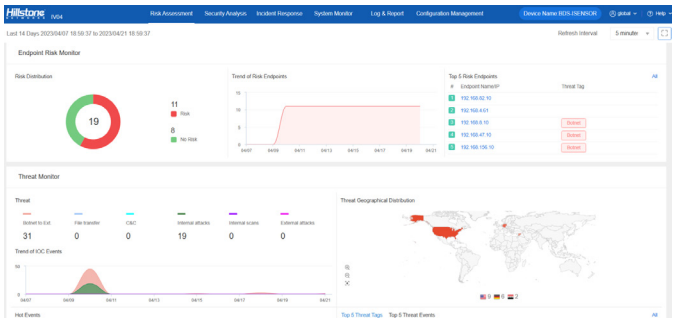
Hillstone Serie-I

Sistema de Detección de Brechas (BDS)

El producto de detección y respuesta (NDR) de Hillstone Networks, Sistema de detección de brechas (BDS) adopta múltiples tecnologías de detección de amenazas que incluyen tecnología tradicional basada en firmas o basada en reglas y modelado de datos para inteligencia de amenazas a gran escala, así como análisis de comportamiento del usuario basado en aprendizaje automático. El sistema proporciona una solución ideal para detectar amenazas avanzadas, incluido el ransomware y el malware de criptominería, y proteger los servidores críticos de alto valor y los datos confidenciales de ser filtrados o robados. Junto con las capacidades analíticas y la visibilidad de la búsqueda profunda de amenazas, Hillstone BDS proporciona a los administradores de seguridad los medios efectivos para detectar eventos del tipo IOC (indicadores de compromiso), localizar hosts y servidores riesgosos y restaurar la cadena de ataque. Además, lleva a cabo la mitigación de amenazas y ataques con la conjunción de NGFW, así como con la integración del sistema Hillstone XDR iSource. El producto BDS de Hillstone ofrece una solución efectiva e integral para detectar y responder a diferentes tipos de ataques y amenazas de red en los activos de una empresa.

Detalles del Producto

Análisis Integral de Correlación de Amenazas para su Detección Avanzada



Los atacantes cibernéticos se han vuelto cada vez más sofisticados, utilizando, ataques persistentes, sigilosos y por fases de objetivos múltiples, que fácilmente pueden evadir la detección perimetral.

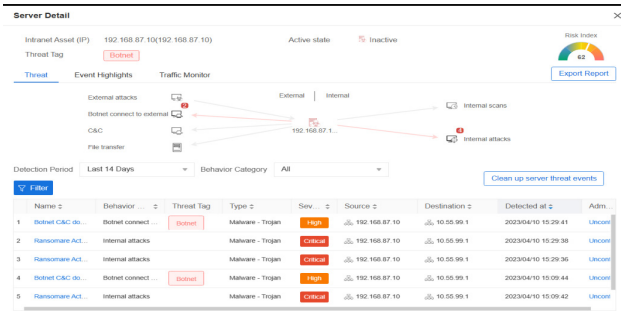
Hillstone BDS cuenta con una amplia variedad de capacidades de detección, que incluyen Detección Avanzada de Amenazas (ATD), Detección de Comportamientos Anómalos (ABD), detección de amenazas mediante engaños, detección de intrusiones y ataques, detección de virus y spam, y detección de centros de control de botnets. Hillstone BDS consiste en múltiples motores de detección enfocados en diferentes aspectos de la detección de amenazas posteriores a la violación, incluida la detección avanzada de malware (ATD), la detección de comportamiento anormal (ABD), así como los motores tradicionales de detección de intrusiones y detección de virus. La plataforma de correlación de amenazas de Hillstone analiza los detalles de las relaciones de cada evento de amenaza sospechoso individual, así como otra información contextual dentro de la red, para conectar los puntos y proporcionar detección precisa y efectiva de malware y de ataques, con altos niveles de confianza.

