DEATHCon 2025
Detection Engineering Automation

Welcome!

Introduction

- ❑ Threat Hunter for a Fortune 100
- ❑ 10+ years of experience in IR, Threat Hunting, and Detection Engineering
- ❑ Previously an adjunct teaching offensive security and EC-Council cert classes
- ❑ Designed and implemented a detections-as-code DE workflow in current role

Initial Post-Install Splunk Setup

Overview

- ❑ Design and creation of custom detections
- ❑ Intro to MITRE ATT&CK
- ❑ Detections-as-code workflow
- ❑ Automated deployment of custom detections
- ❑ Automated validation of custom detections
- ❑ CI/CD pipeline for detection automation
- ❑ Tracking detection coverage with MITRE ATT&CK

Design and Creation of Custom Detections

SECTION 1

What is a custom detection?

Custom Detection

Development

Customized for your environment

Alert

Has one or more trigger actions when matches are found

Configuration

Runs often on a periodic schedule

Search

Search query saved in SIEM or other logging platform

Intro to MITRE ATT&CK

SECTION 2

What is ATT&CK?

- ❑ Open knowledge base of tactics, techniques, and procedures
- ❑ Enterprise, Mobile, and ICS
- ❑ Tactics > Techniques > Procedures
- ❑ Catalog techniques that an attacker can use to compromise an enterprise

Detections-as-code Workflow

SECTION 3

git

- A revision control tool
- Keep track of all previous history of file changes
- Enables collaboration for a team working on the same directory of files
- Functionality to merge changes together
- Advanced functions for reverting and cherry-picking individual changes

Azure DevOps

- ❑ Free for first 5 users
- ❑ Boards
- ❑ Repos
- ❑ Pipelines

Using Azure DevOps Markdown Wiki

- ❑ Combine detection with documentation
- ❑ Easy reference for analysts
- ❑ Historical revisions
- ❑ Manage as code outside of SIEM

