Getting Started with Risk-Based Alerting and MITRE

Bryan Turner
IT Security Analyst | Publix

splunk> .conf19

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 the 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.

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

splunk> .conf19

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:

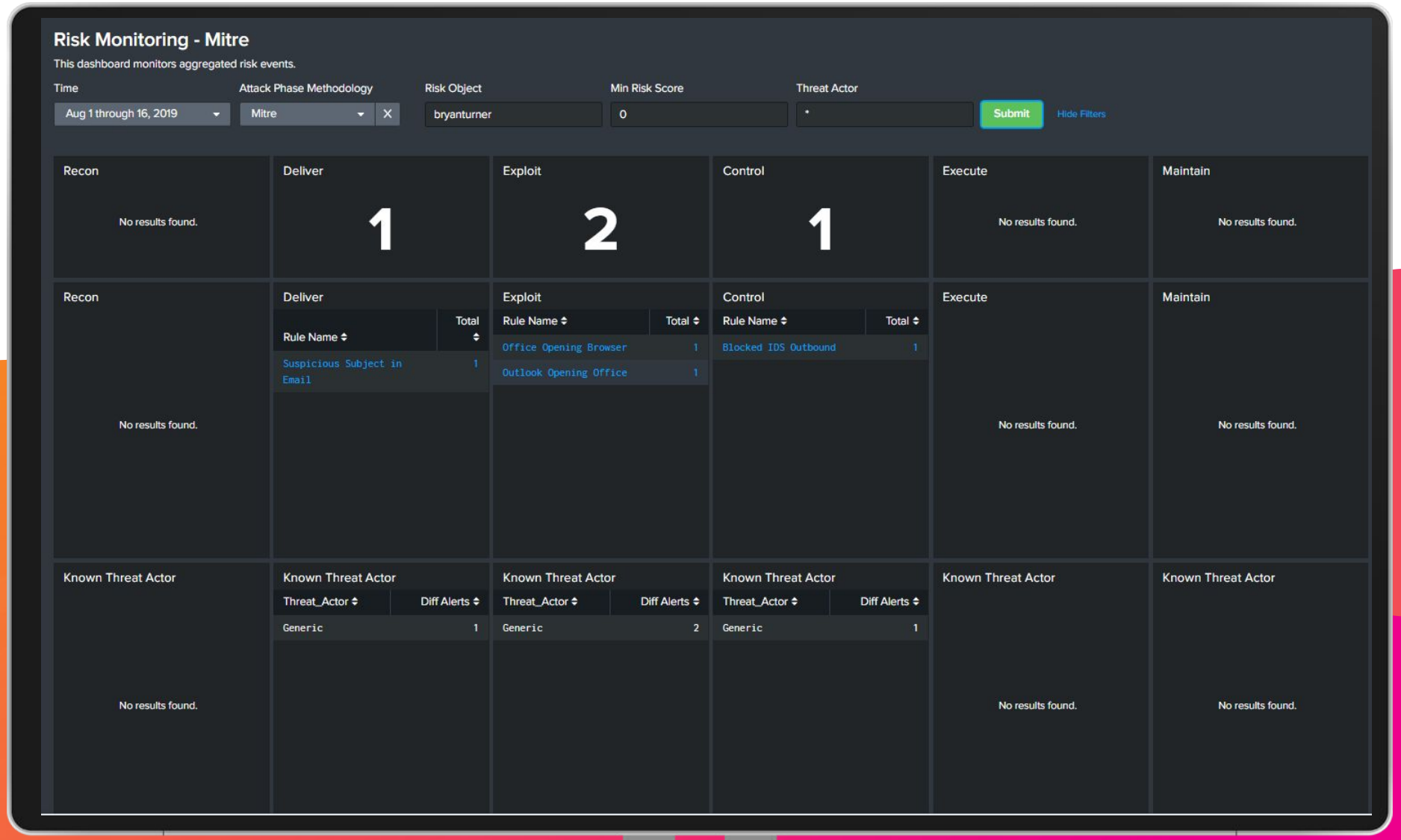
Alerts that provide little context and are not efficiently utilizing analyst's time.

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."

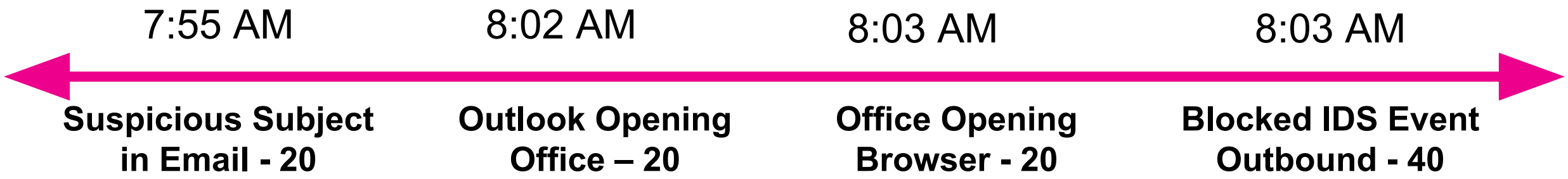
Risk Analysis framework in Splunk ES



splunk> .conf19

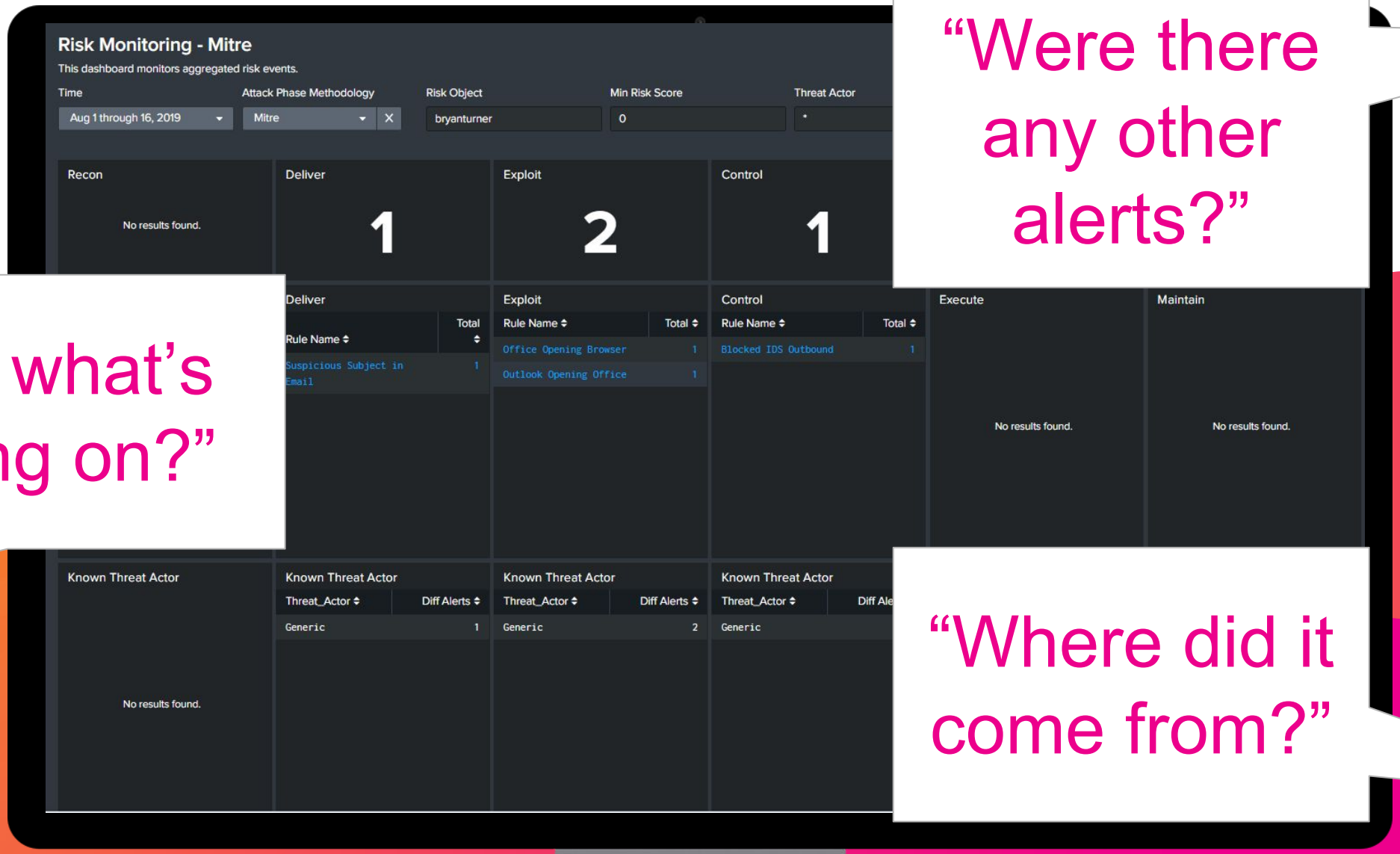
Risk Alerting Pipeline

How Does This Look in Practice?



Total Risk Score= 120

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



"So what's going on?"

"Were there any other alerts?"

"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

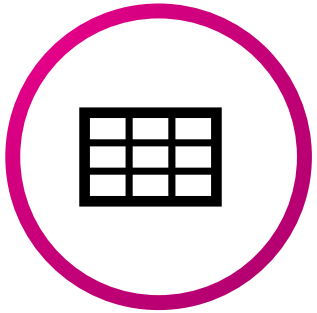
Scales smoothly

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

Phases of Development

Building an Search Inventory

Creating a Risk Matrix

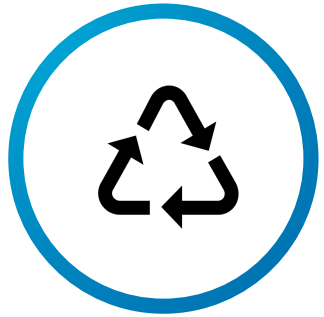


Building a Search Inventory

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

Risk	>50%	10%-50%	<10%
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.

