Active Defense and the Hunting Maturity Model

Session Objectives

- Provide MISO's background for Active Defense
- Share three hunting examples
- Share overall major lessons learned

Active Defense

- Proactive
- Internal Threats
- People
- Learning

Robert M. Lee, “The Sliding Scale of Cyber Security”, A SANS Analyst Whitepaper, Aug. 2015, https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Disclaimer

Examples and data used in this presentation are **NOT** NERC CIP related or regulated in any other way

Also **NOT** an endorsement of any products

About Me

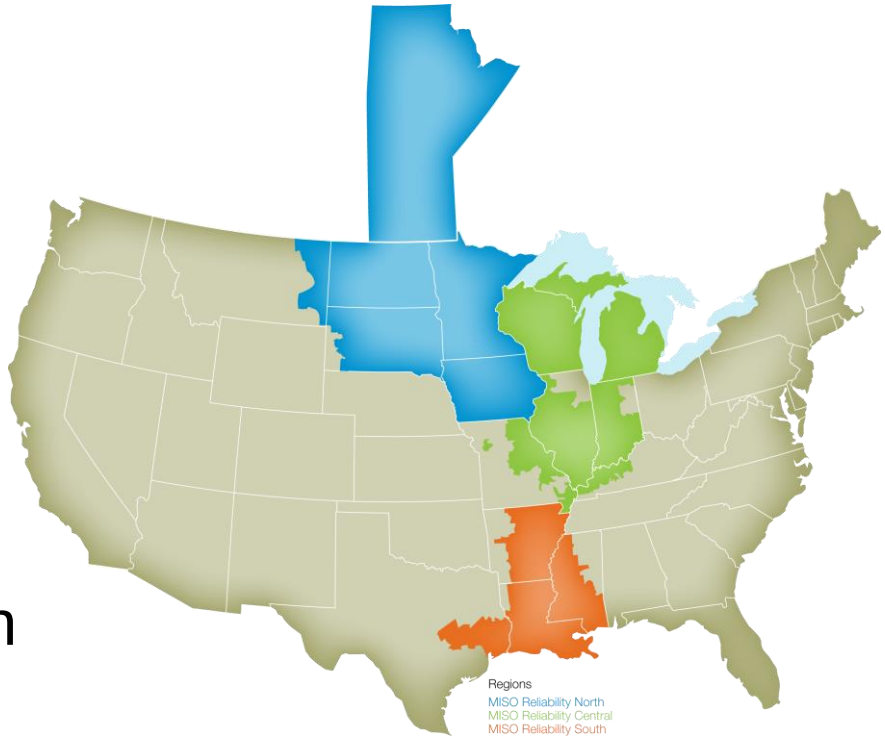
Jamie Buening

- Purdue University
  - Telecommunications & Networking
- ExxonMobil – 7 years
  - UNIX Admin / Network Security
- MISO – 10 years
  - Network Analyst / Compliance / Information Security

What is MISO?

Midcontinent Independent System Operator

- “Air traffic controllers” of the bulk electric system
- Large SCADA network – 291,539 SCADA data points, 6,541 generating units
- Manages one of the world’s largest energy and operating reserves markets - $25.3 billion gross market charges (2016)



Why embrace Active Defense and Hunting?

- Number of alerts
- False positives

- Advanced attacks hide their tracks
- Signature based technology

- Must proactively hunt for anomalies and IOCs
- Using external and internal threat intelligence.

The Way Forward

Leverage internal and external threat intelligence

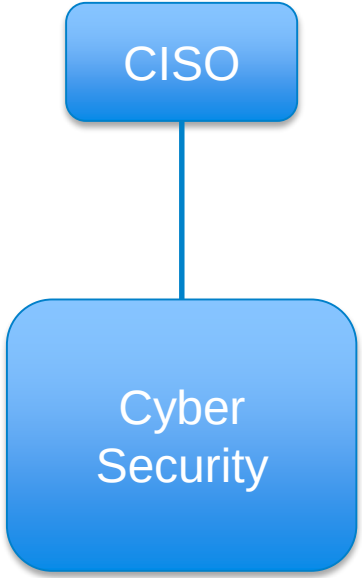
Normalize and baseline the environment

Acquire the correct data

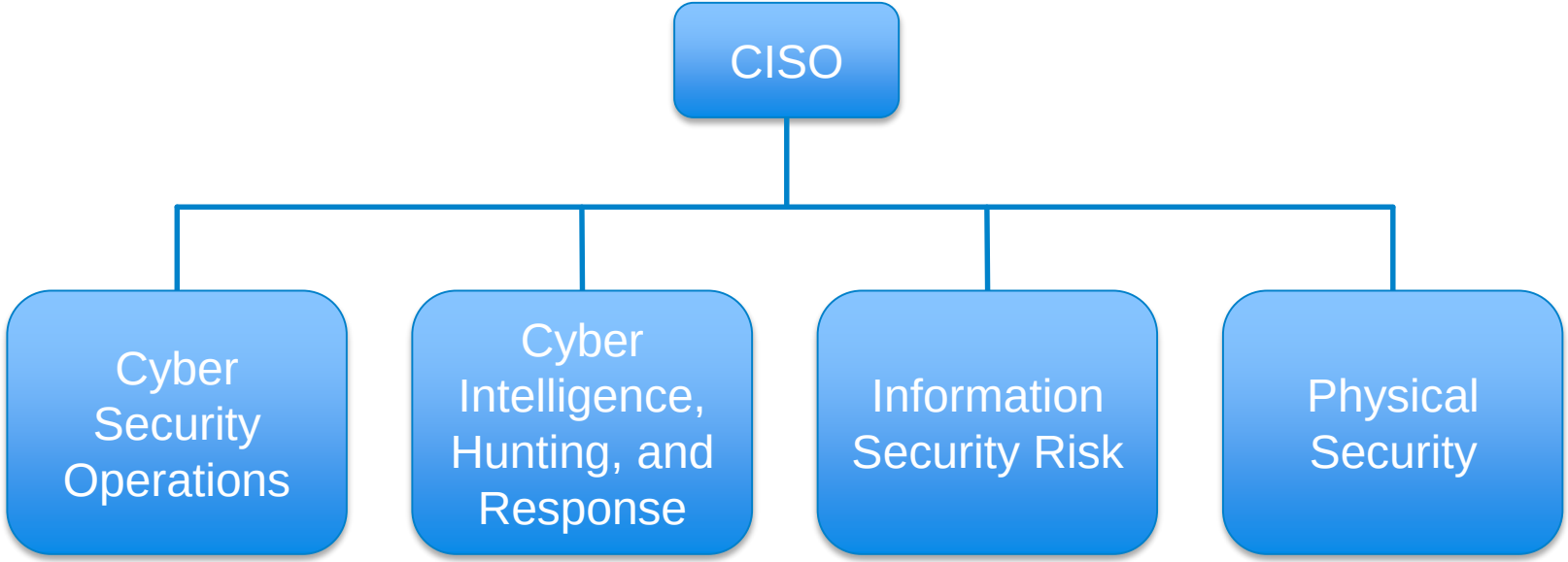
Utilize data analysis tools

Employ people with the right skills that ask the right questions

Original Cyber Security Organization



New Cyber Security Organization



Hunting at MISO

In 6 months, MISO has transitioned from an alert-driven, reactive state to a proactive, maturing cyber hunting capability

- A proactive, intelligence driven security program ensures the organization can detect and respond to security events.
- The goal is to reduce and minimize impact to critical business functions.

Hunting Maturity Model

HMM0 Initial
- Relies primarily on automated alerting
- Little or no routine data collection

HMM1 Minimal
- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

HMM2 Procedural
- Follows data analysis procedures created by others
- High or very high level of routine data collection

HMM3 Innovative
- Creates new data analysis procedures
- High or very high level of routine data collection

HMM4 Leading
- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

MISO

David Bianco, “A Simple Hunting Maturity Model,” Enterprise Detection & Response blog, Oct. 15, 2015, http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

Use Case Examples

Multiple Threat Intelligence Sources, each of which can drive hunting trips

Subscription based services

Industry-Specific Threat Feeds
- EISAC
- ICS-CERT
- East-West Inst.

