# **Blue Team: Summary of Operations**

## **Table of Contents**

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic & Behavior
* Suggestions for Going Further

### **Network Topology**

The following machines were identified on the network:

* Kali
  + **Operating System**: Linux Kali 9.0
  + **Purpose**: Attacking Machine
  + **IP Address**: 192.168.1.90
* ELK
  + **Operating System**: Linux
  + **Purpose**: SIEM
  + **IP Address**: 192.168.1.100
* Target 1
  + **Operating System:** Linux
  + **Purpose:** VulnerableWordPress Host Machine
  + **IP Address:** 192.168.1.110

### 

### **Description of Targets**

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**

Excessive HTTP Errors is implemented as follows:

* **Metric**: WHEN count() GROUPED OVER top 5 ‘http.response.status\_code’ IS ABOVE 400 FOR THE LAST 5 minutes
* **Threshold**: IS ABOVE 400
* **Vulnerability Mitigated**: Enumeration/Brute Force
* **Reliability**: This alert is highly reliable. Our Threshold measures error codes by 400 and above, which will filter out any successful responses. If there are excessive error codes, we will be alerted. We will have hardly any false positives.
* Graphical user interface, text, application, email

  Description automatically generated

#### **Alert 2: HTTP Request Size Monitor**

Alert 2 is implemented as follows:

* **Metric**: WHEN sum() of http.request.bytes OVER all documents
* **Threshold**: IS ABOVE 3500
* **Vulnerability Mitigated**: Code injection in HTTP requests or DDOS
* **Reliability**: Having a large amount of legitimate HTTP requests traffic can result in false positives. This alert is of medium reliability.

Graphical user interface, application

Description automatically generated

#### **Alert 3: CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents
* **Threshold**: IS ABOVE 0.5
* **Vulnerability Mitigated**: Malware running and taking up resources
* **Reliability**: This alert will help determine our CPU usage management. We will be alerted when our CPU usage can be eaten up by a malicious program or even when there is no malicious activity. This alert us highly reliable and will not cause any false positives.
* Graphical user interface, text, application, email

  Description automatically generated