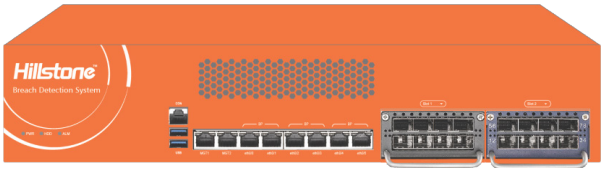
# Hillstone Serie-I

## Servidor de Sistema de Detección de Brechas (sBDS)



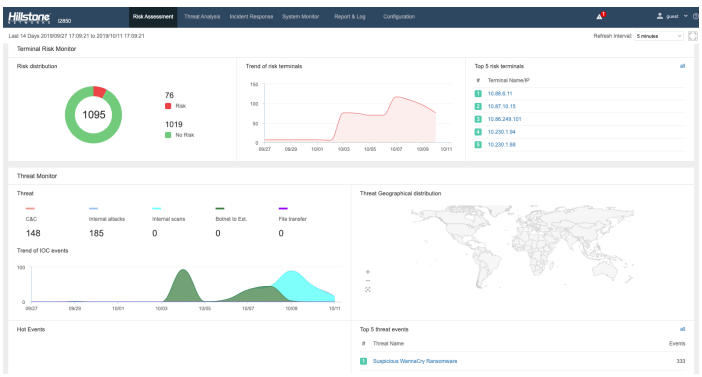




El Sistema de Detección de Fallas del Servidor Hillstone (sBDS) adopta múltiples tecnologías para la detección de amenazas que incluyen tanto tecnología tradicional basada en firmas como la de modelos de datos inteligentes de amenazas a gran escala y modelos de análisis del comportamiento del usuario, que proporcionan una solución ideal para detectar ataques de amenazas desconocidas o de 0-días, para proteger servidores críticos de alto valor y evitar que se filtren o que roben sus datos confidenciales. Junto con capacidades y visibilidad de análisis de amenazas profundas, Hillstone sBDS brinda a los administradores de seguridad los medios efectivos para detectar eventos de IOC (Indicadores de compromiso), restaurar la cadena de ataque de amenazas y proporcionar una amplia visibilidad del análisis y mitigaciones de inteligencia de amenaza.

## 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 sBDS 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.

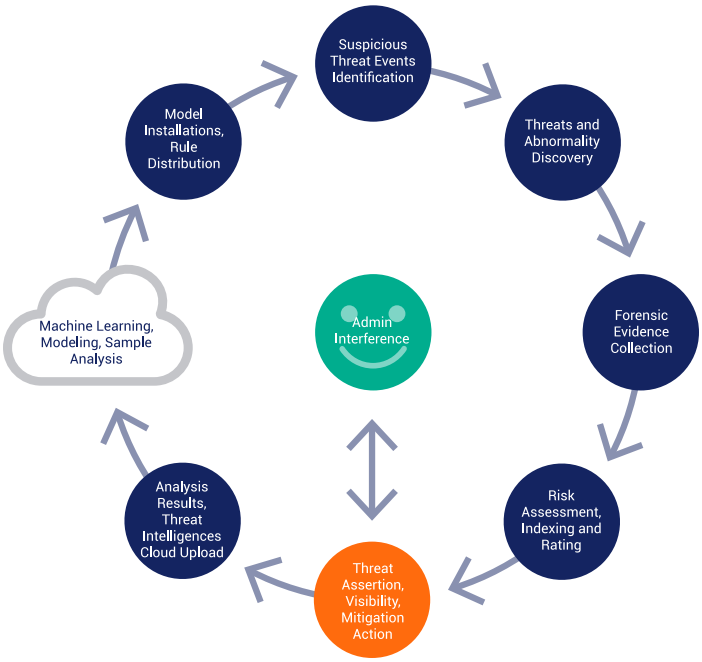
## Monitoreo de Amenazas en Tiempo Real para Hosts y Servidores Críticos


La plataforma sBDS 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 sBDS 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 Cyber Kill

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 sBDS 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 sBDS de Hillstone realiza la mitigación de amenazas consecutivas con dispositivos Hillstone E-Series NGFW y T-Series iNGFW, 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

### Detección Avanzada de Amenazas

- Detección avanzada de malware basada en el comportamiento
- Detección de más de 2000 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

### 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 30.000 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

### Escaneo de Virus

- Base de firmas de más de 4 millones de virus
- Actualizaciones en tiempo real en línea
- Análisis de archivos comprimidos

### 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 ataque

- Deteccion de Ataques de Protocolos Anormales
- Deteccion de Denegacion de Servicios/Denegacion de Servicios Distribuidos, Incluye Inundaciones de Trafico SYN,Inundaciones de Consultas DNS
- 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