Data Analytics
- Machine Learning
- Statistical Analysis
- Visualizations

Internal IT logs and events

Behavioral Analysis
- Performance
- Attendance
- HR/Travel

HTTP Exploit Attempts

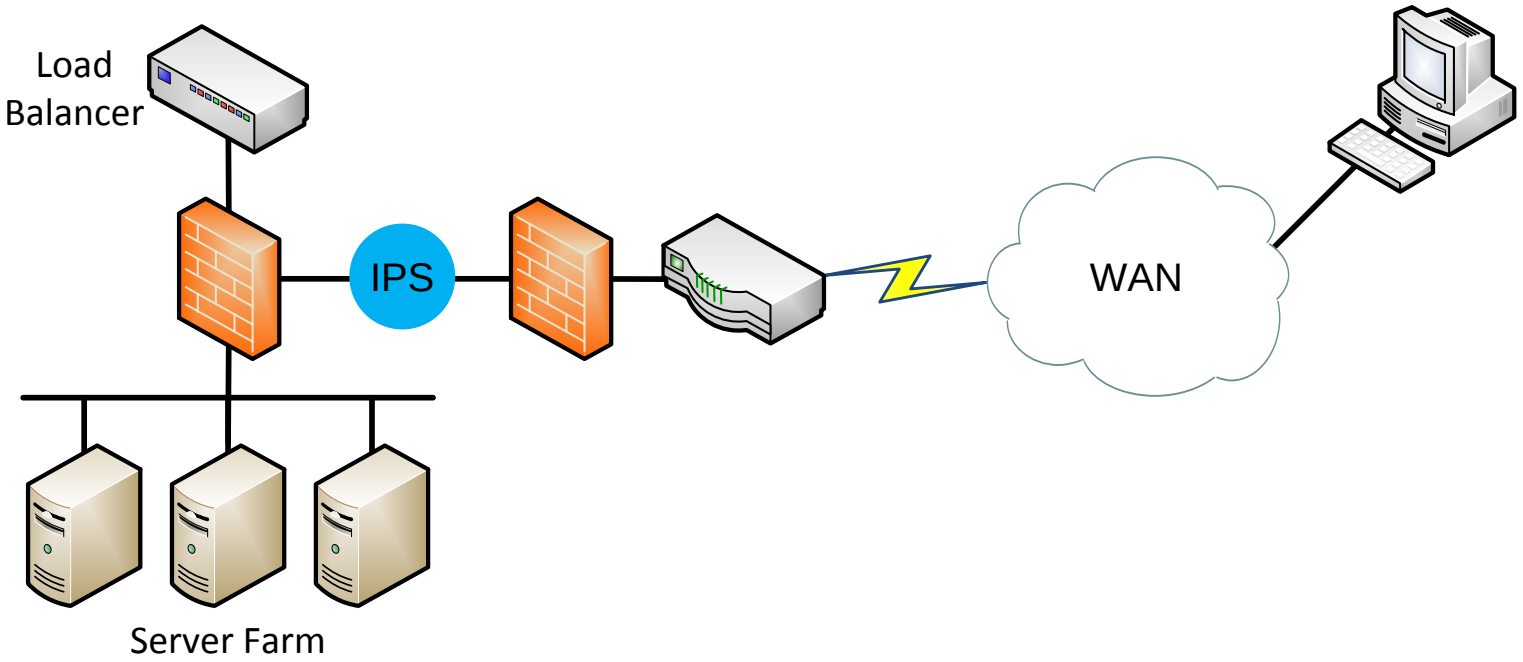
HMM0 - Initial (Automated Alerting)

HTTP Exploit Attempt Alerts

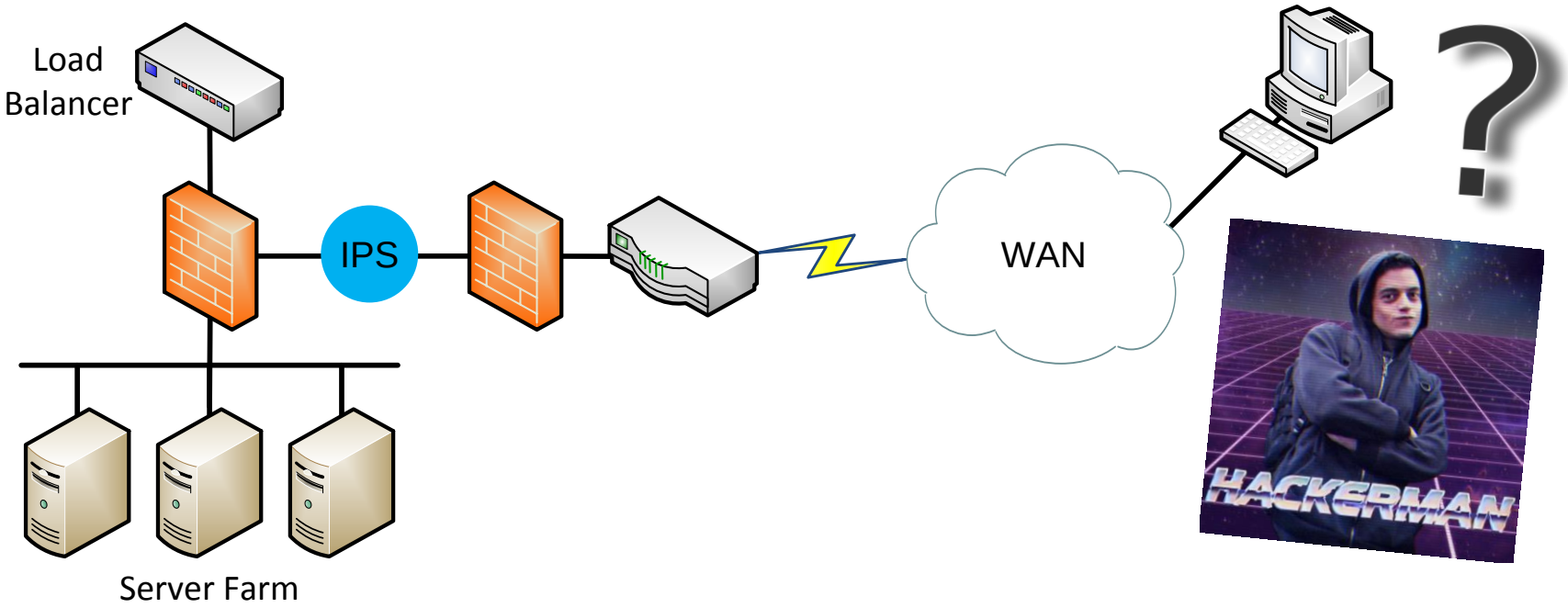
Situation:

- IPS alerts for blocked HTTP exploit attempts from WAN
- Possible they were an accidental scan
- Cyber Security Operations handed over to Cyber Intelligence, Hunting, and Response

