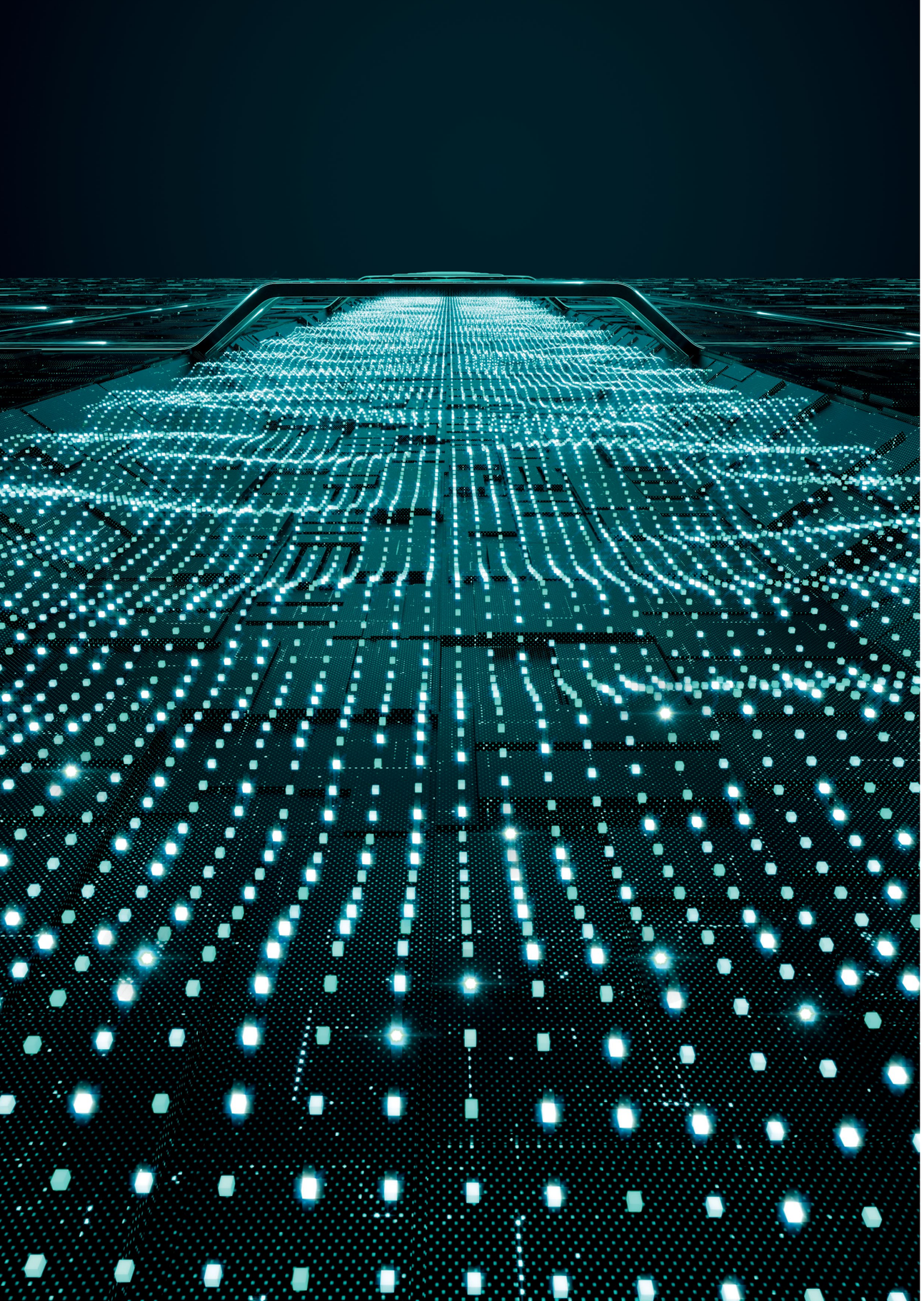
INFORMACIÓN GENERAL DE LA SOLUCIÓN

INSPECT

Componente que brinda **capacidad de detección y respuesta extendida (XDR)** al utilizarlo con la plataforma **ESET PROTECT.**

Progress. Protected.



