



Hall of Fame

EU ATT&CK® Community Workshop, October 2021

About Me

- Florian Roth
- Head of Research @ Nextron Systems
- IT Sec since 2000,
Nation State Cyber Attacks since 2012
- THOR Scanner
- Twitter @cyb3rops
- Open Source Projects:
 - Sigma (Generic SIEM Rule Format)
 - LOKI (Open Source Scanner)
 - APT Groups and Operations Mapping
 - Antivirus Event Analysis Cheat Sheet
 - ...



Overview

- What is Sigma?
- ATT&CK Integration in Sigma
- Hall of Fame: The 5 most successful Sigma rules
- Where's the Sigma project going?
- Cool new or upcoming related projects



What is Sigma?

Sigma is a generic rule format
to **express detection ideas** in form of rules
that match on **log data**.

What is Sigma?

Sigma is for **log data** what

YARA is for **files** and

Snort is for **network traffic**.

Why Sigma?

- **Simplicity and Usability**
 - Users like it: Easy to read and write
 - Developers like it: Manageable specs and expressions
- **Immediate Benefit**
 - Big rule base with more than 1000 rules
 - Integrated converter for 17+ backends (query generator)
 - Active community: you quickly get new rules for burning issues
- **No Product-Specific Focus**
 - No overreaching vendor
 - No SIEM specific expressions
 - No vendor lock-in



MITRE ATT&CK® Integration

- Sigma rules contain ATT&CK techniques as tags
- A matching rule points to one or more techniques
- The tests check against attackcti.com to compare the tags in new rules with a list of all valid ones (live)

The image shows a code editor on the left and the attackcti web interface on the right.

Code Editor (Sigma Rule):

```
driver_load_mal_creddumper.yml M X powershell_alternate_powershell_hosts.yml (deleted) README.md win_s
1 title: Credential Dumping Tools Service Execution
2 id: df5ff0a5-f83f-4a5b-bba1-3e6a3f6f6ea2
3 related:
4   - id: 4976aa50-8f41-45c6-8b15-ab3fc10e79ed
5     type: derived
6 description: Detects well-known credential dumping tools execution via service execution events
7 author: Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community
8 date: 2017/03/05
9 modified: 2021/10/14
10 references:
11   - https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
12 tags:
13   - attack.credential_access
14   - attack.execution
15   - attack.t1003 # an old o
16   - attack.t1003.001
17   - attack.t1003.002
18   - attack.t1003.004
19   - attack.t1003.005
20   - attack.t1003.006
21   - attack.t1035 # an old o
22   - attack.t1569.002
23   - attack.s0005
24 logsource:
25   product: windows
26   category: driver_load
27 detection:
28   selection:
29     - ImagePath|contains:
30       - 'fgexec'
31       - 'dumpsvc'
32       - 'cachedump'
33       - 'mimidrv'
34       - 'gsecdump'
35       - 'servpw'
36       - 'pwdump'
37   condition: selection
38 falsepositives:
39   - Legitimate Administrator using c
40 level: critical
```

attackcti 0.3.4.4 Web Interface:

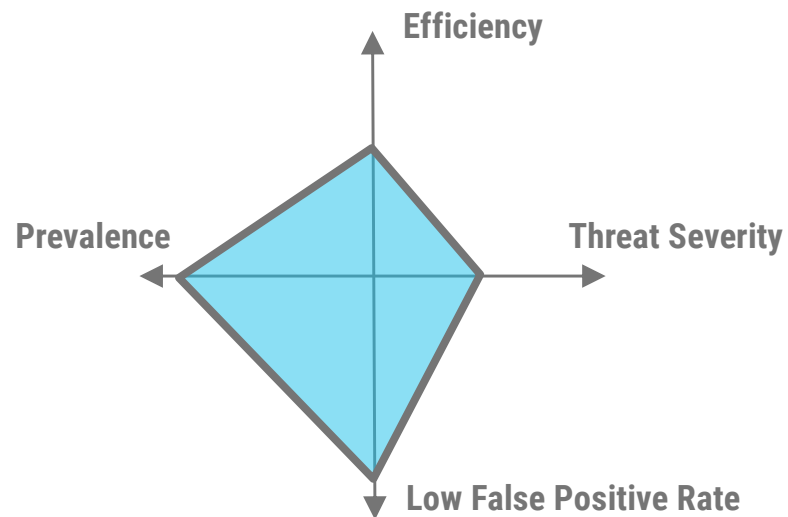
- Search projects:
- pip install attackcti
- ATTACK CTI Library
- Navigation: Project description, Release history, Download files
- Project links: Homepage
- Statistics: GitHub statistics (Stars: 388, Forks: 92), Open issues/PRs: 4
- Project description: ATT&CK Python Client
- Goals: Provide an easy way to access and interact with up to date ATT&CK content available in server, Allow security analysts to quickly explore ATT&CK content and apply it in their daily op, Allow the integration of ATT&CK content with other platforms to host up to date inform, Help security analysts during the transition from the ATT&CK MediaWiki API to the STIX, Learn STIX2 and TAXII Client Python libraries
- Documentation: <https://attackcti.com>



