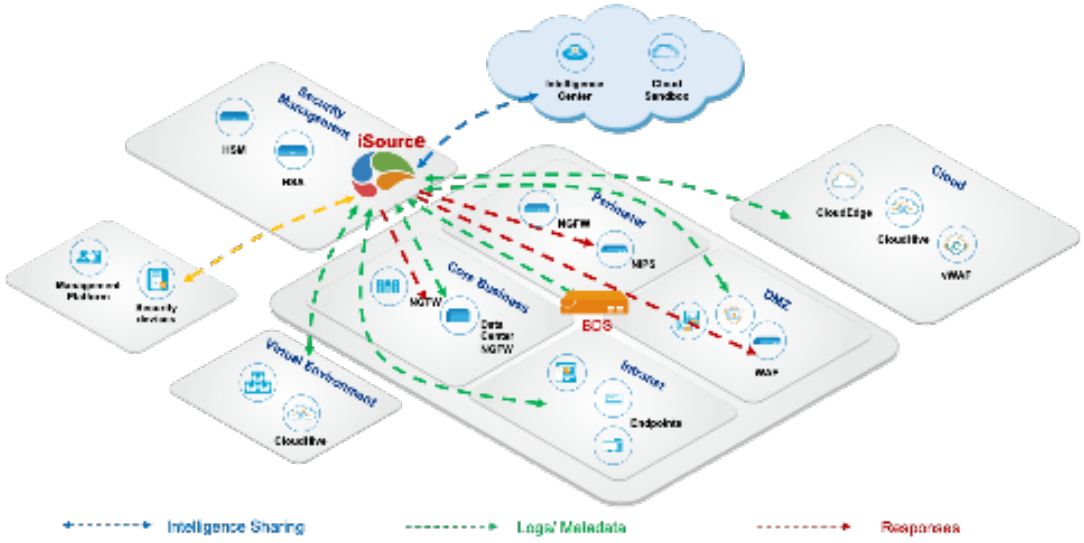
Hillstone iSource

Solución de Detección y Respuesta Extendidas (XDR)

Hillstone iSource es una plataforma de respuesta y detección extendida (XDR) impulsada por inteligencia artificial que integra datos de seguridad masivos, investiga correlaciones de incidentes, identifica amenazas potenciales, automatiza la orquestación de la seguridad y responde de manera coherente a través de múltiples productos y plataformas de seguridad. Aporta un enfoque radicalmente nuevo a la ciberseguridad con visibilidad completa, con identificación de amenazas de alta precisión así como contención y mitigación rápidas para una eficiencia en seguridad operativa inigualable.



Detalles del Producto

Recopilación de datos unificada de múltiples productos de seguridad con visibilidad completa

Hillstone iSource recopila varios tipos de datos, como registros de amenazas e informes de incidentes, de casi cualquier fuente en la pila de productos de Hillstone y también de productos de terceros. Al estandarizar e integrar datos heterogéneos en todos los componentes, incluida la nube, la red y los puntos finales, iSource rompe los silos de información de seguridad. No solo brinda visibilidad de seguridad completa con muchos menos puntos ciegos, sino que también mejora la precisión de detección y brinda una defensa efectiva y eficiente contra las amenazas.

Análisis y detección avanzados basados en ML

Al sinergizar los datos y registros recopilados en todo el tejido de seguridad, así como la inteligencia de amenazas de las principales fuentes de inteligencia de amenazas, Hillstone iSource puede descubrir incluso amenazas furtivas y evasivas, y atribuir los ataques. Desarrollado por tecnología de aprendizaje automático y algoritmos estadísticos, su motor de análisis de comportamiento ayuda a distinguir actividades anómalas entre una gran cantidad de datos integrados. Su motor de análisis de correlación consolida los incidentes individuales para el conocimiento del contexto y aplica el análisis a los datos correlacionados para identificar incidentes

de alta fidelidad, proporcionando una imagen completa de una cadena de ataque y ayudando en la investigación del propósito del ataque. Su potente análisis de registros ha incorporado una capacidad de análisis de correlación y detección basada en el estado y el umbral, que permite a los analistas de seguridad definir reglas personalizables para identificar amenazas claves a través de artefactos. El motor de búsqueda de registros basado en Search Processing Language (SPL) también alivia el dolor de buscar y analizar registros masivos.

Gestión integral de vulnerabilidades y riesgos

La gestión de vulnerabilidades de Hillstone ayuda a identificar y presentar vulnerabilidades aprovechando la solución de evaluación de vulnerabilidades líder en la industria. También admite la adición de nuevos escáneres para la personalización o incluso la importación manual de un archivo de informe de vulnerabilidad para una mayor contención de las amenazas.

