Security Monitoring at VSI

By: Erick Almaraz

Role: SOC Analyst at VSI

01

VSI

Virtual Space Industries (VSI) is a company that develops virtual reality programs for businesses. VSI suspects that their competitor, JobeCorp, is launching cyber attacks to disrupt VSI's business.

02

GOAL

As a SOC analyst, my key role was to utilize Splunk to monitor two key assets:

The Apache web server hosting the admin portal & the Windows system handling back-end operations.

03

SERVICES

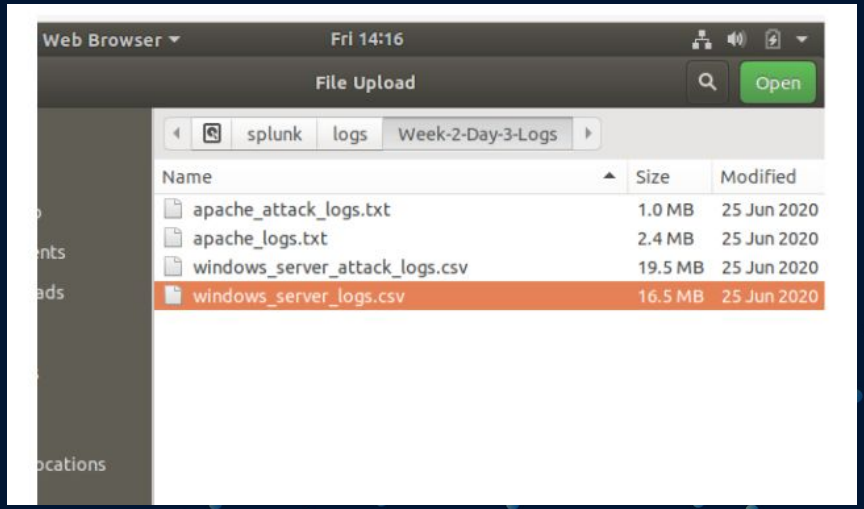
Using historical logs provided by the networking team, I:

- Created activity baselines.
- Built reports to track suspicious behavior.
- Set up alerts for potential threats.
- Designed dashboards for real-time monitoring and response.

Backend Systems Analysis:

Windows & Apache Logs

I collected log data from two main sources: Windows logs from backend systems containing critical IP information, and Apache logs from the public-facing website, using the files: ***windows_server_logs.csv***, ***windows_server_attack_logs.csv,*** ***apache_logs.txt*****, and *apache_attack_logs.txt***.



Windows Logs Analysis: Reports

Three reports were created for the Windows Log:

A report showing Signatures with their matching Signature ID's, allowing VSI to track Windows activity by signature.

A report showing Severity levels along with the count and percentage for each

And a report comparing Successful and Failed Windows Activities

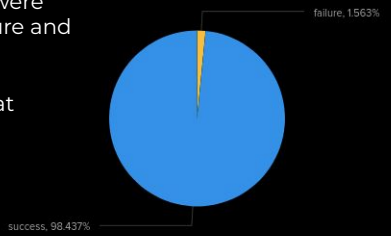
Signature& Signature ID Report

signature	signature_id
A computer account was deleted	4743
A logon was attempted using explicit credentials	4648
A privileged service was called	4673
A process has exited	4689
A user account was changed	4738
A user account was created	4720
A user account was deleted	4726
A user account was locked out	4740
An account was successfully logged on	4624
An attempt was made to reset an accounts password	4724
Domain Policy was changed	4739
Special privileges assigned to new logon	4672
System security access was granted to an account	4717
System security access was removed from an account	4718
The audit log was cleared	1102

Success & Failure of (Normal) Windows Activities

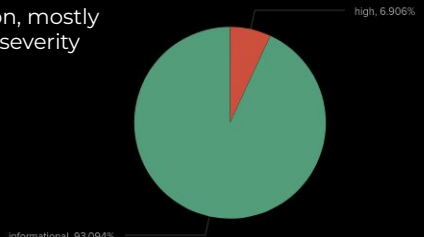
The majority of login activities were successful, with normal signature and user activity patterns.

With a low rate of failed logins at 2.98%.



Severity Level (Normal Activity) Report

Expected severity distribution, mostly low to medium, with a high severity level of 6.9%



Windows Log Alerts

Alerts were designed to notify VSI of suspicious activity

First, I analyzed the Hourly Failed Windows Activity to establish a normal baseline, then set a threshold to flag deviations for further investigation.

Hourly Failed Windows Activity

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" status="failure" | bin _time span=1h | stats count by _time | where count > 10
```

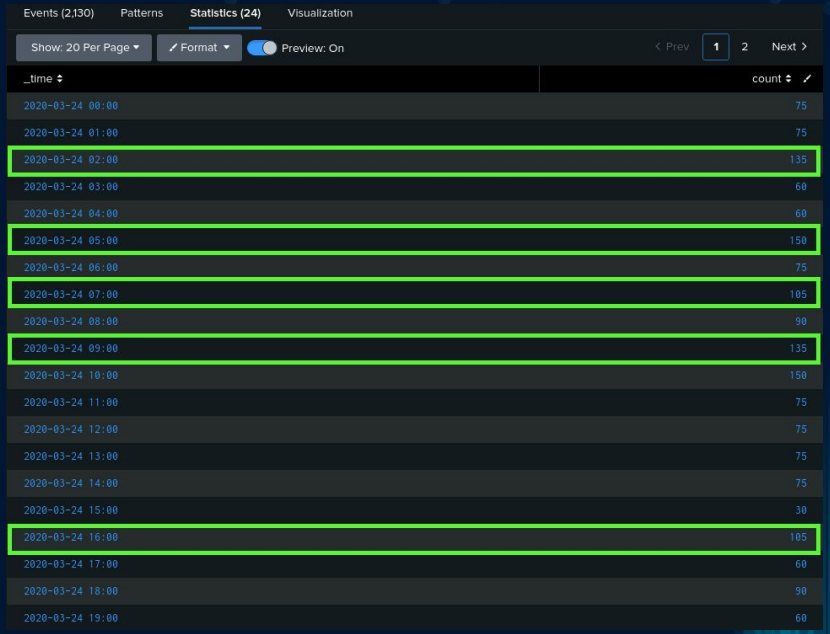
✓ **2,130 events** (before 5/16/25 4:39:18.000 PM) No Event Sampling ▾

This query identifies hourly spikes in failed Windows activity by counting the number of failures per hour and highlighting any hour where failures exceed 10. It's used to detect unusual patterns that may signal brute-force attempts or other suspicious behavior.

According to the Data:

- The minimum count: 30
- The maximum count: 150
- The most common values: 60–90
- With several spikes at 105, 135, and 150

A safe baseline seemed to fall between **60–90 failures/hour**. To catch spikes, the alert threshold was set at **>105 failures/hour**. Setting the threshold at **105** would help avoid false positives from normal activity and still catch the more severe or unusual spikes.



Events (2,130) Patterns **Statistics (24)** Visualization

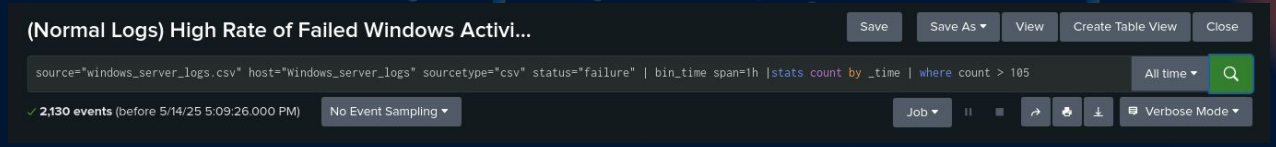
Show: 20 Per Page ▾ Format ▾ Preview: On ‹ Prev 1 2 Next ›

_time	count
2020-03-24 00:00	75
2020-03-24 01:00	75
2020-03-24 02:00	135
2020-03-24 03:00	60
2020-03-24 04:00	60
2020-03-24 05:00	150
2020-03-24 06:00	75
2020-03-24 07:00	105
2020-03-24 08:00	90
2020-03-24 09:00	135
2020-03-24 10:00	150
2020-03-24 11:00	75
2020-03-24 12:00	75
2020-03-24 13:00	75
2020-03-24 14:00	75
2020-03-24 15:00	30
2020-03-24 16:00	105
2020-03-24 17:00	60
2020-03-24 18:00	90
2020-03-24 19:00	60

Alerts

Results of the updated threshold

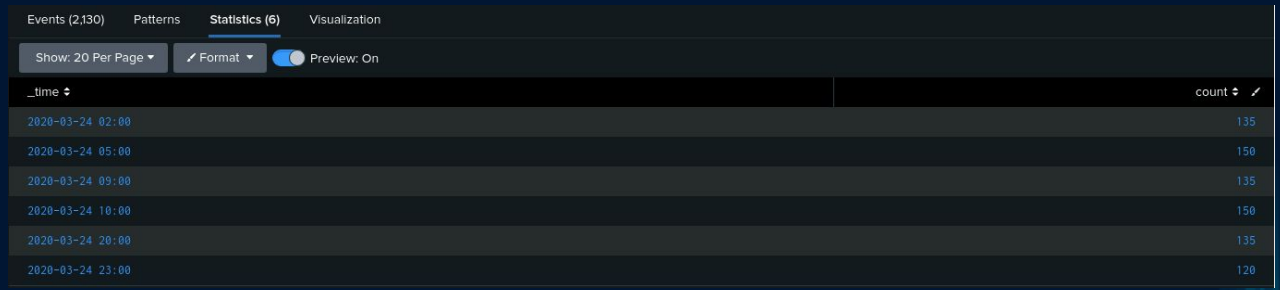
After determining the baseline (between 60-90,) the threshold was set at **>105 failures/hour** to narrow down the spikes.



Results

On March 24th, 2020 spikes in High Rate of Failed Windows Activity were identified:

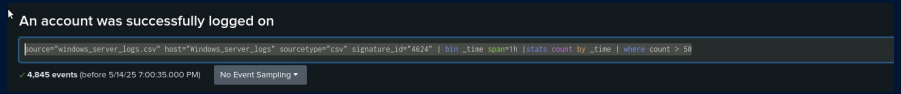
- At 2:00 am, 135 failures/hour
- At 5:00 am, 150 failures/hour
- At 9:00 am, 135 failure/hour
- At 10:00 am, 150 failures/hour
- At 8:00 pm, 135 failures/hour
- At 11:00 pm, 120 failures/hour



Alerts

Alert for Successful Login Activity

A second alert was created to monitor the hourly count of the **'An account was successfully logged on'** event, established a baseline of normal activity and set a threshold to identify abnormal spikes that could indicate potential unauthorized access.



This SPL query searches for Windows logon events (Event ID 4624)/**'An account was successfully logged on'** from a CSV log source, aggregates the number of events per hour, and filters the results to show only the hours where the count exceeds 50.

According to the data:

- The minimum count: 120
- The maximum count: 315
- The most common values: 180–225
- With several spikes at 255, 270, and 315

A safe baseline seemed to fall between 180–225 successful logins per hour. To catch spikes, the alert threshold was set at **>225 logins/hour.** Setting the threshold at 250 helps reduce false positives and help indicate potential **account compromise, brute-force success, or lateral movement**.

_time	count
2020-03-24 00:00	165
2020-03-24 01:00	195
2020-03-24 02:00	225
2020-03-24 03:00	210
2020-03-24 04:00	270
2020-03-24 05:00	195
2020-03-24 06:00	120
2020-03-24 07:00	180
2020-03-24 08:00	270
2020-03-24 09:00	180
2020-03-24 10:00	135
2020-03-24 11:00	240
2020-03-24 12:00	210
2020-03-24 13:00	195
2020-03-24 14:00	195
2020-03-24 15:00	255
2020-03-24 16:00	225
2020-03-24 17:00	195
2020-03-24 18:00	180
2020-03-24 19:00	315

Alerts

Results of the updated threshold

After determining the baseline (between 180–225.) To catch spikes, the alert threshold was set at >225 logins/hour. This would help reduce false positives while still detecting unusually high login activity that may indicate suspicious behavior.

An account was successfully logged on

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" signature_id="4624" | bin _time span=1h |stats count by _time | where count > 225
```

✓ **4,845 events** (before 5/15/25 5:25:42.000 PM) No Event Sampling ▾

_time	count
2020-03-24 04:00	270
2020-03-24 08:00	270
2020-03-24 11:00	240
2020-03-24 15:00	255
2020-03-24 19:00	315

Results: Successful Logins

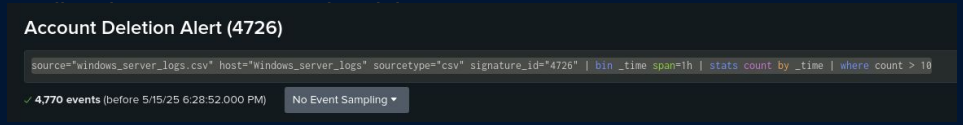
On March 24th, 2020 spikes in High Rate of Failed Windows Activity were identified:

- At 4:00 am 270 logins/hour
- At 8:00 am 270 logins/hour
- At 11:00 am 240 logins/hour
- At 3:00 pm 255 logins/hour
- At 7:00 pm 315 logins/hour

Windows Log Alerts

Alerts were designed to notify VSI of suspicious activity

Lastly, I designed an alert after determining a baseline and threshold for the hourly count of the signature 'A user account was deleted' to detect potential



This query is designed to **monitor spikes** in account deletion events, which could indicate suspicious or malicious behavior (e.g., insider threat, attack in progress). The results help determine when activity exceeds a normal threshold (10)and may need an alert.

According to the Data:

- **Minimum count:** 105
- **Maximum count:** 330
  Most common values: 150–255
- **Notable spikes:** 285, 315, 330

Based on this pattern, a **safe baseline** appears to fall between **150–255 deletions per hour**.

To detect **unusual or excessive account deletion activity**, the **alert threshold** was set at **>255 deletions/hour**.

_time	count
2020-03-24 00:00	195
2020-03-24 01:00	150
2020-03-24 02:00	225
2020-03-24 03:00	255
2020-03-24 04:00	135
2020-03-24 05:00	150
2020-03-24 06:00	150
2020-03-24 07:00	255
2020-03-24 08:00	240
2020-03-24 09:00	210
2020-03-24 10:00	240
2020-03-24 11:00	330
2020-03-24 12:00	165
2020-03-24 13:00	315
2020-03-24 14:00	135
2020-03-24 15:00	285
2020-03-24 16:00	105
2020-03-24 17:00	105
2020-03-24 18:00	255
2020-03-24 19:00	195

Alerts

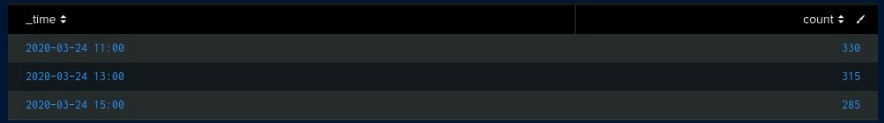
Results of the updated threshold

After determining the baseline (between 150-255,) the threshold was set at **>250 deletions/hour** to narrow down the spikes.

Results

On March 24th, 2020 spikes in High Rate of Failed Windows Activity were identified:

- At 11:00 am 330 accounts were deleted
- At 1:00 pm 315 accounts were deleted
- At 3:00 pm 285 accounts were deleted

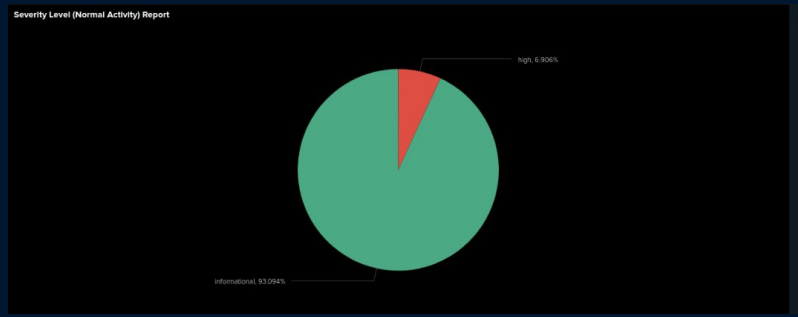


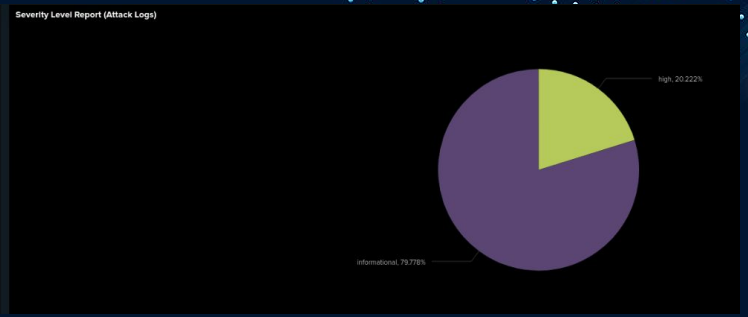
_time	count
2020-03-24 11:00	330
2020-03-24 13:00	315
2020-03-24 15:00	285

Dashboard Overview

Windows Attack Log Analysis

Severity Report





High Severity Logs Results

- On the **attack day**, high severity events triple in proportion **(from 6.91% → 20.22%)**
- This spike in severity, despite fewer total logs, is a red flag and strongly suggests **malicious or disruptive activity**

Log Volume

- While the **normal day** has **13x** more logs, most are low-risk ("informational").
- The **attack day** has far fewer logs, but **every fifth event is high severity**, which increases its operational risk profile.

Severity	Normal Day (3/24)	Attack Day (3/25)
High	4,935 (6.91%)	1,111 (20.22%)
Informational	66,525 (93.09%)	4,383 (79.78%)
Total Logs	**71,460**	**5,494**

Windows Attack Log Analysis

Hourly Failed Activity Report

Baseline Comparison
From the normal day (Mar 24):

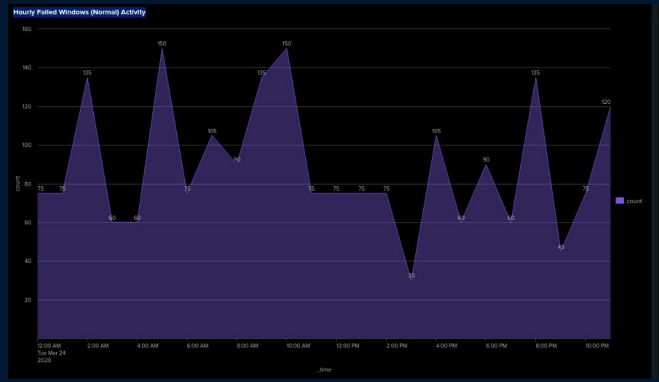
- Average = 79.5 failures/hour
- Standard Deviation = 31.45
- Normal Threshold = ~48–111 failures/hour

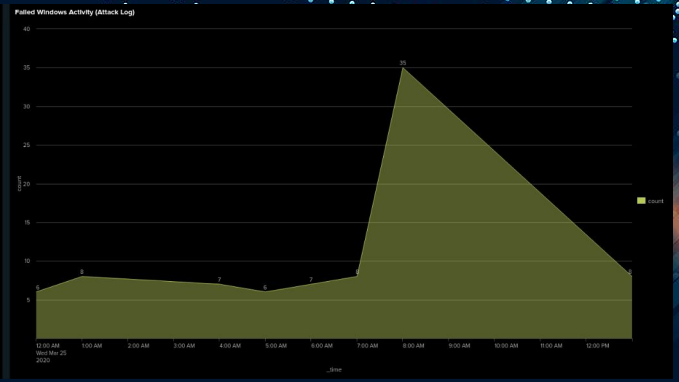
The attack day shows lower overall hourly counts but:

08:00 am shows a significant spike to 35 failures, which:
Is still below the baseline threshold from the normal day, but stands out against other hours on the attack day, where failures averaged between 6–8.

This may indicate:

- A low-and-slow attack pattern (deliberately keeping activity under detection thresholds)
- A targeted brute-force attempt spiking only during one hour





Metric	Normal Day (3/24)	Attack Day (3/25)
Average Failures/Hour	79.5	~10.6 (avg of 8 nonzero hours)
Peak Failures (Hour)	150	35
Hours Over Anomaly Threshold (~111)	4	0
Pattern Type	Repeated spikes hourly	Sparse, with one spike

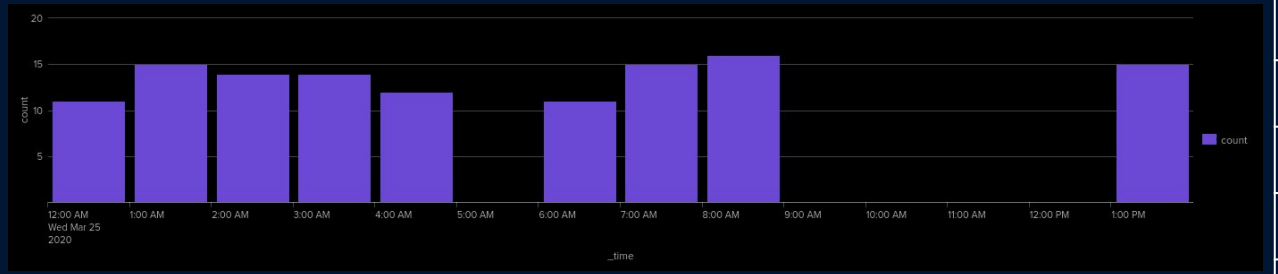
Attack Log Alerts Analysis

Successful Login Alert Analysis

An account was successfully logged on (attack Logs)

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature_id="4624" | bin _time span=1h |stats count by _time | where count > 10
```

✓ **140 events** (before 5/20/25 11:50:02.000 PM) No Event Sampling ▾



Hour	Count
00:00	11
01:00	15
02:00	14
03:00	14
04:00	12
05:00	9
06:00	11
07:00	15
08:00	16
13:00	15

On the **normal day**, successful logins were high-volume but followed a **regular and expected pattern**.

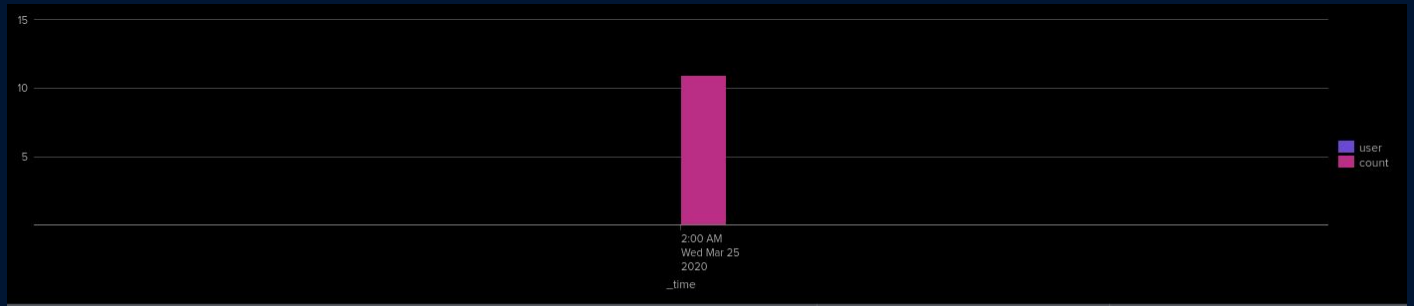
On the **attack day**, the **frequency of logins during off-hours** and their alignment with **previously failed attempts** suggest **unauthorized access**.

Recommendation: Investigate accounts active during attack day logins and consider implementing **MFA**, account lockout policies, or anomaly-based detection rules.

Alerts

Active users

After determining the frequency of logins during off-hours on the day of the attack I located the users most active during this period and found that User_a had attempted to log in a total of 11 times matching the 2 am spike



_time	user	count
2020-03-25 02:00:00	user_a	11

Attack Log Alerts Analysis

Account Deletion Alert Analysis

On the normal day of March 24, 2020, account deletions occurred in high-volume bursts during specific hours, exceeding 255 deletions per hour, indicating scheduled administrative maintenance activities.

- 11:00 - 330 deletions
- 13:00 - 315 deletions
- 15:00 - 285 deletions

The large spikes in deletions suggest planned administrative activity, likely scheduled user cleanup or deprovisioning by authorized personnel.

According to the Data:

The account deletion alerts on the attack day **(March 25, 2020)** show consistent activity across multiple hours with moderate volume, indicating unauthorized or suspicious behavior possibly aimed at covering tracks or disrupting access.

- 13 distinct hours with deletion events
- Highest: 17 deletions at 05:00
- Others range from 1 to 14 deletions/hr
- The deletion volume is lower per hour but persistent and frequent (potential red flag.)
- Indicating **stealthy malicious behavior**, likely trying to avoid detection by:
    - Deleting accounts gradually
    - Possibly removing compromised accounts or covering attacker traces

2020-03-25 Time	Deletions
00:00	14
01:00	7
02:00	5
03:00	9
04:00	14
05:00	17
06:00	13
07:00	11
08:00	11
09:00	3
11:00	1
12:00	13
13:00	13

Apache Logs Analysis: Reports

Three reports were created for the Apache Log:

A report that displays a breakdown of **HTTP methods** used, helping identify the types of requests made to

method	count
GET	9851
POST	106
HEAD	42
OPTIONS	1

A report showing highlighting the top **10 referring domains** to help identify potentially suspicious traffic sources to VSI's website.

referer_domain	count
http://www.semicomplete.com	3038
http://semicomplete.com	2001
http://www.google.com	123
https://www.google.com	105
http://stackoverflow.com	34
http://www.google.fr	31
http://s-chassis.co.nz	29
http://logstash.net	28
http://www.google.es	25
https://www.google.co.uk	23

And a report summarizes the count of each **HTTP response** code to help detect unusual or suspicious server activity.

status	count
200	9126
304	445
404	213
301	164
206	45
500	3
403	2
416	2

Apache Log Alerts

Alerts were designed to notify VSI of suspicious activity

First, I analyzed the hourly activity from any country besides the United States to establish a normal baseline, then set a threshold to flag deviations for further investigation.

Non-US Activity Spike

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | iplocation clientip | search Country!= "United States" | bin _time span=1h | stats count by _time | where count > 100
```

✓ **6,140 events** (before 5/22/25 7:27:30.000 PM) | No Event Sampling

_time	count
2020-03-19 06:00	102
2020-03-19 08:00	108
2020-03-19 11:00	106
2020-03-19 18:00	108
2020-03-19 19:00	113
2020-03-19 23:00	111
2020-03-20 00:00	120
2020-03-20 01:00	108
2020-03-20 09:00	107

This query monitors hourly traffic from countries outside the U.S. and flags any 1-hour window with over 100 such requests — useful for detecting unusual foreign activity or potential attacks.

According to the Data:

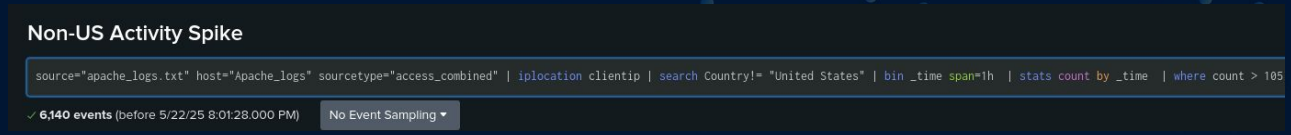
- **The minimum count:** 102
- **The maximum count:** 120
- **The most common values:** 106–113
  With several spikes at: 113, 120

A safe baseline appeared to fall between 100–110 non-U.S. requests per hour. To catch spikes, the alert threshold was set at >105 requests/hour. This threshold helps reduce false positives from normal international traffic while still detecting unusual surges in activity.

Alerts

Results of the updated threshold

After determining the baseline (between 100-110,) the threshold was set at **>105 requests/hour** to narrow down the spikes.



Results

- **Consistently High Activity:**
  Every hour had more than 105 requests, ranging from 106 to 120.
- **Peak Traffic Time:**
  The highest traffic was at 12:00 AM on March 20, with 120 requests.
- **Ongoing Pattern:**
  Elevated traffic happened across 8 different hours — not just once.
- **Repeated Volumes:**
  The number 108 appeared three times, showing steady high traffic.

_time	count
2020-03-19 08:00	108
2020-03-19 11:00	106
2020-03-19 18:00	108
2020-03-19 19:00	113
2020-03-19 23:00	111
2020-03-20 00:00	120
2020-03-20 01:00	108
2020-03-20 09:00	107

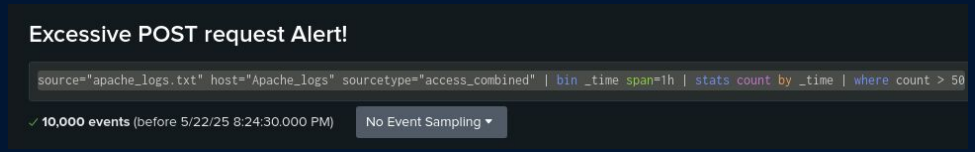
Security Implications:

- The **volume and persistence** of elevated foreign traffic suggest potential **reconnaissance, automated scanning, or bot activity**.
- No sharp dips to baseline were observed, implying either **sustained interest** or **scripted access** attempts from outside the U.S.

Apache Log Alerts

Alerts were designed to notify VSI of suspicious activity

Then analyze the **hourly count of HTTP POST methods** and determine an appropriate **baseline and threshold** for alerting



This query identifies **time periods (hourly)** when the Apache server received **more than 50 requests**, helping detect periods of high traffic or potential suspicious activity.

According to the Data:

- The minimum count: 74
- The maximum count: 129
- The most common values: 115–125

With an outlier at: 74 (at 10:00 AM on March 17)

A safe baseline appeared to fall between 110–125 POST requests per hour. To catch abnormal spikes, the alert threshold was set at >125 requests/hour. This threshold avoids false positives from typical traffic while still detecting potential POST-based attacks or unusual upload activity.

_time	count
2020-03-17 10:00	74
2020-03-17 11:00	111
2020-03-17 12:00	115
2020-03-17 13:00	118
2020-03-17 14:00	120
2020-03-17 15:00	125
2020-03-17 16:00	126
2020-03-17 17:00	123
2020-03-17 18:00	118
2020-03-17 19:00	121
2020-03-17 20:00	129
2020-03-17 21:00	123
2020-03-17 22:00	118
2020-03-17 23:00	111
2020-03-18 00:00	116
2020-03-18 01:00	118
2020-03-18 02:00	125
2020-03-18 03:00	114
2020-03-18 04:00	115
2020-03-18 05:00	125

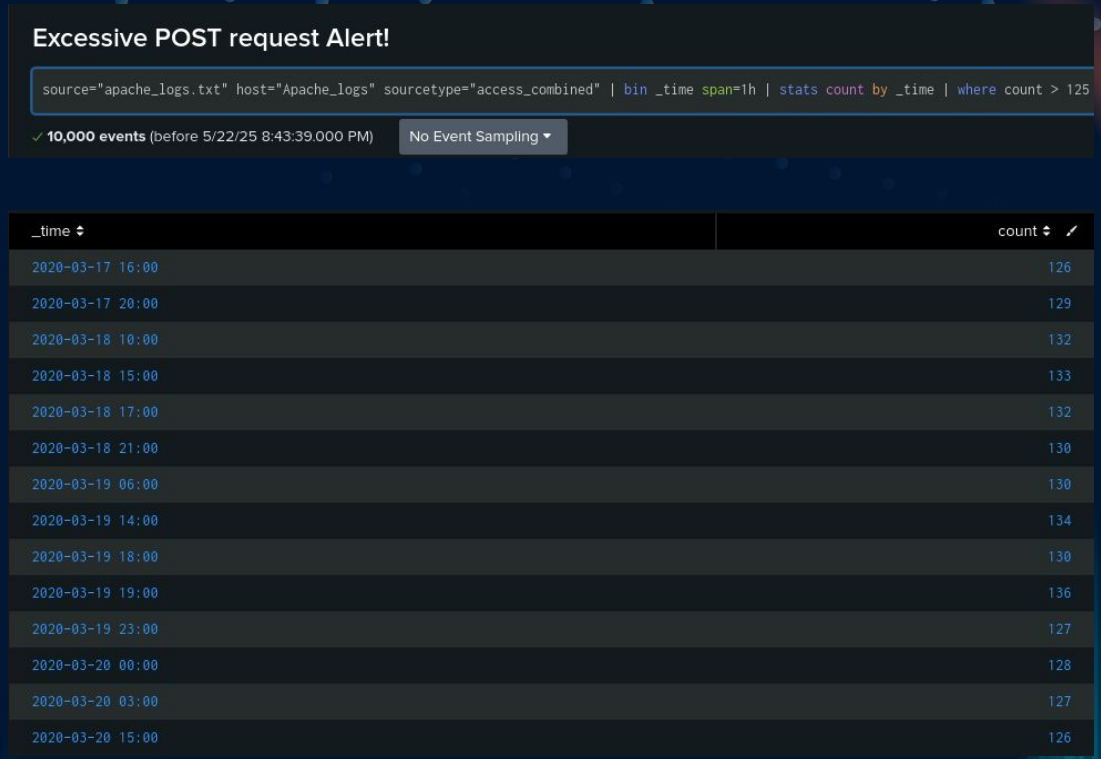
Alerts

Results of the updated threshold

After determining the baseline (between 115-125,) the threshold was set at **>125 requests/hour** to narrow down the spikes.

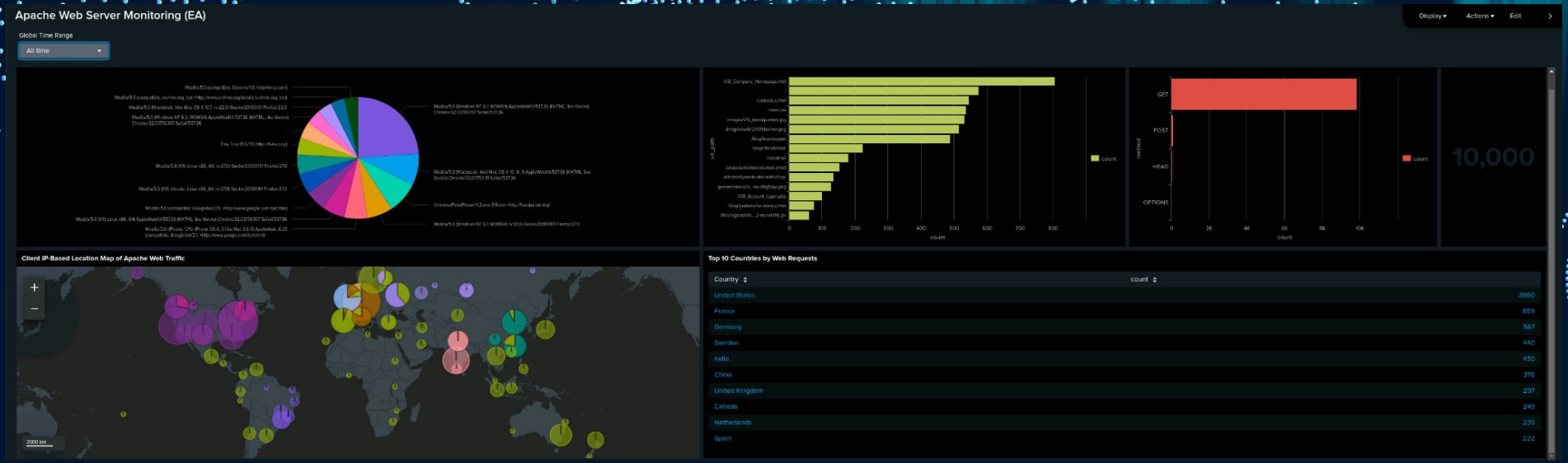
Results

- **Consistently High POST Activity:** Multiple hours across several days recorded POST request counts exceeding 125, ranging from 126 to 136.
- **Peak Traffic Times:** The highest spikes occurred at 7:00 PM on March 19 (136 requests) and 2:00 PM on March 19 (134 requests).
- **Ongoing Pattern:** Elevated POST traffic was observed repeatedly over 14 different hours, indicating sustained activity rather than isolated events.
- **Potential Security Risk:** This repeated high POST volume suggests possible automated attacks such as brute-force attempts, data uploads, or exploitation of vulnerabilities.



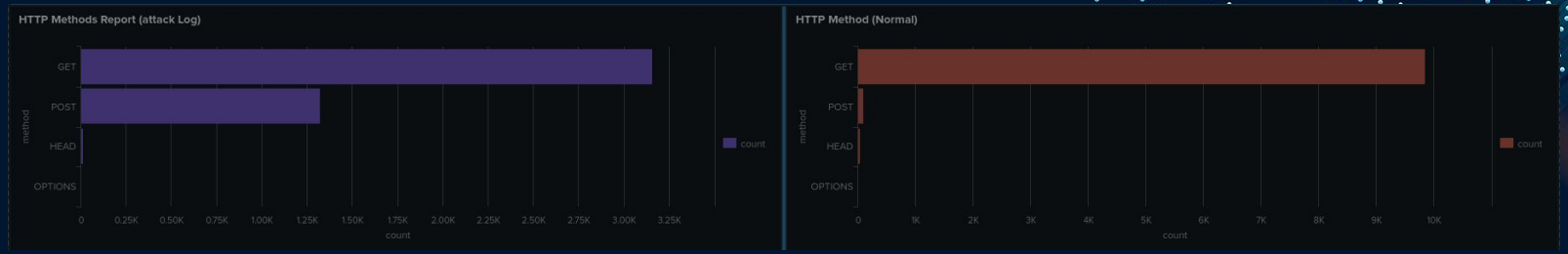
_time	count
2020-03-17 16:00	126
2020-03-17 20:00	129
2020-03-18 10:00	132
2020-03-18 15:00	133
2020-03-18 17:00	132
2020-03-18 21:00	130
2020-03-19 06:00	130
2020-03-19 14:00	134
2020-03-19 18:00	130
2020-03-19 19:00	136
2020-03-19 23:00	127
2020-03-20 00:00	128
2020-03-20 03:00	127
2020-03-20 15:00	126

Dashboard Overview



Apache Attack Log Analysis

HTTP Methods Report



Interpretation:

- **GET requests** dropped during the attack but were still the most common, showing attackers blended in with normal traffic.
- **POST requests** jumped from **106** to **1,324** — a **12x increase**. This likely points to exploit attempts using forms, uploads, or command injection methods.

HTTP Method	Normal Logs	Attack Logs	Observation
GET	9,851	3,157	Significant drop in attacks, but still dominant
POST	106	1,324	Large spike during attacks
HEAD	42	15	Slight drop
OPTIONS	1	1	No change

This behavior suggests:

- A targeted attack leveraging **POST-based methods**, possibly indicating:
  - **Credential stuffing**, brute-force login attempts
  - **Injection attacks** or abuse of web application functionality
- The **unusual volume of POST requests** clearly stands out against the baseline and should be used to **trigger alerts** when exceeding normal activity thresholds (>150 POSTs/hour.)

Apache Attack Log Analysis

Results for Top Referring Domains

Normal Day (Mar 24)

- The server got a lot of traffic from **external sites**, mostly from: **www.semicomplete.com** (3,038 times), semicomplete.com (2,001 times)

Attack Day

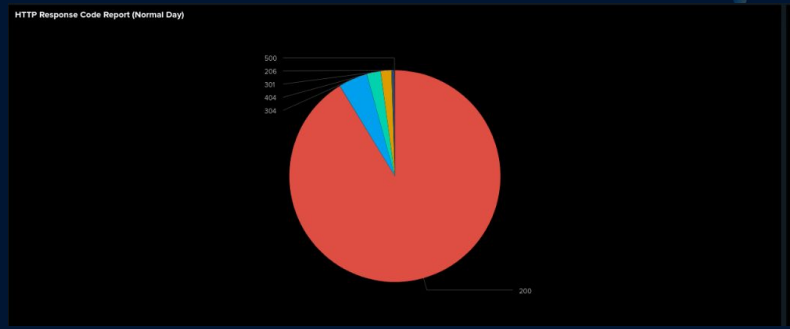
- These same domains **still appear**, but the counts are **much lower**. **www.semicomplete.com** dropped from 3,038 to just 764. Google referrals dropped too.

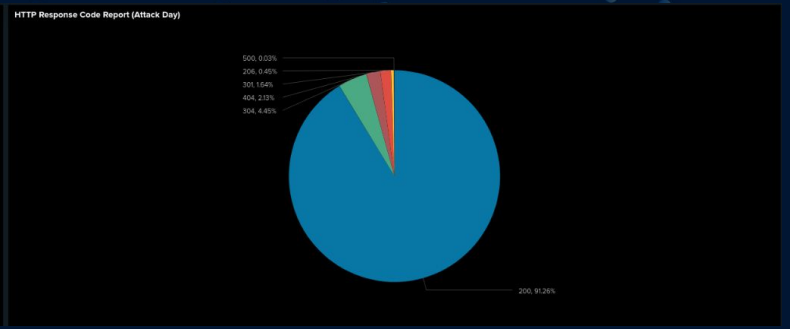
The attackers didn't use normal websites to reach the server. Instead, they likely used **scripts or bots** that send requests **directly** to your server bypassing referrer links. This pattern — low referrer count + traffic spike suggests **automated attack behavior**, not real users browsing.

Referrer Domain	Normal Day	Attack Day
http://www.semicomplete.com	3,038	764
http://semicomplete.com	2,001	572
http://www.google.com	123	37
https://www.google.com	105	25
http://stackoverflow.com	34	15
http://logstash.net	28	6
https://www.google.co.uk	23	6

Attack Log Analysis

Report Analysis for HTTP Response Codes





Normal Day (Mar 24)

The server mostly returned successful responses (like 200 OK), with some normal caching activity (304, 206) and very few errors (404, 500, 403).

Attack Day

Request patterns shifted dramatically:

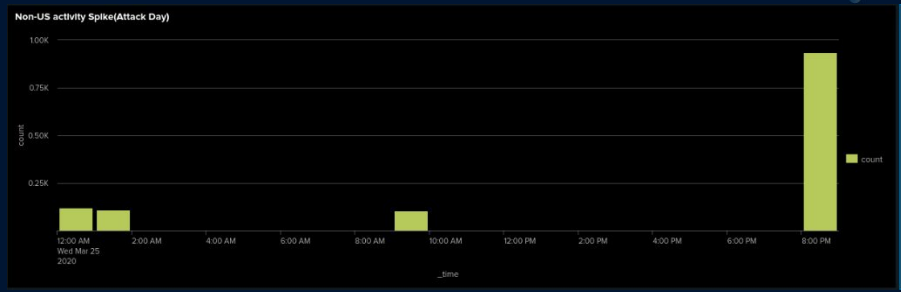
- On the attack day, 200 OK responses dropped from **9,126 to 3,746,** indicating fewer valid sessions; 404 errors tripled from **213 to 679**, suggesting repeated requests to invalid paths; 304 and 206 responses dramatically decreased, pointing to non-browser traffic; while other errors like 500 and 403 stayed low.

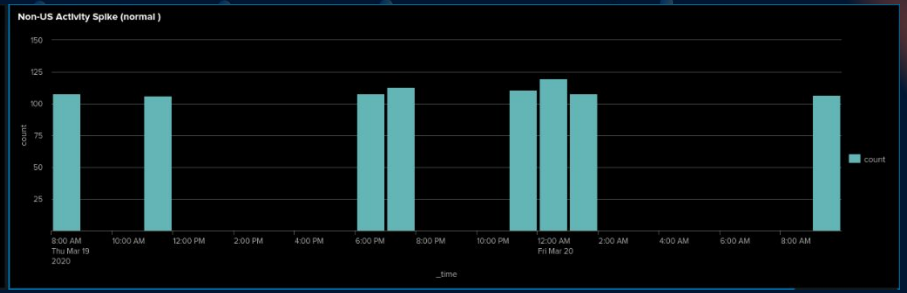
Attackers weren't browsing normally — the drop in 200 responses shows fewer valid page loads, while the spike in 404s suggests directory brute-forcing or path discovery. The low 304 and 206 activity indicates the traffic came from bots or scripts rather than real browsers, consistent with automated attacks scanning for vulnerabilities.

Status Code	Meaning	Normal Day	Attack Day
200	OK (successful requests)	9,126	3,746
304	Not Modified (cached)	445	36
404	Not Found	213	679
301	Moved Permanently (redirects)	164	29
206	Partial Content	45	5
500	Internal Server Error	3	1
403	Forbidden	2	1
416	Range Not Satisfiable	2	0

Alerts

Alert Analysis for International Activity (Foreign IP's)





Normal Day (Mar 19–20):

- Hourly traffic from outside the U.S. peaked between **106–120 requests/hour** This level of traffic occurred sporadically across different times of the day Suggesting typical international user activity.

Attack Day (Mar 25):

- Similar non-U.S. traffic levels appeared at **00:00, 01:00, and 09:00**, consistent with the normal day but at **20:00**, foreign traffic spiked dramatically to **937 requests/hour**

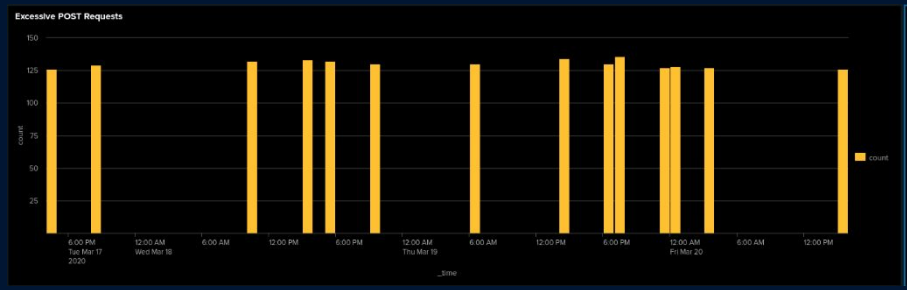
What This Means:

- The massive jump at 20:00 clearly deviates from normal patterns. This likely indicates **coordinated automated activity** from foreign sources — not typical user access. These spikes are red flags for **malicious scans, probing, or bot-driven attacks** targeting the server from outside the U.S.

Metric	Normal Day (Mar 19–20)	Attack Day (Mar 25)	Interpretation
Peak Requests/Hour	120	**937**	Major spike during attack — suggests automated probing or bot activity
Common High-Hour Range	106–120	106–120	Similar hourly values at some times (00:00, 01:00, 09:00) on both days
Number of High-Traffic Hours (>105)	8	4	Fewer spikes on attack day, but one extreme outlier
Anomalous Spike Hour	N/A	**20:00 (937 requests)**	Sudden surge far beyond baseline — likely malicious and not normal user access
Typical Pattern	Spread throughout day	Mostly clustered	Attack traffic was less spread out and more focused — typical of scripted runs

Attack Log Alerts Analysis

HTTP POST Method Alert Analysis



Normal Day (Mar 17–20):

POST requests occasionally exceeded 125 per hour, with peaks ranging from 126 to 136, suggesting legitimate high-usage activity such as form submissions or uploads.

Attack Day (Mar 25):

Early in the day, POST request peaks of 126–128 matched normal patterns, but later surged dramatically to 730 at 18:00 and 1,415 at 20:00.

Interpretation:
The spikes—5 to 11 times higher than normal—strongly suggest automated attacks involving exploits, file uploads, or command injections, and setting an alert at >136 POSTs/hour would catch these without flagging normal activity.

Metric	Normal Day (Mar 17–20)	Attack Day (Mar 25)	Interpretation
Normal POST Range	126–136 requests/hour	126–128 (early day)	Normal early activity matched typical usage patterns
Peak POST Activity	136 requests/hour	**1,415 requests/hour**	11x spike compared to baseline
Number of High-Traffic Hours (>125)	14	5	Fewer peaks overall, but much more extreme during attack
Major Anomalous Hours	None	**18:00 (730), 20:00 (1,415)**	Clear indicators of abnormal, likely automated POST exploitation attempts
Suggested Alert Threshold	>136	—	Captures abnormal POST spikes while ignoring standard user traffic