STEPHEN MENSAH

USER SECURITY LAB

Brute-Force Attack: Screenshots from the Lab

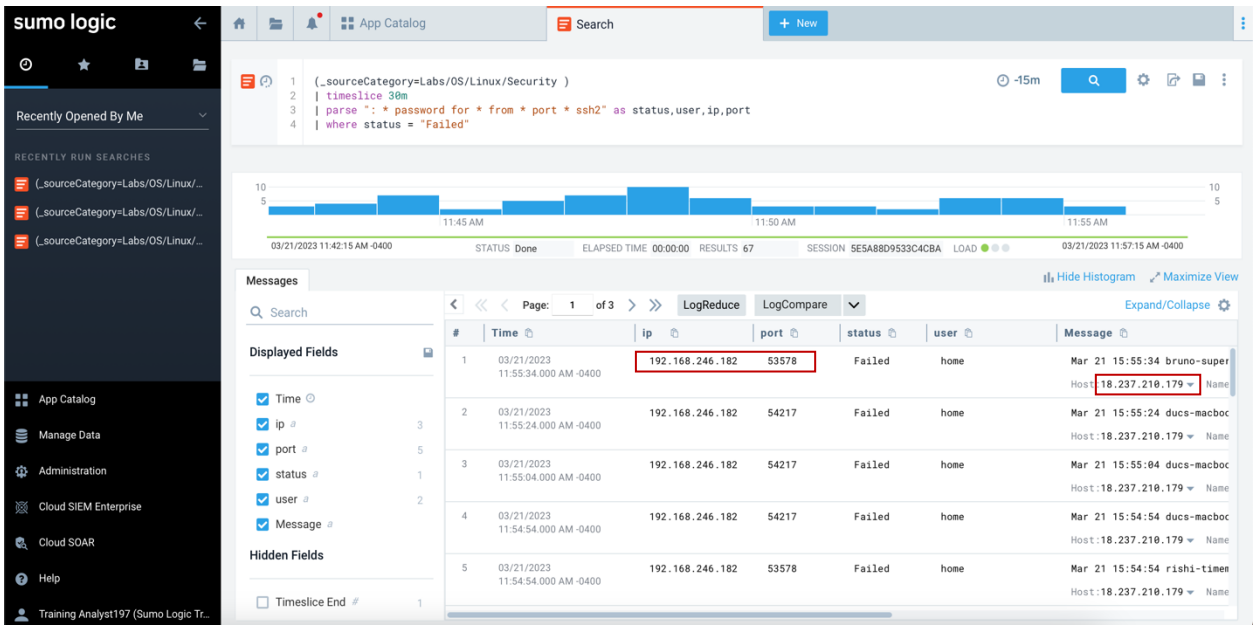

Figure 1: Logs with failed login attempts

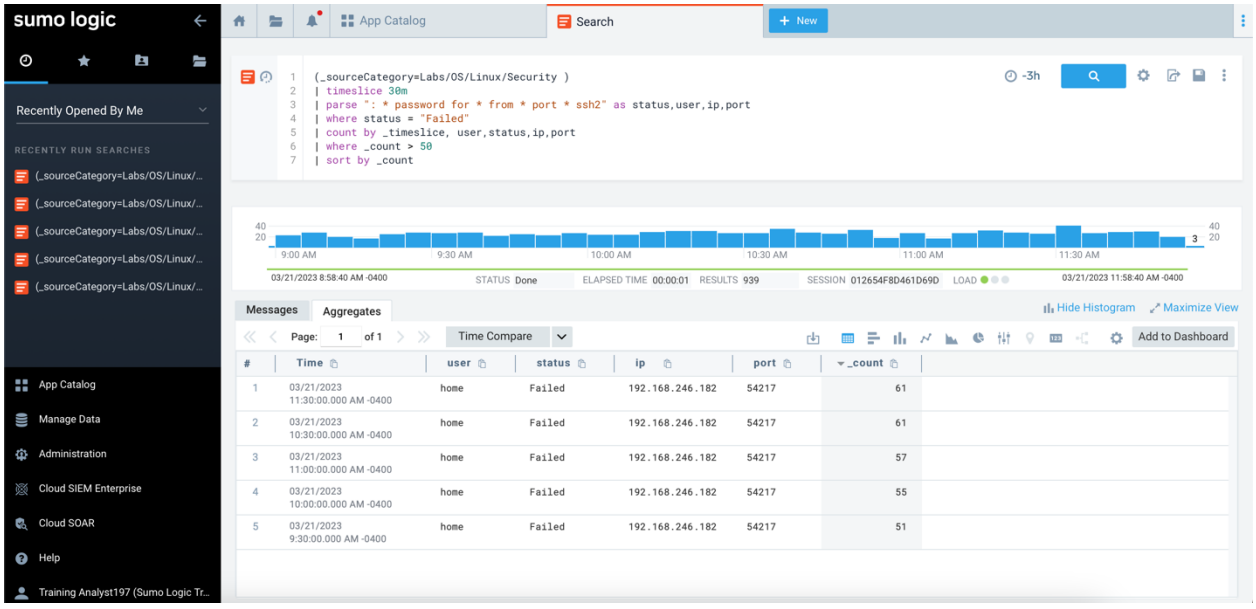

Figure 2: Aggregate of users with more than 50 failed login attempts in 30minutes

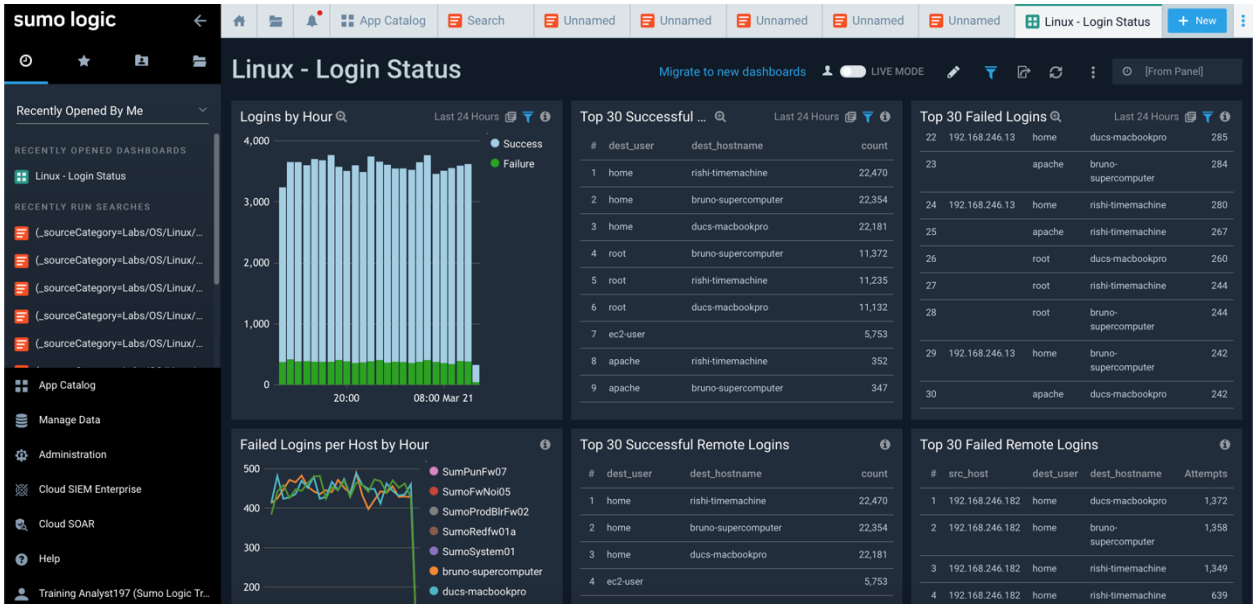

Figure 3: Linux – Login Status Dashboard

Figure 4: Linux – Security Status Dashboard

BRUTE FORCE ATTACK

THREAT SIMULATION

To respond to brute force attacks, I will create an alert that would proactively notify the incident response team when a large number of failed logins are detected from the same user account within a given period of time. When the alert is triggered, I will monitor all logs 2 days prior to the alert and hours after the alert. I will divide the period under review into chunks of 10 minutes and create an outlier to detect any deviation from normal behavior. I will use sumo logic to create queries to search for users with many failed logins and at least one successful login. This will help to monitor any potentially compromised user accounts and their respective actions on our systems. From the logs, it was evident that a user by the name "home" had multiple failed login attempts to the host device with the IP address 18.237.210.179 using the computer with the IP address 192.168.246.182 on port 54217 (figure 1). Investigating further, the same user was able to gain access to the said host on different ports. Analyzing the logs from 3 days will be extremely consuming, as such, I will use the "Log Reduce" functionality to create useful signatures/patterns to efficiently analyze the large volume of logs. I will use the Linux – Login Status, and Linux Security dashboard to monitor logins to our resources and security-related activities from each user respectively. Brute force attacks can have severe impacts, as such, I will assign a high criticality level. An incident response report will be written to document the event and the company's threat intel will equally be updated.

