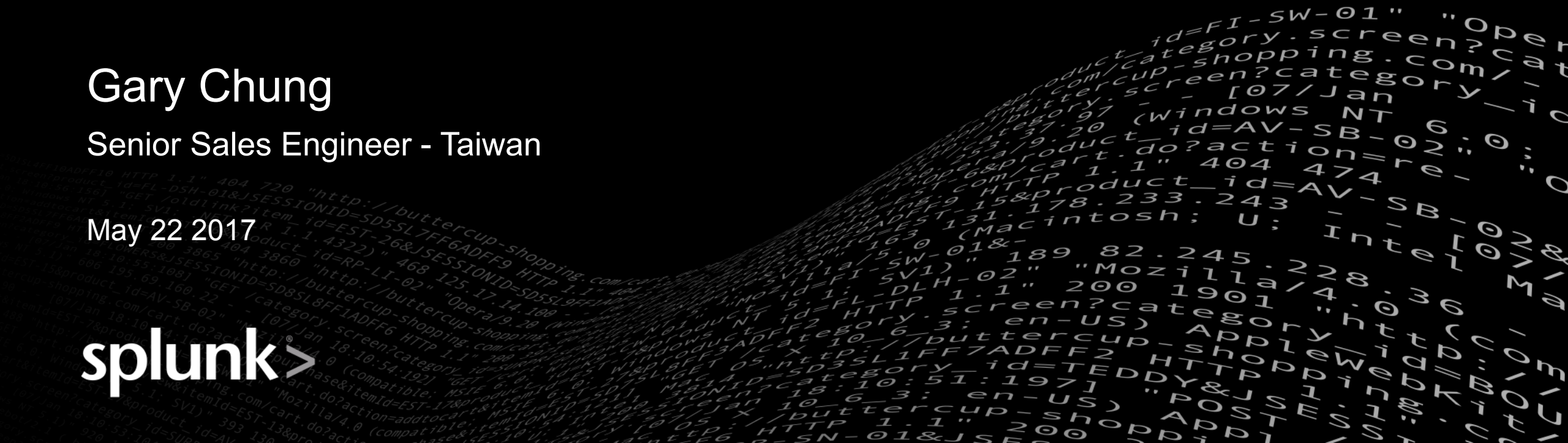
Splunk Enterprise Security

Fast Response on Ransomware - WannaCrypt

Gary Chung

Senior Sales Engineer - Taiwan

May 22 2017



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> listen to your data®

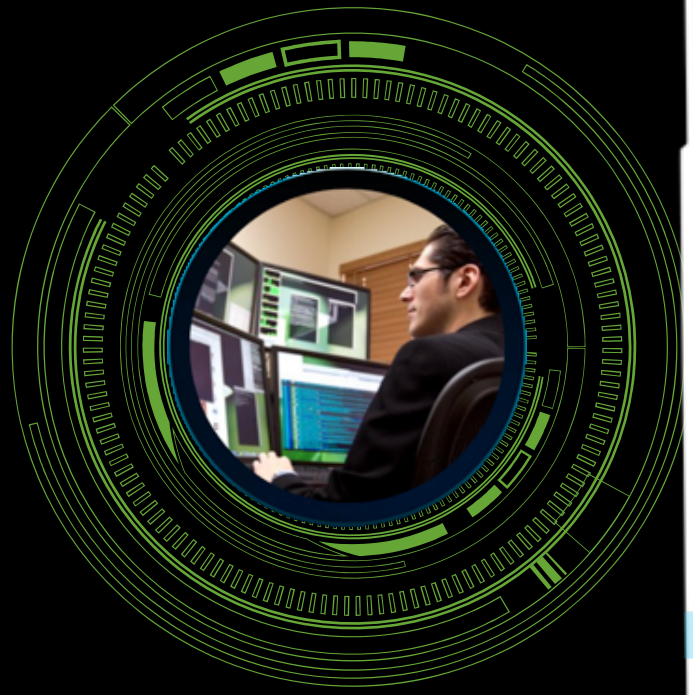
Why should CIO/CISO concern on Security

From simple service denial (DDOS, etc.) to online theft/blackmail

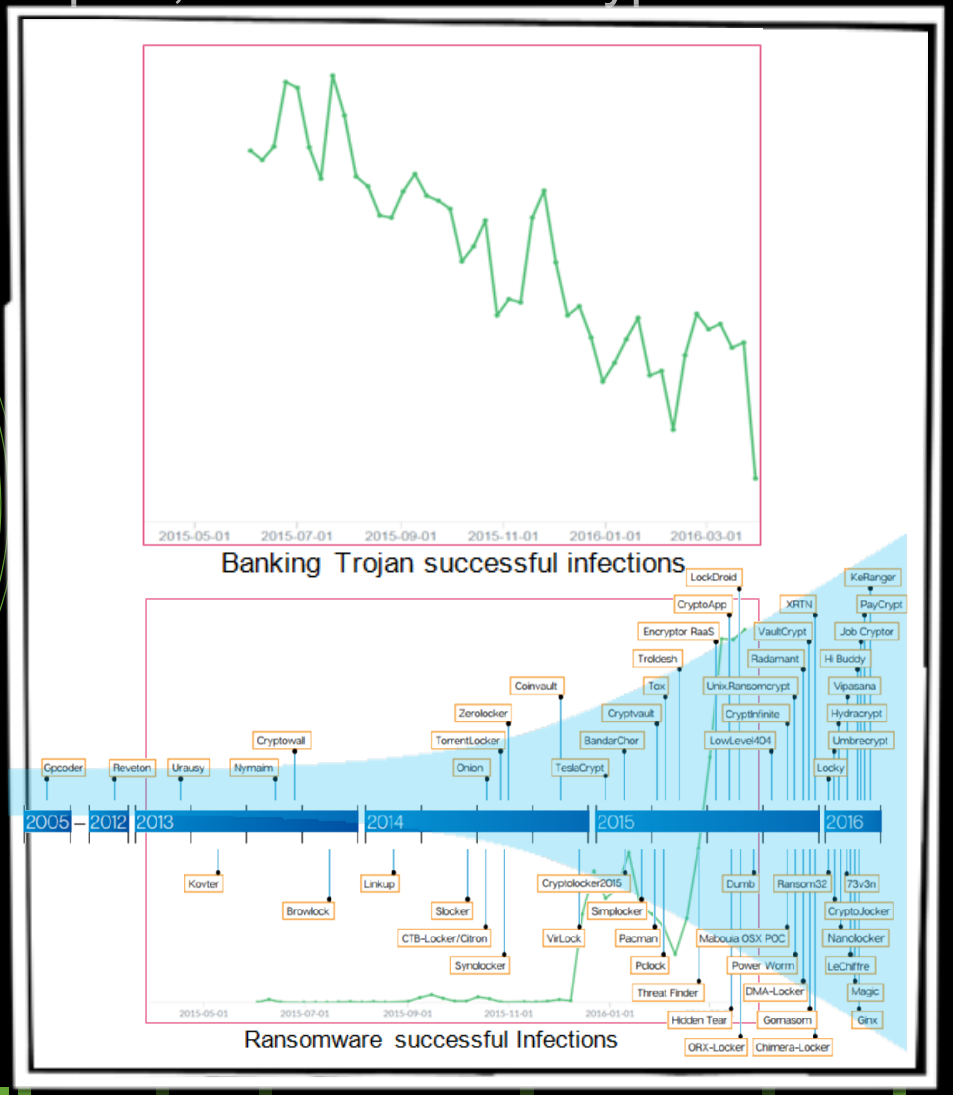
- Online Theft
- Ransomware
- Relay Server Attack
- PIM/Confidential Data Leakage

Security Task is more complicated

Attack schemes are more complex, different attack types AND **directly-related with money**

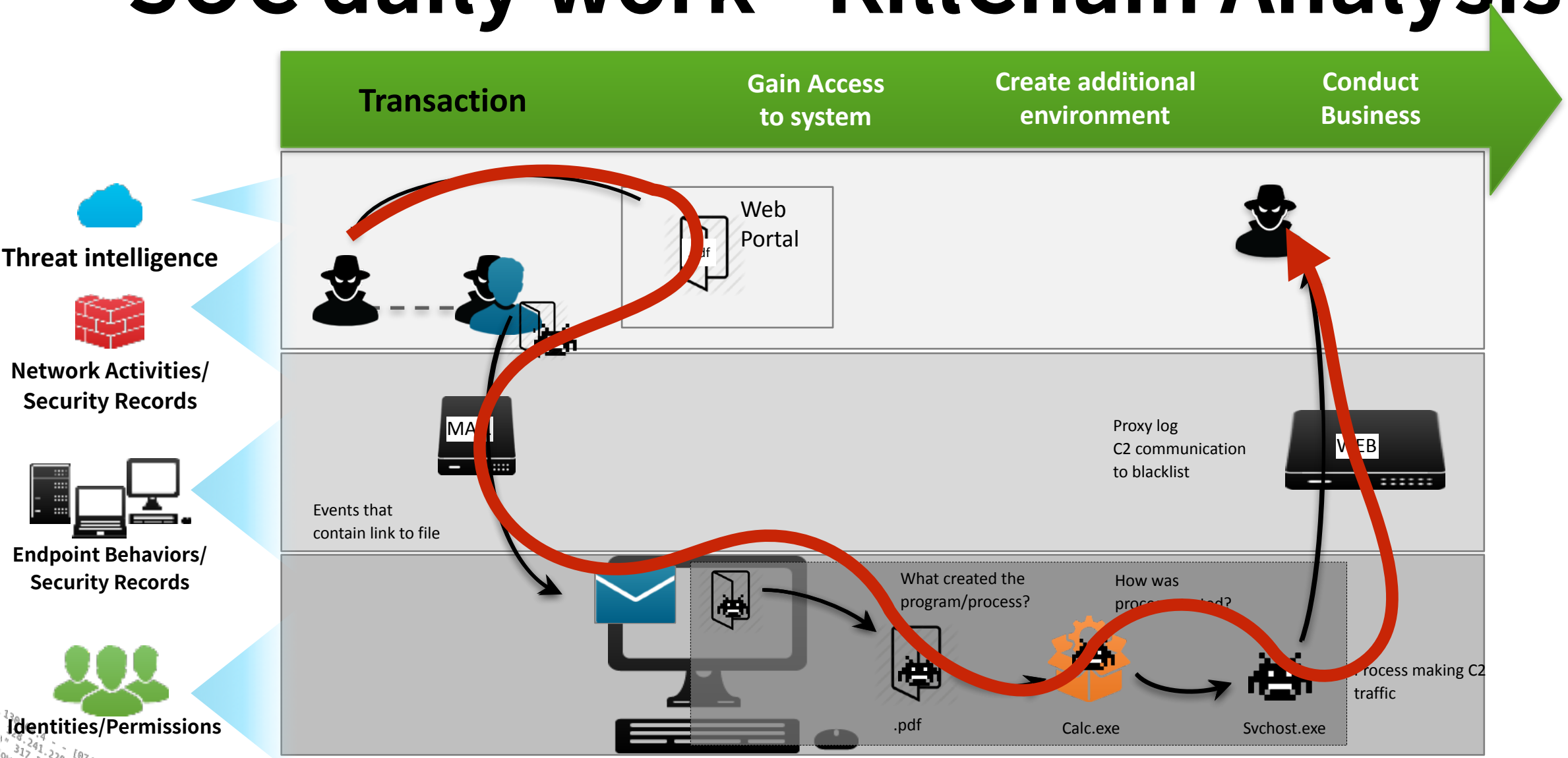


- Small Team



- Global SOC Team

SOC daily work - KillChain Analysis



splunk> listen to your data

SOC daily work - KillChain Analysis

IP Threat intelligence

bad_ip,threat_intel_source
115.29.46.99/32,zeus_c2s
61.155.30.0/24,cymru_http

115.29.46.99 32,zeus_c2s
61.155. 0.0/24,cymru_http

e-mail Record

Subject: new commission report breakdown
From: Jose Dave <jose.dave@butercupgames.com>
To: <chris.gilbert@buttercupgames.com >
Content-type: multipart/mixed;
Content-type: application/pdf; name=" Q2_commission.pdf" "

Windows System Records

54.211.114.134 - - [05/May/2014:22:40:54 -0400] "POST /portal/wp-login.php HTTP/1.1" 200 4395 "-"
54.211.114.134 - - [06/May/2014:00:05:47 -0400] "GET /tech/wp-content/uploads/2014/05/Q2_commission.pdf HTTP/1.1" 206 2475168 "-"
{"action": "create", "path": "...\Content.Outlook\Q2_commission.pdf", "process_guid": "-7751687"}
{"domain": "115.29.46.99", "protocol": 6, "ipv4": "115.29.46.99", "process_guid": "3259531", "port": 443}

User Identities (CMDB)

dest_ip cmdb_bu_owner cmdb_application_name cmdb_system_owner cmdb_app_lifecycle cmdb_s_ox cmdb_GLBA cmdb_app_uses_ssn cmdb_credit_card_data cmdb_priority cmdb_server_software cmdb_supported_by cmdb_server_phase cmdb_db_server cmdb_db_name cmdb_PCI cmdb_PII cmdb_safe_harbor 192.168.56.102 chris.gilbert@buttercupgames.com No No Tier 3 Windows7 Internal Deployed N N/A No No No 172.20.12.224 Marketing Laptop monte@demo.com Production No No No Tier 3 Windows7 Internal Deployed N N/A No No No 172.20.10.217 eCommerce Laptop modesto@demo.com Staging Yes Yes No Yes Tier 1 Windows7 Internal Deployed Y Oracle Yes Yes Yes 172.20.15.229 eCommerce Laptop modesto@demo.com Staging Yes Yes No Yes Tier 1 Windows7 Internal Deployed Y Oracle Yes Yes Yes

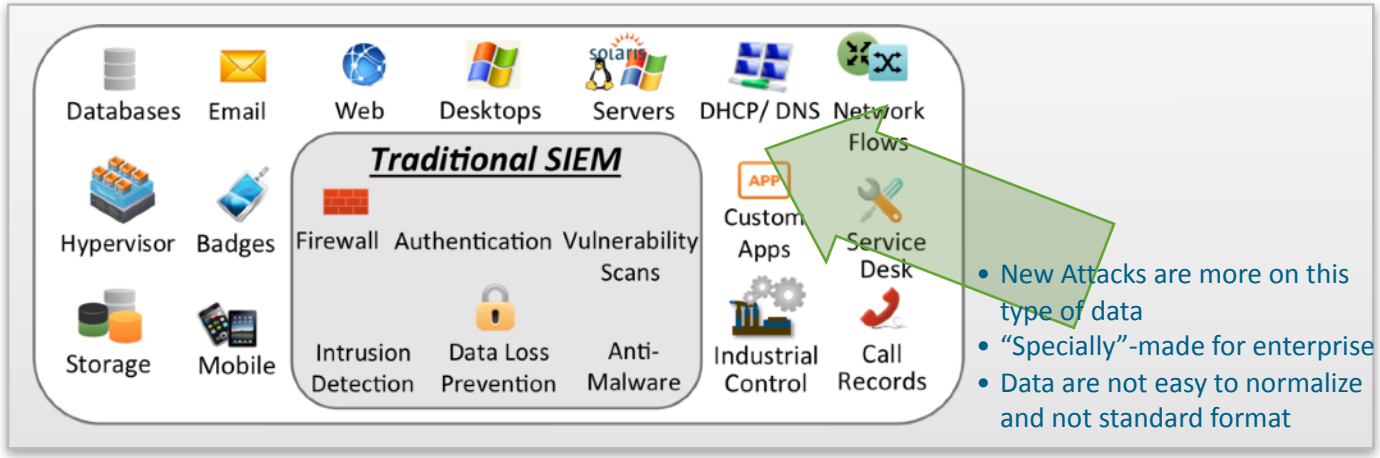
splunk> listen to your data

Splunk – Analytics-Driven Security

- APT detection/hunting (kill chain method)
- Counter threat automation
- Threat Intelligence aggregation (internal & external)
- Fraud detection – ATO, account abuse
- Insider threat detection

- Replace SIEM @ lower TCO, increase maturity
- Augment SIEM @ increase coverage & agility
- Compliance monitoring, reporting, auditing
- Log retention, storage, monitoring, auditing

- Continuous monitoring/evaluation
- Incident response and forensic investigation
- Event searching, reporting, monitoring & correlation
- Rapid learning loop, shorten discover/detect cycle
- Rapid insight from all data



Awards

2015 IoT Evolution Product of The Year

FAST COMPANY

database TRENDS AND APPLICATIONS TREND-SETTING PRODUCTS

CSO50 SECURITY CONFAB + AWARDS

Gartner

BPTW 2015 BEST PLACES TO WORK

CRN BIG DATA 100

SC MAGAZINE AWARDS 2016 WINNER Honored in the U.S.

