



Cybersecurity

Project 3 Review Questions

Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

We did, we observed an increase in severity from

windows_server_logs.csv

High - 6.905961

Informational - 93.094039

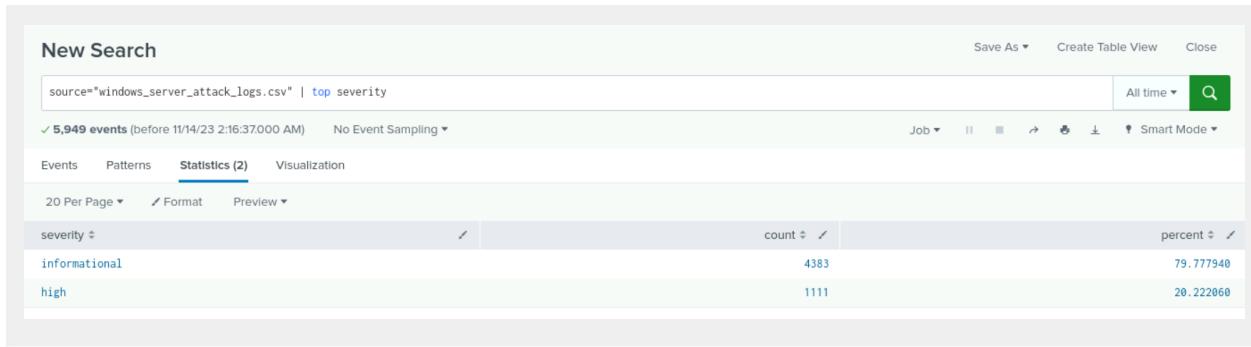


To

Windows_server_attack_logs.csv

High - 20.222060

Informational - 79.777940



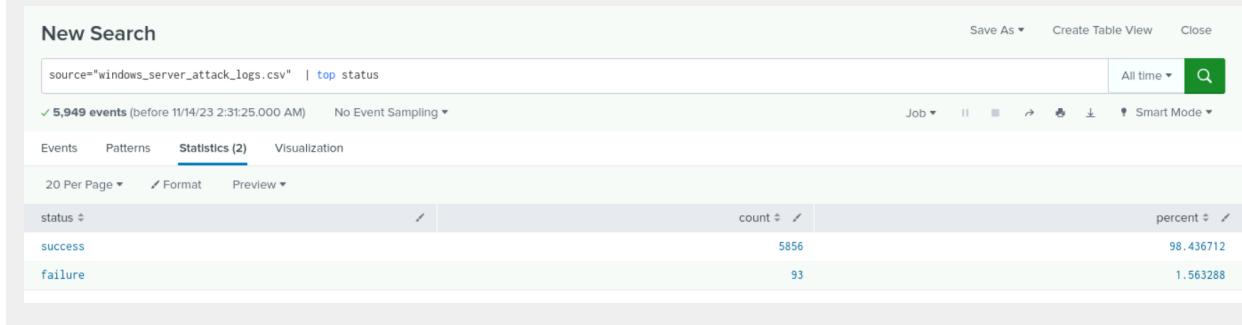
Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Affirmative there were alterations from
windows_server_logs.csv
 Success - 97.019312
 Failure - 2.980688



To
Windows_server_attack_logs.csv
 Success - 98.436712
 Failure - 1.563288



Alert Analysis for Failed Windows Activity

Failed Windows Activity by hour

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Nov 14, 2023 3:10:15 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: Number of Results is > 15. Edit
Actions: 1 Action Edit
Send email

New Search

source="windows_server_attack_logs.csv" status=failure

93 events (before 11/14/23 3:00:12.000 AM) No Event Sampling

Events (93) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾ 1 2 3 4 5 Next >

| Time | Event |
|------------------------|---|
| 3/25/20 1:45:27.000 PM | 2020-03-25T13:45:27.000+0000,"Domain_A", "user_g", "user_k", "Account Management", "ACME-002", "-4724, An attempt was made to reset an account's password, 0, "Audit Failure", "Security", "0xE85F", "An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_g Show all 61 lines host = windows_server_attack_logs.csv source = windows_server_attack_logs.csv sourcetype = csv |
| 3/25/20 1:30:41.000 PM | 2020-03-25T13:30:41.000+0000,"Domain_A", "user_b", "user_e", "Account Management", "ACME-002", "-4724, An attempt was made to reset an account's password, 0, "Audit Failure", "Security", "0x3A81", "An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_b Show all 61 lines host = windows_server_attack_logs.csv source = windows_server_attack_logs.csv sourcetype = csv |
| 3/25/20 1:26:53.000 PM | 2020-03-25T13:26:53.000+0000,"Domain_A", "user_m", "user_b", "Account Management", "ACME-002", "-4724, An attempt was made to reset an account's password, 0, "Audit Failure", "Security", "0x468A", "An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_m |

- Did you detect a suspicious volume of failed activity?