Sigma Hall of Fame

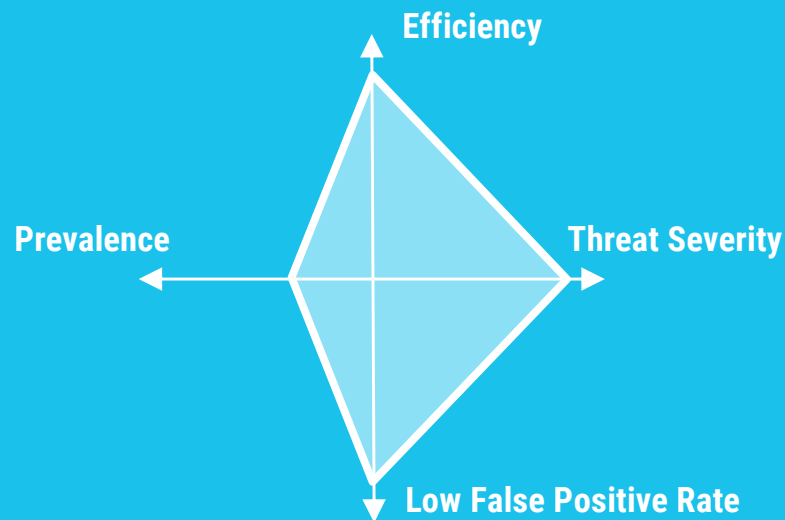
Key Selection Criteria for the Hall of Fame

- Very effective due to generic character
- Low false positive rate
- Detects serious threats
- Detects very common threats



5. Suspicious Whoami Detection

- Stage: Discovery, Privilege Escalation
- Generic privilege escalation detection
- Low false positive rate



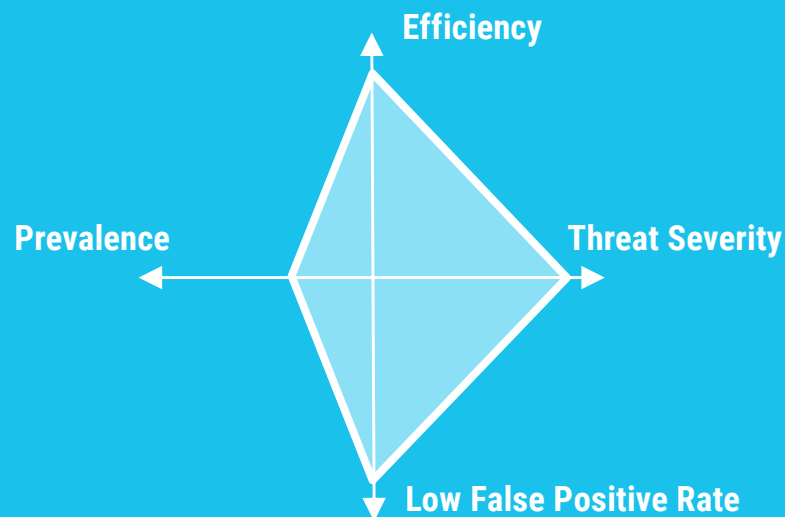
```
win_whoami_as_system.yml × win_susp_whoami_anomaly.yml lnx_back_connect_shell_

1  title: Run Whoami as SYSTEM
2  id: 80167ada-7a12-41ed-b8e9-aa47195c66a1
3  status: experimental
4  description: Detects a whoami.exe executed by LOCAL SYSTEM. This may be a
5  sign of a successful local privilege escalation.
6  references:
7  - https://speakerdeck.com/heirhabarov/
8    hunting-for-privilege-escalation-in-windows-environment
9  author: Teymur Kheirkhabarov
10 date: 2019/10/23
11 modified: 2021/08/26
12 tags:
13 - attack.privilege_escalation
14 - attack.discovery
15 - attack.t1033
16 logsource:
17 - category: process_creation
18 - product: windows
19 detection:
20 - selection:
21   - User|startswith:
22     - 'NT AUTHORITY\SYSTEM'
23     - 'AUTHORITY NT\Sys' # French language settings
24   - Image|endswith: '\whoami.exe'
25   - condition: selection
26 falsepositives:
27 - Unknown
28 level: high
```

T1033

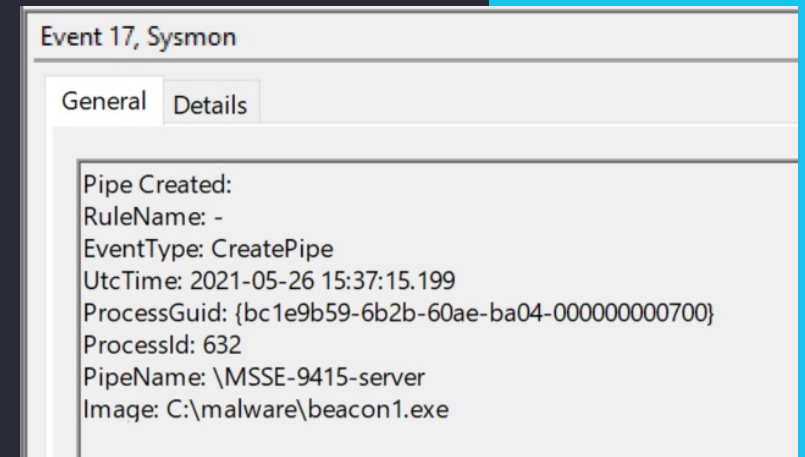
4. CobaltStrike Named Pipe

- Stage: Privilege Escalation, Execution
- No false positives
- Requires Named Pipe Monitoring (Sysmon)