### 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.
- Visualización detallada del estado de amenaza para los activos críticos y otros hosts arriesgados, incluyendo el nivel de riesgo, la certeza de riesgo, ataques por geo-localización, mapeo Kill Chain y otra información estadística
- Detalles visuales de eventos de amenazas de red, incluyendo el nombre, tipo, gravedad y amenaza a la seguridad, análisis de amenazas, base de conocimientos e historia
- 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
- Evaluación de pc en riesgo

### Administración

- Identificacion, Monitoreo Interno de Equipos de Red y Seridores de Red Nombre,Sistema Operativo,Browser,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
- 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 | I-2850 | I-3850 | I-5850 |
|---|---|---|---|---|
| |  |  |  |  |
| **Breach Detection Throughput** [1] | 1 Gbps | 2 Gbps | 5 Gbps | 10 Gbps |
| **New Sessions/s** [2] | 15,000 | 30,000 | 40,000 | 160,000 |
| **Maximum Concurrent Sessions** [2] | 750,000 | 1.5 Million | 3 Million | 6 Million |
| **Form Factor** | 1 U | 1 U | 2 U | 2 U |
| **Storage** | 1T HDD | 1T HDD | 1T HDD | 1T HDD |
| **Management Ports** | 2 x USB Port, 1 x RJ45 port | 2 x USB Port, 1 x RJ45 port, 2 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** | 4 x GE | 4 x GE | 6 x GE | N/A |
| **Available Slots for Expansion Modules** | 1 x Generic Slot | 1 x Generic Slot | 2 x Generic Slot | 4 x Generic Slot |
| **Expansion Module Option** | IOC-S-4GE-B-L, IOC-S-4SFP-L | IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+ | IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+ | IOC-BDS-8GE-H, IOC-BDS-8SFP-H, IOC-BDS-4SFP+-H |
| **Power Supply** | AC 100-240 V 50/60 Hz | AC 100-240 V 50/60 Hz | AC 100-240 V 50/60 Hz | AC 100-240 V 50/60 Hz |
| **Power Specification** | 60W, Single AC | 250W, Single AC | 350W, Dual AC Redundant | 350W, Dual AC Redundant |
| **Dimension (W×D×H, mm)** | 16.9 x 11.8 x 1.7 in (430 x 300 x 44mm) | 16.9 x 11.8 x 1.7 in (430 x 300 x 44mm) | 16.9 x 19.7 x 3.5 in (430 x 500 x 88mm) | 16.9 x 19.7 x 3.5 in (430 x 500 x 88mm) |
| **Weight** | 14.3 lb (6.5 kg) | 15.4 lb (7 kg) | 26.5 lb (12 kg) | 26.5 lb (12 kg) |
| **Temperature** | 32-104°F (0-40°C) | 32-104°F (0-40°C) | 32-104°F (0-40°C) | 32-104°F (0-40°C) |
| **Relative Humidity** | 5-85% (no dew) | 5-85% (no dew) | 5-85% (no dew) | 5-85% (no dew) |

# Opciones de modulo

| Module | IOC-S-4GE-B-L | IOC-S-4SFP-L | IOC-S-4GE-B | IOC-S-4SFP | IOC-S-8SFP |
|---|---|---|---|---|---|
| I/O Ports | 4 x GE Bypass Ports | 4 x SFP Ports | 4 x GE Bypass Ports | 4 x SFP Ports | 8 x SFP Ports |
| Dimension | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) |
| Weight | 0.22. lb (0.1 kg) | 0.22 lb (0.1 kg) | 0.33 lb (0.15 kg) | 0.33 lb (0.15 kg) | 0.55 lb (0.25 kg) |

| Module | IOC-S-4GE-4SFP | IOC-S-2SFP+ | IOC-S-4SFP+ | IOC-BDS-8GE-H | IOC-BDS-8SFP-H | IOC-BDS-4SFP+-H |
|---|---|---|---|---|---|---|
| I/O Ports | 4SFP Ports | 2SFP+ Ports | 4SFP+ Ports | 8 x GE Ports | 8 x SFP Ports | 4 x SFP+ Ports |
| Dimension | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) | 1U (Occupies 1 generic slot) |
| Weight | 0.55 lb (0.25 kg) | 0.33 lb (0.15 kg) | 0.44 lb (0.2 kg) | 0.55 lb (0.25 kg) | 0.55 lb (0.25 kg) | 0.44 lb (0.2 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.



Version:EX-08.01-sBDS-V3.4-1021-SP-01