

Oct 23, 2018



ATT&CK: All the Things

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

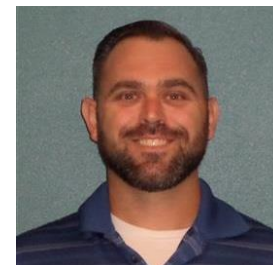
Neelsen Cyrus
@neelsen

David Thompson
@dirty_tizzle

- **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**



- 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



- **“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

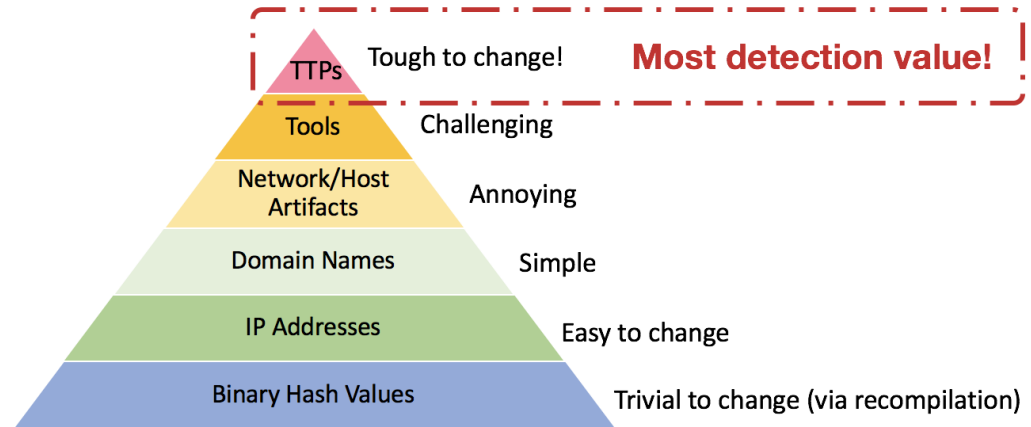
- Threat behavior that is operationally relevant & actionable

➤ 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



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
Applnit 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!



The screenshot shows a GitHub repository interface with a search bar at the top. Below the search bar, three items are listed, each with a title, a description, and a set of labels.

- Credential Manager**
#432 · opened 3 days ago by Thompson, David (PLN4788)
Labels: **ATT&CK Tactic - Credential Access**, **ATT&CK Technique - Create Account**, **Good for Prod**, **In-Development**
Source-IntelProvider Voted-High
- TaskKill Remotely - Parameters**
#431 · opened 3 days ago by Thompson, David (PLN4788)
Labels: **ATT&CK Tactic - Defense Evasion**, **ATT&CK Technique - Disabling Security Tools**, **Good for Prod**, **Source-InternalIdea**
Voted-High
- Powershell Start-BitsTransfer**
#412 · opened 4 weeks ago by Cyrus, Neelsen (ZG45591)
Labels: **ATT&CK Tactic - Exfiltration**, **ATT&CK Tactic - Lateral Movement**, **ATT&CK Technique - Exfiltration Over Alternative Protocol**
ATT&CK Technique - Remote File Copy, **Source-Mitre**, **Voted-High**