BUSINESS IMPACTS

Brute force attacks can be used to gain unauthorized access to targeted systems. Businesses can suffer from short-term risks of sensitive data theft, disruption of business services, hijacking targeted systems, and financial losses. Long-term risks can be in the form of legal and data

compliance battles from users and compliance bodies, damage the company's reputation, pave for further malware attacks, and loss of customer trust.

REMEDIATION

Regularly monitor and analyze user and login activities, stay up to date with security and systems trends, block compromised user accounts and isolate affected systems, enforce secure password policies across the organization, limit the rate of failed login attempts on each system, and implement multi-factor authentication to add an extra layer of security.

Screenshots

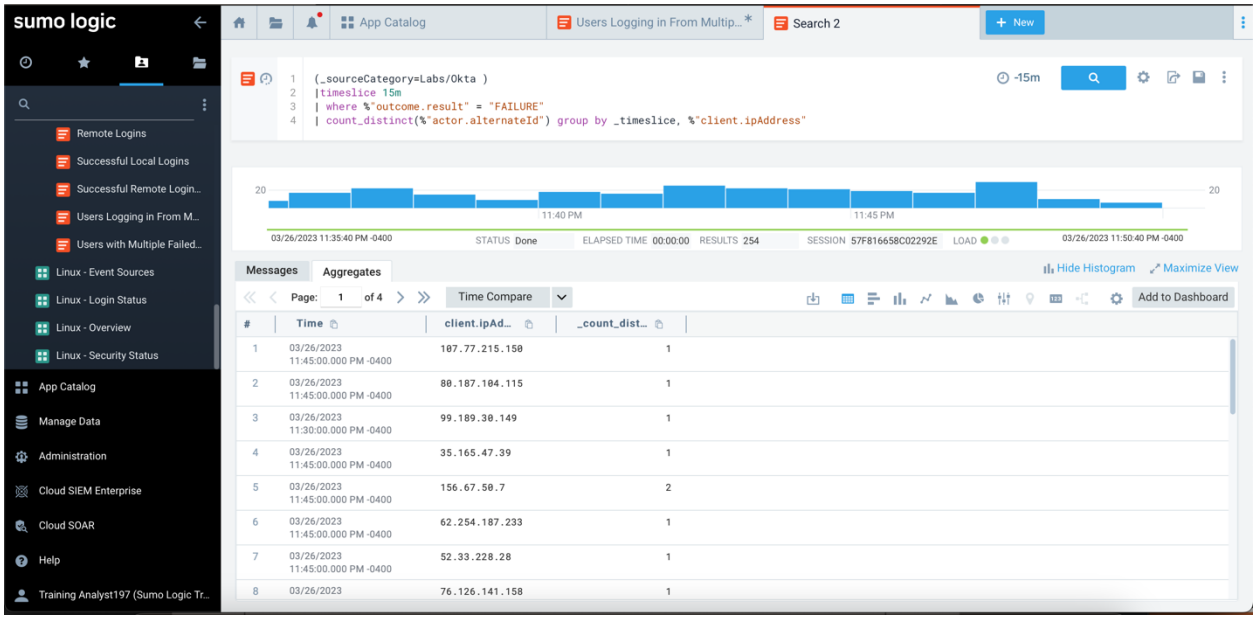

Figure 5: IP addresses with failed login attempts

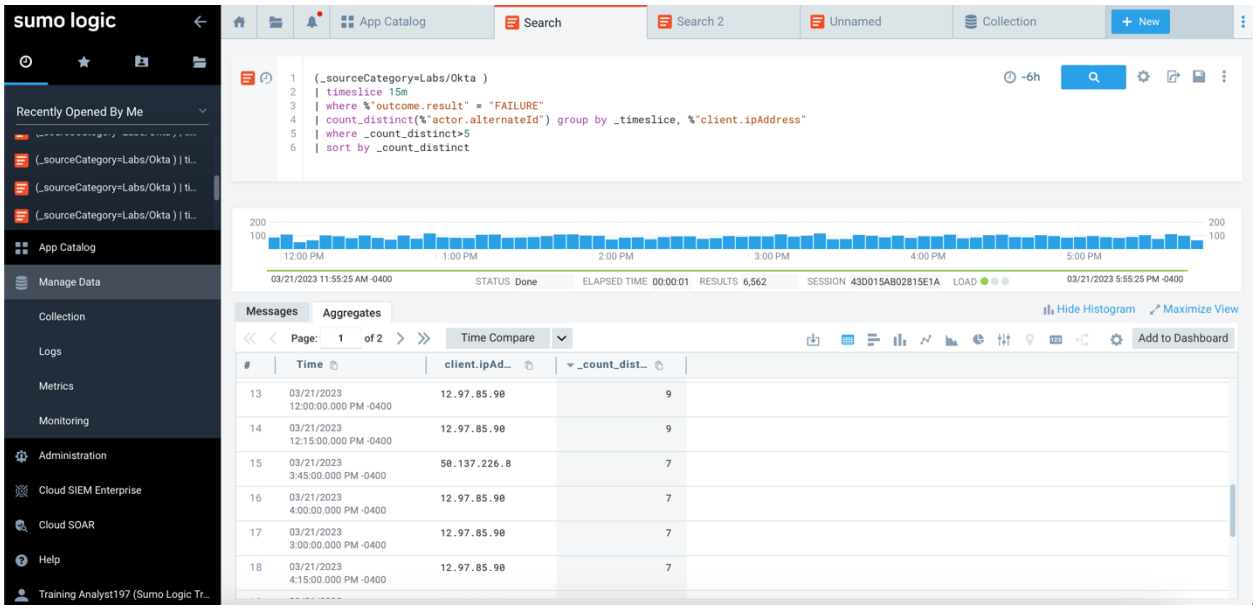

Figure 6: IP addresses with more than 5 failed login attempts in 15 minutes.

