



Cybersecurity

Project 3 Review Questions

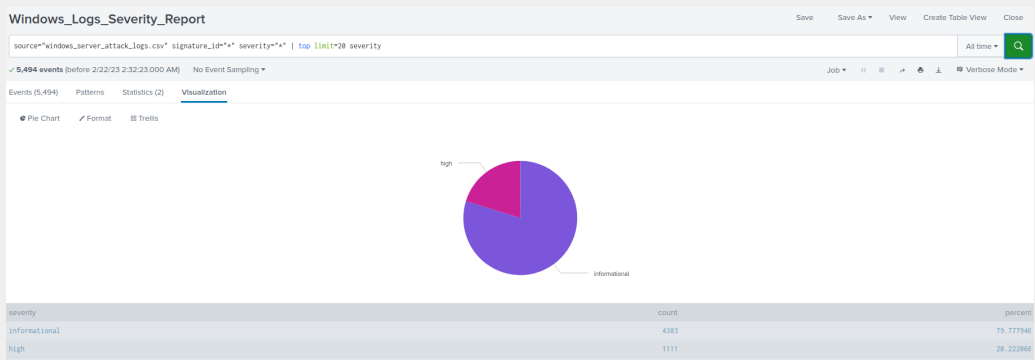
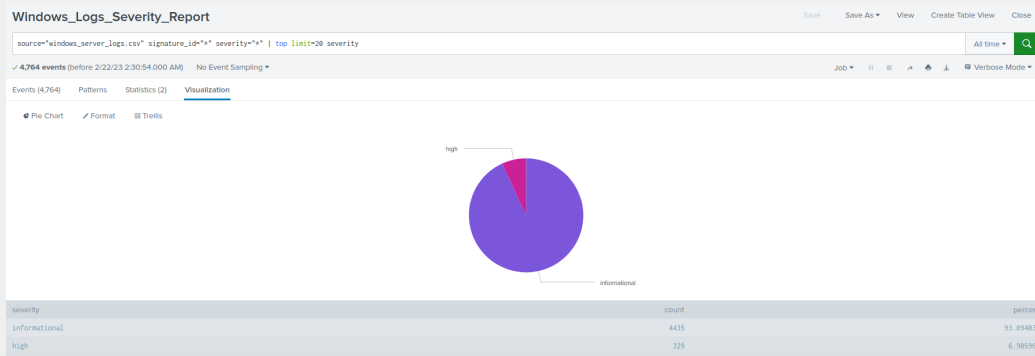
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

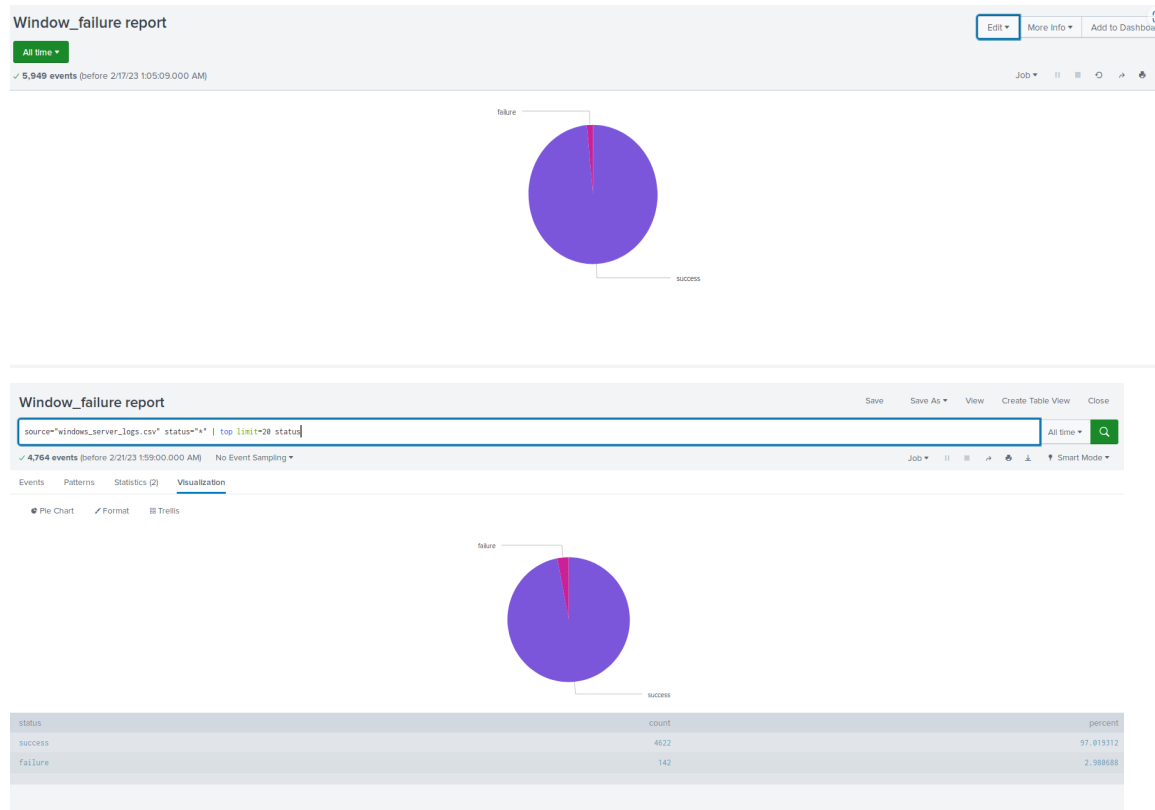
- Did you detect any suspicious changes in severity?

Yes, there were significant changes in severity level for “high”, 6.9% to 20.2% while the severity level for informational decreased from 93.9% to 79.8%



Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?
No, The failure rate dropped from 3.0 to 1.6; my conclusion is that there are no suspicious changes in failed activities.



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes - the suspicious volume of failed activity with events count of 35 on Wednesday, March 25, 2020, at 8:00 AM.

Alert_Failure

Save Save As View Create Table View Close

source="windows_server_logs.csv" status="*" status=Failure

All time

142 events (before 2/21/23 2:04:41:000 AM) No Event Sampling

Job

Smart Mode

Events (142) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account_Domain 1

a Account_Name 100

a action 1

a app 1

a body 100

Time

Event

3/24/20

2020-03-24T23:56:41.000+0000,"Domain_A", "user_a", "Domain_A", "Account Management", "AOE-002", "4724, An attempt was made to reset an account's password.", "Audit Failure", "Security", "0x6C10", "An attempt was made to reset an account's password.", "Subject: Security ID: Domain_A\\user_a", "Show all 61 lines", "host = windowserverlog | source = windows_server_logs.csv | sourcetype = csv"

3/24/20

2020-03-24T23:34:35.000+0000,"Domain_A", "user_a", "Domain_A", "Account Management", "AOE-002", "4724, An attempt was made to reset an account's password.", "Audit Failure", "Security", "0x408A", "An attempt was made to reset an account's password.", "Subject: Security ID: Domain_A\\user_a", "Show all 61 lines", "host = windowserverlog | source = windows_server_logs.csv | sourcetype = csv"

1

2

3

4

5

6

7

8

Next

Alert_Failure

Save Save As View Create Table View Close

source="windows_server_attack_logs.csv" status="*" status=Failure

All time

93 events (before 2/21/23 2:03:09:000 AM) No Event Sampling

Job

Smart Mode

Events (93) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account_Domain 2

a Account_Name 74

Time

Event

3/25/20

2020-03-25T13:45:27.000+0000,"Domain_A", "user_g", "Domain_A", "Account Management", "AOE-002", "4724, An attempt was made to reset an account's password.", "Audit Failure", "Security", "0xE0BF", "An attempt was made to reset an account's password.", "Subject: Security ID: Domain_A\\user_g", "Show all 61 lines", "host = window attack | source = windows_server_attack_logs.csv | sourcetype = csv"

1

2

3

4

5

Next

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

35 events

- When did it occur?

8:00 AM on Wednesday, March 25, 2020

- Would your alert be triggered for this activity?

Yes

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

No, the result appears to be isolated and not an indication of a True Negative.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes

Alert_Successful Logins

Save Save As View Create Table View Close

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

All time

✓ 323 events (before 2/21/23 2:31:30.000 AM) No Event Sampling

Job

Smart Mode

Events (323) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account_Domain 1

a Account_Name 14

a action 1

a app 2

a Authentication_Package 2

Time

Event

>

3/24/20

2020-03-24T23:57:54.000+0000,,Domain_A

Domain_A",,"ACHE-002

user_a",,"Negotiate,,,,,,,,,,,,ACHE-002,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,Delegation,,0,Audit Success,A966,,,Security,,,((00000000-0000-0000-0000-000000000000

00),,"0x70E4

0x0452",,LogonProcess1,9,,,,,"An account was successfully logged on.

Subject:

Show all 159 lines

host = windowsserverlog | source = windows_server_logs.csv | sourcetype = csv

>

3/24/20

2020-03-24T23:58:11.000+0000,,Domain_A

Domain_A",,"ACHE-002

user " Karharoc

ACHE-002

No - 4624,An account was successfully logged on 0

Impersonation

0 Audit Success 1718

Security

((737247F3-197A-4A76-80A1-D1176A7A

Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account_Domain 2

a Account_Name 100+

a action 5

a app 3

a Authentication_Package 2

a body 100+

a category 8

a CategoryString 1

a change_type 2

Time

Event

>

3/25/20

2020-03-25T13:41:51.000+0000,,Domain_A

Domain_A",,"ACHE-002

user_a",,"Kerberos,,,,,,,,,,,,ACHE-002,,,,,,Yes,-,4624,An account was successfully logged on,0,,,,,,,,,Impersonation,,0,,Audit Success,350A,,,Security,,,((27C4A2F2-13CA-AA25-E903-D31

268748239),,"0x70E4

0x6C10",,LogonProcess1,10,,,,,"An account was successfully logged on.

Subject:

Show all 159 lines

host = window attack | source = windows_server_attack_logs.csv | sourcetype = csv

>

3/25/20

2020-03-25T13:40:34.000+0000,,Domain_A

Domain_A",,"ACHE-002

user_b",,"Kerberos,,,,,,,,,,,,ACHE-002,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,Impersonation,,0,,Audit Success,74F2,,,Security,,,((8887F1E4-39EA-053C-804F-31D5

68A86274),,"0x70E4

0xA19C",,Winlogon,2,,,,,"An account was successfully logged on.

Subject:

Show all 159 lines

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

196 events at 11AM on Wednesday, March 25, 2020
77 events at 12PM on Wednesday, March 25, 2020

- Who is the primary user logging in?

user_k

- When did it occur?

11AM and 12PM on Wednesday, March 25, 2020

- Would your alert be triggered for this activity?

Yes

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

No

Alert Analysis for Deleted Accounts

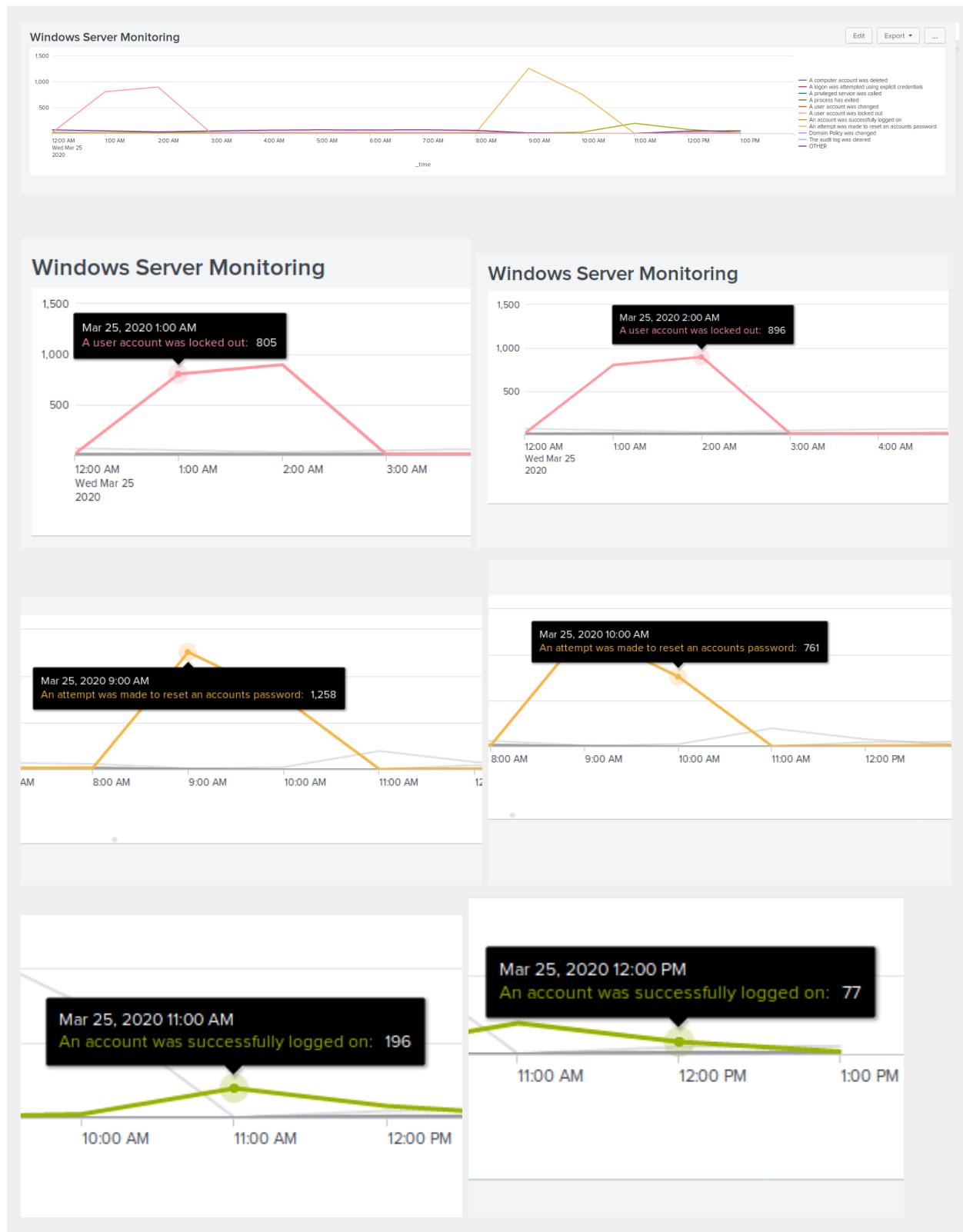
- Did you detect a suspicious volume of deleted accounts?

No



Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?



Yes, there is a significant increase in user accounts being locked out from 1:00 AM - 3:00 AM, attempted password resets from 9:00 AM to 11:00 AM and successful logins from 11:00 AM - 1:00 PM.

- What signatures stand out?

A user account was locked out

An attempt was made to reset an accounts password

An account was successfully logged on

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

A user account was locked out: 1:00 AM - 3:00 AM

An attempt was made to reset an accounts password: 9:00 AM to 11:00 AM

An account was successfully logged on: 11:00 AM - 1:00 PM

- What is the peak count of the different signatures?

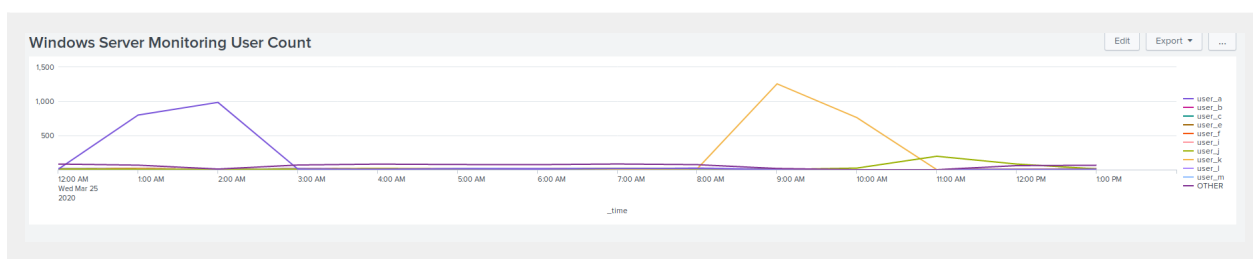
A user account was locked out: 896

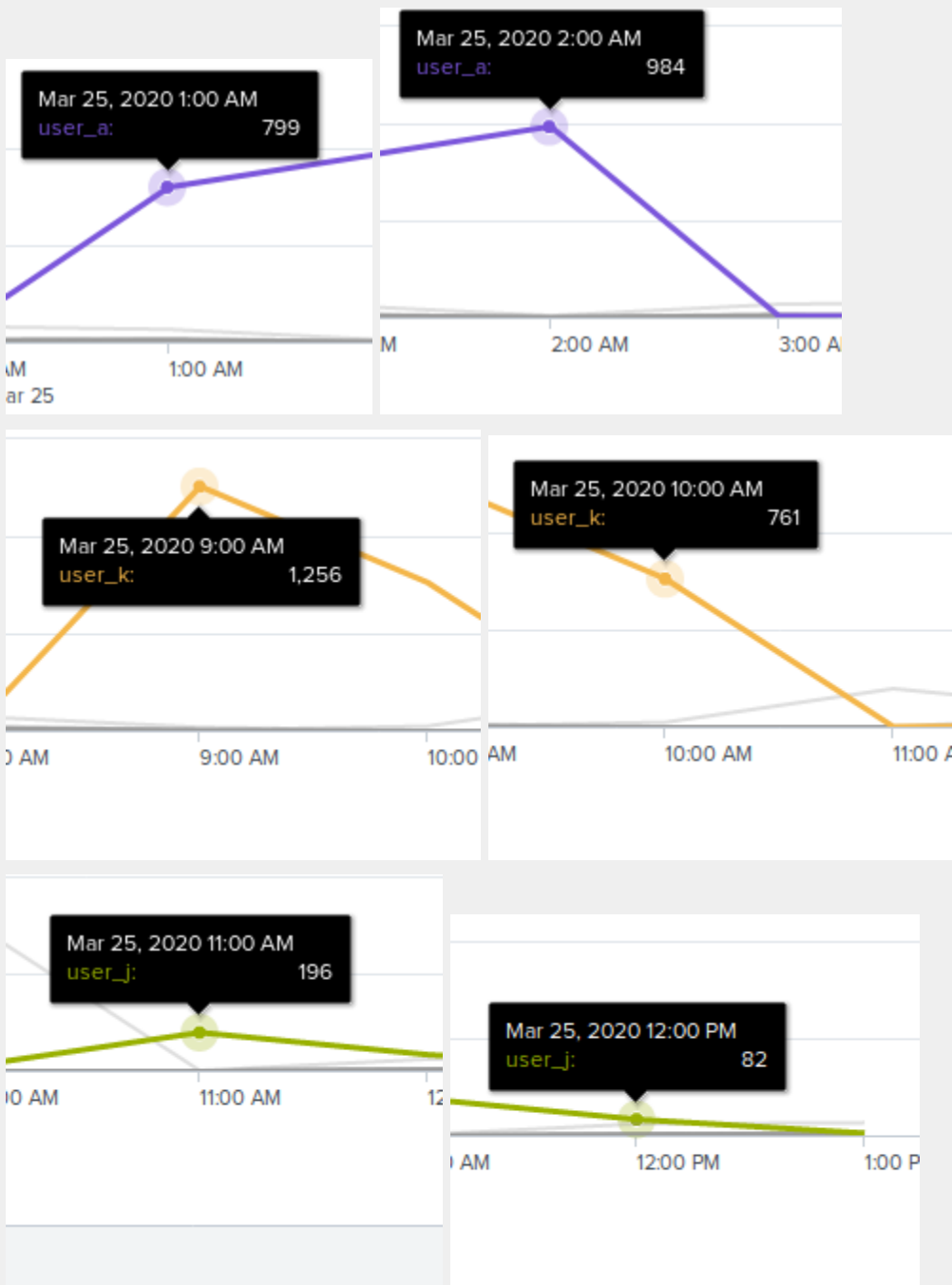
An attempt was made to reset an accounts password: 1258

An account was successfully logged on: 196

Dashboard Analysis for Users

- Does anything stand out as suspicious?





User_a, user_k, and user_j have activity levels far above baseline.

- Which users stand out?

user_a
user_k

user_j

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

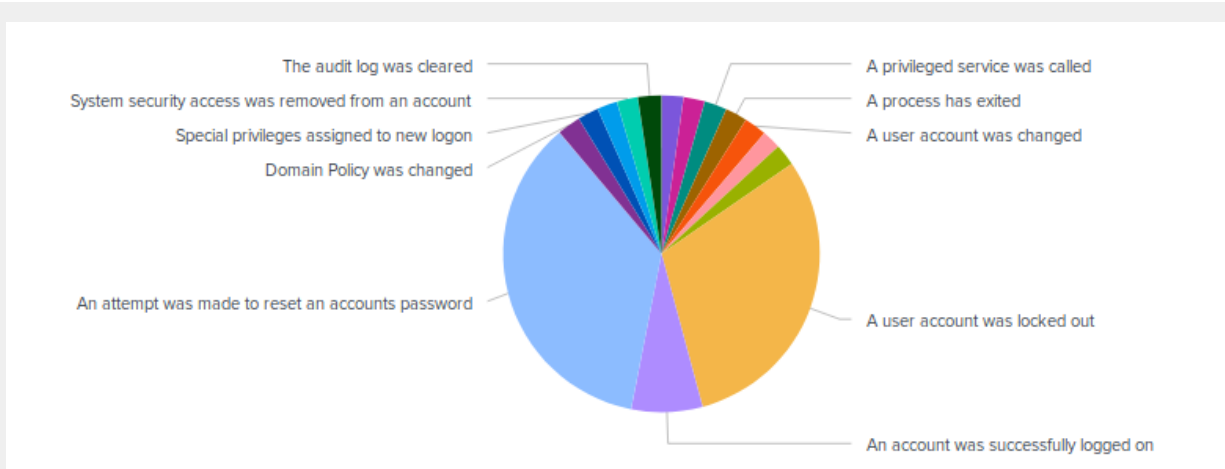
user_a: suspicious activity started 1:00 AM and ended 3:00 AM
user_k: suspicious activity started 9:00 AM and ended 11:00 AM
user_j: suspicious activity started 11:00 AM and ended 1:00 PM

- What is the peak count of the different users?

User_a - 984
User_k - 1256
User_j - 196

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

- Does anything stand out as suspicious?



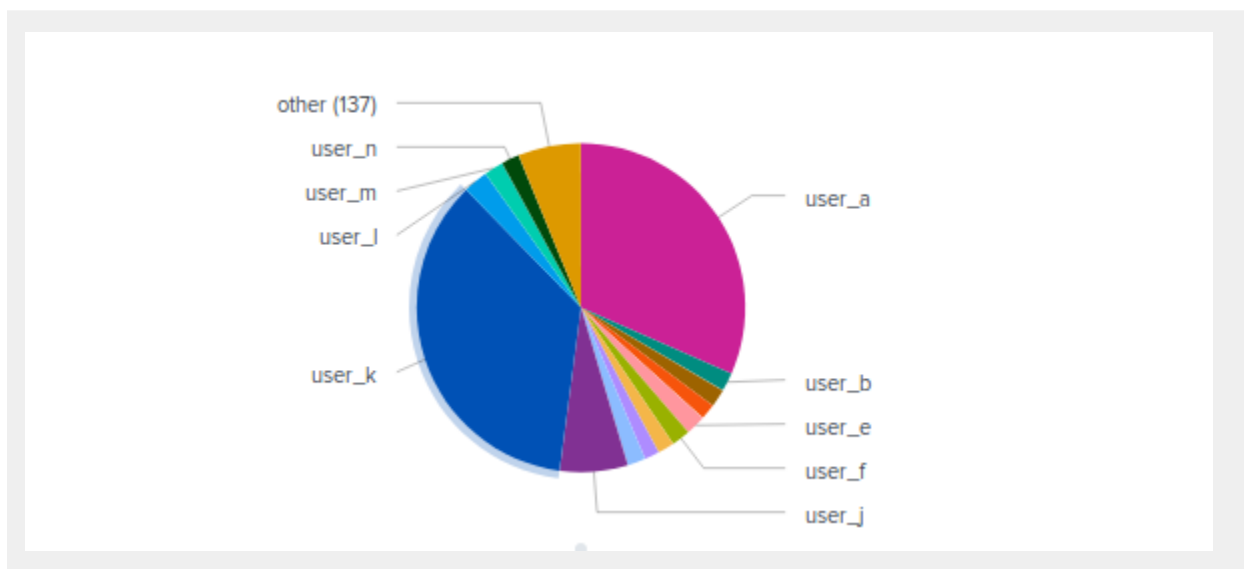
Yes, there is a significant increase in user accounts being locked out, attempted password resets and successful logins.

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

Yes

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

- Does anything stand out as suspicious?



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

Yes

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?

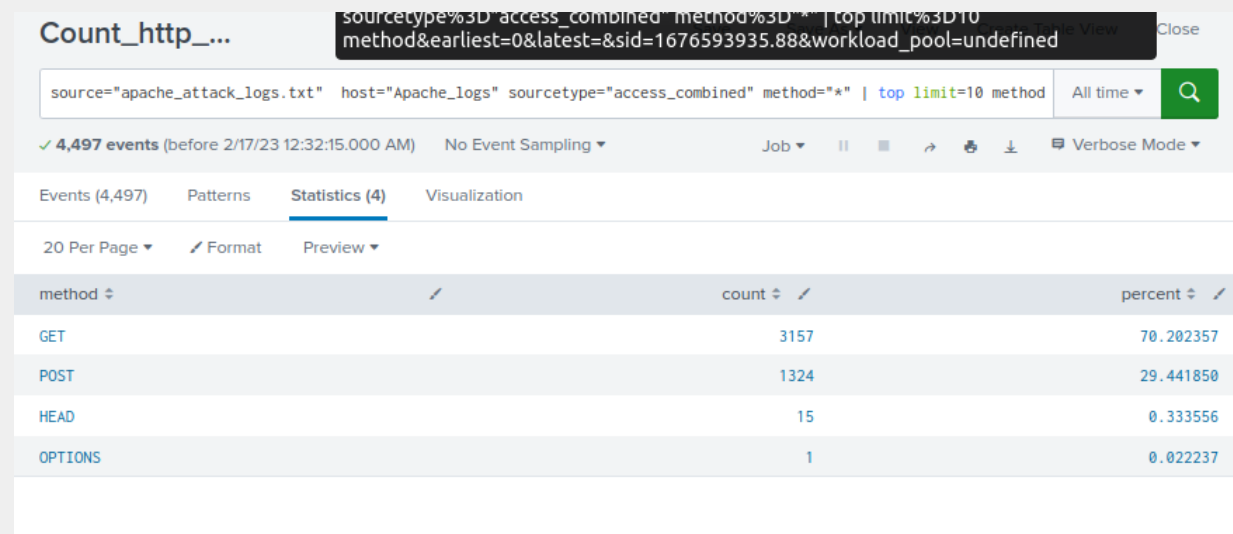
Using this report has more information in one place, whereas the panels have specific but limited information.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, the GET request method count changed from 9851 to 1357 while the POST method changed from 106 to 1324. And Head changed from 42 to 15. There was tremendous change in the POST method which jumped from 1% to 29%.



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

- Search Bar:** Contains the query `source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" method="*" | top limit=10 method`. A tooltip shows the full query: `sourcetype%3D"access_combined" method%3D"*" | top limit%3D10 method&earliest=0&latest=&sid=1676593935.88&workload_pool=undefined`.
- Results Summary:** 4,497 events (before 2/17/23 12:32:15.000 AM). No Event Sampling.
- Navigation:** Events (4,497), Patterns, **Statistics (4)**, Visualization.
- Table:** Displays the top 10 HTTP methods by count and percentage.

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?

POST method is used to send data to the server.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There was a huge drop in the count for <http://www.semicomplete.com> domain from 3038 to 764. Similarly for <http://semicomplete.com> one from 2001 to 572.

Report Analysis for HTTP Response Codes

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

_time	200	206	301	304	403	404	500
2020-03-25 10:00:00	111	0	0	0	1	4	0
2020-03-25 10:30:00	0	0	0	0	0	0	0
2020-03-25 11:00:00	111	0	0	1	0	0	0
2020-03-25 11:30:00	0	0	0	0	0	0	0
2020-03-25 12:00:00	109	0	0	2	0	1	0
2020-03-25 12:30:00	0	0	0	0	0	0	0
2020-03-25 13:00:00	111	0	0	1	0	1	0
2020-03-25 13:30:00	0	0	0	0	0	0	0
2020-03-25 14:00:00	119	0	1	0	0	1	1
2020-03-25 14:30:00	0	0	0	0	0	0	0
2020-03-25 15:00:00	123	0	1	1	0	1	0
2020-03-25 15:30:00	0	0	0	0	0	0	0
2020-03-25 16:00:00	114	0	1	1	0	2	0
2020-03-25 16:30:00	0	0	0	0	0	0	0
2020-03-25 17:00:00	112	0	2	3	0	2	0
2020-03-25 17:30:00	0	0	0	0	0	0	0
2020-03-25 18:00:00	100	3	3	0	0	624	0
2020-03-25 18:30:00	0	0	0	0	0	0	0
2020-03-25 19:00:00	120	0	2	0	0	1	0
2020-03-25 19:30:00	0	0	0	0	0	0	0
2020-03-25 20:00:00	1415	0	0	0	0	0	0
2020-03-25 20:30:00	0	0	0	0	0	0	0
2020-03-25 21:00:00	79	0	0	4	0	3	0

- On 2020-03-25 at 18:00 there were 624 - **404 response code** and the average number of 404 code responses sat around 1-5.
- On 2020-03-25 at 20:00 we had around 1415 -**200 response code**. The average amount sits around 100-120

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes we detect suspicious volume of international activity from Ukraine

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

The attack was between 7-8PM

- Would your alert be triggered for this activity?

Yes the alert would have been triggered for this activity

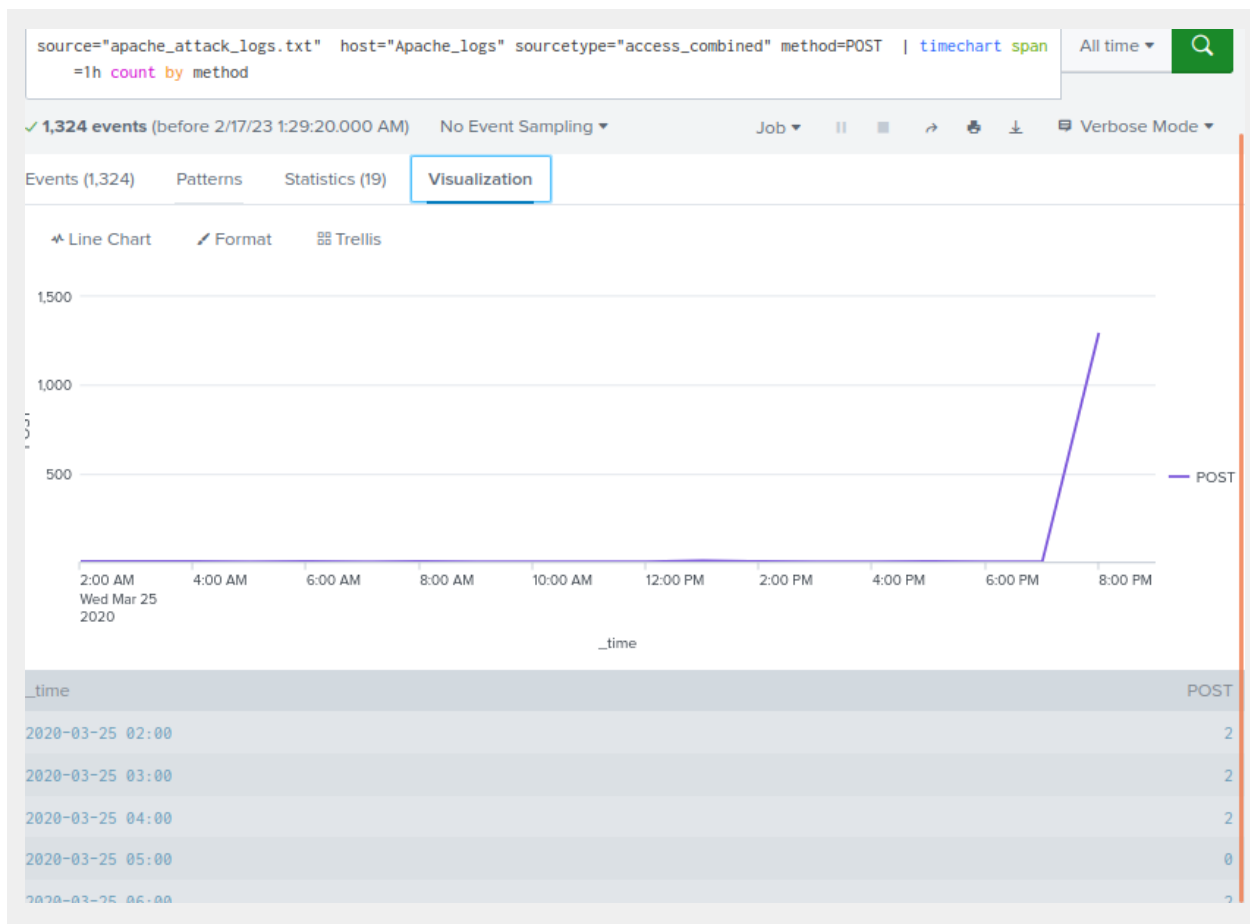
- After reviewing, would you change the threshold that you previously selected?

No, the threshold would not need to be changed from what it currently is.

Alert Analysis for HTTP POST Activity

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

Yes, the count for POST activity jumped from 7 to 1296.



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

Between 7 and 8:00 pm

- When did it occur?

Wednesday March 25th 2020, 8:00 PM

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

No, except at 8:00 PM the average alerts were below the threshold.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

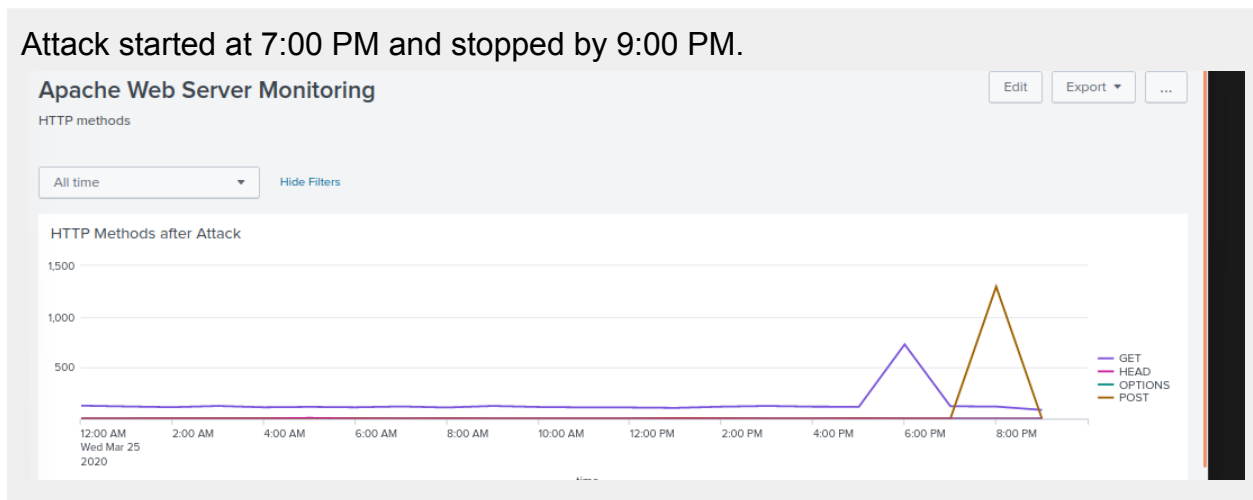
Yes,

- Which method seems to be used in the attack?

POST

- At what times did the attack start and stop?

Attack started at 7:00 PM and stopped by 9:00 PM.



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

1296

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

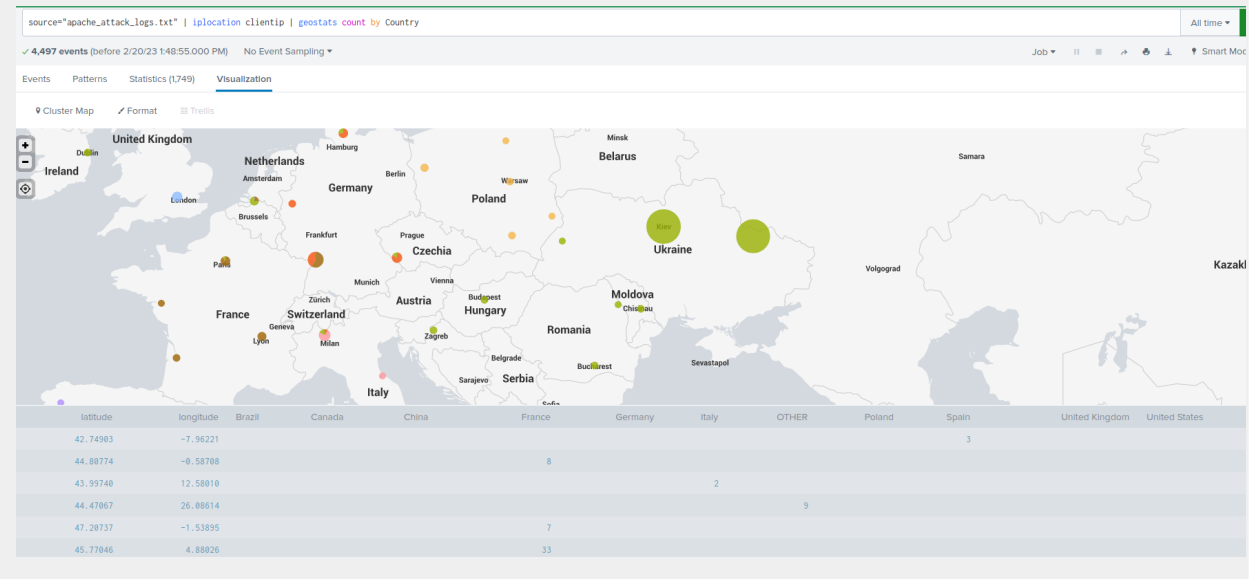
Yes. When looking at the cluster map we were able to see that Ukraine has a suspicious jump in activity.

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

The country is Ukraine and the two cities are Kiev and Kharkiv

- What is the count of that city?

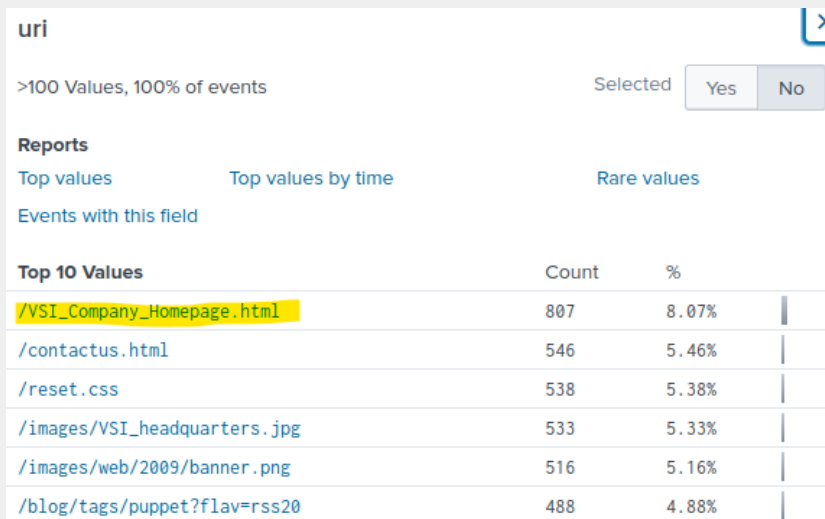
Kiev's number sits at 439 and Kharkiv sits at 433.



Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, prior to the attack the top URI was the company homepage followed by 5 pages that were averaging no more than 5% click rate



uri

>100 Values, 100% of events

Selected

Reports

Top values Top values by time Rare values

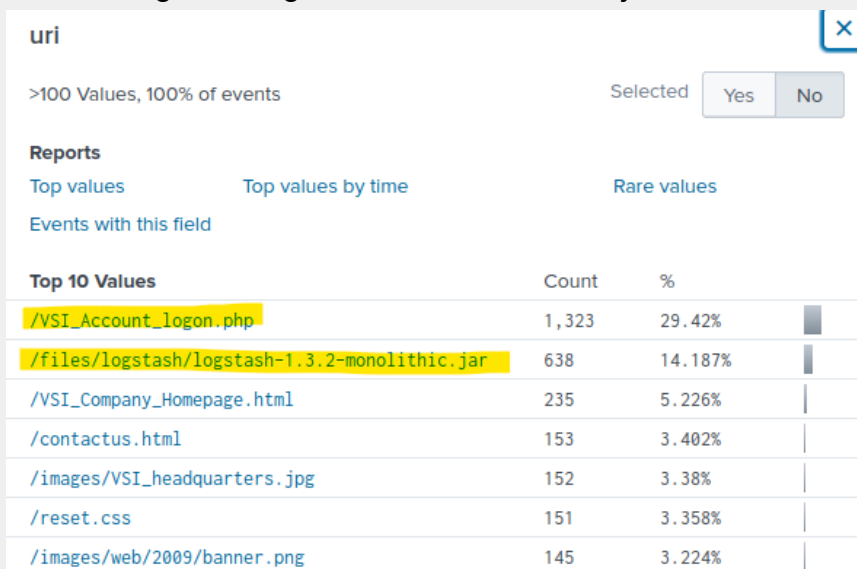
Events with this field

Top 10 Values	Count	%
/VSI_Company_Homepage.html	807	8.07%
/contactus.html	546	5.46%
/reset.css	538	5.38%
/images/VSI_headquarters.jpg	533	5.33%
/images/web/2009/banner.png	516	5.16%
/blog/tags/puppet?flav=rss20	488	4.88%

- What URI is hit the most?

1- /VSI_Account_logon.php

2- /files/logstash/logstash-1.3.2-monolithic.jar



uri

>100 Values, 100% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/VSI_Account_logon.php	1,323	29.42%
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187%
/VSI_Company_Homepage.html	235	5.226%
/contactus.html	153	3.402%
/images/VSI_headquarters.jpg	152	3.38%
/reset.css	151	3.358%
/images/web/2009/banner.png	145	3.224%

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

The attacker made attempts to brute force VSI's account logon page. The logstash file was also used to collect data from the website and transmitted to another destination.