CRN 5 STAR PARTNER PROGRAM WINNER 2015

IDC Analyze the Future

SC 2017 awards Honored in the U.S. Winner

HEALTHCARE INFORMATICS LEADING EDGE 2015

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

CRN WOMEN OF THE CHANNEL 2015

SD Times 2015 100

"Splunk is honored to once again be recognized as one of the Bay Area's Best Places to Work. We know our team is paramount to our continued success so we are deeply invested in individual development, career growth and a workplace environment that fosters our fun, passionate and collaborative community of Splunkers."

Godfrey Sullivan, chairman and CEO, Splunk, San Francisco Business Times Best Places to Work 2015

splunk> listen to your data

Gartner SIEM MQ & Forrester Wave Security Analytics Leadership

Better prevention mechanism, faster and more adaptable responses, easier to correlate data, threat intel on 0day attacks

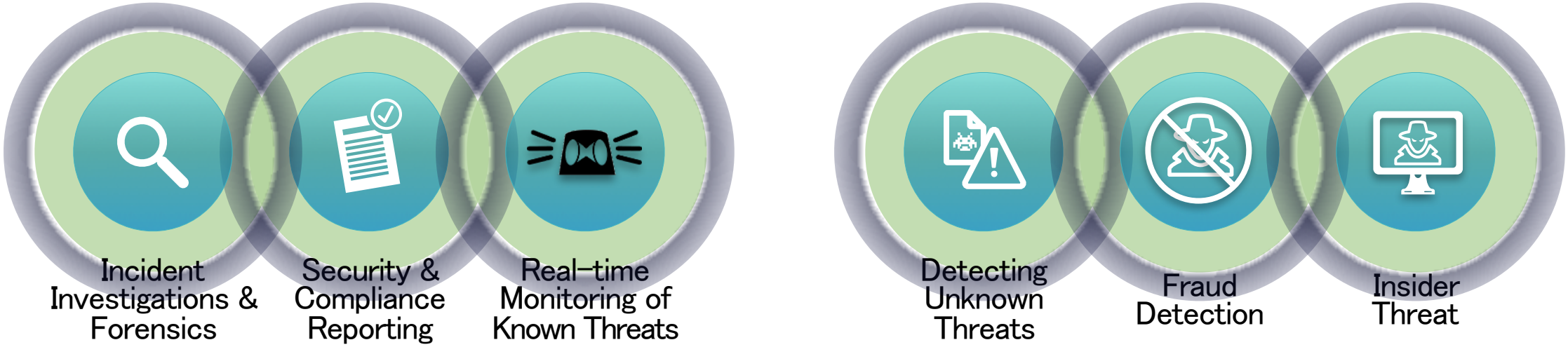
"…the rise in successful targeted attacks has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection"

Threat Management

Real-time monitoring and reporting of user activity, data access and application activity, in combination with effective ad hoc query capabilities

splunk> listen to your data®

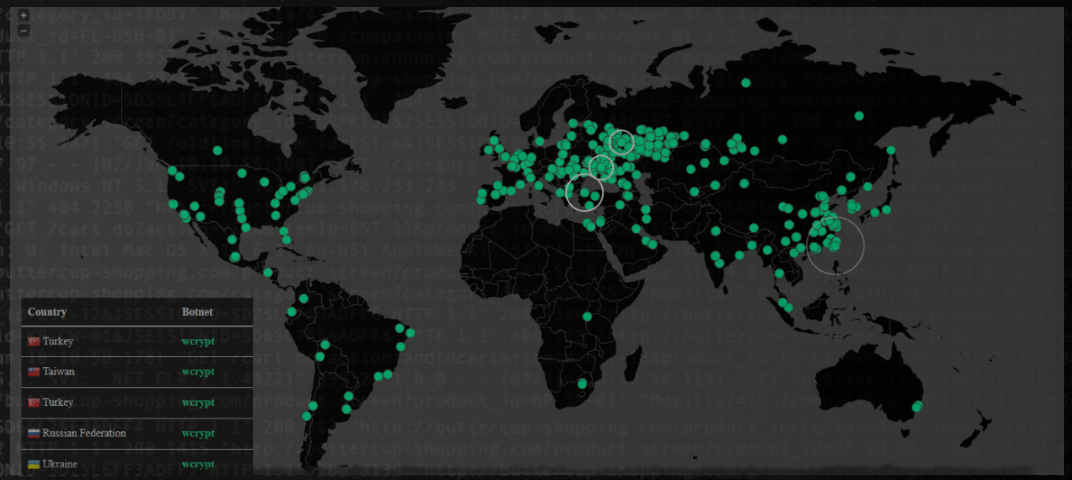
Security Intelligence Use Cases



Splunk Enterprise Security™

Splunk User Behavior Analytics™

splunk> Platform for Operational Intelligence



WannaCrypt

Understanding the lifecycle of a ransomware

splunk> listen to your data

WannaCrypt

Introduction

What is WannaCrypt ? Ransomware with Self-Propagating capabilities (wormable) – See https://www.splunk.com/blog/2017/05/13/steering-clear-of-the-wannacry-or-wanna-decryptor-ransomware-attack.html?linkId=37587259

Who is WannaCrypt's target ? Not specific to individuals/industry. It targets Windows systems worldwide. Estimated >300.000 Victims

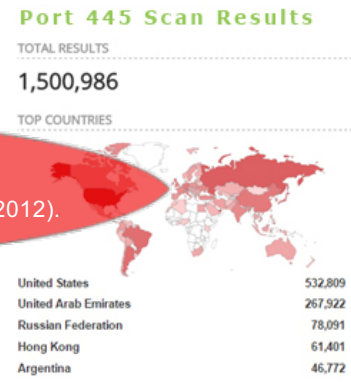
How does WannaCrypt propagate ? Attacks on SMBv1 protocol (port 445) or other vulnerable service (Netbios over TCP/IP: port 139), rumors on OpenRDP (port 3389) as well

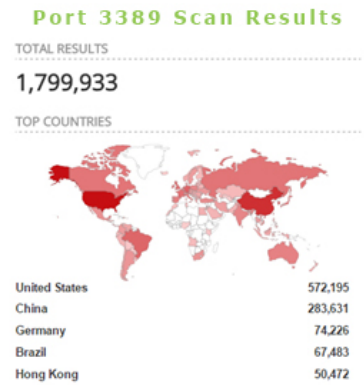
What vulnerability WannaCrypt is using? SMBv1 (MS17-010)、 ETERNALBLUE exploiting CVE-2017-0145

DOUBLEPULSAR
Backdoor

WANNACRY
Ransomware

ETERNALBLUE
Remote Exploit via SMB & NBT (Windows XP to Windows 2012).

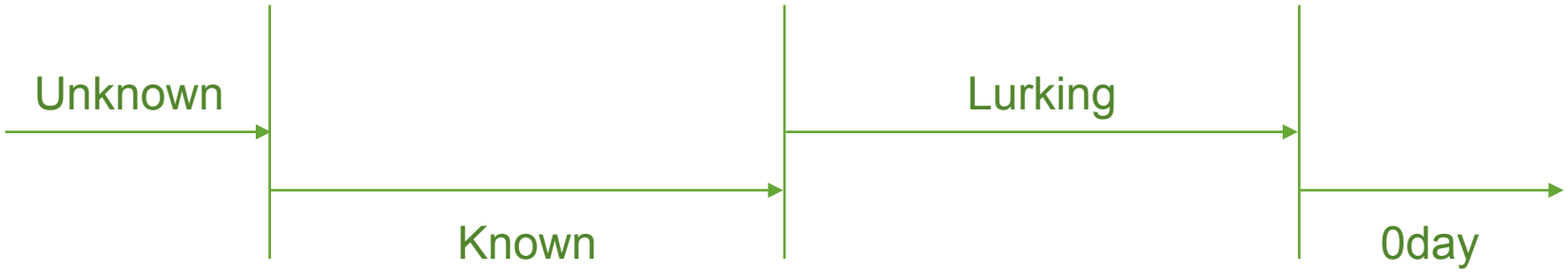




splunk> listen to your data

WannaCrypt

From unknown to known, lurking to 0day



MS releases **MS17-010 Patch** for supported Versions of Windows (not for XP, 8, Server2003)

ShadowBrokers Dump (including EternalBlue and DoublePulsar)

WannaCry "Outbreak"

MS releases MS17-010 Patch also for **XP, 8, Server2003**

splunk> listen to your data

WannaCrypt

KillChain

Scan the internet for exposed **SMBv1** Service

Direct Exploitation of exposed **SMB** service

1. Tampering SMB services/binaries
2. Install WannaCrypt ransomware and propagate through all network interfaces
3. Install Doublepulsar backdoor
4. Install tor for anom. communication

Recon

Search for vulnerable Organizations

Creation of the artifacts

Deliver

Exploit EternalBlue vulnerability

Exploit

Inject code into the SMB process

Wait for the order to act

Control

Take control of the endpoint

Spread to other endpoints

Exploit the EternalBlue vulnerability in the endpoints

Search for exploitable endpoints in the network

Access system files

Block booting in recovery mode

Kill processes to gurantee encryption

Encryption of files and directories

Display a dialog to request the ransom

Execute

Maintain

1. Download Crypto Key
2. Command & control
3. Check killswitch domain

1. Encrypts all data (.wcry)
2. Drop decrypt tool
3. Communicate via tor

Edit desktop image for ransom

splunk> listen to your data

* http://www.pandasecurity.com/mediacenter/news/whos-behind-the-wannacry-cyberattack/

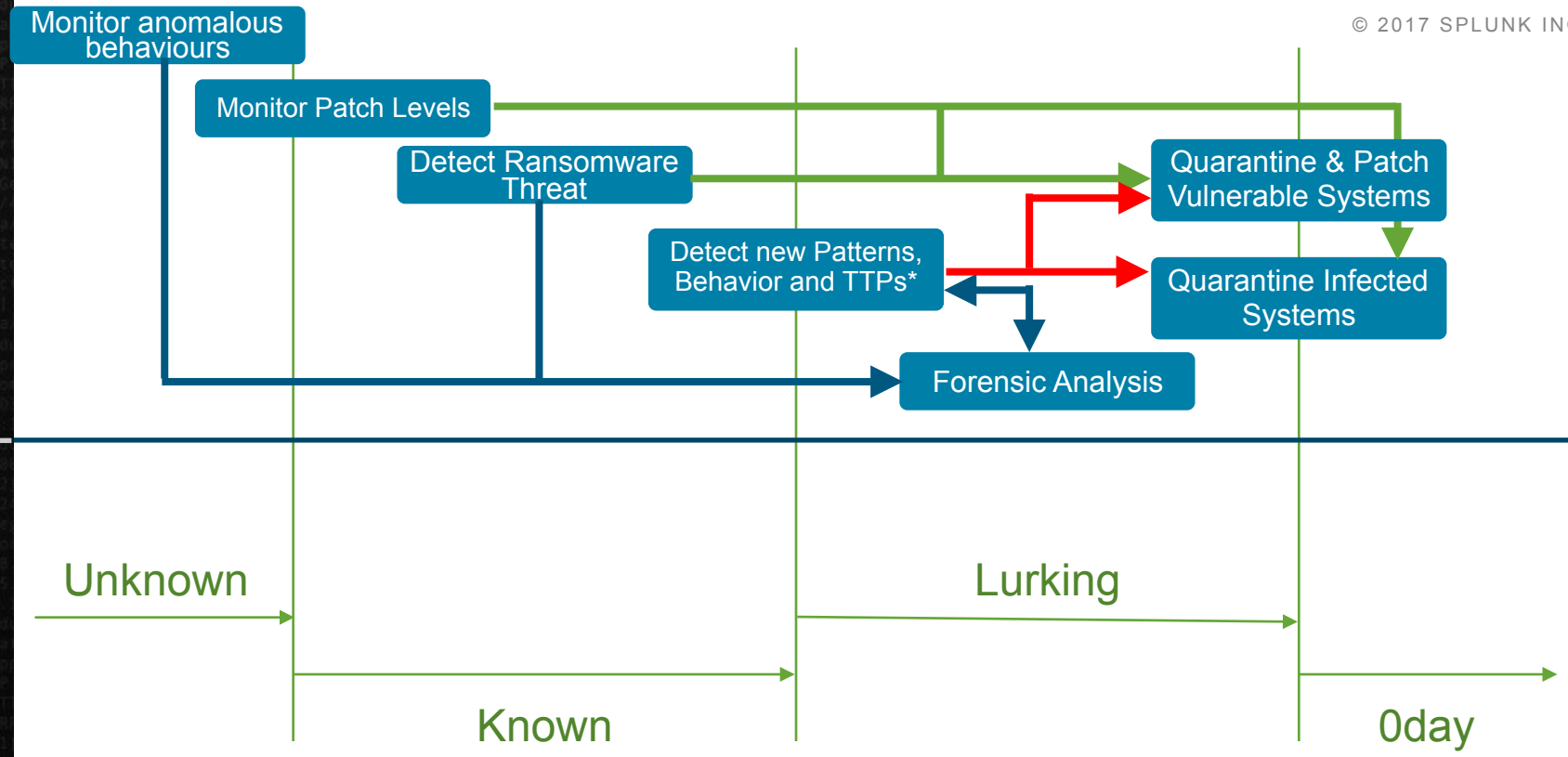
Splunk helps organizations on known & unknown issues

Monitoring patch levels, endpoint behaviors, react in realtime and playbook on ransomware

splunk> playbook

WannaCrypt

From unknown to known, lurking to 0day



MS releases **MS17-010 Patch** for supported Versions of Windows (not for XP, 8, Server2003)

ShadowBrokers Dump (including EternalBlue and DoublePulsar)

WannaCry "Outbreak"

MS releases MS17-010 Patch also for **XP, 8, Server2003**

splunk> listen to your data

splunk>

WannaCrypt

From unknown to known, lurking to 0day

Patch management & Backup Tracking

Protocols, Connections Anomalies

Endpoint Anomalies Tracking

Attack patterns forensic

1. Unknown

1. Track file backup records
2. Detect rare IP internal connections (**Vulnerability Scanner**)
3. Detect external connection from host (**C2 site tracing**)
4. Detect subnet scanning from host (**infection tracing**)
5. Detect software installation/modification records

2. Known

1. Software patch management
2. Detect specific protocol traffic (**smb is known for vulnerability**)
3. Detect “no owner” DNS query from host (**C2 site tracing and also killswitch**)
4. Detect anomalous process (**System overtake evidence tracing**)
5. Detect anomalous registry record

3. Lurking

1. Traffic statistical analysis for anomalies
2. Entropy analysis for C2 site (**Track DGA domains**)
3. Detect files generate, update and access (**Track attacks TTPs**)
4. Detect system files or configuration change (**Overtake the system**)

4. 0day

1. Detect files change (**Encryption**)
2. Trace killswitch DNS records for hosts
3. Detect all internal/external connections (**Check IDS, FW logs from more infections**)
4. Find known encryption filename extension on all hosts (**Find .wncry understand the scope**)
5. quarantine the vulnerable/infected systems

splunk> listen to your data

Quick response on Splunk Apps

Different choices for different situations

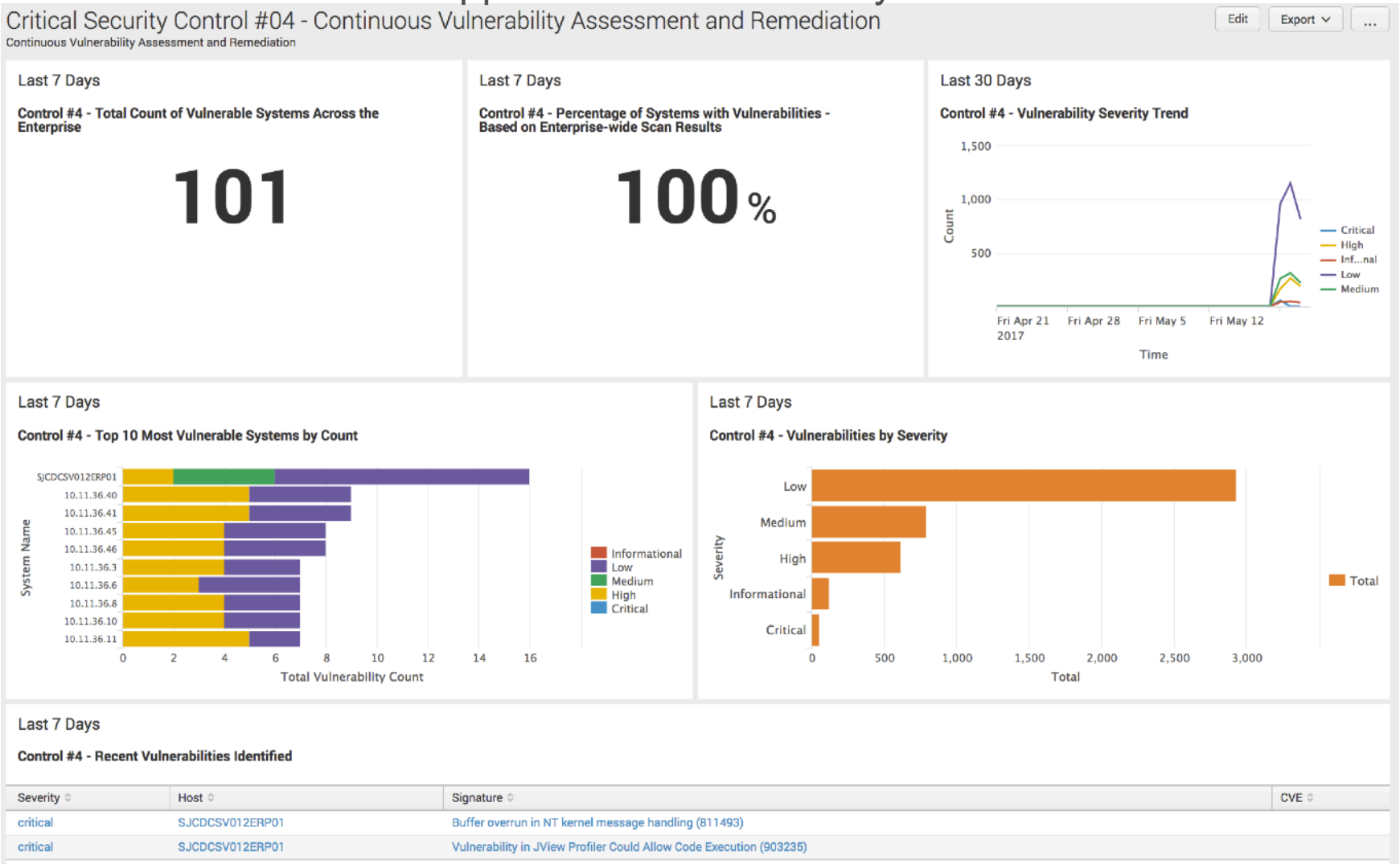
Free CIS critical control app on building a monitor framework

Automated SOC architecture on multiple data type correlations

Machine learning on data anomalies to track advanced threats

Patch management & Backup Tracking

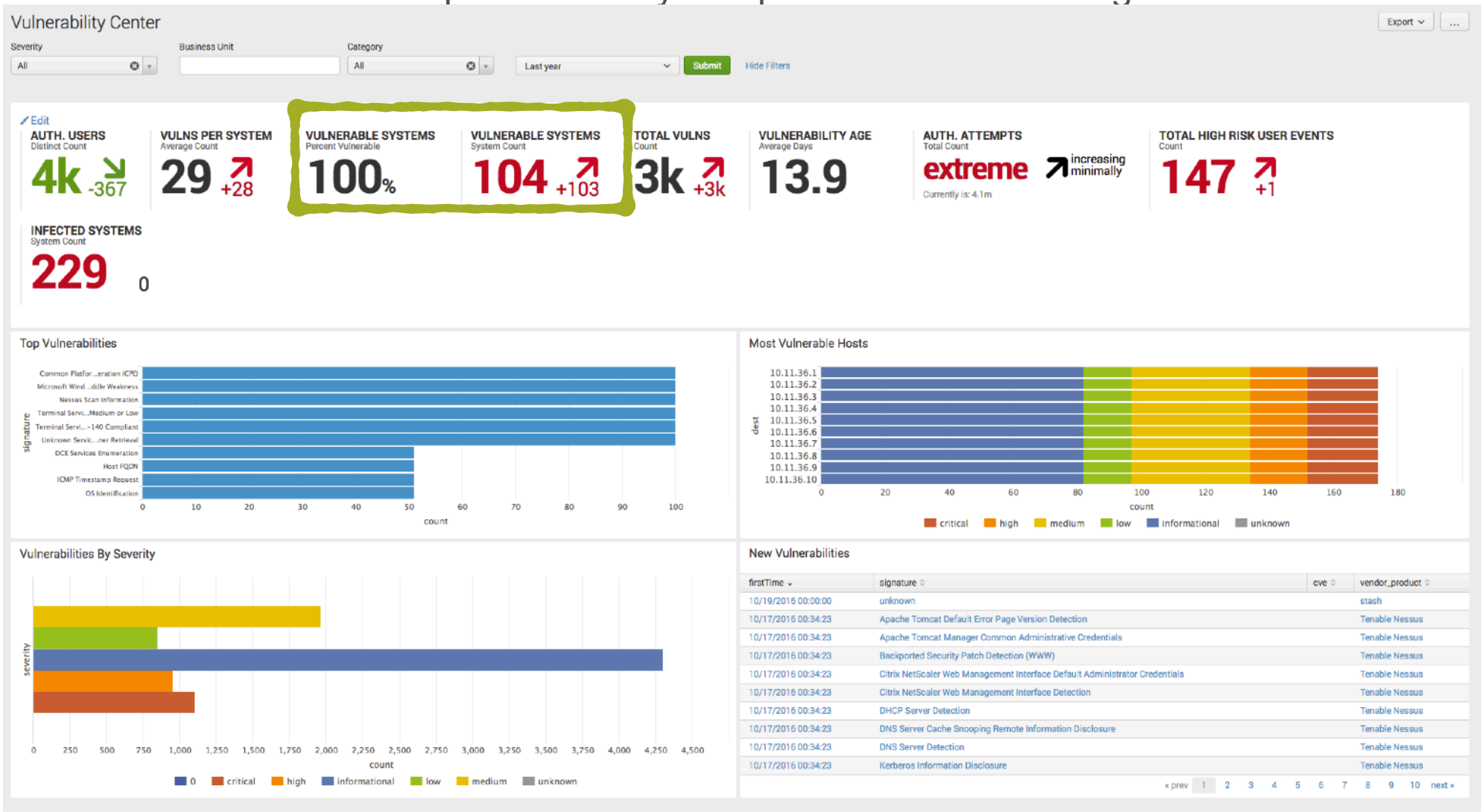
Free App: CIS Critical Security Controls



splunk> listen to your data

Patch management & Backup Tracking

Enterprise Security comprehensive monitoring



splunk> listen to your data

Patch management & Backup Tracking

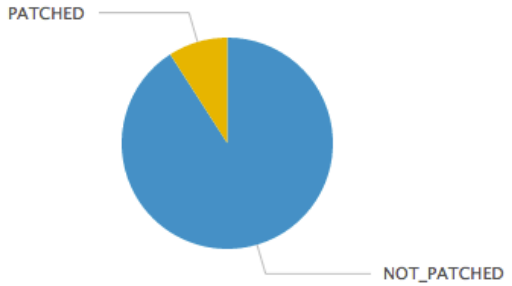
Enterprise Security comprehensive monitoring

Endpoint Vulnerability Status

Vulerability Patch

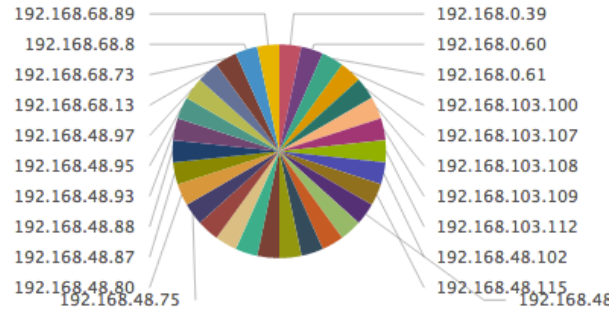
Export ...

Endpoint Patch Status



Outstanding Vulnerability CVE Status

Endpoints with Vulnerability



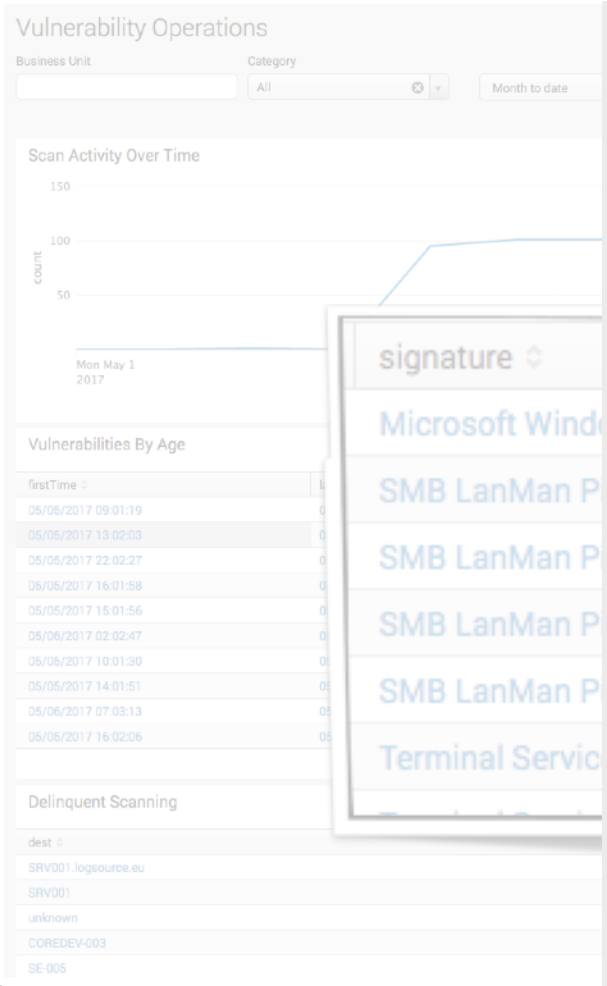
Detailed Vulerability Status

src	count	cve	dc_cve	pluginName
192.168.0.102	1	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	6	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)
192.168.0.39	1	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	6	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)
192.168.0.60	1	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147	6	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)

splunk> listen to your data

Patch management & Backup Tracking

Enterprise Security comprehensive monitoring



Vulnerability Search

Export ...

Vuln. Category: *

Severity: All

Signature:

Reference (bugtraq, cert, cve, etc.):

Destination:

Last 30 days | Submit | Hide Filters

_time	category	severity	signature	cve	dest	count
2017-05-21 03:03:35	unknown	medium	DCE Services Enumeration		SJCDCSV012ERP01	2394
2017-05-21 03:03:35	unknown	medium	SMB Detection		SJCDCSV012ERP01	2394
2017-05-21 03:03:35	unknown	critical	Buffer overrun in NT kernel message handling (811493)		SJCDCSV012ERP01	1197
2017-05-21 03:03:35	unknown	medium	Host FQDN		SJCDCSV012ERP01	1197
2017-05-21 03:03:35	unknown	medium	ICMP Timestamp Request		SJCDCSV012ERP01	1197

« prev 1 2 3 4 5 6 7 8 9 10 next »

i	Time	Event
>	5/21/17 3:04:00.000 AM	start_time="Sun May 21 02:36:32 2017" end_time="Sun May 21 02:36:32 2017" dest_dns="PROD-MFS-005" dest_nt_host="BUSDEV-003" dest_ip="10.11.36.29" os="Microsoft Windows XP Professional SP3" dest_port_proto="microsoft-ds(445/tcp)" severity_id="3" signature_id="10397" signature="SMB LanMan Pipe Server browse listing" category = unknown | dest = PROD-MFS-005 | dvc = unknown | severity = high | signature = SMB LanMan Pipe Server browse listing
>	5/21/17 3:04:00.000 AM	start_time="Sun May 21 02:38:37 2017" end_time="Sun May 21 02:38:37 2017" dest_ip="10.11.36.46" os="Cisco Router" dest_port_proto="general" severity_id="2" signature_id="10180" signature="Ping the remote host" category = unknown | dest = 10.11.36.46 | dvc = unknown | severity = medium | signature = Ping the remote host
>	5/21/17 3:04:00.000 AM	start_time="Sun May 21 02:13:56 2017" end_time="Sun May 21 02:13:56 2017" dest_ip="10.11.36.32" os="Cisco Router" dest_port_proto="general" severity_id="2" signature_id="12053" signature="Host FQDN" category = unknown | dest = 10.11.36.32 | dvc = unknown | severity = medium | signature = Host FQDN
>	5/21/17 3:04:00.000 AM	start_time="Sun May 21 02:59:15 2017" end_time="Sun May 21 02:59:15 2017" dest_ip="10.11.36.25" os="Cisco Router" dest_port_proto="general" severity_id="2" signature_id="10114" signature="ICMP Timestamp Request" category = unknown | dest = 10.11.36.25 | dvc = unknown | severity = medium | signature = ICMP Timestamp Request
>	5/21/17 3:04:00.000 AM	start_time="Sun May 21 03:02:13 2017" end_time="Sun May 21 03:02:13 2017" dest_ip="10.11.36.24" os="Cisco Router" dest_port_proto="general" severity_id="2" signature_id="11936" signature="OS Identification" category = unknown | dest = 10.11.36.24 | dvc = unknown | severity = medium | signature = OS Identification

« prev 1 2 3 4 5 6 7 8 9 10 next »

splunk> listen to your data

Protocols, Connections Anomalies

Free App: CIS Critical Security Controls

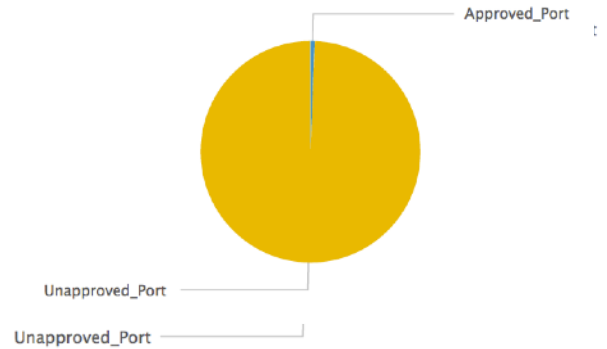
Critical Security Control #09 - Limitation and Control of Network Ports

Limitation and Control of Network Ports

編輯 匯出 ...

