

# Splunk Enterprise Security

## Fast Response on Ransomware - WannaCrypt

Gary Chung

Senior Sales Engineer - Taiwan

May 22 2017

splunk >

# Forward-Looking Statements

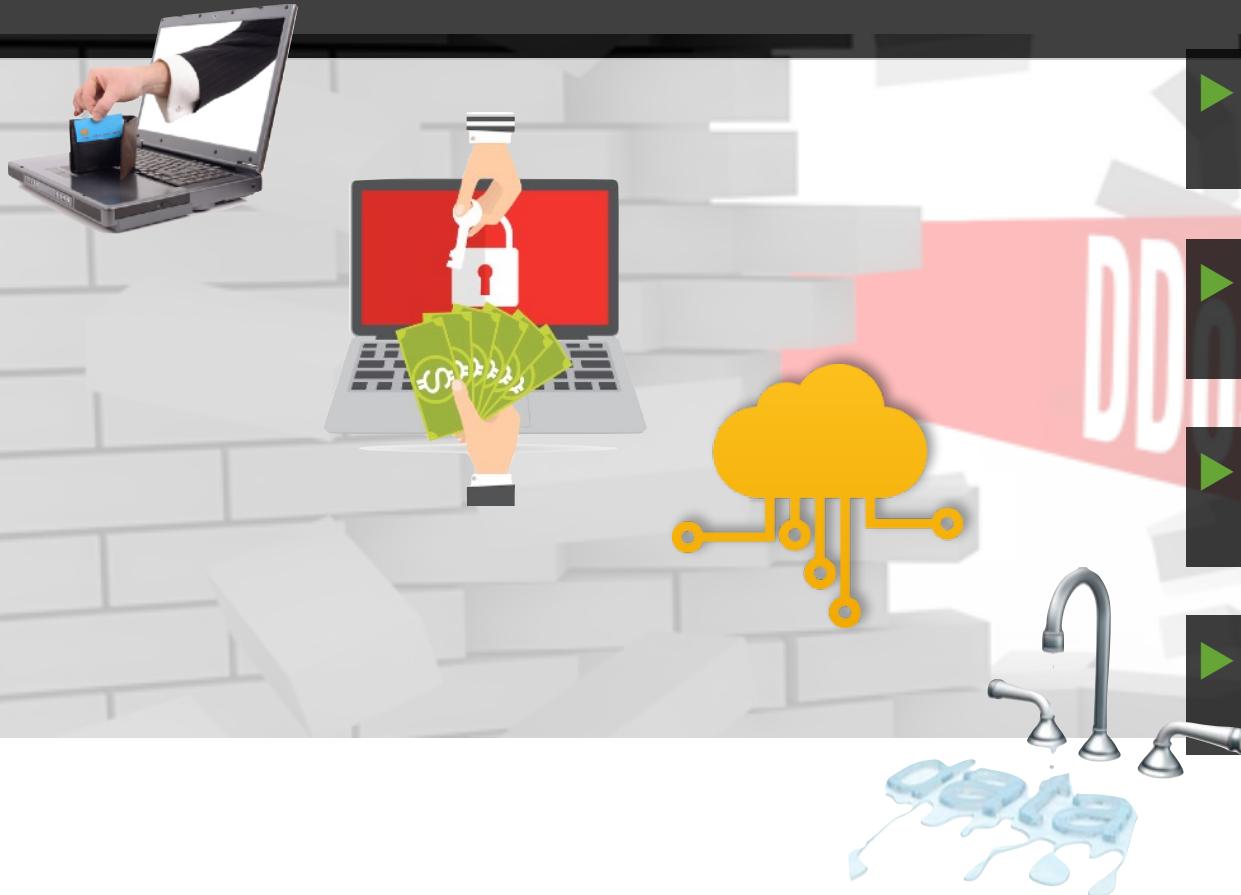
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

# Why should CIO/CISO concern on Security

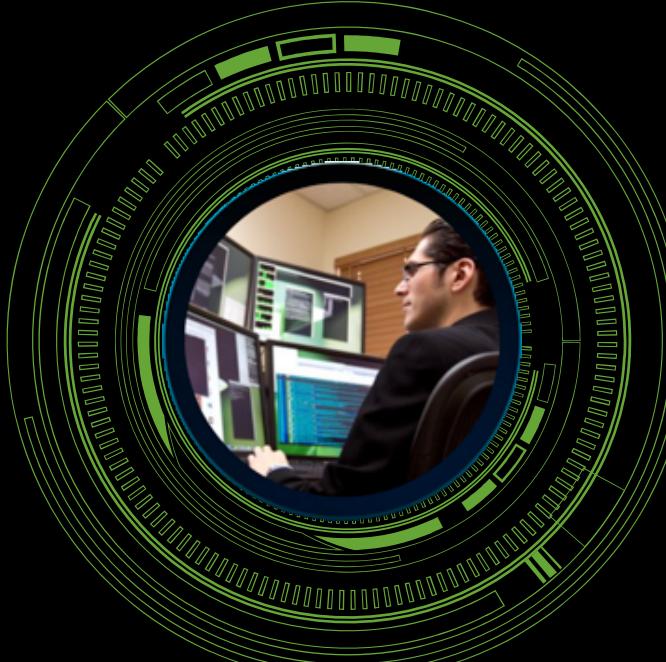
From simple service denial (DDOS, etc.) to online theft/blackmail



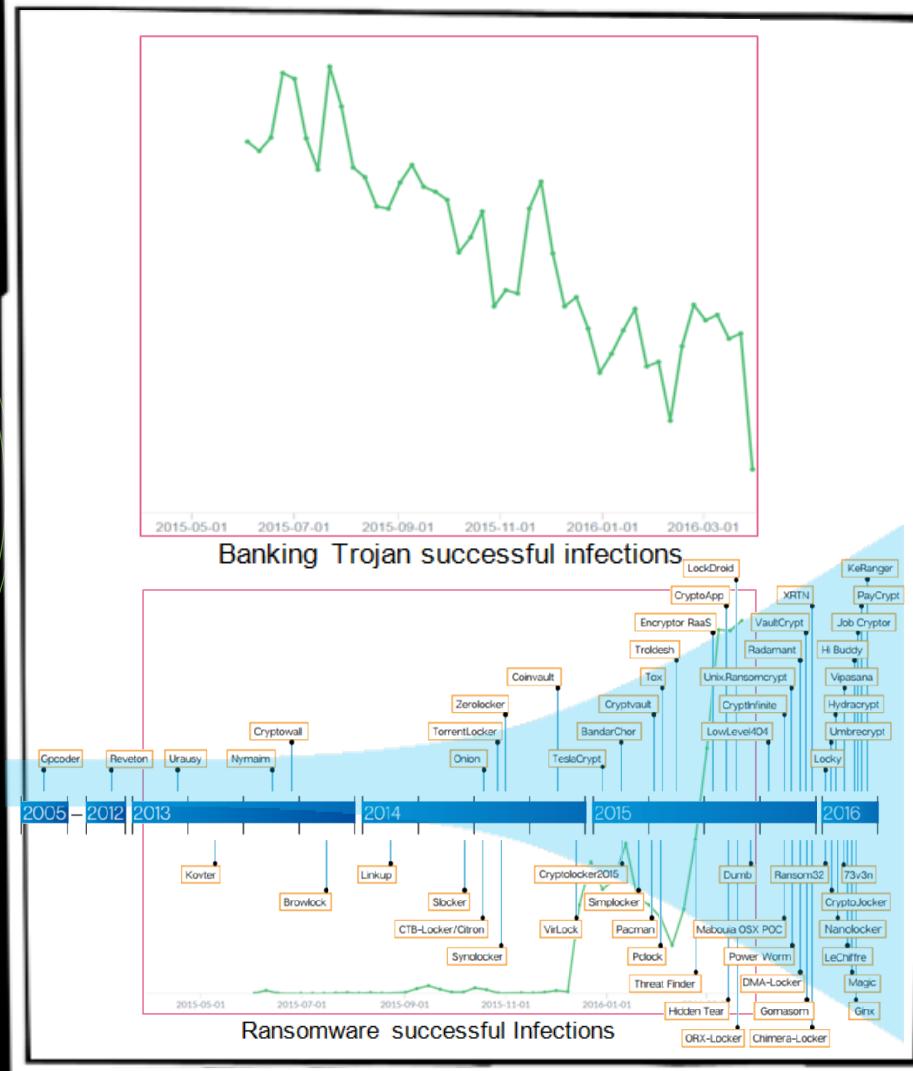
- ▶ Online Theft
- ▶ Ransomware
- ▶ Relay Server Attack
- ▶ PIM/Confidential Data Leakage

# Security Task is more complicated

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

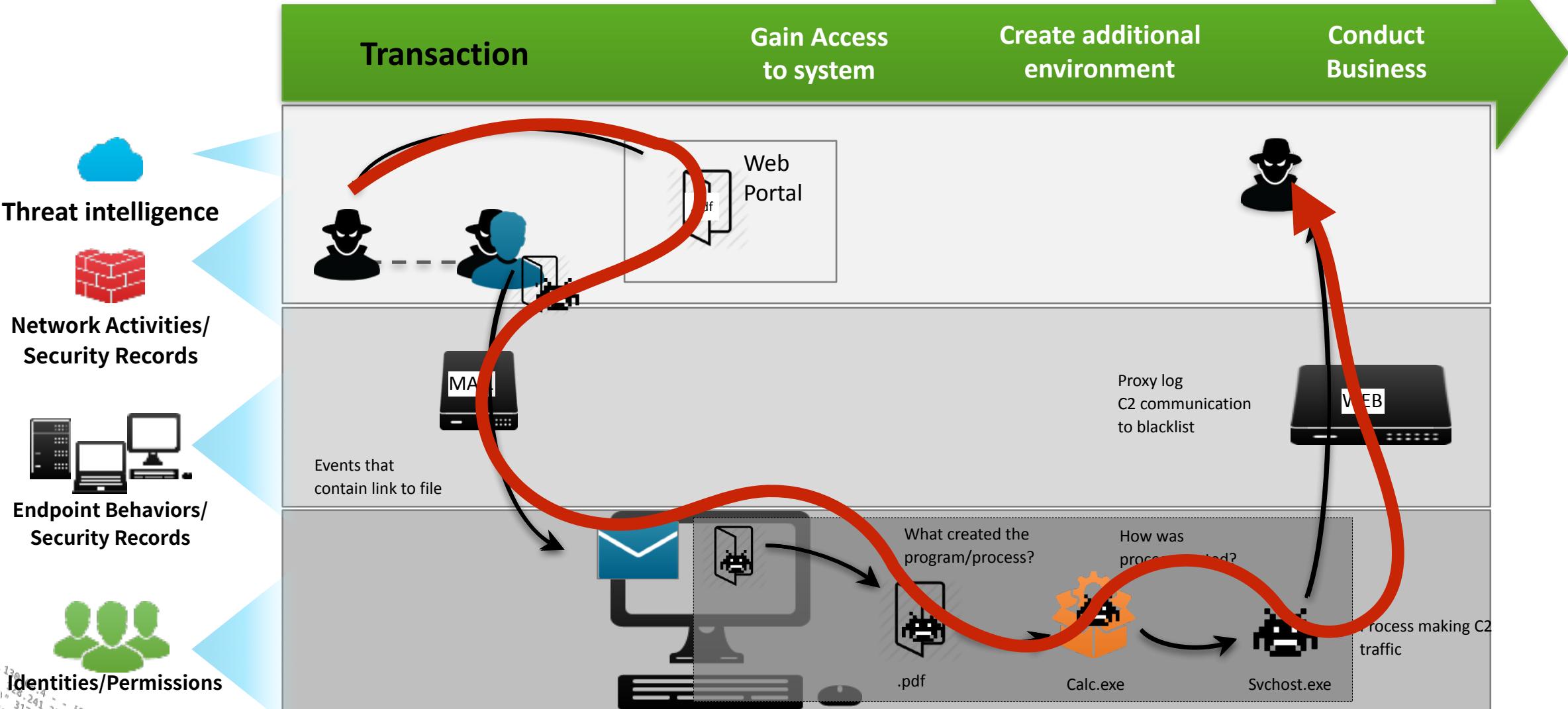


► Small Team



► Global SOC Team

# SOC daily work - KillChain Analysis



# SOC daily work - KillChain Analysis



IP Threat  
intelligence



115.29.46.99/32,zeus\_c2s  
61.155.10.0/24,cymru\_http



e-mail Record



Windows

System Records



User Identities  
(CMDB)

bad\_ip,threat\_intel\_source  
115.29.46.99/32,zeus\_c2s  
61.155.30.0/24,cymru\_http

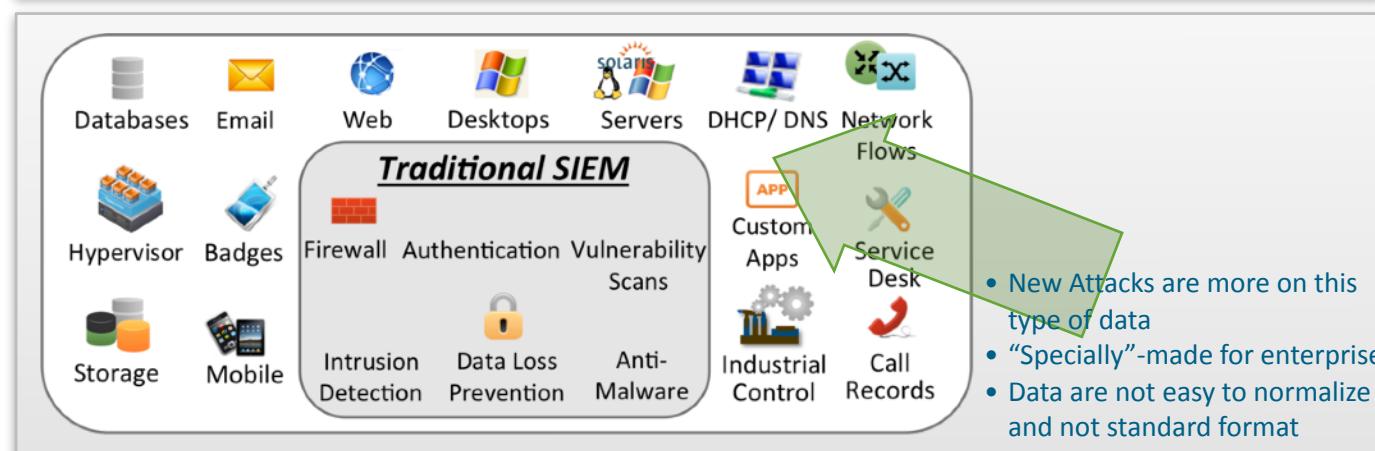
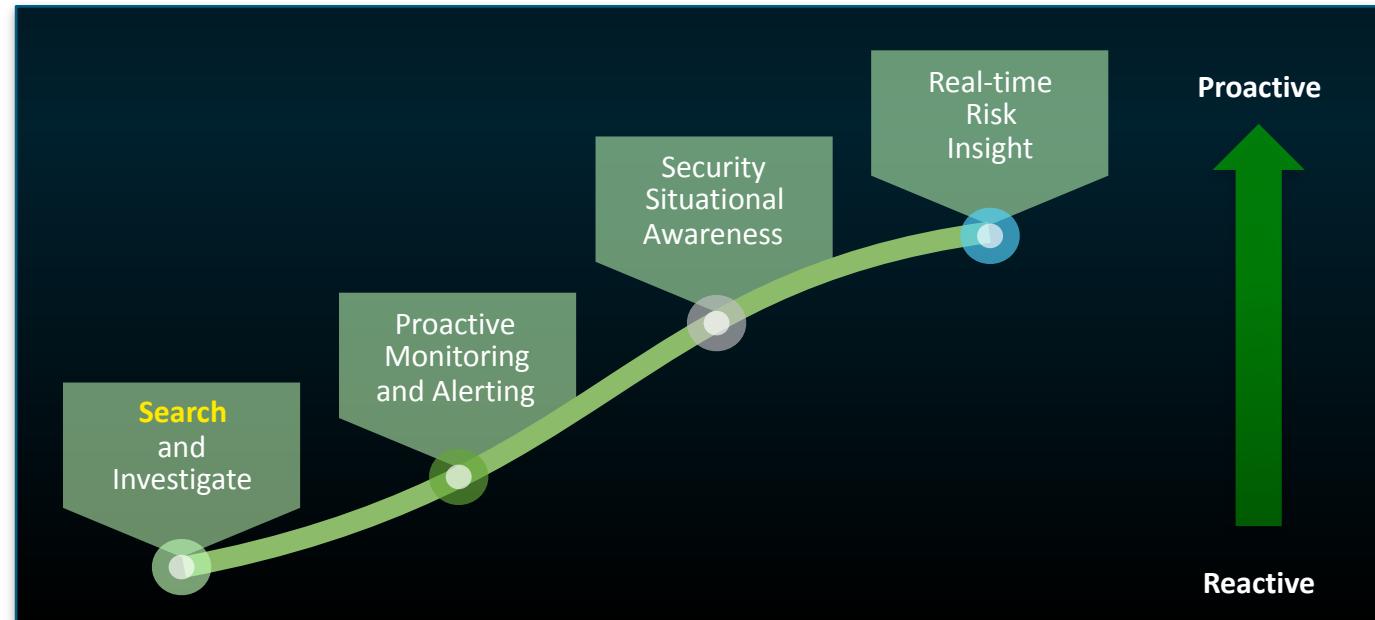
Subject: new commission report breakdown  
From: Jose Dave <jose.dave@buttercupgames.com>  
To: <chris.gilbert@buttercupgames.com>  
Content-type: multipart/mixed;  
Content-type: application/pdf; name="Q2\_commission.pdf"

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}

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 192.168.56.192.168.56.102 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 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 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 – 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 BEST PLACES TO WORK



FAST COMPANY



Honored in the U.S.  
WINNER



Gartner

**"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

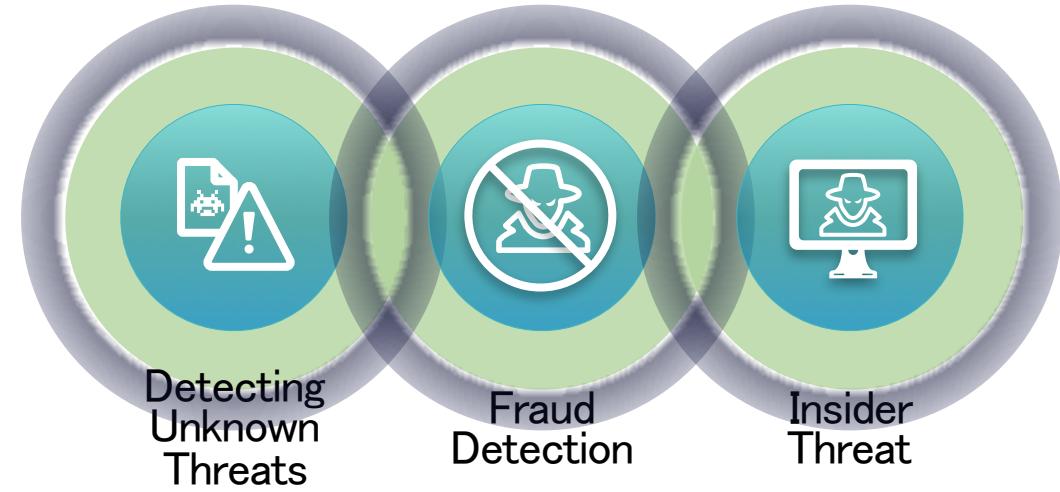


“...the rise in successful targeted attacks has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection”

## Threat Management

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

# Security Intelligence Use Cases



Splunk Enterprise  
Security™



Splunk User Behavior  
Analytics™

Platform for Operational Intelligence

# WannaCrypt

Understanding the lifecycle of a ransomware



splunk > listen to your data

# WannaCry

## Introduction

## What is Wan

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=3758722>

**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](#)

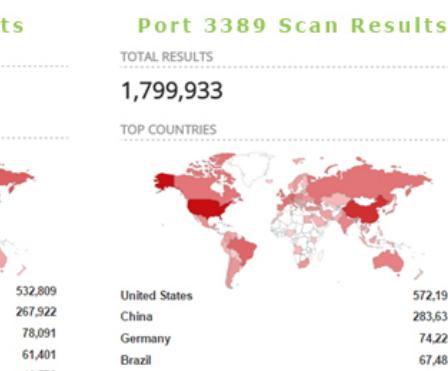
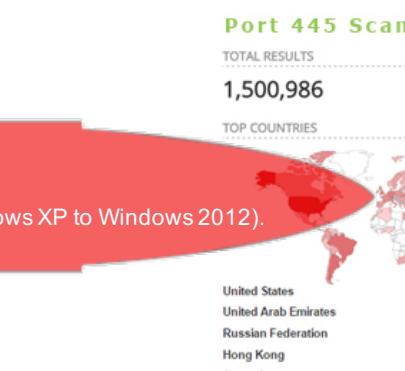


DOUBL  
Backdo

WA  
Bar

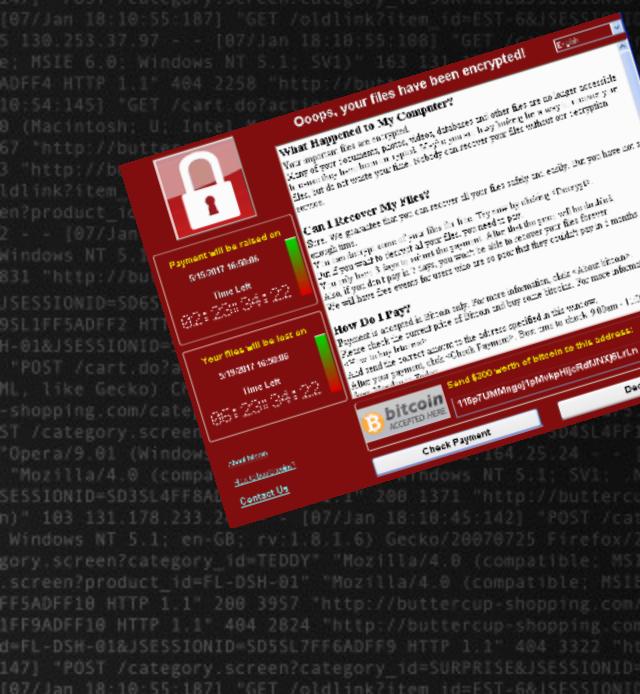
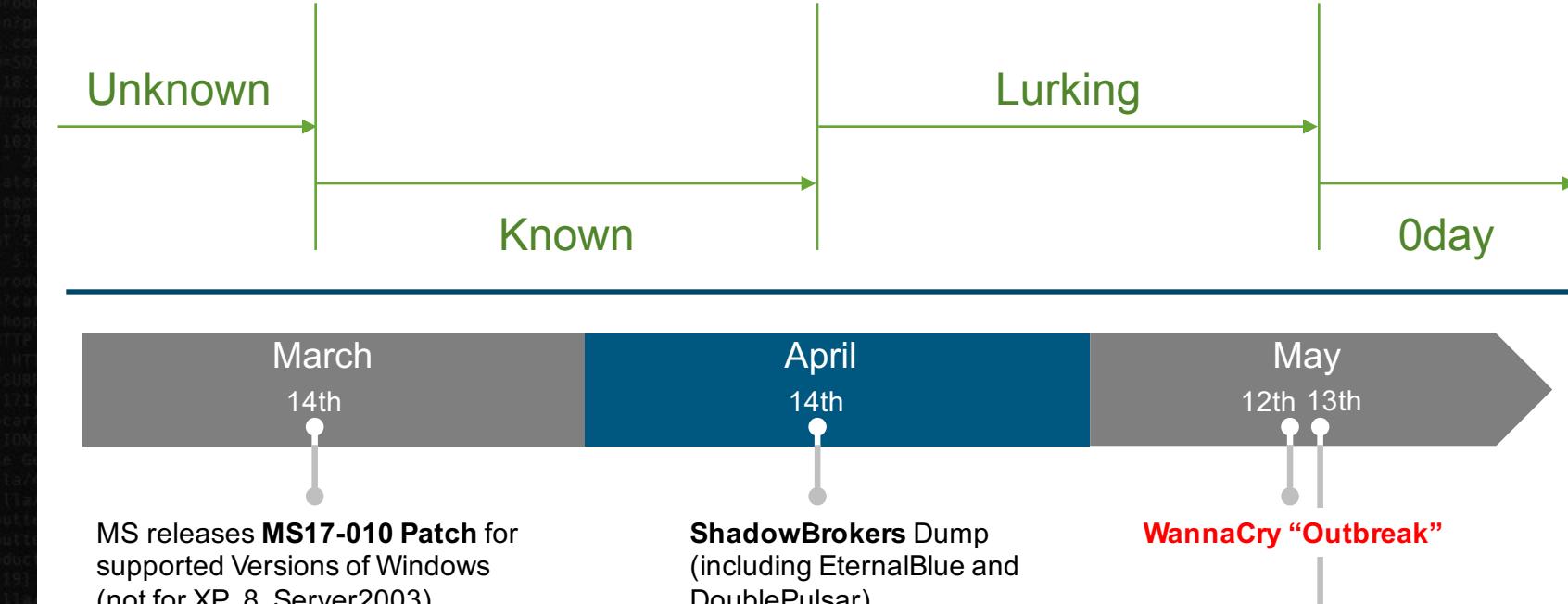
or

