Hillstone Breach Detection System (BDS) I-Series

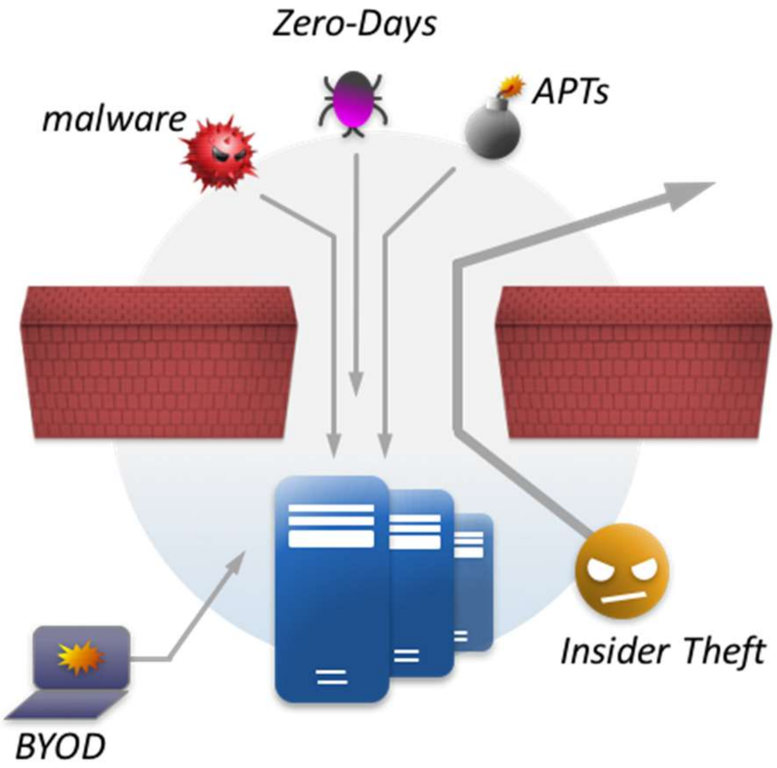
Integrative Cyber Security

Agenda

- Today’s Intranet Security Reality
- Hillstone BDS Value Proposition
- Hillstone BDS Portfolio
- Deployment Scenarios & Winning Cases

Today's Intranet Security Reality

Internal Network Breaches Occur at an Alarming Rate

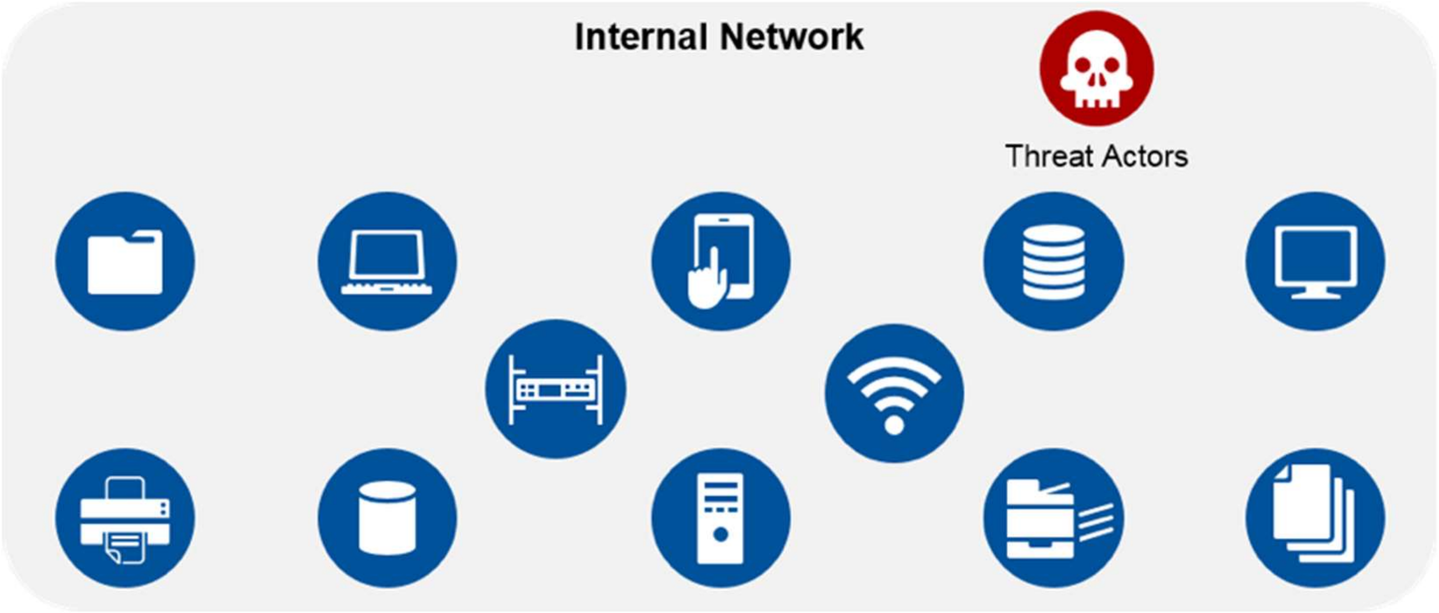


Traditional signature defenses can only stop old “amateur” attacks

New, sophisticated attacks breach every network.

“In 60% of cases,
attackers are able to compromise an organization within ***minutes****.”*
– Verizon 2015 DBIR

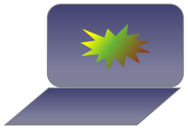
Threat Spreads Easily in Flat Internal Networks…



"…regardless of their motivation, should adversaries gain a foothold on your internal network, they can pivot through and access anything on your internal network. This is a primary reason modern breaches are so devastating in terms of the amount of data lost and the dwell time spent on an organization's network before being discovered. As a result, lateral movement detection/prevention has become an area of considerable focus"

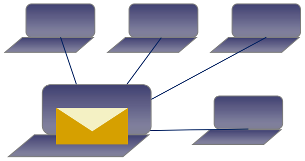
-Source: Gartner (September 2016)

Interrupts Critical Servers and Business Continuity



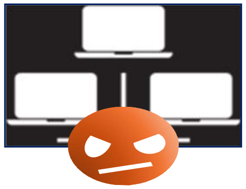
- Phishing occurs when staff surf the internet

- C&C
- Hacker completely controls the host



- Fake internal email and attachment propagates damage internally
- More hosts are compromised

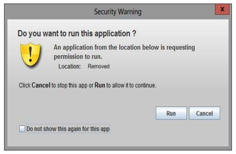
- Host loses control
- Launches DDoS from inside



- Results in server, firewall break-down
- Ultimately, network and business are down

Breaches Sensitive Data Through Compromised Host

- Phishing occurs when staff surf the internet



Do you want to run this application ?

An application from the location below is requesting permission to run.

Location: Removed

Click **Cancel** to stop this app or **Run** to allow it to continue.

□ Do not show this again for this app

- Inject malware with fake or expired antivirus software signatures

- Antivirus software fails to detect malware
- Malware is executed

- C&C
- Downloads PE file
- Hacker completely controls the host

Database server is breached through the compromised host

Hillstone BDS Value Proposition

Hillstone NDR Product BDS

Hillstone NDR product detects and responds to Advanced Network Threats

Threat Detection	Deep Visibility	Digital Forensic & Incidence Response (DFIR)	Effective Mitigation
ABD/ATD/WEB	IOCs	Attack Chain	Admin Actions
NTA/Deception	Dashboards	MITRE ATT&CK	Blacklist / Whitelist
Threat Correlation	Risk/Threat/Traffic	Rich Forensic	Block with Firewall
…	…	…	…

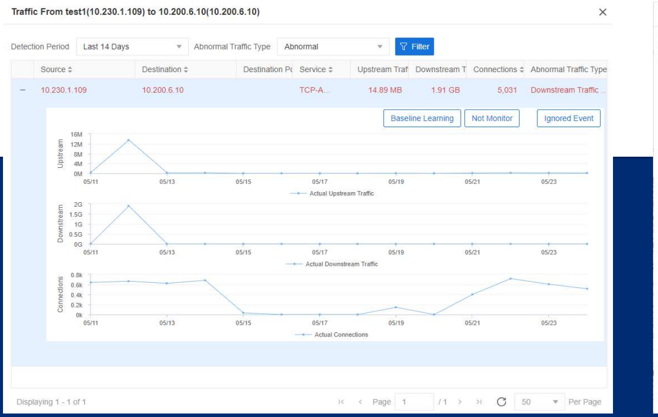
ML-based Analytics for Abnormal Behaviors

Learn and Establish Normal Traffic Baseline and Threshold

Detect Traffic Trend and Identify Abnormal Traffic Behaviors

Monitor Normal and Abnormal Traffic for each server/host

ML-based behavior analytics for URL, UEBA, threat correlations etc.

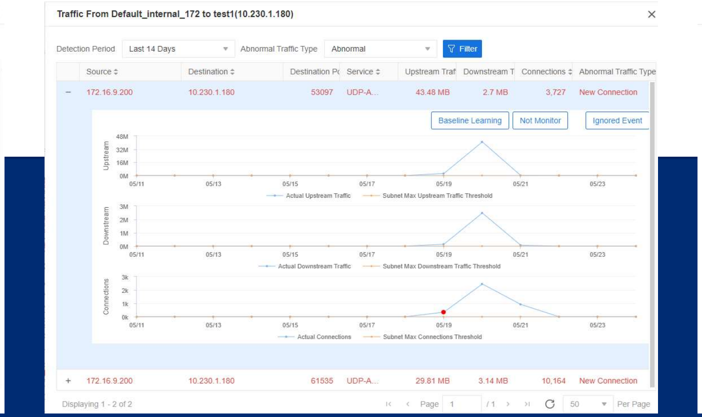


Traffic From test1(10.230.1.109) to 10.200.6.10(10.200.6.10)

Detection Period: Last 14 Days   Abnormal Traffic Type: Abnormal

	Source	Destination	Destination Pc	Service	Upstream Traf	Downstream T	Connections	Abnormal Traffic Type
–	10.230.1.109	10.200.6.10		TCP-A...	14.89 MB	1.91 GB	5,031	Downstream Traffic ...

Displaying 1 - 1 of 1   Page 1 / 1   50 Per Page

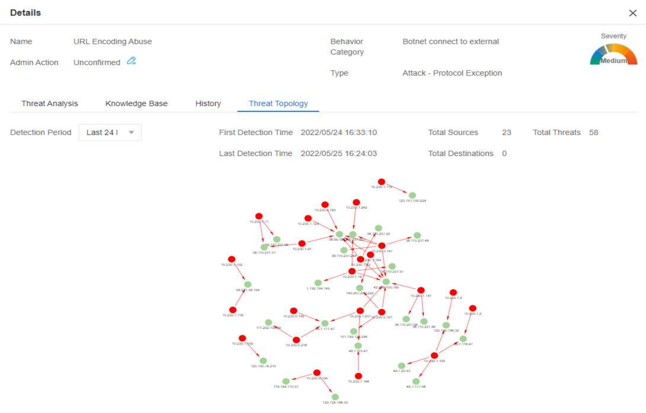


Traffic From Default_internal_172 to test1(10.230.1.180)

Detection Period: Last 14 Days   Abnormal Traffic Type: Abnormal

	Source	Destination	Destination Pc	Service	Upstream Traf	Downstream T	Connections	Abnormal Traffic Type
–	172.16.9.200	10.230.1.180	53097	UDP-A...	43.48 MB	2.7 MB	3,727	New Connection
+	172.16.9.200	10.230.1.180	61535	UDP-A...	29.81 MB	3.14 MB	10,164	New Connection

Displaying 1 - 2 of 2   Page 1 / 1   50 Per Page



Details

Name: URL Encoding Abuse

Admin Action: Unconfirmed

Behavior Category: Botnet connect to external

Type: Attack - Protocol Exception

Severity: Medium

Detection Period: Last 24 I

First Detection Time: 2022/05/24 16:33:10

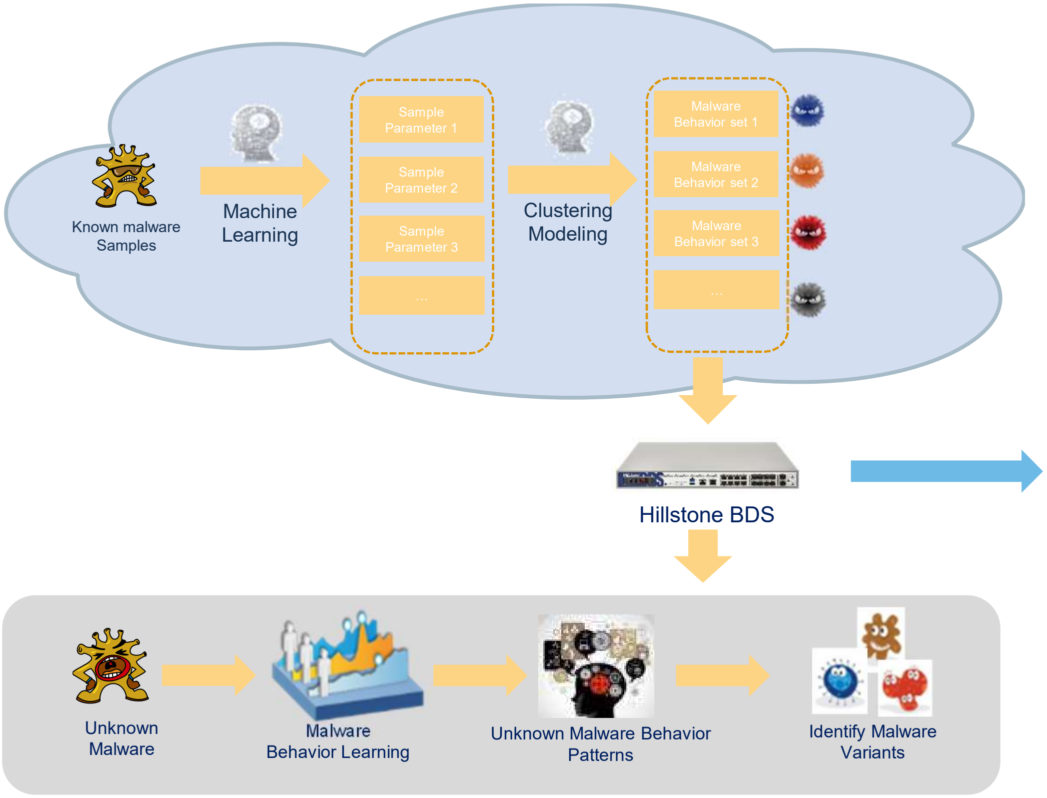
Last Detection Time: 2022/05/25 16:24:03

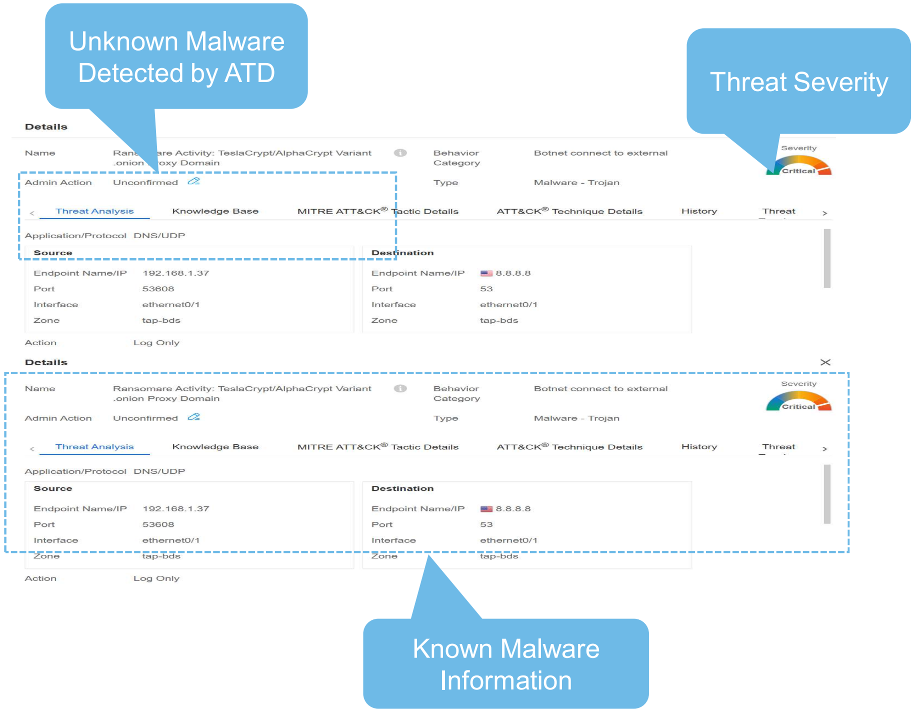
Total Sources: 23

Total Destinations: 0

Total Threats: 58

Detection: Advanced Threat Detection (ATD)




Unknown Malware Detected by ATD

Threat Severity

Details

Name	Ran are Activity: TeslaCrypt/AlphaCrypt Variant .onion oxy Domain	Behavior Category	Botnet connect to external	Severity Critical
Admin Action	Unconfirmed	Type	Malware - Trojan	

< Threat Analysis | Knowledge Base | MITRE ATT&CK® Tactic Details | ATT&CK® Technique Details | History | Threat >

Application/Protocol DNS/UDP

Source		Destination	
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

Action Log Only

Details

Name	Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain	Behavior Category	Botnet connect to external	Severity Critical
Admin Action	Unconfirmed	Type	Malware - Trojan	

< Threat Analysis | Knowledge Base | MITRE ATT&CK® Tactic Details | ATT&CK® Technique Details | History | Threat >