Los activos son el núcleo de la gestión de riesgos. Hillstone iSource proporciona una gestión integral de riesgos para activos como servidores, puntos finales o incluso aplicaciones y servicios, desde múltiples dimensiones, incluidos riesgos, vulnerabilidades y eventos de amenazas. Presenta datos estadísticos, como distribución y tendencias de amenazas y vulnerabilidades, junto con información detallada de activos individuales. Este enfoque holístico protege los activos al identificar y mitigar las posibles exposiciones a amenazas.

Orquestación de seguridad automatizada y respuesta cohesiva

Hillstone iSource ofrece capacidad de respuesta y orquestación de seguridad automatizada con guías integradas, interacciones integradas con los productos de seguridad de Hillstone y la capacidad de asignar tareas para la gestión colaborativa de casos. Además de los playbooks predefinidos que ofrecen flujos de trabajo y respuestas optimizados, Hillstone iSource también ofrece la agilidad y flexibilidad para definir los flujos de trabajo automatizados visualmente en los playbooks basados en incidentes o alertas ingeridos, consultas de inteligencia y acciones de respuesta. Estas respuestas, combinan tareas automatizadas que pueden abarcar varios dispositivos Hillstone, como NGFW, NIPS, CloudEdge, CloudHive, etc., con tareas manuales manejadas respectivamente a través de la gestión de casos de incidentes. Ciertos dispositivos de terceros también se pueden admitir en los playbooks a través de APIs RESTful o conexión SSH. Esto permite una rápida clasificación de incidentes y contención de ataques antes de que se puedan producir daños.

Gestión e informes unificados con una consola intuitiva y personalizable

El panel personalizable permite un acceso simple y rápido a la postura de seguridad de la organización con información estadística completa, como clasificaciones y contadores, así como un resumen de incidentes y tendencias de seguridad con gráficos y listas. El diseño intuitivo proporciona una experiencia de usuario optimizada para la gestión y las operaciones. Hillstone iSource también admite informes personalizados o basados en plantillas que se pueden generar según lo programado o bajo demanda. Las API públicas permiten la integración con herramientas o productos de seguridad de terceros para inyectar datos de seguridad generados en todo el tejido de seguridad y realizar interacciones para contener amenazas.

Funcionalidades

Recopilación de datos

- La solución admite recopilación de datos incluyendo netflow, metadatos, Syslog, Sysmon, Linux Syslog de los dispositivos de seguridad de Hillstone
- Soporte de recopilación de datos de mensaje RADIUS
- La solución admite la integración de dispositivos de terceros para la recopilación de datos

Visibilidad completa

- Soporta la detección de amenazas
- La solución admite el monitoreo de eventos de amenazas y la visualización de activos de riesgo y tendencias de riesgo
- La solución admite la visualización distribuida de conexiones geográficas de amenazas
- La solución admite la visualización en pantalla completa de información estadística y detallada de la seguridad general, seguridad de los servidores, seguridad de los puntos finales, información de vulnerabilidades, seguridad de las áreas, eventos de amenazas y gestión jerárquica
- Soporta el establecimiento de la topología para el conocimiento del flujo de la red recopilando y analizando el tráfico
- Resumen de eventos de amenazas clave
- Admite la lista de eventos de amenazas de BDS individuales

Funcionalidades

Reglas de detección
- Admite la configuración de reglas de detección de amenazas para escaneos, en archivos, detección de HTTP, protocolos sospechosos, fuerza bruta, DNS, blackmail, minería, comportamiento de USB, acceso no autorizado, contraseñas débiles y amenazas definidas por el usuario

Análisis de Amenazas
- Detección de amenazas basada en reglas
- Análisis de registro de amenazas
- Análisis de comportamiento
- Análisis de correlación
- Estadísticas y análisis de servidores en riesgo, terminales en riesgo y eventos de amenazas
- Admite la recopilación de evidencia, el procesamiento y el marcado del estado de los eventos de amenazas
- La información de evidencia de amenazas admite múltiples tipos de decodificación, como URL, Base64, Unicode, UTF-8, HEX, etc.
- Soporte de mapeo de la matriz MITRE ATT & CK
- Admite la agregación de amenazas y la reconstrucción de la cadena de ataque

