EXTENDED DETECTION & RESPONSE

SIEM Management

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Nuestra solución de SIEM gestionado permite una monitorización y detección de amenazas continua en toda tu organización

El alto número de activos TI y entornos heterogéneos en las organizaciones exige una **capacidad de monitorización avanzada y eficiente** que permitan una visión conjunta e inteligente de las amenazas y del cumplimiento normativo.

La detección, a través de una monitorización continua de eventos y logs 24x7, requiere de conocimiento experto y tecnologías avanzadas que garanticen una **automatización en la detección y respuesta ante cualquier incidente.**

En Telefónica Tech facilitamos a los clientes la capacidad de disponer de un **amplio equipo de expertos junto a las últimas tecnologías SIEM**, para obtener una **capa de seguridad eficaz** en la prevención, detección y respuesta frente amenazas e incidentes.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

Organizaciones que necesitan **implantar o ampliar capacidades de monitorización, detección y respuesta** ajustándose a necesidades de seguridad o cumplimiento normativo para reducir costes operativos o de adquisición tecnológica.

Medianas y grandes organizaciones con una capacidad ya establecida de SecOps que buscan externalizar el **gran volumen** de trabajo o la **monitorización 24x7** para centrar sus equipos de seguridad en actividades estratégicas de alto valor.

Organizaciones que buscan **desarrollar a largo plazo capacidades propias ad-hoc de correlación y monitorización de eventos** y optan por crecer y aprender de un partner de confianza con experiencia en SIEM.

NUESTRA PROPUESTA DE VALOR

Nuestro servicio

El servicio de SIEM Management de Telefónica Tech tiene como objetivo ampliar las capacidades de detección y respuesta a través de una monitorización y correlación continua de eventos, *logs* y alertas en el entorno TI del cliente, ofreciendo una visibilidad del estado de la seguridad, así como el apoyo y soporte a los equipos de seguridad ante cualquier amenaza detectada o necesidad de evolución de la monitorización.

El objetivo es proporcionar un servicio con gran automatización en la detección de anomalías de seguridad y ciberamenazas, eliminando la necesidad de disponer de un equipo y/o tecnología SIEM propia, obteniendo capacidades de orquestación y respuesta "As A Service".

¿Qué te permite?

Este servicio te permitirá:

- Adoptar tecnología SIEM de **última generación** de los partners más relevantes del mercado.
- **Ampliar la capacidad de seguridad** sobre todos los entornos tecnológicos (on-premise y cloud) obteniendo una visión global de monitorización y reduciendo riesgos de seguridad.
- **Incrementar las capacidades de detección y tiempos de respuesta** de forma eficiente y continua mediante equipos de analistas expertos 24x7 e inteligencia enriquecida.

Beneficios del servicio

Gestión end-to-end

Nuestros equipos se encargan de la entrega, configuración, despliegue e instalación SIEM, proporcionando una estrecha orientación y apoyo durante todo el proceso a los equipos TI del cliente.

Monitorización y detección 24x7

Incluyendo el triaje, análisis y descarte de falsos positivos, así como el escalado remoto de cualquier amenaza confirmada bajo procedimientos orquestados.

Búsqueda de amenazas

Nuestros analistas más expertos aprovechan la información más reciente de TTPs, vulnerabilidades e IoCs para llevar a cabo búsquedas de amenazas que han pasado desapercibidas.

Detección y personalización

Amplio catálogo de correlación y agregación con una implementación adaptada a los activos y procesos del cliente, apoyado por expertos que mantienen un entorno actualizado con información personalizada.

Valor diferencial de Telefónica Tech

Integración total con capacidades propias de automatizaciones SOAR, *ticketing*, inteligencia de amenazas y portal de clientes.

Ahorro y control de costes con un modelo flexible basado en plataforma *multitenant* o dedicada.

Partner con amplia experiencia a nivel global e inteligencia de amenazas propietaria en tiempo real.

EQUIPO Y LOGROS

Nuestros equipos

- **+150 analistas expertos en SIEM**.
- **› +1.500** certificaciones de seguridad.
- **12** Centros de Operaciones de Seguridad y 2 Centros de Operaciones Digitales Globales.

Logros

- **+600.000** tickets atendidos al año.
- **+4.000** millones de eventos de seguridad monitorizados al día.
- **+19** millones de loCs almacenados en nuestra plataforma de inteligencia de amenazas.
- **+16.500** dispositivos monitorizados al año.

MODELO COMERCIAL

SIEM Management es un servicio basado en la gestión delegada de las plataformas SIEM más relevantes del mercado, adaptable para su inclusión durante cualquier etapa del servicio (provisión, integración o explotación), bajo un **modelo multi-cliente "As a Service" o dedicado.**

Según la cantidad de ingesta de datos (GB/Día o EPS), fuentes de eventos, casos de uso y número de analistas dedicados, el cliente puede, de forma flexible, ajustar sus necesidades de monitorización y análisis obteniendo un **servicio 24x7 con capacidades de detección avanzada.**

PARTNERS RELACIONADOS

CROWDSTRIKE Google IBM

Microsoft NETWITNESS splunk>

SERVICIOS RELACIONADOS

Digital Forensics & Incident Response

Solución de respuesta ante ciberincidentes y cibercrisis para minimizar daños y acelerar la recuperación operativa.

Managed Detection & Response

Monitorización completa de la seguridad de los *endpoints* gracias a la detección, contención y respuesta rápida a brechas de seguridad 24x7 con *Hunting* Proactivo continuo y asistencia experta ante cibercrisis, basado en la mejor tecnología EDR y XDR.

Contáctanos para empezar la transformación digital de tu organización.