Splunk Attack Analyzer Workshop Lab Guide

Splunk Attack Analyzer Exercises

Exercise 1 - Review Live Job Submission Results

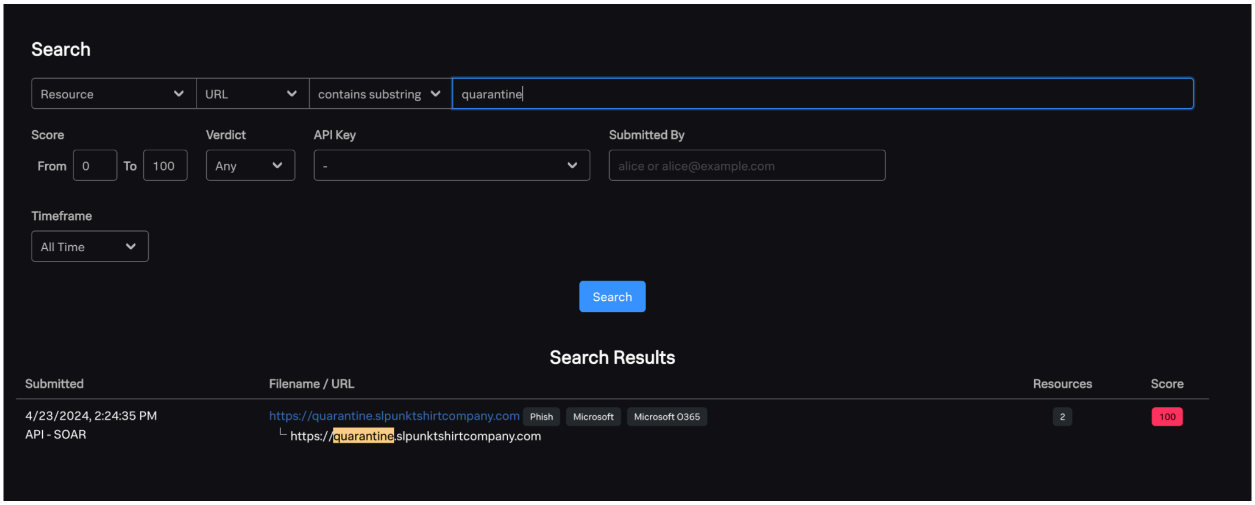
Task 1

1. Review the completed job results via the link provided by the presenter.
2. Answer the following questions about the job.
    - What was the verdict of the submission?
    - What was the brand that was used?
    - How long did it take to analyze the screenshot?

Exercise 2 - Review Job Results

Task 1

1. Click the “Search” tab in the Splunk Attack Analyzer User Interface
2. Select the URL resource option.
3. Select the “contains substring” option.
4. Add “quarantine” to the search parameters
5. Click the blue “Search” button.
6. Click the job in the search results



quarantine

From 0 To 100

Any

-

alice or alice@example.com

All Time

Search Results

Submitted	Filename / URL	Resources	Score
4/23/2024, 2:24:35 PM API - SOAR	https://quarantine.slpunktshirtcompany.com Phish Microsoft Microsoft O365 └ https://quarantine.slpunktshirtcompany.com	2	100

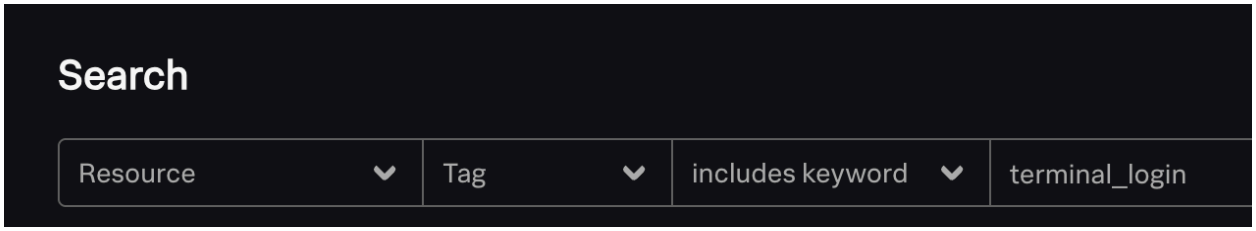
7. Analyze the results
    - What was the verdict of the submission?

- What was the brand that was used?
- What common evasion technique was used on the webpage?
  Hint: Review the detections that fired for this job.