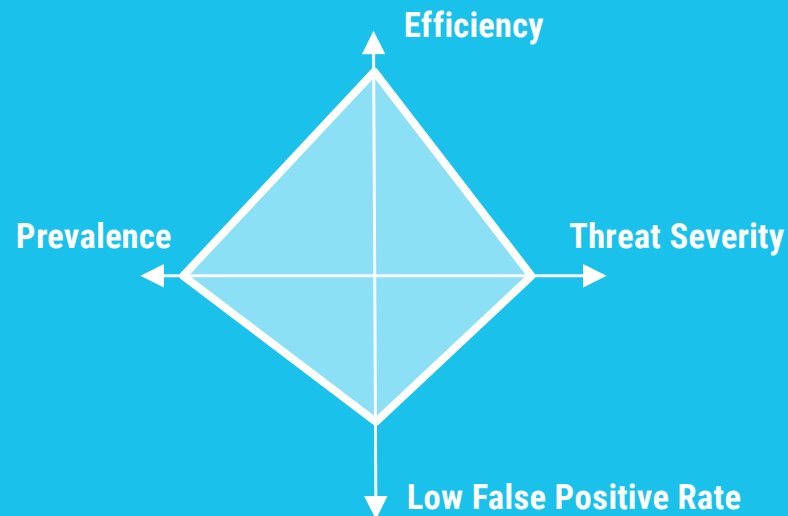
```
sysmon_mal_cobaltstrike.yml •
1  title: CobaltStrike Named Pipe
2  id: d5601f8c-b26f-4ab0-9035-69e11a8d4ad2
3  status: experimental
4  description: Detects the creation of a named pipe as used by CobaltStrike
5  > references: ""
10 date: 2021/05/25
11 author: Florian Roth, Wojciech Lesicki
12 tags:
13   - attack.defense_evasion
14   - attack.privilege_escalation
15   - attack.t1055
16 > logsource: ""
20 detection:
21   selection_MSSE:
22     PipeName|contains|all:
23       - '\MSSE-'
24       - '-server'
25   selection_postex:
26     PipeName|startswith: '\postex_'
27   selection_postex_ssh:
28     PipeName|startswith: '\postex_ssh_'
29   selection_status:
30     PipeName|startswith: '\status_'
31   selection_msagent:
32     PipeName|startswith: '\msagent_'
33   condition: 1 of them
34 falsepositives:
35   - Unknown
36 level: critical
37
```

T1055



3. Shadow Copies Deletion Using Operating System Utilities

- Stage: Impact
- Ransomware detection
- Behavior-based
- Low false positive rates



win_shadow_copies_deletion.yml

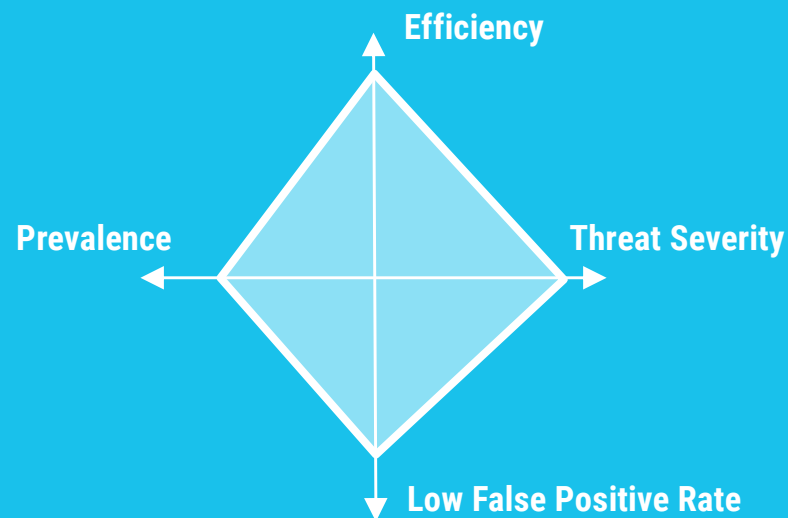
```
1 title: Shadow Copies Deletion Using Operating Systems Utilities
2 id: c947b146-0abc-4c87-9c64-b17e9d7274a2
3 status: stable
4 description: Shadow Copies deletion using operating systems utilities
5 author: Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community, Andreas
6 date: 2019/10/22
7 modified: 2021/06/02
8 > references: ...
16 tags:
17   - attack.defense_evasion
18   - attack.impact
19   - attack.t1070
20   - attack.t1490
21 logsource:
22   category: process_creation
23   product: windows
24 detection:
25   selection1:
26     Image|endswith:
27       - '\powershell.exe'
28       - '\wmic.exe'
29       - '\vssadmin.exe'
30       - '\diskshadow.exe'
31     CommandLine|contains|all:
32       - shadow # will match "delete shadows" and
33       - delete
34   selection2:
35     Image|endswith:
36       - '\wbadmin.exe'
37     CommandLine|contains|all:
38       - delete
39       - catalog
40       - quiet # will match -quiet or /quiet
41   condition: 1 of selection*
```

T1070, T1490



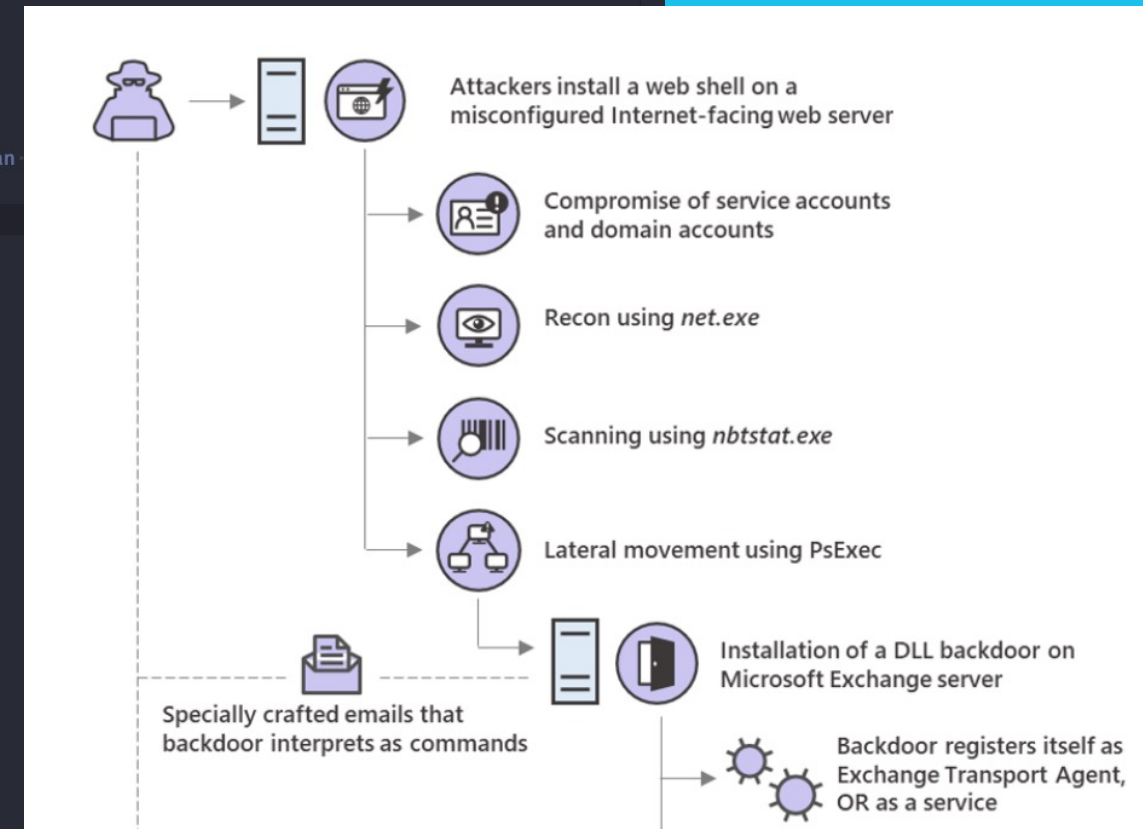
2. Webshell Detection With Command Line Keywords

- Stage: Persistence
- Solid web shell detection
- Behavior-based
- Reasonably low false positive rates (easy to filter)



```
win_webshell_detection.yml X
1 title: Webshell Detection With Command Line Keywords
2 id: bed2a484-9348-4143-8a8a-b801c979301c
3 description: Detects certain command line parameters often used during reconnaissance
  activity via web shells
4 author: Florian Roth, Jonhnathan Ribeiro, Anton Kutepov, oscd.community
5 > references: ...
8 date: 2017/01/01
9 modified: 2021/03/02
10 tags:
11 - attack.persistence
12 - attack.t1505.003
13 - attack.t1018
14 - attack.t1033
15 - attack.t1087
16 - attack.privilege_escalation # an
17 - attack.t1100 # an old one
18 > logsource: ...
21 detection:
22 - parent_is_web_server_process:
23 - ParentImage|endswith:
24 - '\w3wp.exe'
25 - '\php-cgi.exe'
26 - '\nginx.exe'
27 - '\httpd.exe'
28 - ParentImage|contains:
29 - '\apache'
30 - '\tomcat'
31 - net_utility:
32 - Image|endswith:
33 - '\net.exe'
34 - '\net1.exe'
35 - CommandLine|contains:
36 - 'user '
37 - 'use '
38 - 'group '
39 - ping_utility:
40 - Image|endswith: '\ping.exe'
41 - CommandLine|contains: '-n '
42 - change_dir:
43 - CommandLine|contains:
```

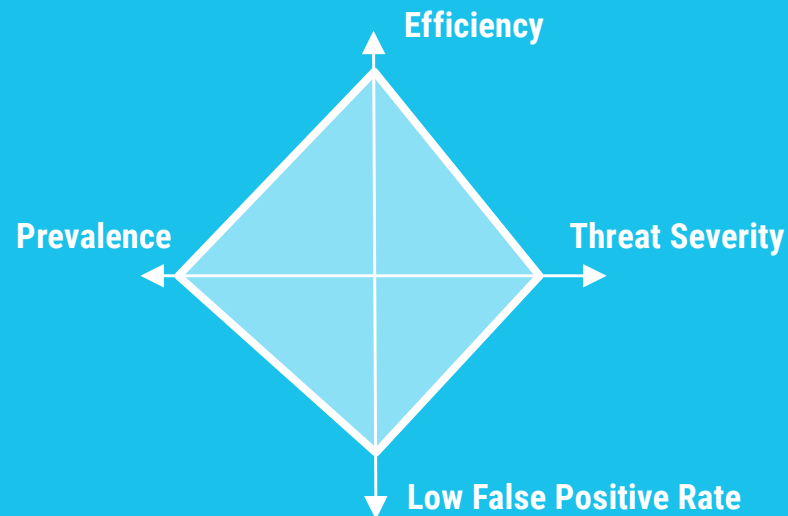
T1505.003



<https://www.microsoft.com/security/blog/2020/02/04/ghost-in-the-shell-investigating-web-shell-attacks/>