Integrating ATT&CK into our Ecosystem

USAA's ATT&CK Visualization tool

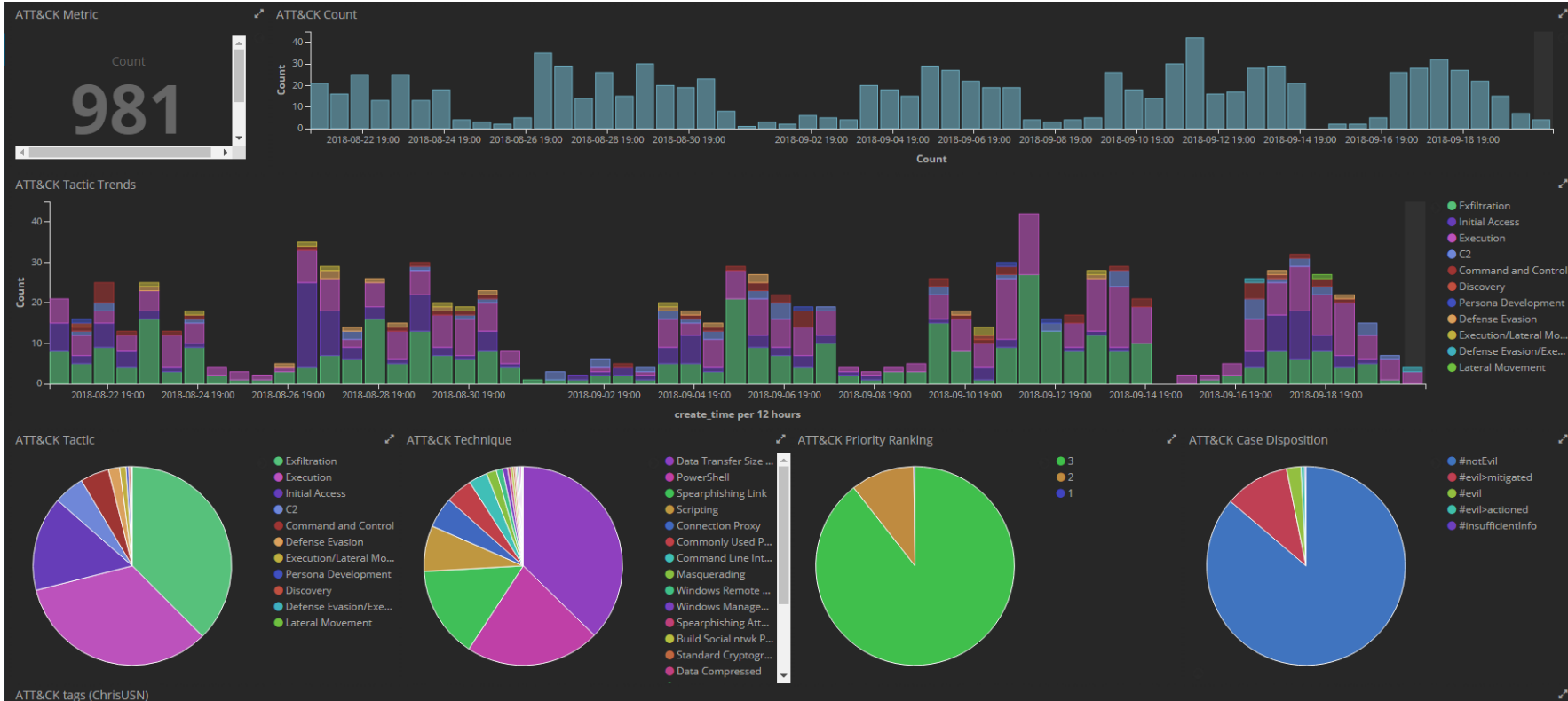
- Custom Tool – Based off of Navigator
- Python Flask App
- Updates MITRE data via API
- Correlating tags with respective techniques
 - Detection test/prod
 - Hunt
 - Intel
 - Adversary Capabilities