Application/Protocol DNS/UDP

Source		Destination	
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

Action Log Only

Known Malware Information

Detection: WEB Attacks Detection

Detect and analyze threats for WEB servers and applications

WEB Attacks Detection

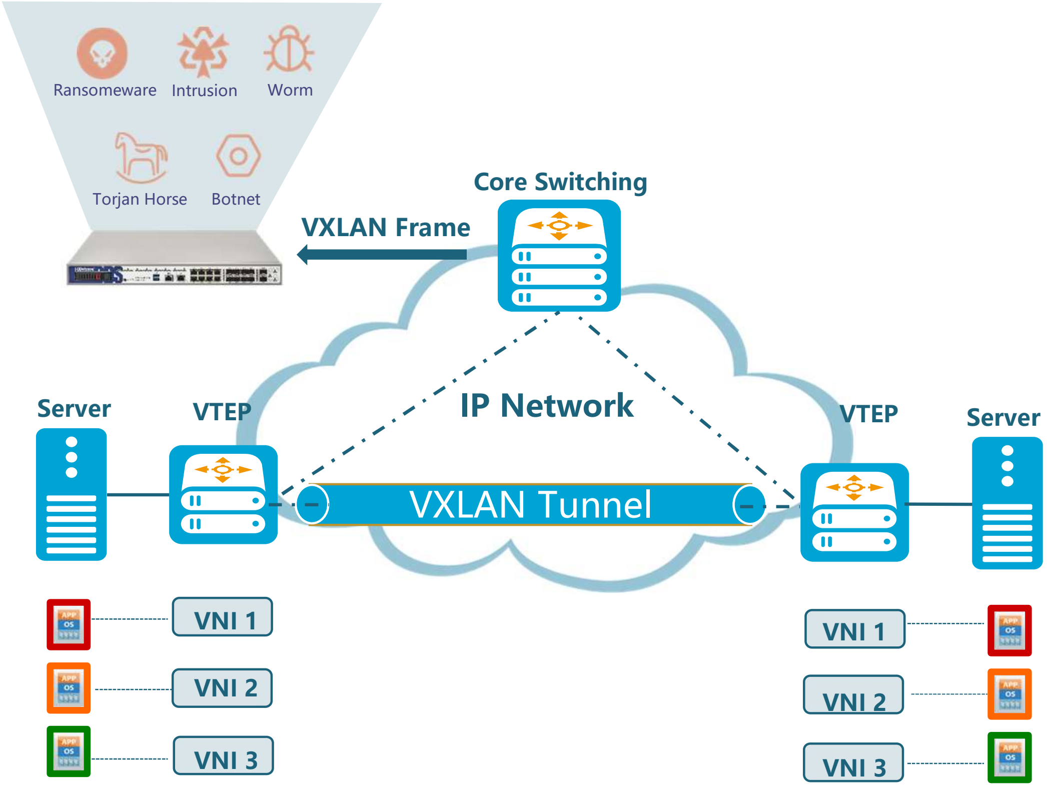
DDoS Attack | Injection Attack | Cross-site Attack

Abnormal HTTP | Special Vulnerability Attack

Information Leakage | Malicious software

Illegal Access to resources

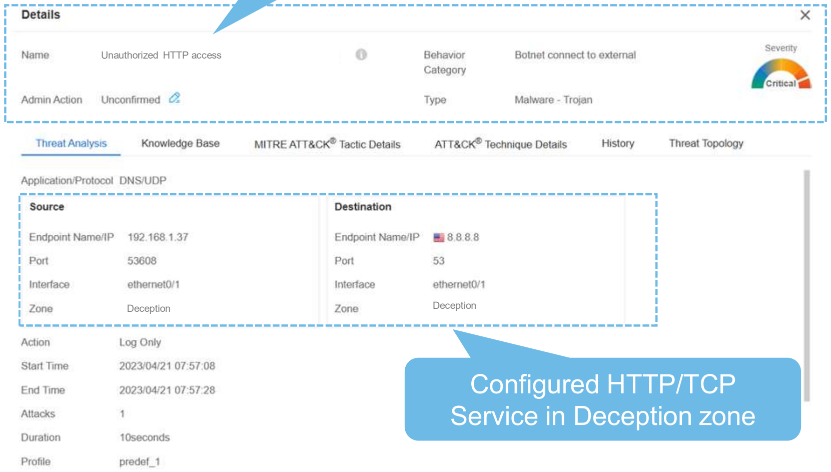
Detection: VxLAN Frame Detection



- Detect VXLAN frame with UDP port 4789 as the destination port
- Do NOT detect non-VXLAN traffic whose destination port is UDP 4789

Detection: Deception Technology

Unauthorized HTTP access detected by Deception engine



Details

Name Unauthorized HTTP access

Behavior Category Botnet connect to external

Severity Critical

Admin Action Unconfirmed

Type Malware - Trojan

Application/Protocol DNS/UDP

Source		Destination	
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	Deception	Zone	Deception

Action Log Only

Start Time 2023/04/21 07:57:08

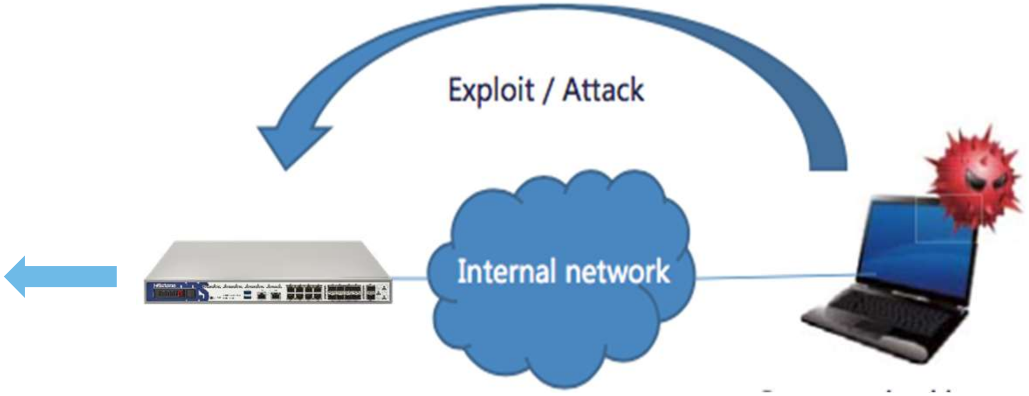
End Time 2023/04/21 07:57:28

Attacks 1

Duration 10seconds

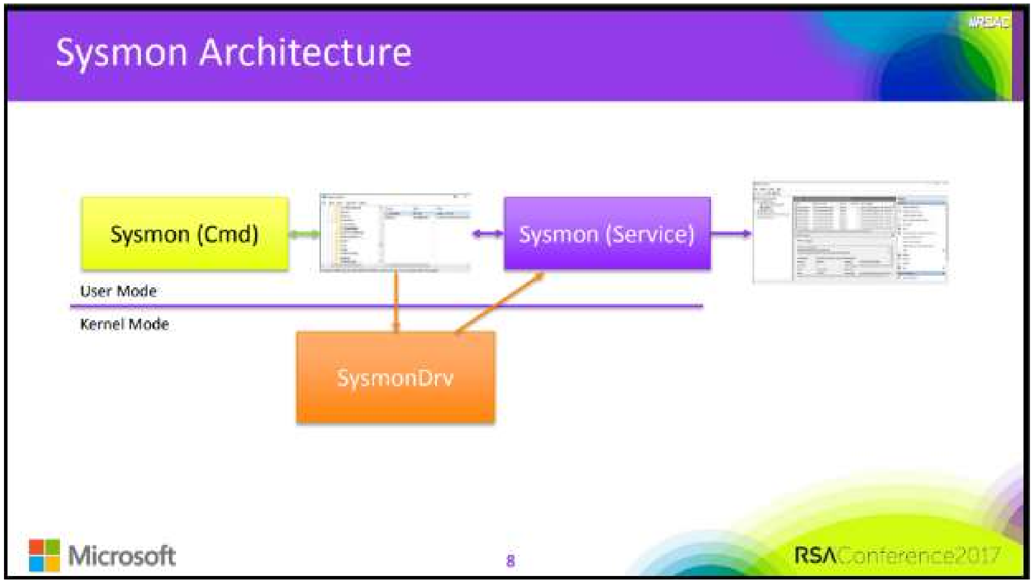
Profile predef_1

Configured HTTP/TCP Service in Deception zone

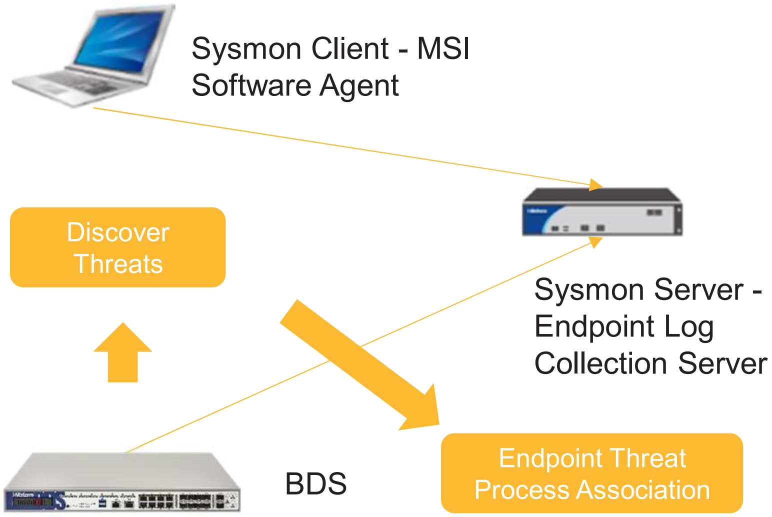


Simulate services in Deception zone, when a hacker visits these services, the attack will be detected

Detection: Sysmon Endpoint Service Integration

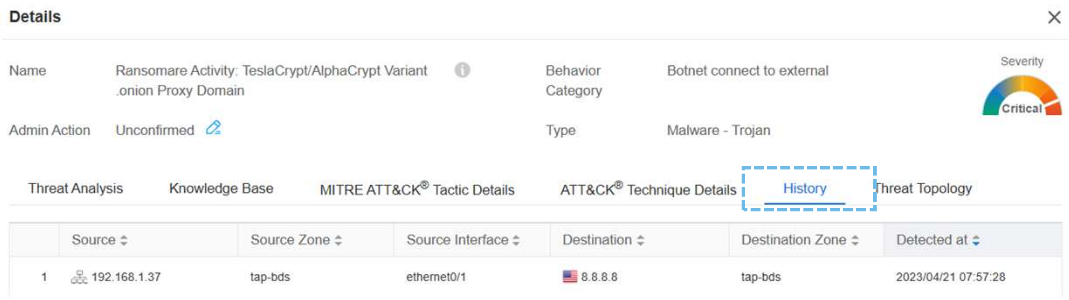


Sysmon Architecture



Sysmon Client - MSI Software Agent
Discover Threats
Sysmon Server - Endpoint Log Collection Server
BDS
Endpoint Threat Process Association

Detection: Detection Efficacy and Lower False Positive



Name: Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain

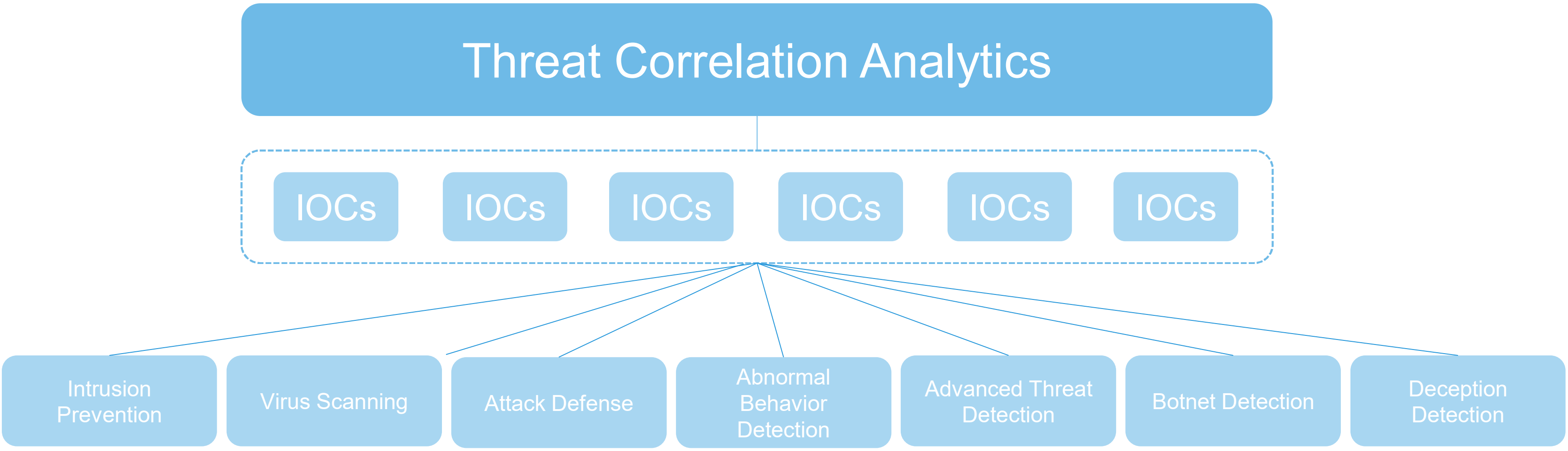
Behavior Category: Botnet connect to external

Admin Action: Unconfirmed

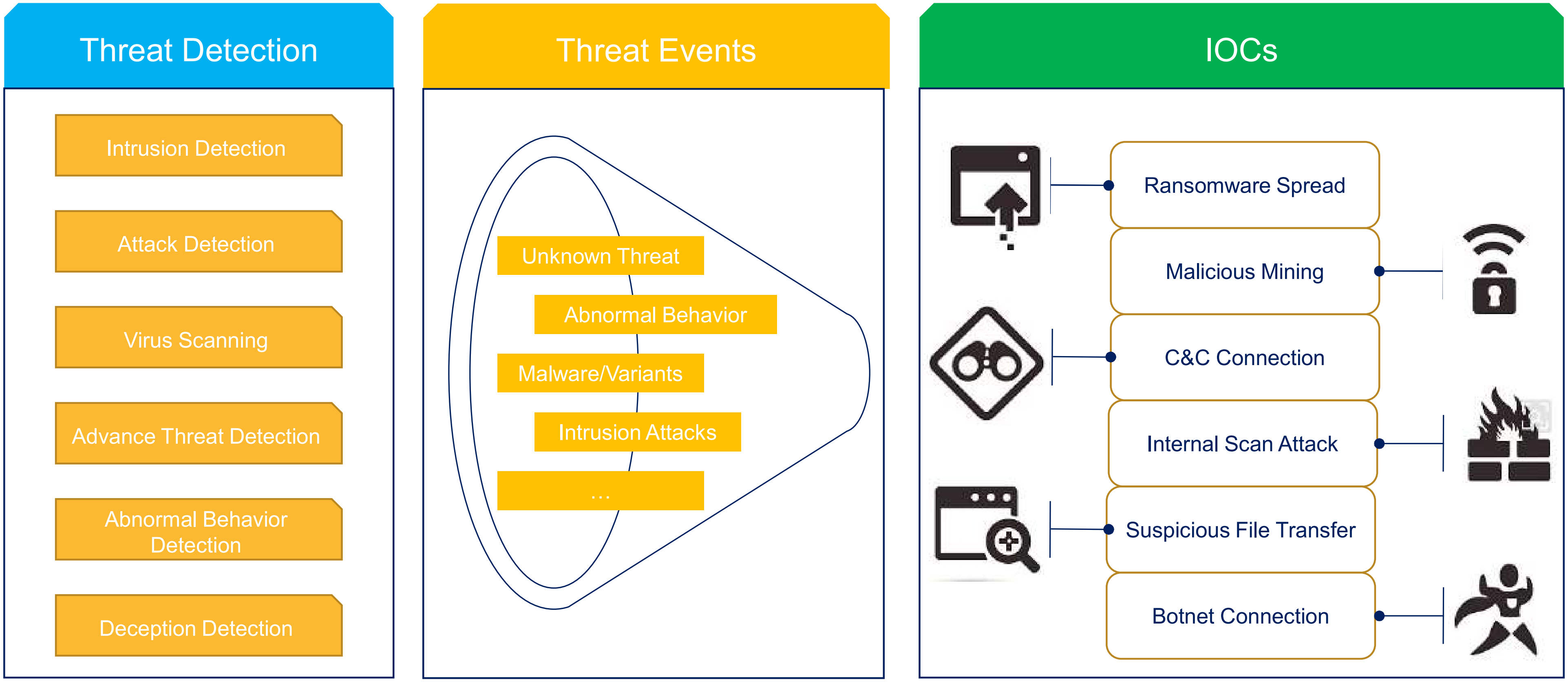
Type: Malware - Trojan

Severity: Critical

	Source	Source Zone	Source Interface	Destination	Destination Zone	Detected at
1	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/21 07:57:28



Visibility: Indicator of Compromises (IOCs) Threats



Threat Detection

- Intrusion Detection
- Attack Detection
- Virus Scanning
- Advance Threat Detection
- Abnormal Behavior Detection
- Deception Detection

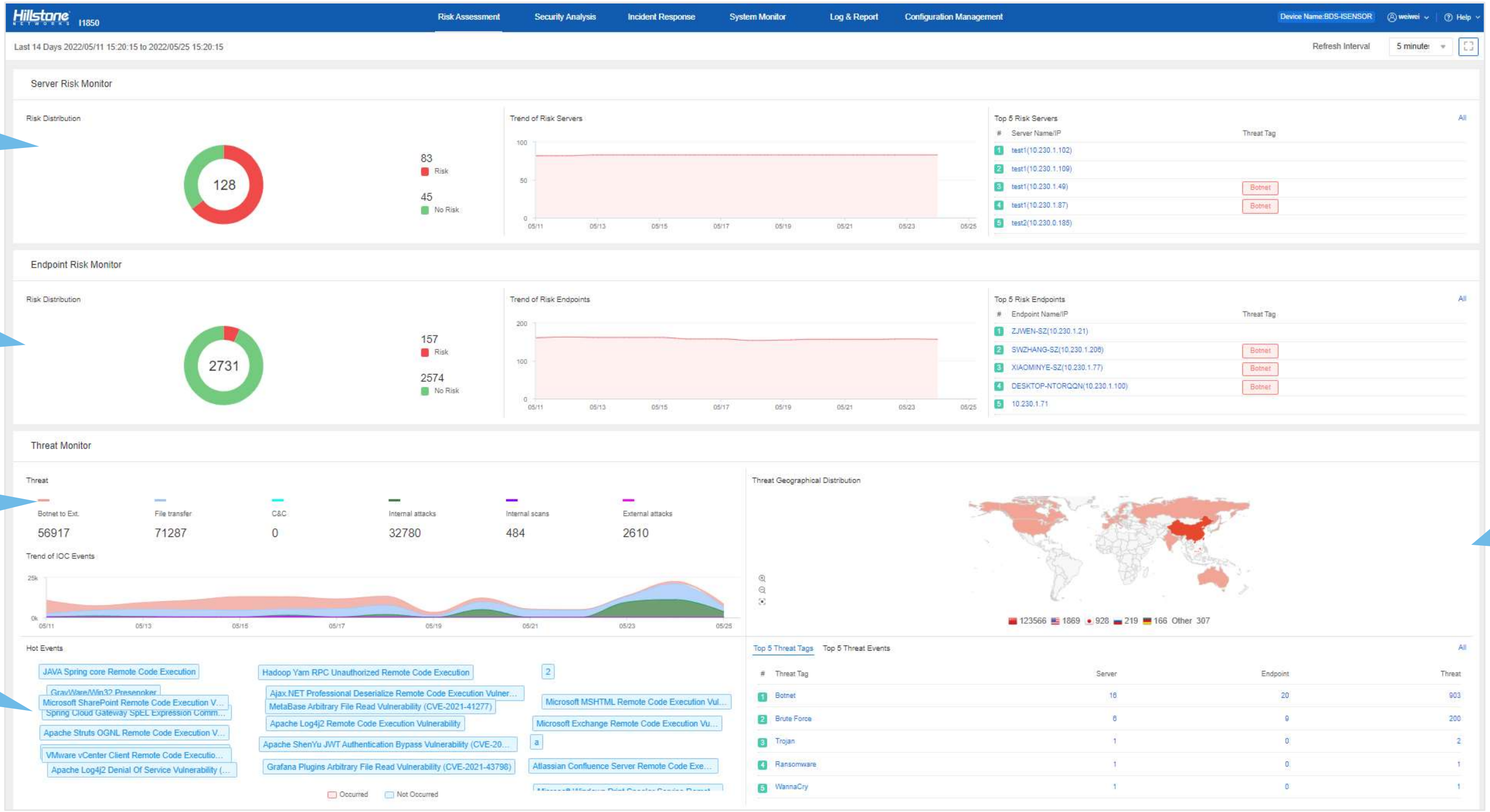
Threat Events

- Unknown Threat
- Abnormal Behavior
- Malware/Variants
- Intrusion Attacks
- …

IOCs

- Ransomware Spread
- Malicious Mining
- C&C Connection
- Internal Scan Attack
- Suspicious File Transfer
- Botnet Connection

