Plataforma ESET PROTECT e IBM QRadar SIEM

Aprovecha el poder de una seguridad mejorada

Digital Security
Progress. Protected.

RESUMEN DE LA SOLUCIÓN

Por un ecosistema holístico de ciberseguridad

La integración de la plataforma ESET PROTECT con IBM QRadar SIEM mejora tu seguridad digital al combinar la IA Native XDR de ESET con las potentes funciones de gestión de eventos e información de seguridad (SIEM) de QRadar.

Diseñada para apoyar a los analistas del Centro de Operaciones de Seguridad (SOC), esta integración simplifica la monitorización y agiliza la detección de amenazas y los flujos de trabajo de respuesta. Aborda los retos que plantea la monitorización de las actividades de los endpoints y la identificación de amenazas en múltiples perímetros.

Obtén visibilidad centralizada de las amenazas, una detección más rápida y una mejor respuesta ante incidentes, todo dentro de un sistema de panel de visión único. Al agregar los datos de ciberseguridad de ESET en IBM QRadar SIEM, **garantizamos una gestión integral de la seguridad, minimizamos las filtraciones de seguridad y damos soporte a una mejor conformidad.**

PRINCIPALES BENEFICIOS

SEGURIDAD REFORZADA

Combina la detección de amenazas basada en IA de ESET con las capacidades SIEM de QRadar para obtener un ecosistema de ciberseguridad holístico.

GESTIÓN CENTRALIZADA DE AMENAZAS

Accede a datos centralizados sobre amenazas dentro de QRadar para reducir los tiempos de respuesta y aprovechar tus potentes funciones de análisis.

RESPUESTA PROACTIVA A AMENAZAS

Permite la telemetría de amenazas entre plataformas y respalda las estrategias de respuesta a amenazas avanzadas.

PRINCIPALES CARACTERÍSTICAS

TRANSFERENCIA/VISIBILIDAD DE DATOS SOBRE AMENAZAS EN TIEMPO REAL

ESET transmite continuamente actualizaciones de eventos de seguridad directamente a QRadar SIEM, lo que garantiza una gestión eficaz y cómoda de las amenazas.

ACTUALIZACIONES PERIÓDICAS DEL MÓDULO DEL MOTOR DE REGLAS

Benefíciate de actualizaciones puntuales con información detallada sobre detecciones específicas, manteniendo tus defensas a punto.

ANÁLISIS EXHAUSTIVO DE EVENTOS

Las propiedades personalizadas de DSM permiten la extracción de puntos de datos específicos, como nombres de dispositivos, acciones de amenazas y actividad de usuarios. Están listas para agilizar tu flujo de trabajo sin esfuerzo añadido.

