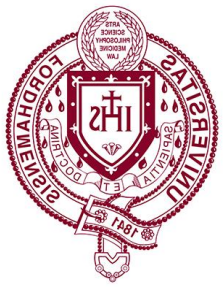


FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

INTRUSION DETECTION & NETWORK FORENSICS (CISC 6680)

Lab: Web Application Investigation

Name: Gopi Gor

FDIN: A21370441

Malicious User Agent Strings

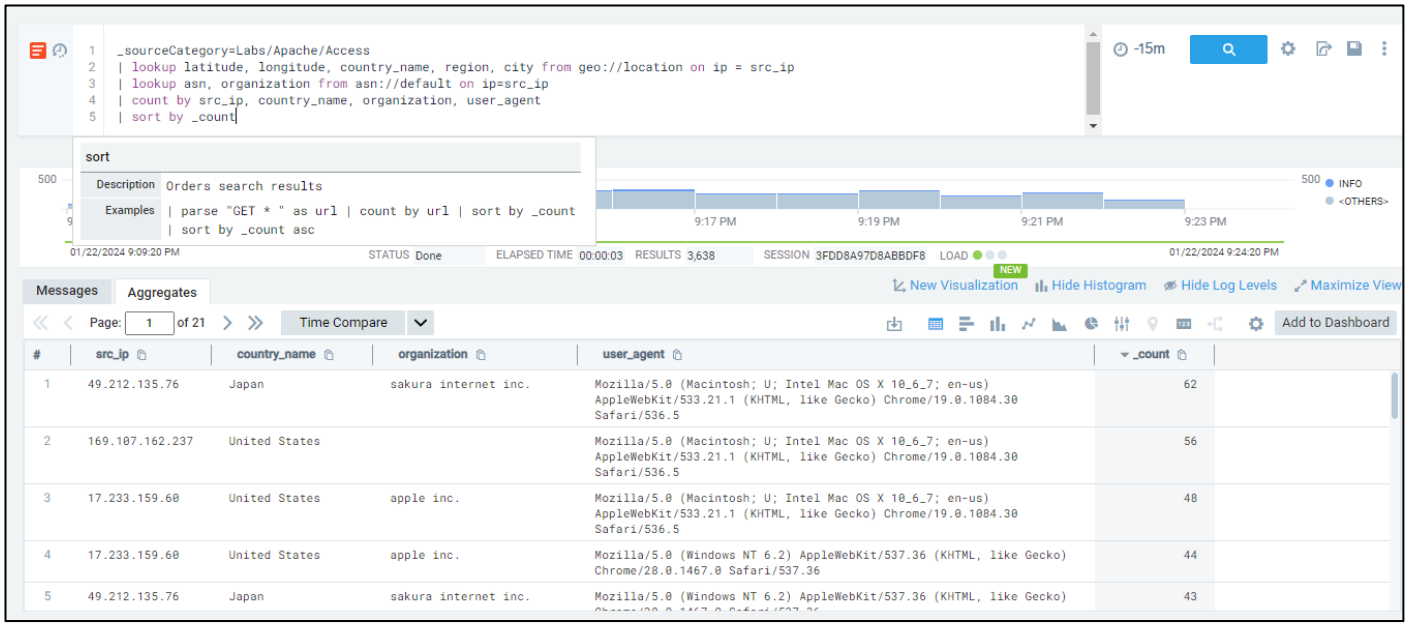
For a user investigating the alert as a SOC analyst, for starters, the traffic and logs generated could be inspected in detail, like organization, source IP, anomalies in the logging behavior, failed attempts to log in and log out, the count of those activities and then a common pattern could be found between the user agent strings. These details and more can be inspected to understand the generated alerts. The findings can be documented at every step along with the assets that have been used in the current during the search test in Sumologic. To assign criticality for this alert created, the criticality could depend on what kind of severity the user string has, for example, if the user string was passing a malicious command to execute a malicious file after the first connection, it could be risky and would be given a **high** criticality. In this alert, it is a **high** criticality due to the nature of the bash command that is running and trying to exploit a vulnerability to get entire control of the system (unauthorized access). The dashboards to be used for this alert type could be dashboards that collect web server details dashboards, user-related dashboards, and network IP-related dashboards. This would allow for easy viewing and be useful in this case scenario.

