

Logistics

- ▶ Download files here
- ▶ <https://github.com/kinkster/bsides/>
 - ▶ Pull down files.zip
- ▶ Network: SALT Secure
- ▶ Username: bsides
- ▶ Password: b-sides2017



Enterprise Wide Visibility into Endpoints

CALGARY BSIDES OCT 2017

I KNOW WHAT I'M
TALKING ABOUT. I
HAVE THIRTY YEARS
IN THIS INDUSTRY!

///



Dilbert.com DilbertCartoonist@gmail.com

HOW DOES THAT HELP
YOU UNDERSTAND
TECHNOLOGY THAT IS
SIX MONTHS OLD IN A
YOUTH-ORIENTED
CULTURE?



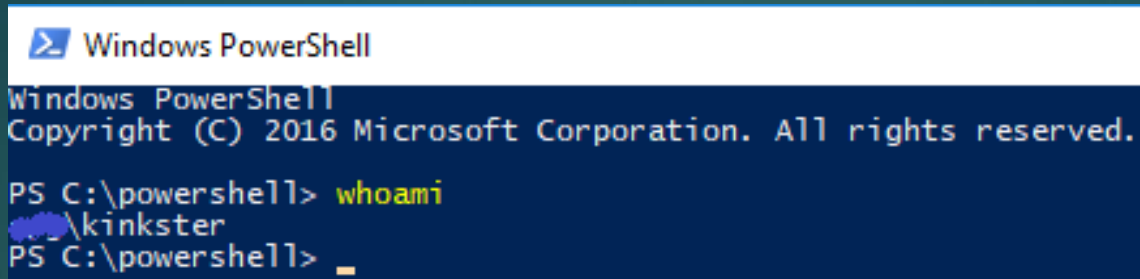
12/23/10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.

PLEASE DON'T
HIT ME WITH
YOUR MODEM.

GRRR...

\\





```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\powershell> whoami
NT AUTHORITY\SYSTEM
PS C:\powershell>
```

- ▶ 31 Years in IT
- ▶ 20 Years in Security
- ▶ Blue Team, GSWN, QSA
- ▶ ArcSight, Splunk
- ▶ SecuredNet
- ▶ Father, Security geek, otaku, nerd, logs, sysmon, primarily blue team
- ▶ @JockStrapp2

Agenda

- ▶ Introduction
- ▶ Install Sysmon in the VM
- ▶ Configure Splunk Server
- ▶ Install Splunk Forwarder on the VM
- ▶ Lunch
- ▶ Review Sysmon App Dashboard
- ▶ Virus Total Integration
- ▶ Deployment Server lessons
- ▶ Future



SwiftOnSecurity

@SwiftOnSecurity

Follow



This is why I emphasize the basics. That security isn't magic. Malware authors win with shitty code and old tricks because nobody's looking.

3:19 PM - 20 Jan 2017

197 Retweets 631 Likes





Gerald Steere

@darkpawH

Follow



Replying to [@jepayneMSFT](#) [@appcompatguy](#)

So much this. Perfection in security is impossible. Secure what you can and monitor the hell out of everything. Assume breach and respond

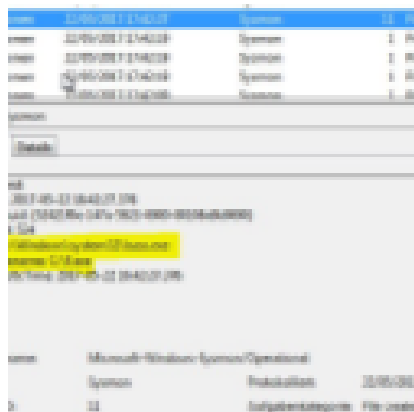
10:08 AM - 10 Oct 2017

↻ You Retweeted



SwiftOnSecurity @SwiftOnSecurity · May 22

If you haven't played with Sysmon, literally takes minutes to grab it and load my rule-set, I guarantee you you'll see something cool.



Kevin Beaumont ✓ @GossiTheDog

Fun with @SwiftOnSecurity's Sysmon configs on SMB Eternal* honeypot. It catches lsass.exe writing out files during EternalBlue exploit.



10



147



405





Matt Swann

@MSwannMSFT

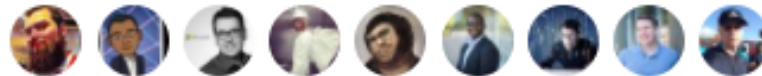
Following



Interested in using ETW for intrusion detection? Check out [@zacbrown](#) at [#DerbyCon](#) today at 10 — source code and samples for .NET and C++ 💪