INVESTIGACIÓN DE INCIDENTES QRADAR MEJORADA

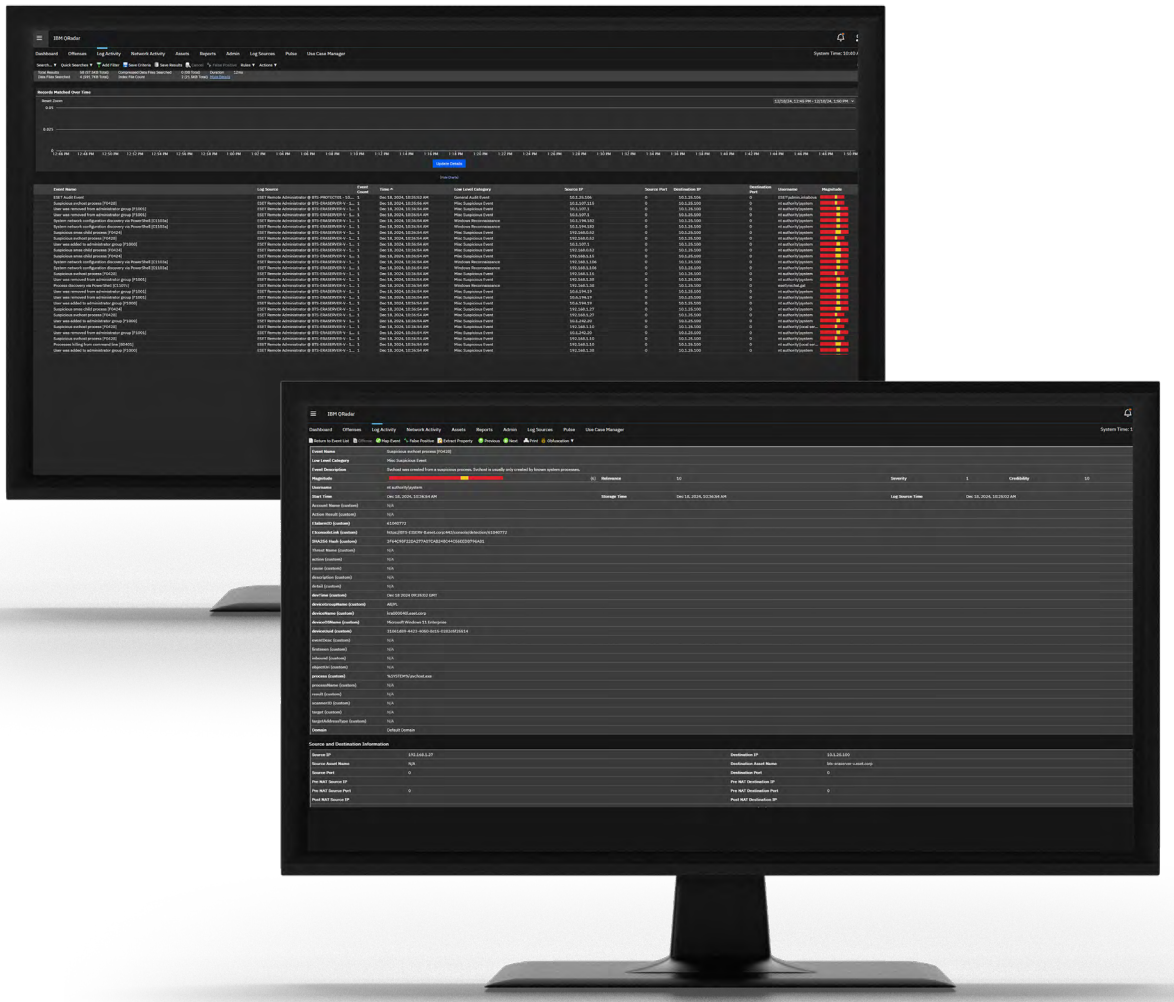
Aprovecha las capacidades de QRadar SIEM para investigar las alertas generadas por ESET y los datos de amenazas para una respuesta a incidentes más rápida y eficaz.

CÓMO FUNCIONA

La integración de la plataforma ESET PROTECT con IBM QRadar SIEM centraliza los datos de ciberseguridad alimentando a la perfección la telemetría de ESET en QRadar. Esto unifica varias perspectivas de seguridad para una gestión integral y una respuesta a amenazas más eficaz.

Al combinar la plataforma AI Native XDR de ESET con las capacidades SIEM de QRadar, la integración permite una visibilidad profunda, inteligencia procesable y una toma de decisiones más rápida, ayudando a las empresas a hacer frente a las amenazas en toda su empresa.

Por ejemplo, cuando un analista del SOC identifica un intento de inicio de sesión sospechoso marcado por ESET como de alto riesgo, la alerta -enriquecida en QRadar con datos contextuales- permite al analista investigar rápidamente y aislar el dispositivo afectado, evitando riesgos mayores. El resultado: operaciones agilizadas, vulnerabilidades reducidas y una postura de seguridad más sólida.



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 IBM QRadar

POTENCIACIÓN DE LOS SOC MODERNOS DE HOY EN DÍA CON IA DE NIVEL DE EMPRESA

A medida que aumenta el coste de una filtración de datos y los ciberataques se vuelven cada vez más sofisticados, el papel de los analistas del centro de operaciones de seguridad (SOC) es más crítico que nunca. IBM QRadar SIEM es más que una herramienta; es un compañero de equipo para los analistas del SOC, con IA avanzada, potente inteligencia de amenazas y acceso al contenido de detección más reciente.

IBM QRadar SIEM utiliza varias capas de IA y automatización para mejorar el enriquecimiento de alertas, la priorización de amenazas y la correlación de incidentes, presentando alertas relacionadas de forma cohesionada en un panel unificado, reduciendo el ruido y ahorrando tiempo. QRadar SIEM ayuda a maximizar la productividad de su equipo de seguridad proporcionando una experiencia unificada en todas las herramientas SOC, con funciones integradas y avanzadas de IA y automatización.

*Fuente: [Página oficial de IBM] https://www.ibm.com/products/qradar-siem

Digital Security
Progress. Protected.

RESUMEN DE LA SOLUCIÓN