer:

Figura 23 Phase 2 - IPsec Crypto Profile. Fuente. Información obtenida de la GUI del firewall PA-3410.

- ✓ Se configuró el IKE Gateway, en base a los parámetros establecidos con el otro Peer:

Figura 24 IKE Gateway. Fuente. Información obtenida de la GUI del firewall PA-3410.

- ✓ Se creó el túnel IPsec y se agregó los objetos creados previamente.

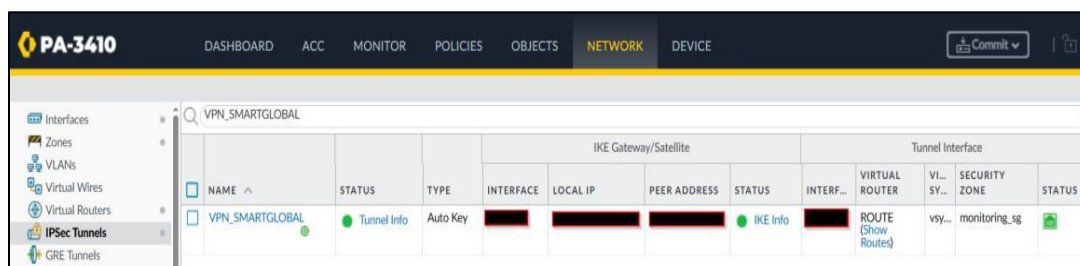


Figura 25 Túnel IPsec. Fuente. Información obtenida de la GUI del firewall PA-3410.

- ✓ Se creó la política de seguridad para la comunicación con el SIEM.

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
234	SMARTGLOBAL-UPAO	SMARTGLOBAL	universal		any	any	any		any	any	any	application-default	Allow

Figura 26 Política de seguridad. Fuente. Información obtenida de la GUI del firewall PA-3410.

3.5.5. Integración ELA – PA-3410

Configuración en la plataforma ELA

- ✓ En el ELA se agregó las IPs de los equipos firewalls Palo Alto de modelo PA-3410 del cliente de la sede Trujillo:

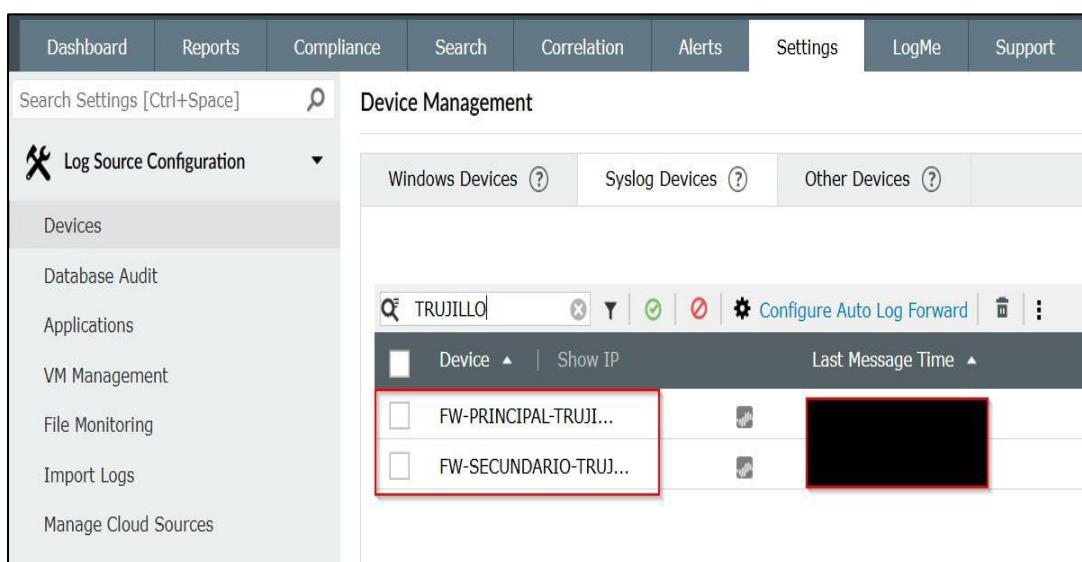


Figura 27 Integración – Equipos PA-3410. Fuente. Información obtenida de la plataforma SIEM – ELA.

Configuración en el Firewall PA-3410

- ✓ En el Firewall Palo Alto se apuntó a la IP que se tiene configurado en la herramienta SIEM - ELA que se encuentran en el Datacenter de Smartglobal.

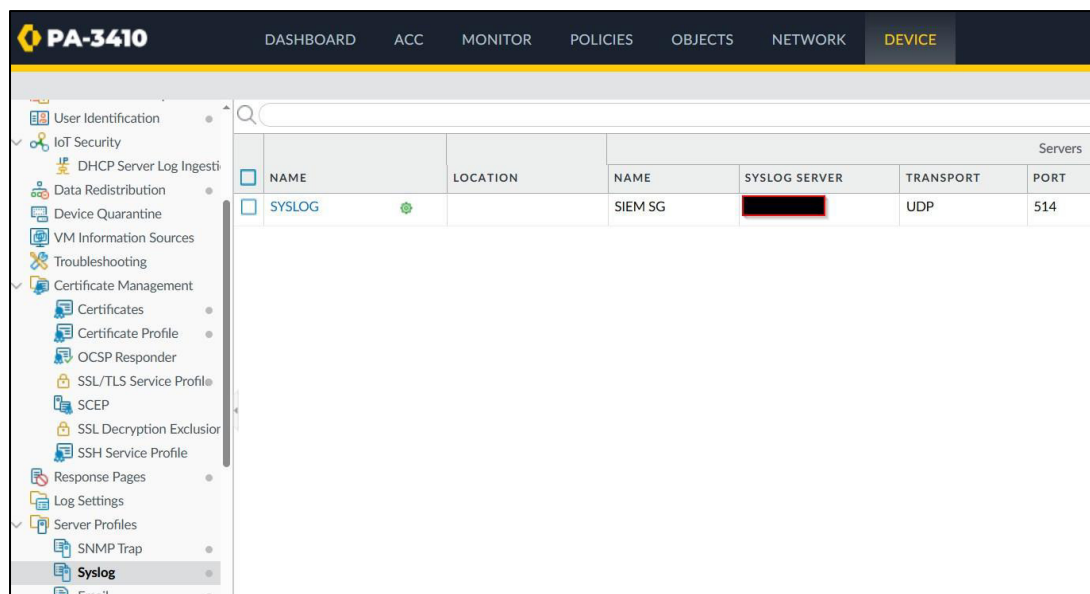


Figura 28 Integración – SIEM-ELA. Fuente. Información obtenida de la GUI del firewall PA-3410.

3.5.6. Configuración Cortex XDR

Información del Tenant:

- ✓ Se muestra el Tenant que se ha desplegado para el cliente UPAO el cual consta de 250 agentes:

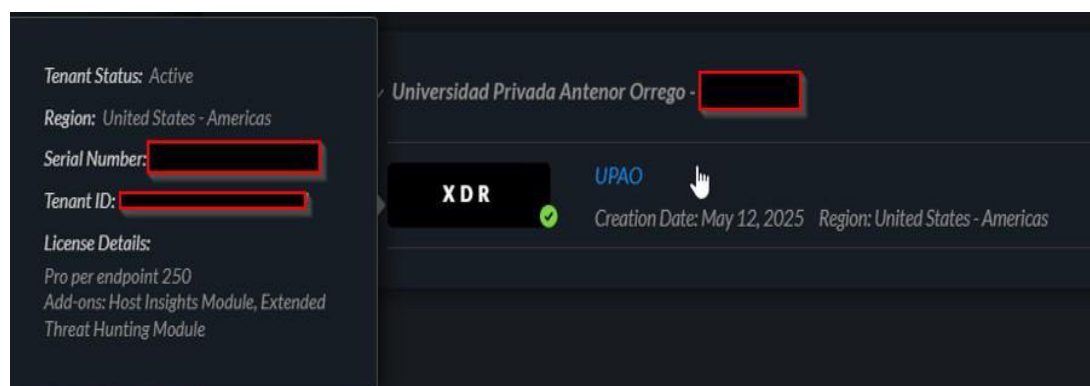


Figura 29 Tenant activado. Fuente. Información obtenida de la plataforma Cortex XDR.

Dashboard:

- ✓ Se muestra el dashboard del equipo donde se observa un resumen de alertas e incidencias.

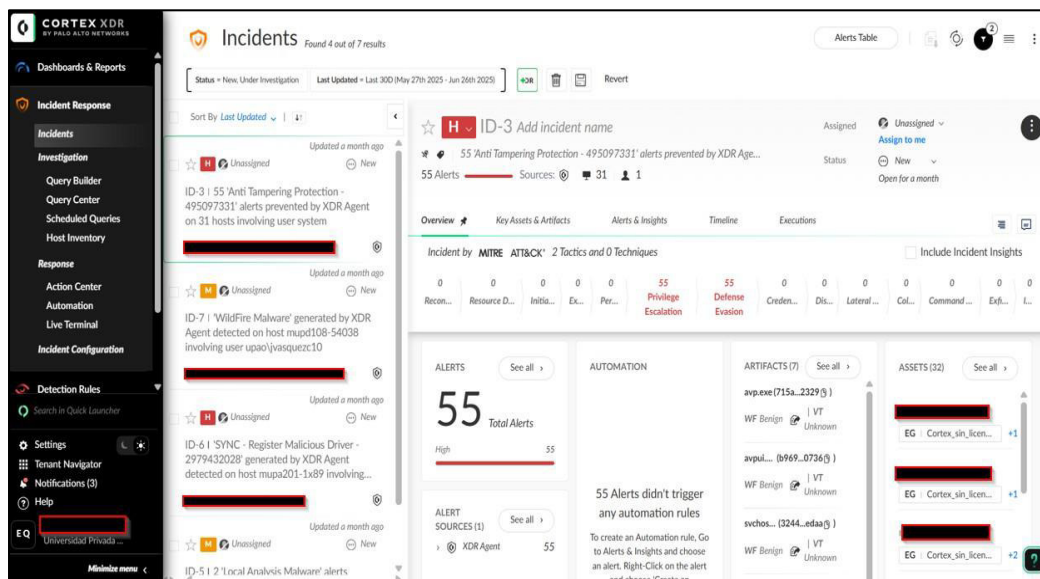


Figura 30 Dashboard Cortex. Fuente. Información obtenida de la plataforma Cortex XDR.

Endpoints registrados:

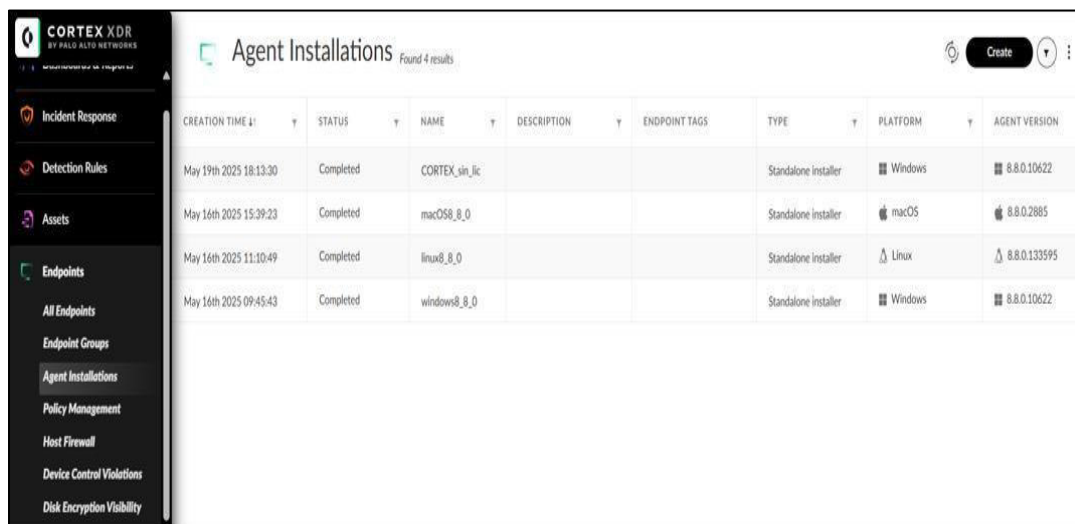
- ✓ En la siguiente imagen se muestra la lista de equipos registrados.

Endpoint Name	Endpoint Type	Endpoint Status	Operating System	Agent Version	IP Address
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Server	Connected	Windows Server 2019	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	
	Workstation	Connected	Windows 10	8.8.0.10622	
	Workstation	Connected	Windows 11	8.8.0.10622	

Figura 31 Endpoints Registrados. Fuente. Información obtenida de la plataforma Cortex XDR.

Agentes Instalados:

- ✓ Se muestra la lista de agentes instalados en los endpoints según la versión del SO de los equipos finales.