ATT&CK Coverage

Groups: None ☐ Prod ☒ Test ☐ Submit

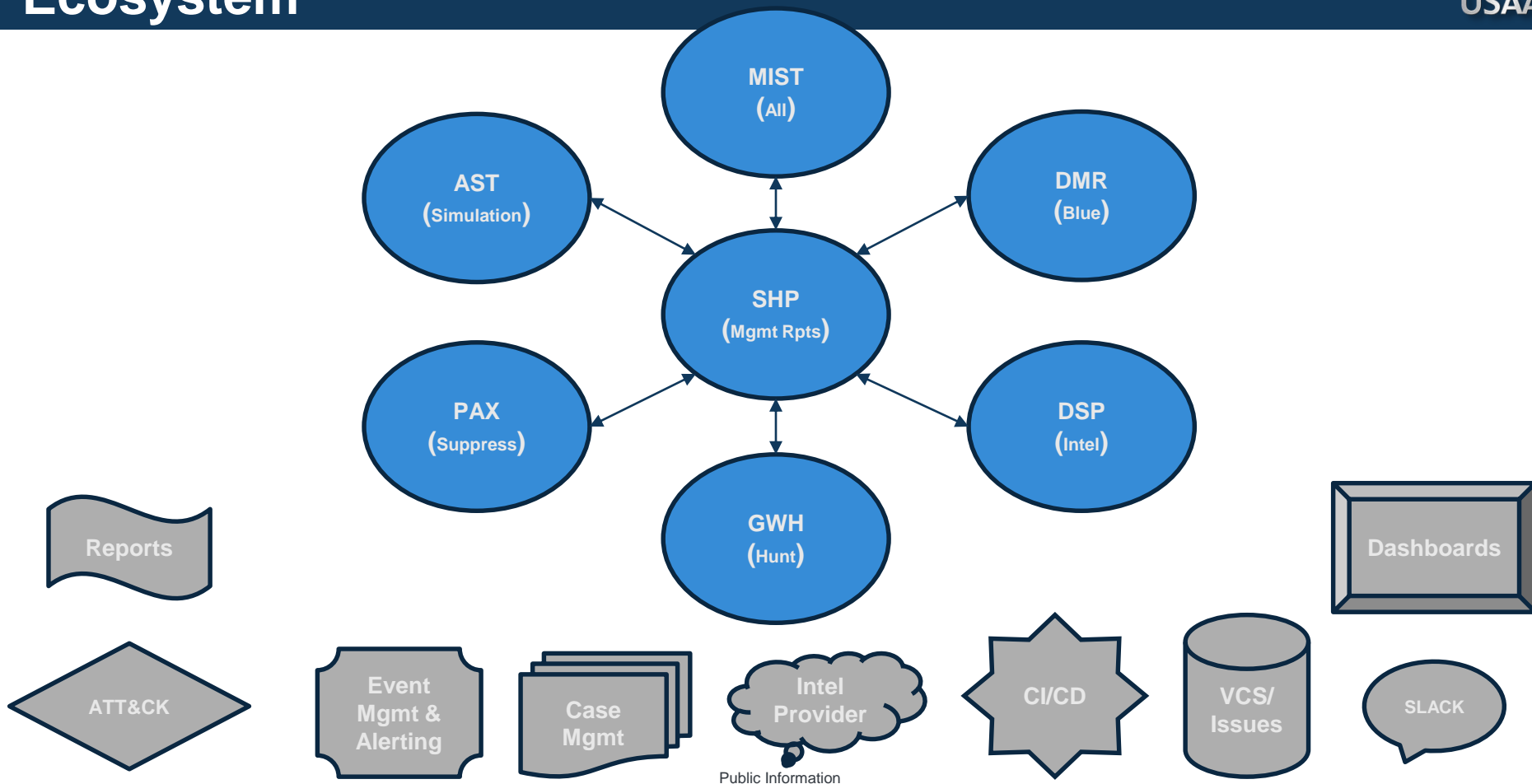
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInet DLLs	AppInet DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Dylib Hijacking	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Input Capture	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Component Firmware	Extra Window Memory Injection	DCShadow	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser	Screen Capture	Multi-Stage Channels
	LSASS Driver	File System Permissions Weakness	File System Permissions Weakness	DLL Search Order Hijacking	Keychain	Query Registry	SSH Hijacking	Video Capture		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Remote System Discovery	Shared Webroot			Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Security Software Discovery	Third-party Software			Multilayer Encryption
	Mishta	DLL Search Order Hijacking	Launch Daemon	Disabling Security Tools	Password Filter DLL	System Information Discovery	Windows Admin Shares			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Extra Window Memory Injection	Securityd Memory					Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	File Deletion	Two-Factor Authentication Interception					Standard Application Layer Protocol
	Rundll32	Hidden Files and	Port Monitors	File System Logical						Standard Cryptographic Protocol
	Scheduled Task									Standard Non-Application Layer Protocol
	Scripting									Uncommonly Used