Monitoreo de Amenazas en Tiempo Real para Hosts y Servidores Críticos

La plataforma BDS de Hillstone se centra en la protección de servidores críticos dentro de la intranet, la detección de ataques de amenazas desconocidos y cercanos a 0-días y la búsqueda de actividades anómalas de nivel de red y de aplicación de servidores y máquinas host. Una vez que se detecta una amenaza o un comportamiento anormal, Hillstone BDS realizará su análisis de amenazas o de comportamiento y utilizará presentaciones gráficas basadas en topología para proporcionar una amplia visibilidad de los detalles de la amenaza y las anomalías de comportamiento. Esto les brinda a los administradores de seguridad información sin precedentes sobre el progreso del ataque, el tráfico en cada dirección, así como toda la evaluación de riesgos de la red.

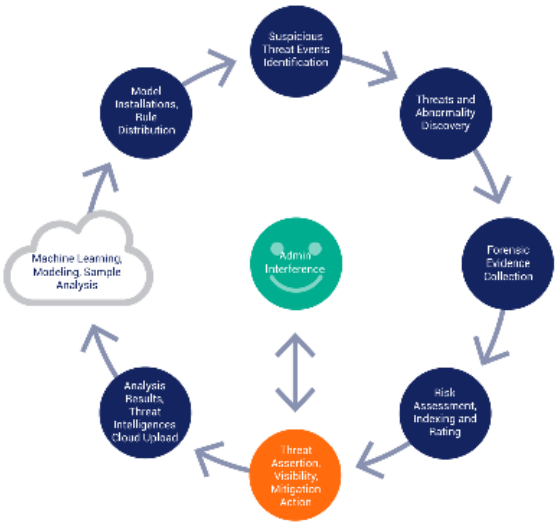
Indicador completo de compromisos y cadena de ataques cibernéticos

Los eventos de IOC son eventos de amenazas detectados durante el ataque posterior a la transgresión. Se identifican entre un gran número de ataques de amenazas en la red que están directamente asociados con el servidor o servidor protegido. Los IOC generalmente se consideran actividades de amenaza con mayor riesgo y con un alto nivel de confianza de que un servidor o host se ve comprometido y eso representa una amenaza potencialmente mayor para los activos críticos dentro de la red corporativa. Para limitar el



robo de datos importantes de activos críticos y evitar que un ataque de amenazas se propague aún más dentro de la red es fundamental detectar de manera efectiva los IOC y realizar una detección profunda de amenazas en estos IOC. Hillstone BDS profundiza y presenta más análisis de amenazas e inteligencia sobre estos eventos de IOC, reconstruye la cadena de ataques basada en estos IOC y correlaciona otros eventos de amenazas asociados con estos IOC dentro de los espectros de tiempo y espacio..

Abundante Información Forense y Mitigación Preventiva



La plataforma BDS de Hillstone realiza la mitigación de amenazas consecutivas con dispositivos Hillstone NGFW de la serie A, NGFW de la serie E y NGFW para centro de datos de la serie X, que se ubican en el perímetro de la red. Después de que el administrador de seguridad o los operadores de red analicen y validen las alertas de amenazas, pueden agregar elementos de amenaza como direcciones IP, tipo de amenazas, etc., a la lista negra o políticas de seguridad y luego sincronizarlos con los firewalls de Hillstone para que futuros ataques del las mismas razas o familias de malware se pueden bloquear en el perímetro de la red. Esto evita que ataques futuros se propaguen a territorios de red más amplios.

Características

Detección de Comportamiento Anormal

- Modelado de comportamiento basado en L3-L7 tráfico de la línea de base para revelar comportamientos anómalos en la red, tales como análisis HTTP, arañas, spam
- La detección de ataques DDoS incluyendo por inundación, Sockstress, zip de la muerte, reflexión, consultas DNS, SSL y aplicaciones DDoS
- Apoya la inspección del tráfico de un túnel encriptado para aplicaciones desconocidas
- En tiempo real, en línea, comportamiento anormal de la actualización de la base de datos modelo
- Soporta la detección de ataques de fuerza bruta RDP/VNC/SMB/SSH/FTP, TOR basado en peticiones HTTP sospechosas
- Soporte para detectar y alertar sobre software de acceso remoto

Detección Avanzada de Amenazas

- Detección avanzada de malware basada en el comportamiento
- Detección de más de 2,000 familias de programas maliciosos conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.
- En tiempo real, en línea, comportamiento del malware, actualización de base de datos modelo
- Soporte para la detección de amenazas en el tráfico cifrado sin descifrarlo

Análisis de Correlación de Amenazas

- Correlación entre las amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales
- Reglas de correlación multidimensional, actualización diaria automática en la nube

Detección de Amenazas Engañosas

- Motor de engaño local con actualización regular de modelos de engaño
- Simula servidores Web, Doc o Database, protocolos de soporte que incluyen FTP, HTTP, MYSQL, SSH y TELNET

Detección de Intrusiones

- Más de 35.000 firmas, detección de anomalías de protocolo y detección basada en la tasa
- Firmas personalizadas, actualización de firmas push or pull automático o manual, enciclo-pedia integrada de amenazas
- Más de 20 tipos de protocolos de detección de anomalías, incluyendo HTTP, SMTP, IMAP, POP3, VoIP, NetBIOS, VxLAN, MPLS, etc.
- Soporte para desbordamiento de búfer, inyección SQL y detección de ataques por scripting de cross-site
- Admite detección de contraseña débil para protocolos FTP / HTTP / SMTP / POP3 / IMAP / TELNET
- Soporte para la detección de shells inversos
- Soporte para capturar paquetes completos de ataques
- Soporte para la detección de contraseñas en texto claro en el tráfico HTTP

Escaneo de Virus

- Base de firmas de más de 15 millones de virus
- Actualizaciones en tiempo real en línea
- Soporte para configurar listas blancas de MD5 y URL

Anti-Spam

- Clasificación y prevención de spam en tiempo real
- Spam confirmado, spam sospechoso, spam masivo, volumen válido
- Protección independientemente del idioma, formato o contenido del mensaje.
- Admite protocolos de correo electrónico SMTP y POP3
- Listas blancas para permitir correos electrónicos de dominios / direcciones de correo electrónico confiables

Cloud-Sandbox

- Cargue archivos maliciosos en la nube para su análisis
- Protocolos de soporte que incluyen HTTP, SMTP, POP3, IMAP4 y FTP
- Tipos de archivos de soporte, incluidos PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP
- Proporcionar un informe completo de análisis de comportamiento para archivos maliciosos
- Intercambio global de inteligencia sobre amenazas, bloqueo de amenazas en tiempo real
- Múltiples motores de detección estática filtran rápidamente archivos normales y amenazas conocidas
- Visualización de amenazas desconocidas basada en registros, informes, información de monitoreo, informes de comportamiento de archivos

Detección de Botnet C&C

- Descubre los hosts de botnet en la intranet mediante la supervisión de conexiones C&C
- Detecta direcciones IP y nombres de dominio de C&C en el tráfico TCP, HTTP y DNS
- Actualiza automáticamente la biblioteca de firmas de defensa contra Botnet C&C
- Soporte para importar inteligencia de amenazas a través de protocolos estandarizados, incluyendo STIX, OpenIOC y JSON

Detección de ataque

- Deteccion de Ataques de Protocolos Anormales
- Soporte para la detección de ataques DoS/DDoS, incluyendo Flood SYN, Flood de Consultas DNS, con mitigación inteligente de DDoS basada en el aprendizaje de líneas base
- Deteccion de Ataques ARP
- Admite detección de ataques WEB basados en reglas WAF para protocolo HTTP anormal, ataque DDoS, ataque de inyección, ataque entre sitios, ataque de vulnerabilidad especial, fuga de información, acceso de detección, software malicioso, acceso ilegal a recursos
- Soporta la creación de una lista blanca en la función de detección WEB

Identificación de Aplicaciones

- Más de 4,000 aplicaciones, incluyendo IM, P2P, correo electrónico, transferencia de archivos, correo electrónico, juegos en línea, medios en streaming, etc.
- Estadísticas multi-dimensionales basada en zonas, interfaz de usuario, ubicación y dirección IP
- Soporte para Android, aplicaciones móviles IOS

Mitigación de Amenazas

- Acciones de administración para cambiar el estado de los eventos de amenaza, a abierto, falso positivo, fijo, ignorar, confirmado
- Lista blanca de eventos de amenazas, incluido el nombre de amenaza, IP de origen/destino, conteo de aciertos, etc.
- Conjunción con las plataformas de firewall Hillstone para bloquear la amenaza
- Limpieza al servidor/computador para amenazas y reevaluación de la seguridad del host, de un solo clic
- Servicio de integración para Endpoint con sistema de symon
- Caprurar Amenazas
- Soporte de mapeo del framework MITRE ATT&CK®
- Soporte para la identificación de atacantes y víctimas en los registros de amenazas

ARP Detección de Falsificación

- Prevenir la falsificación del ARP mediante la unión IP-MAC y la inspección de paquetes APR

Monitoreo

- Estado dinámico, en tiempo real del tablero de instrumentos y widgets de monitoreo drill-in
- Proyección de monitoreo de riesgo intranet
- Visión general de riesgos del estado interno de la red, incluyendo activos críticos, riesgo en el anfitrion, la gravedad y el tipo de amenaza, ataque externo a geo-ubicaciones, etc.
- Detalles visuales del estado de la amenaza para activos críticos y otros hosts de riesgo, incluido el nivel de riesgo, la certeza del riesgo, la ubicación geográfica del ataque, el descu-brimiento de la cadena de ataque e información estadística del mismo.
- Soporte de escaneo activo de activos. Los resultados del escaneo se pueden cargar en iSource de Hillstone.
- Detalles visuales de eventos de amenazas de red, incluido el análisis de amenazas, la base de conocimientos, los detalles tácticos de MITRE ATT&CK®, los detalles de la técnica MITRE ATT&CK®, el historial y la topología.
- Resumen de la situación de riesgo de red interna, incluyendo la lista TOP5 riesgo/servidor y tendencias de amenazas, estado en riesgo de activos críticos, estado en riesgo del host, gravedad de la amenaza y tipo, geo-ubicaciones de ataque externo, etc.
- Servicio de inteligencia de amenazas basado en la nube.

Registros e Informes

- Tres informes predefinidos: Seguridad, Flujo e Informes
- Ofrece informes definidos por el usuario
- Los informes se pueden exportar en formato PDF, a través de correo electrónico y FTP
- Lo registros incluyen eventos, redes, amenazas y registros de configuración
- Los registros se pueden exportar por Syslog o Email
- Admite la agregación de registros de AV y la agregación de registros de botnets
- Evaluación de pc en riesgo

Administración

- Identificacion, Monitoreo Interno de Equipos de Red y Seridores de Red Nombre,Sistema Operativo,Brows-er,Tipos y Amenzas de Red Grabacion Estatica
- Acceso administrativo: HTTP/HTTPS, SSH, Telnet, consola
- Alertas sobre la condición de dispositivos, incluyendo el uso de la CPU, uso de memoria, uso de disco, nuevas sesiones y sesiones simultáneas, el ancho de banda de la interfaz, temperatura del chasis y la temperatura de la CPU
- Alertas de ancho de banda basadas en las aplicaciones y las nuevas conexiones
- Soporte para tres tipos de alertas: correo electrónico, mensaje de texto, de trampa
- Soporte de idiomas: Inglés

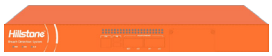
CloudView

- Administración de seguridad de las Bases de Nube
- Acceso 24/7 desde la web o desde una aplicación móvil
- Admite cargar registros de amenazas, paquetes proba-torios, NetFlow, metadatos a iSource para análisis de amenazas
- Estado del dispositivo, tráfico y monitoreo de amenazas

RESTful API

- Soporta las APIs estándar RESTful para acceder a la información de hardware/sistema/eventos de amenaza
- Integración perfecta con el sistema de gestión de redes de terceros

Especificaciones del Producto

	I-1850-IN	I-1870-IN	I-2860-IN
			
Breach Detection Throughput [1]	1 Gbps	1 Gbps	2 Gbps
New Sessions/s [2]	20,700	32,000	75,000
Maximum Concurrent Sessions [2]	750,000	750,000	1.5 Million
Form Factor	1 U	1 U	1 U
Storage	1T HDD	1T SSD	1T SSD
Management Ports	2 x USB port, 1 x RJ45 port	2 x USB port 1 x RJ45 port 1 x MGT	2 x USB port 1 x RJ45 port 2 x MGT
Fixed I/O Ports	4 x GE	2 x SFP+ 8 x SFP 8 x GE	2 x SFP+ 8 x SFP 16 x GE
Available Slots for Expansion Modules	1 x Generic Slot	0	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP-L-IN	N/A	IOC-A-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	60W, Single AC	50W, Single AC	100W, Dual AC Redundant
Dimension (W×D×H, mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)	17.2 x 12.6 x 1.7 in (436 x 320 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	8.8lb (4 kg)	9 lb (4.1 kg)	18.7 lb (8.5 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	5-85% (no dew)	10-95% (no dew)	10-95% (no dew)

	I-3860-IN	I-5850-IN	I-5860-IN
			
Breach Detection Throughput [1]	5 Gbps	10 Gbps	10 Gbps
New Sessions/s [2]	210,000	250,000	500,000
Maximum Concurrent Sessions [2]	3 Million	6 Million	6 Million
Form Factor	1 U	2 U	1 U
Storage	1T SSD	1T HDD	2T SSD
Management Ports	2 x USB port 1 x RJ45 port 3 x MGT	2 x USB port, 1 x RJ45 port, 2 x MGT	2 x USB port 1 x RJ45 port 2 x MGT
Fixed I/O Ports	6 × SFP+ 16 × SFP 8 × GE	N/A	2 × QSFP+ 16 × SFP+ 8 × GE
Available Slots for Expansion Modules	1 x Generic Slot	4 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-A-4SFP+-IN	IOC-BDS-8GE-H-IN, IOC-BDS-8SFP-H-IN, IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100 -240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	289W, Dual AC Redundant	350W, Dual AC Redundant	382W, Dual AC Redundant
Dimension (W×D×H, mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	16.9 x 19.7 x 3.5 in (430 x 500 x 88mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	22.5 lb (10.2 kg)	26.5 lb (12 kg)	22.5 lb (10.2 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	5-85% (no dew)	10-95% (no dew)

Especificaciones y configuración mínima de hardware

	IV04-IN	IV08-IN
Breach Detection Throughput [3]	Up to 1.5 Gbps	Up to 3 Gbps
CPU Support (Min.)	4 Core	8 Core
Memory (Min.)	8G	16G
Storage (Min.)	100G	100G
System Requirement	KVM / Vmware ESXi version 6.5 or above	KVM / Vmware ESXi version 6.5 or above

Tarjeta de interfaz de red compatible

	SR-IOV	All NICs except SR-IOV
KVM	√ (only SR-IOV X710 can be supported)	√
Vmware	×	√

Opciones de modulo

Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN
I/O Ports	4 x SFP Ports	4 x GE Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)

Module	IOC-BDS-8GE-H-IN	IOC-BDS-8SFP-H-IN	IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN
I/O Ports	8 x GE Ports	8 x SFP Ports	4 x SFP+ Ports	4 × SFP+, SFP+ module not included
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U
Weight	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.44 lb (0.2 kg)	2.09 lb (0.96 kg)

Configuración recomendada de Sysmon

Specification	Sysmon Server	Sysmon Client
CPU	4 Core	\
Memory	16G	1G
Storage	1T HDD, extendable	40G HDD
Installation Package	OVF Mirror	MSI Service Program
System Requirement	VMware ESXi	Windows 7 / Windows Server 2008 or above

NOTAS:

(1) El rendimiento se obtiene en virtud de detección de tráfico HTTP bi-dirección con todas las características de detección de amenazas habilitado;
(2) Los datos son obtenidos con la función de detección de ataques WEB desactivada. El rendimiento puede variar si está encendido;
(3) Los datos de rendimiento de la detección de brechas dependen de la configuración del hardware;

Version:EX-08.01-BDS-V5.0-1223-SP-01