Bennett Hall

Professor Anthony Duhaime Candeias

CISC 6680

April 19th, 2021

Lab 5: SIEM and SOC Exercises with Sumo Logic

****Please note that the answers to each question are in bold beneath the question****

Sumo Logic Basics

1) What query would you use to search for logs in the "Labs/OS/Linux/Security" category?

   _sourceCategory=Labs/OS/Linux/Security

2) What query would you use to parse the computer name from the "Labs/Symantec/Scan" logs?

   _sourceCategory=Labs/Symantec/Scan

   | parse "Computer: *," as computer_name

3) What query would you use to count the number of times the computer values appear in the "Labs/Symantec/Scan" logs?

   _sourceCategory=Labs/Symantec/Scan

   | parse "Computer: *," as computer_name

   | count by computer_name

4) How would you filter results in the “Labs/Symantec/Scan” logs to show just logs from the computer “athena.sumolab.org”?

_sourceCategory=Labs/Symantec/Scan

| parse “Computer: *,” as computer_name

| where computer_name = “athena.sumolab.org”

5) How would you perform a geolookup on the IP addresses in “Labs/Apache/Access“ logs?

_sourceCategory=Labs/Apache/Access

| parse "* - -" as ip_of_client

| lookup latitude, longitude from geo://location on ip=ip_of_client

| count by latitude, longitude

| sort _count

6) How would you perform a geolookup on the “Labs/Apache/Access“ logs and include the state in the search?

_sourceCategory=Labs/Apache/Access

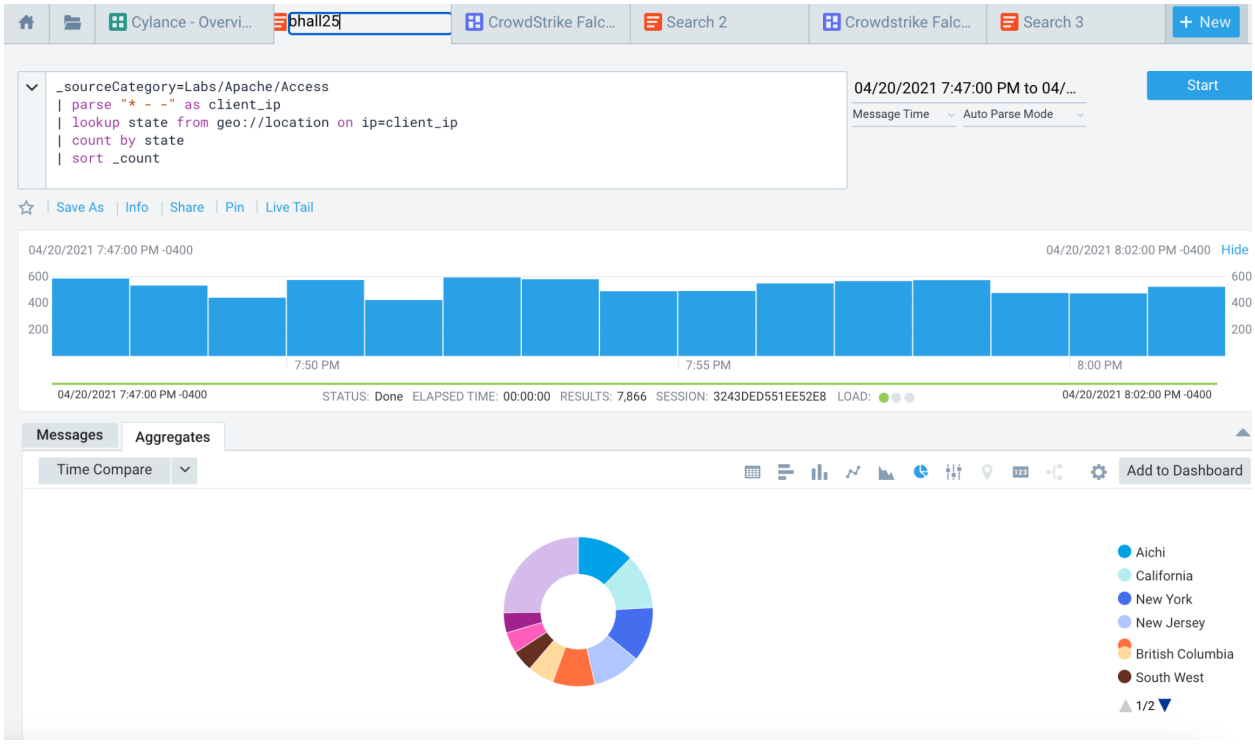
| parse "* - -" as ip_of_client

| lookup latitude, longitude, state from geo://location on ip=ip_of_client

| count by latitude, longitude, state

| sort _count

7) Upload a screenshot of a pie chart showing the breakdown of each state in the "Labs/Apache/Access" logs.

