XDR de Seqrite

SEQRITE

www.seqrite.com

Aporte una ciberprotección holística a su empresa utilizando la búsqueda y corrección automatizada de amenazas del XDR de Seqrite para identificar, rastrear y eliminar las amenazas sigilosas en todas las fuentes de datos.

Las ciberamenazas son cada vez más inteligentes. ¿Está su empresa preparada para defenderla de ellas?

En los últimos años se ha producido una enorme afluencia de ciberataques avanzados que han afectado a casi el 47 % y el 27 % de las organizaciones (pequeñas, medianas y grandes) de Estados Unidos y la India. La tendencia no muestra signos de ralentización, ya que las infracciones de gran repercusión aparecen regularmente en los titulares de todo el mundo.

Según un estudio realizado por los científicos de datos de Seqrite, los ataques se clasifican principalmente en dos secciones:

1. Malware evasivo y ataques de día cero
2. Ataques sin archivos y ataques dirigidos

Los dos últimos son los más difíciles de detectar y los más destructivos, ya que requieren análisis y correlación históricos, junto con técnicas de aprendizaje automático para ser identificados. Los equipos de ciberseguridad son conscientes de la existencia de este tipo de ataques dirigidos, pero no disponían de una herramienta sencilla pero potente que pudiera prevenirlos proporcionando visibilidad a través de todas las fuentes de datos.

La protección básica de puntos finales es insuficiente para detectar el malware más escurridizo y los ataques dirigidos. Para combatirlos se necesitan mecanismos avanzados de detección y respuesta, reforzados con detección de anomalías de comportamiento y búsqueda de eventos históricos. Además, se necesitan mecanismos avanzados de automatización, ya que el volumen de alertas generadas puede abrumar al equipo SOC.

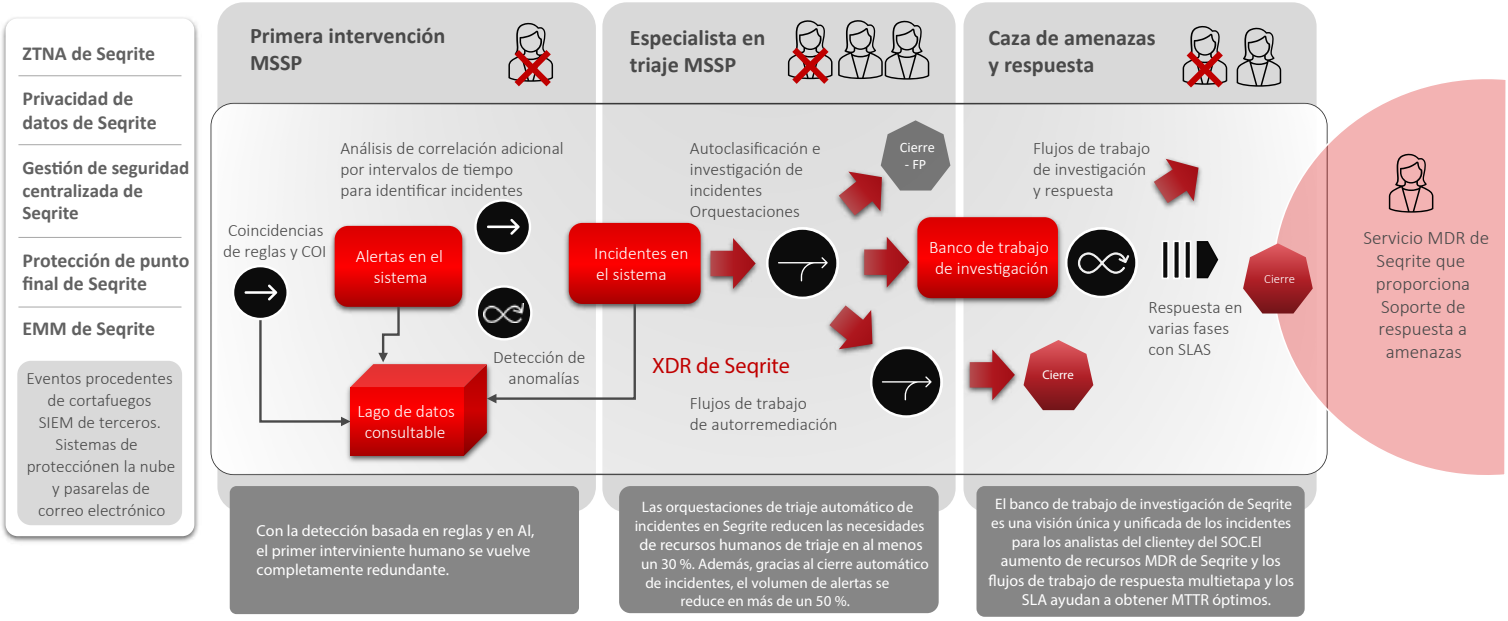
La solución: XDR de Seqrite

Una plataforma de detección y respuesta ampliada que permite un SOC seguro e híbrido a un precio relativamente bajo.

El XDR de Seqrite es una herramienta avanzada de respuesta a incidentes que incorpora datos de múltiples productos de seguridad en un sistema unificado de operaciones de seguridad para ofrecer una protección holística contra los ciberataques. Mediante el uso de análisis y automatización, el XDR de Seqrite centraliza, normaliza y correlaciona datos de diversas fuentes, lo que permite una protección en tiempo real de puntos de control cruzados, a la vez que simplifica y refuerza los procesos de seguridad.

