## **Activity File: Part 2 - Defend Your SOC**

* VSI recently experienced several cyberattacks, likely from their adversary JobeCorp.
* Fortunately, your SOC team had set up several monitoring solutions to help VSI quickly identify what was attacked.
* These monitoring solutions will also help VSI create mitigation strategies to protect the organization.

You have been provided two logs files of suspicious activity:

* One for a Windows server
* One for an Apache web server

### **Windows Server Logs**

Load the logs in your Splunk environment.

* Select all default options provided.
* **Important:** For the time range, always select **All Time**.  
   - **Important:** For the time range, always select **All Time**.
* **Important:** For the time range, always select **All Time**.

Now you will review the reports you created in Part 1 and analyze the results.

#### **Report Analysis for Severity**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report you created to analyze the different severities.
3. Select **Edit** > **Open in Search**.
4. Take note of the percentages of different severities.
5. Change the source from windows\_server\_logs.csv to "source="windows\_server\_attack\_logs.csv
6. Select **Save**.

Review the updated results and answer the following question:

* Did you detect any suspicious changes in severity?

#### **Report Analysis for Failed Activities**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report you created to analyze the different activities.
3. Select **Edit** > **Open in Search**.
4. Take note of the failed activities percentage.
5. Change the source from windows\_server\_logs.csv to "source="windows\_server\_attack\_logs.csv.
6. Select **Save**.

Review the updated results and answer the following question:

* Did you detect any suspicious changes in failed activities?

Now you will review the alerts you created in Part 1 and analyze the results.

#### **Alert Analysis for Failed Windows Activity**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert for suspicious volume of failed activities.
3. Select **Open in Search**.
4. Change the source from windows\_server\_logs.csv to "source="windows\_server\_attack\_logs.csv.

Review the updated results and answer the following questions:

* Did you detect a suspicious volume of failed activity?
* If so, what was the count of events in the hour(s) it occurred?
* When did it occur?
* Would your alert be triggered for this activity?
* After reviewing, would you change your threshold from what you previously selected?

#### **Alert Analysis for Successful Logons**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of successful logons.
3. Select **Open in Search**.
4. Change the source from windows\_server\_logs.csv to "source="windows\_server\_attack\_logs.csv.

Review the updated results, and answer the following questions:

* Did you detect a suspicious volume of successful logons?
* If so, what was the count of events in the hour(s) it occurred?
* Who is the primary user logging in?
* When did it occur?
* Would your alert be triggered for this activity?
* After reviewing, would you change your threshold from what you you previously selected?

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

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of deleted accounts.
3. Select **Open in Search**.
4. Change the source from windows\_server\_logs.csv to "source="windows\_server\_attack\_logs.csv.

Review the updated results and answer the following question:

1. Did you detect a suspicious volume of deleted accounts?

Now you will set up a dashboard and analyze the results.

#### **Dashboard Setup**

1. Access the **Apache Webserver Monitoring** dashboard.  
   * Select **Edit**.
2. Access each panel you created and complete the following:  
   * Select **Edit Search**.
   * Change the source from: windows\_server\_logs.csv to source="windows\_server\_attack\_logs.csv.
   * Select **Apply**.
   * Save the dashboard.
   * Edit the time on the dashboard to be **All Time**.

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

Analyze your new dashboard results and answer the following questions:

* Does anything stand out as suspicious?
* What signatures stand out?
* What time did it begin/stop for each signature?
* What is the peak count of the different signatures?

#### **Dashboard Analysis for Users**

Analyze your new dashboard results and answer the following questions:

* Does anything stand out as suspicious?
* Which users stand out?
* What time did it begin and stop for each user?
* What is the peak count of the different users?

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

Analyze your new dashboard results and answer the following questions:

* Does anything stand out as suspicious?
* Do the results match your findings in your time chart for signatures?

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

Analyze your new dashboard results, and answer the following questions:

* Does anything stand out as suspicious?
* Do the results match your findings in your time chart for users?

#### **Dashboard Analysis for Users with Statistical Charts**

Analyze your new dashboard results, and answer the following question:

* What are the advantages and disadvantages of using this report, compared to the other user panels you created?

### **Apache Web Server Logs**

Load the logs in your Splunk environment.

* Select all default options provided.
* **Important:** For the time range, always select **All Time**.

Now you will review the reports you created in Part 1 and analyze the results.

#### **Report Analysis for Methods**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report that analyzes the different HTTP methods.
3. Select **Edit** > **Open in Search**.
4. Take note of the percent/count of the various methods.
5. Change the source from: source=apache\_logs.txt to source="apache\_attack\_logs.txt.
6. Select **Save**.

Review the updated results and answer the following questions:

1. Did you detect any suspicious changes in HTTP methods? If so which one?
2. What is that method used for?

#### **Report Analysis for Referrer Domains**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report that analyzes the different referrer domains.
3. Select **Edit** > **Open in Search**.
4. Take note of the different referrer domains.
5. Change the source from: source=apache\_logs.txt to source="apache\_attack\_logs.txt.
6. Select **Save**.

Review the updated results, and answer the following question:

1. Did you detect any suspicious changes in referrer domains?

#### **Report Analysis for HTTP Response Codes**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report that analyzes the different HTTP response codes.
3. Select **Edit** > **Open in Search**.
4. Take a note of the different HTTP response codes.
5. Change the source from: source=apache\_logs.txt to source="apache\_attack\_logs.txt.
6. Select **Save**.

Review the updated results and answer the following question:

1. Did you detect any suspicious changes in HTTP response codes?

Now you will review the alerts you created in Part 1 and analyze the results.

#### **Alert Analysis for International Activity**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of international activity.
3. Select **Open in Search**.
4. Change the source from: source=apache\_logs.txt to source="apache\_attack\_logs.txt.

Review the updated results and answer the following questions:

* Did you detect a suspicious volume of international activity?
* If so, what was the count of the hour it occurred in?
* Would your alert be triggered for this activity?
* After reviewing, would you change the threshold you previously selected?

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

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of HTTP POST activity.
3. Select **Open in Search**.
4. Change the source from: source=apache\_logs.txt to source="apache\_attack\_logs.txt.

Review the updated results, and answer the following questions:

* Did you detect any suspicious volume of HTTP POST activity?
* If so, what was the count of the hour it occurred in?
* When did it occur?
* After reviewing, would you change the threshold that you previously selected?

Now you will set up a dashboard and analyze the results.

#### **Dashboard Setup**

* Access the dashboard for Apache Webserver Monitoring.
* Select **Edit**.
* Access each panel and complete the following:  
  + Select **Edit Search**.
  + Change the source from: source=apache\_logs.txt to source="apache\_attack\_logs.txt
  + Select **Apply**.
* Save the whole dashboard.
* Edit the time on the whole dashboard to be **All Time**.

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

Analyze your new dashboard results and answer the following questions:

* Does anything stand out as suspicious?
* Which method seems to be used in the attack?
* At what times did the attack start and stop?
* What is the peak count of the top method during the attack?

#### **Dashboard Analysis for Cluster Map**

Analyze your new cluster map results and answer the following questions:

* Does anything stand out as suspicious?
* Which new city, country on the map has a high volume of activity?  
  + **Hint:** Zoom in on the map.
* What is the count of that city?

#### **Dashboard Analysis for URI Data**

Analyze your dashboard panel of the URI data and answer the following questions:

* Does anything stand out as suspicious?
* What URI is hit the most?
* Based on the URI being accessed, what could the attacker potentially be doing?