1. Microsoft Office Product Spawning Windows Shell

- Stage: Initial Access
- Found in most phishing attacks
- Very stable
- Low false positive rate



```
win_office_shell.yml •
title: Microsoft Office Product Spawning Windows Shell
id: 438025f9-5856-4663-83f7-52f878a70a50
description: Detects a Windows command line executable started from Micro
references:
  - https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html
tags:
  - attack.execution
  - attack.t1059
author: Michael Haag, Florian Roth, Markus Neis
date: 2018/04/06
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    ParentImage:
      - '*\WINWORD.EXE'
      - '*\EXCEL.EXE'
      - '*\POWERPNT.exe'
    Image:
      - '*\cmd.exe'
      - '*\powershell.exe'
      - '*\wscript.exe'
      - '*\cscript.exe'
  condition: selection
falsepositives:
  - Unlikely
level: high
```

T1059

Malicious activity

Dokumentation.xls

MD5: 65CDFC2467F09A971B398B97AAD487A6

Start: 14.05.2020, 14:54 Total time: 60 s

macros macros40 ta505

Indicators:

Get sample IOC Restart Export

Text report Processes graph ATT&CK™ matrix

CPU RAM

PROCESS Filter by name or PID Show only important

2104 EXCELEXE /dde 1k 1k 93

3280 powershell.exe -command IEX (new'-OB'jeCT('Net.WebClient'))... 1k 266 206

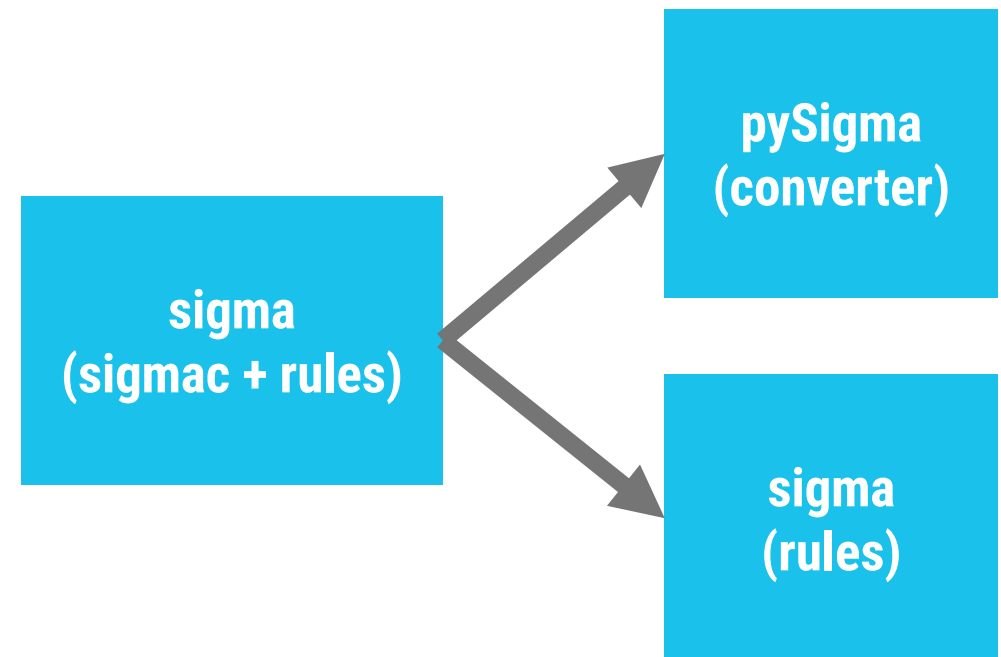
A large, stylized, light blue letter 'O' that serves as a background element for the slide. It is positioned on the right side, with its left edge partially overlapping the text area.

Upcoming Sigma Project Changes

- The new converter uses this module
- Complete rewrite of the old converter
- Support for the new Sigma correlation rules
- New backends should be built with with this module
- All credits go to Thomas @blubbfiction

