DAISYTEK SERVICES

Cóntactanos

contacto@daisytek.services 55 5000 3500 www.daisytek.services

Servicio Gestionado de Detección y Respuesta *(MDR)*

Nuestro objetivo es ayudarle a crear, implantar y mantener un programa continuo para reducir los riesgos cibernéticos de la forma más adecuada para su empresa. Nuestro servicio MDR forma parte de una gama de servicios que hemos desarrollado para ayudarle a tener éxito en un panorama en constante cambio.

¿Qué es el servicio MDR?

MDR es nuestro servicio de ciberseguridad gestionada que proporciona detección integral de intrusiones de malware y actividad maliciosa en su red. Supervisa de forma proactiva puntos finales y dispositivos, ya estén en las instalaciones, en la nube o en dispositivos móviles. El servicio busca puntos de peligro en sus dispositivos y utiliza el agente localmente para tomar decisiones en tiempo real basadas en la actividad detectada, con el valor añadido de disponer de alertas que activan la necesidad de respuesta humana.

¿Cómo funciona?

Aprovechando la avanzada arquitectura de ciberseguridad de nuestra red de socios de confianza, el servicio MDR está diseñado para ayudar a las organizaciones a hacer frente a la explosión de datos actual. El servicio se presta en forma de agente que se conecta a dispositivos móviles y servidores, incluidos los entornos de nube pública y privada. Gestionado de forma centralizada y desplegado en los sistemas operativos Windows, Mac, Linux y Android, ofrece funciones inmediatas de detección de amenazas y análisis forense de datos.

Datos clave

- Completa - integración con nuestro servicio SIEM y Respuesta a Incidentes
- Fiable: cobertura forense en todos los dispositivos y retroceso a puntos específicos en el tiempo.
- Sin fisuras: opciones de despliegue en la nube, local e híbrido
- Rápido: SLA de 30 minutos para incidentes críticos
- Humano: expertos dedicados a ayudar en la toma de decisiones críticas

¿Cuáles son los beneficios?

Ofrece la tranquilidad de un enfoque humano de la ciberseguridad

Nuestro servicio MDR proporciona alertas sobre cuándo es necesaria la intervención humana. Una vez emitida la alerta, un miembro de nuestro equipo especializado puede iniciar el proceso de toma de decisiones para poner en cuarentena, eliminar y/o reparar el dispositivo o dispositivos problemáticos fuera de la red, con el fin de evitar que la infección siga proliferando en sus entornos de TI.

Reduce el gasto en ciberseguridad

Las soluciones EDR (Endpoint Detection and Response) requieren conocimientos forenses antes de tomar decisiones. Con la actual explosión de datos y el aumento del número de incidentes que requieren atención, esto puede provocar un aumento del tiempo de inactividad y de los costes asociados a la contratación de los expertos necesarios. Es importante asegurarse de que, cuando saltan las alarmas, se dispone de la capacidad necesaria para seguir adelante, que es lo que ofrece nuestro servicio MDR.

Minimiza el tiempo de inactividad para que pueda volver rápidamente a las operaciones

Nuestro servicio MDR está integrado en nuestro servicio SIEM (Security Information and Event Management), así como en un equipo del Servicio de Respuesta a Incidentes. Esto significa que todos los equipos pueden interactuar sin problemas cuando se identifican amenazas para que vuelva a estar operativo lo antes posible.

Se integra perfectamente con Office 365

Además de ser compatible con cualquier endpoint y cualquier dispositivo, nuestro servicio MDR se integra completamente con Office 365. Esto significa que puede detectar amenazas dentro de ese entorno y tomar decisiones basadas en los usuarios que utilizan ese software. Nuestro servicio proporciona la tranquilidad de que su configuración de Office 365 está totalmente protegida y segura.

Aprovecha una de las mayores bases de datos de amenazas y vulnerabilidades del mundo

En lugar de comprar datos, aprovechamos la base de datos de amenazas y vulnerabilidades de nuestro servicio MDR, una de las mayores del mundo. Gracias a la mayor visibilidad del sector sobre cuándo y dónde se producen las amenazas, podemos ofrecer una caza de amenazas que proporciona una protección proactiva, ayudándole a prepararse para los problemas antes de que se produzcan.

¿Por qué Nosotros?

Cobertura de todas las plataformas operativas: mejore la visibilidad de sus amenazas	Asistencia las 24 horas del día: refuerce su ciberresiliencia	Cobertura forense de todos los puntos finales: reduzca el impacto de los incidentes.	Protección para entornos de nube pública: garantice su total seguridad	Soporte para tecnología operativa (OT): proteja los sistemas críticos "no parcheables