Case Enrichment with ATT&CK



Way Ahead

Ecosystem



DMR – Detection Management Reporting

➤ Prioritization

➤ Inputs from Intel/Hunt

➤ Self contained

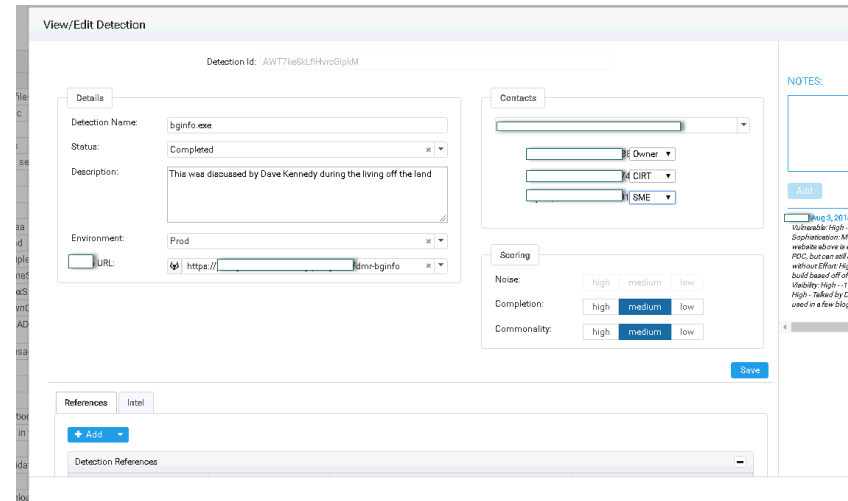
➤ Various components are stored/versioned together

➤ Development Pipeline

➤ Idea to Implementation (and beyond)

➤ Primary data source

➤ Source of record for other tools



View/Edit Detection

Detection Id: AWT7IeSdLfhvcoGlpkM

Details

Detection Name: bginfo.exe

Status: Completed

Description: This was discussed by Dave Kennedy during the living off the land

Environment: Prod

URL: https://dms-bginfo

Contacts

Owner

CIRT

SME

Scoring

Noise: high medium low

Completion: high medium low

Commonality: high medium low

References

Intel

+ Add

Detection References

Save

NOTES:

Aug 5, 2018, Vulnerable: High - E, Sophistication: Med, Mitigation: Above is an POC, but one will be without Effort. High build based off of E, Visibility: High - T E, High - talked by the used in the blog



Technique	Tactic	Url	action
T1127	Execution	https://attack.mitre.org/wiki/Technique/T1127	 
T1127	Defense Evasion	https://attack.mitre.org/wiki/Technique/T1127	 

