



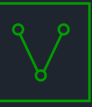
Vertex

Synapse Bootcamp

Module 13

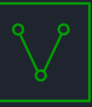
More Fun With Power-Ups

v0.4 - May 2024

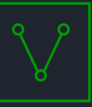


Objectives

- Power-Up refresher
 - Power-Up help
 - Power-Ups, Storm commands, and Node Actions
- Know common options for Power-Up commands
- Understand the purpose of data source (meta : source) nodes
- Use Storm to run Power-Up commands
- Examine specific Power-Ups in depth



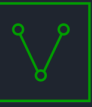
Power-Ups



Power-Ups

- Packages and services that add functionality to Synapse
- Act as connectors to other systems / services
- Perform a specific function
- Managed through Power-Ups Tool
 - Rapid vs Advanced





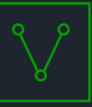
Power-Up Execution

- Power-Up functionality is provided by **Storm commands**
- May be added as Node Actions
 - Run with **default** options
- May be added as Workflows
 - Custom UI for some commands
- Can run Storm commands manually
 - Customize (e.g., via switches)
 - Not suitable for Node Actions (e.g., 'search' commands)
 - Leverage as part of automation





Power-Up Refresher - Demo



Common Power-Up Options



Common Options

- Where applicable, Power-Ups commands have a similar set of options

Option	Meaning	Use Cases
<code>--debug</code>	Output additional detail to the Console	Troubleshooting
<code>--yield</code>	Return the main nodes created by the command	You want to see the results, not the input nodes There are no input nodes (e.g., sync or search commands)
<code>--size</code>	Limit the number of results returned Override the default number of results	Obtain a sampling of data Limit API usage Request additional data beyond the default value
<code>--asof</code>	Override the default cache value (30 days) (currently being deprecated)	Force the command to query for more recent data



Custom Node Actions

- Run a standard Power-Up command with different options:
 - Storm Query Bar:

```
inet:ipv4=152.228.179.67 | shodan.enrich --no-history
```

- Create a custom Node Action:

Add Node Action

Shodan enrich (no history)

shodan.enrich --no-history

inet:ipv4,inet:ipv6

Render Nodes yielded from Action? OFF

+ Add Action



Power-Ups and Sources

- Power-Ups that add data create **source** (meta:source) nodes
- Described in the Power-Up User Guide

Use of meta:source nodes

Synapse-AlienVault uses a meta:source node and -(seen)> light weight edges to track nodes observed from the AlienVault API.

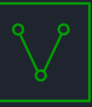
```
> meta:source=448b84f640c8c7f11e210e57d2523e78
meta:source=448b84f640c8c7f11e210e57d2523e78
  .created = 2022/01/10 16:06:58.790
  :name = alienvault api
```

- Nodes returned linked via **seen** light edges

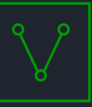
```
meta:source:name='virustotal api' -(seen)> file:bytes
```

```
inet:ipv4=217.7.2.112 <(seen)- meta:source
```

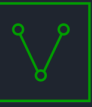
- Track **where** data came from within Synapse



Power-Ups - Demo



Power-Up Examples



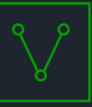
Sample Power-Ups

- Synapse supports a broad range of Power-Ups
 - Different purposes, features, requirements...
- Every organization is different
 - Power-Ups you have access to depend on your configuration / access
- A few Vertex Power-Ups as examples:
 - synapse-fileparser
 - synapse-mitre-attack



synapse-fileparser

- Vertex "Swiss army knife" for extracting data from files (`file:bytes`)
 - Advanced Power-Up - requires Axon storage
- Extract and model metadata for some MIME types
- Recursively parse files
- Extract and link indicators
- View ASCII strings
- View hex



synapse-mitre-attack

- Vertex publicly available Power-Up
 - Rapid Power-Up
- Loads and models the current MITRE ATT&CK Matrix
 - Enterprise / Mobile / ICS
 - Tactics, Techniques, Groups, Software, Mitigations, Campaigns
- Reference and navigate ATT&CK from within Synapse
- Parse / extract and link MITRE ATT&CK elements
 - From node properties (e.g., `inet:service:message:text`)
 - From files (`file:bytes`)



Power-Ups Demo



Summary

- **Power-Ups** add functionality to Synapse
- Most Power-Ups use **Storm commands** to add capabilities
 - Commonly used commands added as **Node Actions** with default options
- Power-Up Storm commands can run:
 - In the **Storm Query Bar**
 - As **custom** Node Actions
- Many Power-Ups share a common set of **command options**
- Precise purpose / functionality is specific to each Power-Up
- **Synapse-fileparser** and **synapse-mitre-attack** are two examples