Hillstone I-Series
Server Breach Detection System(sBDS)

I-2850 / I-3850

The Hillstone Server Breach Detection System (sBDS) adopts multiple threat detection technologies that include traditional signature-based technology as well as large-scale threat intelligent data modeling and user behavioral analytics modeling. The system provides an ideal solution to detect advanced threats including ransomware and cryptomining malware, protect high-value critical servers and sensitive data from being leaked or stolen. Together with deep threat hunting analytical capabilities and visibility, Hillstone sBDS provides security admins the effective means to detect IOCs (Indicators of Compromise) events, locate risky hosts and servers, restore the attack kill chain.

Comprehensive threat correlation analytics for advanced threat detection

Cyber attackers have become ever more sophisticated, using targeted, persistent, stealthy and multi-phased attacks, which can easily evade perimeter detection. Hillstone sBDS consists of multiple detection engines focused on different aspects of post-breach threat detection, including advanced malware detection (ATD), abnormal behavior detection (ABD), as well as traditional intrusion detection and virus scanning engines. Hillstone's threat correlation platform analyzes the details of the relationships of each individual suspicious threat event as well as other contextual information within the network, to connect the dots and provide accurate and effective malware and attack detection with high confidence levels.

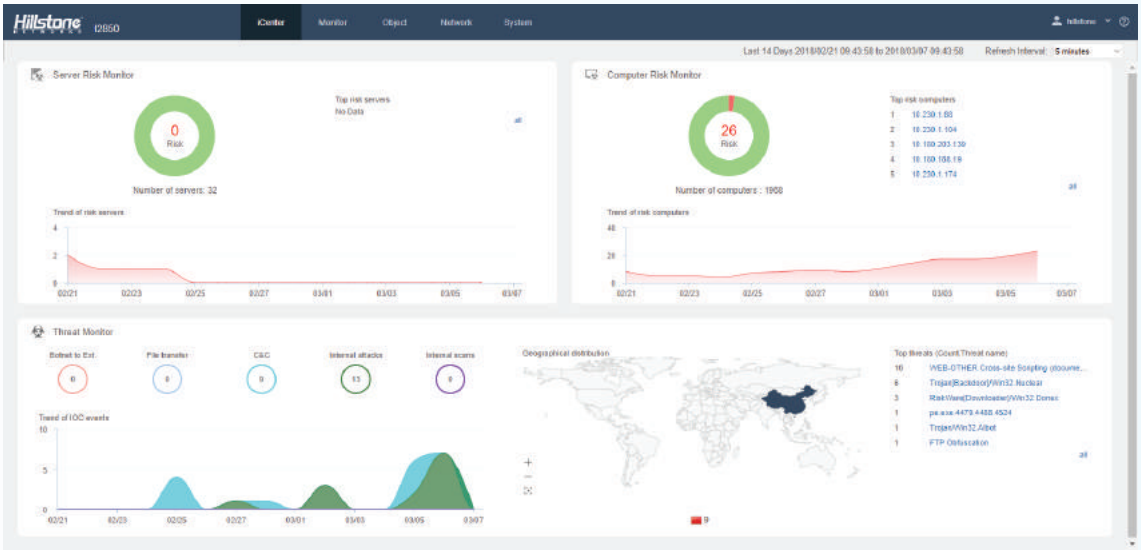

Figure 1. Hillstone sBDS I-2850 iCenter Dashboard

Real-time threat monitoring for critical servers and hosts

The Hillstone sBDS platform focuses on protecting critical servers within the intranet, detecting unknown and near 0-day threat attacks and finding abnormal network and application level activities of server and host machines. Once a threat or an abnormal behavior is detected, Hillstone sBDS will perform threat or behavioral analysis and use topology-based graphic presentations to provide extensive visibility into the threat details and behavioral abnormalities. This gives security admins unprecedented insights into the attack progress, traffic trending in each direction, as well as the entire network risk assessment.

