Oct 23, 2018

ATT&CK: All the Things

- **USAA's journey into integrating ATT&CK into Tools, Techniques, and <tacos>**

Neelsen Cyrus
@neelsen

David Thompson
@dirty_tizzle

>id @neelsen

- **Various operational roles at USAA since 1997**
  - WebSphere farm support for external and internal web applications
  - Configuration Management Database
  - Cyber Threat Operations Center (CTOC)

- **Dual hats in the (CTOC)**

- **Usually behind the scenes and not on stage with real people watching me**

> id @dirty_tizzle

- 6.5 years Air Force Captain doing Vuln Assessments for AF BT and ~2 years at NSA
- Pen Tester for JHU APL working Space Systems and other DoD Projects
- Pen Tester for AF BT (Contractor) working Space Systems, Aircraft and other weapon systems
- Was a Red Team Member, New Detections Lead (Blue Team), and as of 15 Oct, I am now the Manager Leading our Incident Response Team

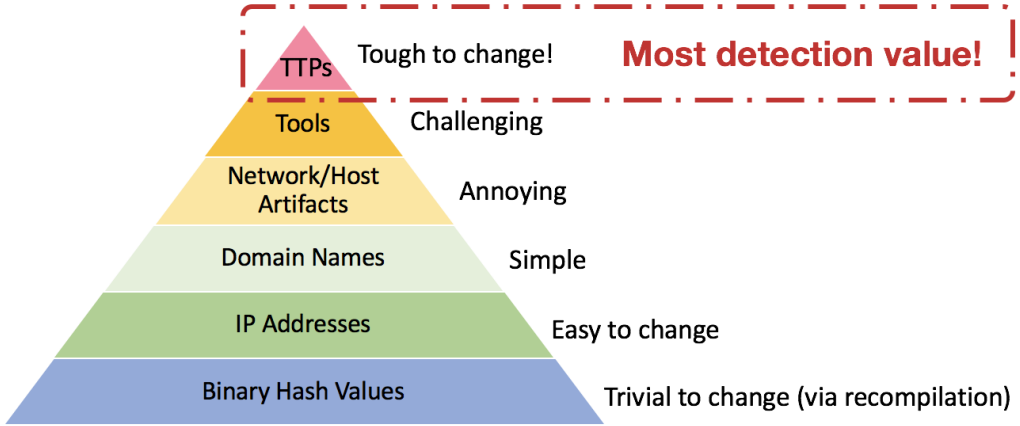
Outline

- “Pre-” ATT&CK Work
- Integrating ATT&CK into our Ecosystem
- Way Ahead
- Questions

“Pre-”ATT&CK Work

Why We Chose ATT&CK

- **Old Method – Kill Chain**
  - 50,000 FT view of threat behavior
- **New Method – ATT&CK**
  - Threat behavior that is operationally relevant & actionable
- **Threat Actor Group Data**
  - Tactics & Techniques of past Intrusion Sets
  - Cataloging Threat Actor Capabilities w/ ATT&CK
- **Meaningful**
  - Proactive vs Reactive in Identifying and Prioritizing Gaps



Why We Chose ATT&CK (cont'd)

USE CASES:

- Gap Analysis with Current Defenses
- Prioritize detection/mitigation
- Information Sharing
- Track a specific adversaries set of techniques
- Adversary Emulation
- New technologies, research

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

Self-Assessment

ATT&CK Techniques	(10 Highest) Priority	Real time/Hunt	USAA Detection Rating	USAA Mitigation Rating	ATT&CK Tactics	ATT&CK Tactics
Redundant Access	X	R/H	X	X	Persistence	Defense Evasion
DLL Injection	X	R/H	X	X	Privilege Escalation	Defense Evasion
Process Hollowing	X	R/H	X	X	Defense Evasion	Execution
Rundll32	X	R/H	X	X	Defense Evasion	Execution
AppInit DLLs	X	R/H	X	X	Persistence	Privilege Escalation
Data Transfer Size Limits	X	R/H	X	X	Exfiltration	
Bootkit	X	R/H	X	X	Persistence	
System Service Discovery	X	R/H	X	X	Discovery	
Exfiltration Over Command and Control Channel	X	R/H	X	X	Exfiltration	
Pass the Hash	X	R/H	X	X	Lateral Movement	
Binary Padding	X	R/H	X	X	Defense Evasion	
DLL Search Order Hijacking	X	R/H	X	X	Persistence	Privilege Escalation
Install Root Certificate	X	R/H	X	X	Defense Evasion	
Regsvcs/Regasm	X	R/H	X	X	Defense Evasion	Execution
System Owner/User Discovery	X	R/H	X	X	Discovery	