Visibility: Global View of Intranet Threat



Last 14 Days 2022/05/11 15:20:15 to 2022/05/25 15:20:15

Server Risk Monitor

Risk Distribution

128

83 🟥 Risk

45 🟩 No Risk

Trend of Risk Servers

Top 5 Risk Servers

#	Server Name/IP	Threat Tag
1	test1(10.230.1.102)	
2	test1(10.230.1.109)	
3	test1(10.230.1.49)	Botnet
4	test1(10.230.1.87)	Botnet
5	test2(10.230.0.185)	

Endpoint Risk Monitor

Risk Distribution

2731

157 🟥 Risk

2574 🟩 No Risk

Trend of Risk Endpoints

Top 5 Risk Endpoints

#	Endpoint Name/IP	Threat Tag
1	ZJWEN-SZ(10.230.1.21)	
2	SWZHANG-SZ(10.230.1.206)	Botnet
3	XIAOMINYE-SZ(10.230.1.77)	Botnet
4	DESKTOP-NTORQQN(10.230.1.100)	Botnet
5	10.230.1.71	

Threat Monitor

Threat

Botnet to Ext.	File transfer	C&C	Internal attacks	Internal scans	External attacks
56917	71287	0	32780	484	2610

Trend of IOC Events

Hot Events

JAVA Spring core Remote Code Execution
GrayWare/Win32.Presenoker
Microsoft SharePoint Remote Code Execution V...
Spring Cloud Gateway SpEL Expression Comm...
Apache Struts OGNL Remote Code Execution V...
VMware vCenter Client Remote Code Executio...
Apache Log4j2 Denial Of Service Vulnerability (...
Hadoop Yarn RPC Unauthorized Remote Code Execution
Ajax.NET Professional Deserialize Remote Code Execution Vulner...
MetaBase Arbitrary File Read Vulnerability (CVE-2021-41277)
Apache Log4j2 Remote Code Execution Vulnerability
Apache ShenYu JWT Authentication Bypass Vulnerability (CVE-20...
Grafana Plugins Arbitrary File Read Vulnerability (CVE-2021-43798)
2
Microsoft MSHTML Remote Code Execution Vul...
Microsoft Exchange Remote Code Execution Vu...
a
Atlassian Confluence Server Remote Code Exe...

Threat Geographical Distribution

123566 1869 928 219 166 Other 307

Top 5 Threat Tags | Top 5 Threat Events

#	Threat Tag	Server	Endpoint	Threat
1	Botnet	16	20	903
2	Brute Force	6	9	200
3	Trojan	1	0	2
4	Ransomware	1	0	1
5	WannaCry	1	0	1

Overview of Critical Servers and risk level

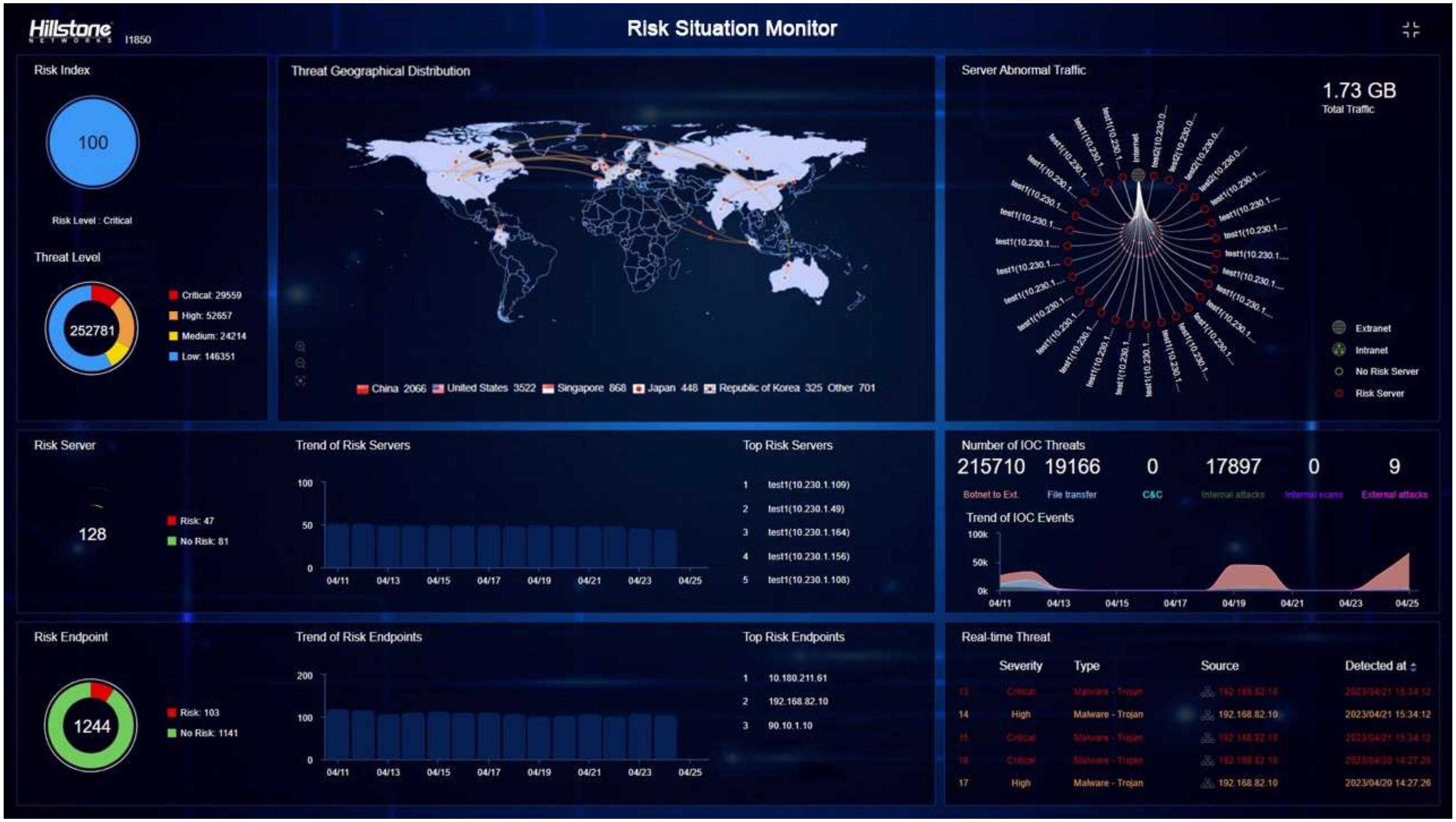
Overview of internal host and risk level

Threat type, statistic, historical distribution etc.

Hot events that need attention

Geo-location threat distribution and top threat

Visibility: Intranet Risk Monitoring Projection



Risk Situation Monitor

Top Risk Servers

1 test1(10.230.1.109)
2 test1(10.230.1.49)
3 test1(10.230.1.164)
4 test1(10.230.1.156)
5 test1(10.230.1.108)

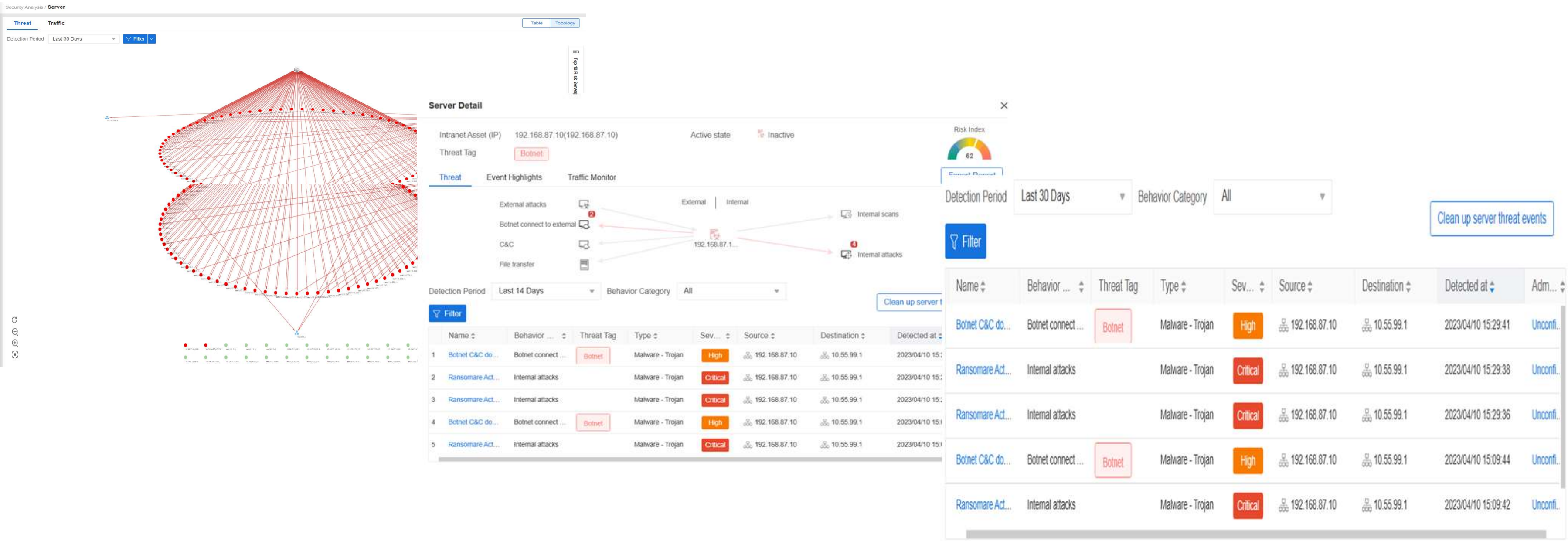
Top Risk Endpoints

1 10.180.211.61
2 192.168.82.10
3 90.10.1.10

Real-time Threat

	Severity	Type	Source	Detected at ⇕
13	Critical	Malware - Trojan	192.168.82.10	2023/04/21 15:34:12
14	High	Malware - Trojan	192.168.82.10	2023/04/21 15:34:12
15	Critical	Malware - Trojan	192.168.82.10	2023/04/21 15:34:12
16	Critical	Malware - Trojan	192.168.82.10	2023/04/20 14:27:26
17	High	Malware - Trojan	192.168.82.10	2023/04/20 14:27:26

Visibility: Server Threat Monitoring



Security Analysis / **Server**

Server Detail

Intranet Asset (IP) 192.168.87.10(192.168.87.10)

Active state: Inactive

Threat Tag: Botnet

Detection Period: Last 14 Days

Behavior Category: All

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

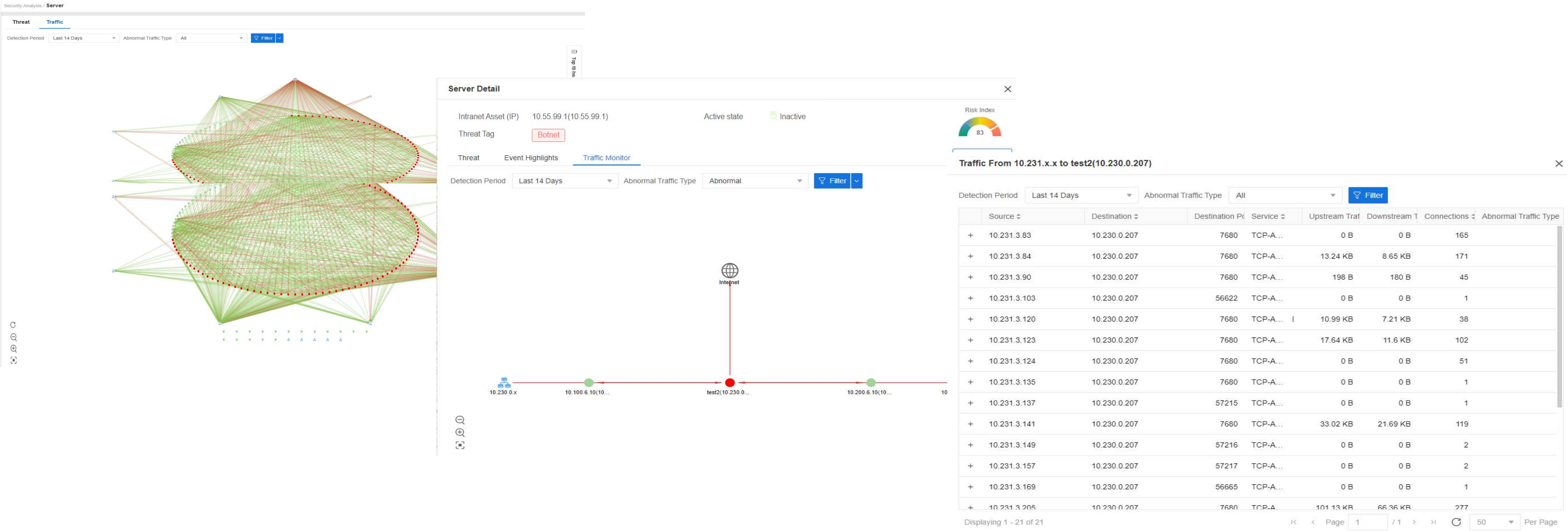
Detection Period: Last 30 Days

Behavior Category: All

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

- Server threat topology for intranet servers: attack direction, severity, relationships
- Threat analysis for individual server: 6 types of attack chain
- Threat events list

Visibility: Server Traffic Monitoring



Detection Period: Last 14 Days Abnormal Traffic Type: All

Server Detail

Intranet Asset (IP): 10.55.99.1(10.55.99.1)
Active state: Inactive
Threat Tag: Botnet

Detection Period: Last 14 Days Abnormal Traffic Type: Abnormal

Traffic From 10.231.x.x to test2(10.230.0.207)

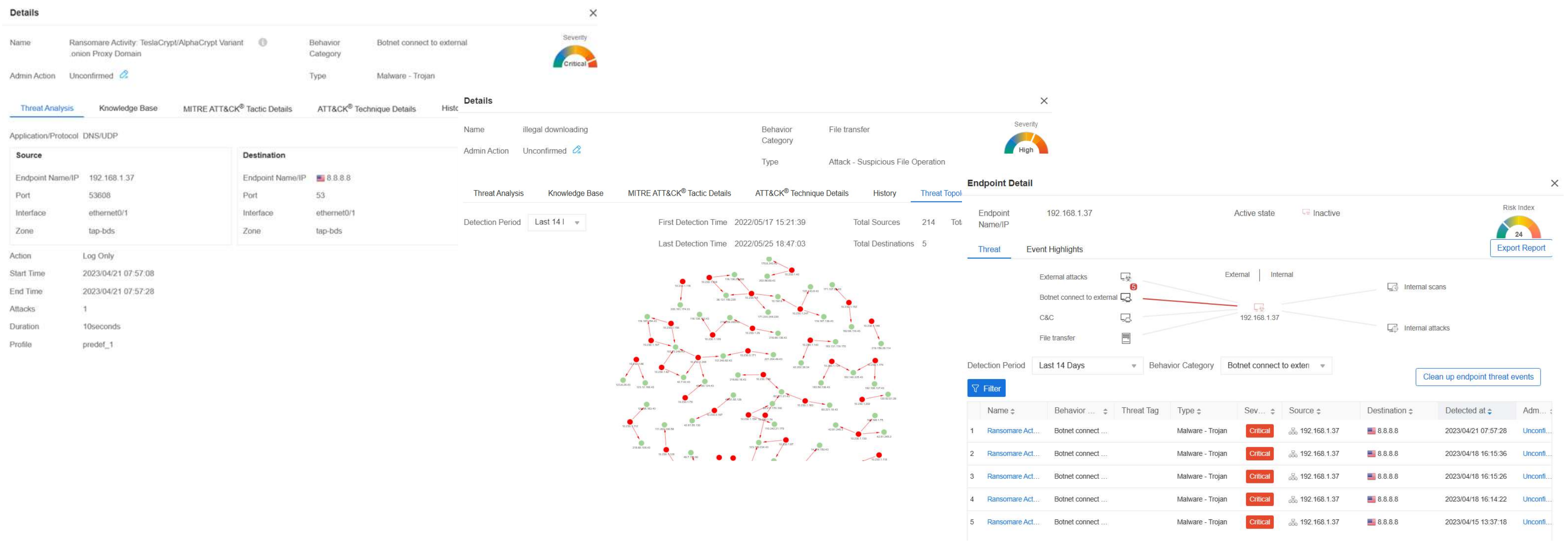
Detection Period: Last 14 Days Abnormal Traffic Type: All

	Source	Destination	Destination Pc	Service	Upstream Traf	Downstream T	Connections	Abnormal Traffic Type
+	10.231.3.83	10.230.0.207	7680	TCP-A...	0 B	0 B	165	
+	10.231.3.84	10.230.0.207	7680	TCP-A...	13.24 KB	8.65 KB	171	
+	10.231.3.90	10.230.0.207	7680	TCP-A...	198 B	180 B	45	
+	10.231.3.103	10.230.0.207	56622	TCP-A...	0 B	0 B	1	
+	10.231.3.120	10.230.0.207	7680	TCP-A...	10.99 KB	7.21 KB	38	
+	10.231.3.123	10.230.0.207	7680	TCP-A...	17.64 KB	11.6 KB	102	
+	10.231.3.124	10.230.0.207	7680	TCP-A...	0 B	0 B	51	
+	10.231.3.135	10.230.0.207	7680	TCP-A...	0 B	0 B	1	
+	10.231.3.137	10.230.0.207	57215	TCP-A...	0 B	0 B	1	
+	10.231.3.141	10.230.0.207	7680	TCP-A...	33.02 KB	21.69 KB	119	
+	10.231.3.149	10.230.0.207	57216	TCP-A...	0 B	0 B	2	
+	10.231.3.157	10.230.0.207	57217	TCP-A...	0 B	0 B	2	
+	10.231.3.169	10.230.0.207	56665	TCP-A...	0 B	0 B	1	
+	10.231.3.205	10.230.0.207	7680	TCP-A	101.13 KB	66.36 KB	277	

Displaying 1 - 21 of 21 Page 1 / 1 50 Per Page

- Server traffic topology for all intranet servers: all traffic relations among all intranet servers
- Server traffic diagram for individual server: traffic in/out of an individual server
- Traffic activity list: all traffic activities between servers

Visibility: Threat Topology



Details

Name: Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain
Behavior Category: Botnet connect to external
Admin Action: Unconfirmed
Type: Malware - Trojan
Severity: Critical

Application/Protocol DNS/UDP

	Source		Destination
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

Action	Log Only
Start Time	2023/04/21 07:57:08
End Time	2023/04/21 07:57:28
Attacks	1
Duration	10seconds
Profile	predef_1

Details

Name: illegal downloading
Behavior Category: File transfer
Admin Action: Unconfirmed
Type: Attack - Suspicious File Operation
Severity: High

Detection Period: Last 14 I
First Detection Time: 2022/05/17 15:21:39
Last Detection Time: 2022/05/25 18:47:03
Total Sources: 214
Total Destinations: 5

Endpoint Detail

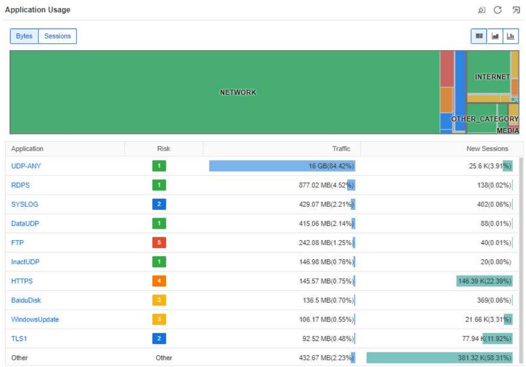
Endpoint Name/IP: 192.168.1.37
Active state: Inactive
Risk Index: 24

Detection Period: Last 14 Days
Behavior Category: Botnet connect to exter

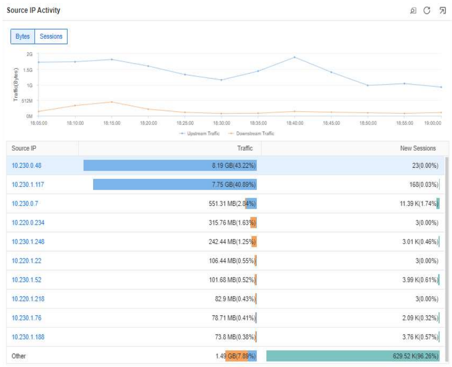
	Name	Behavior ...	Threat Tag	Type	Sev...	Source	Destination	Detected at	Adm...
1	Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/21 07:57:28	Unconfi...
2	Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:15:36	Unconfi...
3	Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:15:26	Unconfi...
4	Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:14:22	Unconfi...
5	Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/15 13:37:18	Unconfi...

- Details of a threat
- Threat topology that shows the interactions between assets involved in this threat event
- View of the detailed activities of a specific IP in this threat topology

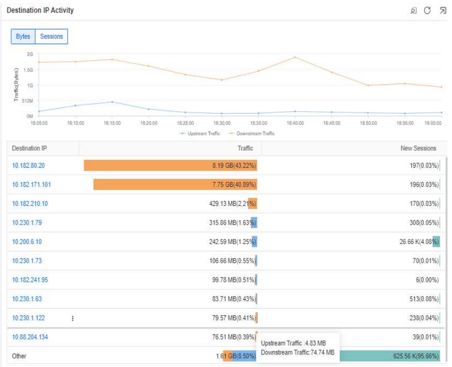
Visibility: Intranet Application Analysis



Application	Risk	Traffic	New Sessions
UDP-ANY	1	16 GB(84.42%)	25.6 K(3.91%)
RDPS	1	877.02 MB(4.52%)	138(0.02%)
SYSLOG	2	429.07 MB(2.21%)	402(0.06%)
DataUDP	1	415.06 MB(2.14%)	88(0.01%)
FTP	5	242.08 MB(1.25%)	40(0.01%)
InactUDP	1	146.98 MB(0.76%)	20(0.00%)
HTTPS	4	145.57 MB(0.75%)	146.39 K(22.39%)
BaiduDisk	3	136.5 MB(0.70%)	369(0.06%)
WindowsUpdate	3	106.17 MB(0.55%)	21.66 K(3.31%)
TLS1	2	92.52 MB(0.48%)	77.94 K(11.92%)
Other	Other	432.67 MB(2.23%)	381.32 K(58.31%)



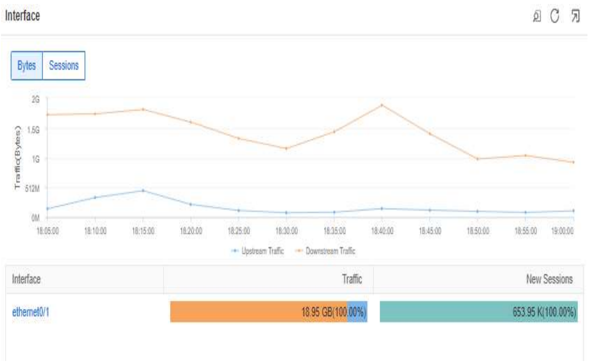
Source IP	Traffic	New Sessions
10.230.0.48	8.19 GB(43.22%)	23(0.00%)
10.230.1.117	7.75 GB(40.89%)	168(0.03%)
10.230.0.7	551.31 MB(2.84%)	11.39 K(1.74%)
10.220.0.234	315.76 MB(1.63%)	3(0.00%)
10.230.1.248	242.44 MB(1.25%)	3.01 K(0.46%)
10.220.1.22	106.44 MB(0.55%)	3(0.00%)
10.230.1.52	101.68 MB(0.52%)	3.99 K(0.61%)
10.220.1.218	82.9 MB(0.43%)	3(0.00%)
10.230.1.76	78.71 MB(0.41%)	2.09 K(0.32%)
10.230.1.188	73.8 MB(0.38%)	3.76 K(0.57%)
Other	1.49 GB(7.89%)	629.52 K(96.26%)



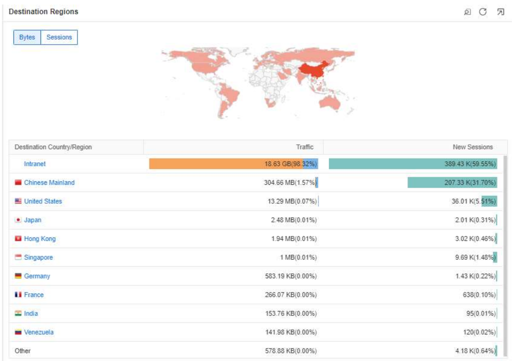
Destination IP	Traffic	New Sessions
10.182.80.20	8.19 GB(43.22%)	197(0.03%)
10.182.171.101	7.75 GB(40.89%)	196(0.03%)
10.182.210.10	429.13 MB(2.21%)	170(0.03%)
10.230.1.79	315.86 MB(1.63%)	308(0.05%)
10.200.6.10	242.59 MB(1.25%)	26.66 K(4.08%)
10.230.1.73	106.66 MB(0.55%)	70(0.01%)
10.182.241.95	99.78 MB(0.51%)	6(0.00%)
10.230.1.63	83.71 MB(0.43%)	513(0.08%)
10.230.1.122	79.57 MB(0.41%)	238(0.04%)
10.88.204.134	76.51 MB(0.39%)	39(0.01%)
Other	1.61 GB(8.50%)	625.56 K(95.66%)

Upstream Traffic :4.83 MB
Downstream Traffic:74.74 MB

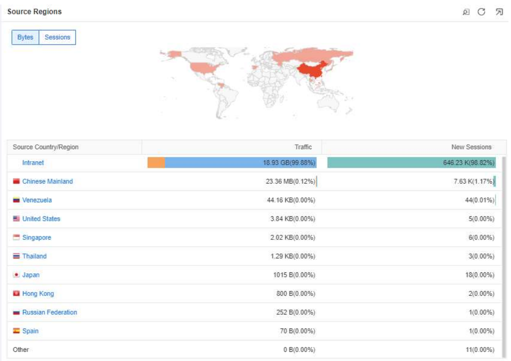
- Application Usage/Ranking
- Source/Destination IP traffic ranking
- Interface Traffic Ranking
- Threat Geo-location



Interface	Traffic	New Sessions
ethernet0/1	18.95 GB(100.00%)	653.95 K(100.00%)

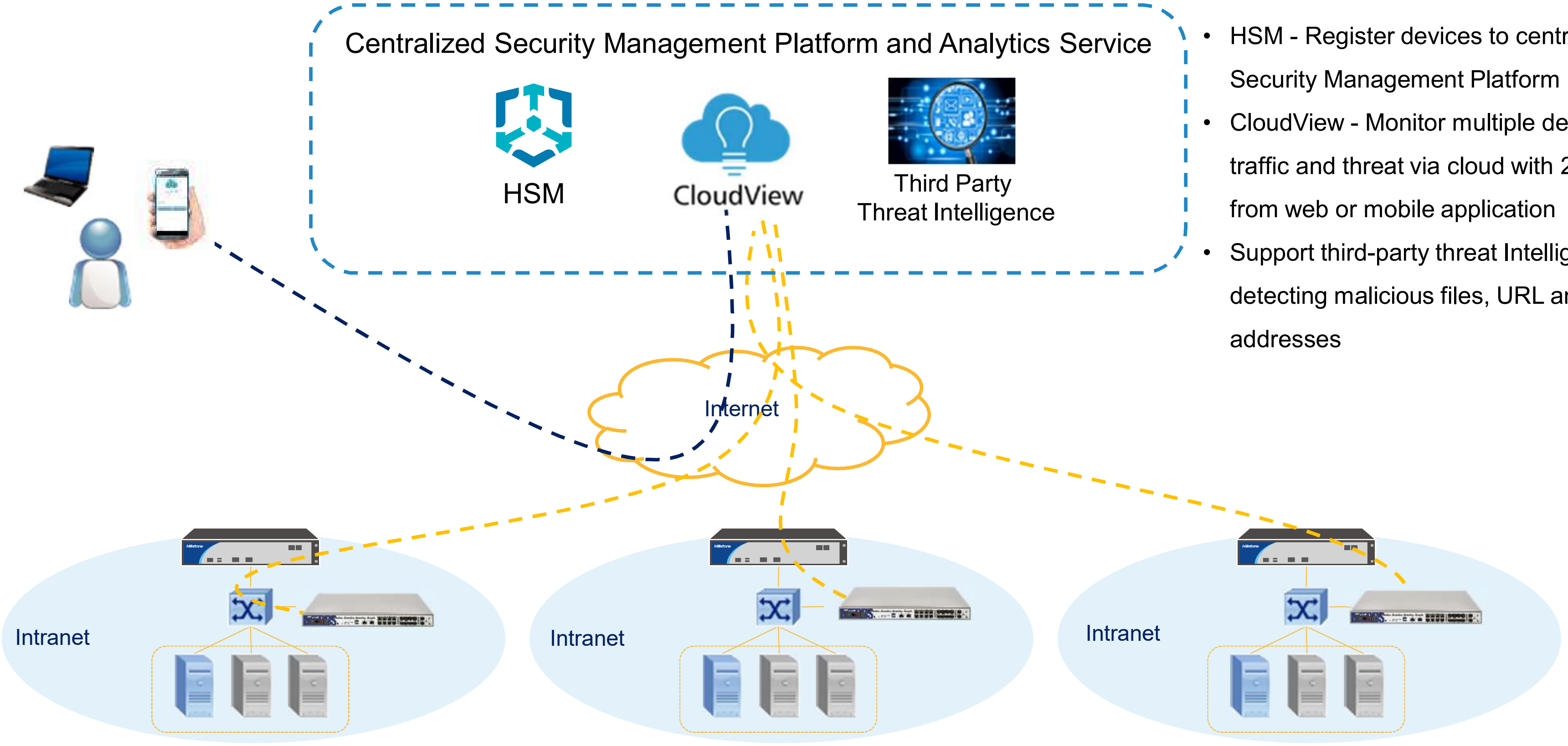


Destination Country/Region	Traffic	New Sessions
Intranet	18.63 GB(98.32%)	389.43 K(59.55%)
Chinese Mainland	304.66 MB(1.57%)	207.33 K(31.70%)
United States	13.29 MB(0.07%)	36.01 K(5.51%)
Japan	2.48 MB(0.01%)	2.01 K(0.31%)
Hong Kong	1.94 MB(0.01%)	3.02 K(0.46%)
Singapore	1 MB(0.01%)	9.69 K(1.48%)
Germany	583.19 KB(0.00%)	1.43 K(0.22%)
France	266.07 KB(0.00%)	638(0.10%)
India	153.76 KB(0.00%)	95(0.01%)
Venezuela	141.98 KB(0.00%)	120(0.02%)
Other	578.88 KB(0.00%)	4.18 K(0.64%)



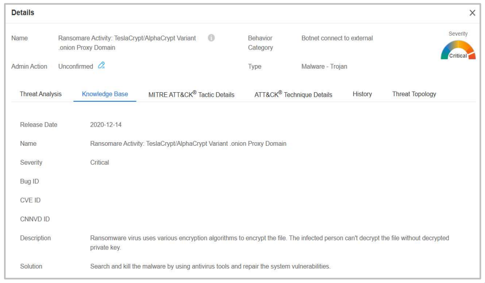
Source Country/Region	Traffic	New Sessions
Intranet	18.93 GB(99.88%)	646.23 K(98.82%)
Chinese Mainland	23.36 MB(0.12%)	7.63 K(1.17%)
Venezuela	44.16 KB(0.00%)	44(0.01%)
United States	3.84 KB(0.00%)	5(0.00%)
Singapore	2.02 KB(0.00%)	6(0.00%)
Thailand	1.29 KB(0.00%)	3(0.00%)
Japan	1015 B(0.00%)	18(0.00%)
Hong Kong	800 B(0.00%)	2(0.00%)
Russian Federation	252 B(0.00%)	1(0.00%)
Spain	70 B(0.00%)	1(0.00%)
Other	0 B(0.00%)	11(0.00%)

Visibility: Centralized Security Management



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

DFIR: Rich Forensics Enables Risk Assessment



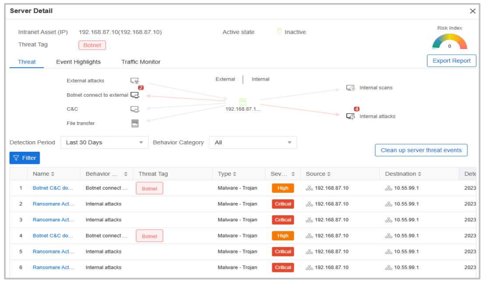
Details

Name	Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain	Behavior Category	Botnet connect to external
Admin Action	Unconfirmed	Type	Malware - Trojan

Severity: Critical

Threat Analysis | **Knowledge Base** | MITRE ATT&CK® Tactic Details | ATT&CK® Technique Details | History | Threat Topology

Release Date	2020-12-14
Name	Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain
Severity	Critical
Bug ID	
CVE ID	
CNNVD ID	
Description	Ransomware virus uses various encryption algorithms to encrypt the file. The infected person can't decrypt the file without decrypted private key.
Solution	Search and kill the malware by using antivirus tools and repair the system vulnerabilities.



