Defensive Security Project
by: [THE EMUS]
[MARTINA, VALERIE, TREVOR, ANDRE]

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

Today, we'll step into the shoes of a Security Operations Center (SOC) analyst at Virtual Space Industries (VSI), a company specializing in virtual reality program design for businesses.

VSI has caught wind of rumors suggesting that their competitor, JobeCorp, might initiate cyber attacks aimed at disrupting VSI's operations.

In our role as SOC analysts, we've been assigned the crucial task of leveraging Splunk to vigilantly monitor for potential attacks targeting VSI's systems and applications.

The VSI products under our watchful eye include:

An administrative webpage: https://vsi-corporation.azurewebsites.net/

An Apache web server, responsible for hosting the aforementioned webpage

A Windows operating system, integral to running various back-end operations for VSI

MaxMind GeoIP database

[MaxMind GeoIP database]

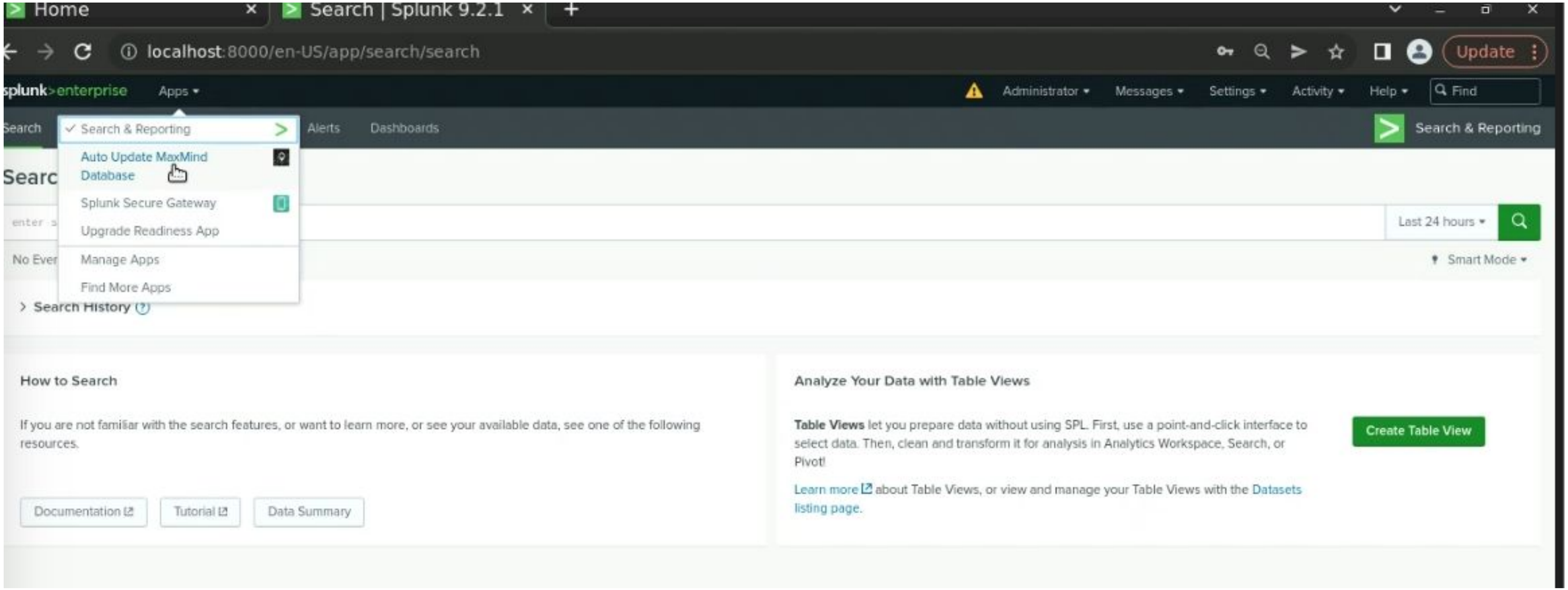
The App we choose was Auto Update MaxMind Database. The objective of this app is to Auto Update the logs in the system. This app is also used for IP location.

[MaxMind GeoIP database]

Imagine you're managing a Splunk environment that heavily relies on geolocation data for various analytics and security purposes. As part of your routine operations, you need to ensure that the MaxMind GeoIP database, which Splunk uses for geolocation data, is always up-to-date. However, manually updating this database can be time-consuming and prone to errors. In such a scenario, the Auto Update MaxMind Database add-on for Splunk becomes invaluable, as it automates the process of fetching and updating the MaxMind GeoIP database, ensuring that your Splunk environment continuously has access to the most recent geolocation data without manual intervention.

[Add-On App Name]

[Images for add-on app]



Logs Analyzed

1 Windows Logs

[Describe the data these logs contain]

The Windows Logs contained the intellectual property of VSI's next-generation virtual-reality programs.

2 Apache Logs

[Describe the data these logs contain]

The Apache Logs contained the Logs for VSI's main public- facing website, vsi-company.com