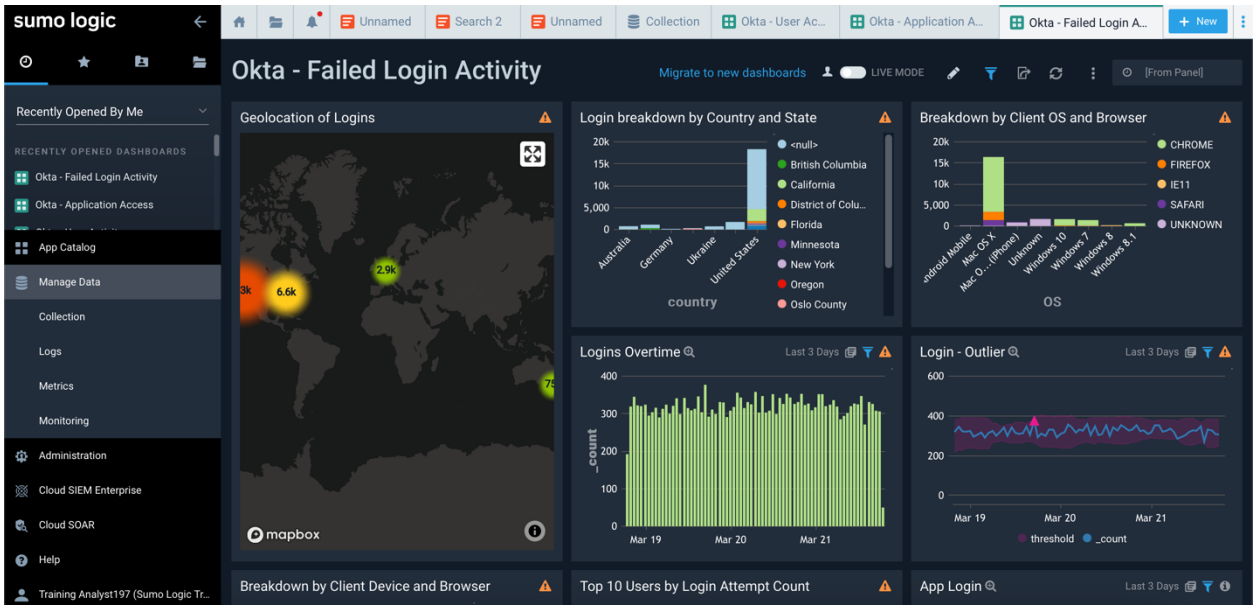

Figure 7: Failed Login Activity Dashboard

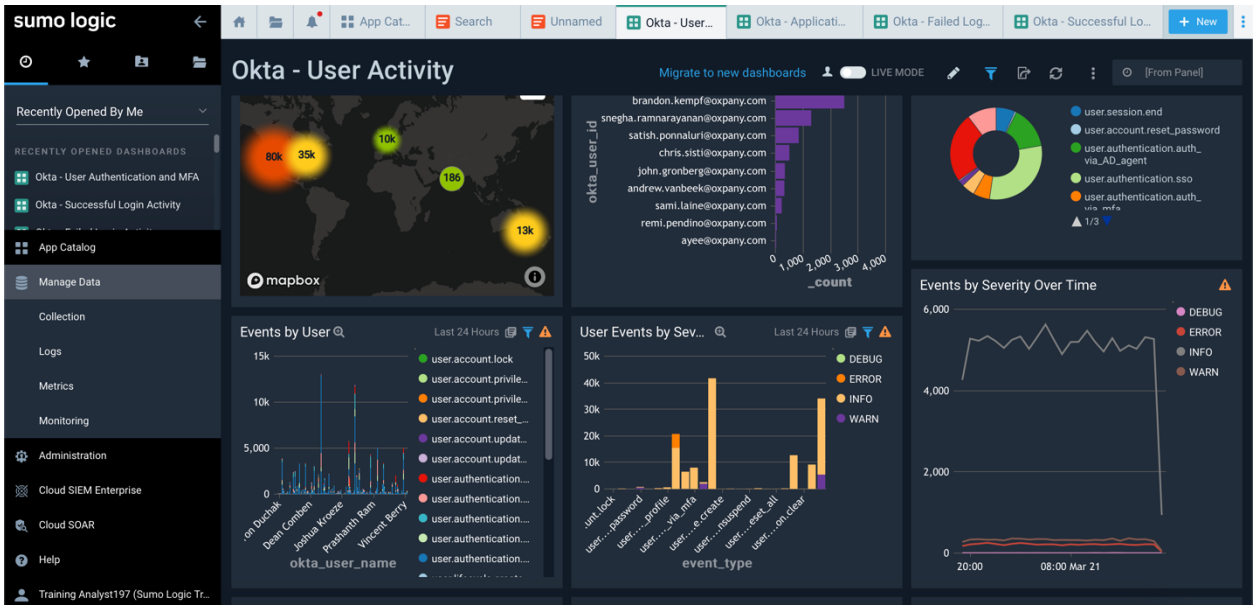

Figure 8: User Activity Dashboard

PASSWORD SPRAY

THREAT SIMULATION

The first step for me to take as a SOC analyst is to create a customized alert to monitor all ongoing activities and notify the security team when the alert is triggered. I will equally use alert query to create a dashboard to enable the team to monitor for such suspicious activity in real time. Because password spraying techniques have a higher successful login rate, I will start analyzing logs captured 7 to 14 days from the time the alert was triggered and monitor all activities after the alert. The analysis will cover all logs from account management services as well as single sign-on applications like Auth0 (from Okta) that use authentication protocols. I will use "timeslice" to break all the log data into time buckets of 10 minutes to determine the number of times a login attempt originated from the same IP address but with different user accounts. 5 successive failed login attempts would be classified as suspicious activity. I will then use the "time compare" button to compare current failed login attempts on a device against past attempts. I will equally build queries to gather the geographical location of each IP address to detect the origin of each attack. From the query, two IP addresses (12.97.85.90 and 50.137.226.8) were seen to be constantly making login attempts every 15 minutes. Having identified these IP addresses, I will further build queries to track successful login attempts and their associated user activities on our system to identify other malicious activities that may have happened. I will use the Okta – failed login activity, user activity, and successful login activity dashboard to monitor and generate insights from the logs. I will also assign a high criticality level to this attack, and build additional attack signatures to update the company's threat intel. An incident response report will be written and shared with all major stakeholders.

BUSINESS IMPACTS

Short-term risks that the business entity can face include disruption of day-to-day business activities, huge financial harm, compromised accounts can be used for other malicious activities, and exposure of sensitive data. Long-term risks are legal and data protection compliance battles, loss of customer's trust and damage to the company's brand.

REMEDIATION

Regularly monitor user and system activities for anomalies, implement Multi-Factor Authentication, block requests from suspicious IP addresses and suspend all compromised user accounts, adopts NIST password guideline and enforce strong password policies across the organization, limit access to critical infrastructure, and set appropriate account lock thresholds.