Server Detail

Intranet Asset (IP) 192.168.87.10(192.168.87.10) Active state Inactive

Threat Tag Botnet

Risk Index 0

Detection Period: Last 30 Days Behavior Category: All

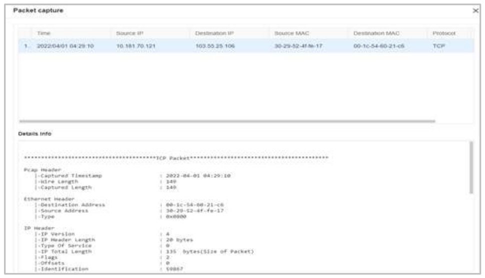
	Name	Behavior ...	Threat Tag	Type	Sev...	Source	Destination	Dete
1	Botnet C&C do...	Botnet connect ...	Botnet	Malware - Trojan	High	192.168.87.10	10.55.99.1	2023
2	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023
3	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023
4	Botnet C&C do...	Botnet connect ...	Botnet	Malware - Trojan	High	192.168.87.10	10.55.99.1	2023
5	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023
6	Ransomare Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023

Restore the Attack Chain and Mapping to MITRE ATT&CK

Knowledge Base

Threat Analysis

PCAP Forensic



Packet capture

	Time	Source IP	Destination IP	Source MAC	Destination MAC	Protocol
1.	2022/04/01 04:29:10	10.181.70.121	103.55.25.106	30-29-52-4f-fe-17	00-1c-54-60-21-c6	TCP

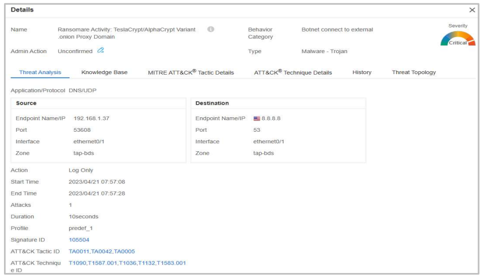
Details Info

```
***************************************TCP Packet*****************************************

Pcap Header
    |-Captured Timestamp              : 2022-04-01 04:29:10
    |-Wire Length                     : 149
    |-Captured Length                 : 149

Ethernet Header
    |-Destination Address             : 00-1c-54-60-21-c6
    |-Source Address                  : 30-29-52-4f-fe-17
    |-Type                            : 0x0800

IP Header
    |-IP Version                      : 4
    |-IP Header Length                : 20 bytes
    |-Type Of Service                 : 0
    |-IP Total Length                 : 135  bytes(Size of Packet)
    |-Flags                           : 2
    |-Offsets                         : 0
    |-Identification                  : 59867
```



Details

Name	Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain	Behavior Category	Botnet connect to external
Admin Action	Unconfirmed	Type	Malware - Trojan

Severity: Critical

Threat Analysis | Knowledge Base | MITRE ATT&CK® Tactic Details | ATT&CK® Technique Details | History | Threat Topology

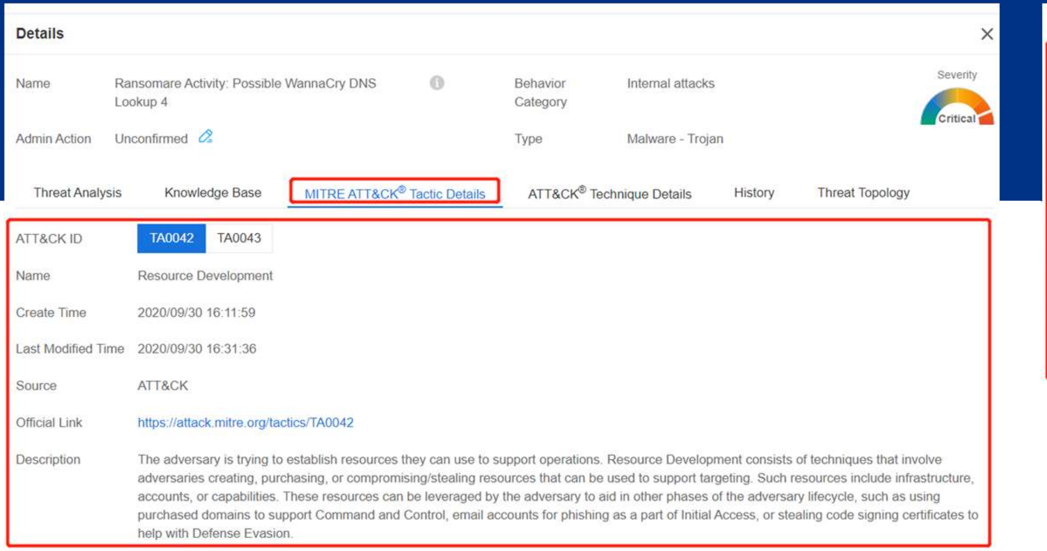
Application/Protocol DNS/UDP

Source		Destination	
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

Action	Log Only
Start Time	2023/04/21 07:57:08
End Time	2023/04/21 07:57:28
Attacks	1
Duration	10seconds
Profile	predef_1
Signature ID	105504
ATT&CK Tactic ID	TA0011,TA0042,TA0005
ATT&CK Technique ID	T1090,T1587.001,T1036,T1132,T1583.001

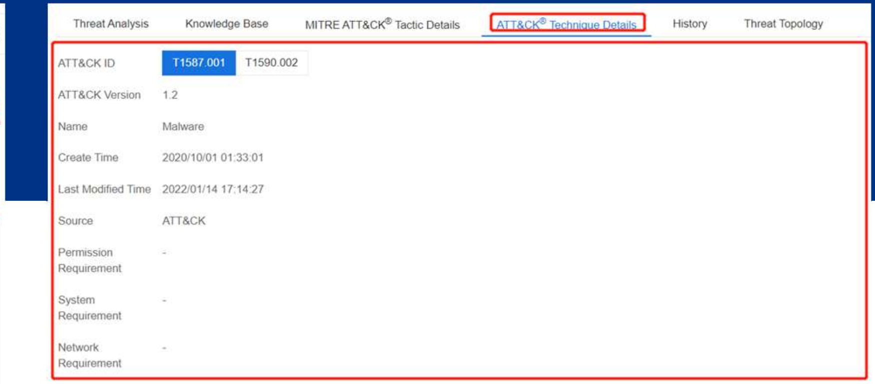
DFIR: MITRE ATT&CK Framework Mapping

MITRE ATT&CK® Stands for Adversarial Tactics, Techniques, and Common Knowledge, is a globally recognized framework developed by the MITRE Corporation to classify and describe the potential threat behaviors.



Name	Ransomare Activity: Possible WannaCry DNS Lookup 4	Behavior Category	Internal attacks
Admin Action	Unconfirmed	Type	Malware - Trojan

ATT&CK ID	TA0042 TA0043
Name	Resource Development
Create Time	2020/09/30 16:11:59
Last Modified Time	2020/09/30 16:31:36
Source	ATT&CK
Official Link	https://attack.mitre.org/tactics/TA0042
Description	The adversary is trying to establish resources they can use to support operations. Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

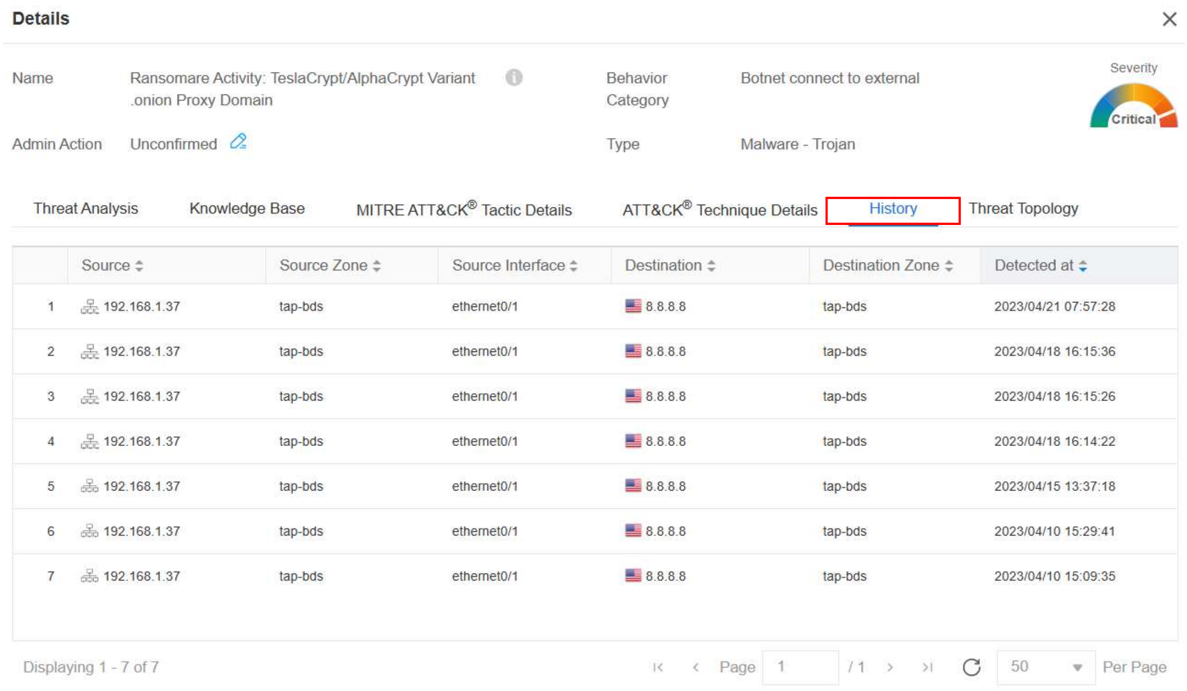


ATT&CK ID	T1587.001 T1590.002
ATT&CK Version	1.2
Name	Malware
Create Time	2020/10/01 01:33:01
Last Modified Time	2022/01/14 17:14:27
Source	ATT&CK
Permission Requirement	-
System Requirement	-
Network Requirement	-

- ATT&CK technique details of threat events

- ATT&CK tactic details of threat events

DFIR: Threat Behavior Details



Details

Name: Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain

Behavior Category: Botnet connect to external

Admin Action: Unconfirmed

Type: Malware - Trojan

Severity: Critical

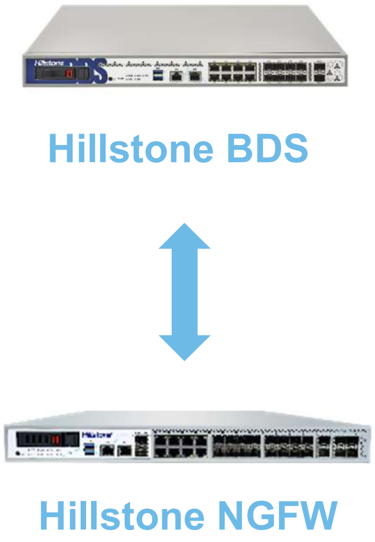
	Source	Source Zone	Source Interface	Destination	Destination Zone	Detected at
1	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/21 07:57:28
2	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/18 16:15:36
3	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/18 16:15:26
4	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/18 16:14:22
5	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/15 13:37:18
6	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/10 15:29:41
7	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/10 15:09:35

Displaying 1 - 7 of 7

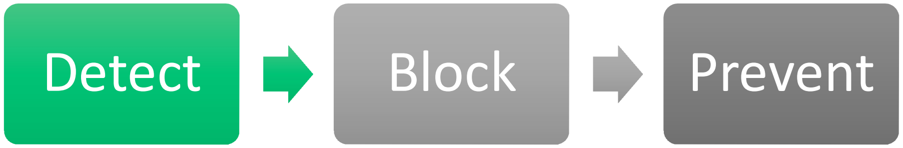
Information tracking for threat events:

- IP, port scanning
- Brute-force cracking of common services such as FTP, LDAP, and MySQL
- Abnormal HTTP access response
- C&C connection

Mitigation: Mitigate/Block Attacks in Conjunction with NGFWs

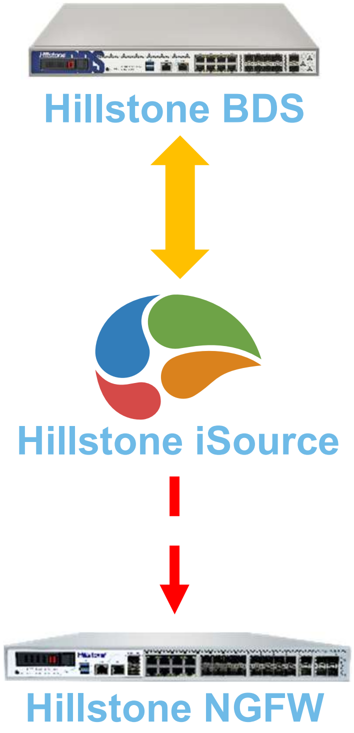


- Detect and identify threat
- Configure Linkage with Hillstone Firewall
- Add the confirmed attacks to Block list


Detect
Block
Prevent

- Linked with Hillstone BDS
- Synchronize Block list from Hillstone BDS
- Block the attacks

Mitigation: Detect and Respond to Threats and Attacks with Integration of iSource



Hillstone BDS

Hillstone iSource

Hillstone NGFW

Data Collection

Detection and Analysis

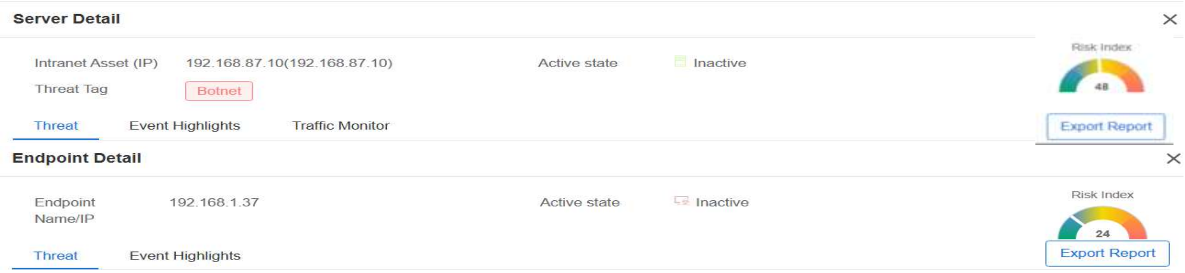
Response

Under the scenario of integrating with iSource:

- BDS uploads data* (threat log/ evidential packets/ metadata/ netflow) to iSource
- BDS can perform active assets scanning task delivered by iSource, and uploads the results to iSource
- Support various types of detection and analysis for advance threats and attacks, including signature based detection, correlation analysis, NTA, etc.
- Provide full visibility and automated response to the integrated security products like NGFWs

*Note: Threat log, metadata, and netflow can be uploaded to iSouce V2.0R4-R8; Threat log, evidential packets, and netflow can be uploaded to iSource V2.0R9 or later

Report: Host Risk Assessment



Server Detail

Intranet Asset (IP) 192.168.87.10(192.168.87.10)

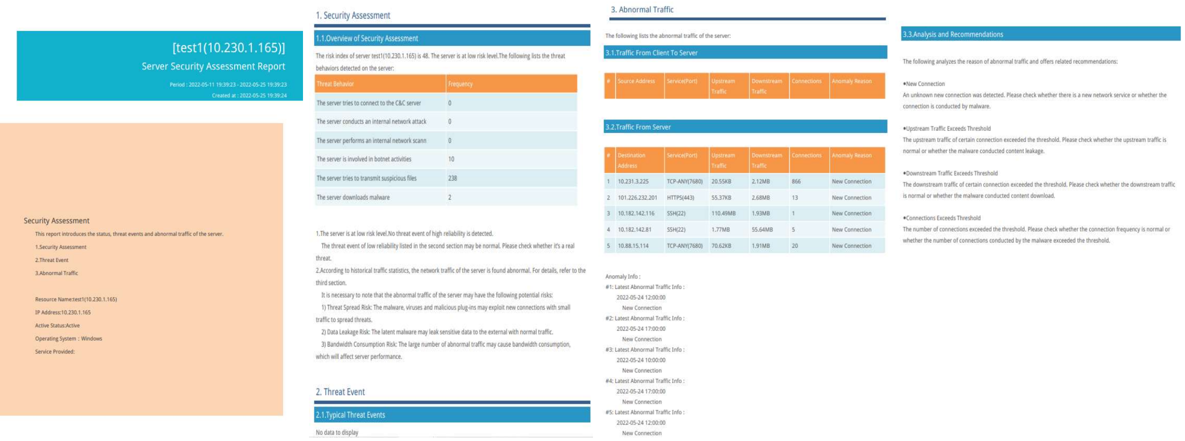
Active state: Inactive

Threat Tag: Botnet

Endpoint Detail

Endpoint Name/IP 192.168.1.37

Active state: Inactive



[test1(10.230.1.165)]

Server Security Assessment Report

Period : 2022-05-11 19:39:23 - 2022-05-25 19:39:23

Created at : 2022-05-25 19:39:24

Security Assessment

This report introduces the status, threat events and abnormal traffic of the server.

1.Security Assessment

2.Threat Event

3.Abnormal Traffic

Resource Name:test1(10.230.1.165)

IP Address:10.230.1.165

Active Status:Active

Operating System：Windows

Service Provided:

1. Security Assessment

1.1.Overview of Security Assessment

The risk index of server test1(10.230.1.165) is 48. The server is at low risk level.The following lists the threat behaviors detected on the server:

Threat Behavior	Frequency
The server tries to connect to the C&C server	0
The server conducts an internal network attack	0
The server performs an internal network scann	0
The server is involved in botnet activities	10
The server tries to transmit suspicious files	238
The server downloads malware	2

1.The server is at low risk level.No threat event of high reliability is detected.

The threat event of low reliability listed in the second section may be normal. Please check whether it's a real threat.

2.According to historical traffic statistics, the network traffic of the server is found abnormal. For details, refer to the third section.

It is necessary to note that the abnormal traffic of the server may have the following potential risks:

1) Threat Spread Risk: The malware, viruses and malicious plug-ins may exploit new connections with small traffic to spread threats.

2) Data Leakage Risk: The latent malware may leak sensitive data to the external with normal traffic.

3) Bandwidth Consumption Risk: The large number of abnormal traffic may cause bandwidth consumption, which will affect server performance.

2. Threat Event

2.1.Typical Threat Events

No data to display

3. Abnormal Traffic

The following lists the abnormal traffic of the server:

3.1.Traffic From Client To Server

#	Source Address	Service(Port)	Upstream Traffic	Downstream Traffic	Connections	Anomaly Reason

3.2.Traffic From Server

#	Destination Address	Service(Port)	Upstream Traffic	Downstream Traffic	Connections	Anomaly Reason
1	10.231.3.225	TCP-ANY(7680)	20.55KB	2.12MB	866	New Connection
2	101.226.232.201	HTTPS(443)	55.37KB	2.68MB	13	New Connection
3	10.182.142.116	SSH(22)	110.49MB	1.93MB	1	New Connection
4	10.182.142.81	SSH(22)	1.77MB	55.64MB	5	New Connection
5	10.88.15.114	TCP-ANY(7680)	70.62KB	1.91MB	20	New Connection

Anomaly Info :
#1: Latest Abnormal Traffic Info :
2022-05-24 12:00:00
New Connection
#2: Latest Abnormal Traffic Info :
2022-05-24 17:00:00
New Connection
#3: Latest Abnormal Traffic Info :
2022-05-24 10:00:00
New Connection
#4: Latest Abnormal Traffic Info :
2022-05-24 17:00:00
New Connection
#5: Latest Abnormal Traffic Info :
2022-05-24 12:00:00
New Connection

3.3.Analysis and Recommendations

The following analyzes the reason of abnormal traffic and offers related recommendations:

•New Connection
An unknown new connection was detected. Please check whether there is a new network service or whether the connection is conducted by malware.

•Upstream Traffic Exceeds Threshold
The upstream traffic of certain connection exceeded the threshold. Please check whether the upstream traffic is normal or whether the malware conducted content leakage.