**ACRY** Remote Exploit via SMB & NBT (Windows X



# WannaCry

# From unknown to known, lurking to



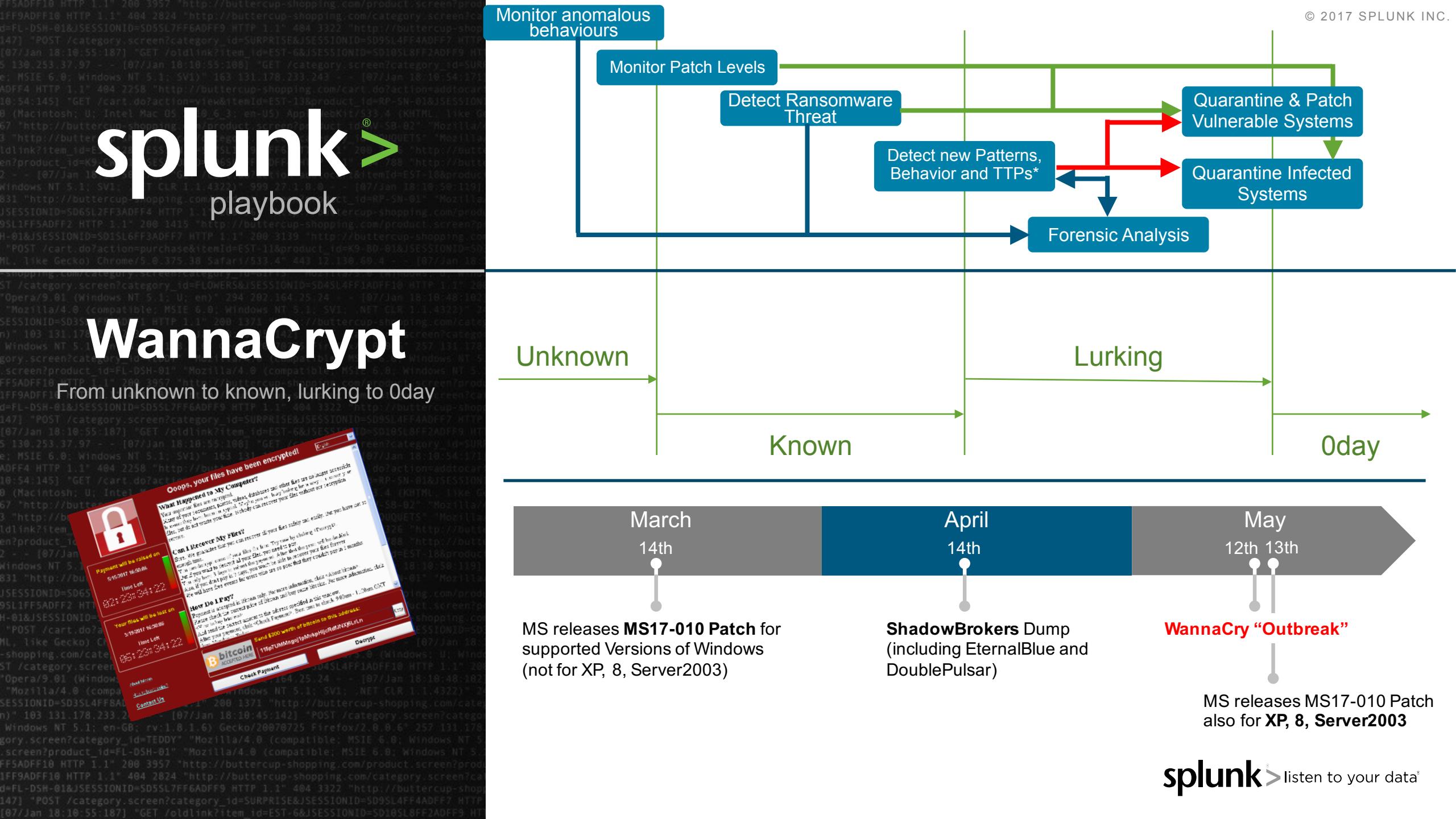


# Splunk helps organizations on known & unknown issues

---

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

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

# Quick response on Splunk Apps

Different choices for different situations



## Free CIS critical control app on building a monitor framework



## Splunk ES Use Case

# Automated SOC architecture on multiple data type correlations

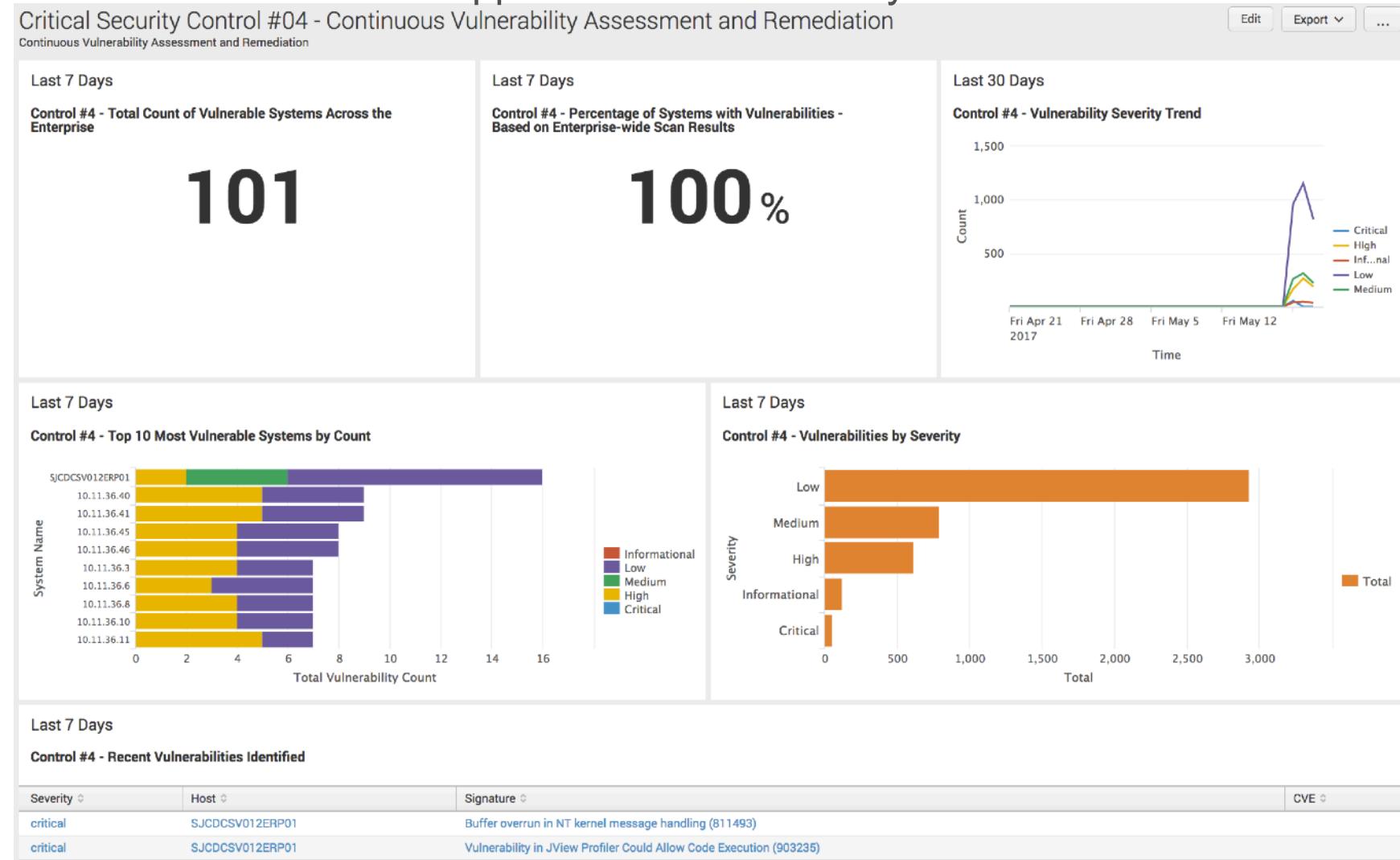


## Splunk UBA Use Case

# Machine learning on data anomalies to track advanced threats

# Patch management & Backup Tracking

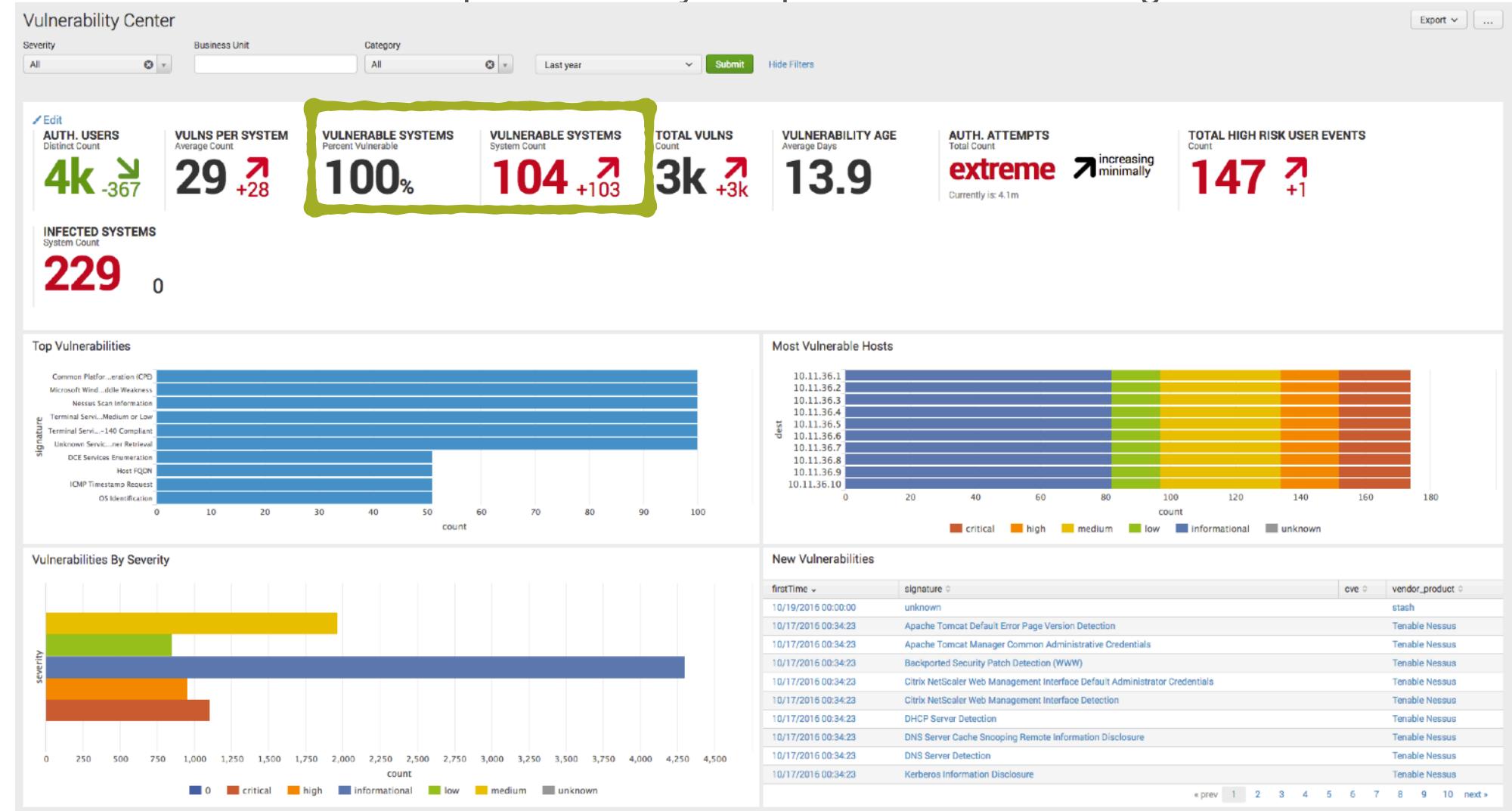
Free App: CIS Critical Security Controls