Screenshot

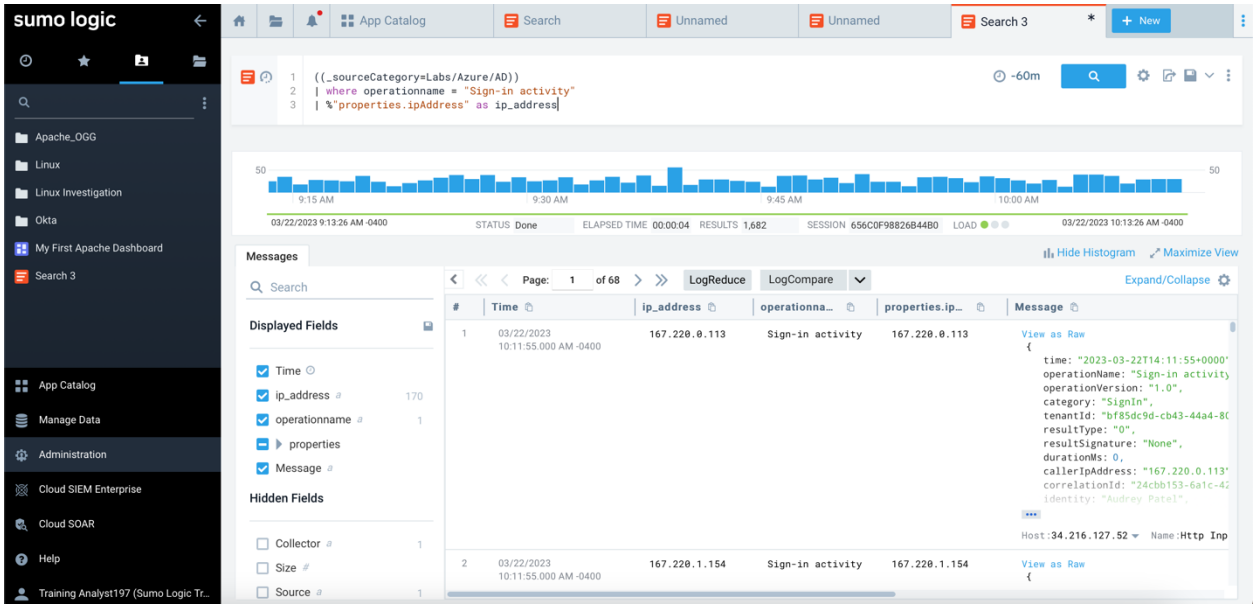

Figure 9: IP address with sign-in activities

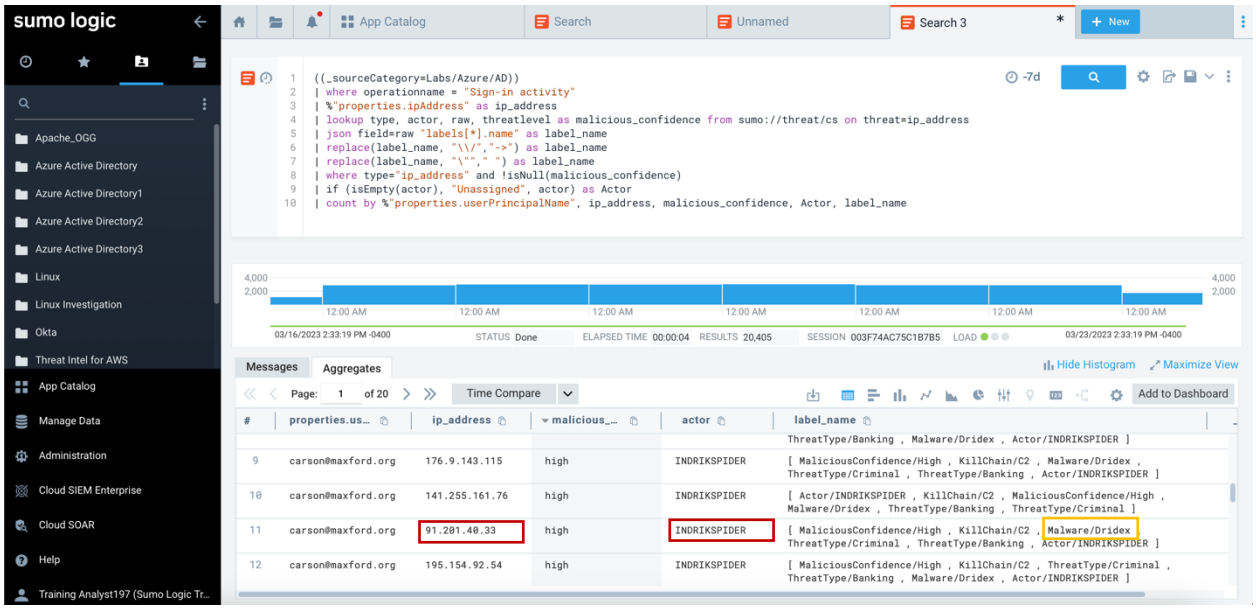

Figure 10: Logs with a known malicious confidence