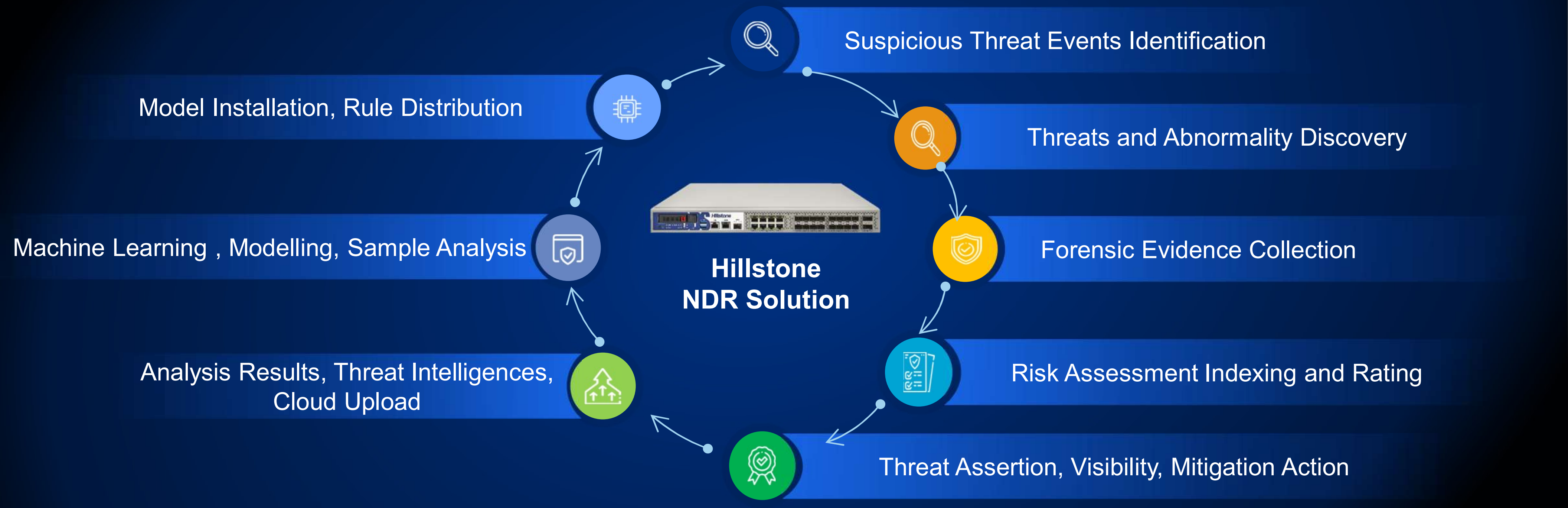
•Downstream Traffic Exceeds Threshold
The downstream traffic of certain connection exceeded the threshold. Please check whether the downstream traffic is normal or whether the malware conducted content download.

•Connections Exceeds Threshold
The number of connections exceeded the threshold. Please check whether the connection frequency is normal or whether the number of connections conducted by the malware exceeded the threshold.

On the risk server or risk endpoint page, the threat and traffic information matching the current interface filtering conditions are exported. A PDF report is generated, which includes the following information:

- Server/endpoint information
- Security status assessment
- Threat event
- Abnormal traffic
- Analytical and disposal recommendations

Closed Cycle: Network Detection and Response



Suspicious Threat Events Identification

Threats and Abnormality Discovery

Forensic Evidence Collection

Risk Assessment Indexing and Rating

Threat Assertion, Visibility, Mitigation Action

Analysis Results, Threat Intelligences, Cloud Upload

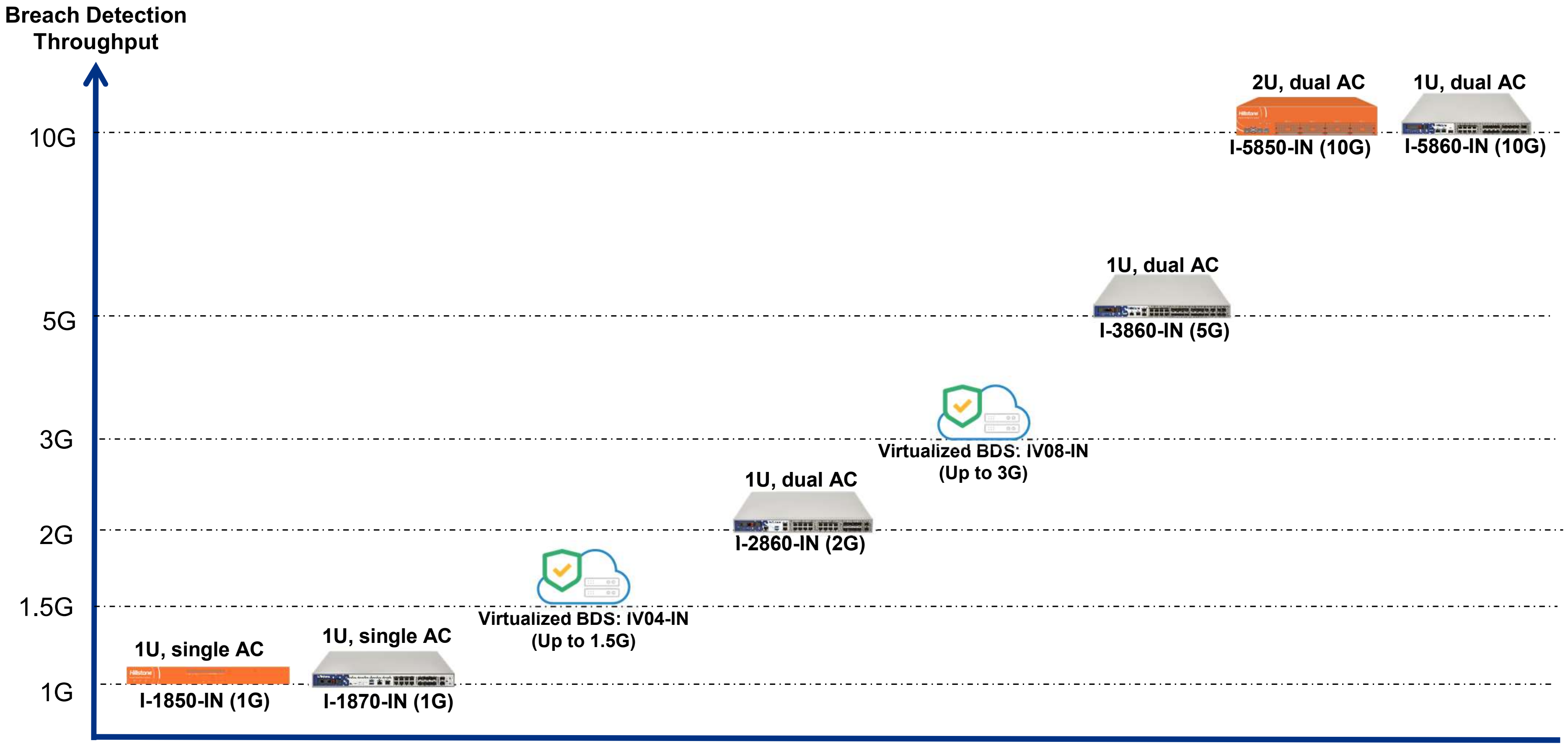
Machine Learning , Modelling, Sample Analysis

