## ALIGNING TO THE THREAT HUNTING MISSION

### APT Falconer Application Overview:

This complimentary threat-hunting application is the focal point for mission-critical end users who wish to utilize Splunk to its fullest - with over 500 pre-built analytics, it automatically categorizes incoming and historical data into 4 categories based on the individual functions:  leadership, network, host and Intel. The leadership panel provides a holistic overview for maximum oversight and visibility, while the additional dashboards segment data specific to each analyst role. This ensures the data is appropriately disseminated and analyzed by the correct member of the team once boots hit the ground; providing peace of mind and immediate action. APT Falconer bridges the gap of the robust Splunk ES application by allowing end users the ability to hunt backwards in time in a more streamlined manner, while utilizing real time data to correlate advanced persistent threats. No more guessing what fields should be called. APT Falconer provides something for everyone, from the completely novice to the subject matter experts leading to faster threat hunting and less downtime.

### APT Falconer Benefits:

- **CIM Compliant:** Information is set to the Splunk Common Information Model. No need to change your current ingestion to use this application, having a CIM means not having to reinvent the wheel. With data feeds being mapped directly to data models, you can easily implement accelerated searches, hardware dependent. This also means that you can share dashboards and techniques with outside agencies or units making this app not only a single solution, but community driven as well.

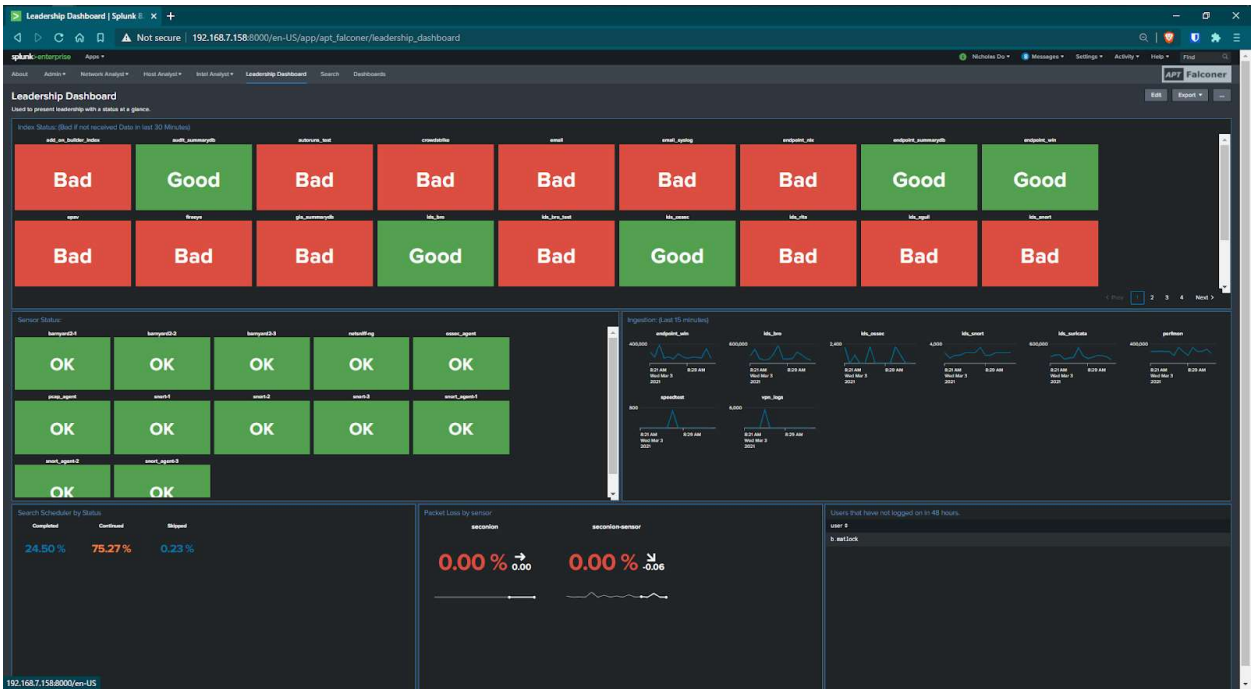
- **Centralized:** This app pulls information from other apps and places it in a central location, meaning less time spent trying to hunt down that dashboard you used on the last mission that was so vital to your success. The main goal is one app to rule them all, with information requirements driven directly from user feedback, and provided in smaller updates as development occurs.

