Cybersecurity

Project 3 Review Questions

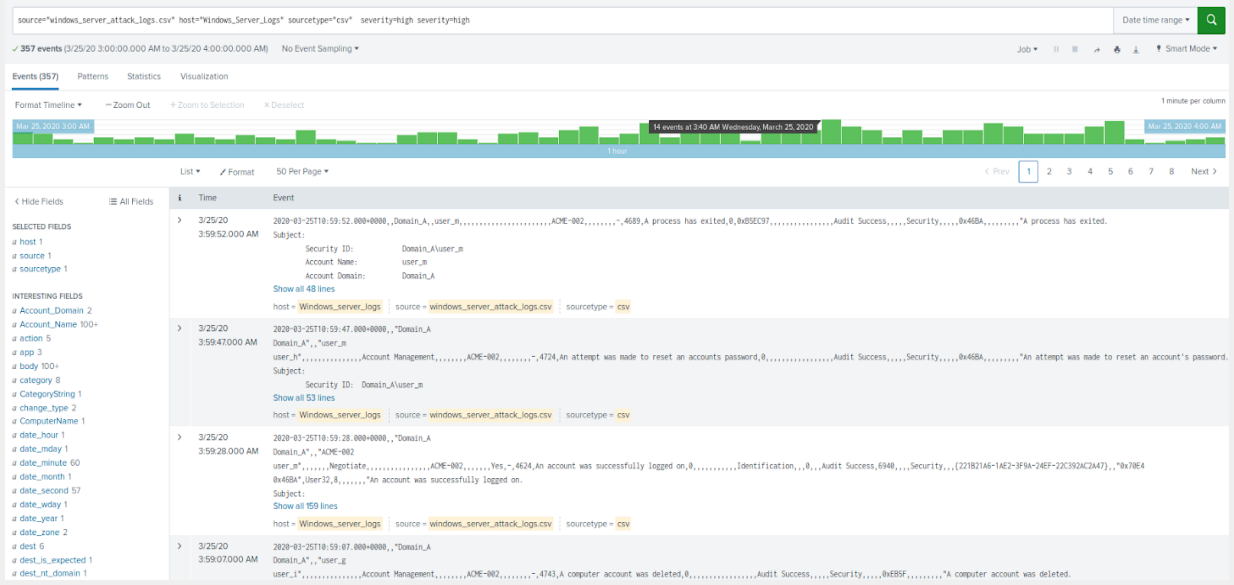
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

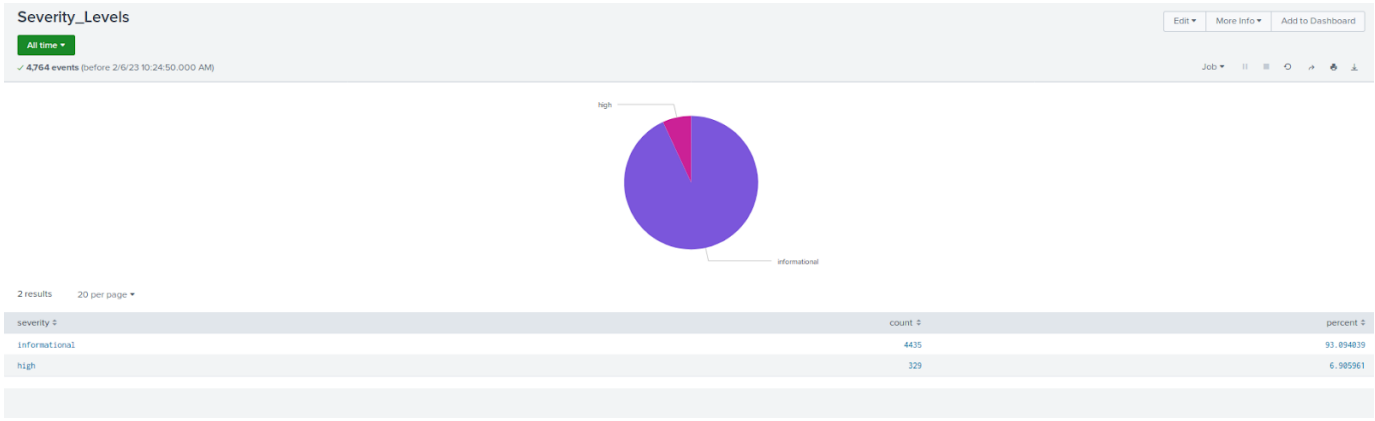
Report Analysis for Severity

- Did you detect any suspicious changes in severity?

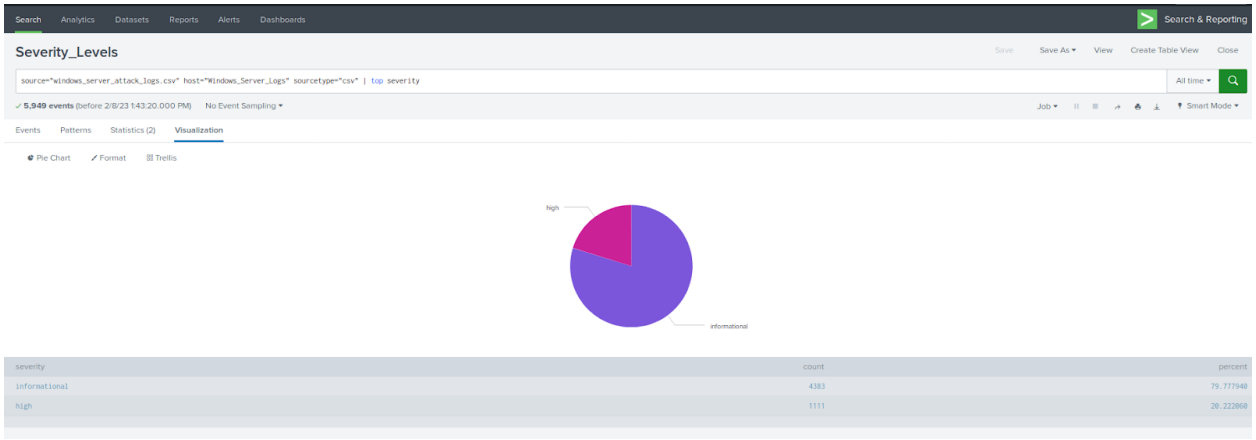
Yes - from 2AM-4AM on March 25, severity levels increased. The peaking hour for these events happened at 3AM. See the screenshot below for the 1hr.



```
source="windows_server_logs.csv" host="Windows_Server_Logs" sourcetype="csv" |
top severity
```



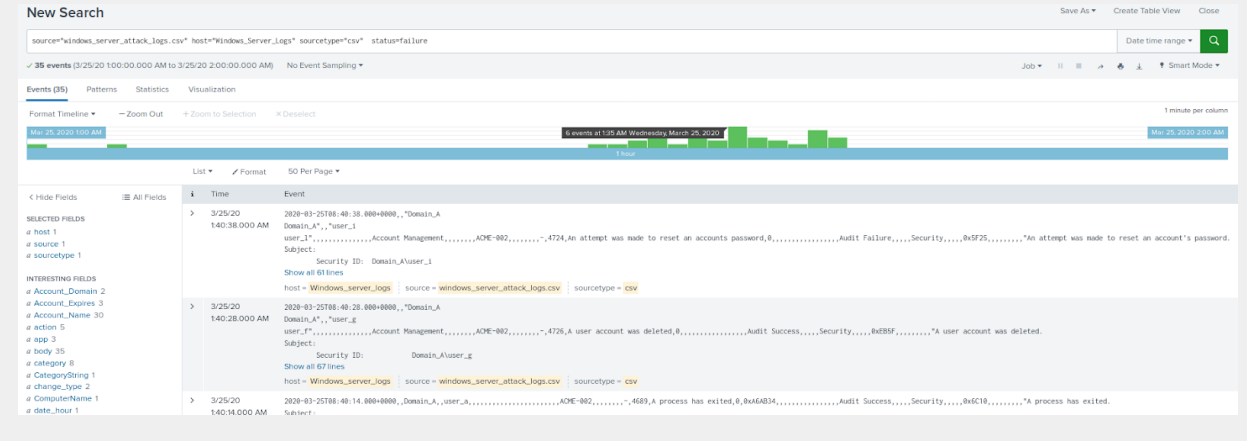

```
source="windows_server_attack_logs.csv" host="Windows_Server_Logs"
sourcetype="csv" | top severity
```

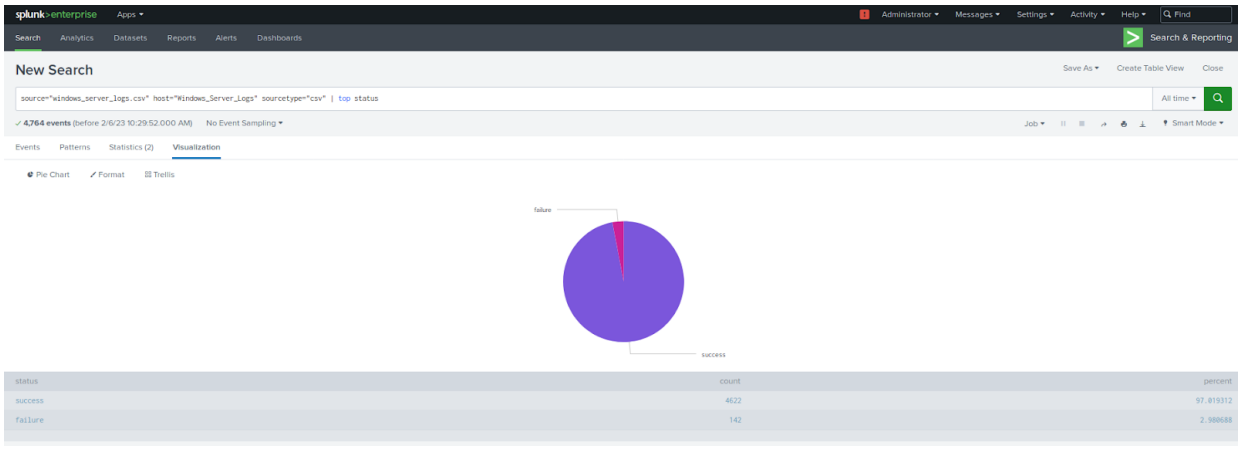


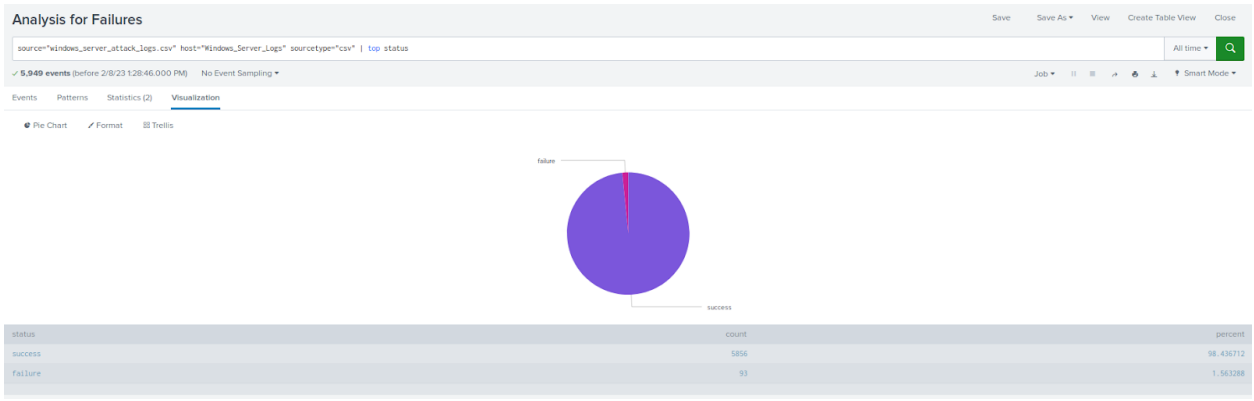
Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes - after pulling the attack log it shows on March 25 from 1:28AM-1:40AM there was an increase in failure activity, 35 events happened in this timeframe. See below:



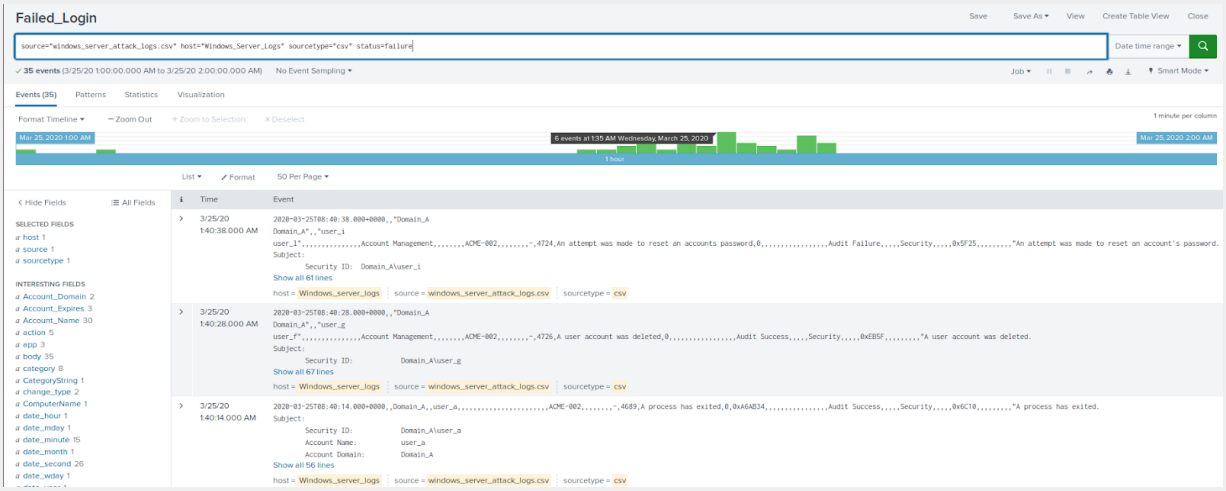




Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes - 93 events between March 24th-25th. Peaking on March 25th between 1AM-2AM.



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

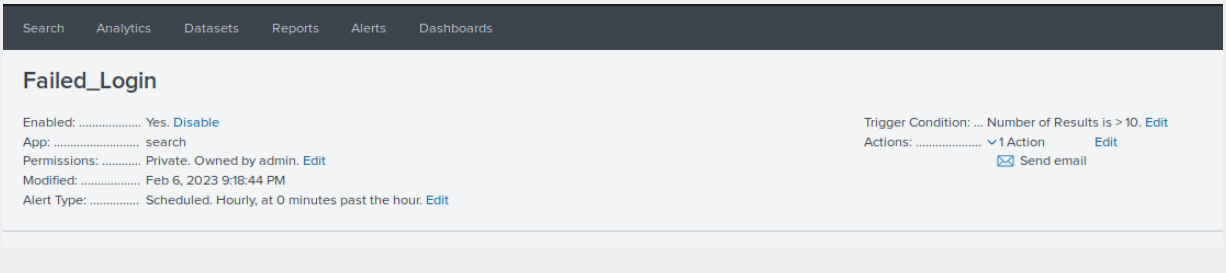
35 events

- When did it occur?

March 25th, 2020 at 1:00AM

- Would your alert be triggered for this activity?

Yes, they would be triggered.



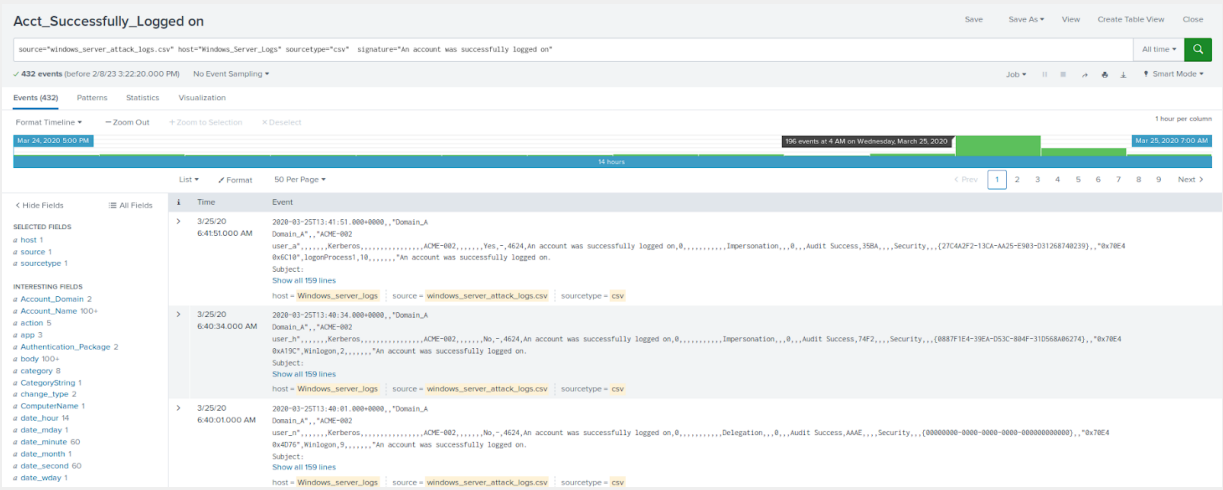
- After reviewing, would you change your threshold from what you previously selected?

No, I would not change the threshold for the alerts as it would have been triggered for review by the SOC team.

Alert Analysis for Successful Logins

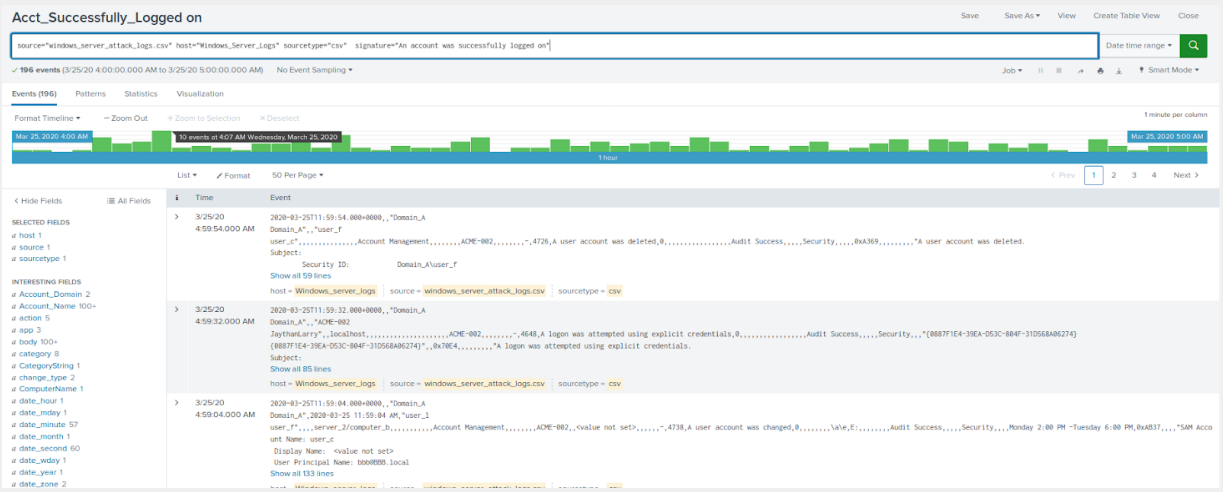
- Did you detect a suspicious volume of successful logins?

Yes, see my screenshot below:



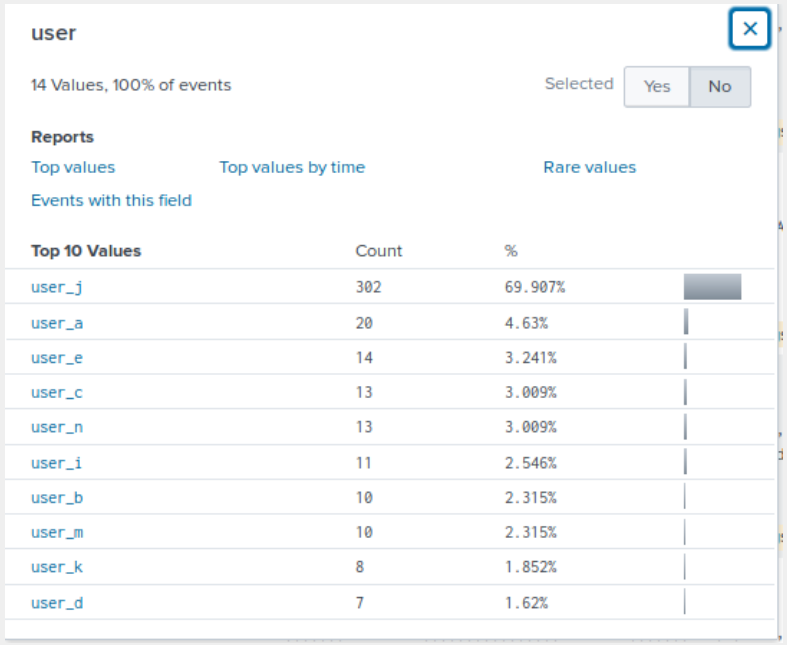
- If so, what was the count of events in the hour(s) it occurred?

196 events



- Who is the primary user logging in?

```
user_j
```

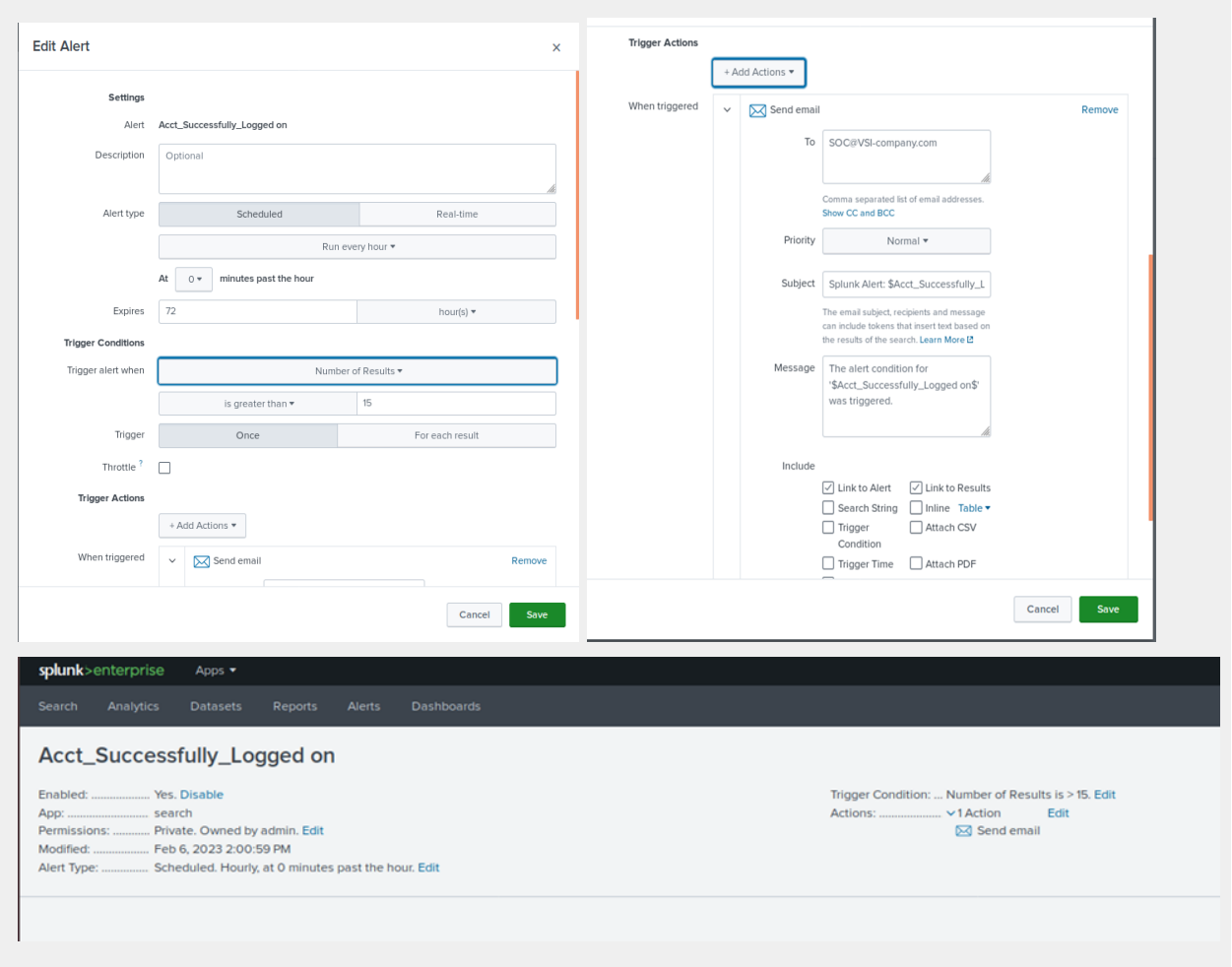


- When did it occur?

```
between 4PM-5PM on March 25th.
```

- Would your alert be triggered for this activity?

```
Yes - see my alert properties below:
```



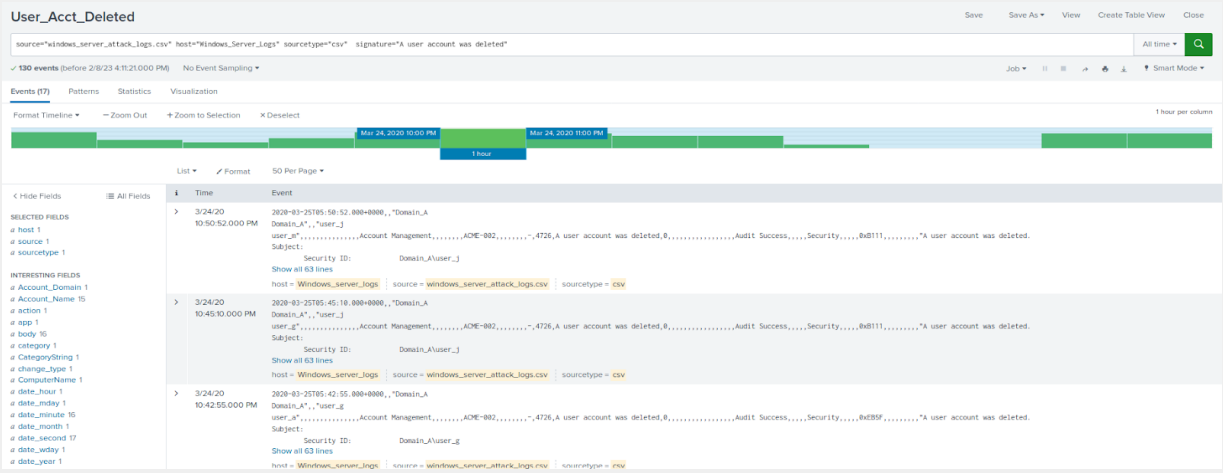
- After reviewing, would you change your threshold from what you previously selected?

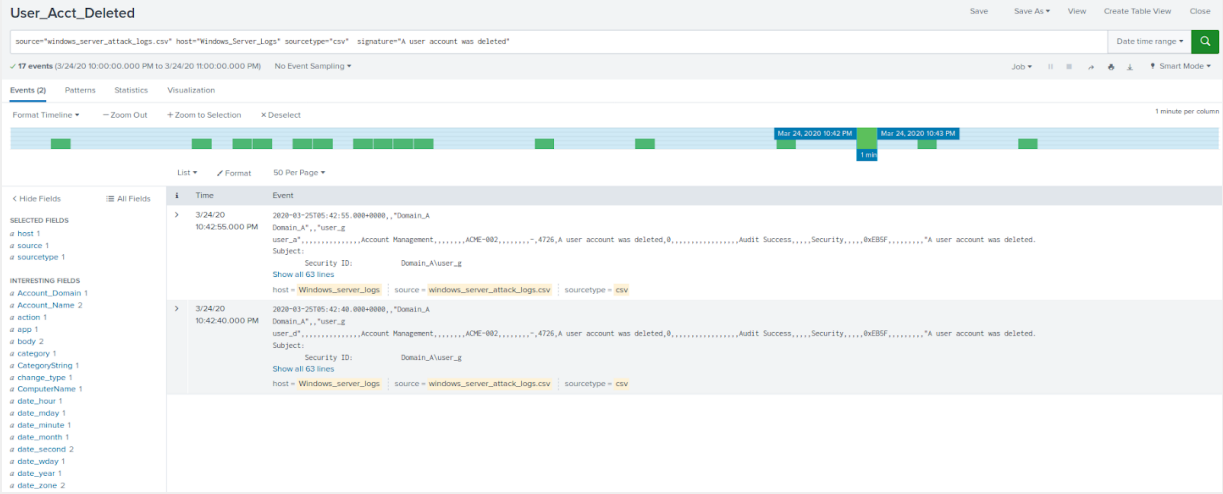
```
No - as my alert setup would trigger to the SOC team for review.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes - between March 24th-25th there were 130 events. On March 24th from 10 PM-11 PM was the highest number of deleted accounts with 17 events.

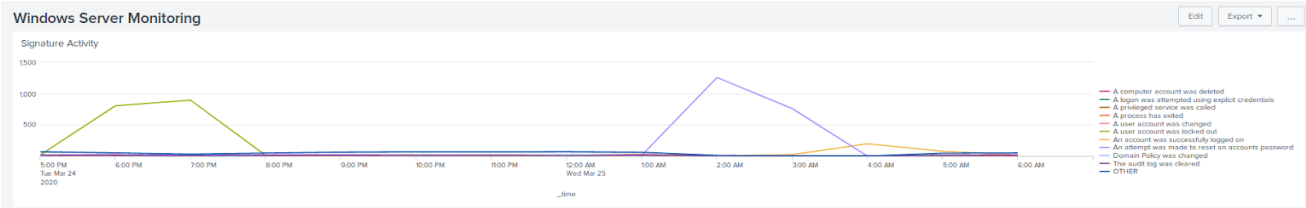




Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes - the first screenshot is prior to the attack logs and the second screenshot is after the attack logs. 3 signatures stand out from the rest.



- 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?

```
5:00PM - 8:00PM A user account was locked out
1:00AM - 4:00PM An attempt was made to reset an accounts password
3:00AM - 5:00PM An account was successfully logged on
```

- What is the peak count of the different signatures?

```
896   A user account was locked out
1,258 An attempt was made to reset an accounts password
196   An account was successfully logged on
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
All 3 events happen after normal business hours. From late evening/night and
early hours of the morning. All events have to do with user credentials for
access whether it's successful or failure.
```

- Which users stand out?

```
user_a
user_k
user_j
```

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

```
user_a 5PM-8PM
User_k 1AM-4AM
```

```
user_j 3AM-6PM
```

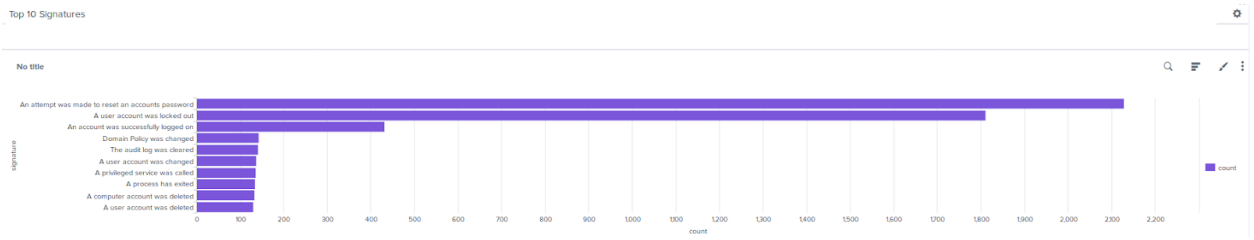
- What is the peak count of the different users?

```
user_a 984
User_k 1,256
user_j 196
```

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

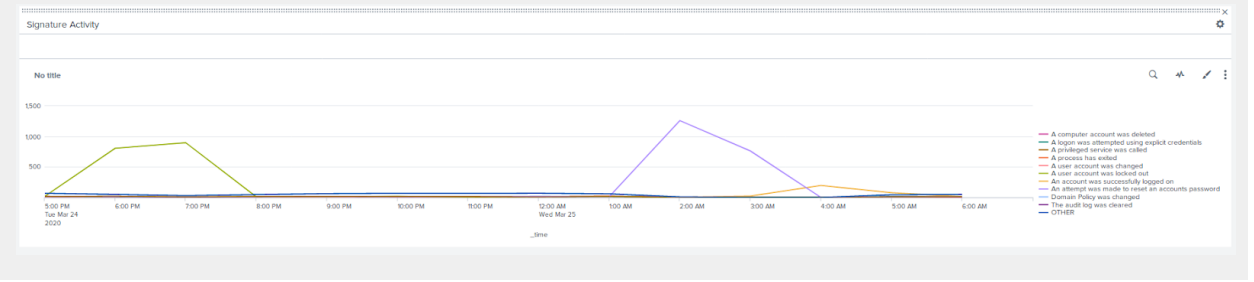
- Does anything stand out as suspicious?

```
Yes - see screenshots below: See screenshots below for the before attack logs and after. The 3 signatures stand out after the attack logs that match the alert section above.
```



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

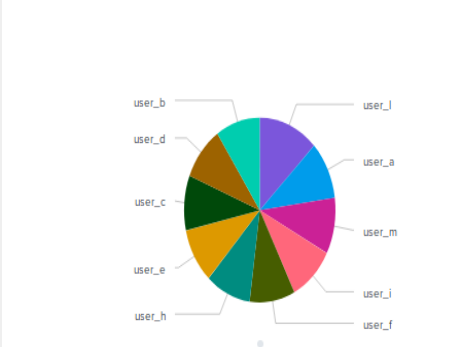
```
Yes - they match
```

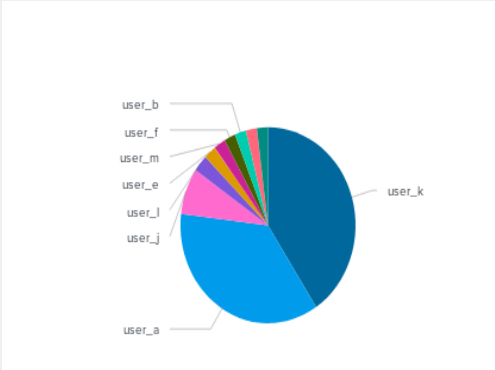


Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

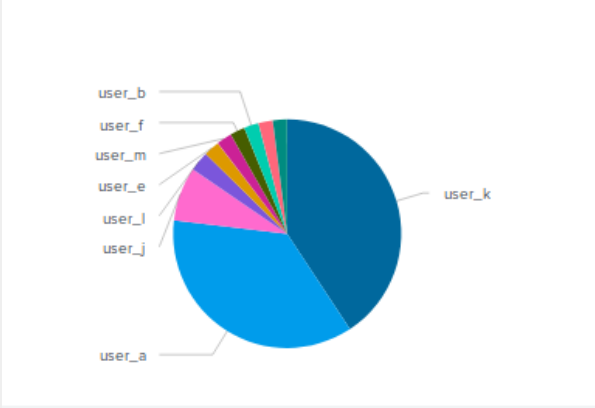
Yes - see screenshots below. For before and after attack log.

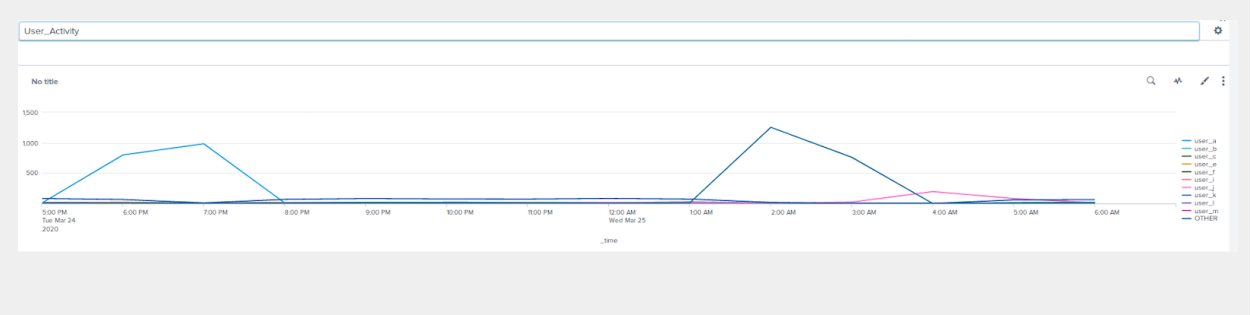




- Do the results match your findings in your time chart for users?

Yes: see results below. The 3 users stand out for both time chart and pie chart.





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?

```
High signatures can distract security teams, allowing attackers to hide
behind smaller ones remaining under the radar.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, Post was increased after attack log.
```

- What is that method used for?

```
The Post method is utilized to modify or revise the configurations of the
server's datbate.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Semicomplete remains the top referrer.
```

Report Analysis for HTTP Response Codes

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

```
There is a significant frequency of HTTP status codes 200, 304 and 404.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, from Ukraine
```

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

```
03/25/2020 8PM-9PM
```

- Would your alert be triggered for this activity?

```
Yes they were triggered.
```

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

```
No, The setup worked and alerted.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, 1296
```

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

```
Within 1 hr
```

- When did it occur?

```
03/25 8:00PM to 9:00PM.
```

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

```
No, as it worked.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, post requests was elevated.
```

- Which method seems to be used in the attack?

```
HTTP POST flood attack, possibly a DDoS.
```

- At what times did the attack start and stop?

```
Started at 03/25 8:00PM, ended at 03/25 9:00PM.
```

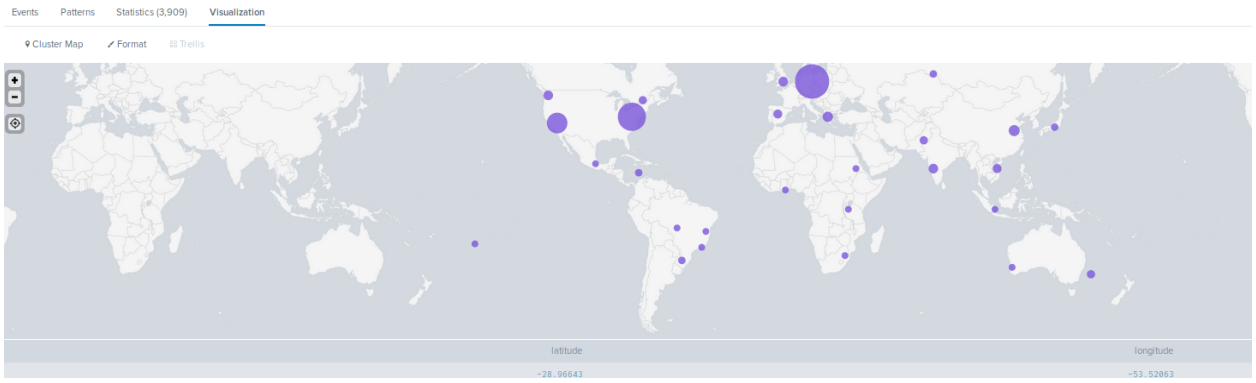
- What is the peak count of the top method during the attack?

```
Post at 1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, there’s a lot of activity in Europe.
```



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

```
Ukraine
```

- What is the count of that city?

```
877
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, there are elevated instances of accessing VSI_Account_logon.php and
logstash-1.3.2-monolithic.jar
```

- What URI is hit the most

```
VSI_account_logon.php
```

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

```
Creating or changing accounts to sabotage or ransom VSI infrastructure.
```

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.