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 or the SEC's website at 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> .conf25

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

Collin Stump

Splunk Consultant | Regeneron

Christopher Filor

Cyber Security Analyst | Regeneron

splunk> .conf25

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?

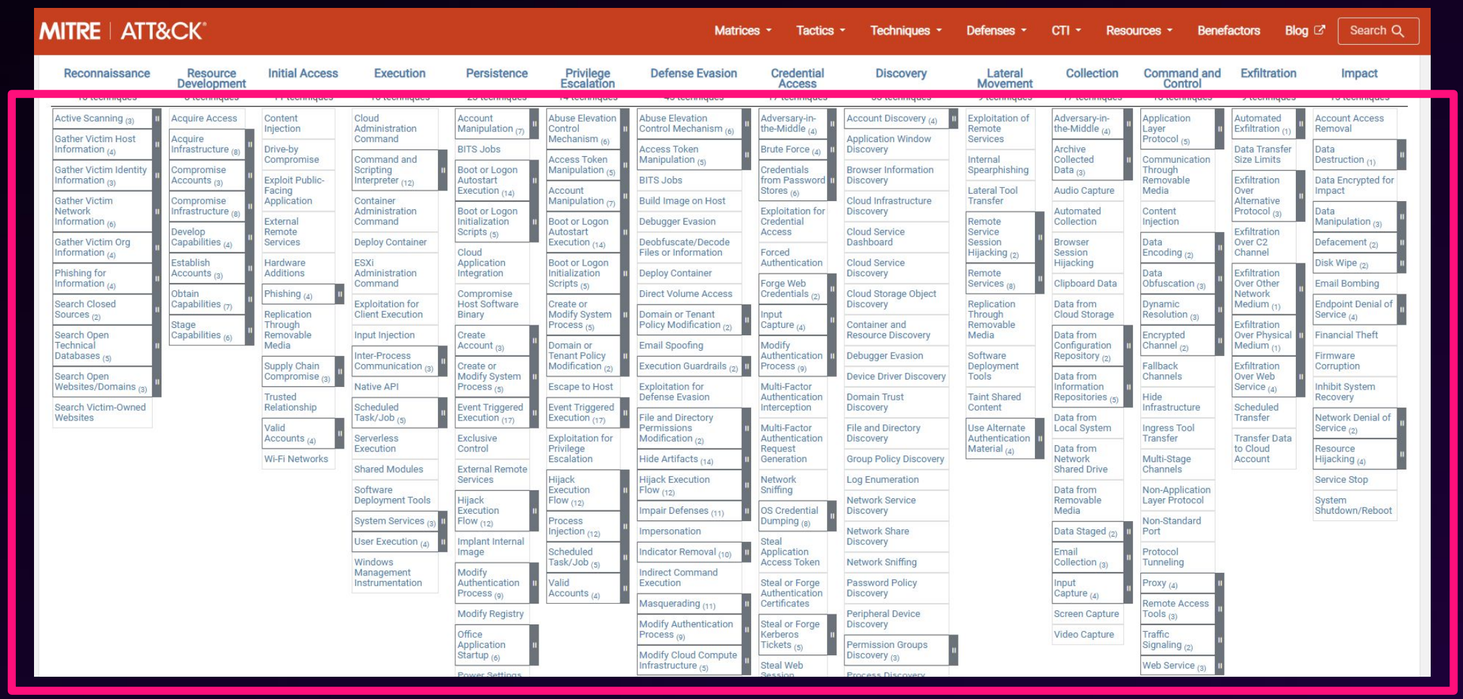
- What data sources and analytics do we need

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.

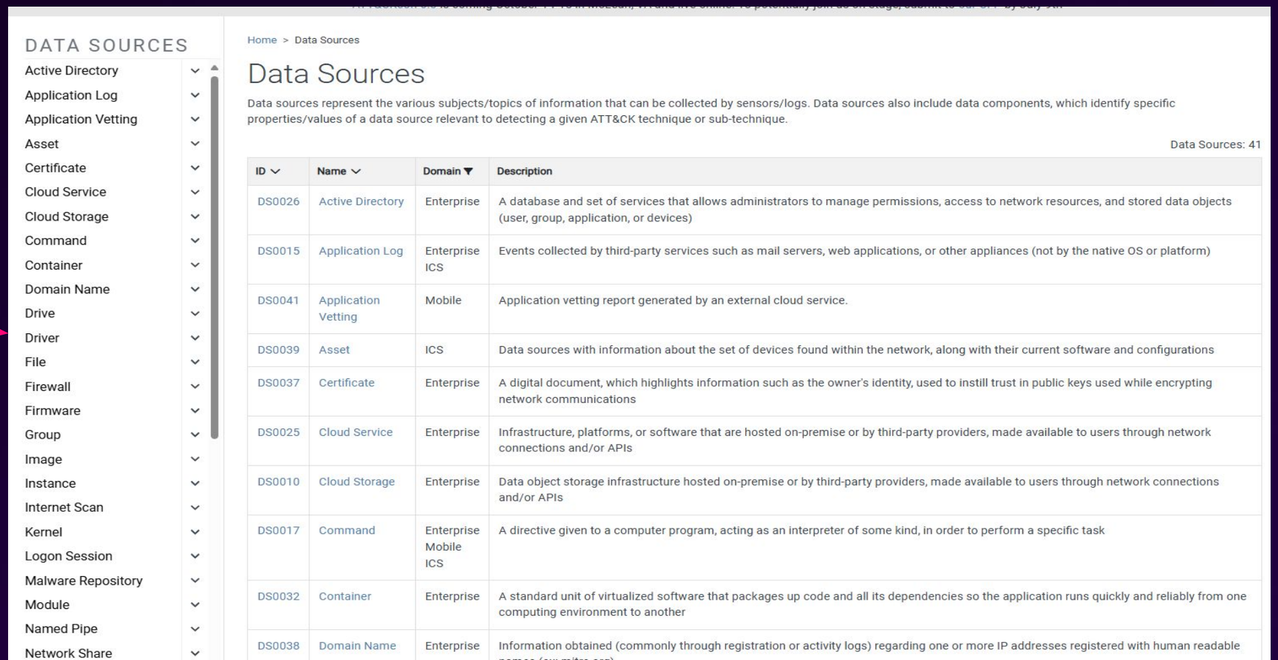
Where to start?

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



Did you know they include the data source information?

https://attack.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?

