**Lab #6**

**CECS 378 – Spring 2021 – Cappel & Uuh**

**Due:** Wednesday, April 14th by 11:59 PM

**Lab #6 is focused on learning about the importance of logging information on various systems. We will discuss what a SIEM system is, the need and use cases for a SIEM capability, and you will learn the basic fundamentals of one of the most popular SIEM tools used in industry – Splunk Enterprise.**

**This lab will be done remotely using the Splunk lab environment residing on the internet. There are 14 modules available in this course. The first 10 modules are all worth 10 points each. The remaining 4 modules are available as extra credit. Point distribution is listed below.**

Now for a little background information…😉.

**SIEM**

**Security Information and Event Management** (**SIEM**) tools are an important part of the data security ecosystem: they aggregate data from multiple systems and analyze that data to catch abnormal behavior or potential cyberattacks. SIEM tools provide a central place to collect events and alerts – but can be expensive, resource intensive, and customers report that it is often difficult to resolve problems with SIEM data.

SIEM capabilities include:

* Collecting log information from security platforms, hardware, and business applications
* Generating regulatory and industry compliance reports
* Aggregating security data from throughout the enterprise IT environment
* Analyzing security data in real time
* Correlating security events and detecting potential indicators of a breach
* Presenting those detection indicators to security professionals

You can think of SIEM solutions as a funnel for your other cybersecurity platforms – for all the activity data your enterprise generates. It brings all those logs together into a centralized location and reformats it into a digestible format for examination.

At the same time, this is a surface view of SIEM capabilities. Digging a little deeper at 7 key SIEM capabilities:

#### **Log Management**

One of the most understood SIEM capabilities, log management collects and stores the log files from multiple disparate hosts into a centralized location. This allows your IT security team to easily access this information. Furthermore, log management also reformats the data it receives so that it is all consistent, making analysis less of a tedious and confusing process.

#### **Security Event Correlation**

Of SIEM capabilities, this is perhaps the most essential. SIEM analyzes all the accumulated data from its log management feature for potential signs of a data breach or threat infiltration. For example, a failed login is probably nothing. However, a failed login from the same user on multiple applications through the IT environment might be an indicator of a digital threat. And only with SIEM capabilities can you see the connection between these applications’ data.

#### **Threat Intelligence Feed Connections**

Staying up to date with threat intelligence – proliferation, evolution, and resolution – is vital to keeping your enterprise safe. SIEM capabilities include connecting to threat intelligence feeds, both from the solution providers’ feed but third-party threat intelligence feeds. Individual feeds tend to contain unique threat data, so drawing from as many feeds as possible is key to getting the most from your solution.

#### **Security Alerts**

Your solution should be keeping your IT security team as updated as possible as to possible threats, whether that be from dashboards updates, email alerts, or text alerts. Without this feature, your IT team might stay in the dark and let a threat dwell on your server.

#### **Report Presentation**

No matter how advanced your SIEM capabilities are, it will all be meaningless if your IT security team cannot make sense of the threat intelligence it presents. Ideally, SIEM solutions should display the security information in an easy-to-digest format – via graphics or clear, clean dashboards. The alternative is having your IT security team slog through the vast log bases accumulated hunting for threats manually.

#### **Compliance**

Compliance via SIEM is not quite as important to enterprises’ selection process, according to the 2017 Gartner Magic Quadrant for SIEM. Yet SIEM can collate events and logs to generate compliance reports. This can help your enterprise fulfill specific regulatory mandates while saving your IT team time and money.

#### **Machine Learning**

Among other SIEM capabilities, machine learning is new but no less essential. It allows your solution to learn to find threat indicators automatically and adapt to new information with no input from your team. This can save your team even more time and improve the effectiveness of your threat management.

Enough background information let’s get to work…😉.

In this lab, you will learn the basic fundamentals of one of the most popular SIEM tools used within Industry – Splunk Enterprise.

