

Project Week

---

# Building a Security Monitoring Environment

Project 3



Welcome

# This Week:

In this project, you will play the role of an SOC analyst at a fictional organization called Virtual Space Industries (VSI).

01

VSI is a company that specializes in the design of virtual-reality programs for businesses.

02

VSI has heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business.

03

As a SOC analyst, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.



## **For your third project,**

you will use the skills that you've learned in the Defensive Security unit to design a custom monitoring environment to protect a fictional organization.





# Defensive Security

In the Defensive Security unit, we've covered:

---

1 Information security continuous monitoring (ISCM)

2 Log types and how they are used for monitoring

3 Log aggregation and correlation

4 Baselining

5 SIEMS

6 Splunk

# Group Work

This is a group project.

- You will complete this project in groups, but every student is required to remain in class.
- Groups are permitted to split up the work on this project, but each student must submit all project deliverables.
- Each day builds on the previous day's work to complete the project, and each day's activities must be completed in order.



# This Week:

You are tasked with monitoring the following VSI products:

01

**An administrative  
webpage:**

<https://vsi-corporation.azurewebsites.net/>

02

**An Apache web server,**  
which hosts this  
webpage.



03

**A Windows  
operating system,**  
which runs many of VSI's  
back-end operations.



Your networking team has also provided you with past logs to help you develop baselines and create reports, alerts, and dashboards to protect VSI from any attacks by JobeCorp.

# This Week's Daily Structure

Class will run a little differently during project week. Each day will include:

## Brief Lecture

We will begin by introducing some new concepts.

## Brief Overview

Then, we'll review the day's project tasks.

## Daily Guides

Finally, you'll use a guide to complete the project tasks during the remaining class time.

Day 2's guide concludes with review questions, which you'll submit at the end of the project.





# Daily Objectives and Milestones

---

## Day 1

You will develop a defensive solution utilizing a variety of Splunk tools that you learned in class in order to protect VSI.

1

You will be given logs of “typical” business functions in order to understand VSI's environment.

2

You will use these logs to create baselines and then design custom alerts, reports, and dashboards.

3

Additionally, you will download and use a Splunk “add-on” app of your choice to monitor against other types of attacks.



# Daily Objectives and Milestones

---

## Day 2

VSI will experience a simulated cyberattack.

1

You will analyze the reports and dashboards that you created on Day 1 in order to determine whether your defensive choices protected VSI from these attacks.

2

You will be provided with and answer review and analysis questions.

3

Additionally, you will start preparing slides to present your findings on Day 3 of class.



# Daily Objectives and Milestones

In your groups, you will present:

## Day 3

The defensive solution that you created.

1

How well or poorly it alerted and protected against the simulated attacks.

2

Any adjustments that you would make to your defensive solution.

# Project Deliverables

The project is due one week from the third day of this project. There is no additional Challenge this week. You will submit the following project deliverables:

## Technical brief and review questions

Answers to a series of questions explaining your monitoring solution and its efficacy at defending against attacks. Screenshots of your monitoring solution will be also be submitted with this document.

## Presentation slides

The slides your group uses for Day 3's presentation.

# Today's Class

---

The rest of today's class will proceed as follows:

01

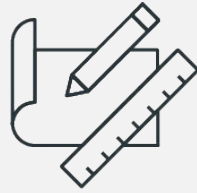
Introduction to the  
project scenario

02

Overview of  
today's tasks

03

Project work



# Day 1 Overview



# Day 1 Project Overview

On Day 1, you will complete the following:

01

Load and analyze Windows logs.

02

Create reports, alerts, and dashboards for the Windows logs.

03

Load and analyze Apache logs.

04

Create reports, alerts, and dashboards for the Apache logs.

05

Install an add-on Splunk application for additional monitoring.

# Step 1

## Load and Analyze Windows Logs

You will be provided with a set of logs from the Windows servers that run VSI's back-end systems.

The logs represent normal business operations.

You will load these logs and analyze the data they contain to determine baselines of normal activity.

The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, showing a 'New Search' page. The search query is `source="windows_server_logs.csv" host="0dcce57faf30" sourcetype="csv"`. Below the query, it indicates '4,764 events' and 'No Event Sampling'. The 'Events (4,764)' tab is selected, showing a timeline visualization with green bars. Below the timeline, a table displays the search results. The table has columns for 'Time' and 'Event'. The first event is from 3/24/20 at 11:59:54.000 PM, with the event text: '2020-03-24T23:59:54.000+0000,, "Domain\_A Domain\_A",, "user\_f user\_l",,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was er account was deleted. Subject: Security ID: Domain\_A\user\_f'. The table also shows the search criteria: host = 0dcce57faf30, source = windows\_server\_logs.csv, and sourcetype = csv.

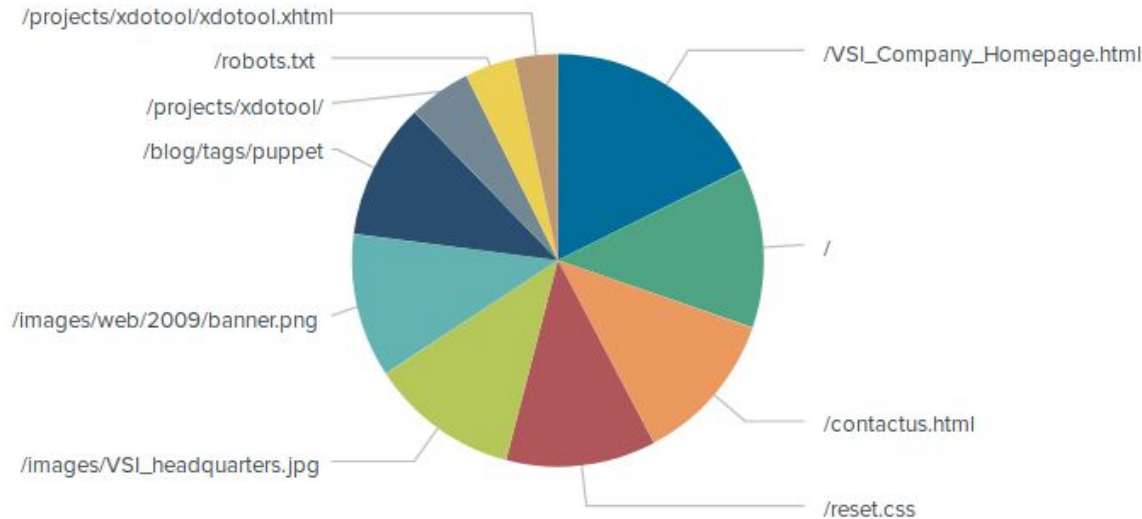
Time	Event
3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,, "Domain_A Domain_A",, "user_f user_l",,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was er account was deleted. Subject: Security ID: Domain_A\user_f



## Step 2

### Create Reports, Alerts, and Dashboards for the Windows Logs

Then, you will create reports, alerts, and dashboards based on your research in the previous step. You'll use these reports, alerts, and dashboards to determine if a future attack occurs.



#### Important:

You must grab screenshots where indicated in the daily guide. You will add them to your presentation.

# Step 3

## Load and Analyze Apache Logs

Next, you will be provided with a set of logs from the Apache web servers that host VSI's web application. The logs represent normal business operations.

You will load these logs and analyze the data that they contain to determine baselines of normal activity.

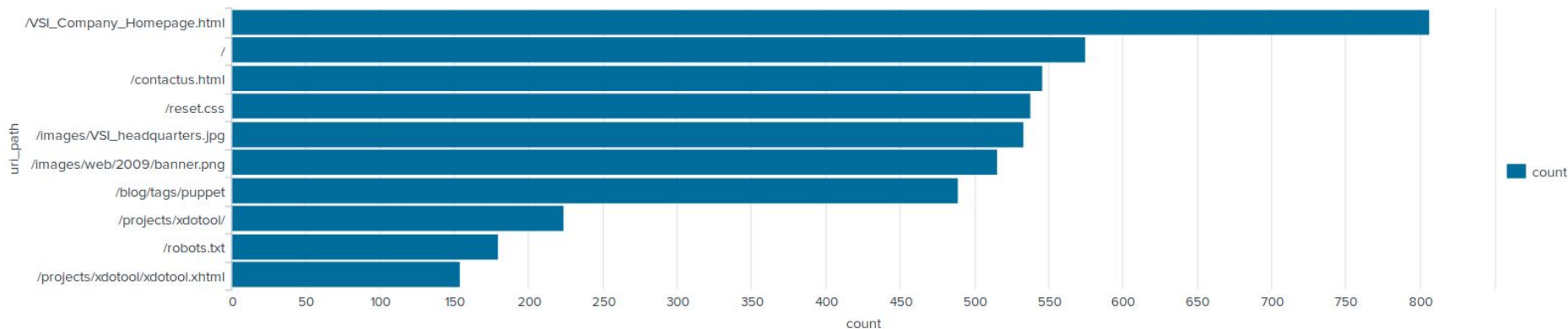
The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active. Below the navigation bar, the 'New Search' section shows a search query: `source="apache_logs.txt" host="0dcce57faf30" sourcetype="access_combined"`. The results are displayed as a bar chart and a table. The table has columns for 'Time' and 'Event'. The 'Event' column contains log entries with details such as IP addresses, timestamps, and user agents. The interface also shows a list of fields on the left, including 'host', 'source', and 'sourcetype'.

Time	Event
3/20/20 9:05:59.000 PM	5.10.83.53 - - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/?C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36" host= 0dcce57faf30 source= apache_logs.txt sourcetype= access_combined
3/20/20 9:05:59.000 PM	66.249.73.135 - - [20/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36" host= 0dcce57faf30 source= apache_logs.txt sourcetype= access_combined
3/20/20 9:05:58.000 PM	63.140.98.80 - - [20/Mar/2020:21:05:58 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36" host= 0dcce57faf30 source= apache_logs.txt sourcetype= access_combined
3/20/20 9:05:57.000 PM	38.99.236.50 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/future.com/presentations/logstash-puppetconf-2012/" HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36" host= 0dcce57faf30 source= apache_logs.txt sourcetype= access_combined

# Step 4

## Create Reports, Alerts, and Dashboards for the Apache Logs

Then, you will create reports, alerts, and dashboards based on your research in the previous step. You'll use these reports, alerts, and dashboards to determine if a future attack occurs against VSI's web server.




# Step 5

## Install Add-On Splunk Applications for Additional Monitoring

You will choose one of several Splunk add-on apps to assist with monitoring.


You will install the app and configure it to protect VSI's systems.

**Splunk Add-on for Unix and Linux**  
By Splunk Inc.

\*\*\* Important: Read upgrade Instructions and test add-on update before deploying to production \*\*\* There are changes to...

**PLATFORM** Splunk Enterprise, Splunk Cloud

**RATING** ★★★★★ 4 (40)

 **SPLUNK SUPPORTED ADDON**

**Splunk Common Information Model (CIM)**  
By Splunk Inc.**Palo Alto Networks Add-on for Splunk**  
By Palo Alto Networks



# Group Assignments



## Activity:

### Building a Security Monitoring Environment — Day 1

---

In this project, you will design reports, alerts, and dashboards, and select and install a Splunk add-on app in order to protect VSI from attacks.

**Suggested Time:**

To end of class





# Project Work Time





**Questions?**







**The End**