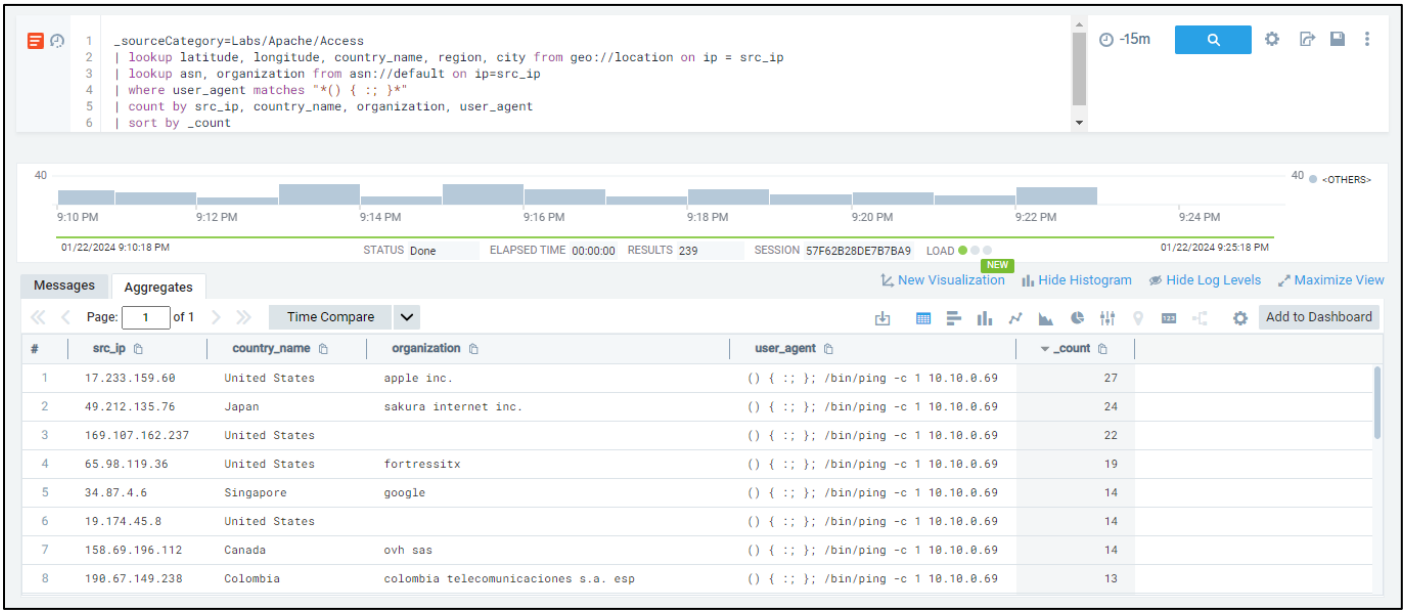
The business implications of the malicious user strings could impact the business in many ways. It would pose a risk to web servers and people using these web server applications for their work. This could also affect the web server's availability such as DOS attacks which can pose a big problem for the whole business not being able to run normally. This could affect the smooth running of the business and revenues generated. Short-term risks would be direct exploitation of vulnerabilities and trapping of important data of the company, whereas long-term risks could mean infiltration and setting up of worms and malicious payloads to run APTs over the course of time.

In terms of holistic remediation, users could be educated through security awareness training. Access control methods could be set up which focus on a double layer of MFA. The web servers being the main entry point, could be elevated on higher detection mechanisms and security tools to cut out anything that we may or may no have missed.

Malicious User Agent Strings

(Screenshots)