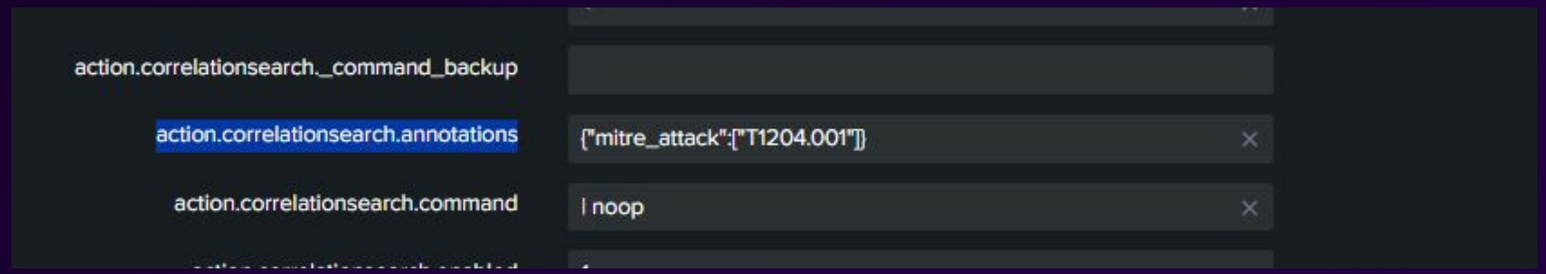
Finding the analytics

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]
```



How Covered Am I?

Measuring and Comparing

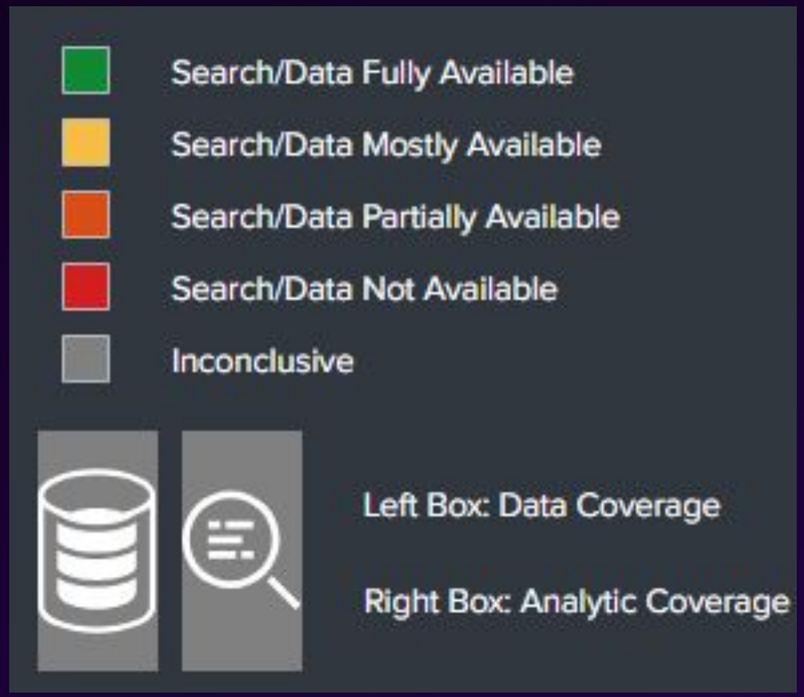
For each MITRE Technique and Sub Technique

- 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.

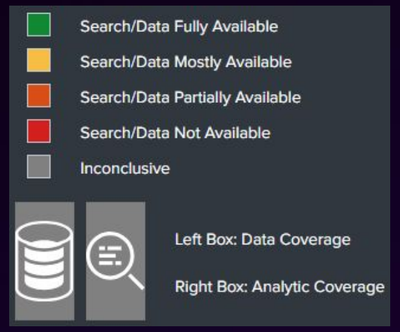
Percent of MITRE Techniques covered by analytics.



Design Decisions

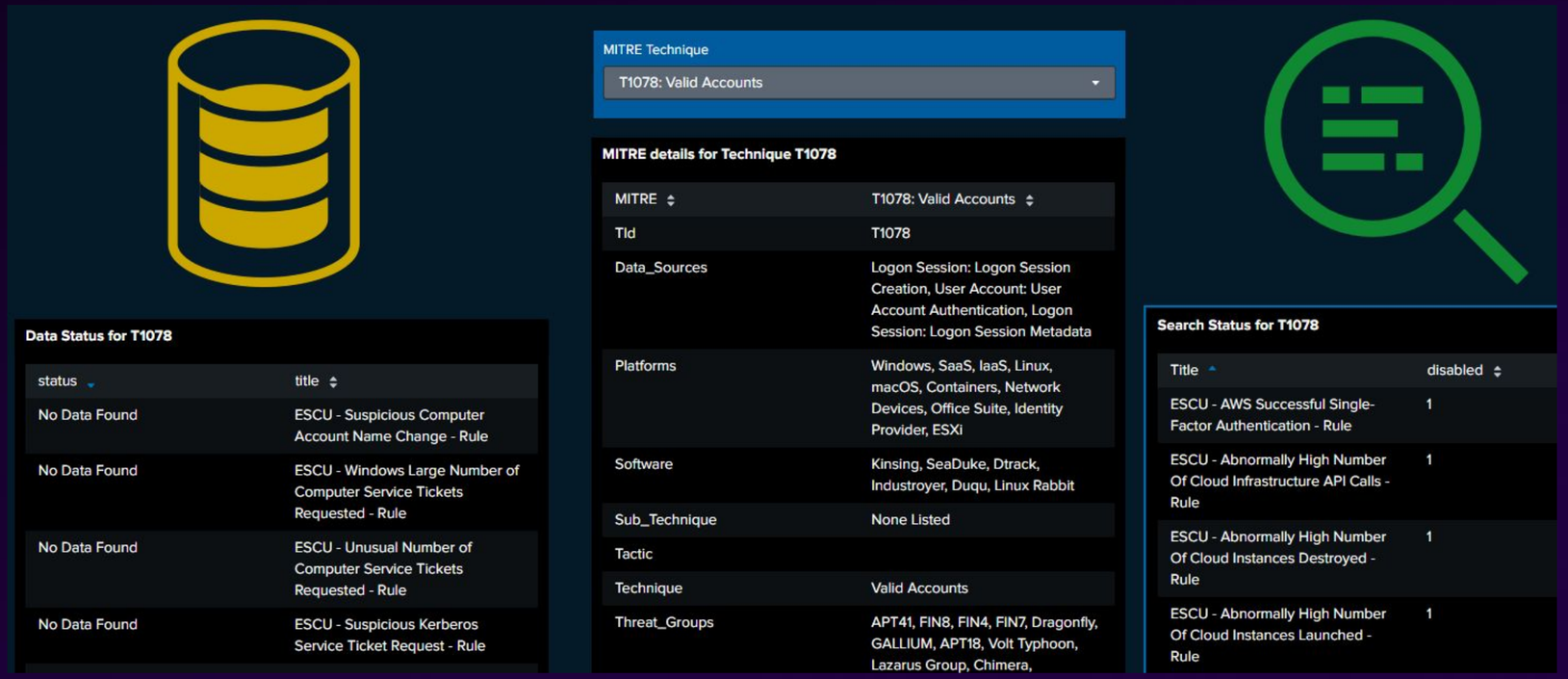
How do we layout the dashboard for the stakeholders