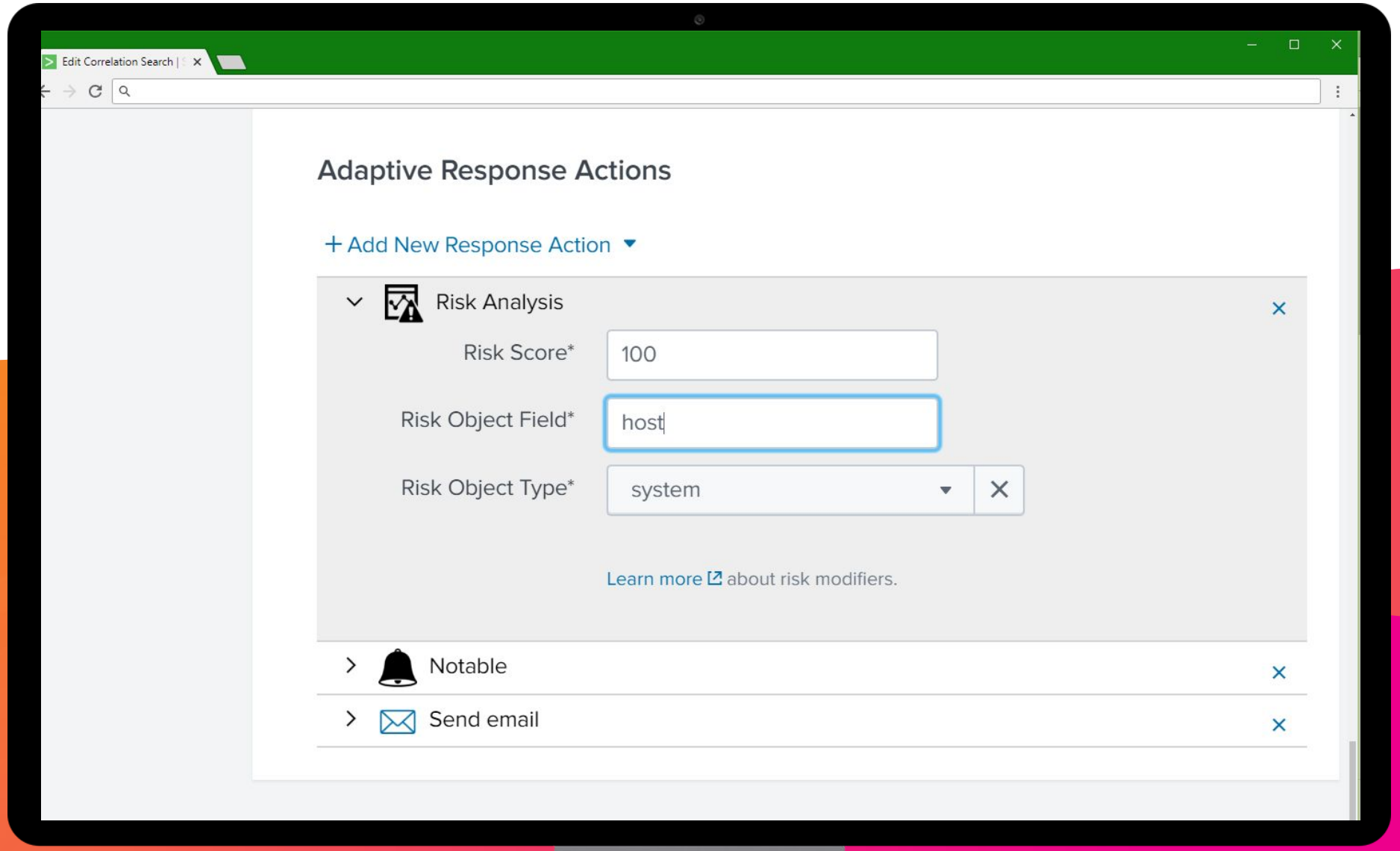
Risk Matrix

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



Sendalert

Customer Alert Actions

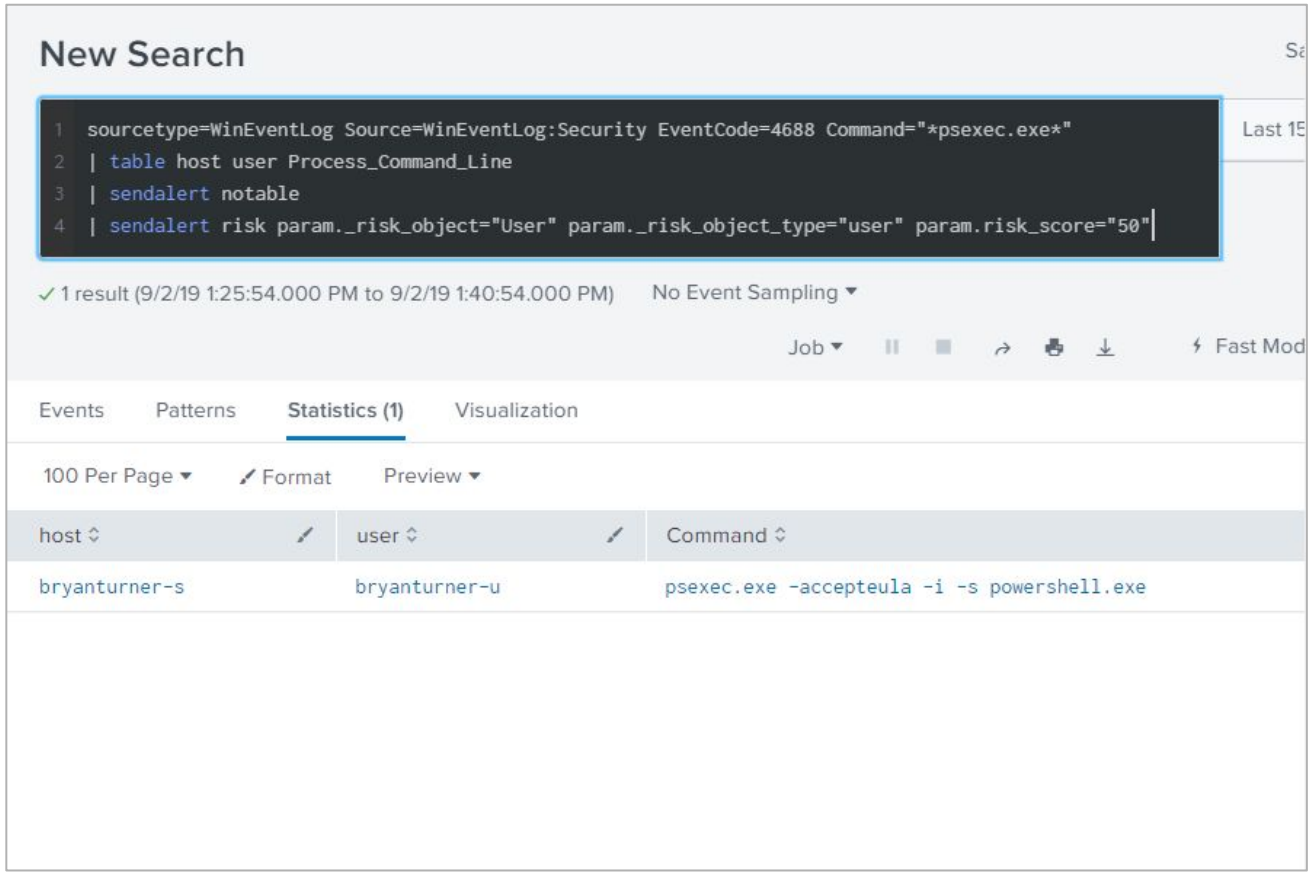
Use the sendalert command to:

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"
```

Last 15

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

Job Fast Mod

Events Patterns **Statistics (1)** Visualization

100 Per Page Format Preview

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

Alert Matrix

Base Value

Severity	Base Value
Informational	20
Low	40
Medium	60
High	80
Critical	100

Getting Fancy

Fidelity	Multiplier
Low <10%	.50
Medium 10%-50%	.75
High >50%	1.00

Criticality

Asset/Identity	Multiplier
Normal	1
Elevated	2
Enterprise	3

**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_iventory.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

splunk> .conf19

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

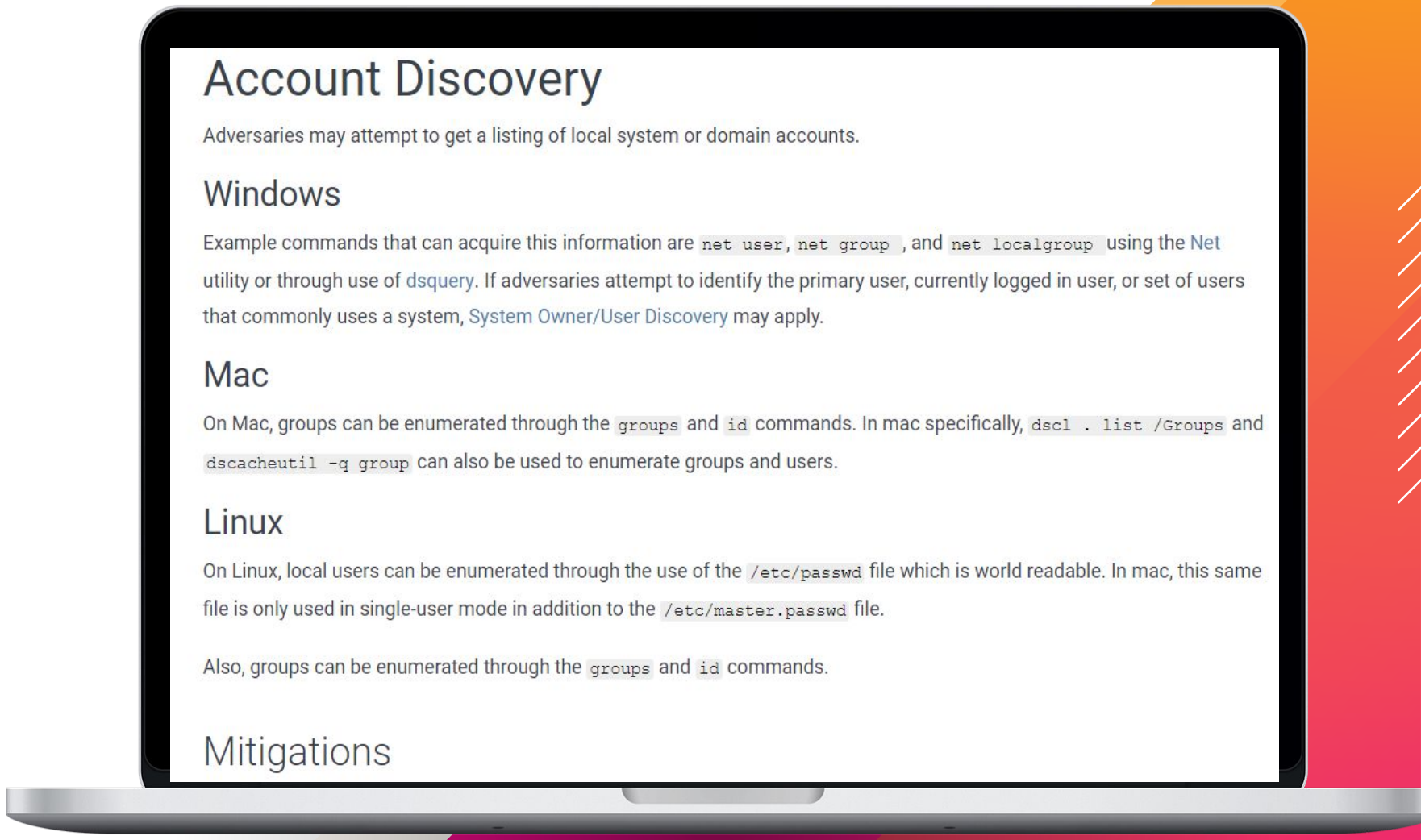
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	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	AppInit 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