Brute Force Discovery

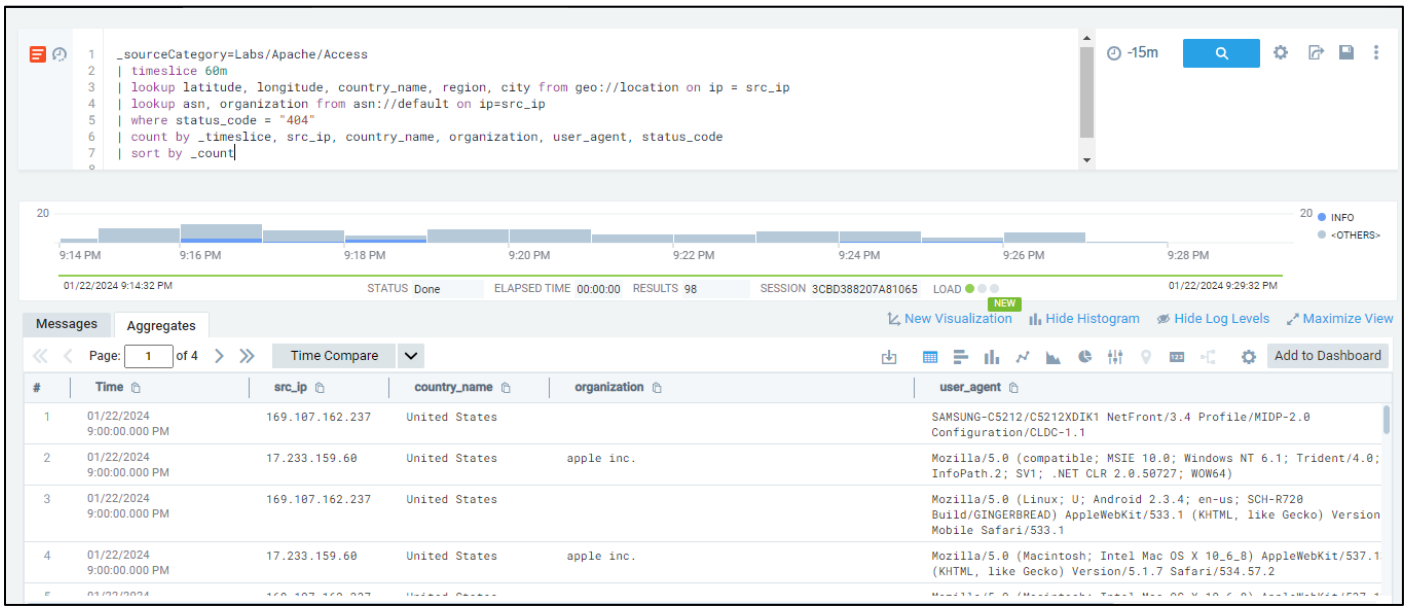
In the event of Brute Force Discovery occurring, a SOC analyst would focus on understanding the patterns and common login attempts. Failed and successful logon attempts could be logged and the number of times a failed attempt occurred before a successful one allows the analyst to investigate the alert. The different IP addresses and users can be analyzed further to comprehend the scope of the alert being triggered. Since a brute-force discovery would mean successful attempts on user accounts and passwords, affecting unauthorized access, the criticality assigned to this alert would be **high**. With regards to the dashboards we would use, it would mainly be regarding user logon-logoff activity, authentication logs and account changes dashboards which would allow the analyst to draw conclusions and take quick decisions about the incident that may occur.

In a business context, brute force discovery of accounts would lead to unauthorized access, therefore leading to loss of confidentiality and availability. Customer and client-sensitive information could be compromised, causing loss of trust in the organization. Some of the short-term risks would be loss of data, and personal sensitive information following which the long-term risk could be identity theft occurring to the customers and employees being prey to a phishing scam. In addition to this, the company data could be sold on the dark web, leading up to the loss of millions of dollars in revenue.

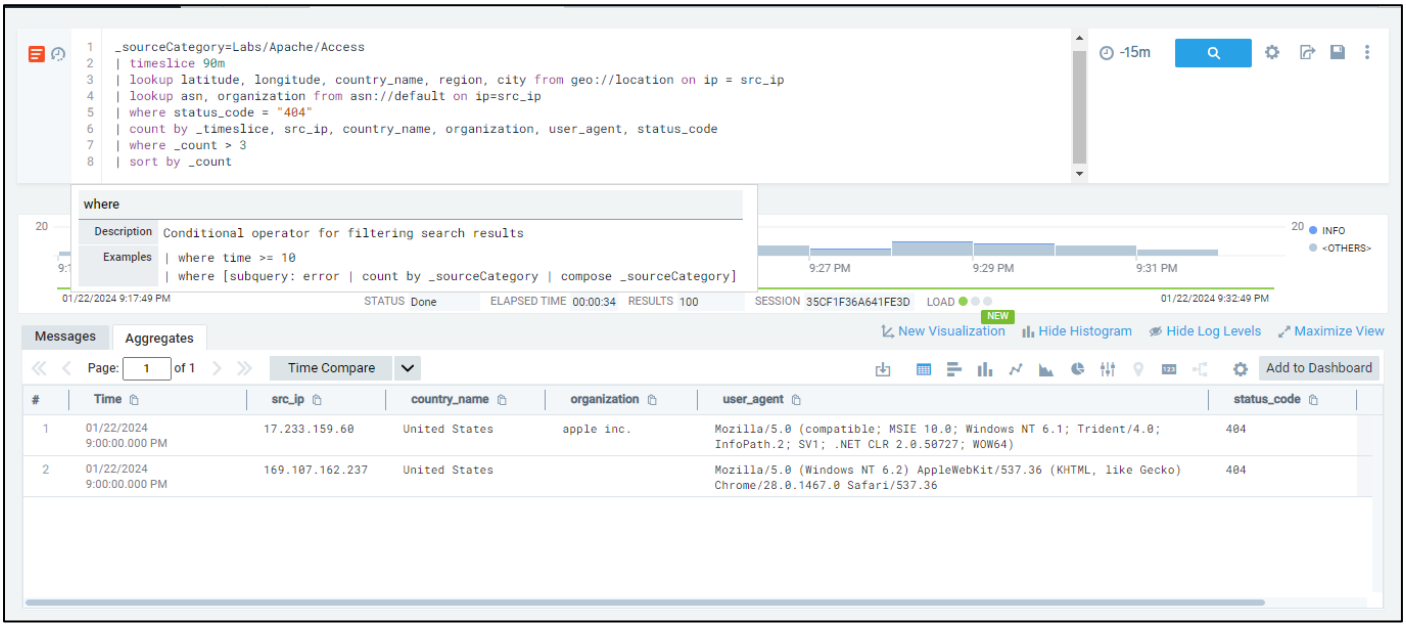
For remediation, the users could be granted specific account permissions, along with a maximum number of attempts before they are locked out. The company policy could also be developed in a way that passwords must be changed every 3-6 months as best practices. Accounts that do not require online connectivity 24/7 could be given local access, thereby avoiding their contact over the internet for sustained periods.

Brute Force Discovery

(screenshots)



The time slice was changed after this step, because there were no results populated in the 60m interval, and the count was reduced to 3.



Crawling Detection

The crawling detection can be investigated by analyzing all the server logs and check for any kinds of patterns of frequencies in the time of expected attack. Since crawling detection would majorly by done by bots, the respective frequencies of requests would be on the higher end. The volume of these requests could be checked and initiated logs can be analyzed in details. The criticality that I would assign to this type of alert would be a **medium** criticality for the simple reason that, crawlers can collect a lot of web server data, but if there are no changes being made, it could be lesser critical than malicious code being transmitted into the web script. The dashboards that could be useful in this case would be web server logs, and maybe bot detection dashboards. Previous data can be collected to understand bot-like activity and these dashboards can be configured to help with the analyzing of the logs.

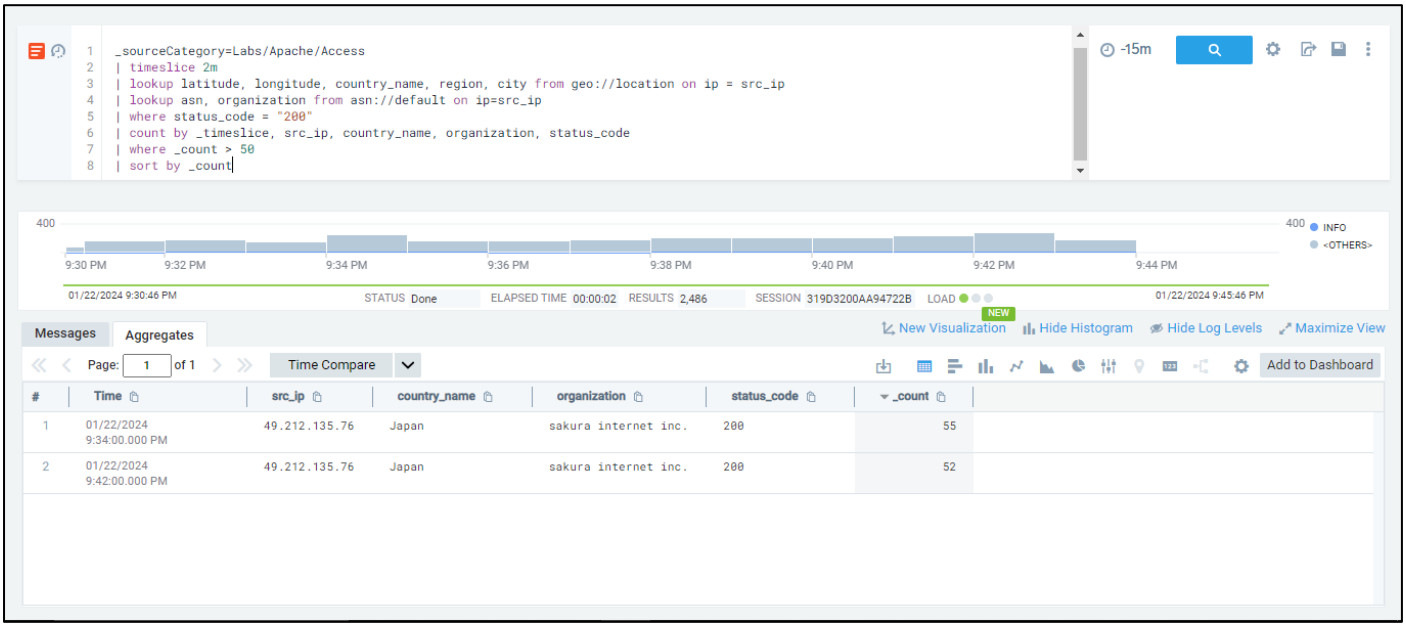
The business impact would be loss of website performance, therefore customer dissatisfaction and unavailability of the web services to an individual. This could result in financial losses for the business if there is personal information exposed. If there are malicious scripts to run on the web server, the business could be ranked amongst the Unreliable Entity list. Short-term risks with crawling detection could unavailability to users of the web application and performance of the server. Long-term risks would be associated with loss of sensitive information, social engineering attacks through the website information, cross-site scripting and loss of trust in all users.

The approach to remediating this could be updating the web pages every few weeks, by changing the internal links, and IP addresses for the server. Software developers could also focus on using CAPTCHA, but a more higher level of CAPTCHA which requires more human intervention in the environment. This would not let bots connect all links at once. Another remedy would be using honeypots for suspected malicious addresses and blocking those with a high amount of requests.

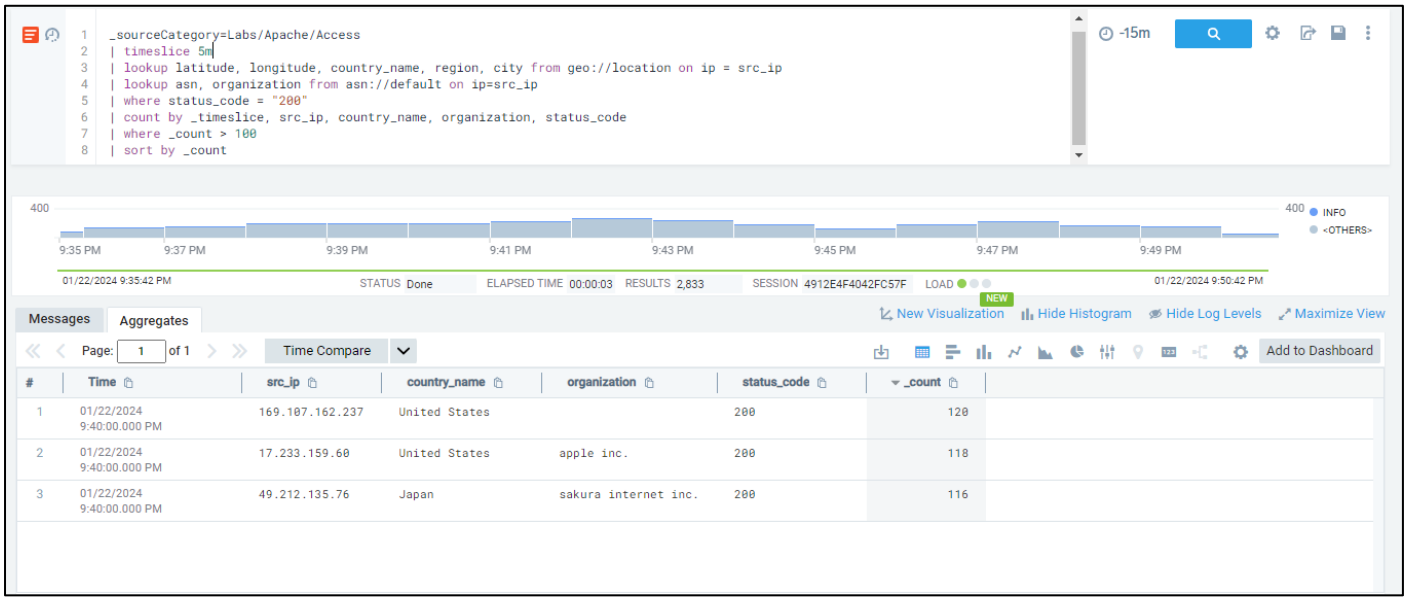
Crawling Detection

(screenshots)

The time slice was increased to detect crawlers from 1m to 2m and a count of greater than 50 requests made to give the status code of 200.



I also tried to see if any results were generated with a time slice of 5m with greater than 100 requests made.



Threat Intelligence

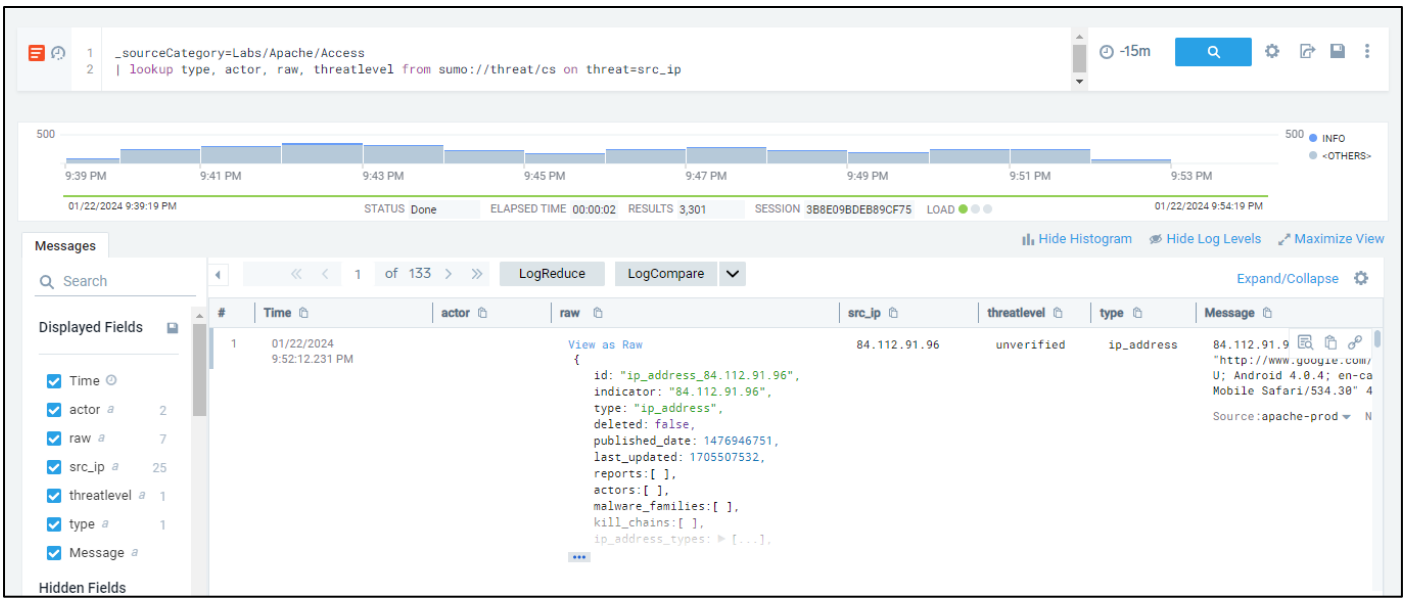
To investigate the alert related to threat intelligence, the SOC analyst needs to maintain a stepwise process. First, the analyst needs to compare the internally collected logs, and then comparing them with different threat feed sources to draw conclusions about the current threat intelligence report generated. Following this, the analyst needs to make sure to use different tools and OSINT pages to understand the anomalies of the compromised part. If the threat intelligence is focusing on the information or infrastructure of the organization, we would assign a **high** criticality, but if the threat intelligence would not be on a big target, it could be a **medium** criticality. The most important dashboard to use in this alert would be the threat feeds collected from different sources and maintaining the dashboard with different behavioral analysis of user trends. A geographical dashboard could be good too, to narrow down the specific locations where higher alerts have been generated.

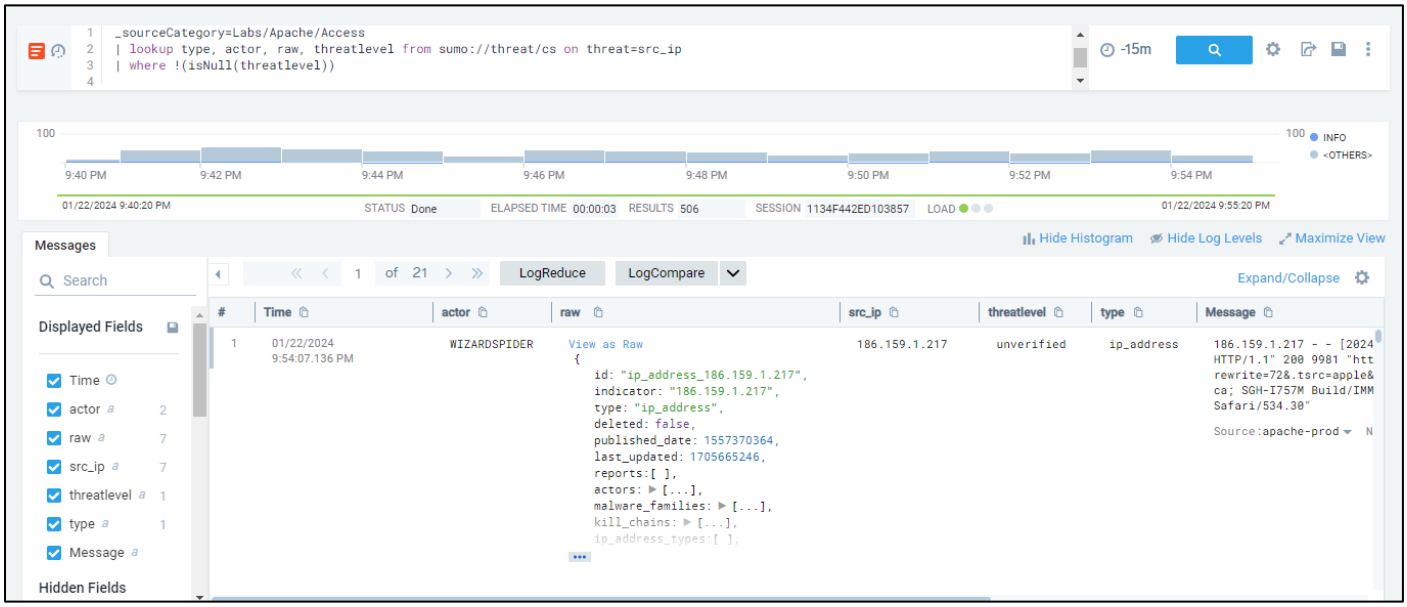
Business impacts for this could mean two things - the right ways of conducting the threat intelligence would be way better for the business to pre-assess the potential threats that can affect it in the long run. The other part could mean that there could be false positives, which would result in disruptions which are not required. A short-term risk in this case would be a very high-cost attack that occurs due to improper mitigation and long-term risks could mean very secretive threats over the course of a long time.

The best way to remediate the incident would be to make sure that based on the constant update of threat feeds being collected, the security policies, and security controls can be updated in regular intervals. Better and newer incident response techniques can be set up in the future occurrences of the like-wise events.

Threat Intelligence

(screenshots)





References:

1. https://cybersecurity.att.com/solutions/security-operations-center/building-a-soc/soc-processes#:~:text=As%20a%20SOC%20analyst%2C%20it's,of%20the%20process%20super%20easy.
2. https://www.semrush.com/blog/what-are-crawlability-and-indexability-of-a-website/
3. https://www.pcmag.com/news/facebook-tops-the-list-of-least-trusted-tech-companies
4. https://blog.imunify360.com/why-malware-on-a-server-is-always-a-bad-thing
5. https://www.anura.io/fraud-tidbits/how-to-stop-bots-from-crawling-my-website