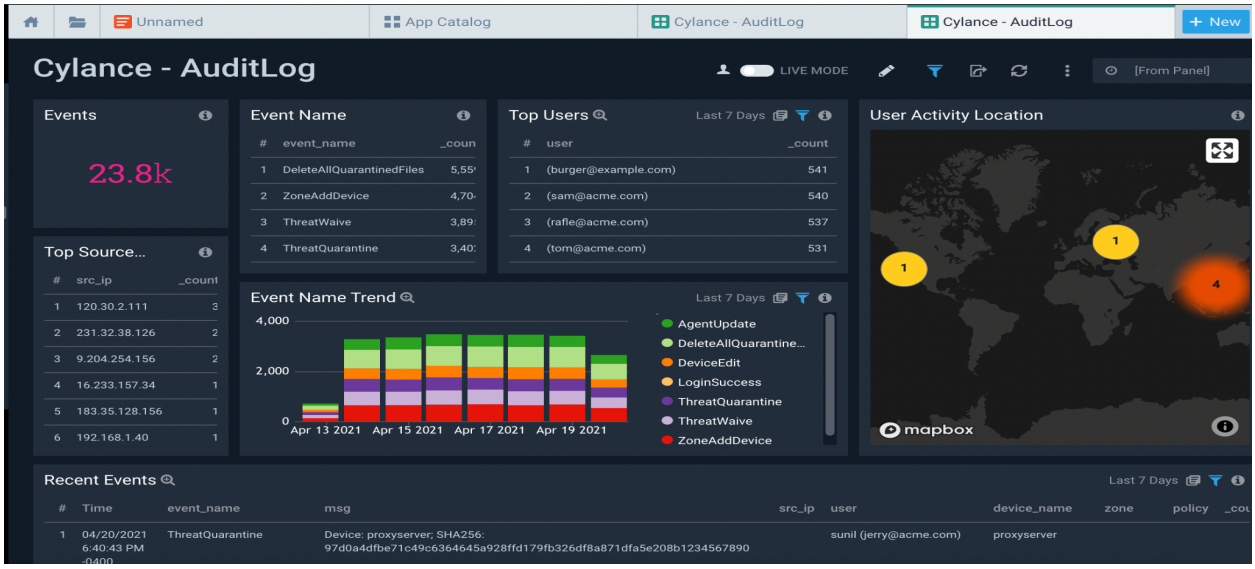


Security Analytics

8) What query would you use to filter "_sourceCategory=Labs/AWS/CloudTrail" logs for root activity?

   _sourceCategory=Labs/AWS/CloudTrail AND root

9) Deploy the Cylance Application Dashboard in sumo and upload a screenshot of any dashboard.



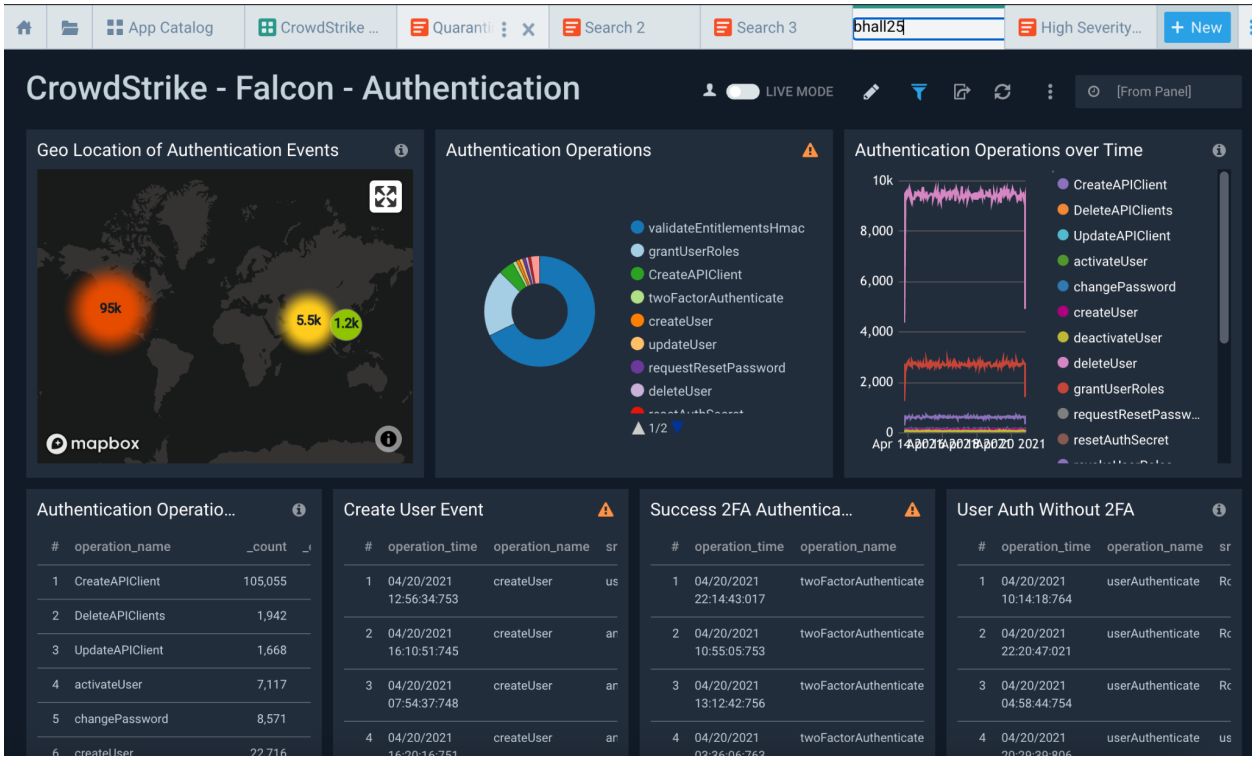
10) What is the device name which has the most "Threat Detections" in the "_sourceCategory=Labs/Cylance" logs?

