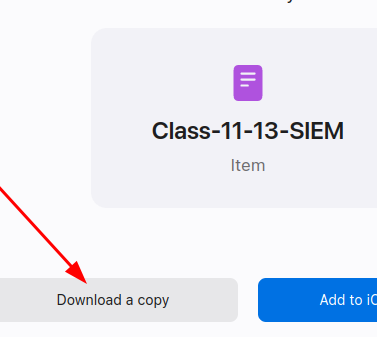
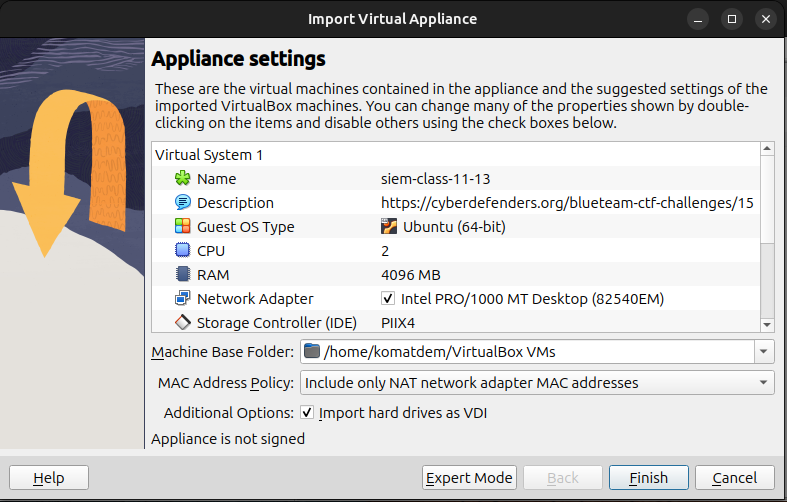
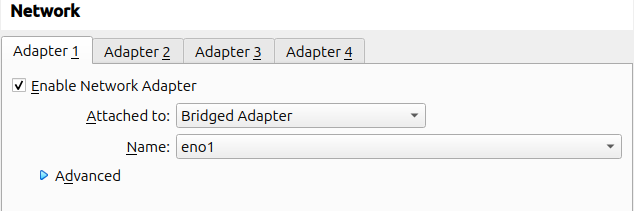
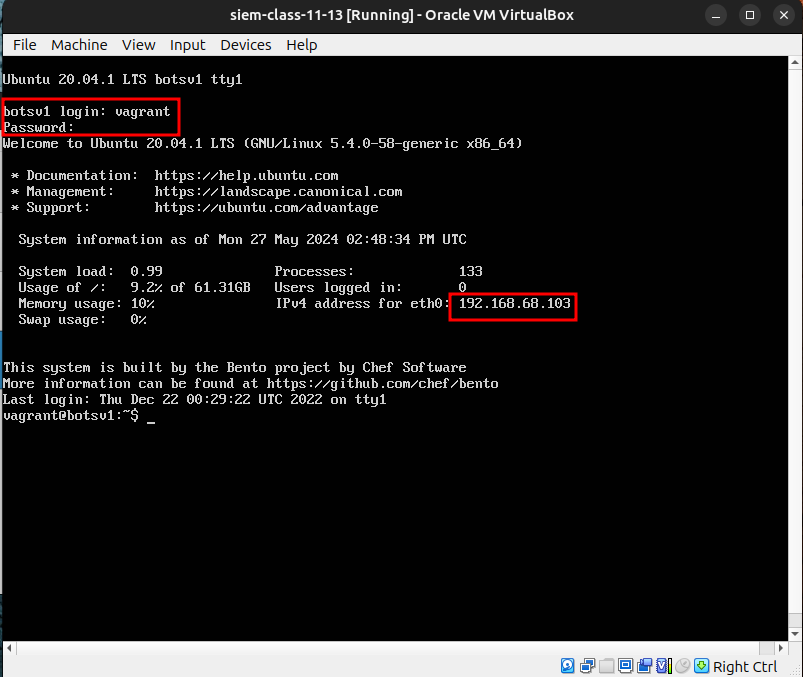
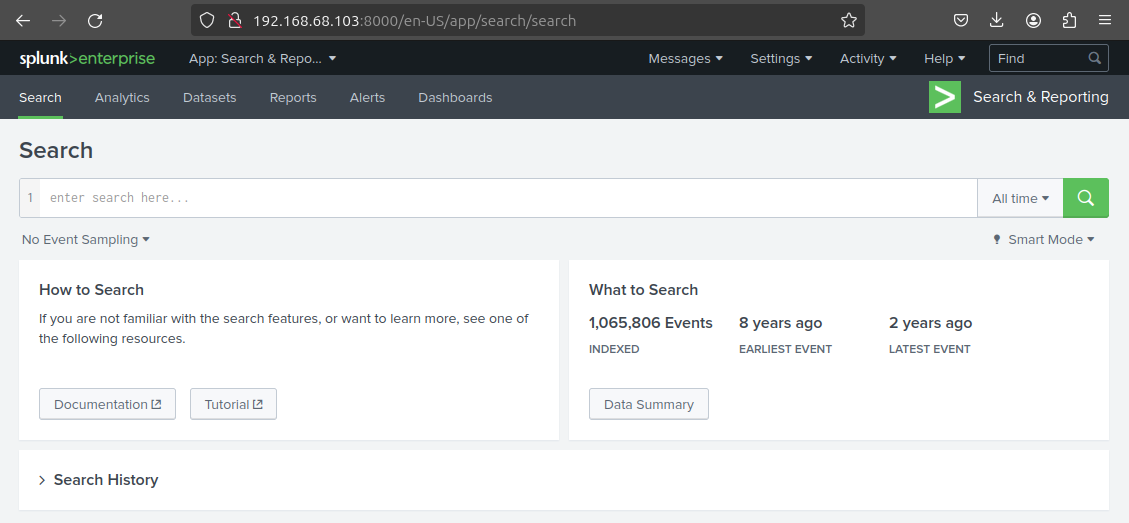
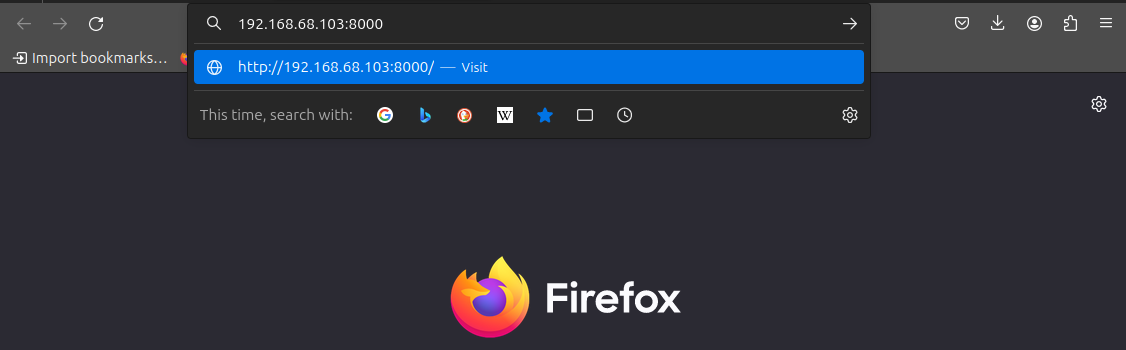
Hélio Ferreira 25/05/2024

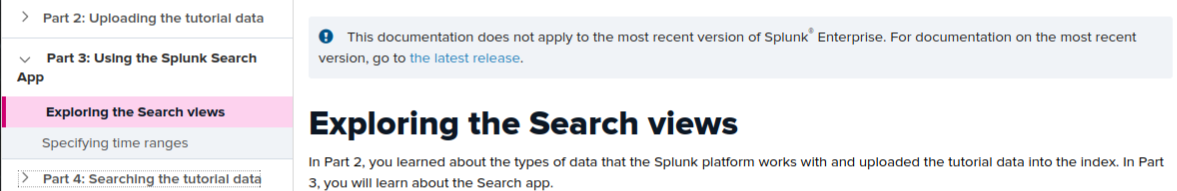
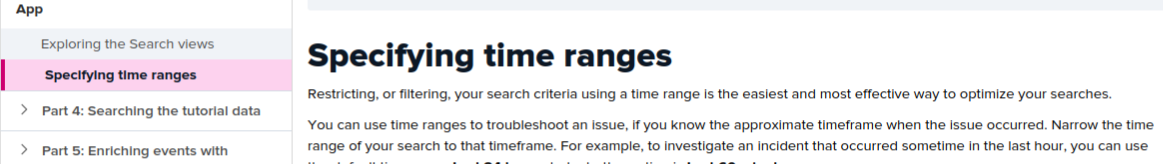
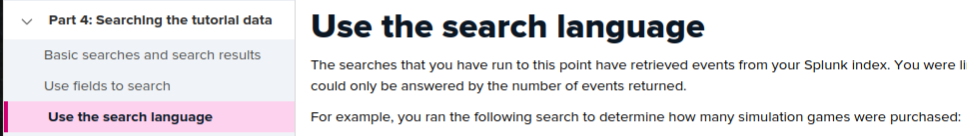
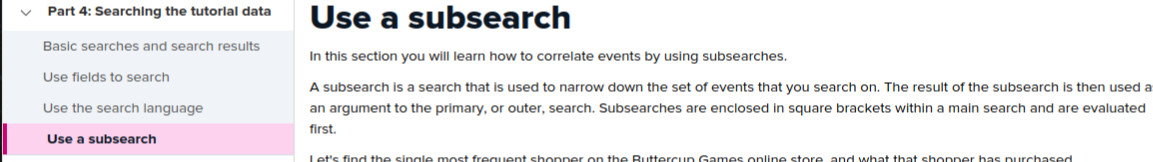
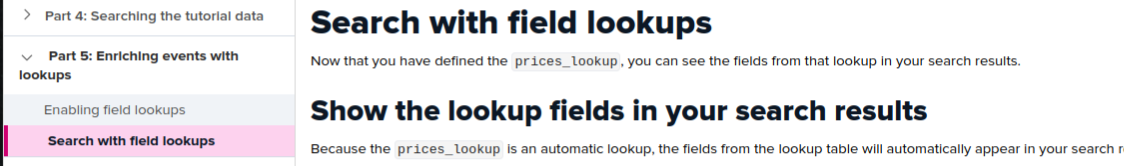
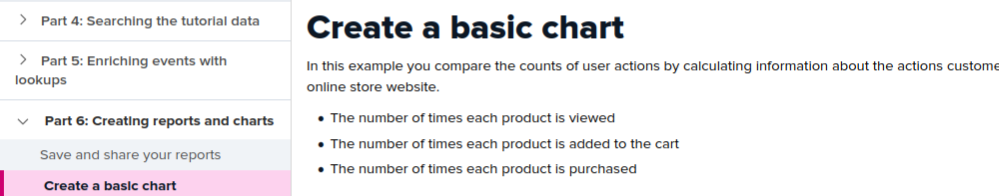
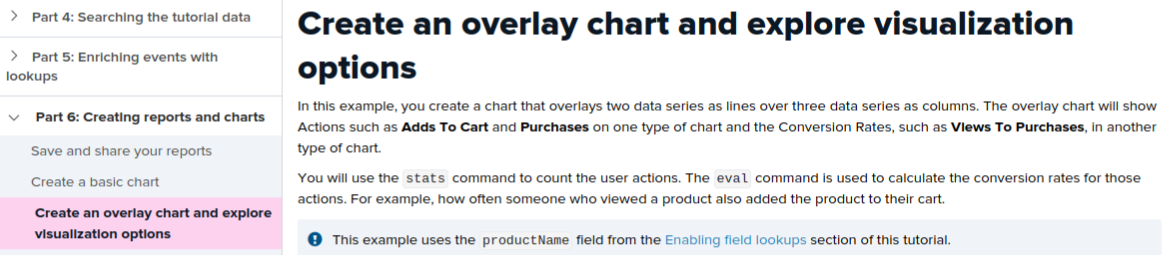
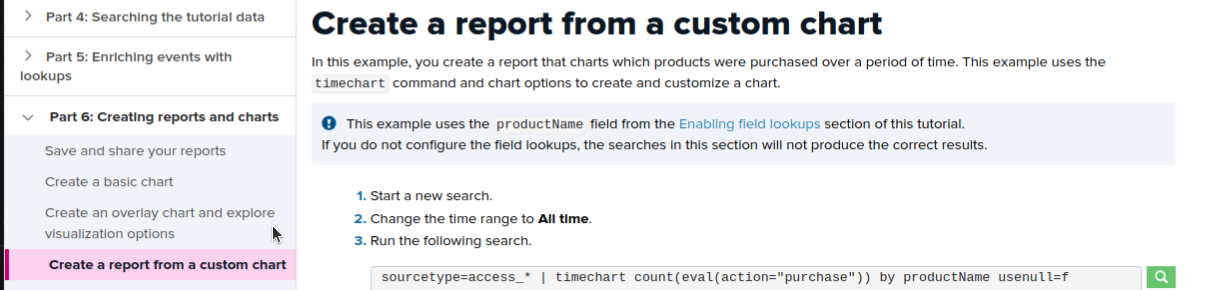
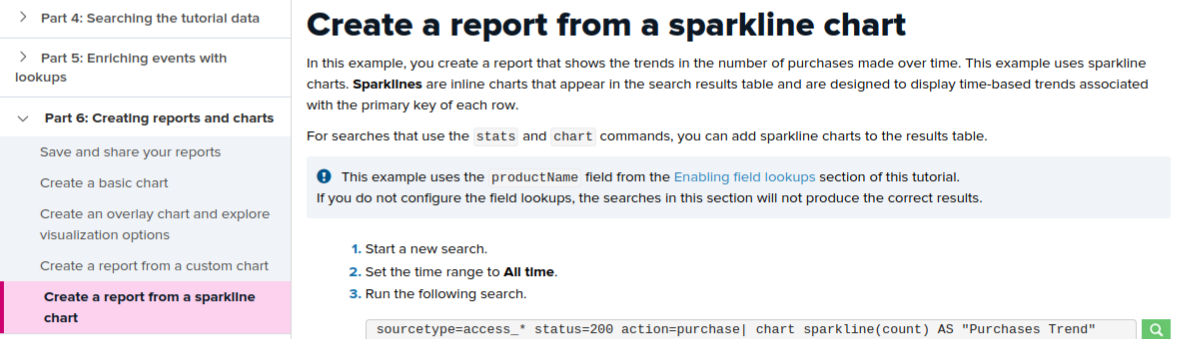
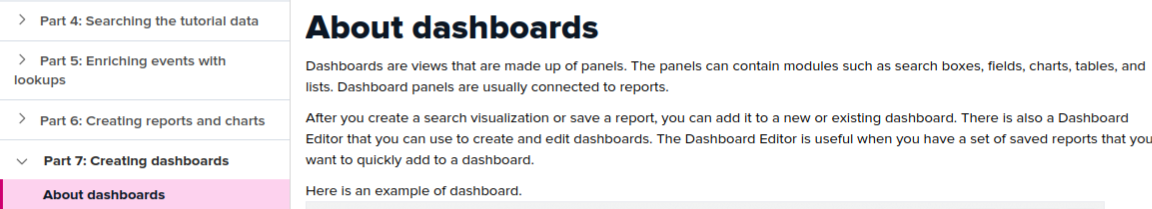
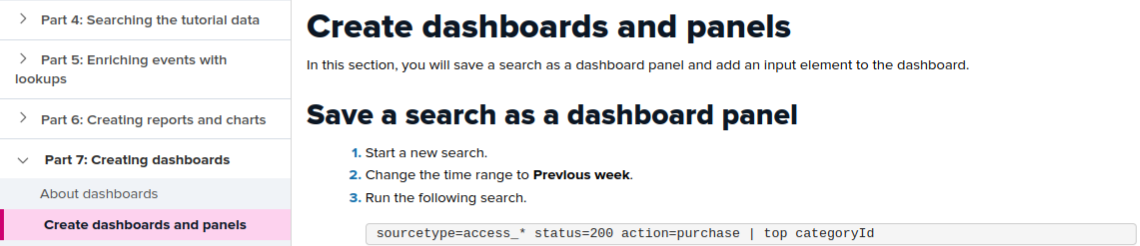
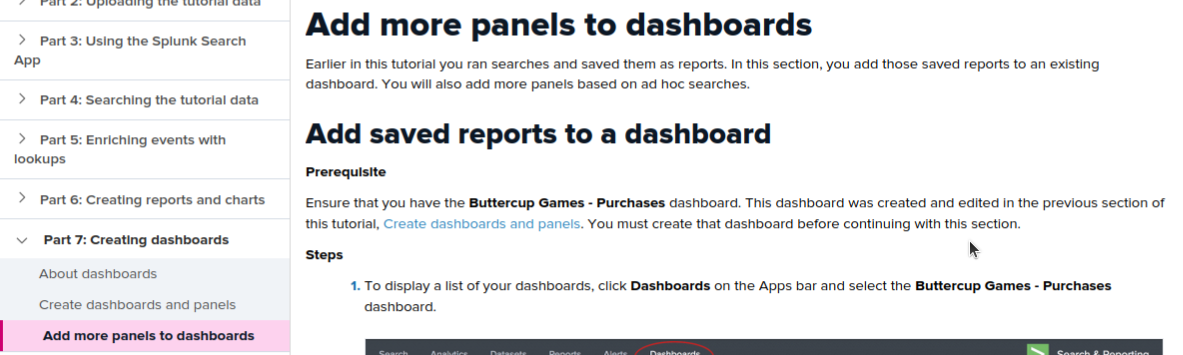
# **Lab: Foundational SIEM Operations**

### **Part 1: Staging Splunk**

* Download the pre-staged Splunk Server from the downloads table.
* Import the VM into VirtualBox.
* Set the network adapter to Bridge Mode. You’ll want to access the web portal via your immediate web browser for the least latency.
* Launch the VM and login to the VM using **vagrant/vagrant** to identify its IP address.
* Access the VM by opening a web browser to **http://ipaddress:8000** where **ipaddress** is replaced with the VM’s IP address.

### **Part 2: Incident and Analysis**

Complete the official [Splunk Search Tutorial](https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchTutorial/WelcometotheSearchTutorial). For each component of the lab tutorial, create notes in your submission including screenshots of successful execution of today’s tutorial.

* Skip Parts 1 and 2. The required datasets have already been uploaded and indexed.
* Part 3: Using the Splunk Search App  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Aboutthesearchapp>  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Aboutthetimerangepicker>  
  
* Part 4: Searching the tutorial data  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Startsearching>  
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Usefieldstosearch>  
    
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Usethesearchlanguage>  
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Useasubsearch>  
  
* Part 5: Enriching events with lookups  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Usefieldlookups>  
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Searchwithfieldlookups>  
  
* Part 6: Creating reports and charts  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Aboutsavingandsharingreports>  
    
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Basicchart>  
    
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Chartoverlays>  
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Chartasareport>  
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Tableasareport>  
  
* Part 7: Creating dashboards  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Aboutdashboards>  
    
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Createnewdashboard>  
    
  <https://docs.splunk.com/Documentation/Splunk/8.0.5/SearchTutorial/Addreportstodashboard>  
  

### **Part 3: Reporting**

Answer the below discussion prompts in your own words in your Google Doc submission.

* Why would a security team benefit from SIEM implementation?  
    
  SIEM benefits security teams by giving them a clearer picture of what's happening on the network, allowing them to spot and respond to threats faster and more efficiently. It also helps with regulatory compliance.
* What is an index?  
    
  In Splunk, an index is a specialized type of repository. It stores data after it's been processed and transformed into searchable events. Think of it like a filing cabinet for Splunk's information. Here's a breakdown of how it works:

**Raw Data:** Data comes into Splunk in its original format, which Splunk calls "raw data."

**Indexing:** Splunk takes this raw data and preps it for searching. This involves parsing it into events and extracting important details.

**Event Storage:** The processed events are then stored in the index. These indexes reside on the Splunk instance known as the "indexer."

So, indexes essentially hold the searchable information that Splunk uses for tasks like security monitoring, log analysis, and threat detection.

* What is a forwarder?  
    
  A forwarder in Splunk is like a data delivery person. It collects information from various devices on your network and sends it to a central location for processing and storage. There are two main types:

**Universal forwarder:** Lightweight, focused on collecting and sending data.

**Heavy forwarder:** More powerful, can also process data locally before sending.

Universal forwarders are generally preferred for their efficiency.

* How does a SIEM add value to an organization like Buttercup Games?  
    
  SIEM can benefit Buttercup Games, a game developer, by:

- Strengthening security for game servers and player data.

- Identifying threats targeting game development assets.

- Enabling faster response to security incidents.

- Helping comply with gaming data privacy regulations.