

IOCs are Dead - Long Live IOCs!

COUNTERMEASURE 2016

Ryan Kazanciyan, Chief Security Architect



whoami



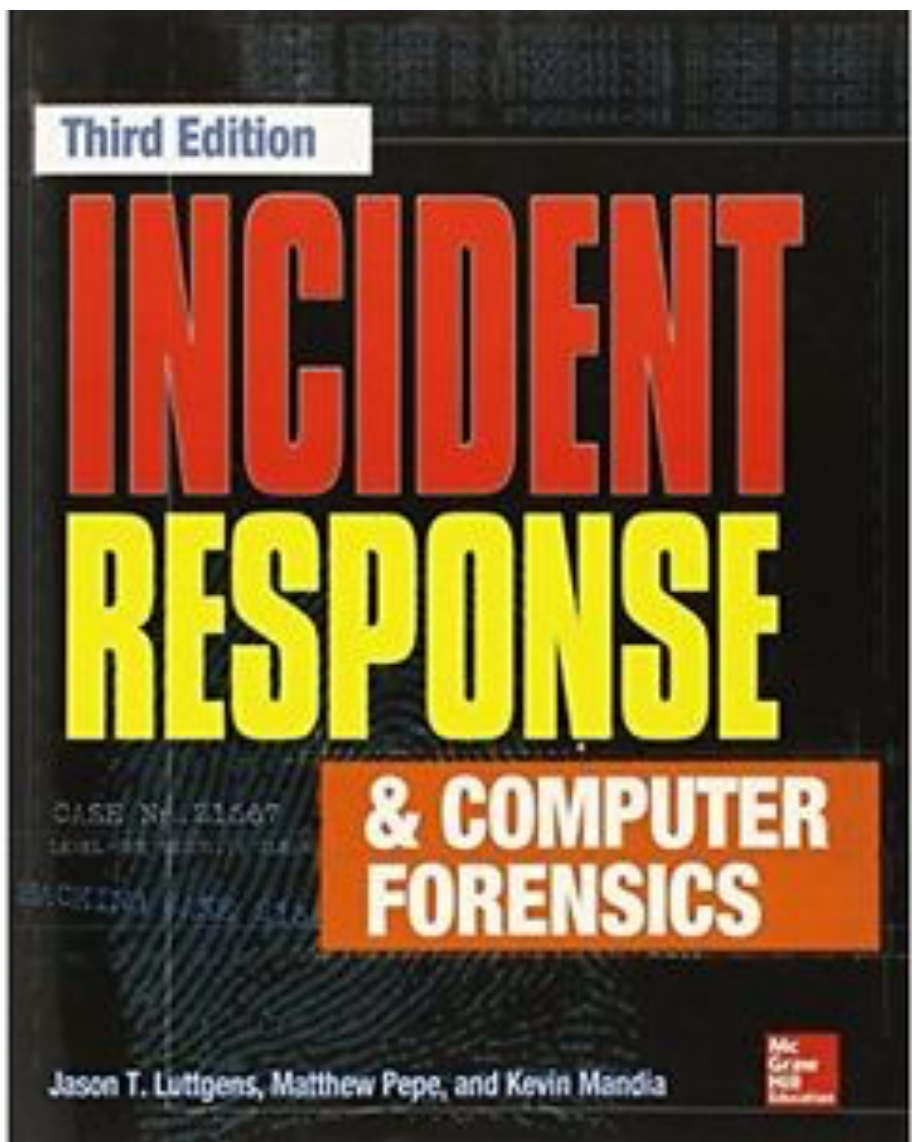
2004 - 2009



2009 - 2015



2015 - Present



Contributing
Author (2014)

Technical Consultant



Stuff I said in 2010

Before OpenIOC

- Lists of stuff to find evil
 - Easy to create
 - Difficult to maintain
 - Terrible to share
- Lists do not provide context
 - An MD5 of what?
 - Who gave me this?
 - Where is the report?
 - Where is the intelligence??
- **Lists encourage reliance on easily mutable forensic artifacts**



IOC allows this...

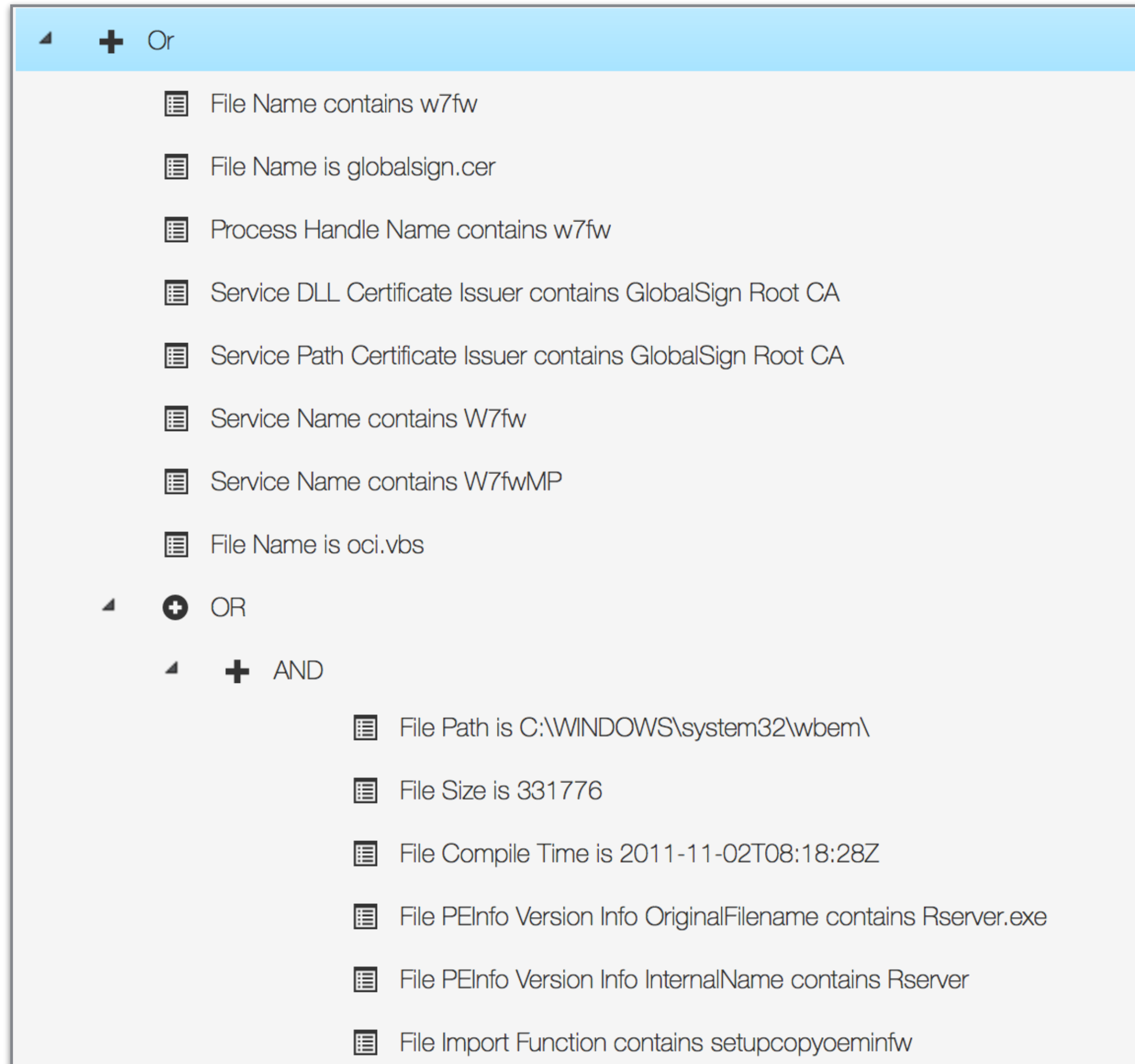
```
File Name is sunjrel6.exe
File Name is eic16ux.sys
File Name is e216ee.msi
File Name is webserv32.exe
File Name is 60927ux.sys
File Name is b26092.msi
File Name is uddi16.exe
File Name is aic16ux.sys
File Name is b216ee.msi
File MD5 is 5611458A5A03998CB1268190E2818C63
File MD5 is 711F4FE93EA0E8F253FA0643E273FE8B
File MD5 is 4BFB1ACBB32348E3D4572CD88B9A6FC
File MD5 is CB8990122D2675990C874B4959306793
File MD5 is 8B911B2D548FF26AE6C236D3DA2DDF2C
File MD5 is 402366D37A54CCA71238A0FC771DEE30
File MD5 is 98A9DF9AC85A1755CB3EBE1d4AEA5498
File Name is cmdm1g64.exe
File Name is ai31ux.sys
File Name is b30ee.msi
File Name is smscfg32.exe
File Name is a0c77ux.sys
File Name is b087ee.msi
File MD5 is 1954EB413FDADE614031B2231E35C7B
File Name contains \Application Data\Microsoft\Media Player\DefaultStore32.exe
File Name contains \Application Data\Microsoft\Media Index\wmplibrary32.db
File Name contains \Favorites\janny.jpg
Process Handle Name is www.TW0901.2.org
Process Handle Name is www.UG0902.2.org
Process Handle Name is www.UG0905.1.org
Process Handle Name is 1.2.UD0804.1z
Process Handle Name is www.WW0902.1.org
```

...to become this

Name: STISVC.DLL	Type	Reference
Author: ryan.kazanciyan@mandiant.com	group	MFR00-0001
GUID: 116fc8d2-41b8-4cfc-8590-978d2414:	report	MA12345
	category	Backdoor
	grade	Release
Description: This malware is a backdoor trojan that gets loaded as a Windows Service. It initiates command and control via an SSL encrypted HTTPS session to a hard-coded C2 address. The backdoor features include remote file transfer, command execution, and screen capture		
Add:	Definition:	
Item	OR	
AND	Process Handle Name contains PccGlobalExitEvent	
OR	Network DNS contains evilsite.com	
	File Name is backins.exe	
	File Name is stisv.dll	
	File MD5 is e996c7ff1709e801376515c1757efe7	
	File MD5 is 44e03e0146729b6720ecc9d2f2964865	
	AND	
	File Import Function is CmdBatNotification	
	File Import Function is FlushConsoleInputBuffer	
	File Size is [99000] TO [125000]	
	File Import Name is wininet.dll	
	File Import Name contains urlmon.dll	
	File Import Name contains changeserviceconfig2a	
	AND	
	Service Name contains StiSvc	

<https://buildsecurityin.us-cert.gov/sites/default/files/RyanKazanciyan-APTPanel.pdf>

IOCs as advertised



- Human-readable, machine-consumable
- Capture a broad set of forensic artifacts
- Foster information sharing
- Provide context around threats
- Do better than “signatures”

Six years later...