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



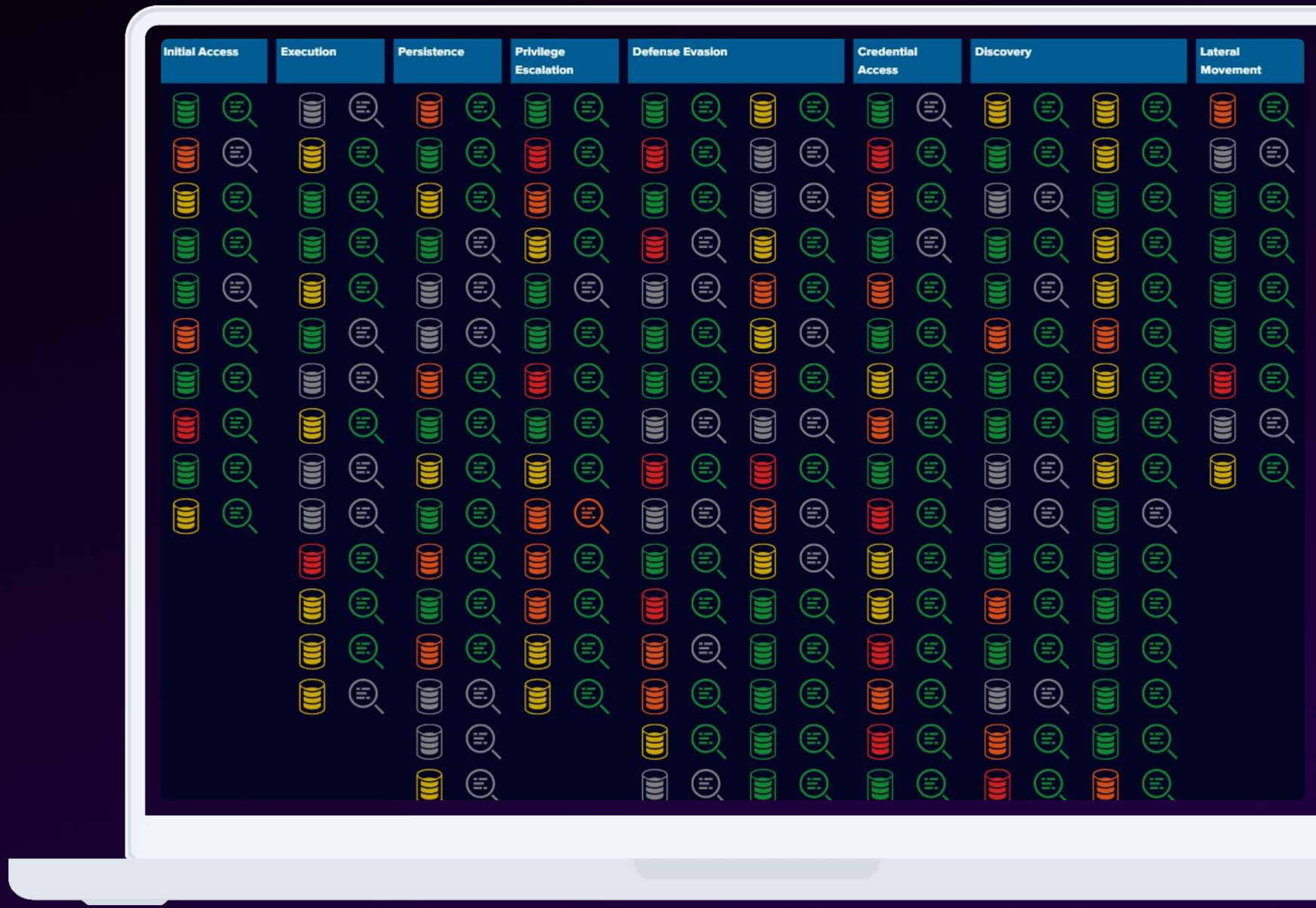
MITRE

ATT&CK



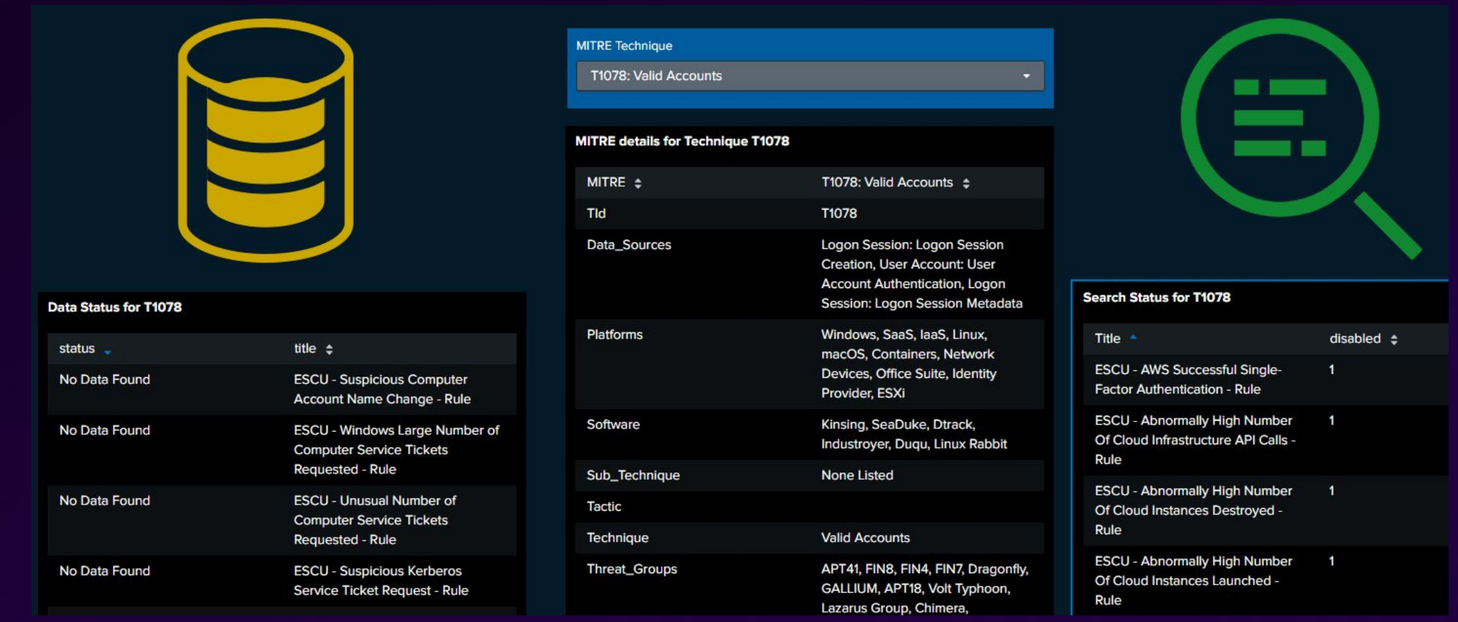
Analytics

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



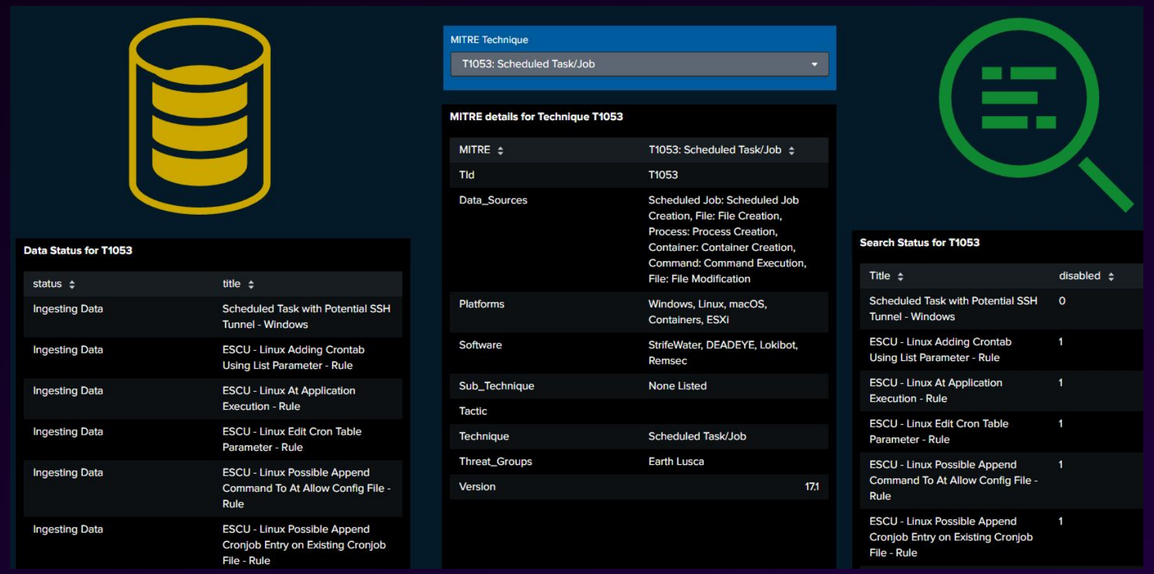
Analyzing Dashboard

- 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



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



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

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

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	Monitor for newly executed processes that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Note: Below is the relevant Events and SourcesWindows: • Sysmon Event ID 1: Process creation, particularly for schtasks.exe, at.exe, Taskeng.exe, crontab, etc. • Windows Event Log EventCode 4688: Process creation that might involve task scheduling. • Windows Task Scheduler Logs: Task creation, modification, or deletion. Linux/macOS: • Auditd logs: Monitoring for cron job creation or modifications. • Syslog: Logs related to cron jobs or scheduled tasks. • File integrity monitoring (FIM): For changes to /etc/cron, */var/spool/cron/*, or user-specific cron jobs. Containers:- Container logs: Detection of scheduled tasks or cron jobs within container environments. Analytic 1 - Look for task execution with unusual parameters. `(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")`

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