Cyb3rWard0g / **ThreatHunter-Playbook**

Watch 168 | Star 863 | Fork 196

A Threat hunter's playbook to aid the development of techniques and hypothesis for hunting campaigns.

threat-hunting sysmon hunting-campaigns hypothesis hunting dfir hunter mitre-attack-db mitre

160 commits | **2** branches | **0** releases | **7** contributors | MIT

Branch: **master** | New pull request | Find file | Clone or download

Cyb3rWard0g Merge pull request #15 from bfuzzy/master … Latest commit `1784011` a day ago

adversary_attribution	Updated Reference Syntax in Description Columns & added IDs	7 months ago

attack_matrix	Added technique name and added WinEvent info	a day ago
metrics	Added Data Quality Dimensions to Hunt Scoring	5 months ago
resources	Added Data Quality Dimensions to Hunt Scoring	5 months ago
templates	Added Data Quality Dimensions to Hunt Scoring	5 months ago
.DS_Store	Added Atomic Sysmon Configs per technique	5 months ago
LICENSE	Initial commit	a year ago
README.md	Update README.md	5 days ago

README.md

The ThreatHunter-Playbook

A Threat hunter's playbook to aid the development of techniques and hypothesis for hunting campaigns by leveraging **Sysmon** and **Windows Events** logs. This project will provide specific chains of events exclusively at the host level so that you can take them and develop logic to deploy queries or alerts in your preferred tool or format such as Splunk, ELK, Sigma, GrayLog etc. This repo will follow the structure of the MITRE ATT&CK framework which categorizes post-compromise adversary behavior in tactical groups. In addition, it will provide information about hunting tools/platforms developed by the infosec community for testing and enterprise-wide hunting.

Goals

- Expedite the development of techniques an hypothesis for hunting campaigns.
- Help Threat Hunters understand patterns of behavior observerd during post-exploitation.

- Reduce the number of false positives while hunting by providing more context around suspicious events.
- Provide enough resources to help on the development of a basic hunting framework for the community.
- Share technical hunt concepts and techniques with others in the community.

Resources

- MITRE ATT&CK
- MITRE CAR
- Sqrrl Hunting Techniques
- Sqrrl Guide to Threat Hunting
- Sysmon DFIR
- CyberWardog Labs Blog
- MalwareSoup Blog
- Threat Hunting Academy
- DFIR and Threat Hunting

Author

- Roberto Rodriguez @Cyb3rWard0g

Contributors

- Andy @malwaresoup
- Dimitrios Slamaris @dim0x69

Contributing

Can't wait to see other hunters' pull requests with awesome ideas to detect advanced patterns of behavior. The more chains of events you contribute the better this playbook will be for the community.

- Submit Pull requests following the TEMPLATE format.
- Highly recommend to test your chains of events or provide references to back it up before submitting a pull request (Article, whitepaper, hunter notes, etc).
    - Hunter notes are very useful and can help explaining why you would hunt for specific chains of events.
- Feel free to submit pull requests to enhance hunting techniques. #SharingIsCaring

TO-DO

☑ Add hunting tools from the community
☑ Create a hunting techniques document
☐ Improve Lateral Movement table format to show source and destination logs
☐ Add PowerShell as an option for the table column "source"
☑ Share HeatMap template for metrics purposes
☐ Hunting in Linux & MAC