Cybersecurity

Project 3 Review Questions

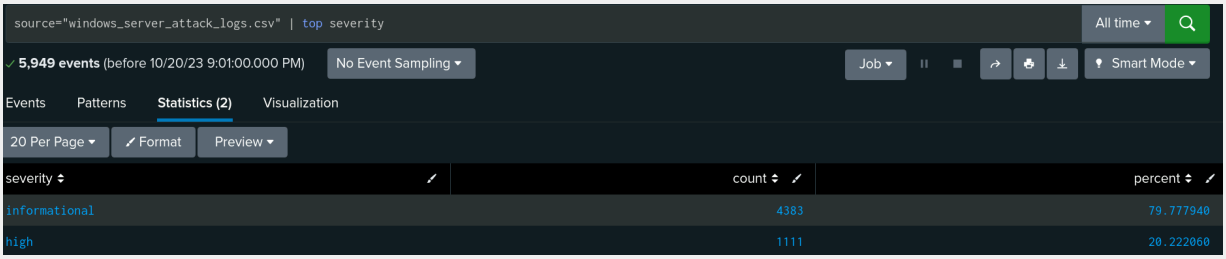
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

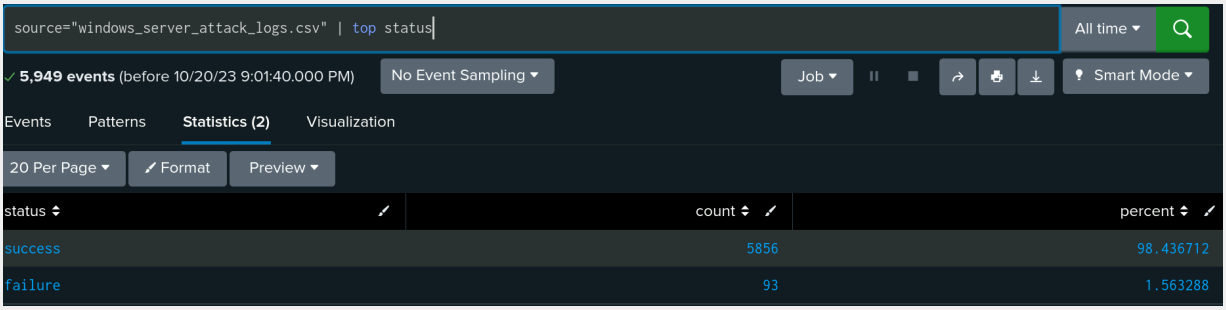
“High” severity levels went up by about 800.



Report Analysis for Failed Activities

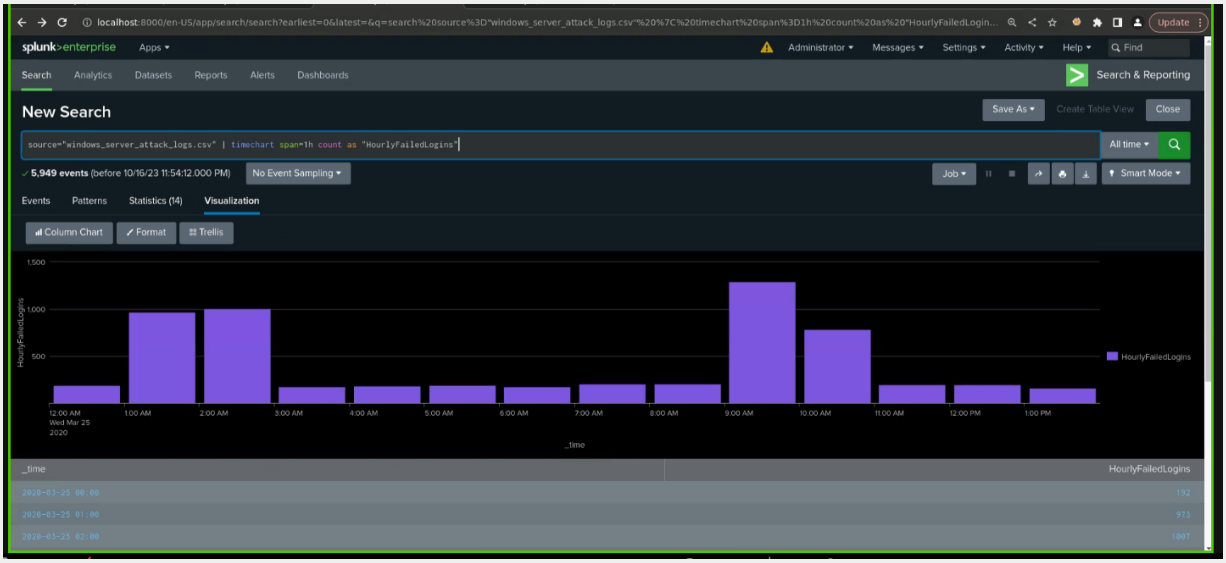
- Did you detect any suspicious changes in failed activities?

The status for failed activities decreased by about 50 events, which is not a significant change. So it isn’t suspicious…



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?



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

```
35 events at 8am
```

- When did it occur?

```
March 25, 2020
```

- Would your alert be triggered for this activity?

```
Yes it would!
```

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

```
No we would not because the suspicious activity we detected was above our baseline so alert fatigue would not be an issue for the cybersecurity term.
```

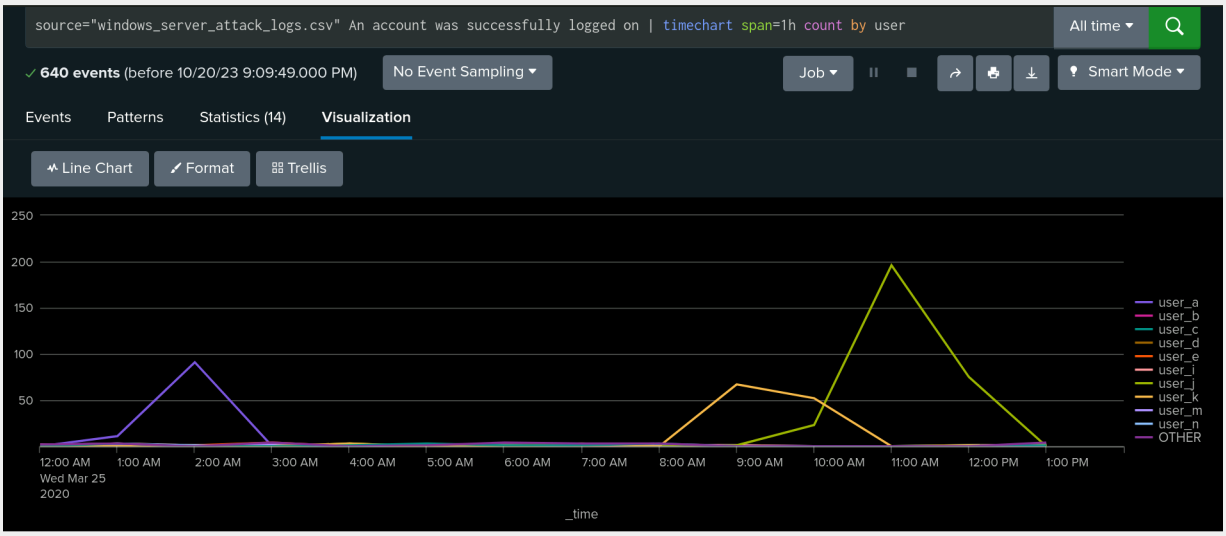
Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes
```

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

```
196 at 11 am
77 events at 12 pm
```



- Who is the primary user logging in?

```
user_j is the primary user logging in.
```

- When did it occur?

```
It occurred from 9:00AM to 1:00PM.
```

- Would your alert be triggered for this activity?

```
My alert would be triggered at 11:00AM, since my threshold is 31
```

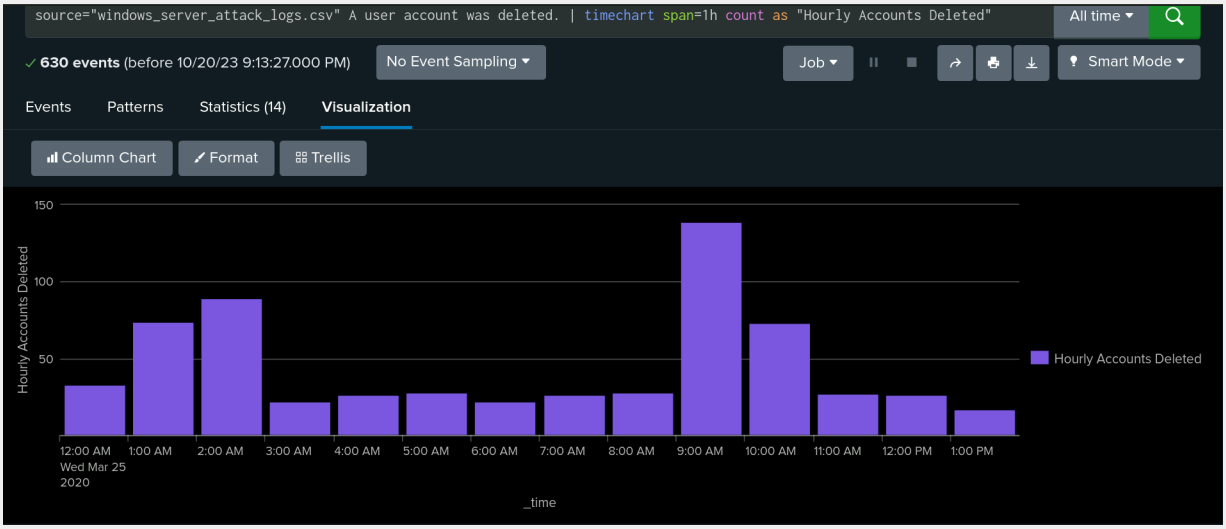
- After reviewing, would you change your threshold from what you previously selected?

```
No, my alert would have triggered only the suspicious activity that has been observed in this attack therefore I would not change it.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes



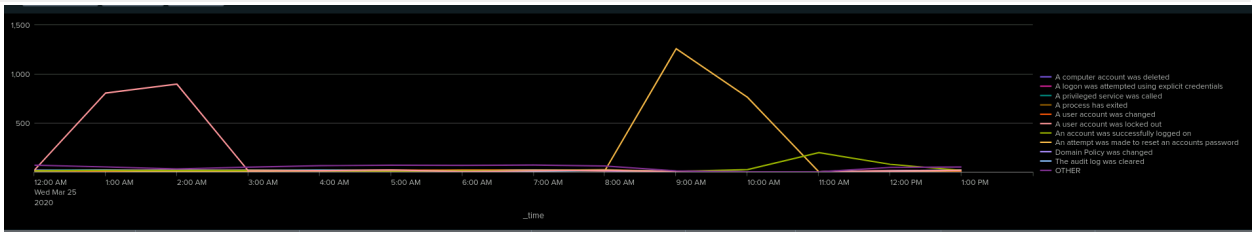
Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

The accounts were deleted in the same hours that we had a suspiciously high number of failed logins.

- What signatures stand out?

The signatures that stand out are:
1. A user account was locked out
2. An attempt was made to reset an accounts password



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

1. A user account was locked out - 1:00AM to 2:00AM
2. An attempt was made to reset an accounts password - 9:00AM to 10:00AM

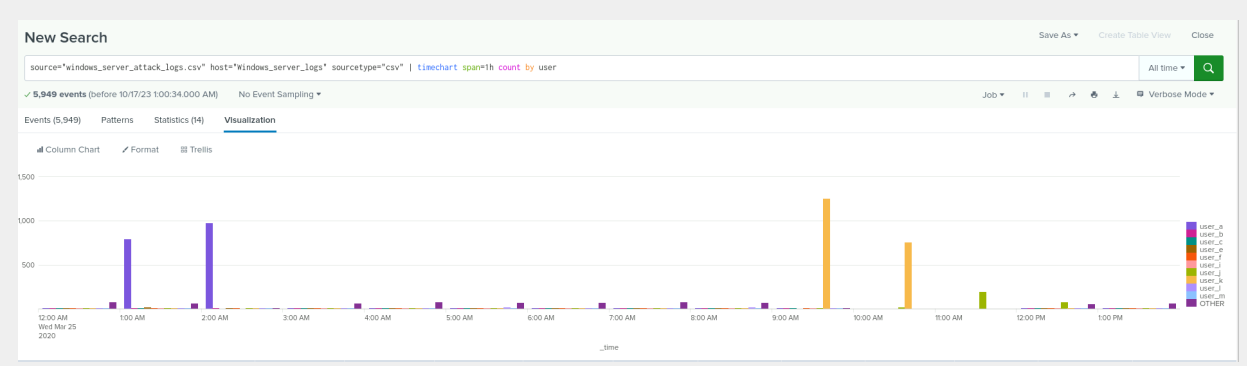
- What is the peak count of the different signatures?

1. A user account was locked out - 896
2. An attempt was made to reset an accounts password - 1258

Dashboard Analysis for Users

- Does anything stand out as suspicious?

There's a large amount of activity at the same times as listed earlier, 1:00AM, 2:00AM, 9:00AM, and 10:00AM



- Which users stand out?

```
user_a, and user_k
```

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

```
user_a - 1:00AM to 2:00AM
user_k - 9:00AM to 10:00AM
```

- What is the peak count of the different users?

```
user_a - 984
user_k - 1256
```

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

- Does anything stand out as suspicious?

```
There’s a large amount of activity at the same times as listed earlier,
1:00AM, 2:00AM, 9:00AM, and 10:00AM
```

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

```
Yes, the results matched my findings. The attacker(s) was/were busy in the
same time frame that these suspicious activities were taking place.
```

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

- Does anything stand out as suspicious?

```
There's a large amount of activity at the same times as listed earlier,
1:00AM, 2:00AM, 9:00AM, and 10:00AM
```

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

```
Yes, the results matched my findings. One graph showed that in the hours
that there was a lot of activity during the hours mentioned above which
reflects the hours that user_a and user_k were being used for their
"nefarious" activities.
```

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?

```
It's easier to interpret the information on the line graph because it
clearly displays the outlier data points, whereas picking this same data on
the pie chart isn't as intuitive.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, suspicious changes were found. We saw a new country have a large
increase in traffic to the site. We saw the HTTP method change from having a
majority of GET requests and changing to a majority of POST requests, our
User Agents changed drastically from having 10 to having only 2, and the URI
top path changed from the homepage to a logon page. The most concerning is
the change for POST method.
```

- What is that method used for?

```
POST is used to submit data to a server, to create/update a resource.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes, suspicious activity was found, specifically in the www.semicomplete.com
domain. From a combined 5039 referrals which then showed a decrease during
the attack to only 1336 referrals.
```

Report Analysis for HTTP Response Codes

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

```
Yes, suspicious activity was found, specifically in the 200 response
code.The 200 response code decreased from 9126 responses to 3746 responses.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, we detected multiple suspicious volumes of international activity on
Wednesday, March 25th. We had a significant surge at 08:00PM in
international activity, 937 events during that hour.
```

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

```
Our alert would have triggered 11 times, since we had the alert set to 80.
We would have had triggers at 12AM, 1AM, 2AM, 3AM, 4AM, 5AM, 7AM, 9AM, 10AM,
7PM and 8PM.
```

- Would your alert be triggered for this activity?

```
Yes, our alert would have triggered at each of those hours.
```

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

```
After reviewing, yes, I would change the threshold. I would increase it by a large margin. Our baseline was set way too low. We would be inundated with alerts almost hourly if we kept it at 80.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, a suspicious volume of activity for HTTP POST activity was detected. Prior to the attack POST rarely went over 3 instances, during the peak of the attack POST went to a high of 1296 instances.
```

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

```
The activity occurred only once, for our baseline, 1296 events specifically in a one hour period.
```

- When did it occur?

```
March 25th, 2020 at 08:00 PM
```

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

```
After reviewing, no I wouldn’t change the threshold.As stated before, typically the instances for POST doesn’t exceed 3.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, a few things stand out as suspicious.
```

- Which method seems to be used in the attack?

```
POST
```

- At what times did the attack start and stop?

```
08:00PM March 25, 2020 it hit its peak. It was over by 09:00PM.
```

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

```
1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Europe had a large surge in volume. Specifically one new country.
```

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

```
Kyiv, Ukraine
```

- What is the count of that city?

```
887
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
The URI count changed significantly. From a max of approx 800 to a new high
of 1323.
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
Trying to login to an account that they don’t actually have access to.
```