Practical Detections w/ Sigma

Presented By:
Tyler Casey

Whoami

Lead Detection Engineer & Deputy of SCYTHE Labs

- Blue Teamer
- DCO Analyst
- Threat Hunter
- Incident Responder

@1qazCasey

/tyler-j-casey

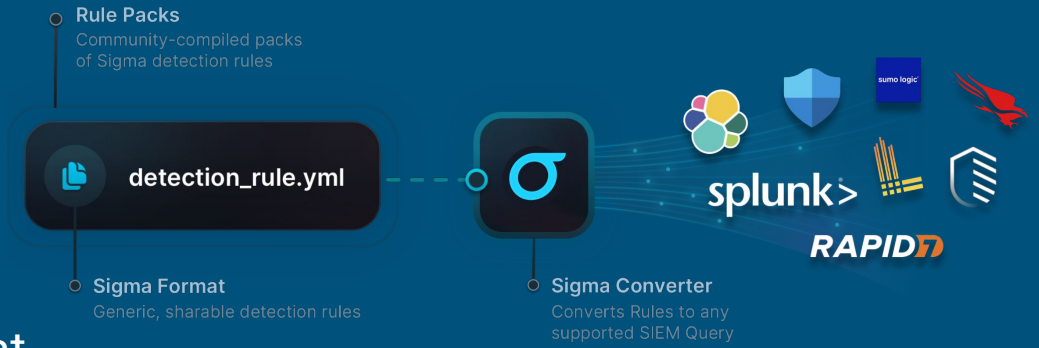
Table of *contents*

01

Sigma

"The shareable detection format for security professionals."

- SigmaHQ



https://sigmahq.io/

Detection Sharing
What It Was (is)

SIEM (Tool) Specific

Manually translate
Non-standard format

Silo

Limited sharing means:
Never leaves organization
Never leaves Notepad

Detection Sharing
What It ~~Could~~ Should Be

Centralized Repo

SigmaHQ Github
Internal Repository

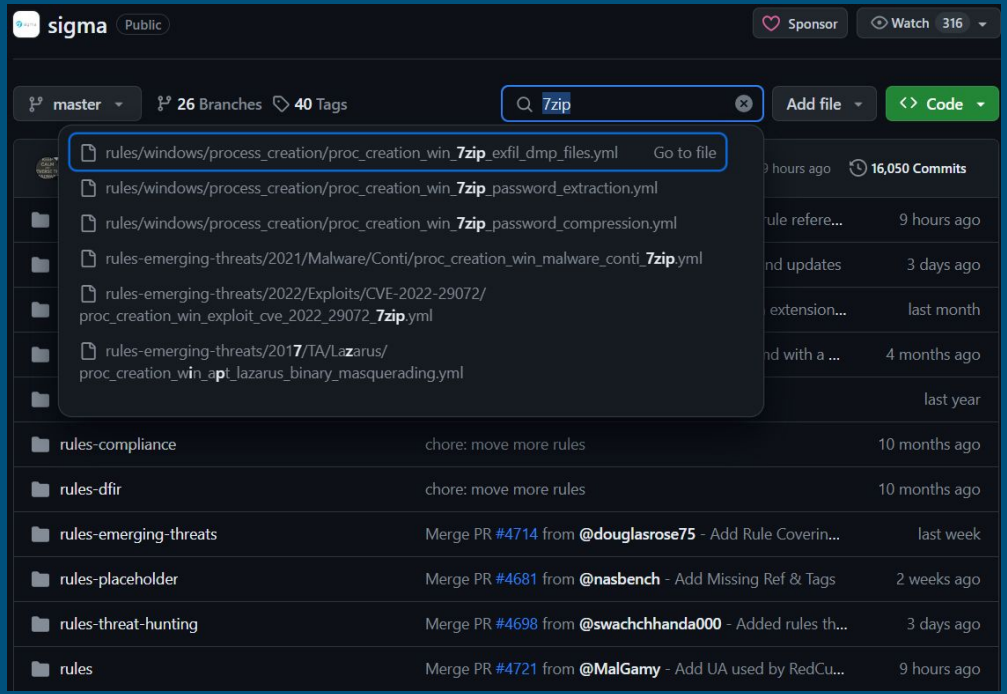
Standard Format

Shareable
Repeatable

Tool Agnostic

Splunk
Elastic Stack
CrowdStrike EDR
Microsoft Sentinel

Sigma HQ



https://github.com/SigmaHQ/sigma
https://detection.fyi

02

Rules 101

Create it, Standardize it, Read it

PowerShell - IWR

```yaml
title: Potential DLL File Download Via PowerShell Invoke-WebRequest
id: 0f0450f3-8b47-441e-a31b-15a91dc243e2
status: test
description: Detects potential DLL files being downloaded using the PowerShell Invoke-WebRequest cmdlet
references:
    - https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution
author: Florian Roth (Nextron Systems), Hieu Tran
date: 2023/03/13
tags:
    - attack.command_and_control
    - attack.execution
    - attack.t1059.001
    - attack.t1105
logsource:
    product: windows
    category: process_creation
detection:
    selection:
        CommandLine|contains:
            - 'Invoke-WebRequest '
            - 'IWR '
        CommandLine|contains|all:
            - 'http'
            - 'OutFile'
            - '.dll'
    condition: selection
falsepositives:
    - Unknown
level: medium
```

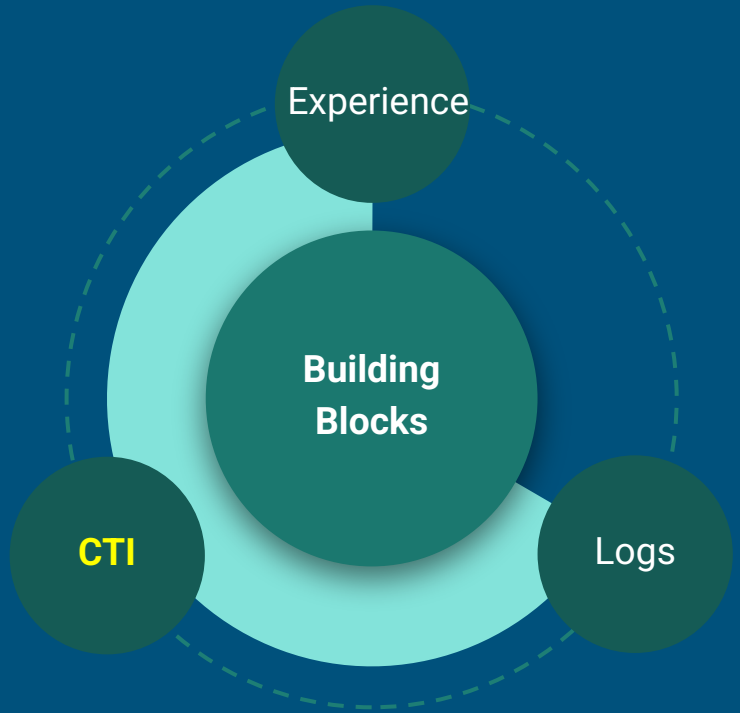
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_powershell_download_dll.yml

Indicator Sources

Enable Automatic Logon

Registry Key	Value	Data
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultUserName	<username>
	DefaultDomainName	<domain name>
	DefaultPassword	<password>

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

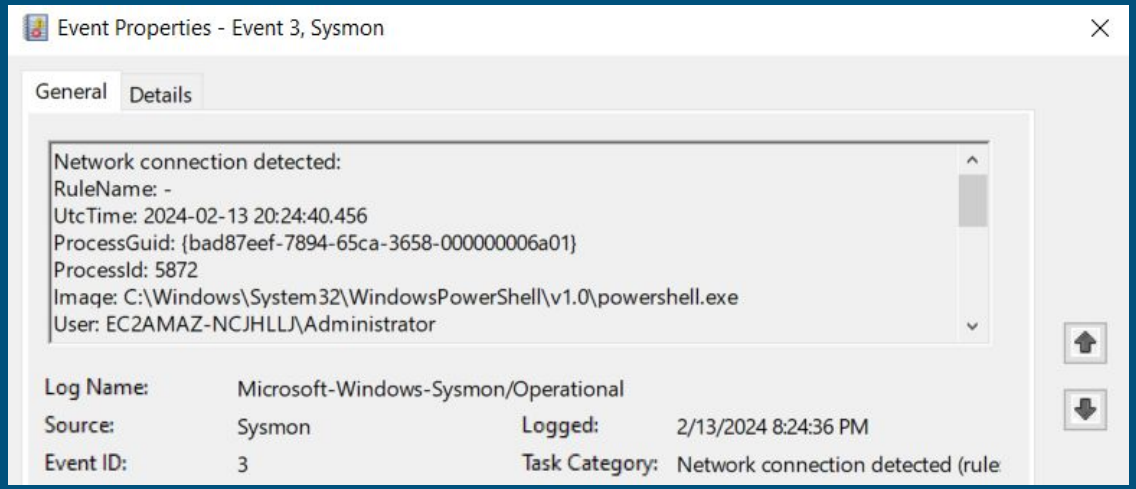


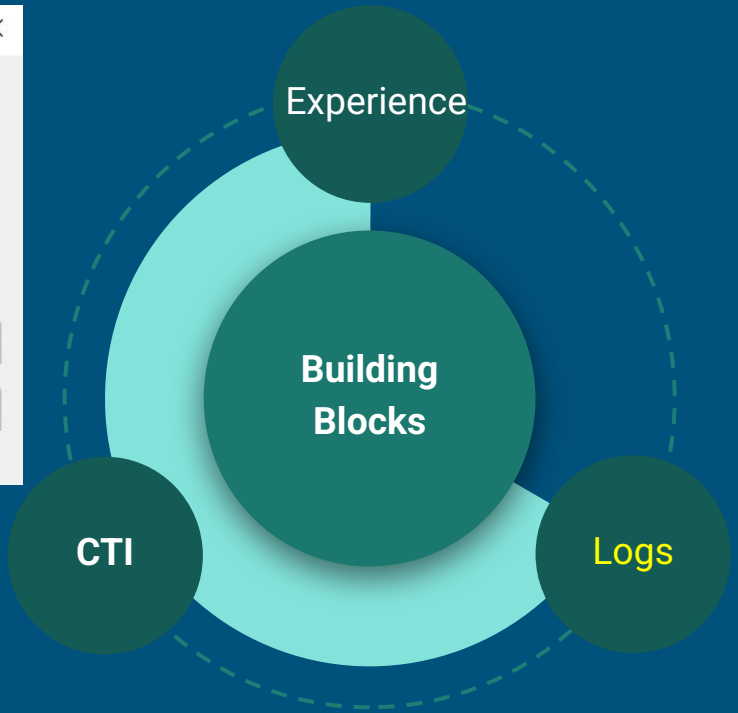
Where Can I Find “Quality”CTI?

- CISA Alerts & Advisories
- DFIR Report
- Google T.A.G
- Infosecn1nja Start.me
- MITRE ATT&CK
- Unit 42

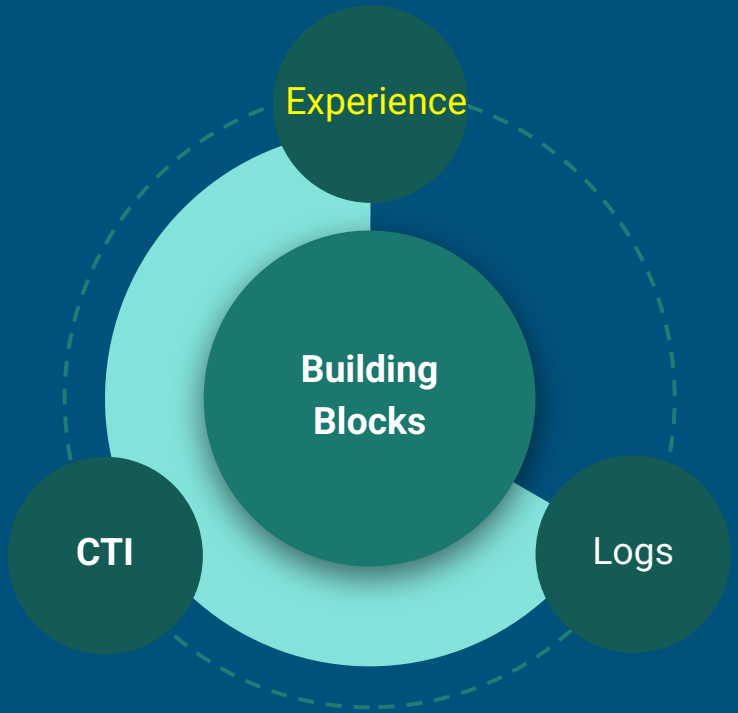
https://start.me/p/wMrA5z/cyber-threat-intelligence

Indicator Sources





Indicator Sources



Sigma Fields

title

Short title of what you are making this detection for, do not use the word "detects"

id

Unique ID, uncoder.io / sigconverter will generate one for you

status

Experimental, until tested

description

Detail what the rule is looking for, start with "Detects ..."

references

List references

author

Separate by comma
Can also put @handle

Sigma Fields

date

Date of rule creation
Also a modified date field

*tags

ATT&CK, CAR, CVE, TLP

*logsource

Annotate where the logs are coming from

*detection

Use selections and conditions to detect

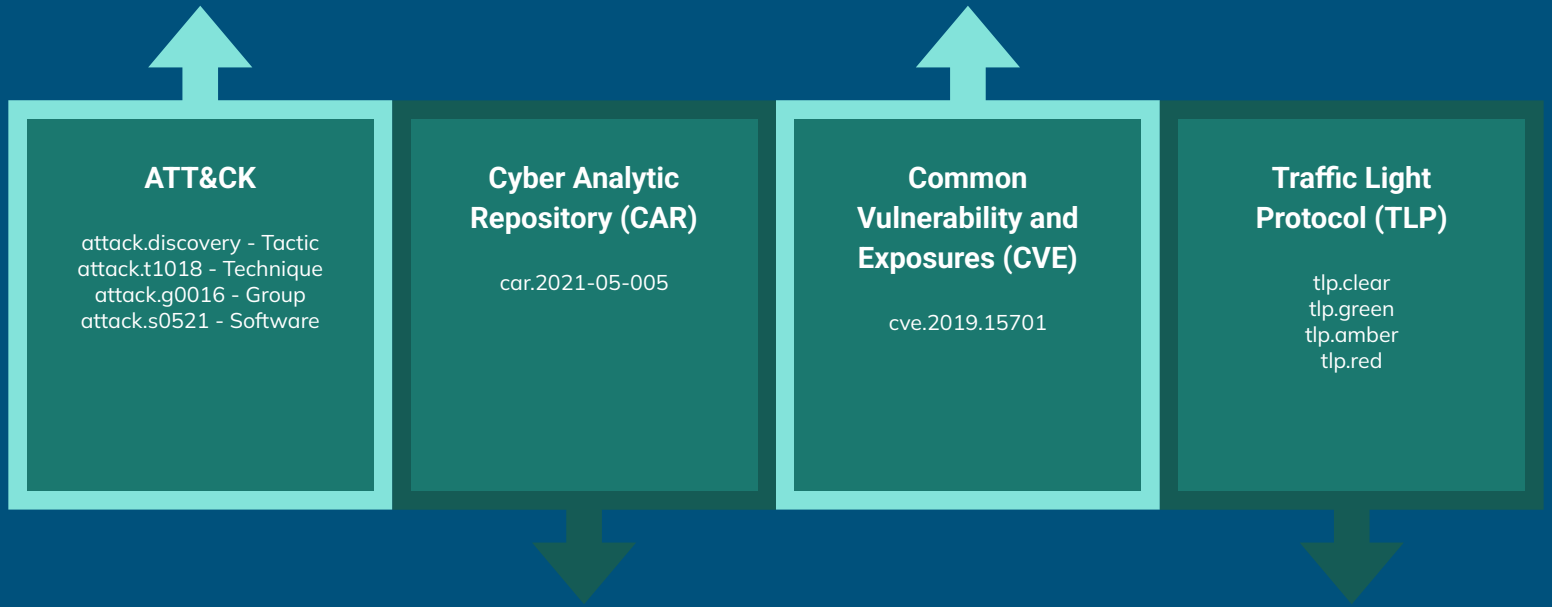
falsepositives

Why might this detection create false positives?

level

Level of this alert: info, low, medium, high, critical

Standards: Tags



https://github.com/SigmaHQ/sigma-specification/blob/main/specification/sigma-appendix-tags.md

Standards: Logsource

Product:
- windows
- zeek
- aws

Category:
- process_creation
- network_connection
- registry_add

Service:
- http
- wmi
- cloudtrail

```
logsource:
    product: windows
    category: process_creation
```

```
logsource:
    product: linux
    service: guacamole
```

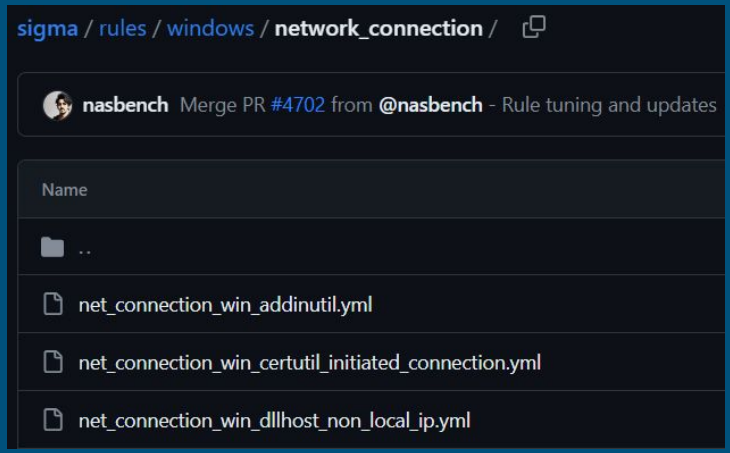
```
logsource:
    product: aws
    service: cloudtrail
```

https://github.com/SigmaHQ/sigma-specification/blob/main/specification/sigma-appendix-taxonomy.md

Standards: Filename

Generally: [**category**|**service**]_**product**_**action**.yml

- proc_creation_win_**7zip_exfil_dmp_files**.yml
- file_delete_win_**delete_backup_file**.yml
- net_connection_lnx_**back_connect_shell_dev**.yml
- file_access_win_**susp_gpo_access_file**.yml



https://github.com/SigmaHQ/sigma-specification/blob/main/sigmahq/sigmahq-filename-convention.md

proc_creation_win_7zip_password_compression.yml

```yaml
title: Compress Data and Lock With Password for Exfiltration With 7-ZIP
id: 9fbf5927-5261-4284-a71d-f681029ea574
status: test
description: An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities
references:
author: frack113
date: 2021-07-27
modified: 2023-03-13
tags:
    - attack.collection
    - attack.t1560.001
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Description|contains: '7-Zip'
        - Image|endswith:
            - '\7z.exe'
            - '\7zr.exe'
            - '\7za.exe'
        - OriginalFileName:
            - '7z.exe'
            - '7za.exe'
    selection_password:
        CommandLine|contains: ' -p'
    selection_action:
        CommandLine|contains:
            - ' a '
            - ' u '
    condition: all of selection_*
falsepositives:
    - Legitimate activity is expected since compressing files with a password is common.
level: medium
```

Detection Logic

selection_img

Description contains 7-Zip
OR Image endswith 7z.exe OR 7zr.exe OR 7za.exe
OR OriginalFileName is 7z.exe OR 7za.exe

selection_password

CommandLine contains ‘ -p’

selection_action

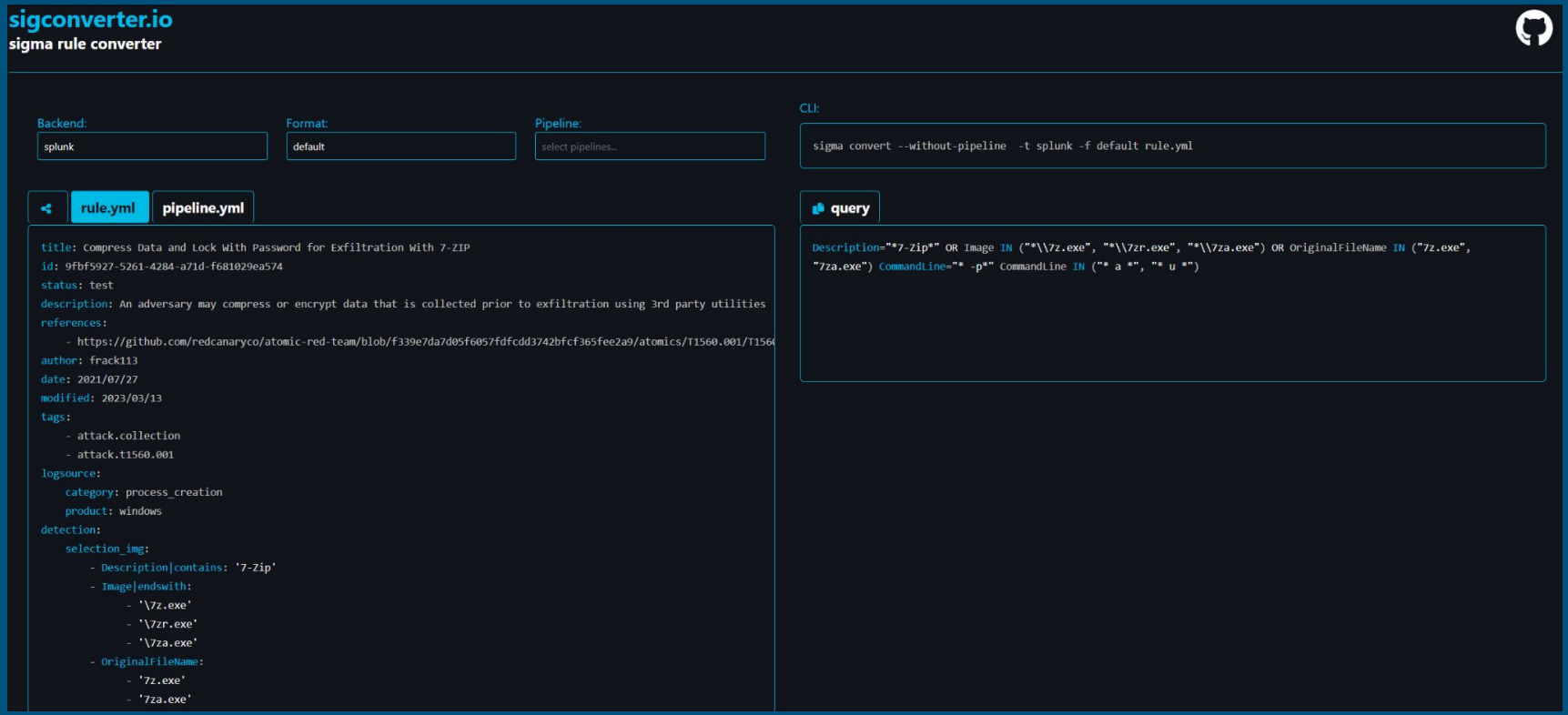
CommandLine contains either ‘ a ’ **OR** ‘ u ‘

condition: all of selection_*

Rule Translation

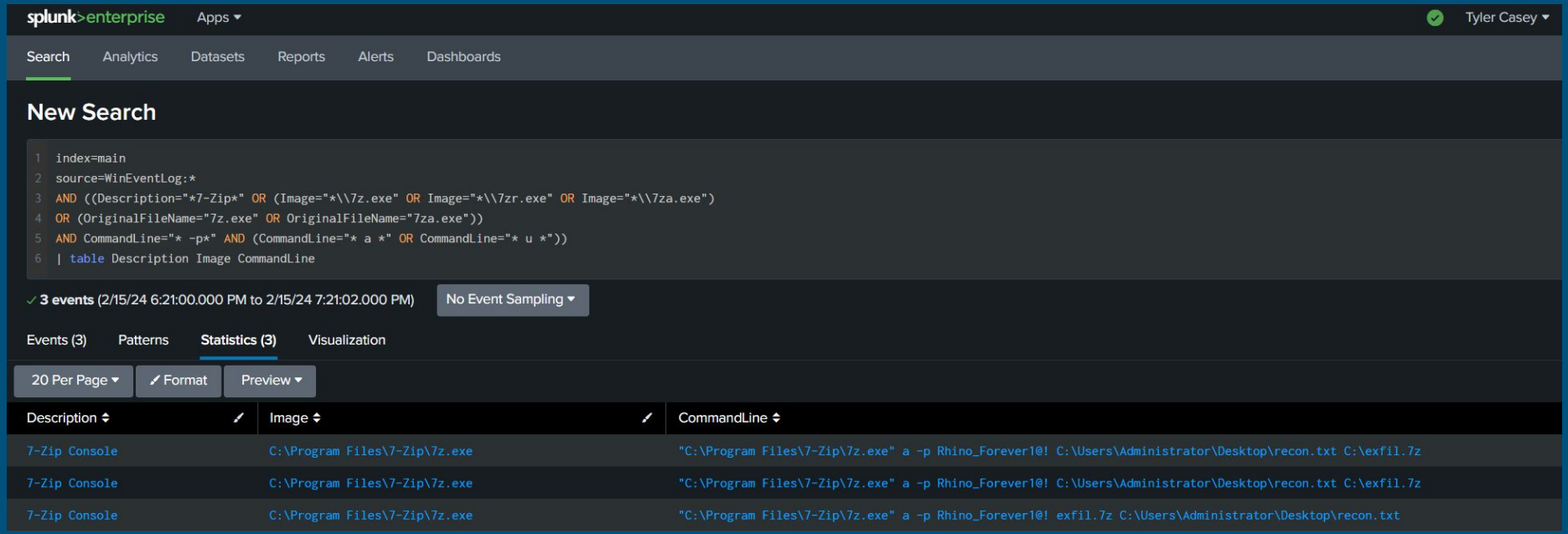
Make it actionable!

SIGCONVERTER



To Install: pip3 install sigma-cli

Detected!


splunk>enterprise
Apps
Tyler Casey
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
index=main
source=WinEventLog:*
AND ((Description="*7-Zip*" OR (Image="*\\7z.exe" OR Image="*\\7zr.exe" OR Image="*\\7za.exe")
OR (OriginalFileName="7z.exe" OR OriginalFileName="7za.exe"))
AND CommandLine="* -p*" AND (CommandLine="* a *" OR CommandLine="* u *"))
| table Description Image CommandLine
3 events (2/15/24 6:21:00.000 PM to 2/15/24 7:21:02.000 PM)
No Event Sampling
Events (3)
Patterns
Statistics (3)
Visualization
20 Per Page
Format
Preview
Description
Image
CommandLine
7-Zip Console
C:\Program Files\7-Zip\7z.exe
"C:\Program Files\7-Zip\7z.exe" a -p Rhino_Forever1@! C:\Users\Administrator\Desktop\recon.txt C:\exfil.7z
7-Zip Console
C:\Program Files\7-Zip\7z.exe
"C:\Program Files\7-Zip\7z.exe" a -p Rhino_Forever1@! C:\Users\Administrator\Desktop\recon.txt C:\exfil.7z
7-Zip Console
C:\Program Files\7-Zip\7z.exe
"C:\Program Files\7-Zip\7z.exe" a -p Rhino_Forever1@! exfil.7z C:\Users\Administrator\Desktop\recon.txt

Lab(s) Time!

https://github.com/tylercasey2263/sigma-workshop

02*

Rules 201

Create it, Standardize it, Read it…
CORRELATE IT

Correlated Sigma Rules

- Most Sigma rules describe **single events**
- **Correlation rules** detect threats by linking **multiple related events**
- Focus on **patterns over time**, not isolated logs
- Used to identify complex attacks that evade simple detections

rules/windows_failed_login_single_user.yml

yaml

```yaml
title: Windows Failed Logon Event
+ name: failed_logon # Rule Reference
description: Detects failed logon events on Windows systems.
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4625
    condition: selection
---
title: Multiple failed logons for a single user (possible brute force attack)
correlation:
    type: event_count
    rules:
        - failed_logon # Referenced here
    group-by:
        - TargetUserName
        - TargetDomainName
    timespan: 5m
    condition:
        gte: 10
```

https://sigmahq.io/docs/meta/correlations.html

How do they work?

```
title: Windows Failed Logon Event
name: failed_logon
status: test
description: |
Detects failed logon events on Windows systems.
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4625
  filter:
    SubjectUserName|endswith: $
  condition: selection and not filter
---
```

```
title: Multiple failed logons for a single user (possible
brute force attack)
status: test
correlation:
  type: event_count
  rules:
    - failed_logon
  group-by:
    - TargetUserName
    - TargetDomainName
  timespan: 5m
  condition:
    gte: 10
```

THANK YOU

@1qazCasey

/tyler-j-casey