

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:

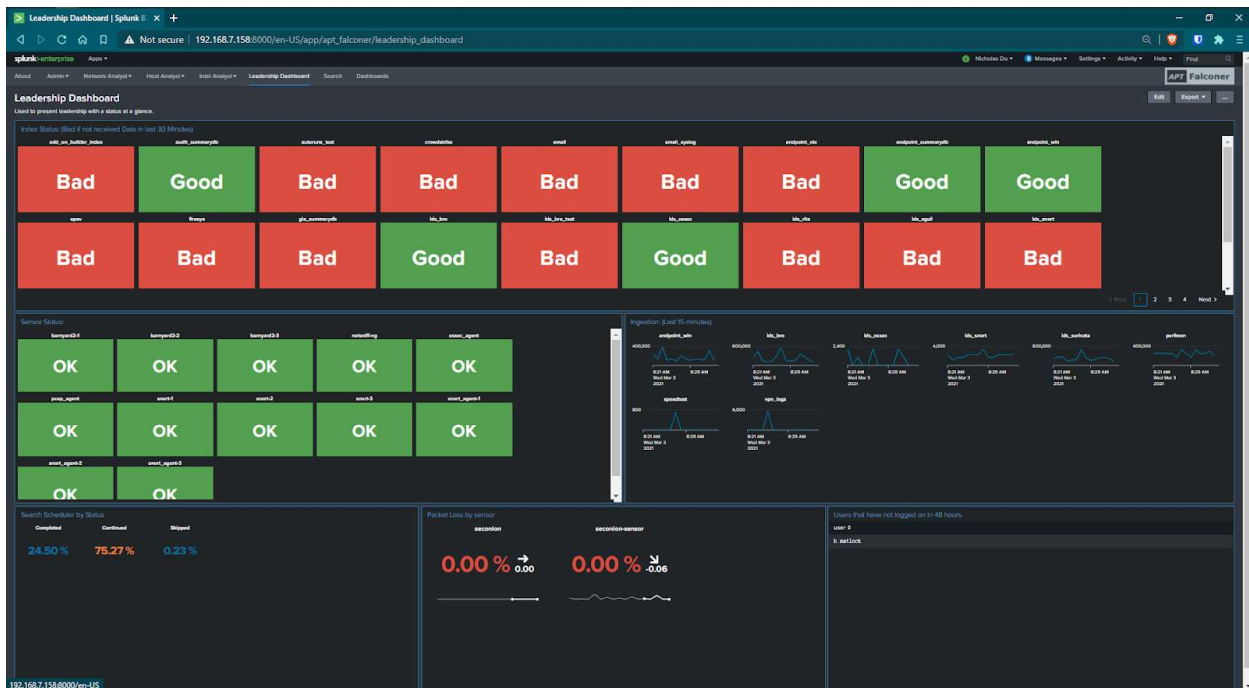
- **CIM Compliant:** Information is set to the Splunk Common Information Model. No need to change your current ingestion to use this application, having a CIM means not having to reinvent the wheel. With data feeds being mapped directly to data models, you can easily implement accelerated searches, hardware 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.

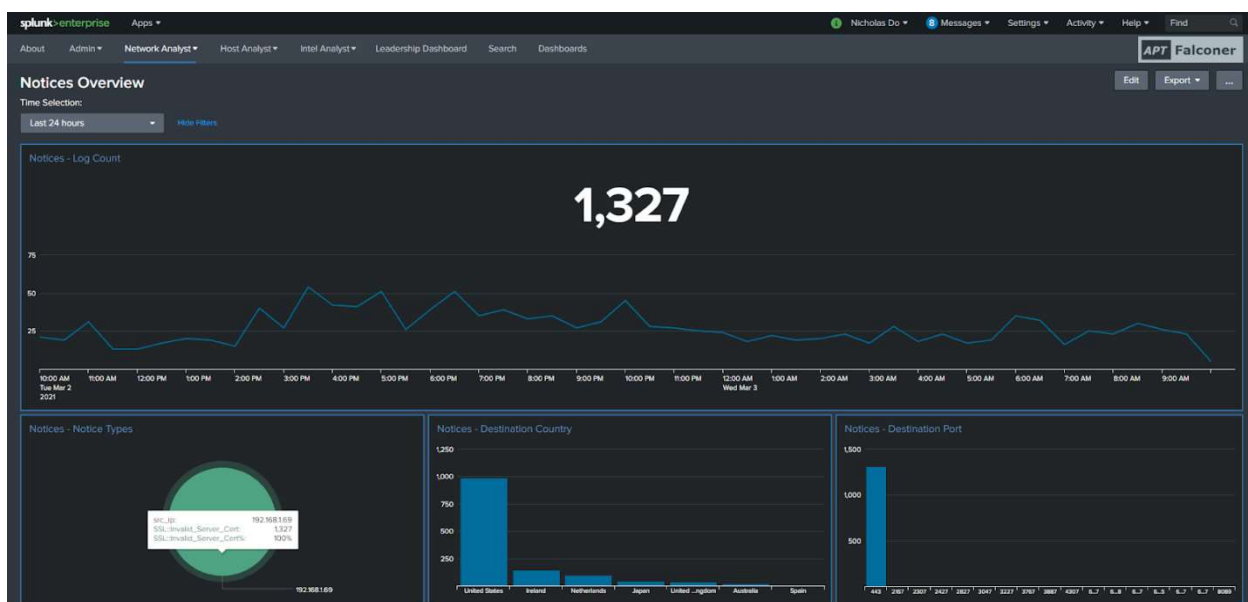
Within the Admin workspace you can view items such as resource usages, software status, ingestion feeds, broken indexes and even infrastructure. APT Falconer also considers network sensors, health of a host, VMs riding on a hypervisor and all other software in need of tracking for a comprehensive view.



