# # Blue Team: Summary of Operations

## Table of Contents

- Network Topology

- Description of Targets

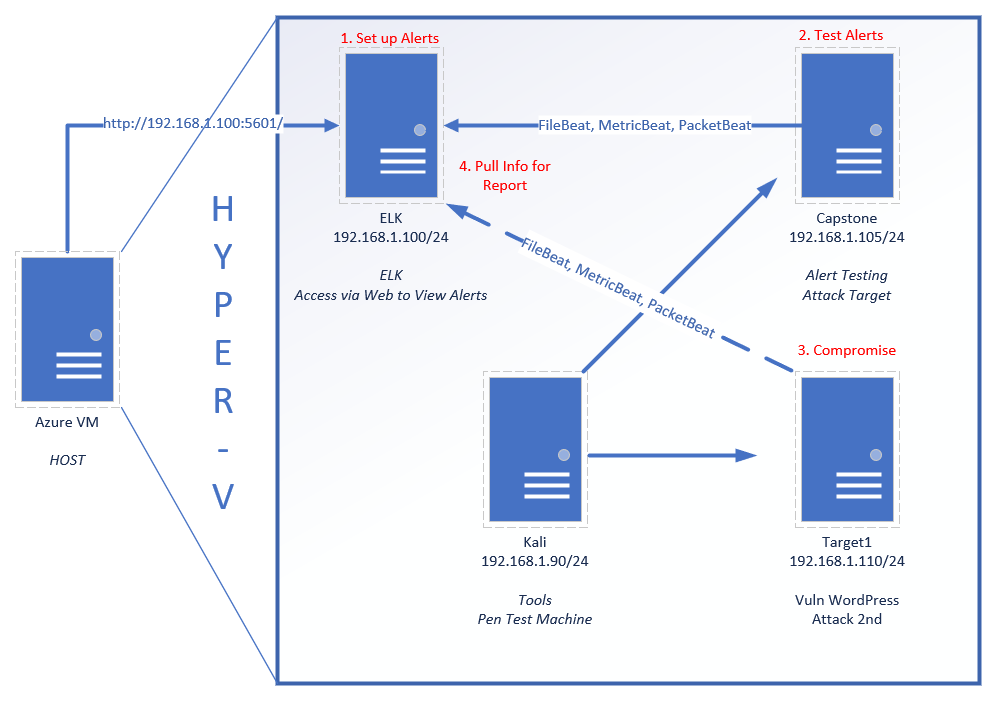
- Monitoring the Targets

- Patterns of Traffic & Behavior

- Suggestions for Going Further

### Network Topology

\_TODO: Fill out the information below.\_



The following machines were identified on the network:

* Azure VM
  + **Operating System**: Windows 10
  + **Purpose**: Using HyperV as a gateway to the other Virtual Machines and to monitor network traffic using Kibana in Port 5601
  + **IP Address**: 192.168.1.100:5601
* Kali Linux
  + **Operating System**: Linux OS
  + **Purpose**: Used to Attack other machines
  + **IP Address**: 192.168.1.90
* ELK
  + **Operating System**: Linux OS
  + **Purpose**: Hosts Kibana logs dashboards.
  + **IP Address**: 192.168.1.100
* Capstone
  + **Operating System**: Linux OS
  + **Purpose**: Filebeat and Metricbeat are installed and forward Logs to the Elk server.
  + **IP Address**: 192.168.1.105
* Target 1
  + **Operating System**: Linux OS
  + **Purpose**: Penetration Testing Vulnerable Machine number 1
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux OS
  + **Purpose**: Penetration Testing Vulnerable Machine number 2
  + **IP Address**:192.168.1.115

### Description of Targets

\_TODO: Answer the questions below.\_

The target of this attack was: `Target 1` (192.168.1.110/24).

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 as described in further detail below have been implemented:

* HTTP Request Size Monitor
  + When there is over 3,500 bytes requested within 1 minute then trigger the alert
* Excessive HTTP Errors
  + When there is 400 or plus HTTP Request codes in the last 5 minutes trigger the alert
* CPU Usage Monitor
  + When the CPU usage goes over 50% trigger the alters