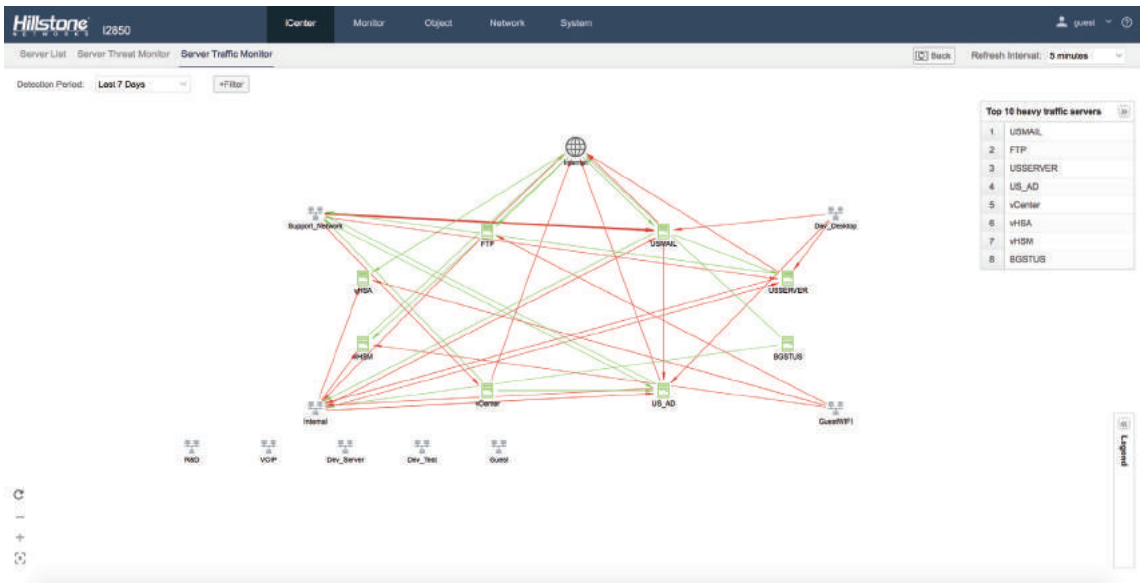

Figure 2. Server Threat and Traffic Monitoring

Complete Indicator of Compromises and Cyber kill chain

IOCs events are threat events detected during the post breach attack. They are identified among large numbers of the threat attacks in the network that are directly associated with the protected server or host. IOCs are typically seen as threat activities with higher risk and with a high confidence level that a server or host is being compromised and that poses a potentially bigger threat to the critical assets within the corporate network. To effectively detect IOCs and perform deep threat detection on these IOCs is critical in throttling the goal of stealing important data from critical assets, and preventing a threat attack from further spreading within the network. Hillstone sBDS drills down and surfaces more threat analysis and intelligence on these IOC events, reconstructing the attack chain based on these IOCs and correlating other threat events associated with these IOCs within time and space spectrums.