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:

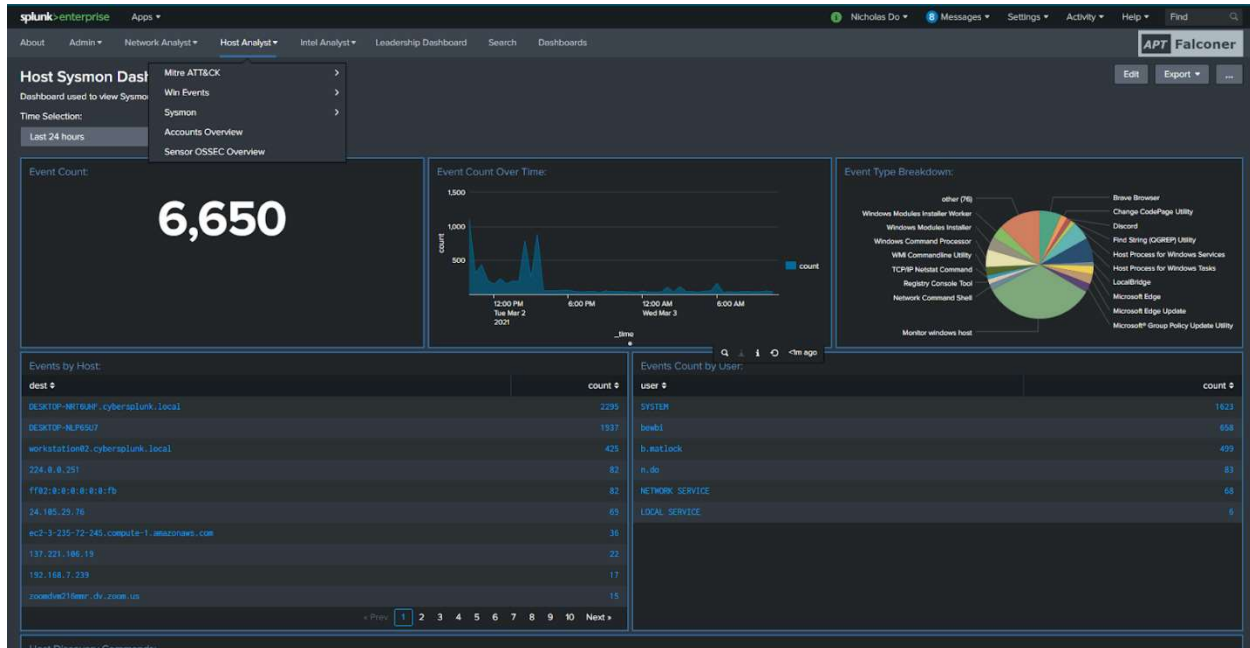
- NIDS (network intrusion detections systems)
- BZAR (Bro/Zeek Attack-based analytics and reporting)
- Suricata
- Snort
- RITA
- Networking collected via Zeek (All 27 protocols)
- Splunk Stream
- Cisco devices.



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 its query language. Its 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

splunk-enterprise Apps

Administrator Messages Settings Activity Help Find

About Admin Network Analyst Host Analyst Intel Analyst Documentation Leadership Dashboard Alerts Search Dashboards

APT Falconer

Intel Dashboard

Dashboard for the Intel Analyst to lookup IOCs against collected data.

Select Method: Process Name Indicator of Compromise: malicious.exe Time Selection: Part of a Day [Hide Filters](#)

Events Found:

Search Preview: eventtype=win_endpoint_all AND (EventCode IN ("7", "4688")) process_name="malicious.exe" OR parent_process_name="malicious.exe" | table _time, dest, parent_process_name, process_name, process

time	dest	parent_process_name	process_name	process
2021-09-07 16:20:01.310	workstation01.cybersplunk.local	malicious.exe	powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -C "Remove-Item -Path '\staged*' -recurse"
2021-09-07 16:17:36.310	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C "Remove-Item -Path '\staged*' -recurse"
2021-09-07 15:55:06.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C "Remove-Item -Path '\staged*' -recurse"
2021-09-07 16:17:22.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C "New-Item -Path '\.' -Name '\staged*' -ItemType '\directory*' -Force foreach (\$_.FullName) Select-Object"
2021-09-07 16:02:50.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C Clear-History;Clear
2021-09-07 14:10:01.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C "Remove-Item -Path '\staged*' -recurse"
2021-09-07 13:50:41.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C "New-Item -Path '\.' -Name '\staged*' -ItemType '\directory*' -Force foreach (\$_.FullName) Select-Object"
2021-09-07 14:06:24.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C Clear-History;Clear
2021-09-07 13:28:29.000	workstation01.cybersplunk.local	powershell.exe	malicious.exe	"C:\Users\Public\malicious.exe" -server http://192.168.7.57:8888 -group red
2021-09-07 13:13:28.000	workstation01.cybersplunk.local	malicious.exe	powershell.exe	powershell.exe -ExecutionPolicy Bypass -C "Remove-Item -Path '\staged*' -recurse"

Prev 1 2 3 4 Next

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 Heat Map of detections:

splunk-enterprise Apps

Administrator Messages Settings Activity Help Find

About Admin Network Analyst Host Analyst Intel Analyst Documentation Leadership Dashboard Alerts Search Dashboards

APT Falconer

MITRE Heatmap

Time Selection: 1:00 PM to 4:00 PM, Sep 7, ...

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
<ul style="list-style-type: none"> Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Replication Through Removable Media Supply Chain Compromise Trusted Relationship Valid Accounts 	<ul style="list-style-type: none"> Command and Control Scripting, Interpreter Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication Malicious API Scheduled Task/Job Shared Modules Software Deployment Tools System Services User Execution Windows Management Instrumentation 	<ul style="list-style-type: none"> Account Hijacking BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Browser Extensions Compromise Client Software Binary Create Account Create or Modify System Process Event Triggered Execution External Remote Services HiJack Execution Flow Implant Internal Tools Notify Authentication Process Office Application Startup Pre-OS Boot Scheduled Cloud Job Server Software Component Traffic Signaling Valid Accounts 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Build Image on Host Overlooked Process Files or Information Deploy Container Direct Volume Access Create or Modify System Process Device Policy Modification Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Hide Artifacts HiJack Execution Flow Inspire Defenses Indicator Removal on Host Scheduled Task/Job Indirect Command Execution Manipulating Hosts Modify Authentication Process Modify Cloud Compute Infrastructure Modify Registry Notify System Image Network Boundary Bridging 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Build Image on Host Overlooked Process Files or Information Deploy Container Direct Volume Access Device Policy Modification Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Hide Artifacts HiJack Execution Flow Inspire Defenses Indicator Removal on Host Scheduled Task/Job Indirect Command Execution Manipulating Hosts Modify Authentication Process Modify Cloud Compute Infrastructure Modify Registry Notify System Image Network Boundary Bridging 	<ul style="list-style-type: none"> Brute Force Credentials from Password Stores Browser Bookmarks Discovery Exploitation for Credential Access Forced Authentication Forgot Web Credentials Input Capture Man-in-the-Middle Notify Authentication Process Network Sniffing OS Credential Dumping Steal Application Access Token Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials 	<ul style="list-style-type: none"> Account Discovery Application Window Discovery Browser Bookmarks Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Remote System Discovery Software Discovery System Information Discovery 	<ul style="list-style-type: none"> Exploitation of Remote Services Internal Spooling Lateral Tool Movement Remote Service Session Hijacking Remote Services Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material 	<ul style="list-style-type: none"> Archive Collected Data Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Encrypted Channel Configuration Repository Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Non-Standard Port Protocol Tunneling Proxy Shell Collection Input Capture Man-in-the-Middle Screen Capture Video Capture 	<ul style="list-style-type: none"> Accounted Exfiltration Data Transfer Size Limits Communication Through Removable Media Data Encoding Protocol Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service 	

Example: Correlation of Heat Map to Threat Group and Software

Threat Group	count	Software	count
APT32	3859	Astaroth	5833
Leviathan	3820	Metamorfo	2819
Cobalt Group	3820	Xbash	2887
Inception	2887	RogueRobin	2775
Blue Mockingbird	2775	Egregor	2775
WIRTE	2768	Koadic	2559
TASS1	2559	Valak	2523
Deep Panda	2548	PUNCHBUGGY	2523
APT19	2523	Orz	2520
MuddyWater	791	More_eggs	2520

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.