El XDR de Seqrite bloquea las ciberamenazas detectando los procesos de cifrado maliciosos y los cierra antes de que perturben cualquier red.

Cómo nuestra plataforma unificada permite al MSSP llevar a cabo la detección y respuesta gestionadas con una reducción de recursos del 50 %.



Lo más destacado del producto

Conveniente: Una plataforma única e integral para la detección y respuesta ante amenazas avanzadas.

Preciso : Lanza menos falsos positivos debido a la lógica específica de la fuente.

De nueva generación: Viene con propiedades mejoradas como la automatización SOAR para Triaje y Respuesta, banco de trabajo de caza de amenazas, búsqueda y eliminación de IOC, y muchas más.

Protección multinivel: ML/AI para una vigilancia 24 horas al día, 7 días a la semana. Detección de anomalías del comportamiento para protección adicional contra amenazas desconocidas. Correlación automatizada de incidentes y enriquecimiento para la asignación de gravedad.

Gestión de respuestas: Garantiza tiempos de respuesta óptimos mediante Gestión de incidentes, gestión de SLA y cuadros de mando SOC detallados.

Automatización basada en playbooks : Garantiza una utilización optimizada de los recursos mediante la automatización.

Inteligencia sobre amenazas compartida: Permite al cliente utilizar la inteligencia global sobre amenazas y la inteligencia generada por la investigación interna de Seqrite para hacer frente a las amenazas de día cero y las amenazas persistentes avanzadas.

Búsqueda de datos históricos: Permite buscar en el COI los acontecimientos que pueden haberse omitido anteriormente.

Soporte: Equipo MDR de Seqrite disponible para asistencia de respuesta y aumento de recursos del SOC.

Lo más destacado del producto

Análisis de comportamiento en tiempo real: Supervisa continuamente la actividad de los usuarios para detectar inicios de sesión inusuales, como viajes imposibles o ubicaciones inesperadas, para la identificación instantánea de amenazas.

Detección de anomalías mediante IA: Aprovecha el aprendizaje automático para identificar actividades anómalas como inicios de sesión desde dispositivos no conformes o intentos de autenticación de un solo factor.

Alertas de amenazas internas: Proporciona notificaciones en tiempo real sobre posibles compromisos de cuentas causados por comportamientos de riesgo o inusuales de los usuarios.

Información de datos integrada: Correlaciona las anomalías de los usuarios con los datos de los puntos finales y la red para acelerar la respuesta ante incidentes y reducir el tiempo de inactividad.

Reducción de la fatiga por alertas: Se centra en las actividades de alto riesgo, minimizando los falsos positivos para agilizar las operaciones de seguridad.

¿Por qué elegir el XDR de Seqrite?

01 **Vigilancia activa** : Énfasis en el aprendizaje automático, detección de anomalías de comportamiento, búsqueda automatizada de IOC/IOA, flujos de trabajo de corrección activados automáticamente para una vigilancia activa 24/7 superior para la organización.

02 **Años de experiencia en ciberseguridad** : Líder en el ámbito de la protección de puntos finales durante más de 20 años, ha protegido más de cuatro millones de puntos finales y cuenta con un laboratorio de investigación interno que proporciona IOC y reglas actualizadas para los actores de amenazas activos a nivel local y regional.

03 **Orientación a los procesos** : Para hacer frente a las amenazas en toda la empresa, los vectores de ataque y las fuentes requieren una orientación decidida en los procesos. El XDR de Seqrite proporciona capacidades completas de gestión de incidentes y definición de SLA para la orientación de procedimientos del SOC.

04 **Precio asequible** : Seqrite ha desarrollado algoritmos de almacenamiento altamente optimizados que permiten almacenar eventos y alertas de hasta 180 días por una fracción del coste de las ofertas de la competencia en el mercado.

05 **Análisis avanzado del comportamiento del usuario (UBA)** : Aprovecha el aprendizaje automático y el modelado del comportamiento para detectar amenazas sofisticadas, como credenciales comprometidas y ataques internos, que las herramientas tradicionales suelen pasar por alto.

06 **Visibilidad de la Seguridad mejorada**: Combina datos de punto final, redes y usuarios para proporcionar información exhaustiva, lo que le permite responder a ataques complejos con precisión.n.

07 **Adelántese a las amenazas sofisticadas**: Detecte, analice y neutralice los riesgos avanzados que las herramientas convencionales pasan por alto con funciones UBA de vanguardia.

Automatización y ML para la búsqueda 24/7 de APTs

Búsqueda de datos históricos de hasta 180 días para detectar COIs pasados por alto

Gestión de incidentes y SLA con una reducción de recursos del 50 %

Acerca de Seqrite

Seqrite es un proveedor líder de soluciones de ciberseguridad empresarial. Con un enfoque en la simplificación de la ciberseguridad, Seqrite ofrece soluciones y servicios integrales a través de nuestra pila tecnológica patentada, impulsada por IA/ML para proteger a las empresas contra las últimas amenazas mediante la protección de dispositivos, aplicaciones, redes, nube, datos e identidad. Seqrite es el brazo empresarial de la marca mundial de ciberseguridad Quick Heal Technologies Limited, la única empresa de productos y soluciones de ciberseguridad que cotiza en bolsa en la India.

En la actualidad, más de 30 000 empresas de más de 76 países confían sus necesidades de ciberseguridad a Seqrite.

SEQRITE | Quick Heal Technologies Limited
Teléfono: 1800-212-7377 | info@seqrite.com | www.seqrite.com | /seqrite