Defensive Solution Project on VSI

BY: HASSAN EVANS, DREW DICKENSON, CAMRON NEAL, HARSHINI LANKA

Monitoring Environment

- We are monitoring solutions to protect the VSI. There is a rumor that JobeCorp may lauch cyberattacks to disrupt VSI business. We went through logs and found where the attacks came from and we also have future mitigations to make sure these attacks don’t happen again.

Splunk App Add-On Unix and Linux

- The Splunk Add-on for Unix and Linux enables collection, parsing, and normalization of logs and system metrics from Unix and Linux servers for better monitoring and analysis in Splunk.

Windows Logs

Report Name	Report of Description
Status Window Log	Shows the comparison for the success and failure of window activities
Signature ID's Window Log	Table of signature id's ex.(An account was sucessfully logged on, A user account was changed, A user account was locked.)
Severity Levels Window logs	Informational means no action needed, general information and High means investigation or action needs to be taken

Window Log Report Images

Events | Patterns | **Statistics (2)** | Visualization

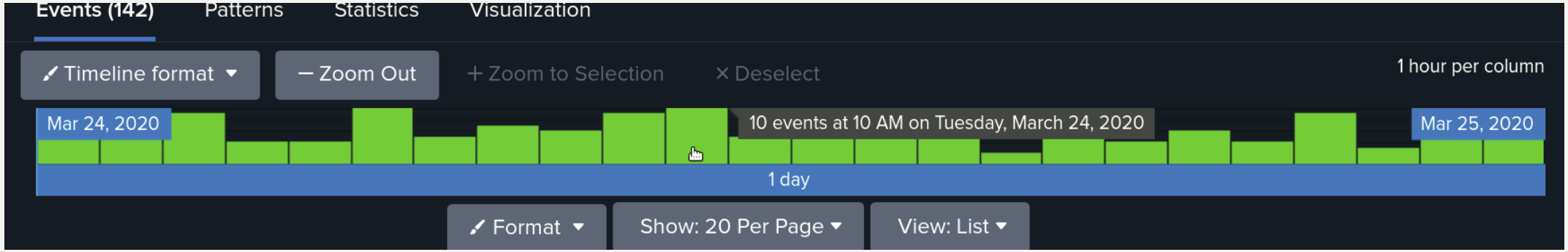
Show: 20 Per Page ▾ | Format ▾ | Preview: On

severity	count	percent
informational	4435	93.094039
high	329	6.905961

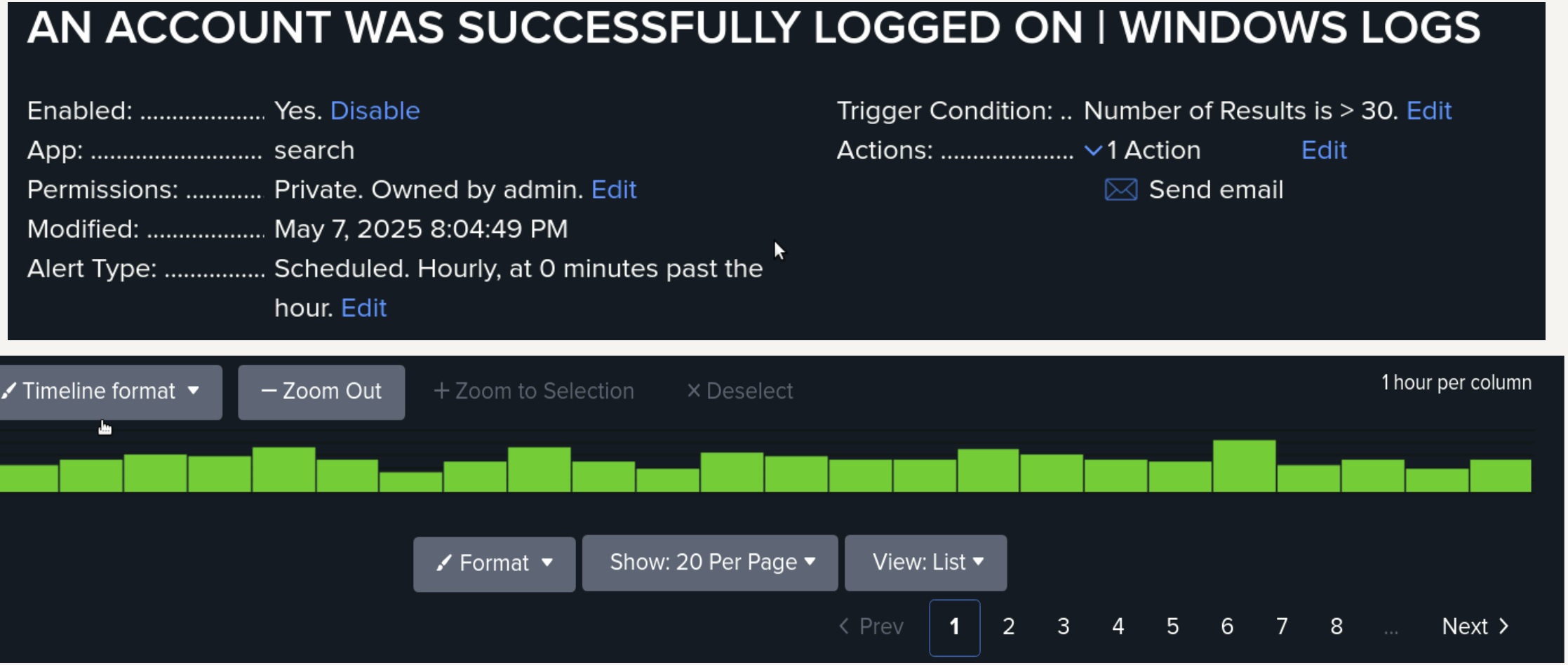
status	count	percent
success	4622	97.019312
failure	142	2.980688

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

Alerts Windows Logs



Alerts Window Logs

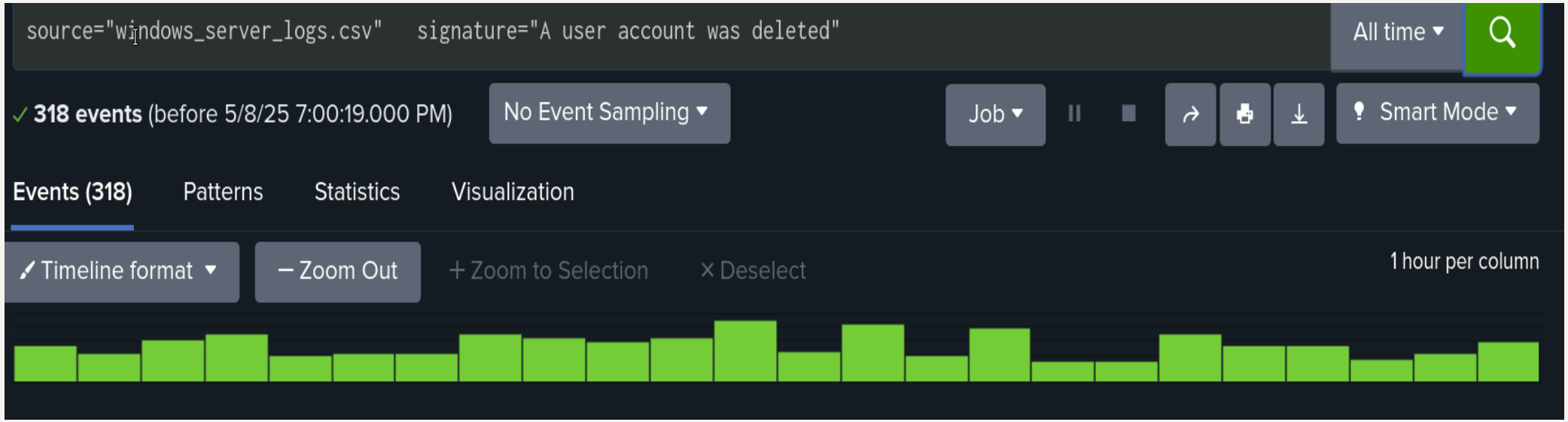


Alerts Window Logs

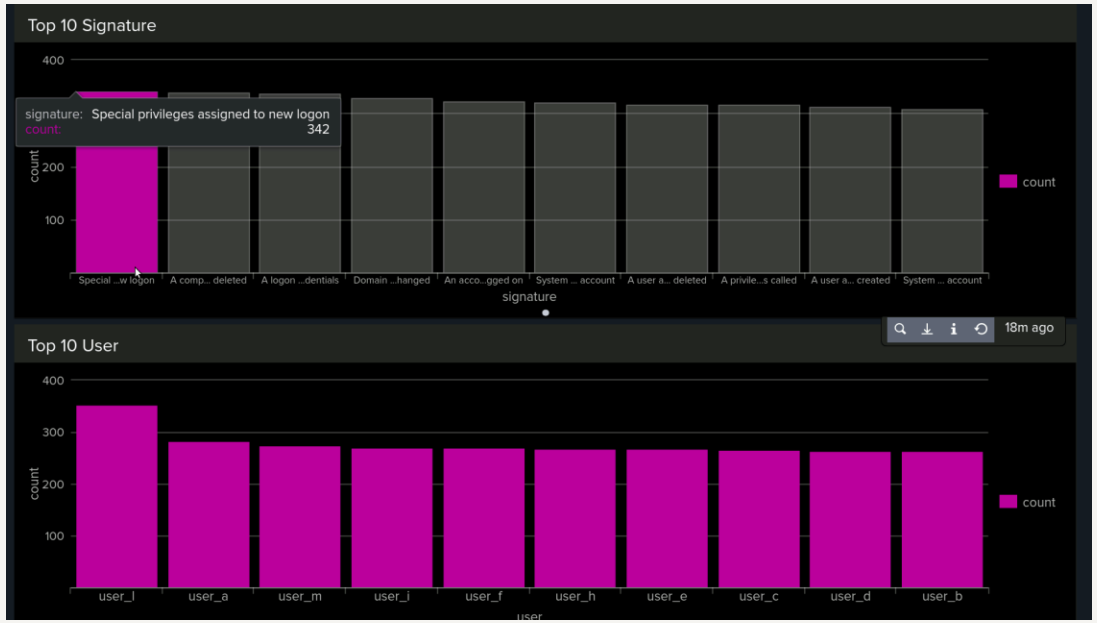
A USER ACCOUNT WAS DELETED | WINDOWS LOGS

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... May 7, 2025 8:04:20 PM
Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 50. Edit
Actions: ..... 1 Action Edit
Send email



Dashboard Windows Logs



Apache Logs

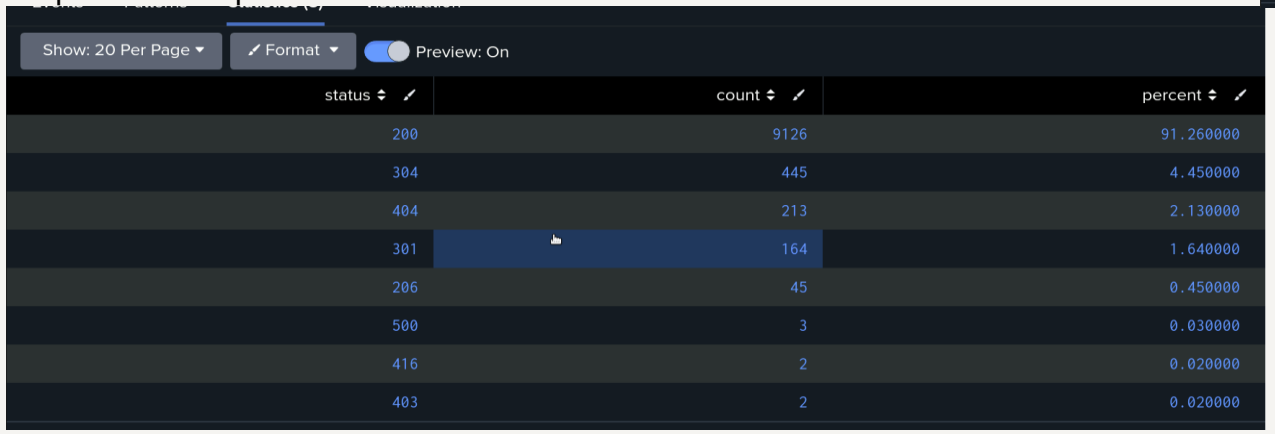
Report Name	Report Description
Apache Logs Method	Table that shows the different HTTP methods (GET,POST, HEAD, ETC)
Apache Logs Domains	Domain shows the most visited websites
Apache Logs Response Code	A report that shows the count of each HTTP response code.

Apache Logs

Apache Logs Method

Apache Top Domains

Apache Top Status



Apache Alerts

Apache_log_Alert_Method=post

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... May 7, 2025 3:20:01 AM
Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. Edit

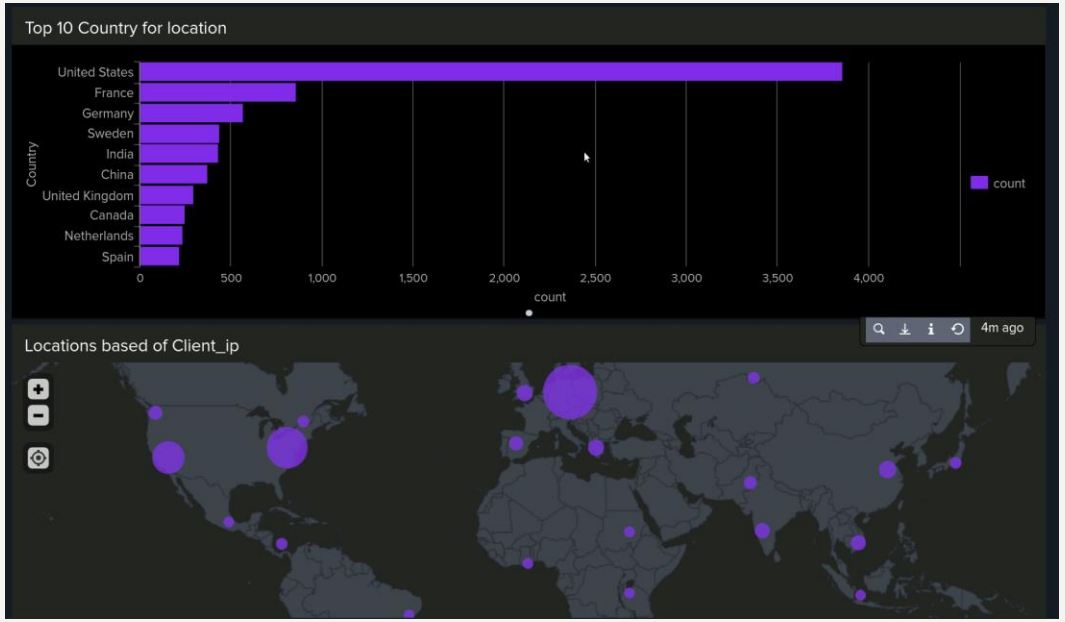
Trigger Condition: .. Number of Results is > 12. Edit
Actions: ..... 1 Action Edit
Send email

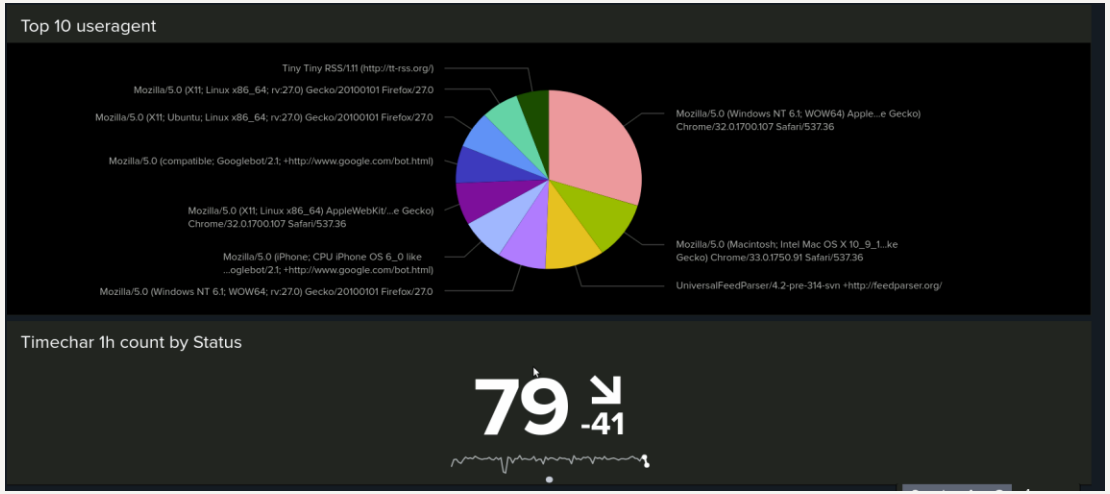
Apache_LOgs_Hourly_Activity_Besides_the_USA

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... May 7, 2025 3:38:01 AM
Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 170. Edit
Actions: ..... 1 Action Edit
Send email

Apache Dashboard

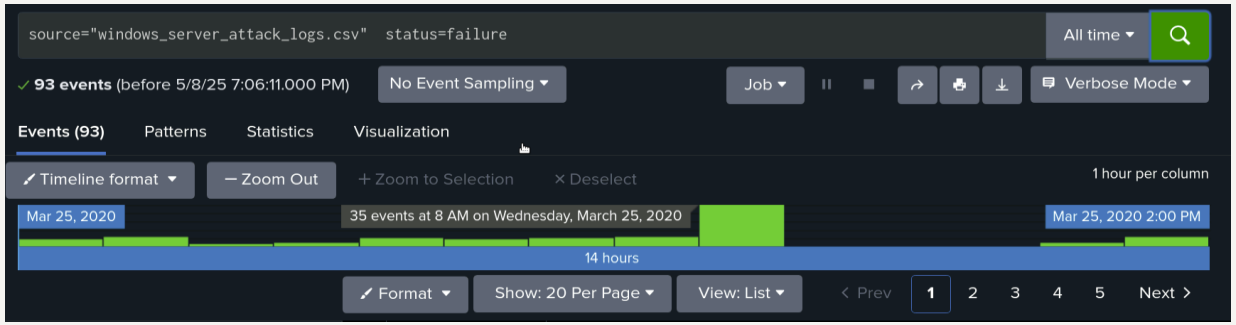


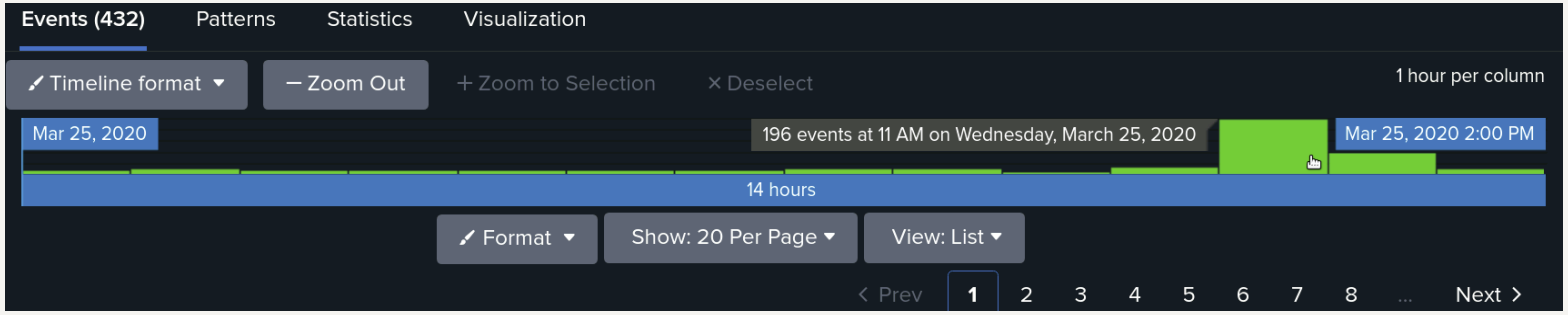


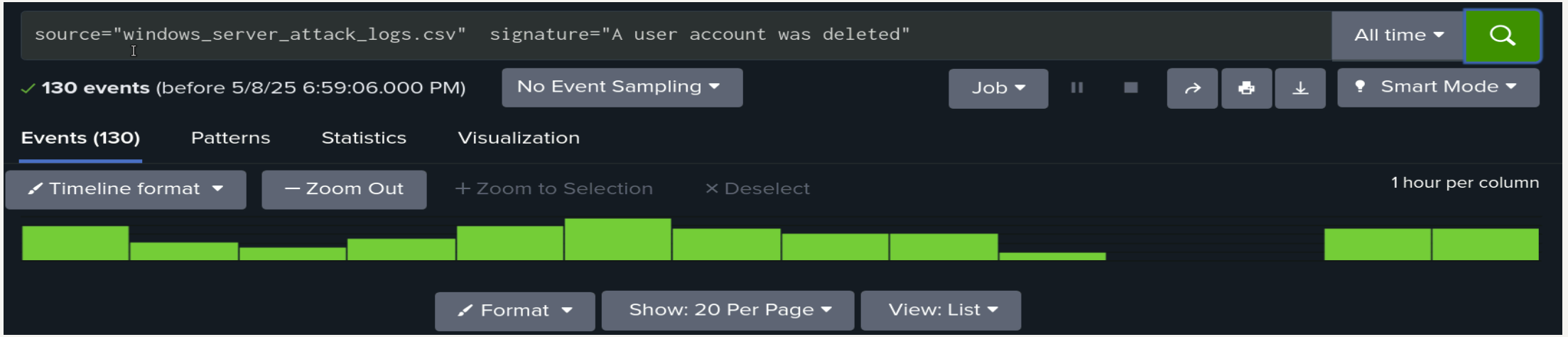
Window Attack Logs Alert Summary

1. We had a spike in the attack logs at 8am on March 25,2020. The count was around 35 which would have been caught by our alert that we already have set up.
2. We observed an average baseline count of around 13–17, but we set our alert threshold at 50, since anything above that would likely indicate suspicious activity. The suspicious activity we found was around 11 a.m, with the count of 196 and 12p.m with the count of 77.
3. For user account was deleted we did not see any suspicious activity both logs looked similar with no suspected activity.

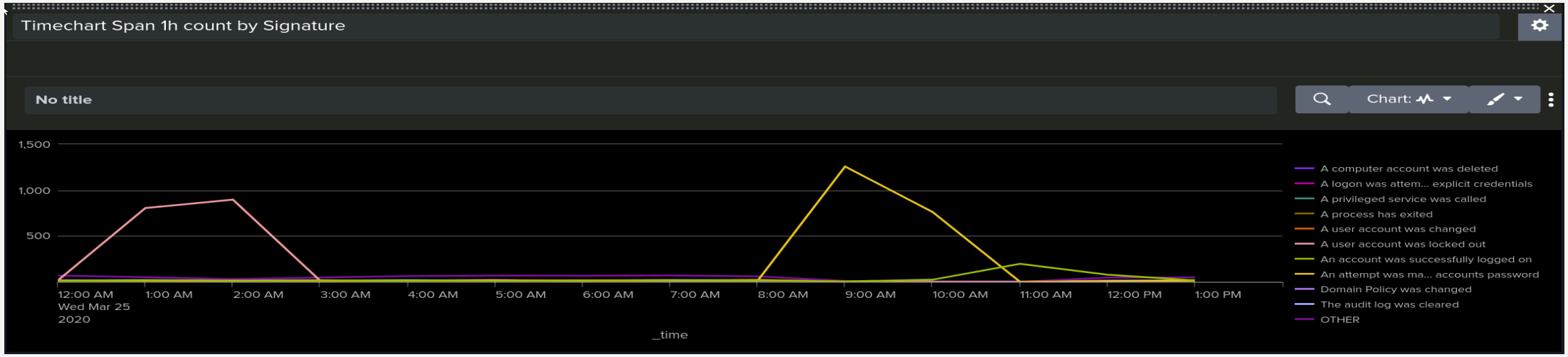
Window Attack log Images

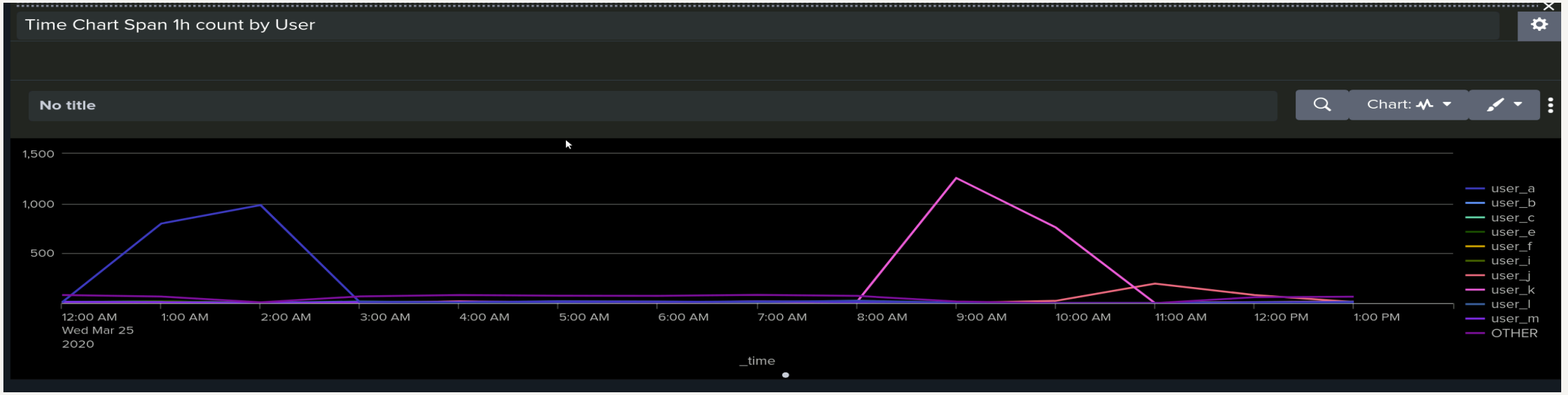






Dashboard analysis for User and Signatures from Attack Logs



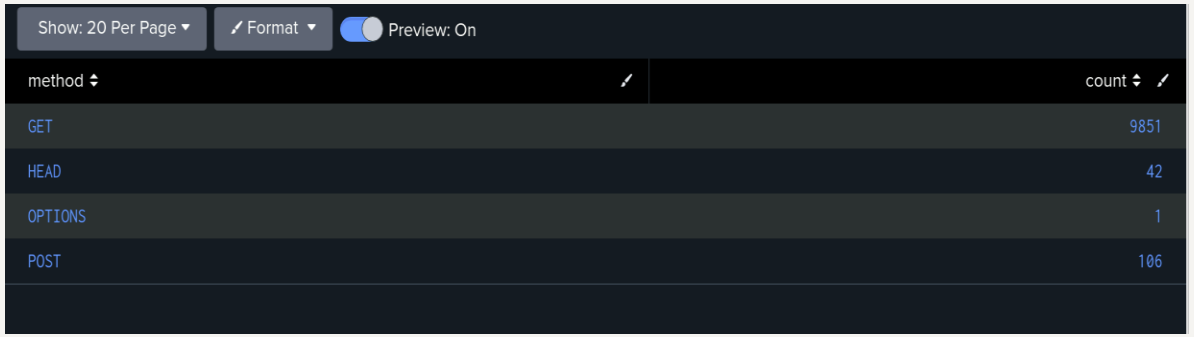


Summary for User and Signature Dashboard Attack Log

- Between midnight and 3 a.m., the most suspicious activity occurred, particularly at 1 a.m. and 2 a.m. The standout event was repeated "User Account is Locked out" alerts, which peaked at 896 occurrences. Additionally, from 8 a.m. to 11 a.m., there were attempts to reset an account password, peaking at 1,258 occurrences. These patterns suggest possible unauthorized access attempts during the early morning hours followed by password reset efforts later in the morning.
- Users A and K both showed significant activity in the attack logs, with User K being more suspicious due to a higher event count. User A's activity occurred between midnight and 3 a.m., peaking at 984 events, while User K's activity took place from 8 a.m. to 11 a.m., with a peak of 1,256 events. These patterns align with the earlier timeline of account lockouts and password reset attempts, reinforcing suspicions of potential unauthorized access or malicious activity.

Apache Logs Before the Attack

Apache Logs Method

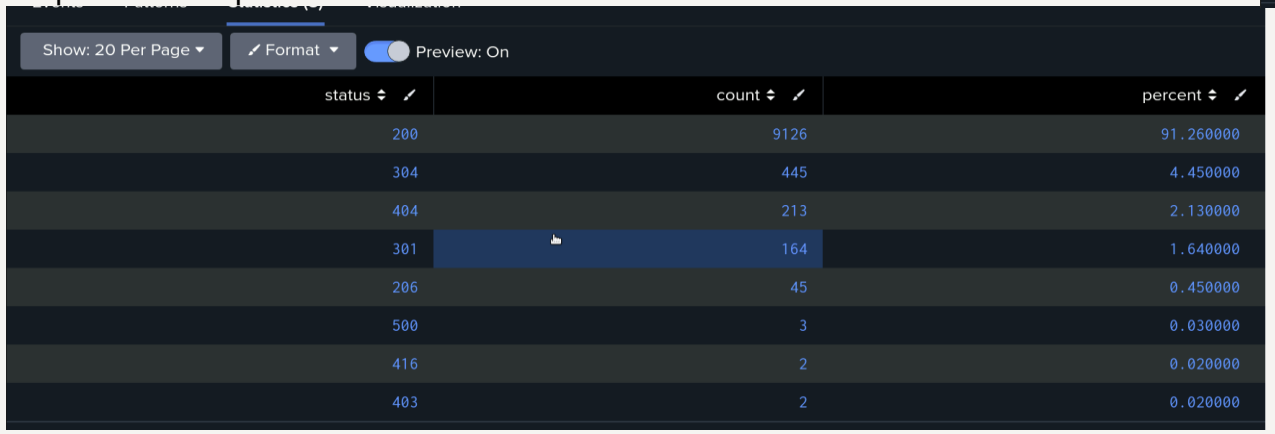


method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106

Apache Top Domains

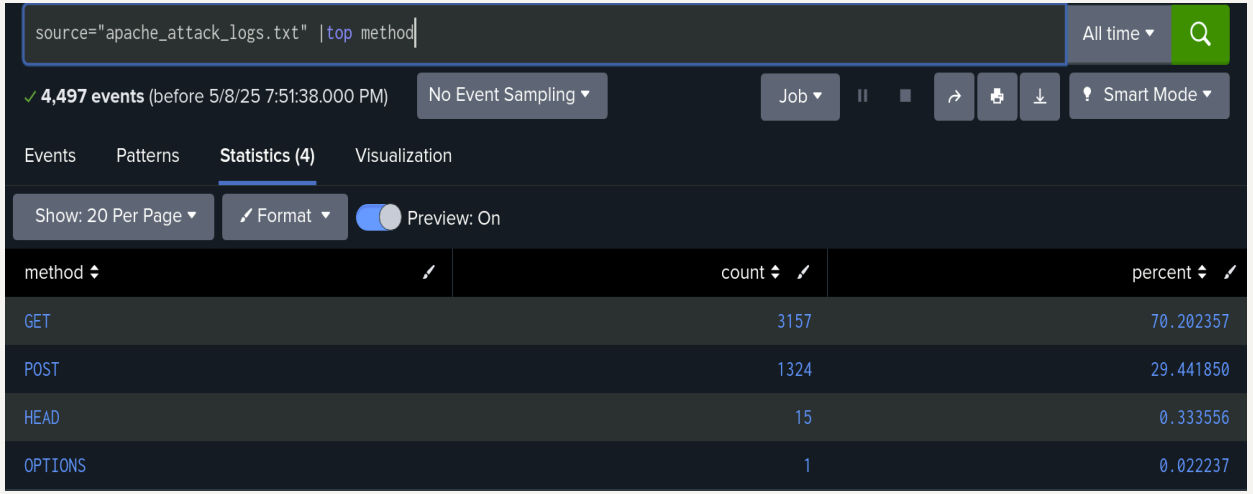
referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

Apache Top Status

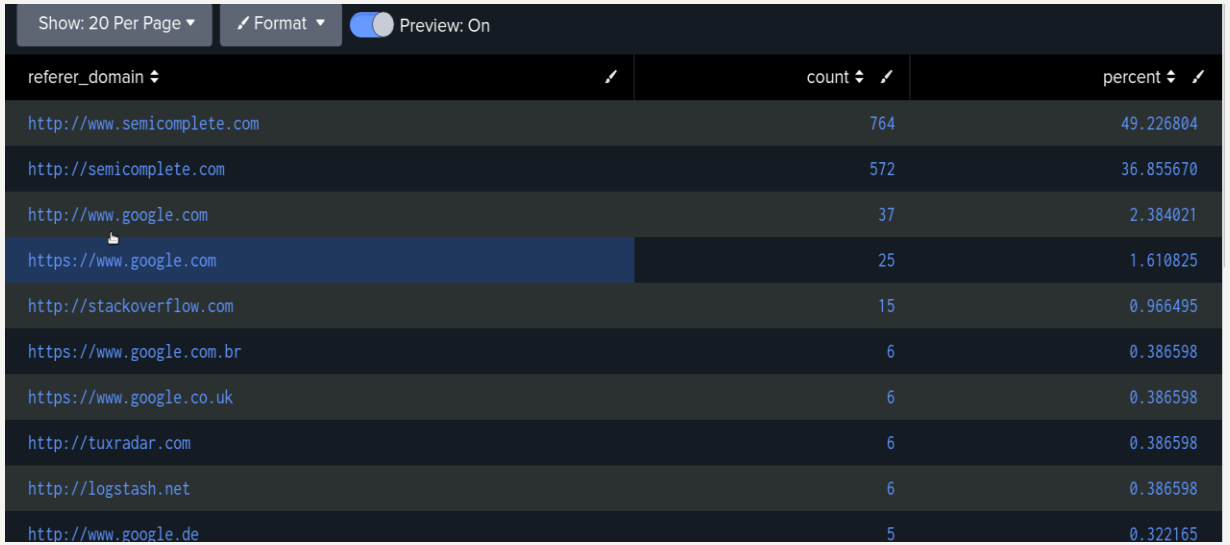


status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

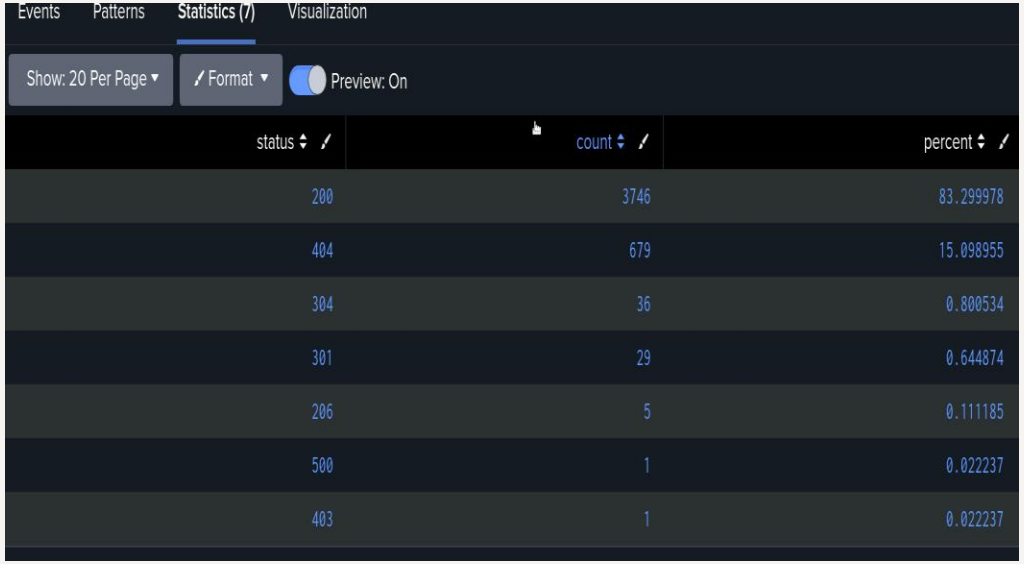
Apache Attack Log Images



Top Domain



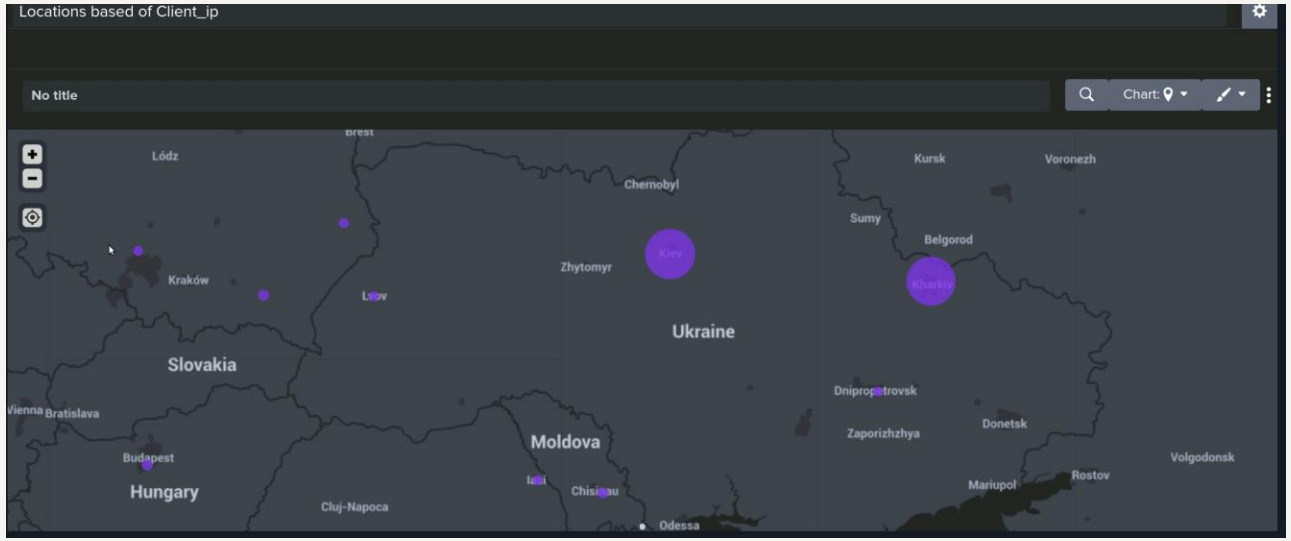
Top status attack log

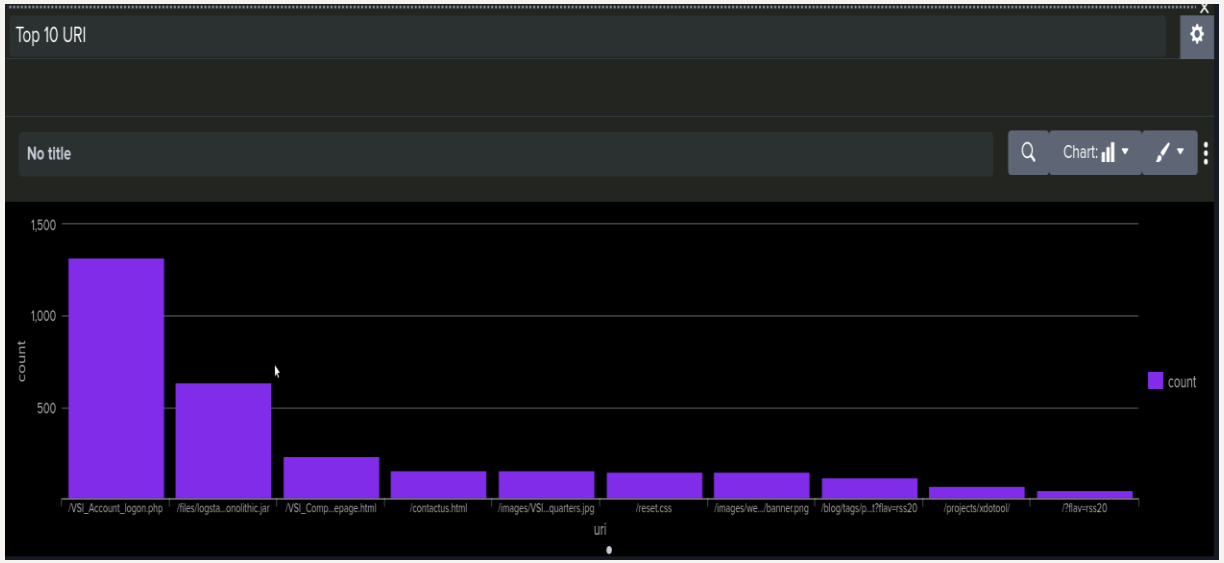


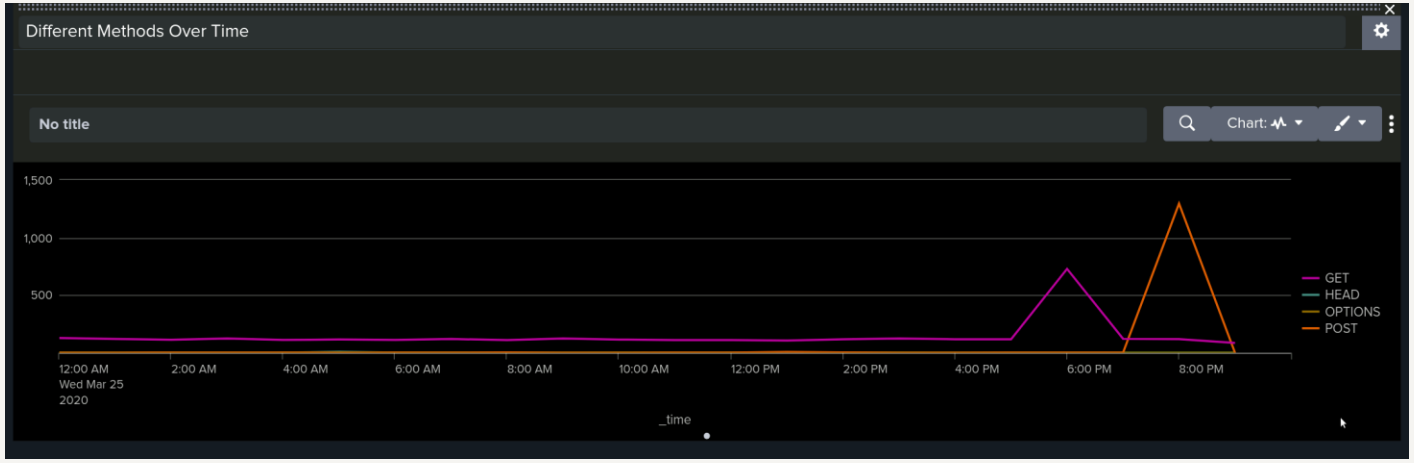
Apache Attack Log Summary

1. There was a suspicious decrease in the GET activity by 29% and we had an suspicious increase in the POST activity which increased by 29%
2. There were no suspicious activity when we pulled the referrer domains log.
3. We observed several minor changes to the top status apache attack log , but the most suspicious finding was the increase in 404 response codes, which jumped from 2% to 15%.

Apache Dashboard Attack Log Images







Apache Attack Log Summary

- We observed a high volume of suspicious activity targeting the URI /VSI_Account_logon.php, which was hit 1,323 times.
- The majority of this activity originated from two cities in Ukraine, with Kiev showing the highest activity followed by Kharkiv.
- Additionally, there was a noticeable increase in HTTP POST methods between 7 a.m. and 9 a.m., aligning with the spike seen in the attack logs from Ukraine.
- These patterns further support the likelihood of a brute-force attempt focused on the login endpoint.

Attack Mitigation Strategies

- To protect VSI On Windows and Apache servers from future attacks, recommended future mitigations.
  - Two-factor authentication, the first line of defense against Brute force attacks and brute force spamming passwords
  - Lock users out after a certain number of login attempts to prevent attacks.
- To protect VSI servers from the resetting of passwords and locked out accounts we can lower thresholds.
- To mitigate any non US activity we can block IP's from certain high risk areas