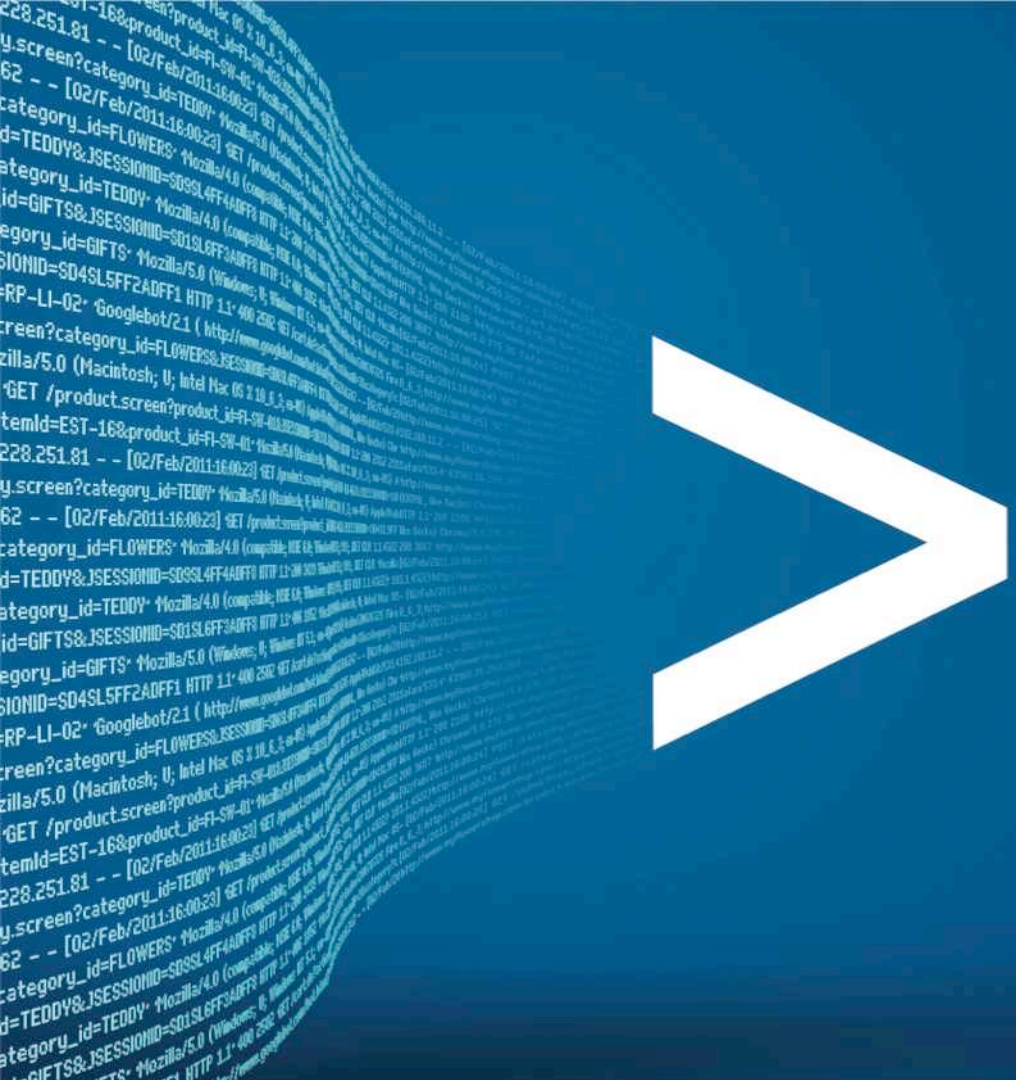


Using Analytics-Driven Security Platform to Find Advanced Attacks and Malware

Cui Yue ｜崔玥
Senior Security Specialist
North Asia Region

splunk>

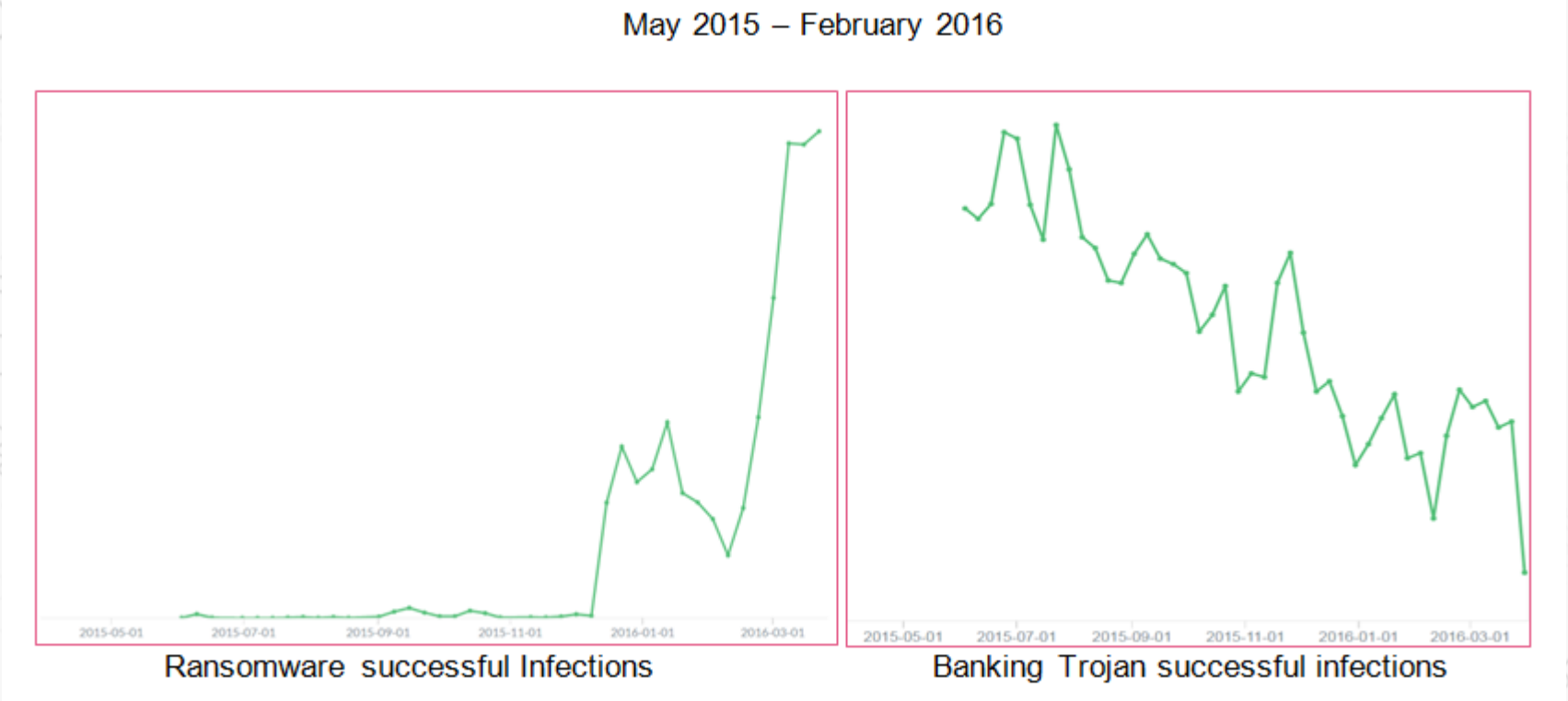
Top Security Concerns from CISO

Advanced Cyber-Attacks

Malicious Insider Threats

Online Account Take over

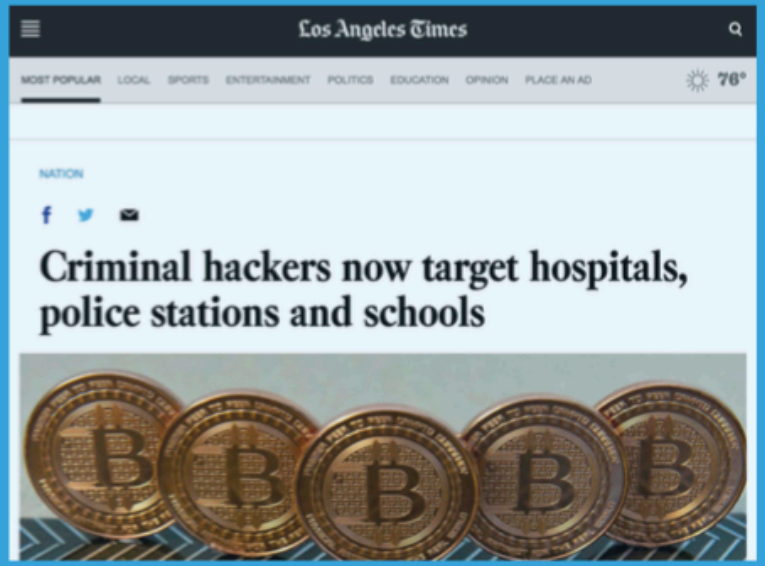
Ransomware : Cybercriminals new attack of choice



http://blog.checkpoint.com/2016/04/06/ransomware-cybercriminals-new-attack-of-choice/

Ransomware : and it's a "good" business

"THE FBI RECENTLY PUBLISHED THAT RANSOMWARE VICTIMS PAID OUT $209 MILLION IN Q1 2016 COMPARED TO $24 MILLION FOR ALL OF 2015."



LA Times

Compliance & Regulations

Reg	Type	Applicability	Protects	How	Penalties
HKMA	Industry, Hong Kong	All Authorized Institutions (AI) doing business in Hong Kong	apply to all IT systems used by financial institutions;	• Provide Guidelines and Circulars and required the AI to impose security controls and measures to address the followings : - • Internet Banking security • Anti-Money Laundering and Counter-Terrorist Financing • And more …	The Hong Kong Monetary Authority (HKMA) has fined the local branch of State Bank of India (SBI) for contravening specified provisions in its Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance. A penalty of HK$ 7.5 million ($970,000) has been imposed. (http://www.hkma.gov.hk/eng/key-information/press-releases/2015/20150731-5.shtml)

HKMA Guidelines

- 2015 Sept : Cyber Security Risk Management
  - Authorized access control, secure configuration, vulnerability management, privileged account control, sensitive data protection, Resilience, Security Education
  - Defense against malware and APT
  - Unusual activities detection
  - Incident Responses (IR), Digital forensic
- 2016 May : Cyber Security Fortification Initiative
  - 1. Structured Assessment Framework (Analysis Threat Intelligence)
  - 2. Focused training for cyber security professionals
  - 3. Simulation Testing

SFC Guidelines

- 2016 Mar: Suggested Cyber Security Control

1) Establish a strong governance framework to supervise cybersecurity management;
2) Implement a formalized cybersecurity management process for service providers;
3) Enhance security architecture to guard against advanced cyber-attacks;
4) Formulate information protection programs to ensure sensitive information flow is protected;
5) Strengthen threat, intelligence and vulnerability management to pro-actively identify and remediate cybersecurity vulnerabilities;
6) Enhance incident and crisis management procedures with more details of latest cyber-attack scenarios;
7) Establish adequate backup arrangements and a written contingency plan with the incorporation of the latest cybersecurity landscape; and
8) Reinforce user access controls to ensure access to information is only granted to users on a need-to-know basis.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