    proxyserver

11) What file has the most "Threat Detections" in the "_sourceCategory=Labs/Cylance" logs?

    MonkeySource.ax

12) Deploy the Crowdstrike Application Dashboard in sumo and upload a screenshot of any dashboard. Use the category of "Labs/CrowdStrikev2"



13) In the Crowdstrike logs which IP has generated the most Failed User Login Events?

43.229.226.218

14) In the Crowdstrike logs what user account has had the most logs in Without 2FA?

Rock@exo.com

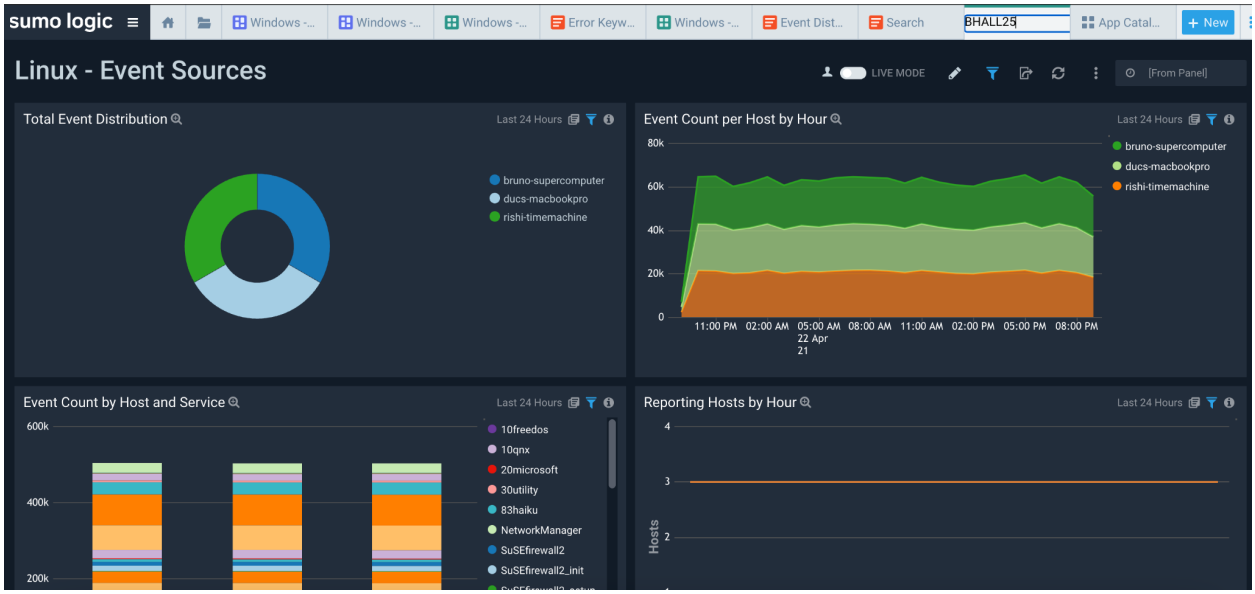
15) Review the Windows event logs. Identify which Event Code produced the most messages?

1102

16) Review the Windows event logs. Identify which User accounts generated the most successful logins? (Provide 1 of the 2 results)

apollo

17) Deploy the Linux Application Dashboard in sumo and upload a screenshot of any dashboard.