Detection Tagging Train

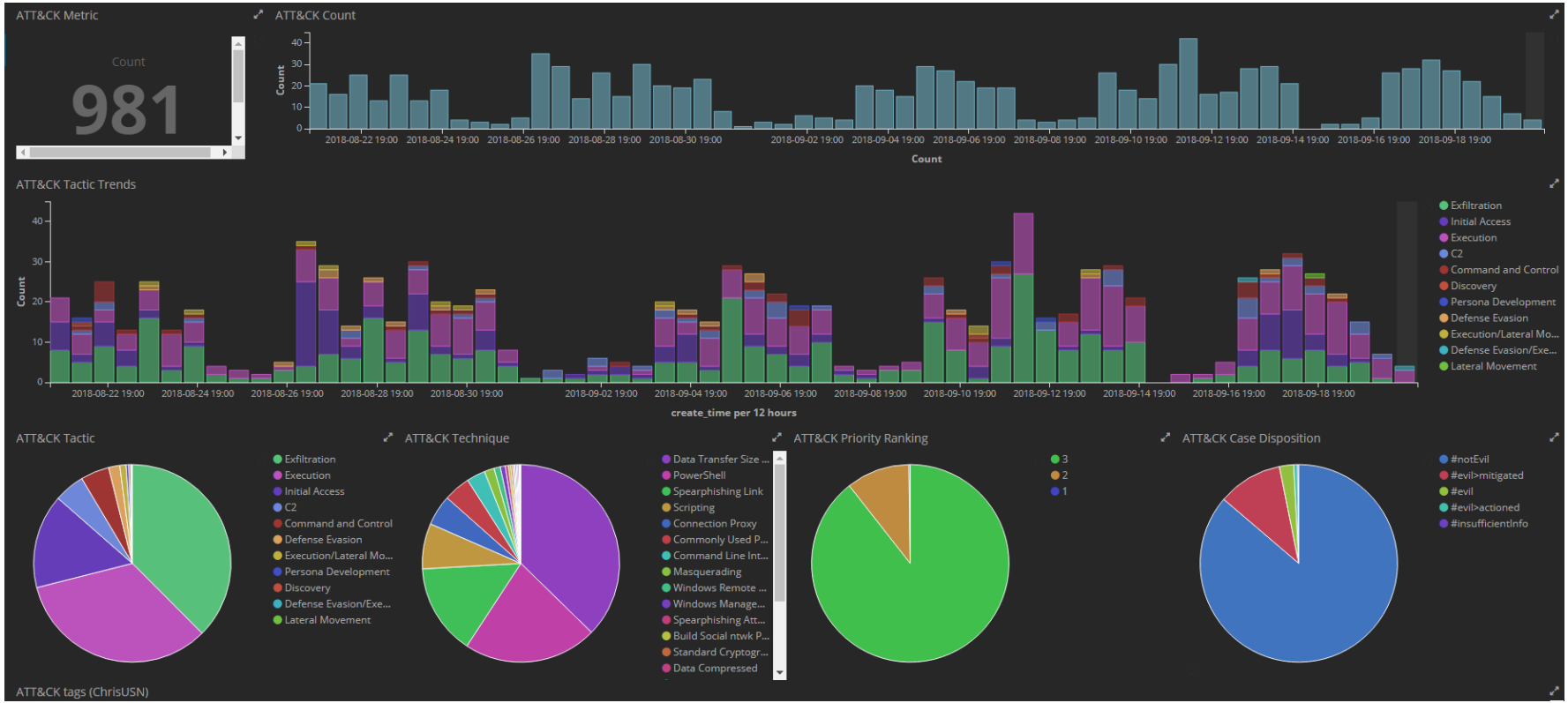
- We started pushing new detections ideas into GIT about a year ago
- Labels For The win (FTW)!
- GIT API Calls based off of ATT&CK Labels to feed our Flask app FTW!