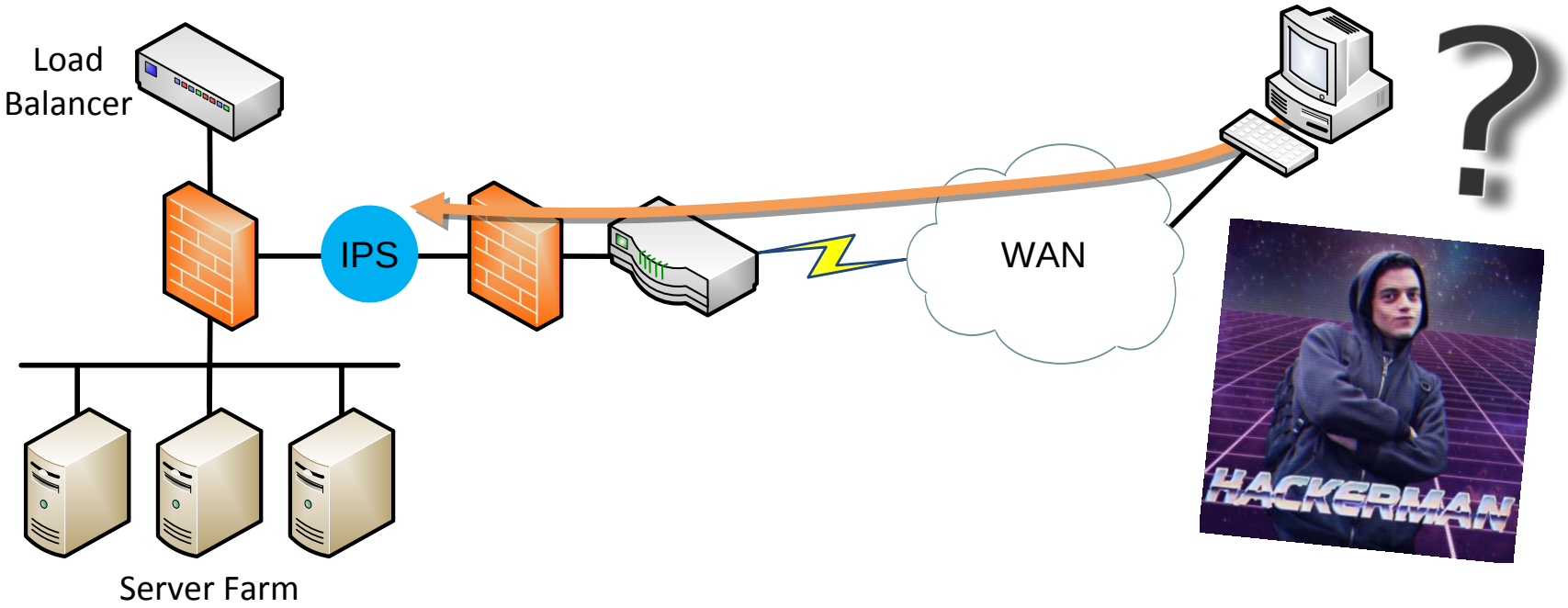
HTTP Exploit Attempt Alerts



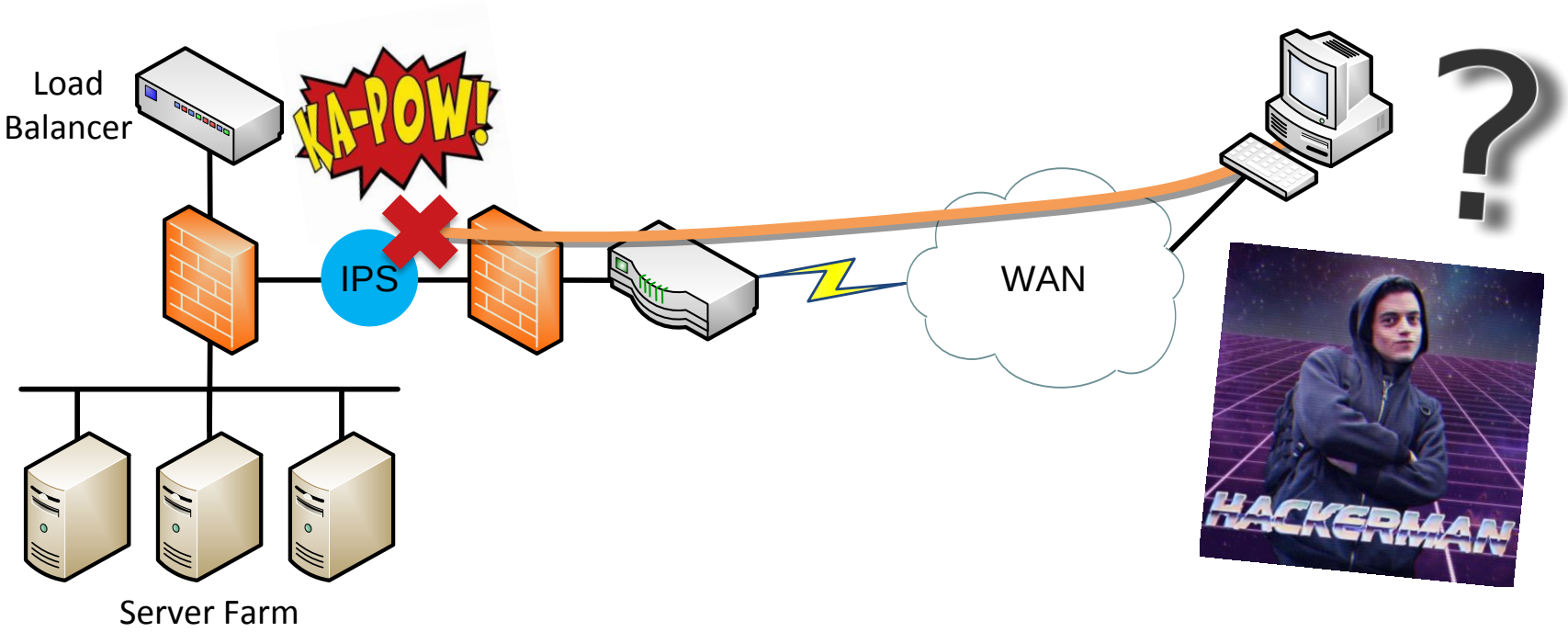
HTTP Exploit Attempt Alerts



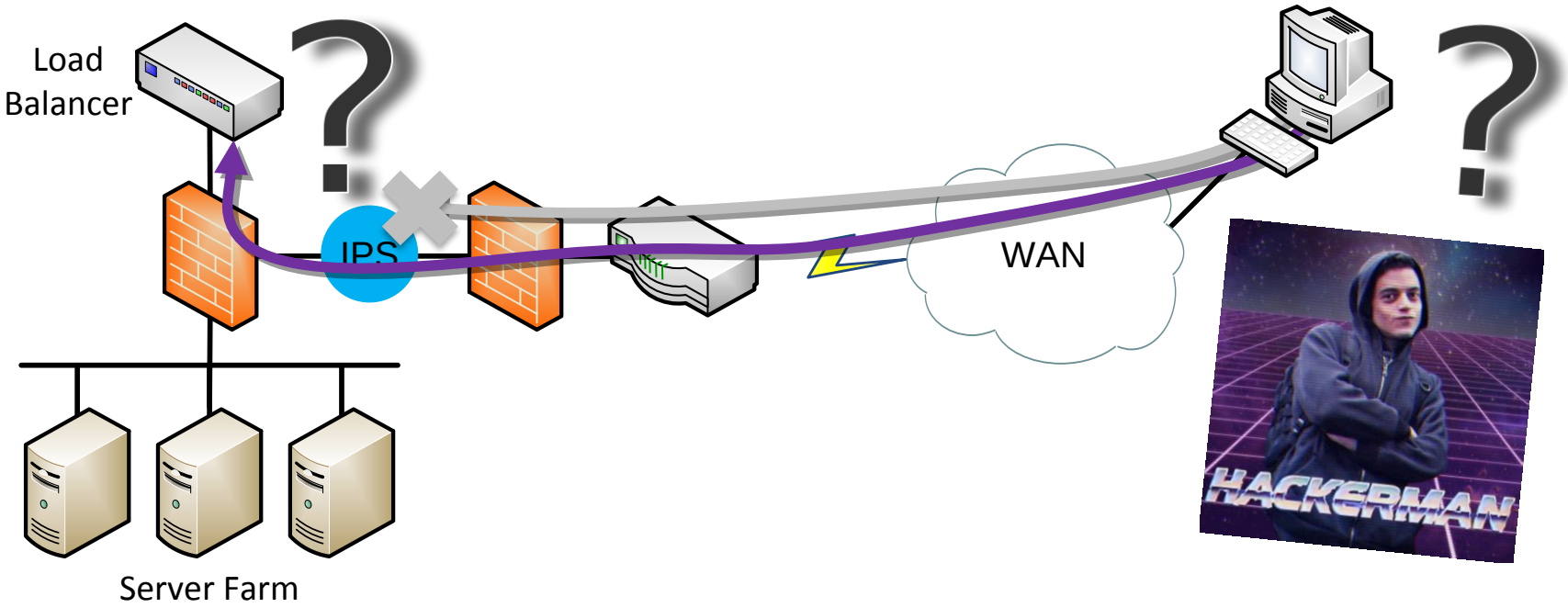
HTTP Exploit Attempt Alerts



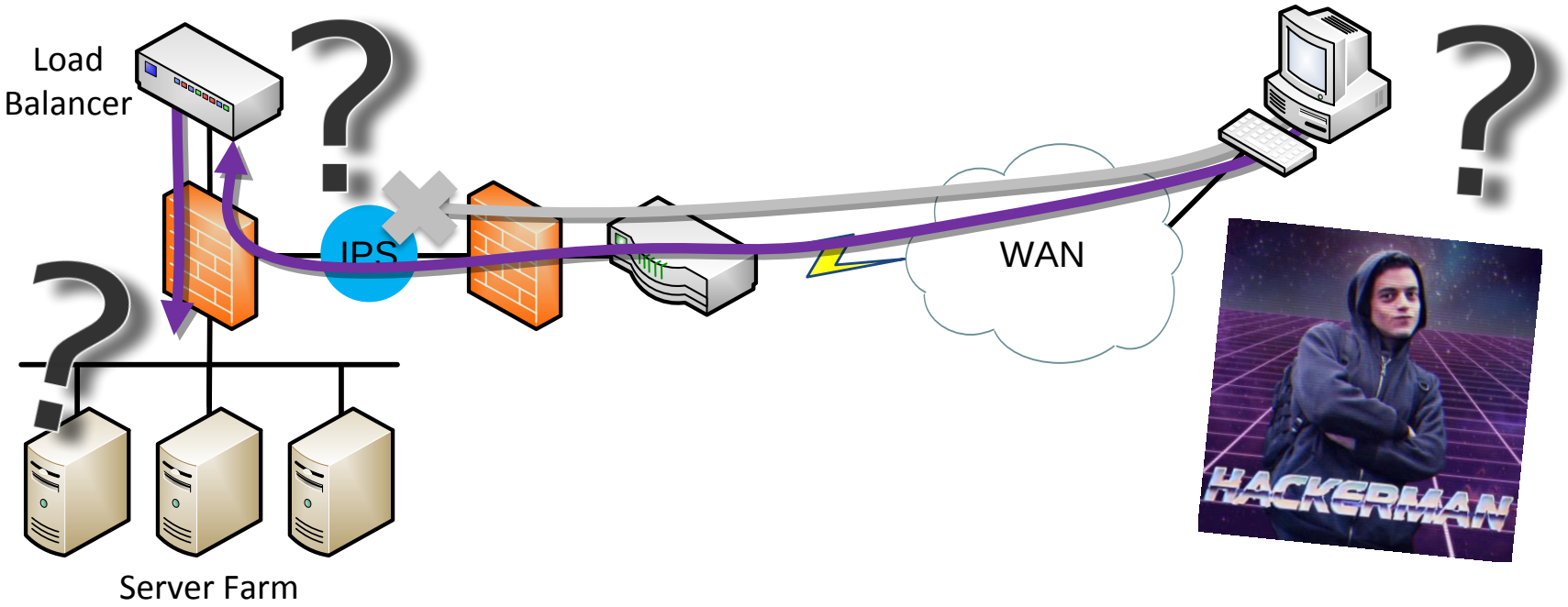
HTTP Exploit Attempt Alerts

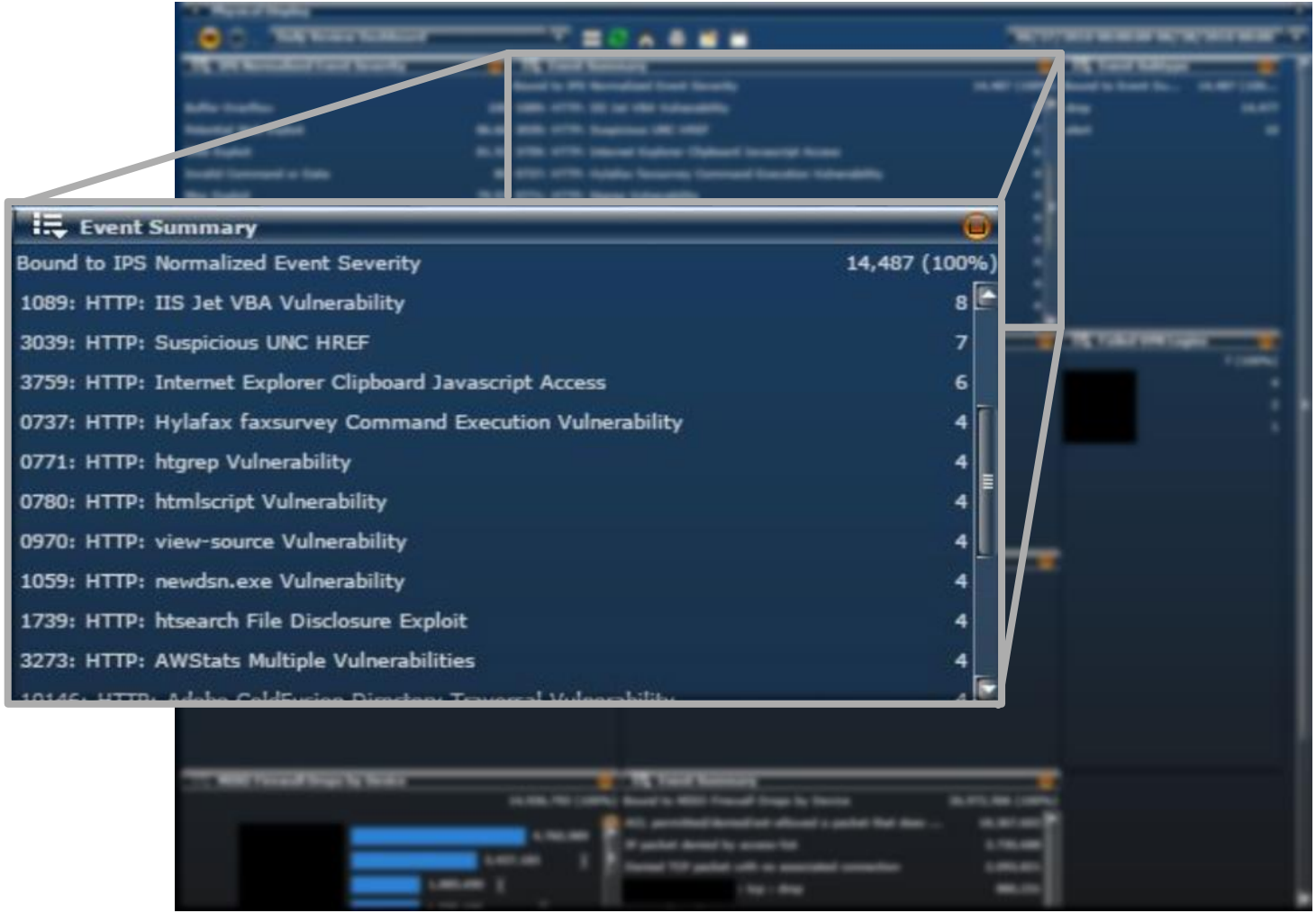


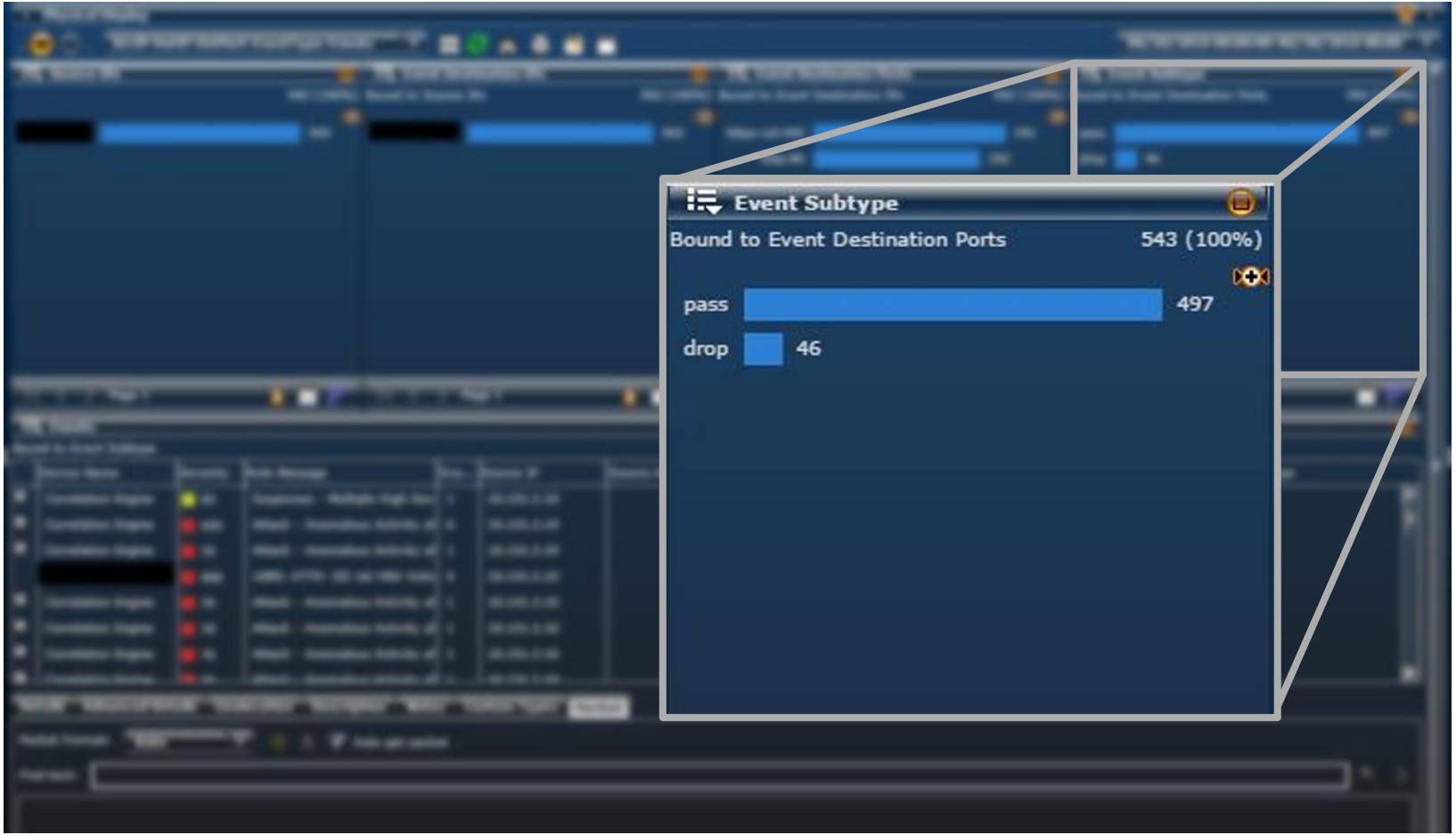
HTTP Exploit Attempt Alerts



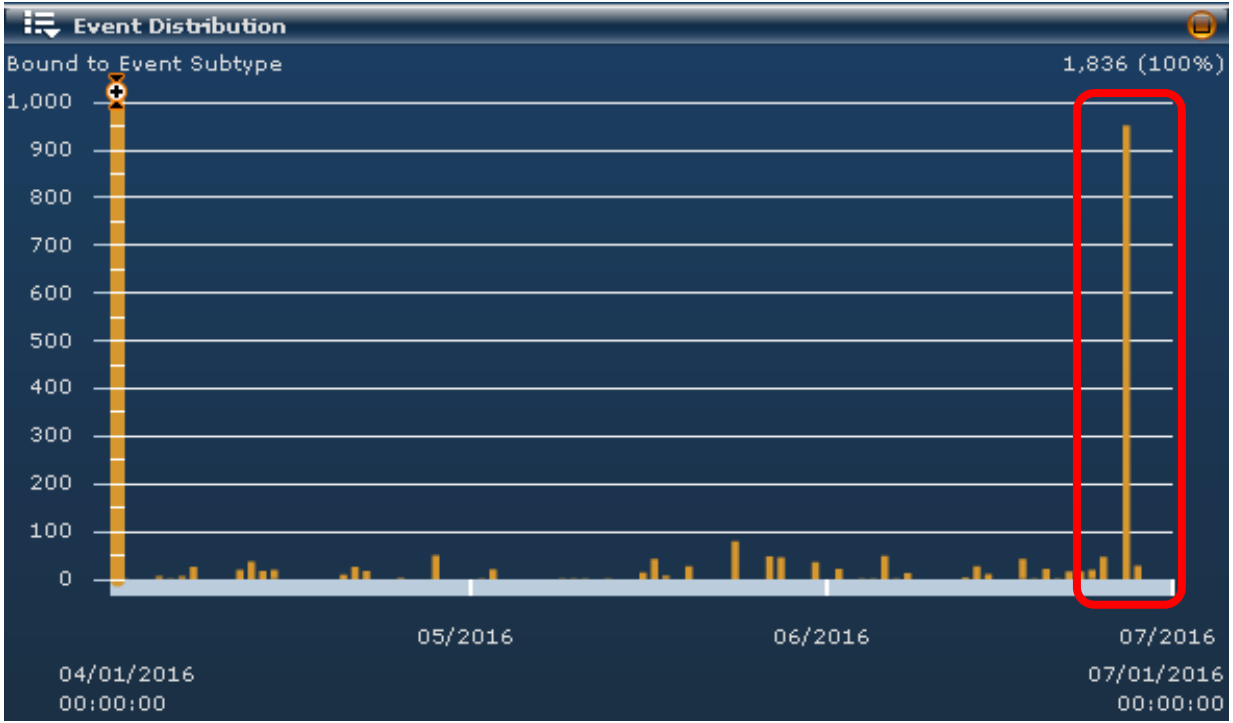
HTTP Exploit Attempt Alerts




Event Summary
Bound to IPS Normalized Event Severity 14,487 (100%)
1089: HTTP: IIS Jet VBA Vulnerability 8
3039: HTTP: Suspicious UNC HREF 7
3759: HTTP: Internet Explorer Clipboard Javascript Access 6
0737: HTTP: Hylafax faxsurvey Command Execution Vulnerability 4
0771: HTTP: htgrep Vulnerability 4
0780: HTTP: htmlscript Vulnerability 4
0970: HTTP: view-source Vulnerability 4
1059: HTTP: newdsn.exe Vulnerability 4
1739: HTTP: htsearch File Disclosure Exploit 4
3273: HTTP: AWStats Multiple Vulnerabilities 4


Event Subtype
Bound to Event Destination Ports
543 (100%)
pass
497
drop
46

HTTP Exploit Attempt Alerts



HTTP Exploit Attempt Alerts

What happened next?

- Investigated load balancer and server logs
- Nothing suspicious found
- Company did verify it was an accidental scan due to a misconfiguration

HTTP Exploit Attempt Alerts

Lessons Learned:

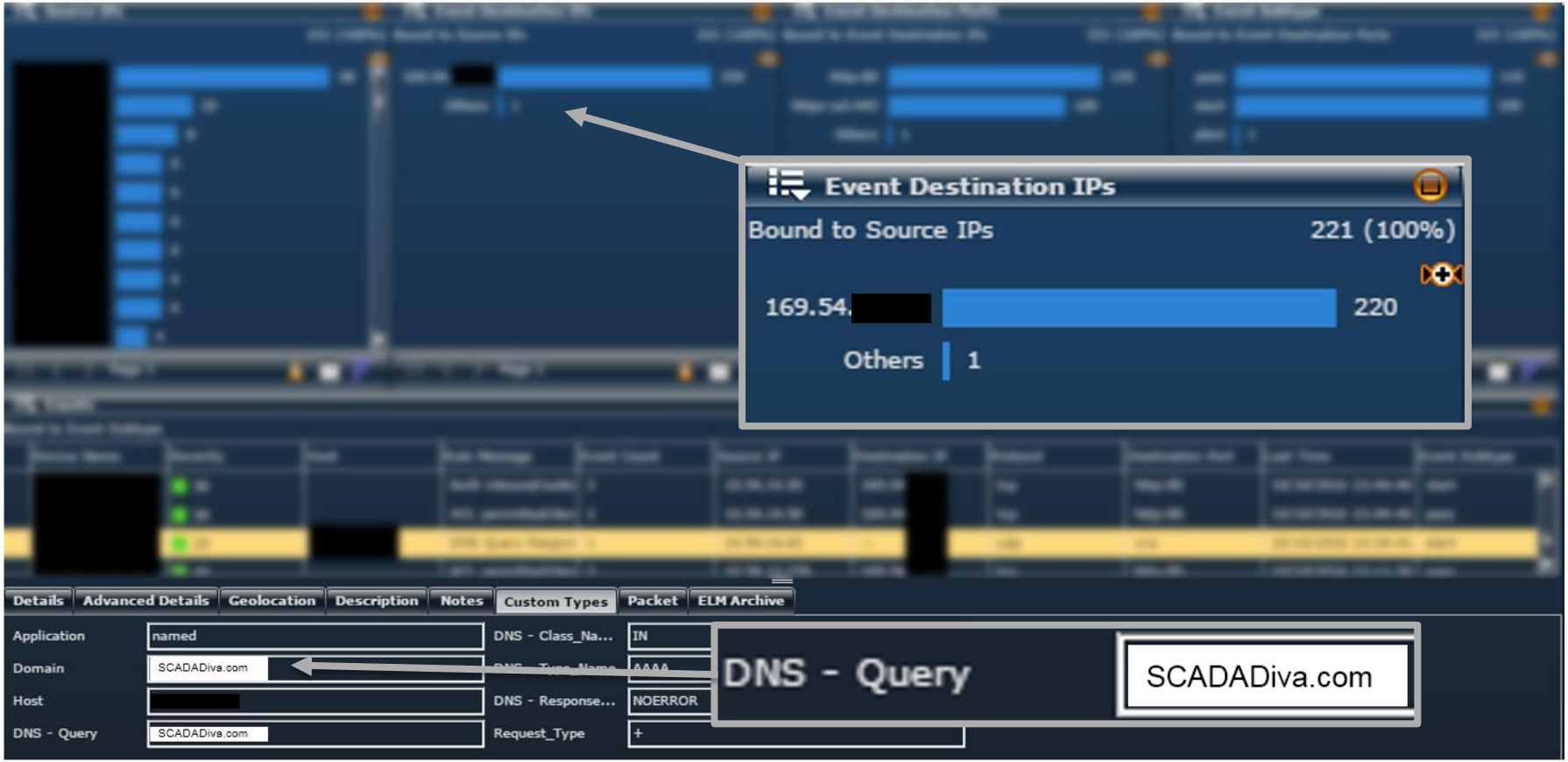
- Process – Cyber Ops identification
- SIEM had data needed for analysis
- Documentation on systems was available
- Additional experience using IR Plan
- Should be able to identify spike

E-ISAC Bulletin - Ransomware

HMM1 – Minimal (Indicator Search, High Collection)

E-ISAC Cyber Bulletin - Ransomware

- Cyber Bulletin with multiple indicators
- Searched logs and found evidence of one indicator related to a payload URL
- Not a strong match to the expected sequence
  - Email attachment with macros
  - Establish C2
  - Retrieve payload
- But didn’t understand why user systems were hitting the payload URL


Event Destination IPs
Bound to Source IPs
221 (100%)
169.54.[redacted]
220
Others
1
Details
Advanced Details
Geolocation
Description
Notes
Custom Types
Packet
ELM Archive
Application
named
Domain
SCADADiva.com
Host
[redacted]
DNS - Query
SCADADiva.com
DNS - Class_Na...
IN
AAAA
DNS - Response...
NOERROR
Request_Type
+
DNS - Query
SCADADiva.com

E-ISAC Cyber Bulletin - Ransomware

What to do next?

- Talk with one of the users
  - They were not familiar with the URL / site
- Analyze their computer
  - Goal – determine what caused the connection
  - How – Use procedure learned in IR training
  - Tool – Mandiant Redline

E-ISAC Cyber Bulletin - Ransomware

SCADADiva.com resolves to 3 IP addresses

Who owns IP addresses?

