INSPECT

El componente de habilitación de XDR de la plataforma ESET PROTECT, que ofrece prevención de infracciones, visibilidad mejorada y reparación

Progress. Protected.

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

ESET Inspect, el componente de la plataforma ESET PROTECT que permite el uso de XDR, es una herramienta para la identificación de comportamientos anómalos y vulneraciones, evaluación de riesgos, respuesta a incidentes, investigaciones y reparación.

Permite a los responsables de la respuesta a incidentes supervisar y evaluar todas las actividades en la red y en los dispositivos conectados. También ayuda a automatizar acciones correctivas inmediatas, si son necesarias. Las más de 800 reglas de detección de ESET (y en aumento) permiten una búsqueda exhaustiva de amenazas.

¿Por qué **la detección y respuesta ampliada?**

VULNERACIONES DE DATOS

Las empresas no solo tienen que identificar que se ha producido una vulneración de datos, sino que también tienen que contenerla y remediarla. Todo esto debe hacerse con la máxima precisión y sin interrumpir la continuidad del negocio. La mayoría de las empresas no están preparadas para llevar a cabo este tipo de investigación completa, y en su lugar contratan a un proveedor externo para que los ayude. Hoy en día, las empresas necesitan una mayor visibilidad de sus ordenadores para garantizar que las amenazas emergentes, el comportamiento arriesgado de los empleados y las aplicaciones no deseadas no pongan en peligro los beneficios y la reputación de la empresa.

Los sectores más afectados por las fugas de información son los que tienen datos valiosos de carácter financiero, minorista, sanitario y sector público. Sin embargo, eso no significa que otros sectores estén a salvo, sino que los cibercriminales suelen considerar el esfuerzo frente a la recompensa.

AMENZAZAS PERSISTENTES AVANZADAS (APTs) Y ATAQUES DIRIGIDOS

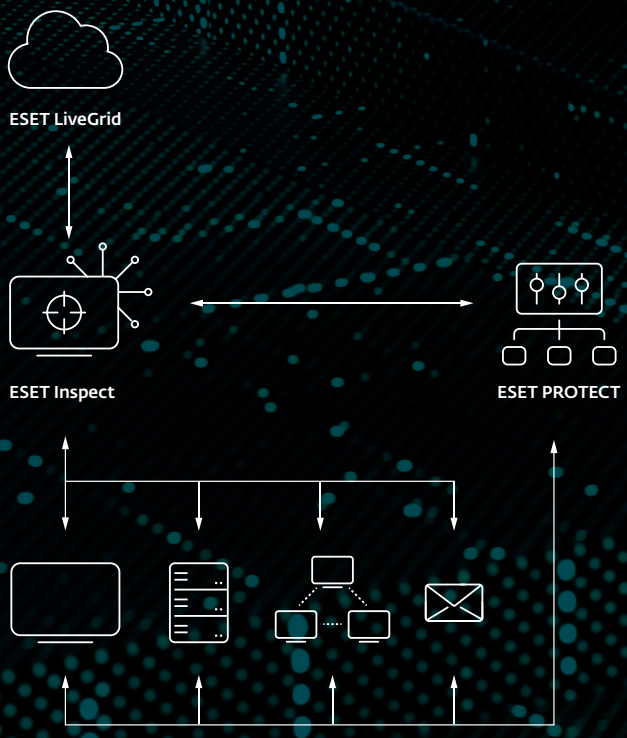
Los sistemas XDR se utilizan habitualmente para: identificar APTs o ataques dirigidos mediante Threat Hunting (detección de amenazas); reducir el tiempo de respuesta ante incidencias; y prevenir futuros ataques de forma proactiva. Descubrir las APTs es particularmente importante para las empresas, puesto que la mayoría de ellas no se sienten preparadas para afrontar los ataques más novedosos que pueden permanecer en la red sin ser detectados durante días o incluso meses.

Proporciona una **detección única basada en el comportamiento y la reputación** que es totalmente transparente para los departamentos de seguridad y que les proporciona información en tiempo real recopilada por más de 100 millones de equipos en nuestra LiveGrid.

