



# **Defensive Security Project** **by: Bootcon9 GP.** **Prepared By S.Asghar**

AI & Web Resources Used Sparingly

# Table of Contents

---

This document contains the following resources:

01

**Monitoring  
Environment**

02

**Attack Analysis**

03

**Project Summary  
& Future  
Mitigations**

The background of the slide is a complex, abstract geometric pattern. It consists of numerous triangles of varying sizes, some in a dark red or maroon color and others in black. These triangles are arranged in a way that creates a sense of depth and movement, resembling a low-poly or isometric design. The overall effect is a textured, three-dimensional appearance.

# Monitoring Environment

# Scenario

---

- Virtual Space Industries (VSI), a company specializing in developing virtual reality programs for businesses, is currently facing concerns about potential cyberattacks from its competitor, JobeCorp, which may target VSI's infrastructure. To safeguard its operations, VSI has tasked an SOC (Security Operations Center) analyst with monitoring its critical systems and applications. The key systems under surveillance include an Apache web server that hosts the administrative webpage and a Windows operating system that handles various back-end operations, including the storage of intellectual property for VSI's next-generation virtual-reality programs.
- The analyst has been provided with logs from both systems—Windows Server Logs and Apache Server Logs—dating back to previous periods. These logs are essential for establishing baseline behavior patterns, which will be used to identify any deviations that may indicate a security incident. Using Splunk, the SOC analyst's primary responsibility is to develop and configure reports, alerts, and dashboards that can detect and notify of any suspicious activity in real time. This will allow the team to promptly respond to any signs of cyberattacks or attempts to disrupt VSI's business operations, ensuring the integrity of both their public-facing website and internal infrastructure.

# ["Add-On" App]

**[Splunk TA Add-on for Apache Web Server]**

**[Splunk TA Add-on for Windows Server]**

# [Splunk Add-on for Apache Web Server]

---

## Here is a summary of the Splunk Apache\_TA app:

- ❖ Purpose: The Apache\_TA app (Splunk Technology Add-on for Apache) is designed to collect and parse Apache HTTP server logs, making it easier to analyze web traffic, identify patterns, and detect potential security incidents.
- ❖ Data Parsing: It supports log formats like access\_combined and error\_log, extracting useful fields such as HTTP methods, response codes, client IPs, user agents, URLs, and referrers.
- ❖ Geolocation: The app includes built-in capabilities like iplocation, which geolocates client IPs, allowing users to visualize traffic patterns geographically, such as through cluster maps.
- ❖ Dashboards: Pre-built dashboards in the app offer visualizations like traffic over time, top methods (GET, POST, etc.), response codes, IP addresses, and referrer statistics, all crucial for web traffic analysis.
- ❖ Use Cases: It's useful for performance monitoring, identifying abnormal traffic spikes, detecting potential security threats (like DDoS attacks or malicious access), and auditing server behavior.

# [Splunk Add-on for Apache Web Server]

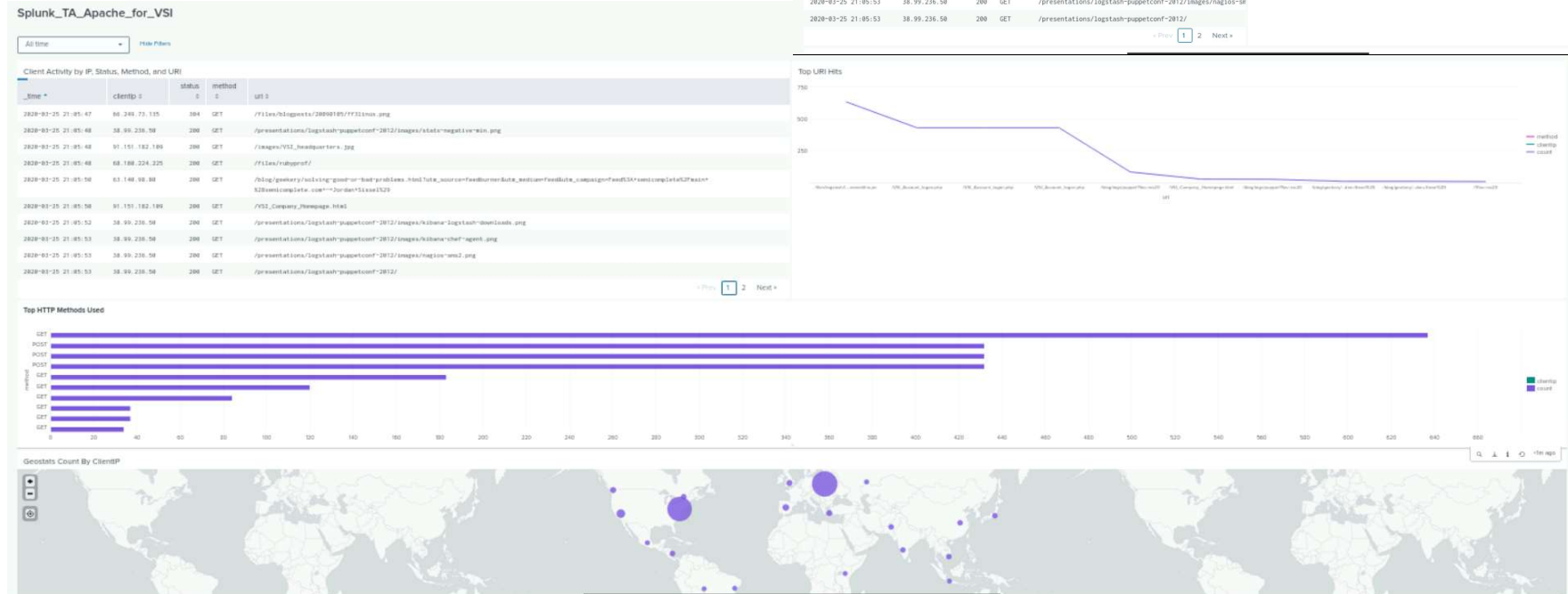
---

## Scenario: Detecting and Mitigating Suspicious Activity on VSI's Web Servers Using the Splunk Apache\_TA App

- ❖ **GeolReal-Time Traffic Monitoring for VSI and Clients:** The Splunk Apache\_TA app tracks web traffic for VSI and its clients, highlighting spikes or unusual patterns, such as high volumes of POST requests to sensitive pages, helping detect potential attacks early.
- ❖ **Geolocation Insights for Global Traffic:** The app provides VSI with geolocation visualizations, identifying suspicious activity originating from unexpected regions like Ukraine or Sweden, and enabling VSI to proactively block traffic from these locations for its clients.
- ❖ **IP and Method Analysis to Identify Malicious Behavior:** By analyzing the methods (GET, POST) and tracking high-frequency IP addresses, the app helps VSI spot unauthorized access attempts or brute-force attacks targeting its infrastructure and client-facing services.
- ❖ **Response Code Tracking for Failed Attempts:** VSI can monitor error response codes (e.g., 403, 404) generated by attacks or unauthorized access attempts, which helps in quickly detecting and mitigating failed attack efforts that may impact its clients.
- ❖ **Proactive Mitigation to Protect VSI and Clients:** Leveraging insights from the dashboard, VSI can take actions such as blocking malicious IPs, rate-limiting requests, and adjusting server configurations to protect both its own infrastructure and the services it provides to clients.

## [Splunk Add-on for Apache Web Server]

## Dashboard VSI's Apache Logs





# Logs Analyzed

---

1

## Windows Logs

Likewise Windows Logs Can Be dashboarded and analyzed as Apache's, that item is not Being Included for brevity and since the procedure is very similar. This aspect was also Discussed with the instructor.

2

## Apache Logs

The Apache logs from VSI and its clients contain crucial data for web traffic and security analysis:

- 1.Client IP (clientip):** Tracks the source of web requests, useful for geolocation analysis and identifying suspicious traffic.
  - 2.Request Method (method):** Shows HTTP methods used (e.g., GET, POST), helping detect abnormal request patterns.
  - 3.URI:** Displays requested resources, highlighting potential targets like login pages.
  - 4.Response Code (status):** Indicates server responses (e.g., 200, 403), useful for detecting failed attempts or unauthorized access.
  - 5.Timestamp (\_time):** Provides request timing, helpful in identifying traffic spikes or attacks.
  - 6.User-Agent (user\_agent):** Identifies browsers or bots making requests, useful for differentiating between legitimate users and automated threats.
- By analyzing these logs, VSI can detect suspicious activity, track traffic patterns, and protect both its own infrastructure and client systems effectively using Splunk dashboards.

# Windows Logs

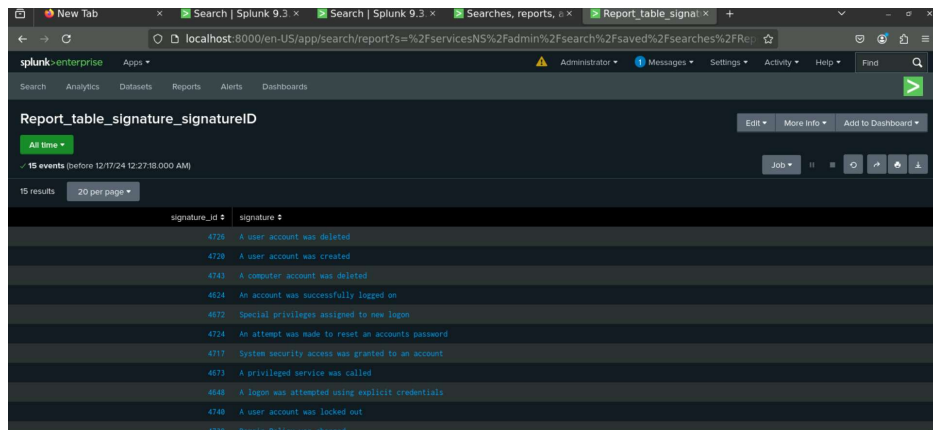
# Reports—Windows

---

Designed the following reports:

Report Name	Report Description
Report_table_signature_signatureID	A report with a table of signatures and associated signature IDs.
Severity_level_count_percent	A report that displays the severity levels, and the count and percentage of each.
Report_Windows_Events_Success_Failure	A report that provides a comparison between the success and failure of Windows activities.

# Images of Reports—Windows

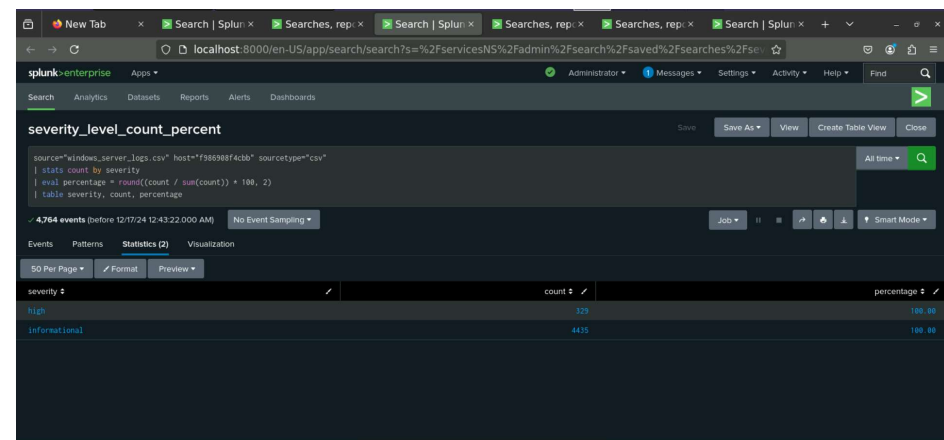


**Report\_table\_signature\_signatureId**

15 events (before 12/17/24 12:27:18.000 AM)

15 results 20 per page

signature_id	signature
4725	A user account was deleted
4720	A user account was created
4741	A computer account was deleted
4824	An account was successfully logged on
4872	Special privileges assigned to new logon
4724	An attempt was made to reset an account's password
4717	System security access was granted to an account
4873	A privileged service was called
4848	A logon was attempted using explicit credentials
4748	A user account was locked out

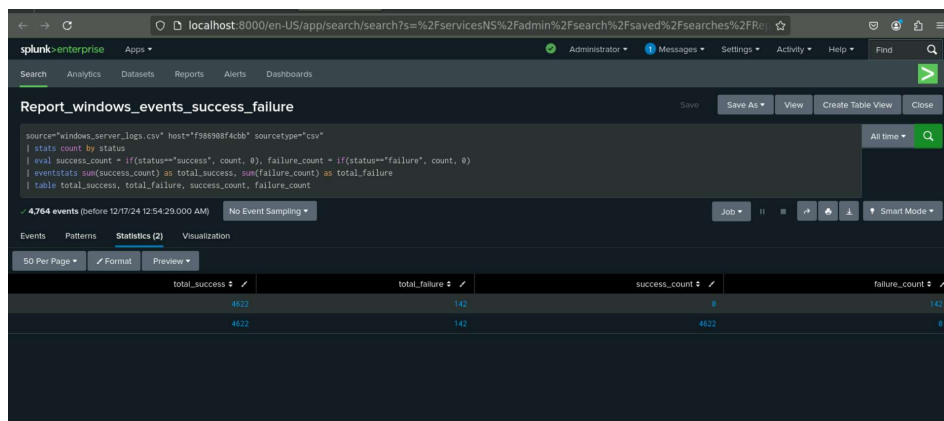


**severity\_level\_count\_percent**

4,764 events (before 12/17/24 12:43:22.000 AM)

50 Per Page Format Preview

severity	count	percentage
high	329	100.00
informational	4435	100.00



**Report\_windows\_events\_success\_failure**

4,764 events (before 12/17/24 12:54:29.000 AM)

50 Per Page Format Preview

total_success	total_failure	success_count	failure_count
4622	142	0	142
4622	142	4622	0

# Alerts—Windows

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Activity Failure Threshold Exceeded	Alert when Hourly Failed Windows Activity Exceeds Threshold (1.5x)	avg_count/hr	(avg_count * 1.5)

**JUSTIFICATION:** This Baseline identifies typical behavior and identifies significant deviations.

# Alerts—Windows

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert:Successful Logins Exceeded Threshold	Alert when Hourly Successful Logins Count Exceeds Threshold (1.25x)	avg_count/hr	(avg_count * 1.25)

**JUSTIFICATION:** This Baseline identifies typical behavior and identifies significant deviations.

# Alerts—Windows

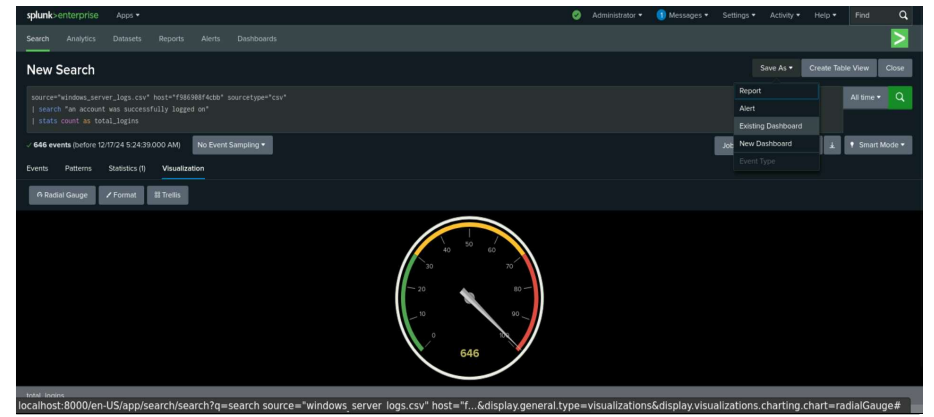
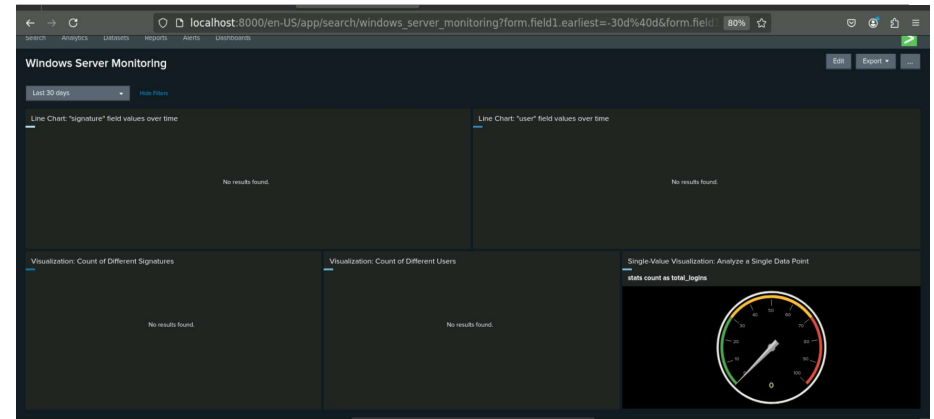
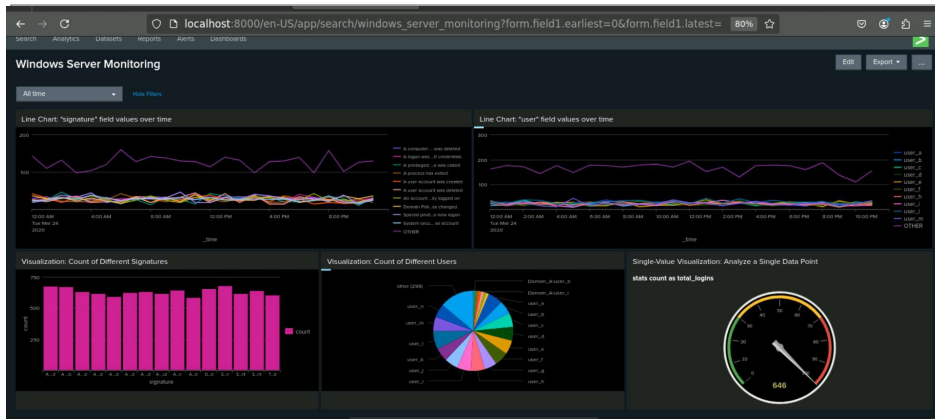
---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deletion Threshold Alert	[Triggered when User Account Deletion Activity Exceeds the Threshold	avg_count/hr	(avg_count * 1.25)

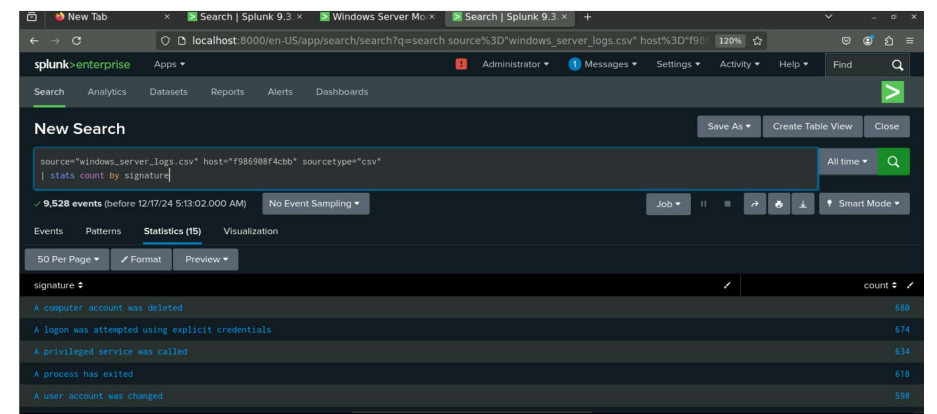
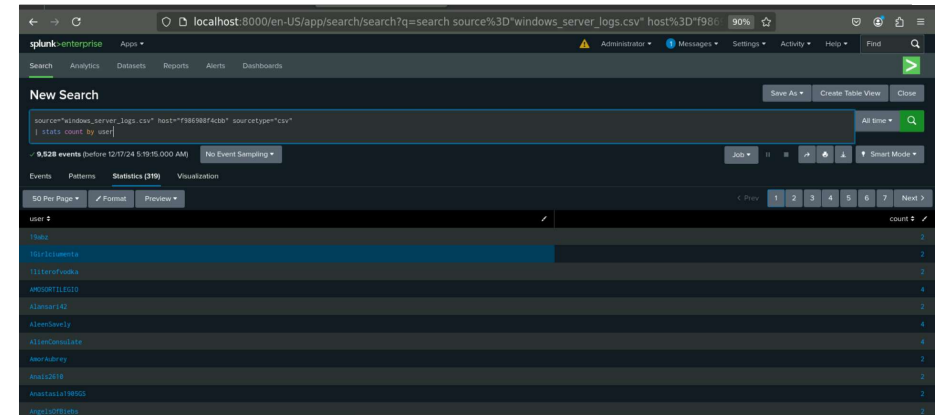
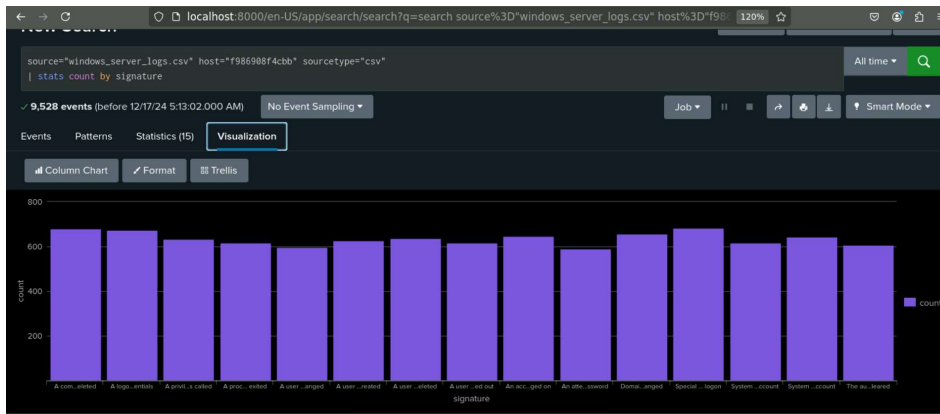
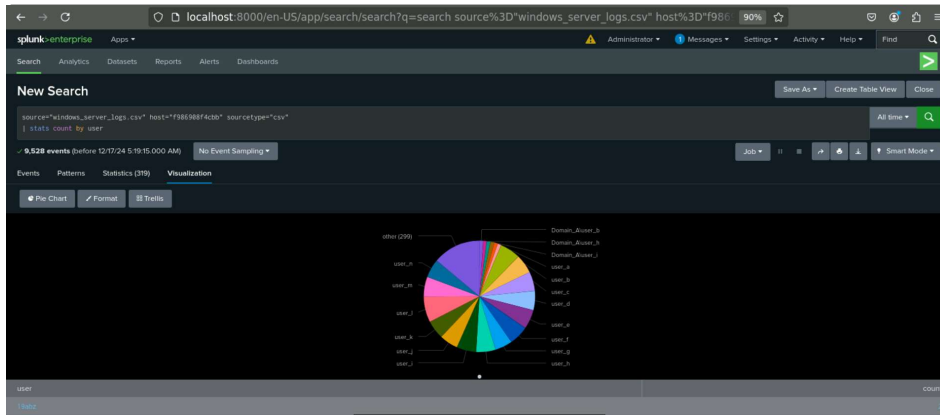
**JUSTIFICATION:** This Baseline identifies typical behavior and identifies significant deviations.

# Dashboards—Windows





# Dashboards—Windows



# Apache Logs

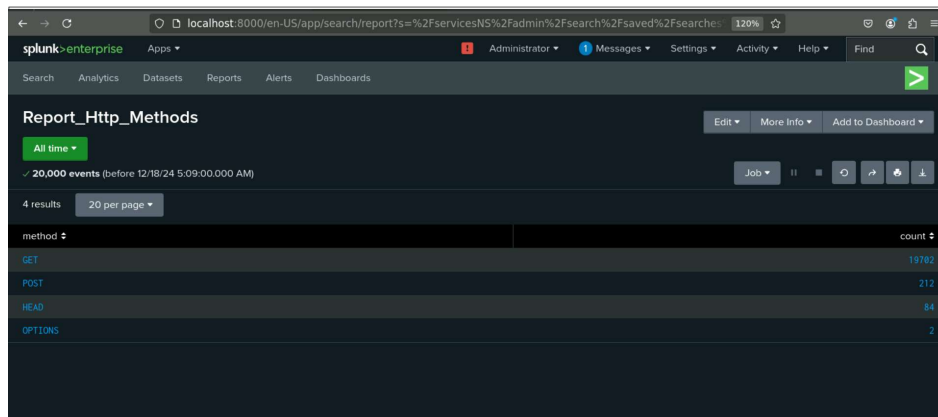
# Reports—Apache

---

Designed the following reports:

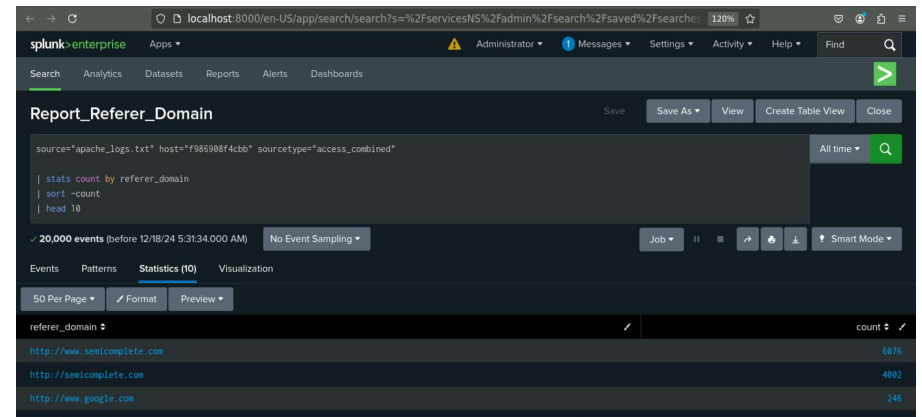
Report Name	Report Description
Report_Http_Methods	Report fetches HTTP method counts
Report_Referer_Domain	Report that shows the top 10 domains that refer to VSI's website
Report_Http_Code	Report that shows the count of each HTTP response code

# Images of Reports—Apache



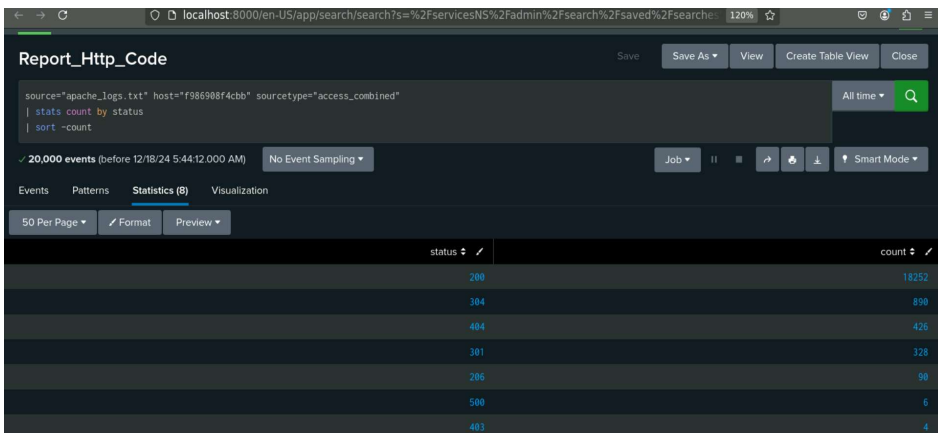
This screenshot shows the 'Report\_Http\_Methods' report in Splunk. The report is based on 20,000 events from before 12/18/24 5:09:00.000 AM. It displays a table with 4 results, showing the HTTP method and its count.

method	count
GET	19762
POST	212
HEAD	84
OPTIONS	2



This screenshot shows the 'Report\_Referer\_Domain' report in Splunk. The report is based on 20,000 events from before 12/18/24 5:31:34.000 AM. It displays a table with 3 results, showing the referer domain and its count.

referer_domain	count
http://www.senicomplete.com	6875
http://senicomplete.com	4882
http://www.google.com	246



This screenshot shows the 'Report\_Http\_Code' report in Splunk. The report is based on 20,000 events from before 12/18/24 5:44:12.000 AM. It displays a table with 7 results, showing the HTTP status and its count.

status	count
200	18252
304	890
404	426
301	328
206	90
500	6
403	4

# Alerts—Apache

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_non_US_by_country	None	Avg_count/hr	(avg_count * 3))

**JUSTIFICATION:** This Baseline identifies typical behavior and identifies significant deviations.

# Alerts—Apache

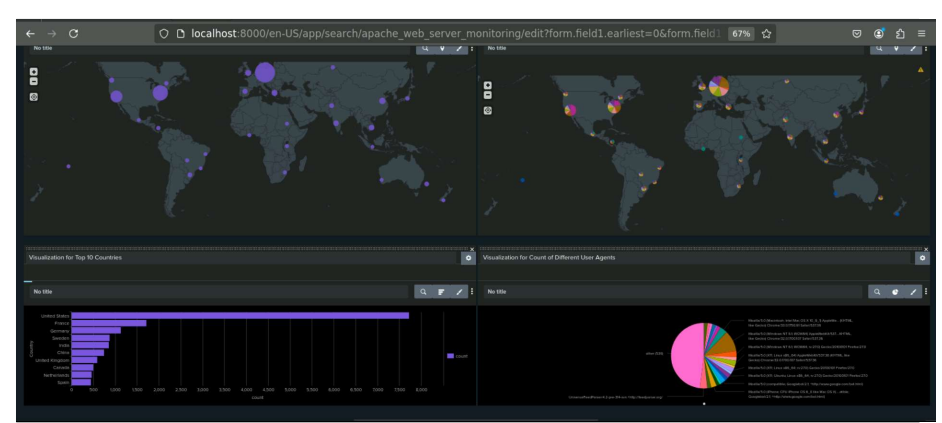
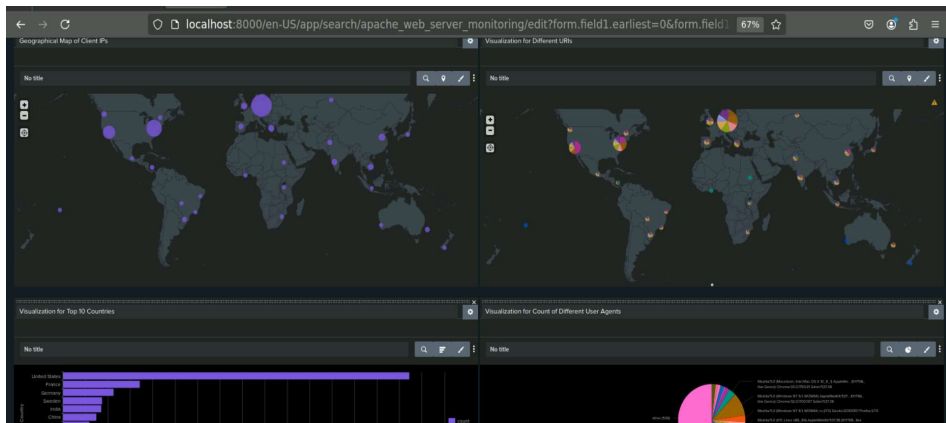
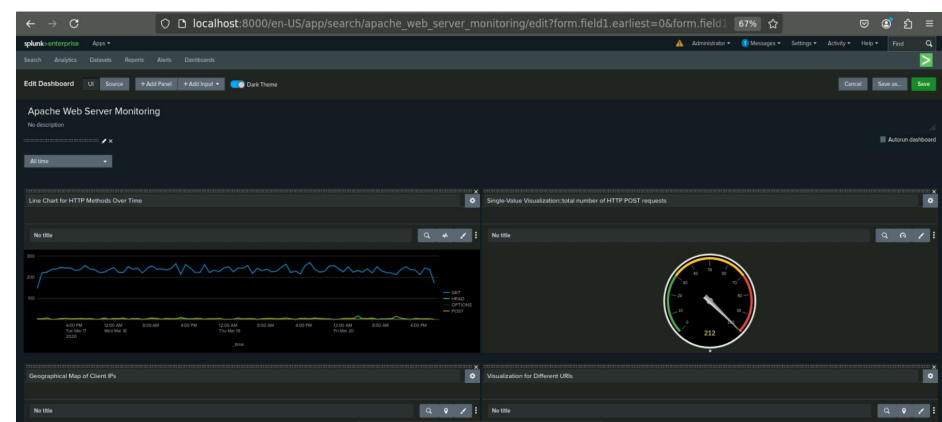
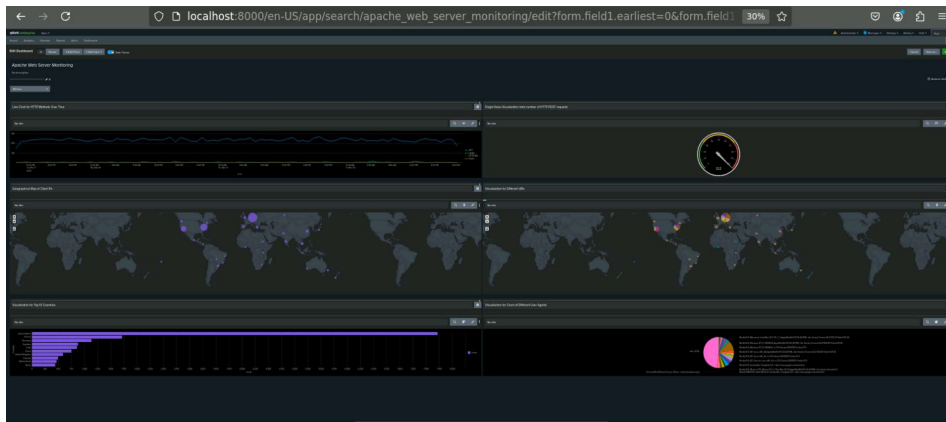
---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_Method_Post_ by_hourly_Count	Hourly POST Alert Exceeding Criteria	avg_count/hr	avg_count/hr*2

**JUSTIFICATION:** This Baseline identifies typical behavior and identifies significant deviations.

# Dashboards—Apache



The background of the slide is a complex, abstract geometric pattern. It consists of numerous triangles of varying sizes, some in a dark red or maroon color and others in black. These triangles are arranged in a way that creates a sense of depth and movement, with some appearing to point towards the center and others away from it. The overall effect is a textured, almost crystalline appearance.

# Attack Analysis



# Attack Summary—Windows

---

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

- [Answer Increased Failed Login Attempts: A significant spike in failed login attempts was observed at certain times (e.g., 01:00 and 02:00), suggesting potential brute force attacks or unauthorized access attempts.
- Suspicious User Activity: User User\_k showed an abnormal spike in activity at 09:00 and 10:00, with unusually high counts of events, which could indicate compromised accounts or automated scripts.
- User Account Deletions: Signature 4726 (user account deleted) had elevated event counts during specific hours (e.g., 00:00, 04:00, and 05:00), possibly pointing to unauthorized account deletions or insider threats.
- Successful Logins Trend: Normal patterns of successful logins were observed with minor fluctuations, indicating that successful login attempts were generally within expected ranges, except for minor spikes in some users' activity.
- Alert Triggering Thresholds: The set threshold for failed login attempts and account deletions helped in detecting suspicious volumes, with certain events surpassing thresholds and triggering alerts for further investigation.
- Time-based Anomalies: Several spikes in user activity occurred during off-hours (e.g., 00:00), highlighting times of potential increased attack risk, such as during non-business hours.
- Significant Outliers: A few users and signatures displayed outlier behavior (e.g., User\_k, signature 4726), warranting deeper investigation to determine whether these actions were legitimate or signs of a security breach.

# Attack Summary—Windows

---

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

- **Alert Threshold Effectiveness:** The thresholds for detecting failed login attempts and account deletions were generally appropriate, triggering alerts during suspicious spikes in activity, indicating potential security threats.
- **False Positives:** There were a few instances where the threshold caused minor alerts that were not indicative of malicious activity, suggesting that some normal fluctuations may have been flagged as suspicious.
- **Threshold Adjustment:** In some cases, the threshold might have been too low, missing larger spikes in activity. A higher threshold could potentially reduce unnecessary alerts while still catching significant anomalies.
- **Timing of Alerts:** Alerts were effectively triggered during off-peak hours (e.g., late night), which is consistent with patterns seen in attack activities, indicating that time-based thresholds for alerting were correct.
- **Relevance of Alerts:** The alerts successfully highlighted high-priority events, such as failed logins and account deletions, aligning with the patterns seen in time-based analysis, confirming the relevance of the chosen alert criteria.

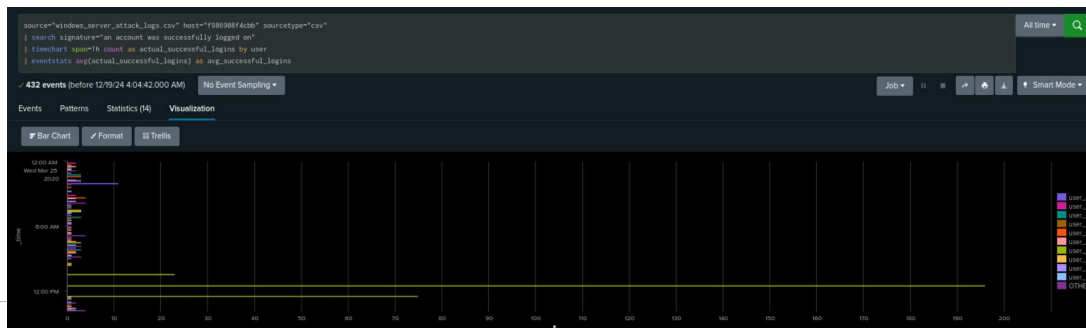
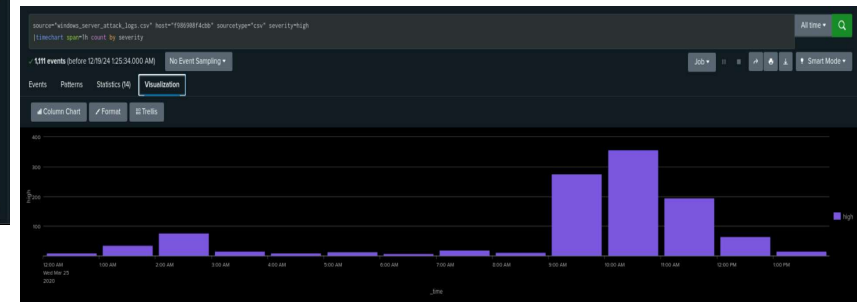
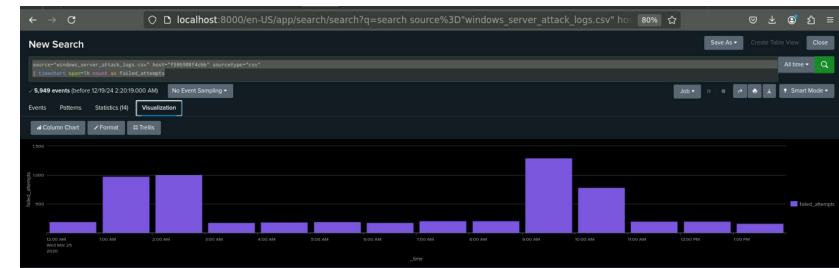
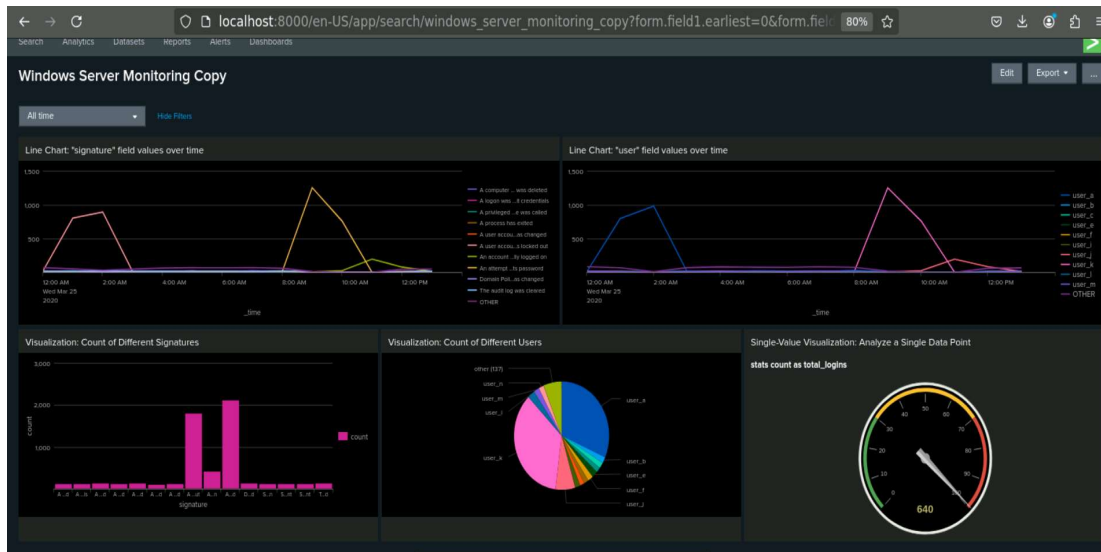
# Attack Summary—Windows

---

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

- [Answer Suspicious Activity Peaks: Dashboards clearly highlighted spikes in failed login attempts and account deletions at specific times (e.g., 01:00, 02:00), suggesting targeted attack attempts or system misconfigurations.
- User Behavior Anomalies: Certain users, like User\_k, showed abnormal activity patterns, especially during off-hours, raising concerns about potential compromised accounts or unauthorized automation.
- Increased Account Deletions: The dashboards displayed notable spikes in account deletion events (signature 4726) during specific hours, pointing to potential insider threats or unauthorized user account management activities.
- Effective Time-based Insights: Visualizations like time charts and pie charts provided clear insights into when suspicious activity peaked, aiding in the identification of high-risk times (e.g., 00:00) for further monitoring.
- Alert Correlation: The dashboards effectively correlated with alert data, confirming that certain thresholds for failed login attempts and account deletions were met, validating the alerts triggered during suspicious activity periods.

# Screenshots of Attack Logs



# Attack Summary—Apache

---

Here are the key findings from the analysis of the Apache attack logs:

- **High GET Requests:** The GET method is the most common HTTP method (3157), which is typical for web traffic, but if spikes in GET traffic occur at specific times, it could indicate reconnaissance or DDoS activity.
- **Suspicious POST Activity:** With 1324 POST requests, a relatively high number could be a concern, as POST is often associated with data submission or malicious activities such as form submission attacks or exploits like SQL injections.
- **Excessive 404 Errors:** The 404 (Not Found) responses, particularly peaking at 18:00 (624 responses), suggest possible scanning or probing activity by attackers searching for vulnerabilities or non-existent resources.
- **Low 403 and 500 Responses:** The 403 (Forbidden) and 500 (Internal Server Error) responses were very low (1 each), but they could indicate unauthorized access attempts or server misconfigurations that should be investigated further.
- **Suspicious Time Patterns:** Spikes in 404 errors at certain times (18:00 and 05:00) stand out, which may indicate potential scanning attempts, and the high volume of 200 responses at 20:00 warrants monitoring for unusual patterns.

# Attack Summary—Apache

---

Here are the key findings from the analysis of the Apache Alert logs:

•**Suspicious POST Activity Detected:** A significant spike in POST requests occurred at **20:00 on March 25, 2020**, with **1296 requests**, well above the average of **94.57**. This suggests possible malicious activity, such as an automated attack or form submission attempt.

•**Threshold for POST Requests:** The threshold of **2x the average POST count** effectively flagged the unusual spike in activity at 20:00. However, in cases with higher traffic volumes, the threshold may need further adjustments to ensure relevant anomalies are caught while avoiding false positives.

•**Ukraine's High Traffic Volume:** The highest volume of international activity was detected from **Ukraine** at **20:00**, with **864 requests**, signaling a potential attack vector or automated traffic from a specific region. This warrants further investigation into the nature of these requests.

•**Alert Triggering:** The alert triggered correctly for the **POST request spike** at 20:00, where the count of 1296 POST requests far exceeded the calculated threshold of **2x the average**. This activity aligns with signs of attack or botnet-related behavior.

•**Threshold Recalibration Needed:** After reviewing the patterns, the thresholds for detecting high POST activity should be recalibrated to handle large fluctuations in traffic more effectively. Lowering or adjusting the multiplier for what constitutes a "suspicious" spike could improve detection accuracy for future incidents.

# Attack Summary—Apache

---

Here is a summary of the findings from the dashboards when analyzing the attack logs:

**2.Excessive 404 Errors:** There were significant spikes in **404 (Not Found)** errors, particularly at **18:00**, which could indicate **scanning** for non-existent resources or attempts to exploit **vulnerabilities** in the server.

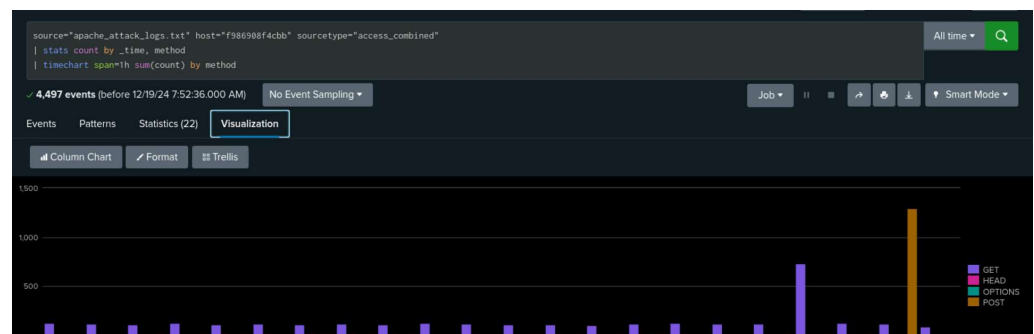
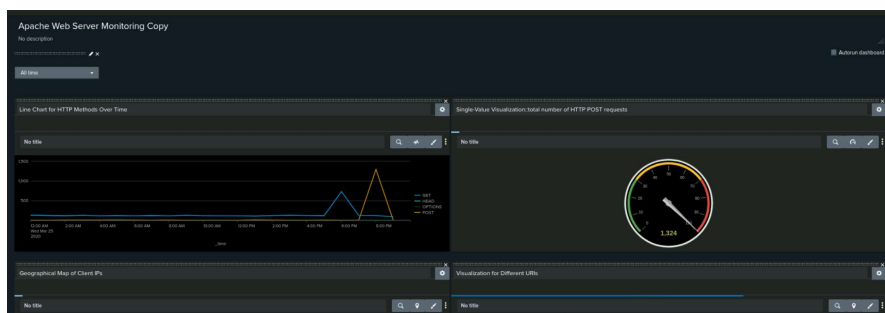
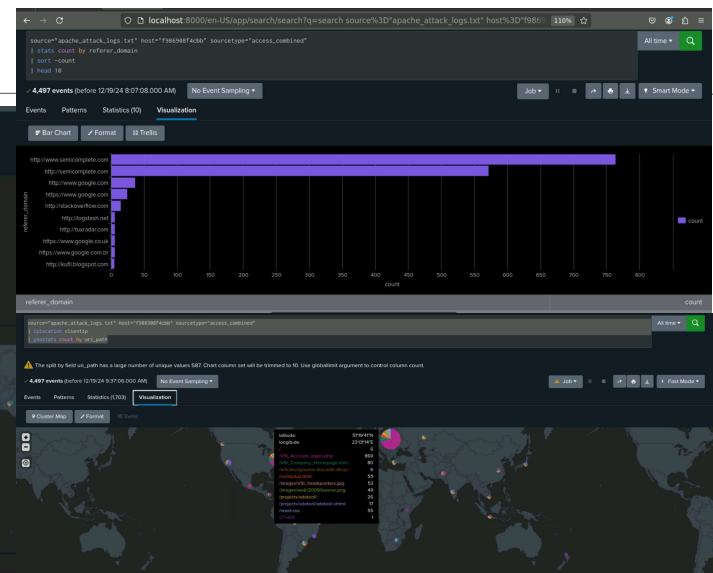
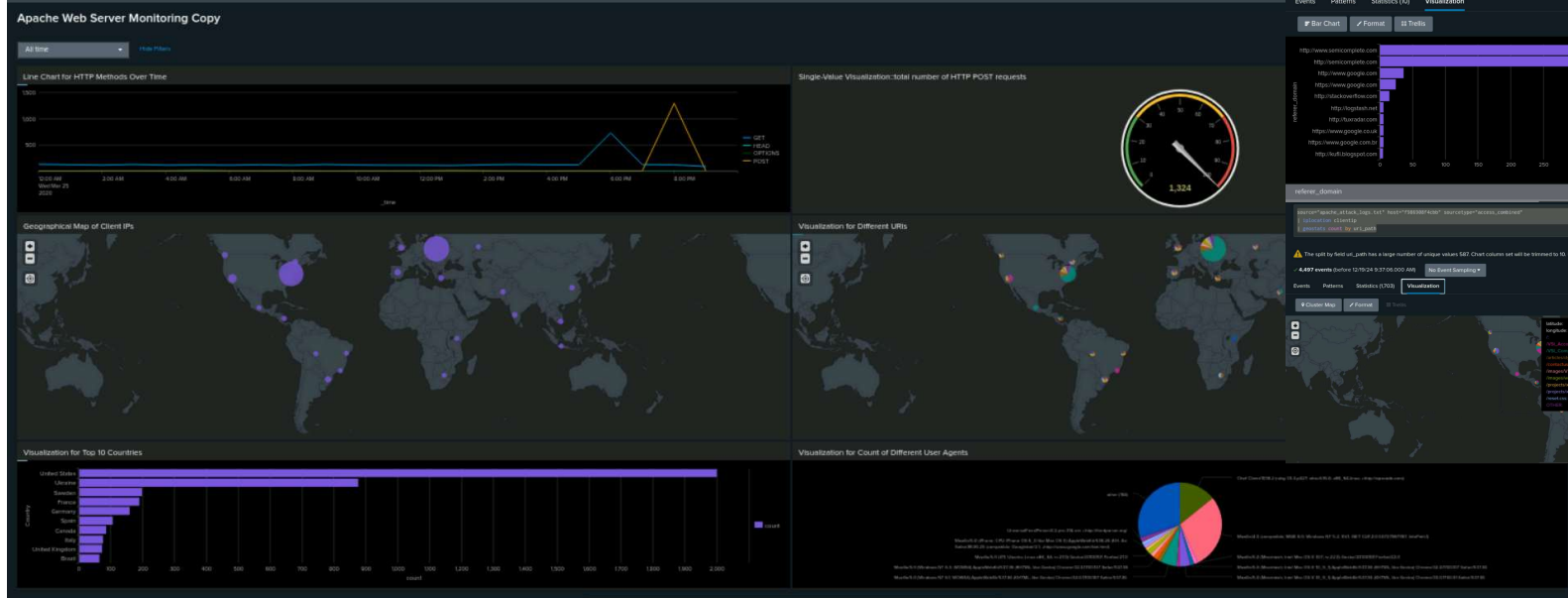
**3.International Activity:** The logs showed **high traffic from multiple countries**, notably from **Ukraine (Kyiv and Kharkiv)**, with **438** and **432** events, which may point to **targeted attacks** originating from specific regions.

**4.Frequent Access to Sensitive URI:** The URI **"/VSI\_Account\_logon.php"** was the most hit with **869** accesses, possibly indicating **brute-force login attempts** or **credential stuffing attacks** aimed at compromising accounts.

**5.Geographic Concentration of Attacks:** Attacks seemed concentrated in specific locations, with **Ashburn, United States** having the highest number of attacks (**668**), indicating a potential **source of the attack infrastructure** or **compromised proxy servers**.

These points highlight suspicious patterns, including abnormal HTTP method usage, error codes, international traffic, targeted login pages, and the geographic concentration of attacks.

# Screenshots of Attack Logs







# Summary and Future Mitigations

# Project 3 Summary

---

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

The attack involved a high volume of **POST requests** targeting the **VSI\_Account\_logon.php** URI, indicating potential **brute-force login attempts** on both the **Windows Server** and **Apache web server**. Additionally, **404 errors** and international traffic, particularly from **Ukraine**, suggest **vulnerability scanning** or attempts to exploit misconfigurations in both the **Windows Server** and **Apache server** setup.

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

To protect VSI from future attacks, implement brute-force protection with account lockout and MFA, deploy a Web Application Firewall (WAF), and restrict access via geo-blocking. Regularly scan for vulnerabilities and apply patches to both Windows Server and Apache. Enhance security with continuous log monitoring and real-time alerts.