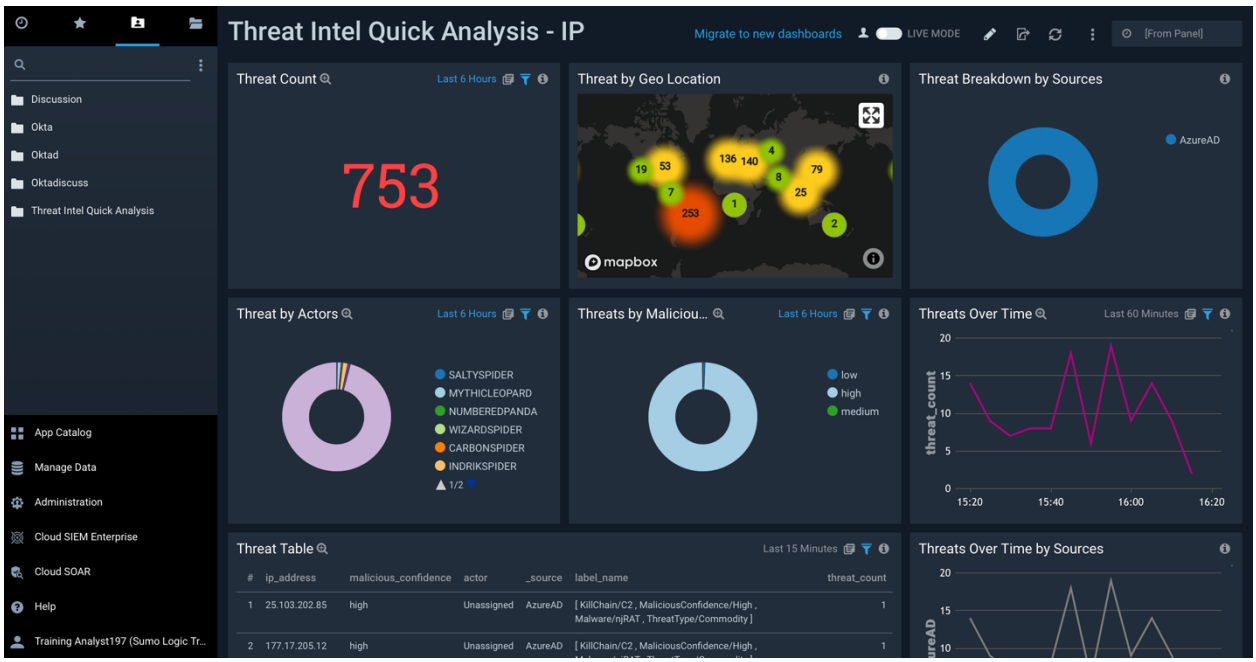

Figure 11: Threat Intel based on IP address Dashboard.

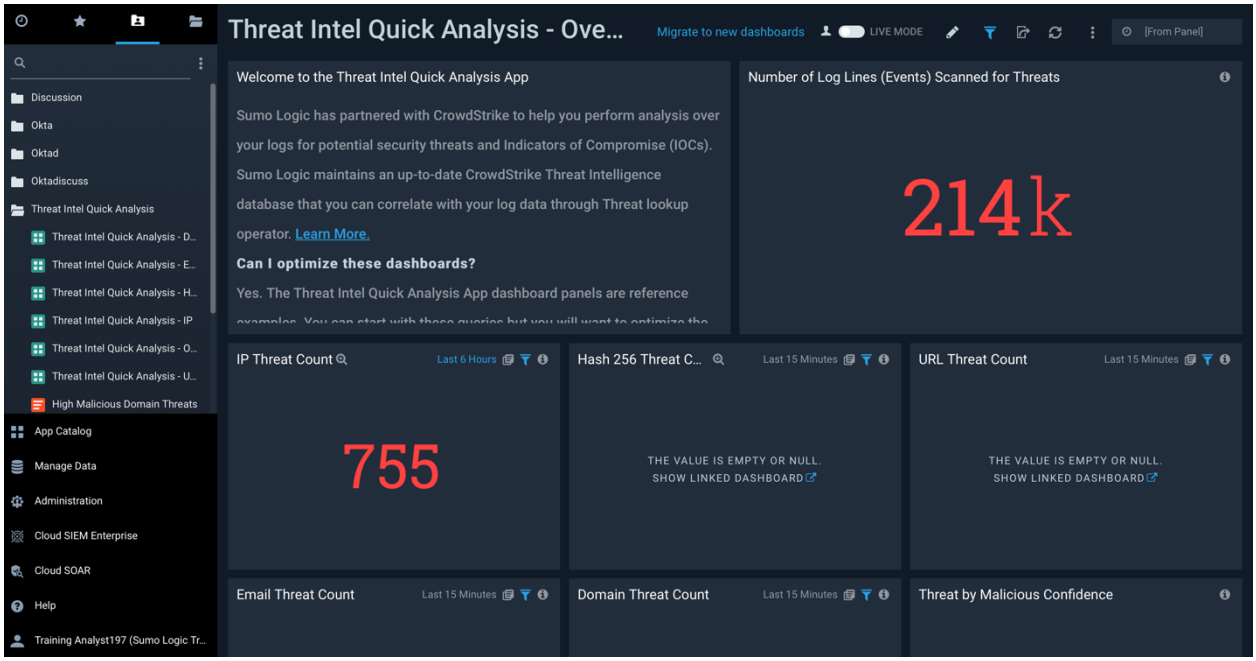

Figure 12: Threat Intel Overview Dashboard.

