sigma

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

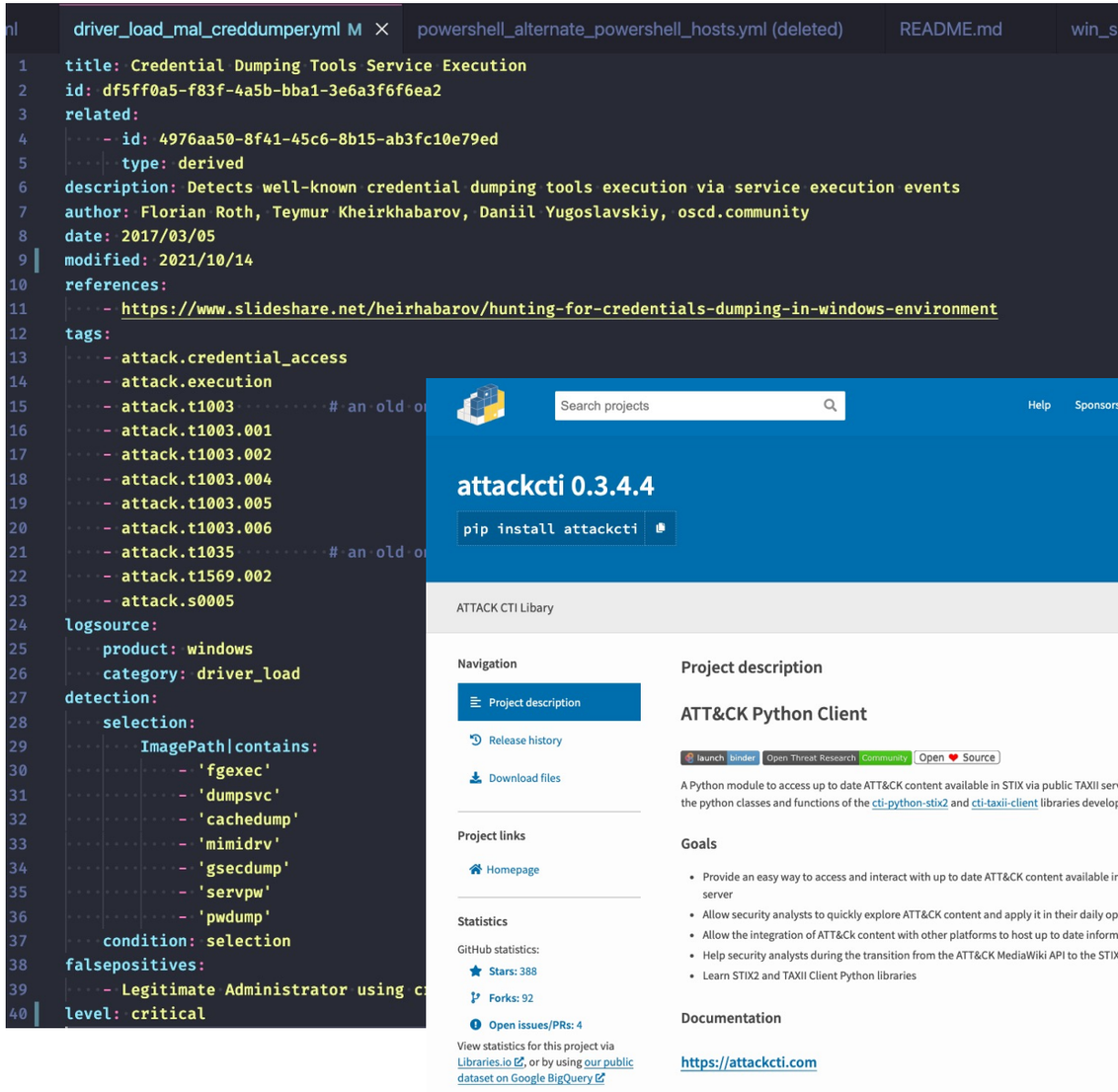
Snort is for **network traffic**.