Integrating ATT&CK into our Ecosystem

USAA's ATT&CK Visualization tool

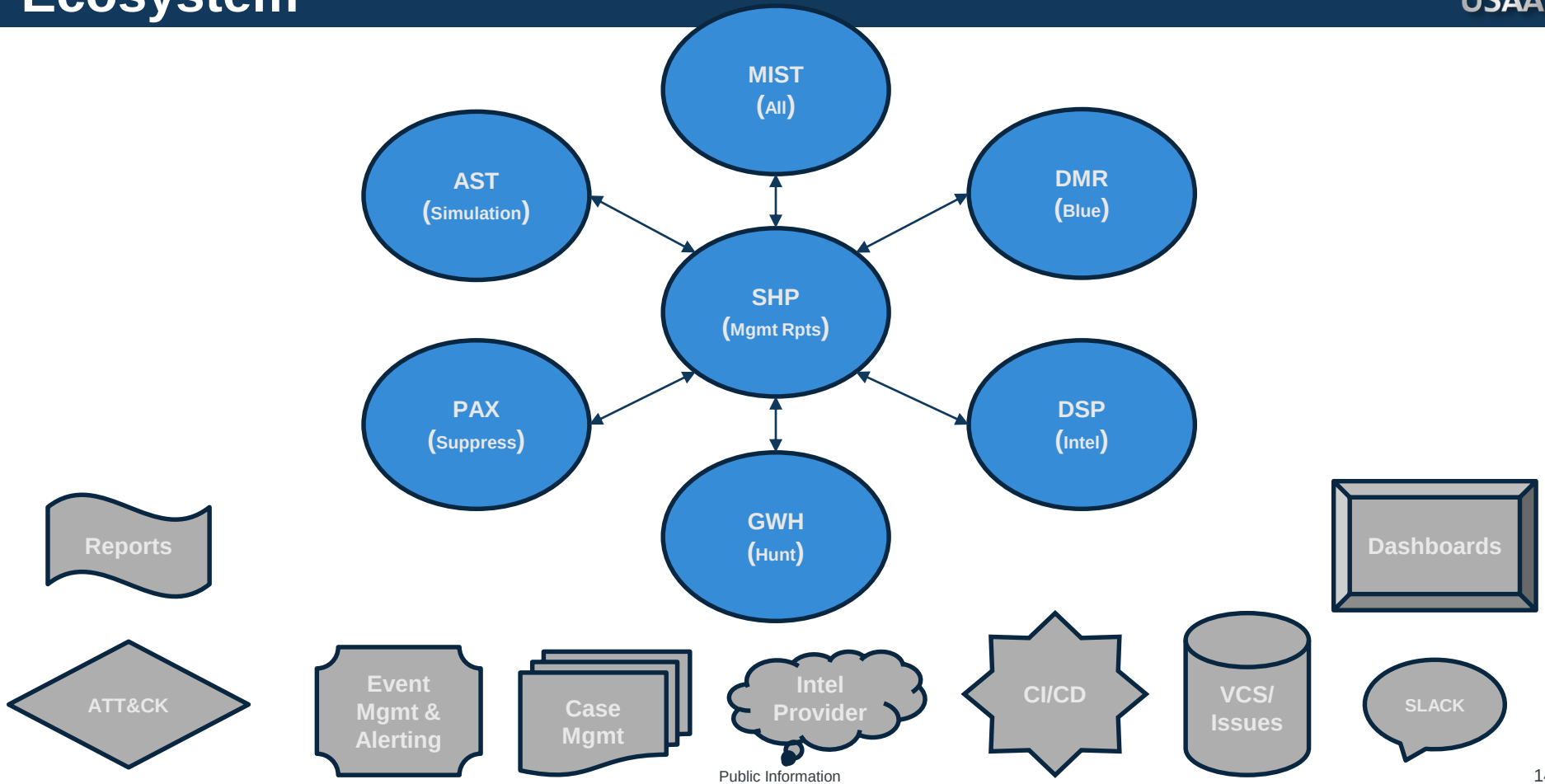
- **Custom Tool – Based off of Navigator**
- **Python Flask App**
- **Updates MITRE data via API**
- **Correlating tags with respective techniques**
  - Detection test/prod
  - Hunt
  - Intel
  - Adversary Capabilities