splunk> .conf19

MITRE

Techniques In-Depth

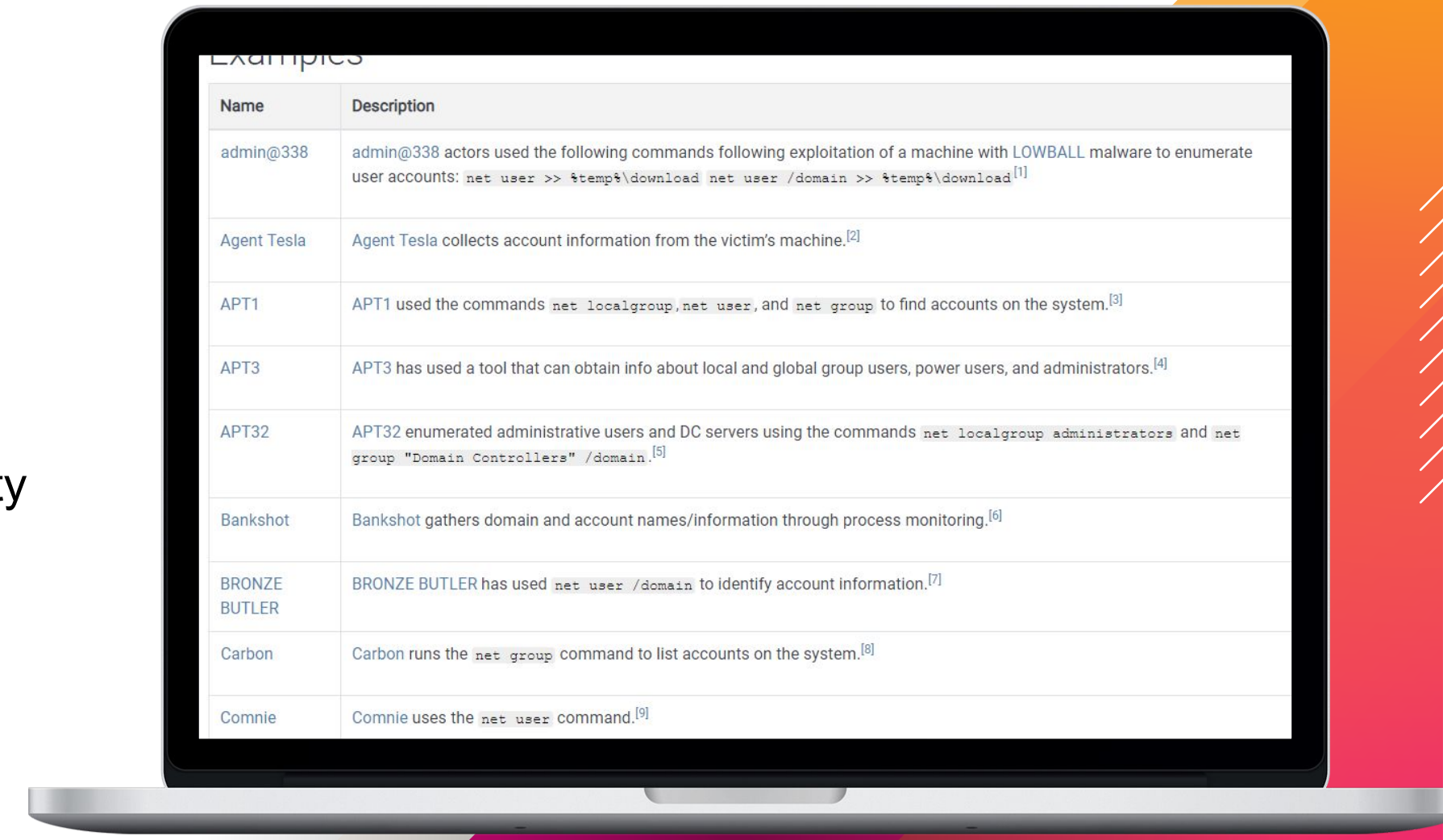
- Description of technique
- Mitigations
- Examples
- Detection
- References



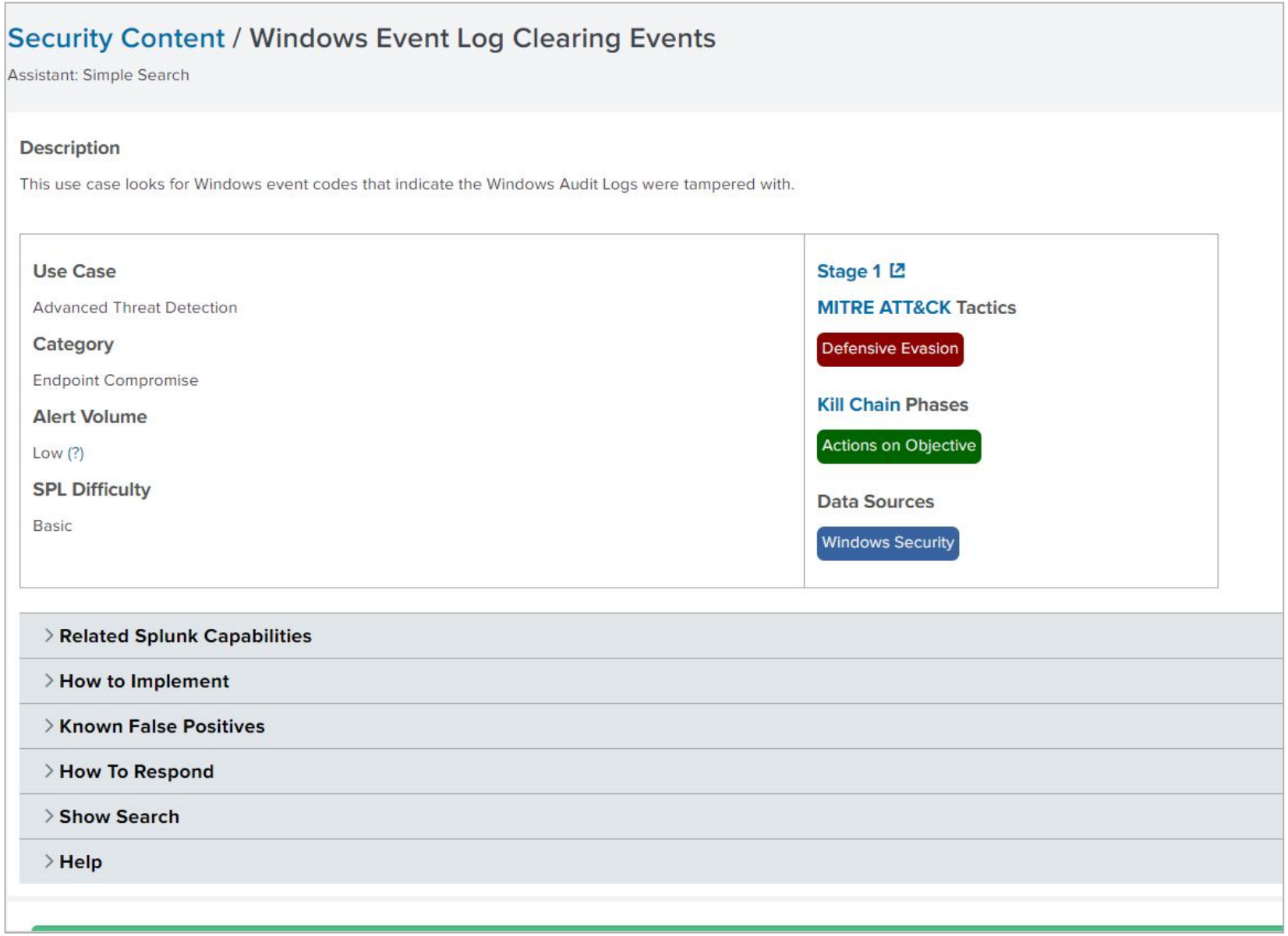
MITRE

Techniques In-Depth

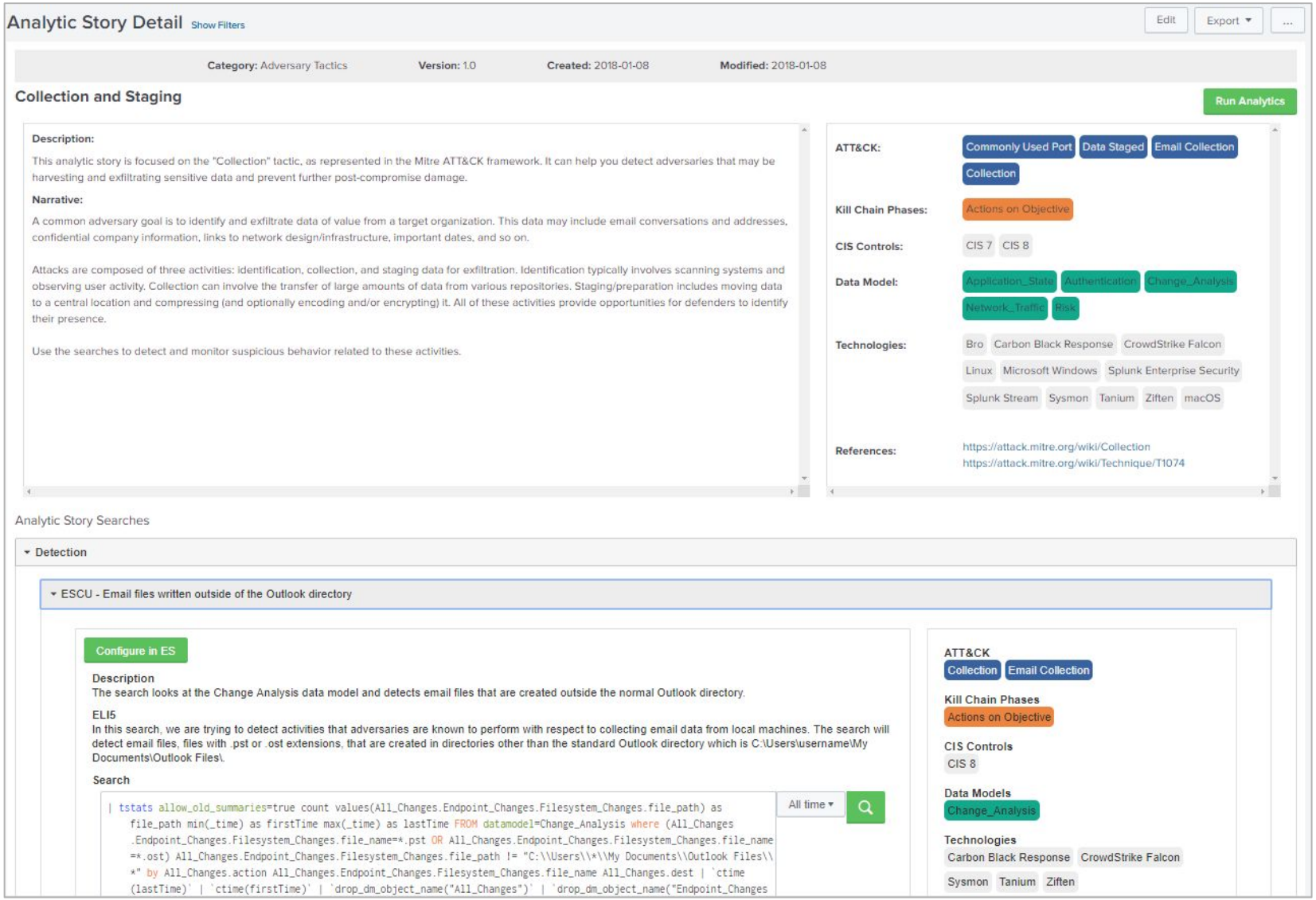
- Use examples to identify search terms
- Split into different severity alerts by fidelity
- Focus on threat actors that are the greatest risk



Security Essentials



Content Update



splunk> .conf19

Using MITRE for Targeted Detections

Building your narratives

splunk> .conf19

Prioritizing Alert Creation

What tools do you need?

MITRE ATT&CK

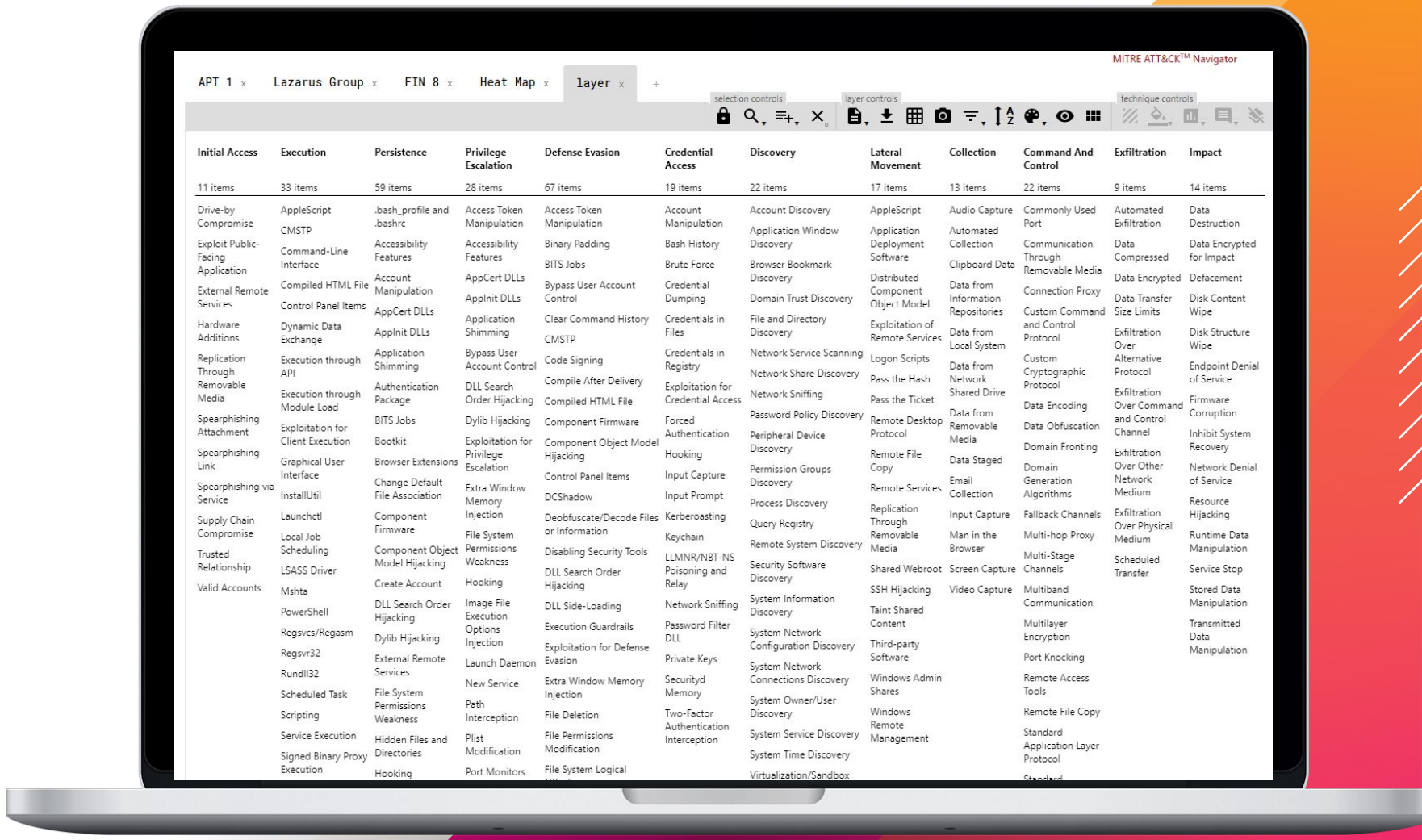
ATT&CK Navigator

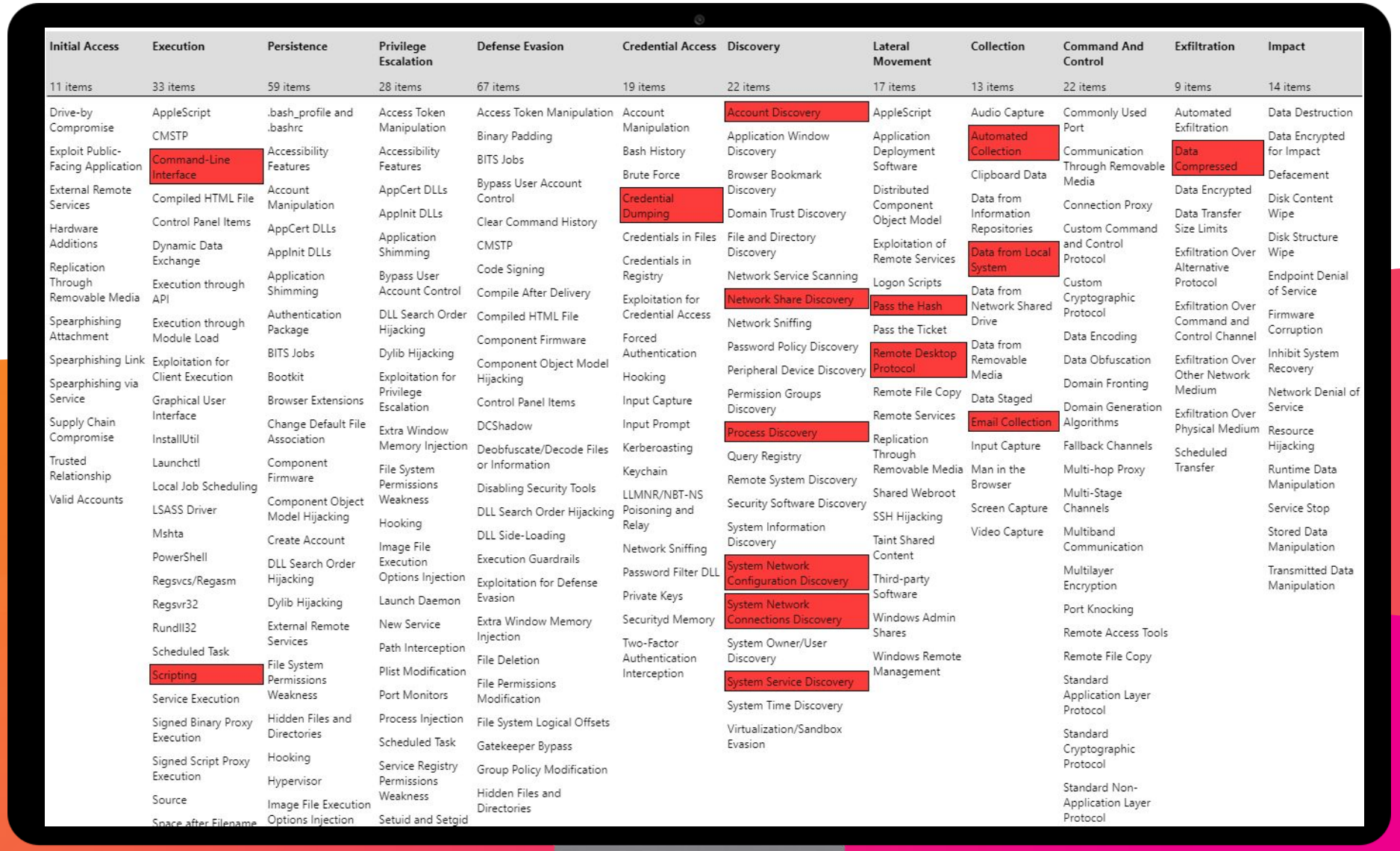
Malware Archaeology

OSINT

ATT&CK NAVIGATOR

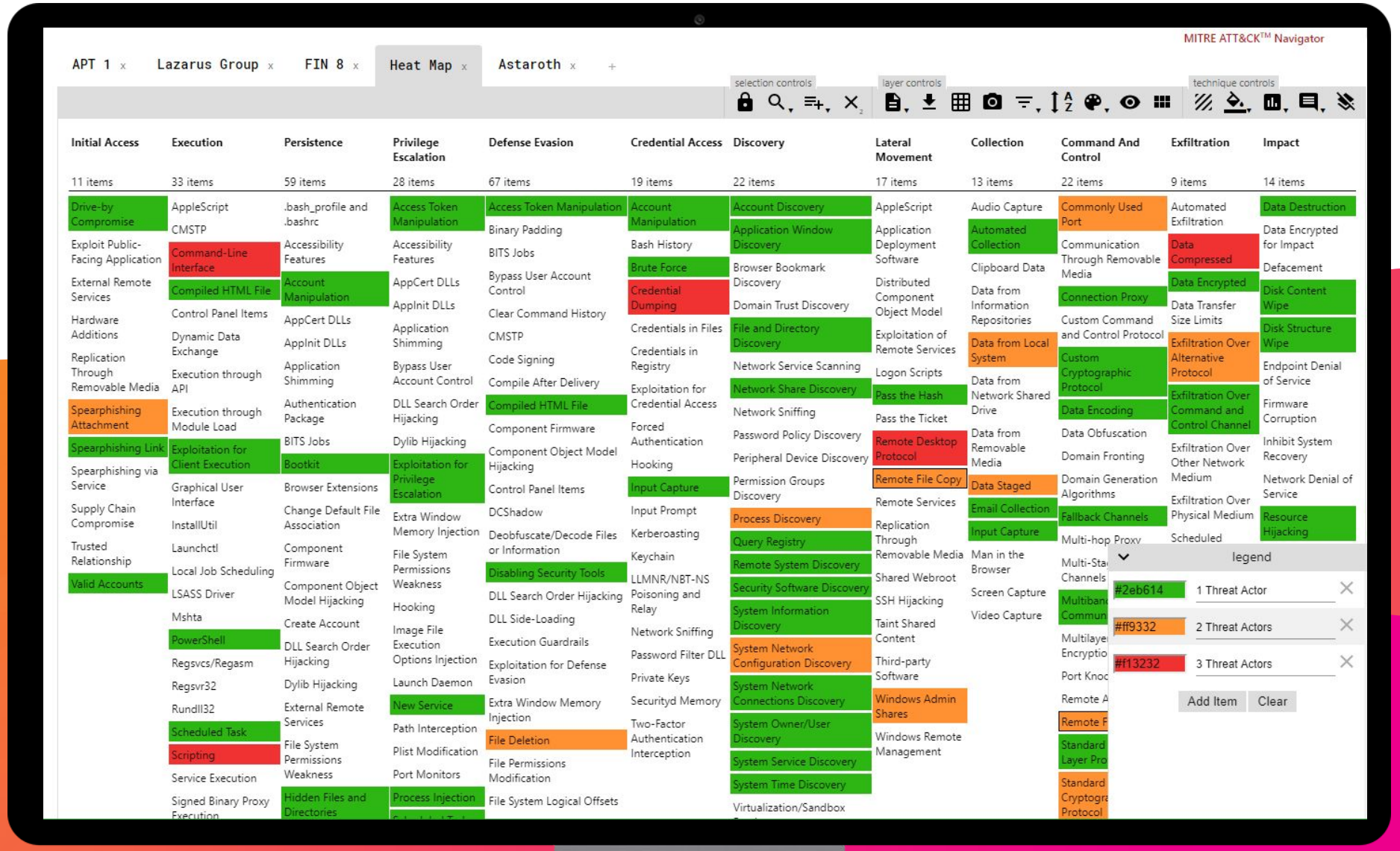
- List techniques by threat actor or malware
