Plataforma ESET PROTECT y Microsoft Sentinel SIEM y SOAR

Integración sin esfuerzo para mejorar la detección y respuesta ante amenazas

eset® Digital Security
Progress. Protected.

RESUMEN DE LA SOLUCIÓN

Integrar y automatizar para maximizar la eficacia

Experimenta operaciones de seguridad fluidas con la potente integración de la plataforma nativa XDR ESET PROTECT y la solución SIEM y SOAR nativa en la nube Microsoft Sentinel. Potencie a los analistas de su centro de operaciones de seguridad (SOC) proporcionando una supervisión continua de las amenazas, garantizando el cumplimiento y permitiendo una respuesta proactiva ante incidentes. Obtenga ingestión automatizada de datos de amenazas desde el motor de protección multicapa de ESET, visibilidad centralizada y análisis avanzado de amenazas dentro de Microsoft Sentinel.

La conexión de ESET PROTECT y Microsoft Sentinel proporciona a tu empresa una completa solución de seguridad en la nube diseñada para proteger entornos híbridos. Esta integración aumenta significativamente la eficiencia de tus equipos de seguridad al reducir las tareas manuales, automatizar la transferencia de datos, correlacionar los datos de los endpoints con la seguridad en la nube y agilizar la gestión de incidentes.

PRINCIPALES BENFICIOS

MAYOR PRECISIÓN

Al fusionar la inteligencia sobre amenazas de ESET con el SIEM de Sentinel, puedes lograr una mayor precisión de detección y tiempos de respuesta a incidentes más rápidos.

UTILIZACIÓN OPTIMIZADA DE LOS DATOS

Las funciones de análisis, automatización y gestión de amenazas de Sentinel te ayudan a transformar los datos de ESET en información práctica, maximizando el valor de tus datos de seguridad.

INTELIGENCIA SUPERIOR MEDIANTE LA INTEGRACIÓN

La integración con marcos de seguridad basados en Azure te proporciona un sistema de defensa unificado, consolidando los datos de amenazas de endpoints con las capacidades avanzadas de Sentinel.

PRINCIPALES CARACTERÍSTICAS

ACTUALIZACIONES DE DATOS SOBRE AMENAZAS SIN ESFUERZO

Recupera automáticamente los últimos registros de detección de ESET PROTECT cada cinco minutos con la función Azure, garantizando que tus datos sobre amenazas estén siempre actualizados.

POTENTE ANÁLISIS DE DATOS

Utiliza tablas de registro personalizadas y consultas gráficas para analizar fácilmente los datos de ESET junto con otra información de seguridad, potenciando el poder analítico de tu equipo SOC.

INSTALACIÓN SENCILLA

Implementa el conector de datos sin esfuerzo con una plantilla ARM, haciendo que la configuración y la ingestión de datos sean muy sencillas.

Mejora y simplificación de la gestión de las amenazas a los endpoints

Simplifica la visibilidad de las amenazas a los endpoints con la plataforma ESET PROTECT y la integración de Microsoft Sentinel SIEM y SOAR. También obtendrás una eficiente correlación y gestión de amenazas entre plataformas. El conector de datos desarrollado por ESET aprovecha una API REST de integración y funciones Azure programadas para automatizar la recuperación de registros de detección. Esto significa que obtendrás información de seguridad continua, todo en una plataforma centralizada.

¿Cómo funciona en la práctica? Su analista SOC recibiría una alerta de ESET PROTECT dentro de Microsoft Sentinel, señalando una amenaza de alto riesgo. Con las guías automatizadas de Sentinel, el analista puede aislar rápidamente el endpoint afectado, investigar los eventos relacionados y mantener informadas a todas las partes interesadas. Es la seguridad hecha simple y efectiva.

Acerca de ESET

DEFENSA PROACTIVA. MINIMIZA LOS RIESGOS CON LA PREVENCIÓN.

Ve un paso por delante de las ciberamenazas conocidas y emergentes con nuestro enfoque basado en la IA y centrado en la prevención. Combinamos el poder de la IA y la experiencia humana para que la protección sea fácil y eficaz.

Experimenta la mejor protección de su clase gracias a nuestra información interna sobre ciberamenazas globales, compilada y examinada durante más de 30 años, que impulsa nuestra amplia red de I+D dirigida por investigadores reconocidos en la industria.

ESET PROTECT, nuestra plataforma de ciberseguridad XDR pionera en la nube, combina capacidades de prevención, detección y detección proactiva de amenazas de última generación con una amplia variedad de servicios de seguridad, incluida la detección y respuesta gestionadas. Nuestras soluciones altamente personalizables incluyen asistencia local y tienen un impacto mínimo en el rendimiento, identifican y neutralizan las amenazas conocidas y emergentes antes de que puedan ejecutarse, respaldan la continuidad de la actividad empresarial y reducen el coste de implementación y gestión.

ESET protege tu negocio para que puedas aprovechar todo el potencial de la tecnología.

Acerca de Microsoft Sentinel

Microsoft Sentinel es un sistema de información de seguridad y gestión de eventos (SIEM) escalable y adaptado a la nube que ofrece una solución inteligente y completa para SIEM y orquestación, automatización y respuesta de seguridad (SOAR). Microsoft Sentinel ofrece detección de ciberamenazas, investigación, respuesta y búsqueda proactiva con una visión panorámica de toda la empresa.

Microsoft Sentinel también incorpora de forma nativa servicios probados de Azure, como Log Analytics y Logic Apps, y enriquece tu investigación y detección con IA. Utiliza el flujo de inteligencia sobre amenazas de Microsoft y también te permite aportar tu propia inteligencia sobre amenazas.

*Fuente: ¿Qué es Microsoft Sentinel? – Aprende con Microsoft.