The suspicious activities occurred between 0800 to 0900 on 03/25/20. There was a suspicious amount of failed activities.

- If so, what was the count of events in the hour(s) it occurred?

There were 35 events from 0800 to 0900.

- When did it occur?

This happened on 03/25/20 from 0800 to 0900.

- Would your alert be triggered for this activity?

Yes it would, we set the trigger condition to > 15, it would then have alerted us.

- After reviewing, would you change your threshold from what you previously selected?

Negative, We concluded that 15 is a perfectly adequate benchmark for alerts, because 15 alerts is higher than the average number of alerts per hour. This works out perfectly because it is not too high to nullify alerts from suspicious activity.

Alert Analysis for Successful Logins

Successful Logins by hour

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Nov 14, 2023 3:30:32 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results Is > 30. Edit
Actions: v1 Action Edit
Send email

There are no fired events for this alert.

New Search

source="windows_server_attack_logs.csv" signature="An account was successfully logged on"

432 events (before 11/14/23 3:14:38.000 AM) No Event Sampling

Events (196) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect

Mar 25, 2020 11:00 AM Mar 25, 2020 12:00 PM 1 hour per column

List Format 20 Per Page ▶ Prev 1 2 3 4 5 6 7 8 ... Next >

| Time | Event |
|-------------------------|---|
| 3/25/20 11:59:54.000 AM | 2020-03-25T11:59:54.000+0000,, "Domain_A Domain_A","user_f user_f",,,,,"Account Management,,,,"ACME-002,,,,-4726,A user account was deleted,0,,,,"Audit Success,,,Security,,,0xA369,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 59 lines |
| 3/25/20 11:59:32.000 AM | host = windows_server_attack_logs.csv source = windows_server_attack_logs.csv sourcetype = csv 2020-03-25T11:59:32.000+0000,, "Domain_A Domain_A","ACME-002 Jaythan\larry",localhost,,,,"Account Management,,,,"ACME-002,,,,-4648,A logon was attempted using explicit credentials,0,,,,"Audit Success,,,Security,,,"(0887F1E4-39EA-D53C-804F-31D568A06274)" ,,,0x70E4,,,,"A logon was attempted using explicit credentials. Subject: Show all 85 lines |
| 3/25/20 11:59:04.000 AM | host = windows_server_attack_logs.csv source = windows_server_attack_logs.csv sourcetype = csv 2020-03-25T11:59:04.000+0000,, "Domain_A Domain_A",2020-03-25 11:59:04 AM,"user_1 user_f",,,server_2\computer_b,,,"Account Management,,,,"ACME-002,<value not set>,,,,-4738,A user account was changed,0,,,,"Audit Success,,,Security,,,Monday 2:00 PM -Tuesday 6:00 PM,0xAB37,,,,"SAM Account Name: user_c Display Name: <value not set> User Principal Name: bbb@BBB.local |

- Did you detect a suspicious volume of successful logins?

Yes we did, at 1100 there were 196 events and at 1200 there were about 77 events. The average login events are from 10 to 25 each hour.

- If so, what was the count of events in the hour(s) it occurred?

At 1100 there were 196 events as stated above and 77 events at 1200.

- Who is the primary user logging in?

User J

- When did it occur?

From 1100 to 1300

- Would your alert be triggered for this activity?

Yes our alert would be triggered because we set the trigger condition as > 30.

- After reviewing, would you change your threshold from what you previously selected?

No, because we can prevent triggering false alerts from the regular login volume by having our benchmark at 30. The benchmark is also high enough that we can be assured that in a triggering event, those activities are suspicious and not a false positive.

Alert Analysis for Deleted Accounts

Deleted Accounts per hour

Enabled: Yes. [Disable](#)
 App: search
 Permissions: Private. Owned by admin. [Edit](#)
 Modified: Nov 14, 2023 3:46:59 AM
 Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: Number of Results is > 10. [Edit](#)
 Actions: 1 Action [Edit](#)
[Send email](#)

There are no fired events for this alert.

New Search

source="windows_server_attack_logs.csv" signature_id=4762

6 events (before 11/14/23 3:39:41:000 AM) No Event Sampling ▾

Events (6) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

| Time | Event |
|-------------------------|--|
| 3/25/20 11:38:27:000 AM | 2020-03-25T11:38:27.000+0000,SeInteractiveLogonRight,Domain_A,"ACME-002 Domain_A\user_1",,,,ACME-002,,,,-4717,System security access was granted to an account, 0,,,,"Audit Success,,,Security,,,0xAB37,,,,"System security access was granted to an account. Subject: Security ID: Domain_A\SYSTEM Account Name: ACME-002 Show all 50 lines host = windows_server_attack_logs.csv source = windows_server_attack_logs.csv sourcetype = csv |
| 3/25/20 2:29:17:000 AM | 2020-03-25T02:29:17.000+0000,,Domain_A,,user_j,,,ACME-002,,,,-4672,Special privileges assigned to new logon,0,,,,"Audit Success,,,Security,,,0xB111,,,,"Special privileges assigned to new logon. Subject: Security ID: Domain_A\user_j Account Name: user_j Account Domain: Domain_A Show all 88 lines host = windows_server_attack_logs.csv source = windows_server_attack_logs.csv sourcetype = csv |
| 3/25/20 2:29:17:000 AM | 2020-03-25T02:29:17.000+0000,,Domain_A,,user_j,,,ACME-002,,,,-4672,Special privileges assigned to new logon,0,,,,"Audit Success,,,Security,,,0xB111,,,,"Special privileges assigned to new logon. Subject: Security ID: Domain_A\user_j Account Name: user_j Account Domain: Domain_A |

< Hide Fields All Fields i Time Event

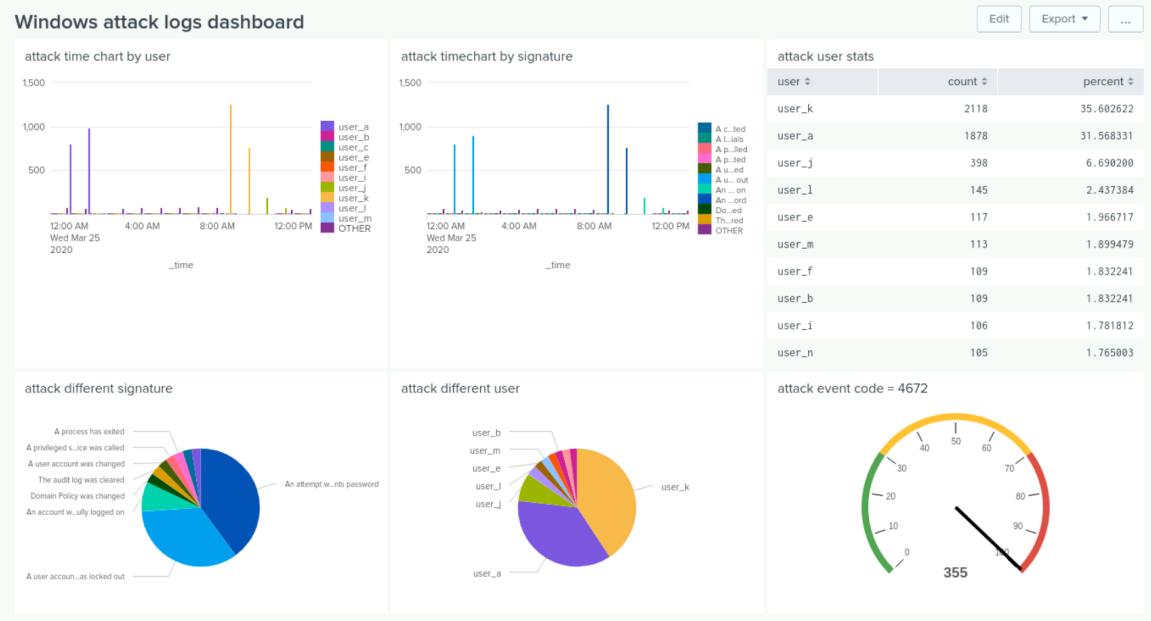
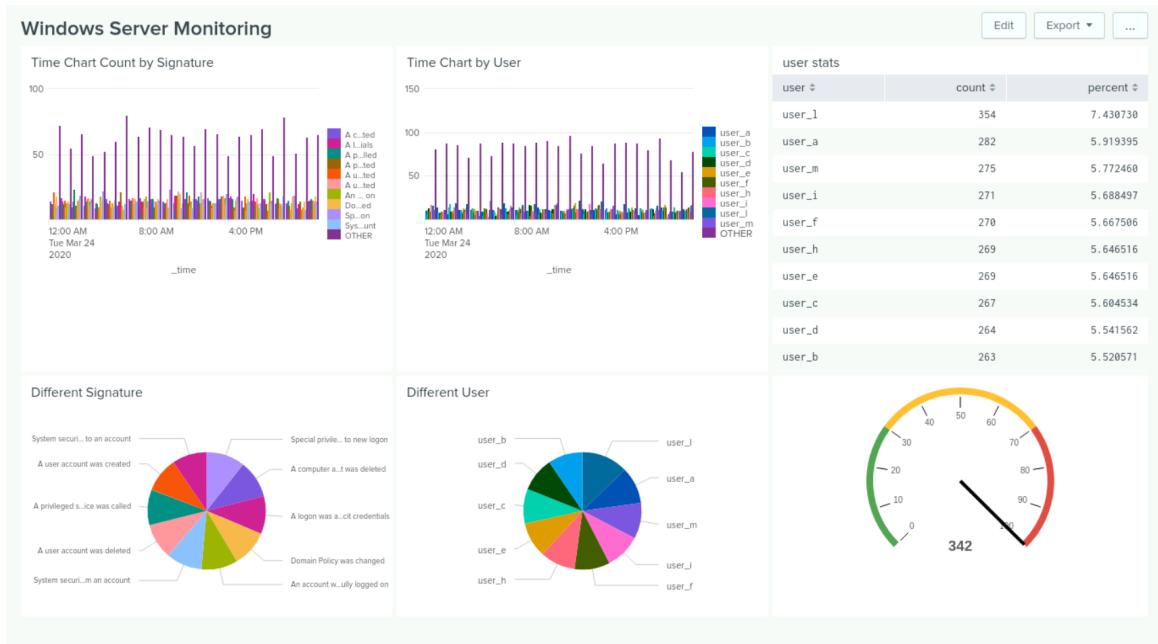
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 1
a Account_Name 2
a action 1
a app 1
a body 2
a category 2
a ComputerName 1
a date_hour 2
a date_mday 1
a date_minute 2
a date_month 1
a date_second 2
a date_wday 1
a date_year 1
a date_zone 2
a dest 1
- dest_in_numbered 1

- Did you detect a suspicious volume of deleted accounts?

No we did not, there was not any suspicious volume of deleted accounts.

Dashboard Analysis for Time Chart of Signatures



- Does anything stand out as suspicious?

Yes, there were several things that stand out, such as users trying to reset passwords a lot at 39.955%, a user got locked out of their account several times at 34.003%, and there were successful logins with 8.111%.

- What signatures stand out?

The reset passwords attempts at 39.955% ,then user lockouts at 34.003%, and lastly successful logins at 8.111%

- What time did it begin and stop for each signature?

“A user account was locked out” - from 0100 to 0300 on 03/25/20

“An attempt was made to reset a users password” - from 0900. to 1100 on 03/25/20

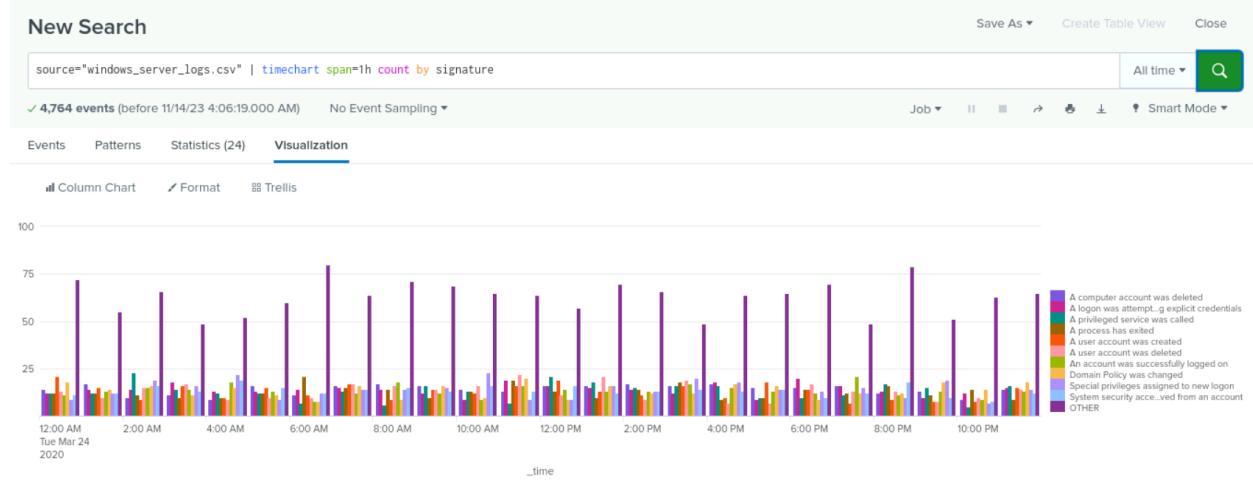
“The account was successfully logged on” - from 1100 and ended at 1300 on 03/25/20

- What is the peak count of the different signatures?

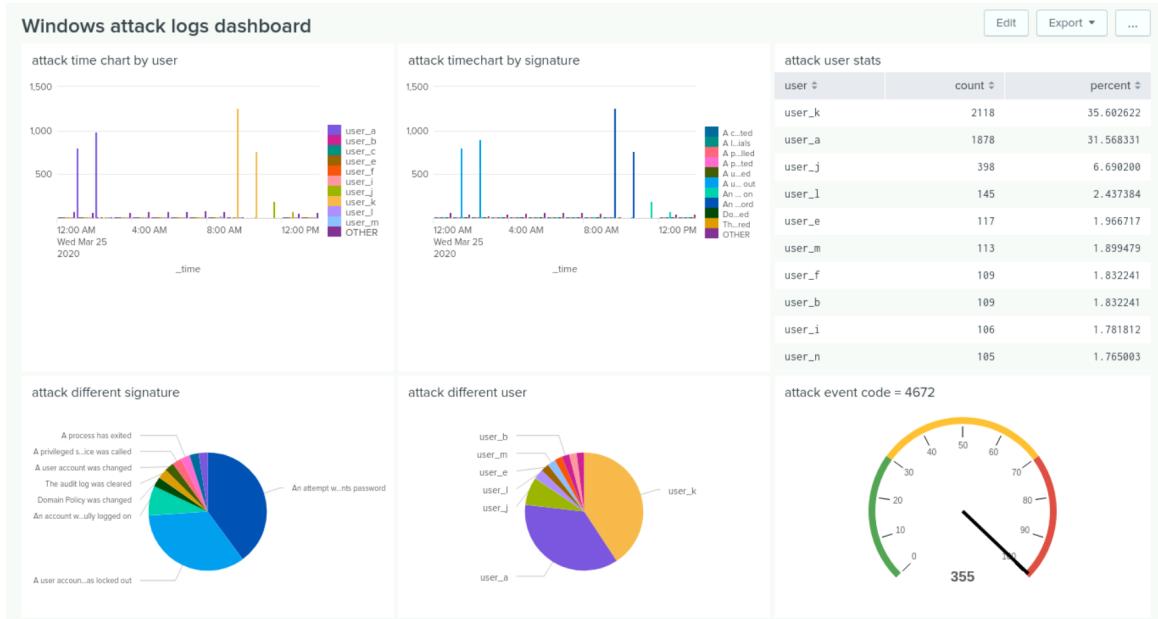
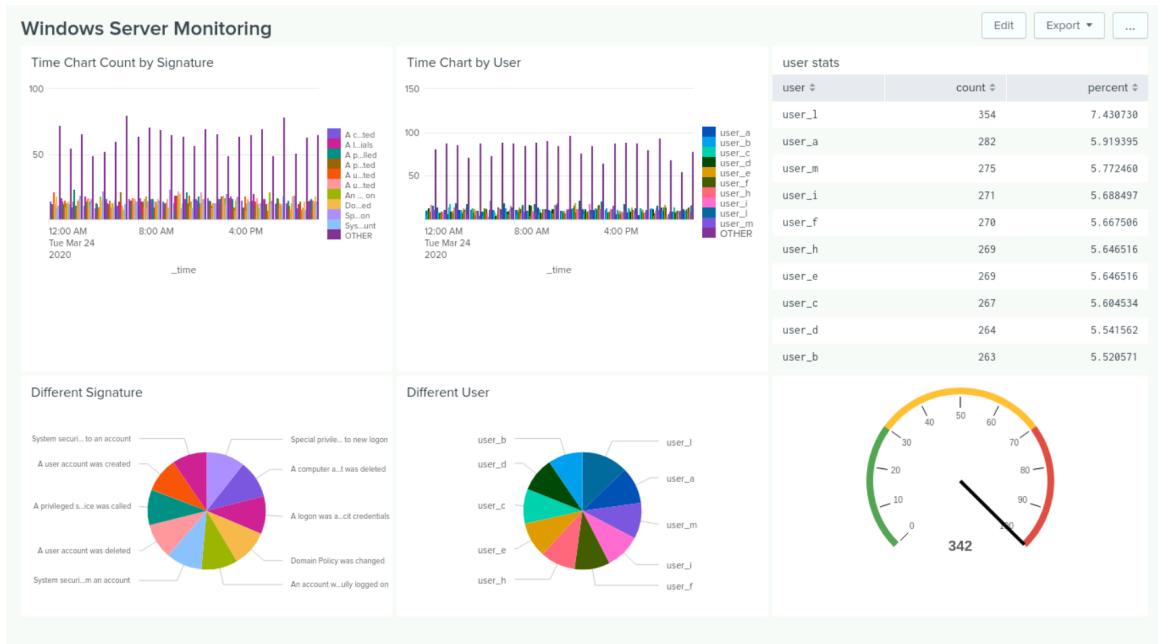
“A user account was locked out” - peak 896 total from 0100 to 0300. was 1701

“An attempt was made to reset a users password” - peak 1,258 total from 0900-1100 was 2019

“The account was successfully logged on” - peak 196 total from 1100-1300 was 273



Dashboard Analysis for Users



- Does anything stand out as suspicious?

Users A, K, and J are the ones who causing these suspicious activities

- Which users stand out?

These following Users A,K and J

- What time did it begin and stop for each user?

User A - from 0100 to 0300 on 03/25/20

User K - from 0900 to 1100 on 03/25/20

User J - from 1100 to 0100 on 03/25/20

- What is the peak count of the different users?

User A - peak 984 total at 1783

User K - peak 1256 total at 2017

User J - peak 196 total 278

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

No

- Do the results match your findings in your time chart for signatures?

All of our visualization and chart information matches the Signatures above

Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

No

- Do the results match your findings in your time chart for users?

Yes, all of our charts information matches with the Users information

Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

Advantage - Provides a comprehensive overview of total user activity or activity percentage.

Disadvantage - Lacks the cumulative perspective offered by a time chart, as Time charts offer a more specific and shorter time frame for detecting suspicious activity.

Apache Web Server Log Questions

Report Analysis for Methods

- Did you detect any suspicious changes in HTTP methods? If so, which one?

Yes we did, there was a conspicuous alteration in the HTTP POST method. It increased exponentially from 1% to 29% and the count raised from 106 to 1324

The image contains two side-by-side screenshots of the Splunk 9.1.1 interface. Both screenshots show a search results page with the following search query in the search bar:

```
source="apache_logs.txt" | top method
```

The top screenshot is titled "New Search" and shows results for "apache_logs.txt". The bottom screenshot is also titled "New Search" and shows results for "apache_attack_logs.txt". Both screenshots have the "Statistics (4)" tab selected. The results table displays the following data:

| method | count | percent |
|---------|-------|-----------|
| GET | 9851 | 98.510000 |
| POST | 106 | 1.060000 |
| HEAD | 42 | 0.420000 |
| OPTIONS | 1 | 0.010000 |

The bottom screenshot shows a slightly different distribution:

| method | count | percent |
|---------|-------|-----------|
| GET | 3157 | 70.202357 |
| POST | 1324 | 29.441850 |
| HEAD | 15 | 0.333556 |
| OPTIONS | 1 | 0.022237 |

- What is that method used for?

The method of POST is designed to update or submit info to a web server.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There weren't any questionable referees during this assault. There was only a minuscule alteration in the first two domains by a few percentages.

The image displays two side-by-side screenshots of Splunk search results. Both searches use the same query: `source="apache_logs.txt" host="Apache Logs" sourcetype="access_combined" | top limit=10 referer_domain`. The top search is for "Apache Logs" and finds 10,000 events, while the bottom search is for "Apache Attack Logs" and finds 4,497 events. Both results show a table of referrer domains with their counts and percentages.

Top Referrer Domains - Apache Logs

| referer_domain | count | percent |
|-----------------------------|-------|-----------|
| http://www.semicomplete.com | 3038 | 51.256960 |
| http://semicomplete.com | 2081 | 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 |

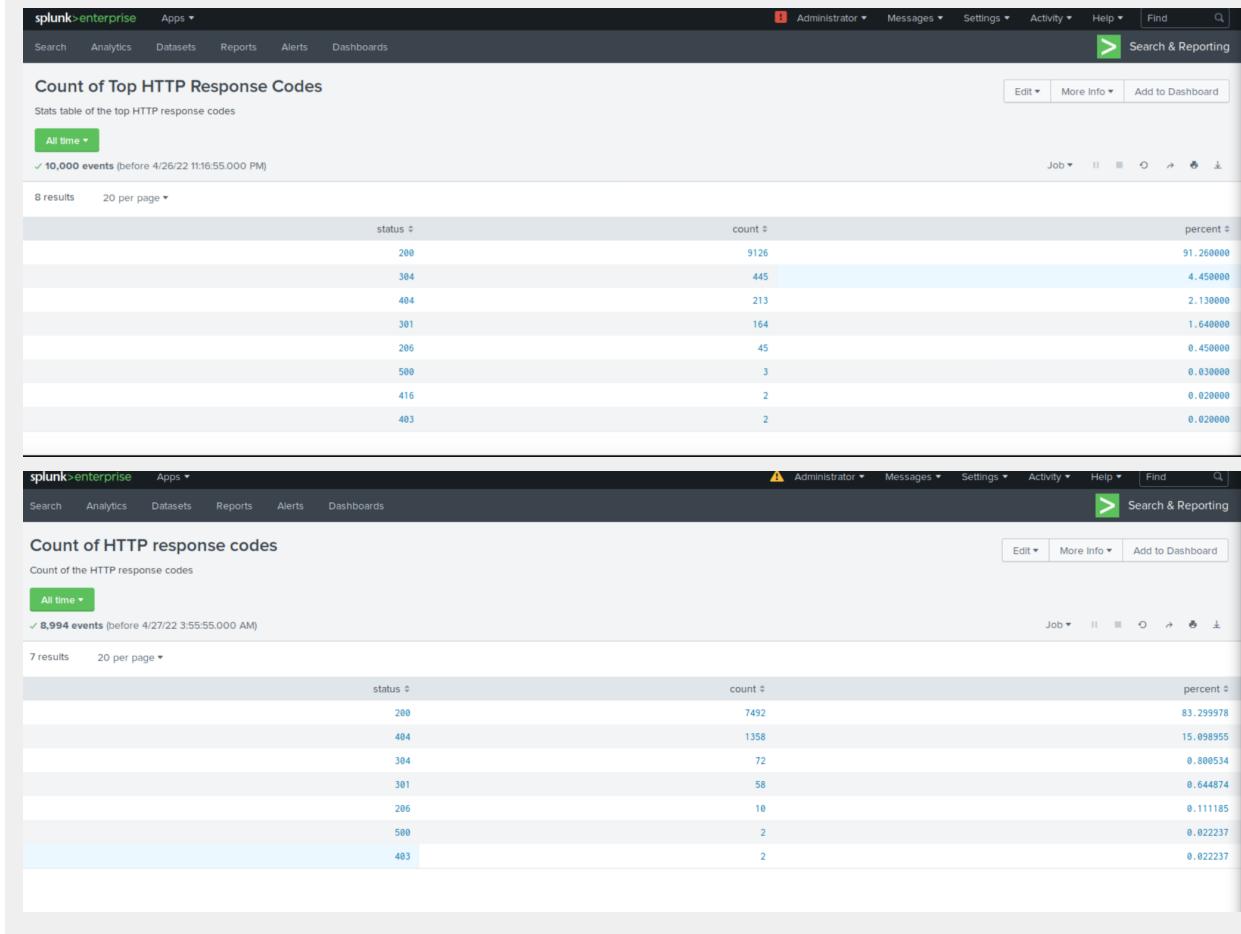
Top Referrer Domains - Apache Attack Logs

| referer_domain | count | percent |
|-----------------------------|-------|-----------|
| http://www.semicomplete.com | 764 | 49.226804 |
| http://semicomplete.com | 572 | 36.855670 |
| http://www.google.com | 37 | 2.384021 |
| https://www.google.com | 25 | 1.610825 |
| http://stackoverflow.com | 15 | 0.966495 |
| https://www.google.com.br | 6 | 0.386598 |
| https://www.google.co.uk | 6 | 0.386598 |
| http://uxradar.com | 6 | 0.386598 |
| http://logstash.net | 6 | 0.386598 |
| http://www.google.de | 5 | 0.322165 |

Report Analysis for HTTP Response Codes

- Did you detect any suspicious changes in HTTP response codes?

There are several small changes, but the most prominent is the 404 response code, which increased from 2% to 15%. The 200 response code went down from 91% to 83%.



Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

There was activity in Ukraine at 8 p.m. on Wednesday March 25th, and had a count of 937 events.

The screenshot shows a Splunk search interface with the following details:

- Search query: `source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States"`
- Results: 2,497 events (3/25/20 12:00:00:00 AM to 3/25/20 10:00:00:00 PM)
- Time range: Mar 25, 2020 10:00 PM to Mar 25, 2020 10:00 PM
- Event count: 937 events at 8 PM on Wednesday, March 25, 2020
- Fields listed in the sidebar include: host, source, country, bytes, City, clientip, Country, date_hour, date_minute, date_second, date_year, date_zone, file, ident, index, lat, linecount, lon, method, punct, referer, and referer_domain.
- The main pane displays a list of log entries, each showing a timestamp, source IP, and a detailed log entry.

- If so, what was the count of the hour(s) it occurred in?

There was a spike in POST method activity between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 1,296 events.

- Would your alert be triggered for this activity?

The average activity per hour was about 75.
We concluded the threshold should be set for 200.

- After reviewing, would you change the threshold that you previously selected?

No as it's above the activity set threshold.

Alert Analysis for HTTP POST Activity

- Did you detect any suspicious volume of HTTP POST activity?

There was a sudden increase in POST method activity and the threshold set is at 15 count.

Count of HTTP POST method

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Nov 17, 2023 6:04:22 PM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 15. Edit
Actions: 1 Action Edit
Send email

- If so, what was the count of the hour(s) it occurred in?

The count was 1,296 events between 8 p.m. and 9 p.m. on Weds, March 25th 2020

- When did it occur?

March 25th 2020 between 8pm and 9pm

- After reviewing, would you change the threshold that you previously selected?

No, we determine 15 is an adequate amount, which would trigger.
The average activity per hour is approximately 5.

Therefore the threshold is set for 15.

We set it to run every hour.

The alert triggers when count is greater than chosen threshold of 15

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, there were suspicious activities of the POST and GET method.



- Which method seems to be used in the attack?

The POST method was used and the GET method was used

- At what times did the attack start and stop?

POST Method commenced at 8 p.m. and finished at 9 p.m.

Get method began at 6 p.m. and ended at 7 p.m.

- What is the peak count of the top method during the attack?

The peak count for the Get method was 3,157.

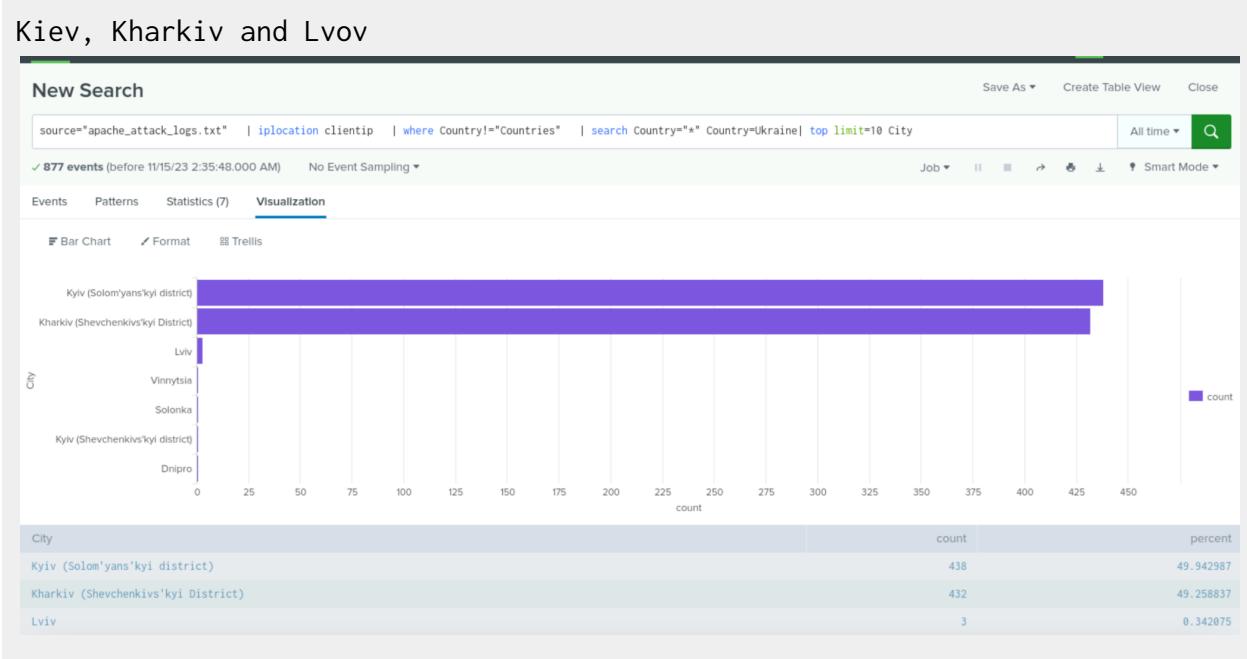
The peak count for the POST method was 1,324.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?



- Which new location (city, country) on the map has a high volume of activity?
(Hint: Zoom in on the map.)



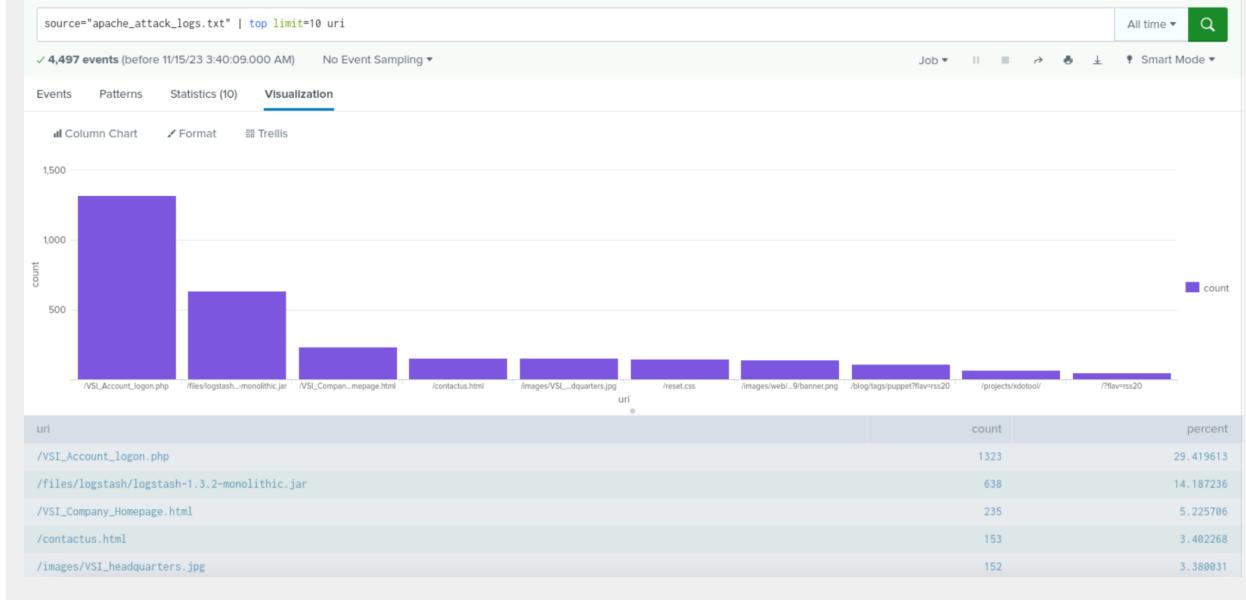
- What is the count of that city?

```
kiev:Count of 438. Kharkiv:Count of 432. Lvov:Count of 3.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, there is suspicious activity against the main VSI logon page:
`/VSI_Account_logon.php`.



- What URI is hit the most?

`/VSI_Account_logon.php`.

- Based on the URI being accessed, what could the attacker potentially be doing?

The attacker may be attempting to brute force the VSI logon page