Gestión de activos
- Admite la gestión de activos de servidor, activos de terminales y activos no clasificados
- La solución admite mostrar un resumen de activos
- Admite la gestión de activos favoritos
- Admite clasificación de activos
- Admite extracción de huellas de activos (fingerprint)
- Admite la gestión de agrupaciones de servidores, terminales y diferentes tipos de negocios en servidores
- Soporte de descubrimiento automático de activos, incluido el escaneo dinámico y la importación manual de activos
- Admite la gestión del inventario de activos
- Compatibilidad con la configuración de prioridad de origen de activos
- Soporta la visualización del estado de usuarios
- Admite la gestión centralizada de los activos que se importarán y los activos que se actualizarán
- Admite la extracción de huellas de activos de los informes de vulnerabilidad (fingerprint)

Administración de vulnerabilidades
- Admite información estadística y detallada de vulnerabilidades
- Admite la importación de informes de vulnerabilidad de terceros
- Admite el escaneo de vulnerabilidades con escáneres integrados y de terceros
- Admite la gestión de tareas de escaneo

Manejo de la Información
- Notificación de información sobre amenazas de hotspot CVE
- Base de datos de inteligencia de soporte de dominios DNS, códigos maliciosos, IP, vulnerabilidades, detecciones de intrusos, geolocalización, URL y base de conocimiento MITRE & ATT & CK®
- Admite detección de intrusos y una base de datos de firmas de detección de ataques web
- Admite una base de datos del modelamiento de comportamiento anormal y de comportamiento de malware, así como una base de conocimientos relacionada con honeypot
- Inteligencia integral con otras amenazas relevantes
- Admite la actualización en línea y fuera de línea de la base de datos de inteligencia de forma manual y periódica
- Admite la lista blanca de archivos, DNS y globales
- Admite listas negras de DNS, códigos maliciosos e IP

Análisis de correlación
- Soporte de análisis de correlación de datos masivos y detección de cadena de muerte
- Soporte de búsqueda centralizada y clasificada de eventos de amenazas globales
- Admite la búsqueda por palabras clave, SPL y condiciones predefinidas
- Admite actualizaciones en línea/fuera de línea de la regla de análisis de Syslog y de la base de datos de reglas de análisis de correlación de amenazas

Respuesta ante incidentes
- La solución admite sistema de gestión de casos
- Actualización y revisión del estado del caso
- Dispositivos / servicios interactivos (dispositivos de seguridad / servicio de inteligencia de amenazas)
- Admite la integración de dispositivos de terceros a través de API RESTful o SSH
- Orquestación y respuesta automática o semiautomática (con doble confirmación) basada en playbooks, con soporte de playbooks predefinidos y configuración del período de validez
- Admite notificación por correo electrónico a los administradores para la confirmación secundaria de la implementación de la política de firewall
- Admite agregación de políticas
- Admite el marcado del estado del evento dentro del playbook
- Admite la reemisión manual de respuestas automatizadas fallidas impulsadas por el playbook
- Admite una gestión ágil de incidentes para contraseñas débiles, ransomware, ataques de minería, activos favoritos y amenazas

Alertas
- Admite alarmas basadas en umbrales y reglas de pulso de tráfico
- Visualización en tiempo real de eventos de amenazas
- Admite notificación de alerta por SMS, correo electrónico y WebUI

Generación de informes
- Admite cuatro plantillas de informes que incluyen el riesgo de seguridad general, el riesgo de seguridad de los endpoints, el riesgo de seguridad del servidor y el informe de respuesta a incidentes
- Admite la función opcional de generar tareas de informes
- Soporte de informes periódicos o bajo demanda
- Soporte de vista previa de informes en línea
- Admite exportación de reportes en formatos PDF / WORD
- Admite logotipo personalizado
- Soporte de notificación por correo electrónico de la generación de informes
- Admite gestión de protección clasificada

Configuración del sistema
- Admite la gestión de la autoridad del usuario, Syslog, Netflow, almacenamiento de registros, información de evidencias, configuración de red, configuración de correo y configuración de licencias
- Admite la asignación de roles de usuario con privilegios de acceso (administrador, operador y auditor)
- Admite configuración de host confiable
- Soporte de integración con HSM
- Récord de registros del sistema
- Sincronización con reglas BDS
- Admite HA y agrupación en clústeres de hasta 5 nodos
- Soporta gestión jerárquica
- Admite customización de logo del sistema y título

Plataformas compatibles
- Linux: CentOS 7
- Windows: Microsoft Windows 10
- VMware: VMware EXSi 6.7

Especificaciones

Models		SG-6000-ISC6305	SG-6000-ISC6310	SG-6000-ISC6320
Performance	Throughput	3Gbps	6Gbps	15Gbps
	Event Processing	5000EPS	8000EPS	15000EPS

Version: EX-08.01-iSource-2.0R10-0923-SP-01