5:57 AM - 23 Sep 2017

6 Retweets 33 Likes



1



6

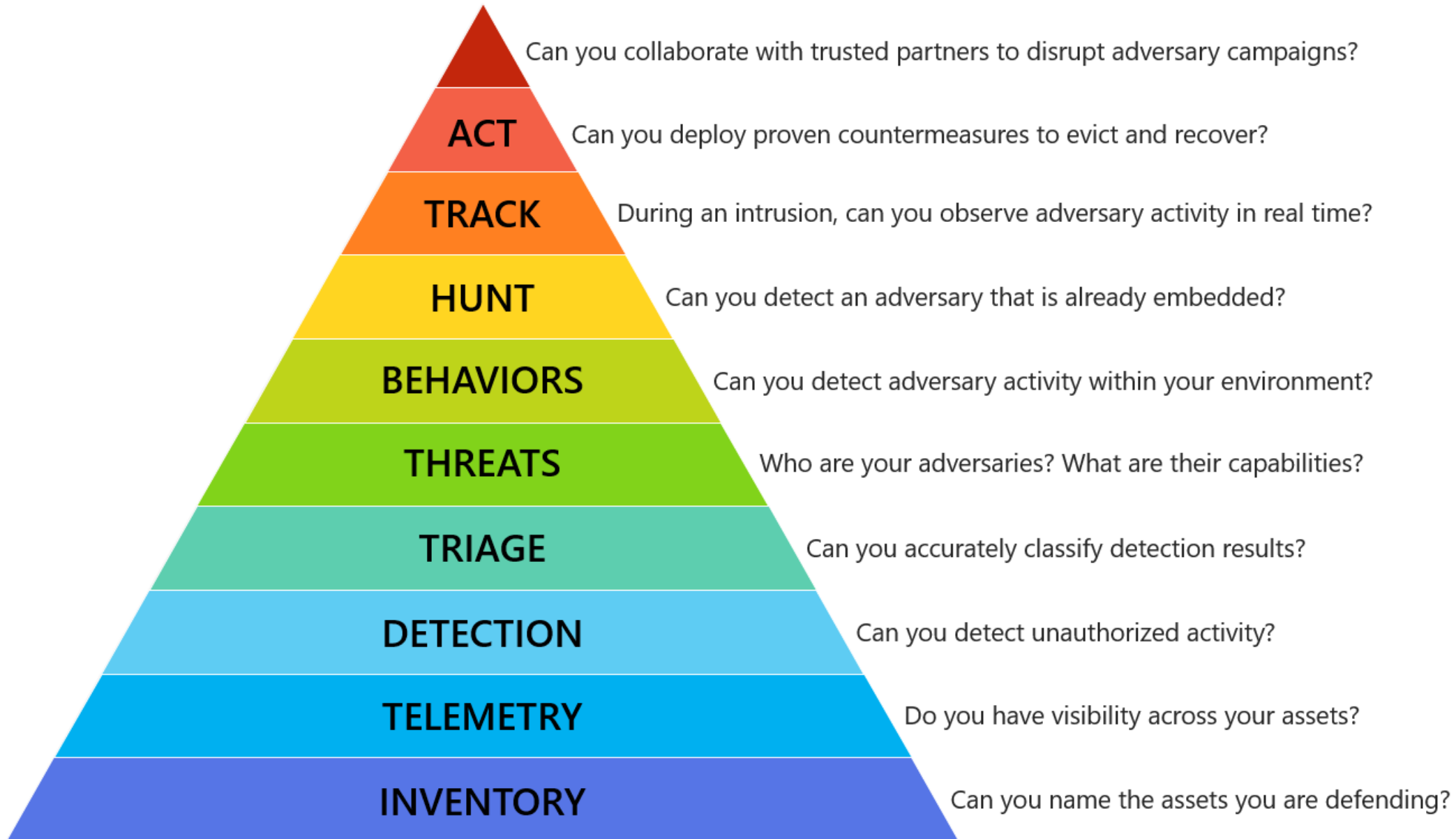


33



www.irongeek.com/i.php?page=videos/derbycon7/t306-defending-thecloud-lessons-from-intrusion-detection-in-sharepoint-online-matt-swann

The Incident Response Hierarchy of Needs



Let's be honest



National Cyber
Security Centre

- Anatomy of most unprecedented, sophisticated cyber attacks:
 1. Attacker does a bit of research on LinkedIn/Facebook (optional)
 2. Attacker sends spear phishing email to an admin
 3. Admin opens email using his admin account, exploiting unpatched stuff
 4. Attacker acts as admin and does nefarious stuff
 5. Monitoring doesn't work so no-one notices
 6. Systems and networks are flat, so no hurdles to total exploitation
 7. Profit!