- Layer different views to form a heat map





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	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	AppInit 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
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery					
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution			File System Logical Offsets							
	Signed Script Proxy Execution			Gatekeeper Bypass							
	Source			Group Policy Modification							
	Space after Filename			Hidden Files and Directories							

splunk> .conf19



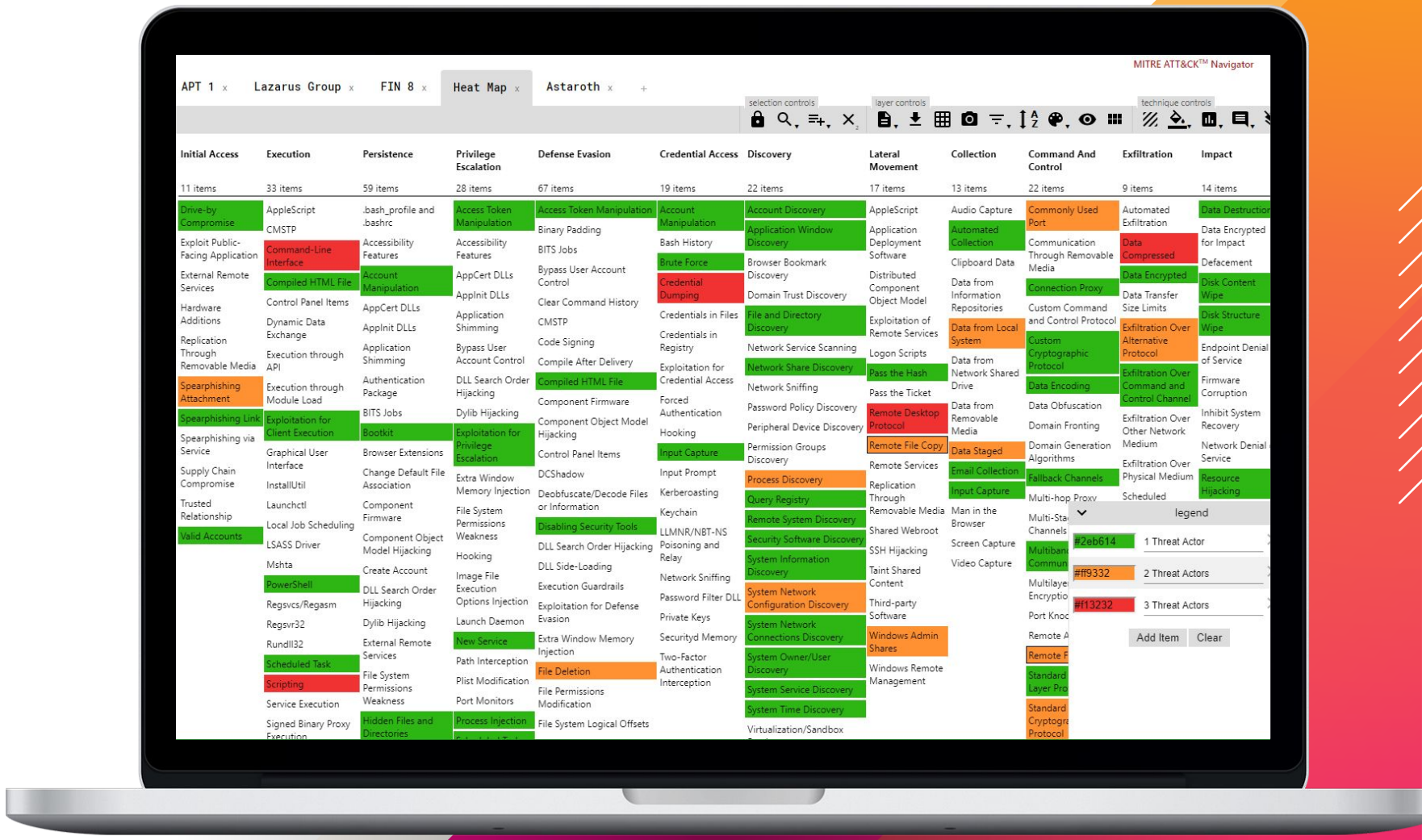
splunk> .conf19

Building a Heat Map

Identifying Priority

High Priority Items

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



splunk> .conf19

Malware Archaeology

https://www.malwarearchaeology.com/logging

Log sources by Tactic>Technique

Highlights whether coverage is:

- Good
- Incomplete
- None

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 monitorin
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 monitorin
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 monitorin

Malware Archaeology

https://www.malwarearchaeology.com/logging

Recommended Sources:

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

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 monitorin
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 monitorin
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 monitorin

OSINT

Digging Deeper

SANS

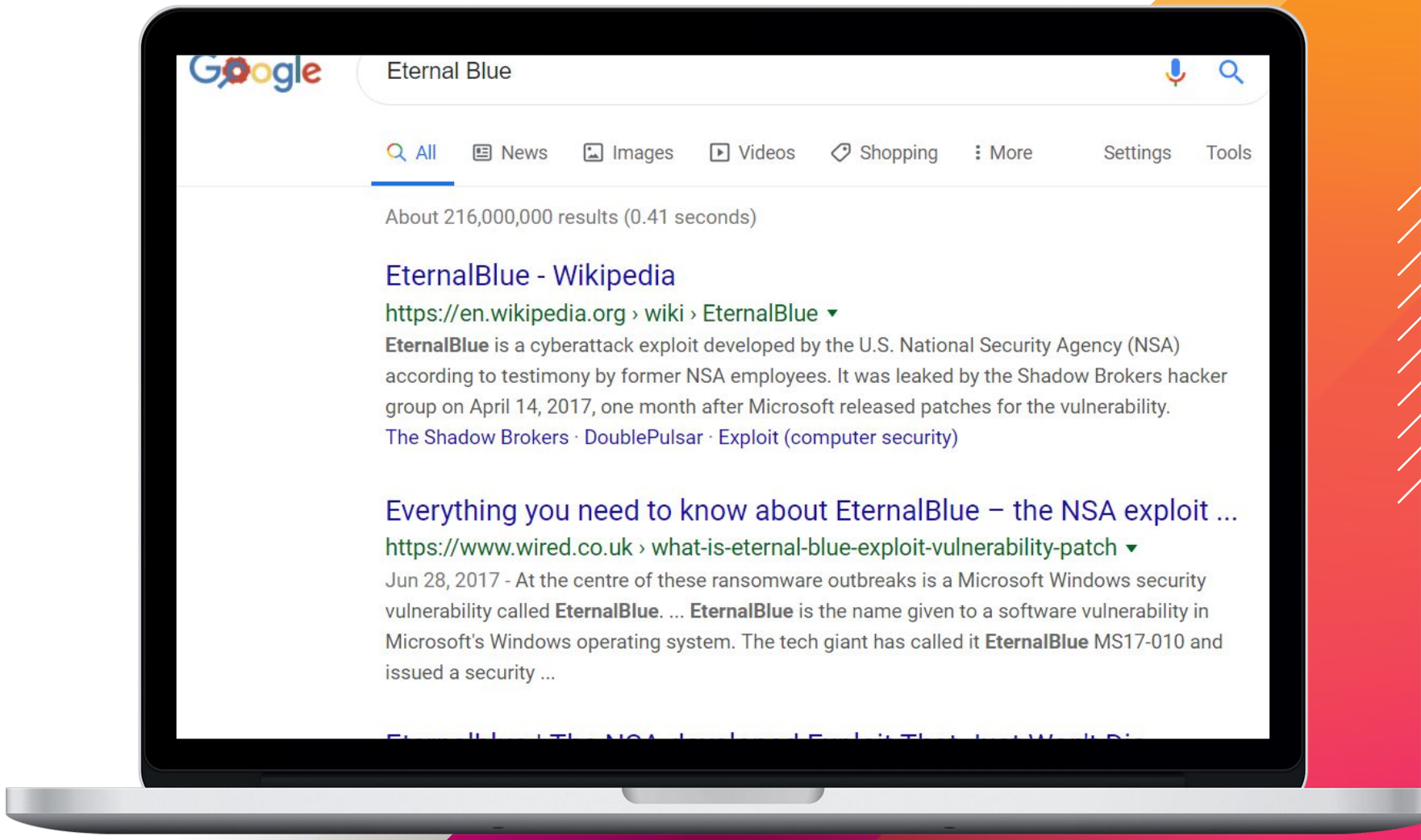
Talos

Microsoft

Twitter

Google

Personal Research



Operationalizing Alerting

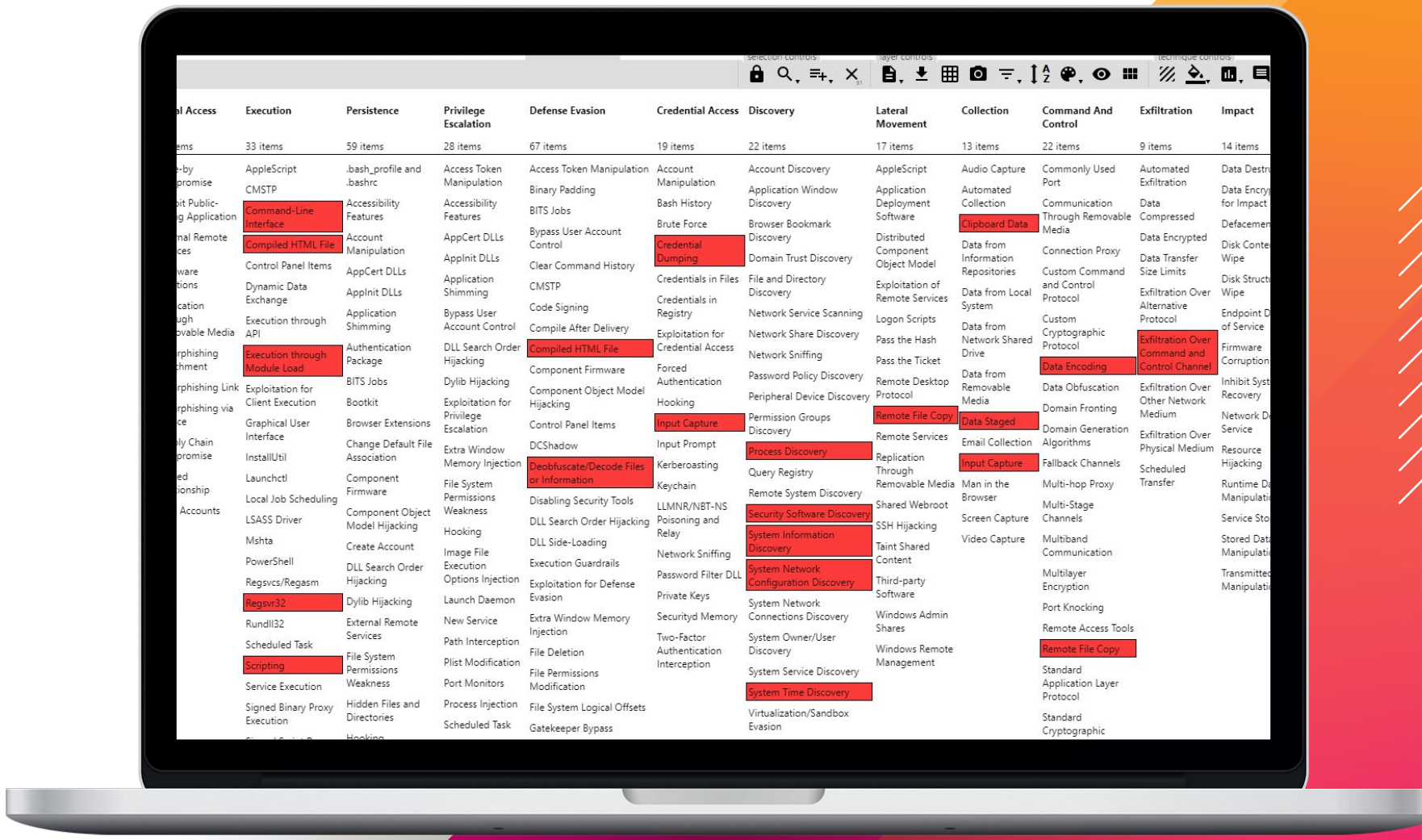
Reading the narrative

splunk> .conf19

Walkthrough

Astaroth – Known Techniques

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

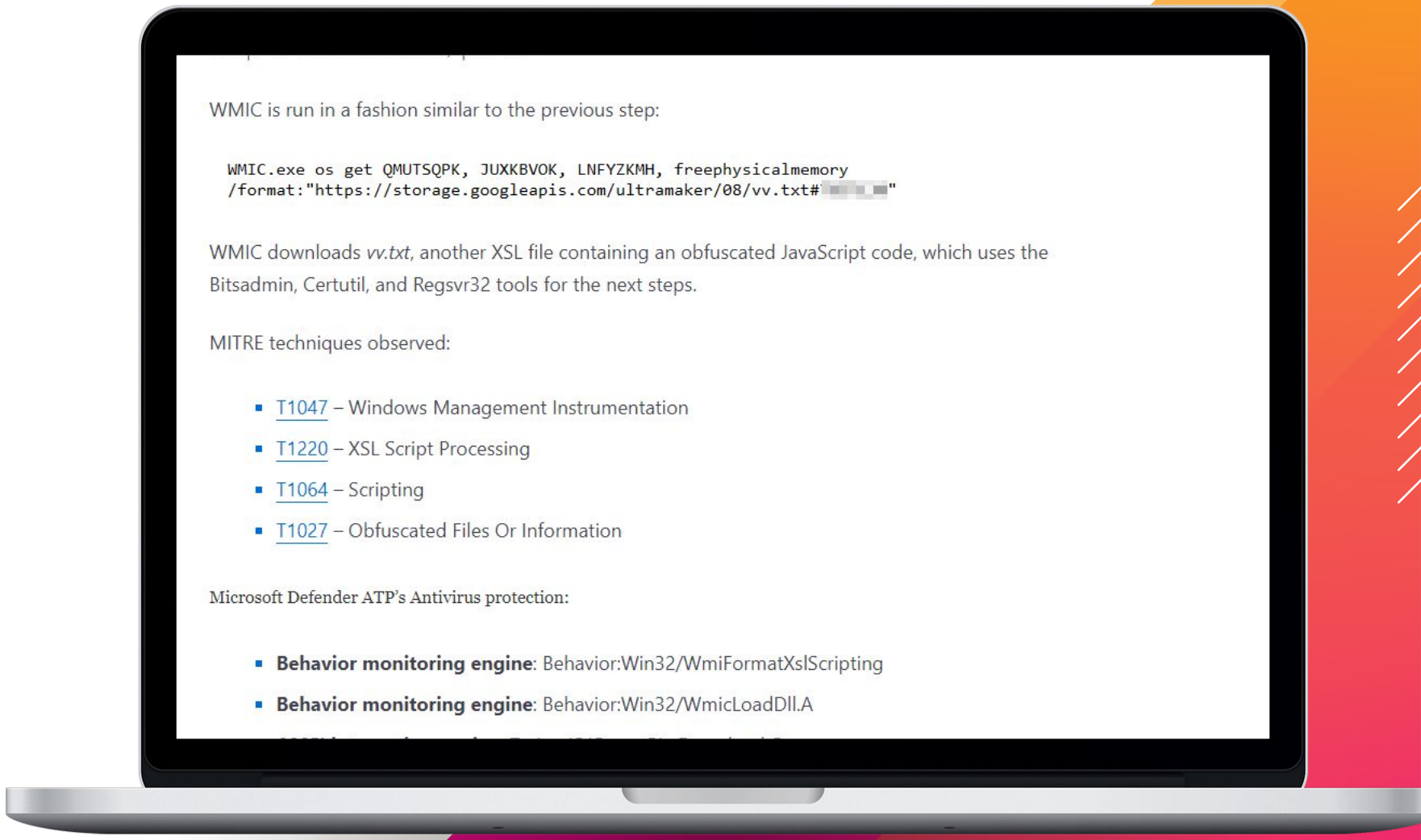