Model Installation, Rule Distribution

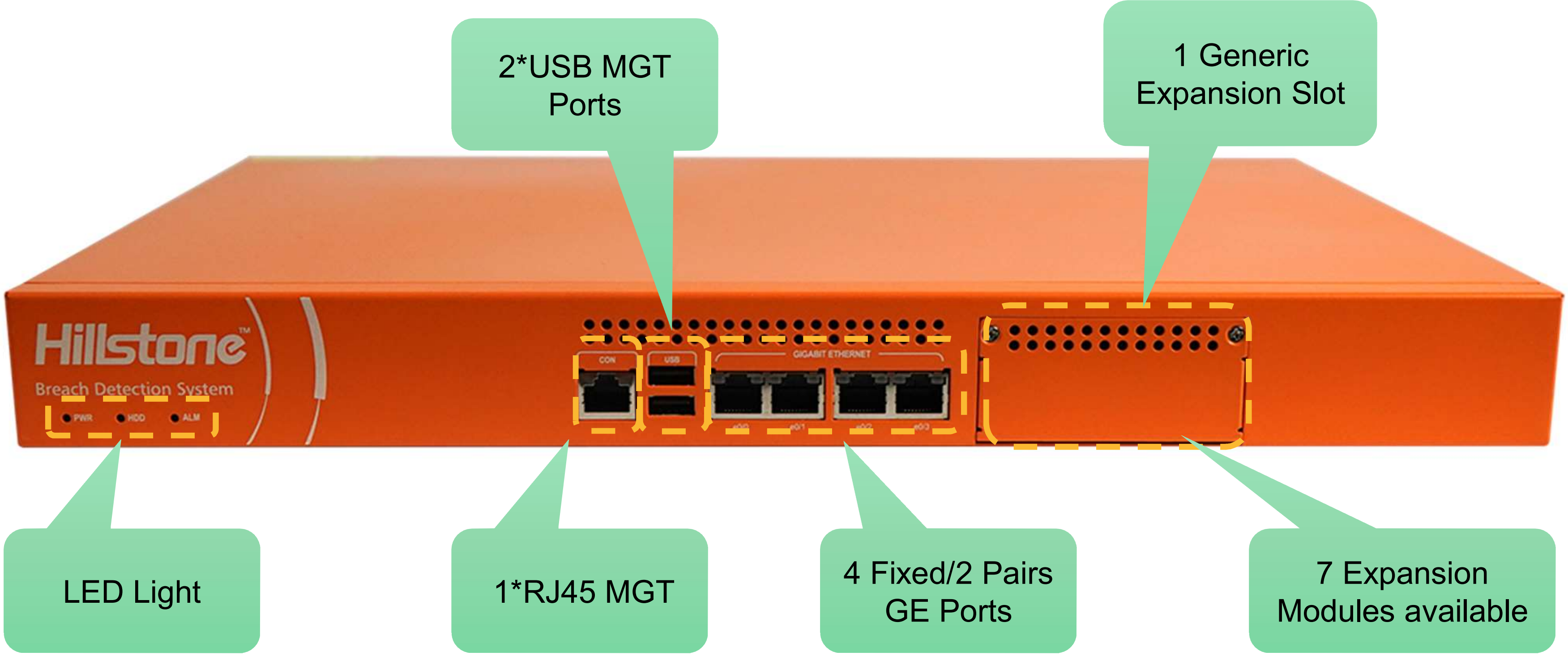
Hillstone NDR Solution

Hillstone BDS Portfolio

BDS Product Portfolio



I-1850 Hardware Specification



2*USB MGT Ports

1 Generic Expansion Slot

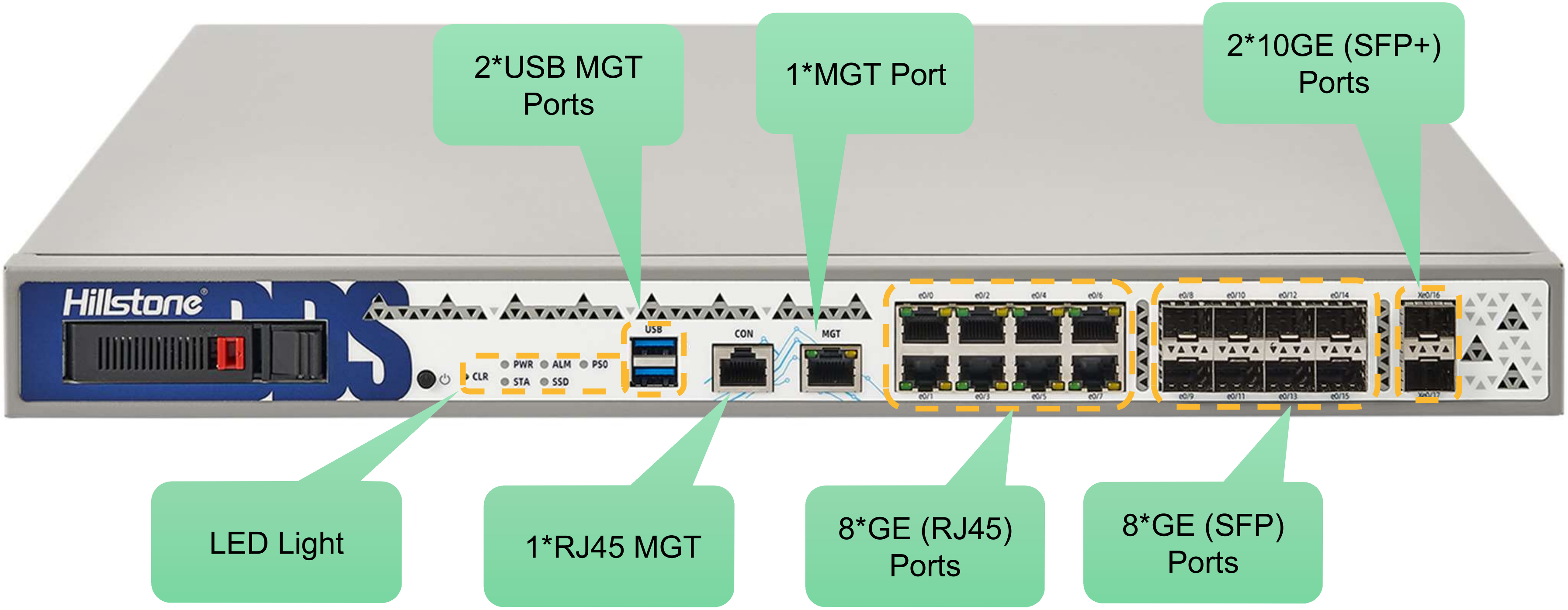
LED Light

1*RJ45 MGT

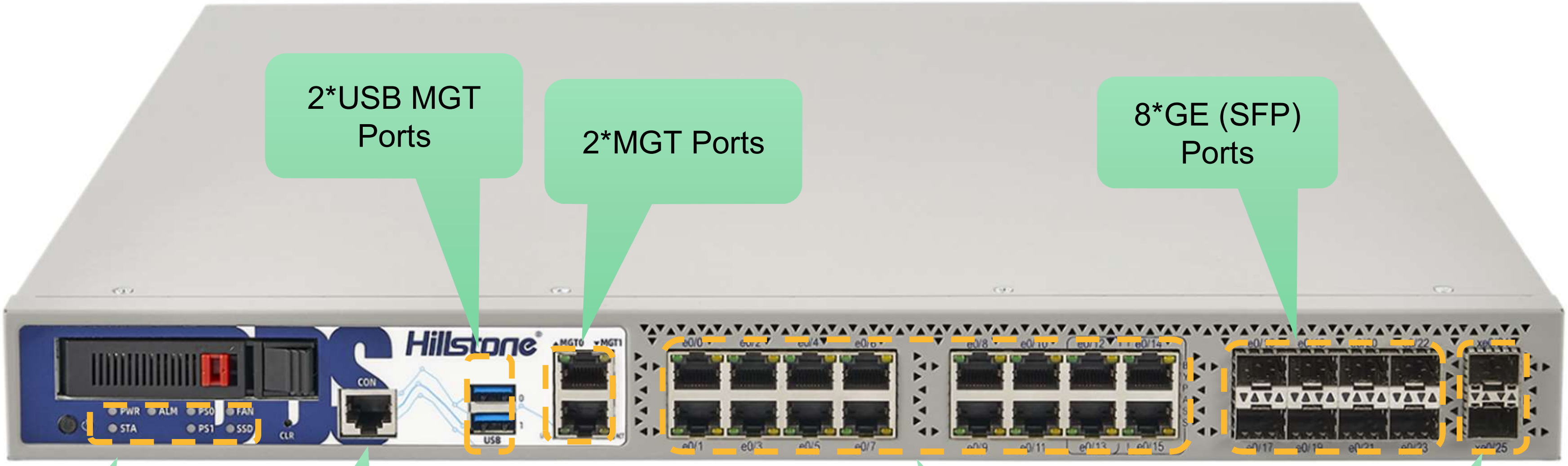
4 Fixed/2 Pairs GE Ports

7 Expansion Modules available

I-1870 Hardware Specification



I-2860 Hardware Specification



2*USB MGT Ports

2*MGT Ports

8*GE (SFP) Ports

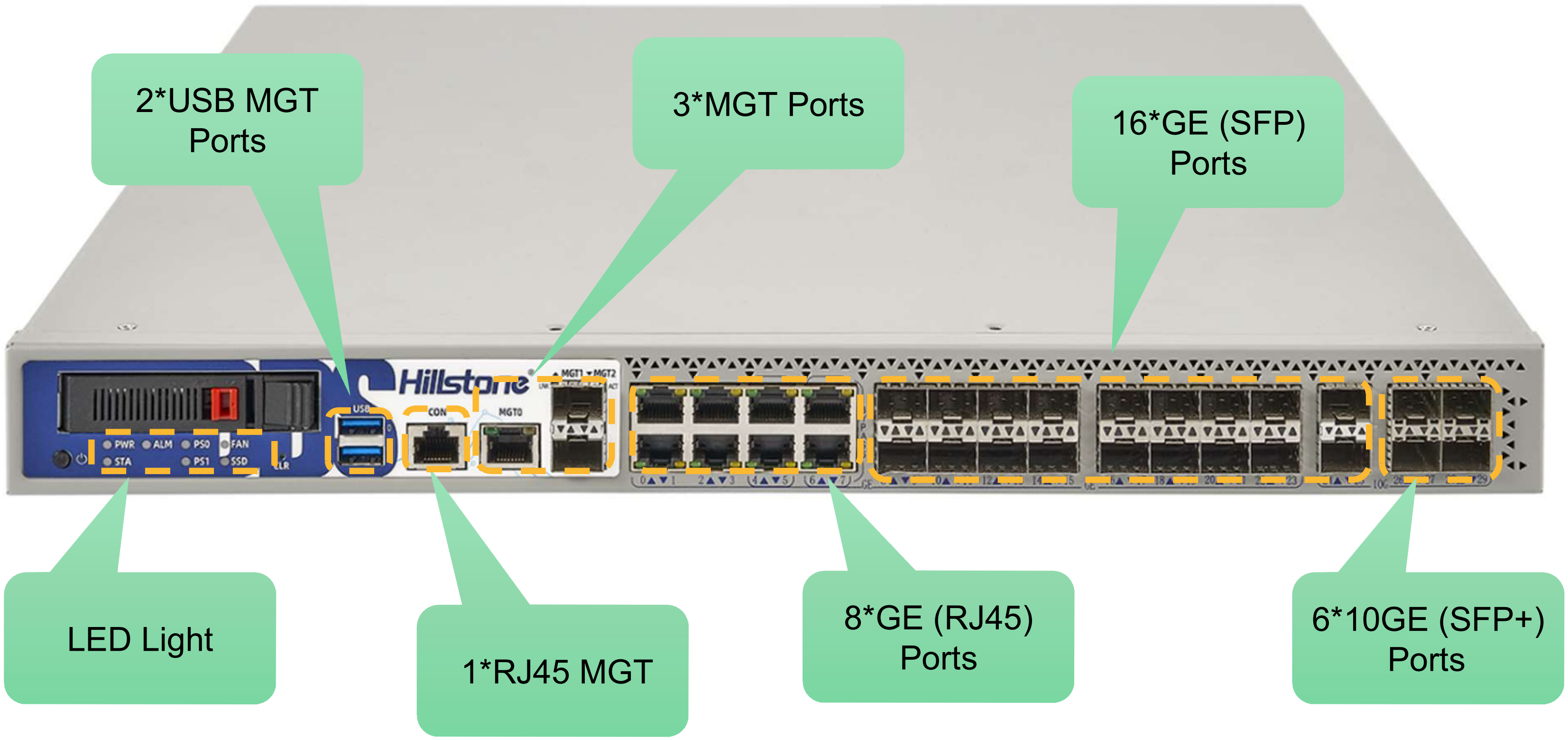
LED Light

1*RJ45 MGT

16*GE (RJ45) Ports

2*10GE (SFP+) Ports

I-3860 Hardware Specification



2*USB MGT Ports

3*MGT Ports

16*GE (SFP) Ports

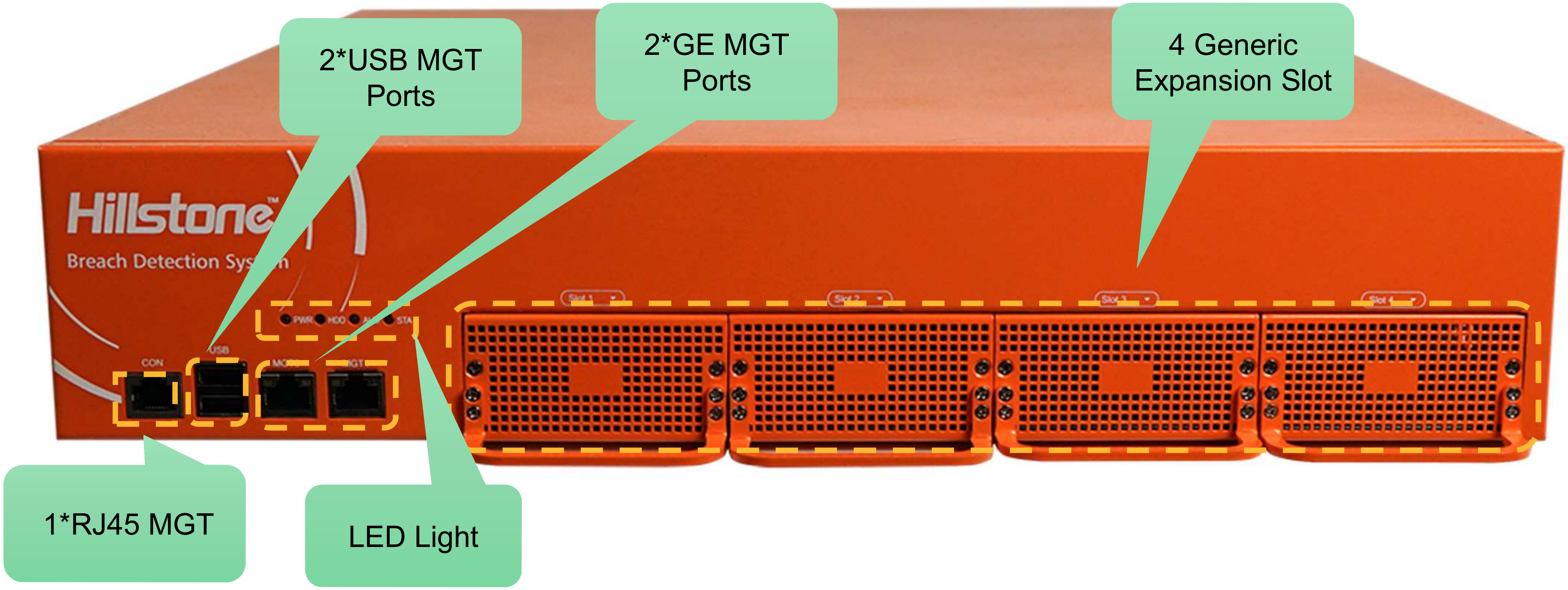
LED Light

1*RJ45 MGT

8*GE (RJ45) Ports

6*10GE (SFP+) Ports

I-5850 Hardware Specification



2*USB MGT Ports

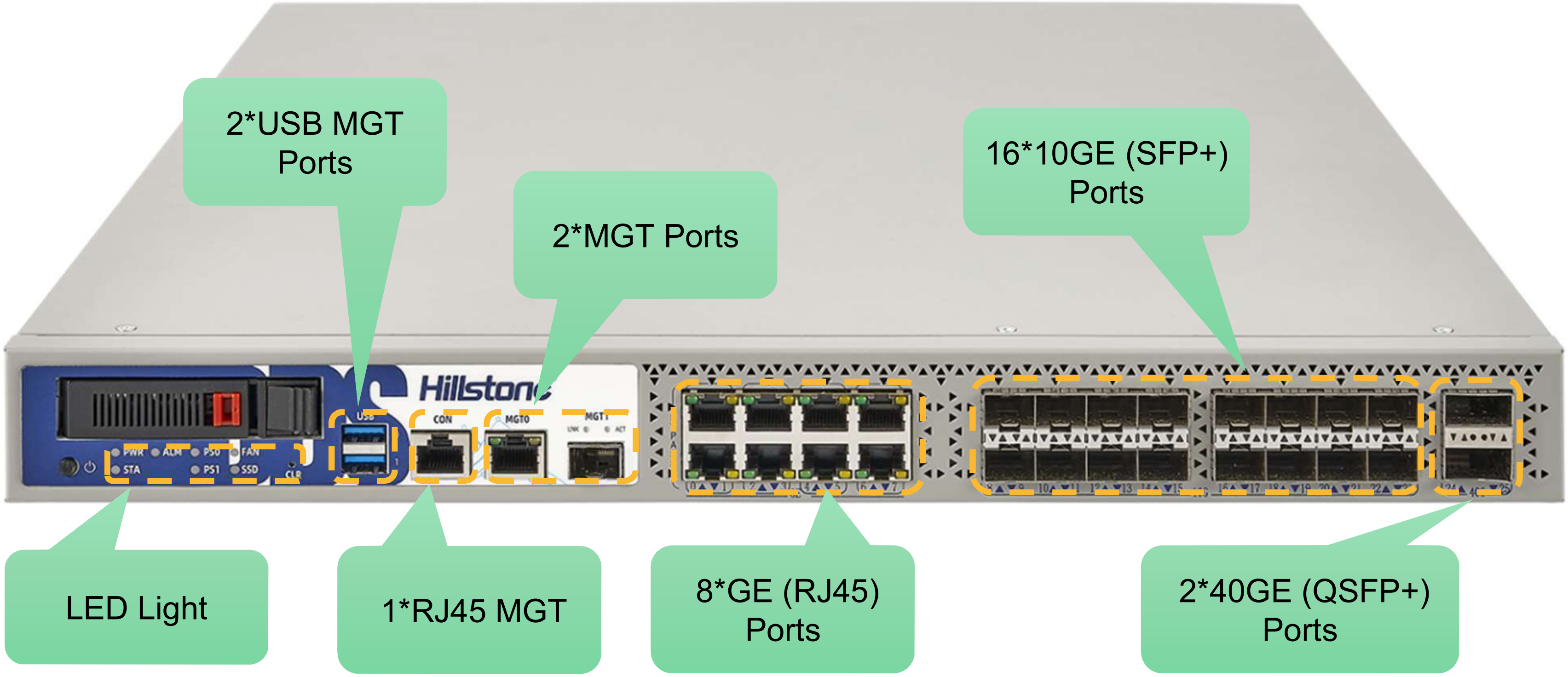
2*GE MGT Ports

4 Generic Expansion Slot

1*RJ45 MGT

LED Light

I-5860 Hardware Specification



2*USB MGT Ports

2*MGT Ports

16*10GE (SFP+) Ports

LED Light

1*RJ45 MGT

8*GE (RJ45) Ports

2*40GE (QSFP+) Ports

BDS Hardware Specification

Model	I-1850-IN	I-1870-IN	I-2860-IN	I-3860-IN	I-5850-IN	I-5860-IN
Breach Detection Throughput	1 Gbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	10 Gbps
New Sessions/s	20,700	32,000	75,000	210,000	250,000	500,000
Maximum Concurrent Sessions	750,000	750,000	1,500,000	3,000,000	6,000,000	6,000,000
Form Factor	1 U	1 U	1 U	1 U	2 U	1 U
Storage	1T HDD	1T SSD	1T SSD	1T SSD	1T HDD	2T 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	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	4 (2 Pairs) GE ports	2×10GE (SFP+) 8 × GE (SFP) 8 × GE (RJ45)	2×10GE (SFP+) 8 × GE (SFP) 16 × GE (RJ45)	6×10GE (SFP+) 16×GE (SFP) 8×GE (RJ45)	N/A	8×GE (RJ45) 16×10GE (SFP+) 2×40GE (QSFP+)
Available Slots for Expansion Modules	1	N/A	1	1	4	1
Expansion Module Option	IOC-S-4SFP-L-IN	N/A	IOC-A-4SFP+-IN	IOC-A-4SFP+-IN	IOC-BDS-8GE-H-IN, IOC-BDS-8SFP-H-IN, IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN

Virtualized BDS Specification & Configuration

Specification and minimum hardware configuration:

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

* The breach detection throughput data is depends on the hardware configuration

Network interface card supported:

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

Expansion Modules

Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN	IOC-BDS-8GE-H-IN	IOC-BDS-8SFP-H-IN	IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN
I/O Ports	4 x SFP Ports	4 x GE Ports	8 x GE Ports	8 x SFP Ports	4 x SFP+ Ports	4 x SFP+, SFP+ module not included
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
Weight	0.22. lb (0.1 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.44 lb (0.2 kg)	2.09 lb (0.96 kg)

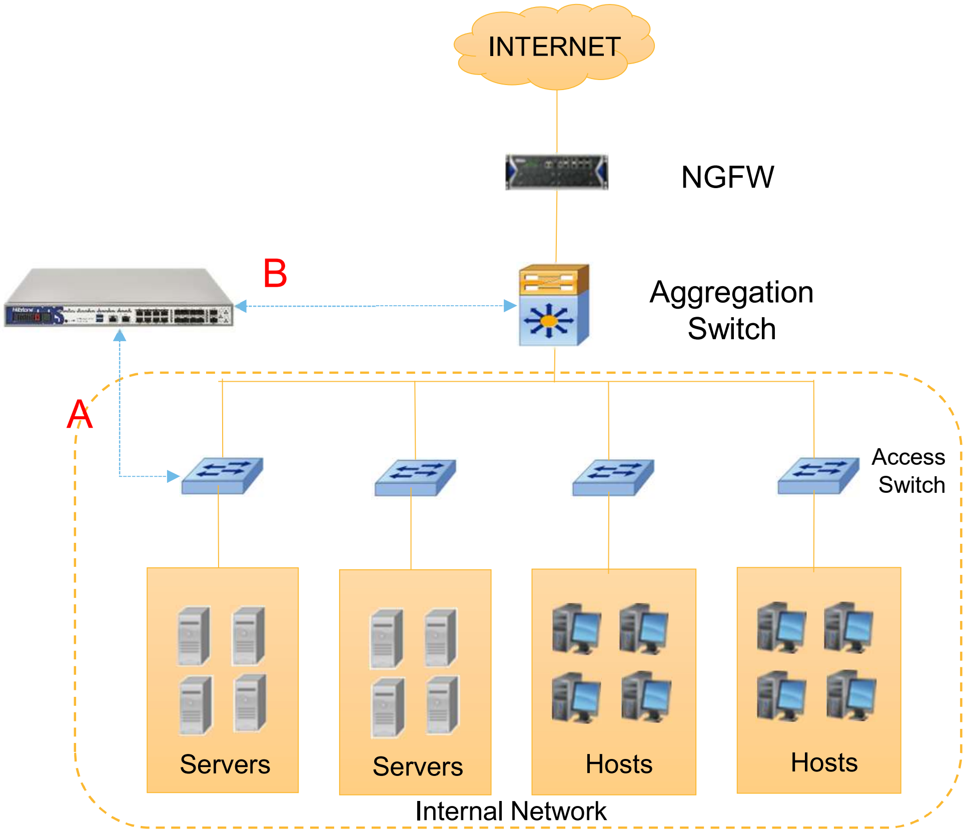
Sysmon Configuration

Specification	Sysmon Server	Sysmon Client
CPU	core*4	\
Memory	16G	1G
Storage	1T HDD, extendable	40G HDD
Installation Package	OVF Mirror	MSI Service Program
Software	VMware ESXi	Windows 7 / Windows Server 2007 or above
Others	• The default configuration supports log storage of 1000 PCs. • Sysmon server stores up to 90 days of data. Data will be automatically deleted (cleaned up) after 90 days. When the disk (/data) usage exceeds 85%, the system will automatically delete the oldest data. • Sysmon Server system has enabled the Log Receiving Service (Logstash) and the Query service (Elasticsearch), using ports 5044 and 9200 respectively.	Two installation methods are available: • direct installation by user • batch installation via Windows Active Directory domain distribution software

Sysmon Client - Installed on user's computer; used to record the process creation and termination initiated by the computer, as well as network connection information; send the information to the Sysmon Server.
Sysmon Server - Receive and store the process information log sent by the client software for BDS device query and display.

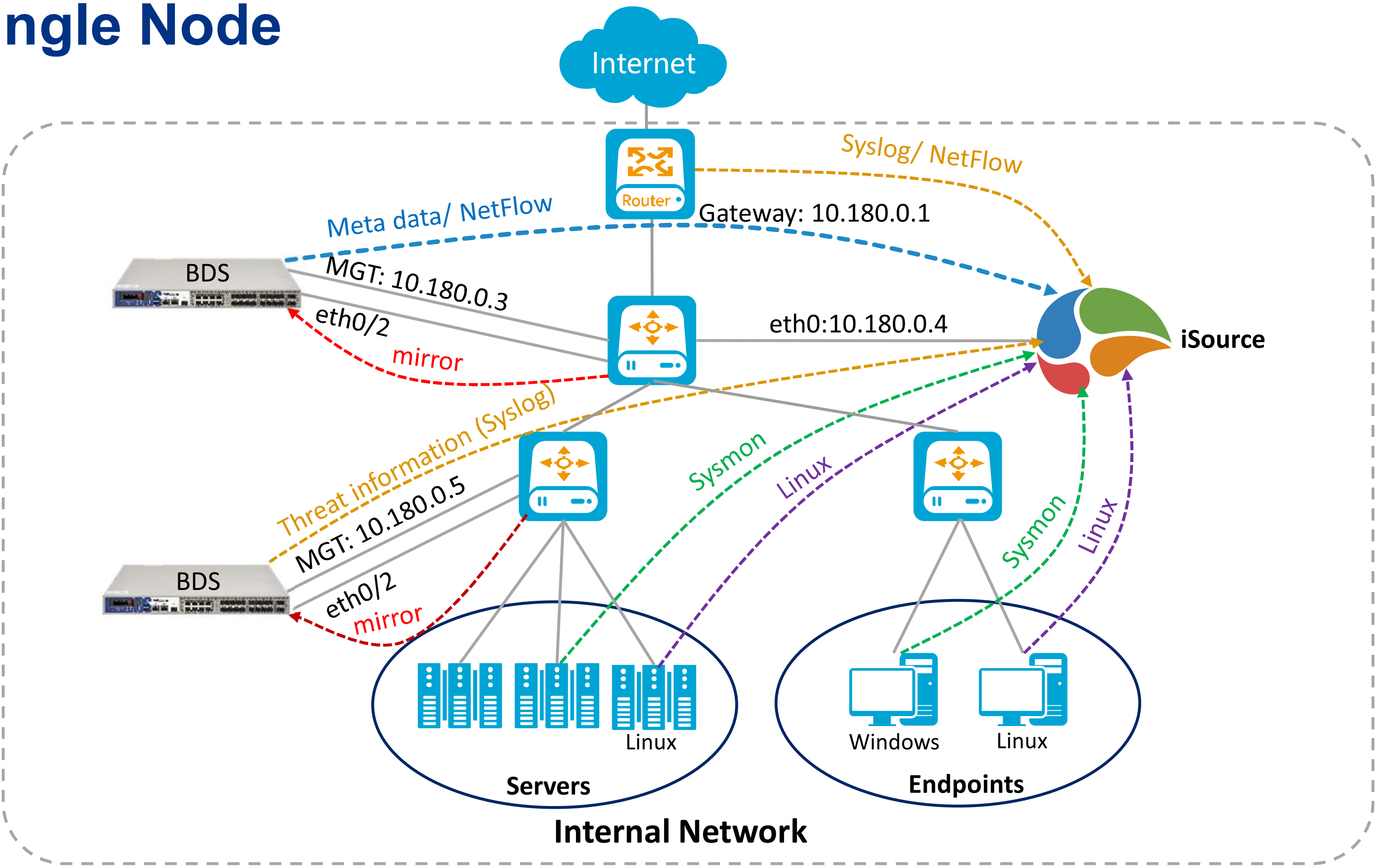
Deployment Scenarios & Winning Cases

Hillstone NDR Deployment Scenarios- BDS and NGFW



- ***Scenario A:** Access Switch connecting to servers or server groups*
  - Monitor traffic between servers within the same segment; servers in different segments; server and internet; servers and other hosts.
- ***Scenario B:** Aggregation switch between Access Switches*
  - Monitor traffic between servers in different segments; servers and internet; servers and other hosts; hosts and internet.
- ***Scenario C:** Combination of the above scenarios*