Automating Detection Deployment

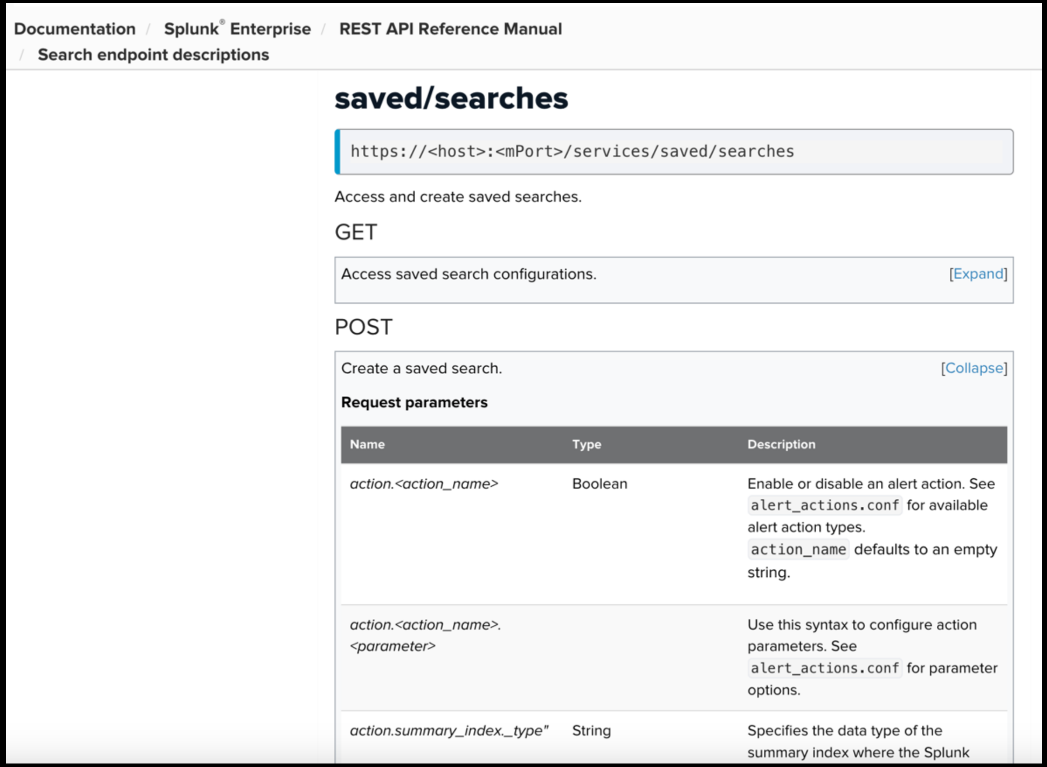
SECTION 4

Splunk

- ❑ Local install for free with daily limited ingestion
- ❑ Splunk cloud 14-day trial
- ❑ Detections are scheduled saved searches
- ❑ Splunk has a robust API that includes the ability to create saved searches

Saved Searches in Splunk API

- ❑ Splunk provides great documentation for their API endpoints
- ❑ Saved searches endpoint provides details on parameters used in requests
- ❑ https://docs.splunk.com/Documentation/Splunk/9.2.1/RESTREF/RESTsearch



Documentation / Splunk® Enterprise / REST API Reference Manual / Search endpoint descriptions

saved/searches

```
https://<host>:<mPort>/services/saved/searches
```

Access and create saved searches.

GET

Access saved search configurations. [Expand]

POST

Create a saved search. [Collapse]

Request parameters

Name	Type	Description
action.<action_name>	Boolean	Enable or disable an alert action. See `alert_actions.conf` for available alert action types. `action_name` defaults to an empty string.
action.<action_name>.<parameter>		Use this syntax to configure action parameters. See `alert_actions.conf` for parameter options.
action.summary_index._type"	String	Specifies the data type of the summary index where the Splunk

Automating It

- ❑ Use markdown files to create detections
- ❑ Python to parse the markdown
- ❑ Splunk API to create the saved searches
- ❑ This can be done at scale on entire sets of markdown files

Automating Detection Validation

SECTION 5

Test Cases

- ❑ Acts like a unit test in software development
- ❑ Just requires another heading in our markdown wiki file
- ❑ Will set us up well for future automation

Automating Test Cases

- ❑ Use python to run powershell remoting
- ❑ Pre-determined testing hosts required
- ❑ Should see Splunk alert shortly after test
- ❑ This can be done at scale on entire sets of markdown files

Tying Automations Together with a CI/CD Pipeline

SECTION 6

Pipelines

- ❑ Automated procedures that follow steps and are triggered by actions
- ❑ Azure DevOps has native support for Pipelines
- ❑ Runs commands on a target system
- ❑ We will run python inside of our pipeline

Setting up in Azure DevOps

- ❑ Create a pipeline and configure the YAML file
- ❑ Add files needed for pipeline
- ❑ Configure pipeline operation

Integrating with Detections

❑ Pipeline API and fetch settings

❑ Integrating the Python script

❑ Adding our markdown files

❑ Setting up target VM

Detection Validation

- ❑ Add good test case and bad test case
- ❑ Can catch mistakes and ingestion issues
- ❑ Pipeline will be set to fail if detection isn’t validated

Track Detection Coverage with MITRE ATT&CK

SECTION 7

ATT&CK Navigator

- ❑ Open-source web application
- ❑ Tons of options for ways to interact with the ATT&CK matrices
- ❑ Hosted version available, but you can also build and host your own

Layers

❑ Add multiple tabs or “layers” to build endless visualizations

❑ Can use layers as a heatmap or scoreboard to track coverage

❑ Layers are stored in JSON files

Course Conclusion

- ❑ Thank you for taking this course!
- ❑ Connect with me on LinkedIn - https://www.linkedin.com/in/glenn-barrett-b379122b4/
- ❑ Feel free to reach out for questions or issues!
- ❑ Feedback is also appreciated!