ANÁLISIS DE LA EMPRESA CON MAYOR PRECISIÓN

Las amenazas internas y los ataques de phishing son dos de los problemas más importantes a los que se enfrentan las empresas. El phishing se lleva a cabo porque en las compañías trabajan un gran número de empleados a quienes se les puede atacar mediante esta técnica. La posibilidad de que algún empleado pique el cebo y ponga en riesgo a toda la empresa es muy alta. Por otro lado, los ataques desde dentro de la empresa son otra amenaza para aquellas que tienen un gran número de empleados, ya que esto aumenta la probabilidad de que uno de ellos trabaje contra los intereses de su empresa.

Los sistemas XDR proporcionan la mayor visibilidad necesaria para que las empresas detecten, identifiquen, bloqueen y corrijan cualquier problema en todos sus dispositivos. ESET Inspect puede, por ejemplo, identificar y detener rápidamente los scripts maliciosos que se hacen pasar por partes de documentos benignos, como los archivos de Word.



Hoy en día, las empresas necesitan mayor visibilidad sobre lo que ocurre en sus equipos para garantizar que las **amenazas emergentes, el comportamiento arriesgado de los empleados** y **las aplicaciones no deseadas** no pongan en peligro los beneficios y la reputación de la empresa.

ESET marca la diferencia

PREVENCIÓN, DETECCIÓN Y RESPUESTA COMPLETAS

Permite un rápido análisis y corrección de cualquier problema de seguridad en tu red. La seguridad multicapa de ESET, en la que cada una de las capas envía datos a ESET Inspect, analiza grandes cantidades de datos en tiempo real para que ninguna amenaza pase desapercibida.

SOLUCIÓN DE UN FABRICANTE QUE DA PRIORIDAD A LA SEGURIDAD

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

MÁS VALE PREVENIR QUE CURAR

El enfoque de ESET respecto a la XDR está estrechamente relacionado con sus productos de prevención, que han sido premiados en varias ocasiones. Gracias a su compromiso de desarrollar tecnología de detección de alta calidad, la tecnología de prevención de ESET es líder mundial.

VISIBILIDAD DETALLADA DE LA RED

Con reglas de detección transparentes (ESET tiene más de 800 y seguimos aumentando), indicadores avanzados de peligro (IoC) y capacidad de búsqueda, una revisión exhaustiva de tu red te permitirá identificar cualquier cosa sospechosa.

LISTO PARA EMPEZAR A TRABAJAR AHORA

La solución de ESET funciona de forma inmediata, pero es lo suficientemente potente para permitir la modificación granular por parte de detectores de amenazas experimentados.

FLEXIBILIDAD DE IMPLEMENTACIÓN

Te dejamos decidir cómo implementar tu solución de seguridad: ESET Inspect puede ejecutarse a través de tus propios servidores en local, o a través de una instalación basada en la nube, lo que te permite ajustar la configuración en función de tus objetivos de TCO y de la capacidad del hardware.

MITRE ATT&CK™

ESET Inspect hace referencia a sus detecciones en el programa MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), que, con un solo clic, te ofrece información completa incluso sobre las amenazas más complejas.

SISTEMA DE REPUTACIÓN

El amplio filtrado de ESET permite a los expertos en seguridad filtrar todas las aplicaciones buenas conocidas utilizando el robusto sistema de reputación de archivos de ESET. Nuestro sistema de reputación contiene una base de datos de cientos de millones de archivos legítimos para garantizar que los equipos de ciberseguridad inviertan su tiempo en combatir las amenazas desconocidas y potencialmente maliciosas y no en los falsos positivos.

AUTOMATIZACIÓN Y PERSONALIZACIÓN

Ajusta fácilmente ESET Inspect al nivel de detalle y automatización que necesites. Elige el nivel de interacción deseado, y el tipo y la cantidad de datos que se van a almacenar, durante la configuración inicial y con la ayuda de los perfiles de usuario preestablecidos, y luego deja que el Modo de Aprendizaje elabore un mapa del entorno de tu empresa y sugiera exclusiones a los falsos positivos cuando sea necesario.

Casos prácticos

Detección profunda de amenazas – ransomware

Actualmente, el ransomware intenta pasar desapercibido en la red, pero se está propagando silenciosamente a través del máximo número de equipos posible. Accede a las copias de seguridad de los equipos para asegurarse que incluso la restauración de imágenes previas no evite la ejecución inmediata del ransomware.

ESET Inspect amplía la funcionalidad de las soluciones de seguridad para endpoints de ESET y te permite detectar de forma proactiva el ransomware que ya está presente en tu red. En un entorno típico de amenaza de ransomware, un usuario recibe un correo electrónico con un documento adjunto en formato Word, lo abre y se le solicita que habilite las macros. Cuando lo hace, se descarga un ejecutable en el sistema que comienza a cifrar todo lo que está a su alcance, incluidas las unidades mapeadas.

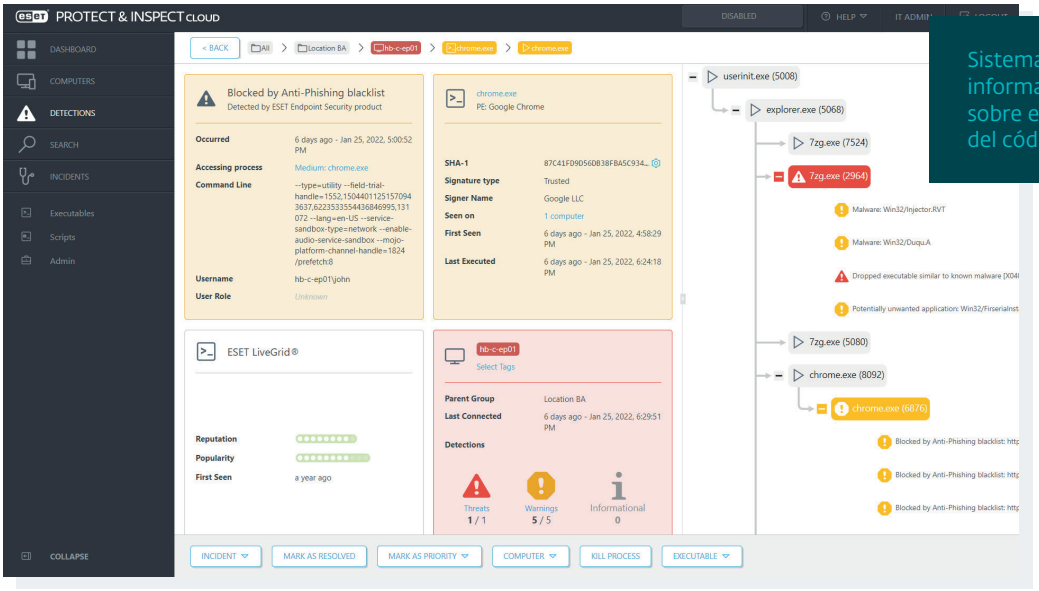
ESET Inspect permite que tu equipo de ciberseguridad detecte este tipo de comportamiento, y con unos pocos clics puedas identificar qué se ha visto afectado, dónde y cuándo se activó un determinado ejecutable, script o acción, además de analizar la causa de esta alerta hasta su origen.

CASO PRÁCTICO

Una empresa quiere herramientas adicionales para detectar el ransomware de forma proactiva, además de recibir notificaciones rápidamente si se detecta un comportamiento parecido a este tipo de malware en la red.

SOLUCIÓN

- ✓ Introduce reglas para detectar aplicaciones cuando se ejecuten desde carpetas temporales.
- ✓ Introduce reglas para detectar archivos de MS Office (Word, Excel, PowerPoint) cuando ejecuten scripts adicionales o ejecutables.
- ✓ Alerta si alguna de las extensiones más comunes de ransomware se detecta en un dispositivo.
- ✓ Visualiza las alertas de Ransomware Shield de ESET Endpoint Security Solutions en la misma consola.



Sistema de procesos e información detallada sobre el comportamiento del código malicioso

Detección del comportamiento y acciones recurrentes de los atacantes

El eslabón más débil en seguridad es a menudo una persona sentada al teclado, incluso sin que tenga malas intenciones.

ESET Inspect identifica fácilmente estos elementos débiles y clasifica los equipos por el número de alarmas activadas. Si un usuario activa múltiples alarmas, es un indicador claro de que debería revisarse esta actividad.

CASO PRÁCTICO

En tu red corporativa tienes usuarios que son atacados una y otra vez con algún tipo de malware. Por este motivo, los mismos usuarios continúan infectándose una y otra vez. ¿Se debe a un comportamiento de riesgo? ¿O son un objetivo más claro ellos que otros usuarios?

SOLUCIÓN

- ✓ Visualiza fácilmente los usuarios y dispositivos problemáticos.
- ✓ Completa fácilmente un análisis de las causas que han provocado el problema de seguridad para encontrar el foco de las infecciones.
- ✓ Elimina los vectores de infección encontrados tales como el correo electrónico, la web o dispositivos con puerto USB.

Detección y bloqueo de amenazas

El valor que marca la diferencia de ESET Inspect radica en una estrategia de detección de amenazas similar a la de "encontrar una aguja en un pajar".

Aplicando filtros a la información que clasifican los archivos según su popularidad o reputación, su firma digital, comportamiento o información contextual, todas las actividades maliciosas pueden identificarse e investigarse fácilmente. Configurar múltiples filtros automatiza la tarea de detección de amenazas y permite ajustar el umbral de detección en el entorno específico de la empresa.

Cualquier actividad maliciosa puede ser fácilmente identificada e investigada.

CASO PRÁCTICO

Tu sistema de alerta temprana o tu centro de operaciones de seguridad (SOC) te proporciona una nueva alerta de amenazas. ¿Cuáles son tus siguientes pasos?

SOLUCIÓN

- ✓ Aprovecha el sistema de alerta temprana para recopilar datos sobre las nuevas o futuras amenazas.
- ✓ Busca en todos los equipos la existencia de una nueva amenaza.
- ✓ Busca en todos los equipos indicadores que revelen que la amenaza existía antes del aviso.
- ✓ Bloquea la amenaza para evitar que se infiltre en una red o que se ejecute dentro de la estructura de la empresa.

Visibilidad de la red

ESET Inspect es una solución de arquitectura abierta, lo cual significa que un equipo de seguridad puede ajustar las reglas de detección que describen las técnicas de ataque al entorno específico de la empresa.

La arquitectura abierta también da flexibilidad para configurar ESET Inspect para detectar infracciones de las políticas de la empresa sobre el uso de software específico, como aplicaciones de torrents, almacenamientos en la nube, navegación Tor, inicio de servidores propios y otro software no deseado.

CASO PRÁCTICO

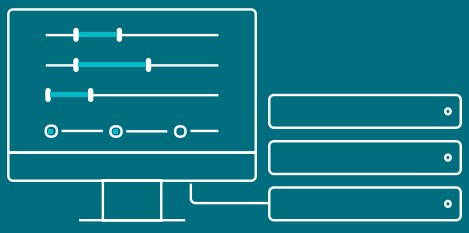
Algunas empresas están preocupadas por determinadas aplicaciones que los usuarios utilizan en sus equipos. No solo deberías preocuparte por las instaladas de manera habitual, sino que también tendrías que revisar las móviles, que en realidad no se instalan. Pero, ¿cómo puedes controlarlas?

SOLUCIÓN

- ✓ Accede fácilmente y filtra todas las aplicaciones instaladas en los dispositivos.
- ✓ Visualiza y filtra todos los scripts de los dispositivos.
- ✓ Bloquea fácilmente todos los scripts no autorizados o las aplicaciones para que no se ejecuten.
- ✓ Notifica a los usuarios sobre las aplicaciones no autorizadas y desinstálalas automáticamente.