<https://github.com/SigmaHQ/pySigma>

pySigma

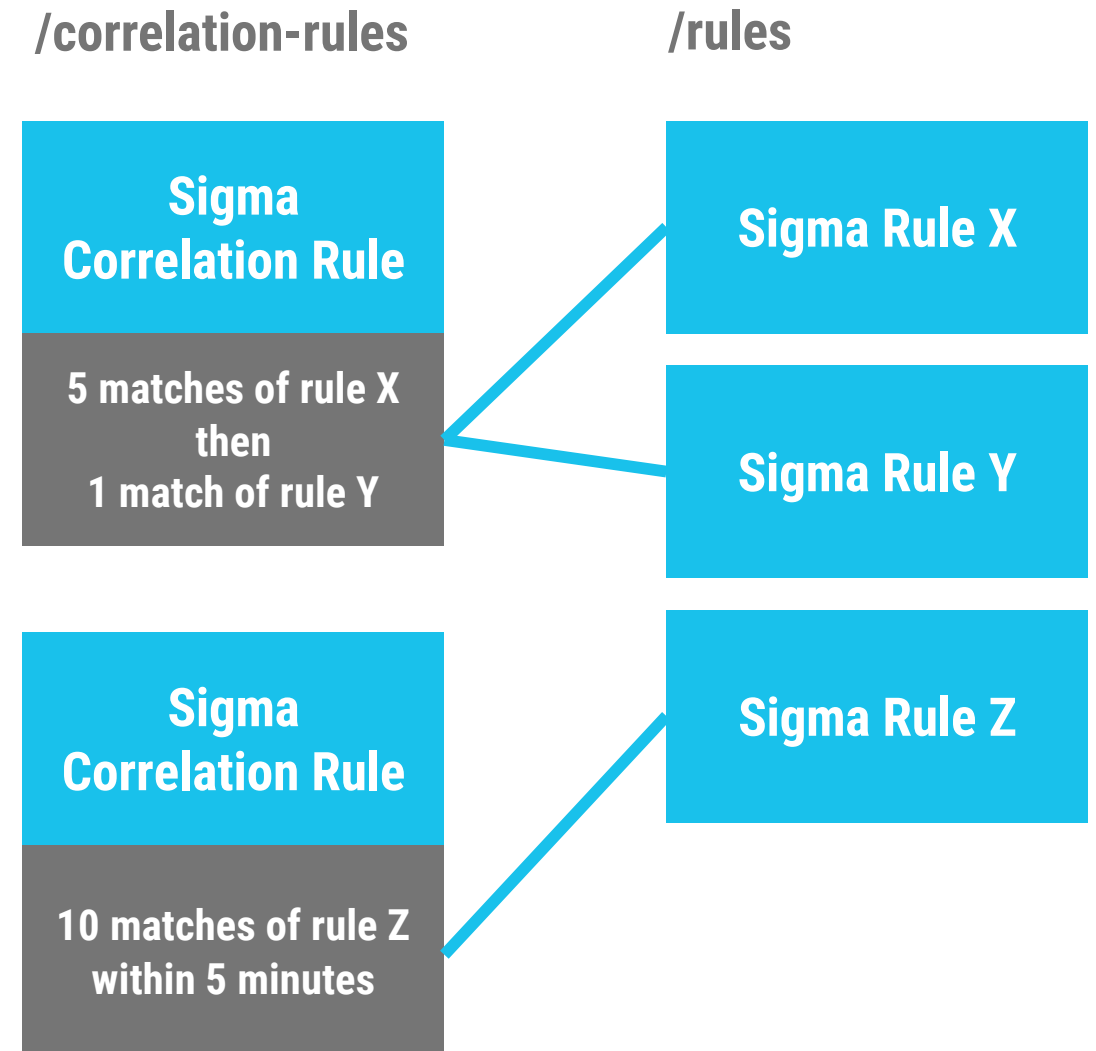


Sigma Correlation Rules

- Correlation rules provide an easy to use solution to complex detection ideas
- Time-based, statistical or sequential correlations
- Correlation rules refer to simple rules (different files)
- The old converter will not support the new correlation rules (> new pySigma)

Draft (already partly outdated)

<https://onedrive.live.com/view.aspx?resid=3454E59DF98D7D65!7485&ithint=file%2cdocx&authkey=!ADb97TgRX9Fr4xQ>



A large, stylized blue letter 'S' that serves as a background logo for the slide. It is positioned on the right side of the image, with its top and bottom curves extending towards the right edge.

**Cool new or
upcoming
projects / tools
that use Sigma**

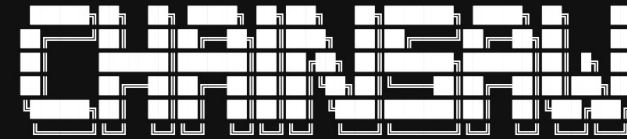
F-Secure: Chainsaw

- Applies Sigma rules on EVTX files
- Digital Forensics Incident Response (DFIR) Use Cases
 - Forensic investigations
 - Collect EVTX files from end points and scan them in the lab
- Rust based – precompiled executables for Windows and Linux
- GPL

<https://labs.f-secure.com/tools/chainsaw/>

Usage Example #1 - Hunting

```
-> % ./chainsaw hunt ./samples --rules ./rules/sigma_rules --mapping ./mapping_files/sigma-mapping.yml --json detections.json
```



By F-Secure Countercept (Author: @FranticTyping)

```
[+] Found 20 EVTX files
[+] Loaded 726 detection rules (72 could not be converted)
[+] Printing results to screen
[+] Saving results to: detections.json
[+] Hunting: [=====] 20/20
```

```
[+] Detection: (Built-in Logic) - Security audit log was cleared
```

system_time	id	computer	subject_user
2019-05-03 15:20:20	1102	"SANS-TBT570"	"student"

```
[+] Detection: (External Rule) - Suspicious Service Installed
```

system_time	id	detection_rules	computer_name	Event.EventData.ImagePath	service_name
2016-08-18 20:40:21	7045	▶ Mimikatz Command Line ▶ FromBase64String Command	"IE10Win7"	%COMSPEC% /b /c start /b /min powershell .exe -nop -w hidden -c if([IntPtr]::Size ...	SYyGmEHvgf

Key Features

Chainsaw provides a range of searching and hunting features which aims to help threat hunters and incident response teams detect suspicious event log entries to aid in their investigations. The key features include:

- + Search through event logs by event ID, keyword, and regex patterns
- + Extraction and parsing of Windows Defender, F-Secure, Sophos, and Kaspersky AV alerts
- + Detection of key event logs being cleared, or the event log service being stopped
- + Users being created or added to sensitive user groups
- + Brute-force of local user accounts
- + RDP logins, network logins etc.
- + Sigma rule detection against a wide variety of Windows event IDs, including:

Zircolite by @waggabat

- Applies Sigma rules on EVTX files
- Digital Forensics Incident Response (DFIR) Use Cases
 - Forensic investigations
 - Collect EVTX files from end points and scan them in the lab
- Python-based
- LGPL

<https://github.com/wagga40/Zircolite>



Battle-tested, standalone and fast SIGMA-based detection tool for EVTX or JSON

```
python 3.8 Platform Win Platform Lin Platform Mac Architecture 64bit
bash-5.1$ python3 zircolite.py --evtx samples.evtx --ruleset rules/rules_windows_sysmon.json

ZIRCOLITE

[+] Checking prerequisites
[+] Extracting EVTX Using 'tmp-00M17500' directory
100%|████████████████████████████████████████████████████████████████████████████████| 1/1 [00:00<00:00, 14.43it/s]
[+] Processing EVTX
100%|████████████████████████████████████████████████████████████████████████████████| 1/1 [00:00<00:00, 1.84it/s]
[+] Creating model
[+] Inserting data
100%|████████████████████████████████████████████████████████████████████████████████| 7346/7346 [00:00<00:00, 14851.92it/s]
[+] Cleaning unused objects
[+] Loading ruleset from : rules/rules_windows_sysmon.json
[+] Executing ruleset - 578 rules
  ↳ Autorun Keys Modification - F2F929C8 - Matches : 17 events
  ↳ Stealthy VSTO Persistence - EEB32A52 - Matches : 14 events
  ↳ Koadic Execution - 0F9F5D47 - Matches : 9 events
  ↳ Whoami Execution - 951021B9 - Matches : 2 events
  ↳ Non Interactive PowerShell - 502D5A86 - Matches : 2 events
  ↳ Scheduled Task Creation - 8A7F536D - Matches : 1 events
  ↳ Local Accounts Discovery - E3BF63F3 - Matches : 2 events
  ↳ MSHSTA Spawning Windows Shell - D7F2B1CB - Matches : 6 events
100%|████████████████████████████████████████████████████████████████████████████████| 578/578 [00:00<00:00, 883.07it/s]
[+] Cleaning

Finished in 1 seconds
bash-5.1$
```

SOC Prime: Uncoder CTI

- Transforms IOCs into Queries
- Online and free (limits apply)
- Support for many different backends: Azure Sentinel, Elastic, Splunk, SentinelOne, Carbon Blac, LogPoint, FireEye Helix, CrowdStrike ... and more

<https://cti.uncoder.io/>

Uncoder CTI

Fast and easy generation of IOC queries tuned for maximum performance. Insert your IOCs, get queries on the fly, and drill down to hunt.

IOCs

18 Hash 0 Domain 0 URL 0 IP

...

