



Cybersecurity

Day 1 Activity Guide

Designing Your Defensive Solution

Today, you will create a monitoring solution to protect VSI. Specifically, you will:

1. **Load and analyze Windows logs.**
2. **Create reports, alerts, and dashboards for the Windows logs.**
3. **Load and analyze Apache logs.**
4. **Create reports, alerts, and dashboards for the Apache logs.**
5. **Install an add-on Splunk application for additional monitoring.**

Resources

- [Splunkbase](#)
- [Splunk Documentation](#)
- [Splunk Add-Ons Guide](#)

Getting Started / Prerequisites

You will use your Web Lab virtual machine for this week's activities.

- This week's classes will use the same Splunk Docker container to run Splunk from inside the local virtual machine that was used during the Splunk lessons. In

the `/splunk` directory inside the virtual machine, you will find a `splunk.sh` script that can be run to start and stop the container as needed.

- If needed, refer back to the guide from Module 19 to configure Splunk on your VM.
- Once the container is running, Splunk can be accessed at <http://localhost:8000> on the virtual machine.

Use the following credentials:

- **Username:** `admin`
- **Password:** `cybersecurity`

Instructions

- Today, you will play the role of an SOC analyst at a small company called **Virtual Space Industries (VSI)**, which designs virtual-reality programs for businesses.
- VSI has heard rumors that a competitor, **JobeCorp**, may launch cyberattacks to disrupt VSI's business.
- As an SOC analyst, you are tasked with using Splunk to monitor potential attacks on your systems and applications.
- The VSI products that you have been tasked with monitoring include:
 - An Apache web server, which hosts the administrative webpage
 - A Windows operating system, which runs many of VSI's back-end operations
- Your networking team has provided you with past logs to help you develop baselines and create reports, alerts, dashboards, and more.

You've been provided the following logs on your machine:

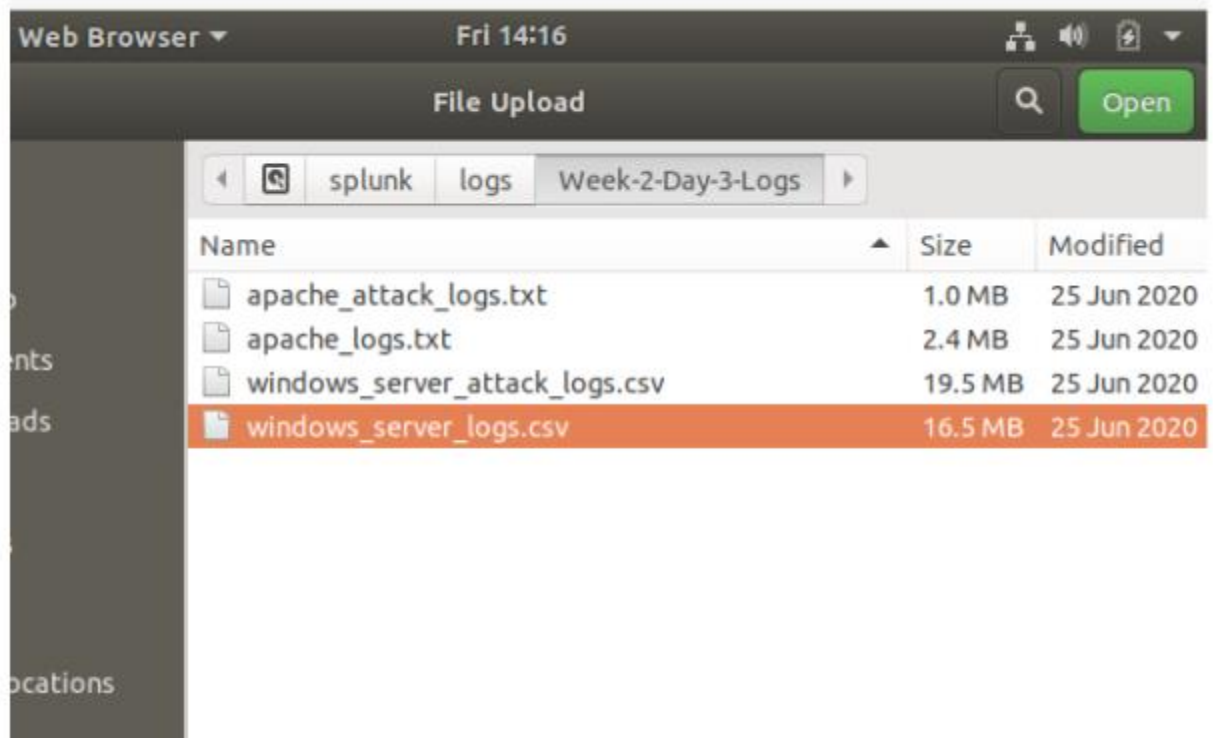
- **Windows Server Logs**
 - This server contains intellectual property of VSI's next-generation virtual-reality programs.
- **Apache Server Logs**
 - This server is used for VSI's main public-facing website, `vsi-company.com`.

Complete the following five parts in order to accomplish your Day 1 tasks.


Part 1: Load and Analyze Windows Logs

In this first part, you will upload and analyze Windows security logs that represent “regular” activity for VSI into your Splunk environment. To do so, complete the following steps:

1. Select the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option under “Or get data in with the following methods.”
 - Then, click “Select File.”
 - Double-click the `windows_server_logs.csv` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory, as the following image shows:



3. You will be brought to the “Set Source Type” page.
 - You don’t need to change any configurations on this page.

- Select “Next” again.
- 4. You’ll be brought to the “Input Settings” page.
 - This page contains optional settings for how the data is input.
 - In the “Host” field value, Splunk uses a random value to name the machine or device that generated the logs.
 - Update the value to “Windows_server_logs” and then select “Review.”
- 5. On the “Review” page, verify that you’ve chosen the correct settings.
 - Select “Submit” to proceed with uploading your data into Splunk.
- 6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear.
- 7. Select “Start Searching.”
- 8.  **Important:** After the data populates on the search, select “All Time” for the time range.
- 9. Briefly analyze the logs and the available fields, specifically examining the following important fields:
 - signature_id
 - signature
 - user
 - status
 - severity

Part 2: Create Reports, Alerts, and Dashboards for the Windows Logs

In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI’s Windows server. Design the following deliverables to protect VSI from potential attacks by JobeCorp:

1. **Reports:** Design the following **reports** to assist VSI in quickly identifying specific information and **be sure to grab screenshots of each report:**

- A report with a table of signatures and associated signature IDs.
 - a. This will allow VSI to view reports that show the ID number associated with the specific signature for Windows activity.
 - b. **Hint:** Research how to remove the duplicate values in your SPL search.
 - c. Take a screenshot of the report.
 - A report that displays the severity levels, and the count and percentage of each.
 - a. This will allow VSI to quickly understand the severity levels of the Windows logs being viewed.
 - b. Take a screenshot of the report.
 - A report that provides a comparison between the success and failure of Windows activities.
 - a. This will show VSI if there is a suspicious level of failed activities on their server.
 - b. **Hint:** Check the “status” field for this information.
 - c. Take a screenshot of the report.
2. **Alerts:** Design the following **alerts** to notify VSI of suspicious activity, and keep this information on hand as you will include it in your presentation:
- Determine a baseline and threshold for the hourly level of failed Windows activity.
 - a. Create an alert that’s triggered when the threshold has been reached.
 - b. The alert should trigger an email to SOC@VSI-company.com.
 - Determine a baseline and threshold for the hourly count of the signature “an account was successfully logged on.”
 - a. Create an alert that’s triggered when the threshold has been reached.
 - b. The alert should trigger an email to SOC@VSI-company.com.

- c. Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.
- Determine a baseline and threshold for the hourly count of the signature “a user account was deleted.”
 - a. Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.
 - b. Create an alert that's triggered when the threshold has been reached.
 - c. The alert should trigger an email to SOC@VSI-company.com.
- 3. **Visualizations and dashboards:** Design the following visualizations, and add them to a dashboard called “Windows Server Monitoring” (be creative with your visualizations, and make sure to grab screenshots of each):
 - A line chart that displays the different “signature” field values over time.
 - a. **Hint:** Add the following after your search: `timechart span=1h count by signature`.
 - b. Take a screenshot of the chart.
 - A line chart that displays the different “user” field values over time.
 - a. Take a screenshot of the chart.
 - Any visualization that illustrates the count of different signatures.
 - a. **Hint:** You can add brand-new custom visualizations by accessing this page inside your VM: [Additional Viz.](#)
 - b. Take a screenshot of the visualization.
 - Any visualization that illustrates the count of different users.
 - a. Take a screenshot of the visualization.
 - Any single-value visualization of your choice that analyzes any single data point, e.g., radial gauge, marker gauge, or a custom visualization from <http://localhost:8000/en-US/manager/search/appsremote?content=visualizations&type=app>.
 - a. Take a screenshot of the visualization.

4. On your dashboard, add the ability to change the time range for all visualizations.
 - Be sure to title all of your panels appropriately.
 - Organize the panels on your dashboard as you see fit.

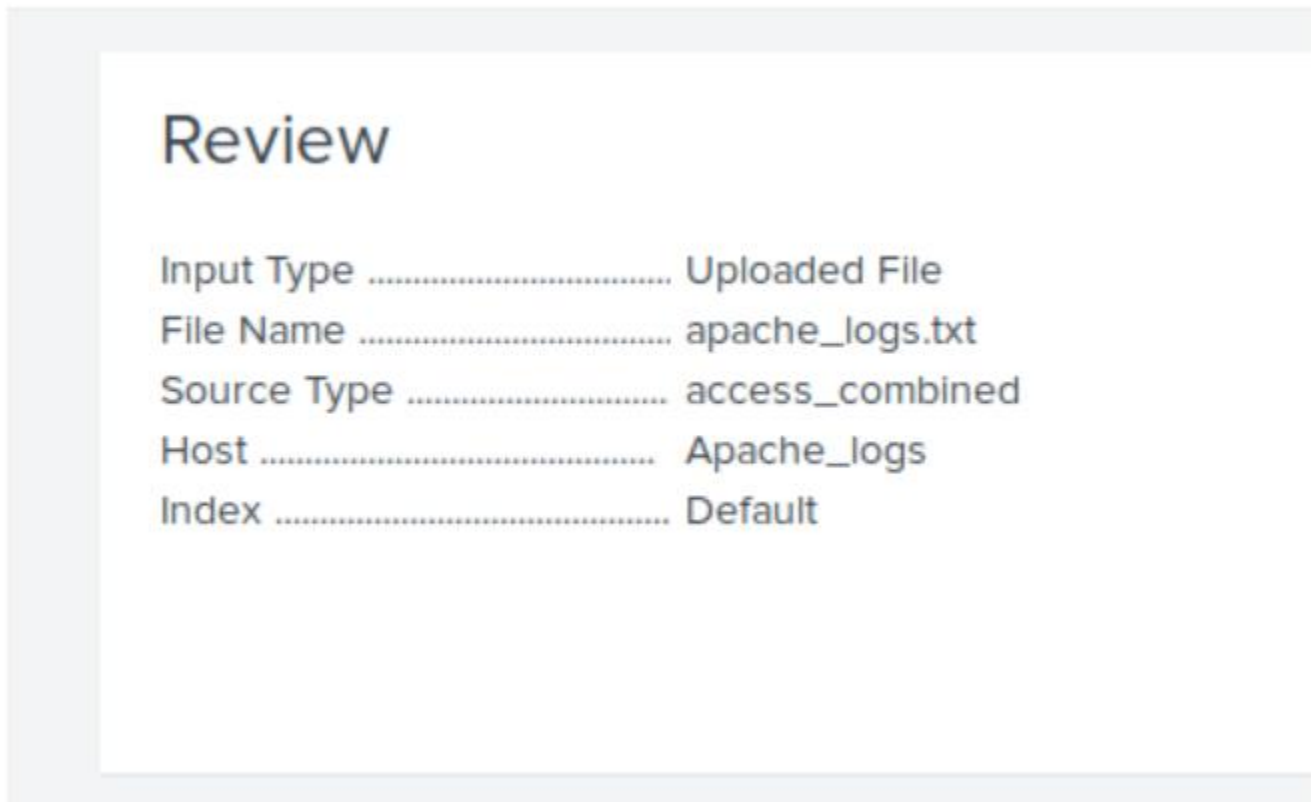
⚠ Checkpoint ⚠
Before continuing, make sure that you have completed the following critical tasks:
✓ Loaded and analyzed Windows logs.
✓ Created reports as indicated.
✓ Created visualizations and dashboards as indicated.

Part 3: Load and Analyze Apache Logs

In this part, you will upload and analyze Apache web server logs that represent “regular” activity for VSI into your Splunk environment. To do so, complete the following steps:

1. Return to the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
 - Click “Select File.”
 - Select the `apache_logs.txt` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
 - Click the green “Next” button in the top right.
3. You’ll be brought to the “Set Source Type” page.
 - You don’t need to change any configurations on this page.
 - Select “Next” again.
4. You’ll be brought to the “Input Settings” page.
 - This page contains optional settings for how the data is input.

- In the “Host” field, Splunk uses a random value to name the machine or device that generated the logs.
 - Update the value to “Apache_logs” and then select “Review.”
5. On the “Review” page, verify that you’ve chosen the correct settings, as the following image shows:



- Select “Submit” to proceed with uploading your data into Splunk.
6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear on the screen.
7. Select “Start Searching.”
8. **⚠ Important:** After the data populates on the search, select “All Time” for the time range.
9. Briefly analyze the logs and the available fields, specifically examining the following important fields:
- method
 - referer_domain

- status
- clientip
- useragent

Part 4: Create Reports, Alerts, and Dashboards for the Apache Logs

In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Apache web server. To do so, complete the following steps:

1. Design the following deliverables to protect VSI from potential attacks by JobeCorp:
 - **Reports:** Design the following **reports** to assist VSI in quickly identifying specific information (make sure to grab screenshots of each report):
 - a. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.).
 - This will provide insight into the type of HTTP activity being requested against VSI's web server.
 - b. A report that shows the top 10 domains that refer to VSI's website.
 - This will assist VSI with identifying suspicious referrers.
 - c. A report that shows the count of each HTTP response code.
 - This will provide insight into any suspicious levels of HTTP responses.
 - **Alerts:** Design the following **alerts**:
 - a. Determine a baseline and threshold for hourly activity from any country besides the United States.
 - Create an alert that's triggered when the threshold has been reached.
 - The alert should trigger an email to SOC@VSI-company.com.

- b. Determine an appropriate baseline and threshold for the hourly count of the HTTP POST method.
 - Create an alert that's triggered when the threshold has been reached.
 - The alert should trigger an email to SOC@VSI-company.com.
 - **Visualizations and dashboards:** Design the following **visualizations**, and add them to a **dashboard** called "Apache Web Server Monitoring" (be creative with your visualizations, and make sure to grab screenshots of each):
 - a. A line chart that displays the different HTTP "methods" field values over time.
 - **Hint:** Add the following after your search: `timechart span=1h count by method`.
 - b. A geographical map showing the location based on the "clientip" field.
 - c. Any visualization of your choice that displays the number of different URIs.
 - **Hint:** You can add brand-new custom visualizations by accessing this page inside your VM: [Additional Viz](#).
 - d. Any visualization of your choice that displays the count of the top 10 countries that appear in the log.
 - e. Any visualization that illustrates the count of different user agents.
 - f. A single-value visualization of your choice that analyzes any single data point: e.g., radial gauge, marker gauge, or a custom visualization from <http://localhost:8000/en-US/manager/search/appsremote?content=visualizations&type=app>.
2. On your dashboard, add the ability to change the time range for all visualizations.
 - Be sure to title all of your panels appropriately.
 - Organize the panels on your dashboard as you see fit.

Part 5: Install an Add-On Splunk Application for Additional Monitoring

NOTE: Splunkbase requires a verified email address to access. You will need to log into <https://www.splunk.com/> for an email verification prompt. For first time registrations you will need to log out and back in for an e-mail verification prompt.

In this part, your team will choose a Splunk add-on app to provide additional monitoring for VSI's systems. To do so, complete the following steps:

1. First, select any **ONE** of the Splunk add-on apps from <https://splunkbase.splunk.com/> to provide additional security monitoring for VSI.
 - You can choose any app from Splunkbase as long as you are able to meet the following requirements:
 - You must be able to install and use the add-on app.
 - You must be able to describe a scenario that illustrates how the app's features will protect VSI.
 - Use the following guide to install your add-on app: [Choosing your own add-on app from Splunkbase](#).
2. You are also welcome to choose one of these Splunk add-on apps with a pre-defined scenario:
 - **Website Monitoring:** App details [here](#) | **Install Instructions:** [Website Monitoring App](#)
 - **Whois XML IP Geolocation API:** App details [here](#) | **Install Instructions:** [Whois XML IP Geolocation API](#)
 - **Website Input:** App details [here](#) | **Install Instructions:** [Website Input](#)
3. **Be sure to grab screenshots of your add-on app!**

Day 1 Milestones

In today's class, you:

- 1. Loaded and analyzed Windows logs.**
- 2. Created reports, alerts, and dashboards for the Windows logs.**
- 3. Loaded and analyzed Apache logs.**
- 4. Created reports, alerts, and dashboards for the Apache logs.**
- 5. Installed an add-on Splunk application for additional monitoring.**

Completing these steps required you to leverage defensive monitoring skills such as baselining and creating Splunk reports, alerts, dashboards, and add-on applications. This is an impressive set of tools to have in your toolkit!