DSP – Defense Security Posture

➤ Detection ideas

➤ Feed DMR

➤ Prioritization

➤ Risk determines detection's priority in DMR

➤ Categorization

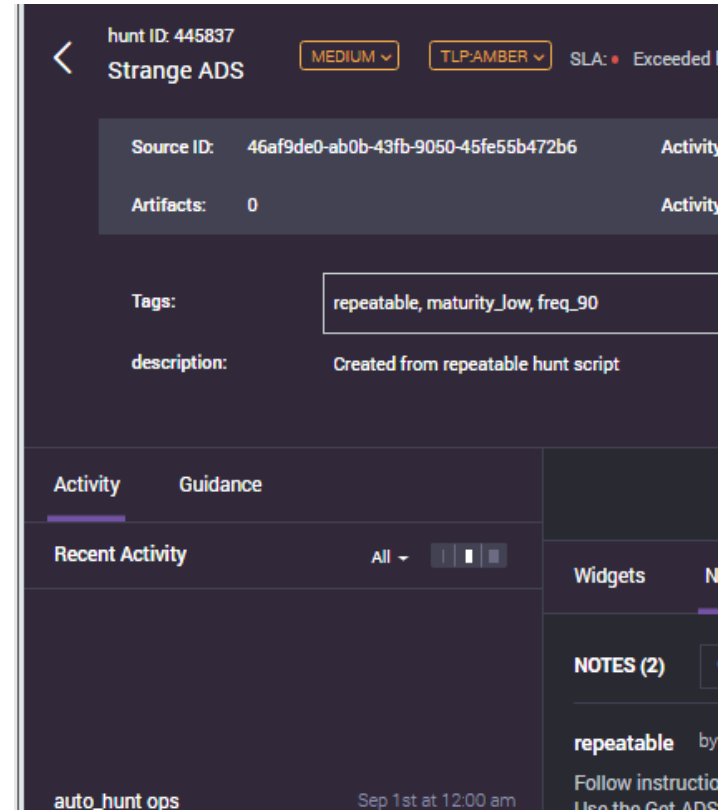
➤ ATT&CK tactics/techniques applied

MITRE ATT&CK

#	Technique	Priority	Real-Time/Hunt	Detection Rating	Mitigation Rating	Tactics	Notes	
+	Print Modification	1	Real-Time	1	1	Defense Evasion, Persistence, Privilege Escalation		Submit
+	DCShadow	1	None	1	1	Defense Evasion		Submit
Δ	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
Q	Fallback Channels	1	Real-Time	2	3	Command And Control	D - None, M - None, Opp - Enable [] signatures for Metasploit, Cobalt Strike and other detections that	Submit
Q	Network Share Discovery	1	Real-Time	1	1	Discovery		Submit
+	Scheduled Task	1	Real-Time	3	2	Execution, Persistence, Privilege Escalation	D - [] for lsat/lsat.exe added to scheduled tasks M - None	Submit