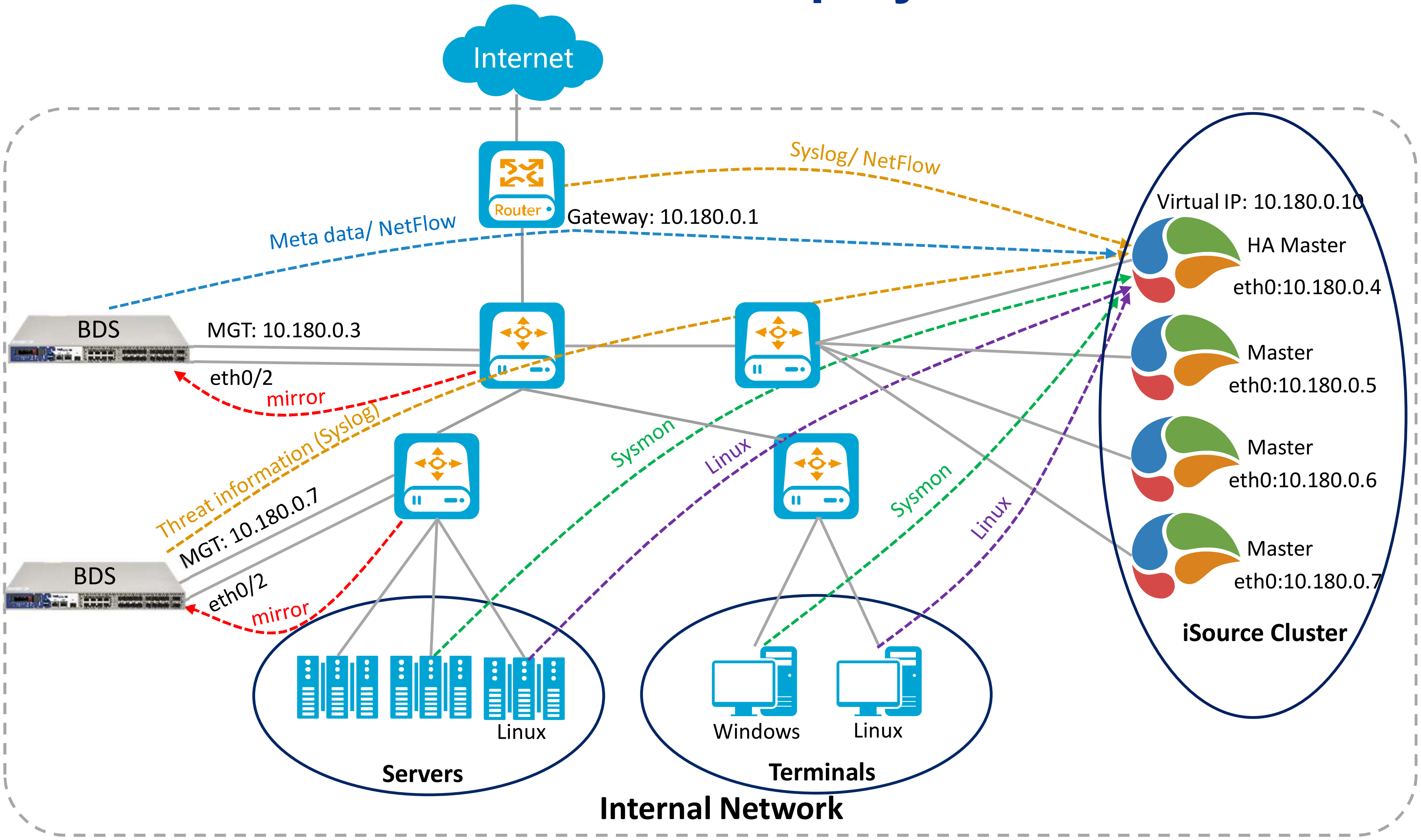
Hillstone BDS and iSource Deployment Scenario-Single Node



Single Node Deployment

- BDS deployed in TAP mode
- iSource deployment has little impact on the existing network environment
- Economic solution

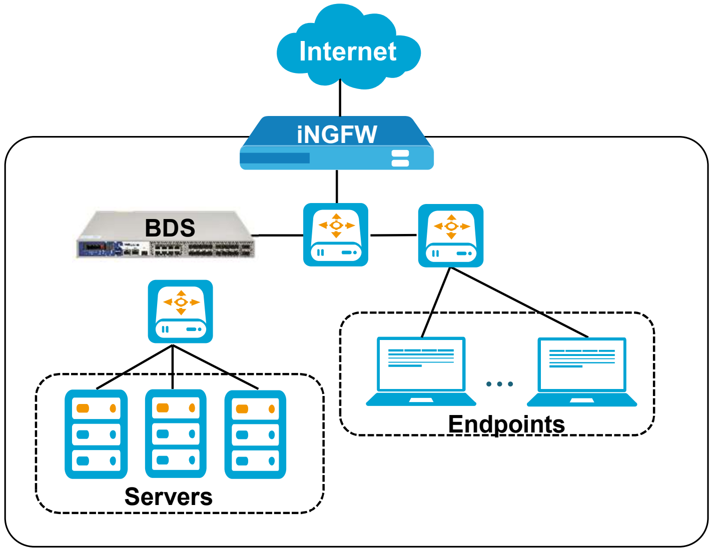
Hillstone BDS and iSource Deployment Scenario- Cluster



Cluster Deployment

- BDS deployed in TAP mode
- Cluster up to 5 nodes
- iSource deployment has little impact on the existing network environment
- Highly scalable solution

Winning Case 1: Protect Critical Information for Large University



Customer Profile

- A large private university with an enrollment of more than 10,000 students, located in South America

Challenges

- There are significant number of users connecting or accessing the networks from various devices, often compromising the perimeter security, and generating breaches that could put critical information at risk.
- The potential cyber attacks could impact business continuity, halting access to University web properties.

Hillstone Solution

- The customer deployed Hillstone BDS in conjunction with Hillstone T-Series intelligent next generation firewalls (iNGFW).
- The intelligence security features of Hillstone BDS and iNGFW – ML-based detection of behavior and threats, helped achieve detection and prevention from the perimeter to the internal network.
- A critical attack was detected by this solution deployed, which would have caused an enormous breach in internal services, as well as compromised data.

Winning Case 2: Secure Critical Assets for Government

Customer Profile

- A regional government with administrative, political and economic autonomy in South America

Challenges

- Organizations constantly conduct operations and procedures online, managing a massive flow of information as well as money. There is a great need to protect these information and assets due to the ever growing wave of cyber-attacks in the world.
- The customer needs to minimize the threat to the services it provides, as well as to guarantee the availability of the applications used by the personnel.

Hillstone Solution

- The customer deployed Hillstone BDS to fully protect their internal network. It can effectively identify advanced threats that lurk within an internal network, and affected from BYOD (bring your own device) of the organization employees.
- The deployed solution protected the customer from threats by detecting the use of devices and access to data that appear abnormal in their network. And also allowed the customer to adopt measures to avoid attacks.

Winning Case 3: Detect Locky Ransomware for a Pharmaceutical Company

Customer Profile:

- A large Pharmaceutical Company has 2000+ employees in 5 countries
- The IT team host and manage all servers in their own facilities cross several sites.
- Customer's R&D site was attacked by Locky ransomware via malicious email attachment

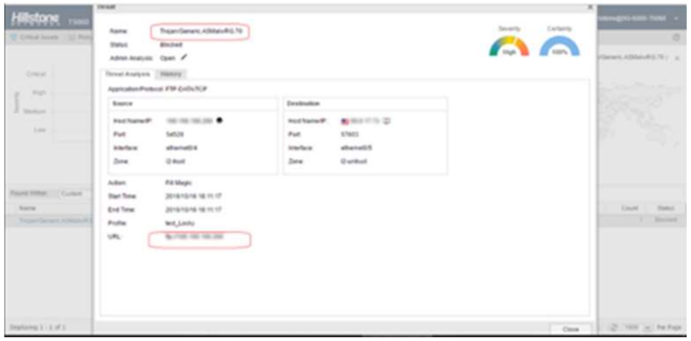
Why did the existing solutions fail?

- The customer deployed viable security solutions including firewall/IPS/Antivirus solutions, but they couldn't detect the ransomware variants in early stage and protect their servers from being locked.
- The customer was also trying to hire security professionals to disinfect their locked systems. but the process takes days, at a much higher cost even than the ransom.

Why did the Hillstone solution win?

- Customer deployed Hillstone NDR product in front of servers area, in Tapping mode by access switch, along with Hillstone NGFW and IPS in the network exit.
- Hillstone NDR product leverage its layered detection engines (ABD/ATD/IPS/AV) to detect and identify the Locky ransomware and other advanced attack and alarm the IT team to take promptly actions to block these blocks.

Winning Case 3: How Did We Win?



Threat

Name: Trojan/Generic.ASMalwRG.70
Status: Blocked
Admin Analysis: Open

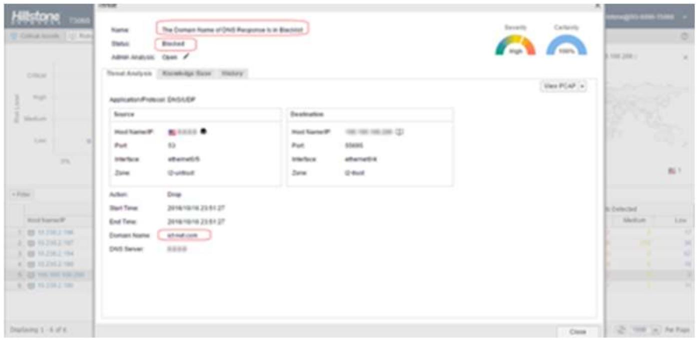
Application/Protocol: FTP-DATA/TCP

Source
Host Name/IP: [illegible]
Port: 54526
Interface: ethernet0/4
Zone: l2-trust

Destination
Host Name/IP: [illegible]
Port: 57603
Interface: ethernet0/5
Zone: l2-untrust

Action: Fill Magic
Start Time: 2016/10/16 18:11:17
End Time: 2016/10/16 18:11:17
Profile: test_Locky
URL: ftp://[illegible]

iNGFW's AV engine detects and recognizes the ransomware payload and quarantines it.



Threat

Name: The Domain Name of DNS Response is in Blacklist
Status: Blocked
Admin Analysis: Open

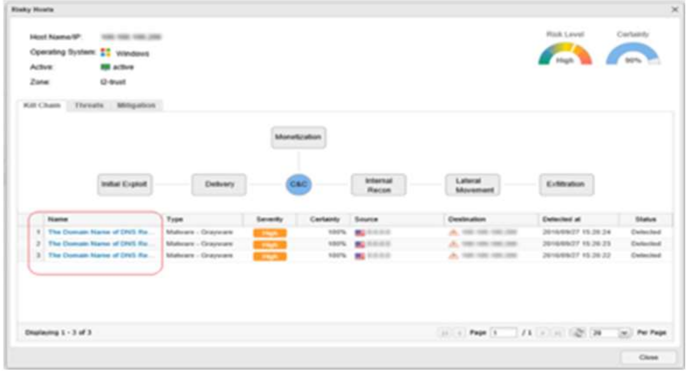
Application/Protocol: DNS/UDP

Source
Host Name/IP: [illegible]
Port: 53
Interface: ethernet0/5
Zone: l2-untrust

Destination
Host Name/IP: [illegible]
Port: 55695
Interface: ethernet0/4
Zone: l2-trust

Action: Drop
Start Time: 2016/10/16 23:51:27
End Time: 2016/10/16 23:51:27
Domain Name: [illegible]
DNS Server: [illegible]

iNGFW Reputation detection engine can recognize the C&C server domain and block it.

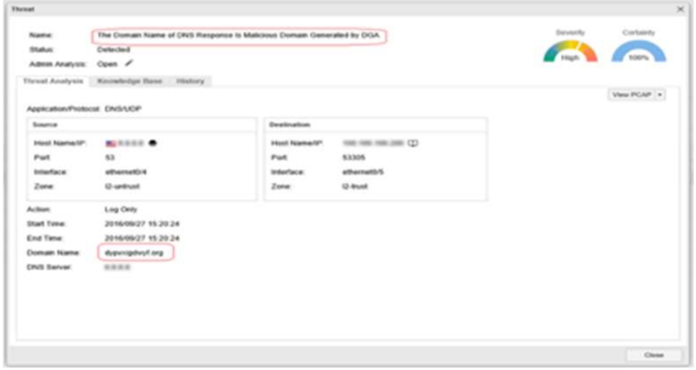


Risky Hosts

Host Name/IP: [illegible]
Operating System: Windows
Active: active
Zone: l2-trust

	Name	Type	Severity	Certainty	Source	Destination	Detected at	Status
1	The Domain Name of DNS Re...	Malware - Grayware	High	100%	[illegible]	[illegible]	2016/09/27 15:20:24	Detected
2	The Domain Name of DNS Re...	Malware - Grayware	High	100%	[illegible]	[illegible]	2016/09/27 15:20:23	Detected
3	The Domain Name of DNS Re...	Malware - Grayware	High	100%	[illegible]	[illegible]	2016/09/27 15:20:22	Detected

Displaying 1 - 3 of 3   Page 1 / 1   20 Per Page



Threat

Name: The Domain Name of DNS Response Is Malicious Domain Generated by DGA
Status: Detected
Admin Analysis: Open

Application/Protocol: DNS/UDP

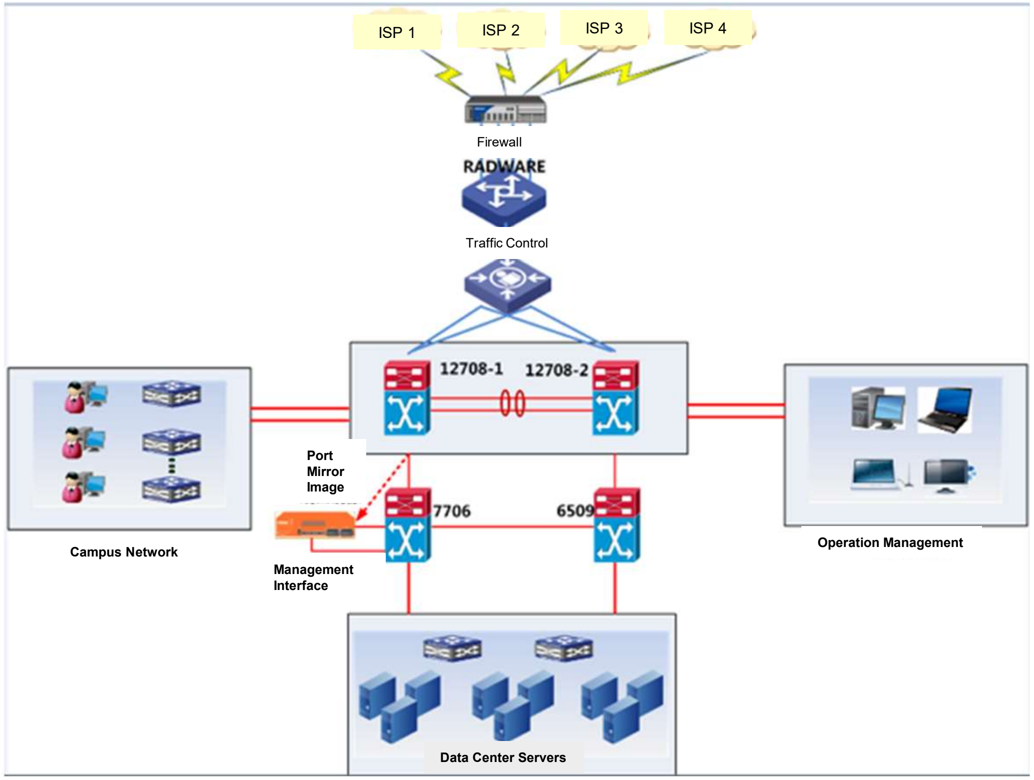
Source
Host Name/IP: [illegible]
Port: 53
Interface: ethernet0/4
Zone: l2-untrust

Destination
Host Name/IP: [illegible]
Port: 53305
Interface: ethernet0/5
Zone: l2-trust

Action: Log Only
Start Time: 2016/09/27 15:20:24
End Time: 2016/09/27 15:20:24
Domain Name: dypvrqdwyf.org
DNS Server: [illegible]

If Locky ransomware pass through AV and Reputation Detection, INGFW ABD and ATD engine can still detect them by machine learning and behavior modeling. For example, ABD engine can detects and recognizes domain names generated by Domain Generation Algorithms (DGA), which are used by Locky and many other ransomware attacks

Winning Case 4:
Protect Critical Servers for a Large University



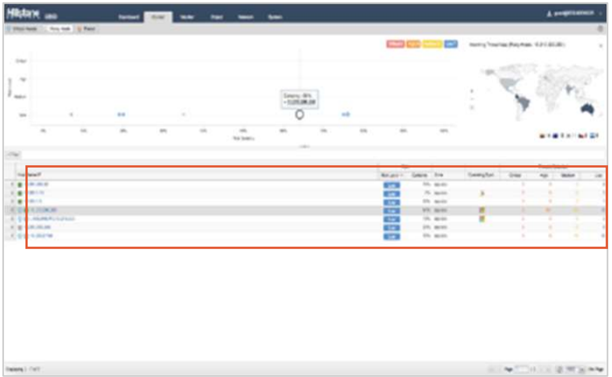
Customer Profile:

- A top university with 25,000 students accessing the campus network and resource
- Flat network with perimeter NGFW, 4 Internet links, 3Gbps bandwidth (1Gbps internal network)

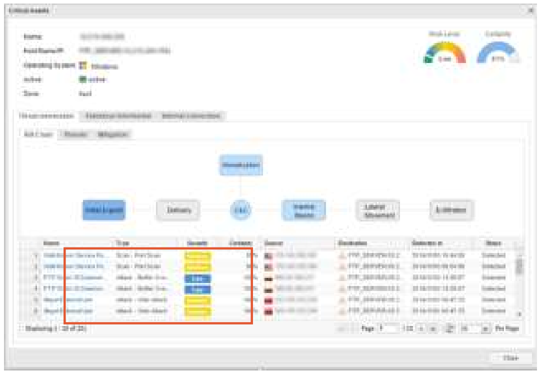
The Challenges:

- Can’t identify and detect the compromised internal host
- No dedicate solution for critical servers in the data center
- The current NGFW and IPS couldn’t detect advanced unknown threat

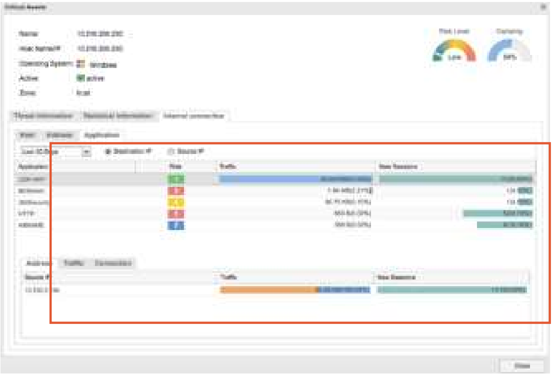
Winning Case 4: How Did We Win?



Detect the risky host in internal network



identify the threat/attack from the risky host



Real-time monitoring for the critical business servers

How did we win?

The customer has a flat network without a dedicated internal network breach detection solution and a network/security operation specialist – Effective customer education on insider threat

The customer’s internal network was compromised, but couldn’t identify the compromised host, the critical servers are exposed to threats and attacks. – A successful PoC. detect risky host quickly.

Higher and stricter compliance requirement on the high education vertical. – NDR product is dedicated breach detection solution meeting the compliance requirement

Customer References

Computer Network Information Center
Government,
China

China Telecom
ISP,
China

Datatell
Communication,
Costa Rica

Shaanxi Regional Electric Power
Group
Energy,
China

Gobierna Regional De Amazonas
Government,
Peru

Woori Bank
Finance,
S.Korea

Bangkok Metropolitan Administration
Government,
Thailand

Camel
Manufacturing,
China

Sichuan Railway Industry Investment Group
Finance,
China

Credimatic
Finance,
Ecuador

Xiangnan University
Education,
China

Nanjing City Vocational College
Education,
China

Jiangsu Agri-animal Husbandry
Vocational College
Education,
China

Changchun Institute of Technology
Education,
China

Hillstone

NETWORKS

Integrative
Cyber
Security

+1 408 508 6750
inquiry@hillstonenet.com
5201 Great America Pkwy, #420
Santa Clara, CA 95054
www.hillstonenet.com