RESUMEN DE LA SOLUCIÓN

Servicios EDR y XDR gestionados de Insight

Retos empresariales

En el panorama digital actual, que evoluciona rápidamente, las empresas se enfrentan a una serie de retos complejos en materia de ciberseguridad. El constante aluvión de ciberamenazas plantea un riesgo significativo para los activos valiosos y los datos confidenciales. A medida que los ciberdelincuentes se vuelven más astutos e innovadores, cada vez es más difícil para las organizaciones detectar y responder a estas amenazas de forma eficaz.

Las empresas se enfrentan a una normativa cada vez más estricta, a la complejidad de los entornos de TI y a la escasez de profesionales cualificados en ciberseguridad. La combinación de estos retos crea la necesidad de ofrecer soluciones de ciberseguridad completas y proactivas para proteger a las empresas de las diversas y sofisticadas amenazas a las que se enfrentan a diario.

La preparación y la resistencia en materia de ciberseguridad son fundamentales para proteger la continuidad y el éxito de cualquier empresa moderna.

Cómo puede ayudar Insight

Nuestro Centro de Operaciones de Seguridad (SOC) ofrece dos ofertas de servicios gestionados que proporcionan capacidades avanzadas de detección, investigación y respuesta ante amenazas:

- **Detección y respuesta gestionadas para endpoints (MEDR)**
  Cubre portátiles, ordenadores de sobremesa y dispositivos móviles.
- **Detección y respuesta ampliadas gestionadas (MXDR)**
  Reúne registros y feeds de una amplia gama de fuentes, ofreciendo la capacidad de detección más sólida para su entorno.

Combinando tecnologías como la IA, la inteligencia sobre amenazas y la analítica, nuestro equipo de expertos en seguridad son capaces de detectar y responder a las amenazas que se presentan en su entorno en tiempo real.

Le ayudamos con:

- Una supervisión completa, detectando y dando respuesta a amenazas en tiempo real.
- Respuestas más rápidas a incidentes y reducción del tiempo de inactividad.
- Mayor visibilidad de las actividades de los endpoints y las posibles amenazas.
- Disponibilidad de servicio 24/7.
- El cumplimiento de requisitos reglamentarios y normas del sector.
- La combinación con otros servicios de Insight como parte de un sistema de seguridad integral.

RESUMEN DE LA SOLUCIÓN

Servicio gestionado de detección y respuesta para endpoints

Diseñado como una capacidad de detección y respuesta asequible y accesible para aquellas organizaciones con un programa de seguridad estructurado limitado o inexistente. Nuestro servicio está diseñado en torno a la tecnología líder del sector de la gama de seguridad de Microsoft y utiliza Microsoft Defender for Endpoint como núcleo de sus funciones de detección.

Los elementos clave de nuestro servicio EDR gestionado incluyen:

- **Supervisión de Endpoints:** Uso de herramientas y técnicas avanzadas para supervisar los endpoints 24/7 en busca de signos de actividad sospechosa, incluidos ataques sin archivos, malware avanzado, ransomware y amenazas internas.
- **Detección de amenazas:** Utilizamos una combinación de inteligencia sobre amenazas, análisis de comportamientos y algoritmos de aprendizaje automático para detectar amenazas avanzadas que puedan eludir los controles de seguridad tradicionales.
- **Investigación y respuesta:** Nuestros analistas de seguridad investigan y priorizan las alertas y proporcionan informes detallados de incidentes a su equipo. Del mismo modo, trabajamos con usted para desarrollar y ejecutar un plan de respuesta que mitigue el impacto de cualquier incidente.
- **Protección de Endpoints:** Nuestra solución EDR incluye funciones avanzadas de protección para endpoints, como antivirus, anti-malware y sistemas de prevención de intrusiones basados en host (HIPS) para ayudar a prevenir y bloquear los ataques antes de que puedan causar daños.
- **Búsqueda de amenazas:** Capacidades proactivas de búsqueda de amenazas, en las que nuestros analistas buscan e investigan posibles amenazas que puedan haber pasado desapercibidas para los sistemas automatizados.

Servicios gestionados de detección y respuesta ampliadas

Una capacidad de detección más robusta que reúne todos sus registros y fuentes de seguridad en una plataforma SIEM centralizada basada en la tecnología Sentinel de Microsoft.

Los elementos clave de nuestro servicio XDR gestionado incluyen:

- **Monitorización:** Utilizando herramientas y técnicas avanzadas para supervisar las 24 horas del día, los 7 días de la semana, en busca de indicios de actividades sospechosas, como ataques sin archivos, malware avanzado y amenazas internas.
- **Recopilación y análisis de registros:** Recopilación y análisis centralizados de datos de registro procedentes de diversas fuentes, como puntos finales, dispositivos de red, aplicaciones y servicios cloud.
- **Detección de amenazas:** Utilizamos una combinación de inteligencia sobre amenazas, análisis de comportamientos y algoritmos de aprendizaje automático para detectar amenazas avanzadas que puedan eludir los controles de seguridad tradicionales.
- **Investigación y respuesta:** Nuestros analistas de seguridad investigan y priorizan las alertas y proporcionan informes detallados de incidentes a su equipo. Del mismo modo, trabajamos con usted para desarrollar y ejecutar un plan de respuesta que mitigue el impacto de cualquier incidente.
- **Protección de Endpoints:** Nuestra solución EDR incluye funciones avanzadas de protección para endpoints, como antivirus, anti-malware y sistemas de prevención de intrusiones basados en host (HIPS) para ayudar a prevenir y bloquear los ataques antes de que puedan causar daños.
- B**úsqueda de amenazas:** Capacidades proactivas de búsqueda de amenazas, en las que nuestros analistas buscan e investigan posibles amenazas que puedan haber pasado desapercibidas para los sistemas automatizados.

Resultados de nuestros servicios EDR/XDR gestionados Le ayudaremos con:

La detección y respuesta proactivas a amenazas	Supervisión y asistencia 24/7	La relación coste/ eficacia	El Cumplimient normativo
Previniendo las brechas de seguridad y minimizando el impacto de posibles ataques	Protección continua y rápida respuesta ante incidentes	Una alternativa rentable a la creación y mantenimiento de un equipo interno	Ayudando a cumplir las normas de seguridad y los requisitos de información.