¿Qué es una **solución de detección y respuesta extendida (XDR)?**

ESET Inspect, el componente que brinda XDR al utilizarlo con la plataforma ESET PROTECT, es una herramienta para la identificación de comportamientos anómalos e infracciones, evaluación de riesgos, respuesta a incidentes, investigaciones y remediación.

Monitorea y evalúa todas las actividades que se llevan a cabo en la red (por ejemplo, eventos de usuarios, archivos, procesos, registros, memoria y red) en tiempo real y le permite tomar medidas de inmediato cuando sea necesario.

Las más de 800 (y contando) reglas de detección de ESET permiten una búsqueda integral de amenazas.

¿Por qué es importante tener una **solución de XDR?**

VIOLACIONES DE SEGURIDAD

Las empresas no solo deben ser capaces de identificar las violaciones de datos, sino también contenerlas y remediarlas. La mayoría de ellas no están preparadas para realizar una investigación minuciosa de este tipo, por lo que suelen contratar a un proveedor externo para que las asista. Hoy en día, las organizaciones necesitan tener mayor visibilidad en sus computadoras para garantizar que las amenazas emergentes, el comportamiento inapropiado de los empleados y las aplicaciones no deseadas no pongan en riesgo las ganancias y la reputación de la empresa.

Los principales tipos de industrias que suelen ser víctimas de la violación de datos son las que tienen información valiosa, como las industrias financieras, minoristas, de la salud y del sector público. No obstante, eso no significa que las demás industrias estén a salvo, solo que los hackers suelen medir cuánto esfuerzo necesitan invertir a cambio de la ganancia.

AMENAZAS PERSISTENTES AVANZADAS Y ATAQUES DIRIGIDOS

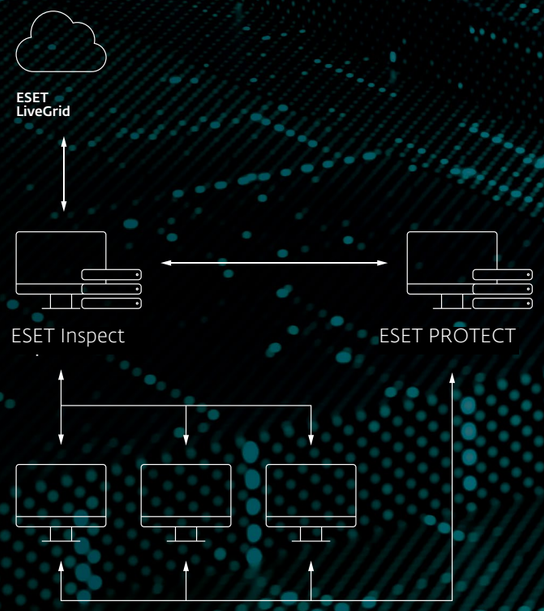
Los sistemas de EDR comúnmente se utilizan para identificar amenazas persistentes avanzadas (APT, del inglés) o ataques dirigidos mediante la Cacería de amenazas, reducir el tiempo de respuesta al incidente, y prevenir ataques futuros en forma proactiva. La detección de amenazas APT en particular es de suma importancia para las empresas, dado que la mayoría de ellas en la actualidad no están preparadas para detener los ataques más nuevos, que pueden estar presentes en su red y pasar desapercibidos por días e incluso meses.

Suministra una **capacidad de detección exclusiva de ESET basada en la conducta y la reputación de los archivos**, que es completamente transparente para los equipos de seguridad, y ofrece datos en tiempo real provenientes de más de 100 millones de endpoints recopilados en nuestro sistema LiveGrid.

MAYOR VISIBILIDAD DE LA ORGANIZACIÓN

Los problemas más importantes para las grandes corporaciones son las amenazas internas y los ataques de phishing. Los ataques de phishing se suelen usar contra grandes empresas debido a la gran cantidad de empleados a los que se puede dirigir la amenaza. De esta forma, son mayores las probabilidades de que un solo trabajador caiga en la trampa y termine infectando toda la empresa. Los ataques internos son otra de las amenazas principales para las grandes corporaciones, aquí también porque la gran cantidad de empleados aumenta las probabilidades de que al menos uno de ellos actúe en contra de los mejores intereses de la empresa.

Los sistemas de EDR proporcionan la visibilidad necesaria para que las organizaciones vean, comprendan, bloqueen y solucionen cualquier problema presente en sus dispositivos. Esto incluye bloquear los archivos adjuntos de correos electrónicos que contienen amenazas, y garantizar que los empleados solo puedan utilizar y acceder a los recursos de la organización que les corresponden.



Hoy en día, las organizaciones necesitan tener mayor visibilidad en sus computadoras para garantizar que las **amenazas emergentes**, el **comportamiento inapropiado de los empleados** y las **aplicaciones no deseadas** no pongan en riesgo las ganancias y la reputación de la empresa.

¿En qué se diferencia ESET?

PREVENCIÓN, DETECCIÓN Y RESPUESTA COMPLETA

Permite un rápido análisis y solución de cualquier problema de seguridad en su red. La seguridad en múltiples niveles de ESET, en la que cada capa envía datos a ESET Inspect, analiza grandes cantidades de datos en tiempo real para que ninguna amenaza pase desapercibida.

SOLUCIÓN DE UN PROVEEDOR PRIMERO DE SEGURIDAD

ESET ha estado luchando contra las ciberamenazas durante más de 30 años. Como empresa basada en la ciencia, lleva mucho tiempo a la vanguardia de desarrollos como el aprendizaje automático, la tecnología en la nube y ahora XDR.

MEJOR PREVENIR QUE CURAR

El enfoque de ESET para XDR está estrechamente relacionado con sus productos de prevención reconocidos por analistas independientes. Gracias a su compromiso de desarrollar tecnología de detección de alta calidad, la tecnología de prevención de ESET es líder mundial.

LISTO PARA COMENZAR A TRABAJAR

La solución de ESET funciona de inmediato, pero es lo suficientemente potente como para permitir la modificación granular por parte de cazadores de amenazas experimentados.

FLEXIBILIDAD DE IMPLEMENTACIÓN

ESET Inspect puede ejecutarse a través de sus propios servidores locales o a través de una instalación basada en la nube, lo que le permite ajustar su configuración de acuerdo con sus objetivos de TCO y la capacidad del hardware.

AUTOMATIZACIÓN Y PERSONALIZACIÓN

Ajuste fácilmente ESET Inspect al nivel de detalle y automatización que necesita. Elija su nivel de interacción deseado, y el tipo y la cantidad de datos que se almacenarán, durante la configuración inicial y con la ayuda de perfiles de usuario preestablecidos, y luego deje que el modo de aprendizaje mapee el entorno de su organización y sugiera exclusiones a falsos positivos cuando sea necesario.

MITRE ATT&CK™

Las detecciones de ESET Inspect 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

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

Casos de uso

Detección de amenazas en profundidad: ransomware

Hoy en día, el ransomware intenta pasar desapercibido en la red, y se extiende silenciosamente entre tantas endpoints como le sea posible. Penetra en los backups de las máquinas para asegurar su ejecución incluso tras la reversión a imágenes anteriores del sistema.

El Agente ESET Inspect Inspector amplía la funcionalidad de las soluciones de seguridad para endpoints de ESET y le permite detectar proactivamente si hay un ransomware presente en su red. En un escenario de ransomware típico, el usuario recibe un correo electrónico con un documento de texto adjunto. A continuación, intenta abrir el documento de Word pero se le pide que habilite el uso de macros. Una vez que el usuario activa las macros, se descarga un archivo ejecutable en el sistema que comienza a cifrar todo lo que puede, incluyendo las unidades asignadas.

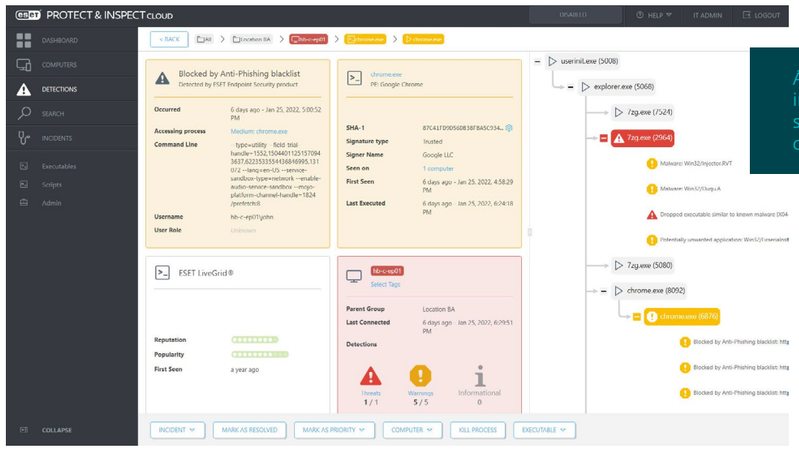
Con ESET Inspect, su equipo de seguridad recibe alertas sobre este tipo de comportamiento, y en unos pocos clics podrá ver qué fue afectado, dónde y cuándo se activó un ejecutable, un script o una acción específica, y analizar su origen.

CASO DE USO

Una empresa desea incorporar herramientas adicionales para detectar en forma proactiva el ransomware, y además quiere recibir notificaciones inmediatas si se observa un comportamiento similar al ransomware en su red.

SOLUCIÓN

- ✓ Incorporar reglas para detectar las aplicaciones que se ejecuten desde carpetas temporales.
- ✓ Incorporar reglas para detectar si los archivos de Office (Word, Excel, PowerPoint) ejecutan scripts o archivos ejecutables adicionales.
- ✓ Emitir una alerta si se detecta alguna de las extensiones de ransomware más comunes en un dispositivo.
- ✓ Ver las alertas de Ransomware Shield correspondientes a las soluciones ESET Endpoint Security en una misma consola.



Árbol de procesos e información detallada sobre comportamiento de código malicioso

Detección del comportamiento y de infractores reincidentes

El punto más débil en materia de seguridad suelen ser los colaboradores, por más que no tenga malas intenciones.

Para identificar estos elementos más débiles, ESET Inspect clasifica las computadoras según la cantidad de alarmas únicas activadas. Si un usuario activa múltiples alarmas, es un indicador claro de que es necesario validar su actividad.

CASO DE USO

Algunos usuarios de la red son infractores reincidentes en lo que respecta a las infecciones de malware. Los mismos usuarios se siguen infectando una y otra vez. ¿Es consecuencia de un comportamiento arriesgado? ¿O son víctimas de ataques dirigidos con más frecuencia que otros usuarios?

SOLUCIÓN

- ✓ Vea fácilmente los usuarios y dispositivos problemáticos.
- ✓ Realice rápidamente un análisis de la causa de origen para encontrar la fuente de las infecciones.
- ✓ Remedie los vectores de infección encontrados, como el correo electrónico, la Web o los dispositivos USB.

Cacería y bloqueo de amenazas

El elemento que distingue a ESET Inspect es la cacería de amenazas mediante el método "encontrar una aguja en un pajar".

Al filtrar los datos según la popularidad o reputación de los archivos, las firmas digitales, el comportamiento y la información contextual, es capaz de identificar e investigar cualquier tipo de actividad maliciosa. La configuración de múltiples filtros permite realizar tareas automatizadas de cacería de amenazas. También permite ajustar el umbral de detección para un entorno específico de la empresa.

Cualquier actividad maliciosa se puede identificar e investigar con facilidad.

CASO DE USO

Su sistema de alerta temprana o centro de operaciones de seguridad (SOC) emite una nueva alerta sobre una amenaza. ¿Qué pasos debería seguir?

SOLUCIÓN

- ✓ Aproveche el sistema de alerta temprana para ver los datos de las amenazas nuevas o inminentes.
- ✓ Examine todas las computadoras para detectar la existencia de la nueva amenaza.
- ✓ Busque en las computadoras los indicadores de compromiso para saber si la amenaza ya existía antes de la emisión de la alerta.
- ✓ Bloquee la amenaza para que no pueda infiltrarse en la red o ejecutarse dentro de la organización.

Visibilidad de red

ESET Inspect es una solución de arquitectura abierta, lo que significa que el equipo de seguridad puede ajustar las reglas de detección que describen las técnicas de ataque de acuerdo con el entorno específico de su organización.

La arquitectura transparente también brinda flexibilidad para configurar ESET Inspect de modo que detecte el incumplimiento de las políticas de la organización respecto al uso de software específico, como aplicaciones de torrents, almacenamiento en la nube, navegación Tor, servidores propios, y otro software no deseado.

