Splunk Attack Analyzer Workshop Lab Guide

Splunk Attack Analyzer Exercises

Exercise 1 - Review Live Job Submission Results

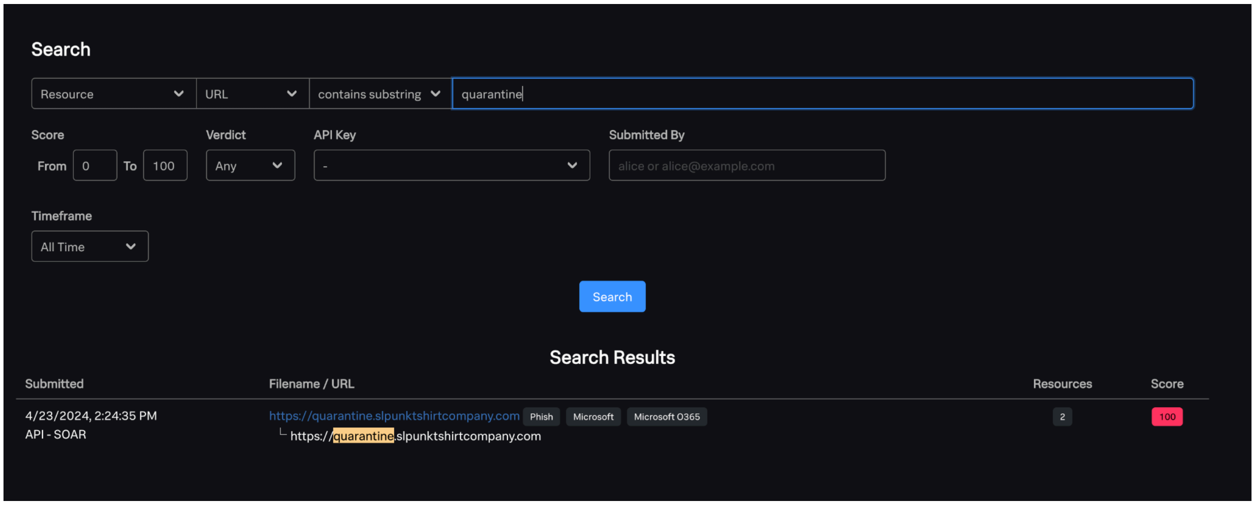
Task 1

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



Resource | URL | contains substring | quarantine

Score From 0 To 100

Verdict Any

API Key -

Submitted By alice or alice@example.com

Timeframe 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

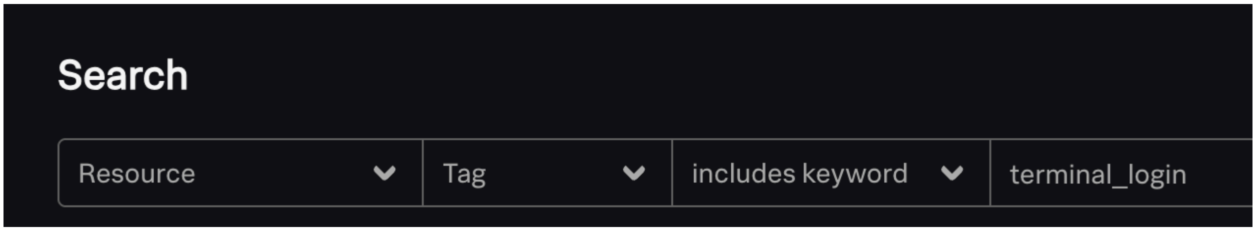
7. Analyze the results
    - What was the verdict of the submission?

- 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

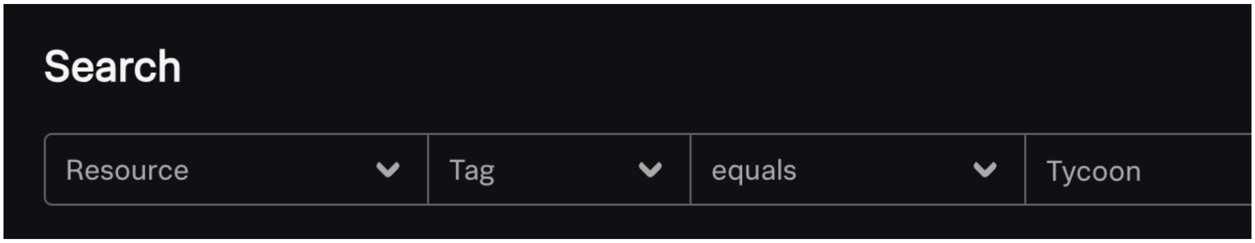
Resource | Tag | includes keyword | terminal_login

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?