No solo deberías preocuparte por las aplicaciones instaladas de manera habitual, sino que también tendrías que revisar las portables, que en realidad no se instalan. Pero, ¿cómo puedes controlarlas?

El departamento de ciberseguridad puede **modificar las reglas de detección** a través de un análisis detallado de las técnicas de ataque al entorno específico de la empresa.



Entorno de investigaciones y soluciones

La "mala intención" de una actividad depende del entorno.

Los ordenadores de los administradores de red y los del departamento financiero llevan a cabo actividades muy diferentes. Los equipos de ciberseguridad pueden confirmar si un usuario está autorizado a realizar una actividad determinada gracias a la organización adecuada de los equipos. La sincronización entre el centro de gestión de seguridad, el conjunto de endpoints de ESET y las reglas de ESET Inspect, produce excelentes resultados en relación a la información sobre el contexto de una posible amenaza.

CASO PRÁCTICO

La calidad de los datos depende de su entorno. Para tomar las decisiones adecuadas, necesitas saber cuáles son las alertas, en qué dispositivos tienen lugar y qué usuarios las activan.

SOLUCIÓN

- ✓ Identifica y agrupa los ordenadores de forma manual o automática con Directorio Activo.
- ✓ Permite o bloquea aplicaciones o scripts basados en el conjunto de ordenadores.
- ✓ Permite o bloquea aplicaciones o scripts basados en los usuarios.
- ✓ Recibe únicamente notificaciones de ciertos grupos.

Fácil instalación y respuesta sin la intervención del equipo de seguridad

Incluso si la empresa tiene equipos de seguridad especializados, la rápida priorización y elección de los pasos a seguir entre todas las alarmas activadas suele ser complicada.

Por lo tanto, se proponen una serie de pasos para solucionar cada alarma activada. Cuando ESET Inspect identifica una amenaza, ofrece una rápida respuesta. Los archivos específicos pueden ser bloqueados por el grupo, los procesos eliminados y puestos en cuarentena, y las máquinas seleccionadas aisladas o desactivadas a distancia.

CASO PRÁCTICO

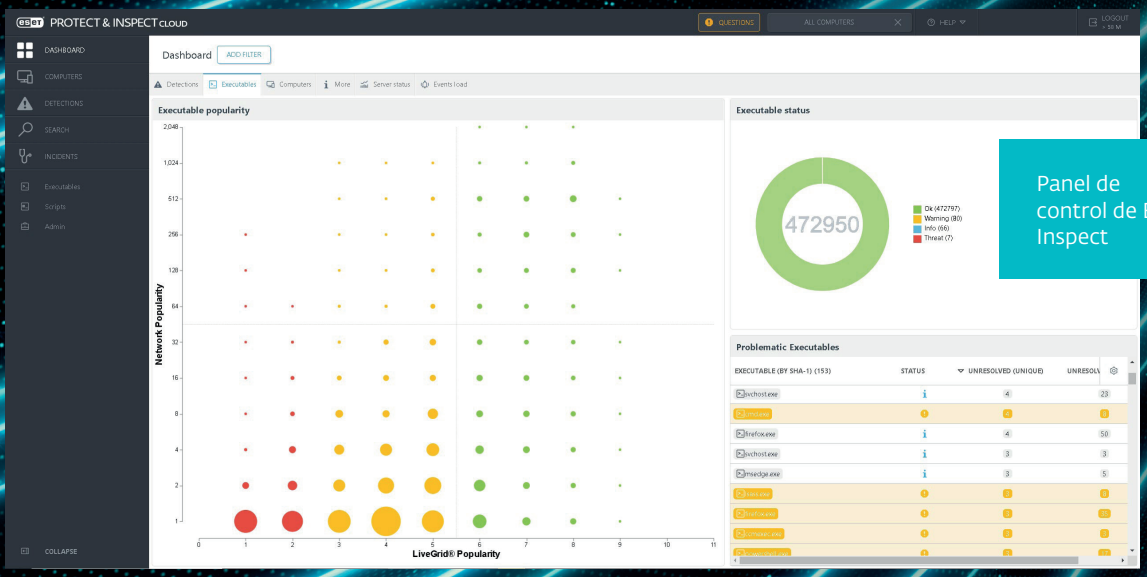
No todas las empresas tienen equipos de ciberseguridad especializados y, por tanto, añadir e implementar las reglas de detección avanzadas puede ser complicado.