IOC quality and sharing in 2016

Indicators of Compromise (IOCs)		
IOC	Type	Notes
91.207.61.208	Destination IP address	Command and control server
109.72.149.42	Destination IP address	Command and control server
130.0.237.22	Destination IP address	Command and control server
5.187.1.198	Destination IP address	Command and control server
ABA833D11679DFEBC95060BD3C557853	File MD5 hash	Malicious driver file
215BDF185C3B35503923FCF8872C75FC	File MD5 hash	Malicious driver file
F9C4E2D38DF8A87F545B6F5BA1F8691B	File MD5 hash	Malicious driver file
F21403B6CF7516B37EFFC17F410CED6F	File MD5 hash	Malicious driver file
6FBD31E7B5A31F5F75BD0D858D3327B5	File MD5 hash	Malicious driver file
68F40544ACD5568BD782434CA0F5AEE5	File MD5 hash	Malicious driver file
540DF6480B393BFA39D2E7CEC608EA12	File MD5 hash	Malicious driver file
%SystemRoot%\system32\drivers	Install path	Malicious driver file

usbf4.exe	e36680a19601f84af6d311e1fb847eef	Detected as Trojan STRPADT.A and pat2.exe
vvb.exe	2a38ff709549b97b4e42b6fae81c6177	Modifies the a
vvb.sfx.exe	f747d5f998e48279cad7e9ed46e86a6b	Drops VVB.exe

Indicators of Compromise	
Show	10 entries
TYPE	INDICATOR
domain	xxxmobiletubez.com
FileHash-SHA256	7b7eeca21a4aee3768b41b9e194052cbb01835ae3b3503c1d635abbe1
FileHash-SHA256	e6c1621158d37d10899018db253bf7e51113d47d5188fc363c6b5c51a6
FileHash-SHA256	f5bc281ee071f6fb0eb8d25f414770fee67e2ea6e02afe53896a2313f6cfe
IPv4	89.144.14.29
IPv4	185.86.148.188
IPv4	195.3.144.90
IPv4	89.144.14.59
IPv4	5.39.222.162
URL	http://185.86.148.188:2080/forms/

Name	FireEye
Description	This IOC contains indicators detailed in the blog post "Operation Double Tap"
Or	
File MD5 is	5a0c4e1925c76a959ab0588f683ab437
File MD5 is	492a839a3bf9c61b7065589a18c5aa8d
File MD5 is	744a17a3bc6dbd535f568ef1e87d8b9a
File MD5 is	5c08957f05377004376e6a622406f9aa
File MD5 is	8849538ef1c3471640230605c2623c67
DNS Record Name contains	join.playboysplus.com
DNS Record Name contains	inform.bedircati.com
DNS Record Name contains	pn.lamb-site.com
DNS Record Name contains	securitywap.com
DNS Record Name contains	walterclean.com
Port Remote IP contains	192.157.198.103

My evolving point of reference

2009 - 2015: Investigator

- Large-scale, targeted attacks
- Designed, tested, and applied IOCs for proactive and reactive hunting

2015 - Present: Builder

- Designing an EDR platform that includes IOC detection
- Helping orgs build self-sustaining, scalable “hunting” capabilities

The erosion of indicator-based detection

Brittle indicators - short shelf-life

Poor quality control in threat data feeds

Hard to build effective homegrown IOCs

Indicator detection tools are inconsistent

IOCs applied to limited scope of data

IOCs are brittle



“IOCs” vs. “threat data” vs. “intelligence”

- IOCs are structured **threat data**
- **Threat data != threat intelligence**
- Threat intelligence provides context and analysis
- Threat intelligence is ineffective without quality threat data

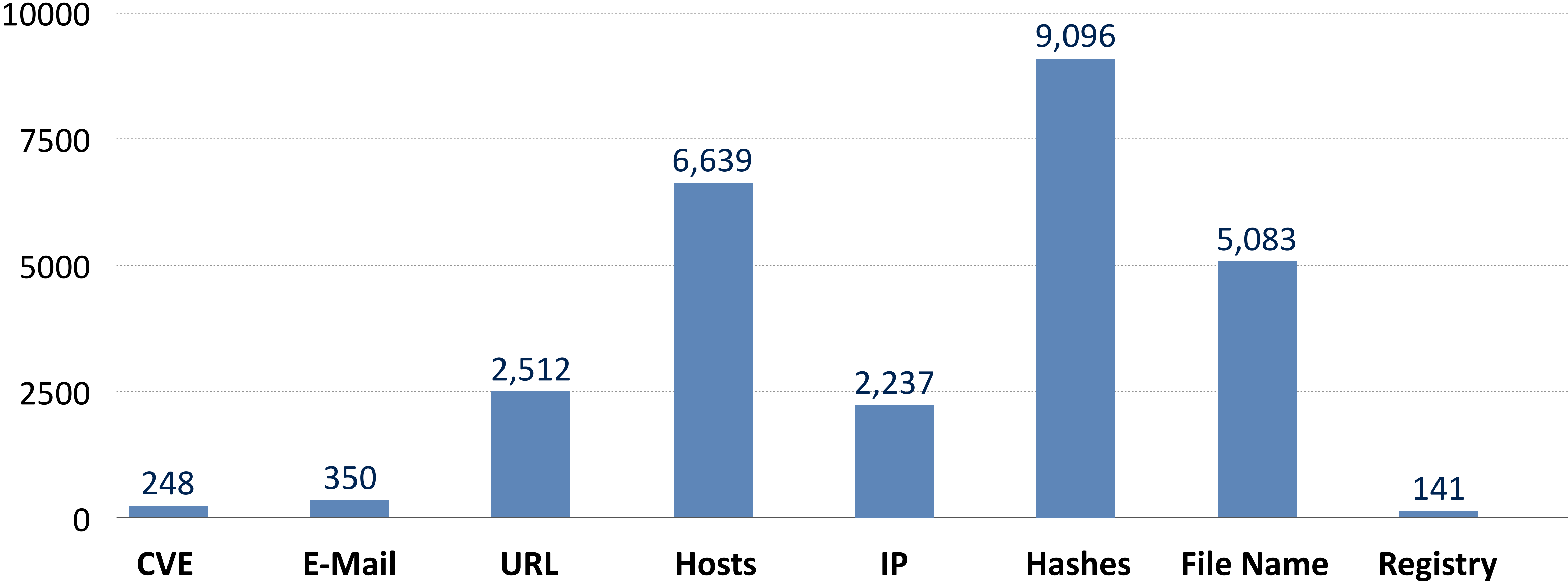
Verizon DBIR 2015: Most shared IOC types

COMMUNITY	IP ADDRESSES	E-MAIL ADDRESSES	FILES	HOSTS	URLS
Common Community	35.9%	1.0%	23.3%	33.0%	6.8%
Event-Based Community #1	77.4%	0.1%	2.5%	19.5%	0.5%
Industry Community #1	16.5%	32.3%	6.3%	43.0%	1.9%
Industry Community #2	47.1%	4.4%	10.3%	29.4%	8.8%
Industry Community #3	8.3%	0.3%	1.2%	87.5%	2.7%
Industry Community #4	25.2%	2.4%	9.0%	58.6%	4.8%
Industry Community #5	50.9%	0.7%	1.3%	22.8%	24.4%
Industry Community #6	66.4%	0.6%	14.0%	13.8%	5.2%
Industry Community #7	59.1%	0.5%	1.4%	23.5%	15.5%
Industry Community #8	39.6%	3.0%	7.7%	36.9%	12.8%
Industry Community #9	51.5%	2.6%	12.6%	23.8%	9.5%
Regional Threat Community #1	49.2%	0.3%	4.5%	42.6%	3.4%
Regional Threat Community #2	50.0%	1.1%	4.5%	30.8%	13.6%
Subscriber Community	45.4%	1.2%	18.4%	24.4%	10.6%
Threat-Based Community #1	50.3%	1.1%	11.0%	24.3%	13.3%

Source: Verizon DBIR 2015

IOCs in the APTnotes data set

Derived from over 350 threat reports (2006 - 2016) archived on <https://github.com/kbandla/APTnotes>



Sheer volume does not solve the problem

- 2007: Bit9 FileAdvisor tracked **4 billion unique files**, catalog grew by 50 million entries per day
- 2009: McAfee Global Threat Intelligence tracked reputation data for **140 million IP addresses**, handling **50 million file lookups** per day
- 2011: Symantec Insight tracked **tens of billions** of linkages between users, files, web sites

Seven years of progress?

“...innovating to provide **predictive security**.

This approach comprises interconnected security technology at multiple layers in the technology stack, backed by **global threat intelligence**. Predictive security will allow security products to **intelligently block attacks much sooner than is currently possible...**”

“...an **intelligence-led approach** to security will be key in detecting the most sophisticated threats and **responding** to them **quickly** and **effectively**.”

**Paid IOCs !=
effective IOCs**



Have you assessed your feeds?



- 74% of enterprise cybersecurity professionals say that it is extremely difficult or somewhat difficult to determine the quality and efficacy of each individual threat intelligence feed.

Jon Oltsik / ESG, <http://www.networkworld.com/article/2951542/cisco-subnet/measuring-the-quality-of-commercial-threat-intelligence.html>

My (not-so-scientific) methodology

- Chose two top-tier paid threat feed services
- Retrieved the most recent ~20 indicators from each
- Spent 15 minutes eyeballing their contents

What are you paying for?

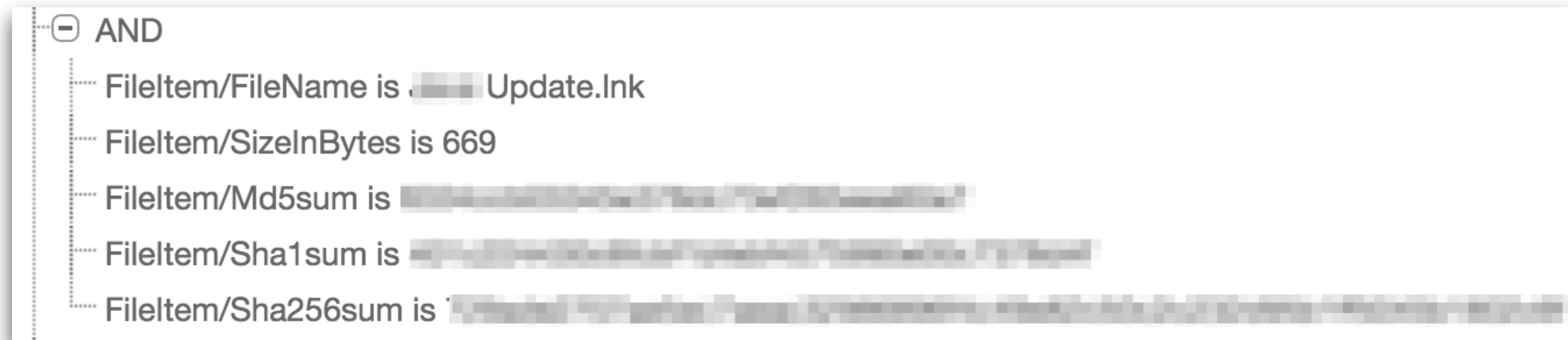
Too specific - malware hash AND'd with a filename



(Real IOC from a commercial feed)

What are you paying for?

Too specific - LNK files are unique per-system



(Real IOC from a commercial feed)

What are you paying for?

Too noisy - matches component of legitimate software

AND

- FileItem/FileName is win32ui.pyd
- FileItem/SizeInBytes is 778752
- FileItem/Md5sum is 9a218123b0474cc1f0f13432f21ec973
- FileItem/Sha1sum is 6688b860c267c84605081719bb888fa87634ef9f
- FileItem/Sha256sum is ecf37713a38e5eb5a32e872249a3018eda2a8ead91c73b01edba762385e3716e

AND

- FileItem/FileName is _socket.pyd
- FileItem/SizeInBytes is 46080
- FileItem/Md5sum is 0a75385123d11bb9a3231155b6fa35e1
- FileItem/Sha1sum is 6688b860c267c84605081719bb888fa87634ef9f
- FileItem/Sha256sum is ecf37713a38e5eb5a32e872249a3018eda2a8ead91c73b01edba762385e3716e

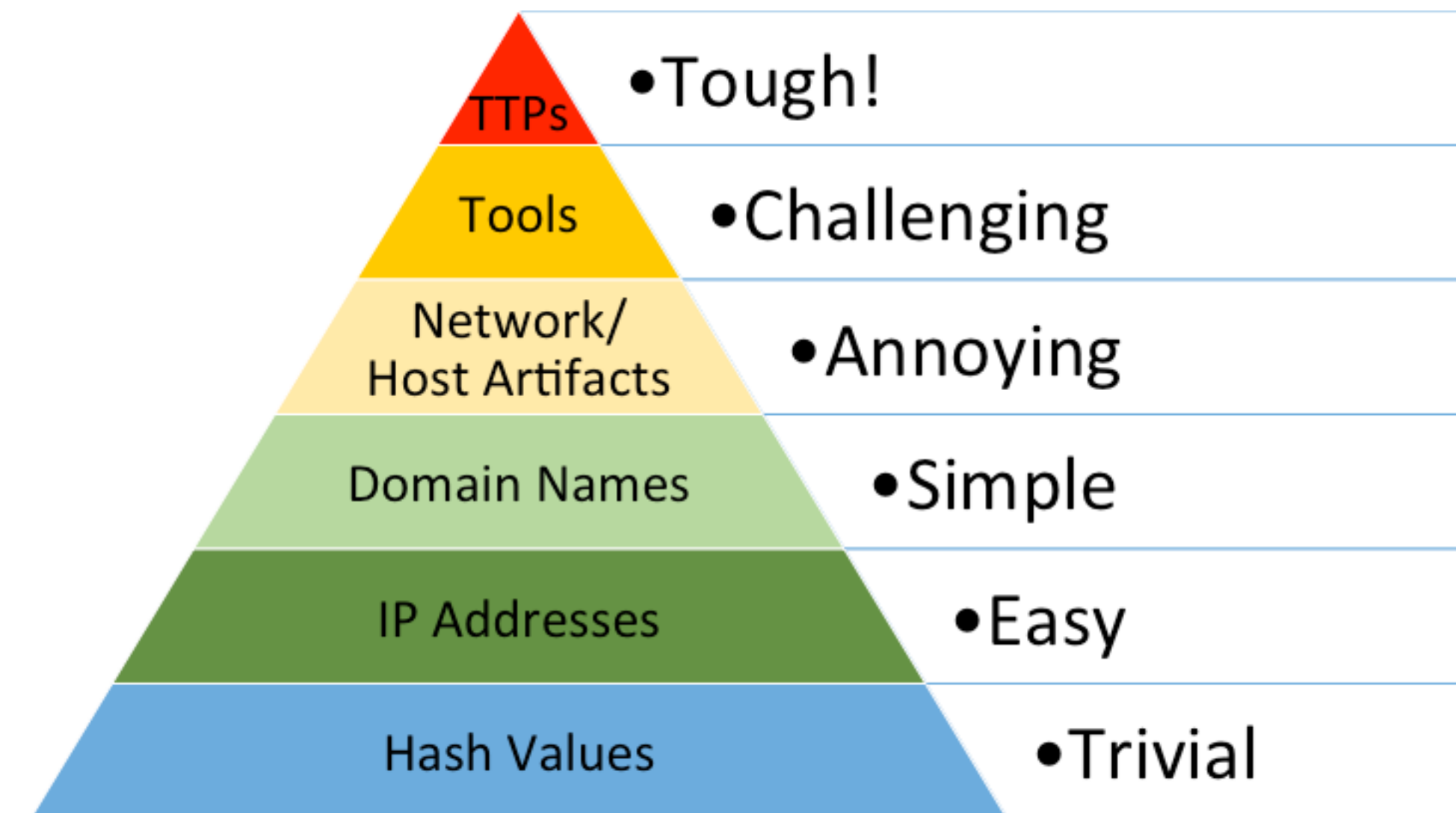
(Real IOC from a commercial feed)

**Building good IOCs
is difficult**



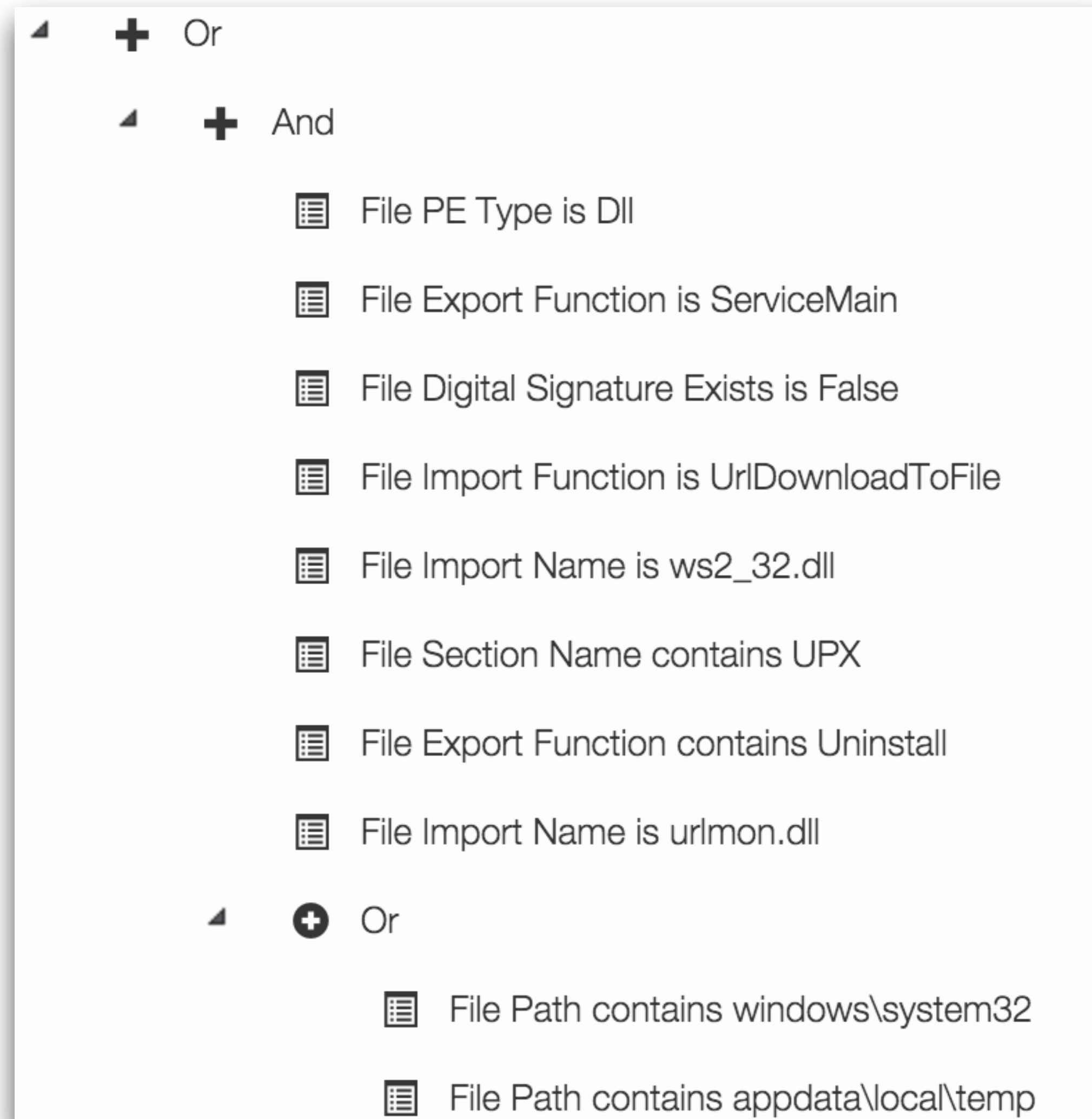
Challenges with IOC development

- Easy to build high-fidelity IOCs
 - (may yield high false-negatives)
- Hard to build robust IOCs
 - (may yield higher false-positives)
- Easy to build IOCs that don't evaluate properly
 - (tools have inconsistent matching logic)



“Pyramid of Pain”, David Bianco
<http://detect-respond.blogspot.co.uk/2013/03/the-pyramid-of-pain.html>

Running aground on a robust IOC



Too broad - may match on uncommon but legitimate binaries

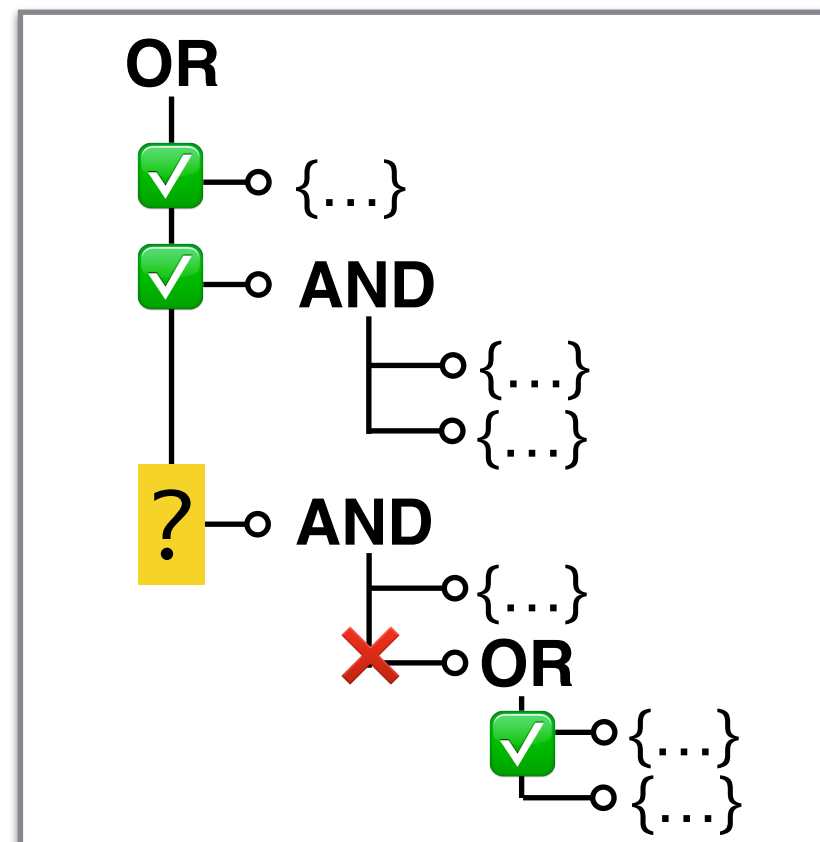
How much time do your analysts have to continuously build, test, and refine IOCs like this?

Inconsistencies in IOC detection tools

Supported Observables

FileItem	✓
EventLogItem	✗
TaskItem	✗
ServiceItem	✓
...	?

Logic Handling



Data Normalization

x86 or x64?	→	\system32\ \SysWoW64\ \WoW6432Node\
HKEY_CURRENT_USER	→	HKEY_USERS\{SID}
%SYSTEMROOT%	→	\Windows\

- STIX & CybOX have a few tools to help with this:
 - maec-to-stix
 - python-cybox/normalize.py

Issues specific to OpenIOC

What happens when you try to turn a proprietary tool's unique output schema into a "standard"...

`ProcessItem/PortList/PortItem/process`

"Process Port Process"

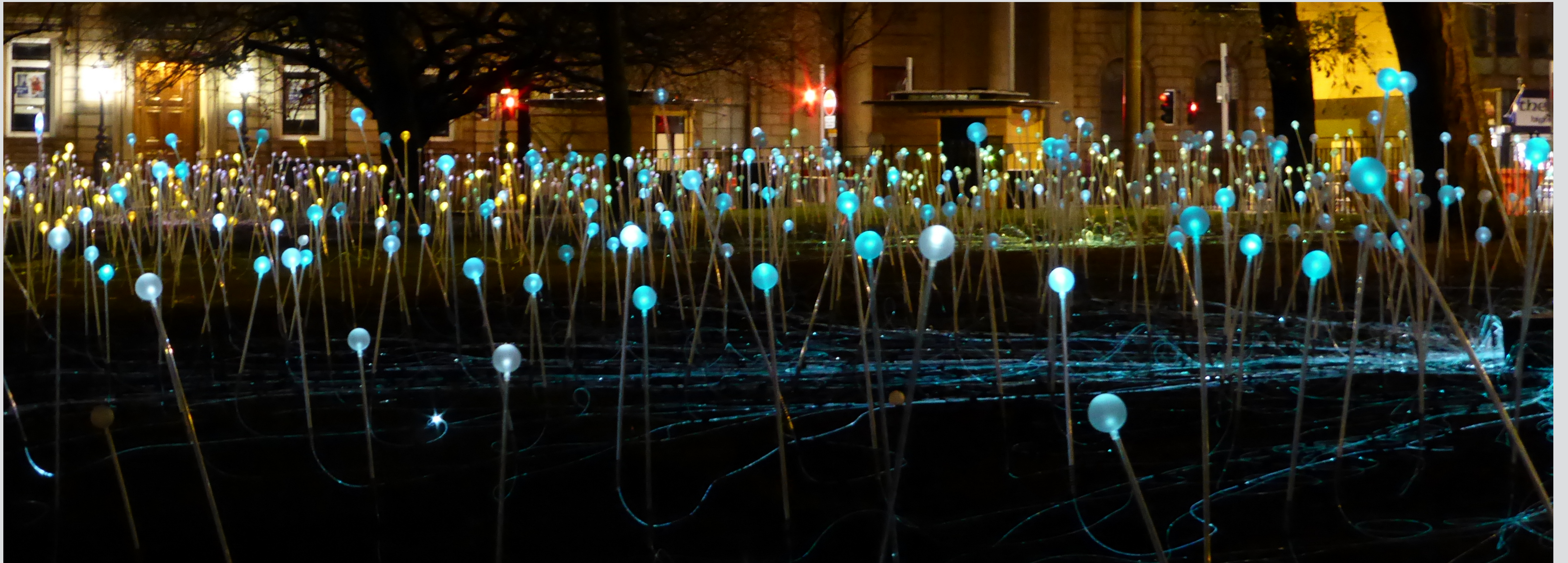
`FileItem/PEInfo/DetectedAnomalies/string`

"File PE Detected Anomalies"

`FileItem/PEInfo/DetectedEntryPointSignature/Name`

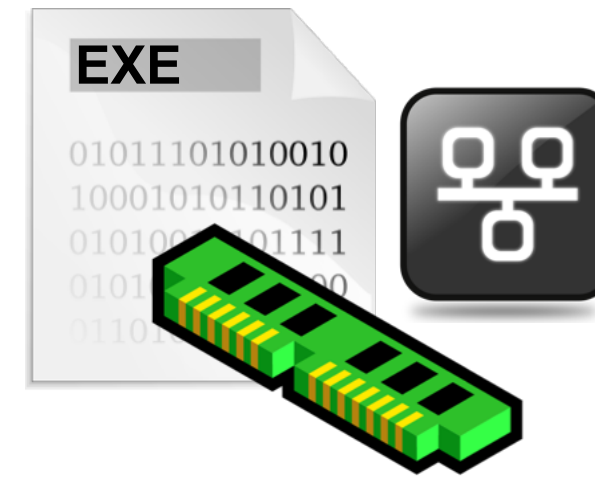
"File EntryPoint Sig Name"

Widening the scope of endpoint indicator usage



What can you see?

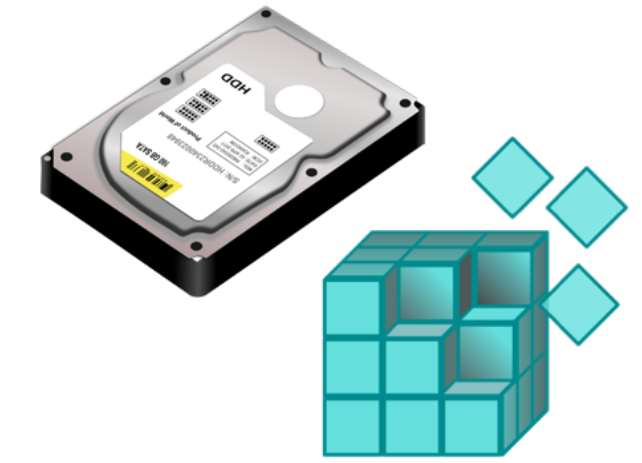
- What are you matching your endpoint IOCs against?
- What's your cadence of detection?
- Where are your gaps?
- What requires data lakes?



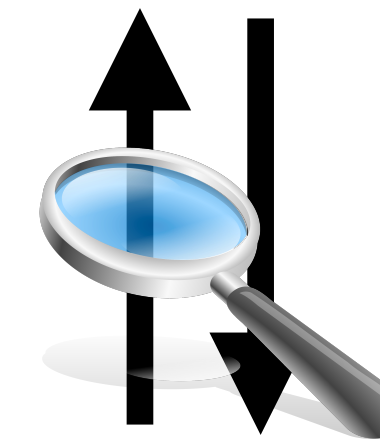
Current Activity
(Processes, Network Connections, Memory)



Historical Activity
(Telemetry, logs, alerts, historical data)



Data at Rest
(Files on disk, registry)



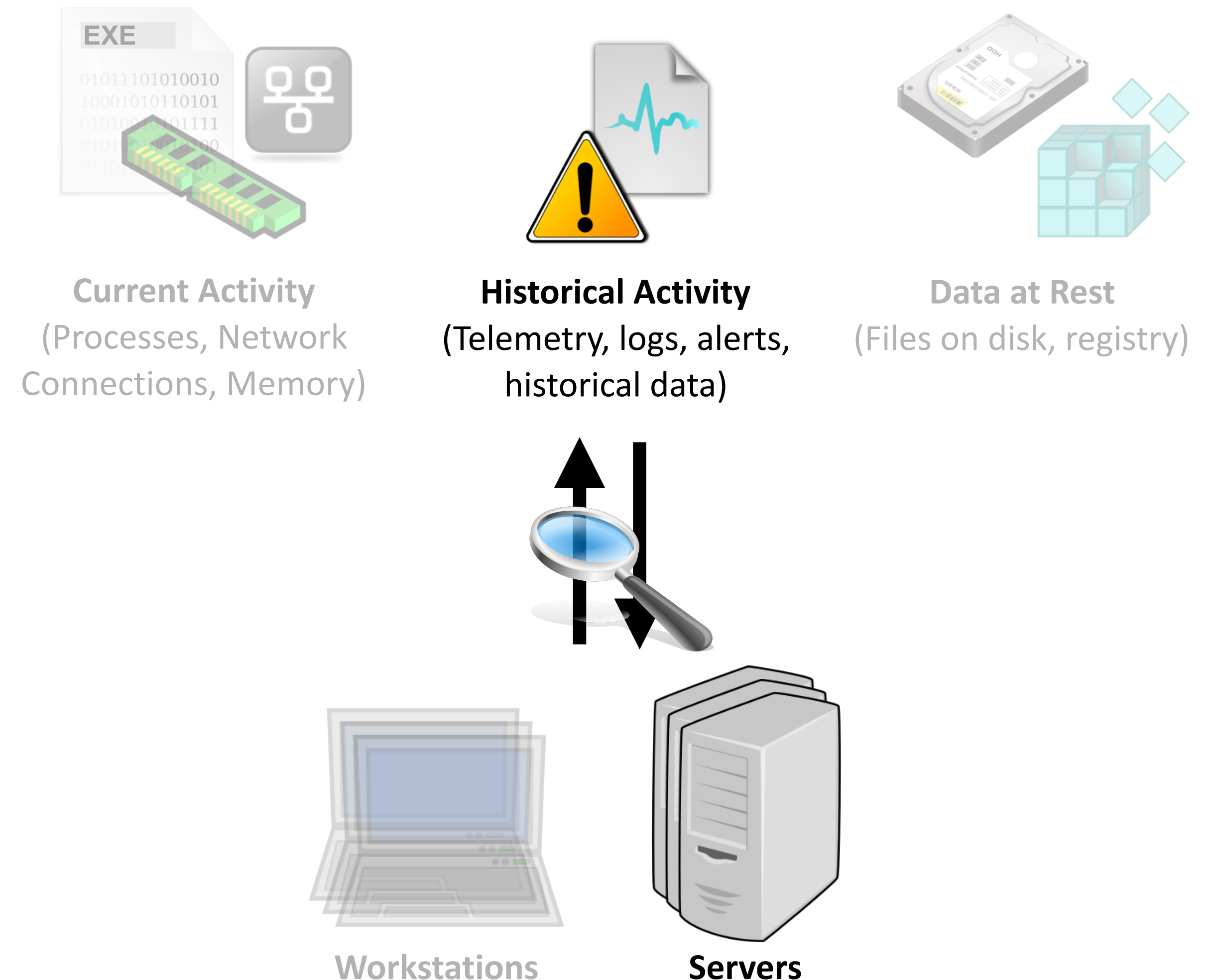
Workstations



Servers

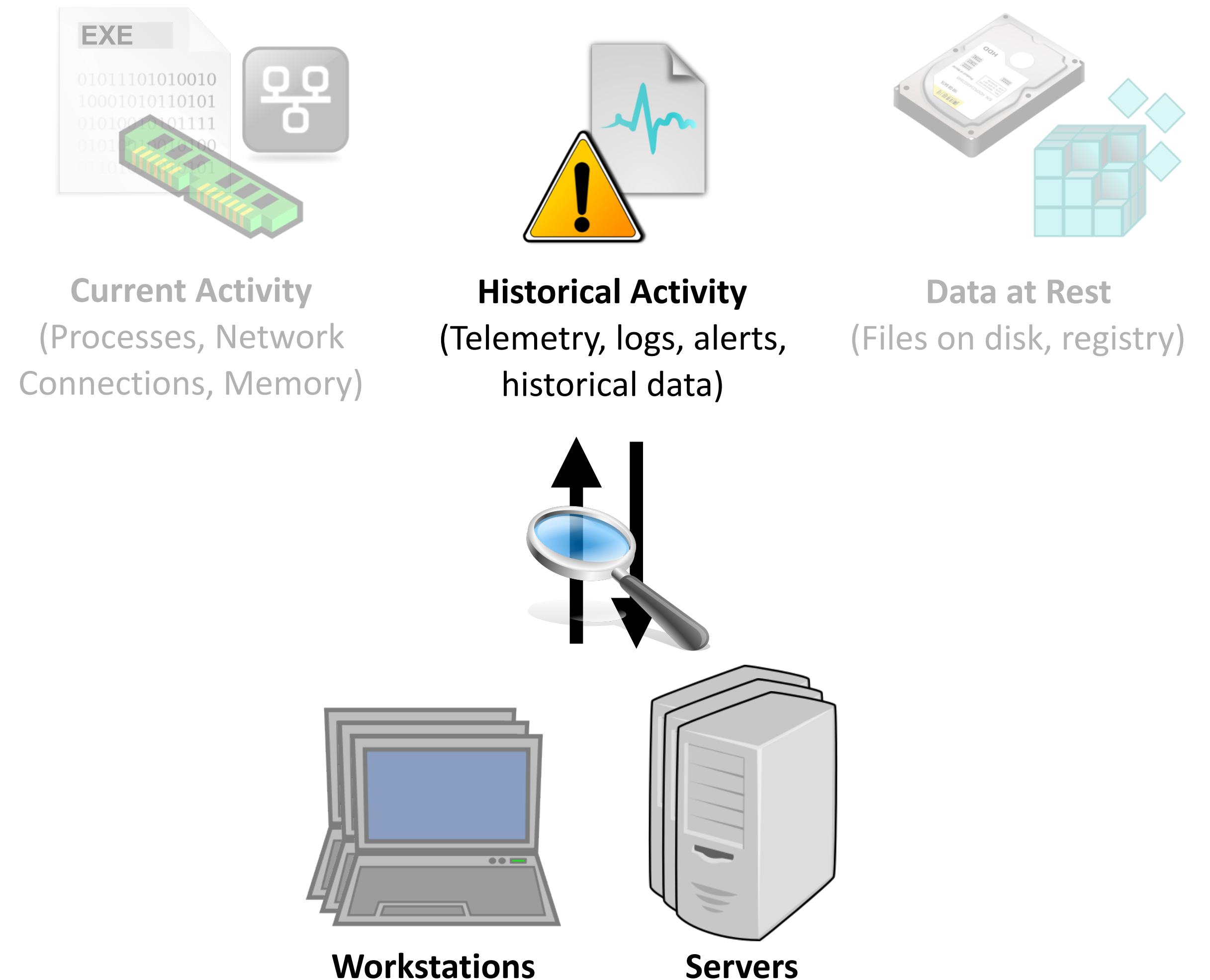
Matching on SIEM / centralized logging

- Most common endpoint data in SIEM:
 - Anti-virus / anti-malware alerts (all systems)
 - Event log data (subset of systems - usually servers)
- **Resource impact** of large-scale event forwarding & storage **limits endpoint coverage & scope of data**



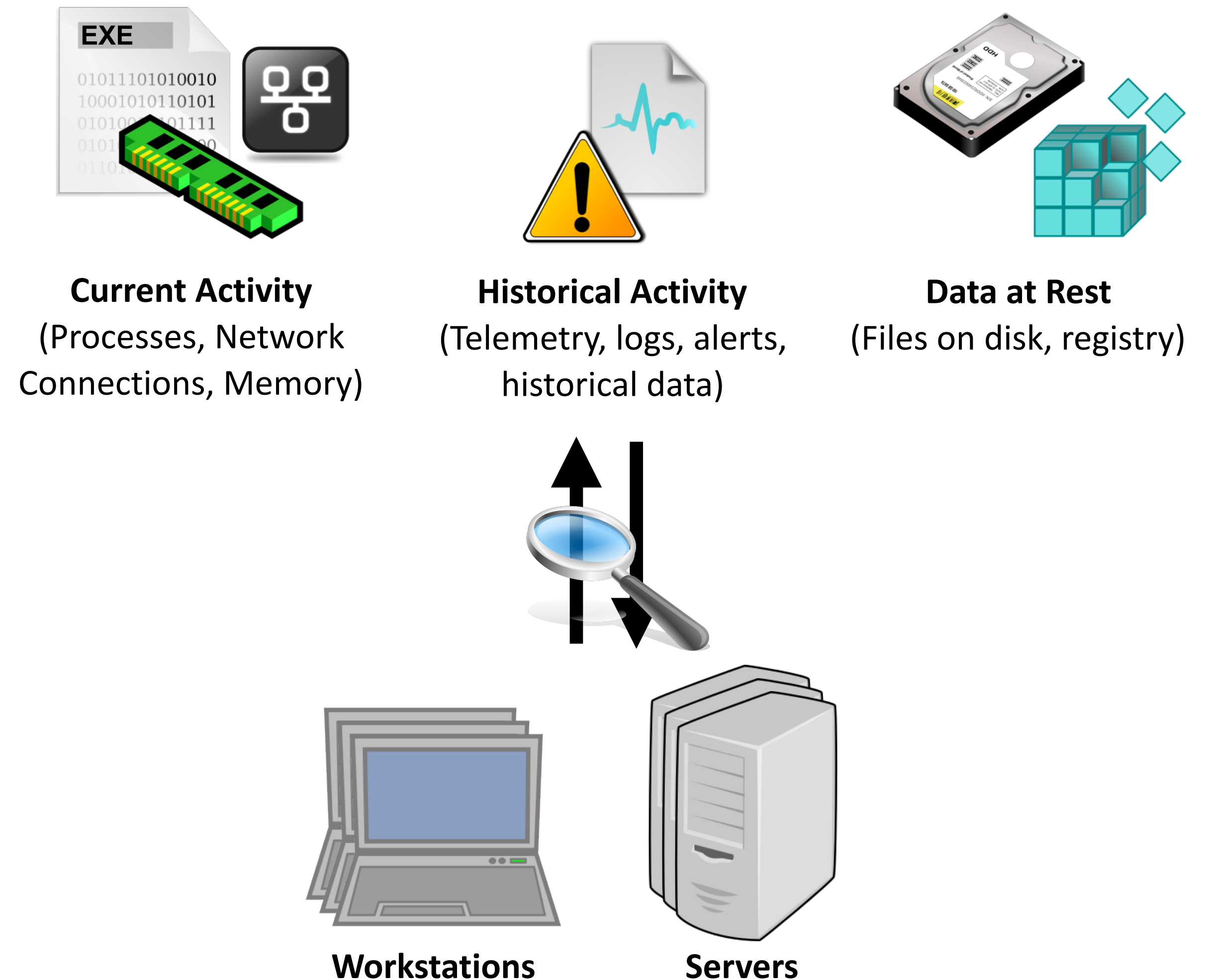
Matching on forensic telemetry

- Process execution, file events, network connections, registry changes
- Preserves historical data, short-lived events
- Expensive to centralize in large environments
- **Limited scope of data for IOC matching**



Matching on live endpoints

- Potentially the broadest set of available data
- Considerations
 - Endpoint impact
 - Availability
 - Time-to-assess
 - Scalability



Shrinking the detection gap



Doing better with what we've got

"The desire to take a technical feed and simply dump it into our security infrastructure doesn't equate to a threat intelligence win...

You cannot get more relevant threat intelligence than what you develop from within your own environment. This should then be enriched with external intelligence"

-Rick Holland, Forrester, 2016 CTI Summit

Source:

<https://www.digitalshadows.com/blog-and-research/another-sans-cyber-threat-intelligence-summit-is-in-the-books/>

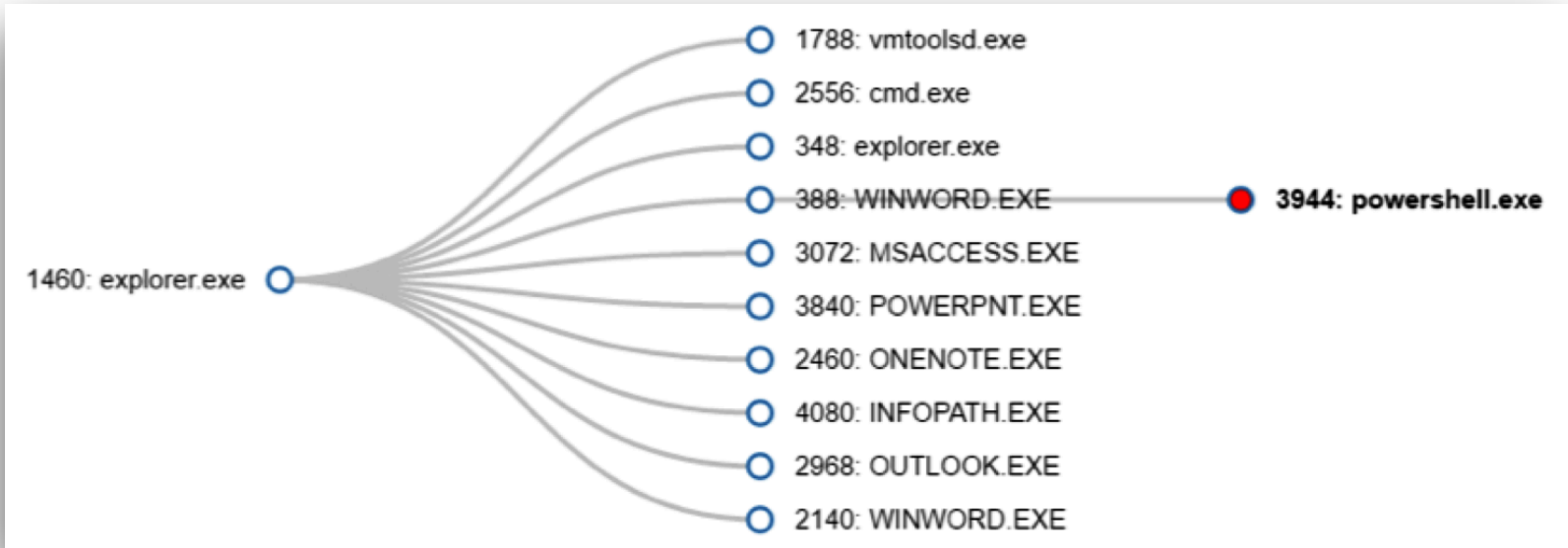
Do you know the basics in your network?

- Privileged account usage
- Use of OS-native tools commonly abused by attackers
- Persistence mechanisms

Employing a blended approach

Indicators of Compromise (IOCs)		
IOC	Type	Notes
91.207.61.208	Destination IP address	Command and control server
109.72.149.42	Destination IP address	Command and control server
130.0.237.22	Destination IP address	Command and control server
5.187.1.198	Destination IP address	Command and control server
ABA833D11679DFEBC95060BD3C557853	File MD5 hash	Malicious driver file
215BDF185C3B35503923FCF8872C75FC	File MD5 hash	Malicious driver file
F9C4E2D38DF8A87F545B6F5BA1F8691B	File MD5 hash	Malicious driver file
F21403B6CF7516B37EFFC17F410CED6F	File MD5 hash	Malicious driver file
6FBD31E7B5A31F5F75BD0D858D3327B5	File MD5 hash	Malicious driver file
68F40544ACD5568BD782434CA0F5AEE5	File MD5 hash	Malicious backdoor file
540DF6480B393BFA39D2E7CEC608EA12	File MD5 hash	Password harvesting file
%SystemRoot%\system32\drivers	Install path	Malware install path

IOCs and reputation data
for noise reduction and
context



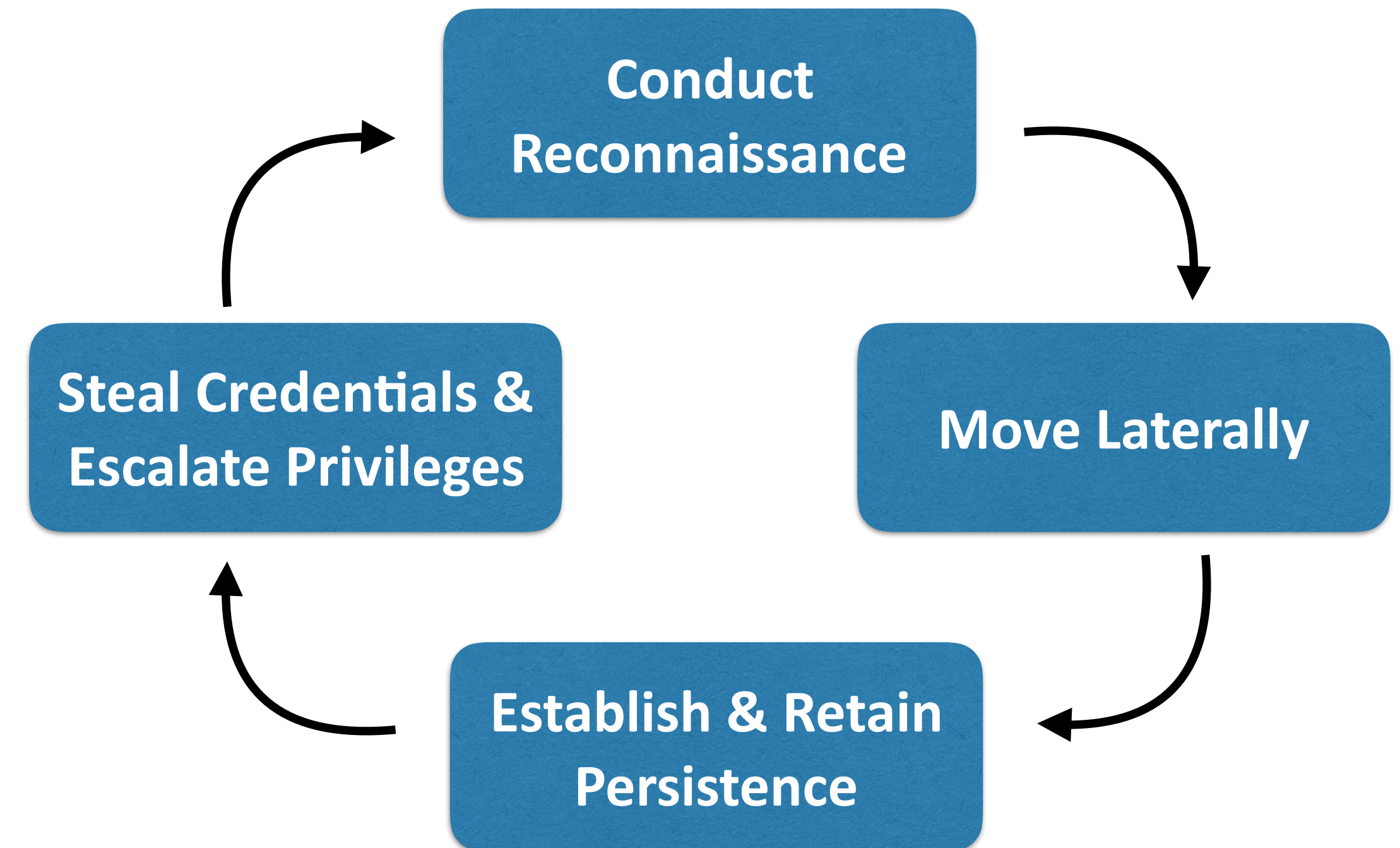
Pattern of attack
detection for common
intrusion workflows



Anomaly analysis tailored
to discrete system and
user groups

Focusing on patterns of attack

- What are the “**lowest common denominators**” across intrusions?
- What evidence do they leave behind?
- What easily-observable outlier conditions do they create?



MITRE's ATT^CK Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Applnit DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol

https://attack.mitre.org/wiki/Technique_Matrix

Example: Detecting host-to-host command execution

Attacker Methods



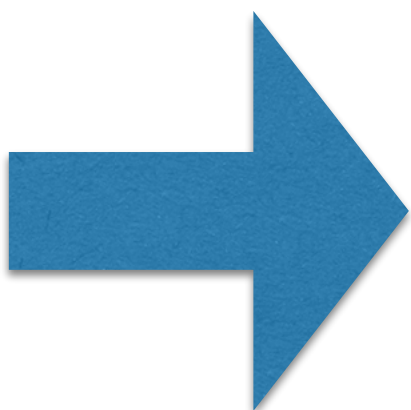
Scheduled
Tasks



WinRM &
PowerShell



PsExec



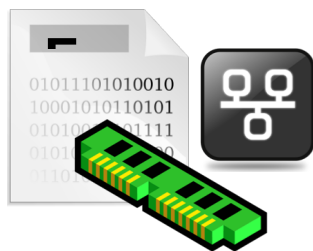
Sources of Evidence



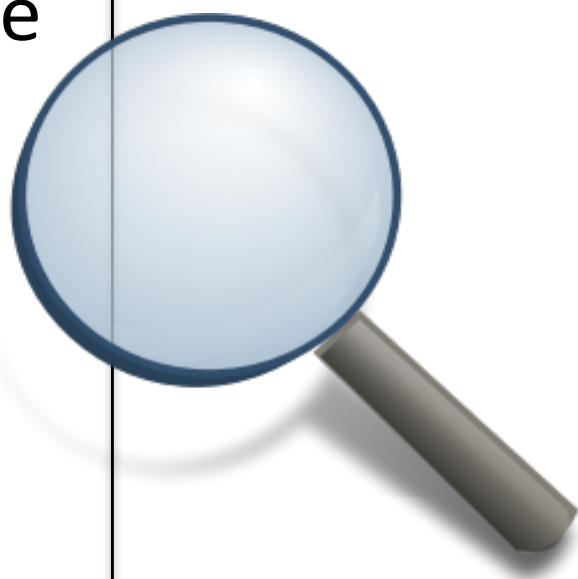
Logon & service
events



Process
history



Other forensic
artifacts



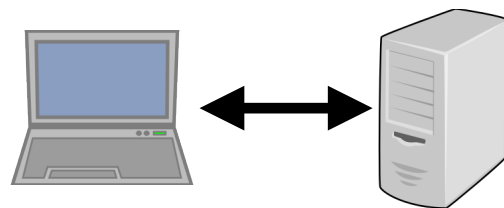
Analysis Criteria

Who?



Accounts used

Where?



Source & target
systems

When?

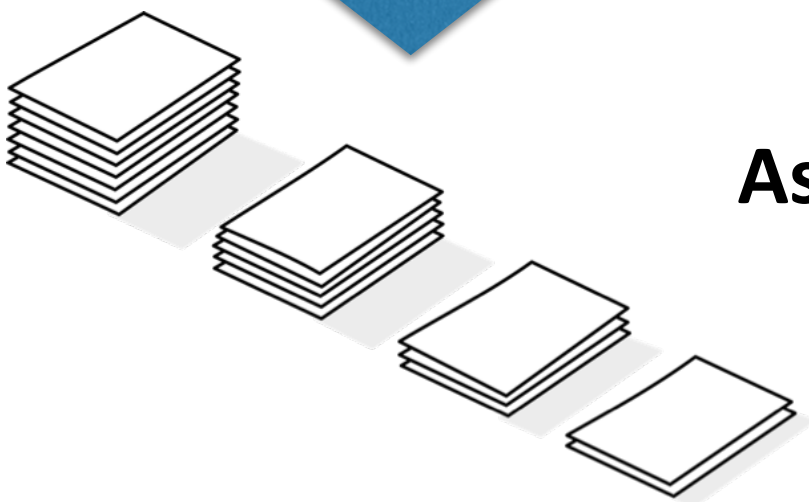
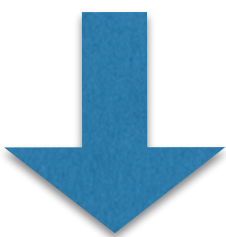


Time & frequency

What?



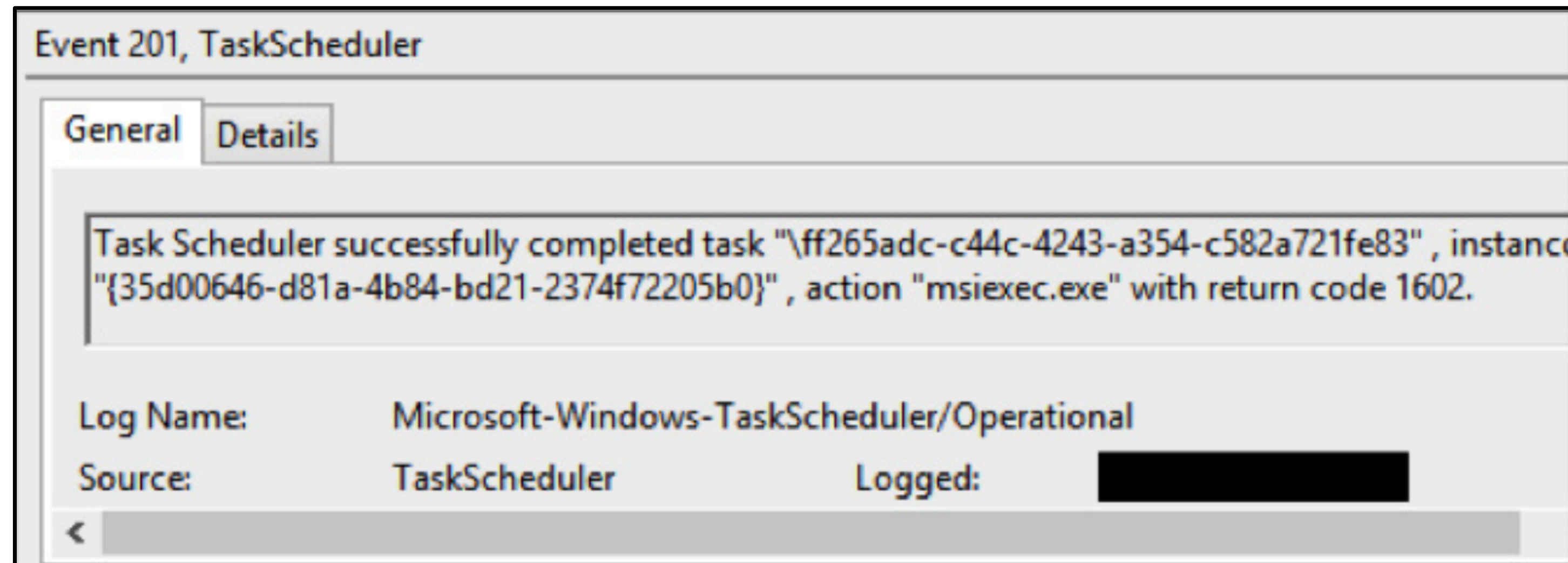
Executed commands,
dropped files, etc.



Assess outliers

Hunting for Duqu 2.0

“In addition to creating services to infect other computers in the LAN, attackers can also use the **Task Scheduler to start ‘msiexec.exe’ remotely**. The usage of Task Scheduler during Duqu infections for lateral movement was also observed with the 2011 version...”



Source:

https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyber_espionage_actor_returns.pdf

What was the shared IOC?

Authored: 06/10/2015 by Kaspersky Lab

Description: Indicators of compromise for the Duqu 2.0 <https://securelist.com/mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor/53111>

OR

- FileItem/Md5sum is 089a14f69a31ea5e9a5b375dc0c46e45
- FileItem/Md5sum is 16ed790940a701c813e0943b5a27c6c1
- FileItem/Md5sum is 26c48a03a5f3218b4a10f2d3d9420b97
- FileItem/Md5sum is a6dcae1c11c0d4dd146937368050f655
- FileItem/Md5sum is acbf2d1f8a419528814b2efa9284ea8b
- FileItem/Md5sum is c04724afdb6063b640499b52623f09b5
- FileItem/Md5sum is e8eaec1f021a564b82b824af1dbe6c4d
- FileItem/Md5sum is 10e16e36fe459f6f2899a8cea1303f06
- FileItem/Md5sum is 48fb0166c5e2248b665f480deac9f5e1
- FileItem/Md5sum is 520cd9ee4395ee85ccb073a00649602
- FileItem/Md5sum is 7699d7e0c7d6b2822992ad485caacb3e

- FileItem/Md5sum is 84c2e7ff26e6dd500ec007d6d5d2255e
- FileItem/Md5sum is 856752482c29bd93a5c2b62ff50df2f0
- FileItem/Md5sum is 85f5feeed15b75cacb63f9935331cf4e
- FileItem/Md5sum is 8783ac3cc0168ebaef9c448fbe7e937f
- FileItem/Md5sum is 966953034b7d7501906d8b4cd3f90f6b
- FileItem/Md5sum is a14a6fb62d7efc114b99138a80b6dc7d
- FileItem/Md5sum is a6b2ac3ee683be6fbbbab0fa12d88f73
- FileItem/Md5sum is cc68fcc0a4fab798763632f9515b3f92
- FileItem/Md5sum is 3f52ea949f2bd98f1e6ee4ea1320e80d
- FileItem/Md5sum is c7c647a14cb1b8bc141b089775130834
- PortItem/remotelP contains 182.253.220.29
- PortItem/remotelP contains 186.226.56.103

How could we do better?

- We could just add a specific **TaskItem** to the IOC...
- ...but what about other variants?
- How can we find evidence of other malicious activity that abuses the same (incredibly common) lateral movement technique?

Stacking tasks in event logs

Stack by User

```
User, Count
...
CORP\ITAdmin,9761
CORP\InfosecAdmin,2240
CORP\DomainAdmin,77
CORP\EBachman,5
AlicePC\Administrator,3
ACMEDC01\Administrator,2
CORP\RHendricks,1
...
```

Stack by ActionName

```
Path, Count
...
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe,1862
c:\temp\patchFix.exe,310
...
c:\test.bat,15
c:\dump.bat,7
c:\temp\1.bat,3
...
```

Summarized "At" Task Events

```
Hostname, Timestamp, EID, UserContext, ActionName
...
AlicePC,2015-08-15 16:44:33,106,AlicePC\Administrator,N/A
AlicePC,2015-08-15 16:45:00,200,N/A,c:\test.bat
...
BobPC,2015-08-15 16:47:18,106,CORP\ITAdmin,N/A
BobPC,2015-08-15 16:49:00,200,N/A,c:\dump.exe
...
AcmeDC01,2015-06-15 09:44:00,200,N/A,c:\temp\patchFix.exe
AcmeDB02,2015-06-15 09:51:00,200,N/A,c:\temp\patchFix.exe
AcmeEX02,2015-06-15 09:37:00,200,N/A,c:\temp\patchFix.exe
...
```

Stack by User

User, Count

...
CORP\ITAdmin,9761
CORP\InfosecAdmin,2240
CORP\DomainAdmin,77
CORP\EBachman,5
AlicePC\Administrator,3
ACMEDC01\Administrator,2
CORP\RHendricks,1
...

Stack by ActionName

Path, Count

...
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe,1862

Hostna

...
Alice
Alice
...
BobPC
BobPC
...
AcmeD
AcmeD
AcmeE
...

```
ACMEDC01\Administrator,2  
CORP\RHendricks,1  
...
```

Stack by ActionName

```
Path, Count  
...  
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe,1862  
c:\temp\patchFix.exe,310  
...  
c:\test.bat,15  
c:\dump.bat,7  
c:\temp\1.bat,3  
...
```

Summarized "At" Task Events

Hostname, Timestamp, EID, UserContext, ActionName

...

AlicePC,2015-08-15 16:44:33,106,AlicePC\Administrator,N/A

AlicePC,2015-08-15 16:45:00,200,N/A,c:\test.bat

...

BobPC,2015-08-15 16:47:18,106,CORP\ITAdmin,N/A

BobPC,2015-08-15 16:49:00,200,N/A,c:\dump.exe

...

AcmeDC01,2015-06-15 09:44:00,200,N/A,c:\temp\patchFix.exe

AcmeDB02,2015-06-15 09:51:00,200,N/A,c:\temp\patchFix.exe

AcmeEX02,2015-06-15 09:37:00,200,N/A,c:\temp\patchFix.exe

...

Stacking tasks “at-rest”

Scheduled Tasks		
	Task Name	Command
☐	At1	cmd.exe /c c:\drop.exe
☐	Pulse_DiskMemCPU_AlwaysOn	
☐	Tanium_Pulse	logman start Tanium_Pulse
☐	At2	cmd.exe /c c:\drop.exe
☐	Adobe Acrobat Update Task	C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe
☐	Adobe Flash Player Updater	C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe
☐	GoogleUpdateTaskMachineUA	C:\Program Files\Google\Update\GoogleUpdate.exe /ua /installsource scheduler
☐	GoogleUpdateTaskMachineCor	
☐	Optimize Start Menu Cache Files-S-1-5-21-4041800420-3685383385-1286802629-500	COM handler

Monitoring tasks “in-motion”

Trace Executed Processes[1424906688340 1551153240000, 0, 1, 0, 0, , , at \\\, , ,]							
Endpoint Name ↑ ≡	Start Time ≡	Parent Process Path ≡	Process Path ≡	Command Line ≡	MD5 ≡	Domain	
Win7-x64-Client	Fri, 26 Feb 2016 00:06:32 +0000	C:\Windows\System32\cmd.exe	C:\Windows\System32\at.exe	at \\\127.0.0.1 12:01 cmd.exe /c	ED4CD10A13080E51F550F560F7	WIN7-X64-CLIENT	

Command Line ≡

at \\\127.0.0.1 12:01 cmd.exe /c

Another example: stacking binaries

“How many unique PE files (EXEs, DLLs, drivers) have loaded on all servers and end-user systems?”

- Different OS versions and add-ons
- User-installed applications
- File names & paths containing GUIDs, per-user data
- Temporary artifacts of software installers
- Updates & patches

Choosing a manageable stack of data

Source: ~250 similar Windows server & workstation VMs in a small demo environment

Items:
2,490 (95,262 total)

Live Updates: Off | 100% (100% available)

Loaded Modules with MD5 Hash

Path ↑

MD5 Hash

☐	c:\windows\...	
☐	c:\windows\...	
☐	c:\windows\...	

Items:
355 (15,152 total)

Live Updates: On | 100%

AutoRun Program Details

Entry Locat

Entry

Category

Profile

Description

Publisher

Image Path

Version

Launch Stri

MD5 H

☐	HKLM\System\...	
☐	HKLM\System\...	
☐	HKLM\System\...	

Items:
225 (8,298 total)

Live Updates: Off | 98% (98% available)

Service Status with MD5 Hash

Short Name

Long Name

Service Account

Command Line

MD5 Hash

☐	OpenDHCPService			
☐	SamSs			
☐	TermService			
☐	WMPNetworkSv			

Items:
4 (501 total)

Live Updates: On | 100%

WMI Event Consumers

Name ↑

Class

Command Line Template

☐	SCM Event Log Consumer	NTEventLogEventConsumer	N/A
☐	BVTConsumer	CommandLineEventConsumer	cscript KernCap.vbs
☐	DoBadThings	CommandLineEventConsumer	C:\Windows\System32\eventMon.exe
☐	EvilConsumer	CommandLineEventConsumer	C:\Windows\System32\evil.exe

Comparing alike assets

Question:

Get AutoRun Program Details from all machines with Operating System containing "windows"

Search

Save this question | Copy to Question Builder

Items: 308 (10,000 total)

Live Updates

AutoRun Program Details

Entry

☐ adpa

☐ adpu

☐ aliide

☐ adp9

☐ amd

☐ aic78

☐ amd

☐ amd

☐ arcsa

Question:

Get AutoRun Program Details from all machines with Installed Applications containing "sql server"

Search

Save this question | Copy to Question Builder

Items: 71 (147 total)

Filter by Computer Group

Contains

Filter by Text

View:

Table

Chart

Bar

Live Updates: On | 100%

Clear Sort

Text Wrap: ☐

Merge

For additional examples

- “Hunting in the Dark”
 - <https://speakerdeck.com/ryankaz>
- Includes coverage of:
 - Pitfalls and success factors for a hunting program
 - Strategies for data reduction
 - Technical examples including lateral movement, persistence mechanisms, process trees

Service activity in event logs

EID 7045

Log Name: System
Source: Service Control Manager
Date: 8/26/2015 9:19:13 AM
Event ID: 7045
Task Category: None
Level: Information
Keywords: Classic
User: AlicePC\Administrator
Computer: AlicePC.acme.com
Description: A service was installed in the system.

Example: cmd.exe as child

Trace Executed Process Trees[cmd.exe, 0, As Child] ↑

	Count ↓
System Idle Process -> explorer.exe -> cmd.exe	3
System Idle Process -> cmd.exe	2
System Idle Process -> cscript.exe -> cmd.exe	1
System Idle Process -> wininit.exe	
System Idle Process -> winlogon.exe	
System Idle Process -> winlogon.exe	
System Idle Process -> winlogon.exe	

Interesting targets

- Shells & interpreters
 - cmd.exe
 - powershell.exe
 - cscript.exe
 - wscript.exe
 - mshta.exe
 - rundll32.exe
- Tools for lateral movement
 - net.exe
 - at.exe
- Commonly “hijacked” processes
 - schtasks.exe / taskeng.exe
 - wmic.exe / wmiprvse.exe
 - svchost.exe
 - w3wp.exe
 - iexplore.exe
 - winword.exe
 - excel.exe

Closing thoughts and takeaways

Evolving standards & platforms

- Platforms
 - MISP
<http://www.misp-project.org>
- Hubs and exchanges
 - Facebook ThreatExchange
<https://threatexchange.fb.com>
- Standards
 - CybOX 3.0 refactoring and simplification



ThreatExchange



Quantitative assessment of threat feeds

- Few efforts to-date - this is difficult!
- **Threat Intelligence Quotient Test (tiq-test)**
 - Statistical analysis of IPs and domains in threat feeds
 - References:
<https://github.com/mlsecproject>

<https://defcon.org/images/defcon-22/dc-22-presentations/Pinto-Maxwell/DEFCON-22-Pinto-and-Maxwell-Measuring-the-IQ-of-your-threat-feeds-TIQtest-Updated.pdf>

Ask your threat feed vendor

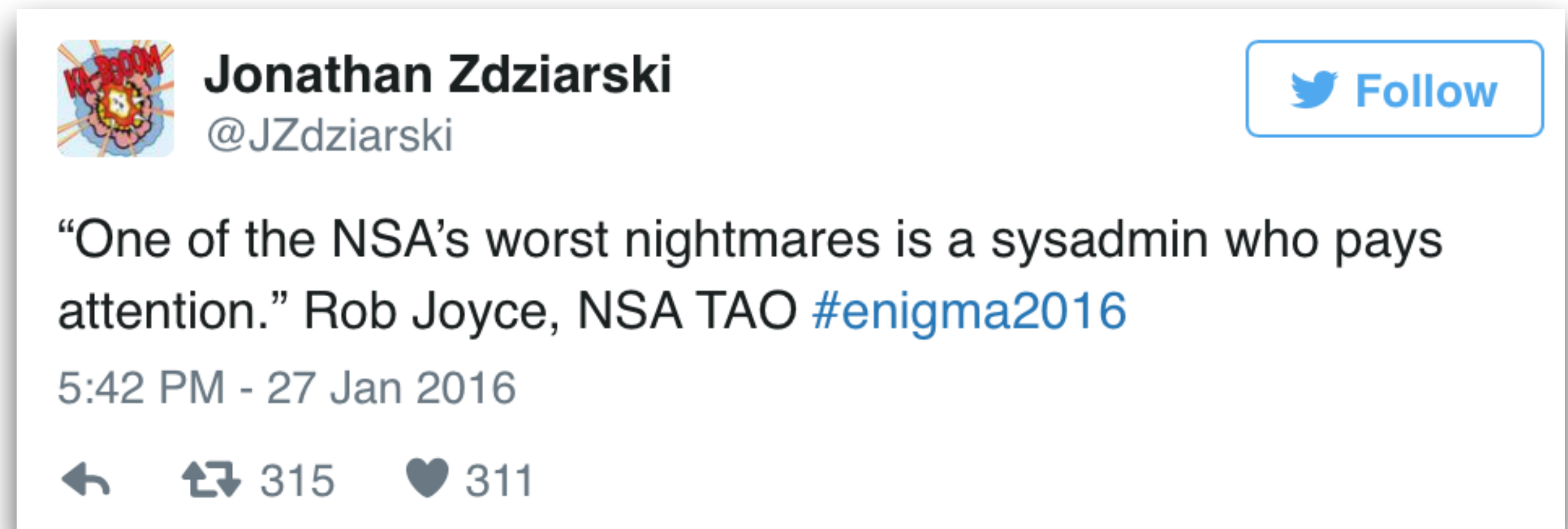
- **Where's the intel coming from?**
 - Professional services
 - Managed security services
 - Partners
 - Honeypots
 - “Open source” data gathering
 - Auto-generated sandbox data
- **What's the breakdown of observable types?**
- **What QC is in place?**
 - Test-cases
 - Documentation
 - Spot-checking

Maximize your IOCs & threat data

- Where are your gaps in endpoint & network **visibility**?
- Can you expand the **scope of data** made available for endpoint IOC matching in your environment?
- Are your tools and threat data sources **fully compatible**?
- How **quickly** are you consuming new threat data? At what **scale**?

Have your investments made you more secure?

- Even the best sources of threat data will never keep pace with emerging attacks
- Know your network above all
- Don't neglect attack surface reduction and security hygiene in favor of buying better IOCs



Thank you!

ryan.kazanciyan [at] tanium.com

@ryankaz42