Sysmon Resources

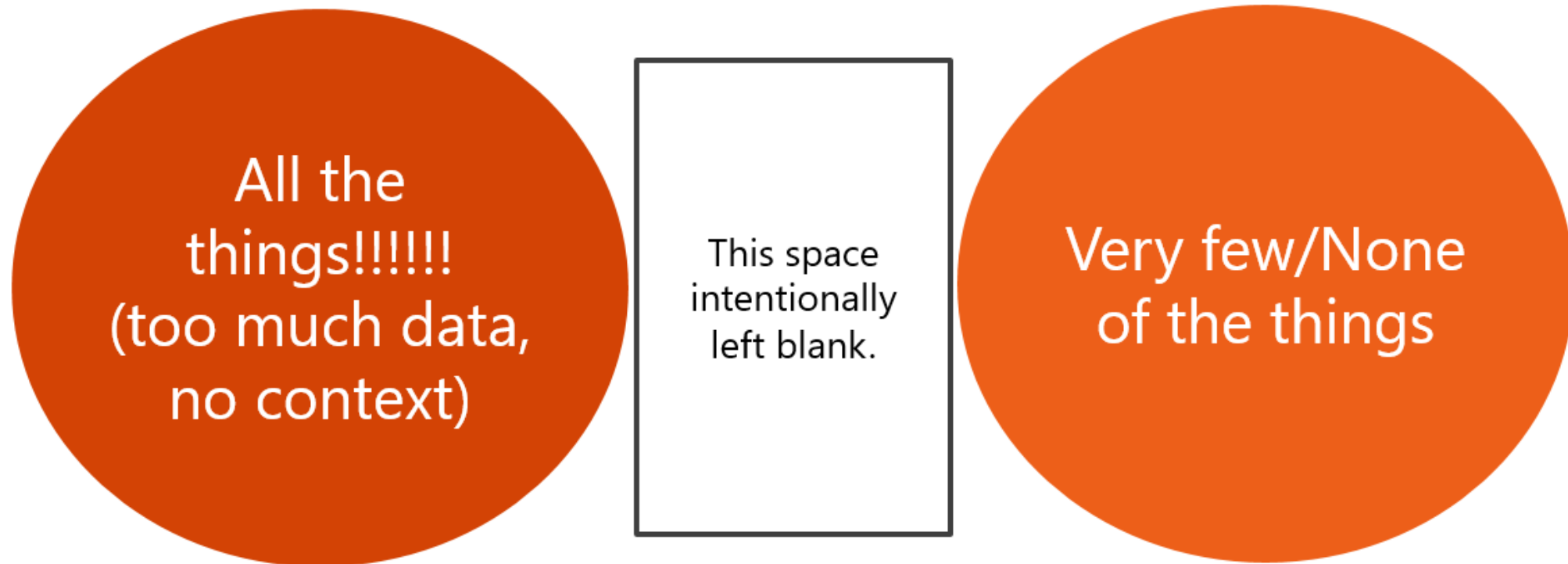
- ▶ Version 6.1 released Sept 11 2017 has Named Pipes and WMI monitoring
- ▶ This site probably has all the resources listed
 - ▶ <https://github.com/MHaggis/sysmon-dfir>
- ▶ John H, (This is a cool title and good article)
 - ▶ <http://909research.com/sysmon-the-best-free-windows-monitoring-tool-you-arent-using/>
- ▶ Mark Russonivich
 - ▶ https://www.rsaconference.com/writable/presentations/file_upload/hta-w05-tracking_hackers_on_your_network_with_sysinternals_sysmon.pdf
- ▶ James Brodsky
 - ▶ https://conf.splunk.com/session/2015/conf2015_Jbrodsky_Splunk_SecurityCompliance_SplunkingTheEndpoint_FINAL.pdf

Sysmon Filter

- ▶ If you are just using the tag without a filter, the rule (onmatch) has opposite effect!
- ▶ `<!-- Do not log FileCreateTime Event ID 2 -->`
- ▶ `<FileCreateTime onmatch="include"/>`
- ▶ `<!-- Log all when FileCreateStream is triggered Event ID 15-->`
- ▶ `<FileCreateStreamHash onmatch="exclude" >`
- ▶ `</FileCreateStreamHash>`

Jessica Payne Security Person at Microsoft.

Venn Diagram of Common Monitoring Strategies



End Point Goals

- ▶ Our first goal is to pull less than 5 MB /day /endpoint
 - ▶ 10 GB/ Day license
- ▶ Meet the basics of monitoring
- ▶ Get more sophisticated as time goes by
- ▶ Monitoring and hardening go hand in hand

Sysmon Command Lines

- ▶ Run as administrator
- ▶ Sysmon.exe -accepteula -i -n (Install with network monitoring)
- ▶ Sysmon.exe -c Test.xml (Apply filter)
- ▶ Sysmon.exe -u (Uninstall)
- ▶ Sysmon.exe -s (Shows schema version for your filter)
- ▶ Install Sysmon in your VM and use the Test.xml configuration file
- ▶ Verify they are coming into your event log
- ▶ You can download this one and test later
- ▶ <https://github.com/ion-storm/sysmon-config>

You should see this

The screenshot displays the Windows Event Viewer application. The left-hand pane shows a tree view of event logs, with 'Sysmon' expanded and 'Operational' selected. The main pane shows a list of events under the 'Operational' log, with the first event (ID 1) selected. The details pane for this event is visible, showing the 'Process Create' event details. The right-hand pane shows the 'Actions' menu for the selected event.

Event Viewer

File Action View Help

Operational Number of events: 32,831 (!) New events available

Level	Date and Time
Information	9/27/2017 5:16:33 PM
Information	9/27/2017 5:16:30 PM
Information	9/27/2017 5:16:30 PM
Information	9/27/2017 5:16:30 PM
Information	9/27/2017 5:16:30 PM
Information	9/27/2017 5:16:30 PM

Event 1, Sysmon

General Details

Process Create:
UtcTime: 2017-09-27 23:16:33.211
ProcessGuid: {d05bc4ce-3151-59cc-0000-00100864180c}
ProcessId: 11532
Image: C:\Windows\System32\backgroundTaskHost.exe
CommandLine: "C:\WINDOWS\system32\backgroundTaskHost.exe" -
ServerName: CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca
CurrentDirectory: C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2bxyew\
User: CPG\klnkster
LogonGuid: {d05bc4ce-1761-59cc-0000-0020554ea30b}
LogonId: 0xBA34E55
TerminalSessionId: 5
IntegrityLevel: AppContainer
Hashes: SHA1=0DA61DE2844E7AABBB0D424722E477F95FFA3632

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 9/27/2017 5:16:33 PM
Task Category: Process Create (rule: Proce
Keywords:
Computer: CPE-1016-05.cpg.local

Actions

Operational

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 1, Sysmon

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Filter, Harden, Audit

- ▶ Disable NetBios in network properties
- ▶ Disable services, WPAD, LLMNR, Windows Browser Protocol, SSDP
 - ▶ `<DestinationPort>5355</DestinationPort> <!-- LLMNR inbound to udp port 5355-->`
 - ▶ `<DestinationPort>1900</DestinationPort> <!-- Disable the SSDP and UPnP services to stop udp 1900 from svchost.exe-->`
 - ▶ `<SourcePort>1900</SourcePort> <!-- Disable the SSDP and UPnP services to stop udp 1900 from svchost.exe-->`
 - ▶ `<SourcePort>5355</SourcePort> <!-- LLMNR inbound to udp port 5355-->`
- ▶ Set your audit Policy, can use Auditpol but recommend just doing it manually.
- ▶ <http://adsecurity.org/?p=3299> Securing Windows Workstations Sean Metcalf

Windows Auditing

- ▶ Windows 10 and Windows Server 2016 security auditing and monitoring reference
 - ▶ <https://www.microsoft.com/en-us/download/details.aspx?id=52630&751be11f-ed8-5a0c-058c-2ee190a24fa6=True>
- ▶ See the recommendations in Auditing.xlsx
- ▶ You want Logon/Logoff, Logon Success and Failure

Centralized log management options

- ▶ Windows Event Forwarder
 - ▶ <https://github.com/palantir/windows-event-forwarding>
 - ▶ <https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/>
- ▶ Flip the Script: PowerShell "Microsoft's Incident Response Language"
- Jared Atkinson May 9 2017 PowerShell EU Conference
 - ▶ <https://www.youtube.com/watch?v=8M30-58SjWE>
- ▶ <https://www.elastic.co/webinars/introduction-elk-stack>
 - ▶ <https://github.com/secabstraction/PowerStashPowerStash>
- ▶ <https://github.com/philhagen/sof-elk>
- ▶ <https://www.graylog.org/>

Configure Splunk Server

- ▶ http://docs.splunk.com/Documentation/SplunkCloud/6.6.1/SearchTutorial/InstallSplunk#Windows_installation_instructions
- ▶ Install as System on your Host
- ▶ Install the Sysmon-TA
- ▶ Install Sysmon App for Splunk
- ▶ Install Windows-TA (Splunk Add-on for Microsoft Windows)
- ▶ Create Index called “endpoints” (lowercase)
- ▶ Forwarding and Receiving, Configure receiving, new, listen on port 9997
- ▶ Server Settings, Search preferences, set to Last 60 minutes
- ▶ Settings, Access Controls, Roles, Admin, add endpoints index to indexes searched by default

Browse More Apps

sysmon



Best Match

Newest

Popular

5 Apps

CATEGORY

- ☐ DevOps
- ☐ IT Operations
- ☐ Security, Fraud & Compliance
- ☐ Business Analytics
- ☐ IoT & Industrial Data
- ☐ Utilities

CIM VERSION

- ☐ 4.9
- ☐ 4.8
- ☐ 4.7
- ☐ 4.6
- ☐ 4.5
- ☐ 4.4
- ☐ 4.3
- ☐ 4.2
- ☐ 4.1
- ☐ 4.0



Sysmon App for Splunk

Open App

The Sysmon App for Splunk provides rapid insights and operational visibility into small and large scale Sysmon deployments. Native out of the box alerting capabilities, reporting and dashboards to provide easy context and visibility into your endpoint data.

The Sysmon App for Splunk is easy to deploy and utilizes the already available Sysmon TA providing easy and instant value into your endpoint data.

****Feature Request****

Submit an issue via repository on Github (<https://github.com/MHaggis/sysmon-splunk-app>) or Twitter @m_haggis or @jarrettp

****Support****

Submit an issue via repository on Github - <https://github.com/MHaggis/sysmon-splunk-app>

[Less](#)

Category: [Security, Fraud & Compliance](#) | Author: [Mike Haag](#) | Downloads: 388 | Released: 6 months ago |

Last Updated: 6 months ago | [View on Splunkbase](#)



Add-on for Microsoft Sysmon

Already Installed

Provides a data input and CIM-compliant field extractions for Microsoft Sysmon. The Microsoft Sysmon utility provides data on process creation (including parent process ID), network connections, and much more.

This add-on was originally created by Adrian Hall. We appreciate Adrian's contribution and his willingness to turn over control to the current team for ongoing maintenance and development.

[Less](#)

Category: [Security, Fraud & Compliance](#), [IT Operations](#) | Author: [David Herralde](#) | Downloads: 4535 | Released: 3 years ago |

Last Updated: 18 days ago | [View on Splunkbase](#)

Browse More Apps

windows ta



CATEGORY

- ☐ DevOps
- ☐ IT Operations
- ☐ Security, Fraud & Compliance
- ☐ Business Analytics
- ☐ IoT & Industrial Data
- ☐ Utilities

CIM VERSION

- ☐ 4.9
- ☐ 4.8
- ☐ 4.7
- ☐ 4.6

Best Match

Newest

Popular

184 Apps



Splunk Add-on for Microsoft Windows

Update

The Splunk for Microsoft Windows add-on includes predefined inputs to collect data from Windows systems and maps to normalize the data to the Common Information Model.

Category: [IT Operations](#), [Utilities](#) | Author: [Splunk Inc.](#) | Downloads: 115406 | Released: 6 years ago |

Last Updated: 6 months ago | [View on Splunkbase](#)

What we did!

- ▶ Installed as system. The only time you need to run as domain or privileged domain account is to automatically run scripts on remote hosts you need access to. You can pull logs at any time with system.
- ▶ We installed the TA's because they do all the heavy parsing of events (Technical Addons)
- ▶ We installed the Sysmon App as that provides a dashboard and some examples
- ▶ We created a new index. Usually used as a security boundary to allow only certain Splunk users
- ▶ We initiated the receiver
- ▶ Set some preferences

Install Splunk Forwarder on the VM

- ▶ Download the Splunk forwarder
- ▶ https://www.splunk.com/en_us/download/universal-forwarder.html
- ▶ Install as system
- ▶ Deployment server = your IP or host name Port 8089
- ▶ Receiving Indexer = your IP or host name Port 9997
- ▶ Look at your indexer /console to ensure you are only receiving security logs
- ▶ Look in Settings, Forwarder Management to see your client
- ▶ Make sure your vm has network connectivity and the firewall is not blocking it.

What we did with forwarder!

- ▶ We told the forwarder to forward only security logs
- ▶ We told the forwarder to use our host as the deployment server
 - ▶ <http://docs.splunk.com/Documentation/Splunk/6.6.3/Data/MonitorWindowsEventlogdata>
- ▶ We are using the default index main

Install Splunk App via Deployment Server

- ▶ On the host VM , copy MyApp to
- ▶ c:\program files\splunk\etc\deployment-apps\
 - ▶ Edit outputs.conf to match your IP address
 - ▶ Ensure the inputs.conf match your sysmon Filter
 - ▶ Should be Test2.xml
- ▶ Go to Forwarder Management, Create Server Class, Add MyApp to the Apps, Add your client to the clients
- ▶ Under MyApp edit it to restart Splunk
- ▶ Run refresh to push out immediately
- ▶ <https://yourhost:8000/en-US/debug/refresh>

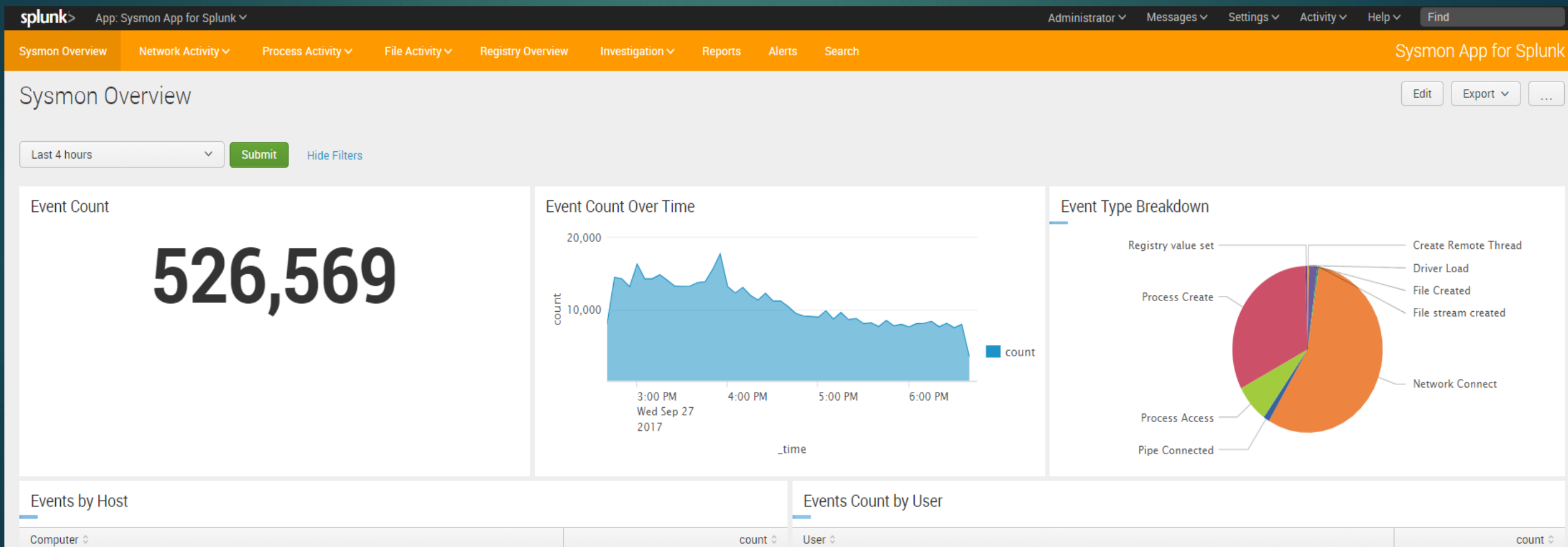
What we did with Deployment Server

- ▶ We pushed out the MyApp application
- ▶ We told the forwarder to forward the logs in our inputs.conf
 - ▶ We specified the endpoint index
 - ▶ We applied some filtering on the inputs.conf
 - ▶ We specified whitelists and black lists
 - ▶ <http://docs.splunk.com/Documentation/Splunk/6.6.3/Data/MonitorWindowseventlogdata>
- ▶ So we can filter with Sysmon and with the forwarder
 - ▶ 4688, 4689 Events should have stopped
 - ▶ Sysmon events should now appear
 - ▶ Index should be endpoints

Lunch



Review Sysmon App Dashboard





Jessica Payne

@jepayneMSFT

Following



You also want System log Event ID 7045 for new service creation, and 1102 for log clears if I haven't said that enough already. :)

4:07 PM - 16 Mar 2017

40 Retweets 105 Likes



Jessica Payne

@jepayneMSFT

Following



If you are not actually monitoring for a well documented and publicly available technique, you should be.

6:46 PM - 20 Jul 2017

7 Retweets 22 Likes



1



7



22



Where to start

- ▶ NSA “Spotting the Adversary with Windows
- ▶ “Intrusion Detection Using Indicators of Compromise Based on Best Practices and Windows Event Logs”
- ▶ JP Cert “Detecting Lateral Movement through Tracking Event Logs”
- ▶ <https://www.malwarearchaeology.com/cheat-sheets/>
- ▶ https://attack.mitre.org/wiki/ATT%26CK_Matrix
 - ▶ <http://www.irongeek.com/i.php?page=videos/derbycon7/t409-blue-team-keeping-tempo-with-offense-casey-smith-keith-mccammon>

User Attribution

- ▶ You need to ensure you are investigating correct system
- ▶ Use, sysmon, AV program, AD, NSLookup, Firewall
- ▶ Create a users CSV and Computers CSV from AD for better context

User Attribution

Attributes user to IP to host name through various sources

\\User

cpg\\kinkster

ComputerName

CPE-1000-00

IP Address

10.0.1.22

Duration

Last 4 days

Submit

Hide Filters

Sysmon via IP 10.0.1.22

user	host	SourceIp
CPE\\kinkster	CPE-1000-00	10.0.1.22

Sysmon Event ID 3 CPE-1000-00

user	host	SourceIp
CPE\\kinkster	CPE-1000-00	10.0.1.22

Sysmon Event ID 3 CPE-1000-00 cpg\\kinkster

User	host	SourceIp
CPE\\kinkster	CPE-1000-00	10.0.1.22

Lookup using CPE-1000-00

Lookup via AD computer

host	IPv4Address	src_ip	ObjectClass	OperatingSystem	OperatingSystemServicePack
CPE-1000-00	10.0.1.22	10.0.1.22	computer	Windows 10 Enterprise	

Lookup using cpg\\kinkster

Lookup via AD user

Name	Department	Title	telephoneNumber	Office	OfficePhone	user
Kenneth Inkster	Information Systems	Consultant - IT Security	587-955-3587	Calgary, AB	587-577-2000	kinkster

Data Enrichment through AD

- ▶ `Get-ADComputer -filter * -Properties Enabled,Name,IPv4Address,ObjectClass,OperatingSystem,OperatingSystemServicePack |`
- ▶ `Where-Object {$_.Enabled -eq "True"} |`
- ▶ `Select-Object @{expression={$_.Name}; label='host'},IPv4Address,ObjectClass,OperatingSystem,OperatingSystemServicePack |`
- ▶ `export-csv "ADcomputers.csv" -NoTypeInfoInformation`
- ▶ `Get-ADUser -filter * -properties Name, Department, Manager, telephoneNumber, Office, OfficePhone, Title, SID, Enabled | Where-Object {$_.Enabled -eq "True"} |`
- ▶ `select-object @{expression={$_.SamAccountName}; label='user' },Name, Department, Manager, telephoneNumber, Office, OfficePhone, Title, SID |`
- ▶ `export-csv "ADusers.csv" -NoTypeInfoInformation`

Keeping your logs down

- ▶ `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" | eval length_in_bytes=len(_raw) | stats sum(length_in_bytes) as bytes by sourcetype host | eval mbytes=(bytes/1024/1024) | eval mbytes=round(mbytes,2) | addcoltotals | fields - bytes`
- ▶ `sourcetype=WinEventlog:Security | eval length_in_bytes=len(_raw) | stats sum(length_in_bytes) as bytes by sourcetype host | eval mbytes=(bytes/1024/1024) | eval mbytes=round(mbytes,2) | addcoltotals | fields - bytes`

Your attacker thinks like my attacker: A common threat model to create better defense

You can't just buy this,
you have to build it.



30:48 / 43:54



<https://youtu.be/ljz7NHF3l28> Jessica Payne MS Ignite 2017

Create output file

- ▶ Here we create some Splunk output of all the executables that have run in the c:\users\ folder structure
- ▶ This will be used to submit to Virus Total
- ▶ `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 (Image=C:\\users* OR Image=*Downloads*) | dedup Hashes | rex mode=sed field=Hashes "s/SHA1=//g" | table Hashes Image host`
- ▶ Append this after `| outputlookup myhashes.csv`
- ▶ Save as report myhashesoutput for later use

Virus Total Integration

- ▶ You should have your API key
- ▶ Place these files in c:\powershell\ folder on your host
 - ▶ VT-SubmitHash-BsidesV1.ps1
 - ▶ VirusTotalv2.psm1
 - ▶ Myhashes.csv
- ▶ Insert your API key
- ▶ Run Powershell with sample myhashes.csv
- ▶ You should see your output in three different files

Every exe checked against VT

APPDATA Virus Total Results Sysmon

Programs run from appdata with and without VT information

_time	host	user	Image	Positives	Total	ScanDate	Hashes
2017-10-04 15:37:08		kinkster	C:\Users\kinkster\AppData\Local\Temp\2521F4B3-5FC9-433B-8A87-AF36033E4E92\DismHost.exe	0	60	2017-05-06 18:52:08	SHA1=505E851852228545903C2423AFA81039E0BD9447
2017-10-04 14:59:30		kinkster	C:\Users\kinkster\AppData\Local\Temp\Procmon64.exe	0	54	2017-01-01 12:20:32	SHA1=E453FEBA236E7D9C145D8FE0FC5B7A6E0CB7F4F7

Sysmon Event ID 1 and then 3

Programs run that connect out to Internet Sysmon Event ID 1 then 3

_time	host	user	EventDescription	Image	Positives	Total	ScanDate	Hashes
2017-10-04 17:12:27		kinkster	Network Connect Process Create	C:\Windows\System32\backgroundTaskHost.exe	0	61	2017-04-18 01:37:34	SHA1=0DA61DE2844E7AABBB0D424722E477F95FFA3632
2017-10-04 16:51:32		kinkster	Network Connect Process Create	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE	0	65	2017-09-14 13:33:56	SHA1=21FB366D2FDFDCACB7CCE63CCEB7187D86BED9DE
2017-10-04 15:49:09		kinkster	Network Connect Process Create	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2017.39081.15820.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe	0	66	2017-10-03 16:08:36	SHA1=EF430FC6AFD641F44A681DB4010C265A571F9910
2017-10-04 15:48:44		kinkster	Network Connect Process Create	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	1	65	2017-09-12 18:32:17	SHA1=B2C52DEEA8548B01EA9F006F672EEB53F328391D
2017-10-04 15:45:21		kinkster	Network Connect Process Create	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE	0	61	2017-05-19 09:25:59	SHA1=CD82B71A998804448CFCD269FF5522E969361616

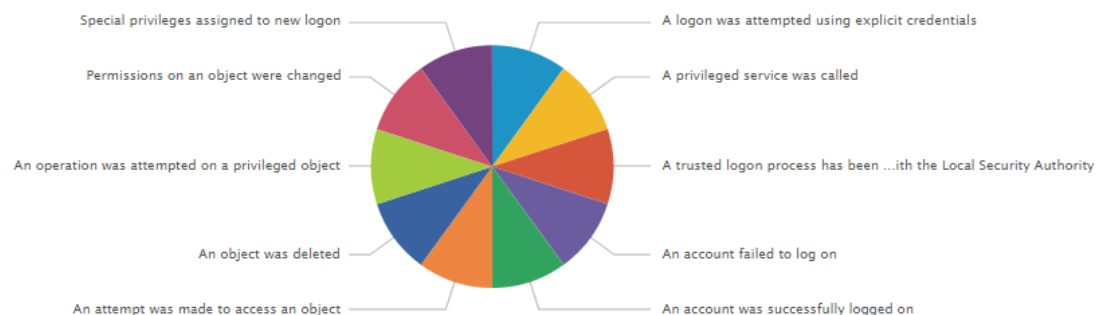
Add example dashboards

- ▶ Copy the Data folder to your host here
 - ▶ C:\Program Files\Splunk\etc\users\admin\search\local\
- ▶ Restart Splunk
- ▶ You should see two dashboards now
- ▶ Start with Triage
- ▶ You can only drill down into CMD.exe dashboard

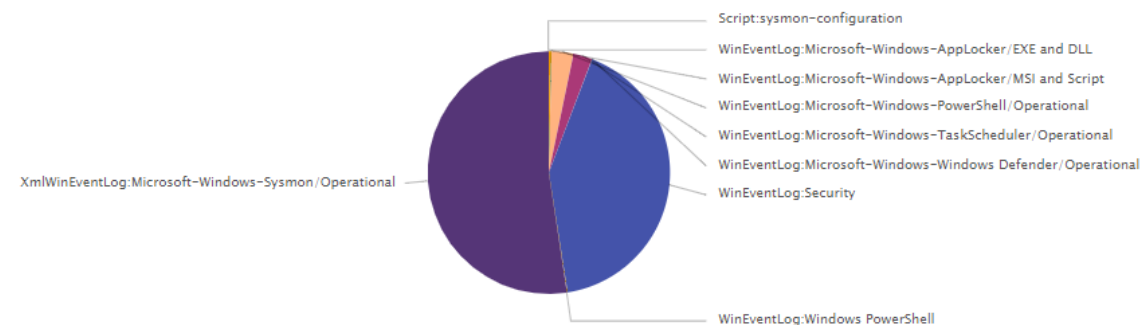
Example Triage Dashboard

Security

Windows Security Events RARE



Log Sources



Sysmon, drills to PowerShell Single Host dashboard

PowerShell

1

Sysmon, drills to Archive Single host dashboard with time

Archived Files

0

Sysmon, drills to new search

Files Created

14

Sysmon, drills to new search

Programs run from C:\user

2

Sysmon, drills to CMD.exe dashboard

Cmd.exe sessions

0

Sysmon, drills to new search

Files in Download folder

0

Palo Alto suspicious files downloaded

0

Deployment Server

- ▶ We used SCCM to deploy sysmon and Splunk forwarder to all agents initially
- ▶ Benefits of deployment server are that you can deploy Sysmon filter changes as needed
- ▶ Can deploy new application such as Investigation collection
 - ▶ Pull in data such as arp, netstat, Powerforensics, memory
- ▶ 1100 Endpoints using deployment server
 - ▶ Changed phoneHomeIntervalInSecs=180 from default of 60
- ▶ Can pull new logs whenever I want
- ▶ You want to push your apps, the Windows TA in particular will help as it has a lot of the built in parsing you need

Deployment server Cont'd

- ▶ We rolled out Applocker with confidence
 - ▶ We saw all audit and blocked events, could respond in real time
- ▶ We rolled out Powershell v5
 - ▶ We can see all Powershell in our Environment
 - ▶ We can see Powershell downgrades
 - ▶ We can see obfuscation
- ▶ EMET was rolled out, can see all EMET events
- ▶ Task Scheduler logs collected
- ▶ EAST West Traffic Analysis capabilities

Truncating

- ▶ Enable this line in the props.conf file, in MyApp or directly on your VM
- ▶ SEDCMD-win = s/(?mis)(Token Elevation Type indicates | This event is generated).*\$ /truncated.../g
- ▶ Stream editor, s/ substitute, find 4688/9 or 4624/34, replace with "truncated..."
- ▶ This can reduce your logs enormously

Jack Crook



Jack Crook @jackcr · Jul 11
Hunting for obfuscated powershell? Strip out alphanumeric and look for repetitive patterns in remaining character sequences. [#DFIR](#)

7 58 135

Jack Crook
@jackcr [Following](#)

Since it takes me forever to do anything these days (especially a blog post), here's a screenshot of what I'm talking about. [#DFIR](#)

/1

splunk App: Search & Reporting Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Close

sourcetype="WinEventlog:Microsoft-Windows-Sysmon/Operational" | bucket span=1h | time | eval orig_command=CommandLine | rex field=CommandLine mode=sed "s/[a-zA-Z0-9]"

Obfuscated PowerShell

- ▶ `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" | bucket span=1h _time | eval orig_command=CommandLine |`
- ▶ `rex field=CommandLine mode=sed "s/[a-zA-Z0-9]//g" | rex field=CommandLine "(?<dstring>.{20})" |`
- ▶ `stats values(orig_command) AS orig_command earliest(_time) AS etime latest(_time) as ltime values(CommandLine) AS CommandLine by dstring |`
- ▶ `fieldformat etime=strftime(etime,"%Y-%m-%d %H:%M:%S") |`
- ▶ `fieldformat ltime=strftime(ltime,"%Y-%m-%d %H:%M:%S") | where etime=ltime AND ltime > relative_time(now(), "-1h")`

Host is not reporting

- ▶ | metadata type=hosts | eval age = now() - lastTime | sort age d |
convert ctime(lastTime) | fields age,host,lastTime | where age >
3600 | table host



Jessica Payne

@jepayneMSFT

Following

Implement monitoring leads to reduce priv,
leads to LAPS, leads to jump servers, leads to
firewalls, leads to whitelisting, leads to
PAW.

10:29 AM - 10 Oct 2017

Future

- ▶ Submit files from remote workstations
- ▶ Improved Triage collection
- ▶ CIMsweep to collect information
- ▶ WMI Events with Sysmon v6.1
 - ▶ See Uproot IDS
- ▶ Auto Start Execution Point (ASEP) Autoruns
- ▶ Sigcheck Integration
- ▶ Host Based Firewall Monitoring
- ▶ ETW for DNS logs

Future Continued

- ▶ Service Resiliency <https://github.com/ion-storm/sysmon-config>
- ▶ Note that Sysmon does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.
- ▶ Windows Protected Processes

Why

- ▶ Security deserves to see all the malware that your users are installing
- ▶ You can see every hash that has run in your enterprise
- ▶ Get your bosses approval for next steps such as hardening
- ▶ Show real numbers that support the risk