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

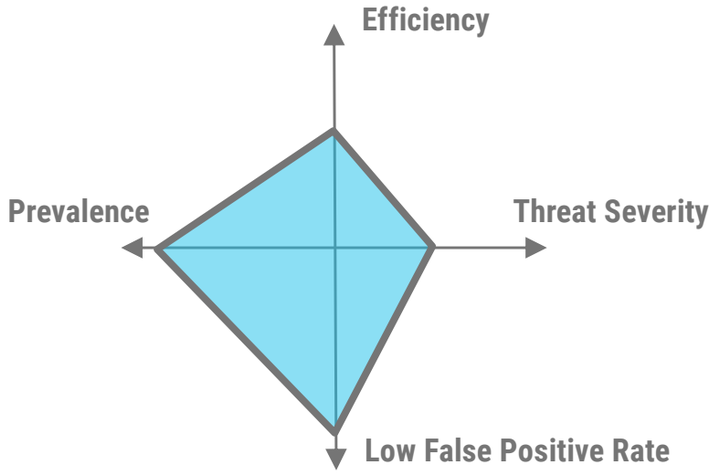
- Sigma rules contain ATT&CK techniques as tags
- A matching rule points to one or more techniques
- The tests check against attackcti.com to compare the tags in new rules with a list of all valid ones (live)



Sigma Hall of Fame

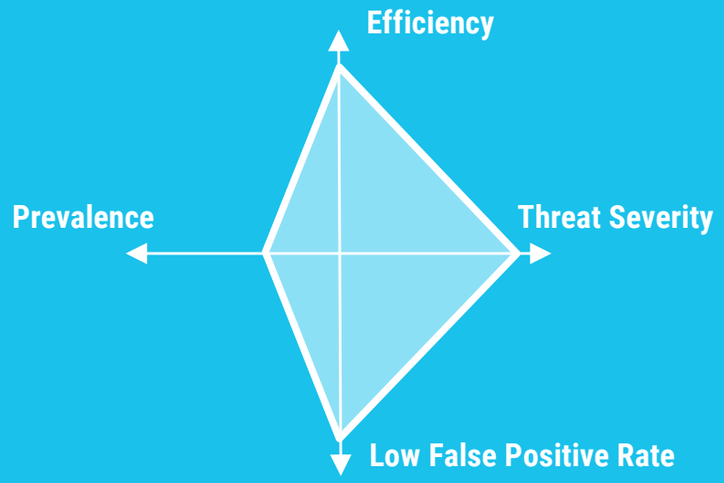
Key Selection Criteria for the Hall of Fame

- 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



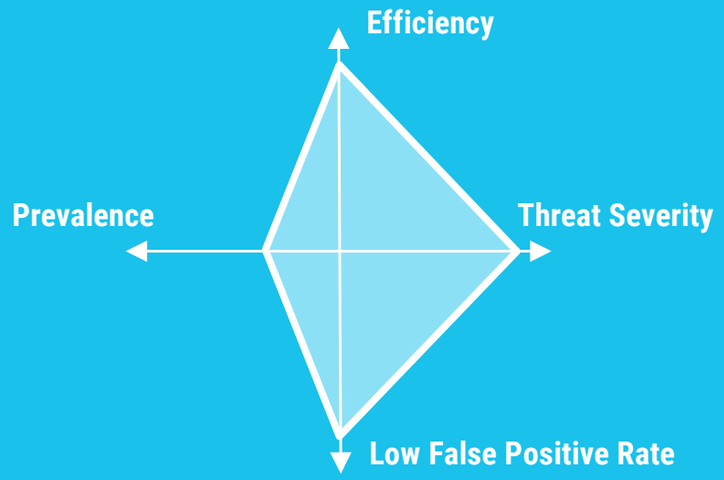
win_whoami_as_system.yml × | win_susp_whoami_anomaly.yml | lnx_back_connect_shell_

```yaml
title: Run Whoami as SYSTEM
id: 80167ada-7a12-41ed-b8e9-aa47195c66a1
status: experimental
description: Detects a whoami.exe executed by LOCAL SYSTEM. This may be a sign of a successful local privilege escalation.
references:
    - https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment
author: Teymur Kheirkhabarov
date: 2019/10/23
modified: 2021/08/26
tags:
    - attack.privilege_escalation
    - attack.discovery
    - attack.t1033
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        User|startswith:
            - 'NT AUTHORITY\SYSTEM'
            - 'AUTORITE NT\Sys' # French language settings
        Image|endswith: '\whoami.exe'
    condition: selection
falsepositives:
    - Unknown
level: high
```

