



# 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. The informational severity count went from 4429 at 93% in the Windows\_server\_logs.csv to 4381 at 80% in the Windows\_server\_attack\_logs.csv. The high severity count went from 329 at 7% to 1111 at 20% in the Windows\_server\_attack\_logs.csv.

#### Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

OG Success: 4616  
OG Fail: 142  
Attack log Success: 5854  
Attack log Fails: 93

#### Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes, there were 35 failed windows activity in one hour.

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

There were 35 events in hour 08:00.

- When did it occur?

08:00

- Would your alert be triggered for this activity?

Yes, we set our threshold at 20

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

No, the set threshold was able to detect the suspicious activity.

## Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, we detected an abnormal amount of logins of 196 at 11:00 and 77 logins at 12:00

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

196 successful logins occurred at 11:00 on Wednesday, March 25, 2020.  
77 successful logins occurred at 12:00 on Wednesday, March 25, 2020.

- Who is the primary user logging in?

user\_j

- When did it occur?

196 successful logins occurred at 11:00 on Wednesday, March 25, 2020.  
77 successful logins occurred at 12:00 on Wednesday, March 25, 2020.

- Would your alert be triggered for this activity?

No, the signature\_id targeted at 4624 prevents the alert being triggered.  
When the signature\_id is removed, the suspicious logins will be detected.

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

The threshold wouldn't need to change but the signature id that we used to identify the logins might need to be adjusted.

### **Alert Analysis for Deleted Accounts**

- Did you detect a suspicious volume of deleted accounts?

No we did not.

### **Dashboard Analysis for Time Chart of Signatures**

- Does anything stand out as suspicious?

Yes

- What signatures stand out?

A user account was locked out (count 896)  
An attempt was made to reset an account password (count 1258)

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

A user account was locked out: 00:00 to 03:00 03/25/20  
An attempt was made to reset an account password: 08:00 to 11:00 03/25/20

- What is the peak count of the different signatures?

A user account was locked out peak count of 896

An attempt was made to reset an account password peak count of 1258

## Dashboard Analysis for Users

- Does anything stand out as suspicious?

Suspicious user activity

user\_a 984 logins

user\_k 1256 logins

user\_j 196 logins

Attempts to reset account passwords (2128)

Account locked out (1811)

- Which users stand out?

user\_a

user\_k

user\_j

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

user\_a started at 00:00 and stopped at 03:00

user\_k started at 08:00 and stopped at 11:00

user\_j started at 10:00 and stopped at 13:00

- What is the peak count of the different users?

user\_k at 2118

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

- Does anything stand out as suspicious?

There are a suspicious amount of attempts to reset an account's password and users locked out.

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

Yes

A User account was locked out (1,811 times)

An attempt was made to reset password (2,128 times)

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

- Does anything stand out as suspicious?

Yes

user\_k and user\_a had suspiciously high event logs

High levels of attempts to reset account password

High levels of account locked out

- 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?

Diverse visualization of reports in a user-friendly GUI

## Apache Web Server Log Questions

### Report Analysis for Methods

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

Yes, there is a significant increase in POST

- What is that method used for?

POST puts information onto the server.

## Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

All the referral websites total counts went down overall.

For example:

http://[www.semicomplete.com](http://www.semicomplete.com) went from 3038 to 764

## Report Analysis for HTTP Response Codes

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

The amount of status code 200 went down significantly from ~9000 to ~3700 and the amount of status code 404 went up from 213 to 679

There was a significant increase in 404 status code from 213 to 679

## Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

There was a stark increase in international activity during hour 20:00.

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

There was a count of 939 international activities during hour 20:00.

- Would your alert be triggered for this activity?

Yes.

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

No, our threshold of 334 would have successfully notified us of the suspicious activity.

### **Alert Analysis for HTTP POST Activity**

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

YES

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

There were 1296 POST requests

- When did it occur?

20:00 on Wednesday March 25, 2020

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

No, our threshold was set to 10.

### **Dashboard Analysis for Time Chart of HTTP Methods**

- Does anything stand out as suspicious?

Yes, both POST and GET stand out as having a large spike.

- Which method seems to be used in the attack?

POST(1296 count)

- At what times did the attack start and stop?

19:00 to 21:00

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

The peak count was 1296 POST requests at 20:00 on March 25, 2020

### Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Non-US country login attempts, with high rates in East Asia.

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

Kiev, Ukraine

- What is the count of that city?

432

### Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, there are high rates of VSI account logon (1323)

- What URI is hit the most?

Other (count 1466)

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



The attacker is attempting to logon to the VSI website, possibly with a Brute Force Attack.