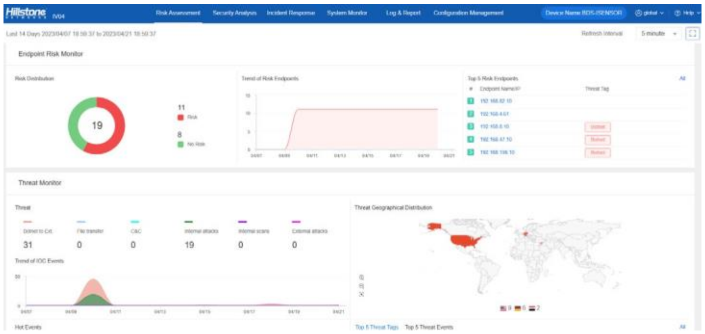
Hillstone Network Detection and Response

Hillstone Network Detection and Response (NDR) provides a robust solution for detecting and responding to sophisticated attacks like ransomware and crypto-mining malware. Hillstone NDR, with its product, the Breach Detection System (BDS), combines proven methods, such as signature- based detection and threat intelligence, with advanced machine learning to analyze user behavior and uncover hidden threats. Once a threat is detected, Hillstone NDR provides deep threat hunting and visibility, helping security administrators quickly identify Indicators of Compromise (IOCs), locate compromised hosts, and reconstruct the entire attack chain. For a complete defense, it integrates with both Hillstone and third-party Next-Generation Firewalls (NGFWs), as well as our iSource XDR system, to automatically mitigate threats and ensure your enterprise assets are comprehensively protected.

Product Highlights

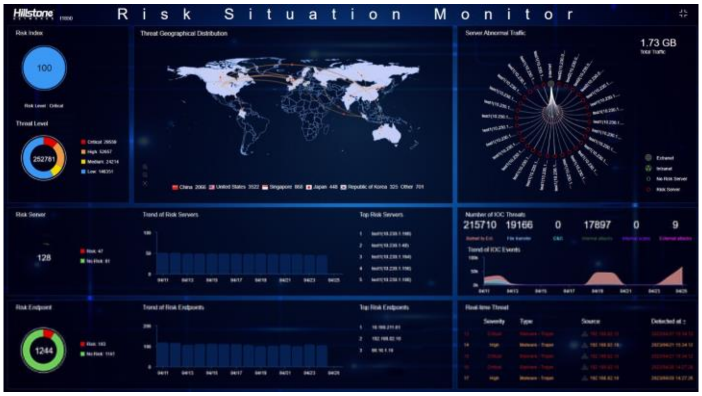
Comprehensive Threat Correlation Analytics for Advanced Threat Detection



Cyber attackers have become ever more sophisticated, using targeted, persistent, stealthy and multi-phased attacks, which can easily evade perimeter detection. Hillstone BDS boasts a diverse range of detection capabilities, including Advanced Threat Detection (ATD), Abnormal Behavior Detection (ABD), deception threat detection, intrusion and attack detection, virus and spam detection, and botnet C&C detection. 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.

Product Highlights (Continued)

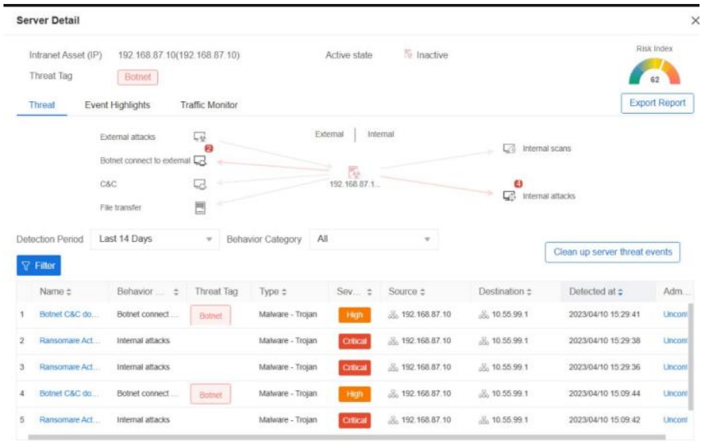
Real-time Threat Monitoring for Critical Servers and Hosts



Hillstone NDR focuses on protecting critical servers within the intranet, detecting unknown and 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 NDR 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.

Complete Indicator of Compromises and Cyber Attack 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 NDR 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.