T1033

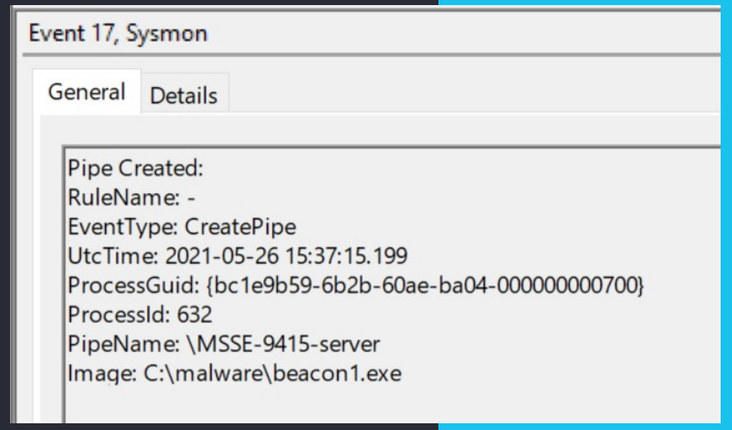
4. CobaltStrike Named Pipe

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



sysmon_mal_cobaltstrike.yml

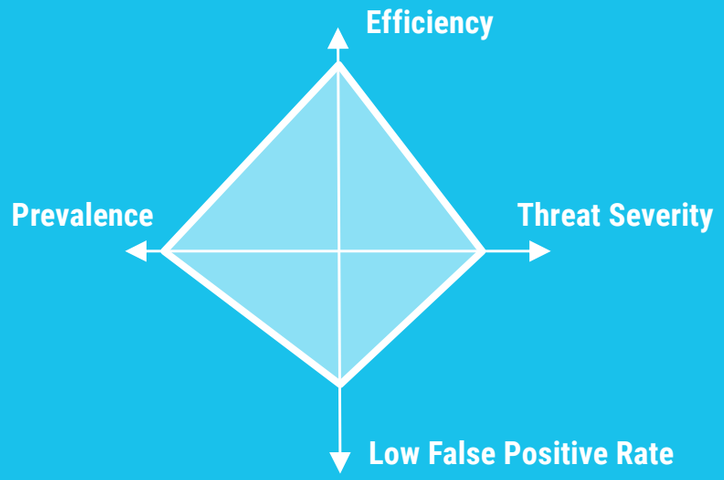
```yaml
title: CobaltStrike Named Pipe
id: d5601f8c-b26f-4ab0-9035-69e11a8d4ad2
status: experimental
description: Detects the creation of a named pipe as used by CobaltStrike
references: ...
date: 2021/05/25
author: Florian Roth, Wojciech Lesicki
tags:
    - attack.defense_evasion
    - attack.privilege_escalation
    - attack.t1055
logsource: ...
detection:
    selection_MSSE:
        PipeName|contains|all:
            - '\MSSE-'
            - '-server'
    selection_postex:
        PipeName|startswith: '\postex_'
    selection_postex_ssh:
        PipeName|startswith: '\postex_ssh_'
    selection_status:
        PipeName|startswith: '\status_'
    selection_msagent:
        PipeName|startswith: '\msagent_'
    condition: 1 of them
falsepositives:
    - Unknown
level: critical
```



T1055

3. Shadow Copies Deletion Using Operating System Utilities

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



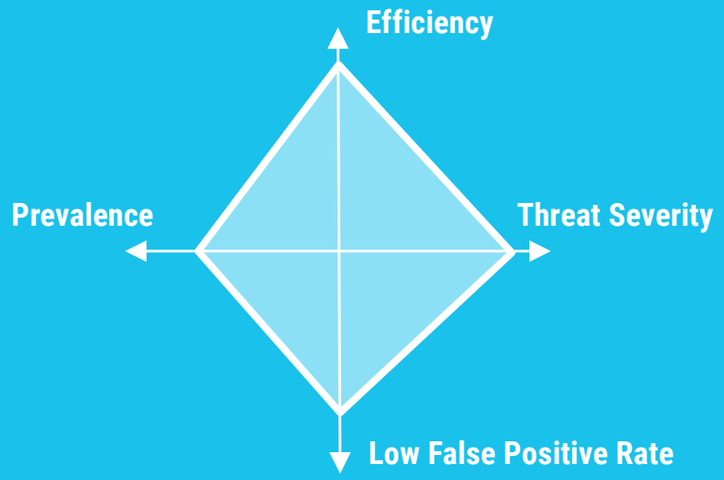
T1070, T1490

win_shadow_copies_deletion.yml

```yaml
title: Shadow Copies Deletion Using Operating Systems Utilities
id: c947b146-0abc-4c87-9c64-b17e9d7274a2
status: stable
description: Shadow Copies deletion using operating systems utilities
author: Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community, Andreas Hunkeler (@Karneades)
date: 2019/10/22
modified: 2021/06/02
references: …
tags:
    - attack.defense_evasion
    - attack.impact
    - attack.t1070
    - attack.t1490
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        Image|endswith:
            - '\powershell.exe'
            - '\wmic.exe'
            - '\vssadmin.exe'
            - '\diskshadow.exe'
        CommandLine|contains|all:
            - shadow  # will match "delete shadows" and '
            - delete
    selection2:
        Image|endswith:
            - '\wbadmin.exe'
        CommandLine|contains|all:
            - delete
            - catalog
            - quiet # will match -quiet or /quiet
    condition: 1 of selection*
```

2. Webshell Detection With Command Line Keywords

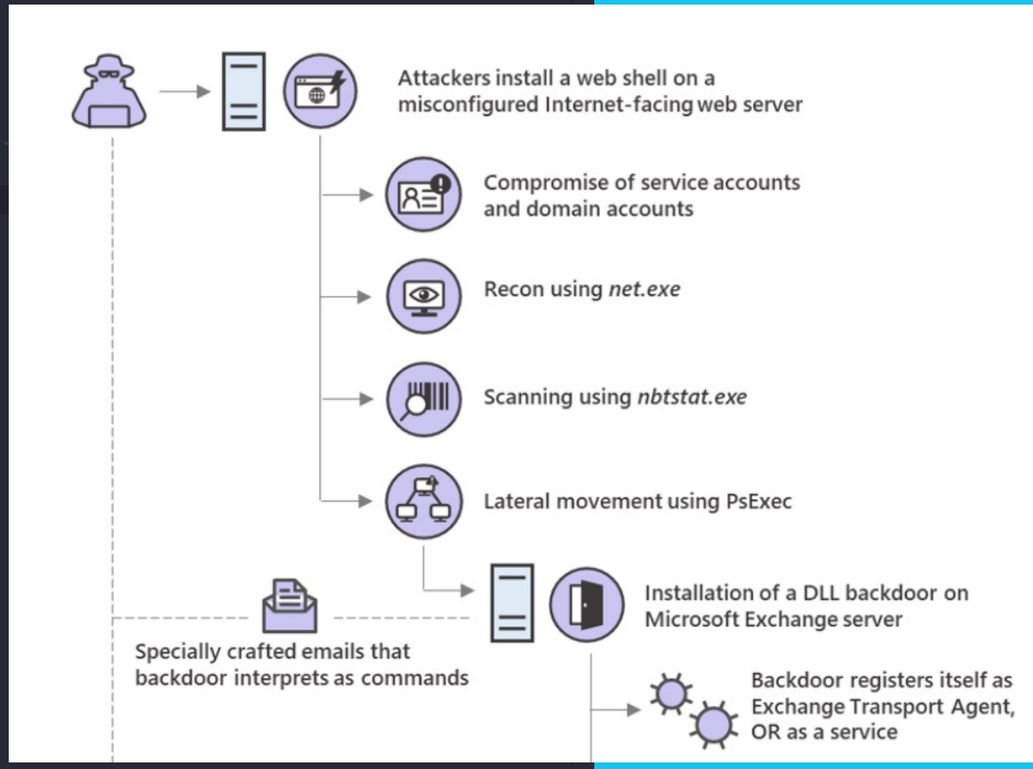
- Stage: Persistence
- Solid web shell detection
- Behavior-based
- Reasonably low false positive rates (easy to filter)



win_webshell_detection.yml

```yaml
title: Webshell Detection With Command Line Keywords
id: bed2a484-9348-4143-8a8a-b801c979301c
description: Detects certain command line parameters often used during reconnaissance activity via web shells
author: Florian Roth, Jonhnathan Ribeiro, Anton Kutepov, oscd.community
references: …
date: 2017/01/01
modified: 2021/03/02
tags:
    - attack.persistence
    - attack.t1505.003
    - attack.t1018
    - attack.t1033
    - attack.t1087
    - attack.privilege_escalation      # an
    - attack.t1100      # an old one
logsource: …
detection:
    parent_is_web_server_process:
        - ParentImage|endswith:
            - '\w3wp.exe'
            - '\php-cgi.exe'
            - '\nginx.exe'
            - '\httpd.exe'
        - ParentImage|contains:
            - '\apache'
            - '\tomcat'
    net_utility:
        Image|endswith:
            - '\net.exe'
            - '\net1.exe'
        CommandLine|contains:
            - ' user '
            - ' use '
            - ' group '
    ping_utility:
        Image|endswith: '\ping.exe'
        CommandLine|contains: ' -n '
    change_dir:
        CommandLine|contains:
```

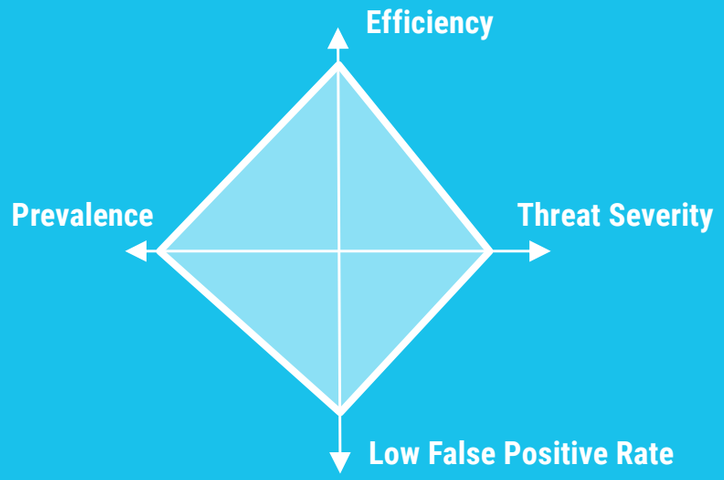
T1505.003



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

1. Microsoft Office Product Spawning Windows Shell

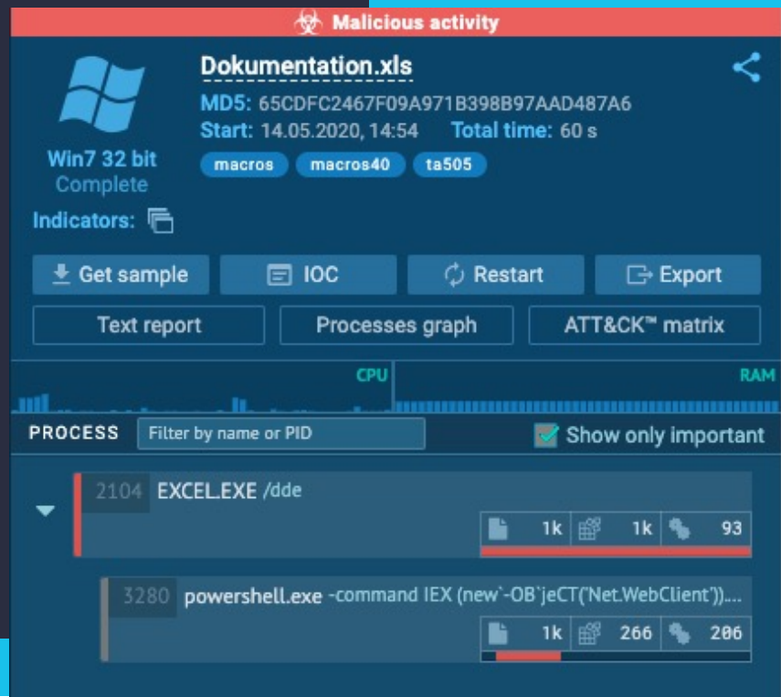
- Stage: Initial Access
- Found in most phishing attacks
- Very stable
- Low false positive rate



win_office_shell.yml

```yaml
title: Microsoft Office Product Spawning Windows Shell
id: 438025f9-5856-4663-83f7-52f878a70a50
description: Detects a Windows command line executable started from Micros
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



https://app.any.run/tasks/b35cc0bc-1493-44bb-a1d8-49b68f92fade/

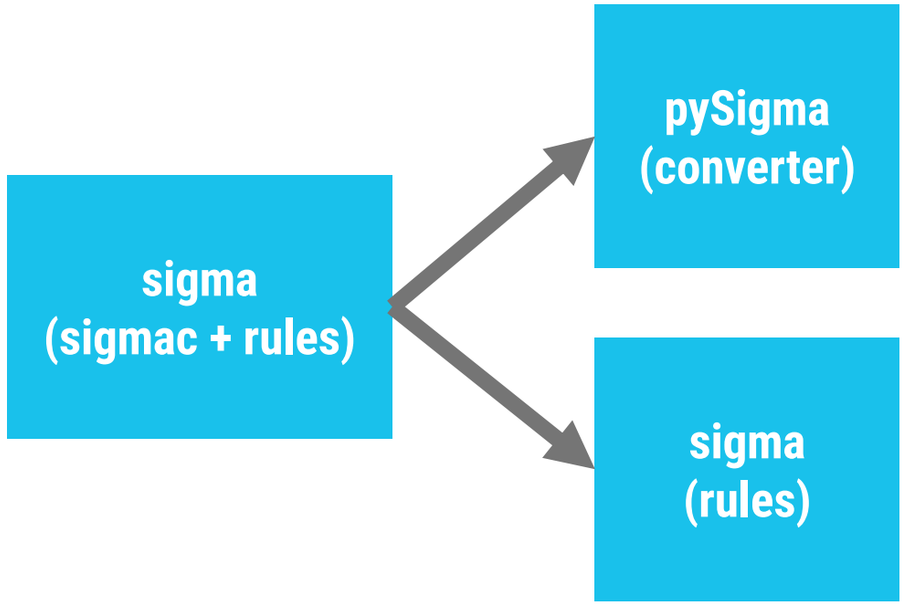
Upcoming Sigma Project Changes

pySigma

- 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

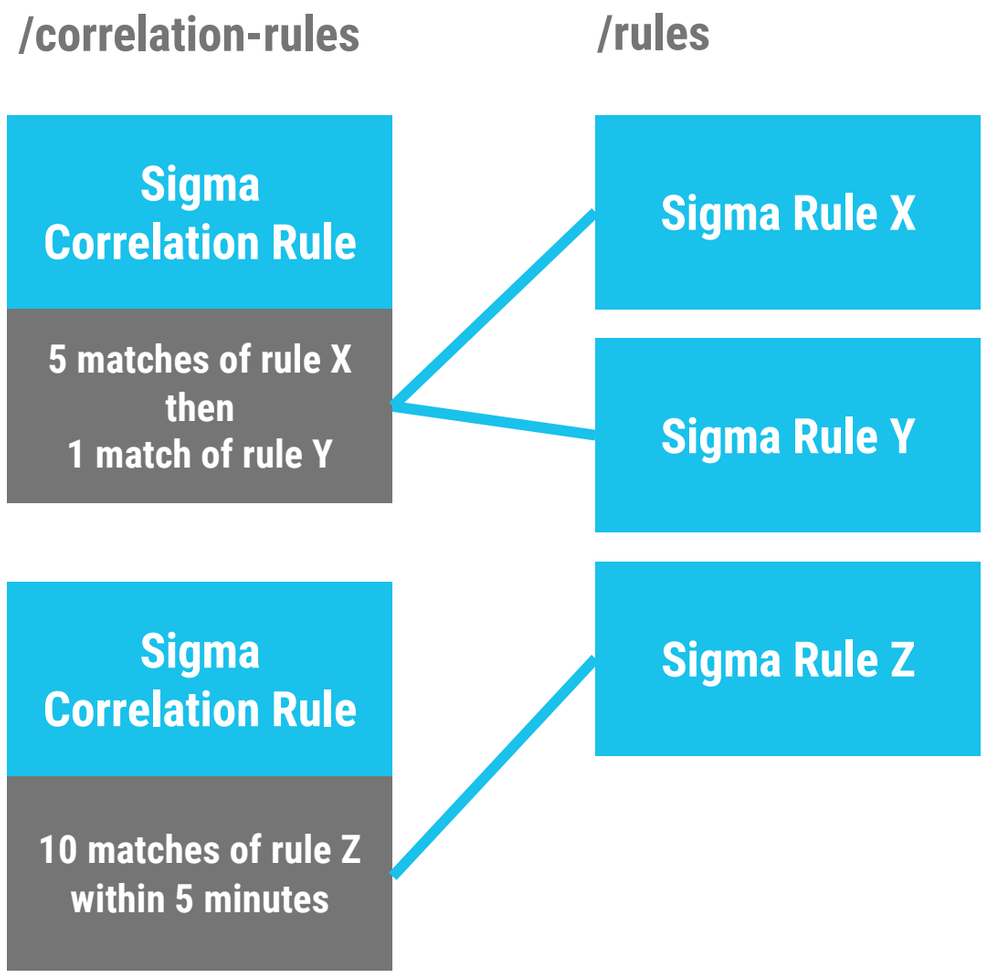


Sigma Correlation Rules

- 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

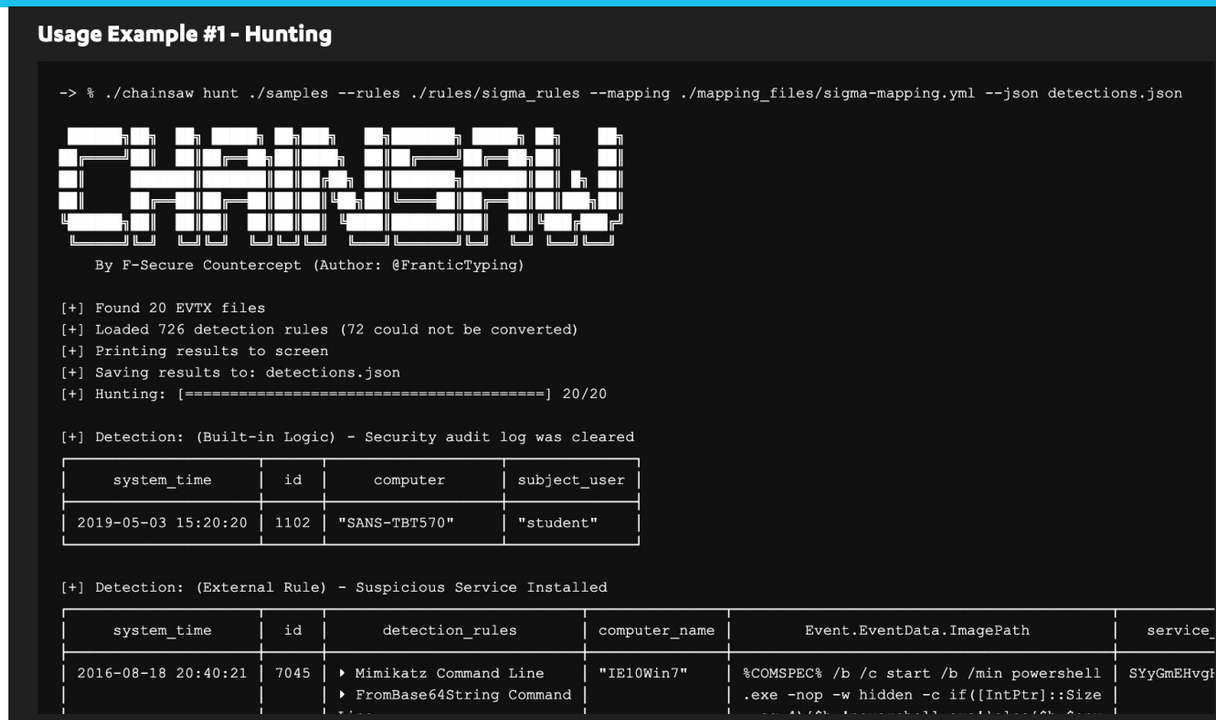


Cool new or upcoming projects / tools that use Sigma

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/



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

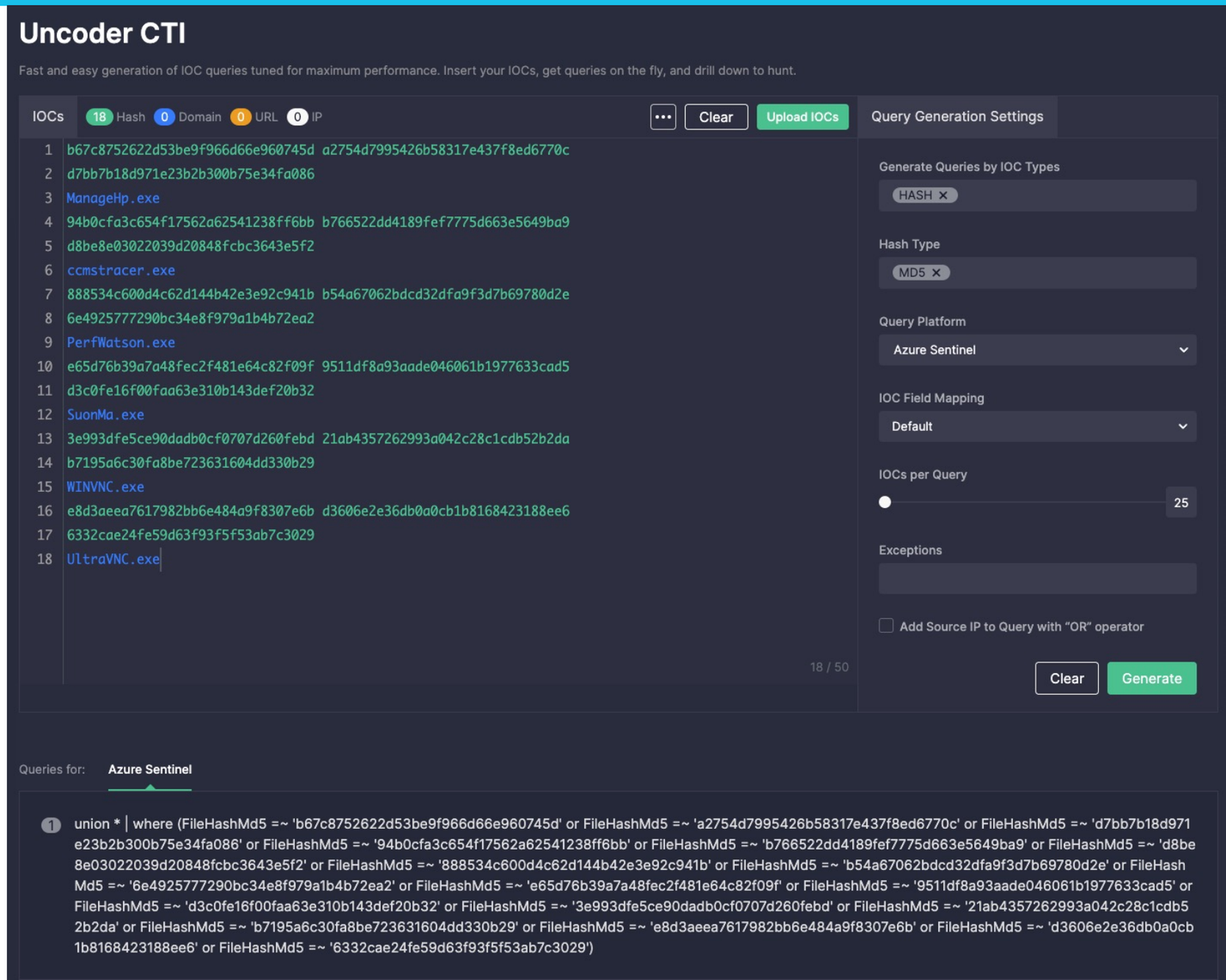
- Applies Sigma rules on EVTX files
- Digital Forensics Incident Response (DFIR) Use Cases
  - Forensic investigations
  - Collect EVTX files from end points and scan them in the lab
- Python-based
- LGPL

https://github.com/wagga40/Zircolite

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

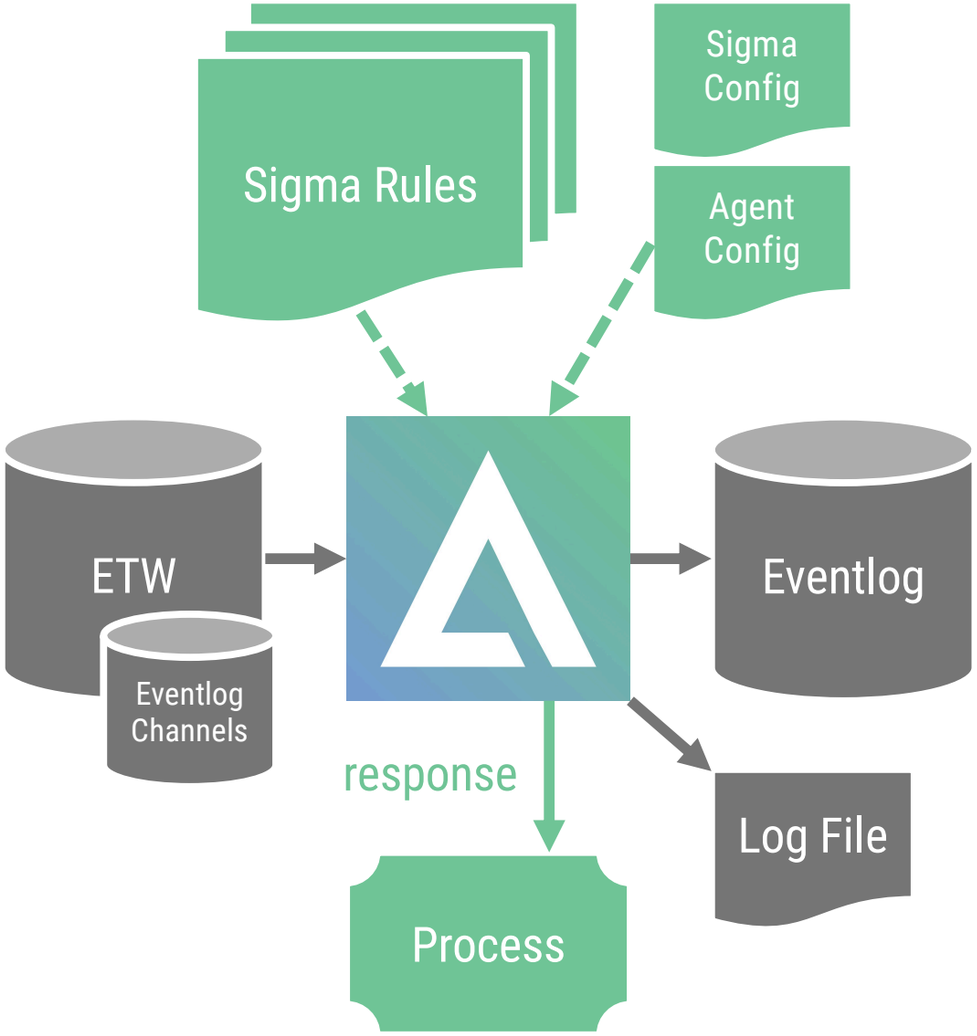
https://cti.uncoder.io/



Nextron: 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

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