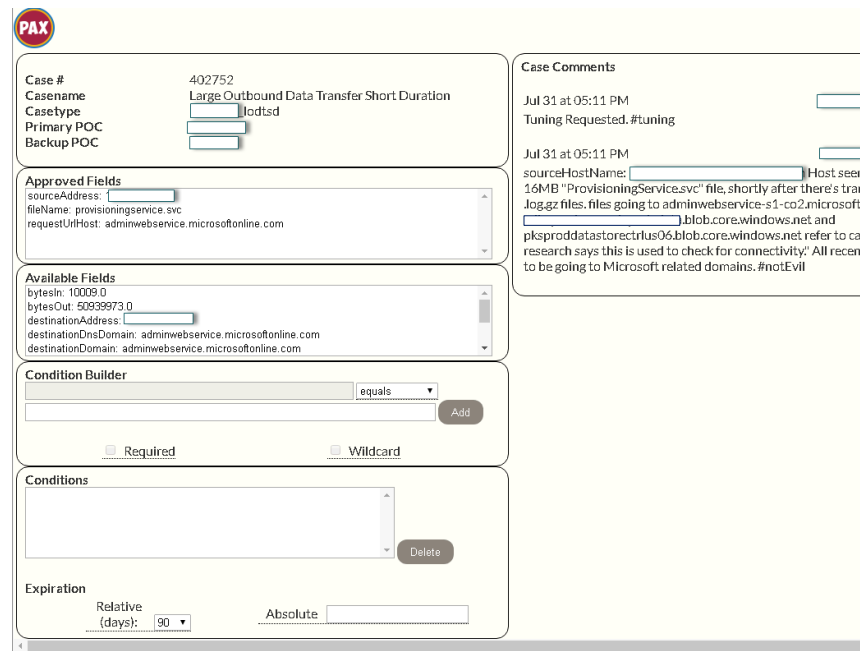
GWH – Good ... Hunting tool

- **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



The screenshot shows the PAX Suppression Engine interface. It includes a 'Case #' field with the value 402752, a 'Casename' field with 'Large Outbound Data Transfer Short Duration', and a 'Casetype' field with 'Jodtsd'. There are also fields for 'Primary POC' and 'Backup POC'. The 'Approved Fields' section contains a list of fields: 'sourceAddress', 'fileName', and 'requestUrlHost'. The 'Available Fields' section contains a list of fields: 'bytesIn', 'bytesOut', 'destinationAddress', 'destinationDnsDomain', and 'destinationDomain'. The 'Condition Builder' section has a dropdown menu set to 'equals' and a 'Add' button. The 'Conditions' section has a 'Delete' button. The 'Expiration' section has a 'Relative' dropdown set to '90' and an 'Absolute' dropdown.

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	

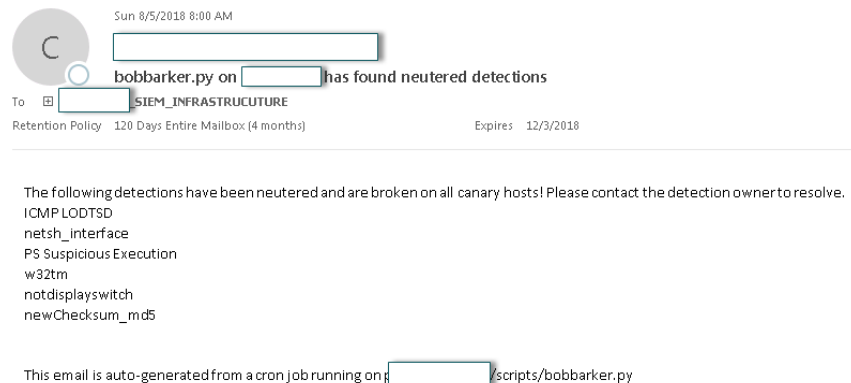
AST – A Simulation Tool

➤ Canaries

- Test plumbing end to end
- Early warning that detections are not working as designed