Case Enrichment with ATT&CK



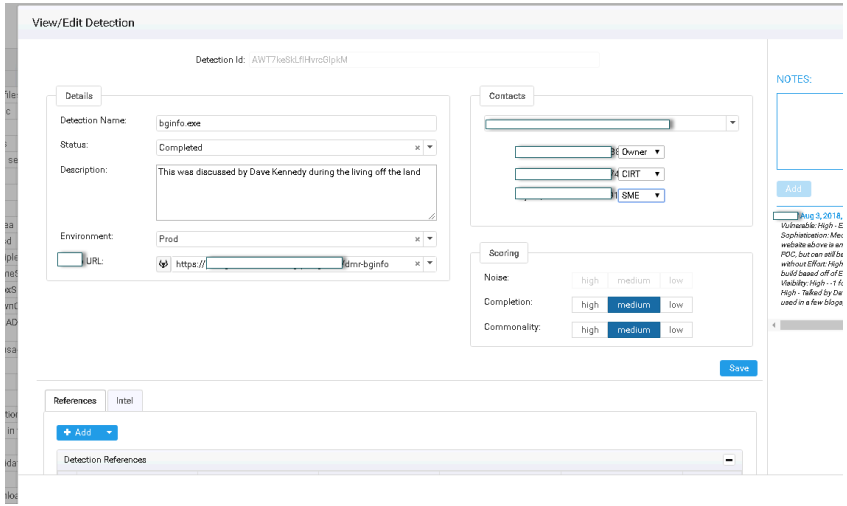
Way Ahead

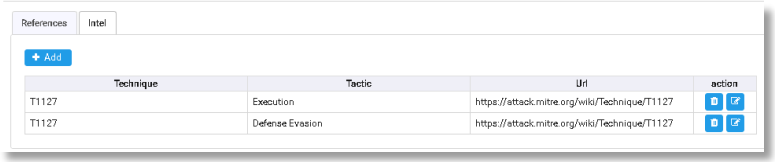
Ecosystem


MIST
(All)
AST
(Simulation)
DMR
(Blue)
SHP
(Mgmt Rpts)
PAX
(Suppress)
DSP
(Intel)
GWH
(Hunt)
Reports
Dashboards
ATT&CK
Event Mgmt & Alerting
Case Mgmt
Intel Provider
CI/CD
VCS/ Issues
SLACK

DMR – Detection Management Reporting

- **Prioritization**
  - Inputs from Intel/Hunt
- **Self contained**
  - Various components are stored/versioned together
- **Development Pipeline**
  - Idea to Implementation (and beyond)
- **Primary data source**
  - Source of record for other tools





DSP – Defense Security Posture

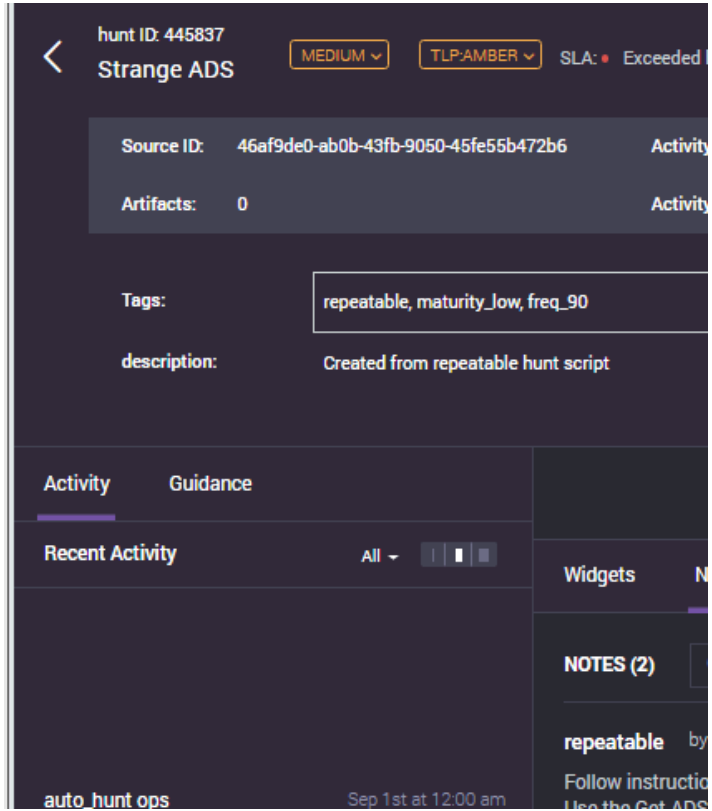
- **Detection ideas**
  - Feed DMR
- **Prioritization**
  - Risk determines detection's priority in DMR
- **Categorization**
  - ATT&CK tactics/techniques applied

