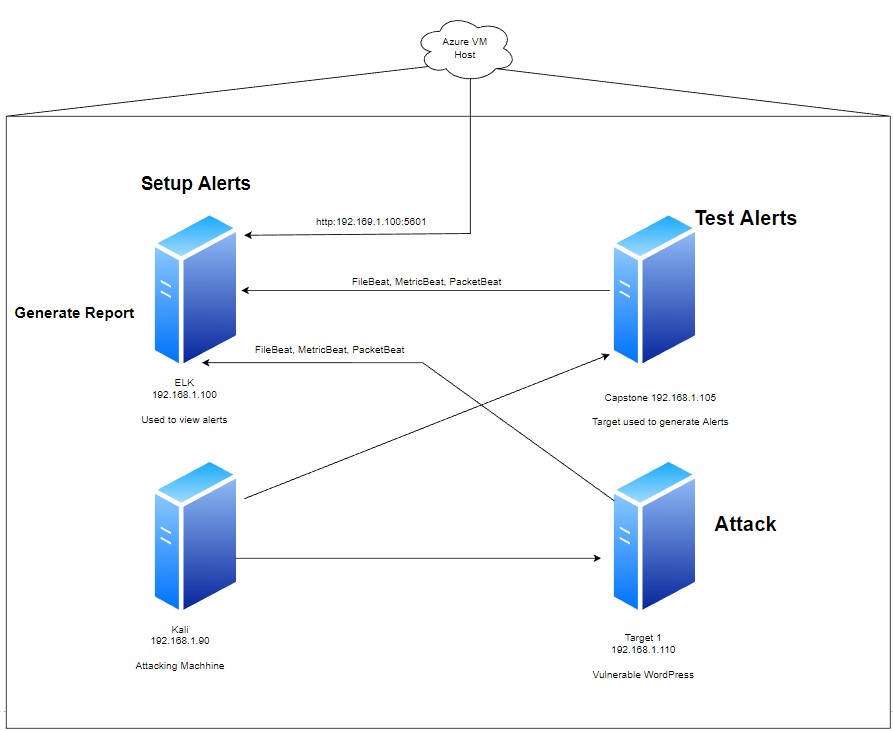
# **Blue Team: Summary of Operations**

## **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:

* Final
  + **Operating System**: Azure
  + **Purpose**: Provide network to conduct offensive and defensive operations
  + **IP Address**:192.168.1.1-255
* Target 1
  + **Operating System**: Linux
  + **Purpose**: Serve as vulnerable web server
  + **IP Address**: 192.168.1.110
* Kali
  + **Operating System**: Kali Linux
  + **Purpose**: Serve as attack machine to conduct offensive operations
  + **IP Address**: 192.168.1.90
* ELK
  + **Operating System**: Linux
  + **Purpose**: Provide Kibana to allow for analyzing logs
  + **IP Address**: 192.168.1.100
* Capstone
  + **Operating System**: Linux
  + **Purpose**: Contains filebeat and metricbeat which allow for testing alerts
  + **IP Address:** 192.168.1.105
* 

### **Description of Targets**

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

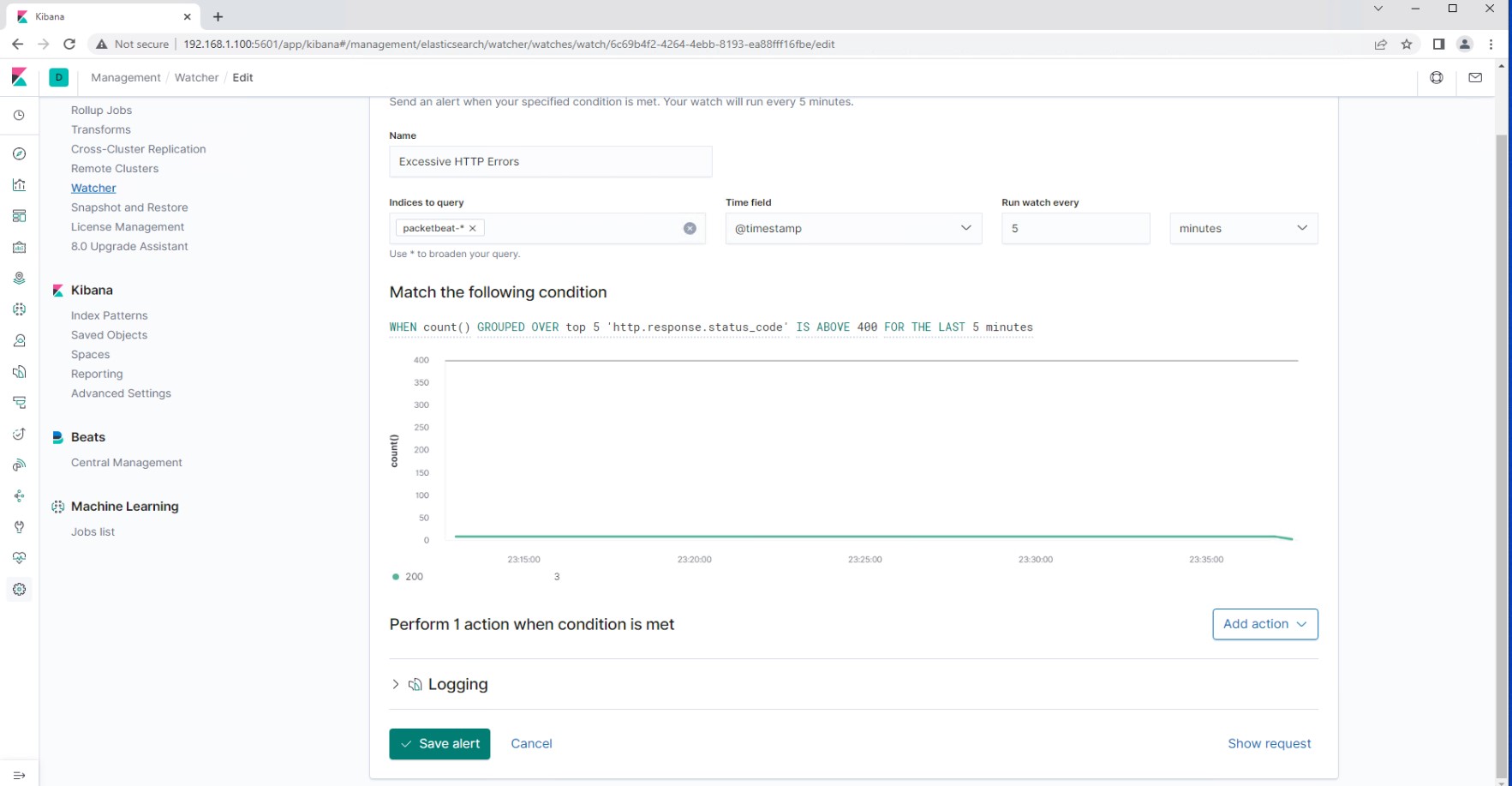
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

### **Monitoring the Targets**

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

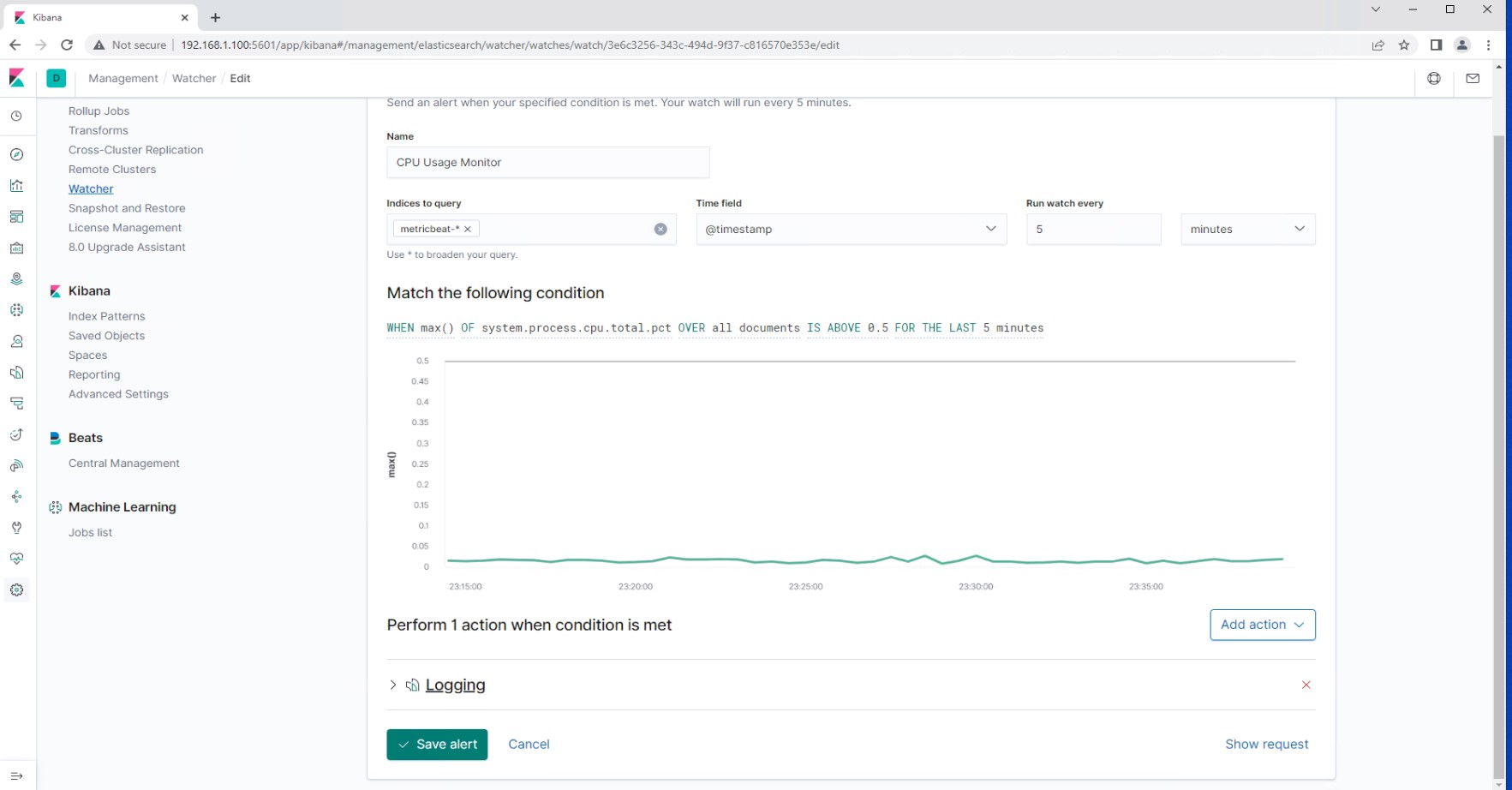
**Excessive HTTP Errors**

Excessive HTTP Errors is implemented as follows:

* **Metric**: http.response.status\_code
* **Threshold**: Top 5 http.response.status\_code is above 400 for the last 5 minutes
* **Vulnerability Mitigated**: Possible SQL Injection
* **Reliability**: This alert has low reliability. It generates false positives quite often.
* 

#### **CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* **Metric**: system.process.cpu.total.pct
* **Threshold**: When system.process.cpu.total.pct over all documents is above 0.5 for the last 5 minutes
* **Vulnerability Mitigated**: Brute Force Attack
* **Reliability**:This alert has low reliability. It generates false positives quite often.
* 

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

HTTP Request Size Monitor is implemented as follows:

* **Metric**: http.request.bytes
* **Threshold**: When sum of http requests is above 3500 bytes in one minute.
* **Vulnerability Mitigated**: HTTP Flood Attack (Type of DDOS)
* **Reliability**: This alert has low reliability. It generates false positives quite often.
* 