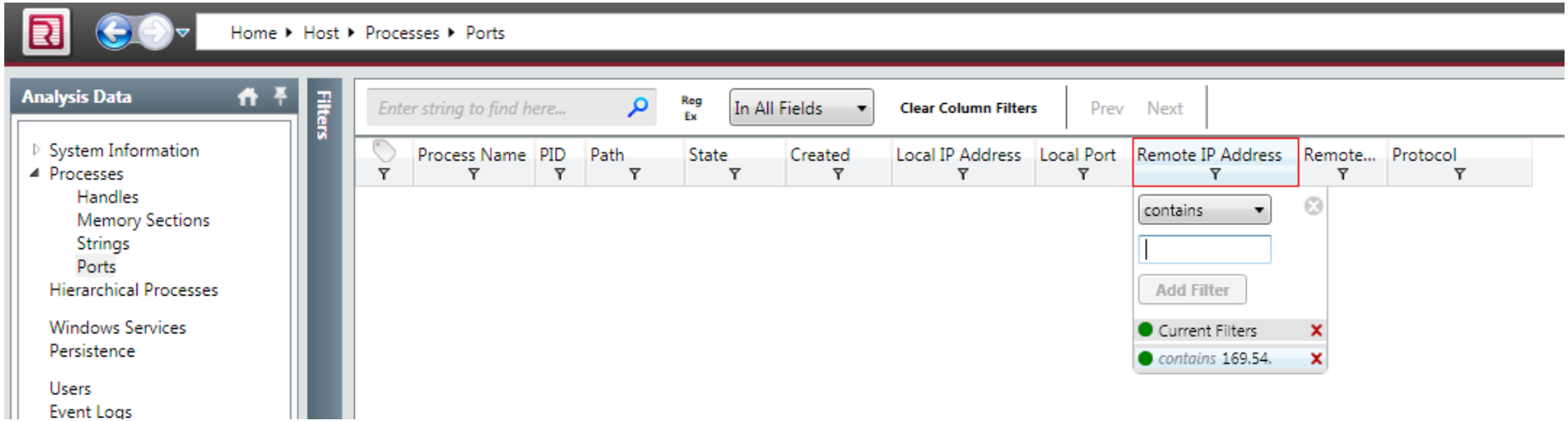
whois results:

169.54.a.b Something, Inc., mnt-by …
169.54.c.d Assante, Inc (d/b/a SCADA Diva), mnt-by …
169.54.e.f Assante, Inc (d/b/a SCADA Diva), mnt-by …

E-ISAC Cyber Bulletin - Ransomware

Open Ports Review – Still communicating?

- Search – 3 IP addresses with 169.54 as first 2 octets



E-ISAC Cyber Bulletin - Ransomware

Web History Review – URL only, no IPs

- Temp URLs, CDNs, Vendor sites

Home ▸ Host ▸ Browser URL History

Analysis Data

- System Information
- Processes
  - Handles
  - Memory Sections
  - Strings
  - Ports
- Hierarchical Processes
- Windows Services
- Persistence
- Users
- Event Logs

Filters

Enter string to find here... | Reg Ex | In All Fields | Clear Column Filters | Prev | Next

Visit Type	Last Visit Date	URL
URL	2016-09-12 15:16:20Z	file:///C:/Users/[redacted]/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/
URL	2016-09-12 15:16:21Z	https://SCADADiva.com ?004?md5=49ee5cb3a7e0a3acb7e1414bb462d6e0
URL	2016-09-12 15:16:21Z	[illegible]
URL	2016-09-12 15:16:21Z	file:///C:/Users/[redacted]/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/
URL	2016-09-12 15:16:22Z	file:///C:/Users/[redacted]/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/
URL	2016-09-12 15:16:27Z	[illegible]

MISO

E-ISAC Cyber Bulletin - Ransomware

Prefetch Review

- What programs first executed between timeframe?

Home ▸ Host ▸ Prefetch ▸

Analysis Data

- System Information
- Processes
  - Handles
  - Memory Sections
  - Strings
  - Ports
- Hierarchical Processes
- Windows Services
- Persistence
- Users
- Event Logs
- Tasks

Enter string to find here... | Reg Ex | In All Fields | Clear Column Filters | Prev | Next

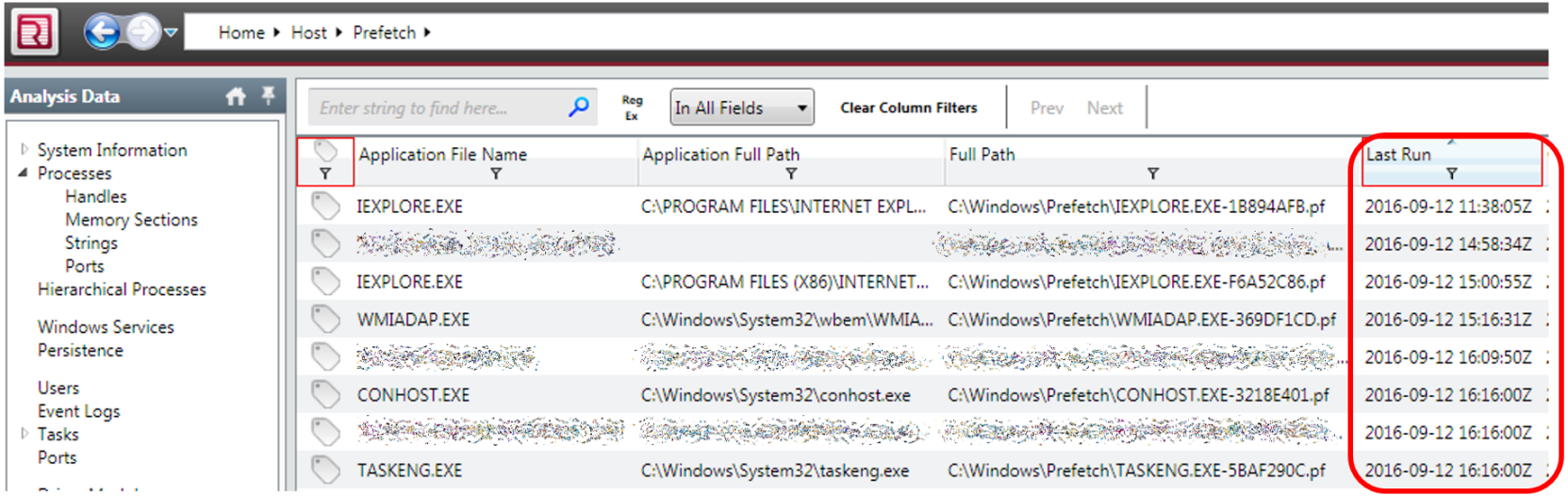
Application File Name	Application Full Path	Full Path	Last Run	Created	Times Executed
[illegible]		[illegible]	2016-09-12 11:20:46Z	2016-09-12 11:20:53Z	1
RUNDLL32.EXE	C:\Windows\System32\rundll32.exe	C:\Windows\Prefetch\RUNDLL32.EXE-465F5810.pf	2016-09-12 13:44:22Z	2016-09-12 13:44:33Z	1
MAGENT.EXE		C:\Windows\Prefetch\MAGENT.EXE-A45D4DEE.pf	2016-09-12 13:45:19Z	2016-09-12 13:45:30Z	1
RUNDLL32.EXE	C:\Windows\System32\rundll32.exe	C:\Windows\Prefetch\RUNDLL32.EXE-AFD98684.pf	2016-09-12 14:09:42Z	2016-09-12 14:09:42Z	1
RUNDLL32.EXE	C:\Windows\System32\rundll32.exe	C:\Windows\Prefetch\RUNDLL32.EXE-4D251445.pf	2016-09-12 14:09:42Z	2016-09-12 14:09:53Z	1
RUNDLL32.EXE	C:\Windows\System32\rundll32.exe	C:\Windows\Prefetch\RUNDLL32.EXE-0775585A.pf	2016-09-12 14:53:38Z	2016-09-12 14:53:39Z	1
RUNDLL32.EXE	C:\Windows\System32\rundll32.exe	C:\Windows\Prefetch\RUNDLL32.EXE-2215047F.pf	2016-09-12 15:15:28Z	2016-09-12 15:15:38Z	1

MISO

E-ISAC Cyber Bulletin - Ransomware

Prefetch Review

- What programs <u>last ran</u> between timeframe?