splunk > listen to your data®

# Patch management & Backup Tracking

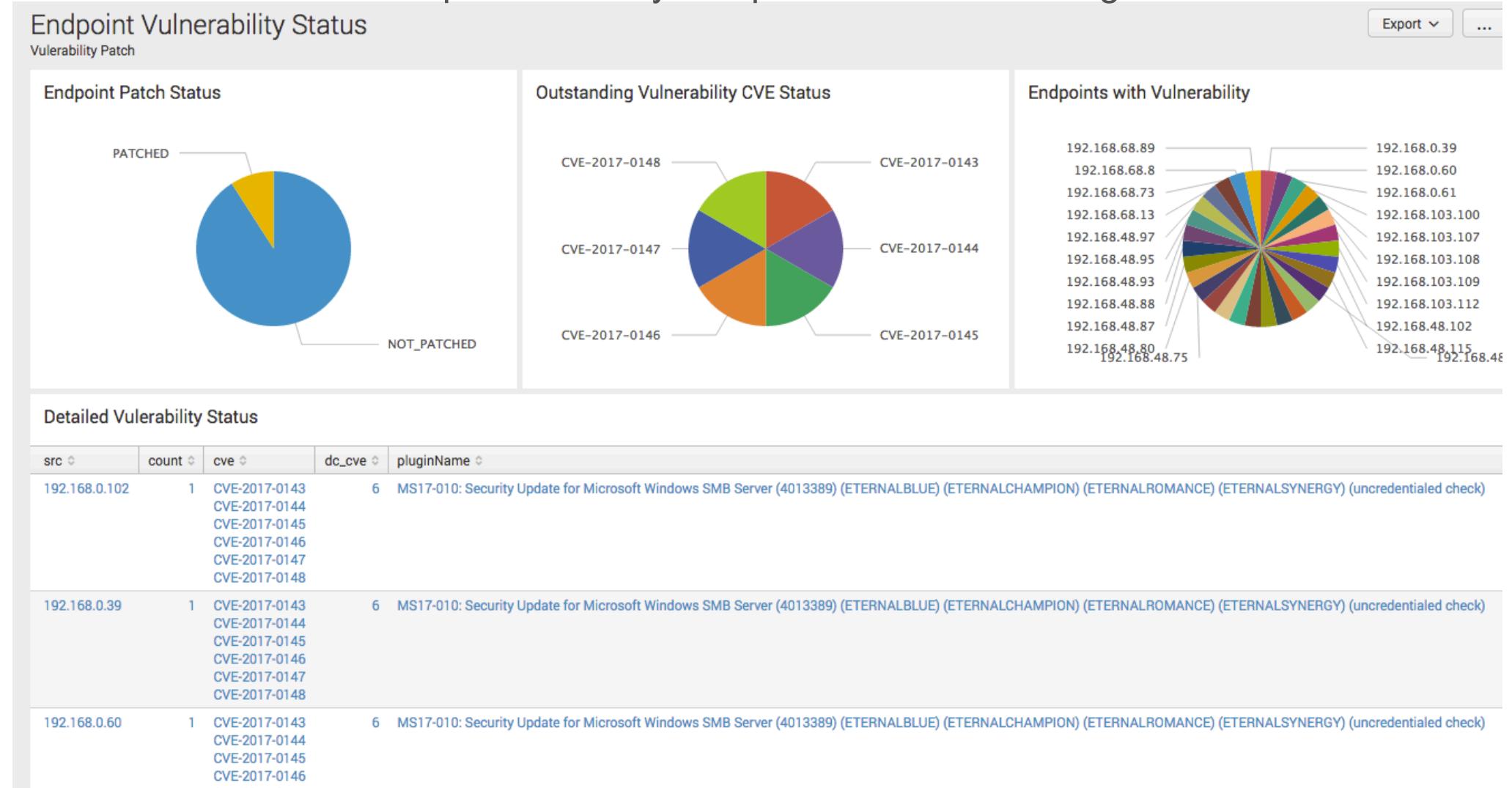
Enterprise Security comprehensive monitoring



splunk > listen to your data\*

# Patch management & Backup Tracking

Enterprise Security comprehensive monitoring



# Patch management & Backup Tracking

Enterprise Security comprehensive monitoring

Vulnerability Operations

Business Unit Category

All Month to date

Scan Activity Over Time

Mon May 1 2017

Vulnerabilities By Age

firstTime	count
05/05/2017 09:01:19	0
05/05/2017 13:02:03	0
05/05/2017 22:02:27	0
05/06/2017 16:01:58	0
05/05/2017 15:01:56	0
05/06/2017 02:02:47	0
05/06/2017 10:01:30	0
05/05/2017 14:01:51	0
05/06/2017 07:03:13	0
05/06/2017 16:02:06	0

Delinquent Scanning

dest	count
SRV001.logsource.eu	0
SRV001	0
unknown	0
COREDEV-003	0
SE-005	0

### Vulnerability Search

Vuln. Category Severity Signature Reference (bugtraq, cert, cve, etc.) Destination

Last 30 days  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	

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

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

Last 60min

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

Category	Percentage
Approved_Port	100%
Unapproved_Port	0%

Last 60min

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

Category	Percentage
Approved_Port	~90%
Unapproved_Port	~10%

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	
	22	
	25	
	28	
	35	
	37	
	41	
	43	
	60	

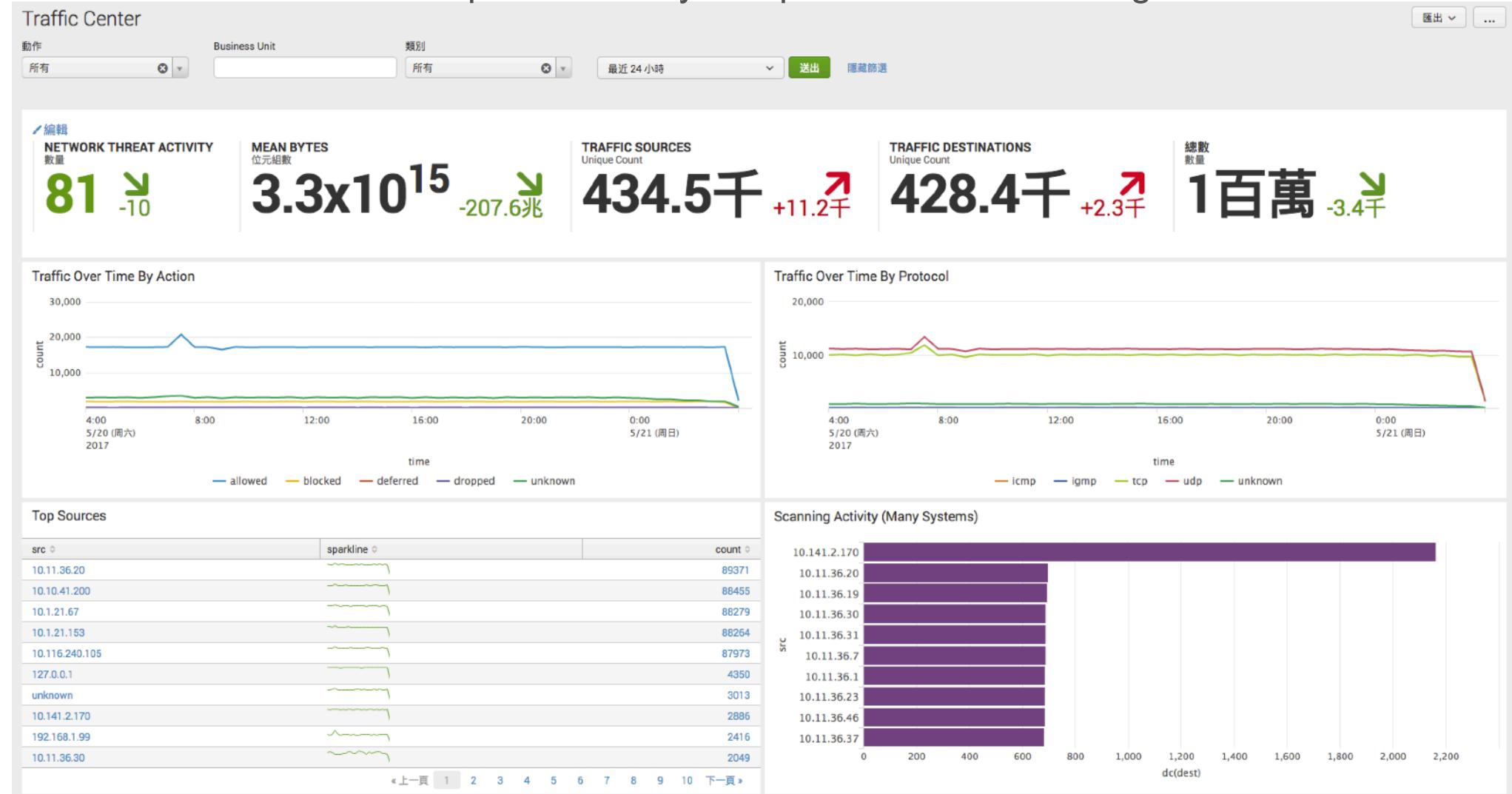
Last 60min

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

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

# Protocols, Connections Anomalies

Enterprise Security comprehensive monitoring



splunk > listen to your data®

# Protocols, Connections Anomalies

Enterprise Security comprehensive monitoring

**Port and Protocol Tracker**

Business Unit 輸入  
Destination Port  
tcp 80 送出 隱藏篩選

**Port/Protocol Profiler**

average / day  
tcp / 80 time  
Last 60 days Last 7 days Today

**New Port Activity - Last 7 Days**

firstTime	lastTime	transport	dest_port	app
05/02/2017 08:04:42	05/03/2017 08:26:58	tcp	135	epmap
05/02/2017 08:51:38	05/03/2017 07:52:37	tcp	139	netbios-ssn
05/02/2017 08:01:10	05/03/2017 08:29:49	tcp	6666	irc-serv
05/02/2017 08:00:10	05/03/2017 08:34:43	tcp	9080	unknown
05/02/2017 08:55:20	05/03/2017 07:55:01	tcp	9997	splunktcp
05/02/2017 08:00:46	05/03/2017 08:29:10	udp	10056	unknown
05/02/2017 08:04:10	05/03/2017 08:30:17	udp	12454	unknown
05/02/2017 08:00:16	05/03/2017 08:29:27	udp	13069	unknown
05/02/2017 08:48:39	05/03/2017 06:50:50	udp	13657	unknown
05/02/2017 08:58:03	05/03/2017 06:48:39	udp	16951	unknown

\* 上一頁 1 2 3 4 下一頁

**Prohibited Or Insecure Traffic Over Time - Last 24 Hours**

count  
time  
4:00 5/20 (周六) 2017 — tcp/22

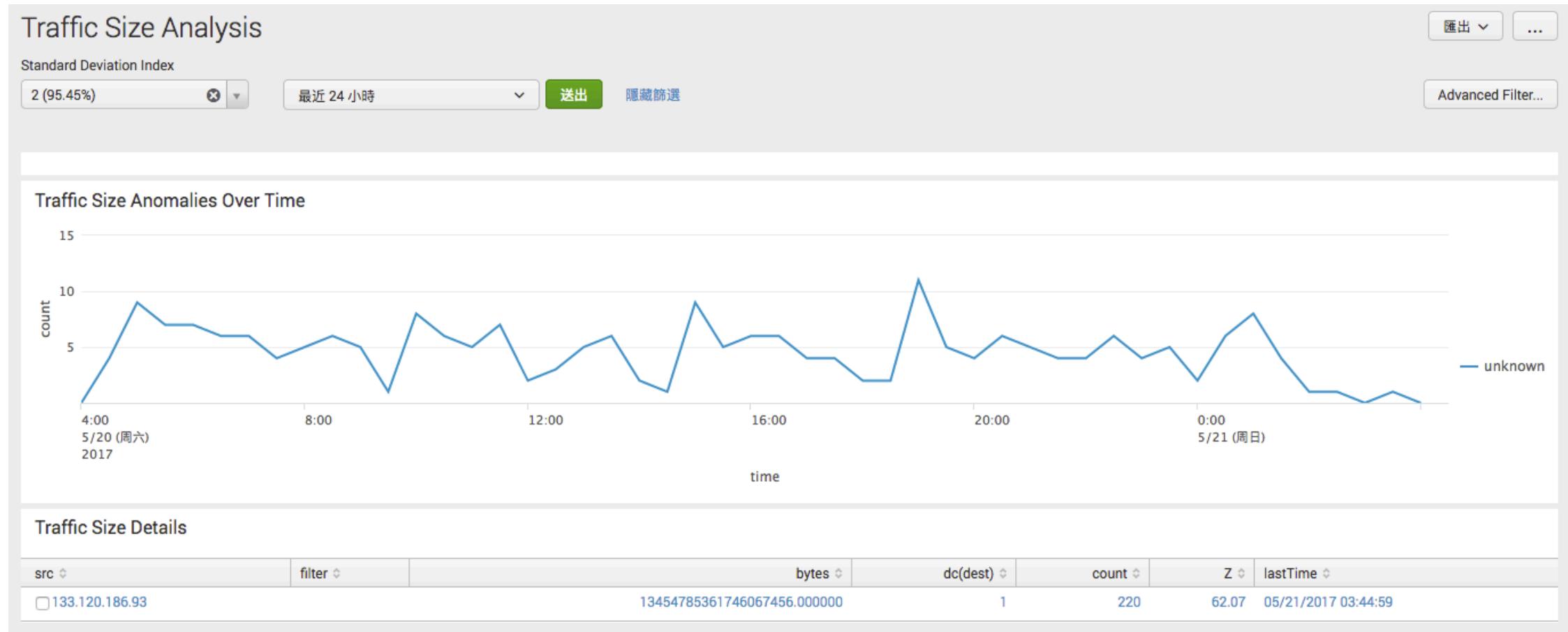
**Prohibited Traffic Details - Last 24 Hours**

_time	src	src_category	dest	dest_category	transport	dest_port	is_prohibited	is_secure
2017/05/21 03:54:31	1.2.3.4	5.6.7.8	herc sox		tcp	22	true	unknown

splunk > listen to your data®

# Protocols, Connections Anomalies

# Enterprise Security comprehensive monitoring



**splunk** > listen to your data®

# Protocols, Connections Anomalies

Enterprise Security comprehensive monitoring

DNS Activity

最近 24 小時 送出

隱藏篩選

Top Reply Codes By Unique Sources

reply_code	dc(src)
No error	~9,000
No such name	~100

Top DNS Query Sources

src	sparkline	count
1.2.3.4		283
0.104.115.103		1
0.112.126.121		1
0.117.133.156		1
0.118.99.17		1
0.119.99.57		1
0.121.15.129		1
0.121.181.226		1
0.125.38.97		1
0.129.70.239		1

Top DNS Queries

query	count
This.exfil.ru	717
vega.vulcan.com	717
www.ckdomains.com	717
www.google.co.uk	717
Confidential.exfil.ru	716
Doc.exfil.ru	716
Doc.exfil.ru	716
Is.exfil.ru	716
www.ieee.com	716
www.inframfs.com	716
www.seccompes.com	716

Queries Per Domain

domain	count	query_count	queries
exfil.ru	2865	4	Confidential.exfil.ru Doc.exfil.ru Is.exfil.ru This.exfil.ru
ckdomains.com	717	1	www.ckdomains.com
google.co.uk	717	1	www.google.co.uk
ieee.com	716	1	www.ieee.com
ietf.org	715	1	www.ietf.org
inframfs.com	716	1	www.inframfs.com
norealportal.co.in	715	1	www.norealportal.co.in
seccompes.com	716	1	www.seccompes.com
slashdot.org	715	1	www.slashdot.org
symanteconline.net	283	1	function.symanteconline.net

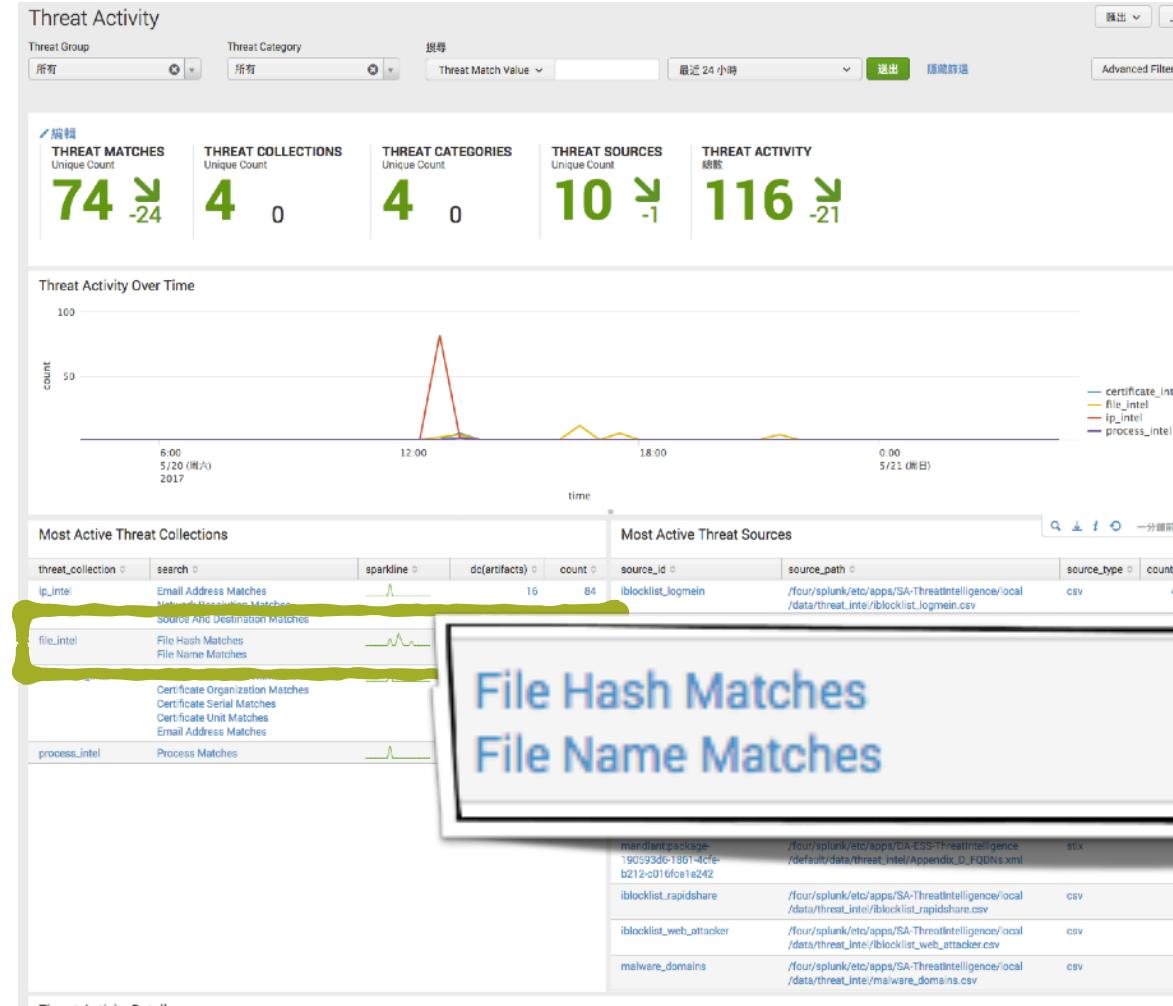
Recent DNS Queries

_time	name	record_type	query_type	query	answer	City	Country	Region
2017/05/21 04:07:29	x50.ru	Host address		x50.ru	97.44.5.1		United States	
2017/05/21 04:06:35	Doc.exfil.ru	Host address		Doc.exfil.ru	99.12.45.6		United States	
2017/05/21 04:05:54	www.ietf.org	Host address		www.ietf.org	104.20.1.85	San Francisco	United States	California
2017/05/21 04:05:45	www.inframfs.com	Host address		www.inframfs.com	172.83.95.22			
2017/05/21 04:05:22	www.google.co.uk	Host address		www.google.co.uk	74.125.131.94	Mountain View	United States	California
2017/05/21 04:05:12	www.slashdot.org	Host address		www.slashdot.org	216.34.181.48	Chesterfield	United States	Missouri
2017/06/21 04:06:11	www.ieee.com	Host address		www.ieee.com	140.98.193.152	Picotaway	United States	New Jersey

splunk > listen to your data®

# Protocols, Connections Anomalies

Enterprise Security comprehensive monitoring

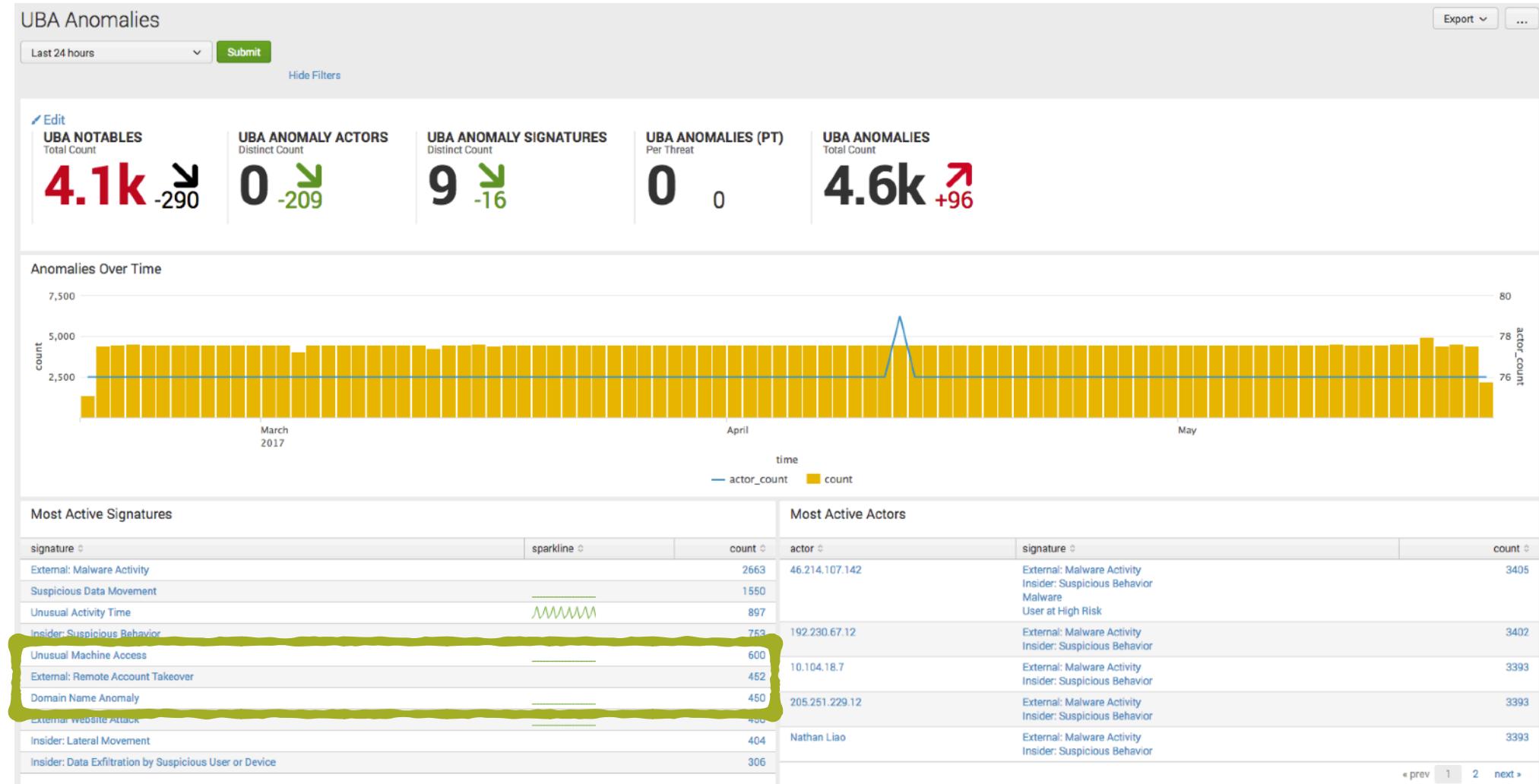


File Hash Matches  
File Name Matches

splunk > listen to your data\*

# Protocols, Connections Anomalies

# Enterprise Security comprehensive monitoring



Insider: Lateral Movement	404	Nathan Liao	External: Malware Activity
Insider: Data Exfiltration by Suspicious User or Device	306		Insider: Suspicious Behavior

**splunk** > listen to your data®

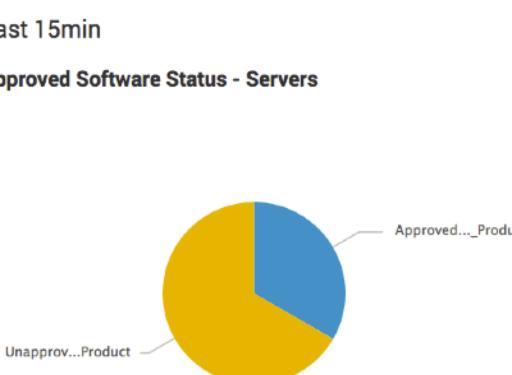
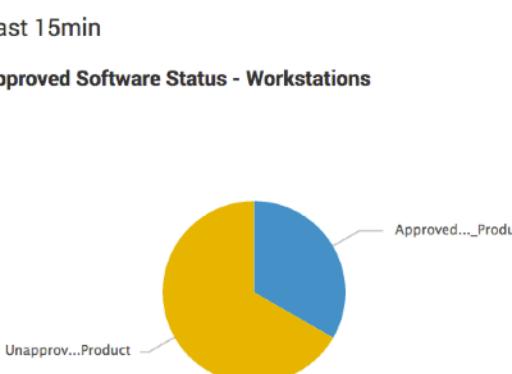
# Endpoint Anomalies Tracking

Free App: CIS Critical Security Controls

Critical Security Control #02 - Inventory of Authorized and Unauthorized Software

Inventory of Authorized and Unauthorized Software

編輯 決出 ...

Last 15min Control #2 - Approved Software Status - Servers - Count  <b>1</b> Approved Application(s)	Last 15min Approved Software Status - Servers  	Last 15min Control #2 - Unapproved Software Status - Servers - Count  <b>2</b> Unapproved Application(s)
Last 15min Control #2 - Approved Software Status - Workstations - Count  <b>1</b> Approved Application(s)	Last 15min Approved Software Status - Workstations  	Last 15min Control #2 - Unapproved Software Status - Workstations - Count  <b>2</b> Unapproved Application(s)

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 <

3

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》

# Endpoint Anomalies Tracking

Free App: CIS Critical Security Controls

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

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	
		dmsys	
		root	
		dmsys	
		root	
		dmsys	
		mercury	
		root	
		dmsys	
		root	
		dmsys	
		mercury	
		dmsys	
		root	
		dmsys	
		root	
		dmsys	
		root	

splunk > listen to your data®

# Endpoint Anomalies Tracking

# Free App: CIS Critical Security Controls

## Critical Security Control #13 - Data Protection

編輯

匯出 ✓

3

## Data Protection

Last 7 days

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

**Endpoint Changes**

Business Unit:  類別:  最近 24 小時:  送出 暫藏篩選

**Endpoint Changes By Action**

**Endpoint Changes By Type**

**Endpoint Changes By System**

dest	sparkline	object_category	count
127.0.0.1	██████████	file registry	72152
ch-od-10-es-prestage	~~~~~	directory file	1497
cps-sys-001		file host_info	7
206.169.145.239	~~~	host_info registry win_event_log	6
5.11.64.17	~~~~~	file host_info registry win_event_log	6
123.125.114.146		file host_info registry win_event_log	5
54.69.58.244	~~~	file registry	5
54.69.58.247	~~~	host_info registry	5
ACME-003		file host_info	5
COREDEV-004	~~~	audit file	5

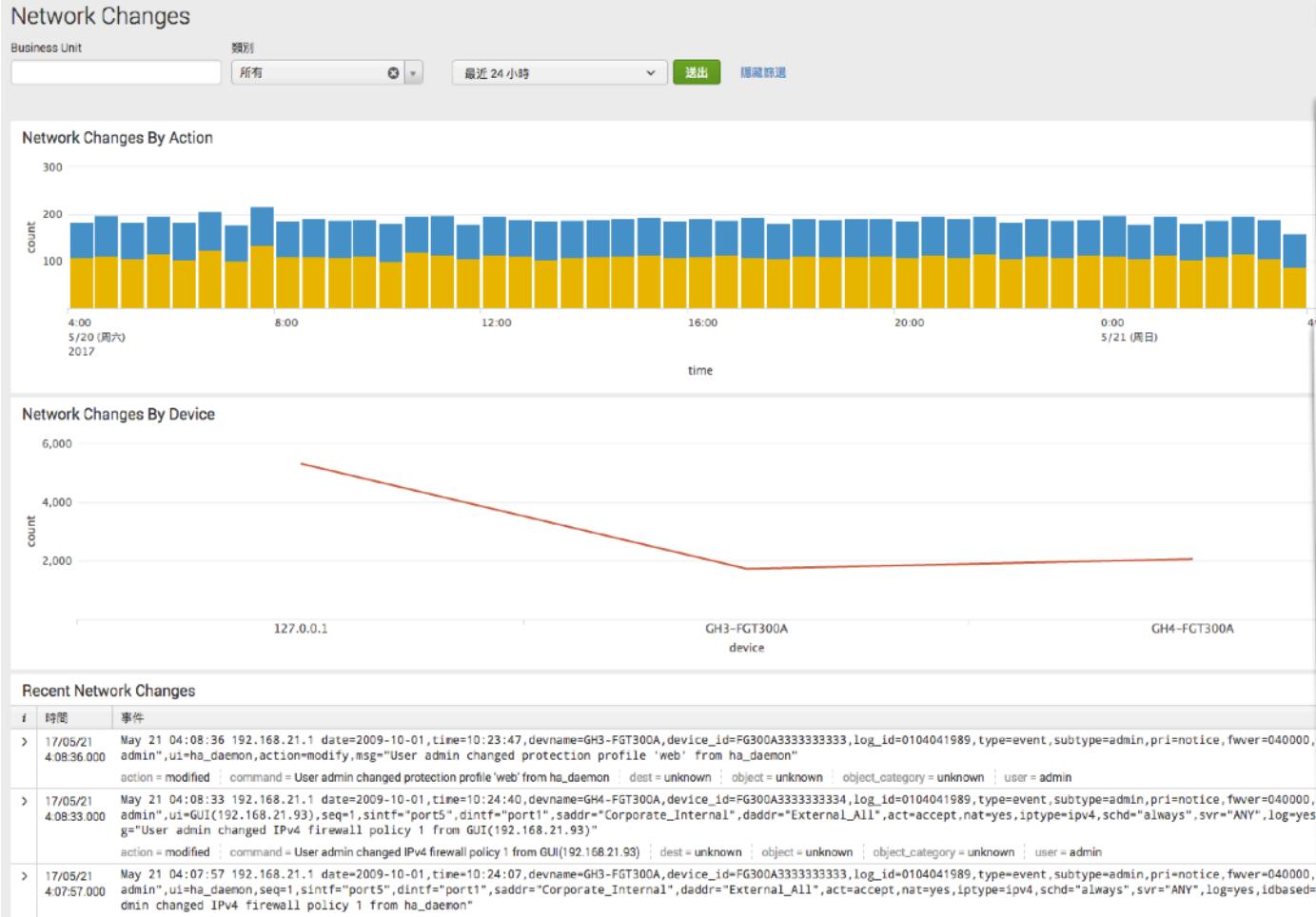
\* 上一頁 1 2 3 4 5 6 7 8 9 10 下一頁\*

**Recent Endpoint Changes**

#	時間	事件
> 1	17/05/21 04:08:59	InsertedAt="2017-05-21 04:08:59"; EventID="837063"; EventType="Tamper protection"; Action="Unknown action"; ComputerName="HOST-003"; ComputerDomain="PONDEROSA"; ComputerIPAddress="69.160.153.232"; EventTime="2017-05-21 04:08:59"; EventTypeID="8"; Name=""; EventName=""; UserName="PONDEROSA\asenjo"; ActionID="0"; SubTypeID="1"; SubType="Successful authentication"; TargetType="0"; TargetType="Unknown"; Target=""; GroupName="PONDEROSA\Computers"; action = modified : dest = 69.160.153.232 : object = Endpoint Protection : object_category = unknown : object_path = unknown : user = PONDEROSA\asenjo
> 2	17/05/21 04:08:59	InsertedAt="2017-05-21 04:08:59"; EventID="837045"; EventType="Tamper protection"; Action="Unknown action"; ComputerName="COREDEV-006"; ComputerDomain="PONDEROSA"; ComputerIPAddress="246.40.89.0"; EventTime="2017-05-21 04:08:59"; EventTypeID="8"; Name=""; EventName=""; UserName="PONDEROSA\fedorini"; ActionID="0"; SubTypeID="1"; SubType="Successful authentication"; TargetType="0"; TargetType="Unknown"; Target=""; GroupName="PONDEROSA\Computers"; action = modified : dest = 246.40.89.0 : object = Endpoint Protection : object_category = unknown : object_path = unknown : user = PONDEROSA\fedorini

# Endpoint Anomalies Tracking

Enterprise Security comprehensive monitoring



**Anomalous New Listening Port**

**Screenshot(s)**

**Correlation Search**

Search Name: Anomalous New Listening Port  
 Application Context: DA-ESS-EndpointProtection  
 Description: Alerts a series of hosts begin listening on a new port within 24 hours. This may be an indication that the devices have been compromised or have had new (and potentially vulnerable) software installed.  
 Search:  
`| inputlookup append=T listeningports_tracker | eval earliestQual=case(match("-24h@h", "id"), tostring("-24h@h"), match("-24h@h", "0|0|+2|0|")) relative_time(me0), true), time0| eval latestQual=case(match("0s", "id"), tostring("0s"), match("0s", "0|0|+0|0|"), relative_time(me0), "+0s"), true), time0| where (firstTime==earliestQual AND firstTime<latestQual) | fields -earliestQual, latestQual | stats count as "dest_count" by "transport", "dest_port" | where dest_count>10`

[Edit search in guided mode](#) [Edit search manually](#)

**Event Detail**

Time: 12/1/16 8:25:23 000 AM Endpoint: Anomalous New Listening Port (tcp/875) Risk: Low Status: New Owner: unassigned Business Unit: Actions

Description: 11 hosts were found to begin listening on port tcp/875 within the last 24 hours. This may indicate that software was recently installed on the hosts; this software may be associated with malware which oftentimes opens a backdoor using a network port.

Correlation Search: Endpoint - Anomalous New Listening Port - Rule

History: View all review activity for this Notable Event

Contributing Events: View systems listening on tcp/875

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2016-12-01T08:25:20-0600	admin	success
Risk Analysis	saved	2016-12-01T08:25:20-0600	admin	success

View Adaptive Response Invocations  
 Next Step: [No Next Steps defined.](#)

splunk > listen to your data®

# Endpoint Anomalies Tracking

Enterprise Security comprehensive monitoring

System Center

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

**Operating Systems**

Operating System	Count
Microsoft Windows 7	10
Microsoft Windows Vista	5
Microsoft Windows XP	5
Microsoft Windows 2008 R2	4
Microsoft Windows 2008	3
Microsoft Windows XP Professional SP3	3
Cisco Router	2
other (7)	7
unknown	1

**Top-Average CPU Load By System**

Time	127.0.0.1 (avg(% cpu))	Database Ratio (avg(% cpu))	Host Connection (%) (avg(% cpu))
4:00 5/20 (周六) 2017	85	45	25
8:00 5/20 (周六) 2017	75	45	25
12:00 5/20 (周六) 2017	90	45	25
16:00 5/20 (周六) 2017	80	45	25
20:00 5/20 (周六) 2017	95	45	25
0:00 5/21 (周日) 2017	85	45	25
4:00 5/21 (周日) 2017	90	45	25

**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

**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 下一頁 上一頁 1 2 3 4 5 6 7 8 9 10 下一頁

# Attack patterns forensic

## Enterprise Security/UBA comprehensive monitoring

New Search  Search

Save As  New Table  Close

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

Job      Smart Mode

Events  Patterns  Statistics (49,393)  Visualization

20 Per Page  Format  Preview   1 2 3 4 5 6 7 8 9 ... Next < Prev

query	ut_netloc	ut_bayesian	ut_shannon
\$1\$buwlmybu\$jsjuf6typlnqecuwlkiqu0	\$1\$buwlmybu\$jsjuf6typlnqecuwlkiqu0	0.9999994498379623	4.172185915404347
\$1\$buwlmybu\$jsjuf6typlnqecuwlkiqu0.defcon.org	\$1\$buwlmybu\$jsjuf6typlnqecuwlkiqu0.defcon.org	0.9999998789725344	4.533643863468259
\$1\$buwlmybu\$jsjuf6typlnqecuwlkiqu0.openwifi.defcon.org	\$1\$buwlmybu\$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		
+0aaaaaaaaabhhawd7jxw==.xklsI29das.mooo.com	+0aaaaaaaaabhhawd7jxw==.xklsI29das.mooo.com		
+0aaaaaaaaanduocqspvfa==.xklsI29das.mooo.com	+0aaaaaaaaanduocqspvfa==.xklsI29das.mooo.com		
+0iaaaaaaaaaabzuil7pzmkxa==.xklsI29das.mooo.com	+0iaaaaaaaaaabzuil7pzmkxa==.xklsI29das.mooo.com		
+0maaaaaaaaaabphjehptqkbg==.xklsI29das.mooo.com	+0maaaaaaaaaabphjehptqkbg==.xklsI29das.mooo.com		
+0qaaaaaaaaahruabi2fmcg==.xklsI29das.mooo.com	+0qaaaaaaaaahruabi2fmcg==.xklsI29das.mooo.com		
+0uaaaaaaaaad20fapu32nga==.xklsI29das.mooo.com	+0uaaaaaaaaad20fapu32nga==.xklsI29das.mooo.com		
+a0aaaaaaaaavh03vx78hq==.xklsI29das.mooo.com	+a0aaaaaaaaavh03vx78hq==.xklsI29das.mooo.com		
+a4aaaaaaaaabiugkmxrhuaw==.xklsI29das.mooo.com	+a4aaaaaaaaabiugkmxrhuaw==.xklsI29das.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>

# 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 ▾

6 Score

✓ 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_U...
Allowed	untrust	Algo...
Infection	untrust	Algo...
Outgoing	untrust	Algo...
SuspiciousPattern	untrust	Algo...
Allowed	untrust	Algo...
Infection	untrust	Algo...
Infection	untrust	Algo...

Domain Name Anomaly

Event Date: Jul 29, 2016 7:33 AM

Categories: Allowed Infection Outgoing Suspicious Pattern

Algorithmically generated domain name detected: www.22avmro21puism29czmsbyn30.ru

Watchlists

USERS (1)  
Pablo Ramirez

DEVICES (2)  
Internal  
10.229.243.213  
External  
69.174.68.124

DOMAINS (1)  
www.22avmro21puism29czmsbyn30.ru

Anomaly Relations

Pablo Ramirez → 69.174.68.124 → www.22avmro21puism29czm...

Critical Major Minor

Triggering Event

[29/Jul/2016:00:33:44 -0700] "admin4\_sys" 10.229.243.213 69.174.68.124 9080 200 TCP\_HIT "GET http://www.22avmro21puism29czmsbyn30.ru/ HTTP/1.0" "unknown" "low risk" "--" 0 0 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:29.0) Gecko/20100101 Firefox/29.0" "--" "--" "0" "" "--"

Device Locations (2)

Map Satellite

United States

splunk > listen to your data®

# Attack patterns forensic

## Enterprise Security/UBA comprehensive monitoring

Source IPs Communicating with Far More Hosts Than Normal (Assistant: Detect Spikes)

Description:  
This will typically detect scanning activity, along with lateral movement activity.  
Alert Volume: Low (?

Security Impact:  
The first phase of the Lockheed Martin Kill Chain is reconnaissance, which can include initial scanning of a target network to map out assets, as well as vulnerabilities for potential entry points using known exploits. It is important to note that this type of activity can happen both on the perimeter as well as inside of a network once an initial foothold has been made. Monitoring for this type of activity can help identify precursors to an attack as well as be an indicator that assets within an organization, or credentials have been compromised.

Examples:  

- Demo Data (You are here)
- Live Data
- Accelerated Data

Data Check	Status	Open in Search	Resolution (if needed)
Must have Demo Lookup	<span style="color: green;">✓</span>	<a href="#">Open in Search</a>	Verify that lookups installed with Splunk Security Essentials is present

**Detect Spikes**

Enter a search

```
| inputlookup od_splunklive_fw_data.csv | convert mktimedate(_time) timeformat="%Y-%m-%d %H:%M:%S.%3Q%z" | bucket _time span=1d | stats dc(dest_ip) as count by src_ip, _time
```

585 個結果 (69/12/31 18:00:00.000 至 17/05/21 5:21:41.000)

Field with data points (?) Field for our subject (?) Threshold method (?) Threshold multiplier (?) Calculate last day of data? (?)  
数量 src\_ip 標準差 2 (required for demo dataset)

[Detected Spikes](#) [Open in Search](#) [Show SPL](#) [Check Cardinality](#) [What is Cardinality?](#) [Create High Cardinality / High Scale Alert](#)

離群檢測

Toggle Help

**Outlier(s) (3)**

**Total Result(s) (57)**

**Raw Event(s) (150,000)**

**Outliers Only**

src_ip	num_data_samples	count	avg	lowerBound	upperBound	isOutlier
10.174.30.134	11	3	1.000000	1.000000	1.000000	1
10.174.30.148	11	227	23.000000	4.66970	41.33030	1
10.174.30.188	8	4	2.166667	0.66112	3.67221	1

[Open in Search](#) [Show SPL](#) [Schedule Alert](#) [Schedule High Cardinality Alert](#)

**All Data**

src_ip	num_data_samples	count	avg	lowerBound	upperBound
10.174.30.134	11	3	1.000000	1.000000	1.000000
10.174.30.148	11	227	23.000000	4.66970	41.33030

[Open in Search](#) [Show SPL](#) [Schedule Alert](#) [Schedule High Cardinality Alert](#)

splunk > listen to your data®

# Attack patterns forensic

## Enterprise Security/UBA comprehensive monitoring

**splunk> App: Enterprise Security**

Angelo Brancato ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Security Posture Incident Review My Investigations Glass Tables Security Intelligence ▾ Security Domains ▾ Audit ▾ Search ▾ Configure ▾ Enterprise Security

Edit Export ...

WannaCry Ransomware Clone

Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers either through Remote Desktop Protocol (RDP) compromise or through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010 (link is external) vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003 (<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>) operating systems on May 13, 2017. According to open sources, one possible infection vector is via phishing emails.

Infected Systems	Vulnerable Systems	Quarantined Systems
2	30	32

Vulnerable Systems (MS17-010)

src	cve	pluginName	first_found	last_found	last_fixed
192.168.103.108	CVE-2017-0148 CVE-2017-0147 CVE-2017-0146 CVE-2017-0145 CVE-2017-0144 CVE-2017-0143	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (unprivileged check)	2017-04-16T06:06:25Z	2017-05-14T06:06:20Z	NOT_FIXED
192.168.68.89	CVE-2017-0148 CVE-2017-0147 CVE-2017-0146 CVE-2017-0145 CVE-2017-0144	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (unprivileged check)	2017-04-17T08:09:04Z	2017-05-14T08:09:30Z	NOT_FIXED

# Attack patterns forensic

Enterprise Security/UBA comprehensive monitoring

<pre>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</pre>	<a href="#">All time</a>									
<span style="color: green;">✓</span> 22 events (before 5/21/17 5:28:07.000 AM) <a href="#">No Event Sampling</a>										
<a href="#">Events (22)</a>	<a href="#">Patterns</a>									
<a href="#">Statistics (22)</a>	<a href="#">Visualization</a>									
<a href="#">20 Per Page</a>	<a href="#">&lt; Prev</a> <a href="#">1</a> <a href="#">2</a> <a href="#">Next &gt;</a>									
_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

# Automatic “Respond” on findings

**splunk >**  
Security Solution  
on everything

**Incident Review**

Urgency	件数
CRITICAL	11
HIGH	960
MEDIUM	4394
LOW	3948
資訊	0

状態:  時間:  持有者:  検索:  Security Domain:  時間:

✓ 9,313 個事件 (17/05/20 5:00:00:000 至 17/05/21 5:36:25:000)  
格式化時間 v - 隱藏 + 延長至選取範圍

編輯已選取 | Edit All 9313 Matching Events | Add Selected to Investigation

i	時間	Security Domain
>	17/05/21 2:45:33.000	Endpoint
<	17/05/21 1:01:06.000	Access

Description:  
The system 10.11.36.20 has failed authentication 73512 times and successfully authen

Additional Fields

Value
login sshd wind
10.11.36.20
americas
pci
splunk
Pleasanton
USA
10.11.36.20
true
37.694452
-121.894461
Bill_Williams
trust
false
true
true

Event Details:

event_id	event_hash	eventtype
5C286601-E91B-4D9C-ABBC-CF3A5AA35979@notable@5d125d8ee61d37f0aa439d9f7f328450	5d125d8ee61d37f0aa439d9f7f328450	modnotable_results
nix-all-logs		
notable		

17/05/20 17:04:42.000 Network Vulnerability Scanner Detected (10.11.36.20) Critical New unassigned

**Adaptive Response Actions**

Select actions to run.  
+ Add New Response Action

Category: All v search

Show only recommended actions

**AWS : Start Instance**  
Category: Permissions Control | Task: allow | Subject: endpoint.server | Vendor: AWS

**Verify latest patch status**  
Verify latest patch status  
Category: Information Gathering | Task: update | Subject: endpoint.workstation | Vendor: TAN

**Dominoes : Order Pizza**  
Category: Device Control | Task: create | Subject: splunk.event | Vendor: Dominoes

**Endpoint : Check for new Hash**  
Endpoint : Check for new Hash  
Category: Device Control | Task: create | Subject: endpoint | Vendor: Generic

**Endpoint : Logout User**  
Category: Device Control | Task: allow | Subject: endpoint | Vendor: Generic

**Stream Capture**

# Automatic - Adaptive Response

Enterprise Security comprehensive monitoring

The screenshot shows the Splunk interface with the following details:

- Events (4)**: The main tab selected.
- Format Timeline**: A dropdown menu with options like "Zoom Out", "Zoom to Selection", and "Deselect".
- 1 minute per column**: A tooltip indicating the timeline scale.
- List**, **Format**, **20 Per Page**: View options at the top of the event list.
- Event Details**:
  - Date: 10/30/14
  - Time: 01:50:43
  - Host: 10.11.36.20
  - Source: vf.travel
  - Type: TCP\_NC\_MISS
  - Port: 225
  - HTTP Method: HTTP/1.0
  - URL: http://208.49.52.149/idle/mkwmYD8QmB8+WhnR/1340
  - Flash: -
- Event Actions** button: Shows dropdown settings for host, source, sourcetype, src, and action.
- Selected Fields** sidebar:
  - host
  - source
  - sourcetype
  - src
- Interesting Fields** sidebar:
  - action
  - app\_version
  - bytes\_in
  - bytes\_out
- Malware Search** context menu (highlighted):
  - Nbtstat 10.11.36.20
  - Nslookup 10.11.36.20
  - Ping 10.11.36.20
  - Stream Capture** (selected)
  - Traffic Search (as destination)
  - Traffic Search (as source)
  - Update Search
  - Vulnerability Search
  - Web Search (as destination)

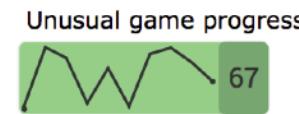
Quarantine infected systems, Shutdown endpoints, Virus scanning, Stream capture , Threat Intelligence update

splunk > listen to your data®

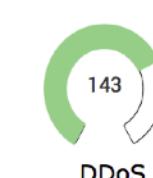
# Security control center - Glasstable

## Buttercup Games Security Overview

### PLAYER / GAMES USERS



### APPLICATIONS & SERVICES



13

Active Investigations

173

Critical Alerts

Resolved Incidents

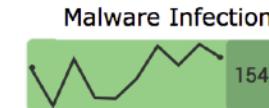
147

Total High Risk User Eve...

12

Default Accounts

### INTERNAL INFRASTRUCTURE

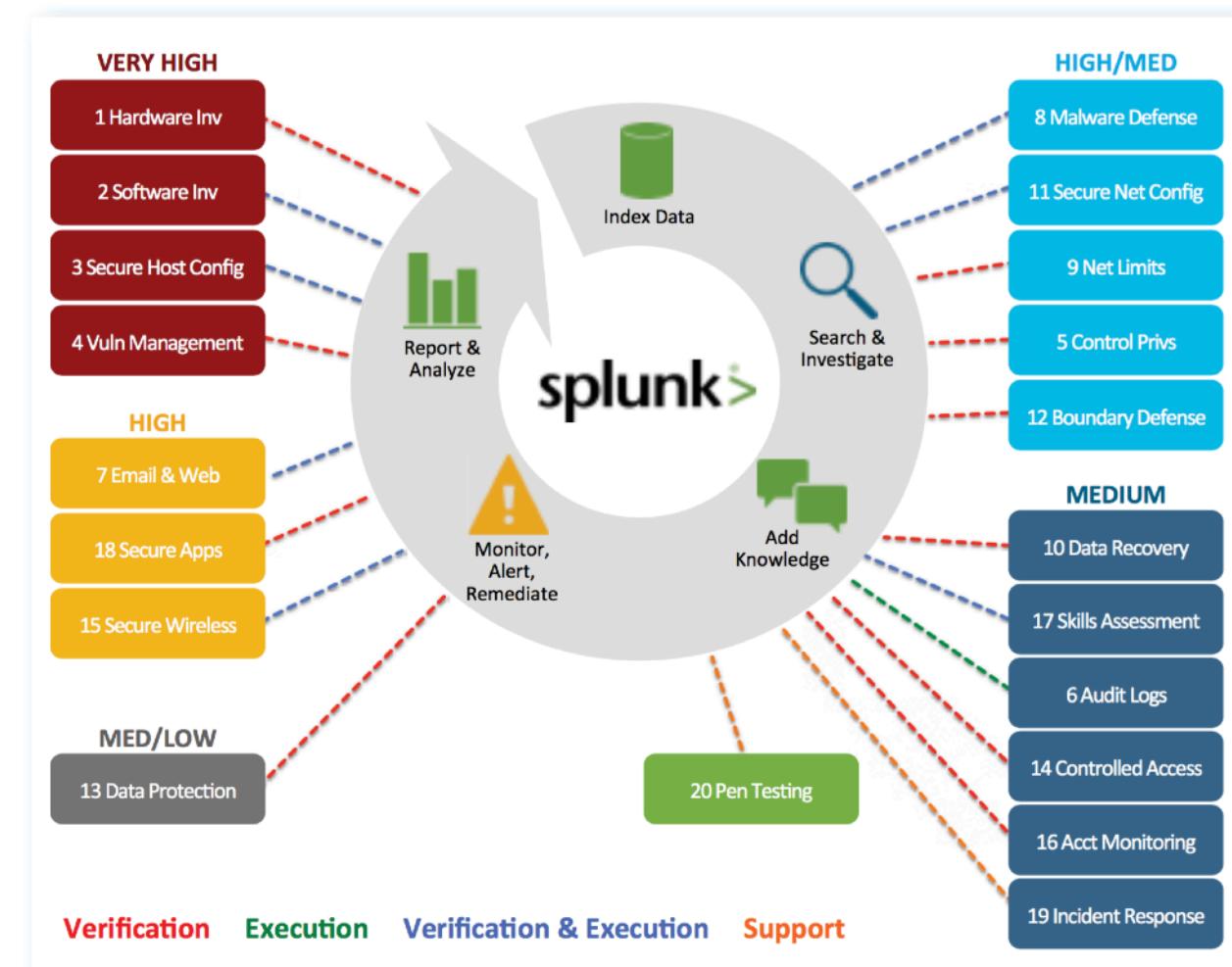


# Defense against the attack chain

ADVERSARY ACTIONS TO ATTACK YOUR ORGANIZATION

Reconnaissance	Get In	Stay In	Exploit
1 Hardware Inv	3 Secure Host Config	5 Control Prvs	10 Data Recovery
2 Software Inv	10 Secure Net Config	12 Boundary Defense	17 Skills Assessment
4 Vuln Management	6 Secure Apps	6 Audit Logs	13 Data Protection
20 Pen Testing	8 Malware Defense	14 Controlled Access	16 Acct Monitoring
	9 Net Limits	16 Acct Monitoring	19 Incident Response
	7 Email & Web		

VERY HIGH    HIGH    HIGH/MED    MEDIUM    MED/LOW    LOW



splunk> listen to your data®

## Free Security Apps or Splunk Enterprise Security

splunk > listen to your data

# Thousands of Global Security Customers



Colorado School of  
**PUBLIC HEALTH**



The  
of University  
Akron

**Deloitte.**



**SAFEWAY**



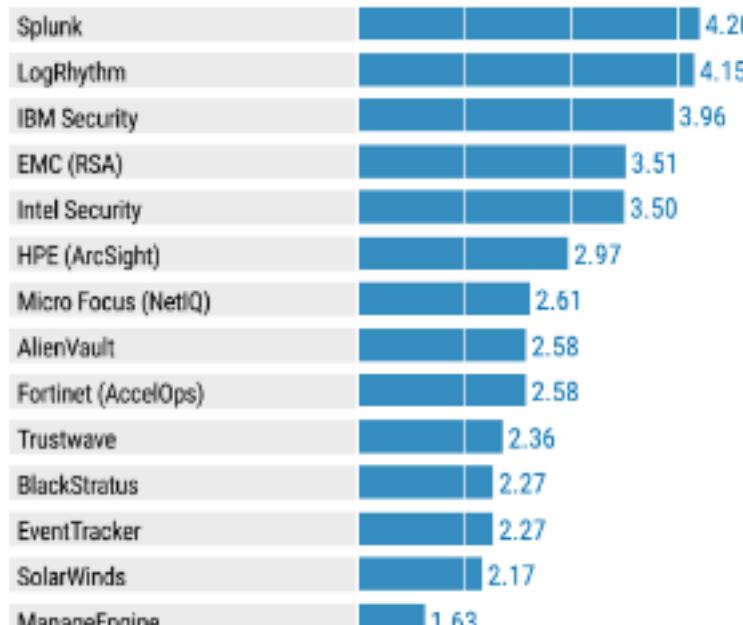
**comcast**

**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

Product or Service Scores for Basic Security Monitoring

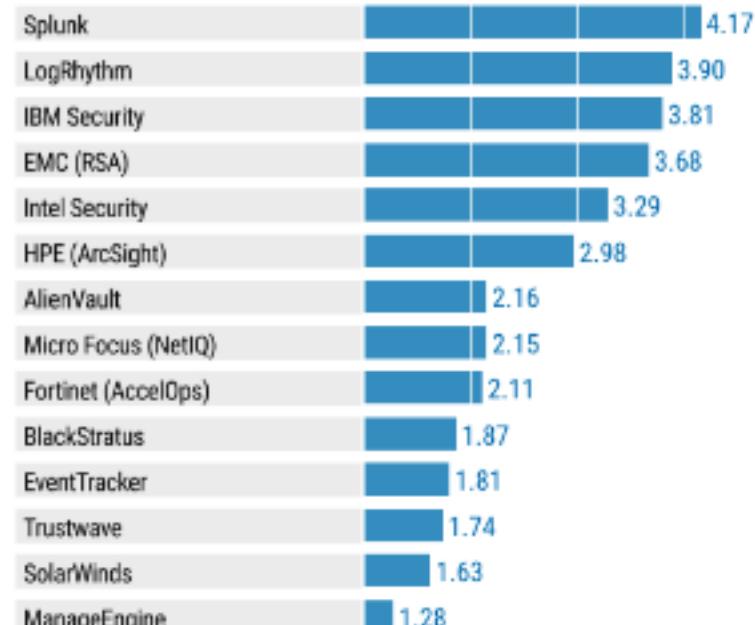


1    2    3    4    5  
As of August 2016

Source: Gartner (August 2016)

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

Product or Service Scores for Advanced Threat Detection

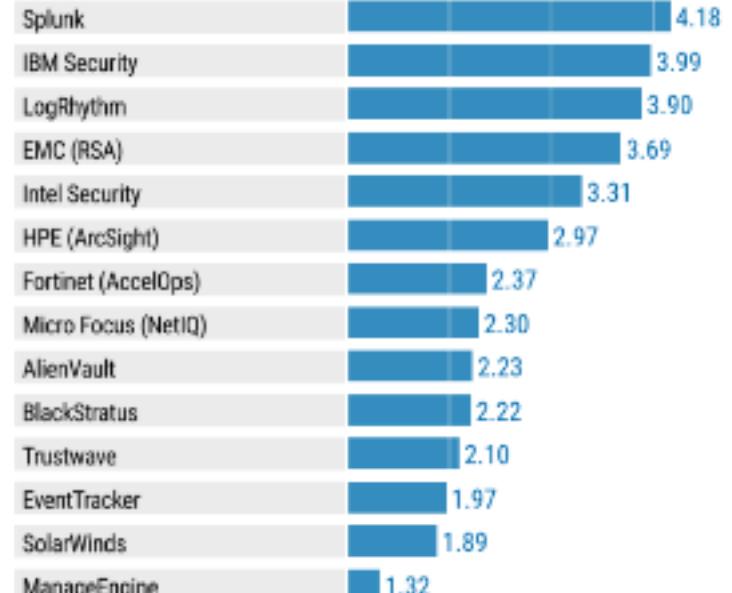


1    2    3    4    5  
As of August 2016

Source: Gartner (August 2016)

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

Product or Service Scores for Forensics and Incident Response



1    2    3    4    5  
As of August 2016

Source: Gartner (August 2016)

\*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.