**Task 1 – Create an account on the Splunk website and register for the free training.**

Perform the following steps from your standard laptop:

1. Access the Splunk website by going to the following URL:

**<https://www.splunk.com/>**

1. On the main menu at the top right of the page, hover over the user icon and select the Sign Up link.
2. Enter your First and Last Name, Job Title (Student), Email Address (CSULB Student Email), Phone Number, Company (CSULB), Zip Code (90840), Username and Password (You choose), check the I Agree checkbox and select Create your Account.
3. Once you are logged in, select the Resources menu at the top of the page, then select the Splunk Training & Certification link.
4. Select the View & Register link in the Free Fundamentals 1 section.
5. At the next web page, select the Register link.
6. At the next web page, check the I have read the terms & conditions, then select the Register link.
7. At the next web page, select Checkout.
8. At the next web page, check the I have read the terms & conditions, then select the Confirm Order link.
9. At the next web page, select the Take me to My Learning Dashboard.
10. At the My Learning Dashboard page, select the Start Course link.

**Note**: You can choose to install Splunk Enterprise on your laptop for the lab components of the course or you may leverage the Splunk cloud environment free of charge for 15 days.

**Note**: At this point, you should be on your way. Please follow all the instructions in the course and make sure you download the course material for future use!

**Task 2 – Perform Modules 1 thru 10 in the Splunk Fundamentals 1 Course.**

**Note**: Grading for the *required* modules will be based on the following point distribution.

1. **Module 1**

– What is Machine Data (5 points)

– Module 1 Quiz (5 points)

1. **Module 2**

– What is Splunk (5 points)

– Module 2 Quiz (5 points)

1. **Module 3**

– Installing Splunk (5 points)

– Module 3 Quiz (5 points)

1. **Module 4**

– Getting Data In (5 points)

– Module 4 Quiz (5 points)

1. **Module 5**

– Basic Searching (5 points)

– Module 5 Quiz (5 points)

1. **Module 6**

– Using Fields (5 points)

– Module 6 Quiz (5 points)

1. **Module 7**

– Best Practices (5 points)

– Module 7 Quiz (5 points)

1. **Module 8**

– SPL Fundamentals (5 points)

– Module 8 Quiz (5 points)

1. **Module 9**

– Transforming Commands (5 points)

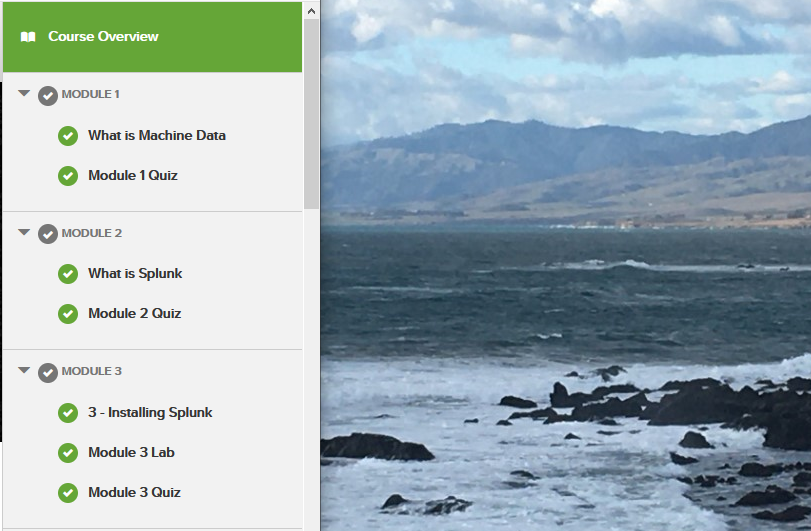
– Module 9 Quiz (5 points)

1. **Module 10**

– Reports and Dashboards (5 points)

– Module 10 Quiz (5 points)

**Note**: This concludes all the modules *required* for CECS 378 Lab 6.



Submit screen shots (like the one shown above) of all the modules you have completed along with something unique in the background on your particular laptop using the snipping tool.

Include any modules listed below you may have completed for extra credit.

Post a file containing your screen shots in dropbox on BeachBoard to validate you performed CECS 378 Lab 6.

The document containing your screen shots is the only required document to be submitted for CECS 378 Lab 6.

**Task 3 – \*\*EXTRA CREDIT\*\* Perform Modules 11 thru 14 in the Splunk Fund 1 Course.**

**Note**: These modules are not *required* but are available for extra credit lab points.

1. **Module 11 (1 extra credit point for labs)**

– Pivot and Datasets

– Module 11 Quiz

1. **Module 12 (1 extra credit point for labs)**

– Lookups

– Module 12 Quiz

1. **Module 13 (1 extra credit point for labs)**

– Scheduled Reports and Alerts

– Module 13 Quiz

1. **Module 14 (2 extra credit points for labs)**

– Final Thoughts

– Final Quiz