INFORMACIÓN GENERAL DE LA SOLUCIÓN

THREAT HUNTING

Investigación de amenazas bajo demanda, análisis de causas de origen y asesoramiento

ESET CYBERSOC

El servicio de Threat Hunting de ESET ayuda a los clientes a investigar un determinado conjunto de datos, eventos y alarmas generados por la solución de detección y respuesta para endpoints ESET Enterprise Inspector.

¿Por qué es necesario el servicio de Threat Hunting 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 en tiempo real todas las actividades que ocurren en la red y les permite a las organizaciones tomar medidas inmediatas de ser necesario.

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

> FALTA DE CONOCIMIENTO SOBRE EL PRODUCTO

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 otro lado, las organizaciones pueden necesitar meses para contratar y capacitar a un equipo que implemente y monitoree una plataforma de detección y respuesta para endpoints.

> TRANQUILIDAD

Si se identifican anomalías o infracciones, nuestros expertos pueden detectar rápidamente la causa de origen y remediar para siempre los problemas encontrados.

> COSTOS A LARGO PLAZO

Crear equipos especializados y contratar expertos para realizar tareas ocasionales pueden tener costos elevados a largo plazo.
La compra de productos y servicios de un único proveedor reduce la complejidad para los departamentos de contabilidad, especialmente en el caso de las corporaciones multinacionales, que de otro modo deberían tener una gran cantidad de proveedores regionales.

Características técnicas del servicio

> SERVICIO BAJO DEMANDA

Las organizaciones se comunican con los operadores de ESET cuando requieren sus servicios.

> ANÁLISIS DE CAUSAS DE ORIGEN

Los operadores de ESET revisan las alarmas consultadas para determinar su causa de origen.

> CONSEJOS PRÁCTICOS

Los operadores revisan las alarmas y compilan sus hallazgos en un informe de estado fácil de entender, además de ofrecerle a la organización consejos prácticos.

> SERVICIO BASADO EN SUSCRIPCIÓN

Las organizaciones adquieren los servicios de ESET Threat Hunting en bloques de tiempo personalizables durante los cuales los expertos investigan las amenazas cuando más se necesitan.

> 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.

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 lo consulten en caso de que necesiten obtener detalles relacionados con la organización para tomar decisiones precisas.
- Se recomienda que las organizaciones se pongan en contacto con ESET ante cualquier cambio en su entorno, debido a la naturaleza bajo demanda del servicio ESET Threat Hunting.

Operaciones regulares

- Cuando se lo soliciten, los expertos de seguridad de ESET comienzan la investigación de los eventos indicados para determinar su causa de origen y brindar asesoramiento práctico personalizado para la organización específica.
- Los resultados de cada investigación se compilan en informes de estado fáciles de entender, con detalles técnicos expresados en un lenguaje accesible.

ESET EN NÚMEROS

+110 Millones de usuarios en el mundo

+ 400 Mil clientes corporativos

+200 países y territorios

13 centros de investigación y desarrollo