- **Something For Everyone:** This application has dashboards for every role on the team. Network Analyst can hunt via PCAP/Network captures, which are typically from Security Onion (Bro/Zeek). Host Analyst can hunt via host logs (Windows EVTX, Sysmon, Registry). Intel Analyst can implement Indicators of Compromise and query the collected data feeds to support in the hunt.

## APT FALCONER BY FUNCTION

**Leadership Dashboard:** Provides a complete organizational view of all data feed statuses to ensure everything is functioning correctly to gain accurate insight into the overall operation.

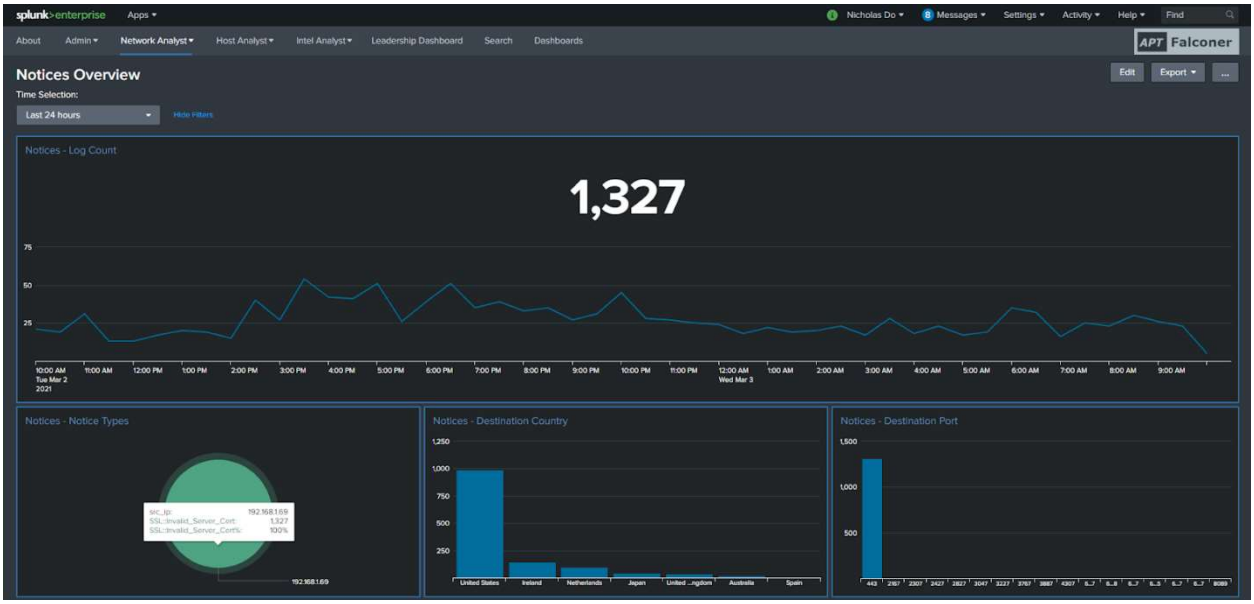
Within the Admin workspace you can view items such as resource usages, software status, ingestion feeds, broken indexes and even infrastructure. APT Falconer also considers network sensors, health of a host, VMs riding on a hypervisor and all other software in need of tracking for a comprehensive view.



**Network Analyst workspace:** This dashboard provides the end user the ability to work in a centralized location to seek anomalies within network traffic.

Pre-built dashboards for:

- NIDS (network intrusion detections systems)
- BZAR (Bro/Zeek Attack-based analytics and reporting)
- Suricata
- Snort
- RITA
- Networking collected via Zeek (All 27 protocols)
- Splunk Stream
- Cisco devices.




---

**Host Analyst workspace:** This dashboard focuses on endpoints such as Windows Event logs, Nix audit/Processes/Bash history and Sysmon. All analytics are mapped directly to the MITRE Attack framework where it's aligned to look for tactics and techniques rather than specific process names and commands.