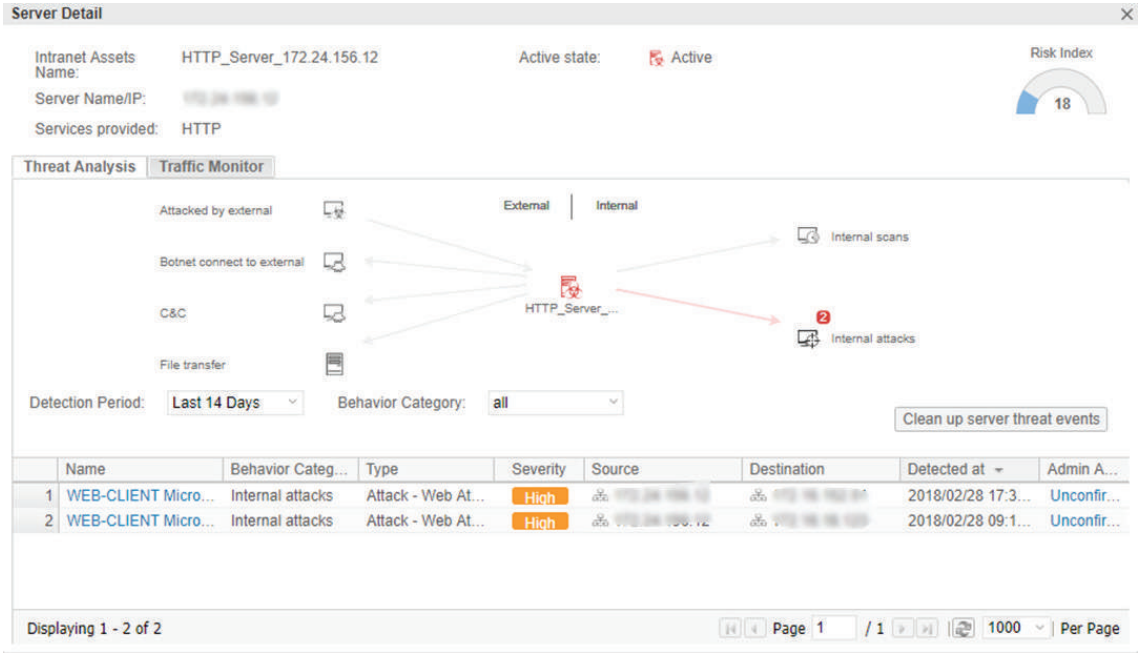

Figure 3. Kill Chain mapping of post-breach threats

Rich Forensic Information and Preemptive Mitigation

The Hillstone sBDS platform conducts threat mitigation with conjunction of Hillstone E-Series NGFW and T-Series iNGFW devices, which are positioned at the network perimeter. After the security admin or network operators analyze and validate threat alerts, they can add threat elements such as IP addresses, type of threats etc., to the blacklist or security policies, and then synchronize them to the Hillstone firewalls so that future attacks from the same breeds or malware family can be blocked at the network perimeter. This prevents future attacks from spreading to broader network territories.

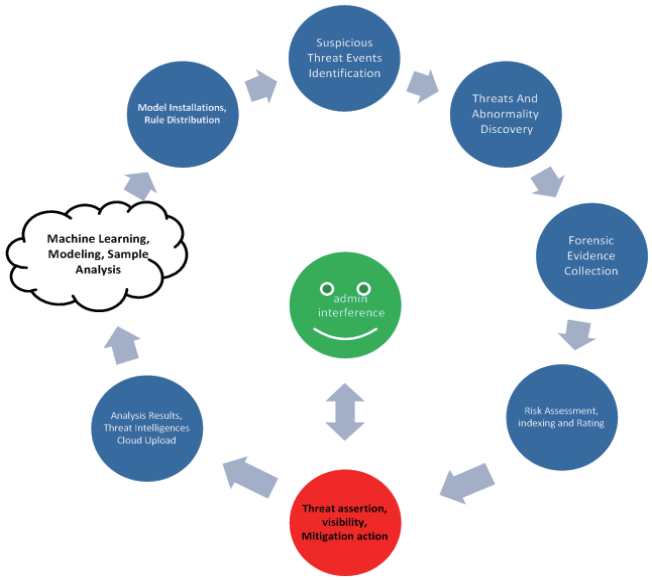

Figure 4. Hillstone sBDS Threat Mitigation Cycle

Core Features

Abnormal Behavior Detection
- ☐Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM, SSH/FTP weak password
- ☐Detect DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL and application DDoS
- ☐Support inspection of encrypted tunneling traffic for unknown applications
- ☐Real-time, online, abnormal behavior model database update

Advanced Threat Detection
- ☐Behavior-based advanced malware detection
- ☐Detect more than 2000 known and unknown malware families including Virus, Worm, Trojan, Overflow etc
- ☐Real-time, online, malware behavior model database update
- ☐Detect major ransomware and cryptomining malware

Threat Correlation Analytics
- ☐Correlation among unknown threats, abnormal behavior and application behavior to discover potential threat or attacks
- ☐Multi-dimension correlation rules, automatic daily update from the cloud

Deception Threat Detection
- ☐Local deception engine with regular deception models update
- ☐Simulate to Web, Doc or Database Servers, support protocols including FTP, HTTP, MYSQL, SSH and TELNET

Intrusion Detection
- ☐8000+ signatures, protocol anomaly detection and rate-based detection
- ☐Custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- ☐Over 20 types of protocols anomaly detection, including HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS, etc
- ☐Support for buffer overflow, SQL injection and cross-site scripting attack detection

