INFORMACIÓN GENERAL DE LA SOLUCIÓN

THREAT MONITORING

Reciba el aviso proactivo de ESET cuando se detecte una anomalía de seguridad en tiempo real

ESET CYBERSOC

El servicio de Threat Monitoring de ESET ayuda a los clientes a navegar por la gran cantidad de datos, eventos y alarmas generados por nuestra solución de detección y respuesta para endpoints, ESET Enterprise Inspector, y a aprovechar todo el potencial de esta herramienta sin tener que modificar sus prioridades de TI existentes.

¿Por qué es necesario el servicio de Threat Monitoring de ESET?

> APROVECHE AL MÁXIMO SU SOLUCIÓN EDR DE ESET

ESET Enterprise Inspector es una herramienta sofisticada de detección y respuesta para endpoints que permite identificar comportamientos anómalos y violaciones de seguridad, evaluar riesgos, así como responder a incidentes, investigarlos y remediarlos.

Supervisa y evalúa todas las actividades que ocurren en la red en tiempo real y les permite a las organizaciones tomar medidas inmediatas cuando es necesario.

El servicio de Threat Monitoring de ESET requiere tener instalado ESET Enterprise Inspector.

> FALTA DE CONOCIMIENTO

La utilización de nuevos productos sin conocimientos previos puede complicarse incluso para organizaciones con equipos de seguridad o de TI especializados. Además, mantenerse actualizado sobre el panorama de amenazas cibernéticas que cambia tan rápidamente puede ser un gran desafío, por lo que a veces es mejor dejarlo en manos de expertos.

> ESCASEZ DE PERSONAL

Identifica los eventos importantes para que los equipos de seguridad y los administradores de TI puedan priorizar su carga de trabajo más fácilmente. Por otra parte, a las organizaciones les puede llevar meses contratar y capacitar a un equipo que implemente y monitoree una plataforma de detección y respuesta para endpoints.

> TRANQUILIDAD

Las organizaciones pueden quedarse tranquilas al saber que los expertos en seguridad están controlando su entorno a diario en busca de cualquier anomalía o de posibles violaciones. En caso de encontrar alguna, los expertos se ponen en contacto proactivamente para que puedan remediar lo antes posible los problemas detectados.

> COSTOS A LARGO PLAZO

Crear equipos especializados y contratar expertos para realizar tareas ocasionales pueden tener costos elevados a largo plazo. Por otro lado, la compra de productos y servicios a un único proveedor es un alivio para los departamentos contables, en especial en corporaciones multinacionales.

Características técnicas del servicio de Monitoreo de amenazas de ESET

> MONITOREO DIARIO

Un operador en vivo de ESET revisa la consola de amenazas de la organización al menos una vez cada 24 horas en días hábiles regulares.

> INFORMES DE ESTADO

Los operadores del Monitoreo de amenazas compilan sus hallazgos en Informes de estado claros y comprensibles y luego se ponen en contacto con el representante de la organización para alertarlos sobre cualquier evento crítico que requiera atención inmediata.

> AJUSTES CONTINUOS

Después de crear el informe, los operadores del Monitoreo de amenazas crean nuevas reglas o exclusiones, y ofrecen recomendaciones sobre cómo proceder en caso de una amenaza real.

> LOS DATOS NO SALEN DE LA EMPRESA

Todos los datos de amenazas y de la organización permanecen en las instalaciones de la empresa. Para ello, se configura una conexión VPN segura entre ESET y la organización.

> EVALUACIÓN INICIAL

ESET realiza una evaluación inicial exhaustiva para determinar las políticas de seguridad de cada organización específica, así como para desarrollar su perfil interno.

En caso de encontrar alguna anomalía o posible violación de seguridad, los expertos se ponen en contacto con las organizaciones en forma proactiva para que puedan remediar lo antes posible los problemas detectados.

Las etapas

Evaluación inicial

- Cada servicio comienza con la evaluación no solo del entorno del cliente, sino también de su composición organizativa y su actitud general ante la seguridad cibernética.
- Se realiza una entrevista completa con los miembros relevantes del personal de la organización para recopilar toda la información requerida.
- Como resultado de esta fase, se crea un Perfil de seguridad de la organización. Este perfil sirve en el futuro para que los operadores del Monitoreo de amenazas lo consulten en caso de que necesiten obtener detalles relacionados con la organización para tomar decisiones precisas.

Optimización

- Esta fase comienza después de unos días consecutivos de haber ejecutado ESET Enterprise Inspector (la solución EDR de ESET) en el entorno en vivo de la organización.
- Durante esta fase, los operadores revisan las alarmas activadas y las reglas que las accionaron.
- Teniendo en cuenta el entorno de la organización y la evaluación inicial, se crean exclusiones para todos los falsos positivos y eventos inofensivos.

Operaciones regulares

- Los operadores del Monitoreo de amenazas de ESET se conectan todos los días para controlar los eventos y las alarmas; luego ajustan las reglas internas y las configuraciones según se necesite.
- Los resultados de cada investigación se compilan en informes de estado fáciles de entender, con detalles técnicos expresados en un lenguaje accesible.
- Se contacta a las organizaciones para alertarlas sobre cualquier evento crítico que requiera atención inmediata.

ESET EN NÚMEROS

+110 Millones de usuarios en el mundo

+ 400 Mil clientes corporativos

+200 países y territorios

13 centros de investigación y desarrollo