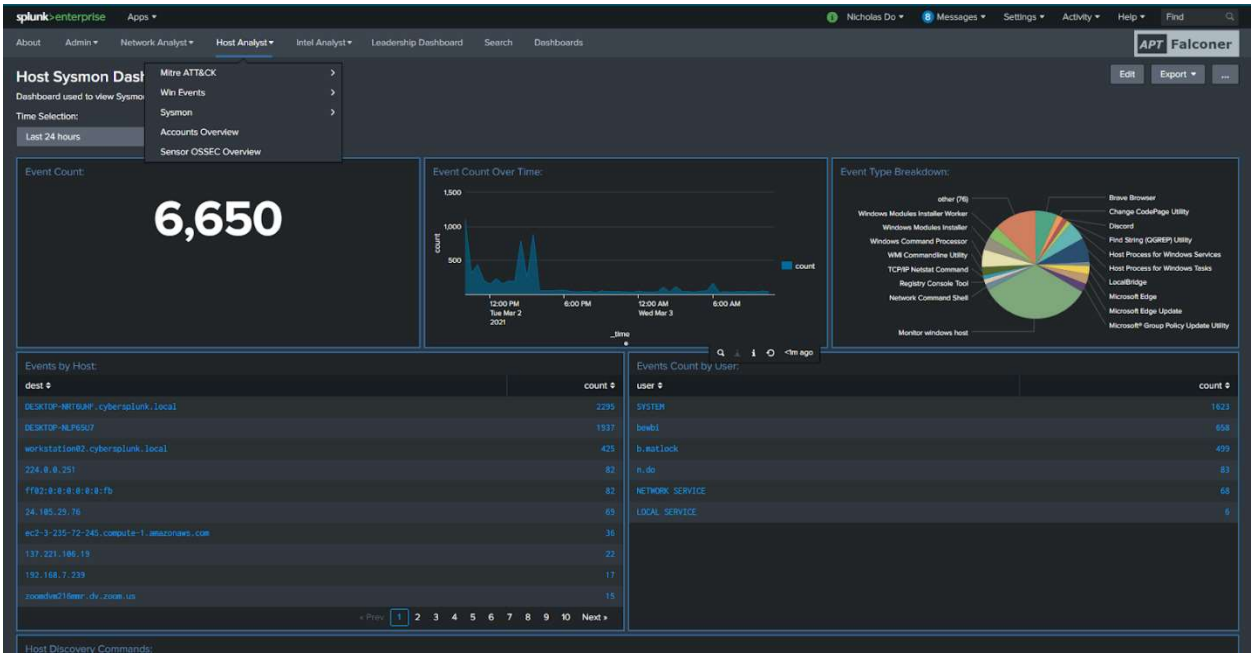
- Dashboards: Provide pre-built dashboards that cover the MITRE ATT&CK Matrix, utilizing Windows Event logs and/or Sysmon.

- MITRE ATT&CK: Analytics mapped to techniques within the framework. Currently covers roughly 80% of all techniques and tactics

- Win Events: Includes default dashboards to display overview such as commands by process, process connections and new services added

- Sysmon: Includes dashboards for Registry overview, File creations, Process Watch, Host Investigator and more