MITRE ATT&CK

Technique	Priority	Real-Time/Hunt	Detection Rating	Mitigation Rating	Tactics	Notes	
Plist Modification	1	Real-Time	1	1	Defense Evasion, Persistence, Privilege Escalation		Submit
DCShadow	1	None	1	1	Defense Evasion		Submit
Standard Application Layer Protocol	1	None	2	3	Command And Control	D - None, M - Outbound FTP restricted. Opp - Implement DNS exfil capability. Check inbound/outbound HTTP/S ratio.	Submit
Fallback Channels	1	Real-Time	2	3	Command And Control	D - None, M - None. Opp - Enable [redacted]ignatures for Metasploit, Cobalt Strike and other detections that	Submit
Network Share Discovery	1	Real-Time	1	1	Discovery		Submit
Scheduled Task	1	Real-Time	3	2	Execution, Persistence, Privilege Escalation	D - [redacted]gs for .bat/.wbs/.exe added to scheduled tasks M - None	Submit

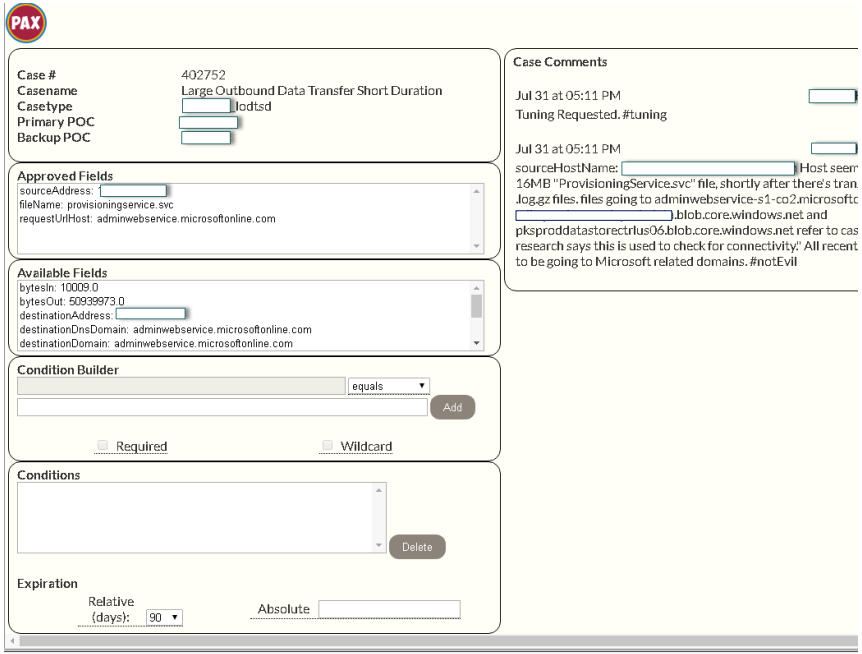
GWH – Good … Hunting tool

- **Detection ideas and feedback**
  - Feed DMR
  - Provide more insight for better detection creation
- **Recurring hunts**
  - Constraints limit some detections



PAX – Suppression Engine

- **Provide quick queue relief**
  - Silence noisy/false positive cases until detection can be updated
- **Multi-purpose**
  - Works at both the Event Alerting and Case Management level