THREAT INTELLIGENCE

THREAT SIMULATION

To provide prompt responses to malicious login activities, all system logs will be collected and monitored in real time. An alert will be created from a search query to notify the incident response team. When an alert is triggered, a comprehensive log analysis will be conducted by the security team on sumo logic to search for potential threats and any indicator of compromise. I will parse (using regex) all collected log fields and run them against an up-to-date threat database from CrowdStrike which is available on Sumo Logic. I will then screen the logs by applying additional filters to focus on logs with known threat confidence, both verified and unverified. In addition, since sumo updates its threat database once every day, I will develop scheduled log queries that will run once the database has been refreshed to have an accurate result. The analysis scope will be set to include logs collected 7 days prior to the alert to track any further malicious activity conducted in our system. I will use the "time compare" button to compare past aggregated malicious activities from the same threat actors. From the logs, some of the activities were conducted by known threat actors while some were "unassigned". One notable actor is "INDRIKSPIDER" – a Russian-based cybercrime gang responsible for the Dridex (figure 10) ransomware which was identified to be targeting online banking systems since 2017. The different criticality levels ranging from low to high will be assigned to different suspicious login activities. The Threat Intel Quick Analysis – Overview and IP dashboard will be employed for this analysis. An incident response report will be written and shared with stakeholders and the threat intel for the company will be updated.

BUSINESS IMPACT

Businesses that use Azure services can face short-term risks such as exposure of sensitive data, and financial losses from potential business disruption and ransomware. Long-term risks can be in the form of legal battles and loss of customers' trust. Legal fees and customer settlement amounts can also collapse the business.

REMEDIATION

Regularly monitor and analyze system logs, employ automated systems to provide prompt alerts, isolate privileged accounts, enforce strong password policy or utilize passwordless solutions, and train employees on trending threats and secure practices.

References

Splunk (2023, January 10). Brute Force Attacks in 2023: Techniques, Types & Prevention. Retrieved March 21, 2023 from https://www.splunk.com/en_us/blog/learn/brute-force-attacks.html

Kaspersky (n.d). Brute Force Attack: Definition and Examples. Retrieved March 21, 2023 from https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Crowdstrike (2022, July 27). Password Spraying. Retrieved March 21, 2023 from https://www.crowdstrike.com/cybersecurity-101/password-spraying/

Ranjan, R (n.d). Password Spraying Attack. Retrieved March 21, 2023 from https://owasp.org/www-community/attacks/Password_Spraying_Attack

Splunk (2021, June 10). Detecting Password Spraying Attacks: Threat Research Release May 2021. Retrieved March 21, 2023 from https://www.splunk.com/en_us/blog/security/detecting-password-spraying-attacks-threat-research-release-may-2021.html

MITRE (2020, February 11). Brute Force: Password Spraying. Retrieved March 21, 2023 from https://attack.mitre.org/techniques/T1110/003/

Poza, D (2021, July 8). What Is Password Spraying? How to Stop Password Spraying Attacks. Retrieved March 21, 2023 from https://auth0.com/blog/what-is-password-spraying-how-to-stop-password-spraying-attacks/

Grassi, P., Garcia, M. & Fenton, J. (2017). *Digital Identity Guidelines, Special Publication (NIST SP)*, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-63-3 (Accessed March 21, 2023)

Ninocrudele (2022, September 30). The three most effective and dangerous cyberattacks to Azure and countermeasures (part 2 – attack the Azure Storage Service). Retrieved March 23, 2023 from https://ninocrudele.com/the-three-most-effective-and-dangerous-cyberattacks-to-azure-and-countermeasures-part-2-attack-the-azure-storage-service

Alspach, K (2022, June 1). 6 'nightmare' cloud security flaws were found in Azure in the last year. Does Microsoft have work to do? Retrieved March 23, 2023 from https://www.protocol.com/enterprise/microsoft-azure-vulnerabilities-cloud-security

Microsoft (2022, December 30). Five steps to securing your identity infrastructure. Retrieved March 23, 2023 from https://learn.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity