# Blue Team: Summary of Operations

## Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic & Behavior

### Network Topology

Diagram

Description automatically generated

### Description of Target

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:

#### Alert 1: Excessive HTTP Errors

Graphical user interface, text, application, chat or text message

Description automatically generated

Alert 1 is implemented as follows: - **Metric**: http.response.status\_code - **Threshold**: 400 - **Vulnerability Mitigated**: TODO - **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

#### Alert 2: HTTP Request Size Monitor

Text

Description automatically generated with medium confidence

Alert 2 is implemented as follows: - **Metric**: http.request.bytes - **Threshold**: 3500 bytes **Vulnerability Mitigated**: TODO - **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

#### Alert 3: CPU Usage Monitor

Graphical user interface, text, application, email

Description automatically generated

Alert 3 is implemented as follows: - **Metric**: system.process.cpu.total.pct - **Threshold**: .5 - **Vulnerability Mitigated**: TODO - **Reliability**: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

*TODO Note: Explain at least 3 alerts. Add more if time allows.*