

# SEC1474 - Splunk and MITRE ATT&CK: Everything Covered? How We Know.

SEC1474



# Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at [www.investors.splunk.com](http://www.investors.splunk.com) or the SEC's website at [www.sec.gov](http://www.sec.gov). The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

---

Splunk, Splunk> and Turn Data Into Doing 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.

© 2025 Splunk LLC. All rights reserved.

# Splunk and MITRE ATT&CK: Everything Covered? How We Know.



**Collin  
Stump**

Splunk Consultant | Regeneron



**Christopher  
Filor**

Cyber Security Analyst | Regeneron

# Agenda

## Data

- Measuring your Security Posture
- Stakeholders
- What to Compare Against - MITRE
- Finding the analytics
- Finding and labeling the Data Feeds
- Calculations
- Design Decisions
- Aspirations

## Analytics

- Selecting Technique
- Research Detection Options
- Building Detection

## Operations

- Risk Based Alerting
- ADS Framework
- Quality Control

# Measuring Security Posture

What does our security posture look like?

- What data sources do we have available to us?
- What analytics are in place?

- What data sources and analytics do we need





# Stakeholders

- Leadership (from CISO down)
  - aid decision-making, reporting.
- Detection Engineering Team
  - prioritize work.
- Incident Response Team
  - where we have and do not have coverage.





# Where to start?

## Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

MITRE   ATT&CK														
Matrices   Tactics   Techniques   Defenses   CTI   Resources   Benefactors   Blog   Search														
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
Active Scanning (3)	Acquire Access (8)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services (1)	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal (1)	
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise (1)	Command and Scripting Interpreter (12)	BITS Jobs (1)	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery (1)	Internal Spearphishing (1)	Archive Collected Data (3)	Communication Through Removable Media (1)	Data Transfer Size Limits (1)	Data Destruction (1)	
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application (1)	Container Administration Command (1)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host (1)	Credentials from Password Stores (6)	Browser Information Discovery (1)	Lateral Tool Transfer (1)	Audio Capture (1)	Content Injection (1)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact (1)	
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services (1)	Deploy Container (1)	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion (1)	Exploitation for Credential Access (1)	Cloud Infrastructure Discovery (1)	Remote Service Session Hijacking (2)	Automated Collection (1)	Data Encoding (2)	Exfiltration Over C2 Channel (1)	Data Manipulation (3)	
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions (1)	ESXi Administration Command (1)	Cloud Application Integration (1)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information (1)	Forced Authentication (1)	Cloud Service Dashboard (1)	Remote Services (8)	Browser Session Hijacking (1)	Data Obfuscation (3)	Exfiltration Over Physical Medium (1)	Defacement (2)	
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution (1)	Compromise Host Software Binary (1)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Input Capture (4)	Cloud Storage Object Discovery (1)	Replication Through Removable Media (1)	Clipboard Data (1)	Dynamic Resolution (3)	Exfiltration Over Network Medium (1)	Disk Wipe (2)	
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media (1)	Input Injection (1)	Create Account (3)	Create or Modify System Process (5)	Email Spoofing (1)	Modify Authentication Process (9)	Container and Resource Discovery (1)	Software Deployment Tools (1)	Data from Cloud Storage (1)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Email Bombing (1)	
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Event Triggered Execution (17)	Event Triggered Execution (17)	Execution Guardrails (2)	Multi-Factor Authentication Interception (1)	Debugger Evasion (1)	Taint Shared Content (1)	Data from Configuration Repository (2)	Fallback Channels (1)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)	
Search Open Websites/Domains (3)		Trusted Relationship (1)	Native API (1)	Exclusive Control (1)	Exclusive Control (1)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation (1)	Device Driver Discovery (1)	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure (1)	Scheduled Transfer (1)	Financial Theft (1)	
Search Victim-Owned Websites (1)		Valid Accounts (4)	Scheduled Task/Job (5)	Serverless Execution (1)	Serverless Execution (1)	Hide Artifacts (14)	Network Sniffing (1)	Domain Trust Discovery (1)		Data from Local System (1)	Ingress Tool Transfer (1)	Transfer Data to Cloud Account (1)	Network Denial of Service (2)	
		Wi-Fi Networks (1)	Shared Modules (1)	External Remote Services (1)	External Remote Services (1)	Hijack Execution Flow (12)	OS Credential Dumping (8)	File and Directory Discovery (1)		Data from Network Shared Drive (1)	Multi-Stage Channels (1)		Resource Hijacking (4)	
			Software Deployment Tools (1)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Impersonation (1)	Steal Application Access Token (1)	Group Policy Discovery (1)		Data from Removable Media (1)	Non-Application Layer Protocol (1)		Service Stop (1)	
			System Services (3)	Implant Internal Image (1)	Implant Internal Image (1)	Indicator Removal (10)	Steal or Forge Authentication Certificates (1)	Log Enumeration (1)		Data Staged (2)	Non-Standard Port (1)		System Shutdown/Reboot (1)	
			User Execution (4)	Modify Authentication Process (9)	Modify Authentication Process (9)	Indirect Command Execution (1)	Steal or Forge Kerberos Tickets (5)	Network Service Discovery (1)		Email Collection (3)	Protocol Tunneling (1)			
			Windows Management Instrumentation (1)	Modify Registry (1)	Modify Registry (1)	Masquerading (11)	Modify Cloud Compute Infrastructure (5)	Password Policy Discovery (1)		Input Capture (4)	Proxy (4)			
				Office Application Startup (6)	Office Application Startup (6)	Modify Authentication Process (9)		Peripheral Device Discovery (1)		Screen Capture (1)	Remote Access Tools (3)			
								Permission Groups Discovery (3)		Video Capture (1)	Traffic Signaling (2)			
								Steal Web Session (1)			Web Service (3)			

## Did you know they include the data source information?

<https://attack.mitre.org/>

DATA SOURCES			
Active Directory	Application Log	Application Vetting	Asset
Certificate	Cloud Service	Cloud Storage	Command
Container	Domain Name	Drive	Driver
File	Firewall	Firmware	Group
Image	Instance	Internet Scan	Kernel
Logon Session	Malware Repository	Module	Named Pipe
Network Share			

Home > Data Sources			
Data Sources			
Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique.			
Data Sources: 41			
ID	Name	Domain	Description
DS0026	Active Directory	Enterprise	A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)
DS0015	Application Log	Enterprise ICS	Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)
DS0041	Application Vetting	Mobile	Application vetting report generated by an external cloud service.
DS0039	Asset	ICS	Data sources with information about the set of devices found within the network, along with their current software and configurations
DS0037	Certificate	Enterprise	A digital document, which highlights information such as the owner's identity, used to instill trust in public keys used while encrypting network communications
DS0025	Cloud Service	Enterprise	Infrastructure, platforms, or software that are hosted on-premise or by third-party providers, made available to users through network connections and/or APIs
DS0010	Cloud Storage	Enterprise	Data object storage infrastructure hosted on-premise or by third-party providers, made available to users through network connections and/or APIs
DS0017	Command	Enterprise Mobile ICS	A directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task
DS0032	Container	Enterprise	A standard unit of virtualized software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another
DS0038	Domain Name	Enterprise	Information obtained (commonly through registration or activity logs) regarding one or more IP addresses registered with human readable names (e.g., mitre.org)

# Where to start?

Did you know: ES has a really good mitre lookup?



- Resource: The MITRE Lookup found in the Security Essentials App
- `| inputlookup mitre_enterprise_list`



# Finding and labeling the Data

What data sources do we have available for our analytics?

- Focused on index – sourcetype combinations.
- What are all the critical feeds?
- What data are the searches “considering”
- What Data Source IDs from MITRE are we associating with?

# Finding the analytics

What searches are we running that provide security value?

- Rest endpoints for Splunk and Lookups for other sources
- MITRE Annotations in Splunk
  - Most provided by vendor
- Looking for searches that are enabled and Scheduled

```
| rest splunk_server=local /services/saved/searches `saved_search_field_list`  
| search mitre_attack{}=*  
  
|append [  
  | rest splunk_server=local /servicesNS/-/-/saved/searches  
  search="eai:acl.app=anvilogic"  
  | search title="avl:ti:*" OR title="avl:ts:*"  
  | rex field=title "^avl:(ti|ts):(?<avl_rule_id>.+)\.:"  
  | lookup avl_rule_inventory_workspace avl_rule_id OUTPUTNEW  
  avl_mitre_ext_ids avl_title]
```

action.correlationsearch._command_backup	
action.correlationsearch.annotations	{"mitre_attack":["T1204.001"]}
action.correlationsearch.command	noop
action.correlationsearch.enabled	

# How Covered Am I?

## Measuring and Comparing

For each MITRE Technique and Sub Technique

- Are there searches in place?
  - As a percentage
- Have there been any recent alerts regarding that Technique?
  - `index=_internal sourcetype=scheduler.`
  - As a whole number
- Are we missing any MITRE data sources from our feeds.
  - As a percentage



# Dashboard Icons



Percent of MITRE Technique covered by Data.



Percent of MITRE Techniques covered by analytics.

Search/Data Fully Available

Search/Data Mostly Available

Search/Data Partially Available

Search/Data Not Available

Inconclusive

Left Box: Data Coverage

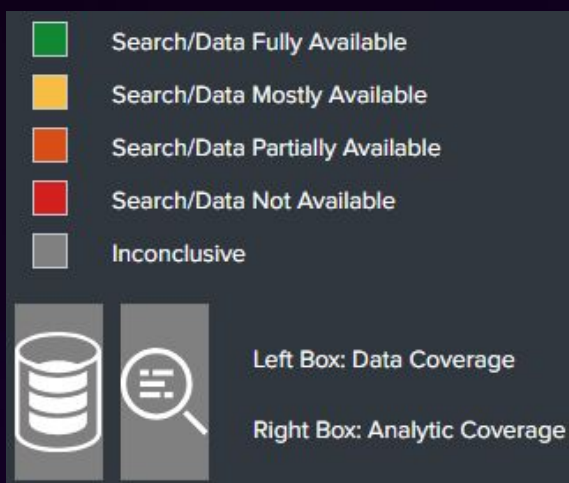
Right Box: Analytic Coverage

# Design Decisions

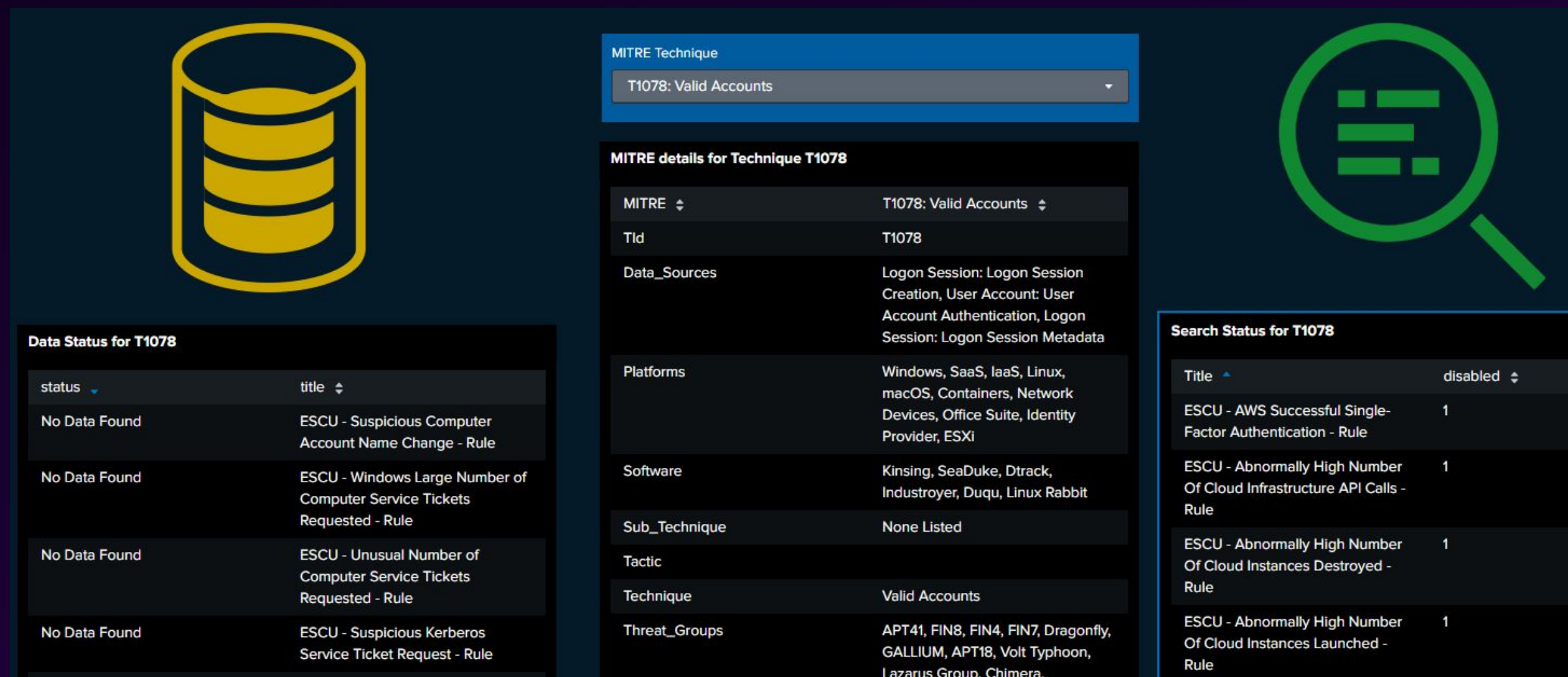
How do we layout the dashboard for the stakeholders

- Traditional “Vertical” MITRE Display
- Magnifying glass = search status
- Database = data status
- What data sources do we have available to us?
- Multiple Tabs






















































































© 2025 SPLUNK LLC





# Analytics

- Analyzing Dashboard
- Selecting & Researching Techniques
- Building Detections
  - Standardize Detection Format
  - Searching tips


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
 	 	 	 	 	 	 	 
	 	 	 	 	 	 	 
	 	 	 	 	 	 	 
	 	 	 	 	 	 	 
	 	 	 	 	 	 	 
		 		 	 	 	 
		 		 	 	 	 



# Analyzing Dashboard

- Sourcing detections
  - Where do we have data and no detections
- TTP in new attack chain
  - Check if we have data, have detections or need to build
- Requests to gather required data if none available for TTP





MITRE Technique

T1078: Valid Accounts

MITRE details for Technique T1078


MITRE	T1078: Valid Accounts
Tid	T1078
Data_Sources	Logon Session: Logon Session Creation, User Account: User Account Authentication, Logon Session: Logon Session Metadata
Platforms	Windows, SaaS, IaaS, Linux, macOS, Containers, Network Devices, Office Suite, Identity Provider, ESXi
Software	Kinsing, SeaDuke, Dtrack, Industroyer, Duqu, Linux Rabbit
Sub_Technique	None Listed
Tactic	
Technique	Valid Accounts
Threat_Groups	APT41, FIN8, FIN4, FIN7, Dragonfly, GALLIUM, APT18, Volt Typhoon, Lazarus Group, Chimera,

Data Status for T1078

status	title
No Data Found	ESCU - Suspicious Computer Account Name Change - Rule
No Data Found	ESCU - Windows Large Number of Computer Service Tickets Requested - Rule
No Data Found	ESCU - Unusual Number of Computer Service Tickets Requested - Rule
No Data Found	ESCU - Suspicious Kerberos Service Ticket Request - Rule

Search Status for T1078


Title	disabled
ESCU - AWS Successful Single-Factor Authentication - Rule	1
ESCU - Abnormally High Number Of Cloud Infrastructure API Calls - Rule	1
ESCU - Abnormally High Number Of Cloud Instances Destroyed - Rule	1
ESCU - Abnormally High Number Of Cloud Instances Launched - Rule	1





# Selecting and Researching Techniques

- Select a technique where you have data available
- Drilldown in dashboard will show
  - Available data sources
  - Information on Technique
  - Searches in the environment
- Review Mitre’s page for extra information
  - All Data Sources to detect this
  - Example SPL



MITRE Technique

T1053: Scheduled Task/Job

MITRE details for Technique T1053


MITRE	T1053: Scheduled Task/Job
Tid	T1053
Data_Sources	Scheduled Job: Scheduled Job Creation, File: File Creation, Process: Process Creation, Container: Container Creation, Command: Command Execution, File: File Modification
Platforms	Windows, Linux, macOS, Containers, ESXi
Software	StrifeWater, DEADEYE, Lokibot, Remsec
Sub_Technique	None Listed
Tactic	
Technique	Scheduled Task/Job
Threat_Groups	Earth Lusca
Version	17.1

Data Status for T1053

status	title
Ingesting Data	Scheduled Task with Potential SSH Tunnel - Windows
Ingesting Data	ESCU - Linux Adding Crontab Using List Parameter - Rule
Ingesting Data	ESCU - Linux At Application Execution - Rule
Ingesting Data	ESCU - Linux Edit Cron Table Parameter - Rule
Ingesting Data	ESCU - Linux Possible Append Command To At Allow Config File - Rule
Ingesting Data	ESCU - Linux Possible Append Cronjob Entry on Existing Cronjob File - Rule

Search Status for T1053

Title	disabled
Scheduled Task with Potential SSH Tunnel - Windows	0
ESCU - Linux Adding Crontab Using List Parameter - Rule	1
ESCU - Linux At Application Execution - Rule	1
ESCU - Linux Edit Cron Table Parameter - Rule	1
ESCU - Linux Possible Append Command To At Allow Config File - Rule	1
ESCU - Linux Possible Append Cronjob Entry on Existing Cronjob File - Rule	1



DS0009	Process	Process Creation	<div>Monitor for newly executed processes that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.</div> <div>Note: Below is the relevant Events and SourcesWindows:</div> <div><ul style="list-style-type: none"><li>• Sysmon Event ID 1: Process creation, particularly for schtasks.exe, at.exe, Taskeng.exe, crontab, etc.</li><li>• Windows Event Log EventCode 4688: Process creation that might involve task scheduling.</li><li>• Windows Task Scheduler Logs: Task creation, modification, or deletion.</li></ul></div> <div>Linux/macOS:</div> <div><ul style="list-style-type: none"><li>• Auditd logs: Monitoring for cron job creation or modifications.</li><li>• Syslog: Logs related to cron jobs or scheduled tasks.</li><li>• File integrity monitoring (FIM): For changes to /etc/cron, /var/spool/cron/, or user-specific cron jobs.</li></ul></div> <div>Containers:- Container logs: Detection of scheduled tasks or cron jobs within container environments.</div> <div>Analytic 1 - Look for task execution with unusual parameters.</div> <div><pre>(sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" OR sourcetype="WinEventLog:Security" OR sourcetype="linux_auditd" OR sourcetype="syslog")   where Image IN ("schtasks.exe", "at.exe", "Taskeng.exe", "cron", "crontab", "systemd-timers")</pre></div>
--------	---------	------------------	---



# Building Detections

- Standardize a format for detections
- Build a template to start with
- Comment your code!!!!
- Normalize data for Risk framework and future use
- Index time to catch delayed events

## • TEMPLATE EXAMPLE

```
• `` DATA RETRIEVAL MACROS & INITIAL SEARCH TERMS ``
• `get_endpoint_data` `get_endpoint_data_winevent`

• `` DATA NORMALIZATION ``
• `map_winevent`

• `` DATA TRANSFORMATION (STATS, EVENTSTATS, TABLE, ETC...) ``
• |fillnull value="n/a"
• |stats count as raw_event_count max(_time) as event_occured_time
  by field1 field2 field3 field4

• `` ALLOWLISTING ``
• |lookup <allow_list_lookup> field1 field2 field3 OUTPUT is_allowed
• |fillnull value="false" is_allowed
• |search is_allowed=false

• `` DATA ENRICHMENT ``
• |lookup threat_intel_ip_lookup src_ip OUTPUT field4 field5

• `` REQUIRED FIELDS AND SNOW MACROS ``
• |eval risk_message="Create the risk message here"
• |fillnull short_description value="N/A something broke here, submit
  request to detection team for troubleshooting."
```



# Operations

- Risk Based Alerting
- Alerting and Detection Strategy Framework
- Quality Control



# Risk Based Alerting

- Run all detections through Risk
  - Few cases where best to go straight to notable (phishing to group by campaigns)
- 0 Risk scoring
  - Informational level events
  - Detections that directly create tickets (phishing example)
- Risk Factors
  - Create tags in Asset & Identity framework
  - Use tags to adjust risk score (VIP's, Admins, Leavers)



# ADS Framework

- Standard for documenting detections
  - Goal
  - Categorization (Mitre ATT&CK/Kill Chain)
  - Strategy Abstract
  - Technical Context
  - Blind Spots and Assumptions
  - False Positives
  - Validation
  - Risk Scoring
  - Response

# Quality Control

## Detection Engineering

- Create Intake process (new detections, break/fix, allowlisting, logic tuning)
- Standardize format for detections (create a template)
- Comment your code!!!

## Operations

- Monitor Signal to noise ratio
- Create repeatable process for reviewing duplicates and false positives
- Tune our expected and known activity in your environment

# Thank you

