| 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 detected changes in severity, the biggest suspicious change for high severity events. The value increased from 7% to 20% during the attack  Attack Log:    Normal Log: |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| Yes, we detected suspicious changes in failed activities between normal and attack logs. There was an increase in successful activities and decrease in failed activities.  **Normal Logs:**    **Attack Logs:** |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes our alert did detect a volume of failed Windows activity that was suspicious |
| --- |

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

| [The count was 35 failed Windows activities at 8am] |
| --- |

* When did it occur?

| March 25, 2020 at 8:00am |
| --- |

* Would your alert be triggered for this activity?

| [Yes, it is way above the threshold of 15: |
| --- |

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

| No, the threshold built for VSI would is at > 15, which did trigger and an email was sent to [SOC@VSI-company.com](mailto:SOC@VSI-company.com). The Alert is set high enough to ensure that normal usage will not cause alert fatigue |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| After review of the logs, we determined there was a suspicious amount of logins, not due to an abundance of logins but rather a lack of logins.  Normal Logs:  Attack Logs: |
| --- |

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

| March 25, 2020 at 8:00am there were 16 total successful logins then dropped to 4 by 9:00am and is at 0 from 10-11am then goes back up to 4 logins at 12:00pm |
| --- |

* Who is the primary user logging in?

| Normal Logs:    Attack Logs:    Upon further review of the logs, user\_a logins spiked at around 2:30am with 10 logins |
| --- |

* When did it occur?

| March 25, 2020 at 2:30am |
| --- |

* Would your alert be triggered for this activity?

| No, our alert would not have triggered. VSI has a threshold of greater than 30 and this would not have alerted. |
| --- |

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

| Yes, the alert threshold should be modified, but more log data needs to be analyzed to determine a proper number to avoid failure fatigue. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| [Normal logs :  Attack logs:  Yes, but not in excessive numbers. During the attack between 9am-11am there was a significant decrease in account deletions] |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Normal logs:    Attack logs: |
| --- |

* What signatures stand out?

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

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

| A user account was locked out:  Mar 25, 2020 1:00am - 2:00am   An attempt was made to reset an account password:  Mar 25, 2020 9:00am - 10:00am |
| --- |

* What is the peak count of the different signatures?

| A user account was locked out:  896  An attempt was made to reset an account password:  1268 |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes, There is a significant increase in user activity for 2 users  Normal Logs:  Attack Logs: |
| --- |

* Which users stand out?

| The 2 users that stand out due to increased activity is: 1. User\_a  2. User\_k |
| --- |

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

| User\_a had increased activity between the hours of 1:00am to 2:30am User\_k had increased activity between the hours of 9:00am to 10:00am |
| --- |

* What is the peak count of the different users?

| User\_a peaked at 984  User\_k peaked at 1256 |
| --- |

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

* Does anything stand out as suspicious?

| We can see a significant increase in two signature types:   1. an attempt was made to reset a account 2. A user account was locked out   Normal Logs:  Attack Logs:    Pie Chart:  Normal Logs:    Attack Logs: |
| --- |

* 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?

| Normal Logs:  Pie Chart:    Attack Logs:    Pie Chart: |
| --- |

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

| Yes they do |
| --- |

**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?

| There are many differences in using statistical charts vs using visual charts. An advantage of using a statistical time chart for signatures and users is that you can easily see when and where there may be anomalies per hour. A disadvantage of using these over the bar graph or pie chart visualizations is that it may not be as obvious where the change occurred. Where the benefit of the visualiztions is that you can see which event or use has an increase in 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 detected suspicious changes in HTTP methods, specifically with POST there was an increase of 1,218 during the attack  Normal Apache Logs:    Attack Logs: |
| --- |

* What is that method used for?

| POST is used to send data from the client to the server |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| We saw some changes in the results of the top 10 referrer domains, specifically with the last 5 of the list  Normal logs:  attack logs: |
| --- |

**Report Analysis for HTTP Response Codes**

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

| We detected a suspicious change in HTTP response codes, specifically with response code 200 and 404. Response code 200 had a significant decrease while response code 404 saw an increase during the attack.  Normal logs:    Attack logs: |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| [A volume of suspicious international activity was detected  Normal logs:    Attack logs: |
| --- |

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

| 937 on March 20, 2020 at around 12 AM |
| --- |

* Would your alert be triggered for this activity?

| [Yes, the alert would have been triggered as the threshold was set to more than 150 in an hour to send an alert and this was above that] |
| --- |

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

| [I would keep the threshold the same, but continue to monitor the Apache logs to see if we could raise the threshold amount in the future] |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Normal Logs:    Attack Logs: |
| --- |

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

| The count was 1296 at 8:00 pm |
| --- |

* When did it occur?

| 8 pm on March 25, 2020 |
| --- |

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

| After reviewing, I would decrease the number from 15 to 10 minutes |
| --- |

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

* Does anything stand out as suspicious?

| Yes, we can see a significant spike in the POST and GET Method  Normal Logs:  Attack Logs: |
| --- |

* Which method seems to be used in the attack?

| POST |
| --- |

* At what times did the attack start and stop?

| It occurred between the hours of 7:00pm to 9:00pm |
| --- |

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

| 1296 was the peak |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| Normal Logs:    Attack Logs: |
| --- |

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

| There was a major increase in Kiev and Karkhev |
| --- |

* What is the count of that city?

| Kiev: Count of 440.  Kharkiv: Count of 432 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes, the URI Chart shows suspicious activity  Normal Logs:  Attack logs: |
| --- |

* What URI is hit the most?

| VSI\_Account\_logon.php was the most hit URL |
| --- |

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

| Based on the URI being accessed the attacker could potentially be trying a brute force attack or an SQL injection.Factoring in the large amounts of 404 errors would help us to better narrow it down to an attacker scanning the network through a brute force attempt in an effort to gain information through reconnaissance. |
| --- |

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.