CASO DE USO

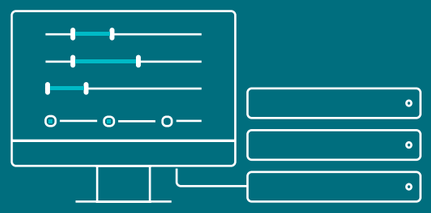
A algunas empresas les preocupan las aplicaciones que los usuarios ejecutan en los sistemas. Pero no solo hay que preocuparse por las aplicaciones instaladas de manera tradicional, sino también por las aplicaciones portátiles que no requieren instalación. ¿Qué puede hacer para controlar esta situación?

SOLUCIÓN

- ✓ Vea y filtre fácilmente las aplicaciones instaladas en todos los dispositivos.
- ✓ Vea y filtre los scripts de todos los dispositivos.
- ✓ Bloquee fácilmente la ejecución de scripts o aplicaciones no autorizados.
- ✓ Notifique a los usuarios cuáles son las las aplicaciones no autorizadas y desinstálelas automáticamente.

No solo debe preocuparse por las aplicaciones instaladas de manera tradicional, sino también por las aplicaciones portátiles que no requieren instalación. ¿Qué puede hacer para controlar esta situación?

El equipo de seguridad puede **ajustar las reglas de detección** que describen las técnicas de ataque de acuerdo con el entorno específico de su organización.



Investigación y remediación basadas en el contexto

La gravedad de una actividad maliciosa depende del contexto.

Las actividades realizadas en las computadoras de los administradores de red son muy diferentes a las del departamento de finanzas, por ejemplo. Al agrupar las computadoras en forma adecuada, los equipos de seguridad pueden identificar fácilmente si un usuario en particular tiene permiso de llevar a cabo cierta actividad en una máquina determinada. La sincronización de los grupos de endpoints de ESET Protect con las reglas de ESET Inspect proporciona excelentes resultados basados en información contextual.

CASO DE USO

Los datos solo son útiles si están acompañados por su contexto. Para poder tomar las decisiones correctas, necesitará saber de qué se tratan las alertas, cuáles son los dispositivos afectados y qué usuarios las están activando.

SOLUCIÓN

- ✓ Identifique y clasifique todas las computadoras con Active Directory, grupos automáticos o grupos manuales.
- ✓ Permita o bloquee aplicaciones o scripts por grupo de equipos.
- ✓ Permita o bloquee aplicaciones o scripts por usuario.
- ✓ Reciba únicamente las notificaciones de ciertos grupos específicos.

Fácil configuración y respuesta (no necesitan un equipo de seguridad)

Por más que la empresa tenga equipos de seguridad exclusivos para realizar estas tareas, muchas veces es difícil priorizar rápidamente entre todas las alarmas activadas y decidir qué hacer a continuación.

Por lo tanto, cada vez que se activa una alarma, se muestran los pasos convenientes a seguir para su remediación. Cuando ESET Inspect identifica una amenaza, ofrece una respuesta de ejecución rápida. Permite bloquear archivos específicos por su hash, eliminar los procesos y ponerlos en cuarentena, y aislar o apagar las máquinas seleccionadas en forma remota.

CASO DE USO

No todas las empresas tienen equipos de seguridad dedicados a estas tareas, por lo que incorporar e implementar reglas avanzadas de detección puede convertirse en un problema.

SOLUCIÓN

- ✓ Nuestra solución incluye más de 180 reglas preconfiguradas.
- ✓ Responda fácil y rápidamente a las amenazas con un solo clic para bloquearlas, detenerlas o poner los dispositivos en cuarentena.
- ✓ Las alarmas ya tienen incorporadas las propuestas de remediación y los pasos a seguir.
- ✓ Las reglas se pueden editar a través de XML para personalizarlas o crear nuevas reglas con facilidad.

La gravedad de una actividad maliciosa depende del contexto. La sincronización de los grupos de endpoints de ESET PROTECT con las reglas de ESET Inspector proporciona excelentes resultados basados en información contextual.

Cada vez que se activa una alarma, se muestran los pasos convenientes a seguir para su remediación.

Las posibilidades

CACERÍA DE AMENAZAS

Utilice la potente búsqueda IOC basada en consultas y aplique filtros a los datos sin procesar para clasificarlos según la popularidad del archivo, la reputación, la firma digital, el comportamiento u otra información contextual. Configuración de varios filtros

permite la caza de amenazas y la respuesta a incidentes automatizada y fácil, incluida la capacidad de detectar y detener APT y ataques dirigidos.

DETECCIÓN DE INCIDENTES (ANÁLISIS DE CAUSAS DE ORIGEN)

Vea rápida y fácilmente todos los incidentes de seguridad en la sección de alertas. Con unos pocos clics, sus equipos de seguridad podrán ver el análisis completo de la causa de origen, incluyendo qué resultó afectado, dónde y cuándo se activó el ejecutable, el script o la acción en cuestión, entre otros datos.

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. Toda la información se almacena en forma local para prevenir la fuga de datos confidenciales.

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, departamento u otros criterios les permite a los equipos de seguridad saber si el usuario tiene permiso para realizar una acción específica y así detectar rápidamente acciones inusuales.

VIOLACIÓN DE POLÍTICAS CORPORATIVAS

Bloquea la ejecución de módulos maliciosos en todas las computadoras de su red corporativa. La arquitectura abierta de ESET Inspect le otorga flexibilidad para detectar 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.

ARQUITECTURA ABIERTA Y LAS INTEGRACIONES

ESET Inspect proporciona una detección única basada en el comportamiento y la reputación que es totalmente transparente para los equipos de seguridad. Todas las reglas se pueden editar fácilmente a través de XML o se crean para satisfacer las necesidades de entornos empresariales específicos, incluidas las integraciones SIEM.

OPCIONES DE RESPUESTA EN VIVO

ESET Inspect viene repleto de acciones de respuesta de un solo clic fácilmente accesibles, como reiniciar y cerrar un punto final, aislar puntos finales del resto de la red, ejecutar un análisis bajo demanda, eliminar cualquier proceso en ejecución y bloquear cualquier aplicación en función de su valor hash. Además, gracias a la opción de respuesta en vivo de ESET Inspect, llamada Terminal, los profesionales de seguridad pueden beneficiarse del conjunto completo de opciones de investigación y corrección en PowerShell.

SISTEMA DE GESTIÓN DE INCIDENCIAS

Agrupe objetos como detecciones, computadoras, ejecutables o procesos en unidades lógicas para ver posibles eventos maliciosos en una línea de tiempo, con acciones de usuario relacionadas. ESET Inspect sugiere automáticamente al respondedor de incidentes todos los eventos y objetos relacionados que puede ser de gran ayuda en las etapas de clasificación, investigación y resolución de un incidente.

DETECCIÓN DE VIOLACIÓN DE LA POLÍTICA DE LA EMPRESA

Bloquee la ejecución de módulos maliciosos en cualquier computadora de la red de su organización. La arquitectura abierta de ESET Inspect ofrece la flexibilidad para detectar violaciones de políticas que se aplican al uso de software específico como aplicaciones de torrent, almacenamiento en la nube, navegación Tor u otro software no deseado.

API PÚBLICA

ESET Inspect presenta una API REST pública que permite el acceso y la exportación de detecciones y su remediación para permitir una integración efectiva con herramientas como SIEM, SOAR, herramientas de emisión de boletos y muchas otras.

Acerca de ESET

Desde hace más de 30 años, desarrollamos soluciones de seguridad que ayudan a más de 100 millones de usuarios en el mundo a disfrutar la tecnología de forma segura.

Al no estar limitados por las exigencias de accionistas del mercado, podemos enfocarnos exclusivamente en la seguridad de la información, mediante investigación y desarrollo constante.

ESET EN NÚMEROS

+110 millones
de usuarios en el mundo

+400 mil
clientes corporativos

+200
países y territorios

13
centros de investigación y desarrollo

ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

protegido por ESET desde 2017, más de 9.000 endpoints

Allianz Suisse

protegido por ESET desde 2016, más de 4.000 buzones de correo

Canon
Canon Marketing Japan Group

protegido por ESET desde 2016, más de 32.000 endpoints

partner de seguridad ISP desde 2008 con una base de clientes de 2 millones

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES

AV comparatives
APPROVED
Business Security
DEC 2021

ESET recibió el premio Business Security APPROVED de AV-Comparatives en el Business Security Test en diciembre de 2021.

G2
Leader
WINTER
2022

ESET logra consistentemente las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son avaladas por clientes de todo el mundo.

FORRESTER®

Las soluciones de ESET fueron reconocidas por el analista Forrester como sample vendor en **"The Forrester Tech Tide(TM): Zero Trust Threat Detection and Response, Q2 2021".**

Digital Security
Progress. Protected.