# Blue Team: Summary of Operations

## Table of Contents



### Network Topology

*TODO: Fill out the information below.*

The following machines were identified on the network:

- **Kali**
  - **Operating System**: Linux 5.4.0
  - **Purpose**: Attacker machine
  - **IP Address**: 192.168.1.90
- **ELK**
  - **Operating System**: Ubuntu 18.04.4
  - **Purpose**: Monitoring loggings
  - **IP Address**: 192.168.1.100
- **Capstone**
  - **Operating System**: Ubuntu 18.01.1
  - **Purpose**: Alert testing
  - **IP Address**: 192.168.1.105

### Description of Targets

*TODO: Answer the questions below.*

The target of this attack was: Target 1 (192.168.1.110 ).

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

### Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**Excessive HTTP errors**.

Alert 1 is implemented as follows:

- **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status.code
- **Threshold**: Above 400
- **Vulnerability Mitigated**: Enumeration/Brute Force
- **Reliability**: High reliability

**HTTP Request Size Monitor**

Alert 2 is implemented as follows:

- **Metric**: WHEN sum() of http.request.bytes OVER all documents
- **Threshold**: Above 3500 in the last minutes
- **Vulnerability Mitigated**: Code injection in HTTP requests or DDOS
- **Reliability**: Medium reliability

**CPU Usage Monitor**

Alert 3 is implemented as follows:

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents
- **Threshold**: Above 0.5
- **Vulnerability Mitigated**: Malicious software
- **Reliability**: high reliability