EXTENDED DETECTION & RESPONSE

Identity Threat Detection & Response

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Ofreciéndote visibilidad sobre las amenazas que acechan a tu Directorio Activo y respondiendo ante ellas. También asesorándote con las medidas de prevención a implantar para tus identidades no sean comprometidas por un atacante

El Directorio Activo (AD) es una **herramienta *legacy*** objeto prioritario de los atacantes por su posición dominante en el mercado. Además, **carece de la capacidad de detectar configuraciones anómalas** y su interdependencia con otros sistemas de información suele generar vulnerabilidades que aprovechan los atacantes para moverse lateralmente dentro de la infraestructura de IT de una organización.

Para ello, en **Telefónica Tech** ofrecemos tecnologías de **ITDR (Identity Threat Detection & Response)** además de un equipo de expertos que operan el servicio desde el SOC (presente en 12 ubicaciones). Los analistas **investigan, responden e informan** de amenazas detectadas, asesoran sobre mitigaciones de riesgos debido a malas configuraciones del AD o credenciales comprometidas y proponen automatismos de prevención basados en condiciones dinámicas de riesgo.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

Para empresas que quieran evolucionar la detección, investigación y respuesta de puestos de trabajo y servidores con capacidades extendidas de respuesta ante amenazas en el ámbito tecnológico del Microsoft AD y Azure AD.

Para empresas que necesiten visibilidad y asesoramiento sobre políticas de credenciales débiles, rutas de ataque vulnerables, credenciales comprometidas en la dark web o usuarios con sobreprivilegios para así poder higienizar y proteger su Directorio Activo con mejores garantías.

Para empresas que no tengan el conocimiento suficiente y requieran de un partner de seguridad con experiencia en gestión de amenazas sofisticadas de identidad como pueden ser el DCSync, el Golden Ticket, Pass-the-Hash u otros ataques de protocolo tipo Kerberos.

NUESTRA PROPUESTA DE VALOR

Nuestro servicio

El servicio monitoriza en 24x7x365 las amenazas de movimientos laterales del atacante desde el PC o servidor hasta el Directorio Activo y te ofrece respuesta guiada o automática, según sea el caso, para remediar el ataque mediante el bloqueo del usuario, el forzado de reseteo de contraseña o la solicitud de un doble factor de autenticación (MFA).

Gracias a reuniones e informes periódicos, te proponemos recomendaciones para la higiene del AD. Adicionalmente, el servicio recomienda y despliega automatismos de prevención con condiciones de riesgo dinámicas. Por ejemplo, si una credencial de la organización ha sido robada y detectada en la dark web, el automatismo forzará al usuario de dicha credencial a resetar la contraseña en el próximo acceso.

¿Qué te permite?

Este servicio te permitirá:

- **Tener visibilidad, severidad y asesoramiento de los riesgos de amenaza según la configuración del Directorio Activo.**
- **Detectar, investigar y responder** ante los movimientos laterales del atacante dentro de tu infraestructura IT, que podrían llegar a comprometer el Directorio Activo como pasos previos en su ataque.
- **Desplegar automatismos de prevención de riesgo de identidades basados en directrices Zero-Trust.**

Beneficios del servicio

Mejora de la cobertura de detección y respuesta

El servicio detecta comportamientos anómalos con análisis continuo y machine learning, identificando riesgos en el Directorio Activo como escalado de privilegios o suplantación.

Asesoramiento de buenas prácticas de configuración del Directorio Activo

La evaluación continua de riesgos por configuraciones débiles o credenciales comprometidas protege el Directorio Activo e identifica cambios de privilegios o usuarios inactivos.

Prevención automática que cierra puertas de entrada al atacante

Gracias a los controles automáticos de acceso basados en riesgo, como MFA puntual o bloqueo por IPs maliciosas, protegen las identidades y detienen accesos no autorizados.

Valor diferencial de Telefónica Tech

No solo alertamos e investigamos amenazas, también proponemos, desarrollamos y auditamos respuestas de prevención automatizadas basadas en riesgo.

Nuestra experiencia en asesoramiento te ayudará a prevenir futuros ataques mediante la mejora de la postura continua de seguridad del Directorio Activo.

Muchos de los procesos operativos de nuestro SOC están automatizados, lo que nos permite detectar, investigar y responder ante la amenaza en un tiempo reducido.

EQUIPO Y LOGROS

Nuestros equipos

- **+2.500** profesionales de ciberseguridad.
- **+3.000** certificaciones de seguridad.
- **2** centros digitales globales con 11 localizaciones **mundiales.**

Logros

- **+50.000** identidades protegidas.
- **+19 millones** de IoCs almacenados en nuestra plataforma de inteligencia de amenazas.
- **Certificación MSSP Élite** de CrowdStrike.

MODELO COMERCIAL

Identity Threat Protection & Response puede ser contratado en modalidad personalizada, con dedicación exclusiva de analistas, o con un alcance predefinido como parte del servicio MDR de Telefónica.

En la modalidad de alcance predefinido, el precio es mensual, sin coste de alta, y variará según el número de identidades a proteger.

Ofrecemos la opción de comprar las licencias como suministro o las podemos incluir como parte del servicio.

PARTNERS RELACIONADOS

CROWDSTRIKE

SERVICIOS RELACIONADOS

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.

Digital Forensics & Incident Response

Solución de respuesta ante ciberincidentes y cibercrisis para minimizar daños y acelerar la recuperación operativa, incluyendo gestor de incidentes dedicado, análisis forense/ malware y asistencia a la contención, recuperación y erradicación ante amenazas.

SIEM Management

Monitorización y correlación de eventos de seguridad con gestión de alertas 24x7, proporcionando una base sólida en la detección de amenazas de seguridad a través de nuestro catálogo de casos de uso global, SOAR y plataforma de inteligencia de amenazas

Contáctanos para empezar la transformación digital de tu organización.