Project: Performing Incident Response using Splunk SOAR

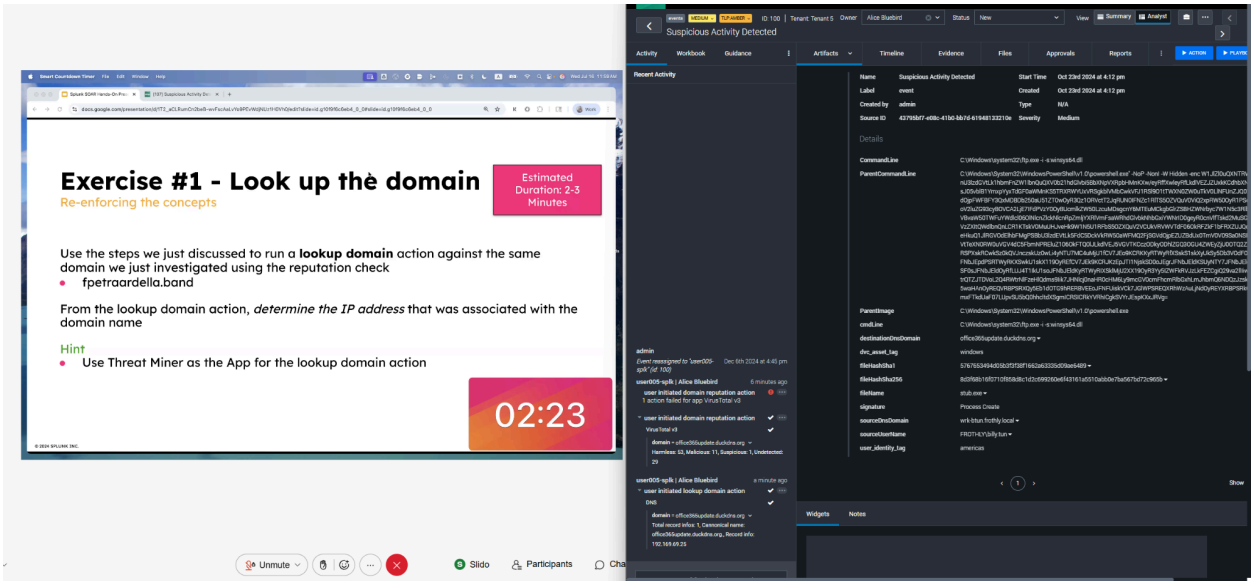
Clay Jones

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.

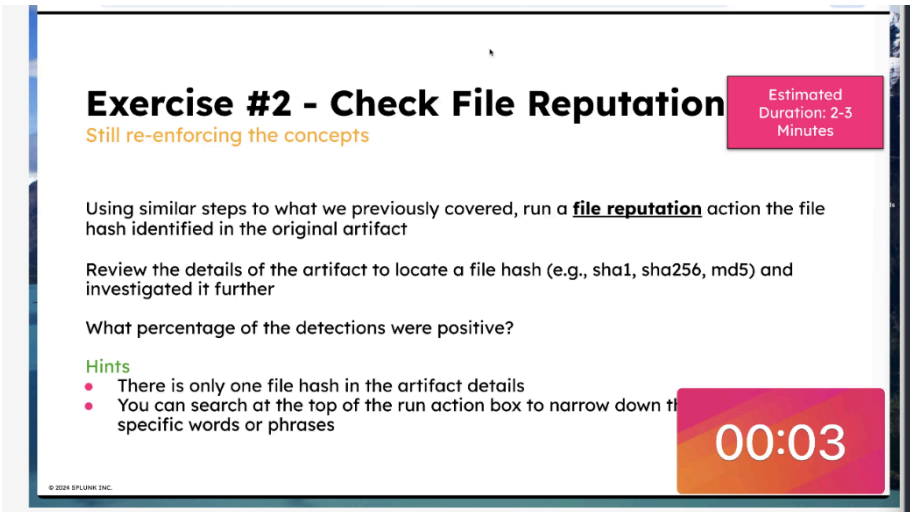
Step 1:

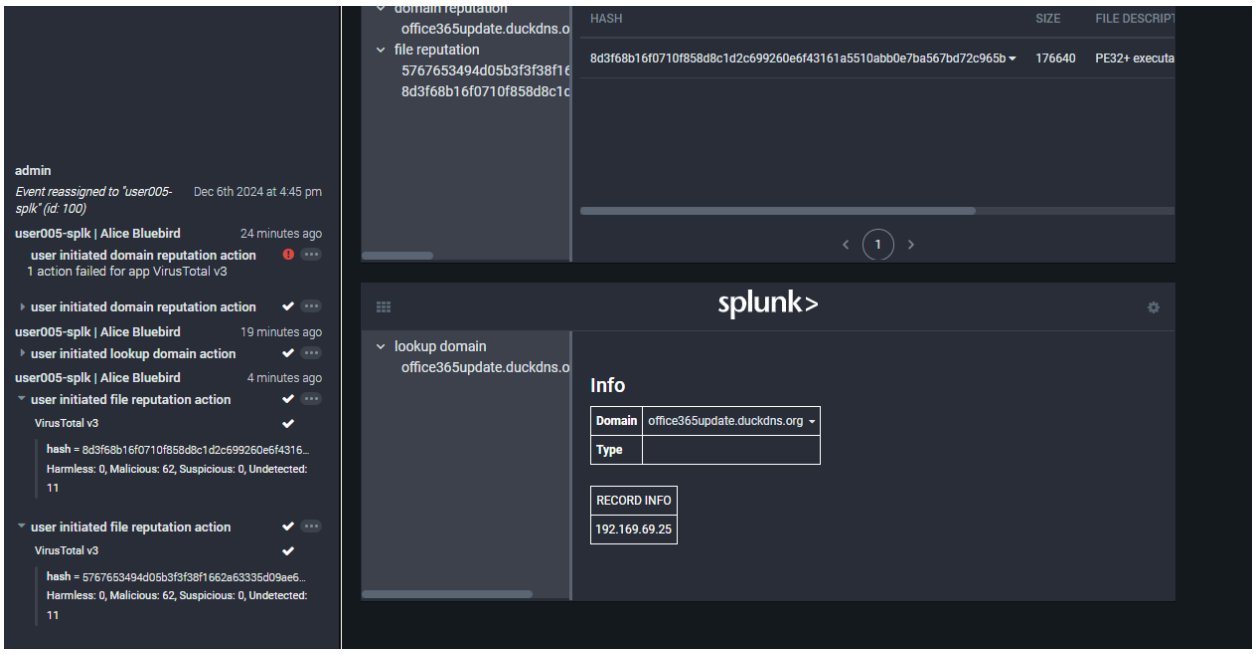
First, using a domain reputation action, we scanned the domain using virustotal. Using this action, we were able to determine that the domain had a bad reputation. We then found the IP address by using the lookup domain action by performing a DNSlookup.



Step 2:

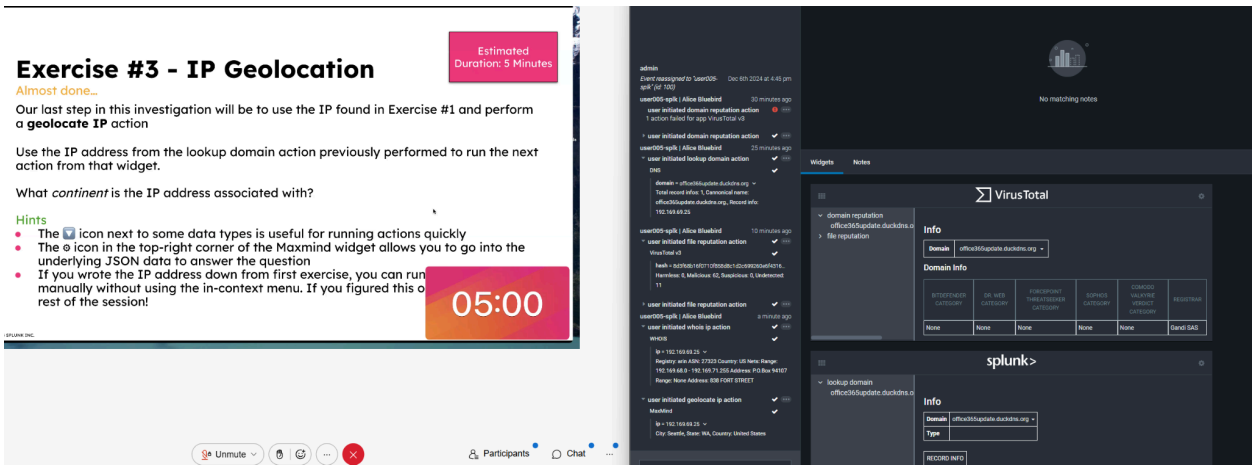
Afterwards, using a file reputation action, we scanned the file's hashes using virustotal. Using this action, we were able to determine that the hashes had a bad reputation also.