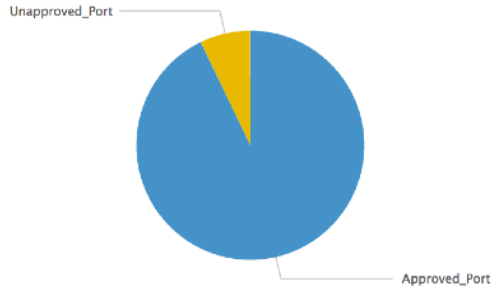
Last 60min

Control #9 - Approved vs. Unapproved Listening Ports - Linux Servers - Chart



Last 60min

Control #9 - Approved vs. Unapproved Listening Ports - Windows Servers - Chart



Last 60min

Control #9 - Approved vs. Unapproved Listening Ports - Linux Servers

host	port	is_approved
ACME-004	22	
	25	
	68	
	17500	
ch-demo-cis20	9	1
	22	
	25	
	28	
	35	
	37	
	41	
	43	
	60	

Last 60min

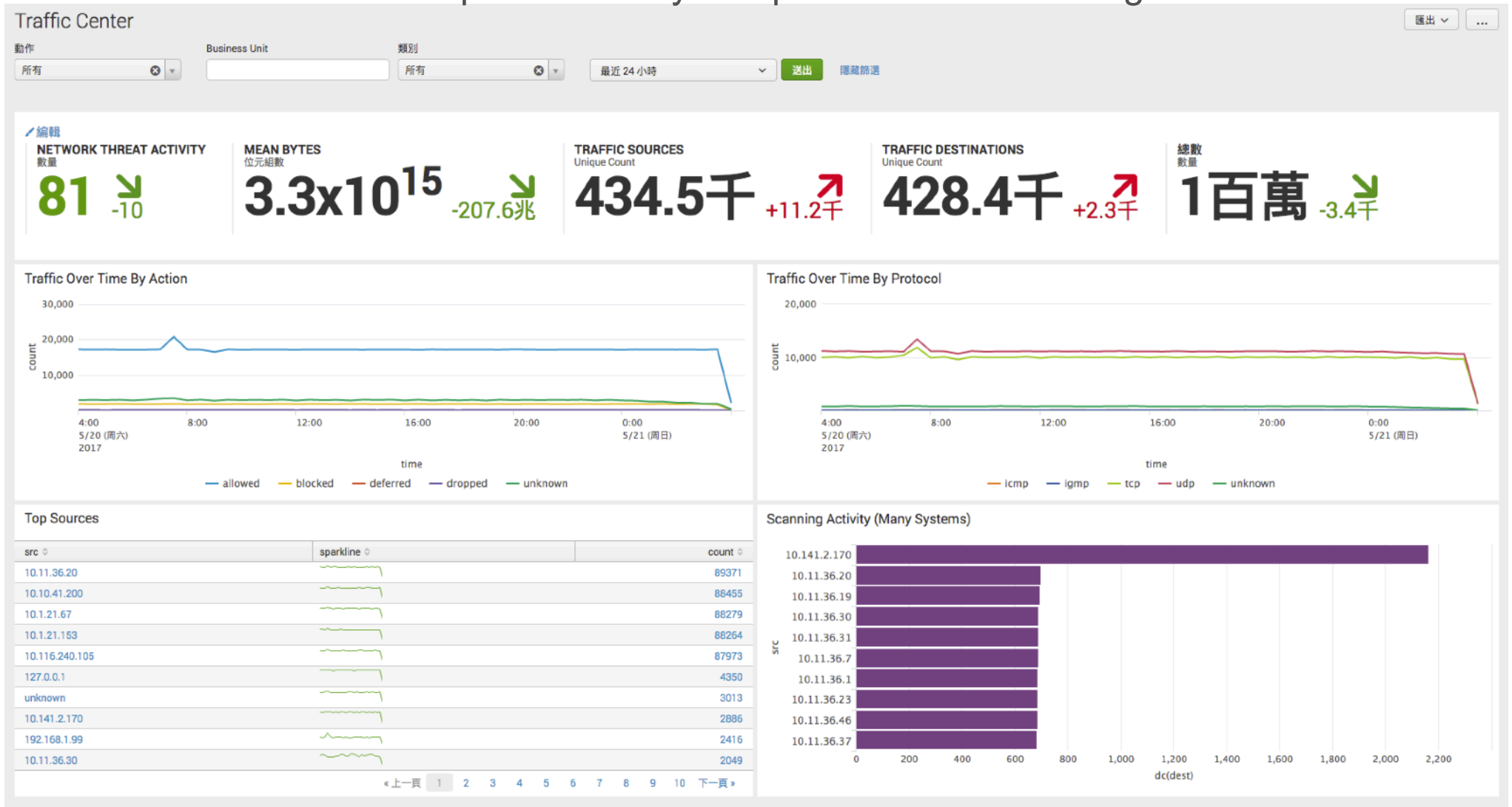
Control #9 - Approved vs. Unapproved Listening Ports - Windows Servers

host	port	is_approved
Windows-File-Server	25	
	139	
	445	
	3389	

splunk> listen to your data

Protocols, Connections Anomalies

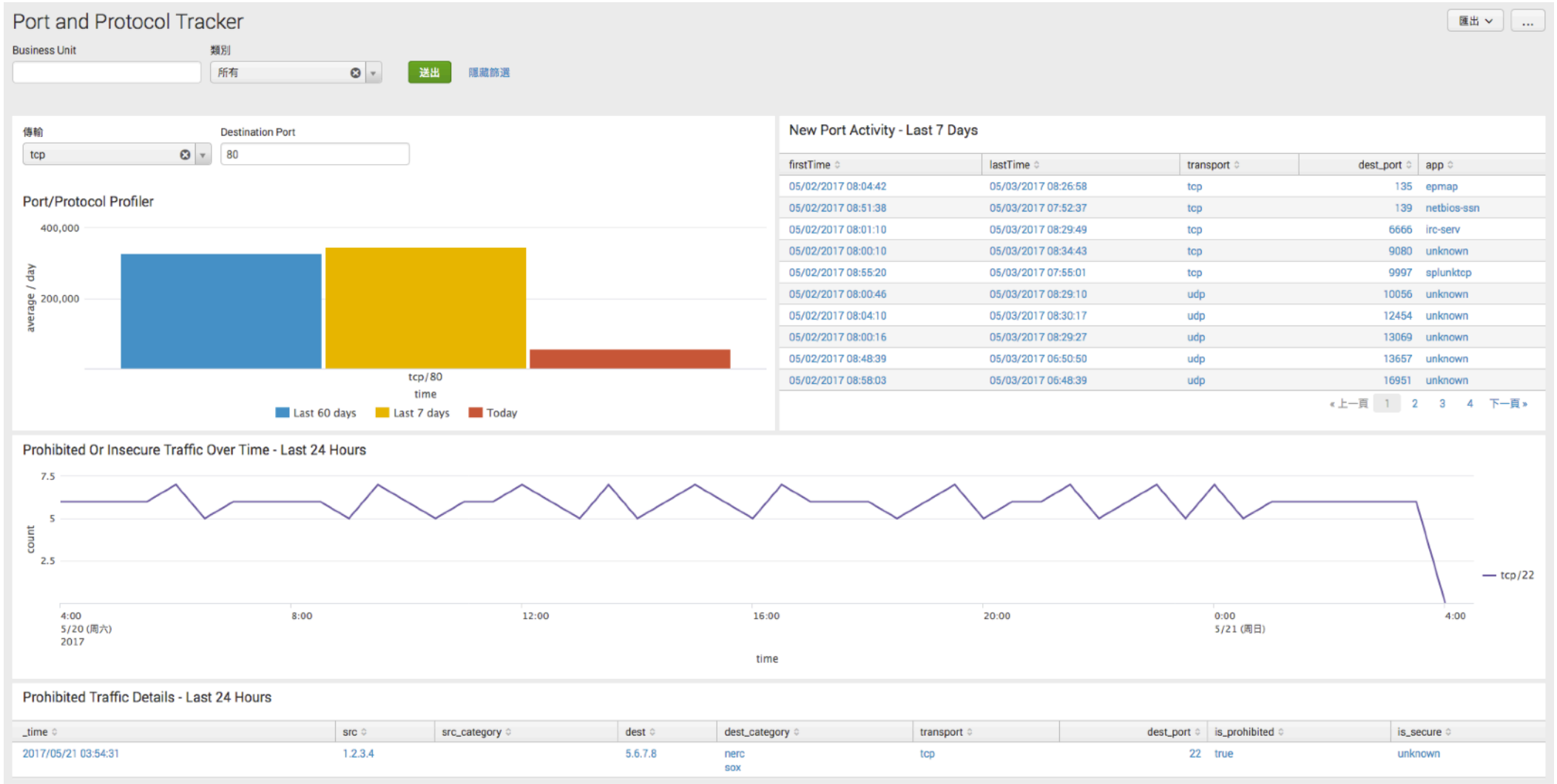
Enterprise Security comprehensive monitoring



splunk> listen to your data®

Protocols, Connections Anomalies

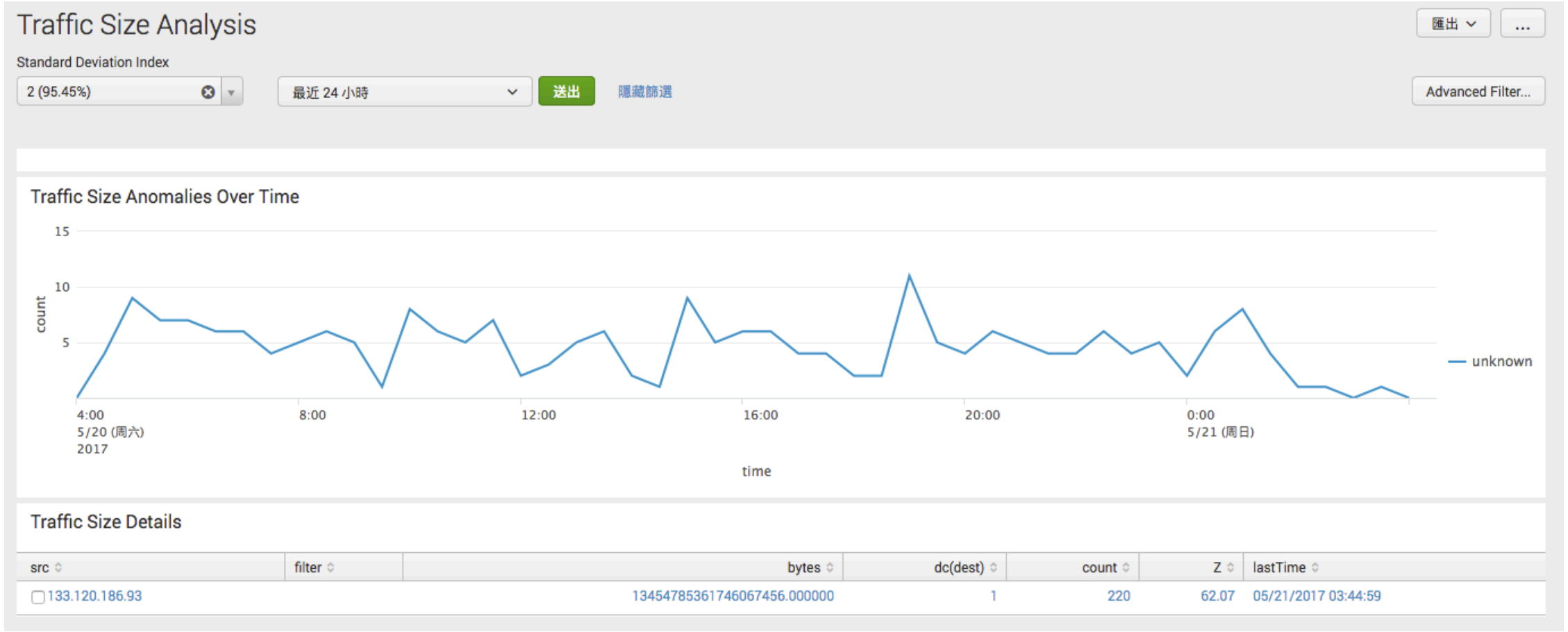
Enterprise Security comprehensive monitoring



splunk> listen to your data®

Protocols, Connections Anomalies

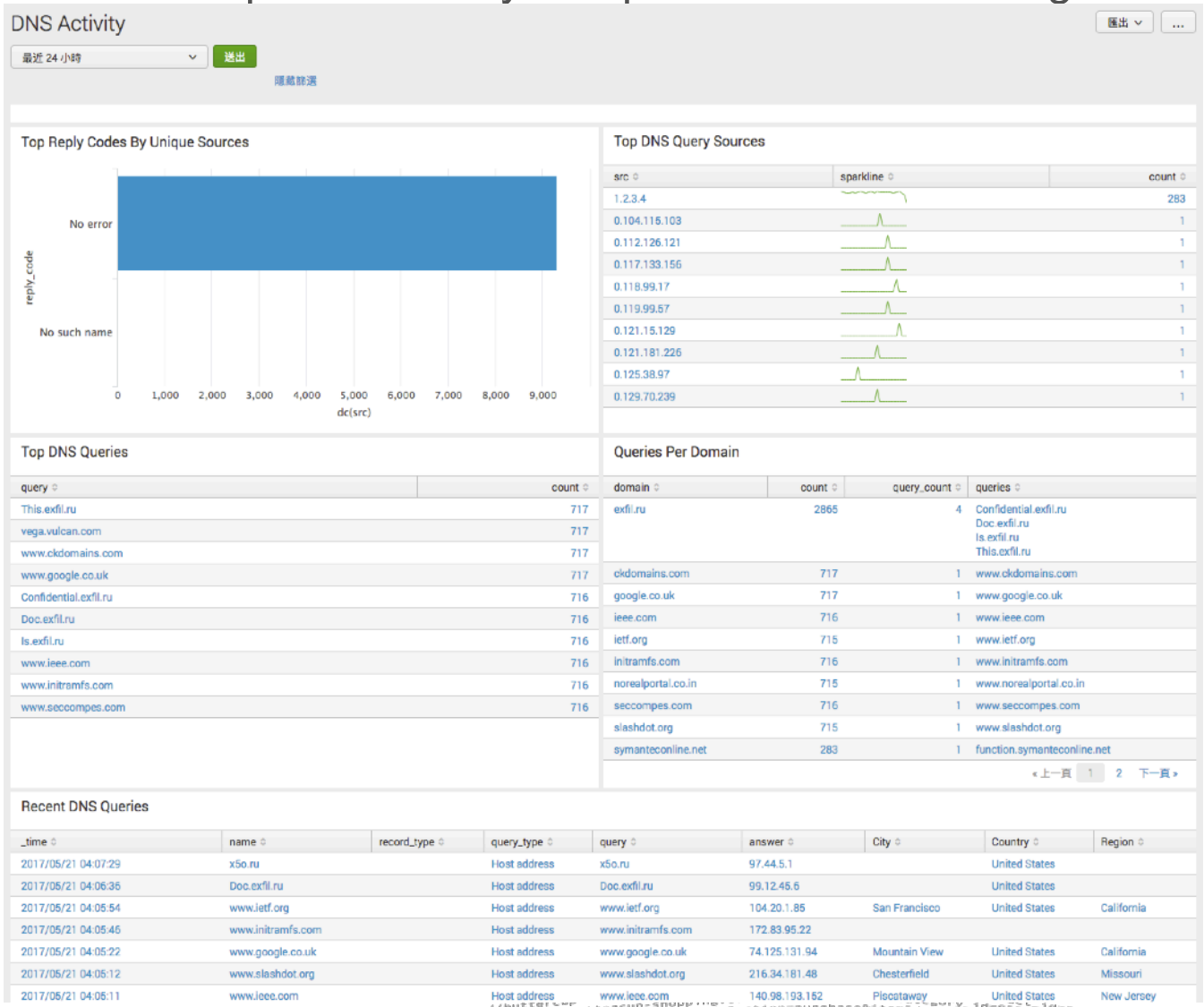
Enterprise Security comprehensive monitoring