E-ISAC Cyber Bulletin - Ransomware

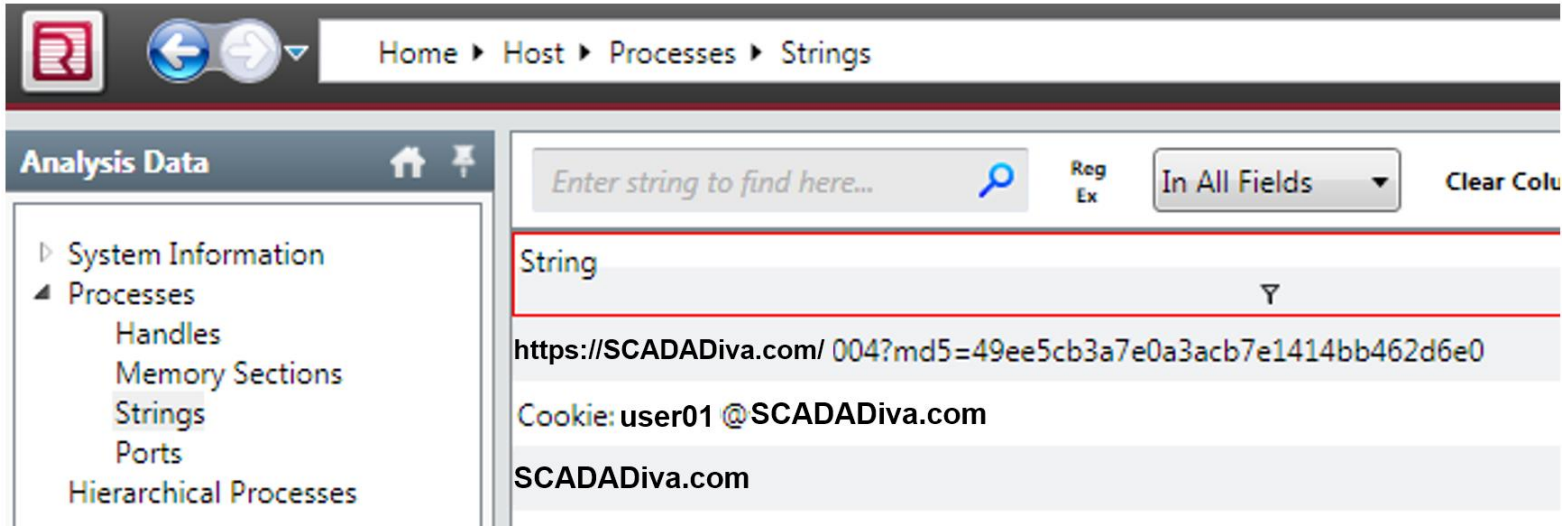
Identify purpose of non-standard OS binaries

File	Description/Purpose
MAGENT.EXE	Mandiant Redline Agent – used to perform Redline collection.
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
CERTLOADER.EXE	Custom program written by MISO IT

E-ISAC Cyber Bulletin - Ransomware

Memory Strings

- 105 Domain matches / no IP address matches



E-ISAC Cyber Bulletin - Ransomware

For PIDs containing string

- Memory sections digitally signed & verified?
- Any signs of process injection?

PID	Signed/Verified	Injection
5732	Yes	No
5096	N/A	No
768	N/A	No
4368	Yes	No
1848	N/A	No
2512	Yes	No
3316	No (MD5 ok)	No
5056	N/A	No
2952	Yes	No
5912	Yes	No

E-ISAC Cyber Bulletin - Ransomware

Took a step back to review work

- Nothing obvious showing up
- Considered everything within context
  - Browsing history / processes / URL had MD5 hash / cookie in memory string
  - Made most sense it was a tracker

E-ISAC Cyber Bulletin - Ransomware

Determination: Not Malicious

- SCADADiva.com page is for 1x1 pixel tracking
- URL in memory strings included MD5 hash
- Cookie also found in memory strings
- Found information showing SCADA Diva, Inc. sells marketing intelligence /consumer data
- No malicious executables or memory injections

E-ISAC Cyber Bulletin - Ransomware

Lessons Learned:

- Building familiarity with Windows processes
- Practice with newer analysis
- Even more experience with IR plan
- First collection failed (USB drive space)
- User interruption
- Needed assistance to execute Mandiant Redline

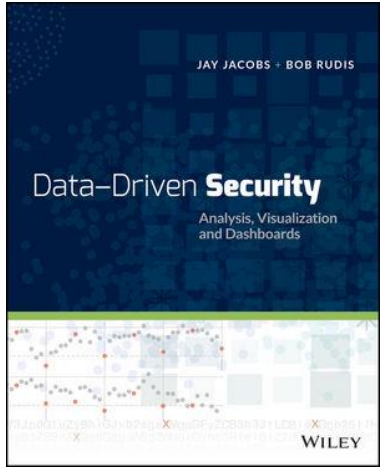
DNS Analysis

HMM2 – Procedural (Others' Procedures, High Collection)

DNS Analysis

Why DNS?

- Good source of data
- Available ideas
- Detailed logs available
- *Data-Driven Security – Analysis, Visualization and Dashboards*



DNS Analysis

Specifically…

- Adversaries can utilize DNS Tunneling for:
  - Command and Control
  - Data Exfiltration
  - Tunneling of any IP traffic
- If tunneling at MISO
  - We will see long DNS query lengths

Greg Farnham, “Detecting DNS Tunneling”, Feb. 25, 2013
https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152

DNS Analysis

Steps taken:

- Get the data
- Perform data munging
- Using R
  - Exploratory Data Analysis (EDA)
  - Dig into anomalies

DNS Analysis

The Data

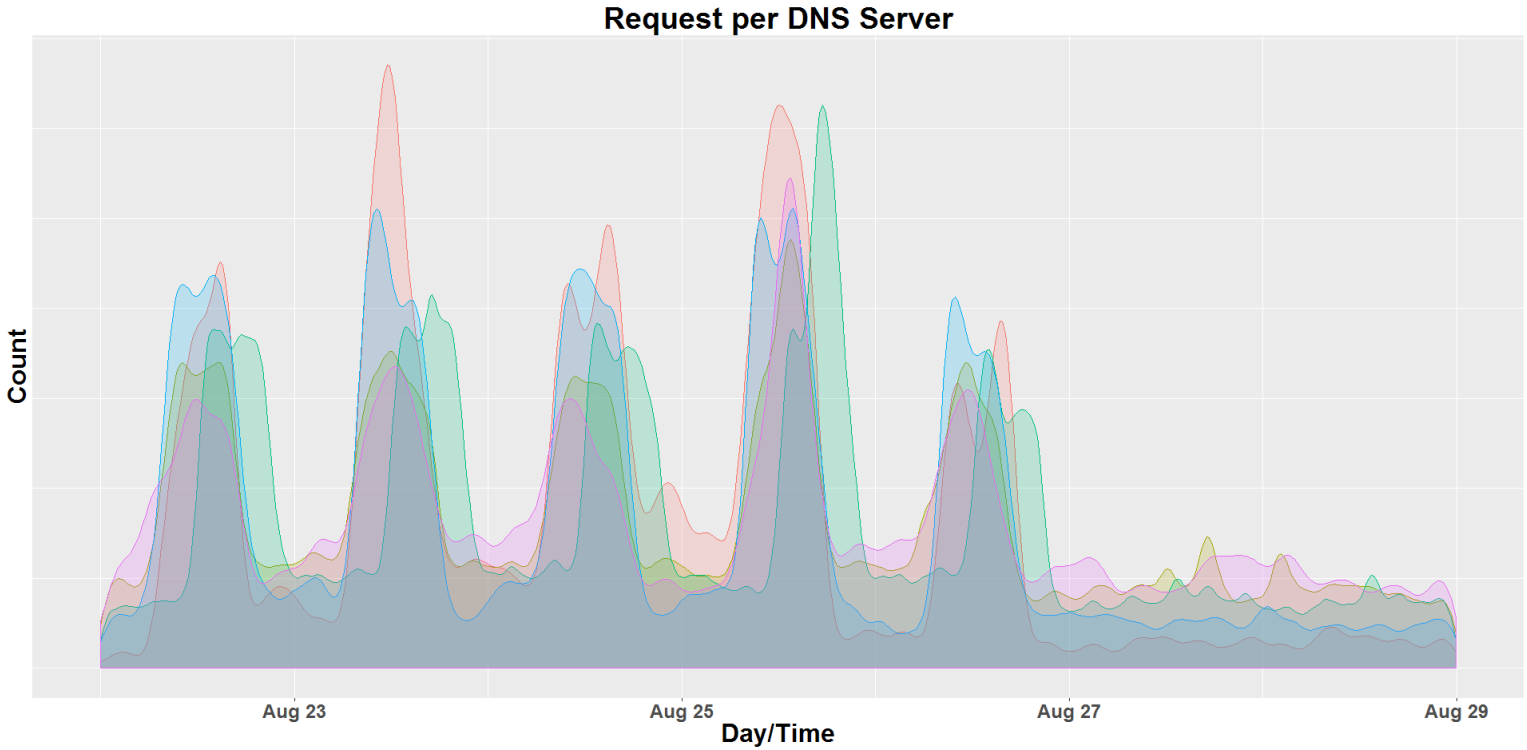
- Pulled from SIEM
- User subnets only
- 1MM+ records / 7 days
- Had consistent fields
- Created some new values
- Removed MISO domains