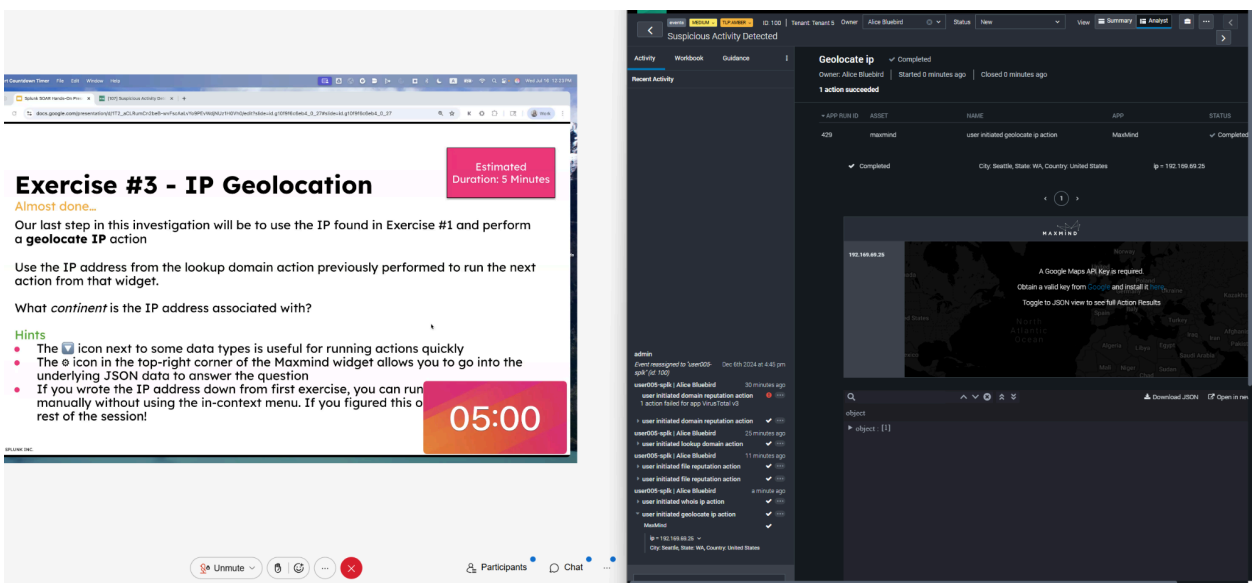




Step 3:

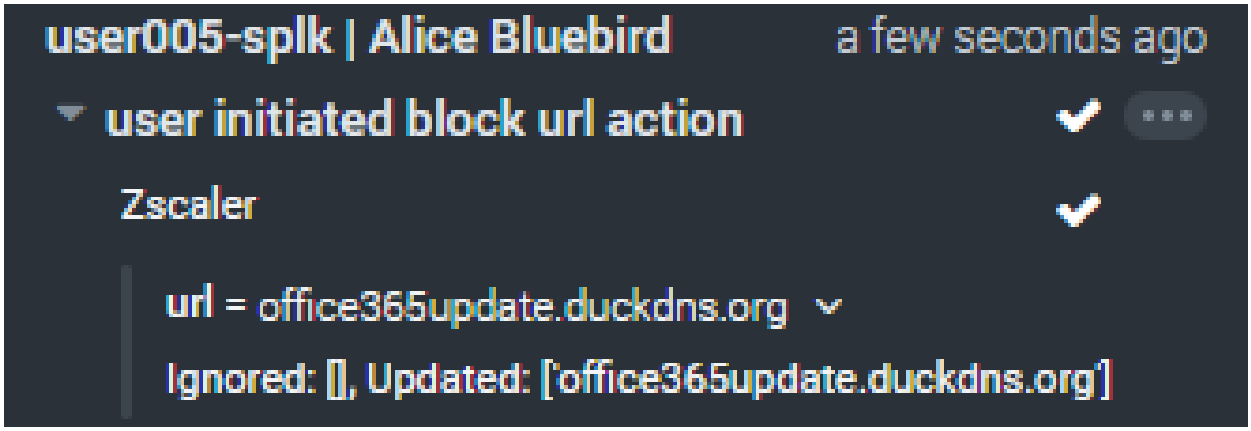
Moving on, we then had to find the location of the who that IP traces back to and find the location. We used the whois ip action to determine the registry of the IP and used the geolocate IP action to find the location associated with this IP address.





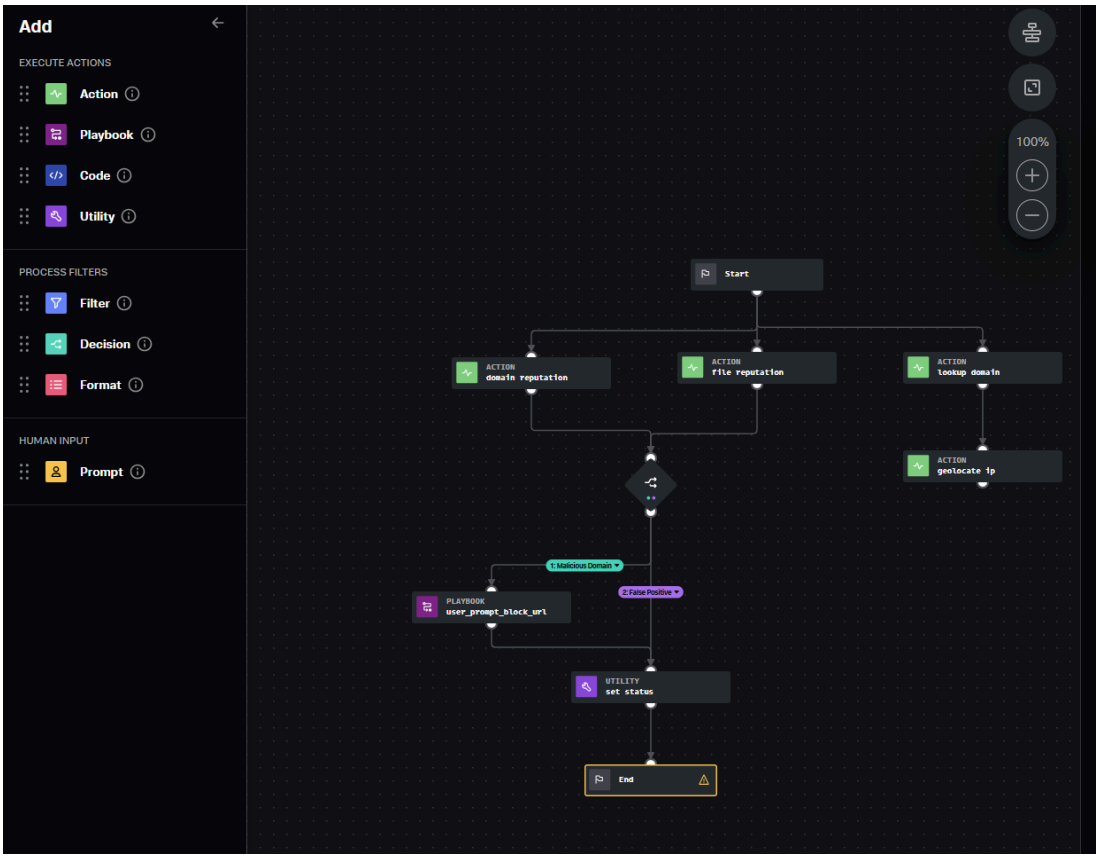
Step 4:

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.