Virus Scan
- ☐Over 2 million virus signature database and online real-time update
- ☐Support compressed file scan

Botnet C&C Detection
- ☐Discover intranet botnet host by monitoring C&C connections
- ☐Detect C&C IP and domain name in TCP, HTTP and DNS traffic
- ☐Automatically update the botnet C&C defense signature library

Network Layer Attack Detection
- ☐Abnormal protocol attack detection
- ☐DoS/DDoS detection, including SYN Flood, DNS Query Flood
- ☐ARP attack detection

Application Identification
- ☐Over 3000 applications, including IM, p2p, email, file transfer, email, online games, media streaming, etc.
- ☐Multi-dimension application statistic based on zones, interface, location, user, and IP address
- ☐Support for Android, IOS mobile applications

Threat Mitigation
- ☐Admin actions to change threat events status, open, false positive, fixed, ignore, confirmed
- ☐One-click cleanup of server/computer threat and reevaluation of host security
- ☐Threat events whitelist, including threat name, source/destination IP, hit count etc.
- ☐Conjunction with Hillstone firewall platforms to block threat
- ☐Sysmon endpoint service integration
- ☐Threat hunting

Monitoring
- ☐Dynamic, real-time dashboard status and drill-in monitoring widgets
- ☐Intranet risk monitoring projection
- ☐Overview of internal network risk status, including TOP5 risk server/computer list and threat trends, critical assets risk status, host risk status, threat severity and type, external attack geo-locations, etc
- ☐Visual details of threat status for critical assets and other risky host, including risk level, risk certainty, attack geo-location, kill chain mapping and other statistical information
- ☐Visual details of network threat events, including threat analysis, knowledge base, history and topology

Logs & Reporting

- Three predefined reports: Security, Flow and System reports
- Support user defined reporting
- Reports can be exported in PDF via Email and FTP
- Logs, including events, networks, threats, and configuration logs
- Logs can be exported via Syslog or Email
- Host risk assessment

Administration

- Monitoring internal network hosts and servers, identifing name, operation system, brswer, type, and network threat statistic record
- Management access: HTTP/HTTPS, SSH, telnet, console
- Device condition alerts, including CPU usage, memory usage, disc usage, new session and concurrent sessions, interface bandwidth, chassis temperature and CPU temperature
- Alerts based on application bandwidth and new connection
- Support for three types of alerts: email, text message, trap
- Language support: English

Centralized Management

- Register devices to Hillstone Security Management Platform (HSM)
- Monitor multiple devices status, traffic and threat via cloud with 7/24 access from web or mobile application (CloudView)
- Support third-party threat Intelligence for detecting malicious files, URL and IP addresses

Product Specification

Model	I-2850	I-3850
		
Breach Detection Throughput[1]	2 Gbps	5 Gbps
Form Factor	1 U	2 U
Storage	1T HDD	1T HDD
Management Ports	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	6 x GE
Available Slots for Extension Modules	1 x Generic Slot	2 x Generic Slot
Expansion Module Option	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz
Maximum Power Consumption	250 W	350 W
Dimension (W×D×H, mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)	16.9 x 19.7 x 3.4 in (430 x 500 x 88mm)
Weight	15.4 lb (7 kg)	26.5 lb (12 kg)
Temperature	32-104 F (0-40°C)	32-104 F (0-40°C)
Relative Humidity	5-85% (no dew)	5-85% (no dew)

Module Options

Module	IOC-S-4GE-B	IOC-S-4SFP	IOC-S-8GE-B	IOC-S-8SFP	IOC-S-4GE-4SFP	IOC-S-2SFP+	IOC-S-4SFP+
I/O Ports	4 x GE Bypass Ports	4 x SFP Ports	8 x GE Bypass Ports	8xSFP Extension Module	4SFP Extension Module	2SFP+ Extension Module	4SFP+ Extension Module
Dimension	1U	1U	1U	1U	1U	1U	1U
Weight	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.33 lb (0.15kg)	0.44 lb (0.2kg)

Recommended Sysmon Configuration

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 2007 or above

NOTES:(1) Breach Detection Throughput is obtained under bi-direction HTTP traffic detection with all threat detection features enabled.