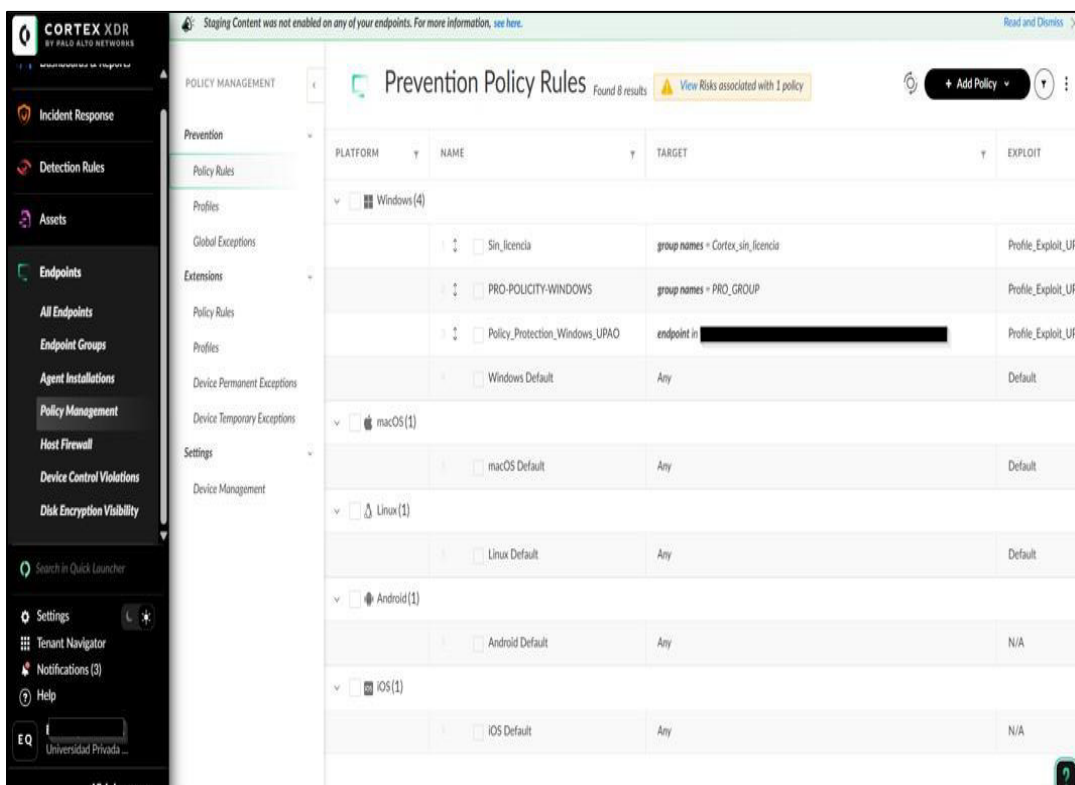


CREATION TIME	STATUS	NAME	DESCRIPTION	ENDPOINT TAGS	TYPE	PLATFORM	AGENT VERSION
May 19th 2025 18:13:30	Completed	CORTEX_sin_lic			Standalone installer	Windows	8.8.0.10622
May 16th 2025 15:39:23	Completed	macOS8_8_0			Standalone installer	macOS	8.8.0.2885
May 16th 2025 11:10:49	Completed	linux8_8_0			Standalone installer	Linux	8.8.0.133595
May 16th 2025 09:45:43	Completed	windows8_8_0			Standalone installer	Windows	8.8.0.10622

Figura 32 Agentes. Fuente. Información obtenida de la plataforma Cortex XDR.

Políticas:

- ✓ Se muestran las políticas aplicadas en la herramienta de Cortex XDR.



PLATFORM	NAME	TARGET	EXPLOIT
Windows (4)	Sin_licencia	group names = Cortex_sin_licencia	Profile_Exploit_UPAC
	PRO-POLICY-WINDOWS	group names = PRO_GROUP	Profile_Exploit_UPAC
	Policy_Protection_Windows_UPAC	endpoint in [REDACTED]	Profile_Exploit_UPAC
	Windows Default	Any	Default
macOS (1)	macOS Default	Any	Default
Linux (1)	Linux Default	Any	Default
Android (1)	Android Default	Any	N/A
iOS (1)	iOS Default	Any	N/A

Figura 33 Políticas. Fuente. Información obtenida de la plataforma Cortex XDR.

Esto puede dejar una brecha abierta para posibles infecciones que se puedan dar de forma interna.

Las ventajas que ofrece tener una arquitectura basada en SIEM y Protección de Endpoints con Cortex XDR son las siguientes:

Visibilidad unificada y en tiempo real

Se muestra una visión integral de toda la red, endpoints e incidencias de seguridad.

✓ ELA-SIEM:

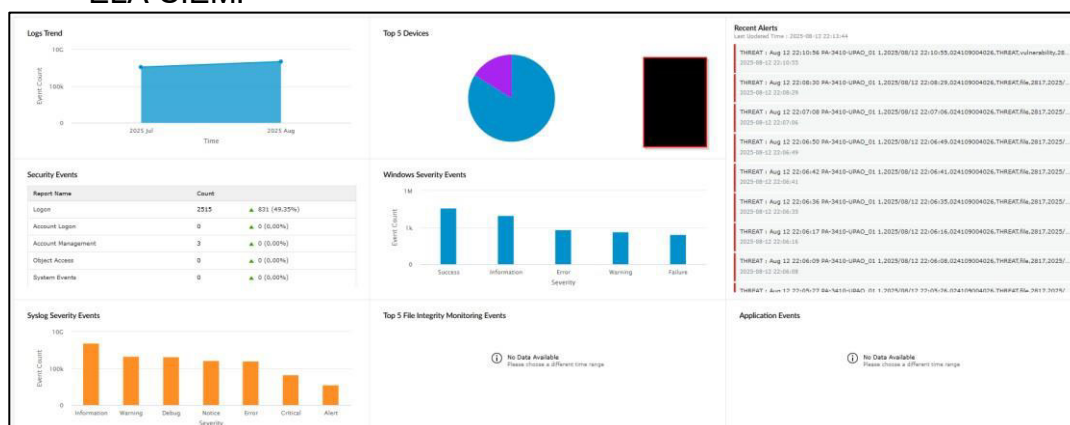


Figura 35 ELA Dashboard. Fuente. Información obtenida de la plataforma SIEM – ELA

✓ Cortex XDR:

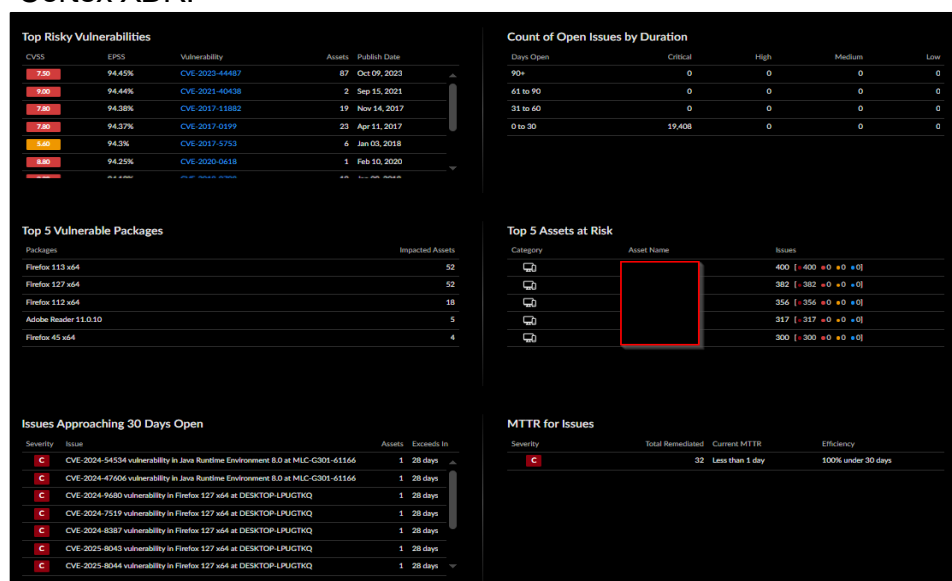


Figura 36 Cortex XDR Dashboard. Fuente. Información obtenida de la plataforma Cortex XDR.

✓ Cortex XDR:

El Cortex XDR en principio toma la acción de “detected”, para posteriormente analizar la incidencia.

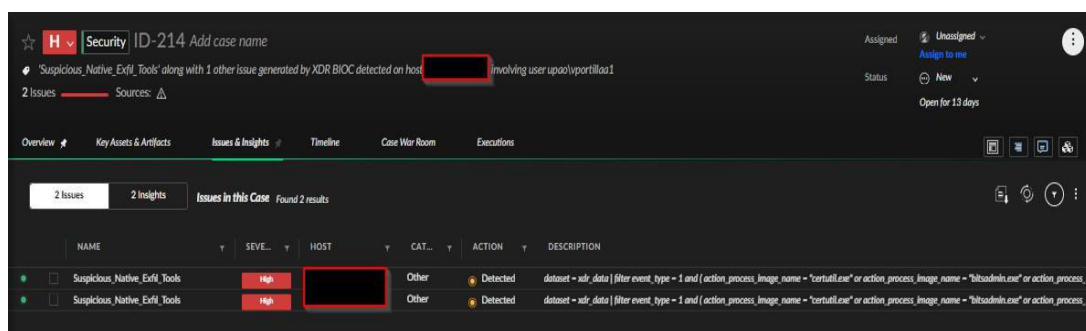


Figura 39 Alertas – Cortex XDR. Fuente. Información obtenida de la plataforma Cortex XDR.

Respuesta automatizada

Posibilidad de aislar endpoints, bloquear IPs y detener procesos maliciosos.

✓ Cortex XDR:

El Cortex XDR al detectar una acción o proceso malicioso, por prevención toma la acción de bloquear esta actividad de manera inmediata.

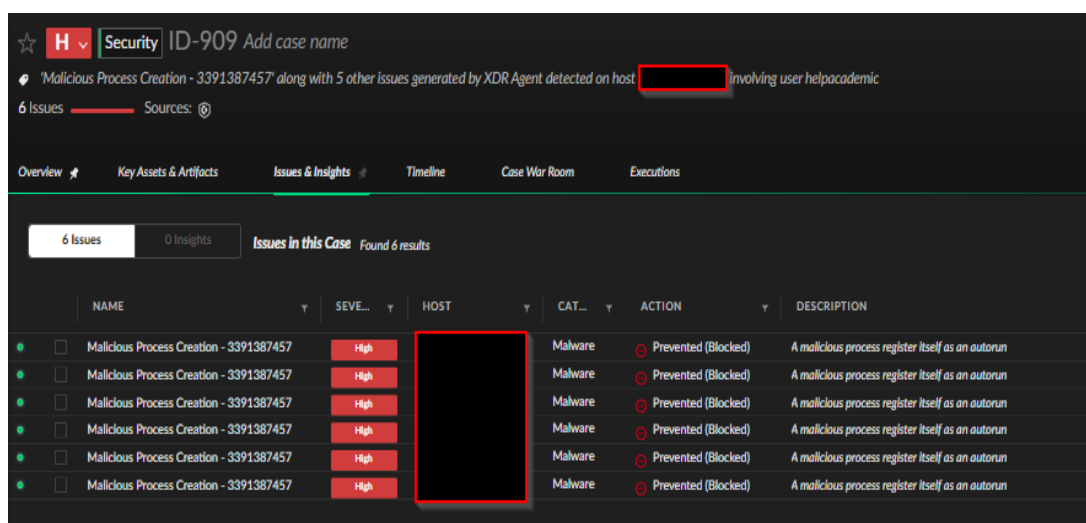


Figura 40 Alertas bloqueadas – Cortex XDR. Fuente. Información obtenida de la plataforma Cortex XDR.

De acuerdo al análisis realizado y expuesto de cada herramienta, se puede observar que el tiempo de respuesta se tiene casi al instante por medio de las alertas configuradas y hasta se pueden automatizar para una acción de forma inmediata. Esto es una ventaja superior a lo que se tenía anteriormente, en la cual no se tenía alertas para detectar algún posible ataque a los servicios internos y tampoco respuestas automatizadas para los endpoints dentro de la red interna de la institución educativa.

3.6.2. *Diseño de la arquitectura de seguridad propuesta*

La adaptación de las soluciones SIEM — ELA y protección de endpoints mediante Cortex XDR al entorno de la UPAO e integrarlo eficientemente al Firewall Palo Alto, se realizó de la siguiente forma:

Visión general de la arquitectura:

- ✓ Firewall PA-3410: Principal función control perimetral y filtrado de tráfico.
- ✓ ELA – SIEM: Centraliza la información y eventos del firewall para un análisis avanzado y generación de alertas.
- ✓ Cortex XDR: Proporciona monitoreo continuo y respuesta ante amenazas en los endpoints institucionales.

Integración de las soluciones:

- ✓ **Firewall Palo Alto → SIEM:**

Envío de logs de tráfico, servicios de snmp y eventos de syslogs mediante la VPN Ipsec levantada entre la PA-3410 de la sede Trujillo y el Firewall Hillstone de Smartglobal.

- ✓ **Firewall Palo Alto → Endpoints → Cortex XDR:**

La información ingresante del Firewall PA-3410 hacia los endpoints es analizado y registrados por el Cortex XDR.

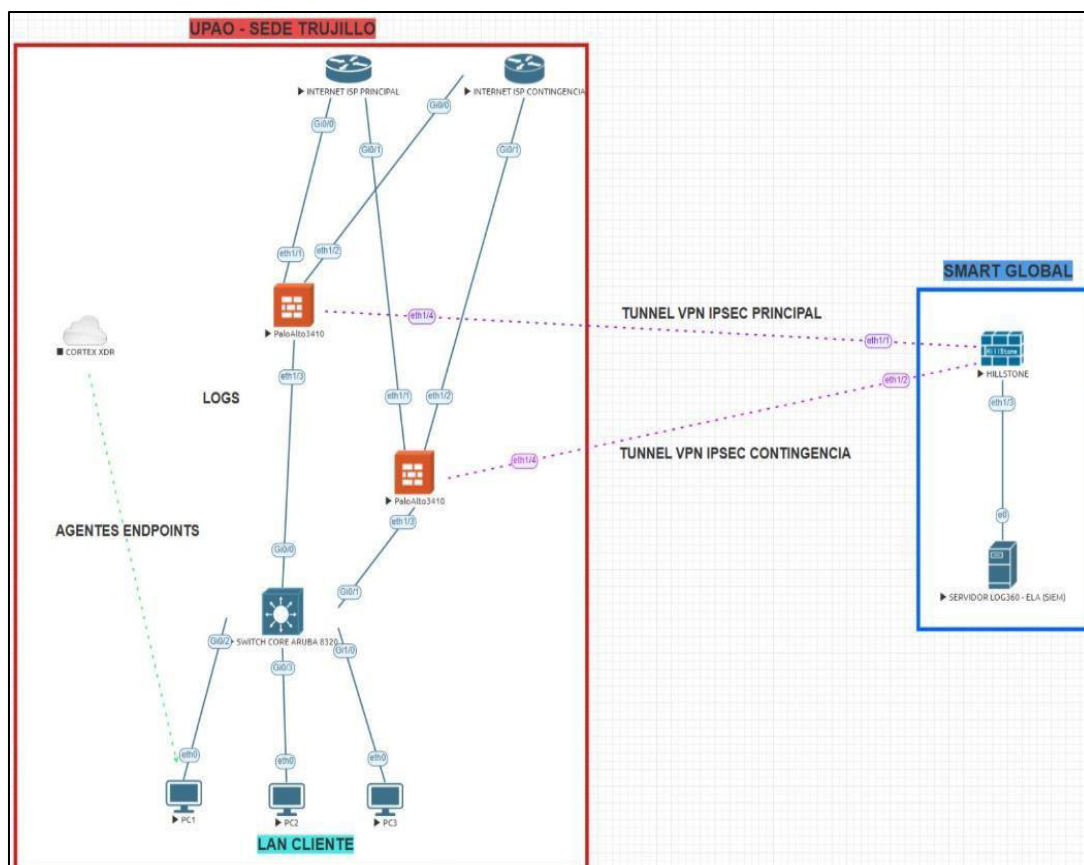


Figura 41 Diagrama de integración. Fuente. Diagrama realizado de mi autoría.