- OSSEC Overview: Interesting events forwarded via Security Onion Sensor

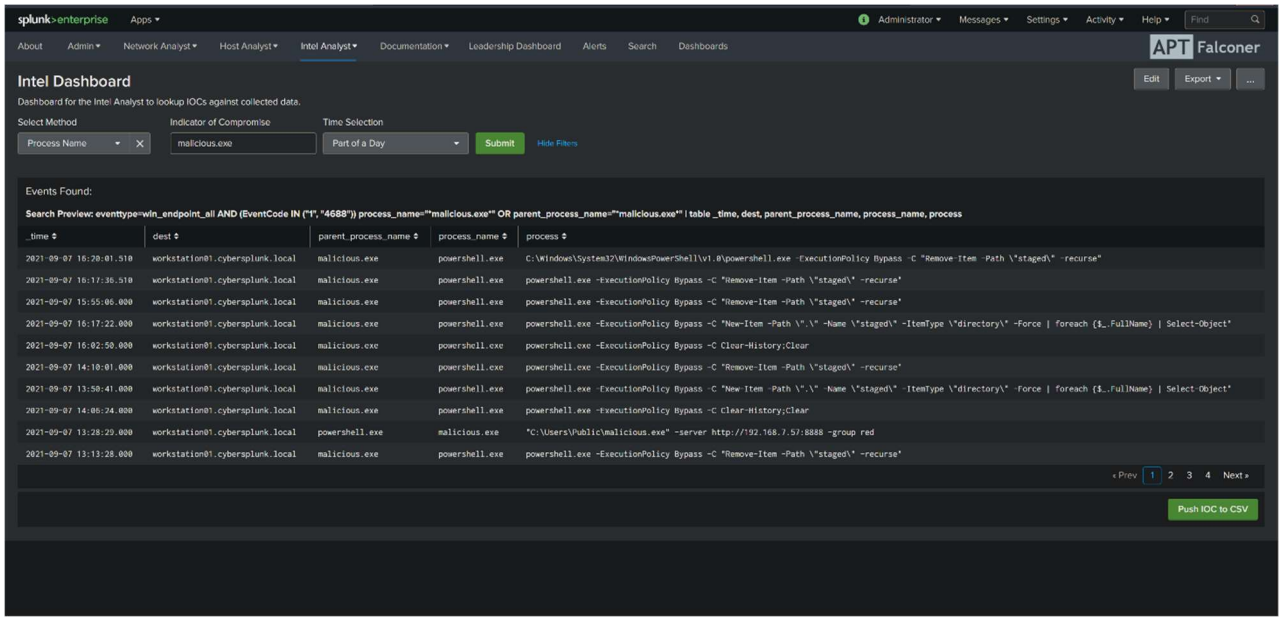



---

**Intel Analyst Workspace:** This dashboard is designed for an end user that has no prior experience with Splunk or it's query language. It's single panel interface allows the analyst to generate queries, indicators of compromise (IOC) and question future events with a simple point and click of a button.

Available methods for IOC searching with the ability to push IOC to CSV:

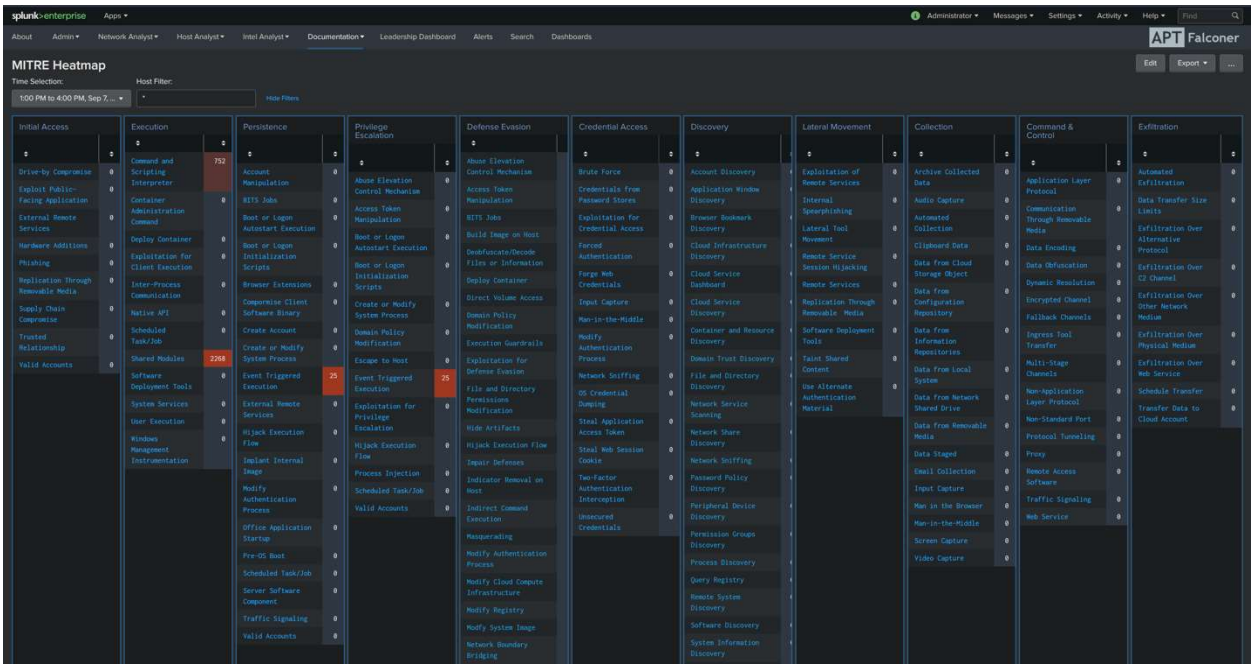
- IP
- SHA1/SHA256
- MD5
- Process Name
- File Name
- Command Line
- JA3/JA3S




## APT FALCONER FUTURE ENHANCEMENTS

**Heat Mapping** based on IOCs found within any environment, mapping those results to a specific threat group and most likely software being leveraged during an attack.

Example Heath Map of detections:



Example: Correlation of Heat Map to Threat Group and Software


Future features and capabilities are community driven by you the user.

To view a pre-recorded demo,

Any questions can be directed to APT Falconer creator and developer, Brent Matlock, Principal Practice Architect for Security at bmatlock@splunk.com.