INFORMACIÓN GENERAL DE LA SOLUCIÓN

ENTERPRISE INSPECTOR

Descubra lo desconocido en su red con esta solución de detección y respuesta para endpoints, provista por los expertos en seguridad cibernética

CYBERSECURITY EXPERTS ON YOUR SIDE

ESET Enterprise Inspector es una herramienta sofisticada de detección y respuesta para endpoints que permite la identificación de comportamientos anómalos y violaciones de políticas, la evaluación de riesgos, la respuesta a incidentes, la investigación y la remediación.

Monitorea y evalúa todas las actividades que se llevan a cabo en la red (por ejemplo, usuario, archivo, proceso, registro, memoria y eventos de red) en tiempo real y le permite tomar medidas inmediatas de ser necesario.

Plataforma de protección para endpoints de ESET
Seguridad para endpoints en múltiples capas, donde cada capa envía datos a ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Sofisticada herramienta de detección y respuesta para endpoints que analiza grandes cantidades de datos en tiempo real para que no quede ninguna amenaza sin detectar.

=

Solución completa de prevención, detección y respuesta que permite realizar análisis rápidos y solucionar problemas de seguridad en la red.

ESET cumple con ISO/IEC 27001:2013, un estándar de seguridad de reconocimiento y aplicación internacional para la implementación y gestión de la seguridad de la información. La certificación es otorgada por SGS un organismo acreditado independiente de certificación, y demuestra el pleno cumplimiento de ESET con las mejores prácticas líderes en la industria.

¿En qué se diferencia ESET?

RESPUESTA SINCRONIZADA

Al basarse en la oferta existente de soluciones de seguridad para endpoints de ESET, crea un ecosistema consistente que permite el cruce de datos de todos los objetos relevantes y la remediación sincronizada de incidentes. Los equipos de seguridad pueden eliminar procesos, descargar el archivo que activó una alerta o simplemente iniciar el apagado o reinicio de la computadora directamente desde la consola.

ARQUITECTURA ABIERTA

Proporciona una detección única basada en el comportamiento y en la reputación de archivos, que es completamente transparente para los equipos de seguridad. Todas las reglas se pueden editar fácilmente a través de XML para permitir un ajuste detallado y también pueden crearse desde cero para cubrir las necesidades de entornos corporativos específicos, incluyendo las integraciones con SIEM.

ACCESO REMOTO

ESET Enterprise Inspector cuenta con funcionalidades remotas de PowerShell, que les permiten a los ingenieros de seguridad inspeccionar y configurar las computadoras corporativas de manera remota, con lo que se logra una respuesta sofisticada sin interrumpir el flujo de trabajo del usuario.

MULTIPLATAFORMA

ESET Enterprise Inspector es compatible con Windows y MacOS, por lo que constituye la opción perfecta para entornos que trabajan con diversas plataformas.

API PÚBLICA

ESET Enterprise Inspector ofrece una API que permite acceder a las detecciones, exportarlas y remediarlas, además se integra en forma efectiva con las herramientas SIEM, SOAR, los sistemas de tickets y muchos otros.

SENSIBILIDAD AJUSTABLE

Configure la sensibilidad de las reglas de detección para diferentes grupos de computadoras o usuarios y elimine fácilmente las falsas alarmas. Combine criterios como nombre de archivo, ruta, hash, línea de comandos y firmante para ajustar con precisión las condiciones de activación de las alertas.

MITRE ATT&CK™

Las detecciones de ESET Enterprise Inspector incluyen una referencia al marco MITRE ATT&CK™ (Tácticas, Técnicas y Conocimiento Común de Adversarios). De esta forma, con un solo clic se obtiene información completa incluso sobre las amenazas más complejas.

SISTEMA DE REPUTACIÓN

El sistema de filtrado de ESET de gran alcance les permite a los ingenieros de seguridad filtrar todas las aplicaciones conocidas mediante el sistema de reputación de archivos provisto por ESET. Nuestro sistema de reputación contiene una base de datos de cientos de millones de archivos no infectados para garantizar que los equipos de seguridad se ocupen solamente de lo desconocido, y no pierdan tiempo con falsos positivos.

ESET EN NÚMEROS

+110 Millones
de usuarios en el mundo

+ 400 Mil
clientes corporativos

+ 200
países y territorios

13
centros de investigación y desarrollo

Las posibilidades

CACERÍA DE AMENAZAS

Aplique filtros a los datos para ordenarlos según la popularidad, la reputación, la firma digital, el comportamiento o la información contextual del archivo. La configuración de filtros múltiples permite la detección automatizada de amenazas, que se puede personalizar según el entorno de cada empresa. Facilita la búsqueda de amenazas, incluyendo las amenazas persistentes avanzadas (APT) y los ataques dirigidos.

DETECCIÓN DE INCIDENTES (ANÁLISIS DE CAUSAS DE ORIGEN)

Vea en forma rápida y fácil todos los incidentes de seguridad en la sección de alarmas. Sus equipos podrán consultar el análisis completo de la causa de origen, que incluye: qué se vio afectado, dónde y cuándo se activó el ejecutable, el script o la acción en cuestión.

INVESTIGACIÓN Y REMEDIACIÓN

Use un conjunto de reglas integradas o cree propias para responder a los incidentes detectados. Cada alarma activada muestra el paso conveniente a seguir para la remediación. La funcionalidad de respuesta rápida permite bloquear archivos específicos por su hash, eliminar procesos y ponerlos en cuarentena, y aislar o apagar las máquinas seleccionadas en forma remota. La funcionalidad de respuesta rápida ayuda a garantizar que ningún incidente individual se filtre al resto de la empresa.

AISLAMIENTO CON UN SOLO CLIC

Defina políticas de acceso a la red para detener rápidamente los movimientos laterales del malware. Aísle un dispositivo infectado del resto de la red con un solo clic en la interfaz de EEI. Asimismo, quite fácilmente los dispositivos del estado de contención.

PUNTAJE

Priorice la gravedad de las alarmas mediante la funcionalidad de puntaje, que atribuye un valor de gravedad a los eventos y le permite al administrador identificar fácilmente las computadoras que corren mayor riesgo de sufrir un incidente potencial.

ETIQUETAS

Agregue o quite etiquetas para filtrar más rápido los objetos en EEI, como computadoras, alarmas, exclusiones, tareas, ejecutables, procesos y scripts. Las etiquetas se comparten entre los usuarios y, una vez creadas, se pueden asignar en cuestión de segundos.

RECOPILACIÓN DE DATOS

Vea la información detallada de los módulos recién ejecutados, incluyendo el tiempo de ejecución, el usuario que lo ejecutó, el tiempo de espera y los dispositivos atacados.

INICIO DE SESIÓN SEGURO

Habilite la autenticación en dos fases, que añade una capa adicional de seguridad para su cuenta de administrador e impide que un adversario pueda iniciar sesión, incluso aunque tenga su contraseña.

DETECCIÓN DE INDICADORES DE SISTEMAS COMPROMETIDOS

Vea y bloquee módulos en base a más de 30 indicadores diferentes, incluyendo el hash, las modificaciones del registro, las modificaciones de archivos y las conexiones de red.

DETECCIÓN DE ANOMALÍAS Y DEL COMPORTAMIENTO

Verifique las acciones llevadas a cabo por un ejecutable y utilice el sistema de reputación de archivos ESET LiveGrid® para evaluar rápidamente si los procesos ejecutados son seguros o sospechosos. La agrupación de computadoras por usuario o departamento les permite a los equipos de seguridad identificar si el usuario tiene permiso para realizar una acción específica o no.

VIOLACIÓN DE POLÍTICAS CORPORATIVAS

Bloquee la ejecución de módulos maliciosos en su red. Detecte violaciones de las políticas corporativas sobre el uso de software específico, como aplicaciones de torrents, almacenamiento en la nube, navegación Tor u otro software no deseado.