splunk> listen to your data

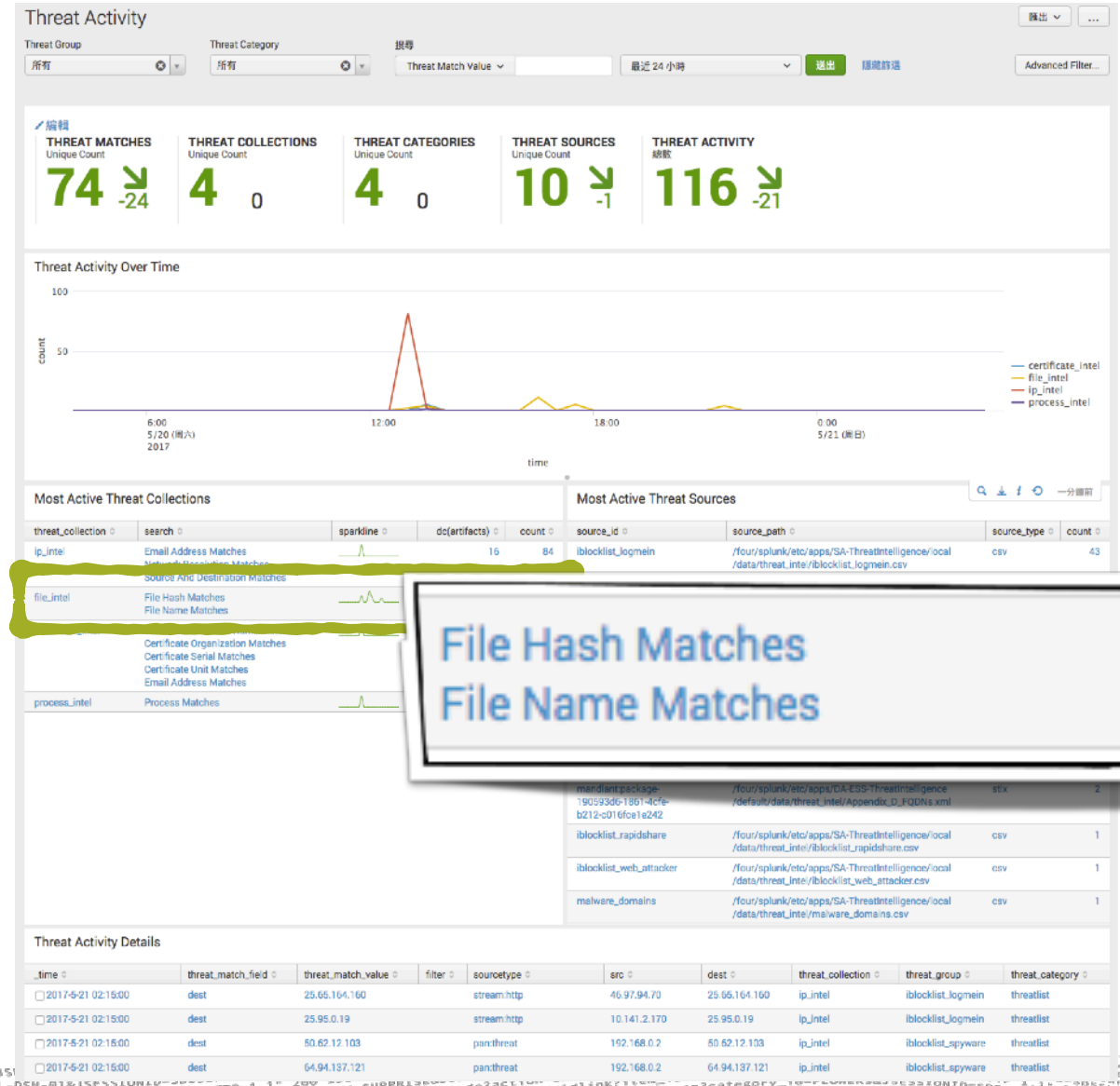
Protocols, Connections Anomalies

Enterprise Security comprehensive monitoring



Protocols, Connections Anomalies

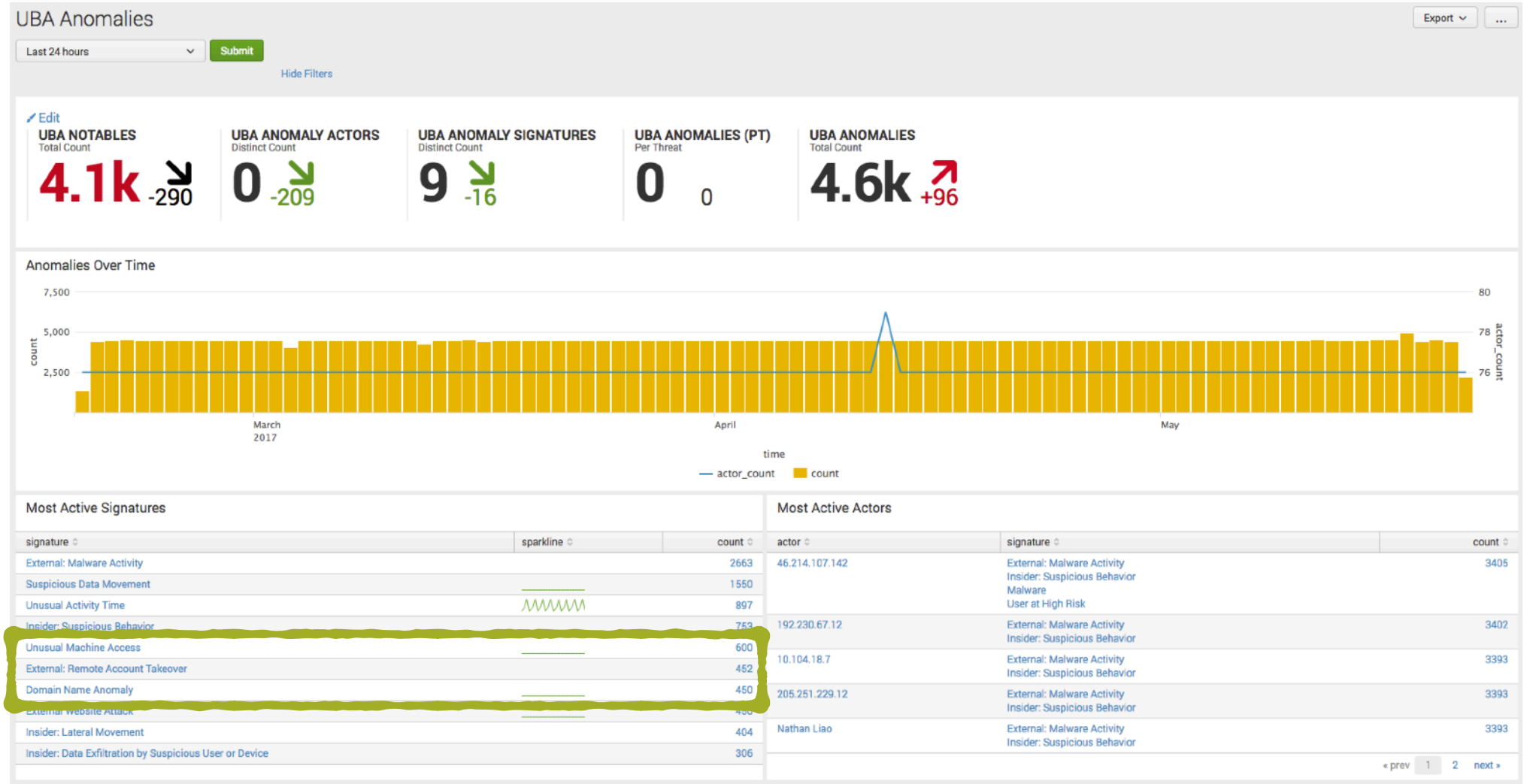
Enterprise Security comprehensive monitoring



splunk> listen to your data®

Protocols, Connections Anomalies

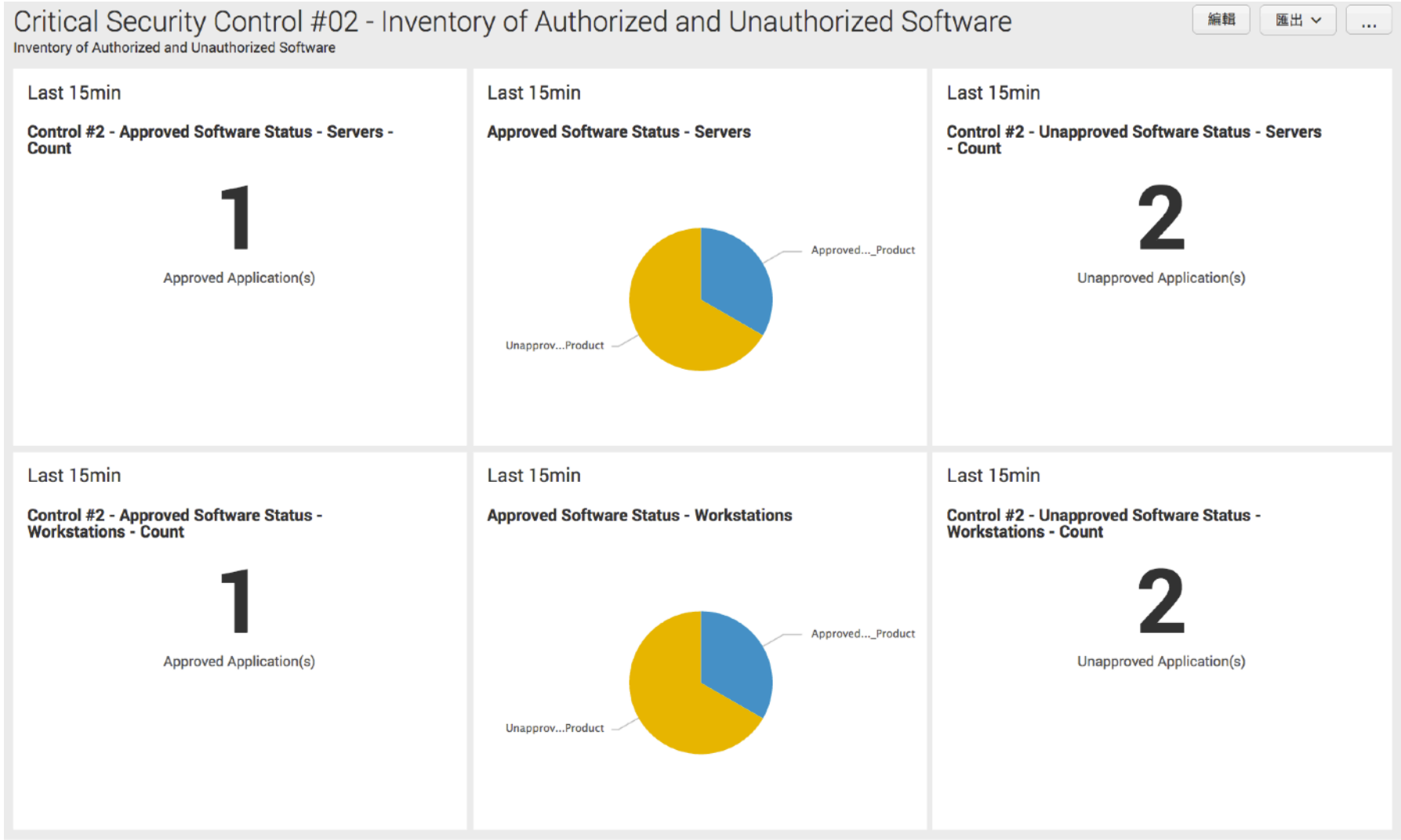
Enterprise Security comprehensive monitoring



splunk> listen to your data®

Endpoint Anomalies Tracking

Free App: CIS Critical Security Controls



splunk> listen to your data

Endpoint Anomalies Tracking

Free App: CIS Critical Security Controls

Critical Security Control #03 - Secure Configurations for Hardware and Software

編輯 匯出 ...

Secure Configurations for Hardware and Software

Last 15min

Filesystem Configuration Activity

_time	host	user	action	eventtype	change_type	file_name
2017/05/21 16:34:07	ch-demo-cis20	0	created	fs_notification	filesystem	passwd
2017/05/21 16:34:07	ch-demo-cis20	0	created	fschange	filesystem	passwd
2017/05/21 16:34:07	ch-demo-cis20	0	created	fschange_add_file	filesystem	passwd
2017/05/21 16:33:46	ch-demo-cis20	0	created	fs_notification	filesystem	passwd
2017/05/21 16:33:46	ch-demo-cis20	0	created	fschange	filesystem	passwd
2017/05/21 16:33:46	ch-demo-cis20	0	created	fschange_add_file	filesystem	passwd
2017/05/21 16:33:24	ch-demo-cis20	0	created	fs_notification	filesystem	hosts
2017/05/21 16:33:24	ch-demo-cis20	0	created	fschange	filesystem	hosts
2017/05/21 16:33:24	ch-demo-cis20	0	created	fschange_add_file	filesystem	hosts
2017/05/21 16:33:06	ch-demo-cis20	0	created	fs_notification	filesystem	passwd

« 上一頁 1 2 3 4 5 6 7 8 9 10 下一頁 »

splunk> listen to your data

Endpoint Anomalies Tracking

Free App: CIS Critical Security Controls

Critical Security Control #05 - Controlled Use of Administrative Privileges - Other Activity

編輯 匯出 ...

Controlled Use of Administrative Privileges

Last 24hr

Control #5 - Successful Logins from 10 Most Rare Users - Privileged Accounts

src_user	count	percent
ACMEAPP$	60	5.671078
root	497	46.975425
jack.bauer	501	47.353497

Last 15min

Control #5 - Privileged Actions/Activities (excluding auth and account creation/deletion events)

host	escalating_user	admin_account	system_message_(where_applicable)
ComputerName=WIN-L25DGSHI03K		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
		WIN-L25DGSHI03K$	A privileged service was called
ch-demo-cis20	mgarrahy	root	
	root	dmsys	
	root	dmsys	
	root	root	
	root	dmsys	
	root	mercury	
	root	root	
	root	dmsys	
	root	dmsys	
	root	mercury	
	root	dmsys	
	root	root	
	root	dmsys	
	root	dmsys	
	root	root	

Endpoint Anomalies Tracking

Free App: CIS Critical Security Controls

Critical Security Control #13 - Data Protection

Data Protection

編輯 匯出 ...

Last 7days

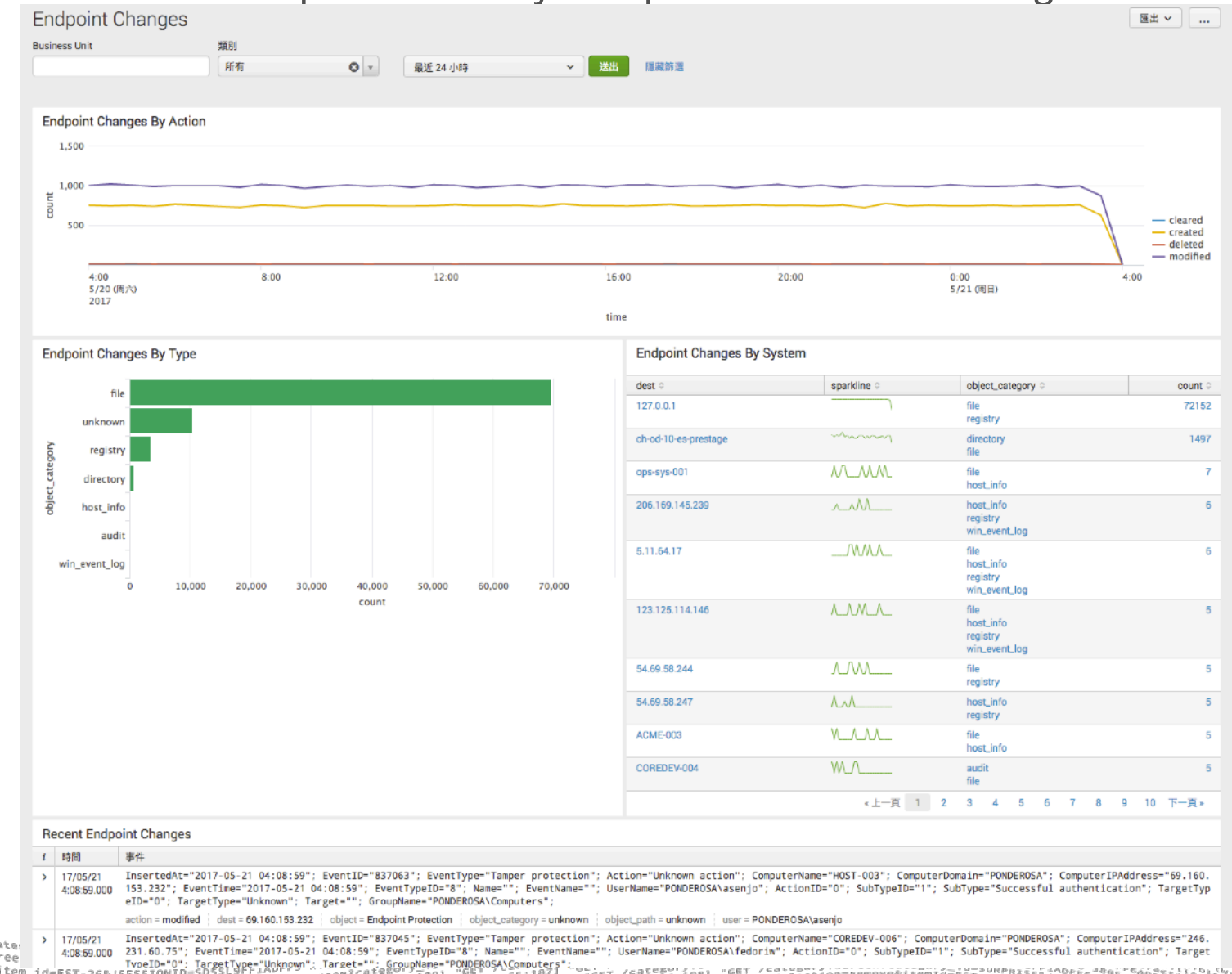
Control #13 - Rare DNS queries (Potential Exfil Domains)

dns_query	count	percent
0.14.169.135.dnsbugtest.0.14.169.135.in-addr.arpa	1	0.000242
0.146.165.107.dnsbugtest.0.146.165.107.in-addr.arpa	1	0.000242
0.165.181.7.in-addr.arpa	1	0.000242
0.167.122.70.dnsbugtest.0.167.122.70.in-addr.arpa	1	0.000242
0.167.4.238.in-addr.arpa	1	0.000242
0.208.106.176.in-addr.arpa	1	0.000242
0.212.127.82.in-addr.arpa	1	0.000242
0.217.198.8.in-addr.arpa	1	0.000242
0.238.30.183.in-addr.arpa	1	0.000242
0.51.54.66.in-addr.arpa	1	0.000242

splunk> listen to your data

Endpoint Anomalies Tracking

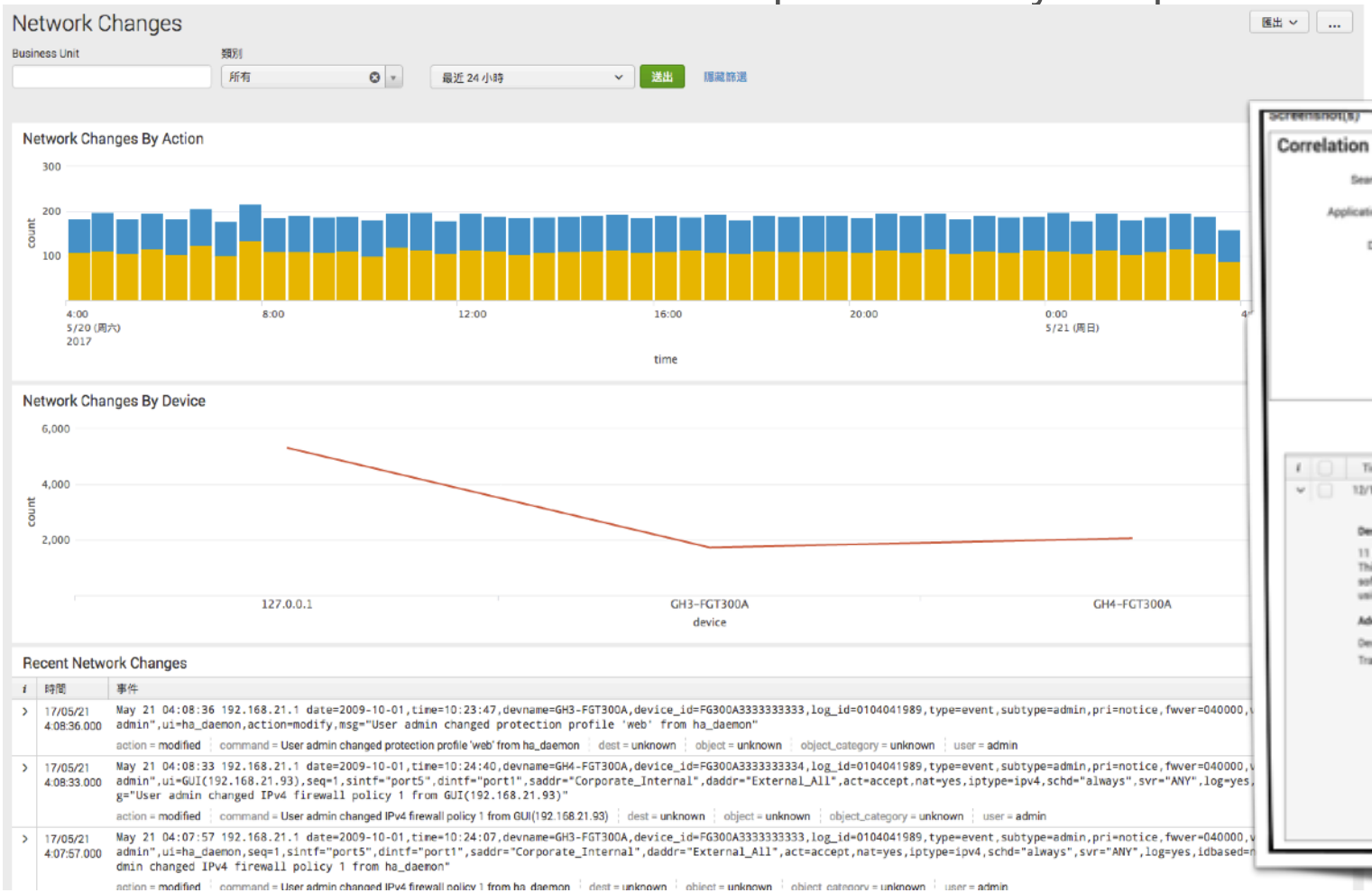
Enterprise Security comprehensive monitoring



splunk> listen to your data

Endpoint Anomalies Tracking

Enterprise Security comprehensive monitoring



Anomalous New Listening Port

splunk> listen to your data

Endpoint Anomalies Tracking

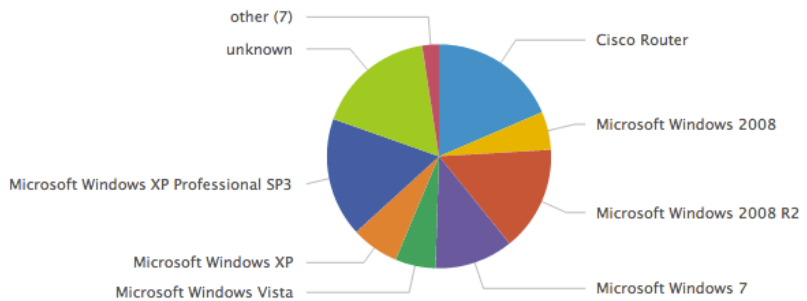
Enterprise Security comprehensive monitoring

System Center

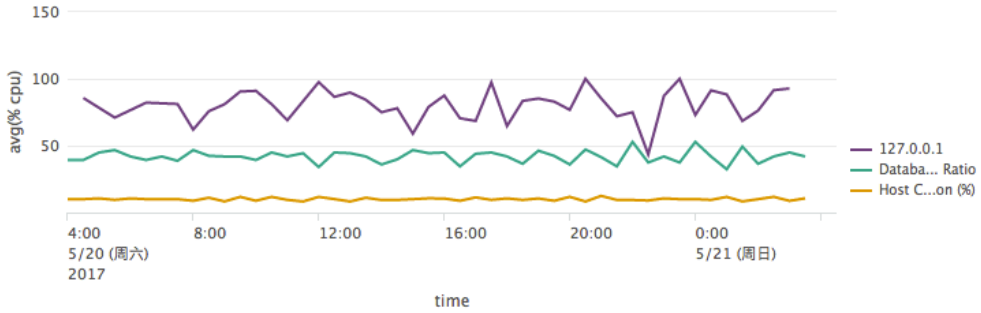
匯出 ...

Destination | Business Unit | 類別: 所有 | 最近 24 小時 | 送出 | 隱藏篩選

Operating Systems



Top-Average CPU Load By System



Services By System Count

service	dest_count
/etc/rc2_d/S47pppd	1
/etc/rc2_d/S89PRESERVE	1
/network/install:default	1
/network/nis/domain:default	1
/system/device/mpxio-upgrade:default	1
EvernoteHelper	1
Google Drive	1
Microsoft Database Daemon	1
NetworkManager	1
OSEASV	1

« 上一頁 1 2 下一頁 »

Ports By System Count

transport	dest_port	dest_count
tcp	270	10
tcp	1012	9
tcp	752	9
tcp	168	8
tcp	178	8
tcp	182	8
tcp	328	8
tcp	501	8
tcp	586	8
tcp	788	8

« 上一頁 1 2 3 4 5 6 7 8 9 10 下一頁 »

splunk> listen to your data

Attack patterns forensic

Enterprise Security/UBA comprehensive monitoring

New Search

```
index=bro sourcetype=bro_dns | stats count by query |  `ut_parse_simple(query)` | table query ut_netloc | `ut_shannon(ut_netloc)` | `ut_bayesian(ut_netloc)`
```

All time

✓ 375,958 events (before 4/11/17 6:08:24.000 PM) No Event Sampling

Events | Patterns | Statistics (49,393) | Visualization

20 Per Page | Format | Preview

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

query	ut_netloc	ut_bayesian	ut_shannon
1buwlmybu$jsjuf6typlnqecuwlkiqu0	1buwlmybu$jsjuf6typlnqecuwlkiqu0	0.9999994498379623	4.172185915404347
1buwlmybu$jsjuf6typlnqecuwlkiqu0.defcon.org	1buwlmybu$jsjuf6typlnqecuwlkiqu0.defcon.org	0.9999998789725344	4.533643863468259
1buwlmybu$jsjuf6typlnqecuwlkiqu0.openwifi.defcon.org	1buwlmybu$jsjuf6typlnqecuwlkiqu0.openwifi.defcon.org	0.9999999509980713	4.525190687461469
%28http.defcon.org	%28http.defcon.org	0.9831518861758666	3.836591668108979
(empty)	(empty)	0.6162352890255021	2.8073549220576046
(none)	(none)	0.6422373171805791	2.2516291673878226
*.2002:5968:c28e::53	*.2002:5968:c28e::53		
*.2002:d596:2a92:1:71:53::	*.2002:d596:2a92:1:71:53::		
*.defcon.org	*.defcon.org		
*.ns1.censurfridns.dk	*.ns1.censurfridns.dk		
*.ns2.censurfridns.dk	*.ns2.censurfridns.dk		
*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00	*\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00		
+0aaaaaaaabhhavwd7tjxw==.xklsl29das.mooo.com	+0aaaaaaaabhhavwd7tjxw==.xklsl29das.mooo.com		
+0eaaaaaaaanduocqspvfa==.xklsl29das.mooo.com	+0eaaaaaaaanduocqspvfa==.xklsl29das.mooo.com		
+0iaaaaaaabzuil7pzmkxa==.xklsl29das.mooo.com	+0iaaaaaaabzuil7pzmkxa==.xklsl29das.mooo.com		
+0maaaaaaabphjehptqkbg==.xklsl29das.mooo.com	+0maaaaaaabphjehptqkbg==.xklsl29das.mooo.com		
+0qaaaaaaaahruabi2fmcg==.xklsl29das.mooo.com	+0qaaaaaaaahruabi2fmcg==.xklsl29das.mooo.com		
+0uaaaaaaad20fapu32nga==.xklsl29das.mooo.com	+0uaaaaaaad20fapu32nga==.xklsl29das.mooo.com		
+a0aaaaaaaavh03vxx78hq==.xklsl29das.mooo.com	+a0aaaaaaaavh03vxx78hq==.xklsl29das.mooo.com		
+a4aaaaaaabiuigkmxruaw==.xklsl29das.mooo.com	+a4aaaaaaabiuigkmxruaw==.xklsl29das.mooo.com	0.9999989941387581	3.988316710610012

Find DGA domain names

```
| `ut_parse(query)`
| `ut_shannon(ut_netloc)`
| `ut_bayesian(ut_netloc)`
```

URL Toolbox
https://splunkbase.splunk.com/app/2734

splunk> listen to your data

Attack patterns forensic

Enterprise Security/UBA comprehensive monitoring

新搜尋

另存為 新表格 關閉

```
| `datamodel("UEBA","UEBA_Anomalies")` | search All_UEBA_Events.signature="Domain Name Anomaly" | stats count by anomaly_category dvc_pci_domain
  All_UEBA_Events.description
```

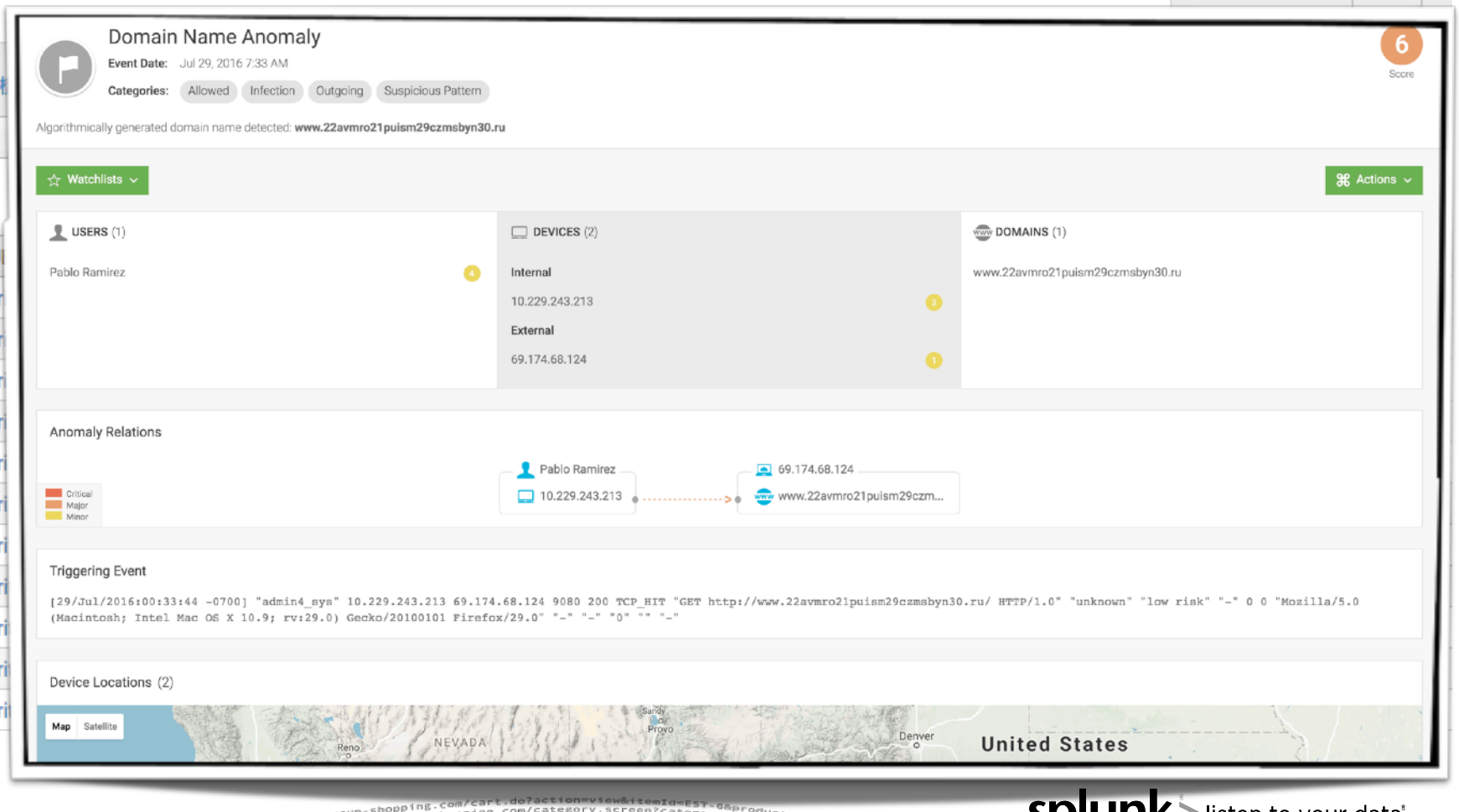
日期時間範圍

✓ 432 個事件 (17/05/20 5:00:00.000 至 17/05/21 5:03:30.000) 無事件取樣

事件 模式 統計資料 (24) 視覺化

每頁 20 個 格式 預覽

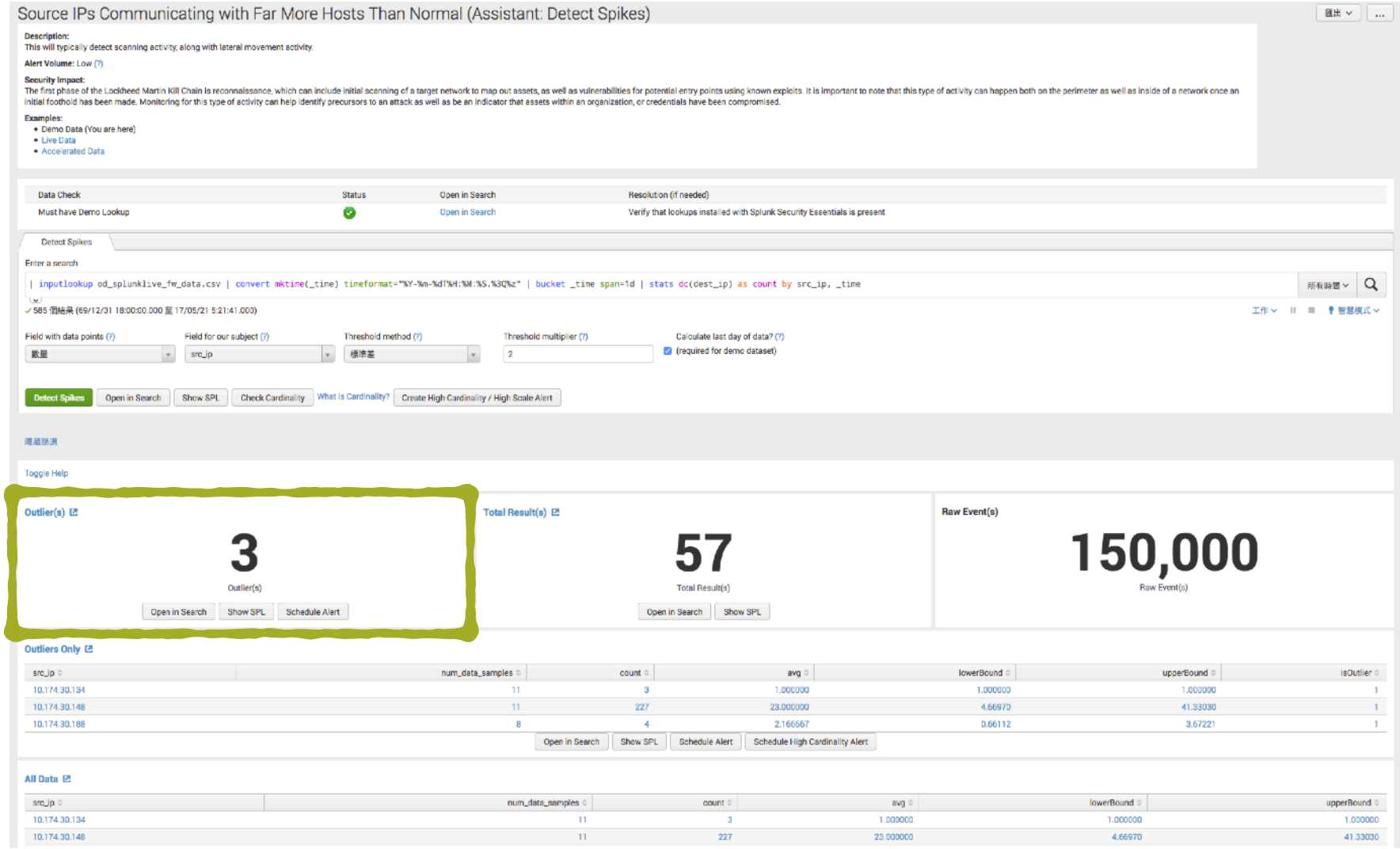
anomaly_category	dvc_pci_domain	All_UI
Allowed	untrust	Algori
Infection	untrust	Algori
Outgoing	untrust	Algori
SuspiciousPattern	untrust	Algori
Allowed	untrust	Algori
Allowed	untrust	Algori
Allowed	untrust	Algori
Allowed	untrust	Algori
Allowed	untrust	Algori
Infection	untrust	Algori
Infection	untrust	Algori



splunk> listen to your data

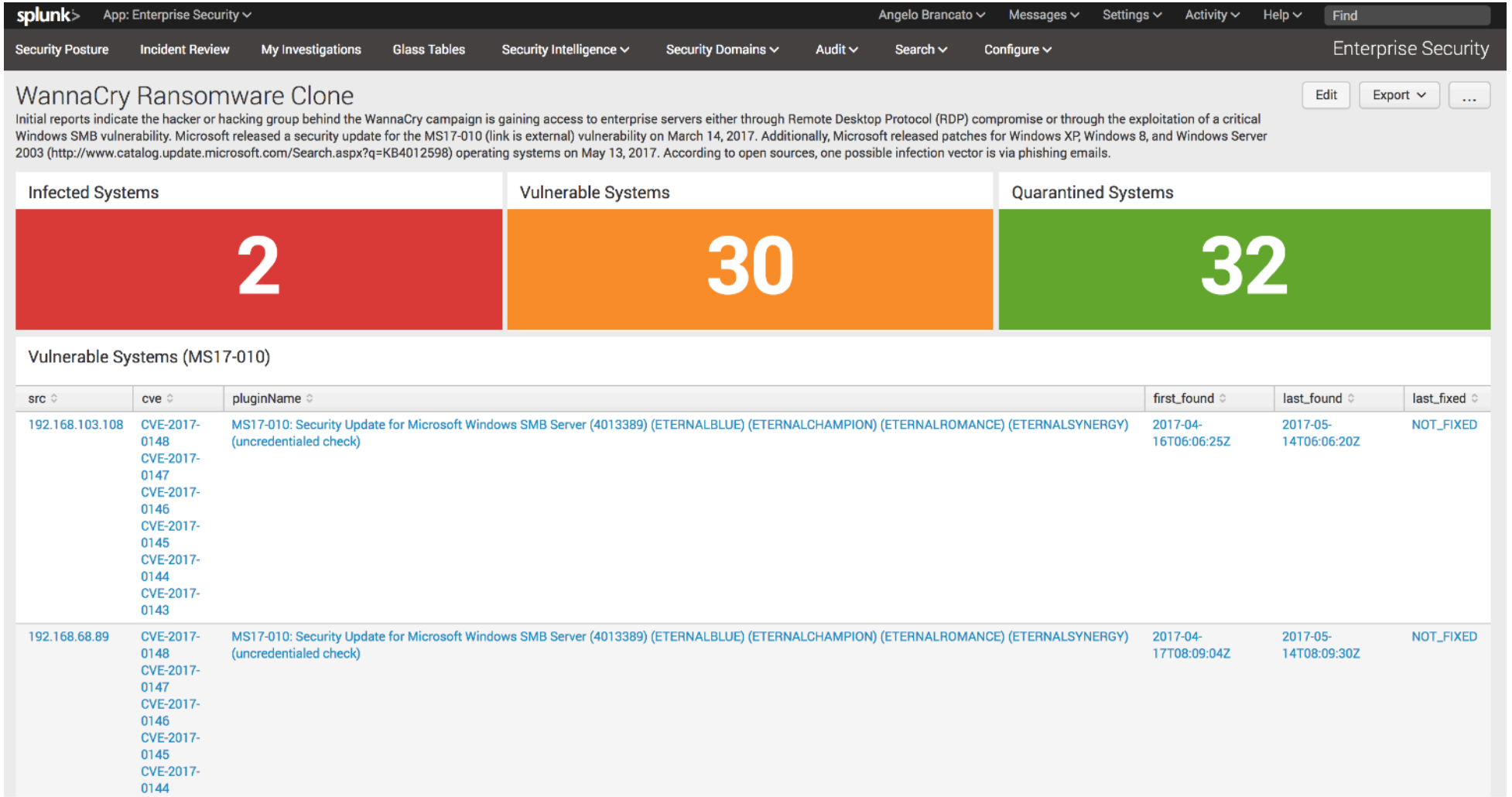
Attack patterns forensic

Enterprise Security/UBA comprehensive monitoring



Attack patterns forensic

Enterprise Security/UBA comprehensive monitoring



Attack patterns forensic

Enterprise Security/UBA comprehensive monitoring

```
index=ransomware tag=communicate sourcetype="stream:tcp" src=* dest*
| table _time, sourcetype, src src_port dest dest_port app bytes
| sort + _time
| lookup ip_intel ip as dest
| fields - address city country domain organization_id organization_name postal_code registration_time state_prov weight
```

All time

✓ 22 events (before 5/21/17 5:28:07.000 AM) No Event Sampling

Job Verbose Mode

Events (22) Patterns Statistics (22) Visualization

20 Per Page Format Preview

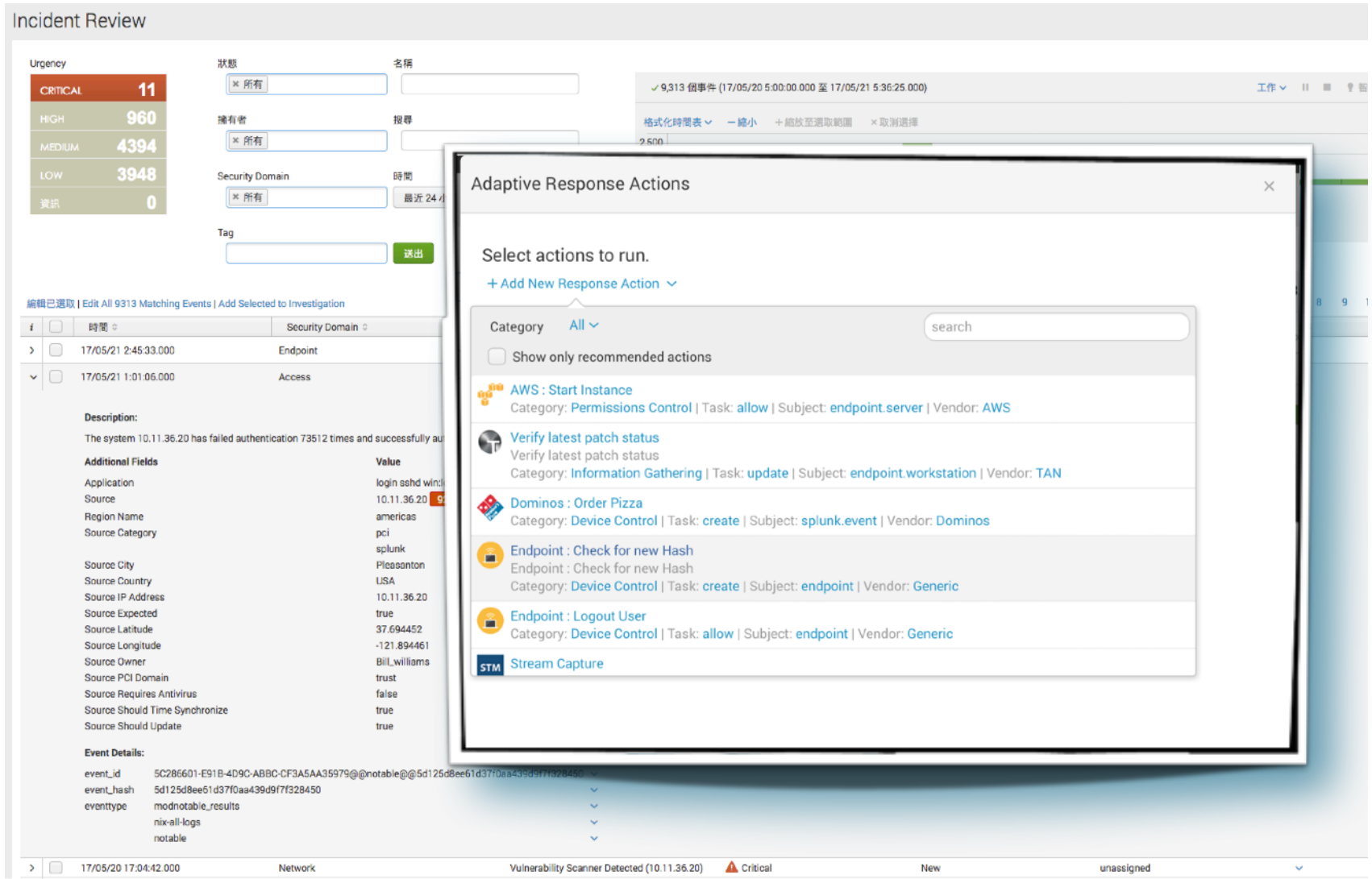
< Prev 1 2 Next >

_time	sourcetype	src	src_port	dest	dest_port	app	bytes	description	threat_key	time
2017-05-12 14:33:39.002	stream:tcp	192.168.56.10	49389	128.31.0.39	9101	tor	773267	The Onion Router	iblocklist_tor	1495328475.605377
2017-05-12 14:33:39.818	stream:tcp	192.168.56.10	49393	217.172.190.251	443	tor	684651	The Onion Router	iblocklist_tor	1495328476.174747
2017-05-12 14:33:39.990	stream:tcp	192.168.56.10	49388	163.172.35.247	443	unknown	192	The Onion Router	iblocklist_tor	1489111277.972336
2017-05-12 14:33:43.819	stream:tcp	192.168.56.10	49391	178.62.173.203	9001	tor	369609	The Onion Router	iblocklist_tor	1495328475.927543
2017-05-12 14:33:43.989	stream:tcp	192.168.56.10	49392	136.243.176.148	443	tor	344675	The Onion Router	iblocklist_tor	1495328475.605377
2017-05-12 14:33:44.100	stream:tcp	192.168.56.10	49392	136.243.176.148	443	tcp	5510	The Onion Router	iblocklist_tor	1495328475.605377
2017-05-12 14:33:44.132	stream:tcp	192.168.56.10	49392	136.243.176.148	443	tcp	13694	The Onion Router	iblocklist_tor	1495328475.605377
2017-05-12 14:33:47.142	stream:tcp	192.168.56.10	49387	171.25.193.9	80	ssl	8723	Tor The Onion Router	iblocklist_proxy iblocklist_tor	1476682443.022237 1495328475.927543
2017-05-12 14:34:45.444	stream:tcp	192.168.56.10	49412	163.172.185.132	443	tor	6185	The Onion Router	iblocklist_tor	1495328475.927543
2017-05-12 14:34:47.447	stream:tcp	192.168.56.10	49410	83.162.202.182	9001	tor	6178	The Onion Router	iblocklist_tor	1495328474.835394
2017-05-12 14:35:44.438	stream:tcp	192.168.56.10	49400	217.172.190.251	443	tor	883017	The Onion Router	iblocklist_tor	1495328476.174747

splunk> listen to your data®

Automatic “Respond” on findings

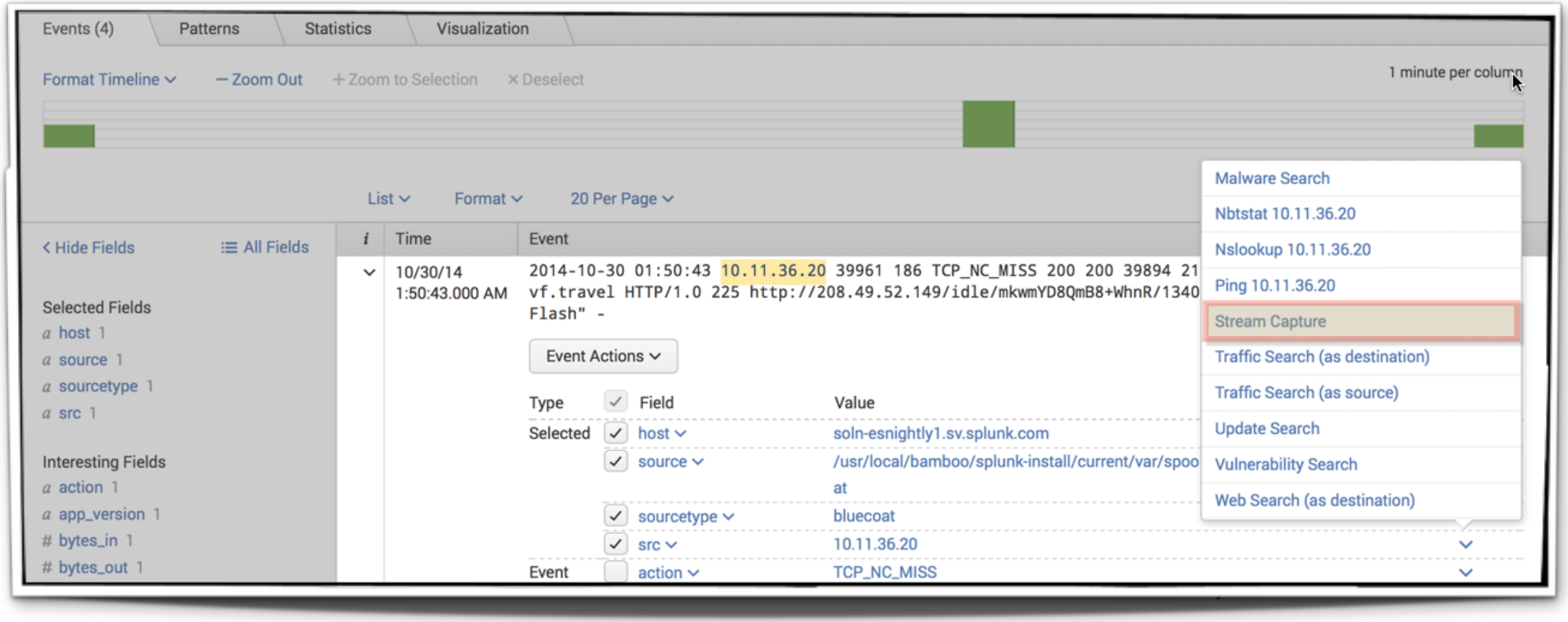
splunk>
Security Solution
on everything



splunk> listen to your data

Automatic - Adaptive Response

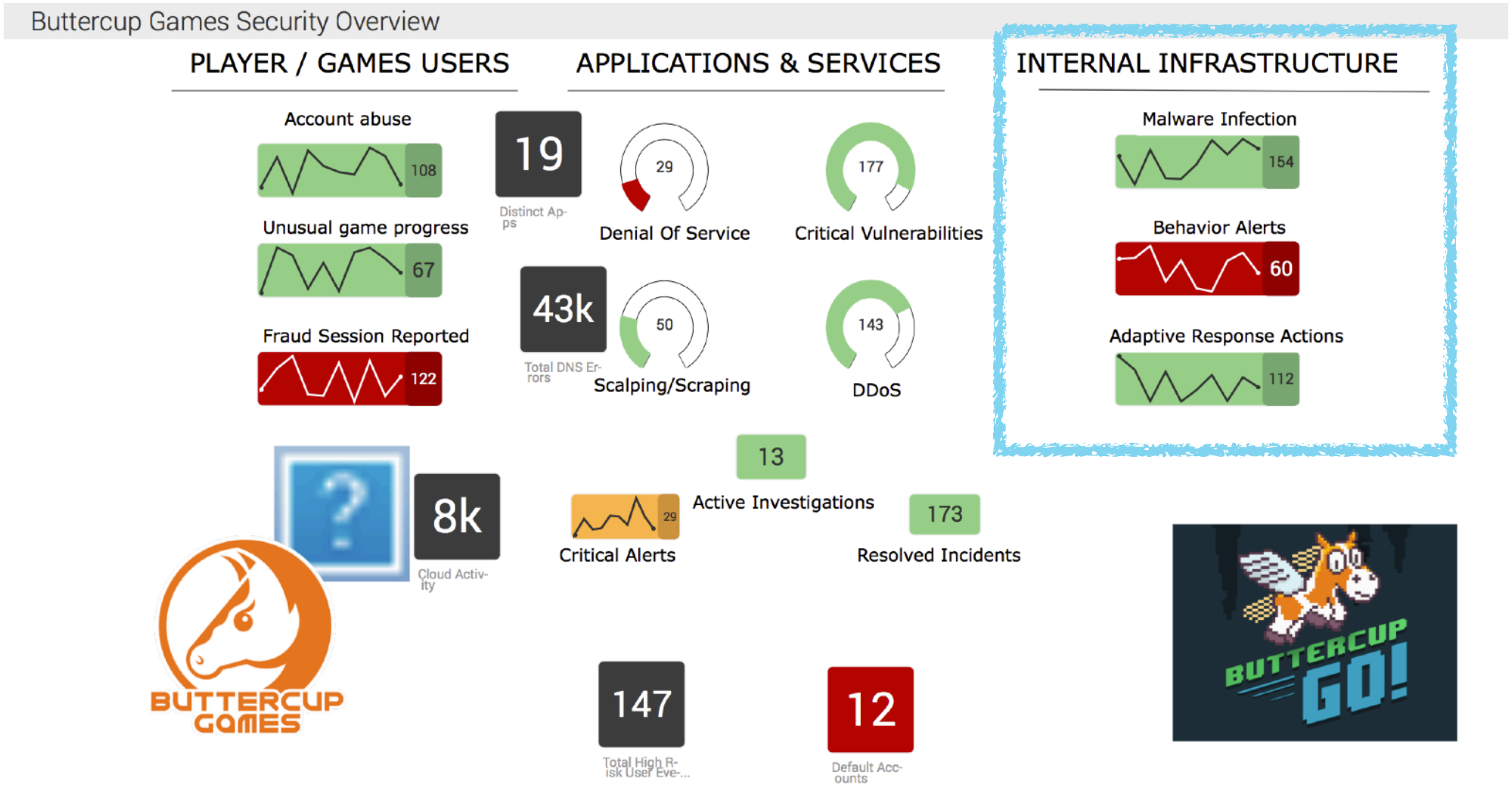
Enterprise Security comprehensive monitoring



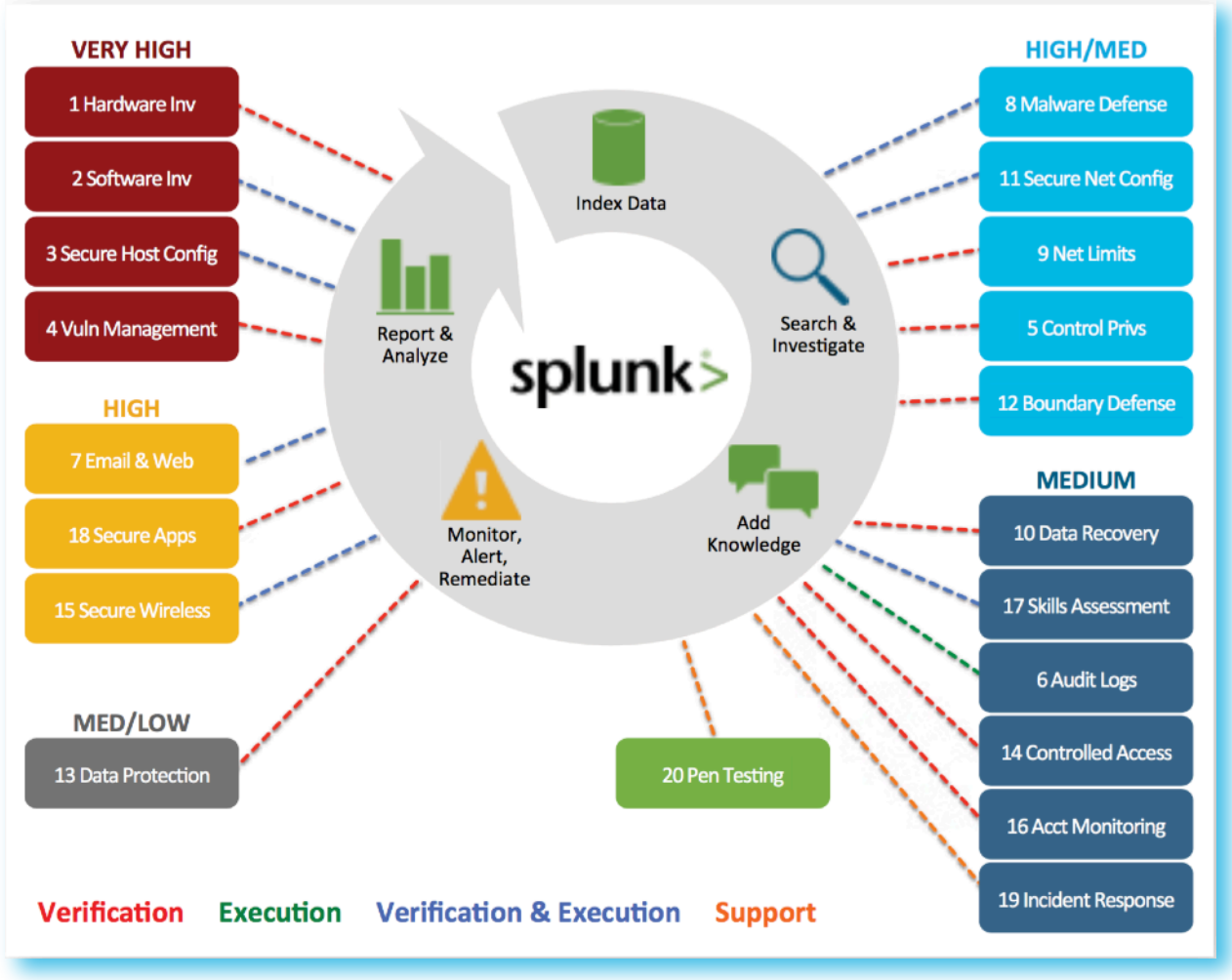
Quarantine infected systems, Shutdown endpoints, Virus scanning, Stream capture , Threat Intelligence update

splunk> listen to your data

Security control center - Glasstable



Defense against the attack chain



splunk> listen to your data®

Splunk Security Customers

Free Security Apps or Splunk Enterprise Security

Thousands of Global Security Customers

ExxonMobil
MOTOROLA
BT
Raytheon
JOHNS HOPKINS MEDICINE
UnionBank
CISCO
First Data
CommonwealthBank
China unicom中国联通
BARCLAYS
sears
Interac
verizon
BEA東亞銀行
HUGHES
ACCOR HOTELS
UALR
SAMSUNG
Taleo
AmericanData TECHNOLOGY, INC.
METRO BANK
sky
intuit
Colorado School of PUBLIC HEALTH
ABN·AMRO Private Banking
MLB.com
PSA PEUGEOT CITROËN
LinkedIn
The University of Akron
Deloitte.
GENERAL DYNAMICS
THE UNIVERSITY OF TEXAS AT AUSTIN
CEDARCRESTONE
FIS
SAFEWAY
TRIWEST HEALTHCARE ALLIANCE
Comcast

splunk> listen to your data

Splunk scores highest in 2016 Critical Capabilities for SIEM* report in all three Use Cases

Figure 1. Vendors' Product Scores for the Basic Security Monitoring Use Case

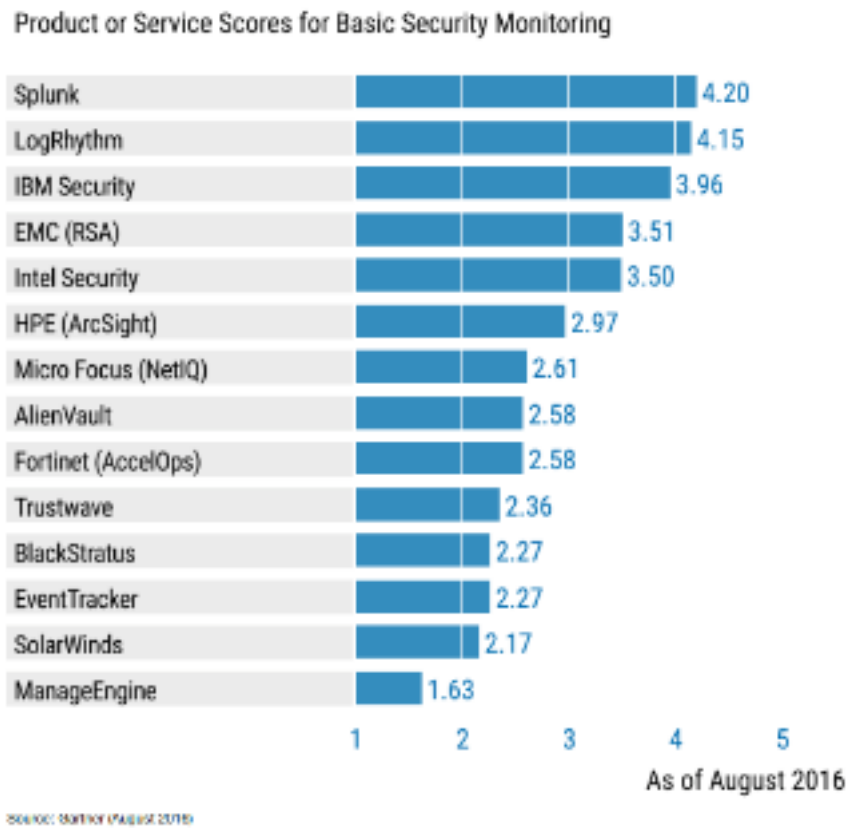


Figure 2. Vendors' Product Scores for the Advanced Threat Detection Use Case

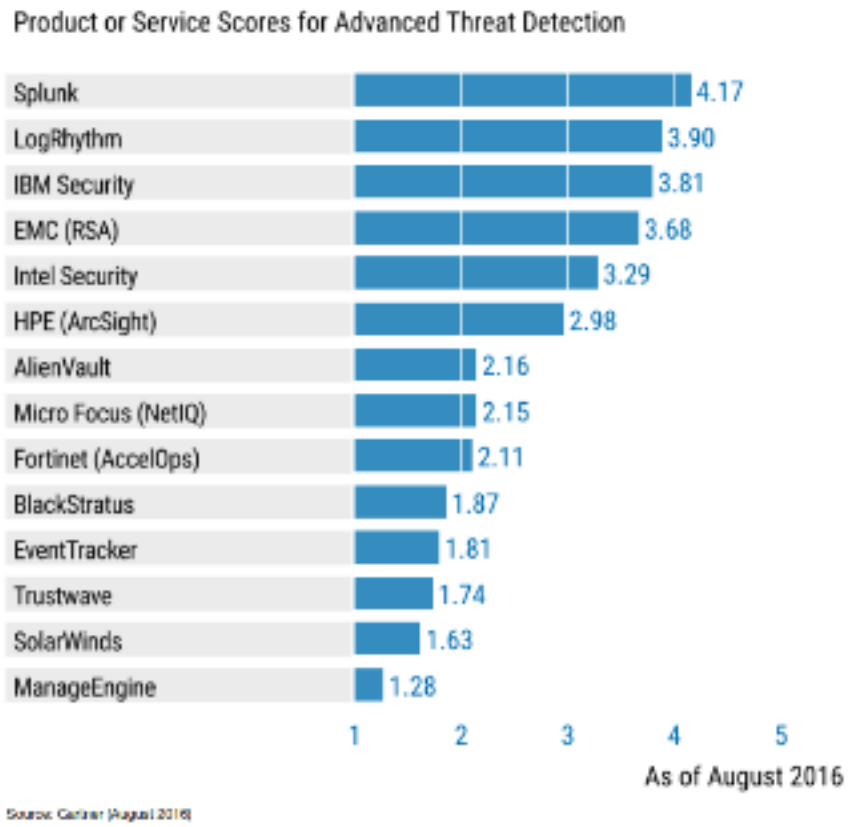
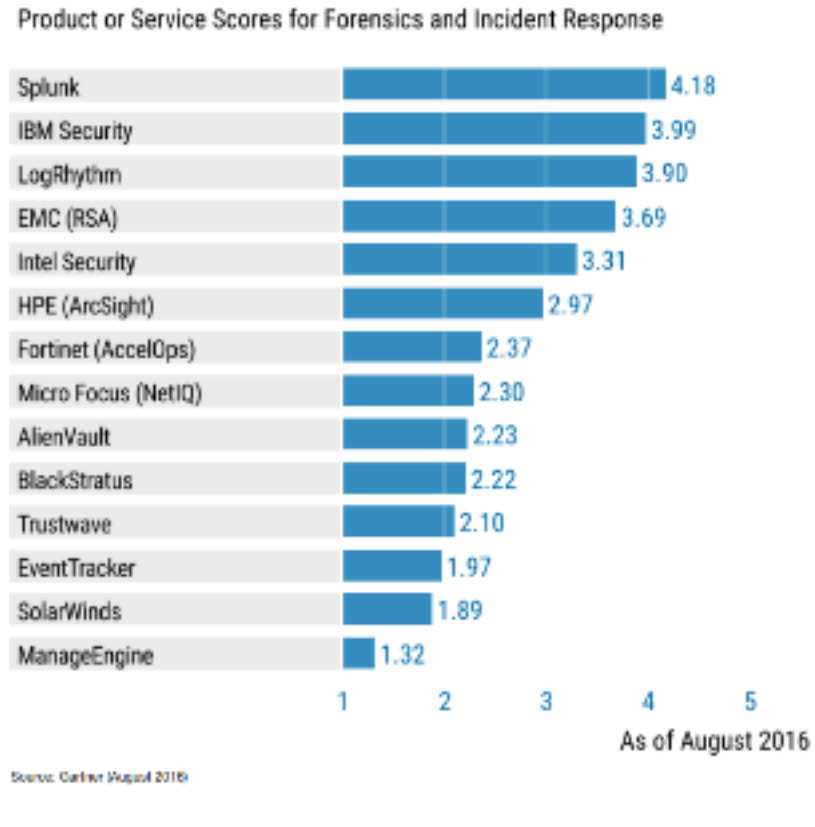


Figure 3. Vendors' Product Scores for the Forensics and Incident Response Use Case



*Gartner, Inc., Critical Capabilities for Security Information and Event Management, Oliver Rochford, Kelly M. Kavanagh, Toby Bussa. 10 August 2016 *This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Splunk. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose*.

splunk> listen to your data®