Walkthrough

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



Walkthrough

Astaroth – Building Detections

Shortcut Modification

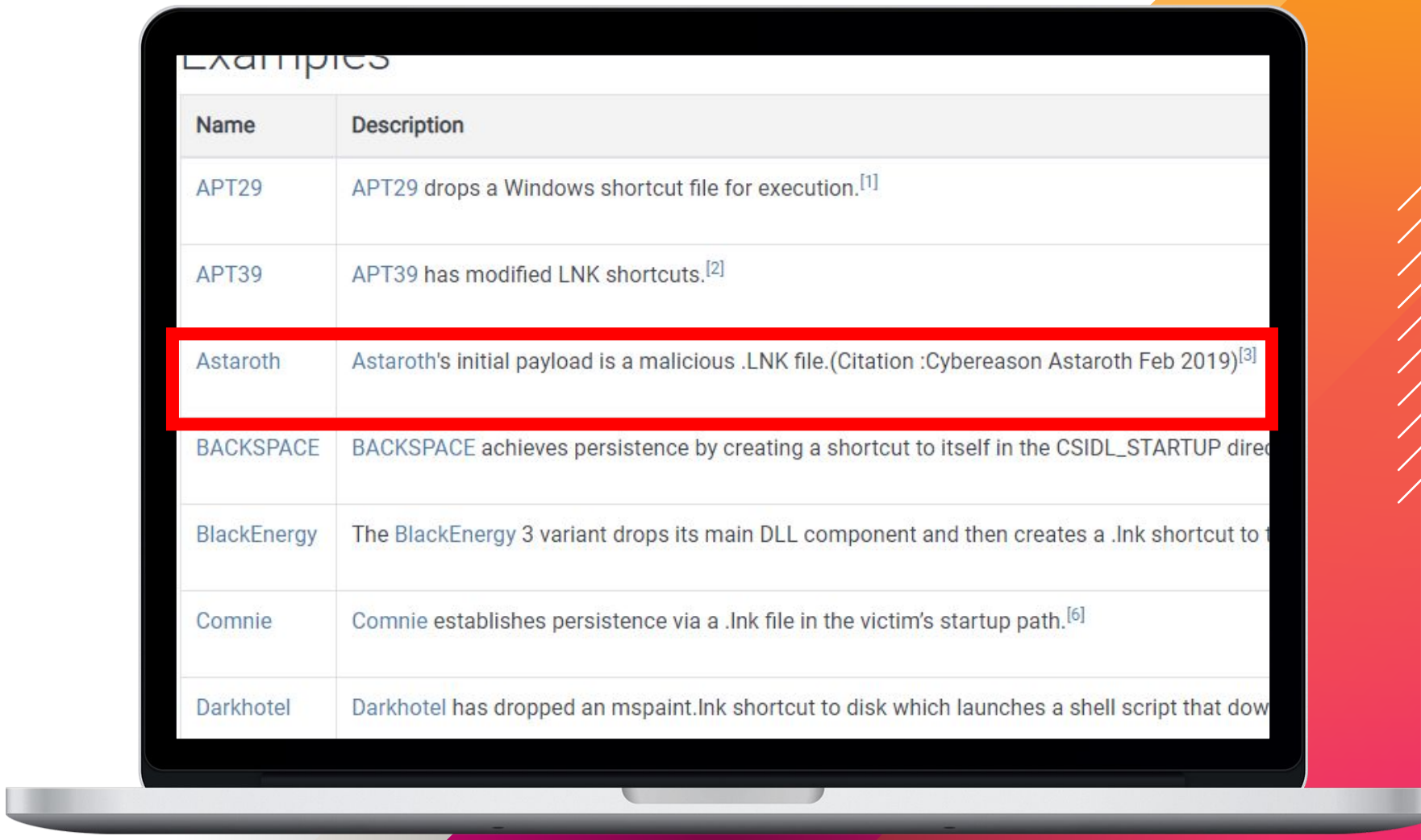
- Malicious LNK shortcuts

Obfuscated Files or Information

- Obfuscated jscript

Deobfuscate/Decode Files or Information

- Uses fromCharCode()

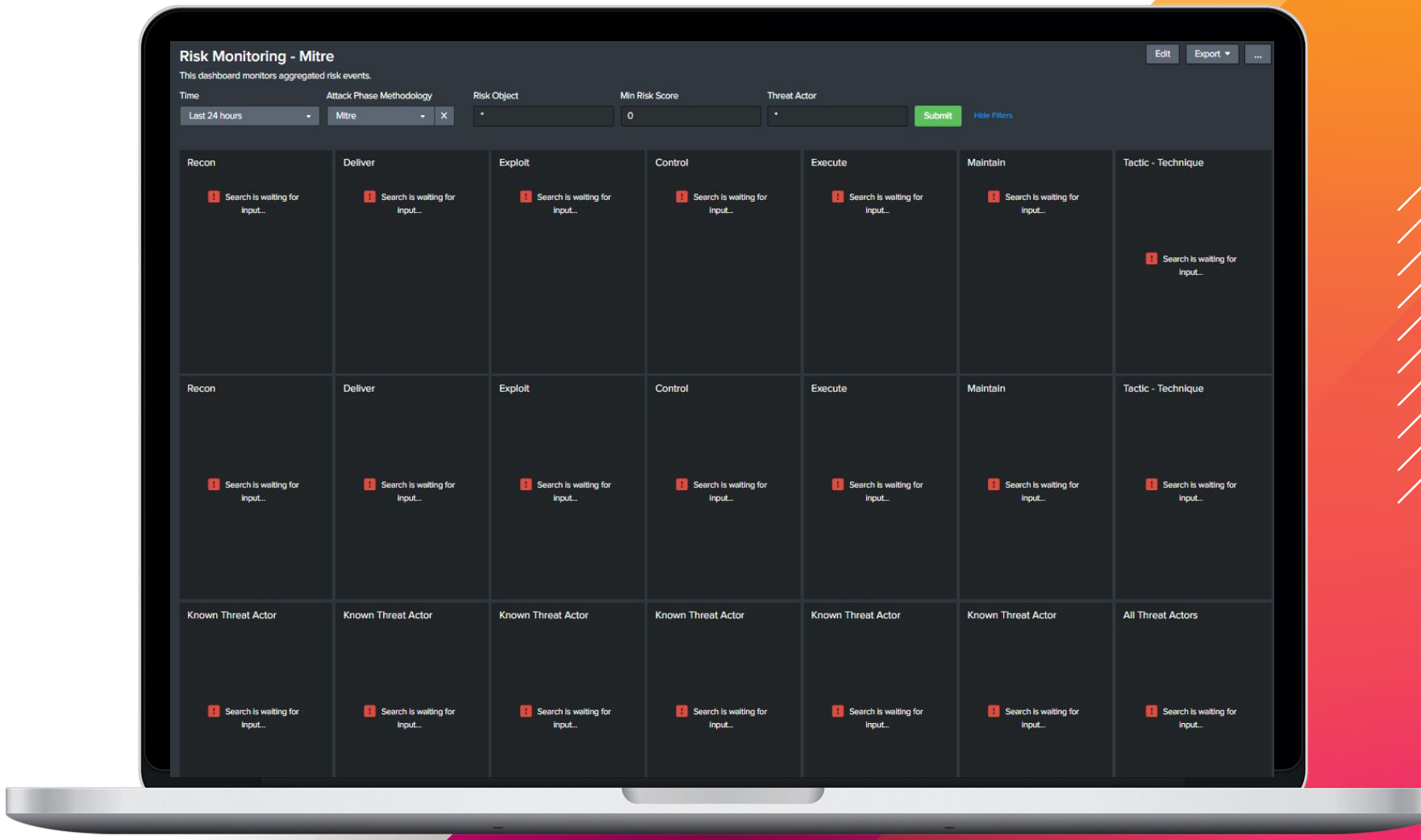


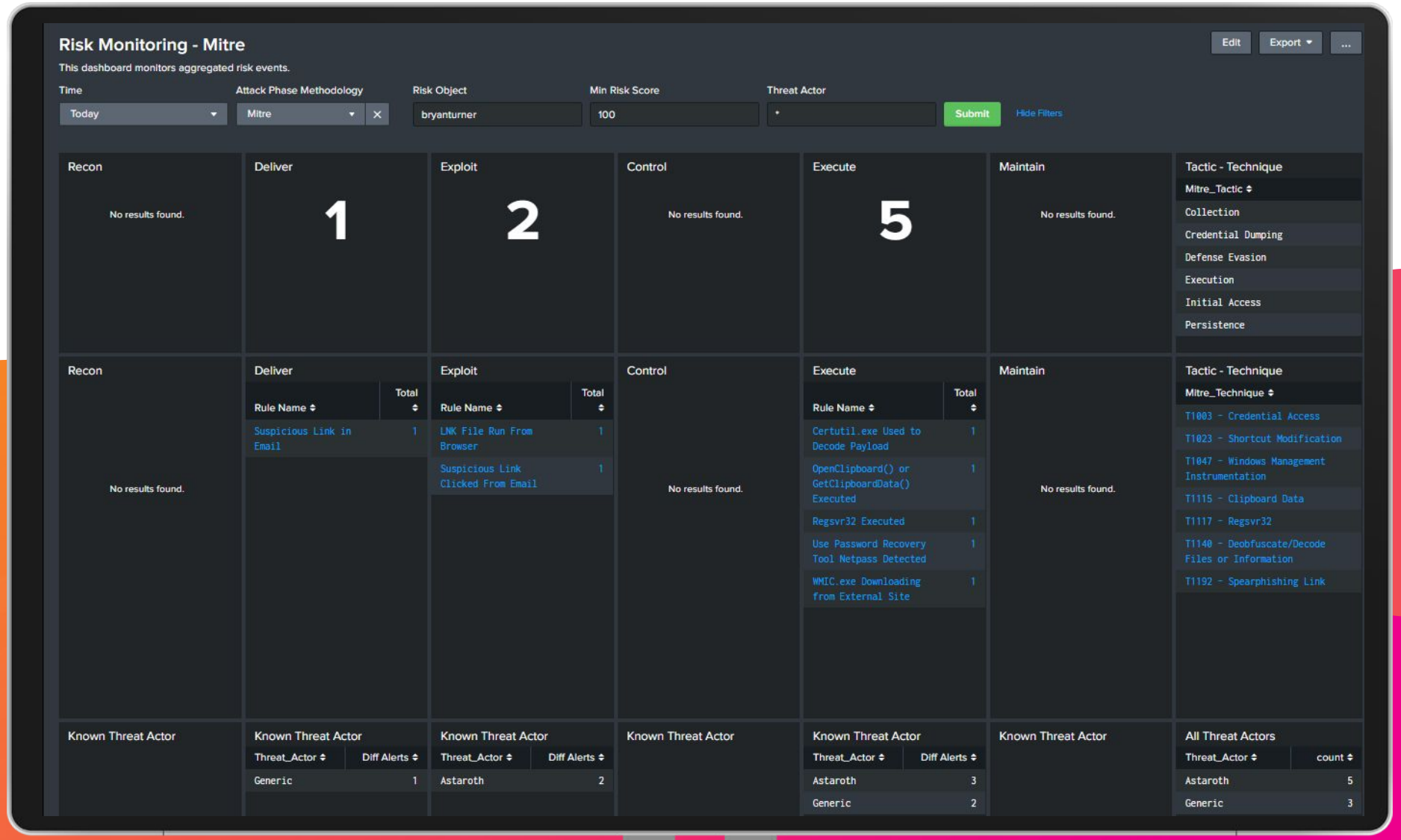
ATT&CK	Tactic	Technique	RiskObjectType	RiskScore	RiskObject	RuleName	Threat Actor
Deliver	Initial Access	T1193 - Spearphishing Attachment	user	20	recipient	Suspicious Subject in Email	Generic
Exploit	Execution	T1203 - Exploitation for Client Execution	user	20	Account	Outlook Opening Office	Generic
Exploit	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

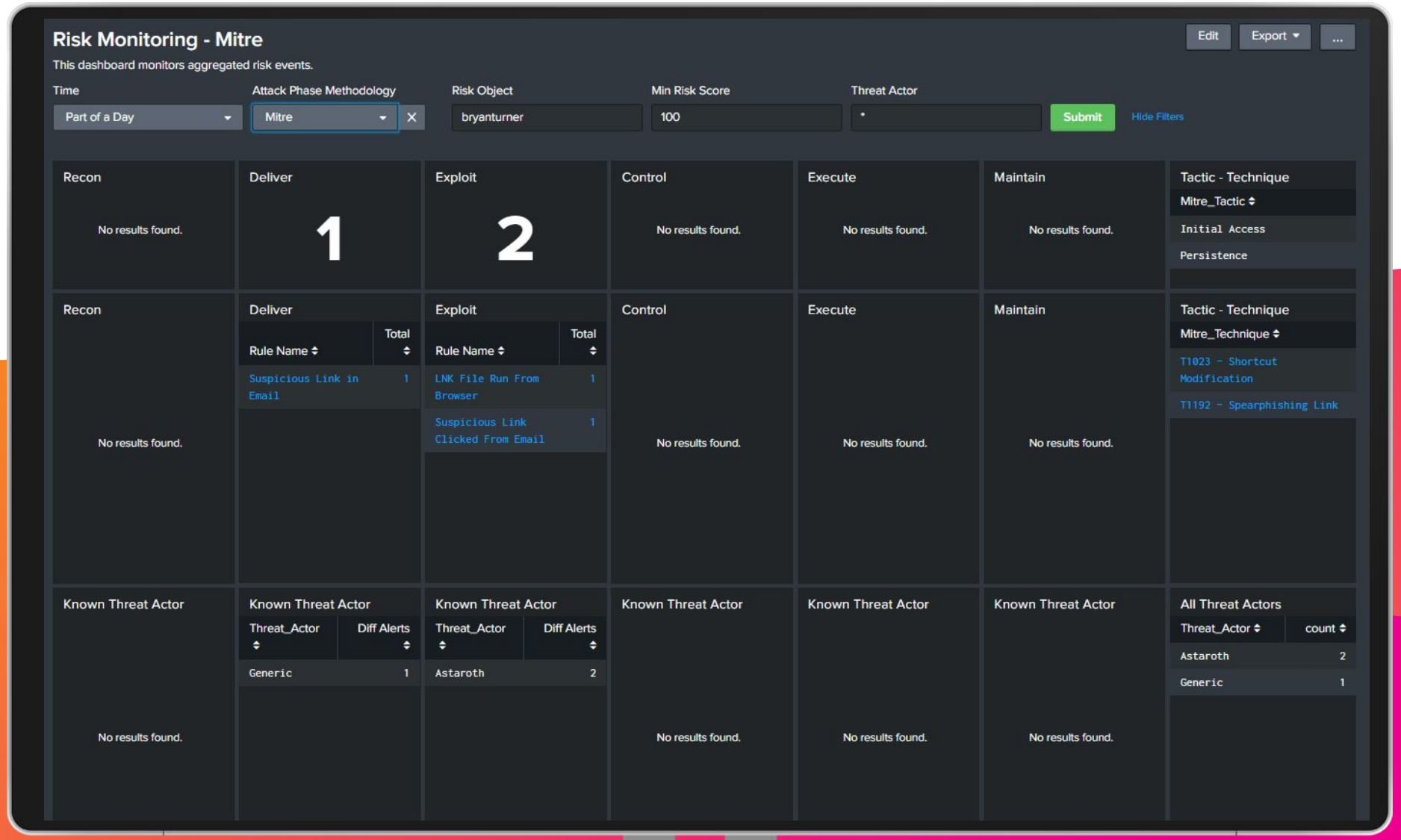
Building a Dashboard

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