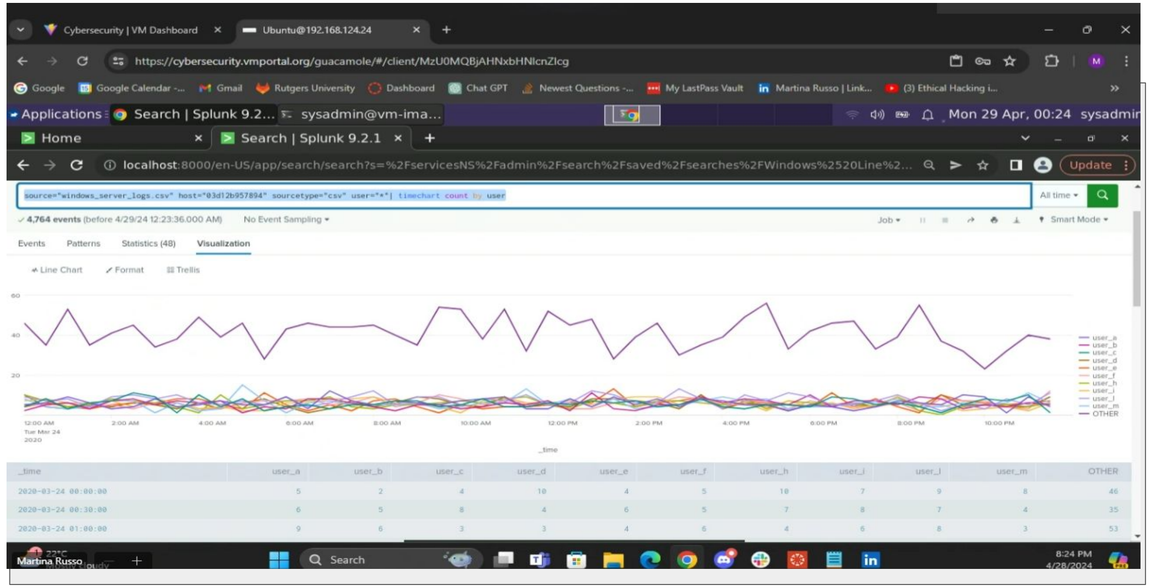
Windows Logs

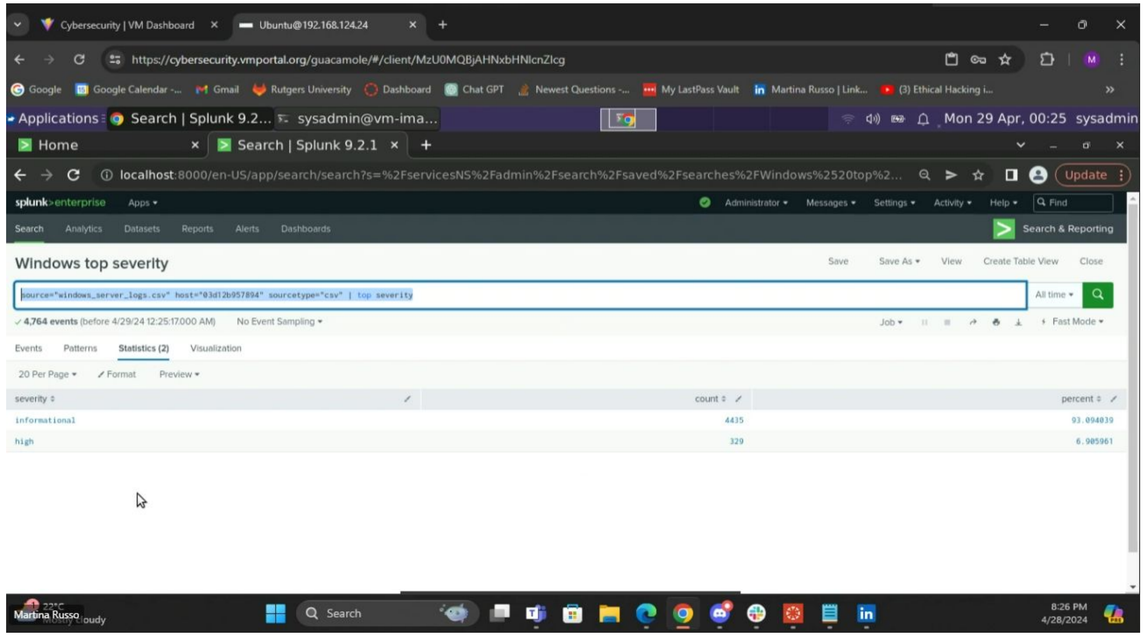
Reports—Windows

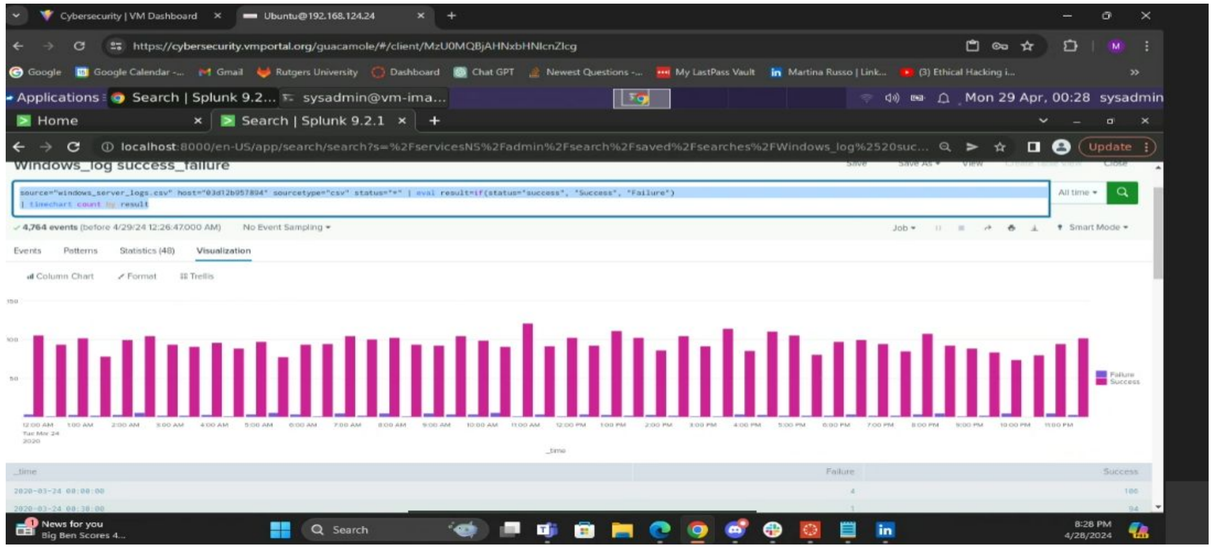
Designed the following reports:

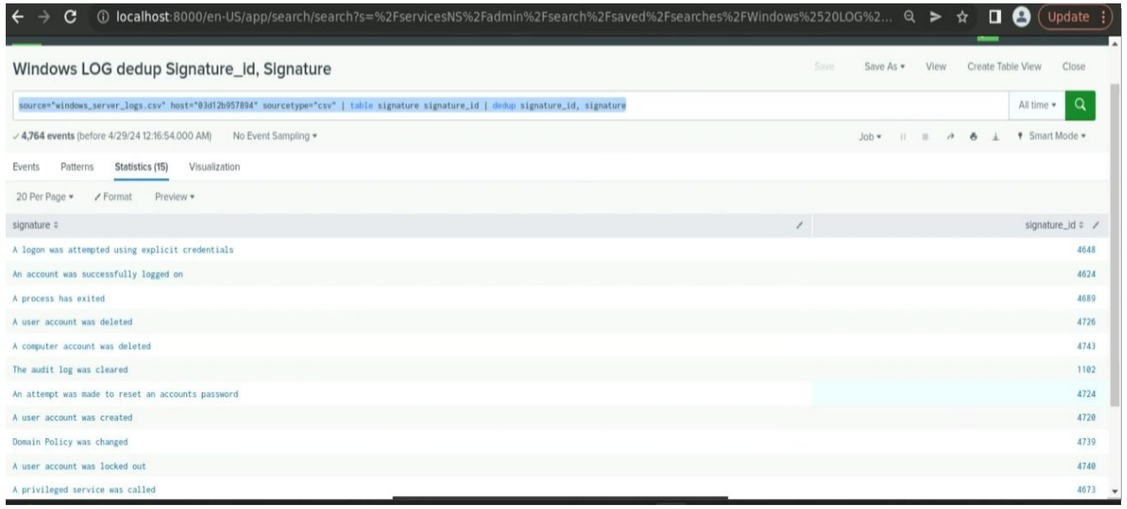
Report Name	Report Description
Windows Line chart User	Displays the user, visual logs , and field values over time
Windows top severity	Displays the most common severity levels observed in the dataset, allowing for quick insight into the distribution and frequency of severity levels in the logs
Windows Log success and failures	Displays and helps in understanding the distribution regarding trends of success and failure statuses within your log events
Windows Log Dedup Signature id, and Signature	Displays and retrieves unique combinations of signature and signature_id while eliminating duplicate
	events with specified field criteria.

Images of Reports—Windows









Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Successful Logins	This Windows alert is to notify how many Successful logins were made by each user	1 hour	25

JUSTIFICATION:
We selected this specific alert configuration to focus on monitoring successful logins for each user due to its critical nature in detecting potential security issues or unusual activity. By setting a threshold at 25 and receiving hourly alerts, we aim to promptly detect and respond to any significant deviations from expected login patterns, enhancing overall system security and proactive incident response.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Alert count by Signature	This Windows alert is to visualize the frequency of different signature values	1 hour	30

JUSTIFICATION: We selected this alert to monitor Windows log events categorized by different signature values over time. The alert triggers hourly if any signature activity occurs.

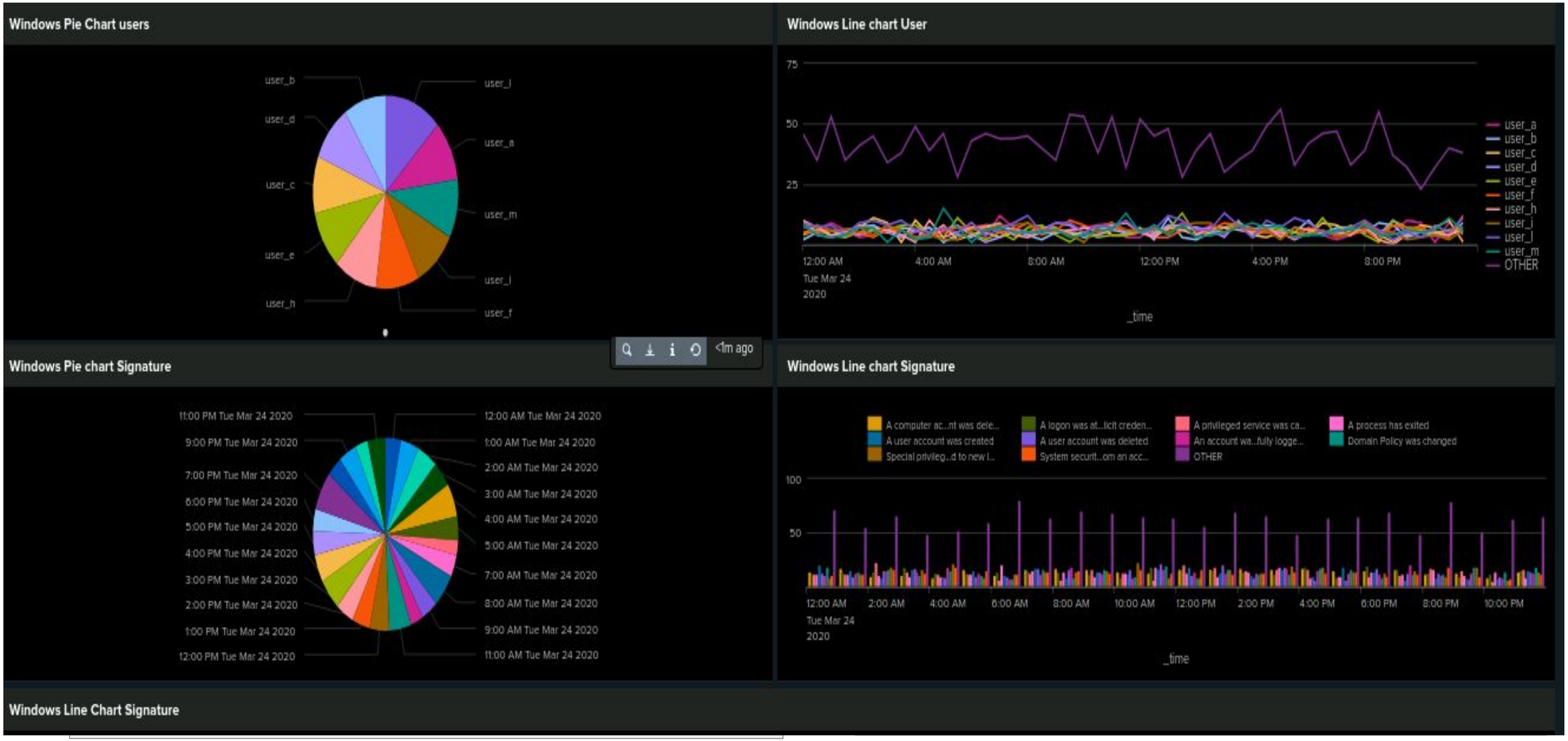
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Alert Failure Activity	This Windows alert is configured to monitor failure activity in log events	1 hour	10

JUSTIFICATION: We selected this specific alert configuration to monitor failure activity in order to proactively detect and respond to significant levels of failure events within our log data. This will enable us to respond promptly to potential issues and uphold system integrity and security.

Dashboards—Windows



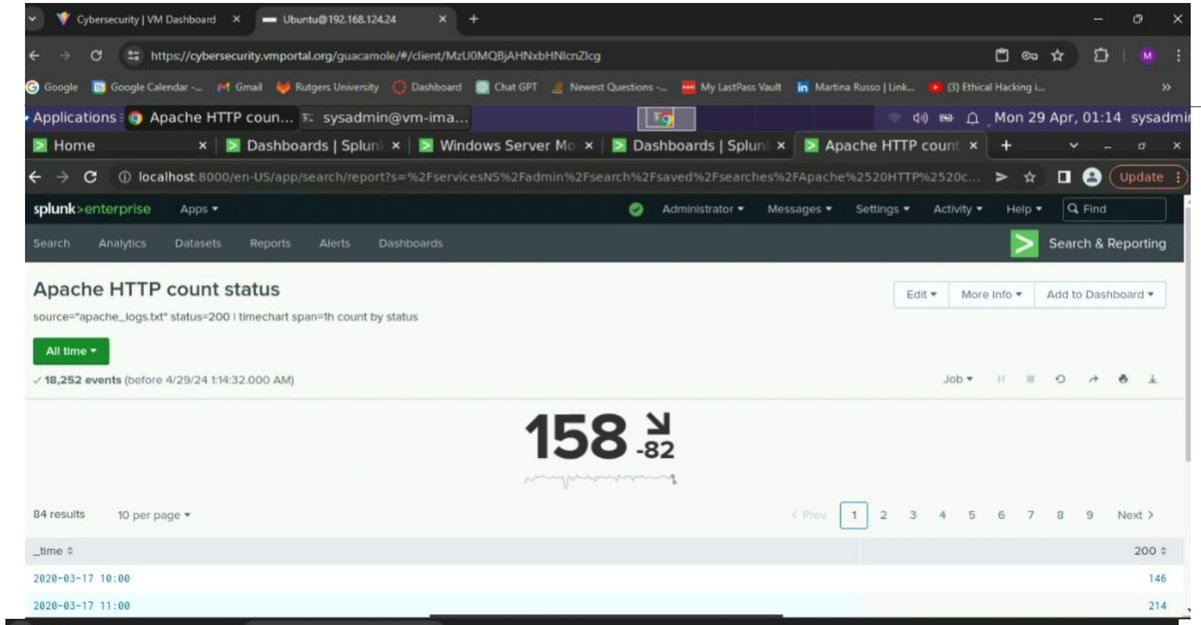
Dashboards—Windows

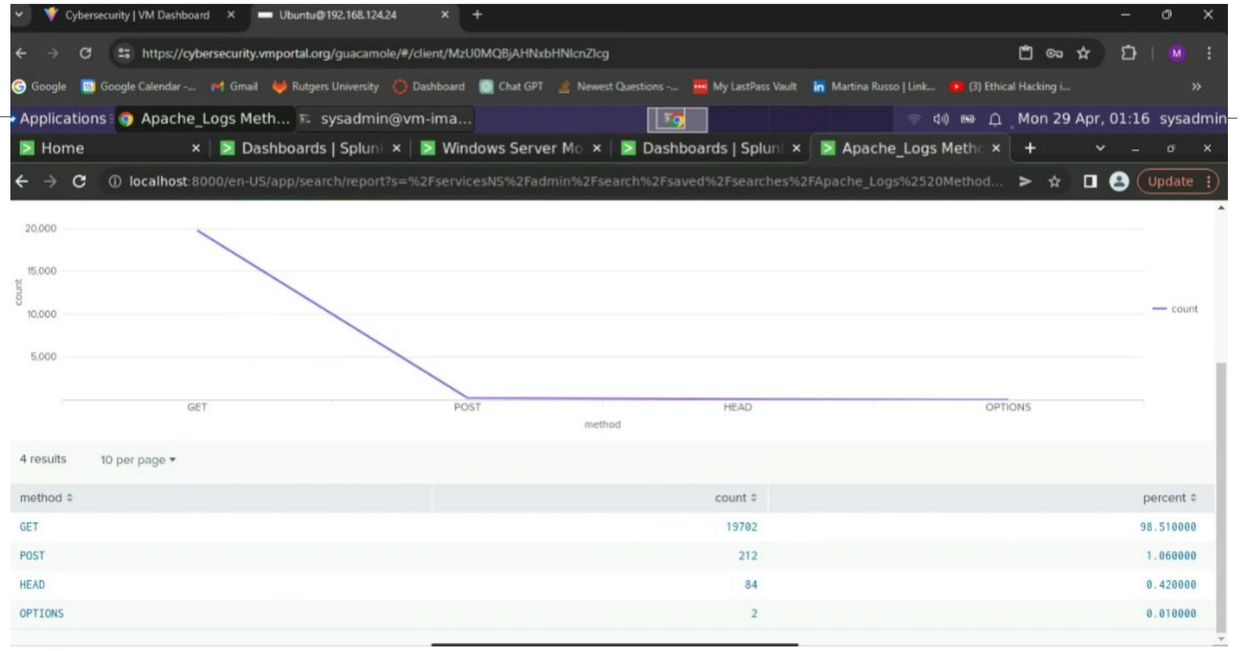
Apache Logs

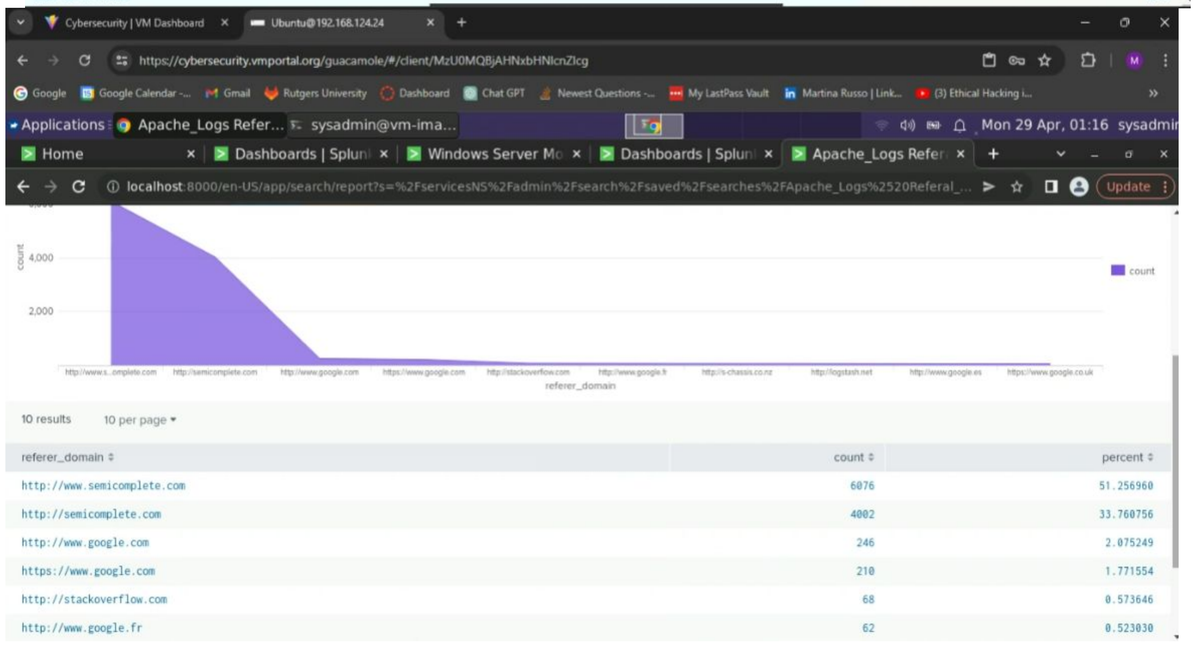
Reports—Apache

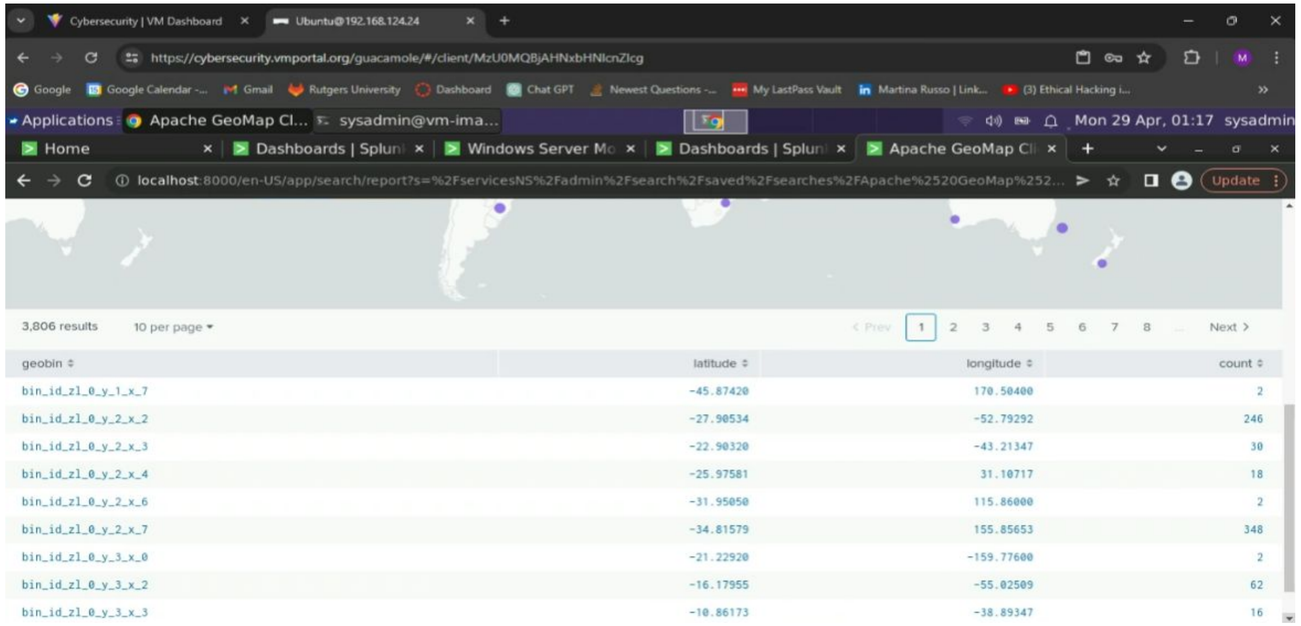
Report Name	Report Description
Apache HTTP Count Status	This report can help in monitoring the performance and availability of the Apache web server, understanding traffic patterns, and identifying any unusual spikes or trends in successful requests over time.
Apache_Logs Methods count	This report can be useful for understanding how clients interact with the Apache server, which methods are most frequently utilized, and detecting any unusual or unexpected usage patterns.
Apache_Logs Referral_Domain	This report can provide insight into the sources of incoming traffic to the Apache server and help identify popular referring domains.
Apache GeoMap Client	This report provides statistical information on log events categorized by geographical locations based on client IP addresses. It visualizes this data on a map or in a tabular format, highlighting the geographic origins of requests.

Images of Reports—Apache









Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache alert GeoMap	This Apache alert setup enables proactive monitoring of international access to the Apache server, helping to enhance security posture and response capabilities by promptly identifying and investigating non-US access activities.	1 hour	0

JUSTIFICATION: We selected this specific alert to monitor hourly activity originating from any country besides the United States in the Apache access logs. The alert triggers every hour at the beginning of the hour if there is any non-US activity detected.

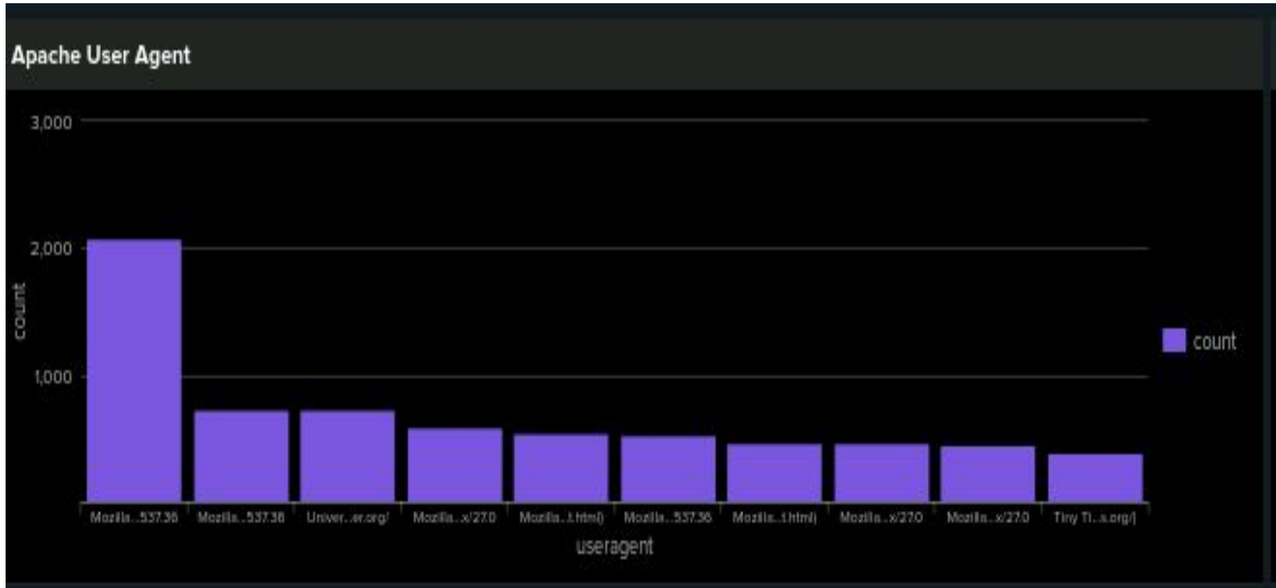
Alerts—Apache

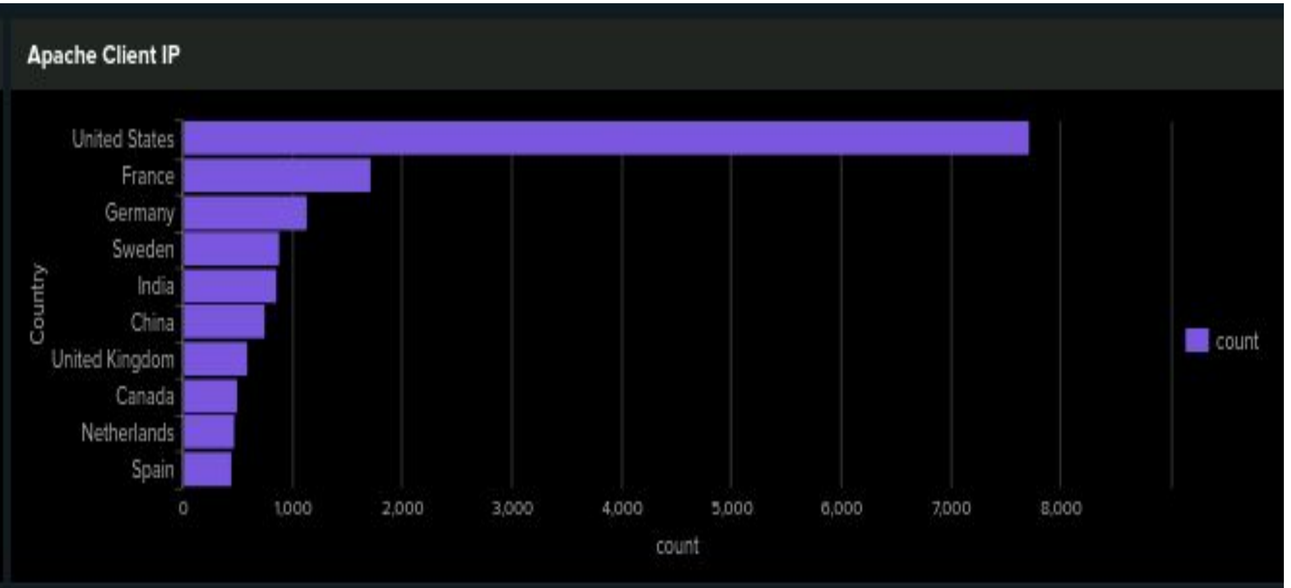
Designed the following alerts:

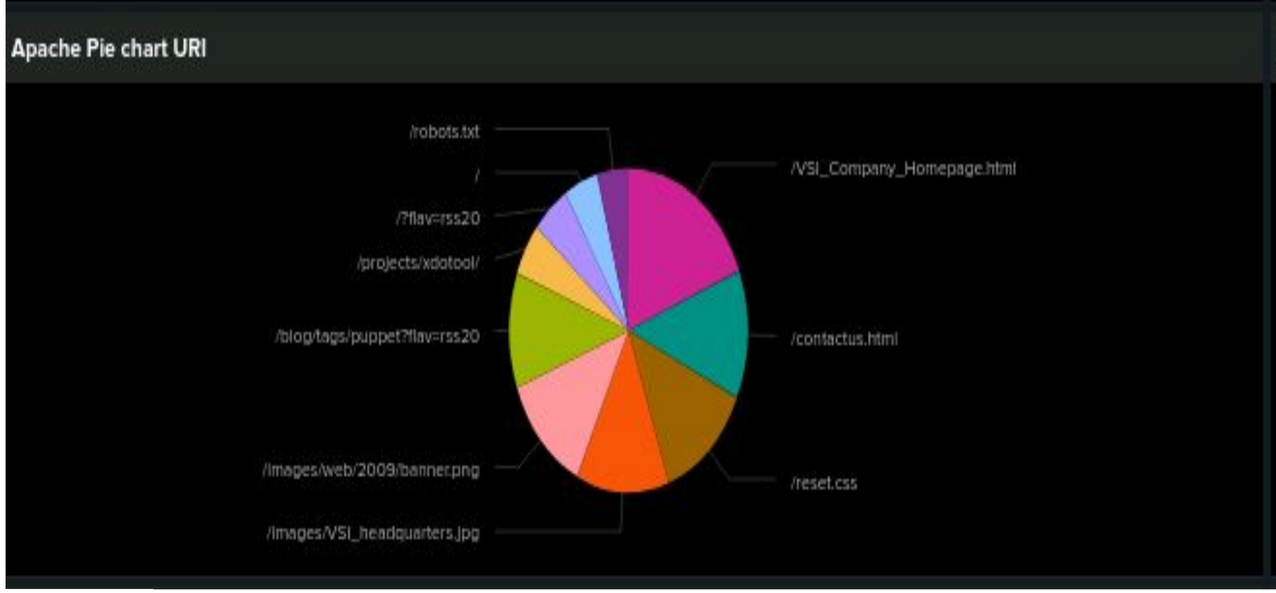
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Alert HTTP	This Apache alert setup allows for proactive monitoring of HTTP POST method activity in Apache access logs, helping to detect and respond promptly to relevant events.	1 hour	0

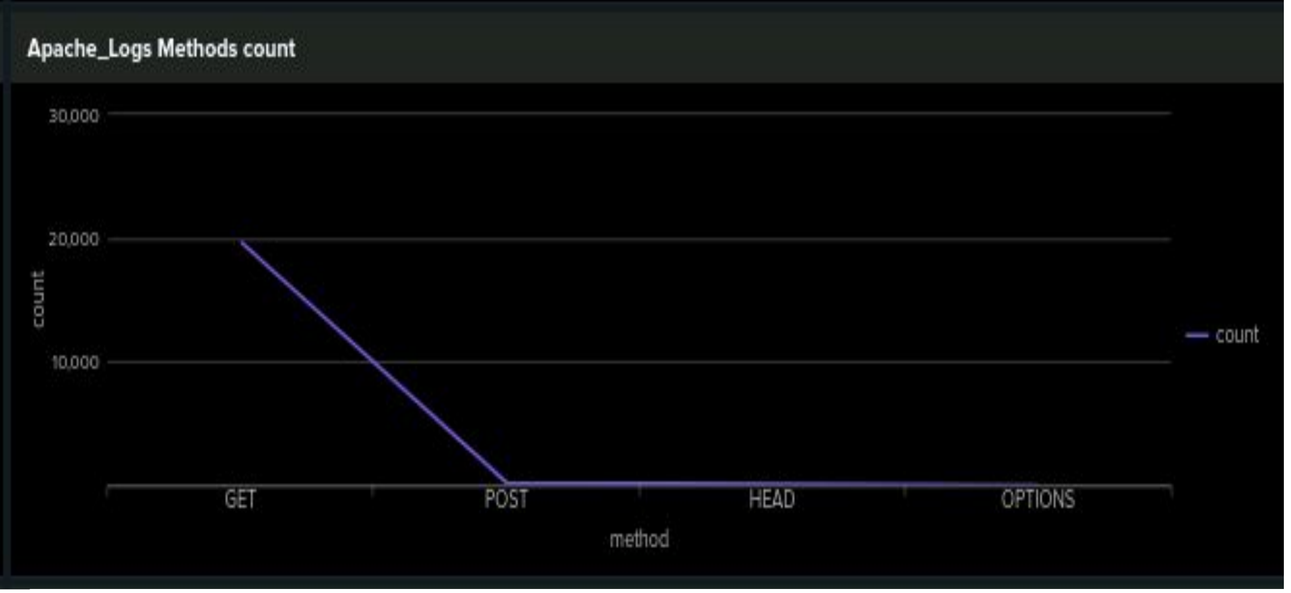
JUSTIFICATION: We selected this specific alert to monitor HTTP POST method activity in the Apache access logs. The alert triggers every hour at the beginning of the hour if any HTTP POST requests are detected.

Dashboards—Apache









Dashboards—Apache

Attack Analysis

Attack Summary—Windows

Summarize your findings from your reports when analyzing the attack logs.

Based on the analysis of the Windows attack logs and the event counts exceeding normal thresholds, there are indications of potential security threats originating from specific IP addresses. The activities observed, including repeated account password resets (Event ID 4724), user account creations (Event ID 4720), successful logins (Event ID 4624), and account deletions (Event ID 4726), suggest a pattern of suspicious behavior that warrants further investigation.

The notable increase in event counts, particularly during specific hours, may indicate abnormal levels of activity that could be indicative of orchestrated attacks, such as distributed denial-of-service (DDoS) attacks. DDoS attacks involve overwhelming a target system with a large volume of traffic or requests, potentially causing slowdowns or unresponsiveness.

Attack Summary—Windows

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

The event analysis conducted on March 25, 2020, revealed significant deviations from the typical event range of 0 to 200 events per hour. At 1:00 AM, 2:00 AM, 9:00 AM and 10:00 AM event counts exceeded 900 per hour. This far surpasses the normal threshold allowed. The peak occurred at 9:00 AM, with 1293 events, indicating a substantial spike in activity. By 10:00 AM, although reduced, event counts remained elevated at 784 events. These findings suggest abnormal patterns or increased activity levels during specific hours.

- Windows Successfully Log On Alert:

  Description: Triggered by successful logon events

  Conditions: Triggered hourly if logon events exceed 25
- Windows Deleted Account Alert:

  Description: Monitors account deletion events

  Conditions: Triggers hourly if account deletions exceed 15
- Windows Alert Failure Activity:

  Description: Monitors failure activity in log events

  Conditions: Triggers hourly if failure events exceed 10

Attack Summary—Windows

Summarize your findings from your dashboards when analyzing the attack logs.

The dashboard charts indicate that a third party has executed a high volume of activities related to changing passwords, deleting user accounts, and performing privilege escalation using special system privileges. These activities include events such as account password resets (Event ID 4724), user account deletions (Event ID 4726), and granting special privileges to new logons (Event ID 4672).

These patterns of behavior suggest potential security threats involving unauthorized access and manipulation of system resources. The actions performed, especially in large volumes, could indicate malicious intent aimed at compromising the system's integrity or gaining unauthorized privileges.

Screenshots of Attack Logs

[Optional: Place images that illustrate attack findings here.]

Summarize your findings from your reports when analyzing the attack logs.

Attack Summary—Apache

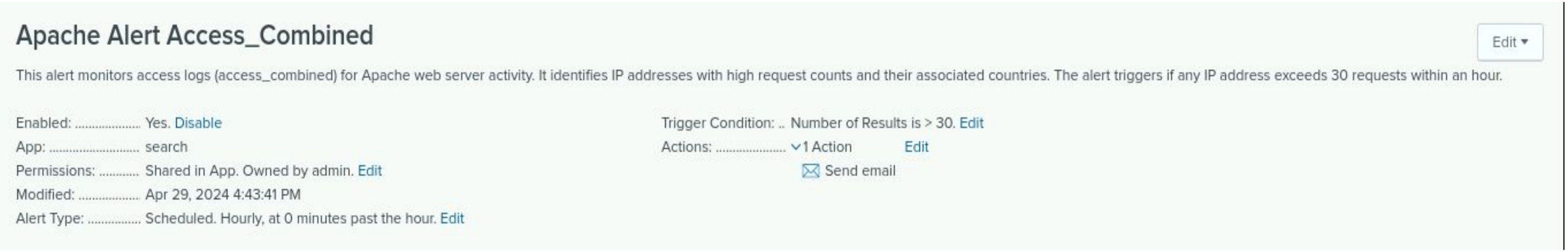
The analysis of the log data indicates that the IP address 208.91.156.11 was observed repeatedly attempting to access the resource "/files/logstash/logstash-1.3.2-monolithic.jar" using GET requests. However, the server consistently responded with HTTP 404 (Not Found) status codes, suggesting that the resource was not available.

On the other hand, the IP address 194.105.145.147 engaged in a series of POST requests targeting "/VSI_Account_logon.php", which consistently returned HTTP 200 (OK) status codes. This behavior indicates that the IP address was successfully accessing the specified endpoint.

In summary, the analysis reveals distinct patterns of behavior from these IP addresses, with one IP encountering resource-not-found errors while the other was successfully accessing the targeted endpoint.

Attack Summary—Apache

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

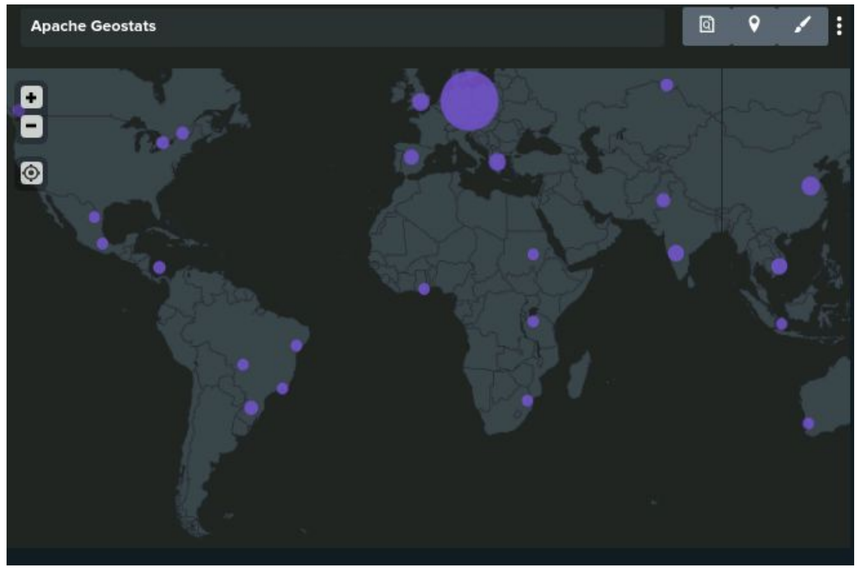


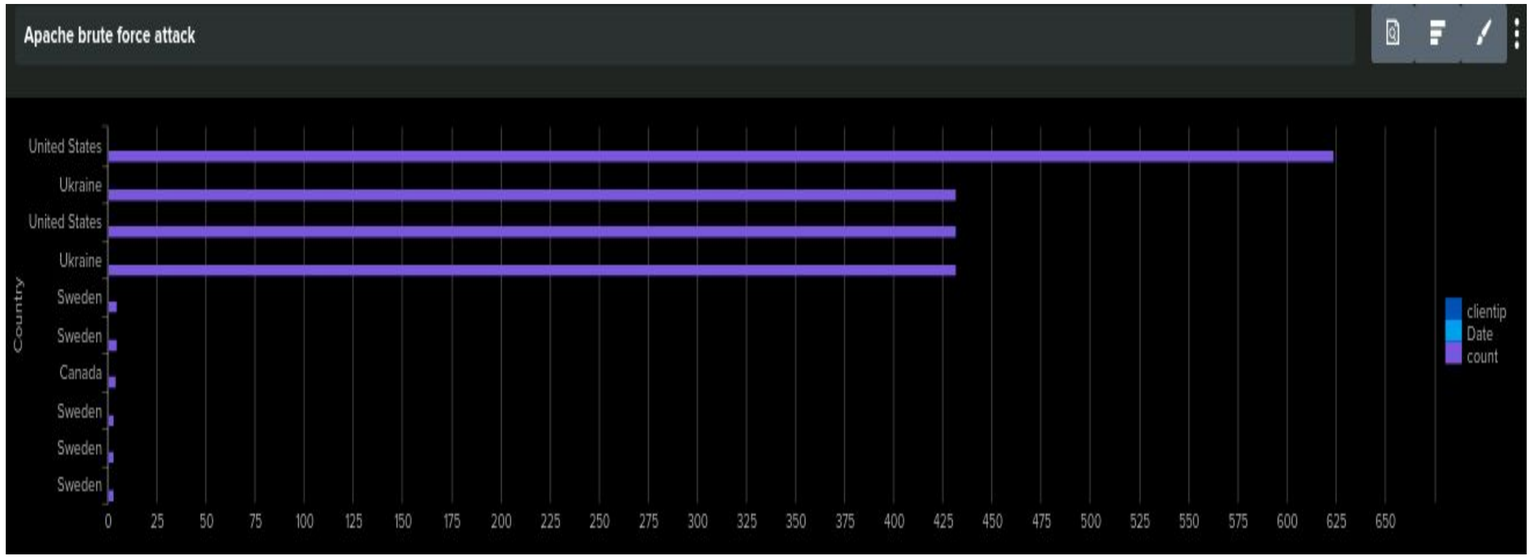
This alert monitors access logs (access_combined) for Apache web server activity.
It identifies IP addresses with high request counts and their associated countries.
The alert triggers if any IP address exceeds 30 requests within an hour.

Attack Summary—Apache

Summarize your findings from your dashboards when analyzing the attack logs.

The analysis of the attack logs reveals that Ukraine and the USA are the countries with the highest number of attempted accesses. This data suggests that these countries are prominent sources of traffic and potentially pose higher security risks due to the volume of access attempts recorded in the logs.





Screenshots of Attack Logs

[Optional: Place images that illustrate attack findings here.]

208.91.156.11	United States	2020-03-25 18:05:55	624
194.105.145.147	Ukraine	2020-03-25 20:05:59	432
194.146.132.138	United States	2020-03-25 20:05:59	432
79.171.127.34	Ukraine	2020-03-25 20:05:59	432

clientip	Date	count	City	Country	Region	lat	lon
208.91.156.11	2020-03-25 18:05:55	624	Ashburn	United States	Virginia	39.04380	-77.48740

clientip	Date	count	City	Country	Region	lat	lon
194.105.145.147	2020-03-25 20:05:59	432	Kyiv (Solom'yans'kyi district)	Ukraine	Kyiv City	50.42240	30.50600
194.146.132.138	2020-03-25 20:05:59	432	New York	United States	New York	40.71280	-74.00600
79.171.127.34	2020-03-25 20:05:59	432	Kharkiv (Shevchenkivs'kyi District)	Ukraine	Kharkiv	50.03680	36.22020

5.10.83.53 - - [25/Mar/2020:21:05:59 +0000] "GET /files/grok/?C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"

host = Apache attacklog | source = apache_attack_logs.txt | sourcetype = access_combined

194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)"

host = Apache attacklog | source = apache_attack_logs.txt | sourcetype = access_combined

Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?

Windows findings

The examination of Windows attack logs on March 25, 2020 uncovered various security events suggesting potential malicious activities. Noteworthy findings include multiple account management events such as user account deletions (Event ID 4726) and password reset attempts (Event ID 4724), which could indicate unauthorized access or compromise of user accounts. Additionally, instances of special privileges being assigned to new logons (Event ID 4672) were detected, which may indicate attempts to escalate privileges within the system. Records of system security access granted to accounts (Event ID 4717) also raised concerns regarding potential unauthorized access or privilege misuse.

Apache findings

The review of Apache attack logs on March 25, 2020 revealed suspicious activities targeting specific resources. Notably, repeated requests from specific IP addresses were observed, targeting non-existent resources and resulting in HTTP 404 responses, indicating potential scanning or probing activities.

Automated behavior was also identified through consistent usage of user-agent strings like "Chef Client/10.18.2",POST /VSI_Account_logon.php HTTP/1.1, across multiple requests.

- To protect VSI from future attacks, what future mitigations would you recommend?

Windows: Implement Strong Access Controls by using the principle of least privilege to grant users only the necessary permissions for their tasks.

Regularly update access control lists (ACLs) to limit unauthorized access to sensitive resources.

Configure auditing policies to monitor critical security events like account creations, deletions, and privilege escalations.

Use security information and event management (SIEM) tools to collect logs centrally and monitor security events in real-time.

Regularly Review and Rotate Credentials

Enforce regular password changes for user and service accounts. Implement multi-factor authentication (MFA) to enhance security.

Conduct Security Awareness Training, Patch and Update Systems Regularly

Configure intrusion detection and prevention systems (IDPS) to identify and mitigate threats in real-time.

Implement account lockout policies to prevent brute-force attacks by locking accounts after multiple failed login attempts.

Monitor and investigate repeated failed login attempts for signs of attacks.

Regular Security Audits and Penetration Testing.

Apache: Set up real-time monitoring of Apache access logs to detect suspicious patterns or anomalies.

Utilize IP reputation services to identify known malicious IPs and block them at the firewall or web server level.

Implement geo-blocking rules to restrict access from specific countries or regions that are associated with high-risk activity.

Deploy a WAF (Web Application Firewall) to inspect incoming HTTP requests and filter out malicious traffic before it reaches the web server.

Configure the WAF to detect and block common web-based attacks like SQL injection, XSS (Cross-Site Scripting), and directory traversal.

Conduct regular reviews of Apache access logs to identify patterns of attacks or unusual traffic.

Look for trends in user-agent strings, URLs, or IP addresses that indicate potential threats.

Develop and maintain an incident response plan specific to Apache web server attacks.