SIEM/SOAR TESTBED IMPLEMENTATION FOR USE IN UNDERGRAD AND POSTGRAD MODULES

Functional Specification

Name: Darragh Murphy
Student ID: C00135047
Project Supervisor: James Egan
12/02/2022

Table of Contents

Introduction

The purpose of this project is to create an environment where students can generate log events and network traffic that can then be analyzed by students using a SIEM tool as part of their undergrad and postgrad studies. From the experience I gained on my internship, I know how valuable such experience can be.

The test environment that will be deployed is the Detection Lab by Chris Long. This is a lab that he has built that is designed to be vulnerable and used for testing purposed by cybersecurity defenders. The testing environment will be accompanied by a series of lab exercises that will provide both theory learning and a practical demonstration surrounding specific techniques used by various malicious actors and the logs that they generate. Students will use the SIEM tool to analyse the logs that are generated during the demonstration.

Document Scope

This document provides detailed information about how to implement this testing environment, and it will document how any actors may interact with the system. The document will clearly outline the steps to take, and what should be expected.

Project Overview

Lab Exercises

The lab exercises will contain content that is based around the MITRE ATTACK framework and the techniques contained in their matrix. The lab exercises will contain a theory section where students will be provided with information about a specific technique. Following this, students will be required to research the technique further, using the internet to find out more information. The final section will be the demonstration and this will contain two parts. The student logs into the client machine to perform a series of tests and then the student logs into the SIEM and searches for the log data surrounding the tests. Throughout their research, the student will find information relating to the log data generated by their various tests.

In summary, the lab exercises will be formatted as follows:

- **Section 1:** Theory Section relating to MITRE ATTACK Technique.
- **Section 2:** Research Section containing questions relating to the MITRE ATTACK Technique.
- **Section 3:** Demonstration Section which contains two parts.
    - **Technique Demonstration:** Students perform the tests using the Atomic Red Team atomics tests.
    - **Log Search:** Use the SIEM tool to search and locate the logs generated by your test.

Test Environment

The implementation will consist of a series of virtual machines that will be configured to collect and forward logs to an instance of a SIEM for storage and analysis. I have chosen to implement an instance of Chris Long's *Detection Lab* in order to be able to replicate this with ease. The *Detection Lab* is a series of scripts that, when executed, configure an environment that is designed to be used by defenders to aid with research and testing.

The *Detection Lab* is deployed using Vagrant scripts that will configure four virtual machines on a virtual network. The *Detection Lab* is versatile and is deployed using a series of scripts, and it can be deployed in a number of different environments including:

- VirtualBox
- VMware Workstation
- AWS
- Azure

The *Detection Lab* is designed to be able to spin up the lab quickly. Per the documentation, this will take approximately two hours when the installation scripts are executed.

Detection Lab Features

The *Detection Lab* consists of four virtual machines that are configured to be used by security defenders and researchers. As such, they are configured to be insecure and to allow the collection of a variety of logs from multiple security tools.[1] The core features that we will be interested in will be as follows:

- Splunk pre-configured on the Ubuntu Log Collector server and the Splunk forwarder installed on the Windows Event Forwarder server.
- Custom Windows Group Policy Objects (GPOs) that configure command line process logging.
- The logging of all PowerShell activity.
- Zeek and Suricata installed as the IDS/IPS and are configured to monitor network traffic.
- A Sysmon configuration that uses Olaf Hartong's *Sysmon-modular* configuration. Olaf's blog advised that he designed this configuration with the MITRE ATTACK framework in mind. This enables process creation logging, among various other events. [2] [3]
- Atomic Red Team installed that will allow the students to perform the tests, which emulate techniques used by malicious actors. The Atomic Red Team is mapped to the MITRE ATTACK framework.

[1] (Detection Lab, 2022)
[2] (Hartong, 2022)
[3] (Hartong, 2018)

Log Collector

The virtual machine that will be used to collect logs is an Ubuntu Server 20.04 vagrant box that is hosted on Vagrant Cloud and downloaded during installation. This box was created by the Progress Chef Bento project, which is a project that encapsulates Packer templates in order to build Vagrant base boxes.[4] Progress Chef, formerly Chef, is a systems integration framework that is used for configuration management.[5]

This host will be configured as follows:

- Splunk Enterprise
- Fleet osquery Manager
- Apache Guacamole
- Suricata
- Zeek
- Velociraptor Server

Domain Controller

The virtual machine that will be used as a domain controller is a Windows Server 2016 vagrant box hosted on Vagrant Cloud and downloaded during installation. This box was created by Chris Long from *Detection Lab.*

This host will be configured as follows:

- WEF Server Configuration GPO
- PowerShell logging GPO
- Enhanced Windows Auditing policy GPO
- Sysmon
- Velociraptor
- osquery
- Splunk Universal Forwarder (Forwards Sysmon & osquery)
- Sysinternals Tools
- Microsoft Advanced Threat Analytics Lightweight Gateway

[4] (Chef, 2022)
[5] (Robbins, 2009)

Windows Event Forwarder

The virtual machine that will be used as the Windows Event Forwarder server is a Windows Server 2016 vagrant box hosted on Vagrant Cloud and downloaded during installation. This box was created by Chris Long from *Detection Lab.*

This host will be configured as follows:

- Microsoft Advanced Threat Analytics
- Windows Event Collector
- Windows Event Subscription Creation
- PowerShell transcription logging share
- Sysmon
- Velociraptor
- osquery
- Splunk Universal Forwarder (Forwards WinEventLog & PowerShell & Sysmon & osquery)
- Sysinternals tools

Student Machine

The virtual machine that will be used as the Student machine is a Windows 10 vagrant box hosted on Vagrant Cloud and downloaded during installation. This box was created by Chris Long from *Detection Lab.*

This host will be configured as follows:

- Simulates employee workstation
- Sysmon
- Velociraptor
- osquery
- Splunk Universal Forwarder (Forwards Sysmon & osquery)
- Sysinternals Tools

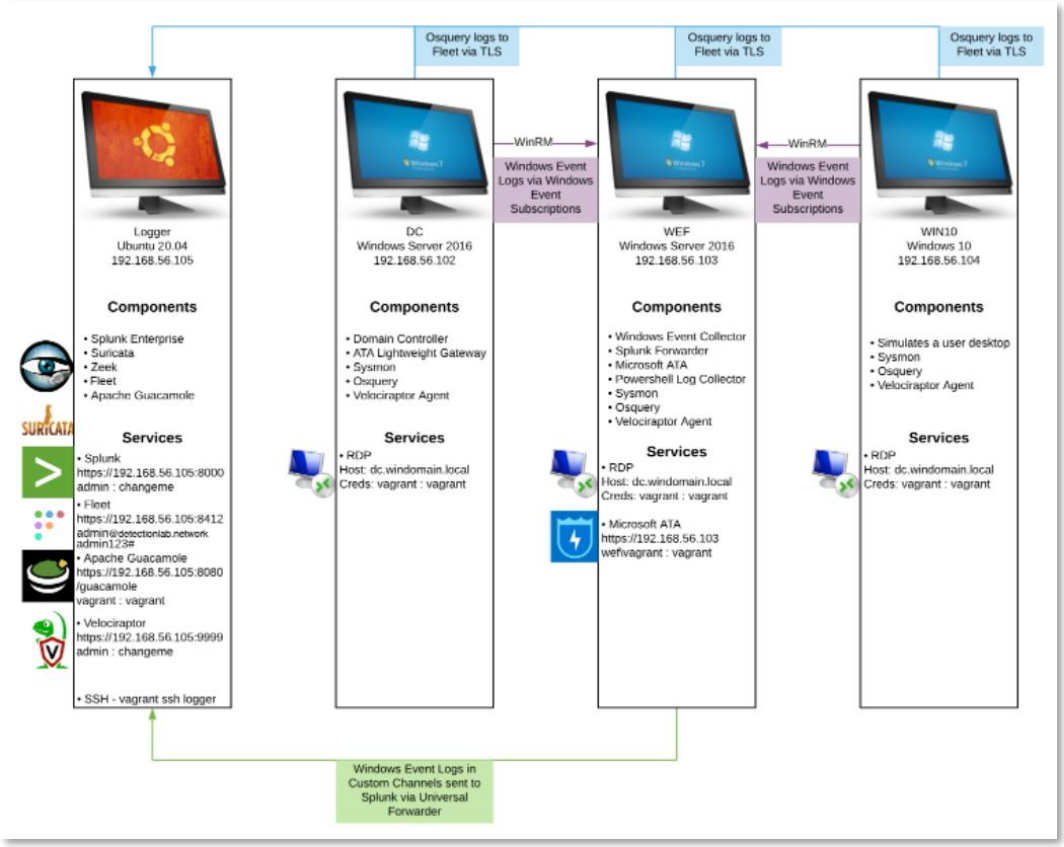

Figure 1: Detection Lab Configuration

Core Deliverables

The *Detection Labs* comes packaged with a variety of different tools, and it is fully customizable. My stated aim is to create an environment where students can gain experience using a SIEM tool and to produce lab exercises that will enhance their learning surrounding common techniques used from the MITRE ATTACK framework and the logs that they generate.

The core aspects of that I would like to deliver are as follows:

- Create five lab exercises for students and lecturers.
- Run the scripts and spin up the Detection Lab successfully.
- Sign in as an admin in Splunk and create a standard user account.
- Successfully sign into Splunk as the created user.
- Create alerts in Splunk based upon the five lab exercises.
- Create a user account on the Domain.
- Install Invoke-AtomicTest on Windows 10 machine to enable automatic testing.

- Use Splunk to search for logs generated by tests.

Users of System

I plan to deploy this on my personal machine, however in an environment such as the college, there may be a requirement for 3 users.

Systems Administrator:

A Systems Administrator in the college will require access to execute the scripts and to bring the lab online if the lab is to be hosted on site. If the lab is to be hosted in the Cloud, the lab is compatible with certain services. If the college has an AWS or Azure account, the Systems Administrator may be required to run the scripts to bring the labs online also.

Lecturer (Admin):

The lecturer will have administration access to the devices configured by using the Detection Lab vagrant scripts. It will be the lecturer's responsibility to provide access to the environment for their students. The lecturer may also create alerts within Splunk for the activity that will be demonstrated in the lab exercises. The lecturer will also have access to the Domain Controller and can add accounts to the Domain for the student's access.

Students (User):

The students will have general user accounts on the Windows 10 machine and will have access to PowerShell and Command Prompt, which will enable them to perform the testing included in the lab exercises. Students will also have a general user account for the Splunk instance that will allow them to access Splunk's Search and Reporting App. This app will enable students to search for the log events that are generated by the activities they performed.

System Requirements

I plan to install the virtual machines using Virtual Box on my personal machine. The system requirements are as follows:

- VirtualBox 6.0+
- Vagrant 2.2.9+
- 55GB+ HDD Space
- 16GB+ RAM
- 8 Cores

Use Cases

Use Case Diagrams

Here I will use Use-Case diagrams to demonstrate how the users of the labs can interact with the variety of systems in place.

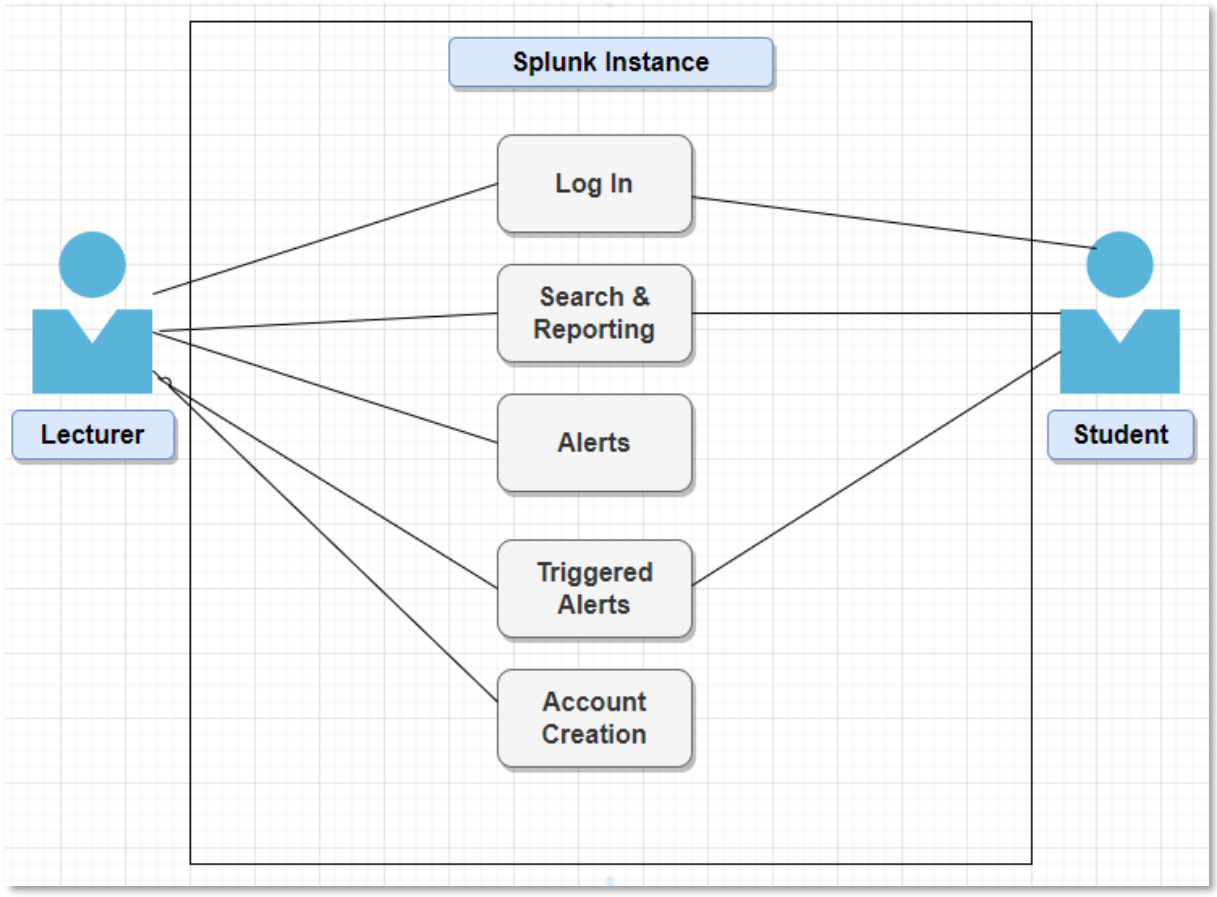

Figure 2: Splunk Instance Use Case Diagram

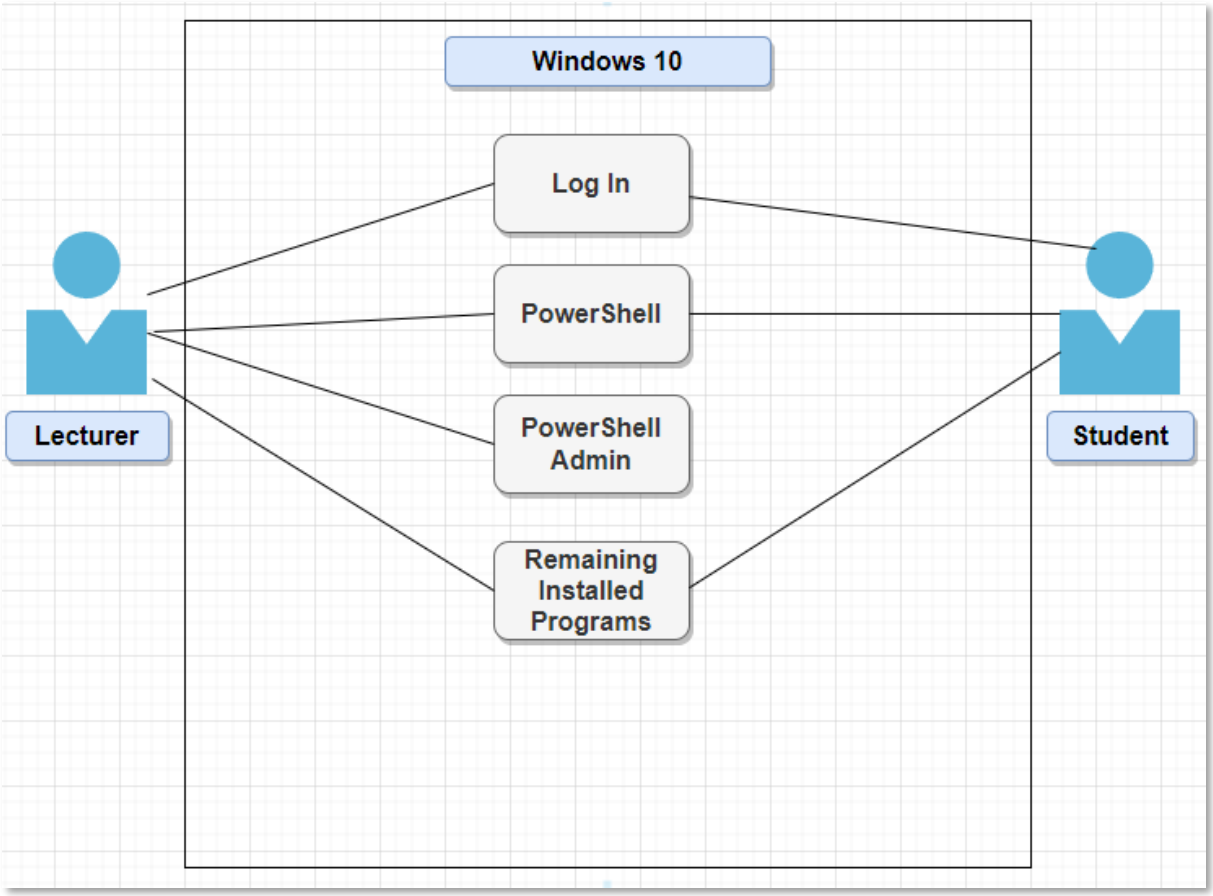

Figure 3: Windows 10 Use Case Diagram

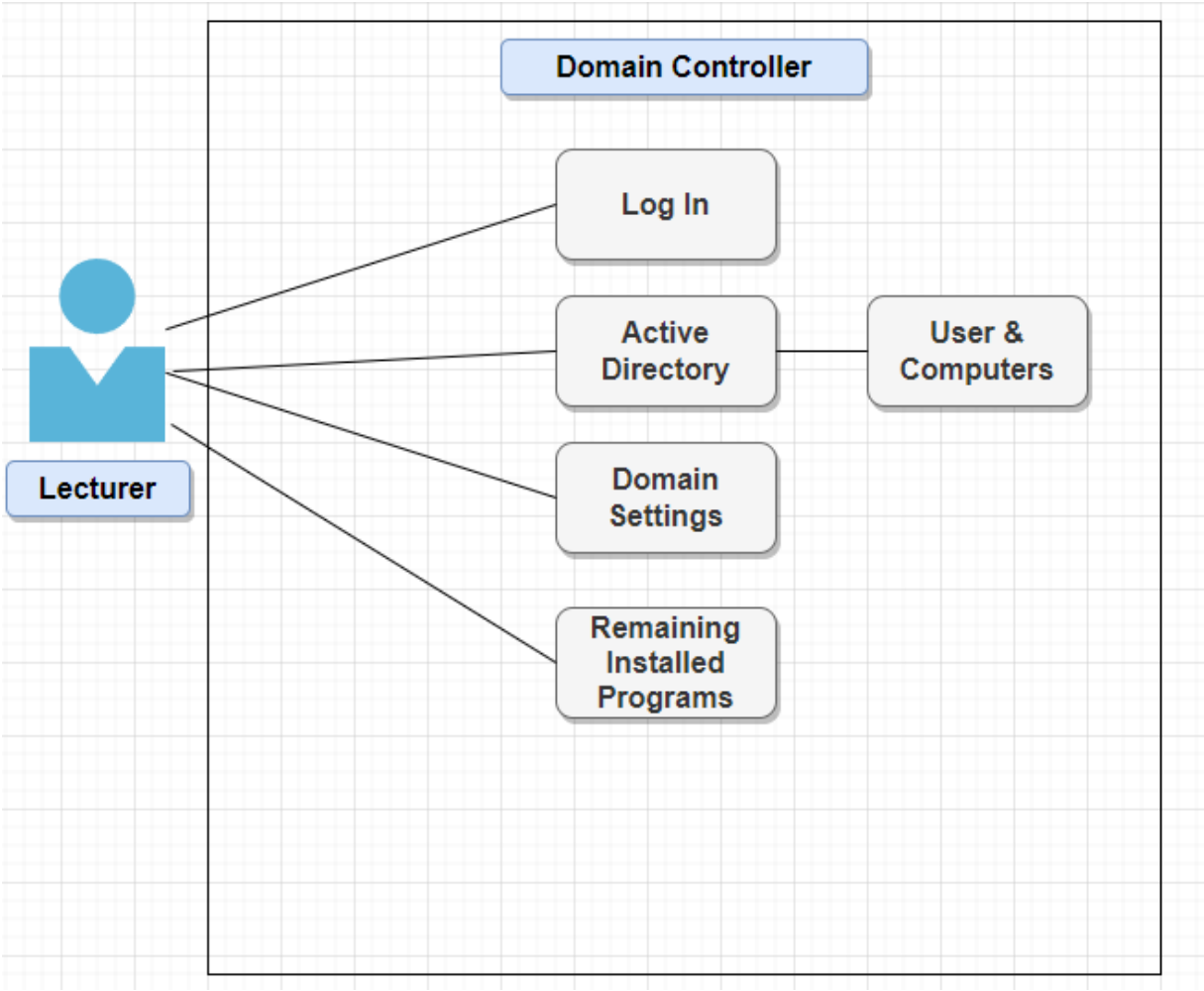

Figure 4: Domain Controller Use Case Diagram

Brief Use Cases

Student Account Creation

The lecturer will have to create user accounts for the student in the Splunk instance by logging in using the Admin account.

Primary Actor: Lecturer

Precondition: The lecturer uses the admin account to create user accounts for students in Splunk.

Steps:

- Sign into the Admin account with Splunk
- Go to Settings → Users

- Click New User
- Enter Student's details and click save.

Expected Result: A new student account is created.

Adding a Student to the Domain

The lecturer will be required to add the students to the domain, in order to access the windows 10 machines. They will do this by signing into the Domain Controller and creating the user accounts.

Primary Actor: Lecturer

Precondition: The lecturer creates user accounts on the Domain for the students using the Domain Controller.

Steps:

- Sign into the Domain Controller.
- Go to Start → Administrative Tools → Active Directory Users and Computers
- Drop down the contents of the domain.
- Right Click Users → New → User
- Enter User Details and click Next.
- Review Details and click Finish.
- Right Click User and Add them to the User Group.

Expected Result: A student account is created on the Domain.

Student Performing Test in Windows

As part of the lab exercises, student will perform various tests on the Windows 10 machine using the Atomic Red Team tests from PowerShell.

Primary Actor: Student

Precondition: Student performs a series of tests using the Atomic Red Team tests.

Steps:

- Sign-in to Windows 10 Machine.
- Open Up PowerShell.

- Perform steps contained in labs.

Expected Result: Test was executed successfully.

Student Searching for Logs in Splunk

The student will use Splunk to search for the logs generated during the testing stage of the lab exercise.

Primary Actor: Student

Precondition: Student uses Splunk to Search for Logs related to test.

Steps:

- Sign-in to Splunk Instance
- Go to Search & Reporting
- Use the search bar to search for log events.

Expected Result: Students locate the logs related to the tests performed.

Metrics

To gauge how successful my project will be in demonstrating the usefulness of the created labs and the SIEM tool I will:

- Demonstrate the labs to the lecturers of the Incident Handling and Risk Analysis module and get their feedback.
- Get quotes from the cybersecurity industry relating to the prevalence of SIEM tools within the industry.

Project Relevance

I will deploy an instance of the *Detection Lab* to demonstrate that learning how to use such tools as a SIEM will be very beneficial for students in the future. Most graduates who end up in a cybersecurity role will end up using a SIEM tool at some point in their careers and having this knowledge before entering the workplace will go a long way for students.

Project Plan

Sprint #	Plan	Due Date	Deliverable
0	Submit Research Document Draft	26/11/2021	Research Document
1	Plan Project	10/12/2021	Project Plan
2	1st Presentation	16/12/2021	Presentation to Project Supervisors
3	Submit Functional Spec Draft	17/12/2021	Functional Specification Document
Christmas Break			
4	2nd Presentation	17/02/2022	Presentation to Project Supervisors
5	Plan Project Redirection	25/02/2022	New Plan Created
6	Research Mitre Attack Framework	04/03/2022	Made a Decision on Techniques to Test
7	Create Lab 1	11/03/2022	Lab 1 Created
8	Create Lab 2	17/03/2022	Lab 2 Created
9	Create Lab 3	25/03/2022	Lab 3 Created
10	Create Lab 4	01/04/2022	Lab 4 Created
11	Create Lab 5	08/04/2022	Lab 5 Created
12	Create Alerts in Splunk	15/04/2022	Create Alerts surrounding the created lab exercises
13	Complete Documentation	24/04/2022	Required Documentation Completed
14	Final Submission	25/04/2022	Submit Project Documentation on Blackboard
15	Project Demonstration	29/04/2022	Demonstration of Project to Supervisors

References

Chef, 2022. *bento.* [Online]
Available at: https://github.com/chef/bento
[Accessed 21st April 2022].

Detection Lab, 2022. *INTRODUCTION.* [Online]
Available at: https://detectionlab.network/introduction/
[Accessed 21st April 2022].

Hartong, O., 2018. *Endpoint detection Superpowers on the cheap — part 1.* [Online]
Available at: https://medium.com/@olafhartong/endpoint-detection-superpowers-on-the-cheap-part-1-e9c28201ac47

Hartong, O., 2022. *sysmon-modular.* [Online]
Available at: https://github.com/olafhartong/sysmon-modular

Robbins, J., 2009. *Announcing Chef.* [Online]
Available at: https://www.chef.io/blog/announcing-chef
[Accessed 21st April 2022].