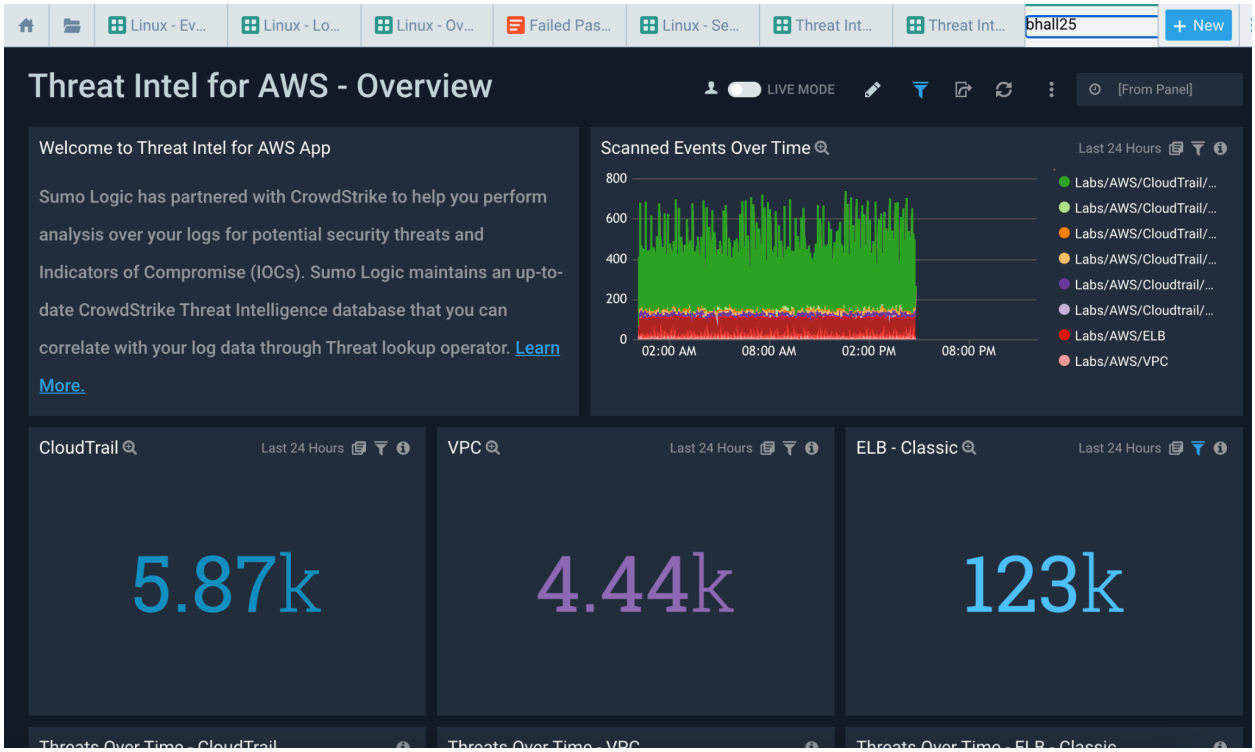
18) In the "_sourceCategory=Labs/OS/Linux/Security" which dest user has the most excessive failed su?

root

19) In the "_sourceCategory=Labs/OS/Linux/Security" which dest user has the most successful password changes?

Sumo

20) Deploy the Threat Intel for AWS and upload a screenshot



21) Write a 1 paragraph summary of your findings in the Threat Intel for AWS.

Deploying the AWS threat intel dashboard gives me the ability to view recent security events over a period of time. The default is 24 hours. I can also view total events over a period of the past 24 hours for CloudTrail, VPC, and ELB. I can also view scanned events and the time when those events occurred. The dashboard gives me the ability to identify what time of day has the most potential security events and what time of days has the lowest number of potential events over a period of time, in this case 24 hours.

22) Write a 2 paragraph summary of your experience using a SIEM (SUMO) and how it would benefit you as an Security Incident Responder.

My experience using SEIM, in this case Sumo, is that it's beneficial to have a system that can collate data across entire networks and present it to incident responders in real time. Companies of varying sizes would benefit from having information about their attack surface centralized. It makes the process of scanning for threats and detecting them much easier. Instead of having to monitor multiple systems and having to do many things at once the process is streamlined with software like SUMO.

If I were a security responder I would be much more organized for and better prepared to respond to an incident with an SEIM. SUMO alerts on incidents, but SUMO also helps to gather vital forensic information. The ability to have a centralized system would make it simpler amidst a chaotic situation that would be brought on by a breach.

Work Cited

1. Sumo Logic. “Hands-on Labs: Sumo Logic Basics.” *Sumo Logic*, October 4th, 2018, Hands-on Labs: Using Sumo Logic. Accessed April 19th, 2021.

2. Sumo Logic. “Hands-on Labs: Security Analytics.” *Sumo Logic,* Hands-on Labs: Security Analytics. Accessed April 19th, 2021.