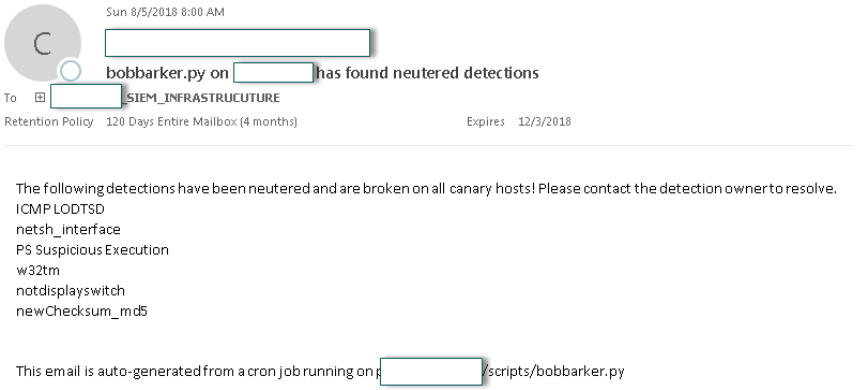


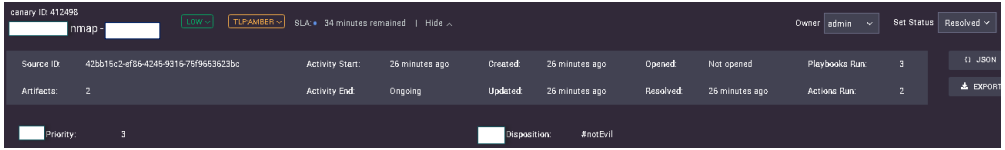
pax certutil.exe fake certificate with encoded binary

Condition	Last Match	Match Count	Case URL	Status
fileName equals davidsCanaryTesting CertUtil_Encode.txt	2018-08-06 18:50:12	47	Case	enabled

AST – A Simulation Tool

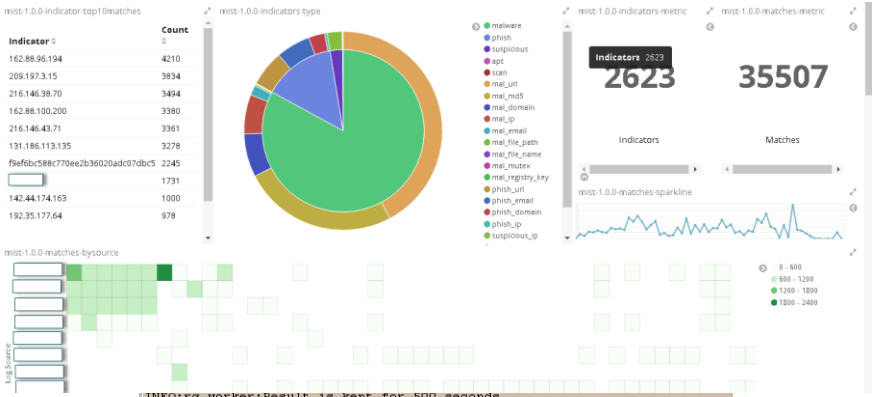
- **Canaries**
  - Test plumbing end to end
  - Early warning that detections are not working as designed
- **POC Execution**
  - Assists with detection development





MIST – Malicious Intel Search Tool

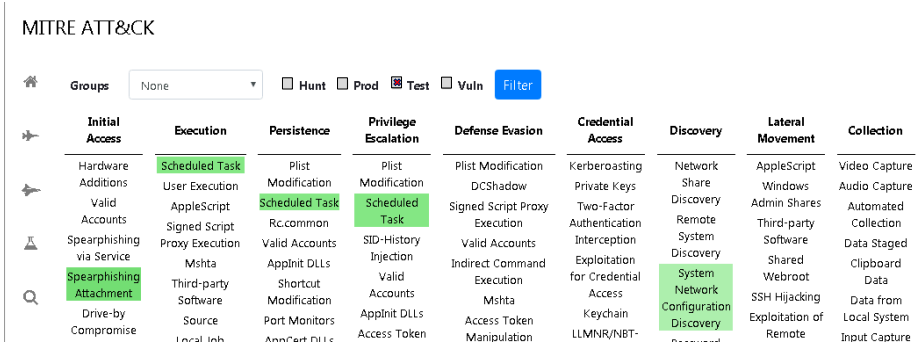
- **Tagged indicators of compromise**
  - Regressive search
- **Multiple queues**
  - Triage – determining if IOC worth tracking
  - Intel – IOCs being tracked
  - IR – IOCs identified during an incident
- **Matching events tagged and copied to a dedicated index**
  - Longer retention

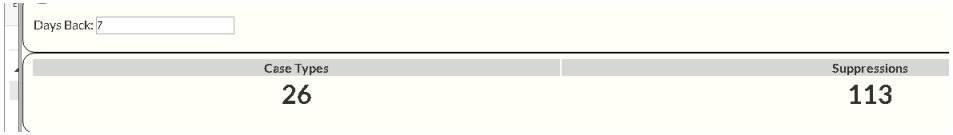



```
INFO:rq.worker:Result is kept for 500 seconds
21:06:20 default: intel_search.search(u'2443a4d58ad4bb70bac889bdfde9aebc',
 (2f541488-6757-48dd-ba43-5c3c37688168)
21:06:21 default: Job OK (2f541488-6757-48dd-ba43-5c3c37688168)
INFO:rq.worker:default: Job OK (2f541488-6757-48dd-ba43-5c3c37688168)
21:06:21 Result is kept for 500 seconds
INFO:rq.worker:Result is kept for 500 seconds
21:06:21 default: intel_search.search(u'2443a4d58ad4bb70bac889bdfde9aebc',
263124-307c-4ccb-a675-c57a4f941634)
21:06:22 default: Job OK (c7263124-307c-4ccb-a675-c57a4f941634)
INFO:rq.worker:default: Job OK (c7263124-307c-4ccb-a675-c57a4f941634)
21:06:22 Result is kept for 500 seconds
INFO:rq.worker:Result is kept for 500 seconds
21:06:22 default: intel_search.search(u'163554c8add0b45a404fd3f43e7f7b8b',
ccaa08d-41c5-456c-8797-cb3e709b38c5)
21:06:22 default: Job OK (2ccaa08d-41c5-456c-8797-cb3e709b38c5)
INFO:rq.worker:default: Job OK (2ccaa08d-41c5-456c-8797-cb3e709b38c5)
21:06:22 Result is kept for 500 seconds
```

SHP – Secure Hub Portal

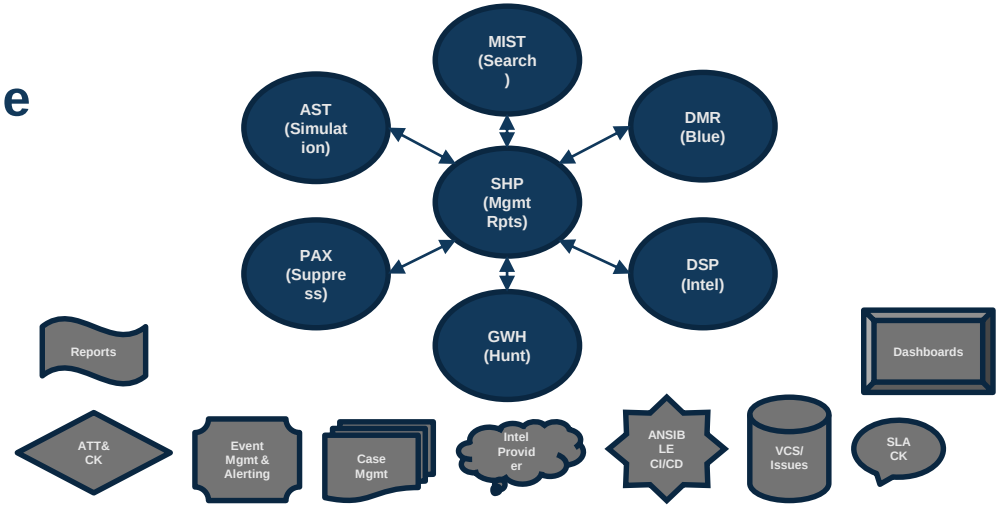
- **Management view**
  - Metrics
- **Reports**
  - Gaps
  - Detections on hold because of infrastructure/manpower/etc
  - Successes
  - ATT&CK tactics/techniques that gained more coverage
- **View into rest of tools**
  - How many new detections deployed





TBD – Gory Details and the Future

- **Python FTW**
- **Built on the great work in the community**
  - Ideas
  - Open source projects
- **Hope to give back**
  - Because we have used and learned so much
  - Slow to change, but trying…



Thank you for your time!

Any Questions?

USAA®