Exercise 3 - Review System Tags

Task 1

1. Search for the job that got tagged as a terminal login.



Search

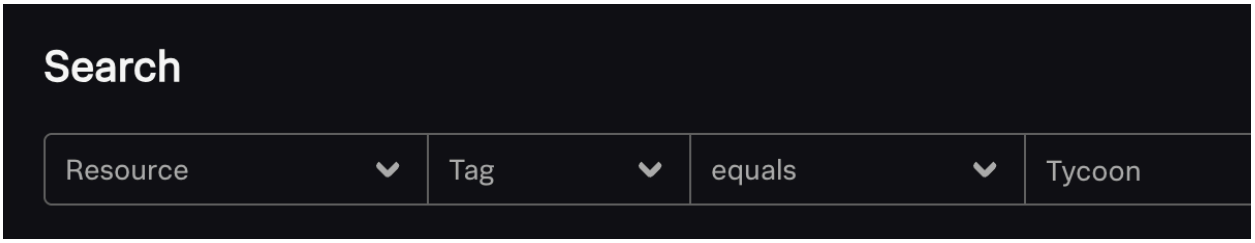
Resource | Tag | includes keyword | terminal_login

2. Analyze the results
   - Which file sharing service was used to send the files?

Exercise 4 - Review Captcha bypass job

Task 1

1. Search for the job that got tagged as using the Tycoon phish kit family



Search

Resource | Tag | equals | Tycoon

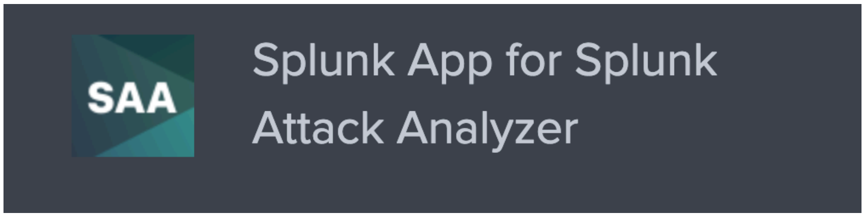
2. Analyze the results
   - What captcha provider was discovered and bypassed automatically by Splunk Attack Analyzer?

Splunk Enterprise Exercises

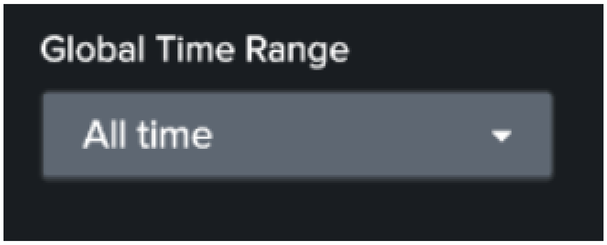
Exercise 1 - Review Dashboards

Task 1

1. Login to the Splunk Enterprise Security instance.
2. Navigate to the Splunk Attack Analyzer App.



3. When proceeding through the following steps, set all dashboards to “**All Time**”



Global Time Range

All time

4. Review the “**Usage Overview**” dashboard to see an Executive Overview of Splunk Attack Analyzer Submissions.
    - How many submissions are tagged as malware?
5. Click on the “**Observations**” tab in the Splunk Attack Analyzer App navigation bar.
6. Review the “**Credential Phishing and Malware**” dashboard to see phishing and malware trends over time
    - What is the most analyzed malware?
7. Click on the “**Observations**” tab in the Splunk Attack Analyzer App navigation bar.
8. Review the “**Phished Brands**” dashboard to see what brands have been involved in phishing attacks
    - What is the most Phished Brand?

Exercise 2 - Search job data

Task 1

1. Click the “**Other**” tab in the Splunk Attack Analyzer app for Splunk Enterprise.
2. Click “**Search**”
3. Set search parameters to “**all time**”

4. Using your new knowledge of sourcetypes, find the data for job 0972b55c-a5a1-4e9d-8c01-064487fc4b62 to answer the following questions.
    - What was the verdict?
    - What was the task score for the Email Analyzer engine?
    - Which engine(s) returned a display score greater than or equal to 75?

Task 2

5. The sandbox was used on the exe discovered in the job.
    - Which detection fired in the windows 7 sandbox indicated the malware was unpacked?
6. Review the job data to answer the following.
    - Which detection on this job had the maximum possible display severity?

Challenge Task

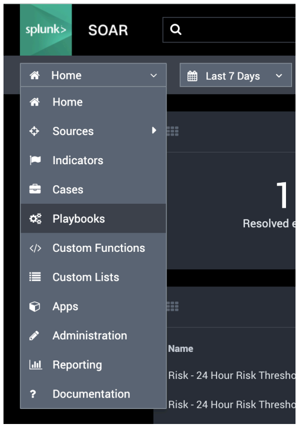
1. Find a new job that meets the below criteria.
    - What is the Job ID for the SMS phishing (smish) that included an AT&T brand impersonation?
2. As part of the Splunk Attack Analyzer built in optical character recognition (OCR) feature, screenshots of SMS messages are analyzed for text extraction including any URLs, and phone number or sender information. This data is part of the forensics that can be ingested into Splunk.
    - What was the phone number used to send the AT&T smish?

Splunk SOAR Exercises

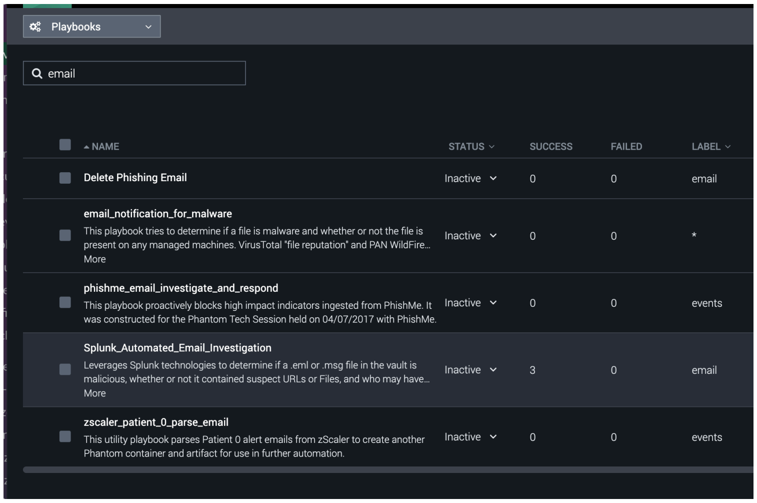
Exercise 1 - Splunk SOAR Playbooks

Task 1 - Review Playbooks the Splunk Automated Email Investigation Playbook

1. Login to the SOAR instance.
2. Select “**Playbooks**” on the menu dropdown



3. Click “**Playbooks**”
4. Search for the “**Splunk Automated Email Investigation**” playbook
5. Open the **local** version of the playbook

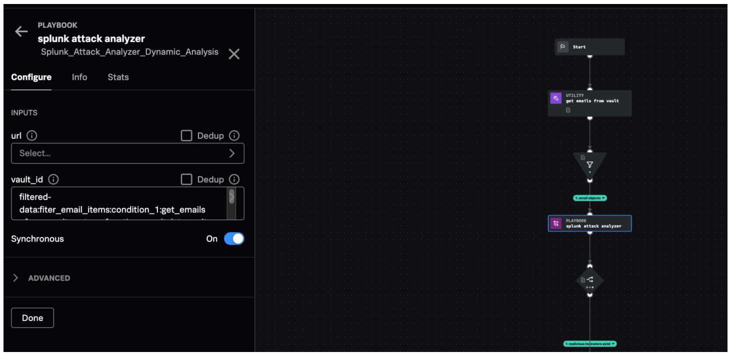


	NAME	STATUS	SUCCESS	FAILED	LABEL
□	Delete Phishing Email	Inactive	0	0	email
□	email_notification_for_malware This playbook tries to determine if a file is malware and whether or not the file is present on any managed machines. VirusTotal "file reputation" and PAN WildFire... More	Inactive	0	0	*
□	phishme_email_investigate_and_respond This playbook proactively blocks high impact indicators ingested from PhishMe. It was constructed for the Phantom Tech Session held on 04/07/2017 with PhishMe.	Inactive	0	0	events
□	Splunk_Automated_Email_Investigation Leverages Splunk technologies to determine if a .eml or .msg file in the vault is malicious, whether or not it contained suspect URLs or Files, and who may have... More	Inactive	3	0	email
□	zscaler_patient_0_parse_email This utility playbook parses Patient 0 alert emails from zScaler to create another Phantom container and artifact for use in further automation.	Inactive	0	0	events

6. Review the playbook to answer the following questions
    - What file types would work with this playbook? Hint: look at the first filter block.
    - What is the name of the playbook block that checks whether or not SAA found a sample to be malicious? Hint: Open the blocks to review and see names
    - *Challenge question*: What is the minimum score in *Splunk Attack Analyzer* that is used for the threshold when adding artifacts (URLs, files, hashes) to SOAR? Hint: Open up the sub playbook (as described below) and put your Python hat on.

Task 2 - Review the Splunk Attack Analyzer Dynamic Analysis Playbook

1. Click on the “**Splunk Attack Analyzer**” playbook block



PLAYBOOK
splunk attack analyzer
Splunk_Attack_Analyzer_Dynamic_Analysis

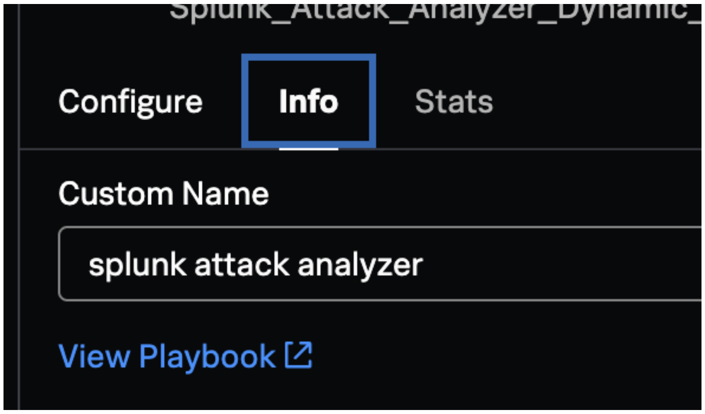
INPUTS

url — □ Dedup
Select...

vault_id — □ Dedup
filtered-data:fiter_email_items:condition_1:get_emails

Synchronous: On

2. On the left panel, click the "**Info**" tab



Splunk_Attack_Analyzer_Dynamic_

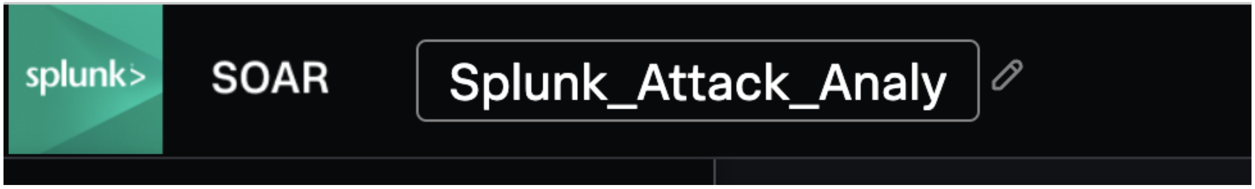
Custom Name: splunk attack analyzer

3. Click the link to "**view playbook**"
4. Review the playbook to answer the following questions
   - What is the name of the Splunk Attack Analyzer Connector for SOAR action used in the "get file summary output" action block? (Hint Connector name is cut off "Splunk Attack Analyzer C…")
5. Challenge Question: Utilize the Splunk Message Identifier Activity Analysis playbook to answer the following question
   - What fields are used to search Splunk for who received the email?

Exercise 2 - Splunk SOAR Investigation

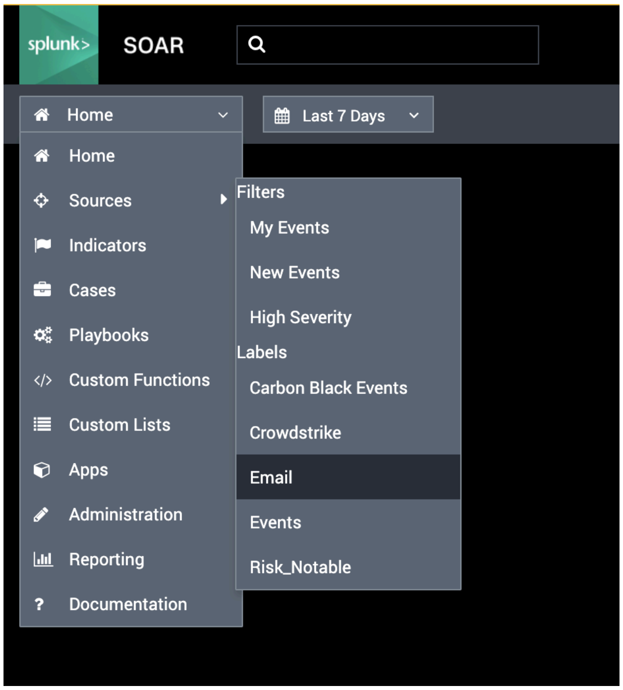
Task 1 - Run the Splunk Automated Email Investigation Playbook

1. Click the SOAR logo on the left of the webpage to go back to the SOAR homepage

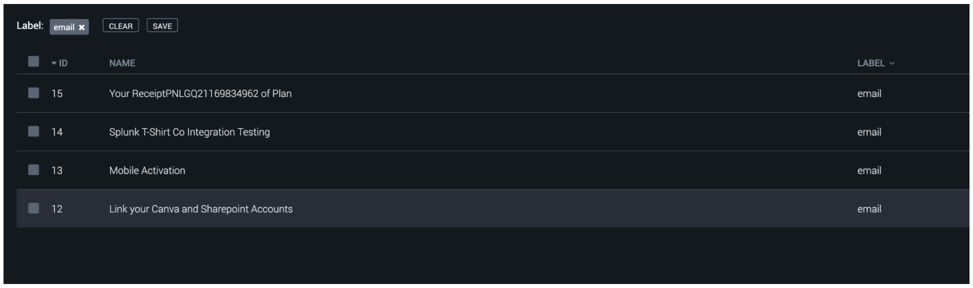


Splunk_Attack_Analy

2. Click the Menu dropdown
3. Select "**Sources**"
4. Select "**Email**"



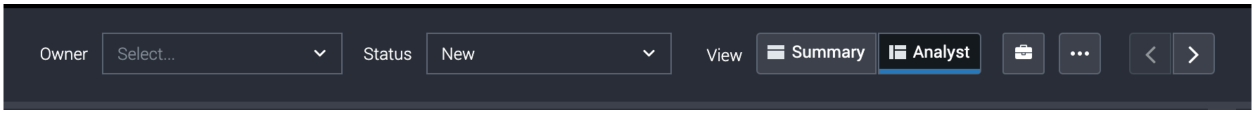
5. Find an event with the name “**Link your Canva and Sharepoint Accounts**”



Label: email ✖ CLEAR SAVE

ID	NAME	LABEL
15	Your ReceiptPNLGQ21169834962 of Plan	email
14	Splunk T-Shirt Co Integration Testing	email
13	Mobile Activation	email
12	Link your Canva and Sharepoint Accounts	email

6. On the right side of the page, select the Analyst view.

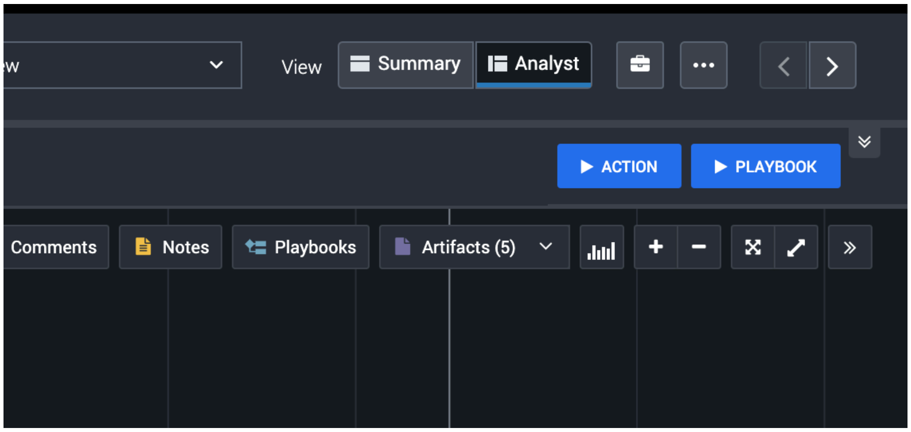


Owner: Select...

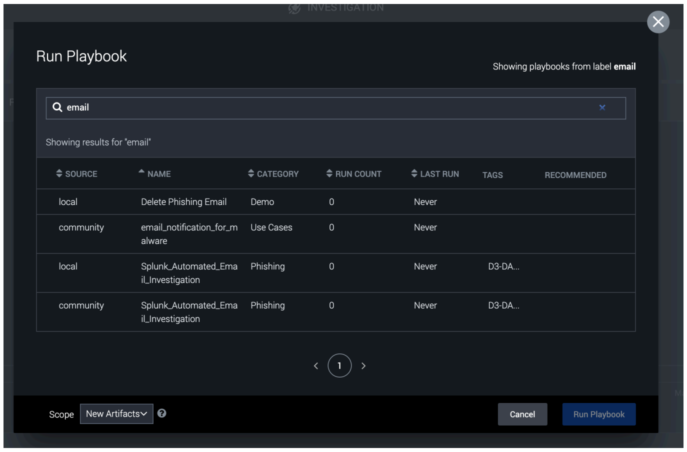
Status: New

View: Summary | Analyst

7. Click “**Playbook**”



8. Search for “**email**”



Run Playbook

Showing playbooks from label **email**

email

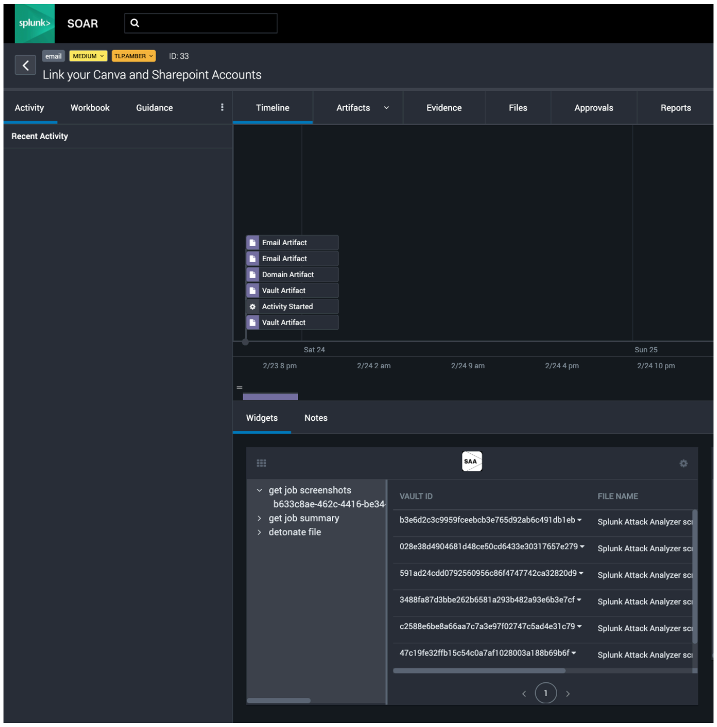
Showing results for "email"

SOURCE	NAME	CATEGORY	RUN COUNT	LAST RUN	TAGS	RECOMMENDED
local	Delete Phishing Email	Demo	0	Never		
community	email_notification_for_malware	Use Cases	0	Never		
local	Splunk_Automated_Email_Investigation	Phishing	0	Never	D3-DA...	
community	Splunk_Automated_Email_Investigation	Phishing	0	Never	D3-DA...	

Scope: New Artifacts

Task 2 - Review the Results of the Playbook Run

1. Click on the “**Notes**” populated by the playbook



ID: 33

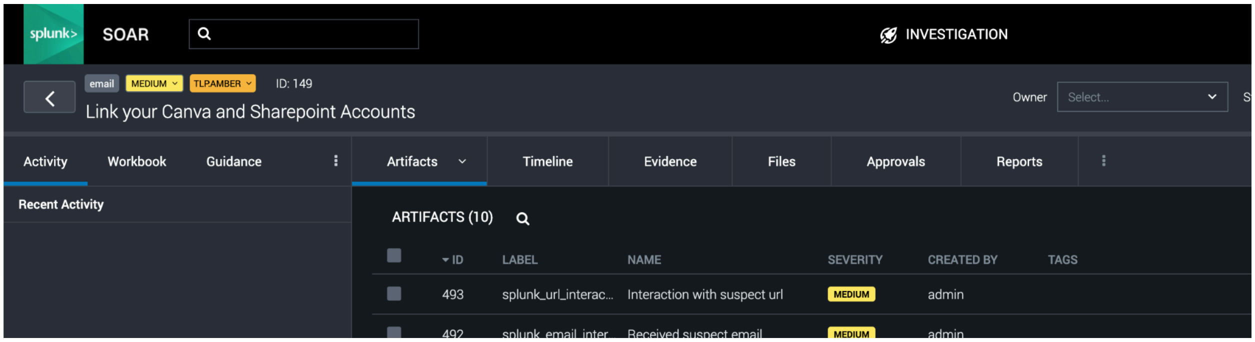
Link your Canva and Sharepoint Accounts

VAULT ID	FILE NAME
b3e6d2c3c9959fceebcb3e765d92ab6c491db1eb	Splunk Attack Analyzer sc
028e38d4904681d48ce50cd6433e30317657e279	Splunk Attack Analyzer sc
591ad24cdd0792560956c86f4747742ca32820d9	Splunk Attack Analyzer sc
3488fa87d3bbe262b6581a293b482a93e6b3e7cf	Splunk Attack Analyzer sc
c2588e6be8a66aa7c7a3e97f02747c5ad4e31c79	Splunk Attack Analyzer sc
47c19fe32ffb15c54c0a7af1028003a188b69b6f	Splunk Attack Analyzer sc

- What was the classification of the Splunk Attack Analyzer analysis?
- Did anyone else receive the email? If so, who?
- Did anyone click on the malicious link? If so, who?

Task 3 - Take Actions

1. Click on “**Artifacts**”



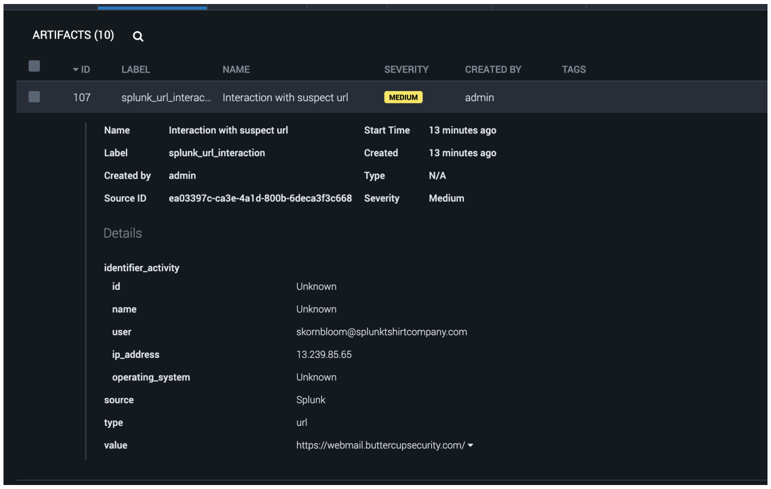
ID: 149

Link your Canva and Sharepoint Accounts

ARTIFACTS (10)

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
493	splunk_url_interac...	Interaction with suspect url	MEDIUM	admin	
492	splunk_email_inter...	Received suspect email	MEDIUM	admin	

2. Click on the “**Interaction with suspect url**” artifact
3. Click the value that contains the suspect url


ARTIFACTS (10)

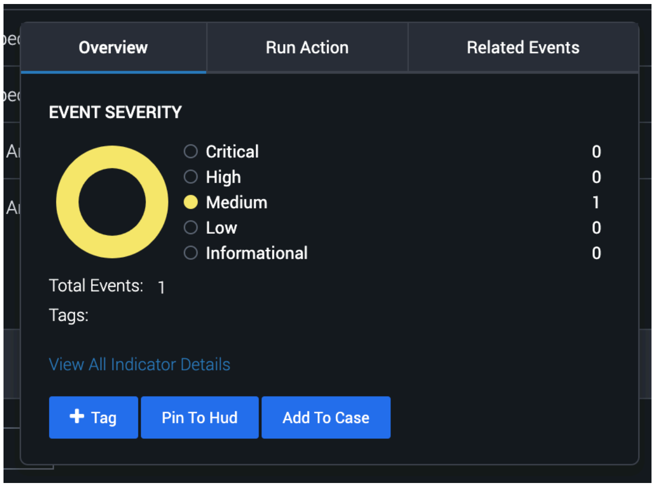
ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
107	splunk_url_interac...	Interaction with suspect url	MEDIUM	admin	

Name	Interaction with suspect url	Start Time	13 minutes ago
Label	splunk_url_interaction	Created	13 minutes ago
Created by	admin	Type	N/A
Source ID	ea03397c-ca3e-4a1d-800b-6deca3f3c668	Severity	Medium

Details

identifier_activity	
id	Unknown
name	Unknown
user	skornbloom@splunktshirtcompany.com
ip_address	13.239.85.65
operating_system	Unknown
source	Splunk
type	url
value	https://webmail.buttercupsecurity.com/ ▾

4. Click “**Run Action**”



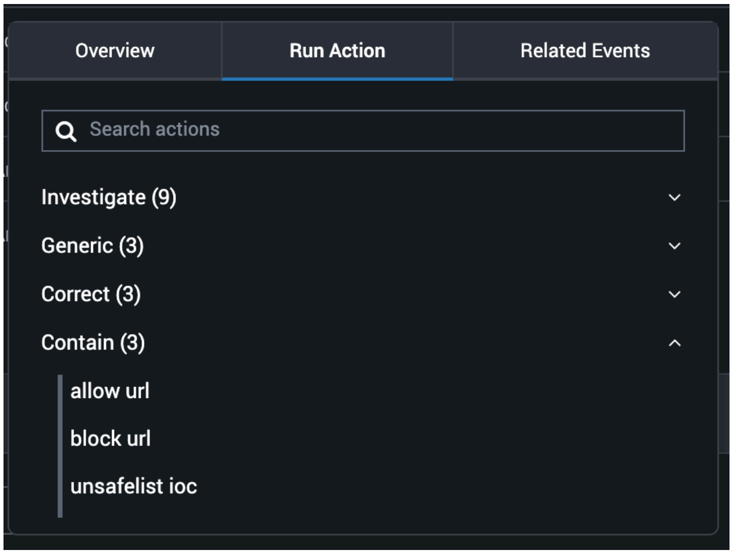
EVENT SEVERITY

○ Critical	0
○ High	0
● Medium	1
○ Low	0
○ Informational	0

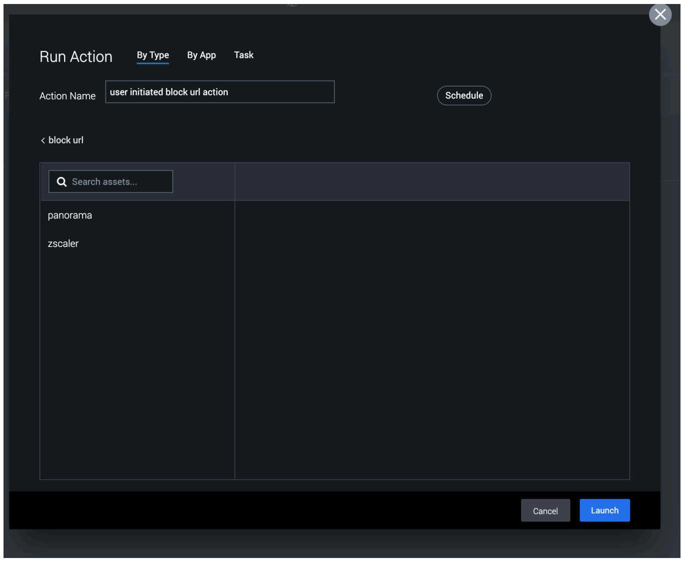
Total Events: 1

Tags:

5. Click the **Contain** action
6. Click “**block url**”

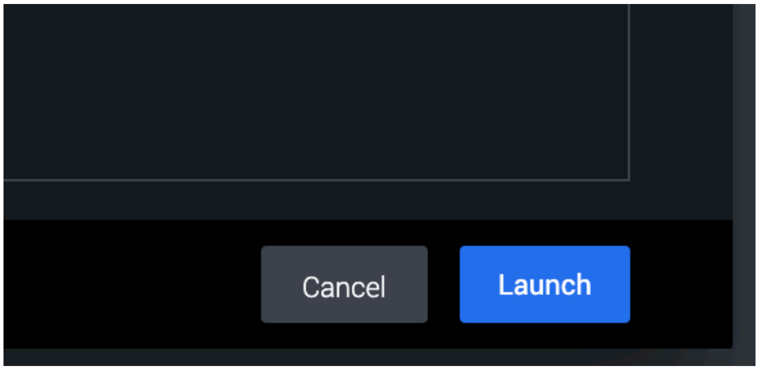


7. Select the zscaler app



Action Name: user initiated block url action

8. Click Launch


Cancel
Launch