Seqrite **EDR en las instalaciones**

En la era de la inestabilidad geopolítica y la recesión económica, los establecimientos gubernamentales y las empresas han sido objetivos constantes de amenazas avanzadas. Las soluciones tradicionales de seguridad para puntos finales suelen ser ineficaces a la hora de detectar o prevenir estos ataques, ya que no consiguen obtener los datos necesarios para sacar a la luz comportamientos inusuales y responder eficazmente a las ciberamenazas furtivas.

Seqrite EDR es una sólida solución de detección y respuesta que resuelve este problema proporcionando a los clientes una visibilidad ininterrumpida de los datos y un mayor control sobre el hardware, el sistema operativo y las aplicaciones de su sistema. Permite a los clientes investigar alertas y eventos pasados, consultar el sistema para obtener la información más reciente y llevar a cabo respuestas y soluciones manuales o automatizadas en tiempo real.

Características de Seqrite EDR:

Verificación multifase

Analiza todos los eventos del sistema a través de múltiples capas de análisis de comportamiento, comparaciones de firmas y detección basada en ML.

Soporte para redes fuera de línea y con bloqueo aéreo

Seqrite EDR tiene el soporte más avanzado para redes con bloqueo aéreo. Puede actualizar las reglas de comportamiento y los IOC, y dispone de funciones de respuesta autónoma basada en políticas fuera de línea para este tipo de entornos.

Búsqueda automatizada y manual de IOC

Realiza búsquedas automatizadas y manuales de IOC en datos históricos, obteniendo IOC de los últimos datos de inteligencia sobre amenazas del equipo de inteligencia sobre amenazas de Seqrite y de agencias gubernamentales como CERT-IN.

Sistema de notificación avanzado

Se integra perfectamente con todas las soluciones SIEM y envía alertas por SMS o correo electrónico.

Panel de control y widgets

Presenta una visión general completa del estado del sistema, incluidos los principales incidentes, el resumen general, los incidentes afectados y los índices de falsos positivos a través de widgets intuitivos.

Informes

Los informes detallan el resumen de alertas a lo largo del tiempo, proporcionando información alineada con los TTP de MITRE.

Creador de reglas y normas

Permite elaborar reglas del sistema y personalizadas. Aprovecha el creador de reglas para elaborar reglas personalizadas con el fin de capturar actividades relacionadas con MITRE u otras actividades inusuales o interesantes en los terminales.

Orquestación de políticas de acción y respuesta basada en riesgos

Implementa políticas de acción de respuesta en tiempo real y fuera de línea, con ámbitos definidos para la respuesta automática basada en riesgos utilizando políticas genéricas o personalizadas.

Banco de trabajo de investigación

Ayuda a investigar incidentes y alertas con desgloses detallados, información contextual, acceso basado en consultas a información del sistema en tiempo real y una lista exhaustiva de alertas con acceso a la lista de alertas y al árbol de alertas, lo que permite realizar acciones de alerta centralizadas desde una ubicación.

Gestión de incidentes

Permite la gestión de incidentes a través de la lista de incidentes y la información sobre endpoints y usuarios, al tiempo que formula acciones de reparación.

SEQRITE

Ventajas del Seqrite EDR

Disuada los ataques avanzados

Nuestro sistema de detección de punto final analiza cada evento de telemetría generado en los sensores a través de múltiples etapas de análisis para realizar un análisis contextual exhaustivo. Si se detecta actividad sospechosa, nuestro sistema EDR puede bloquearla inmediatamente.

Detenga el malware antes de que ataque

Al tomar medidas automatizadas en tiempo real, como aislar el sistema o detener la ejecución, disminuyen considerablemente las posibilidades de que un adversario ejecute un ataque con éxito.

Benefíciese de investigaciones exhaustivas

Al recopilar información de gran utilidad sobre ejecuciones, scripts, comandos y cadenas de procesos, se reduce significativamente el tiempo de triaje y respuesta de los analistas de seguridad. Esta función amplía la capacidad de satisfacer las necesidades y normas de cumplimiento.

Reduzca la necesidad de contratar empresas externas de respuesta a incidentes y análisis forense

Nuestro módulo Detección y respuesta de punto final permite a los analistas de seguridad y a los equipos de administración de TI llevar a cabo investigaciones detalladas de los ataques de forma independiente, lo que reduce la necesidad de contratar a agencias externas para realizar dichas investigaciones.

Busque amenazas ocultas en el historial

Los ataques avanzados utilizan tecnología de ocultación para permanecer ocultos en el entorno durante muchos meses. Utilizando nuestro almacenamiento de datos de eventos y Caza de amenazas, combinado con la Inteligencia de Amenazas más reciente, se pueden descubrir dichas amenazas ocultas y tomar medidas de respuesta inmediatas.

Requisitos del sistema (solo para la versión local)

Windows (64-bit) (Windows 8.1, 10, 11, 2012, 2016, 2019, 2022).

MacOS - Procesador: Intel core o chip Apple M1, M2, M3 compatible
- macOS 10.14, 10.15, 12 y 14

Linux (64-bit) - Fedora 32, Linux Mint 20, Ubuntu 17.04, 20.04, 22.10, CentOS 8, 8.2, RHEL 8.1, 8.2, 9.1, openSUSE 15.1, Rocky Linux, Boss 8

Requisitos mínimos del sistema para el servidor (solo versión local) - Hasta 1000 puntos finales.

Requiere 3 servidores – 1) Máquina del trabajador: 40 núcleos, 96 GB de memoria, 3,7 TB de disco - SO Ubuntu 22.04 LTS
2) Máquina principal: 4 núcleos, 8 GB de memoria, 500 GB de disco - SO Ubuntu 22.04 LTS
3) Gestor de actualizaciones - 2 núcleos, 4 GB de memoria, 50 GB de disco (para el sistema operativo, haga clic aquí)

Refuerce su Protección de punto final con la capacidad de detectar y bloquear malware complejo y de respaldar investigaciones y análisis de puntos finales mediante EDR real.

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