➤ POC Execution

- Assists with detection development

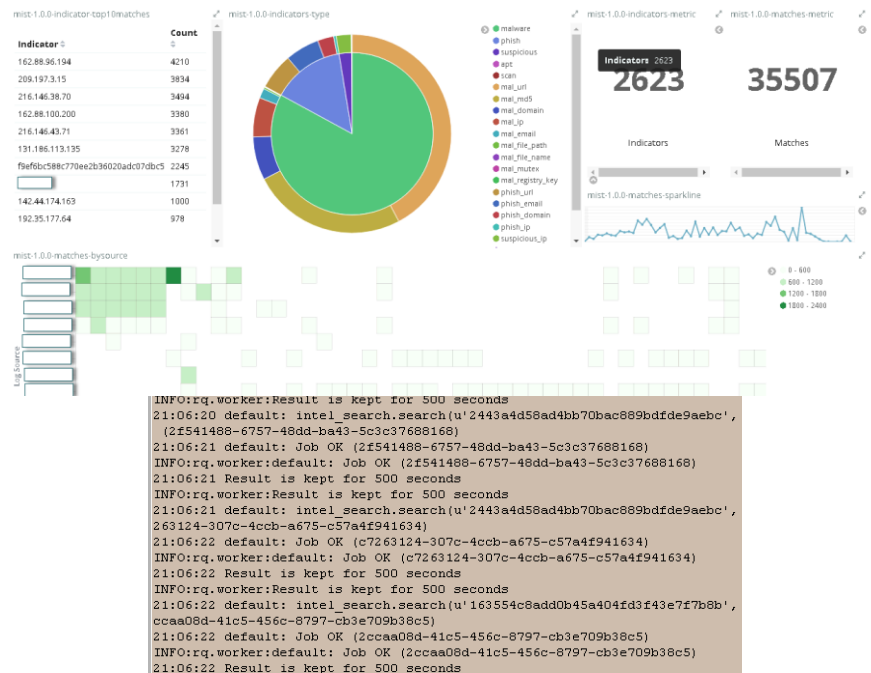


canary ID 412498									
[redacted] nmap - [redacted]		LOW	TLPAMBER	SLA: 34 minutes remaining	Hide		Owner: admin	Set Status: Resolved	
Source ID:	42bb15c2-ef06-4245-9316-79f9653623bc	Activity Start:	26 minutes ago	Created:	26 minutes ago	Opened:	Not opened	Playbooks Run:	3
Artifacts:	2	Activity End:	Ongoing	Updated:	26 minutes ago	Resolved:	26 minutes ago	Actions Run:	2
Priority: 3		Disposition: #notEvil							

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



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

MITRE ATT&CK

Groups: ☐ Hunt ☐ Prod ☒ Test ☐ Vuln

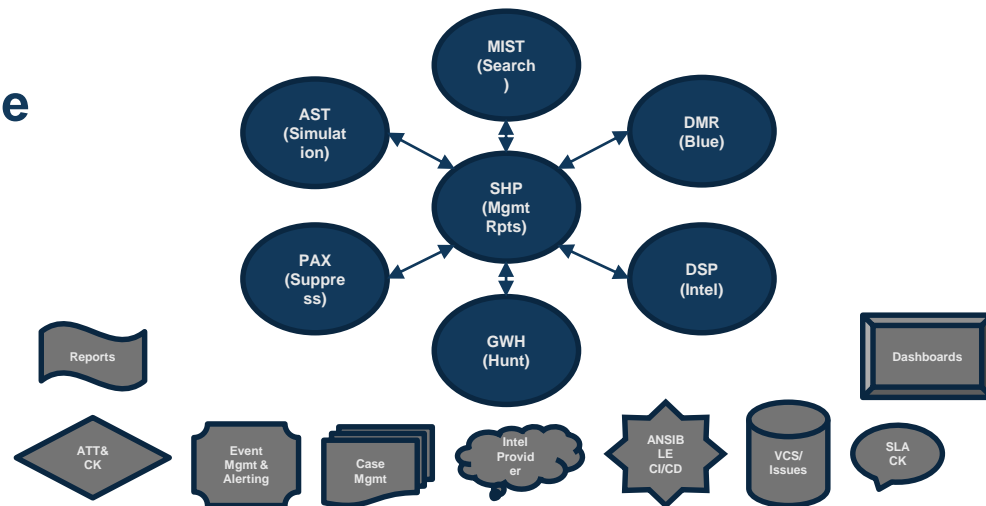
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Hardware Additions	Scheduled Task	Plist Modification	Plist Modification	Plist Modification	Kerberoasting	Network Share	AppleScript	Video Capture
Valid Accounts	User Execution	Modification	Modification	D/CShadow	Private Keys	Share Discovery	Windows Admin Shares	Audio Capture
Accounts	AppleScript	Scheduled Task	Scheduled Task	Signed Script Proxy Execution	Two-Factor Authentication Interception	Remote Discovery	Third-party Software	Automated Collection
Spearphishing via Service	Signed Script Proxy Execution	Rc.common	Scheduled Task	Valid Accounts	Exploitation for Credential Access	System Network Configuration Discovery	Shared Webroot	Data Staged
Spearphishing Attachment	Mshta	Valid Accounts	SID-History Injection	Indirect Command Execution	Keychain	SSH Hijacking	Webroot	Clipboard Data
Drive-by Compromise	Third-party Software	Applnit DLLs	Valid Accounts	Mshta	LLMNR/NBT-	Exploitation of Remote	SSH Hijacking	Data from Local System
	Source	Shortcut Modification	Applnit DLLs	Access Token Manipulation				Input Capture
	Local Job	Port Monitors	Access Token					
	Local Job	AppExec DLLs	Access Token					

Days Back:

Case Types	Suppressions
26	113

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?

