# **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:

* ELK
  + **Operating System**: Linux
  + **Purpose**: Monitor logs (packetbeat, metricbeat) for network activity
  + **IP Address**: 192.168.1.100
* Kali
  + **Operating System**: Linux
  + **Purpose**: Penetration testing of network
  + **IP Address**: 192.168.1.90
* Target1
  + **Operation System**: Linux
  + **Purpose**: the vm being attacked
  + **IP Address**: 192.168.1.110

### **Description of Target(s)**

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

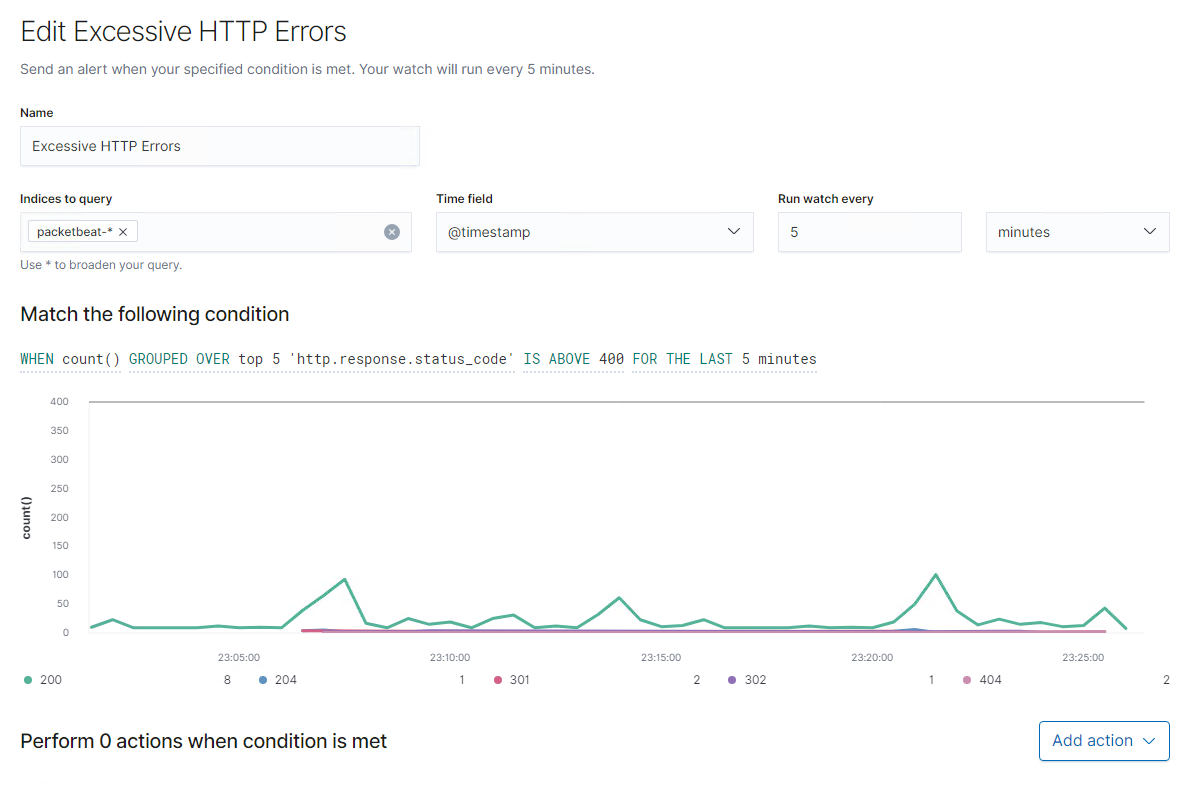
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

### **Monitoring the Targets**

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

**Excessive HTTP Errors** is implemented as follows:

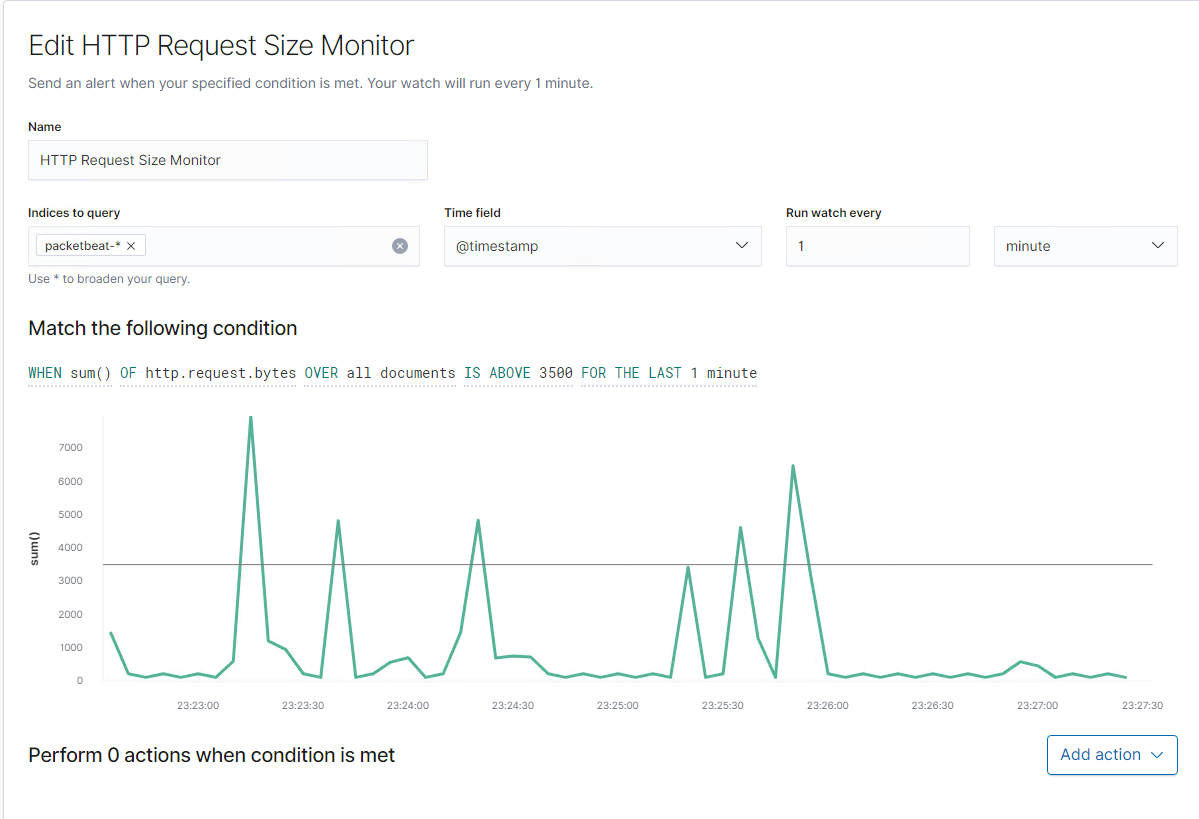
* **Metric**: (packetbeat\*) count of ‘http.response.status\_code’
* **Threshold**: above 400 for the last 5 minutes
* **Vulnerability Mitigated**: brute force attacks/unauthorized access
* **Reliability**: medium



#### 

#### **HTTP Request Size Monitor**

* **Metric**: (packetbeat\*) sum of ‘http.request.bytes’
* **Threshold**: above 3500 for the last 1 minute
* **Vulnerability Mitigated**: DDoS attacks
* **Reliability**: medium



#### 

#### **CPU Usage Monitor**

* **Metric**: (metricbeat\*) max of ‘system.process.cpu.total.pct’
* **Threshold**: above 0.5 for the last 5 minutes
* **Vulnerability Mitigated**: virus/malware that is taking up CPU
* **Reliability**: high