SOLUCIÓN

- ✓ Más de 300 reglas preconfiguradas incorporadas.
- ✓ Respuesta fácil y rápida para bloquear, eliminar o poner en cuarentena con un solo clic.
- ✓ Las soluciones y pasos a seguir se convierten en alarmas.
- ✓ Las reglas se pueden editar a través del lenguaje XML para permitir un fácil ajuste o creación de nuevas reglas.

La “maldad” de una actividad depende del contexto. La sincronización de los grupos de endpoints de ESET PROTECT y las reglas de ESET Inspect proporcionan resultados extraordinarios de información contextual.

Para cada alarma activada, se proponen los siguientes pasos a realizar para su corrección.



Panel de control de ESET Inspect

Características de la solución

SISTEMA DE GESTIÓN DE INCIDENTES

Agrupa detecciones, equipos, ejecutables o procesos en unidades lógicas para ver posibles eventos maliciosos en una franja de tiempo, con acciones de usuario relacionadas. ESET Inspect sugiere automáticamente al encargado de responder a los incidentes todos los eventos y objetos relacionados que pueden ser de gran ayuda en las etapas de clasificación, investigación y resolución de un incidente.

OPCIONES DE RESPUESTA EN TIEMPO REAL

ESET Inspect viene provisto de acciones de respuesta fácilmente accesibles con un solo clic, como reiniciar y apagar un equipo, aislar los equipos 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 tiempo real de ESET Inspect, denominada Terminal, los profesionales de la seguridad pueden beneficiarse de todo el conjunto de opciones de investigación y reparación de PowerShell.

ANÁLISIS DESDE LA RAÍZ DEL PROBLEMA

Visualiza fácilmente el análisis desde la raíz del problema, y el mapa de procesos completo, de cualquier cadena de eventos potencialmente maliciosos, profundiza en el nivel de detalle deseado y toma decisiones basadas en el amplio contexto proporcionado y en las explicaciones de las causas tanto benignas como maliciosas, elaboradas por nuestros expertos en malware.

API PÚBLICA

ESET Inspect cuenta con una API REST pública que permite acceder y exportar las detecciones y su reparación para permitir una integración efectiva con herramientas como SIEM, SOAR, herramientas de ticketing y muchas otras.

DETECCIÓN DE AMENAZAS

Utiliza la potente búsqueda IOC basada en consultas y aplica filtros a los datos sin procesar para clasificarlos en función de la popularidad de los archivos, reputación, firma digital, comportamiento u otra información contextual. La configuración de varios filtros permite la detección automatizada y sencilla de amenazas y la respuesta a incidentes, incluyendo la capacidad de detectar y detener APTs y ataques dirigidos.

ACCESO REMOTO SEGURO Y SIN COMPLICACIONES

La respuesta a incidentes y los servicios de seguridad son tan fluidos como la facilidad con la que se accede a ellos, tanto en lo que respecta a la conexión del responsable del incidente con la consola, como a la conexión con los equipos de destino. La conexión funciona a una velocidad prácticamente en tiempo real y con las máximas medidas de seguridad aplicadas, todo ello sin necesidad de herramientas de terceros.

AISLAMIENTO CON UN SOLO CLIC

Define políticas de acceso a la red para detener rápidamente los movimientos laterales de malware. Aísla de la red un dispositivo comprometido con un solo clic en la interfaz de ESET Inspect. Además, elimina fácilmente los dispositivos del estado de contención.