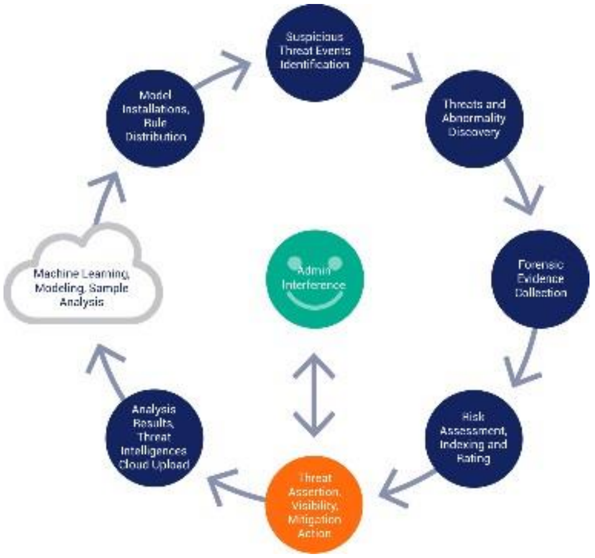

Server Detail

Intranet Asset (IP) 192.168.87.10(192.168.87.10)
Active state Inactive
Threat Tag Botnet
Risk Index 62

Detection Period Last 14 Days
Behavior Category All

	Name	Behavior ...	Threat Tag	Type	Sev...	Source	Destination	Detected at	Adm...
1	Botnet C&C do...	Botnet connect ...	Botnet	Malware - Trojan	High	192.168.87.10	10.55.99.1	2023/04/10 15:29:41	Uncon
2	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023/04/10 15:29:38	Uncon
3	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023/04/10 15:29:36	Uncon
4	Botnet C&C do...	Botnet connect ...	Botnet	Malware - Trojan	High	192.168.87.10	10.55.99.1	2023/04/10 15:09:44	Uncon
5	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023/04/10 15:09:42	Uncon

Rich Forensic Information and Preemptive Mitigation


Suspicious Threat Events Identification
Threats and Abnormality Discovery
Forensic Evidence Collection
Risk Assessment, Indexing and Rating
Threat Assertion, Visibility, Mitigation Action
Analysis Results, Threat Intelligence Cloud Upload
Machine Learning, Modeling, Sample Analysis
Model Installations, Rule Distribution
Admin Interference

Hillstone NDR conducts threat mitigation with conjunction of Hillstone A-Series NGFW, and X-Series data center NGFW, as well as third-party NGFW devices. 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 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.

Features

Abnormal Behavior Detection

- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM
- 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
- Support the detection of RDP/VNC/SMB/SSH/FTP brute force attack, TOR based suspicious HTTP requests
- Support detecting and alerting on remote access software

Advanced Threat Detection

- Behavior-based advanced malware detection
- Detect more than 2,000 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
- Support threat detection on encrypted traffic without decryption
- Support threat detection for encrypted HTTPS, SMTPS, POP3S, and IMAPS traffic by decryption in TAP mode

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

- 35,000+ 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, VxLAN, MPLS, etc
- Support for buffer overflow , SQL injection and cross -site scripting attack detection
- Support weak password detection for protocols of FTP/HTTP/SMT/ POP3/IMAP/TELNET/Cassandra/DB2/IRC/NNTP/PGSQL/REDIS/ Rexec/Rlogin/ RTSP/Socket5/Sybase
- Support advanced evasion detection, including port remapping, IP/TCP fragmentation, and URL/Unicode encoding bypass techniques
- Support customizable protocol inspection depth with configurable scan lengths exceeding 4KB
- Support reverse shell detection
- Support capturing complete attack packets
- Support plaintext password detection in HTTP traffic
- Support brute-force detection for over 30 applications/protocols

Antivirus

- Over 15 million virus signature database and online real-time update
- Support compressed file scanning across multiple archive formats including Zip, Rar, 7z, and Tar, with up to 100 recursive decompression layers
- Support custom MD5 and URL blocklists/allowlists with external dynamic list integration
- Support configuring MD5 and URL whitelists
- Support dual Antivirus detection engines, including MD5-based detection and AI -powered detection

Botnet C&C Detection

- Support discovering intranet botnet host by monitoring C&C connections
- Support detecting C&C IP and domain name in TCP, HTTP and DNS traffic
- Support C&C traffic detection over TCP, HTTP, DNS, and TLS encrypted protocols
- Support detecting C & C channels based on Domain Generation Algorithms (DGA)
- Support importing threat intelligence through standardized protocols including STIX, OpenIOC, and JSON
- Support auto-update the botnet C&C defense signature database

Anti-Spam

- Real-time spam classification and prevention• Confirmed Spam, Suspected Spam, Bulk Spam, Valid Bulk
- Protection regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Whitelists to allow emails from trusted domain/email addresses

Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP, SMTP, POP3, IMAP4 and FTP
- Support file types including PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Multiple static detection engines quickly filter normal files and known threats
- Unknown threat visualization based on logs, reports, monitoring information, file behavior reports