DNS Analysis

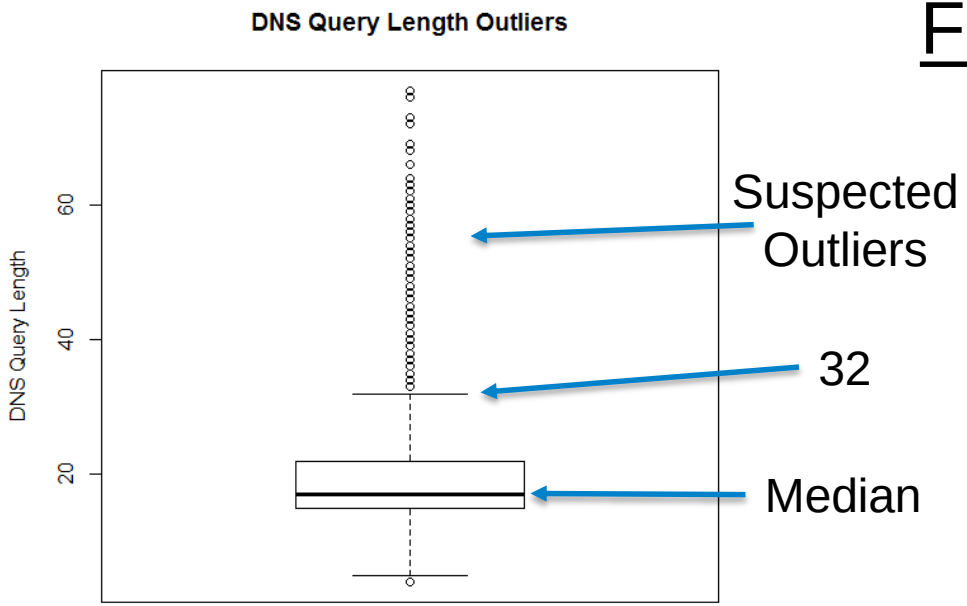
Data Structure

```
> str(no_miso)
Classes ‘data.table’ and 'data.frame':  304719 obs. of  7 variables:
 $ SourceIP     : chr  “XX.XX.XX.167" “XX.XX.XX.29" “XX.XX.XX.176”...
 $ DestinationIP: chr  “XX.XX.XX.40" “XX.XX.XX.40" “XX.XX.XX.40"...
 $ LastTime     : POSIXct, format: "2016-08-23 23:59:00" "2016-08-23...
 $ DNSQuery     : chr  "safebrowsing.google.com" "enroll.cisco.com" ...
 $ Domain       : chr  "google" "cisco" "microsoft" "overdrive" ...
 $ Suffix       : chr  "com" "com" "com" "com" ...
 $ DNSQLen      : int  23 16 17 58 15 16 17 24 16 14 ...
 - attr(*, ".internal.selfref")=<externalptr>
```

DNS Analysis



DNS Analysis



Focusing on length

- Long length suspect
- Multiple suspected outliers in data
- Key for us here is the number 32

DNS Analysis

8,715 total - 1,409 unique DNS Queries over 32

```
> unique(subset(no_miso, DNSQLen>32, select=c(DNSQuery, DNSQLen)))
                                                                    DNSQuery DNSQLen
   1: p2-nytq2ty2ssh5g-6ohe55ab7e4mi62m-220801-i2-bogus-dnssec-bd.gexperiments3.com      77
   2:  w2txo5aa-47149d468df87e00c8009c0a7b6d1decfa76c427-sac.d.aa.online-metrix.net      76
   3:  o7f2hmf6-49aa8aacca5dd493c21f35eb890b65aad138e62f-sac.d.aa.online-metrix.net      76
   4:  usllpic0-0c2b62d317ebd39248fb3f687199830e3ab4dc47-sac.d.aa.online-metrix.net      76
   5:  vmc1e5k7-a49b8c90bc5e8e311547fe8e07a10edc1bca5ce3-sac.d.aa.online-metrix.net      76
  ---
1405:                                                r17---sn-5uaeznez.googlevideo.com      33
1406:                                                r18---sn-ab5l6ne6.googlevideo.com      33
1407:                                                tve_static-snappytvpoc.nbcuni.com      33
1408:                                                r20---sn-5uaeznl7.googlevideo.com      33
1409:                                                r18---sn-vgqs7n7y.googlevideo.com      33
```

DNS Analysis

“Detecting DNS Tunneling” - Guy, J. suggests 52

```
> unique(subset(no_miso, DNSQLen>52, select=c(DNSQuery, DNSQLen)))
                                                                  DNSQuery DNSQLen
  1: p2-nytq2ty2ssh5g-6ohe55ab7e4mi62m-220801-i2-bogus-dnssec-bd.gexperiments3.com      77
  2:  w2txo5aa-47149d468df87e00c8009c0a7b6d1decfa76c427-sac.d.aa.online-metrix.net      76
  3:  o7f2hmf6-49aa8aacca5dd493c21f35eb890b65aad138e62f-sac.d.aa.online-metrix.net      76
  4:  usllpic0-0c2b62d317ebd39248fb3f687199830e3ab4dc47-sac.d.aa.online-metrix.net      76
  5:  vmc1e5k7-a49b8c90bc5e8e311547fe8e07a10edc1bca5ce3-sac.d.aa.online-metrix.net      76
 ---
555:                 a386e424f6261e8deacf6bc74ea602b4.clo.footprintdns.com      53
556:                 e8d814547dc0486dc29304a82989b41f.clo.footprintdns.com      53
557:                 a967efd7edaff2662973cf20bd9f7a58.clo.footprintdns.com      53
558:                 1c3df74af49bc3a4d2a07501f1836a25.clo.footprintdns.com      53
559:                 00910f1a812aeaf9db1a7c5ee9869d1d.clo.footprintdns.com      53
```

559

DNS Analysis

Exclude major companies and CDNs with many entries

```
> unique(subset(no_miso, select=c(DNSQuery, DNSQLen)))
                                                                    DNSQuery DNSQLen
1: p2-nytq2ty2ssh5g-6ohe55ab7e4mi62m-220801-i2-bogus-dnssec-bd.gexperiments3.com      77
2:     ifx-keyid-9c7df5a91c3d49bbe7378d4aba12ff8e78a2d75c.microsoftaik.azure.net      73
3:              snow-ress-l2bf3pfj1ift.mq84pu3qhz.us-east-1.elasticbeanstalk.com      64
4:               apimgmthsomxbrr21hkiiznhyym02x1a3hk8damjvs1fnvkhua.cloudapp.net      63
5:                  spc--cefdcgbhjdcgdemgcebejglg--imp.telemetryverification.net      60
6:                       spc--cekhpgdfffidgdjflecgfdbe.telemetryverification.net      55
7:                       spc--cecgjhcdihgdgehhbdcgiebe.telemetryverification.net      55
```

DNS Analysis

A little bit of digging with Google's help…

Domain	Description
`gexperiments3.com`	Part of Google, possibly DNSSEC testing
`microsoftaik.azure.net`	Microsoft Attestation Identity Key – Windows 10
`elasticbeanstalk.com`	AWS Elastic Beanstalk orchestration service
`cloudapp.net`	Part of URI for Microsoft Azure applications
`telemetryverification.net`	Tracks "click through" for video ads

DNS Analysis

Result

- All long queries appear fine

Possible next steps

- Collect more data and repeat
- Try another method within:
  - Payload Analysis or Traffic Analysis

DNS Analysis

Lessons Learned:

- Windows 10 in testing
- Increased familiarity with MISO DNS
- Lots of good DNS data
- Difficult to retrieve data
- Were not raw logs – TTL missing

In Conclusion

- Three examples, all provided value to MISO
- Malicious activity detected with same analysis
- We are not experts
- First success above HMM0 will solidify executive management’s understanding

In Conclusion

Overall Lessons Learned

- Management Support – time in thirds
  - Learning | Applying | Projects
- Create a culture of trust
- Data availability
- Leverage existing BI coworkers
- Practice Incident Response
- Prepare for more incidents

Questions?

Twitter: @JamieBuening

Email: jbuening@misoenergy.org

LinkedIn: https://www.linkedin.com/in/jbuening/

Image Credits

- Lawyer - https://clipartfox.com
- Alert - https://clipartfest.com
- Signature - http://www.clipartbest.com
- Hackerman - http://knowyourmeme.com/memes/hackerman
- Question Mark - https://commons.wikimedia.org/wiki/File:Question_dropshade.svg
- Notepad - https://commons.wikimedia.org/wiki/File:Notepad_icon.svg
- Magnifying Glass - http://clipart.me/objects/magnifying-glass-clip-art-41547
- Ransomware - http://www.ransomizer.com
- Idea Bulb - http://www.clipartpanda.com/clipart_images/we-re-full-of-ideas-44874507
- Checkmark - https://commons.wikimedia.org/wiki/File:Checkmark_green.svg