DETECCIÓN DE ANOMALÍAS Y COMPORTAMIENTOS

Comprueba las acciones llevadas a cabo por un ejecutable y utiliza el sistema de reputación LiveGrid® de ESET para evaluar rápidamente si los procesos ejecutados son seguros o sospechosos. La monitorización de incidentes anómalos relacionados son posibles gracias a reglas específicas escritas para ser activadas por el comportamiento, no por simples detecciones de malware o firmas. La agrupación de ordenadores por usuario o departamento permite a los equipos de ciberseguridad identificar si el usuario está autorizado a realizar una acción específica o no.

ETIQUETADO

Asigna y deniega etiquetas para un filtrado rápido a objetos de ESET Inspect como ordenadores, alarmas, exclusiones, tareas, ejecutables, procesos y scripts. Las etiquetas se comparten entre los usuarios y, una vez creadas, pueden asignarse en cuestión de segundos.

MÚLTIPLES INDICADORES DE COMPROMISO

Examina y bloquea módulos basados en más de 30 indicadores diferentes, incluyendo hash, modificaciones del registro, modificaciones de archivos y conexiones de red.

ARQUITECTURA E INTEGRACIONES AVANZADAS

ESET Inspect proporciona una detección única basada en el comportamiento y la reputación totalmente transparente para los equipos de seguridad. Todas las reglas son fácilmente editables a través de XML para permitir el ajuste o crear nuevas fácilmente para satisfacer las necesidades de entornos empresariales específicos, incluyendo las integraciones SIEM.

DETECCIÓN DE INCUMPLIMIENTO DE LA POLÍTICA DE LA EMPRESA

Bloquea la ejecución de módulos maliciosos en cualquier ordenador de la red de tu empresa. La arquitectura abierta de ESET Inspect ofrece la flexibilidad necesaria para detectar los incumplimientos de las políticas que se aplican al uso de software específico como las aplicaciones torrent, el almacenamiento en la nube, la navegación Tor u otro software no deseado.

PUNTUACIÓN AVANZADA

Prioriza la gravedad de las alarmas con una funcionalidad de puntuación que atribuye un valor de gravedad a los incidentes y permite al administrador identificar fácilmente los ordenadores con una mayor probabilidad de un incidente potencial.

OBTENCIÓN DE DATOS LOCALES

Examina datos completos sobre un proceso recién ejecutado, incluyendo la hora de ejecución, el usuario que lo ejecutó, el tiempo de permanencia y los dispositivos atacados. Todos los datos se almacenan localmente para evitar la fuga de datos sensibles.

Acerca de ESET

Durante más de 30 años, ESET® ha desarrollado software y servicios de seguridad informática líderes en el sector para ofrecer una protección completa y multicapa contra las ciberamenazas a empresas y consumidores de todo el mundo.

ESET es pionera en tecnologías de aprendizaje automático y en la nube que previenen, detectan y responden al malware. ESET es una empresa privada que promueve la investigación y el desarrollo científico en todo el mundo.

ESET EN CIFRAS

+100M
de usuarios seguros en todo el mundo

+400k
clientes de empresa

+200
países y territorios

13
centros de I+D en el mundo

ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

Protegido por ESET desde 2017, con más de 9.000 endpoints

Allianz Suisse

Protegido por ESET desde 2016, con más de 4.000 buzones de correo

Canon
Canon Marketing Japan Group

Protegidos por ESET desde 2016, con más de 32.000 endpoints

Colaborador de seguridad de ISP desde 2008, con una base de 2 millones de clientes

COMPROMETIDOS CON LOS MÁS ALTOS ESTÁNDARES DE LA INDUSTRIA

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.

Leader WINTER 2022

ESET consigue de manera consecutiva las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son apreciadas por clientes de todo el mundo.

FORRESTER®

Las soluciones de ESET son constantemente reconocidas por las principales firmas analistas, incluyendo en "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" como fabricante ejemplar.

Digital Security
Progress. Protected.