> SC US
SC UK

UN report says encryption protects people's liberties and expression

Repor
zero-d
part o
to anc
uptick

NEWS | PRODUCTS | BLOGS | RESOURCES | VIDEOS

SC Magazine > News > Japan's national pension fund breach affects 1.25M

Robert Abel, Content Coordinator

June 01, 2015

Japan's national pension fund breach affects 1.25M

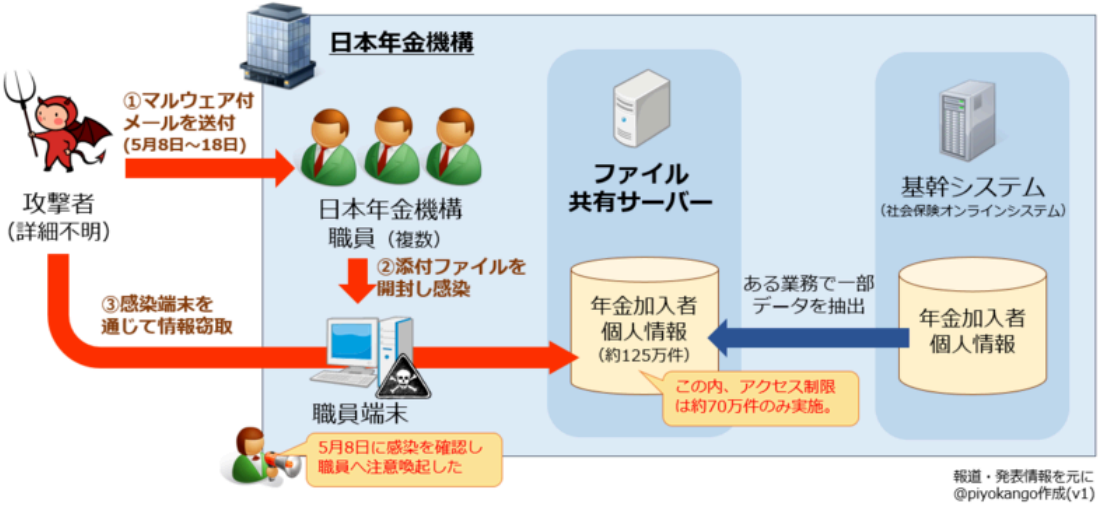
Share this article:

A recent attack on Japan's national pension system compromised the information - including names, pension identification numbers, addresses and birth dates - of more than 1.25 million people, according to a report in the *Wall Street Journal*.

The breach, discovered on May 28, was the result of pension employees opening a malicious email attachment.

Authorities said the pension fund's core system, which houses the most sensitive data including payment and benefit information, wasn't affected. Pension system President Toichiro Mizushima promised new pension identification numbers to those affected, the *Journal* said.

日本年金機構 情報漏えいの概要イメージ



APT malware is hard to prevent

- signature update is always not fast enough
- On target (phishing email)
- Cannot be found in Security Logs

MISSION CRITICAL

Cyber Security Analytic Team

Small Team

Global Security Operations Center

Security Analytics Needs >

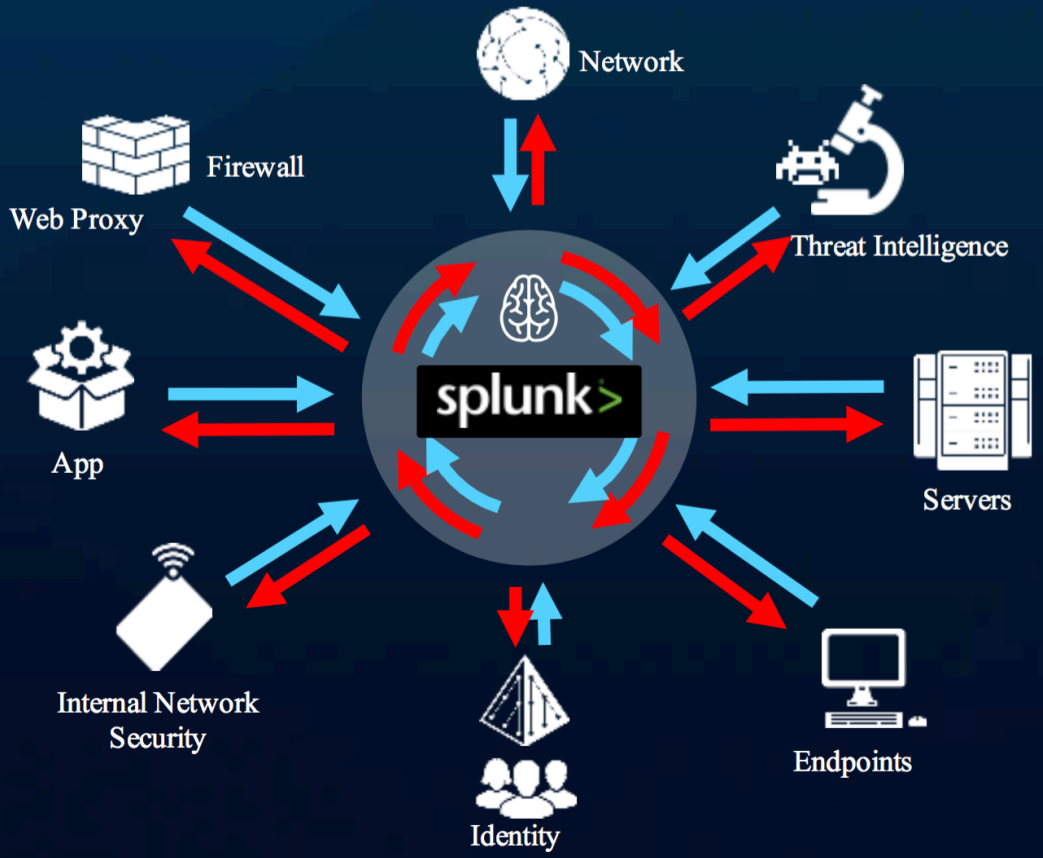
What are some of the technical challenges in managing data?

Ability to process large volumes of transactional data for long period of time.

Ability to process transactions in real-time for detection of fraud

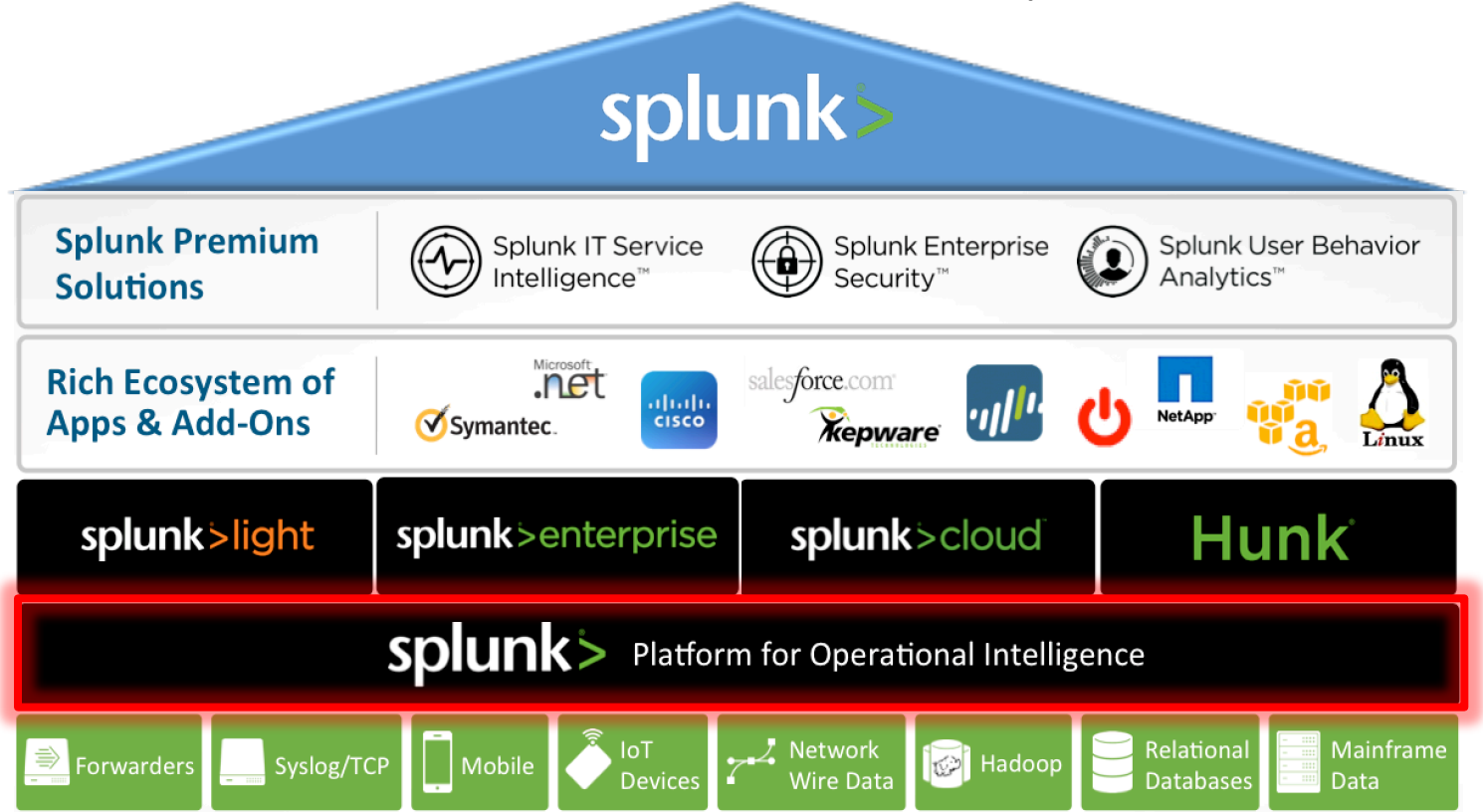
Ability to analyze complex patterns of transactions and be able to profile user objects

Splunk is the Security Nerve Center



Splunk Portfolio

Across Data Sources, Use Cases & Consumption Models



ADVANCED
SECURITY ANALYTICS

splunk>enterprise

Security Analytics &
Event Repository

splunk> UBA

Data Science &
Decision Engine

splunk> ES

Key Security Indicators &
Risk Scoring

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

fifth consecutive year !!

ADVANCED SECURITY ANALYTICS

splunk>enterprise

Best Fraud Prevention Solution

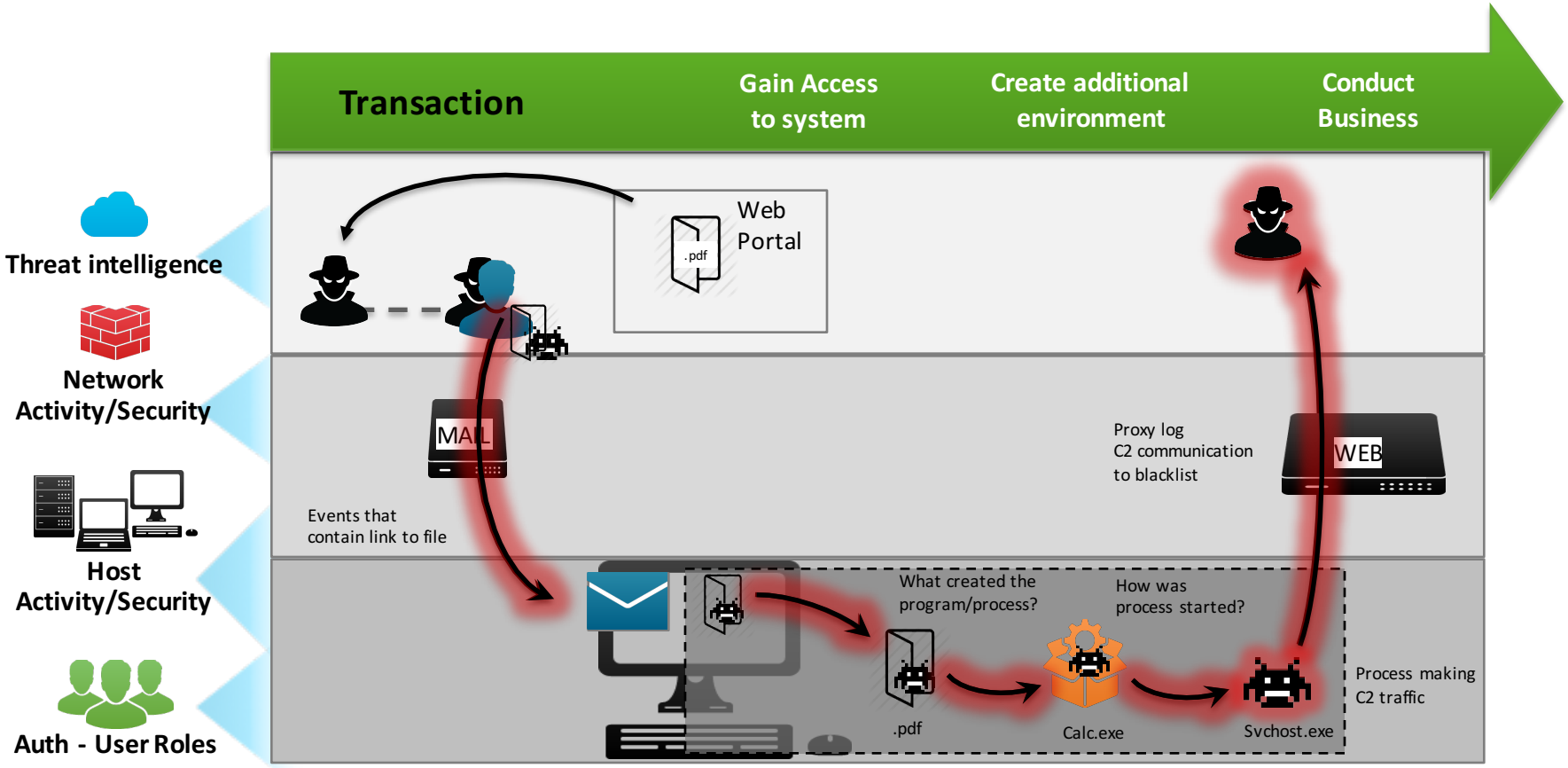
splunk> UBA

Data Science & Decision Engine

splunk> ES

Best SIEM Solution

Cyber Kill Chain : APT Detection and Response



All Machine Data is important for hunting

Threat intelligence & Analytics

Network Activity/Security

Host Activity/Security

Auth - User Roles

Context

Are you currently collecting ALL IT Data (Authentication, DNS/DHCP, Proxy and Firewall events) for security analytics ?

Do you have a list of Assets and Identities by priority?

How about your "CLOUD data "??

DATA SOURCES for your Security Analytic Team

Identity/Auth

- Active Directory/ Domain Controller
- Single Sign-on
- HRMS
- VPN
- DNS, DHCP

Activity (N-S, E-W)

- Email Gateway
- Web Gateway
- Firewall
- Netflow, PCAP
- DLP, File Server/Host Logs

Security Products

- Malware
- End-point
- IDS, IPS, AV

Traditional

SaaS/Mobile

- AWS CloudTrail
- Box, SF.com, Dropbox, other SaaS apps
- Mobile Devices

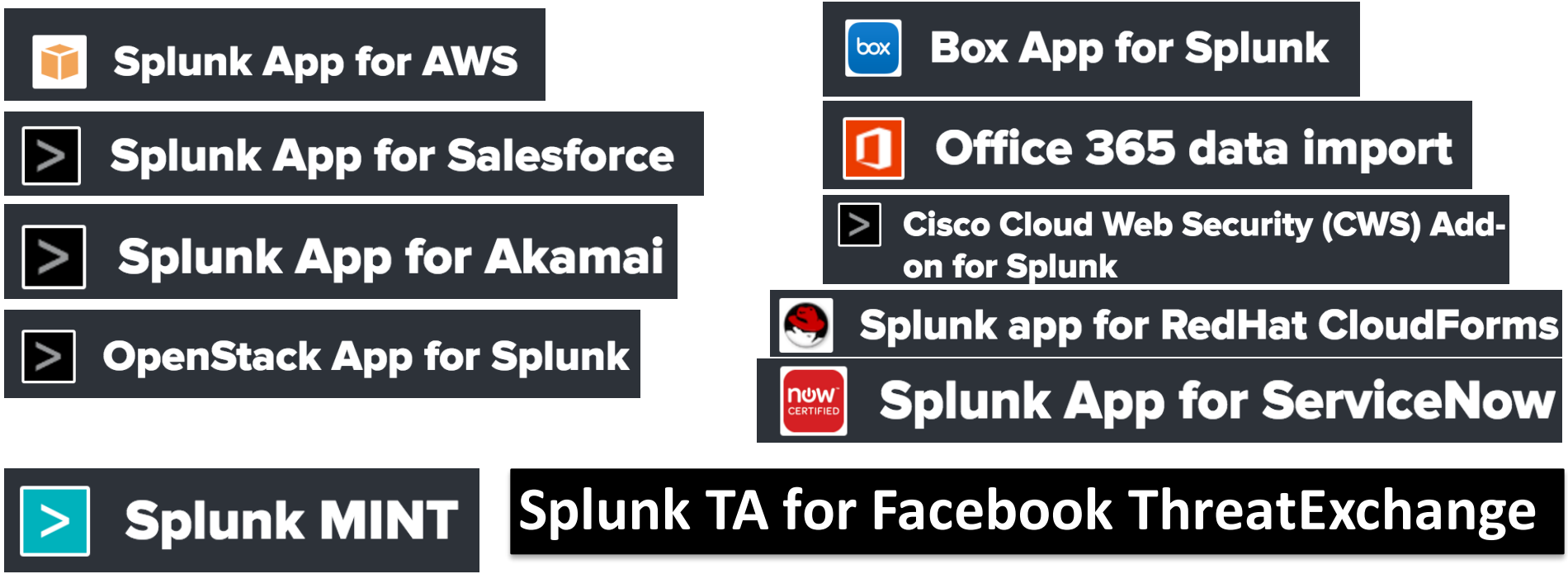
External Threat Feeds

- Cisco Threat Intelligence, Norse, Threat Stream, FS-ISAC, STIX/TAXII, Facebook ThreatExchange or other blacklists for IPs/domains, username, MD5 hash

New Challenge

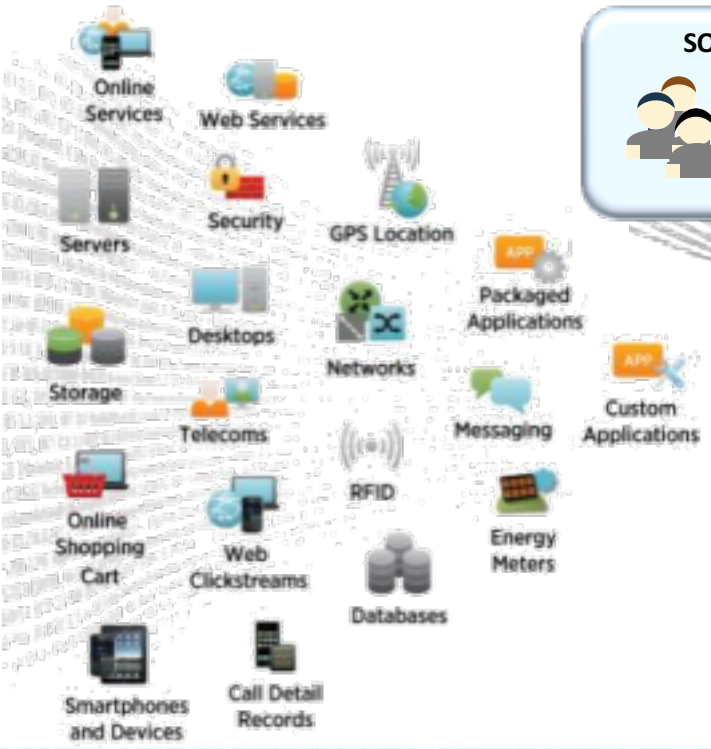
Great apps for Cloud and mobile data source

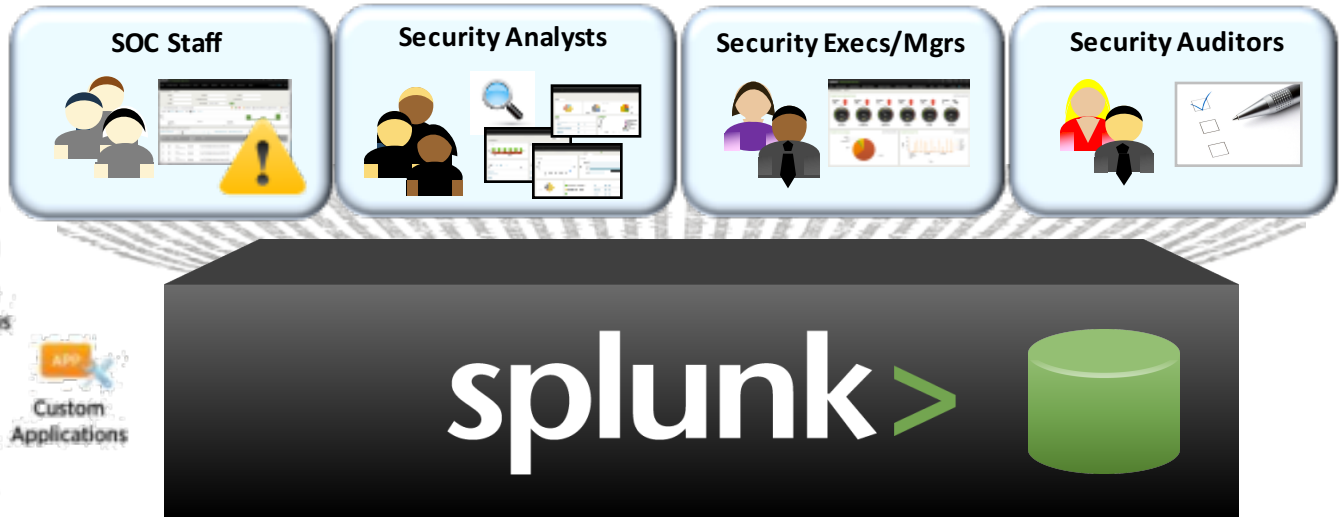
- https://splunkbase.splunk.com



Splunk App for Enterprise Security

First solution with out-of-the-box content to manage known and unknown threats.

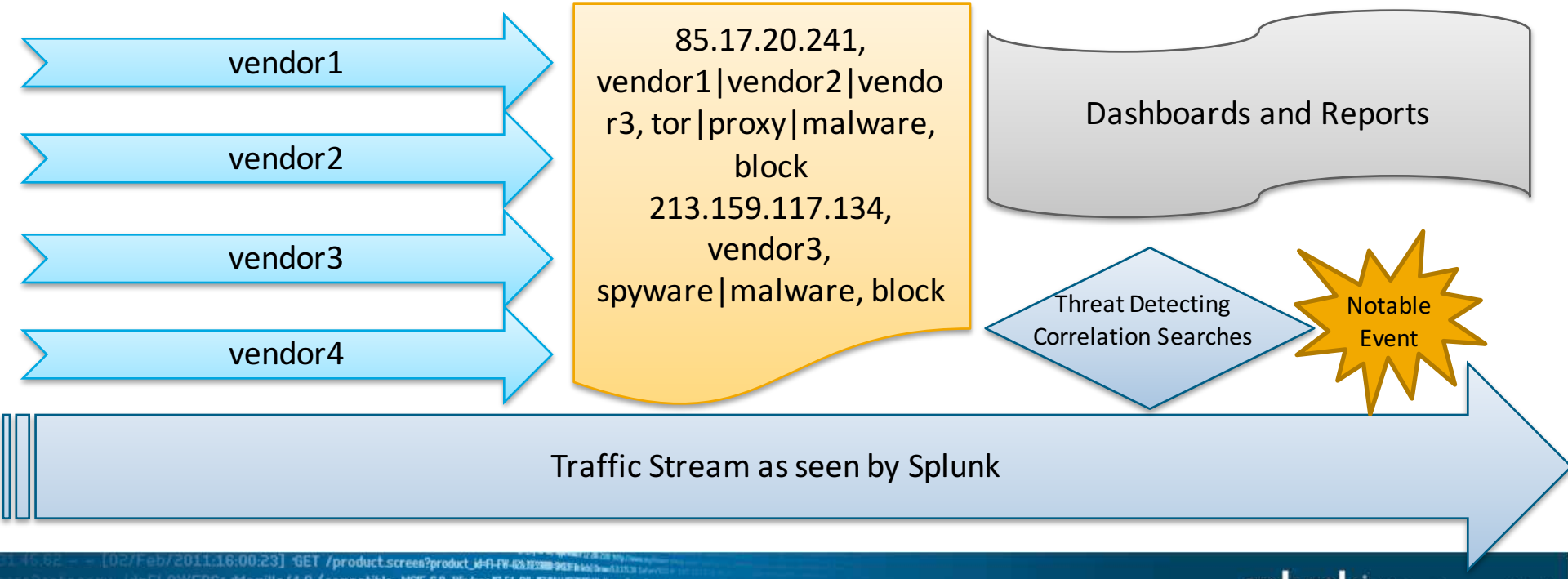




- Scalability to manage multi-terabytes of real-time and historical data
- Pre-built security correlation rules, reports, and dashboards
- Statistical analysis for defining 'normal'
- Incident investigation and management framework

Using Threat Data to enrich context in REAL-TIME

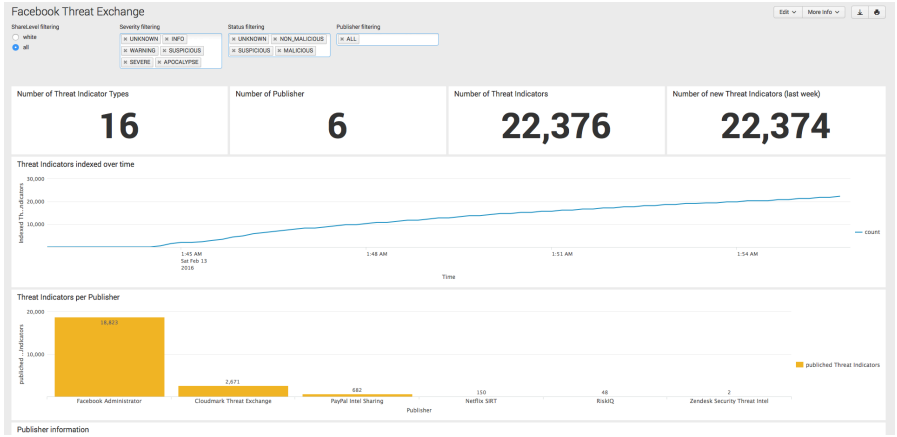
- Make it easier to ingest and de-duplicate threat intelligence
- Workflow actions and dashboards to view threat data in context



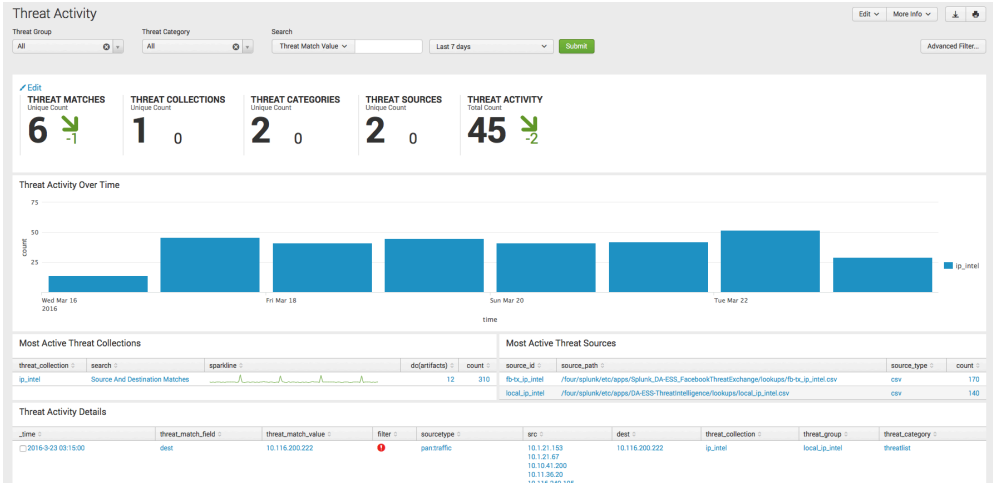
Threat Data from Mandiant APT1

```
MANDIANT-APT1-DOMAIN,MANDIANT-APT1-MD5SUM,MANDIANT-APT1-FILENAME,MANDIANT-APT1-FILESIZE,MANDIANT-APT1-STRINGLIST
*advanbusiness.com*,*001dd76872d80801692ff942308c64e6*,*121.exe*,*10233*,*!@#%$^#@!*
*aoldaily.com*,*002325a0a67fded0381b5648d7fe9b8e*,*162.exe*,*10240*,*@***@*@@@
```

Facebook ThreatExchange

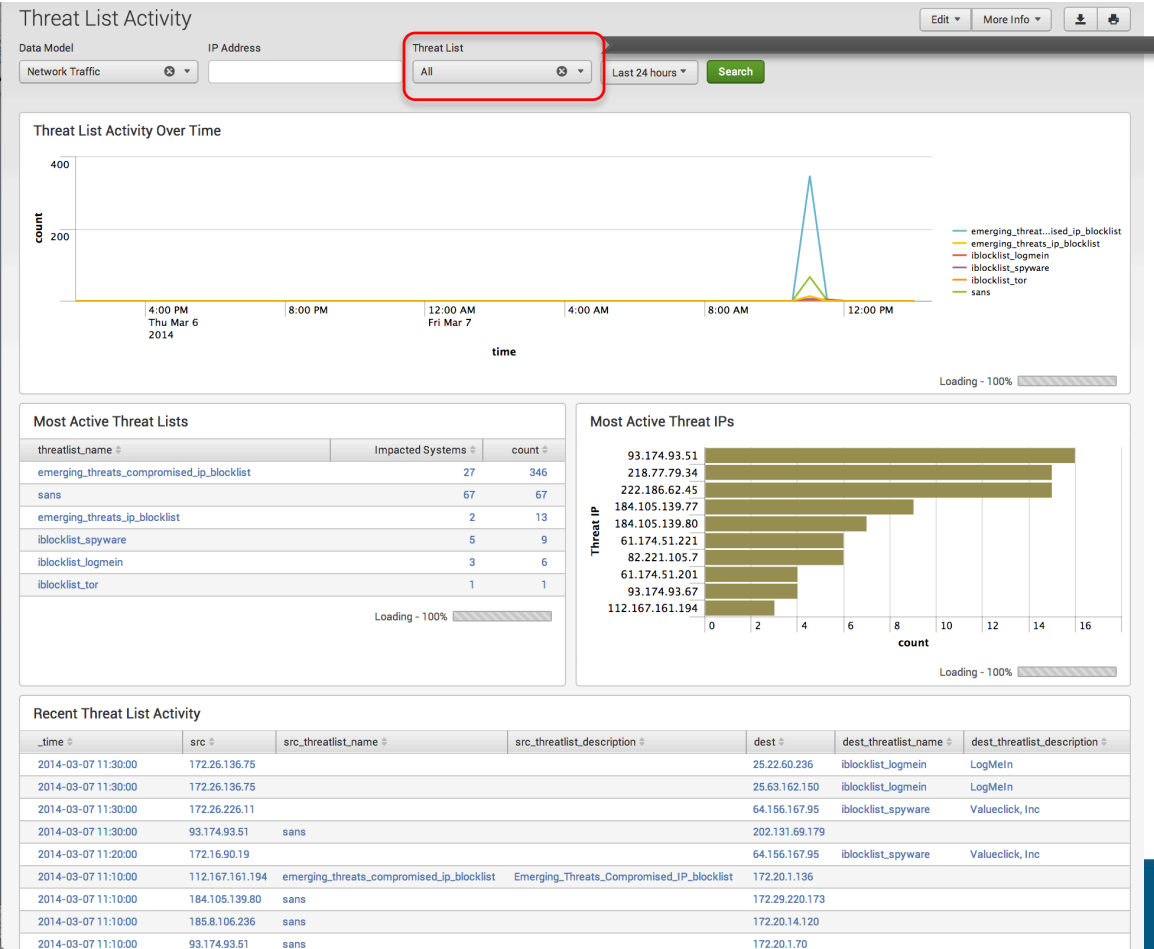


- Provides domain names, IPs, hash threat indicators
- Use with ad hoc searches and investigations



- Need an app ID and secret from Facebook
- Config Splunk add-on for FB ThreatExchange
- Customers already use !

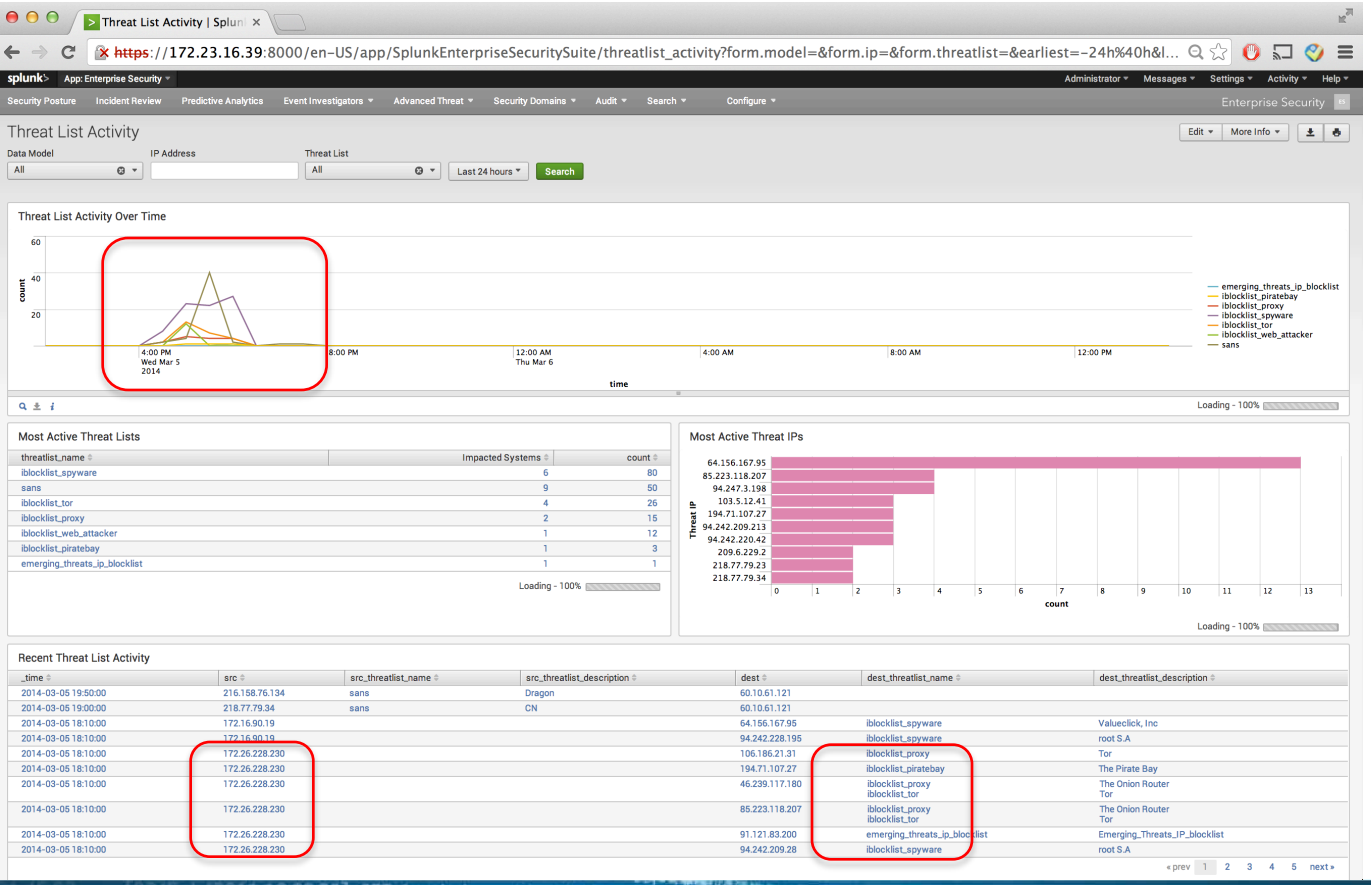
Threat Intelligence – Pre-config Threat Lists



Description

- Emerging Threats compromised IPs blocklist
- Emerging Threats fwip rules
- Emerging Threats Malvertisers blocklist
- Addresses that are used by the LogMeIn product to enable unauthorized remote access
- Addresses that are commonly associated with known PirateBay sites
- Addresses that are commonly associated with known traffic-proxy sites
- Addresses that are commonly associated with known RapidShare sites
- Addresses that are commonly associated with known spyware sites
- Addresses that are commonly associated with known Tor sites
- Addresses that are commonly associated with known malicious attacker sites
- Custom list of threat IP addresses
- Norse Darklist
- abuse.ch Palevo C&C IP Blocklist
- SANS blocklist
- abuse.ch SpyEye IP blocklist
- abuse.ch ZeuS blocklist (bad IPs only)
- abuse.ch ZeuS blocklist (standard)

Customer Case: Client running P2P (BT bit torrent)



Client IP : 172.26.228.230
Time : 18:10 5/3/14

Threats :
Accessing following Bad IP

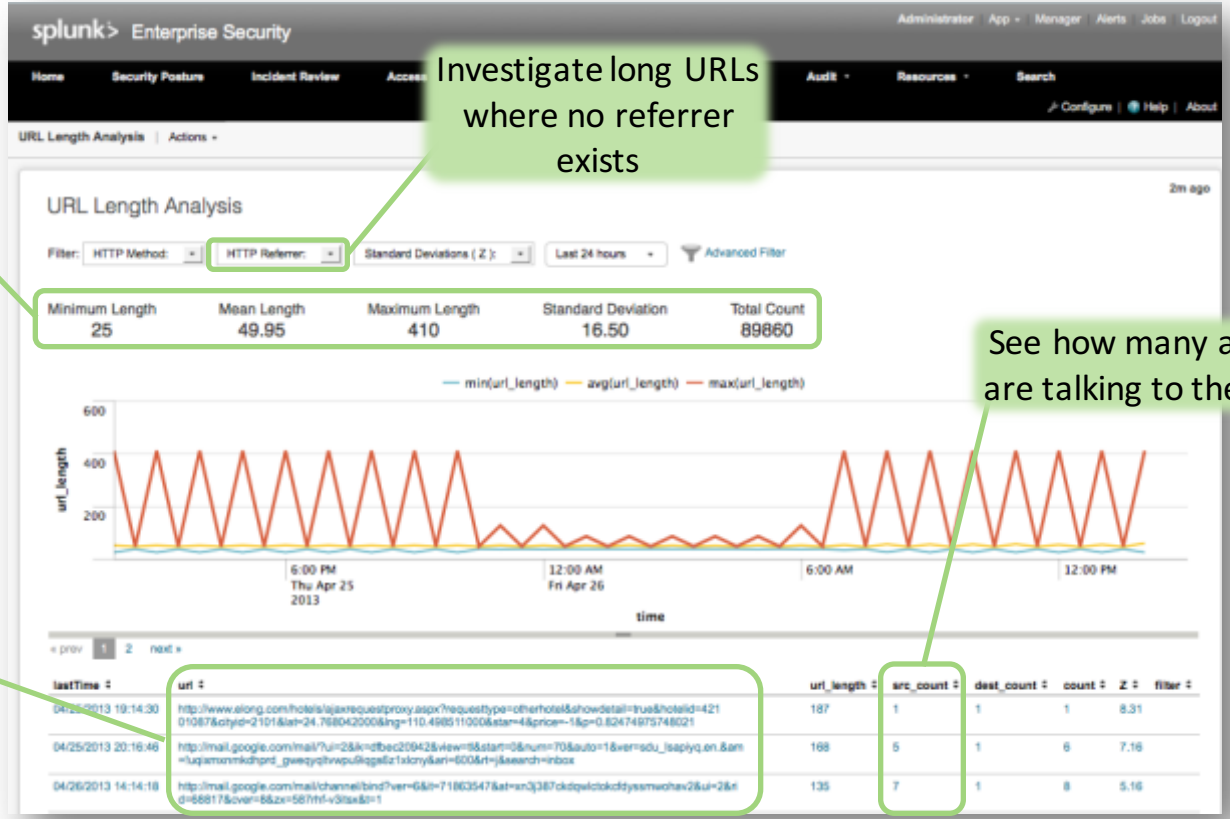
- Tor (anonymous proxy)
- Piratebay (BT host)
- Blocked IP site
- Known spyware site

Verified with PC configuration and this PC has installed the BT client software.

Advance Threat Detection example : URL Length Analysis

Compare each URL statistically to identify outliers

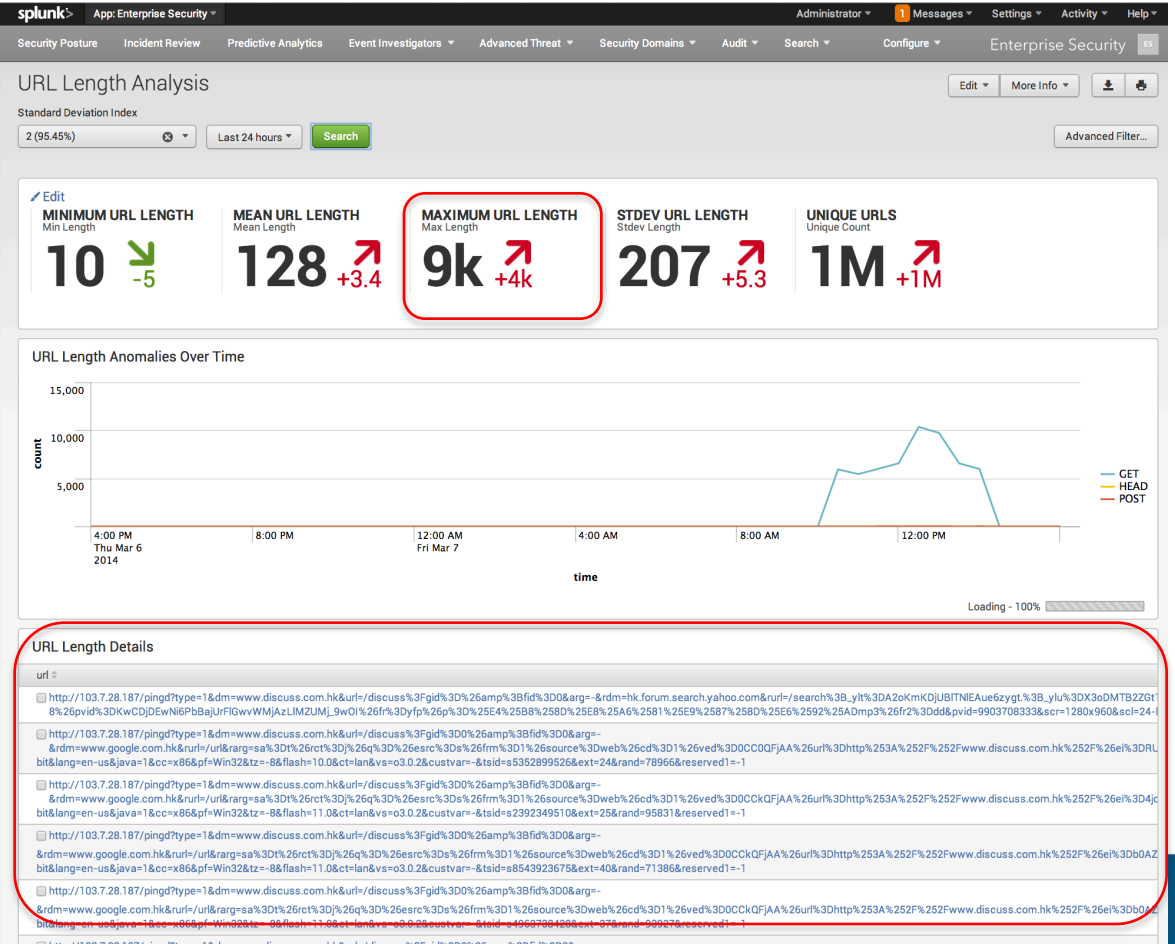
Investigate long URLs where no referrer exists



See how many assets are talking to the URL

Look for long URLs that may include embedded C&C instructions

A lot of web-based attack are using VERY long URL

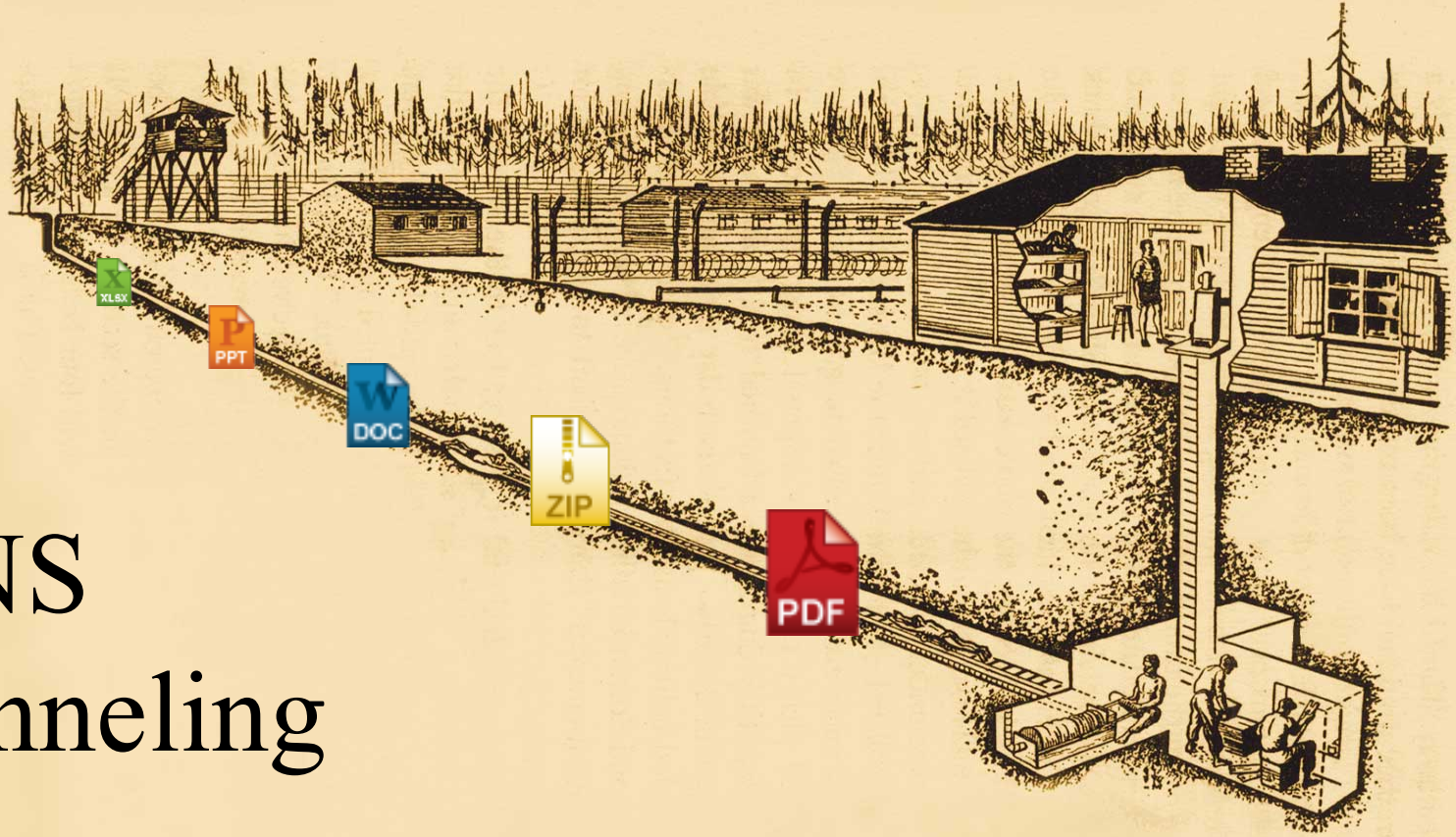


Mean URL length for 128 Byte looks Normal

But for Max URL length for 9KB size, it looks suspicious.

We found a lot of LONG URLs which is trying to access the external site : "http://103.7.28.187/pingd?type-1&dm=www.discouss.com.hk ... "

After verified with http://urlquery.net/report.php?id=2182484, they are Tencent QQ/wechat Message. The long http packages are encrypted SMS.



DNS Tunneling

Finding Clients with extremely Looooooooooooong queries

- DNS Tunneling

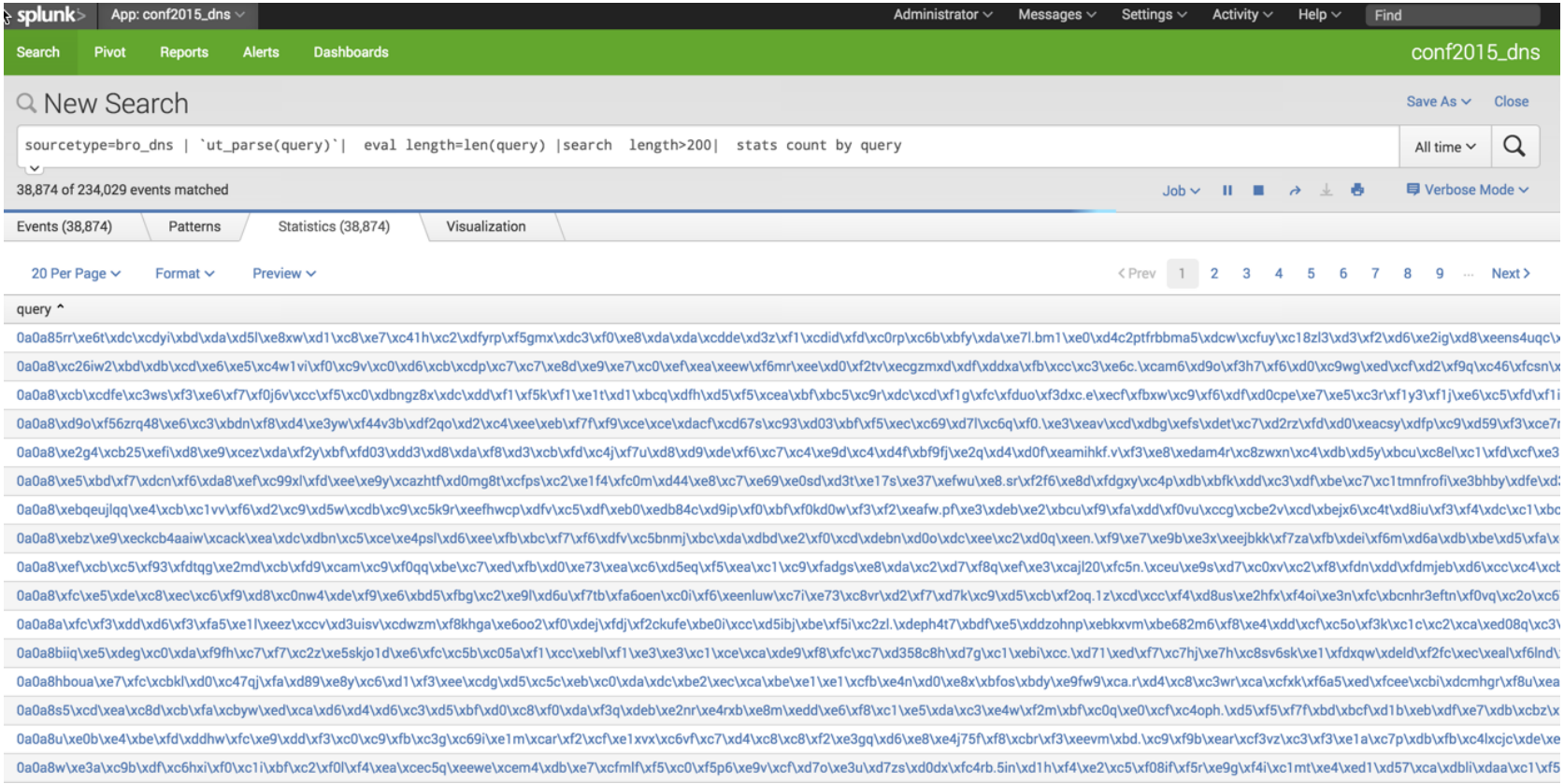
Find anything that is 2 standard deviations

```
sourcetype=bro_dns  |eval len=len(query) | eventstats stdev(len) AS stdev avg(len) AS avg p50(len) AS p50 | eval length=len(query) | where length>(stdev*2)  | stats count by length stdev avg p50 qtype_name query | sort -length
```

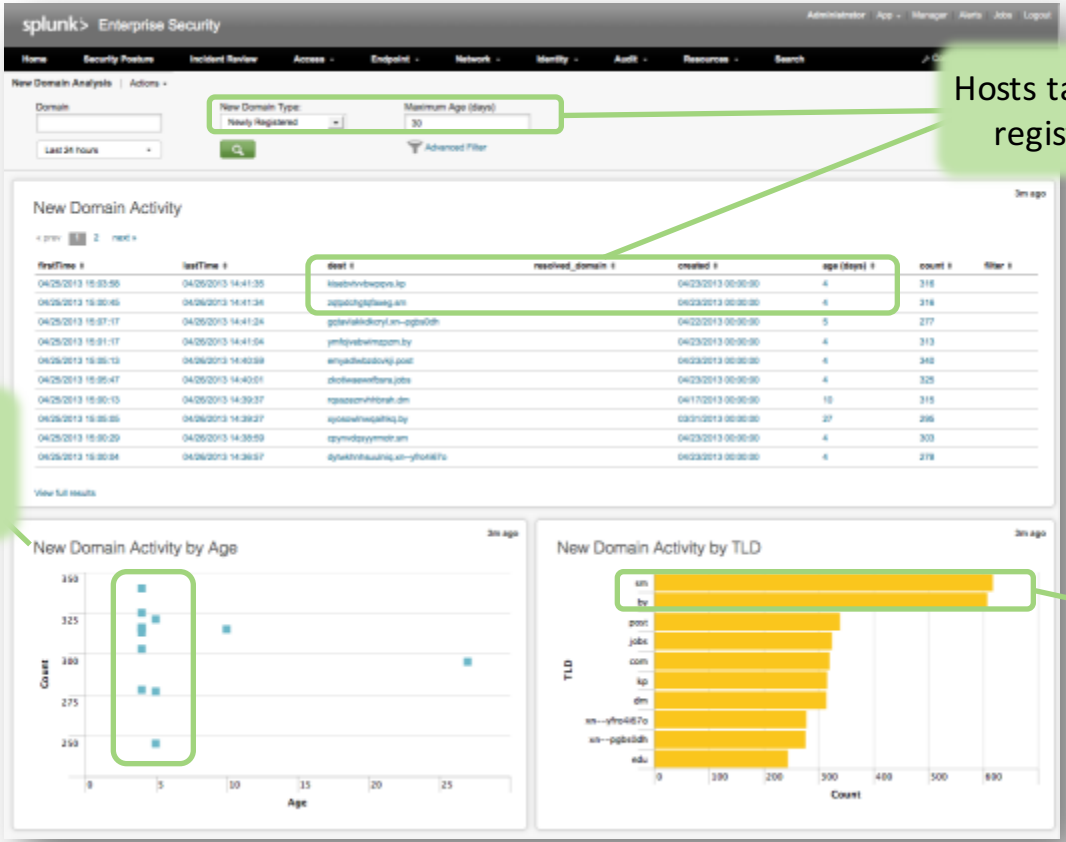
Finding queries over 200 characters long

```
sourcetype=bro_dns  | `ut_parse(query)`|  eval length=len(query) |search  length>200|  stats count by query
```

Finding Queries Over 200 characters



Advance Threat Detection example : New Domain Analysis



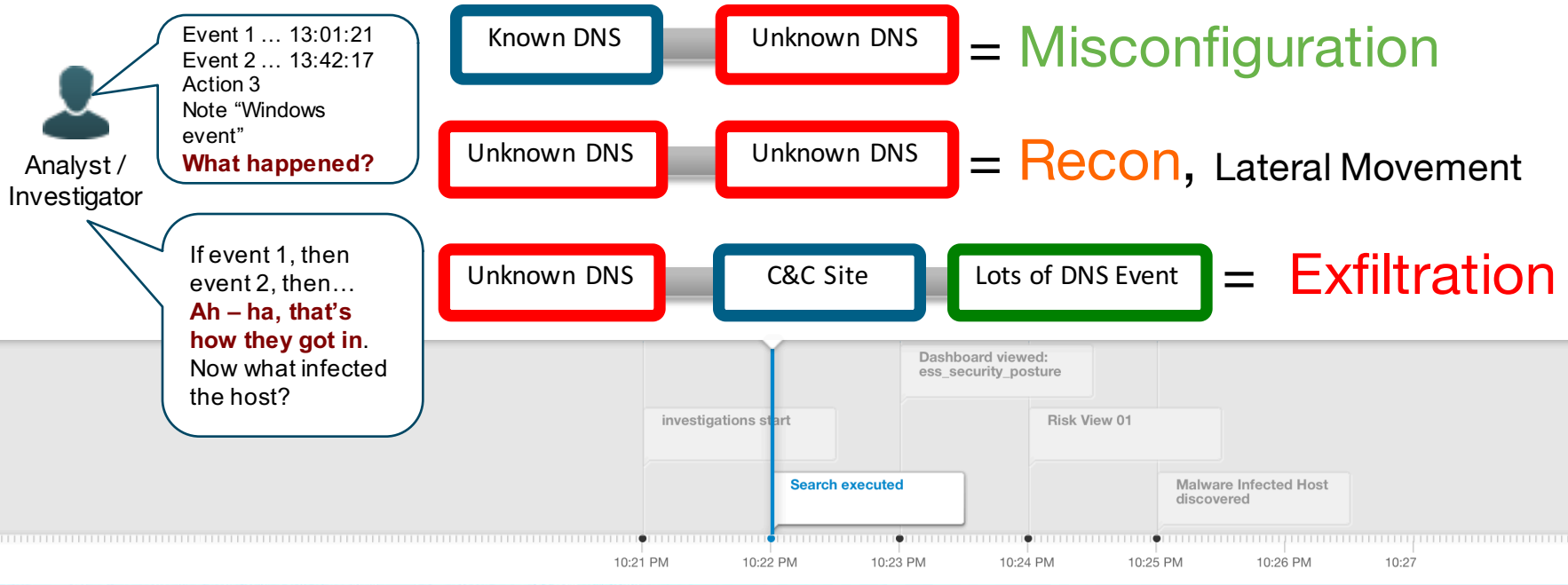
Hosts talking to recently registered domains

Discover outlier activity to newly registered domains

Identify unexpected top level domain activity

Inside Threat : How to detect and trace Unknown Data Exfiltration ??

Same events can have different security meanings, based on sequence:



Chasing Ransomware

Standard Remediation steps :

1) Isolate “the patient(s)”
2) Fix the “the patient(s)”
3) How did it get in?
   - What’s the link?
   - Who else has the link?(vector)
   - Who else has clicked the link?
4) Disconnect Shared drives
5) Start the restore ….

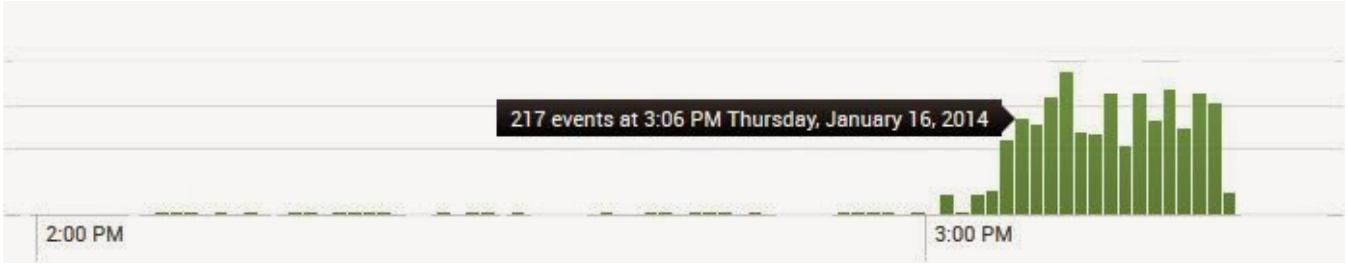
Who is patient ZERO ?

4663 (File/Reg Auditing) – In Splunk

_time	host	Security_ID	Handle_ID	Object_Type	Object_Name	Process_ID	Created_By	Accesses
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0xb4	File	C:\Windows\rescache\ResCache.mni	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0xa8	File	C:\Windows\rescache\rc0017\Segment1.cmf	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0xa0	File	C:\Windows\rescache\rc0017\Segment0.cmf	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0x9c	File	C:\Windows\rescache\rc0017\ResCache.hit	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0x98	File	C:\Windows\rescache\rc0017\ResCache.dir	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)

```
sourcetype=WinEventLog:Security EventCode=4663 NOT (Process_Name="*\\Windows\\servicing\\TrustedInstaller.exe" OR "*\\Windows\\System32\\poqexec.exe") NOT (Object_Name="*\\Users\\svc_acct\\pnp“ OR Object_Name="C:\\Users\\Surf\\AppData\\Local\\Google\\Chrome\\User Data*" NOT Object_Name="C:\\Users\\Surf\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations") NOT (Object_Name="C:\\Windows\\System32\\LogFiles\\*" OR Object_Name="*ProgramData\\Microsoft\\RAC\\*" OR Object_Name="*\\Microsoft\\Windows\\Explorer\\thumbcache*" OR Object_Name="*.MAP" OR Object_Name="*counters.dat" OR Object_Name="*\\Windows\\Gatherlogs\\SystemIndex\\*") | rename Process_Name as Created_By | table _time, host, Security_ID, Handle_ID, Object_Type, Object_Name, Process_ID, Created_By, Accesses
```

Detect CryptoLocker Type attack



View of a typical CryptoLocker events. EventID4663 = file deleted/write success

sourcetype="WinEventLog:Security" AND EventCode=4663 | stats count by src_ip

you can see the events and setup alerts to trigger when a threshold outside the norm of your users is reached. E.g. "> 250 events per hour"

sourcetype="WinEventLog:Security" AND EventCode=4663 | stats count by src_ip | where count > 250

⇨ **Alert !**

http://hackerhurricane.blogspot.hk/2014/01/how-to-detect-cryptolocker-type-attack.html

Drill down view for the patient zero

sourcetype="WinEventLog:Security" EventCode=4663 | stats count values(Object_Name) by src, user | where count > 2000

Events | Patterns | Statistics (1) | Visualization

20 Per Page | Format | Preview

src	user	count	values(Object_Name)
same-ad3	admin_Hax0r	121194	E:\S h ir d\ J I Te pl it s E:\S h ir d\ J I Te pl it s\ .docx E:\S h ir d\ J I Te pl it s\ .rtf E:\S h ir d\ J I Te pl it s\ S I e ie A s E:\S h ir d\ J I Te pl it s\ S I e ie w :\ 2 5 t p t s.rtf E:\S h ir d\ J I Te pl it s\ S I e ie w :\ 2 E i .rtf E:\S h ir d\ J I Te pl it s\ S I e ie w :\ 2 E .rtf E:\S h ir d\ J I Te pl it s\ S I e ie v :\ 3 .rtf E:\S h ir d\ J I Te pl it s\ S I e ie v :\ .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e v :\ 2 4 .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e v :\ 2 .docx E:\S h ir d\ J I Te pl it s\ J S I e v e v :\ 4 1 .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e v :\ 5 6 .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e r s \ 3 1 : 2 .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e r s \ 3 7 D .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e r s \ 4 X .rtf E:\S h ir d\ J I Te pl it s\ J S I e v e r s \ 5 1 .docx

Who

Where

What

Find the infection relationship by one search

We know:

– User IDs of encrypted files on shared drives

We assume:

– Payload/link was delivered by e-mail or web

What does Splunk know:

– Mail header logs

– Proxy logs

```
sourcetype="MSExchange:2010:MessageTracking"
recipients="*user1*" OR recipients="*user2*" OR
recipients="*user3*" OR recipients="*user4*"

|eval user1=if(searchmatch("user1"),1,0)
|eval user2=if(searchmatch("user2"),1,0)
|eval user3=if(searchmatch("user3"),1,0)
|eval user4=if(searchmatch("user4"),1,0)

| stats  count,sum(user1),sum(user2),
         sum(user3), sum(user4) by
    sender_domain,sender
```

Specify email

Select users

Mark each email based on who received it

Show me a table of senders and receivers

We can find the hacker's email in sec …

Email Senders

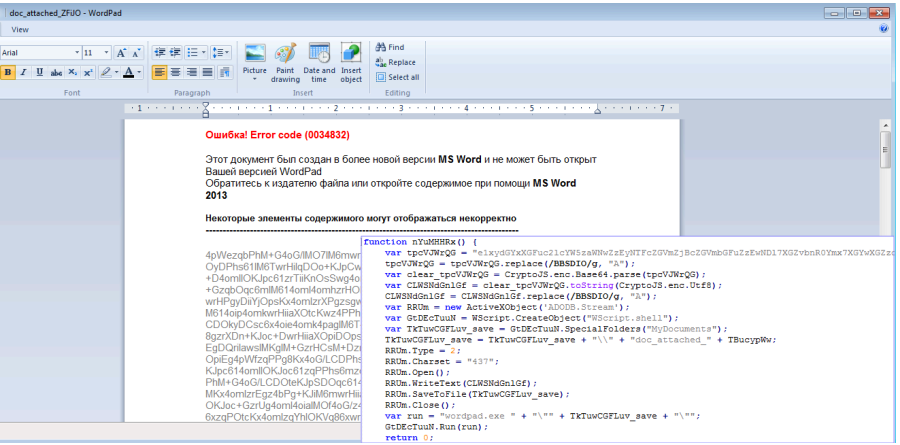
Each Infected User

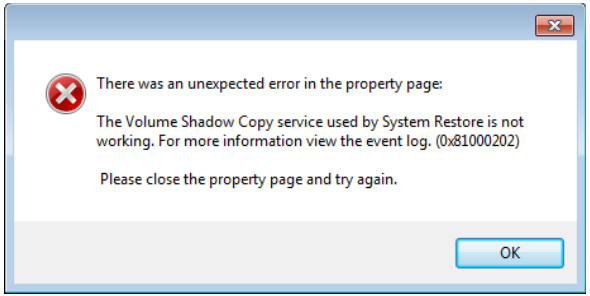
sender_domain	sender	count	User1	User2	User3	User4
auspost.com.au	22q531ret431@auspost.com.au	2	2	2	2	2
cscinfo.com	CSCMatterManagement@cscinfo.com	2	0	0	2	0
cscinfo.com	proofpoint-pps@cscinfo.com	6	0	0	6	0

Every user received this email

Same process for proxy logs

RAA, a new Ransomware variant using only JavaScript





- exclusively uses JavaScript in order to encrypt personal files using AES.
- this ransomware also drops Pony malware (a well-known info-stealer).
- malicious email attachments pretending to be .doc files. when executed, is drop a file in the %userprofile%\documents folder and open that with WordPad, pretending it is corrupt.
- to make sure that files cannot be recovered using the File History option, the Volume Shadow Service (VSS) is deleted.

http://blog.emsisoft.com/2016/06/15/raa-a-new-ransomware-variant-using-only-javascript/

Detect the creation of the new run service

```
} while (jcayrm < lCMTwJKZ.length);
if (AFtKLHIjDtkM < 2 && QCY == 0) {
    var TKVUdGUkzCmE = WScript.ScriptFullName;
    TKVUdGUkzCmE = TKVUdGUkzCmE + " argument";
    var qPOGRFfINeNb = WScript.CreateObject("WScript.Shell");
    qPOGRFfINeNb.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\", TKVUdGUkzCmE, "REG_SZ");
    HxBG();
} else {
    null;
}
return 0;
```

sourcetype="WinEventLog:Security" AND EventCode=7045 | stats count by src_ip

Service added to the endpoint

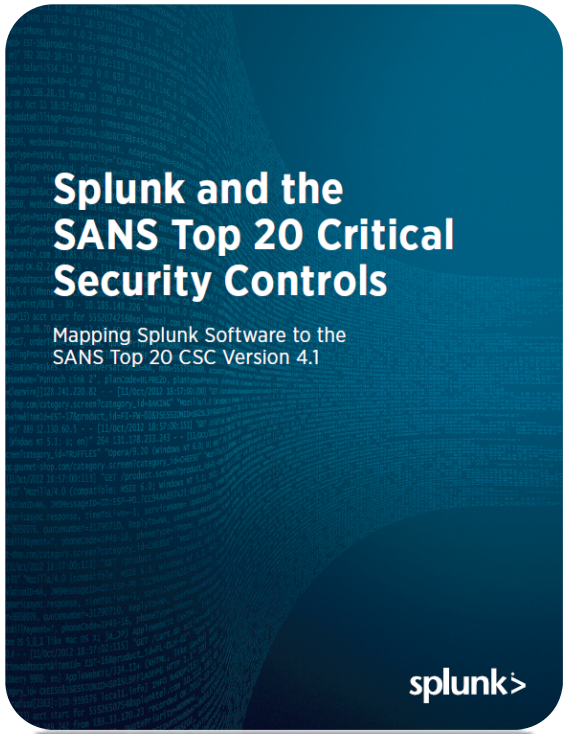
Six Windows Events to monitor

Win ID	What	Impact to Security	Activity detected
4688/592	New Process executed	Malware executed or malware actor trying to take action	New programs installed by attacker (not by user)
4624/528 /540	Some account logged in	Attacker authenticated to the endpoint	What accounts did and what accounts at what times are normal?
5140/560	A share was accessed	What endpoints were accessed	C$ share or File share accessed
5156	Windows Firewall Network connection by process	Command and Control or origin of attack	What application was used to communicate with external or internal IP
7045/601	Service added to the endpoint	Persistence to load malware on restart	Service added or modified
4663/567	File & Registry auditing	Modifications to the system that create holes or payloads used at a later time	Files added and Registry Keys added to audited locations

Best Practice **Guidelines**

Refer to the Splunk SANS 20 whitepaper for detailed use cases and examples of how customers use Splunk for security to achieve the anticipated improvement with:

- ✓ **Faster Detection of Security Events**
- ✓ **Faster Research and Investigation**
- ✓ **Reduced Risks with Data Breach and further protect your Brand**



Thank You

cyue@splunk.com

splunk>

Steps You Will Need to Take

- Enable Advanced Audit Policy in Windows
  - The "Windows Logging Cheat Sheet"
  - Audit Process Creation = Success — 4688
  - Audit Logon = Success & Failure — 4624
  - Audit File Share = Success — 5140
  - Audit File System = Success — 4663
  - Audit Registry = Success — 4663 & 4657
  - Audit Filtering Platform Connection = Success — 5156 (Any/Any min)
  - Services already captured by System Log — 7045 & 7040
- Enable and Configure to capture ***Process Command Line***
- Use the Splunk Universal Forwarder or Splunk Window Infrastructure App or syslog… to get data to central location
  - Modify the inputs.conf to blacklist or whitelist as needed

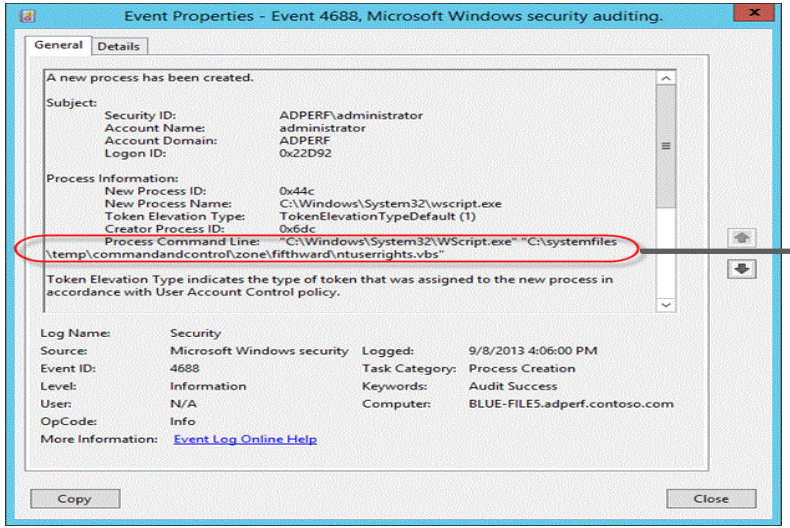
Enable Command Line Logging : Windows 7 Through 2012 (Win 10 too)

"Include command line in process creation events“

- http://technet.microsoft.com/en-us/library/dn535776.aspx

1. Windows 8.1 and 2012 R2
   - Administrative Templates\System\Audit Process Creation
2. You must have the patch for MS15-015 (KB3031432) for Win 7 and Win 2008, From Feb 2015
3. Registry key tweak
   - Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit\ProcessCreationIncludeCmdLine_Enabled to DWORD - 1

And You Will See this Added to Your Logs



- Only a fraction more data
- Most valuable thing to log

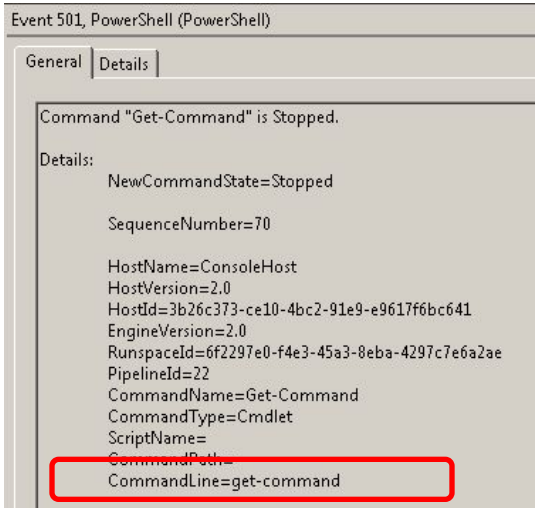
Additional context important to identify abnormal behavior

_time	host	Account_Name	Process_Command_Line	New_Process_Name	New_Process_ID	Creator_Process_ID	Short_Message
2015-07-27 05:27:33	Some Server	Some_Admin	Powershell.exe -v 2 [illegible]\Powershell [illegible]cmas.ps1	C:\Windows\System32 \WindowsPowerShell \v1.0\powershell.exe	0x3a70	0x2118	A new process has been created

PowerShell – Command Line

Details on setting PowerShell preference variables
- http://technet.microsoft.com/en-us/library/hh847796.aspx

1. Create a default profile for all users:
   - C:\Windows\System32\WindowsPowerShell\v1.0Profile.ps1
2. Add these to your default profile.ps1 file
   - $LogCommandHealthEvent = $true
   - $LogCommandLifecycleEvent = $true
3. Splunk - Inputs.confindows platform specific input processor
   - [WinEventLog://Windows PowerShell]
   - disabled = 0
4. Upgrade PowerShell to ver 3 or ver 4



- Investigating PowerShell Attacks (DefCon & Blackhat 2014)
  - Ryan Kazanciyan TECHNICAL DIRECTOR, MANDIANT
  - Matt Hastings CONSULTANT, MANDIANT