Attack Detection

- Abnormal protocol attack detection
- Support DoS/DDoS detection, including SYN Flood, DNS Query Flood, with intelligent DDoS mitigation based on baseline learning
- ARP attack detection
- Support WEB attack detection based on WAF rules for abnormal HTTP protocol , DDoS attack, injection attack, cross-site attack, special vulnerability attack, information leakage, detection access, malicious software, illegal access to resources
- WEB detection function whitelist

Application Identification

- Over 4,000 applications, including IM, p2p, 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

ARP Spoofing Detection

- Prevent ARP spoofing by IP-MAC binding and APR packet inspection

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 hosts, including risk level, risk certainty, attack geo- location, attack chain uncovering and other statistical information
- Support active scanning for assets; scanning results can be uploaded to Hillstone XDR platform iSource
- Support automated attack surface management
- Visual details of network threat events, including threat analysis, knowledge
- base, MITRE ATT&CK® tactic details, MITRE ATT&CK® technique details, history and topology
- Send alert notifications via Email, SMS, WeCom, Feishu, DingTalk and Trap
- Cloud-based threat intelligence push service

Threat Mitigation

Features (Continued)

- 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.
- Support integration with Hillstone and third-party firewalls to block threats
- Sysmon endpoint service integration
- Support global threat detection whitelist for centralized exemption management across all detection policies
- Threat hunting
- Support MITRE ATT&CK® framework mapping
- Support identification of attackers and victims in threat logs

Critical Protection Mode

- Support one-click Critical Protection Mode with built-in global policy template for instant hardening and lossless rollback
- Support signature updates with high-frequency refresh during Critical Protection Mode

Logs & Reporting

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

Administration

- Monitor internal network hosts and servers: name, OS, browser, type, and network threat statistics
- 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
- Unknown threat visualization based on logs, reports, monitoring information, file behavior reports
- Seamless integration with 3rd party network management system
- Support High Availlability
- Support web-based CLI access to the device directly through the management GUI
- Support web-based CLI access to the device directly through the management GUI

RESTful APIs

- Support standard RESTful APIs for accessing hardware/system/threat event information

Centralized Management

- Support registering devices to Hillstone Security Management Platform (HSM)
- Support 24/7 monitoring of multiple devices, traffic and threat via Hillstone CloudView (web or mobile)
- Support uploading threat logs, evidential packets, NetFlow, metadata to Hillstone iSource XDR for threat analysis
- Support integration with third- party threat Intelligence to detect malicious files, URLs and IP addresses

Specifications

	I-1870-IN	I-2860-IN
Breach Detection Throughput [1]	1 Gbps	2 Gbps
New Sessions/s [2]	25,000	50,000
Maximum Concurrent Sessions [2]	750,000	1.5 Million
Form Factor	1 U	1 U
Storage	1T SSD	1T SSD
Management Ports	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	2 × SFP+ 8 × SFP 8 × GE	2 × SFP+ 8 × SFP 16 × GE
Available Slots for Expansion Modules	N/A	1 x Generic Slot
Expansion Module Option	N/A	IOC-A-BDS-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	50W, Single AC	100W, Dual AC Redundant
Dimension (W×D×H, mm)	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	9 lb (4.1 kg)	18.7 lb (8.5 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)

Specifications (Continued)

	I-3860-IN 	I-5860-IN
Breach Detection Throughput [1]	5 Gbps	10 Gbps
New Sessions/s [2]	120,000	500,000
Maximum Concurrent Sessions [2]	3 Million	6 Million
Form Factor	1 U	1 U
Storage	1T SSD	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
Fixed I/O Ports	6 ×SFP+ 16 × SFP 8 × GE	2 × QSFP+ 16 × SFP+ 8 × GE
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-A-BDS-4SFP+-IN	IOC-A-BDS-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	289W, 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)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	22.5 lb (10.2 kg)	22.5 lb (10.2 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)

Specification and Minimum Hardware Configuration

	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
Public Cloud Support	Alibaba Cloud / Tencent Cloud	Alibaba Cloud / Tencent Cloud

Network Interface Card Supported

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

Module Options

Module	IOC-A-BDS-4SFP+-IN
I/O Ports	4 x SFP Ports
Dimension	1U (Occupies 1 generic slot)
Weight	0.42 lb (0.19 kg)

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 2008 or above

NOTES:

(1) Breach detection throughput is measured under bidirectional HTTP traffic with all threat detection features enabled;
(2) The data reflects performance with web attack detection disabled. Performance may vary if it's enabled;
(3) Breach detection throughput varies based on hardware configuration.
Unless specified otherwise, all performance are based on BDS 5.0. Results may vary based on BDS version and deployment.