Defensive Security Project
by: Jason King

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

In this scenario, I'll be playing my current role of role of a SOC analyst for Virtual Space Industries (VSI), a company that designs virtual-reality programs. VSI has heard rumors that a competitor, JobeCorp, may be planning cyberattacks to disrupt our operations. My job is to use Splunk to monitor potential attacks on key systems, including an Apache web server that hosts our administrative webpage and a Windows server running our backend operations.

On Day 1, I started by reviewing past logs from the systems to establish baselines and create alerts, reports, and dashboards. On Day 2, I was informed that VSI had experienced cyber attacks, likely from JobeCorp, which targeted the Windows and Apache servers I'd been monitoring. I received new logs from the attack period and used them to analyze the effectiveness of the monitoring solutions I set up. Finally, this presentation, showcasing my monitoring solutions and findings to senior management.

XML IP Geolocation API

XML IP Geolocation API

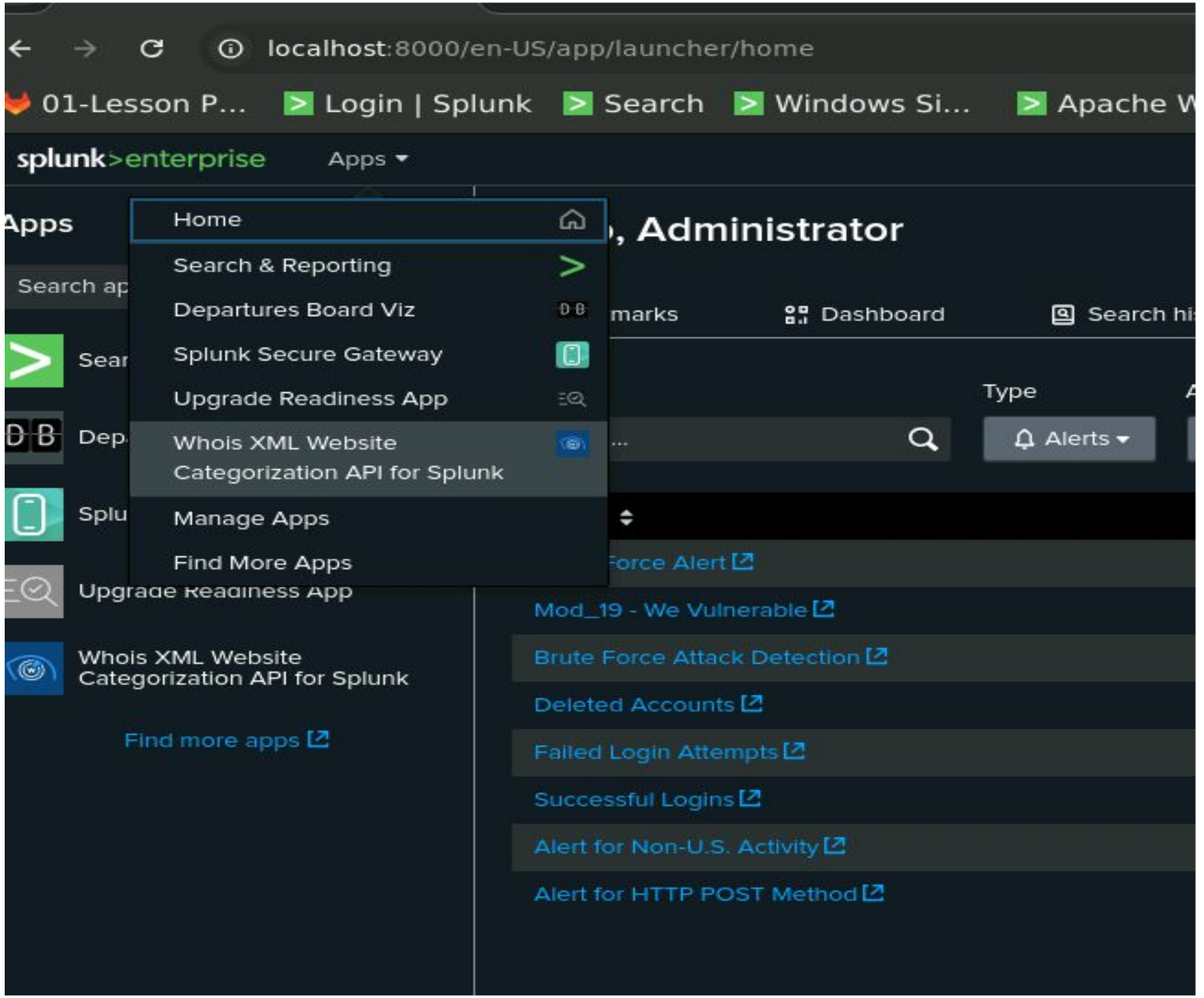
The "XML IP Geolocation API" add-on for Splunk allows users to enrich their data by determining the geographical location of IP addresses within their logs. It uses an API to provide details such as country, region, city, latitude, longitude, and ISP for each IP address. This information can be used to identify the origin of web visitors or users, customize user experiences, or detect potential fraud.

The add-on integrates with Splunk to help monitor and analyze geographic patterns in network traffic, which can enhance security measures, ensure regulatory compliance, and improve incident response. It is optimized for performance and supports both IPv4 and IPv6 addresses. Installation involves adding the app to Splunk and configuring API keys for geolocation lookups. This tool is useful for SOC analysts or network admins looking to visualize and track IP-based threats more effectively.

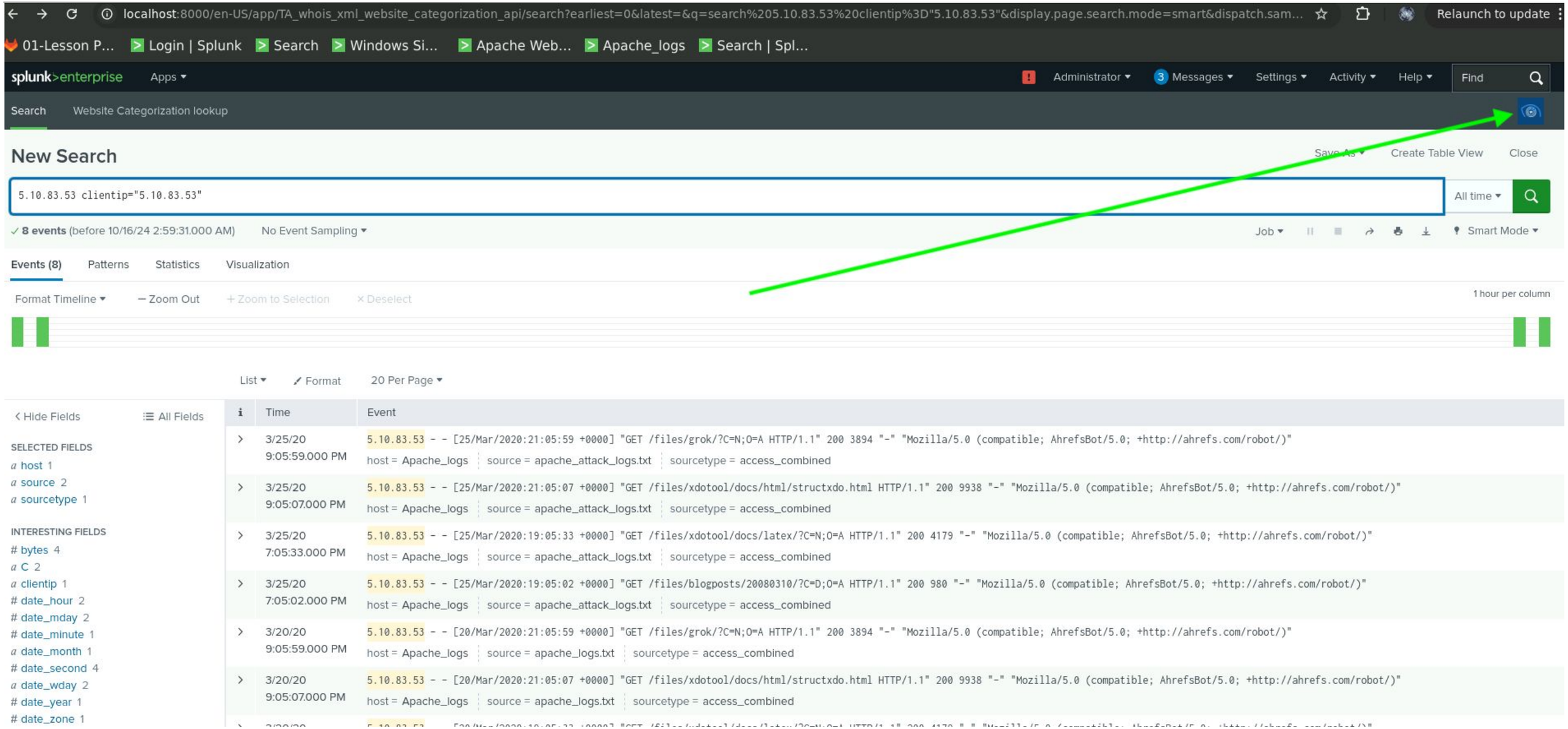
XML IP Geolocation API

Imagine a scenario where a company, "TechGlobal," operates a public-facing e-commerce website. Recently, the security team notices a sharp increase in traffic from various countries where they don’t usually do business. They suspect a potential Distributed Denial of Service (DDoS) attack or malicious activity. Using the XML IP Geolocation API add-on for Splunk, the SOC team can quickly determine the geographic origin of the suspicious IP addresses. By identifying patterns—such as clusters of IPs coming from regions not associated with legitimate users—they can flag the traffic as malicious and act to block these regions temporarily. The add-on also provides insights into whether these IPs are associated with known proxy servers or anonymization tools like Tor, helping the team confirm their suspicions. This geographic analysis not only helps the company mitigate the attack quickly but also allows them to create more focused defensive rules in their firewall or web application filters. Over time, they can continue monitoring geolocation data to detect any future anomalies, greatly improving their security posture. In this way, the geolocation API helps TechGlobal react faster to threats, reduce downtime, and protect customer data from large-scale attacks.

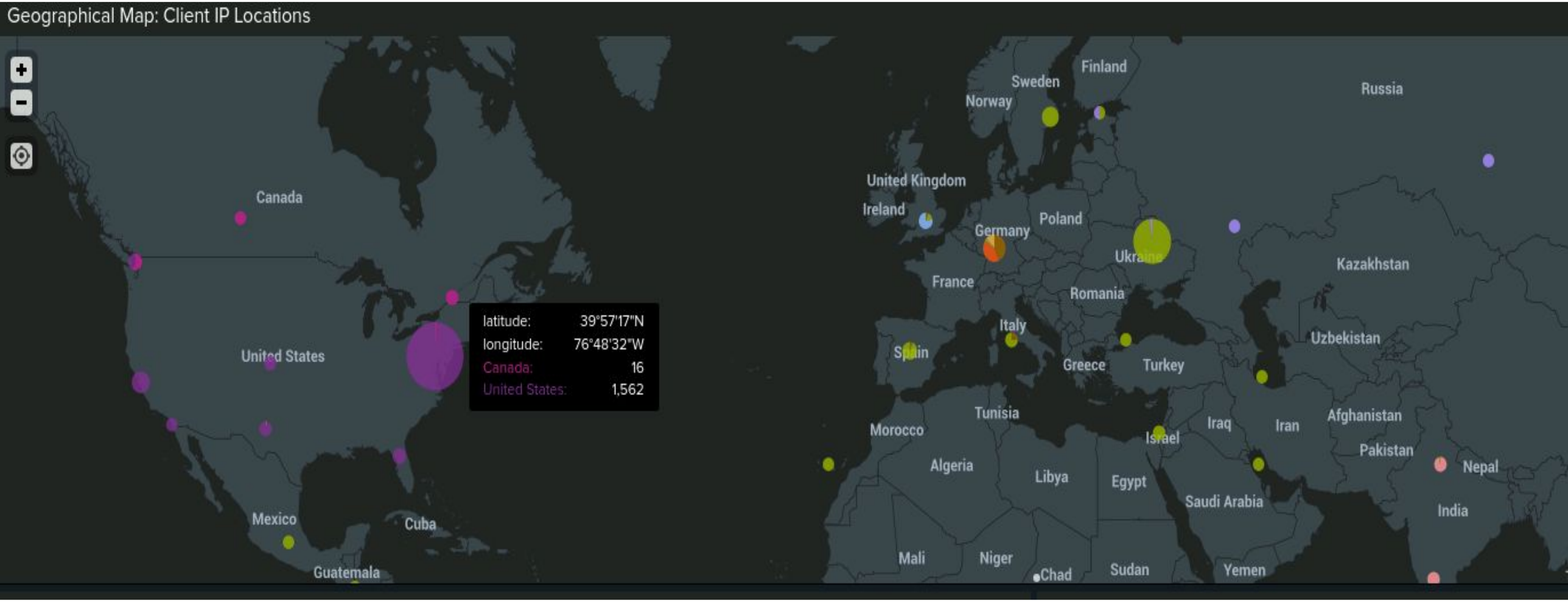
XML IP Geolocation API



XML IP Geolocation API



XML IP Geolocation API



Logs Analyzed

1 Windows Logs

1. **Severity Levels:** They include changes in the severity of events, such as unauthorized access attempts or system misconfigurations, which can escalate to critical incidents.
2. **Failed and Successful Activities:** The logs show success and failure rates of system actions, such as login attempts or privileged actions like account deletions and password resets. For example, a suspicious volume of failed activity (e.g., password reset attempts) could indicate a targeted attack.
3. **User Activity:** Logs include details about login activities, particularly focusing on users with abnormal activity, such as an unusually high number of logins by a single user in a short time.
4. **Account Management:** Suspicious actions like account deletions or lockouts are tracked, which can signal potential insider threats or compromised credentials.
5. **Timestamps and Event Counts:** The logs provide timestamps of events, enabling analysts to identify when an attack begins and ends, which is crucial for pinpointing the exact time of a security breach.

2 Apache Logs

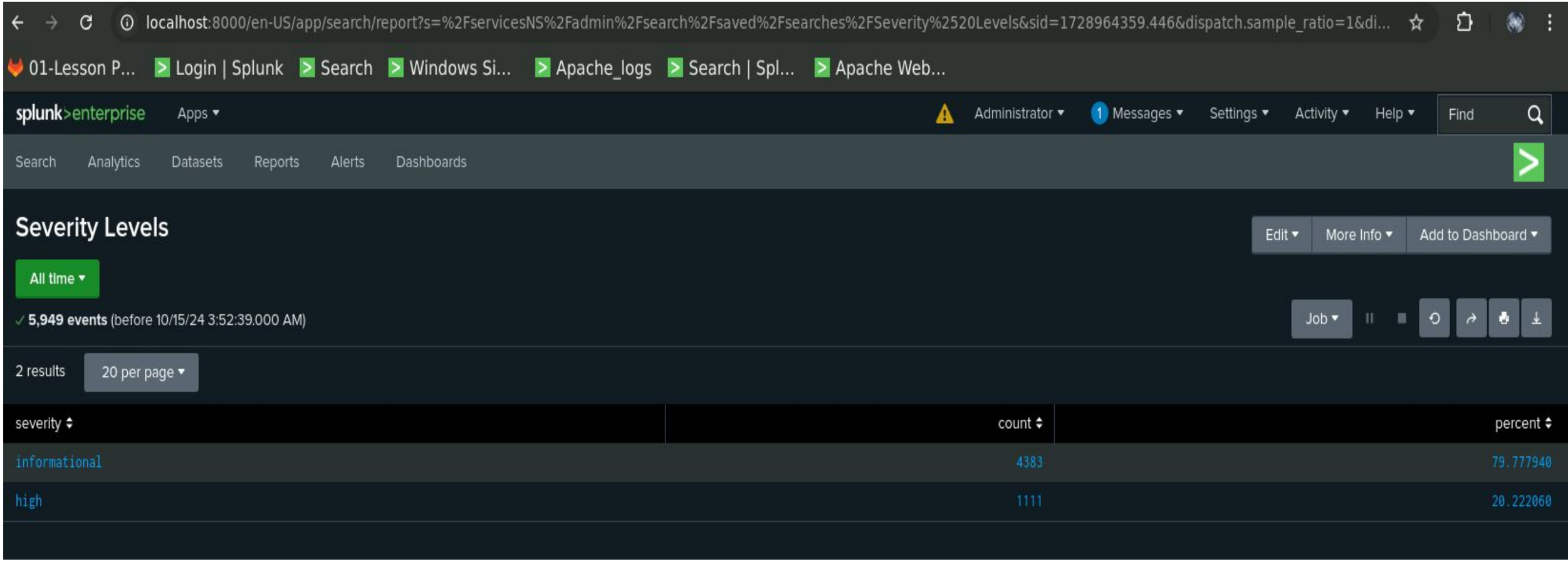
1. **HTTP Methods:** Tracks methods like GET and POST. A spike in POST requests can indicate malicious activities like file uploads or brute-force attacks; we will look at this later..
2. **Response Codes:** Logs status codes such as 200 (success) and 404 (not found). An increase in 404 errors may signal attackers scanning for vulnerabilities..
3. **Referrer Domains:** Monitors where traffic originates. Sudden changes in referrer traffic can be a sign of malicious activity.
4. **International Activity:** Logs traffic from different regions. A spike from unfamiliar countries not often seen by a companies customers.
5. **URI Access:** Tracks frequently accessed web pages, such as login pages, which could signal brute-force attempts.

Windows Logs

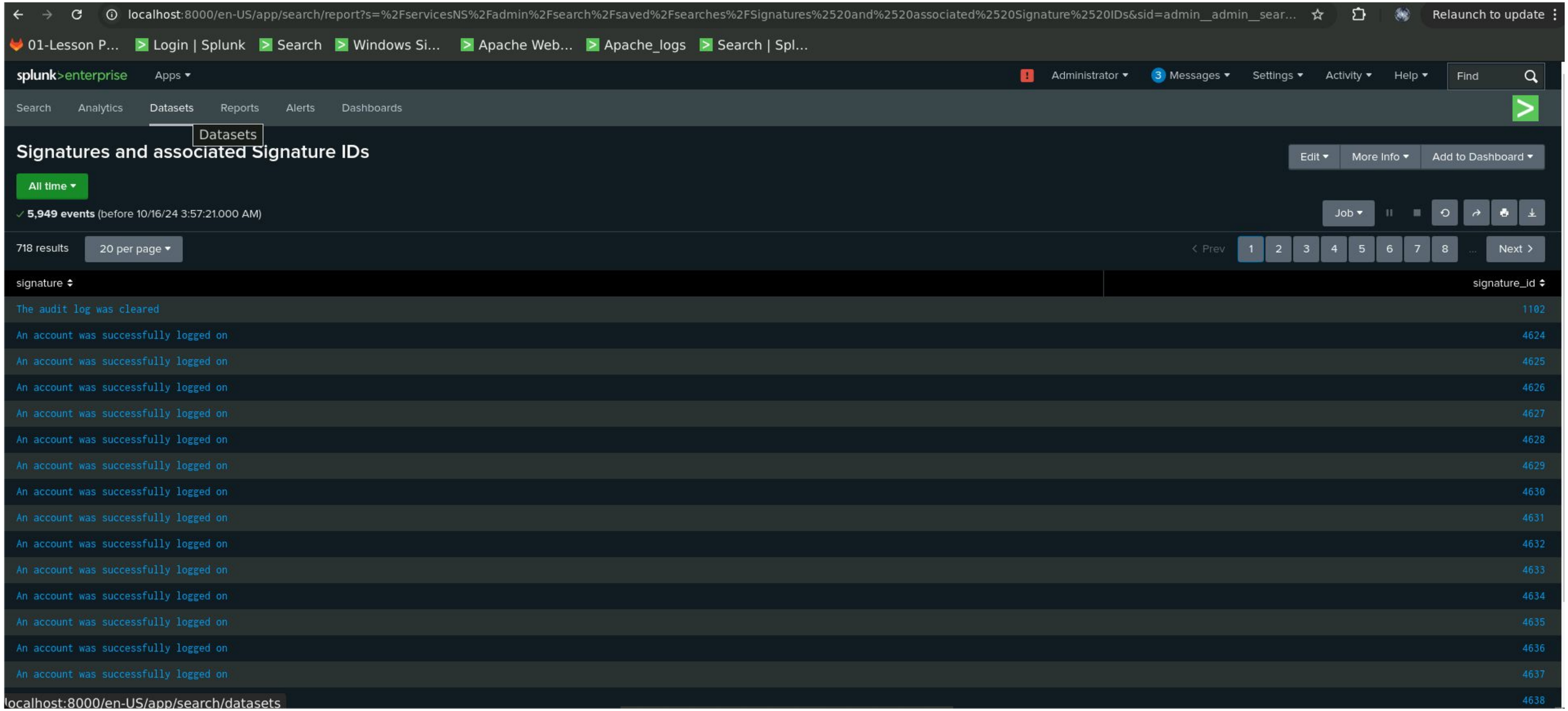
Reports — Windows

Report Name	Report Description
Severity Level	Severity levels of the Windows logs being viewed.
Signatures and Signature IDs	ID number associated with the specific signatures for Windows activity.
Success and Failure	Shows VSI if there is a suspicious levels of failed activities on their server.

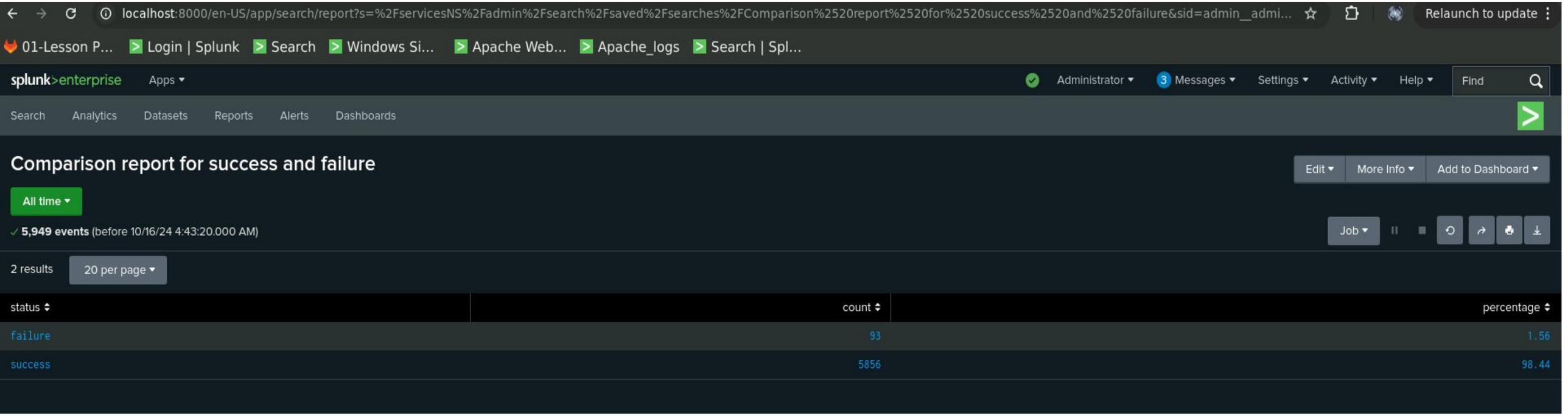
Severity Levels Report — Windows



Signatures & Associated Signature IDs Reports—Windows



Success & Failure Comparison Report — Windows



Alerts — Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Logins	Failed Logins Alert	5.79	12

JUSTIFICATION:
The alert baseline is set at 5.91, representing the average number of failed logins during normal operations, with typical spikes reaching 9 around 8 a.m. The threshold is set at 12 to avoid false positives while effectively detecting abnormal login activity. This threshold is high enough to account for regular fluctuations but low enough to catch potential security threats like brute-force attacks, ensuring the alert remains both accurate and actionable.

Alerts — Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Login	Successful Login Alert	13.45	18

JUSTIFICATION:
The baseline of 13.45 logins per hour reflects normal activity. The threshold is set at 18 logins per hour to detect unusual spikes, which could indicate unauthorized access attempts. This threshold is high enough to prevent false positives during busy periods but low enough to catch potential security issues.

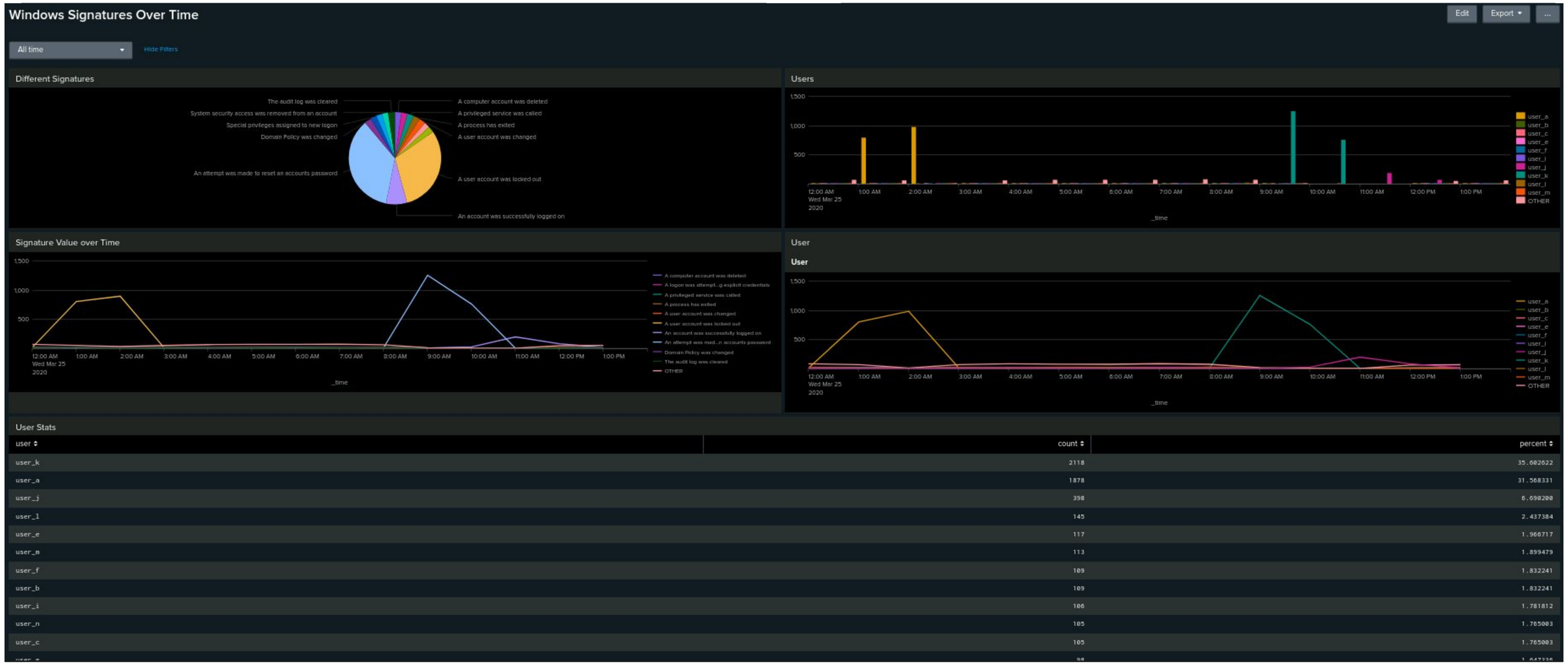
Alerts — Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deleted	Account Deleted Alert	13.25	18

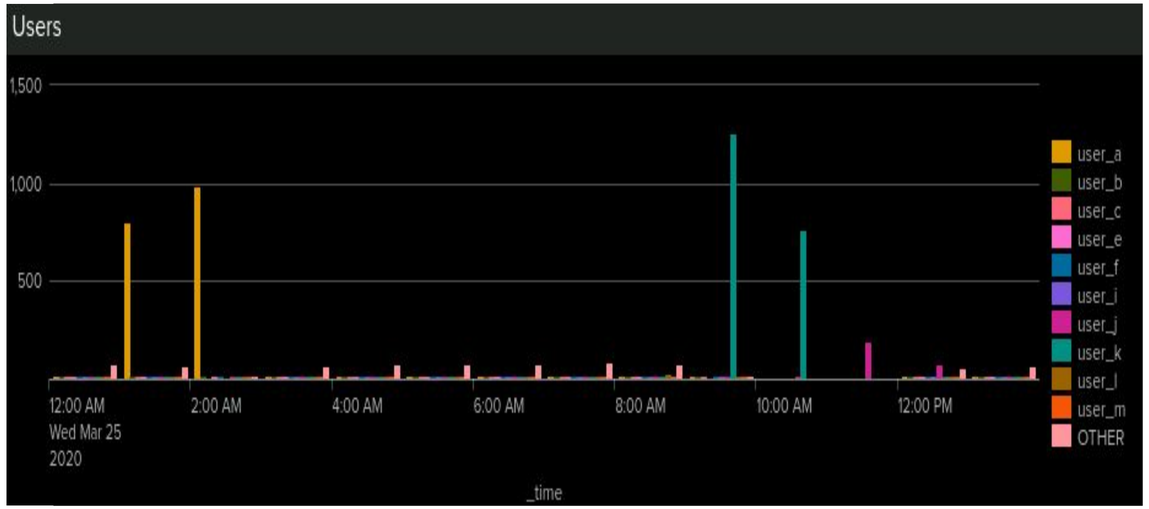
JUSTIFICATION:

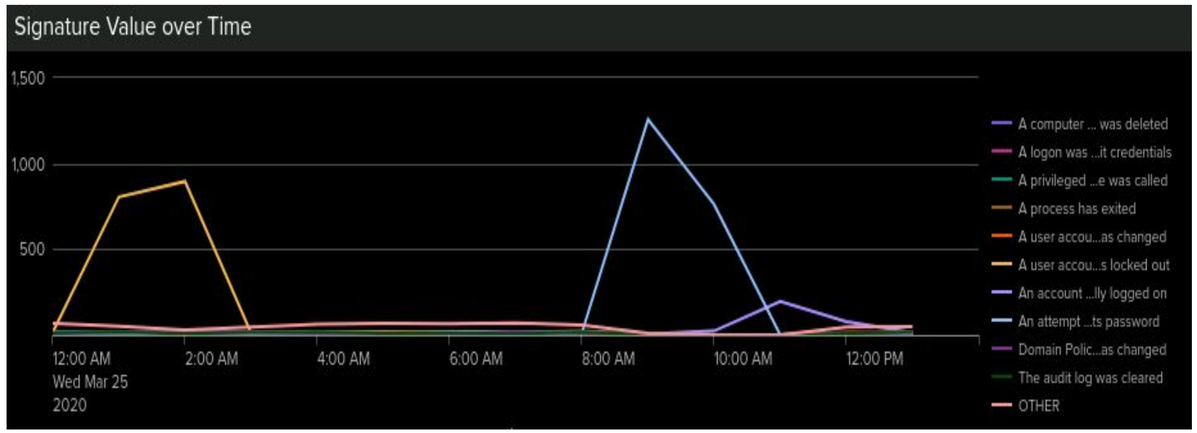
The alert baseline is set at 13.25, reflecting normal account deletions during operations. The threshold is set at 18 to detect abnormal spikes, signaling potential unauthorized actions. This threshold is high enough to avoid false positives but low enough to catch suspicious activity, ensuring accurate monitoring without excessive alerts.

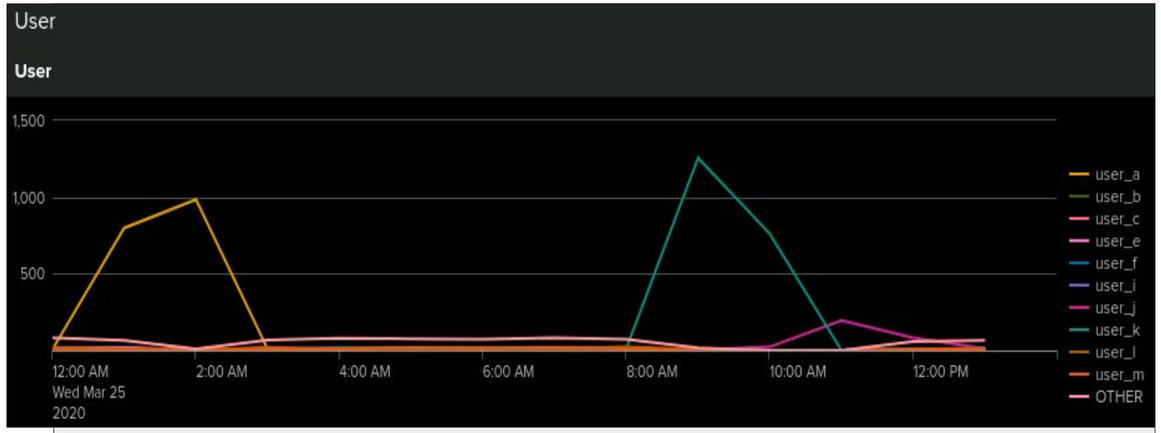
Dashboards — Windows



Dashboards — Windows





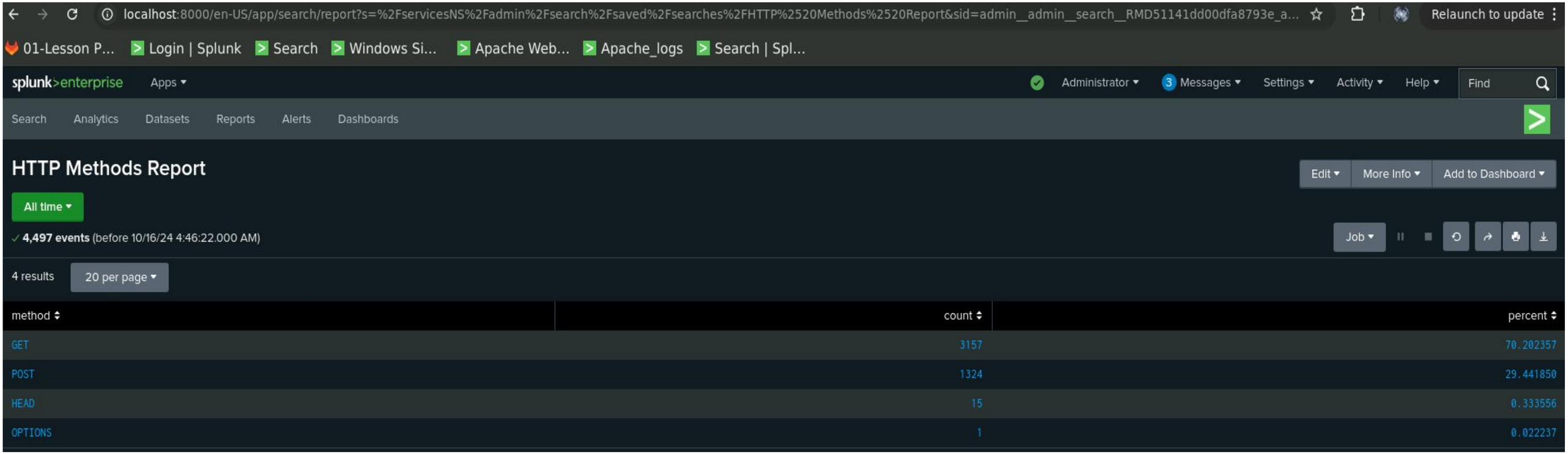


Apache Logs

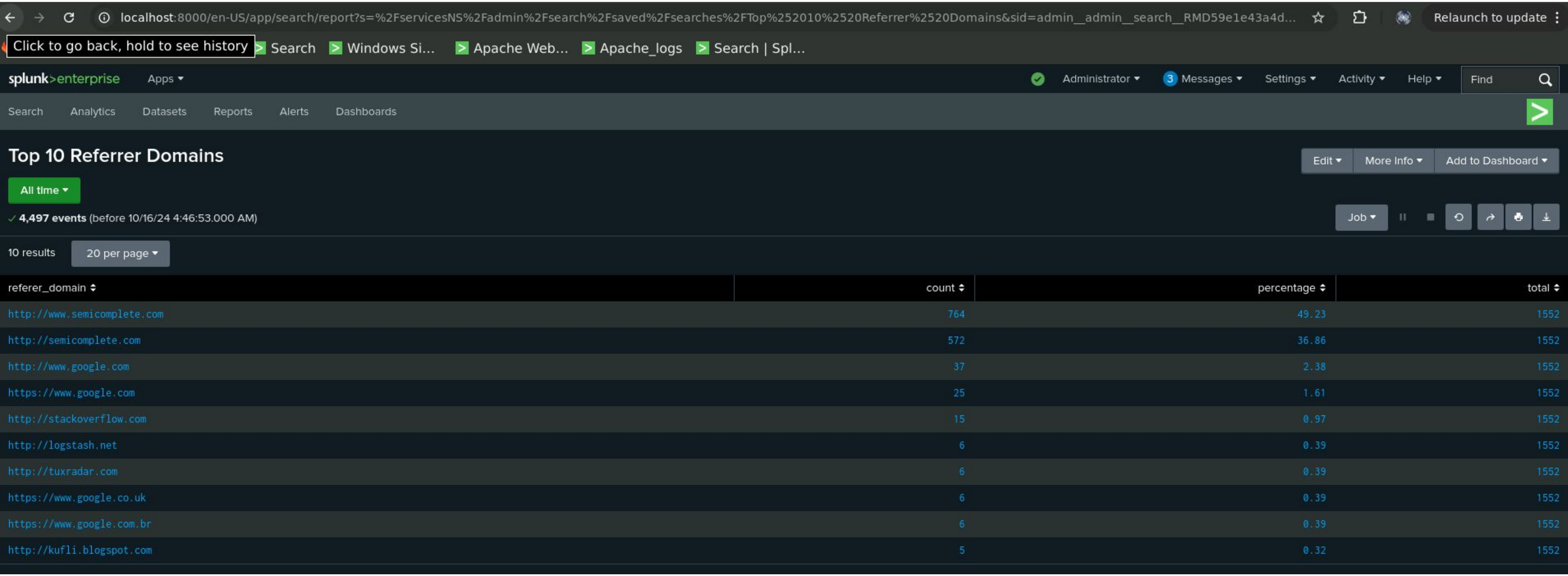
Reports — Apache

Report Name	Report Description
HTTP Methods	HTTP activity being requested against VSI’s web server.
Top 10 Domains (VSI)	Identify suspicious referrers
HTTP Response Code Count	Shows suspicious levels of HTTP responses

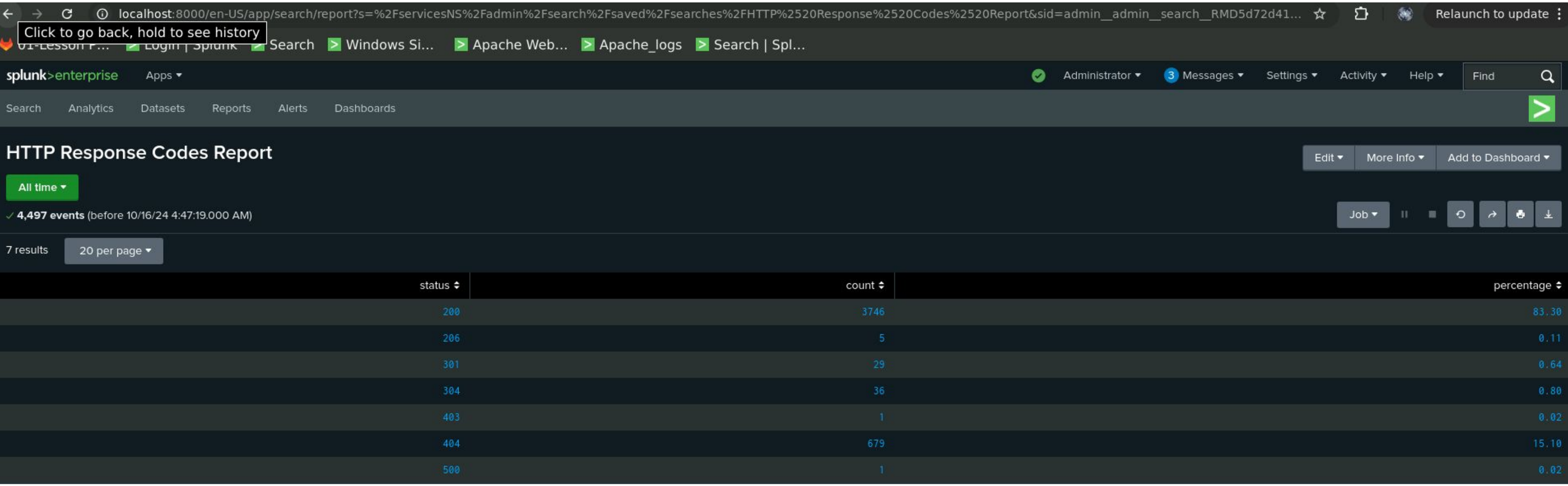
Images of Reports—Apache



Images of Reports—Apache



Images of Reports—Apache



Alerts — Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Activity	Non-US Activity Alert	73.09	100

JUSTIFICATION:
Although the events spiked to 937, my threshold was set at 100. However, surrounding event activity remained at about 81, which indicates the spike was an anomaly. As a result, I will keep the threshold set at 100 to account for potential future spikes without triggering too many false positives. This ensures the alert remains sensitive to significant increases in non-U.S. activity while avoiding unnecessary alerts during normal fluctuations.

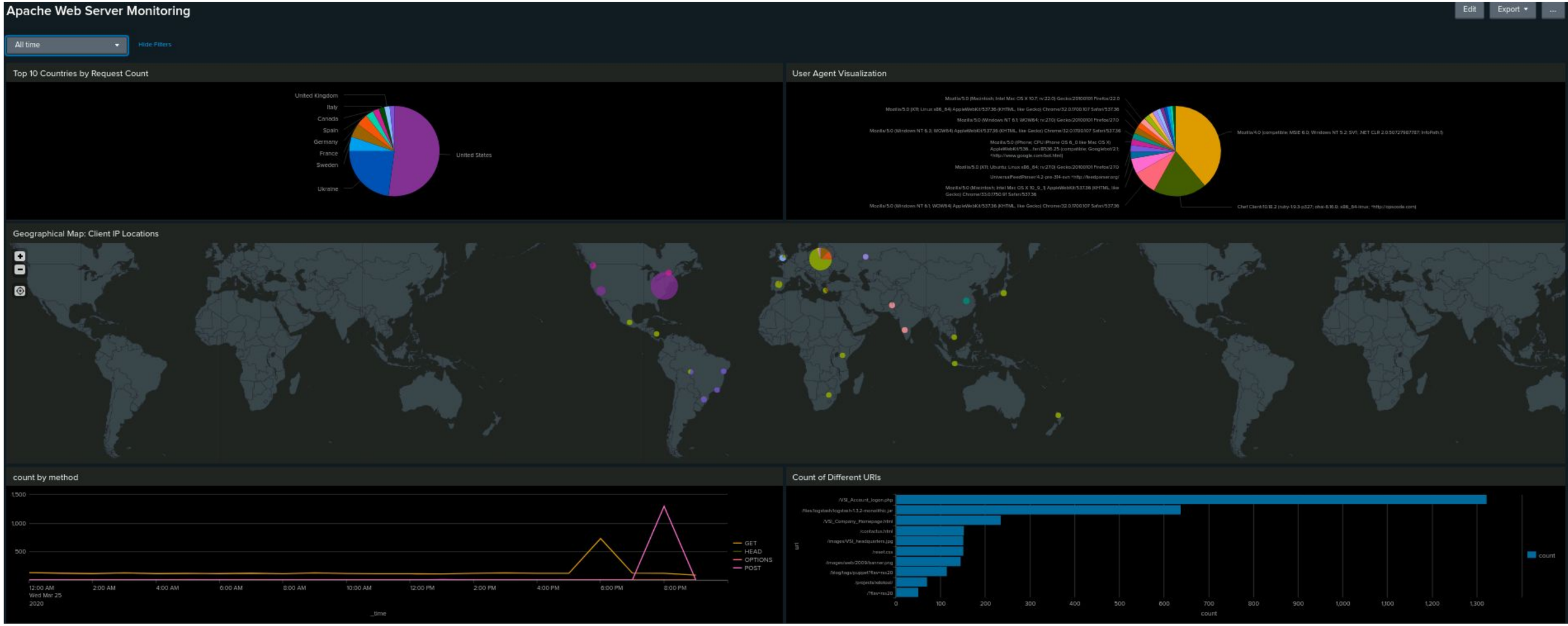
Alerts — Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Method	HTTP POST Method Alert	1.27	6

JUSTIFICATION:

The baseline for the HTTP POST Method Alert is set at 1.27 events per hour, reflecting normal activity. During the attack, the event count spiked, but in the surrounding hours, it dropped to just 1 event per hour. Therefore, setting the threshold at 6 ensures it captures significant spikes, such as during attacks, while avoiding false positives from normal fluctuations. This balance ensures effective detection without overwhelming the system with unnecessary alerts.

Dashboards—Apache



Attack Analysis

Attack Report Summary — Windows

Severity Level Shift: There was a significant shift in severity levels, with high-severity events decreasing from 93.09% to 79.77%, and low-severity events increasing from 6.90% to 20.22%. This shift suggests a change in the nature of logged events, potentially indicating system misconfigurations or increased low-priority issues such as routine errors or minor security anomalies, all requiring further investigation.

Failed Activities: While the overall failure rate remained stable at 2.98%, I detected a suspicious spike in failed activity between 8 a.m. and 9 a.m. on March 25th (which is a strange time for an attack). There were 35 failed events, involving privileged actions like password resets and account deletions, which may point to a targeted attack or insider threat.

Suspicious Logins: I observed a large volume of successful logins, with 196 events recorded between 11 a.m. and 12 noon, all attributed to "User J." This concentrated activity from a single user is unusual and may suggest credential compromise or misuse.

Suspicious Signatures: During the attack, notable spikes occurred with account lockouts (896 events) and password reset attempts (39.955%), particularly between 12 a.m. and 3 a.m. and again between 8 a.m. and 11 a.m. These patterns indicate coordinated attempts to access or manipulate accounts. Overall, these findings point to a coordinated and potentially insider-driven attack, targeting user accounts and system configurations.

Attack Alert Summary — Windows

Failed Logins Alert: A spike of 35 failed login attempts was detected between 8 a.m. and 9 a.m. This exceeded the baseline of 5.91 and triggered the alert threshold of 12. These failures included privileged actions like password resets, suggesting possible unauthorised access attempts.

Successful Logins Alert: Between 11 a.m. and 12 p.m., 196 successful logins were recorded, all linked to "User J." This is highly unusual given the baseline of 13.45 and exceeded the alert threshold of 18, indicating a potential compromise of user credentials.

Account Deletion Alert: No suspicious account deletions were detected during the analysis. The alert remained inactive, consistent with normal activity. These findings point to a targeted attack focusing on gaining unauthorised access, particularly involving credential misuse or insider activity.

Attack Summary — Windows

Signature Activity: The spike in specific signatures, including password reset attempts and account lockouts, suggests a targeted attack focused on user accounts. The period between 12 a.m. and 11 a.m. showed a significant increase in these activities, with the highest peak reaching over 1,200 lockout events.

User Activity: Users **A**, **K**, and **J** displayed suspicious patterns. **User A** was active between 1 a.m. and 3 a.m., with a peak of over 900 events, and **User K** showed similar peaks between 9 a.m. and 11 a.m. These users, with high activity in a short timeframe, may indicate compromised accounts.

Correlated Signatures: The dashboard charts confirm a strong correlation between abnormal signature activity (e.g., password resets, lockouts) and specific users, suggesting the attack targeted specific accounts and likely involved an attempt to gain unauthorised access. These findings indicate a concerted effort to exploit user credentials and disrupt access, requiring immediate investigation to prevent further unauthorised access. This Dashboard proved very useful.

Windows Attack Logs - Count by Signature

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"
| stats count by signature
| eventstats sum(count) as total_count
| eval percentage = (count / total_count) * 100
| table signature count percentage
```

All time

✓ **5,949 events** (before 10/17/24 1:01:17.000 AM) No Event Sampling

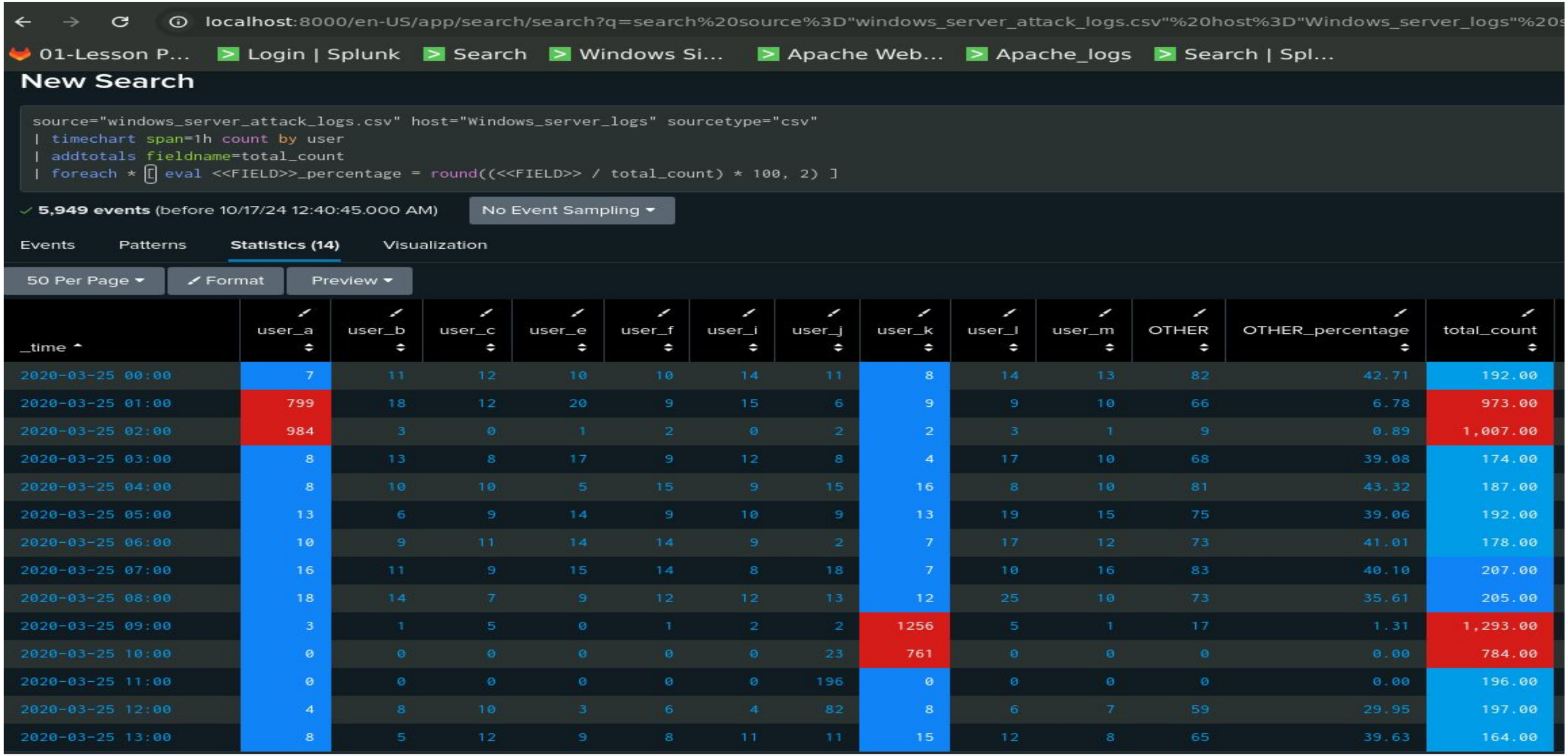
Job Smart Mode

Events Patterns **Statistics (15)** Visualization

50 Per Page Format Preview

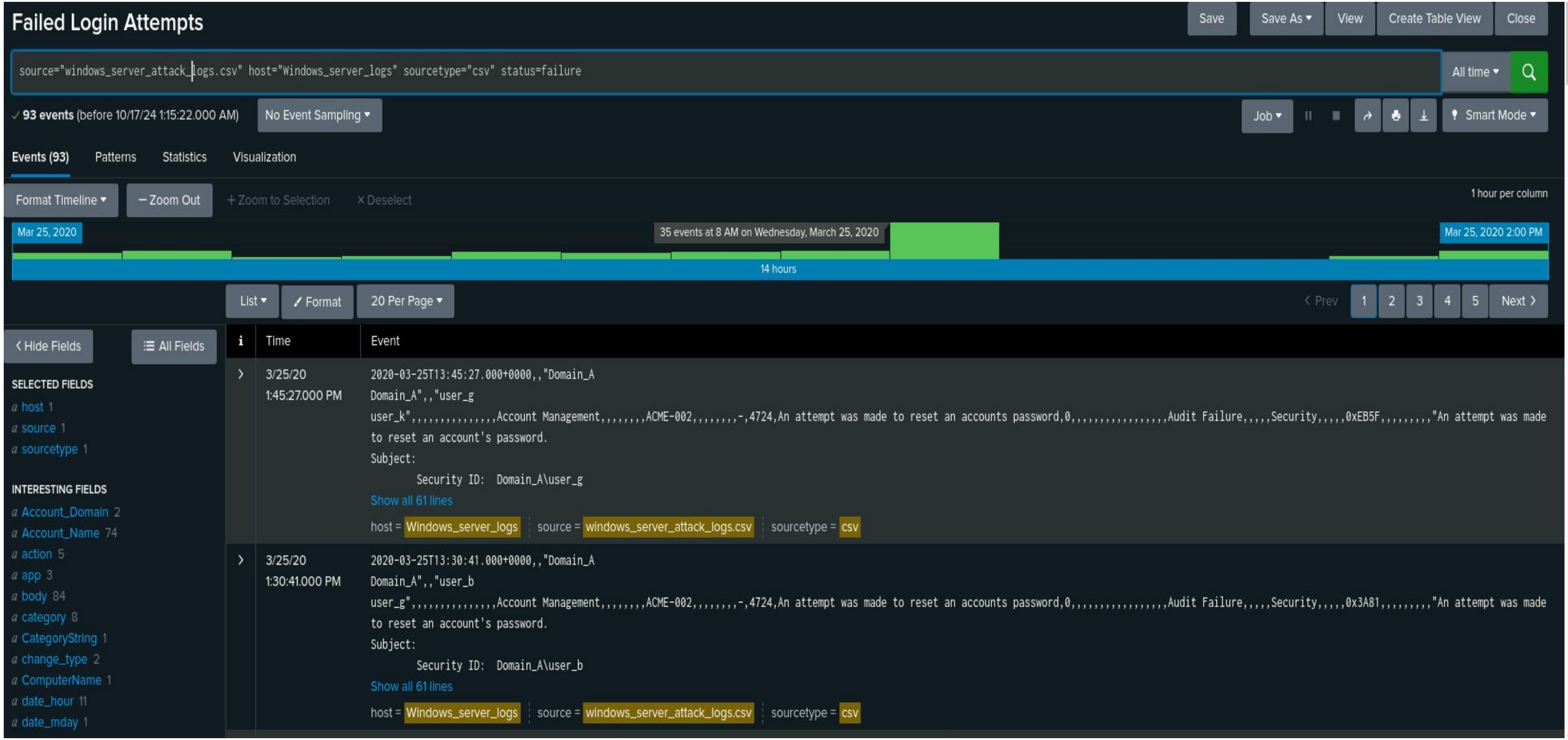
signature	count	percentage
An attempt was made to reset an accounts password	2128	35.77071776769205
A user account was locked out	1811	30.442091107749203
An account was successfully logged on	432	7.2617246596066565
Domain Policy was changed	143	2.4037653387123887
The audit log was cleared	142	2.3869557908892247
A user account was changed	137	2.3029080517734073
A privileged service was called	136	2.2860985039502437
A process has exited	134	2.2524794083039166
A computer account was deleted	133	2.235669860480753
A logon was attempted using explicit credentials	130	2.1852412170112623
A user account was deleted	130	2.1852412170112623
System security access was removed from an account	128	2.1516221213649356
Special privileges assigned to new logon	127	2.134812573541772

Windows Attack Logs - Count by User



_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER	OTHER_percentage	total_count
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82	42.71	192.00
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66	6.78	973.00
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9	0.89	1,007.00
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68	39.08	174.00
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81	43.32	187.00
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75	39.06	192.00
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73	41.01	178.00
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	16	83	40.10	207.00
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73	35.61	205.00
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17	1.31	1,293.00
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0	0.00	784.00
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0	0.00	196.00
2020-03-25 12:00	4	8	10	3	6	4	82	8	6	7	59	29.95	197.00
2020-03-25 13:00	8	5	12	9	8	11	11	15	12	8	65	39.63	164.00

Windows Attack Logs - Count by User (8am Spike)



Attack Report Summary — Apache

HTTP Methods Report: This report showed a dramatic rise in HTTP POST requests, increasing from 1.06% to 29.44%, with the count rising from 106 to 1,324. POST requests are used to send data to the server, and this spike suggests potential malicious activity, such as file uploads or exploitation attempts.

Top 10 Referrer Domains: There were minimal changes in the top referrer domains, with the most notable change being a 2.03% increase in traffic from semicomplete.com. This increase in traffic likely reflects a normal fluctuation in website traffic rather than a sign of attack.

HTTP Response Codes: The sharp increase in 404 error codes from 2% to 15% suggests that attackers were scanning for vulnerable or non-existent files, possibly using tools like **gobuster or dirbuster** to scan VSI's directories. Simultaneously, successful 200 responses dropped from 91% to 83%, indicating a higher rate of failed requests during this period.

Attack Alert Summary — Apache

HTTP POST Activity: There was a significant spike in HTTP POST requests, with 1,296 events detected between 8 p.m. and 9 p.m. This unusual volume suggests potential attempts to upload malicious files or exploit server-side vulnerabilities. The threshold for POST requests was correctly set at 6, allowing the alert to capture this activity with a normal baseline of 1.27.

International Activity: A sharp increase in traffic from Ukraine was flagged, with 937 events occurring within a one-hour window. This abnormal spike indicated possible probing or a coordinated distributed attack using compromised systems. The alert threshold was set at 150, which captured this surge in international traffic with a normal baseline of 73.09.

Attack Summary—Apache

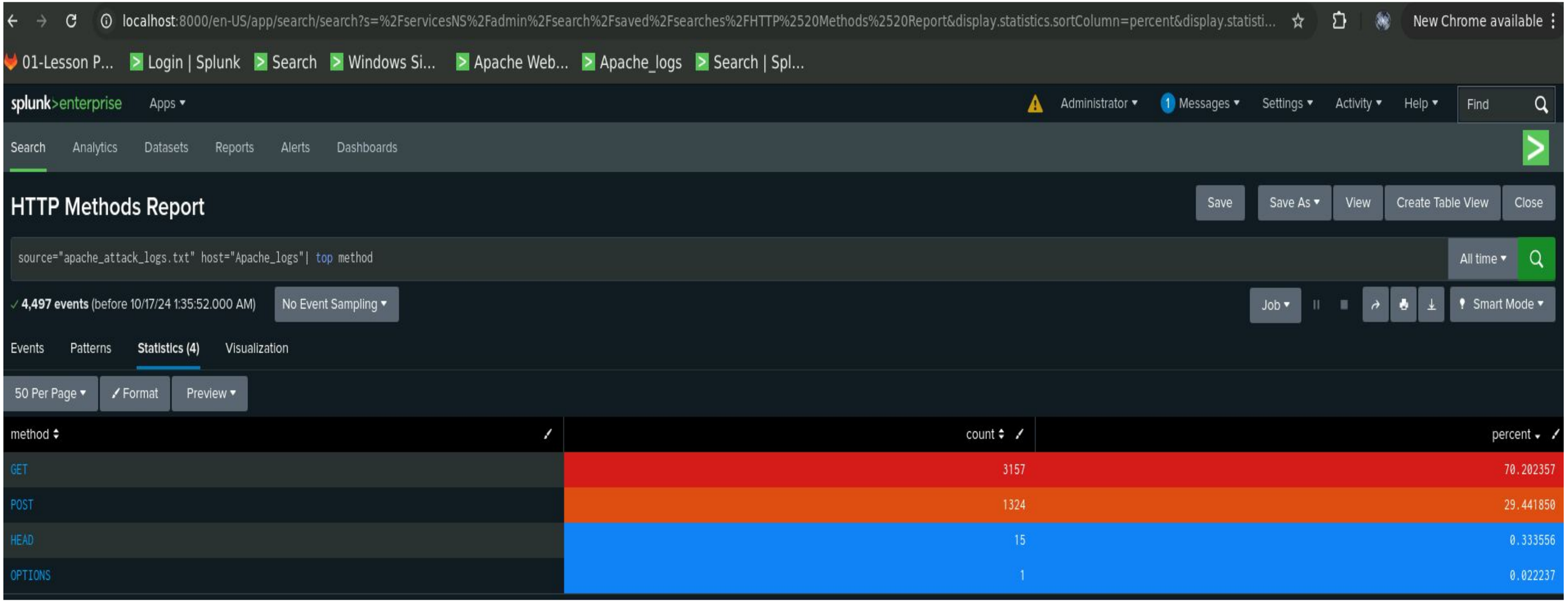
HTTP Methods: There was a sharp increase in POST requests, spiking to 1,296 between 8 p.m. and 9 p.m. This indicates attempts to upload data or exploit vulnerabilities through POST methods, which are commonly used for sending data to the server.

Response Codes: The sharp rise in 404 errors, jumping from 2% to 15%, suggests that attackers were scanning the server for vulnerable or non-existent files. This activity was likely aimed at identifying weaknesses in the server's structure.

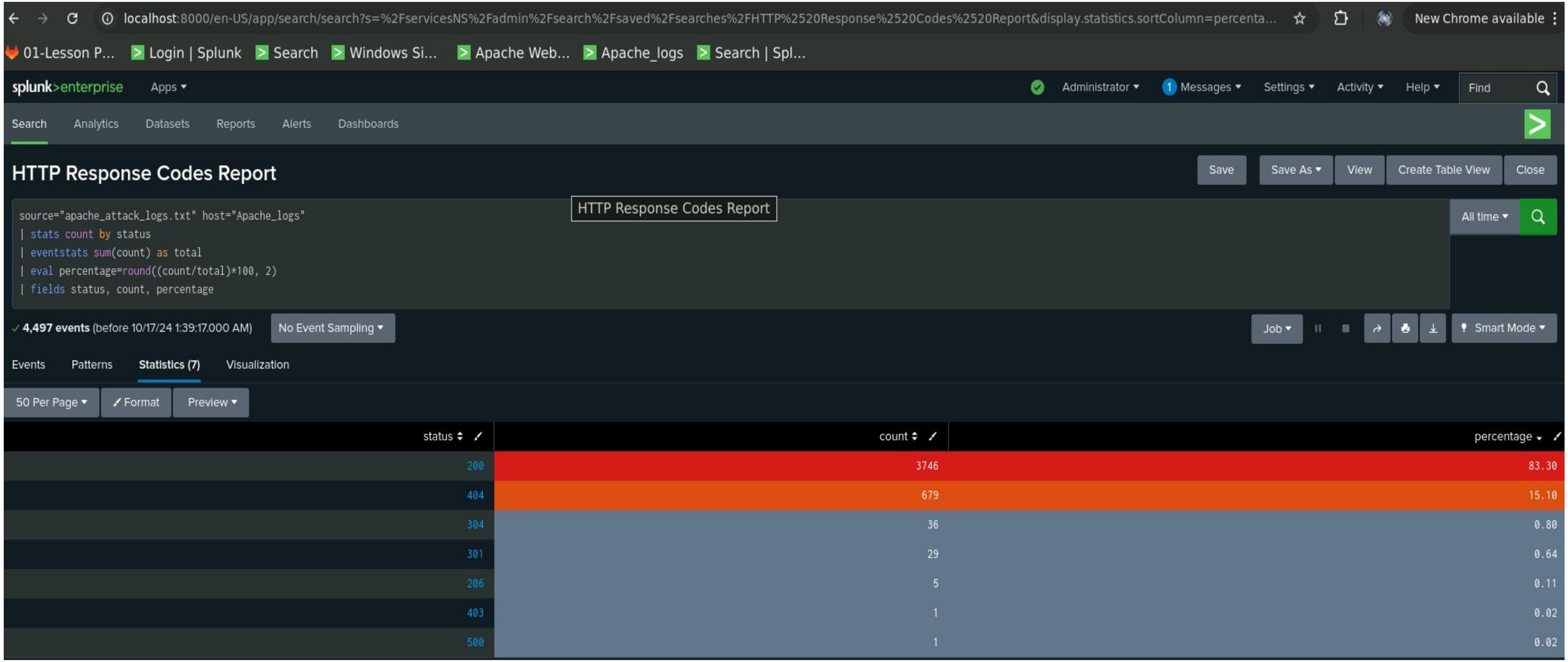
International Activity: A notable surge in traffic from Ukraine (937 events in one hour) was detected. This increase raises concerns about a coordinated attack from this region, possibly involving compromised systems.

Suspicious URI Access: A large volume of requests to the /VSI_Account_logon.php URI was observed. This is likely an attempt to brute force login credentials or exploit vulnerabilities in the authentication system.

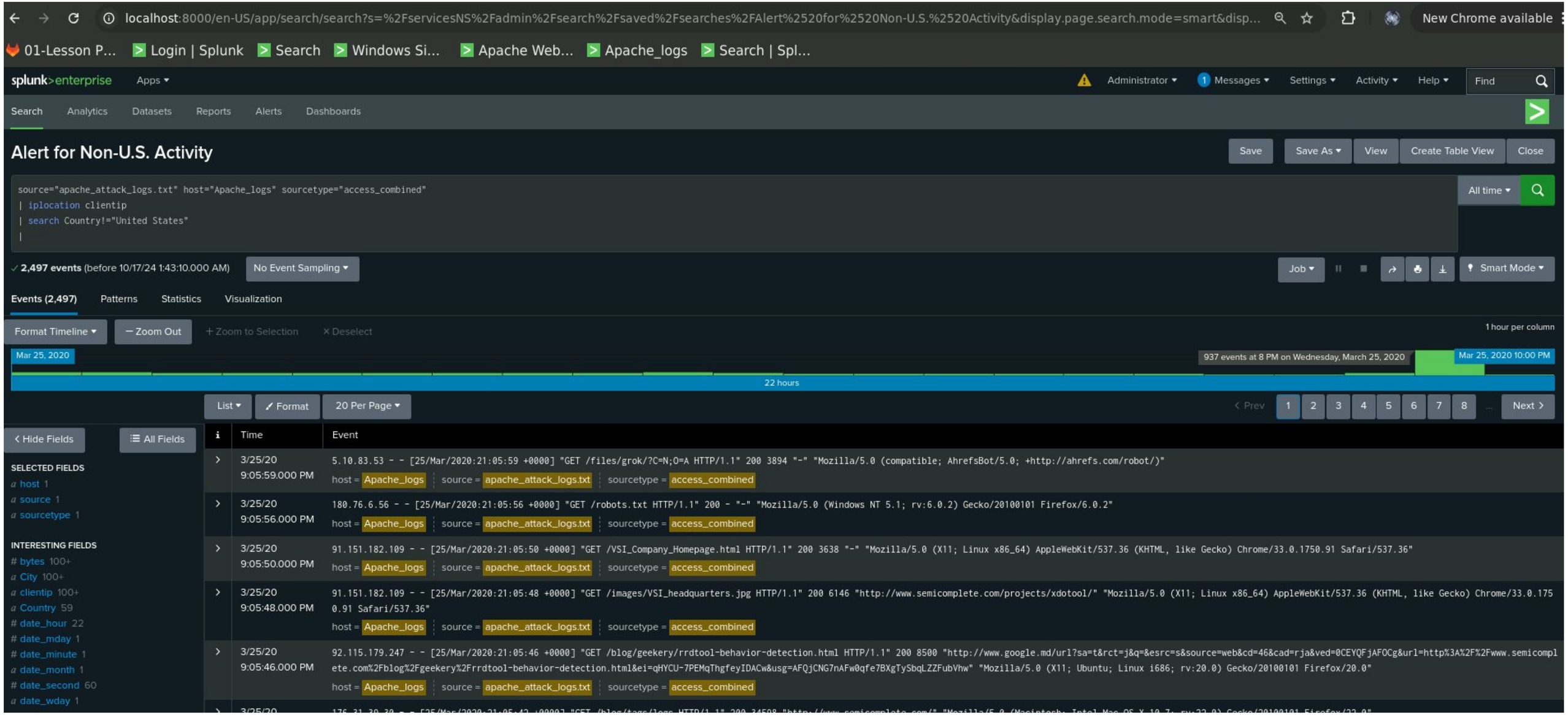
Screenshots of Attack Logs - HTTP Methods



Screenshots of Attack Logs - Response Codes



Screenshots of Attack Logs - Non-US Activity



Summary and Future Mitigations

Project 3 Summary - Overall Findings:

The attack on VSI involved coordinated attempts to exploit vulnerabilities in both Windows and Apache systems. The key findings included:

- A sharp increase in **HTTP POST** requests, which are often used to upload files or send data, indicating potential exploitation or file upload attacks.
- A notable rise in **404 error codes**, suggesting that attackers were scanning the server for non-existent or vulnerable files.
- **Suspicious login activities** in the Windows environment, particularly by a few users, suggesting credential compromise or insider threats.
- Increased international traffic from Ukraine, pointing to possible external, coordinated attacks.

Project 3 Summary - Future Mitigations:

To protect VSI from future attacks, I recommend:

- **Implementing rate limiting**, **CAPTCHA** or **MFA** mechanisms to reduce brute-force login attempts and limit the number of POST requests per user.
- **Strengthening input validation** and securing file upload mechanisms to prevent malicious data being uploaded through POST requests.
- **Geo-blocking** high-risk regions and monitoring international traffic more closely.
- **Enhancing logging and monitoring** to detect abnormal behaviour sooner, including user login patterns and system access attempts.
- Regular **vulnerability scans** and **penetration testing** to uncover potential weak points before attackers do.