Project Obsidian

Forensics

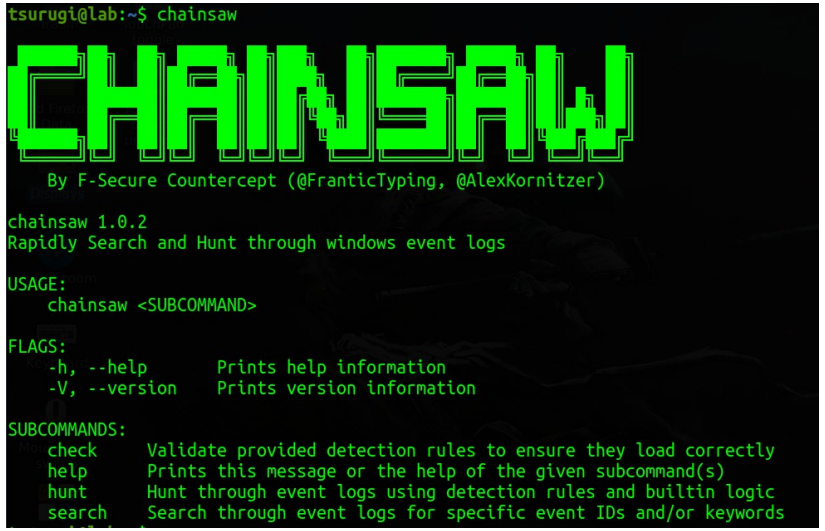
Using Chainsaw to Identify Malicious Activity

Agenda

- Chainsaw Overview
- SIGMA Rules
- Demo (/w Obsidian Project)

Chainsaw Overview

- First-response capability to quickly identify threats via event logs
- Command-line tool running Sigma rule detection logic
- Can search by keyword, regex, or specific Event IDs
- Can export data to TXT file or CSV for carving into spreadsheets



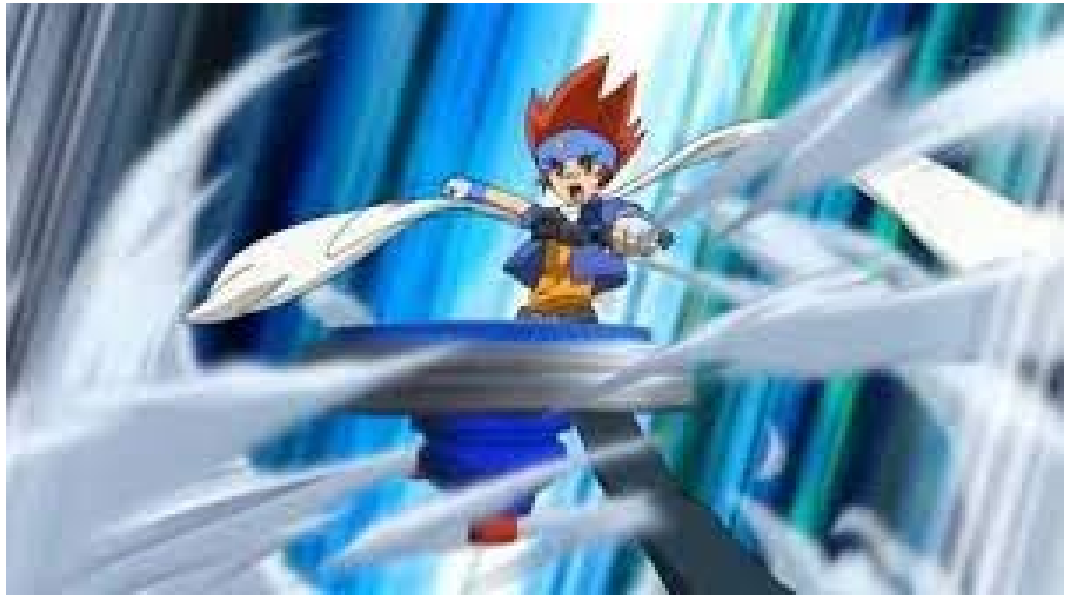
Sigma Rules

- Generic signature format for SIEMs in YAML designed for Windows Event Logs
  - Is to Event Logs as Yara is to Malware
- Developed by Florian Roth and Thomas Patzke

```
logsource:
 category: process_creation
 product: windows
detection:
 selection:
   ParentImage|endswith:
     - '\svchost.exe'
     - 'cmd.exe'
     - 'powershell.exe'
   Image|endswith:
     - '\mshta.exe'
 condition: selection
```

Intezer example, CSO Online

DEMO TIME



LET IT RIP!

References

- Chainsaw
  - **WithSecure Labs:** https://labs.withsecure.com/tools/chainsaw/
  - **CounterCept GitHub:** https://github.com/countercept/chainsaw
- Sigma Rules
  - **Ax Sharma, CSO Online:** https://www.csoonline.com/article/3663691/sigma-rules-explained-when-and-how-to-use-them-to-log-events.html
  - **Adam Swan, SOC Prime:** https://socprime.com/blog/sigma-rules-the-beginners-guide/