splunk> .conf19

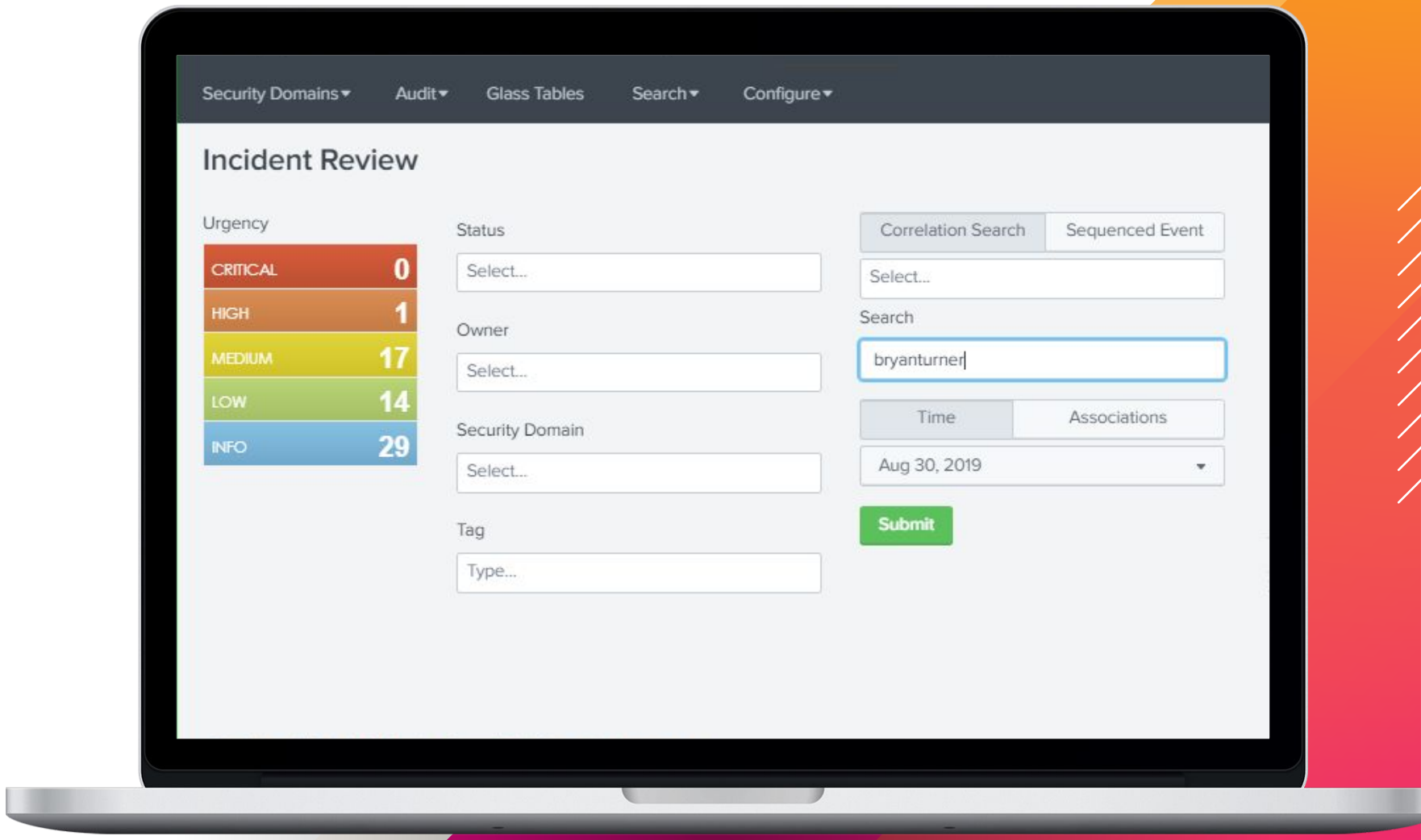


splunk> .conf19

Walkthrough

Incident Review

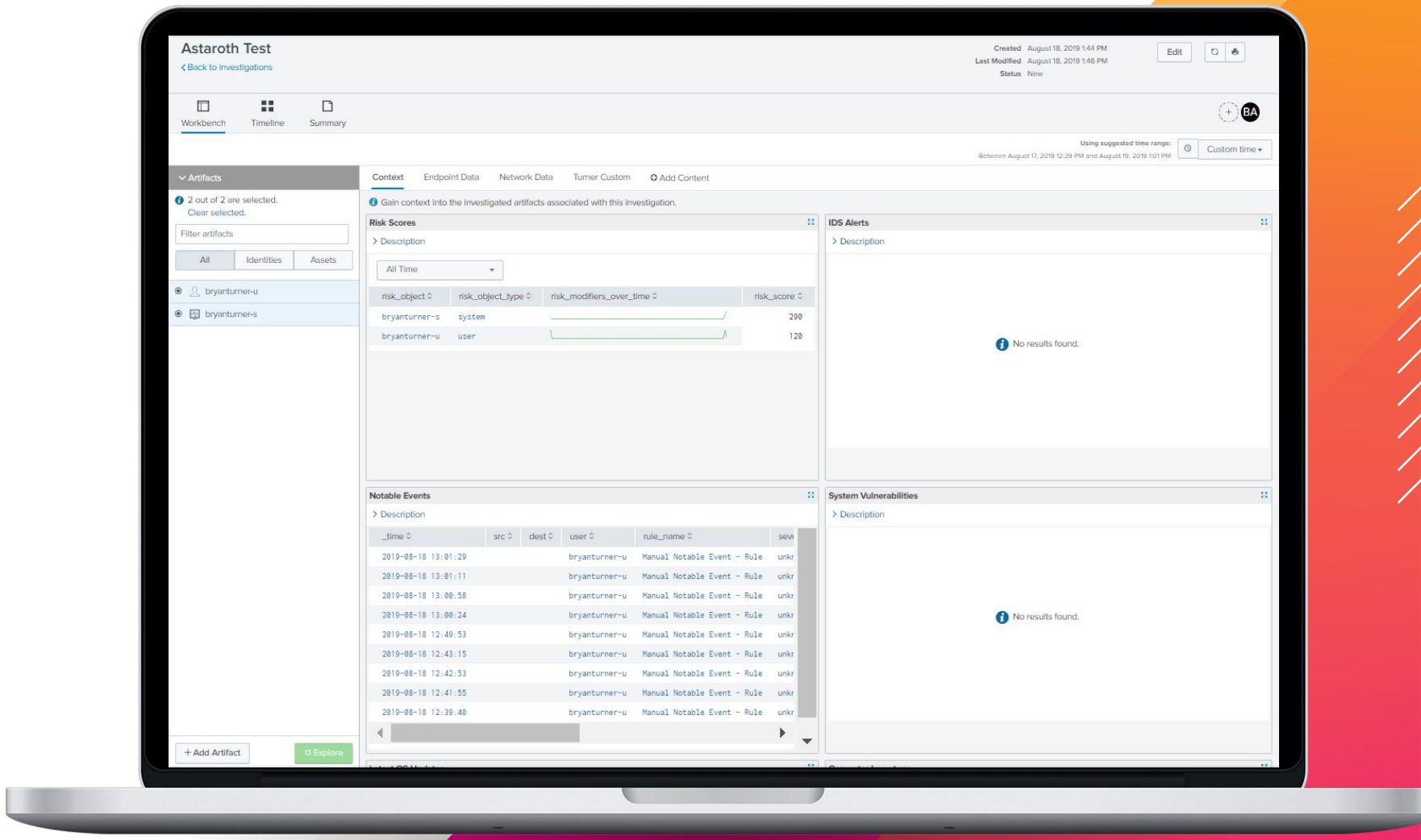
- Search by risk object and severity
- Add all events to the same investigation



Walkthrough

Building Investigations

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

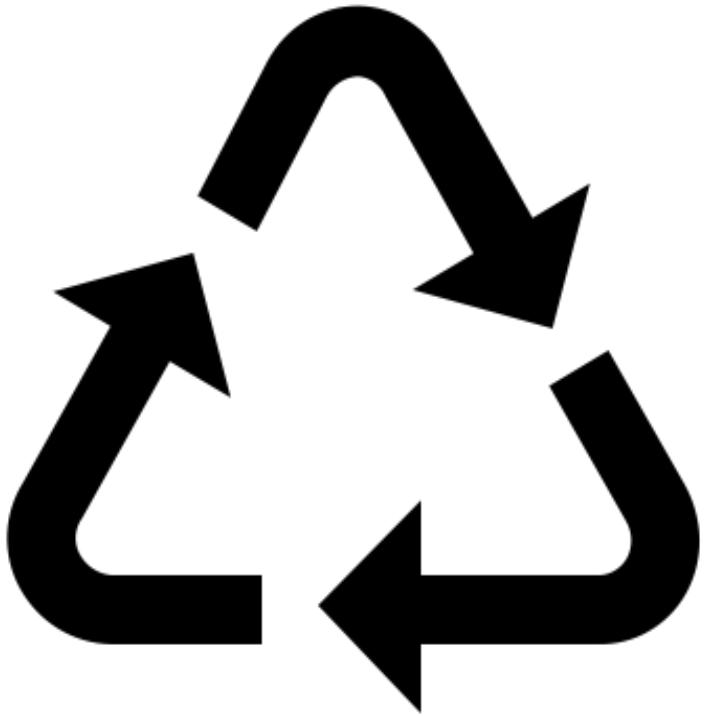


Ongoing Maintenance

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

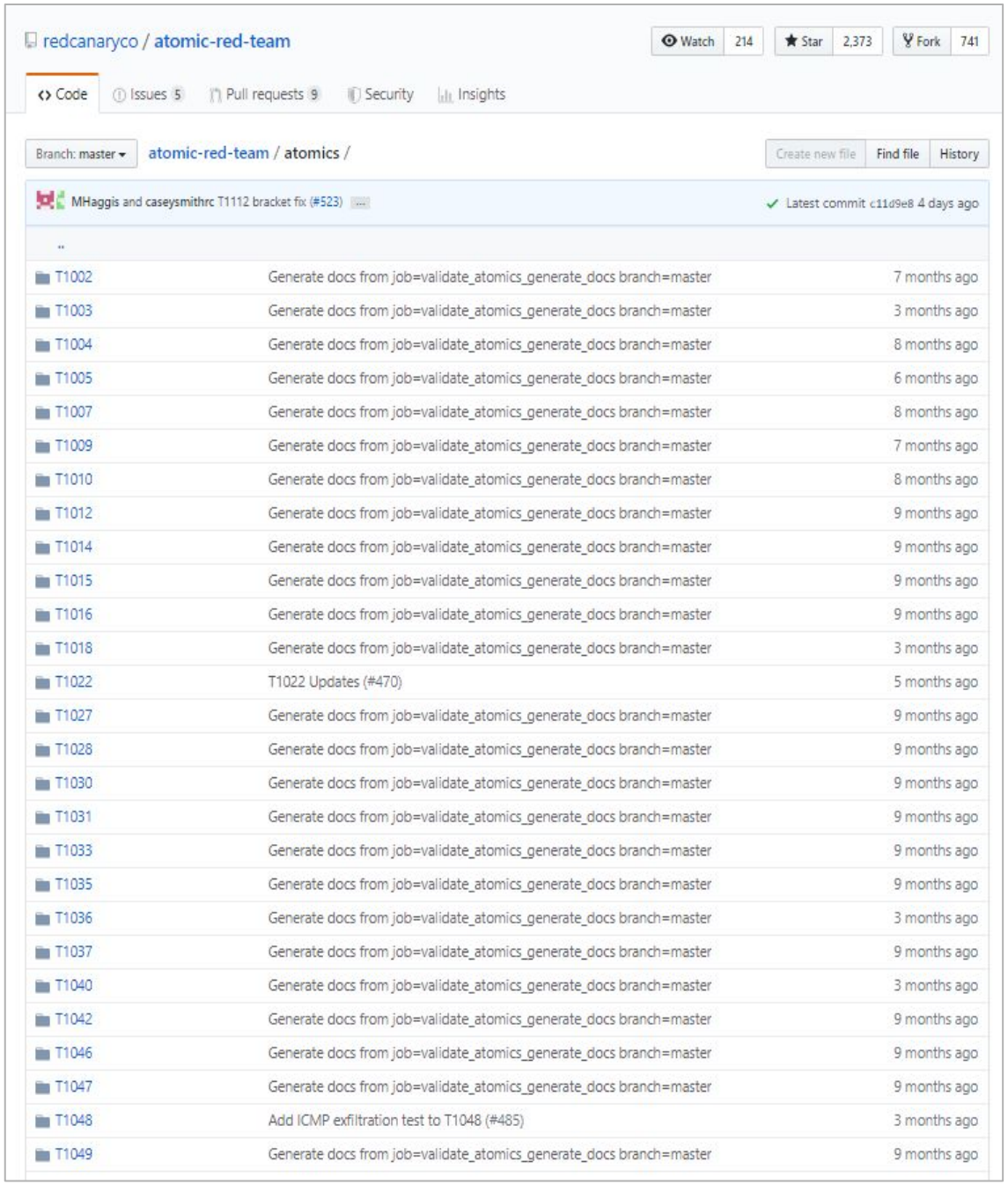
1. Validate logic
   - Log format changes
   - Additional / Removed systems
2. Identify additional or deprecated search terms
3. Research additional detections
   - Is this search still needed?

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 | Fork 741

Code | Issues 5 | Pull requests 9 | 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

splunk> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION