

Project: Performing Incident Response using Splunk SOAR

Clay Jones

Objective:

In the project, I took part in a splunk workshop that involved teaching the participants how to automate incident responses by using Splunk's SOAR application. This seminar involved investigating a suspicious domain, acting on it, and creating an automated workflow for it.

Step 1:

First, using a domain reputation action, we scanned the domain using virustotal. Using this action, we were able to determine that the domain had a bad reputation. We then found the IP address by using the lookup domain action by performing a DNSlookup.

Exercise #1 - Look up the domain

Re-enforcing the concepts

Estimated Duration: 2-3 Minutes

Use the steps we just discussed to run a **look up domain** action against the same domain we just investigated using the reputation check

- fpteraardela.band

From the lookup domain action, *determine the IP address* that was associated with the domain name

Hint

- Use Threat Miner as the App for the lookup domain action

02:23

© 2024 SILVER INC.

Step 2:

Afterwards, using a file reputation action, we scanned the file's hashes using virustotal. Using this action, we were able to determine that the hashes had a bad reputation also.

Exercise #2 - Check File Reputation

Still re-enforcing the concepts

Estimated Duration: 2-3 Minutes

Using similar steps to what we previously covered, run a **file reputation** action the file hash identified in the original artifact

Review the details of the artifact to locate a file hash (e.g., sha1, sha256, md5) and investigated it further

What percentage of the detections were positive?

Hints

- There is only one file hash in the artifact details
- You can search at the top of the run action box to narrow down the results by using specific words or phrases

00:03

© 2024 SPLUNK INC.

admin

Event reassigned to "user005-splk" (id: 100) Dec 6th 2024 at 4:45 pm

user005-splk | Alice Bluebird 24 minutes ago

user initiated domain reputation action 1 action failed for app VirusTotal v3

user initiated domain reputation action ✓

user005-splk | Alice Bluebird 19 minutes ago

user initiated lookup domain action ✓

user005-splk | Alice Bluebird 4 minutes ago

user initiated file reputation action ✓

VirusTotal v3 ✓

hash = 8d3f68b16f0710f858d8c1d2c699260e6f4316...
Harmless: 0, Malicious: 62, Suspicious: 0, Undetected: 11

user initiated file reputation action ✓

VirusTotal v3 ✓

hash = 5767653494d05b3f3f38f1662a63335d09ae6...
Harmless: 0, Malicious: 62, Suspicious: 0, Undetected: 11

domain reputation

office365update.duckdns.org

file reputation

5767653494d05b3f3f38f1662a63335d09ae6...
8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b

HASH	SIZE	FILE DESCRIPTION
8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b	176640	PE32+ execut

splunk>

lookup domain

office365update.duckdns.org

Info

Domain	office365update.duckdns.org
Type	

RECORD INFO

192.169.69.25

Step 3:

Moving on, we then had to find the location of the who that IP traces back to and find the location. We used the whois ip action to determine the registry of the IP and used the geolocate IP action to find the location associated with this IP address.

Exercise #3 - IP Geolocation

Estimated Duration: 5 Minutes



Almost done...

Our last step in this investigation will be to use the IP found in Exercise #1 and perform a **geolocate IP** action

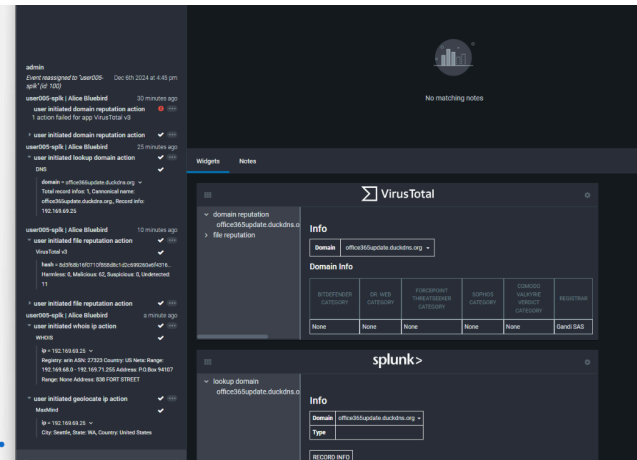
Use the IP address from the lookup domain action previously performed to run the next action from that widget.

What *continent* is the IP address associated with?

Hints

- The  icon next to some data types is useful for running actions quickly
- The  icon in the top-right corner of the Maxmind widget allows you to go into the underlying JSON data to answer the question
- If you wrote the IP address down from first exercise, you can run manually without using the in-context menu. If you figured this out, rest of the session!

05:00



The screenshot shows the Splunk interface with search results for domain reputation and file reputation. The search results are displayed in a table format. The domain reputation results show a domain of office365update.duckdns.org with a reputation of None. The file reputation results show a file of office365update.duckdns.org with a reputation of None. The interface also includes a sidebar with search filters and a top navigation bar.

Exercise #3 - IP Geolocation

Estimated Duration: 5 Minutes



Almost done...

Our last step in this investigation will be to use the IP found in Exercise #1 and perform a **geolocate IP** action

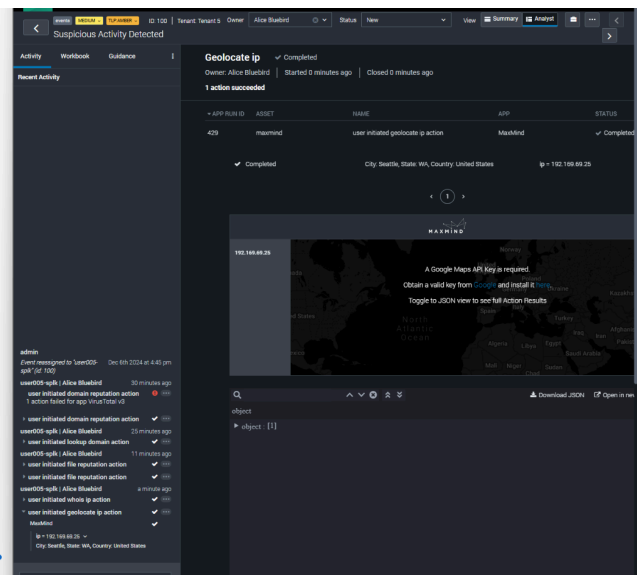
Use the IP address from the lookup domain action previously performed to run the next action from that widget.

What *continent* is the IP address associated with?

Hints

- The  icon next to some data types is useful for running actions quickly
- The  icon in the top-right corner of the Maxmind widget allows you to go into the underlying JSON data to answer the question
- If you wrote the IP address down from first exercise, you can run manually without using the in-context menu. If you figured this out, rest of the session!

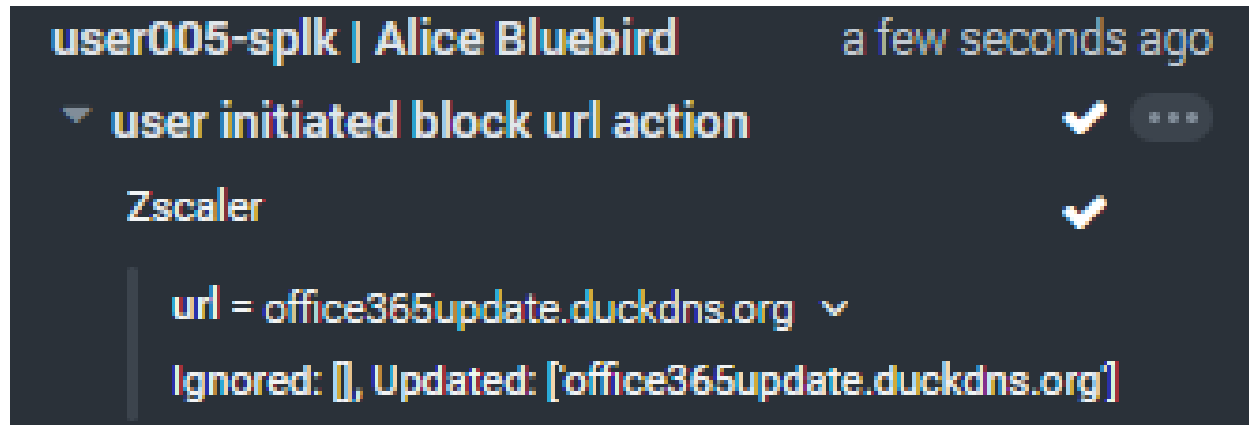
05:00



The screenshot shows the Splunk interface with the Geolocate IP action results. The results are displayed in a table format, showing the IP address 192.168.69.25 and its location: City: Seattle, State: WA, Country: United States. The interface also includes a sidebar with search filters and a top navigation bar.

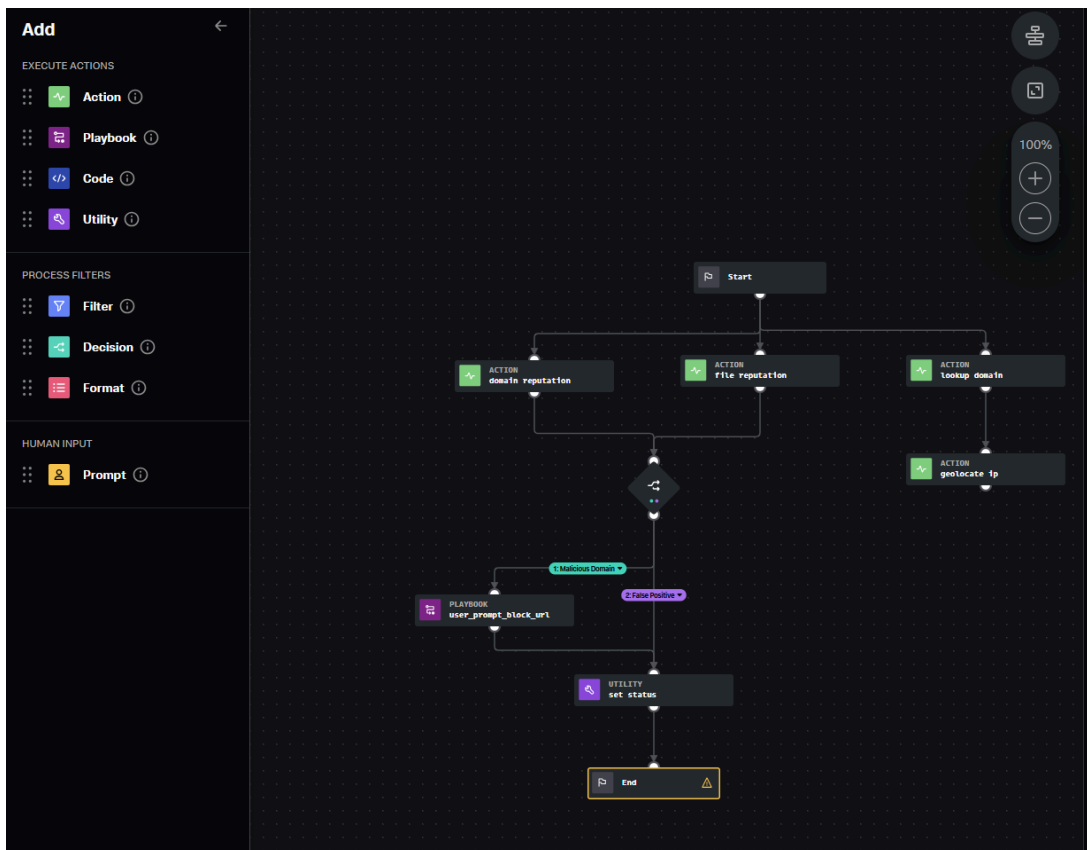
Step 4:

Finally, after gathering all of the data from the previous steps, we determined that this domain was malicious and we used the block url action to use zscaler to block this URL.



Step 5:

To streamline our Incident Response and prevent future incidents, we developed an automated workflow by integrating several processes. Any suspicious or unfamiliar domain detected on the network triggers a series of actions, starting with domain and file reputation scans. If the domain accumulates a predefined number of malicious flags, it will be automatically blocked. If the threshold isn't met, the domain is classified as a false positive. Additionally, the workflow runs parallel to domain lookups and geolocation checks to gather further context. To enhance the accuracy of these workflows, we can introduce more conditions for each action.



Lessons learned:

Automating is a powerful tool and when using Splunk's SOAR application, the incident response process is easier and more centralized.