El diseño implementado si bien no tiene una correlación y trabajan de forma independiente ambas herramientas. La idea principal fue la protección general contra las ciberamenazas en tiempo real, tanto para los servicios expuestos a internet, como de los endpoints que maneja la institución educativa.

3.6.3. Análisis de tipos de ciberataques identificados por las arquitecturas SIEM y Cortex XDR

CASO 1: SIEM - ELA & Firewall PA-3410

- ✓ Análisis del Caso ALERTA EXTERNAL THREAT SOURCE

Resumen:

Se ha alertado el siguiente caso ALERTA EXTERNAL THREAT SOURCE con la categoría 'Spam Sources' y 'windows Exploits' desde la IP publica 147.185.132.221 hacia una publicación de la UPAO.

El SIEM - ELA envió una alerta hacia la bandeja de correo de Smartglobal, lo que indica que se ha presentado un evento la cual requiere una pronta revisión y análisis:

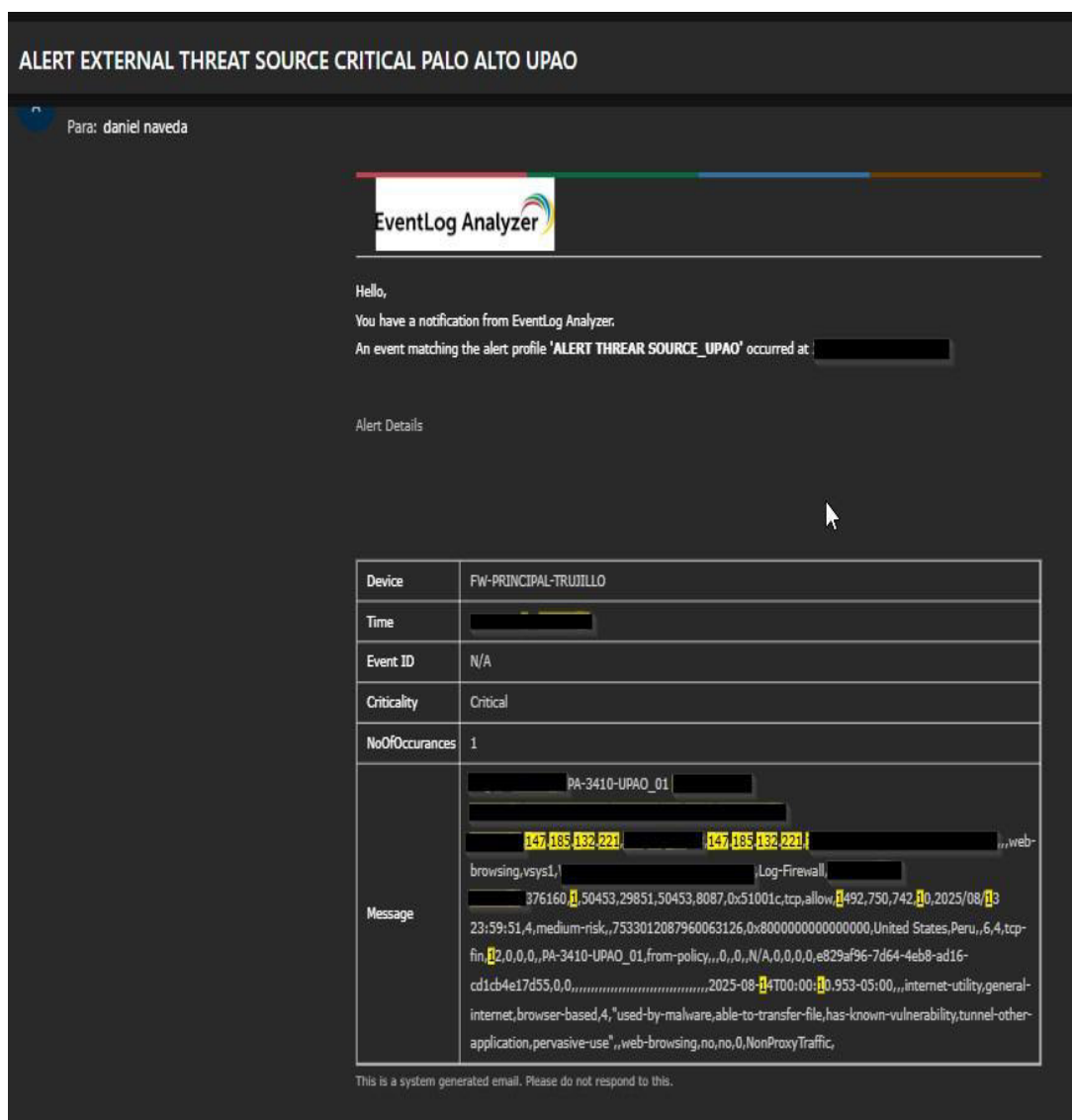


Figura 42 Correo enviado desde el SIEM - ELA. Fuente. Información obtenida de la plataforma de correo – Smartglobal.

DETALLES DEL INCIDENTE:

En la información mostrada por el SIEM - ELA, se puede observar la categoría de la amenaza, la cual es de “spam source y Windows exploits” y la reputación de esta IP a lo largo del tiempo.

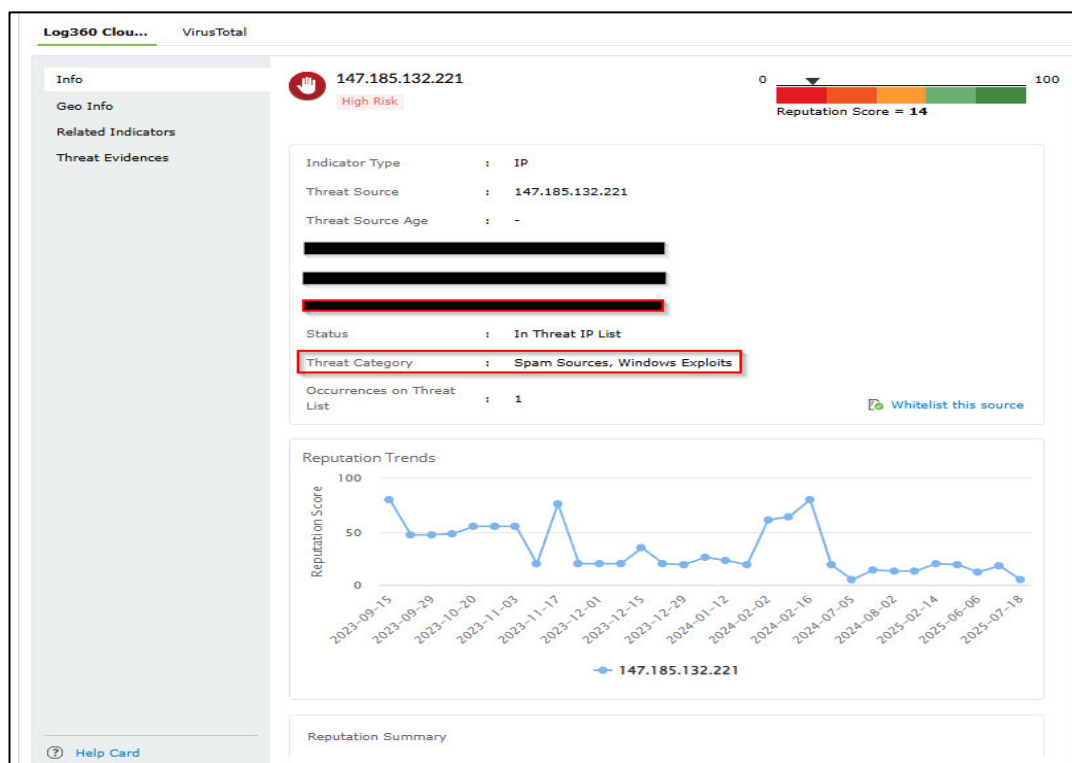


Figura 43 Información general de la amenaza. Fuente. Información obtenida de la plataforma SIEM – ELA.

La herramienta también está mostrando la información geográfica proveniente de la amenaza.

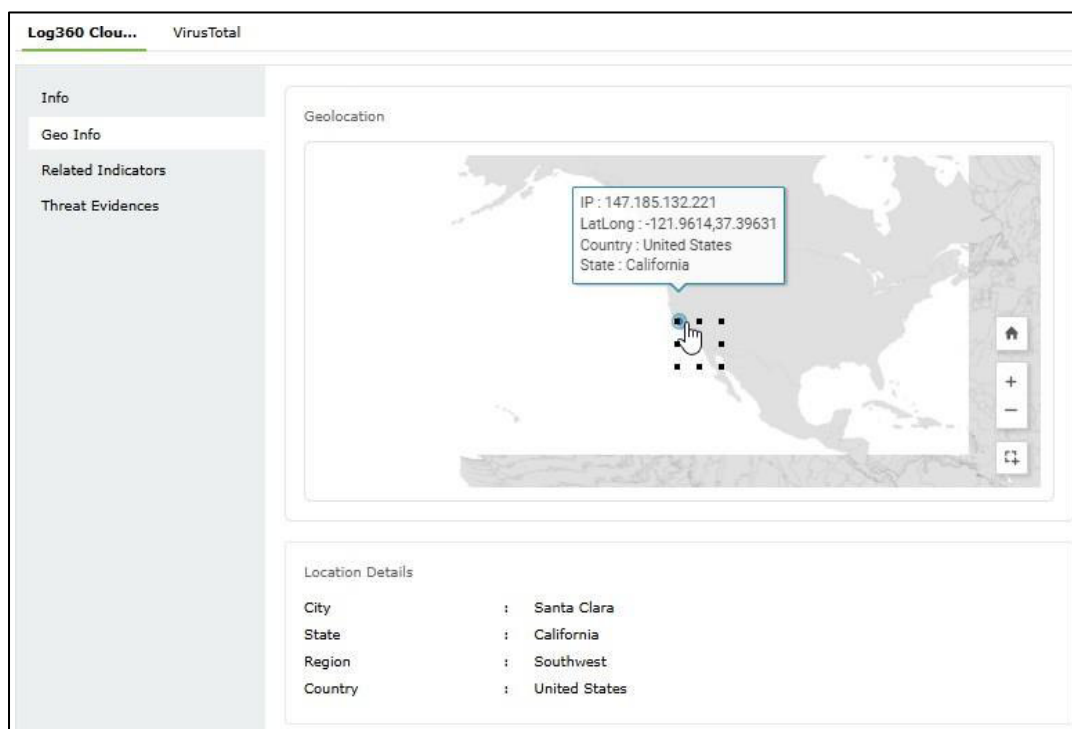


Figura 44 Información geográfica de la amenaza. Fuente. Información obtenida de la plataforma SIEM – ELA.

La herramienta muestra un análisis de reputación de IP/ASN.

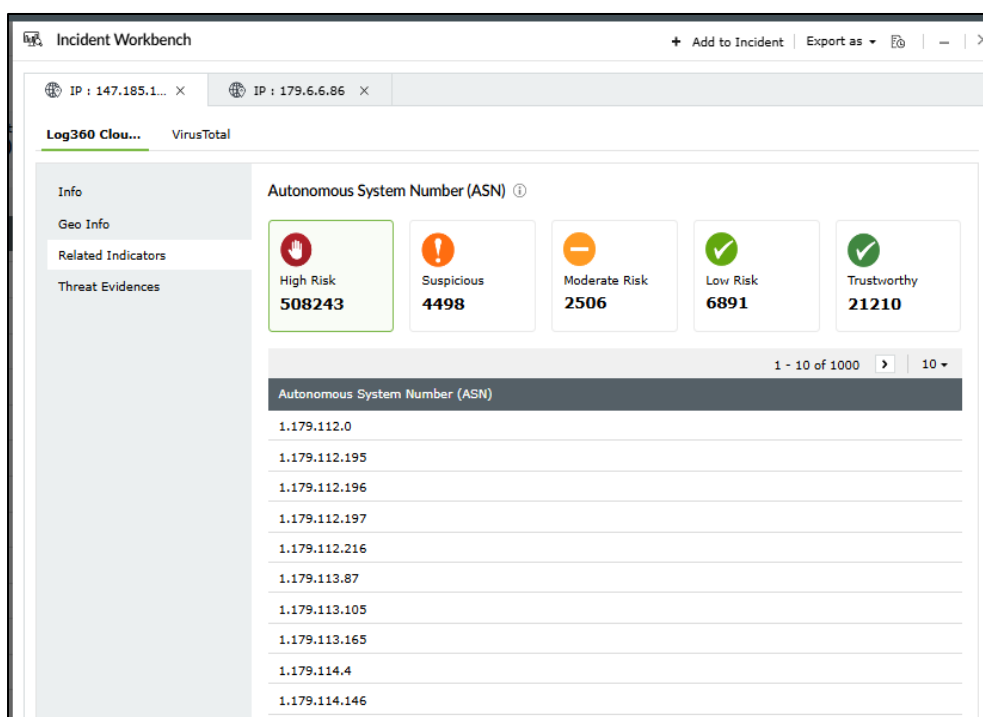


Figura 45 Información de reputación de la amenaza. Fuente. Información obtenida de la plataforma SIEM – ELA.

La herramienta muestra evidencias de la amenaza atreves del tiempo que empezó la interacción con el servicio publicado de la UPAO.

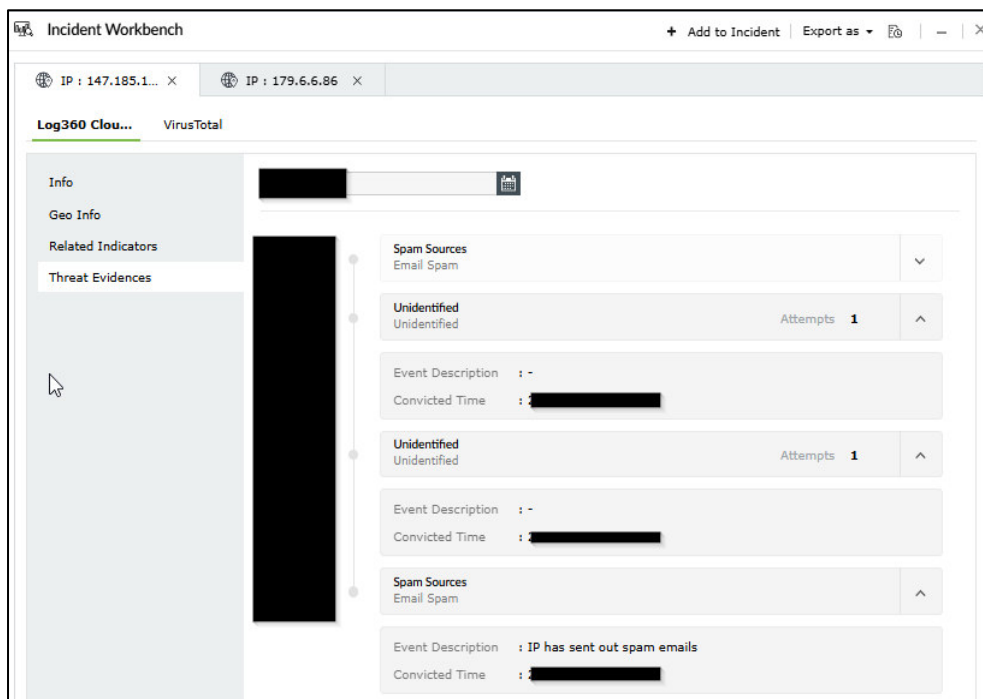


Figura 46 Información de reputación de la amenaza. Fuente. Información obtenida de la plataforma SIEM – ELA.

La herramienta muestra lo revisado por la función ATA, la cual recopila información, en este caso relacionado con la página de VIRUSTOTAL.

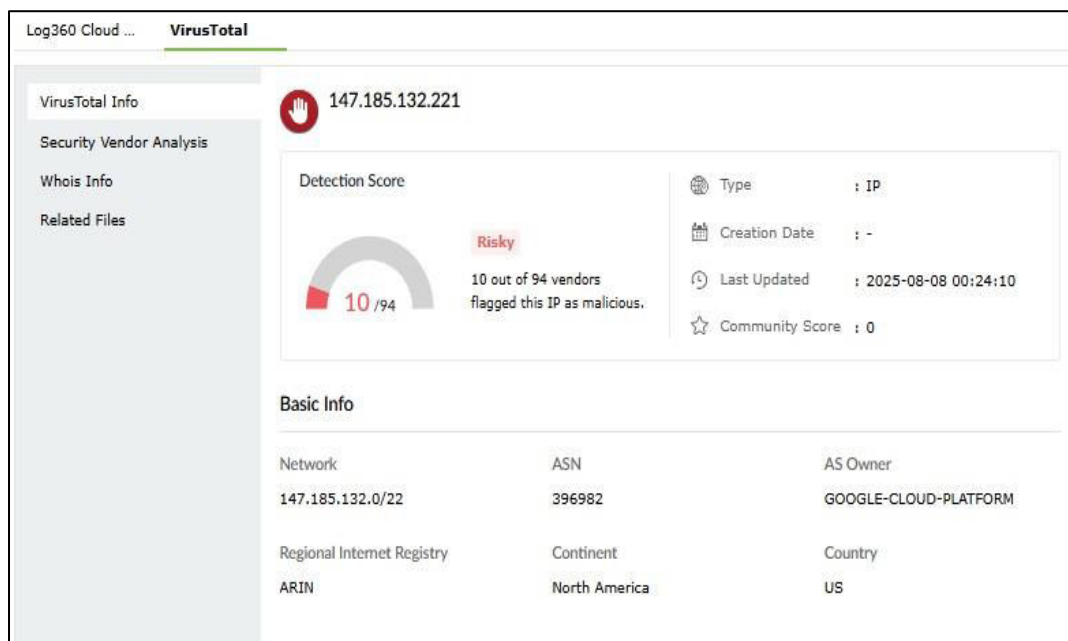


Figura 47 Información recopilada por la función ATA. Fuente. Información obtenida de la plataforma SIEM – ELA.

Se contrasta la información previamente mostrada en el SIEM – ELA, con la WEB de VIRUSTOTAL.

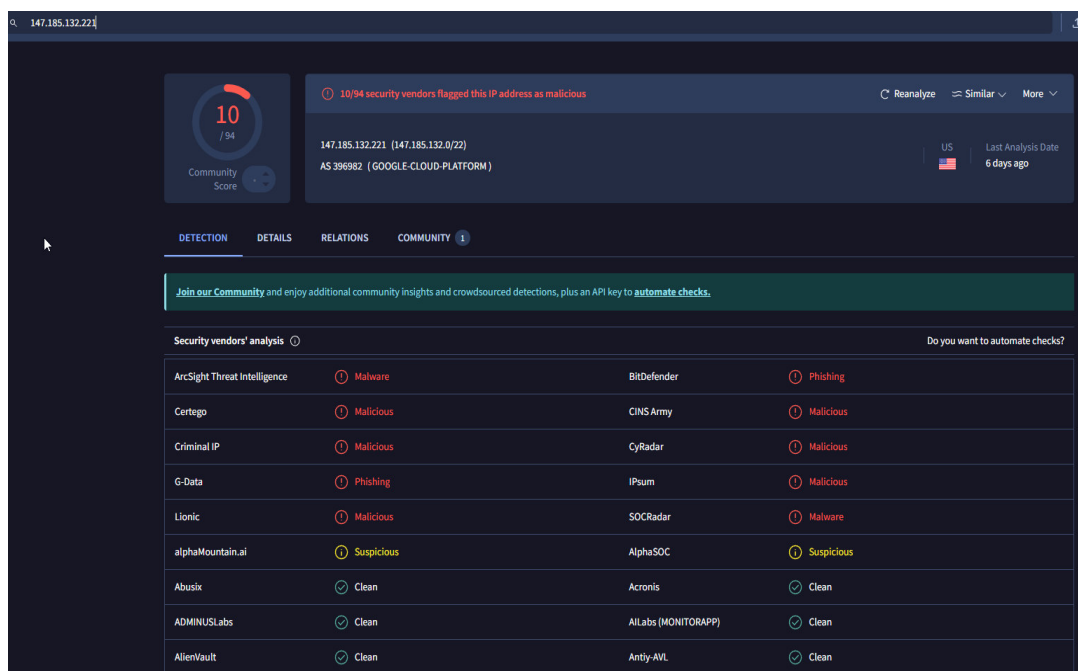
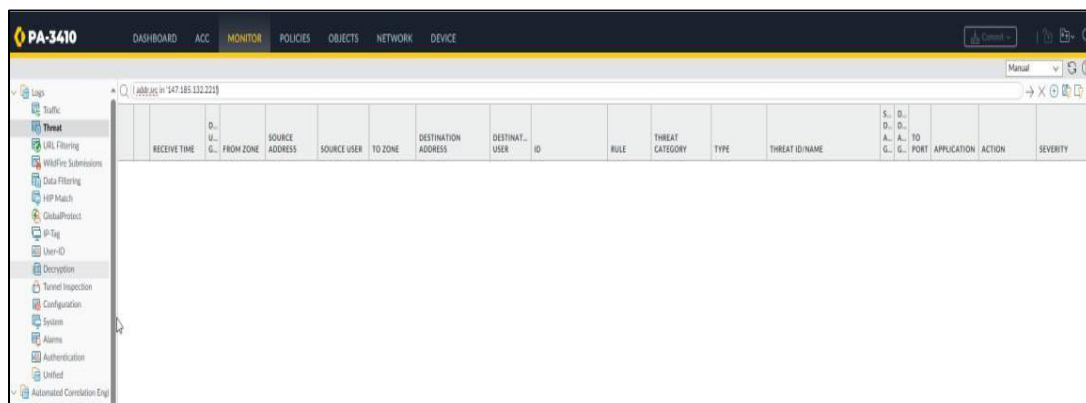


Figura 48 Información recolectada de VirusTotal. Fuente. Información obtenida desde la web Virus Total.

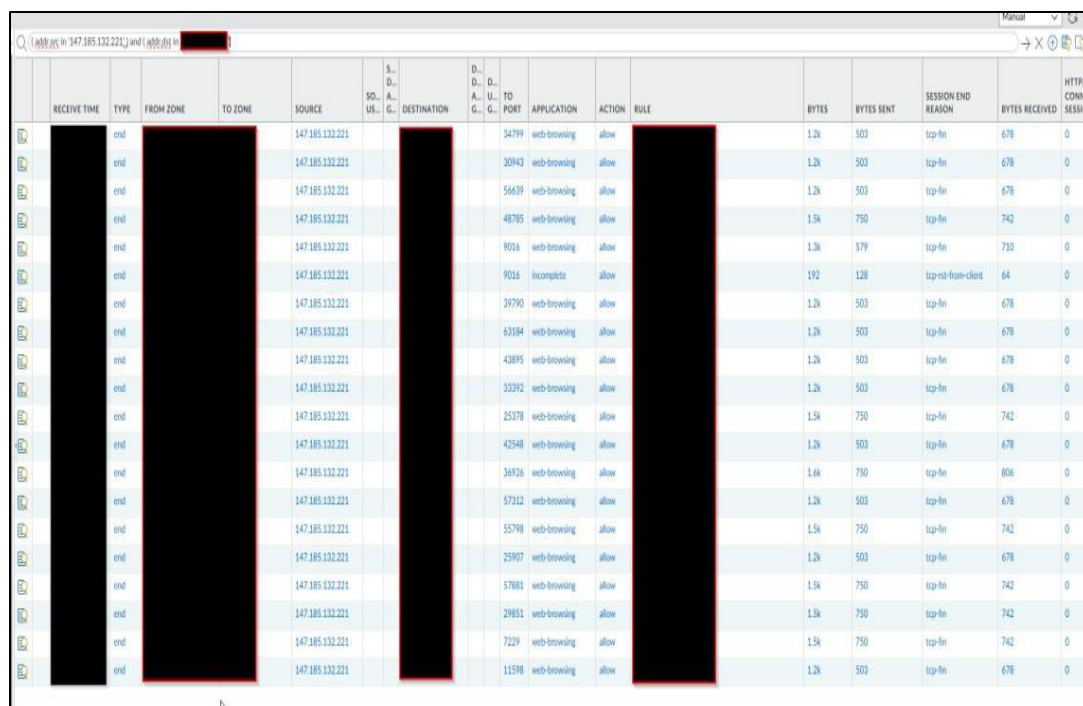
En la información que se muestra en el Firewall PA-3410, se puede observar que el equipo no lo detecta como amenaza. Lo cual valida que una herramienta adicional como la del SIEM — ELA es importante para el análisis de ciberseguridad en la red.



RECEIVE TIME	FROM ZONE	SOURCE ADDRESS	SOURCE USER	TO ZONE	DESTINATION ADDRESS	DESTINATION USER	ID	RULE	THREAT CATEGORY	TYPE	THREAT ID/NAME	SEVERITY
--------------	-----------	----------------	-------------	---------	---------------------	------------------	----	------	-----------------	------	----------------	----------

Figura 49 Logs Threat – Firewall PA-3410. Fuente. Información obtenida de la GUI del firewall PA-3410.

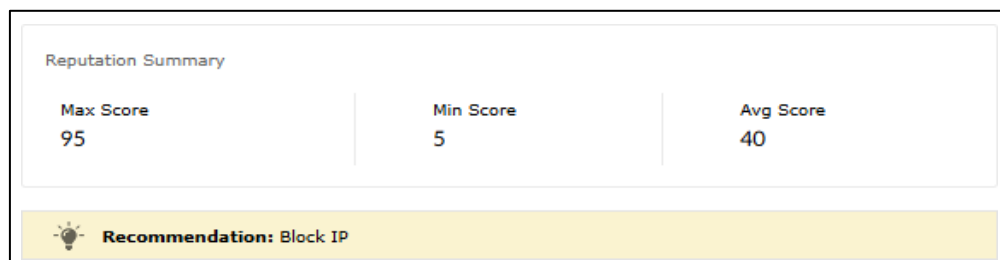
Por lo que se mencionó anteriormente el firewall PA-3410, estaba permitiendo esta comunicación.



RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE ADDRESS	DESTINATION	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	RULE	BYTES	BYTES SENT	SESSION END REASON	BYTES RECEIVED	HTTP/2 CONN. SESSION
end				147.185.132.221				34799	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				30843	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				56639	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				46785	web-browsing	allow		1.5K	750	tcp-fin	742	0
end				147.185.132.221				9016	web-browsing	allow		1.2K	579	tcp-fin	730	0
end				147.185.132.221				9016	incomplete	allow		192	128	tcp-rst-from-client	64	0
end				147.185.132.221				39790	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				63184	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				43895	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				33392	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				25378	web-browsing	allow		1.5K	750	tcp-fin	742	0
end				147.185.132.221				42548	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				36926	web-browsing	allow		1.6K	750	tcp-fin	806	0
end				147.185.132.221				57312	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				55798	web-browsing	allow		1.5K	750	tcp-fin	742	0
end				147.185.132.221				25907	web-browsing	allow		1.2K	503	tcp-fin	678	0
end				147.185.132.221				57681	web-browsing	allow		1.5K	750	tcp-fin	742	0
end				147.185.132.221				29851	web-browsing	allow		1.5K	750	tcp-fin	742	0
end				147.185.132.221				7229	web-browsing	allow		1.5K	750	tcp-fin	742	0
end				147.185.132.221				11598	web-browsing	allow		1.2K	503	tcp-fin	678	0

Figura 50 Logs Threat – Firewall PA-3410. Fuente. Información obtenida de la GUI del firewall PA-3410.

Además de lo comentado anteriormente, la herramienta SIEM - ELA, como conclusión, está recomendando bloquear esta IP pública que se muestra.



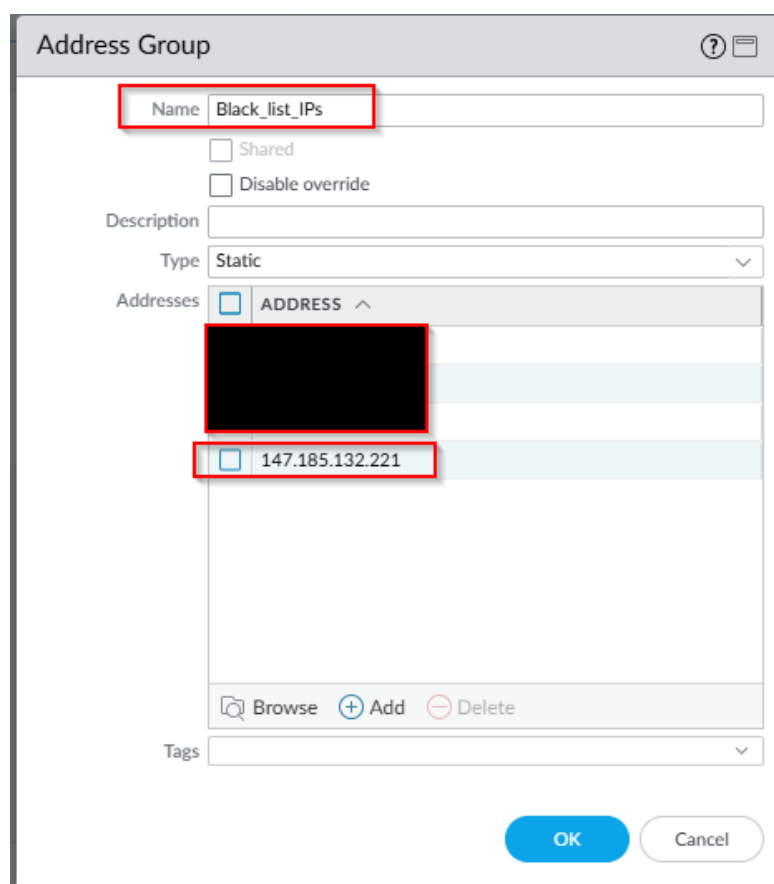
Reputation Summary		
Max Score	Min Score	Avg Score
95	5	40

 **Recommendation:** Block IP

Figura 51 Conclusión de la información de la amenaza. Fuente. Información obtenida de la plataforma SIEM – ELA.

ACCIONES EJECUTADAS:

Se procedió con el bloqueo en el Firewall PA-3410, el cual se agregó la IP en el grupo “Black_list_IPs”.



Address Group

Name: Black_list_IPs

☐ Shared

☐ Disable override

Description:

Type: Static

Addresses:

ADDRESS

☒ 147.185.132.221

Tags:

Buttons: Browse, Add, Delete

Buttons: OK, Cancel

Figura 52 Address Group – Firewall PA-3410. Fuente. Información obtenida de la GUI del firewall PA-3410.

El grupo mencionado anteriormente se encuentra en las siguientes políticas de bloqueo en el Firewall PA-3410.

2	BLACK_LIST_OUT	PA...	BLACK_LIST	universal	any	any	any	any	any	Black_list_IPs	any	any	application-default	Deny
3	BLACK_LIST_IN	PA...	BLACK_LIST	universal	any	Black_list_IPs	any	any	any	any	any	any	application-default	Deny

Figura 53 Policy security – Firewall PA-3410. Fuente. Información obtenida de la GUI del firewall PA-3410.

CASO 2: Endpoints & Cortex XDR

✓ Análisis del Caso ID-189

Resumen:

Se ha registrado el incidente ID-189 con la categoría '**Malware**' en un dispositivo 'MUPL2B-XXXXX'.

La herramienta describe las alertas como “Suspicious executable detected”, lo que indica que se ha detectado un archivo ejecutable (como un .exe) que presenta comportamientos o características inusuales o potencialmente maliciosas, detectada por el agente XDR en el host, asociada al usuario int\X.

☐	NAME	SEVERI...	HOST	CATEGORY	ACTION	INITIATOR PATI
☐	WildFire Malware	Medium	MUPL2B-	Malware	Prevented (Blocked)	C:\Users\bibliote
☐	WildFire Malware +2	Medium	MUPL2B-	Malware	Prevented (Blocked)	C:\Users\bibliote
☐	WildFire Malware	High	MUPL2B-	Malware	Prevented (Post Detected)	C:\Users\bibliote

Figura 54 Alertas relacionadas al incidente ID-189. Fuente. Información obtenida de la plataforma Cortex XDR.

DETALLES DEL INCIDENTE:

Se brinda detalles como el nombre de la alerta, la ruta y así como el score e indicadores de compromiso (IoC).

Tabla 5 Detalles del incidente ID-189

File Name	WildFire Malware
File Path	C:\Users\X\Documents\WonderfulAppAdsDrainage\UpdateHelper\ExtractDir\MicrosoftUpdateHelper.exe
Wildfire Score	Malware
SHA- 256	9a36ee0d11b74c2f48d343bee8d5d033d291c79b60ae7c6b17f196c6fe0cf342
STATUS	Prevented (Blocked)

Fuente. Información obtenida de la herramienta Cortex XDR.

ACCIONES EJECUTADAS:

El archivo MicrosoftUpdateHelper.exe, ubicado en la ruta C:\Users\X\Documents\WonderfulAppAdsDrainage\UpdateHelper\ExtractDir\MicrosoftUpdateHelper.exe puntuación que lo clasifica como malware. Las alertas fueron bloqueadas preventivamente Prevented (Blocked).

De acuerdo al análisis realizado en los casos expuestos, ambas herramientas identificaron las amenazas, los catalogó; brindando información crucial de estos eventos. En el SIEM — ELA se observa que la amenaza detectada catalogada como “Spam Sources” y “windows Exploits” con la herramienta, no se observa en el Firewall palo alto, esto puede generar un problema si no se tendría esta herramienta para una detección y acción temprana. Para el caso del Cortex XDR, la ejecución de un programa malicioso detectado como “Malware” y la acción temprana de la herramienta, se pudo controlar un posible esparcimiento de una potencial amenaza que podría haber infectado a diferentes endpoints dentro de su red interna.

4. CAPITULO IV: DISCUSION DE RESULTADOS

4.1. Descripción de la implementación

En este capítulo se mostrará que la implementación integral del SIEM con la solución Cortex XDR, complementada con el firewall PA-3410, logró establecer un diseño de monitoreo y detección de incidentes más robusto en la arquitectura de red de la UPAO.

Uno de los hallazgos más significativos fue la variación al nivel de una visibilidad centralizada, con la cual no se contaba con la arquitectura anterior. Antes de su puesta en marcha, la identificación de eventos se basaba en evaluaciones manuales y parciales de los registros locales, lo que ocasionaba demoras sustanciales en la detección de las diferentes amenazas. Con el SIEM integrado con el firewall PA-3410, el tiempo para la detección de incidentes de red se ha reducido de manera estimada de varias horas a menos de 10 minutos, lo que permite tomar acción de forma más rápida.

En el contexto de los endpoints, Cortex XDR evidenció una notable efectividad en la detección de comportamientos atípicos, como procesos anómalos, conexiones no permitidas y la detección temprana de malwares. En pruebas internas, cerca del 92% de las alertas producidas por el Cortex XDR se relacionaron con amenazas auténticas, mientras que la tasa de falsos positivos permaneció por debajo del 5%, lo que permitió una mejor priorización de las acciones correctivas.

A pesar de que en esta implementación del SIEM únicamente recopila datos del Firewall PA-3410 y no establece una correlación directa con Cortex XDR,

la integración de ambas soluciones brindó al equipo de ciberseguridad una mayor amplitud de protección, apoyo con el monitoreo de la red, además de una supervisión centralizada de los eventos de la red, restricción ante tráfico malicioso y reportes detallados de amenazas externas, para una respuesta inmediata contra las incidencias que se puedan presentar.

El análisis post implementación reveló que la integración parcial de estas soluciones ya proporciona beneficios considerables, disminuyendo el riesgo de intrusiones y aumentando la trazabilidad de los incidentes. Sin embargo, se detectó como una oportunidad futura la creación de un sistema de correlación avanzada que combine los eventos de red y endpoints para mejorar la identificación de amenazas complejas y ataques con múltiples vectores.

4.2. Evaluación económica

Se presenta el presupuesto de proyecto de implementación (ver Tabla 6 y 7) para el servicio de ciberdefensa para la UPAO, en el que se precisa lo siguiente:

- El costo de los equipos firewalls, el servicio de Cortex XDR y las licencias correspondientes, fue proporcionado por los proveedores de Ingram Micro S.A.C.
- El costo del servicio y licencia del SIEM-ELA, fue proporcionado por los proveedores de Techcore Solutions.
- El costo del soporte del servicio de cibersoc, fue proporcionada por la empresa Smartglobal S.A.C.
- El costo de la prestación de accesoria, fue proporcionada por la empresa Smartglobal S.A.C.

Tabla 6 Presupuesto del proyecto – Firewalls & Cortex XDR – Marca: Palo Alto

Descripción De la Solución /					
Part Number	Term (m)	Descripción	Cant.	Precio Socio de Negocio	
PAN-PA-3410	-	Palo Alto Networks PA-3410 with redundant AC power supplies	2	\$273,001.00	
PAN-PA-3410-BND-CORESEC-3YR	36	PA-3410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN), 3 years (36 months) term	2		
PAN-PA-3410-GP-3YR	36	PA-3410, GlobalProtect subscription, 3 years (36 months) term.	2		
PAN-PA-3410-VSYS-10	-	Virtual systems upgrade - Additional 10 virtual systems (1 to 11) for PA-3410	2		
PAN-SVC-PREM-3410-3YR	37	Premium support 3-year term, PA-3410	2		
PAN-SFP-SX	-	SFP form factor, SX 1Gb optical transceiver, 550m reach on OM2 MMF, duplex LC, IEEE 802.3z 1000BASE-SX compliant	12		
PAN-SFP-PLUS-SR	-	SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant	8		
PAN-PWR-450W-AC	-	PA-3400, PA-1400, ION 5200 and ION 9200 450W spare power supply	2		
PAN-PA-3400-RACK4	-	Palo Alto Networks PA-3400 Series 4 post rack mount kit	2		
PAN-PA-1410	-	Palo Alto Networks PA-1410	2		
PAN-PA-1410-BND-CORESEC-3YR	36	PA-1410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN), 3 years (36 months) term	2		
PAN-PA-1410-GP-3YR	36	PA-1410, GlobalProtect subscription, 3 years (36 months) term.	2		
PAN-PA-1410-VSYS-5	-	Virtual systems upgrade - Additional 5 virtual systems for PA-1410	2		
PAN-SVC-PREM-1410-3YR	37	PA-1410, Premium support, 3 years (36 months) term.	2		
PAN-SFP-SX	-	SFP form factor, SX 1Gb optical transceiver, 550m reach on OM2 MMF, duplex LC, IEEE 802.3z 1000BASE-SX compliant	12		
PAN-SFP-PLUS-SR	-	SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant	8		
PAN-1RU-RACK-KIT-4POST	-	Palo Alto Networks 4-Post rack mount kit for 1U PA-1400, ION 5200 and ION 9200	2		
PAN-PWR-450W-AC	-	PA-3400, PA-1400, ION 5200 and ION 9200 450W spare power supply	2		
PAN-M-300	-	Palo Alto Networks M-300, 16TB RAID storage (4 8TB RAID certified drives preinstalled), Dual power supplies. Rack mount rails included.	1		
PAN-M-300-P-25	-	Panorama central management software license, 25 devices or log collector for the M-300	1		
PAN-SVC-PREM-M-300-P-25-3Y	37	Premium support 3-year term, Panorama M-300 25 devices or log collector	1		
PAN-XDR-ADV-EP	38	Cortex XDR Pro for 1 endpoint, includes 30 days of data retention and standard success	250		
PAN-XDR-HOST-INST	38	Host Insights add-on for Cortex XDR	250		
PAN-XDR-XTH	38	Extended Threat Hunting (enhanced visibility) add-on for Cortex XDR ProEP/Cloud (price per Endpoint). Includes 30 days of data retention.	250		
				Subtotal	\$ 273,001.00
				18%	\$ 49,140.18
				Total	\$ 322,141.18

Fuente. Información obtenida de la empresa Smartglobal S.A.C.

Tabla 7 Presupuesto del proyecto – SIEM - ELA – Marca: Manage Engine

Item	Descripción	UNIT	Cant	Precio Canal Unitario anual	Periodo anual	Precio Canal Total	
1	Evaluar la seguridad informática de forma Externa/Interna, mediante la ejecución de pruebas y análisis sobre 4 FW Palo Alto. Explorar, verificar, evaluar y reportar las vulnerabilidades existentes en los sistemas informáticos, redes de datos, aplicaciones incluyendo las webs, bases de datos, servidores, equipos móviles, etc. Simular posibles escenarios donde se reproduzcan ataques o penetraciones de manera controlada, así como actividades propias de individuos no autorizados y/o ajenos a la información como: crackers, hackers, exempleados, empleados, competidores, proveedores, entre otros. Identificar aquellas vulnerabilidades que puedan llegar a redundar en pérdidas económicas o de imagen para la organización o cualquiera de sus asociados. Garantizar la seguridad de los datos de los clientes y que los mismos solo puedan realizar las acciones que le fueron otorgadas, evitando que operen con cuentas de terceros u otros. Proveer recomendaciones, conclusiones y nivel de riesgos, en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades encontradas y verificables y así reducir el riesgo de ocurrencia de un evento desfavorable.	M360/SEC	1	\$ 4.320,00	3	\$ 12.960,00	
						Subtotal	\$ 12.960,00
						IGV 18%	\$ 2.332,80
						Total	\$ 15.292,80

Fuente. Información obtenida de la empresa Smartglobal S.A.C.

El presupuesto de 36 meses por la empresa Smartglobal para gestionar el proyecto de implementación y brindar el servicio de Ciberdefensa fue alrededor de los \$932,725.00.

Corresponde al presupuesto por venta de los equipos y licencia de la marca Palo Alto (ver Tabla 8), y para el servicio de Ciberdefensa y prestación accesoria en un tiempo de 36 meses.

Tabla 8 Presupuesto del proyecto y servicio por 36 meses

Ítem	Unidad	Descripción	P.U.	Sub Total
1	1	ADQUISICIÓN DE EQUIPOS FIREWALL, LICENCIAS XDR Y CONSOLA DE GESTIÓN D LA MARCA PALO ALTO. PRESTACION PRINCIPAL		
1.1.	2 unidades	Equipos PA-3410 [Bundle] Marca Palo Alto Networks, Mode PA3410	188,267.52	376,535.04
1.2.	2 unidades	Equipos PA-1410 [Bundle] Marca Palo Alto Networks, Mode PA1410	115,887.36	231,774.72
1.3.	1 unidad	Equipo Panorama M-300 [Bundle]Marca Palo Alto Network Modelo M300	71,984.64	71,984.64
1.4.	250 unidades	Licencias Cortex XDR Pro [Bundle]Marca Palo Alto Network Modelo -	442.98	110,745.60
2	36 meses	SERVICIO DE CIBERSOC. PRESTACION ACCESORIA	3,157.00	113,652.00
TOTAL, INCLUYE I.G.V. US\$				904,692.00

Fuente. Información obtenida de la empresa Smartglobal S.A.C.

El costo de la venta, implementación y servicio de este proyecto es de \$337,433.98, lo cual es equivalente al 36.18% del total de la inversión realizada en el proyecto.

5. CAPITULO V: CONCLUSIONES

Respecto el primer objetivo del presente trabajo de suficiencia profesional, se logró analizar las ventajas de la implementación de la herramienta SIEM y del Cortex XDR, el cual brindó un tiempo de respuesta optimo de acuerdo a las alertas configuradas, mayor detalle de los diferentes ataques, locación de origen de los diferentes ataques cibernéticos, un registro de estos eventos, categorización de la reputación de la amenaza de diferentes fuentes y una plataforma centralizada en donde se pueden observar diferentes estadísticas del tráfico que puede estar teniendo la institución educativa tanto como en tiempo real y para la generación de informes. De este análisis se concluye que a diferencias de arquitecturas tradicionales en donde no se tiene un monitoreo eficiente, esta propuesta brinda una visualización más completa de lo que puede estar afectando los servicios internos, endpoints y la red en general de la institución educativa. Además de proporcionar una respuesta más rápida ante incidentes que se pueden presentar.

Respecto al segundo objetivo del presente trabajo de suficiencia profesional, el diseño (ver Figura 41) donde se muestra el diagrama de integración de ambas herramientas. Este diseño se realizó de forma transparente, esto quiere decir que no intervino en alguno de los servicios internos con lo que la UPAO ya contaba. El diseño fue pensando aprovechando los registros de firewall Palo Alto, el cual se pudo integrar con la herramienta SIEM mediante una VPN site to site entre la sede de Trujillo de la UPAO y la sede en Lima de Smartglobal, en donde se tiene llevando el servicio del SIEM en un servidor. Para la herramienta del Cortex XDR, el cual se encuentra en la nube, se sincroniza los endpoints de la red interna de la UPAO sin afectando su operabilidad. De este diseño se concluye que, si bien, no están

correlacionados ambas herramientas, fueron precisas para las necesidades que presentaba la UPAO. Debido a que se integran en un plan de protección general, el cual se brinda una mejora significativa en la detección, registros y respuestas contra los ciberataques que puedan presentarse.

Finalmente, respecto al tercer objetivo del presente trabajo de suficiencia profesional, se concluye que los diferentes tipos de ciberataques en ambas herramientas identificó la amenaza, la catalogó; brindando información crucial de estos eventos con la arquitectura propuesta. En los resultados se pudo observar que ambas herramientas informaron sobre el tipo de ciberataque que identificó, mostrando una serie de información detallada del impacto que puede generar en la red de la UPAO y además de la respuesta efectiva que se puede realizar al tener una correcta configuración de alertas y respuestas automatizadas. Adicional, con los informes que se pueden generar en ambas herramientas, se puede determinar el tipo de ciberataque que más se frecuente en la UPAO, y con esa información realizar configuraciones de alertas y políticas acorde a los ciberataques que se presentan en el día a día.

6. CAPITULO VI: RECOMENDACIONES

Para un análisis más avanzado integrar las soluciones de información del Cortex XDR al SIEM es un buen plan para activar la correlación de eventos.

Si la topología actual tendría algún cambio a nivel de segmentos o Vlan, tener en consideración en volver a revisar la configuración del túnel VPN Ipsec, debido a que es por donde se transmiten los datos provenientes del Firewall PA-3410.

Tener al personal que gestiona estas soluciones altamente capacitadas para poder entender y analizar las alertas y de esta forma brindar una respuesta oportuna con un plan estratégico.

Realizar chequeos en las versiones, posibles bugs y vulnerabilidades que se puedan dar en las soluciones integradas, y de esta forma evitar brechas que puedan perjudicar el entorno de la arquitectura de red.

Llevar un registro del desarrollo de los incidentes que se puedan presentar y de esta forma estar sincronizados con la realidad de la arquitectura y las soluciones implementadas.

7. CAPITULO VII: REFERENCIAS

- Cyber Magazine. (2023, julio 20). *The history of cybersecurity*. Cyber Magazine.
<https://cybermagazine.com/cyber-security/history-cybersecurity>
- Certauri. (2024, febrero 15). *Understanding the evolution of cybersecurity: A timeline*. Certauri.
<https://www.certauri.com/understanding-the-evolution-of-cybersecurity-a-timeline/>
- Saltzer, J., & Schroeder, M. D. (1975). The protection of information in computer systems.
- Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, 27(5), 781-799.
- Seeley, N. (2024). Seminal Papers in Cybersecurity: A Review (Part 2 of 2).
- Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). *Comprehensive review on cybersecurity: Modern threats and advanced defense strategies*. *Computer Science & IT Research Journal*, 5(2), 293-310. <https://doi.org/10.51594/csitrj.v5i2.758>
- Ban, T., Takahashi, T., Ndichu, S., & Inoue, D. (2023). Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response. *Applied Sciences*, 13(11), 6610.
<https://doi.org/10.3390/app13116610>
- SentinelOne. (2025). SIEM architecture.
<https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/>
- Palo Alto Networks. (s.f.). What is SIEM?
<https://www.paloaltonetworks.lat/cyberpedia/what-is-siem>
- Sleem, A. (2022). *A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age*. *Journal of Cybersecurity and Information Management*,

10(2), 35-46. <https://doi.org/10.54216/JCIM.100204>

López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & García Rosado, D. (2021). *Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures*. *Sensors*, 21(14), 4759.

George, A., et al. (2021). *XDR: The evolution of endpoint security solutions – Superior extensibility and analytics to satisfy the organizational needs of the future*. ResearchGate.

TechTarget. (2024, mayo 15). *What is cybersecurity? Definition, practices, threats*. SearchSecurity. <https://www.techtarget.com/searchsecurity/definition/cybersecurity>

ORSYS Le Mag. (2025, marzo 3). *Ciberamenazas (Riesgo)*. ORSYS Le Mag. Recuperado de <https://www.orsys.fr/orsys-lemag/es/glossary/amenaza-cibernetica>

Palo Alto Networks. (s. f.). *What is Cybersecurity?* Cyberpedia. Recuperado de <https://www.paloaltonetworks.co.uk/cyberpedia/what-is-cyber-security>

Hoverman, D. (2017, junio 13). *6 common types of cyber attacks* [Infographic]. Total Pro Source Blog. Recuperado de <https://blog.totalprosource.com/6-common-types-of-cyber-attacks>

ServerWatch. (2023, 21 de septiembre). *What is a server? Definition, types, and features*. <https://www.serverwatch.com/guides/what-is-a-server/>

Palo Alto Networks. (s.f.). *PA-3400 Series Specification Sheet*. Palo Alto Networks. <https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series>

González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). *Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures*. *Sensors*, 21(14), 4759. <https://doi.org/10.3390/s21144759>

Cloudflare. (2025). *What is IPsec? | How IPsec VPNs work*. Cloudflare Learning Center. Recuperado de <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>

Zohaib, S. M., et al. (2024). *Zero Trust VPN (ZT-VPN): A Systematic Literature Review*. Information.

National Institute of Standards and Technology. (2020). *Guide to IPsec VPNs (SP 800-77 Rev. 1)*. NIST.

ManageEngine. (s. f.). *¿Qué es Log360? Preguntas frecuentes*. Recuperado de <https://www.manageengine.com/latam/log-management/preguntas-frecuentes-faq.html>

ManageEngine. (s. f.). *About EventLog Analyzer*. Recuperado de <https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/Introduction/about-eventlog-analyzer.html>

ManageEngine. (s.f.-b). *System requirements for Log360*. ManageEngine. <https://www.manageengine.com/log-management/system-requirements.html>

8. CAPITULO VIII: ANEXOS

Anexo A:

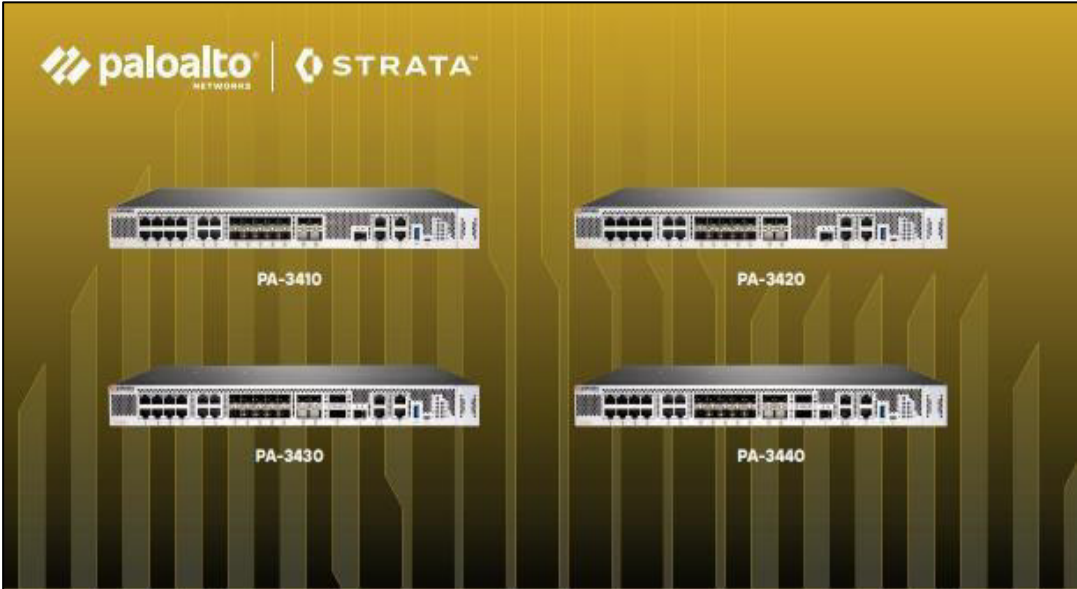
Certificación ISO 27001:2022 – SmartGlobal



Figura A1 Certificación ISO 27001:202. Fuente. Información obtenida de la empresa Smartglobal S.A.C.

Anexo B:

Datasheet Palo alto PA-3410



paaloalto NETWORKS | **STRATA**

PA-3410 PA-3420

PA-3430 PA-3440

Serie PA-3400 Series

Los cortafuegos de nueva generación con aprendizaje automático de la serie PA-3400 Series de Palo Alto Networks, que incluye los modelos PA-3440, PA-3430, PA-3420 y PA-3410, están concebidos para implementaciones de puertas de enlace de internet de alta velocidad. Los dispositivos de la serie PA-3400 Series protegen todo el tráfico.

Características destacadas

- El primer cortafuegos de nueva generación del mundo con aprendizaje automático
- Líder en el Magic Quadrant de Gartner para cortafuegos de red en once ocasiones
- Líder en el informe The Forrester Wave: Enterprise Firewalls, Q4 2022
- Visibilidad y seguridad garantizadas de todos los dispositivos, incluidos los no gestionados de IoT, sin necesidad de sensores adicionales
- La compatibilidad de los cortafuegos de nueva generación con proxies web nativos simplifica y consolida la gestión de las funciones de los cortafuegos y proxies
- Compatibilidad con configuraciones de alta disponibilidad (modos activo/activo y activo/pasivo)
- Rendimiento predecible de los servicios de seguridad
- Administración centralizada con el servicio de gestión de la seguridad de la red Panorama®
- Rentabilidad máxima de la inversión en seguridad y prevención de las interrupciones de la actividad empresarial con Strata™ Cloud Manager

Figura B1 Datasheet Palo alto PA-3410 – parte 1. Fuente. Información obtenida de la página web de Palo alto network.

El primer cortafuegos de nueva generación (NGFW, por sus siglas en inglés) del mundo con aprendizaje automático ayuda a prevenir las amenazas desconocidas, a ver y proteger todos los dispositivos (incluidos los del internet de las cosas, o IoT) y a reducir errores gracias a las recomendaciones de políticas automáticas.

El elemento de control de la serie PA-3400 Series es PAN-OS®, el mismo software que utilizan todos los NGFW de Palo Alto Networks, que clasifica de forma nativa todo el tráfico (incluido el de las aplicaciones, amenazas y contenido) y lo vincula al usuario, independientemente de su ubicación o del tipo de dispositivo que utilice. Las aplicaciones, el contenido y los usuarios —es decir, los elementos que hacen funcionar la empresa— sirven como base para las políticas de seguridad, lo que mejora la estrategia de seguridad y reduce los tiempos de respuesta a incidentes.

Principales funciones de seguridad y conectividad

Cortafuegos de nueva generación con aprendizaje automático

- Integra el aprendizaje automático (ML, por sus siglas en inglés) en el propio cortafuegos para prevenir los ataques sin firmas de forma integrada (cuando se producen ataques basados en archivos) e identificar y detener de inmediato los intentos de phishing nunca vistos.
- Cuenta con procesos de ML basados en la nube que facilitan firmas sin demora y envían instrucciones al NGFW.
- Detecta dispositivos de internet de las cosas (IoT, por sus siglas en inglés) y recomienda políticas analizando el comportamiento; es un servicio basado en la nube e integrado de forma nativa en el NGFW.
- Recomienda políticas automáticamente, lo que ahorra tiempo y reduce la posibilidad de errores humanos.

Inspecciona todo el tráfico de la capa 7, lo que permite identificar y clasificar todas las aplicaciones, en todos los puertos y en todo momento

- Identifica las aplicaciones presentes en la red independientemente del puerto, el protocolo, las técnicas de evasión o el tipo de cifrado (SSL o TLS) empleados. Además, la suscripción al servicio SaaS Security permite detectar y controlar las nuevas aplicaciones automáticamente para seguir el ritmo al boom del software como servicio (SaaS, por sus siglas en inglés).
- Se basa en la aplicación, no en el puerto, para tomar todas las decisiones de habilitación segura de políticas: permitir, denegar, programar, inspeccionar y aplicar la catalogación del tráfico.
- Permite crear etiquetas App-ID™ personalizadas para aplicaciones que sean propiedad de la organización (o, en el caso de que Palo Alto Networks saque nuevas aplicaciones, solicitar el desarrollo de los App-ID correspondientes).
- Identifica todos los datos de la carga útil de una aplicación (p. ej., archivos y patrones de datos) para bloquear los archivos maliciosos y frustrar los intentos de exfiltración de datos.
- Crea informes de utilización de aplicaciones estándar y personalizados, lo que permite, entre otras cosas, elaborar informes relativos al SaaS con información útil sobre todo su tráfico —autorizado y no autorizado— que circula por la red.
- Incorpora la función Policy Optimizer, que permite migrar sin riesgos conjuntos de reglas obsoletos de capa 4 a otros basados en App-ID, más seguros y fáciles de gestionar.

Consulte el [informe tecnológico de App-ID](#) para obtener más información.

Aplica a los dispositivos de usuarios las políticas de seguridad que correspondan, estén donde estén, y adapta también las políticas en función de la actividad de los usuarios

- Permite ver la actividad asociada a determinados usuarios y grupos (y no solo a ciertas direcciones IP), así como aplicarles políticas de seguridad, elaborar informes sobre ellos o someterlos a investigaciones forenses.
- Se integra fácilmente con un amplio abanico de repositorios que contienen información de los usuarios: controladores LAN inalámbricos, redes VPN, servidores de directorio, sistemas de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés), proxies, etc.
- Permite definir grupos de usuarios dinámicos (DUG, por sus siglas en inglés) en el cortafuegos para tomar medidas de seguridad temporales sin esperar a que se aplique ningún cambio a los directorios de usuarios.
- Aplica políticas coherentes estén donde estén los usuarios (en la oficina, en casa, de viaje, etc.) e independientemente del tipo de dispositivo (dispositivos móviles iOS y Android; equipos de escritorio y portátiles macOS, Windows y Linux; infraestructuras de escritorios virtuales [VDI, por sus siglas en inglés] de Citrix y Microsoft; y servidores de terminales).
- Activa la autenticación multifactor (MFA, por sus siglas en inglés) en la capa de la red de cualquier aplicación, un método que, sin necesidad de hacer cambios en la aplicación, impide que las credenciales corporativas se filtren a sitios web de terceros y que, en caso de robo, alguien pueda reutilizarlas.

Figura B2 Datasheet Palo alto PA-3410 – parte 2. Fuente. Información obtenida de la página web de Palo alto network.

- Proporciona medidas de seguridad dinámicas basadas en el comportamiento de los usuarios para imponer restricciones a aquellos que se consideran sospechosos o malintencionados.
- Autentica y otorga autorizaciones a los usuarios de forma coherente, independientemente de dónde estén y de dónde resida su almacén de identidades, para acelerar la transición a una estrategia de seguridad Zero Trust (confianza cero) con Cloud Identity Engine, una novedosa arquitectura en la nube para la seguridad basada en la identidad.

Consulte el [resumen de la solución Cloud Identity Engine](#) para obtener más información.

Impide ocultar actividad maliciosa en el tráfico cifrado

- Inspecciona y aplica políticas al tráfico cifrado con SSL/TLS, tanto el entrante como el saliente, incluido el que emplea los protocolos TLS v1.3 y HTTP/2.
- Proporciona una visibilidad total del tráfico que se transmite a través del protocolo TLS, lo que permite saber, por ejemplo, cuánto tráfico se cifra y qué versiones de SSL/TLS y conjuntos de cifrados se utilizan. Además, toda esta información se obtiene sin recurrir al descifrado.
- Permite controlar el uso de protocolos TLS obsoletos, tipos de cifrado poco seguros y certificados configurados de manera incorrecta, lo que contribuye a mitigar los riesgos.
- Ayuda a implementar el descifrado con facilidad y permite utilizar los logs integrados para solucionar problemas (p. ej., los relacionados con las aplicaciones con certificados fijos).
- En aras de la privacidad y el cumplimiento normativo, permite activar o desactivar el descifrado libremente, por ejemplo, en función de la categoría de URL, el origen y el destino, la dirección, el usuario, el grupo de usuarios, el dispositivo y el puerto.
- Permite crear una copia del tráfico descifrado desde el cortafuegos (técnica que recibe el nombre de «reflejo de descifrado») y enviarla a herramientas de recopilación de tráfico para realizar análisis forenses, ir creando un historial de tráfico o prevenir la pérdida de datos (DLP, por sus siglas en inglés).
- Permite desviar todo el tráfico (TLS descifrado, TLS sin descifrar y tráfico que no se transmite a través del protocolo TLS) a herramientas de seguridad de terceros de forma inteligente con Network Packet Broker, así como optimizar el rendimiento de la red y reducir el gasto operativo.

Consulte este [informe técnico dedicado al descifrado](#) para aprenderlo todo sobre dónde, cuándo y cómo descifrar el tráfico para evitar las amenazas y proteger su negocio.

Ofrece gestión y operaciones unificadas basadas en la IA con Strata Cloud Manager

- **Prevenga interrupciones de red:** con los análisis predictivos, puede prever el estado de las implementaciones y detectar cuellos de botella con hasta siete días de antelación para prevenir interrupciones en las operaciones de forma proactiva.
- **Refuerce la seguridad en tiempo real:** análisis de políticas basados en la inteligencia artificial (IA) y comprobaciones en tiempo real para garantizar que se sigan las prácticas recomendadas del sector y de Palo Alto Networks.
- **Habilite las operaciones y la gestión de la seguridad de la red:** gestione fácilmente la configuración y las políticas de seguridad en todos los formatos—incluidas las soluciones de servidor perimetral de acceso seguro (SASE, por sus siglas en inglés), los cortafuegos de hardware y software, y todos los servicios de seguridad—para garantizar la coherencia y reducir la carga operativa.

Compatibilidad de los cortafuegos de nueva generación con proxies web nativos

- Consolida las funciones de los cortafuegos y proxies en una sola plataforma de gestión centralizada para la creación de políticas.
- Permite utilizar un proxy explícito mediante archivos PAC o un proxy transparente.
- El proxy explícito puede ayudarle con las arquitecturas de red de rutas no predeterminadas en las implementaciones de proxy locales.
- Además, es compatible con los métodos de autenticación de Kerberos y SAML.
- Simplifica la configuración de proxy transparente sin necesidad de aplicar el protocolo de control de caché web (WCCP, por sus siglas en inglés) ni políticas de autenticación.

Figura B3 Datasheet Palo alto PA-3410 – parte 3. Fuente. Información obtenida de la página web de Palo alto network.

Servicios de seguridad en la nube insuperables con tecnología Precision AI

La superficie de ataque típica de las empresas ha crecido notablemente debido a la adopción generalizada del trabajo híbrido, la nube, los dispositivos IoT y el SaaS. Además, la intensidad con la que se suceden las amenazas es cada vez mayor, ya que los atacantes pueden acceder a herramientas y recursos para hackers y utilizarlos en sus campañas con facilidad. Las estrategias y soluciones de seguridad de la red tradicionales ya no son eficaces. Con los servicios de seguridad en la nube de Palo Alto Networks, los clientes obtienen la mejor seguridad en tiempo real para ayudarles a proteger todos los dispositivos y datos de su red, y a todos los usuarios, independientemente de dónde se encuentren.

Los servicios de seguridad de Palo Alto Networks utilizan el poder de la tecnología Precision AI® integrada para anticiparse a los actores de amenazas y detener amenazas nuevas y nunca vistas en tiempo real. También aprovechan la inteligencia sobre amenazas compartida que recopilan de más de 70 000 clientes de todo el mundo para obtener información clave sobre las amenazas emergentes y actuar de manera proactiva. Por último, la integración fluida con los NGFW y el SASE elimina las lagunas de seguridad y ofrece a los clientes una solución centralizada para ver y gestionar su seguridad.

Estos son algunos de los servicios:

- **Advanced Threat Prevention:** detenga las amenazas conocidas y desconocidas de exploits, malware, spyware y comando y control —lo que incluye un 60 % más de ataques por inyección y un 48 % más de tráfico de comando y control muy evasivo que con los sistemas de prevención de intrusiones (IPS, por sus siglas en inglés) tradicionales— con la prevención de ataques de día cero pionera en el sector.
- **Advanced WildFire®:** garantice el acceso seguro a los archivos con el mayor motor de prevención de malware del sector, capaz de detener hasta un 22 % más de malware desconocido y de convertir la detección en prevención 180 veces más rápido que la competencia.
- **Advanced URL Filtering:** garantice el acceso seguro a internet y evite un 40 % más de amenazas en tiempo real que con las bases de datos de filtrado tradicionales gracias a la primera tecnología de prevención de ataques de phishing conocidos y desconocidos del sector, que detiene hasta el 88 % de las URL maliciosas al menos 48 horas antes que las soluciones de la competencia.
- **Advanced DNS Security:** proteja el tráfico DNS y detenga las amenazas avanzadas que, como el secuestro de DNS, afectan a la capa de DNS. Todo, en tiempo real y con el doble de cobertura que la competencia.
- **CASB de nueva generación:** vea y controle el consumo de SaaS total en su red gracias a la visibilidad de más de 60 000 aplicaciones SaaS y proteja sus datos con más de 28 integraciones de API.
- **IoT Security:** evite los ángulos muertos y proteja todos los dispositivos conectados específicos de su sector gracias a la solución Zero Trust para dispositivos IoT más completa del sector, que le permitirá detectar el 90 % de los dispositivos en 48 horas.

La arquitectura de un único paso procesa los paquetes de un modo especial

- La conexión de red, la búsqueda de políticas y la identificación y descodificación de la aplicación, así como el cotejo de firmas para todos los contenidos y amenazas, se realizan en un solo paso. De este modo, se reduce de forma considerable la carga de trabajo de procesamiento necesaria para ejecutar varias funciones en un solo dispositivo de seguridad.
- Utiliza un formato de firmas uniforme para analizar el tráfico y cotejar todas las firmas en el propio flujo, en un solo paso y sin generar latencia.
- Al habilitarse las suscripciones de seguridad, se consigue un rendimiento coherente y predecible. (En la tabla 1, el «rendimiento de Threat Prevention» se ha medido con varias suscripciones activadas).

Habilita la funcionalidad de SD-WAN

- Permite incorporar fácilmente una red de área extensa definida por software (SD-WAN, por sus siglas en inglés) con solo habilitarla en los cortafuegos existentes.
- Hace posible la implementación segura de la tecnología SD-WAN, que se integra de forma nativa con nuestras soluciones de seguridad líderes del sector.
- Proporciona una experiencia excepcional al usuario final, ya que reduce al mínimo la latencia, la vibración y la pérdida de paquetes.

Figura B4 Datasheet Palo alto PA-3410 – parte 4. Fuente. Información obtenida de la página web de Palo alto network.

Tabla 1: Rendimiento y capacidad de la serie PA-3400 Series				
	PA-3410	PA-3420	PA-3430	PA-3440
Rendimiento del cortafuegos (combinación de aplicaciones)*	14 Gb/s	19 Gb/s	29 Gb/s	35 Gb/s
Rendimiento de Threat Prevention (combinación de aplicaciones)†	7,5 Gb/s	10 Gb/s	15 Gb/s	20 Gb/s
Rendimiento de VPN IPsec‡	6,6 Gb/s	9,9 Gb/s	12 Gb/s	14,5 Gb/s
Máximo de sesiones simultáneas§	1,4 mills.	2,2 mills.	2,5 mills.	3 mills.
Nuevas sesiones por segundo¶	145 000	220 000	240 000	268 000
Sistemas virtuales (base/máx.)*	1/11	1/11	1/11	1/11

Nota: Los resultados se midieron con PAN-OS 11.2.

* El rendimiento del cortafuegos se calcula con App-ID y la creación de logs activados usando transacciones de combinación de aplicaciones.

† El rendimiento de Threat Prevention se calcula con App-ID, el sistema de prevención de intrusiones, la protección antivirus y antispyware, WildFire, el bloqueo de archivos y la creación de logs activados usando transacciones de combinación de aplicaciones.

‡ El rendimiento de VPN IPsec se calcula con transacciones HTTP de 64 kB y la creación de logs activada.

§ El número máximo de sesiones simultáneas se calcula usando transacciones HTTP.

¶ El cálculo de las nuevas sesiones por segundo se realiza con cancelación de aplicación usando transacciones HTTP de 1 byte.

* Para añadir sistemas virtuales a la cantidad base, es preciso adquirir una licencia por separado.

Tabla 2: Funciones de red de la serie PA-3400 Series	
Modos de interfaz	
L2, L3, TAP, cable virtual (modo transparente)	
Enrutamiento	
OSPF v2/v3 con reinicio correcto, BGP con reinicio correcto, RIP y enrutamiento estático	
Reenvío basado en políticas	
Protocolo punto a punto sobre Ethernet (PPPoE)	
Multidifusión: PIM-SM, PIM-SSM, IGMP versiones 1, 2 y 3	
Detección de reenvío bidireccional (BFD)	
IPsec y VPN SSL	
Intercambio de claves: clave manual, IKEv1 e IKEv2 (clave precompartida, autenticación basada en certificados)	
Cifrado: 3DES, AES (128 bits, 192 bits, 256 bits)	
Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512	
VPN a gran escala de GlobalProtect® para una configuración y una gestión más sencillas*	
Acceso seguro mediante túneles IPsec y VPN SSL con la puerta de enlace y los portales de GlobalProtect*	
Redes VLAN	
Etiquetas VLAN 802.1Q por dispositivo/interfaz: 4094/4094	
Interfaces agregadas (802.3ad), LACP	
Traducción de direcciones de red (NAT)	
Modos de NAT (IPv4): IP estática, IP dinámica, IP dinámica y puerto (traducción de direcciones de puertos)	
NAT64, NPTv6	
Funciones NAT adicionales: reserva de IP dinámica, IP dinámica optimizable y sobresuscripción de puertos	

* Requiere una licencia de GlobalProtect.

Figura B5 Datasheet Palo alto PA-3410 – parte 5. Fuente. Información obtenida de la página web de Palo alto network.

Tabla 2: Funciones de red de la serie PA-3400 Series (continuación)	
Alta disponibilidad	
Modos: activo/activo, activo/pasivo, clúster de alta disponibilidad	
Detección de errores: supervisión de rutas y supervisión de interfaces	
Infraestructura de la red móvil (PA-3440 y PA-3430)	
Seguridad 5G	
Seguridad de GTP	
Seguridad de SCTP	
† Para obtener más información, consulte la ficha técnica de los cortafuegos de nueva generación con aprendizaje automático para 5G.	
Tabla 3: Especificaciones del hardware de la serie PA-3400 Series	
E/S	
PA-3410: (12) puertos de 1 Gb/2,5 Gb/5 Gb/10 Gb, (10) puertos SFP/SFP+ de 1 Gb/10 Gb, (4) puertos SFP28 de 25 Gb	
PA-3420: (12) puertos de 1 Gb/2,5 Gb/5 Gb/10 Gb, (10) puertos SFP/SFP+ de 1 Gb/10 Gb, (4) puertos SFP28 de 25 Gb	
PA-3430: (12) puertos de 1 Gb/2,5 Gb/5 Gb/10 Gb, (10) puertos SFP/SFP+ de 1 Gb/10 Gb, (4) puertos SFP28 de 25 Gb, (2) puertos QSFP/QSFP28 de 40 Gb/100 Gb	
PA-3440: (12) puertos de 1 Gb/2,5 Gb/5 Gb/10 Gb, (10) puertos SFP/SFP+ de 1 Gb/10 Gb, (4) puertos SFP28 de 25 Gb, (2) puertos QSFP/QSFP28 de 40 Gb/100 Gb	
Gestión de E/S	
(1) puerto de gestión fuera de banda 100/1000	
(2) puertos 100/1000 de alta disponibilidad, (1) puerto SFP+ de 10 Gb de alta disponibilidad	
(1) puerto de consola RJ-45, (1) micro-USB	
Capacidad de almacenamiento	
480 GB en disco SSD	
Módulo de plataforma segura (TPM)	
Integración con el TPM para garantizar un arranque seguro, la raíz de confianza de hardware y la protección de secretos del sistema.	
Fuente de alimentación (consumo de energía medio/máx.)	
Redundante de 450 W CA (133 W/190 W)	
BTU/h máximo	
650	
Tensión de entrada (frecuencia de entrada)	
CA: 100–240 V CA (50–60 Hz)	
Consumo máximo de corriente	
CA: 1,9 A a 100 V CA, 0,8 A a 240 V CA	
Tiempo medio entre fallos (MTBF)	
22 años	
Dimensiones de montaje en rack	
1U, rack estándar de 48,3 cm: 35,94 x 43,56 x 4,32 cm	
Peso (solo dispositivo/embalado)	
7,03 kg/11,34 kg	
Seguridad	
cTUVus, CB	
EMI	
Clase A de FCC, Clase A de CE, Clase A de VCCI	
Tabla 3: Especificaciones del hardware de la serie PA-3400 Series (continuación)	
Certificaciones	
Consulte la página paloaltonetworks.com/company/certifications.html	
Entorno	
Temperatura de funcionamiento: de 0 °C a 40 °C	
Temperatura de almacenamiento: de -20 °C a 70 °C	
Tolerancia a la humedad: del 10 % al 90 %	
Altura máxima: 3048 m	
Flujo de aire: de delante atrás	

Figura B6 Datasheet Palo alto PA-3410 – parte 6. Fuente. Información obtenida de la página web de Palo alto network.

Anexo C:

Datasheet Eventlog Analyzer

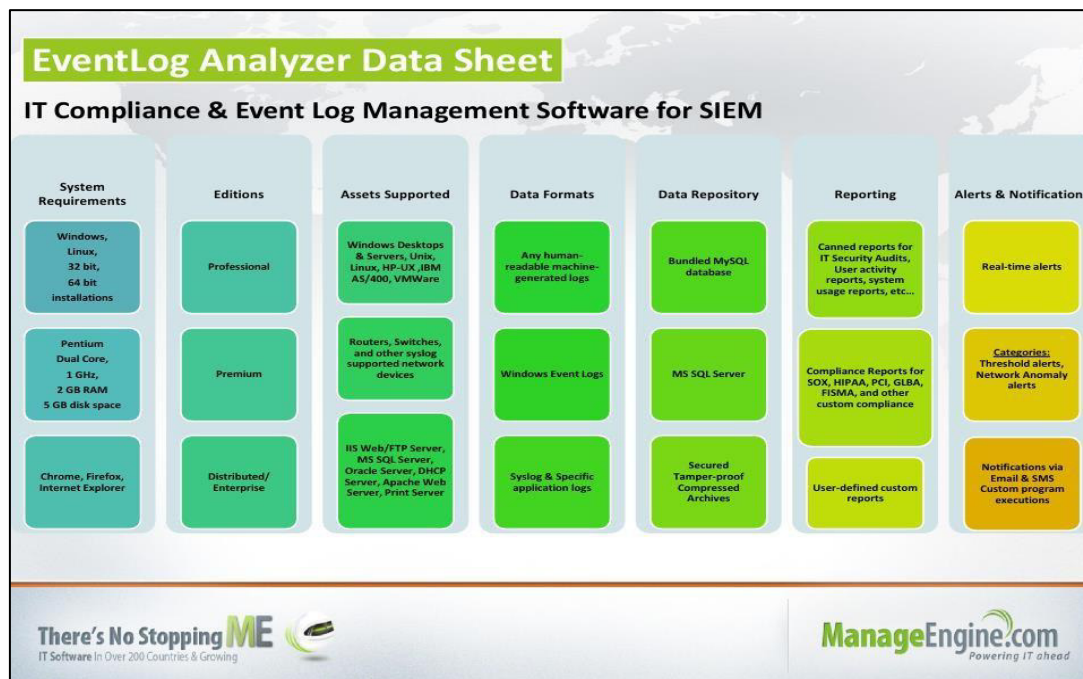


Figura C1 Datasheet SIEM – ELA. Fuente. Información obtenida del manual de manage Engine.

Anexo D:

Reporte del caso: ALERTA EXTERNAL THREAT SOURCE.



Figura D1 Reporte caso: ALERTA EXTERNAL THREAT SOURCE. Fuente. Información obtenida de la plataforma SIEM – ELA.

Log360 Cloud Threat Analytics	
Info	
Field	Value
Indicator	147.185.132.221
Reputation Score	14
Indicator Type	IP
Threat Source	147.185.132.221
Threat Source Age	-
First Release Date	2024-09-02 21:40:08
Last Release Date	2024-09-02 21:40:08
Current Release Date	2025-08-19 20:00:35
Status	In Threat IP List
Threat Category	Spam Sources, Windows Exploits
Occurrences on Threat List	1
Is Whitelisted	false

Figura D2 Reporte – Log360 Cloud Threat Analytics. Fuente. Información obtenida de la plataforma SIEM – ELA.

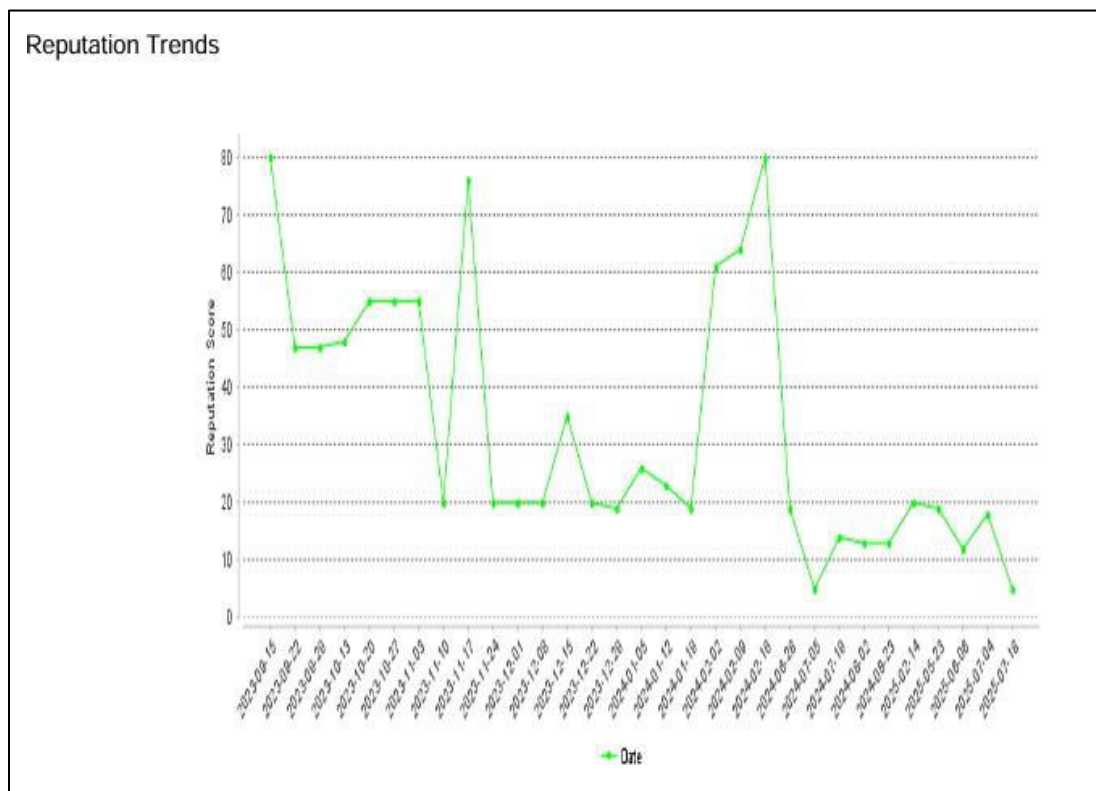


Figura D3 Reporte – Reputation Trends. Fuente. Información obtenida de la plataforma SIEM – EL

Reputation Summary	
Field	Value
Max Score	95
Min Score	5
Avg Score	40

Figura D4 Reporte – Reputation Summary. Fuente. Información obtenida de la plataforma SIEM – ELA.

Location Details	
Field	Value
City	Santa Clara
State	California
Region	Southwest
Country	United States

Figura D5 Reporte – Location Details. Fuente. Información obtenida de la plataforma SIEM – ELA.

Related Indicators					
Section	High Risk	Suspicious	Moderate Risk	Low Risk	Trustworthy
Autonomous System Number (ASN)	508243	4498	2506	6891	21210

Figura D6 Reporte – Related Indicators. Fuente. Información obtenida de la plataforma SIEM – ELA.

VirusTotal Info	
Field	Value
Indicator	147.185.132.221
Detection Score	10 out of 94 vendors flagged this IP as malicious.
Type	IP
Creation Date	-
Last Updated	2025-08-08 00:24:10
Community Score	0
Network	147.185.132.0/22
ASN	396982
AS Owner	GOOGLE-CLOUD-PLATFORM
Regional Internet Registry	ARIN
Continent	North America
Country	US

Figura D7 Reporte – Virus Total Info. Fuente. Información obtenida de la plataforma SIEM – ELA.

Security Vendor Analysis		
Security Vendor	Analysis Category	Analysis Result
Zvelo	Undetected	Unrated
Snort IP Sample List	Harmless	Clean
PrecisionSec	Undetected	Unrated
Underworld	Undetected	Unrated
AutoShun	Undetected	Unrated
Benkow.cc	Harmless	Clean
Abusix	Harmless	Clean
Quttera	Harmless	Clean
Heimdal Security	Harmless	Clean
Securolytics	Harmless	Clean
AlphaMountain.ai	Suspicious	Suspicious
Chong Lua Dao	Harmless	Clean
Phishing Database	Harmless	Clean
PREBYTES	Harmless	Clean
SafeToOpen	Undetected	Unrated
Dr.Web	Harmless	Clean
MalwarePatrol	Harmless	Clean
EmergingThreats	Harmless	Clean
Threatsourcing	Harmless	Clean
Quick Heal	Harmless	Clean
URLhaus	Harmless	Clean

Figura D8 Security Vendors Analysis. Parte 1. Fuente. Información obtenida de la plataforma SIEM – ELA.

Blueliv	Harmless	Clean
Desenmascara.me	Harmless	Clean
AlienVault	Harmless	Clean
Viettel Threat Intelligence	Harmless	Clean
Xcitium Verdict Cloud	Harmless	Clean
GreenSnow	Harmless	Clean
ZeroFox	Undetected	Unrated
Webroot	Harmless	Clean
Sansec EComscan	Undetected	Unrated
Gridinsoft	Undetected	Unrated
Phishtank	Harmless	Clean
SecureBrain	Undetected	Unrated
Sophos	Harmless	Clean
Axur	Undetected	Unrated
CRDF	Harmless	Clean
VIPRE	Undetected	Unrated
ZeroCERT	Harmless	Clean
Malward	Harmless	Clean
PhishFort	Undetected	Unrated
Lumu	Undetected	Unrated
AlphaSOC	Suspicious	Suspicious
Emsisoft	Harmless	Clean
AILabs (MONITORAPP)	Harmless	Clean
Forcepoint ThreatSeeker	Undetected	Unrated
Seclookup	Harmless	Clean
Bkav	Undetected	Unrated
GCP Abuse Intelligence	Undetected	Unrated
Scantitan	Harmless	Clean

Figura D9 Security Vendors Analysis. Parte 2. Fuente. Información obtenida de la plataforma SIEM – ELA.

Sucuri SiteCheck	Harmless	Clean
ThreatHive	Harmless	Clean
Criminal IP	Malicious	Malicious
Netcraft	Undetected	Unrated
SOCRadar	Malicious	Malware
CMC Threat Intelligence	Harmless	Clean
Kaspersky	Undetected	Unrated
G-Data	Malicious	Phishing
ViriBack	Harmless	Clean
Bfore.Ai PreCrime	Undetected	Unrated
CINS Army	Malicious	Malicious
ESTsecurity	Harmless	Clean
0xSI_f33d	Undetected	Unrated
CSIS Security Group	Undetected	Unrated
Certego	Malicious	Malicious
Spam404	Harmless	Clean
ArcSight Threat Intelligence	Malicious	Malware
Cyan	Undetected	Unrated
Acronis	Harmless	Clean
URLQuery	Undetected	Unrated
PhishLabs	Undetected	Unrated
Cluster25	Undetected	Unrated
Cyble	Harmless	Clean
SCUMWARE.org	Harmless	Clean
Google Safebrowsing	Harmless	Clean
IPsum	Malicious	Malicious
DNS8	Harmless	Clean
Ermes	Undetected	Unrated

Figura D10 Security Vendors Analysis. Parte 3. Fuente. Información obtenida de la plataforma SIEM – ELA.

Yandex Safebrowsing	Harmless	Clean
ADMINUSLabs	Harmless	Clean
Mimecast	Undetected	Unrated
Hunt.io Intelligence	Undetected	Unrated
OpenPhish	Harmless	Clean
Malwares.com URL Checker	Harmless	Clean
Lionic	Malicious	Malicious
StopForumSpam	Harmless	Clean
Trustwave	Harmless	Clean
VX Vault	Harmless	Clean
Juniper Networks	Harmless	Clean
CyRadar	Malicious	Malicious
ESET	Harmless	Clean
Fortinet	Harmless	Clean
Antiy-AVL	Harmless	Clean
BitDefender	Malicious	Phishing
MalwareURL	Undetected	Unrated

Figura D11 Security Vendors Analysis. Parte 4. Fuente. Información obtenida de la plataforma SIEM – ELA.