Clear

Upload IOCs

1 b67c8752622d53be9f966d66e960745d a2754d7995426b58317e437f8ed6770c

2 d7bb7b18d971e23b2b300b75e34fa086

3 ManageHp.exe

4 94b0cfa3c654f17562a62541238ff6bb b766522dd4189fef7775d663e5649ba9

5 d8be8e03022039d20848fcbc3643e5f2

6 ccmstracer.exe

7 888534c600d4c62d144b42e3e92c941b b54a67062bdcd32dfa9f3d7b69780d2e

8 6e4925777290bc34e8f979a1b4b72ea2

9 PerfWatson.exe

10 e65d76b39a7a48fec2f481e64c82f09f 9511df8a93aade046061b1977633cad5

11 d3c0fe16f00faa63e310b143def20b32

12 SuonMa.exe

13 3e993dfe5ce90dadb0cf0707d260febd 21ab4357262993a042c28c1cdb52b2da

14 b7195a6c30fa8be723631604dd330b29

15 WINVNC.exe

16 e8d3aeea7617982bb6e484a9f8307e6b d3606e2e36db0a0cb1b8168423188ee6

17 6332cae24fe59d63f93f5f53ab7c3029

18 UltraVNC.exe

18 / 50

Clear

Generate

Query Generation Settings

Generate Queries by IOC Types

HASH X

Hash Type

MD5 X

Query Platform

Azure Sentinel

IOC Field Mapping

Default

IOCs per Query

25

Exceptions

☐ Add Source IP to Query with "OR" operator

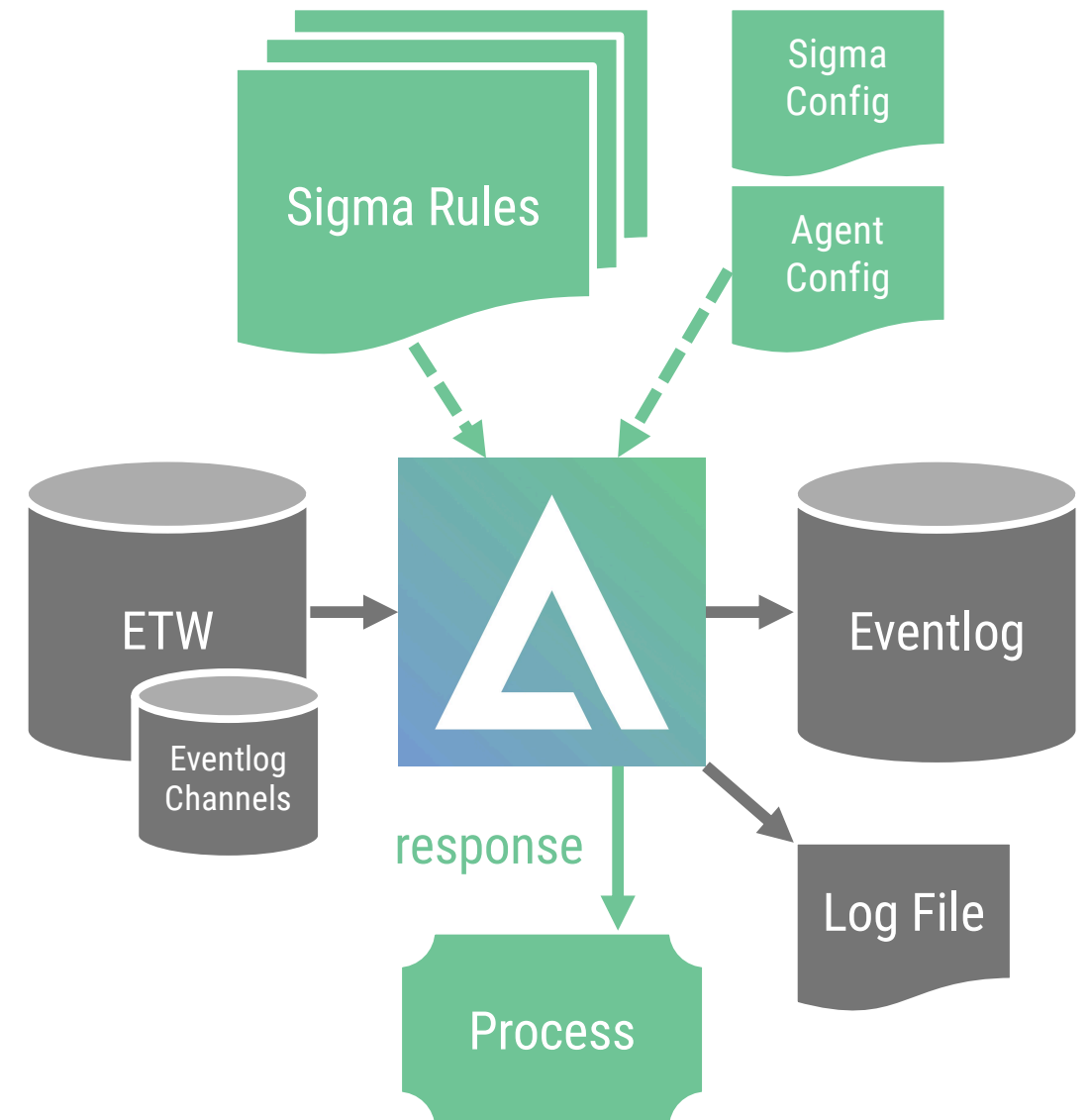
Queries for: Azure Sentinel

1 union * | where (FileHashMd5 =~ 'b67c8752622d53be9f966d66e960745d' or FileHashMd5 =~ 'a2754d7995426b58317e437f8ed6770c' or FileHashMd5 =~ 'd7bb7b18d971e23b2b300b75e34fa086' or FileHashMd5 =~ '94b0cfa3c654f17562a62541238ff6bb' or FileHashMd5 =~ 'b766522dd4189fef7775d663e5649ba9' or FileHashMd5 =~ 'd8be8e03022039d20848fcbc3643e5f2' or FileHashMd5 =~ '888534c600d4c62d144b42e3e92c941b' or FileHashMd5 =~ 'b54a67062bdcd32dfa9f3d7b69780d2e' or FileHashMd5 =~ '6e4925777290bc34e8f979a1b4b72ea2' or FileHashMd5 =~ 'e65d76b39a7a48fec2f481e64c82f09f' or FileHashMd5 =~ '9511df8a93aade046061b1977633cad5' or FileHashMd5 =~ 'd3c0fe16f00faa63e310b143def20b32' or FileHashMd5 =~ '3e993dfe5ce90dadb0cf0707d260febd' or FileHashMd5 =~ '21ab4357262993a042c28c1cdb52b2da' or FileHashMd5 =~ 'b7195a6c30fa8be723631604dd330b29' or FileHashMd5 =~ 'e8d3aeea7617982bb6e484a9f8307e6b' or FileHashMd5 =~ 'd3606e2e36db0a0cb1b8168423188ee6' or FileHashMd5 =~ '6332cae24fe59d63f93f5f53ab7c3029')

Nexttron: Aurora Agent

- Lightweight agent that applies Sigma rules on log data in real-time on endpoints
- Free
(Pro version has additional features)
- Uses ETW
- Supports the upcoming Sigma correlation rules
- Extends the Sigma standard with response actions ⚡
 - Kill, KillParent, Suspend, Dump
 - Custom actions: e.g.
copy %Image% %%ProgramData%%\%ProcessID%.bin
- Consider it your “custom Sigma-based HIPS”

Release: December 2021 🙌



Thanks to all contributors



Contributors 260



+ 249 contributors

Rules: @cyb3rops and frack113

Rule Converter: @blubbfiction Thomas Patzke

Twitter: @sigma_hq

Slack: siemexchange.slack.com (contact us for invites)

More information: <https://github.com/SigmaHQ/sigma>