### Monitoring the Targets

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

#### CPU Usage Monitor

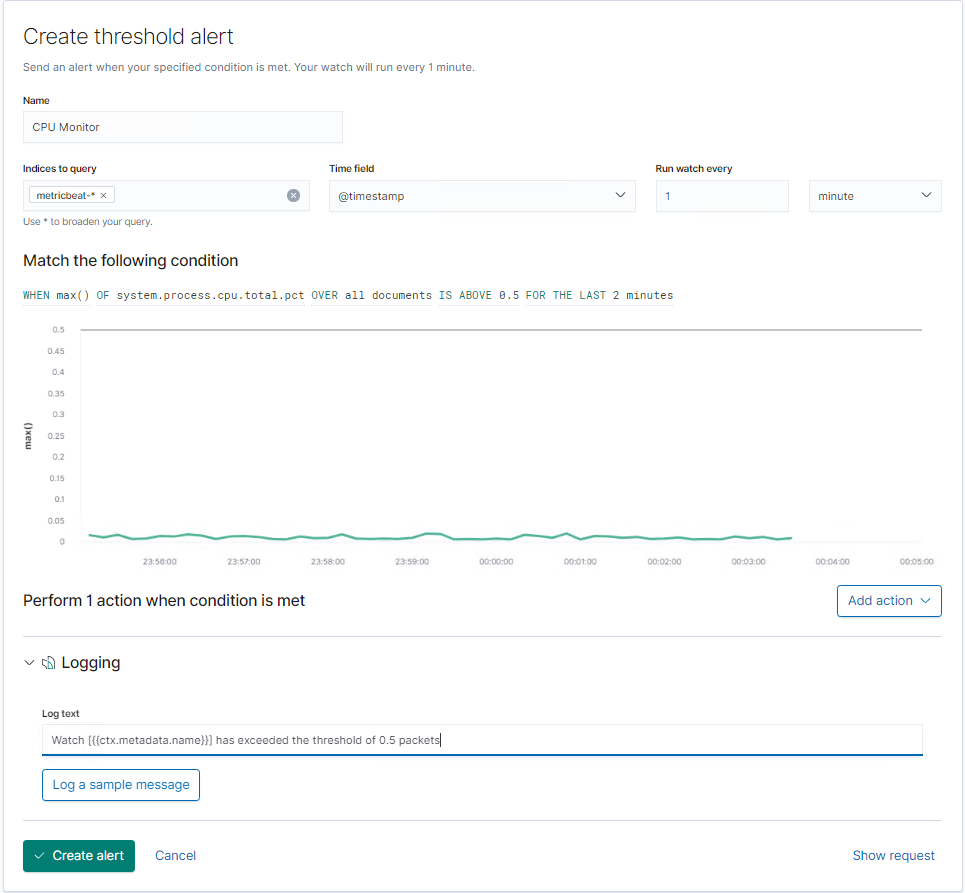
CPU Usage Monitor is implemented as follows:

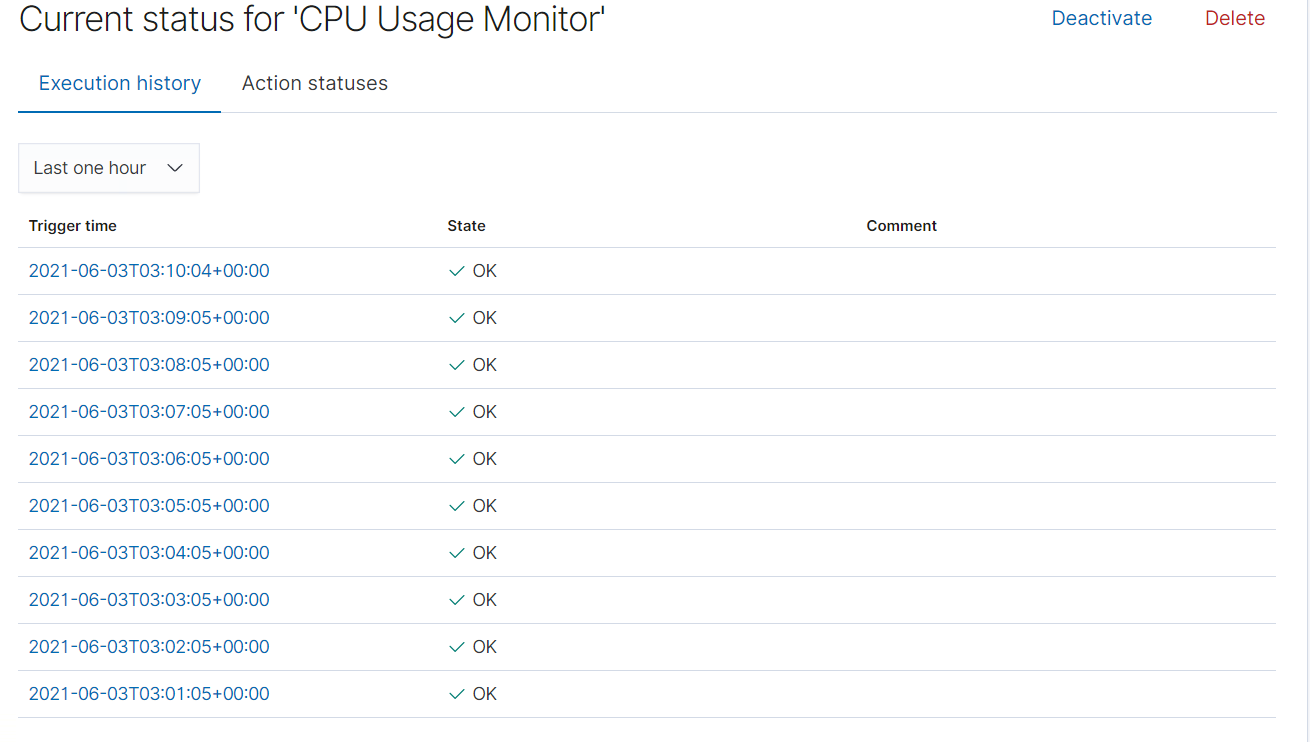
- Metricbeat

-CPU usage over 50% in the last 5 minutes

- \*\*Vulnerability Mitigated\*\*: Brute force attacks

- \*\*Reliability\*\*: Medium





#### HTTP Request Size Monitor

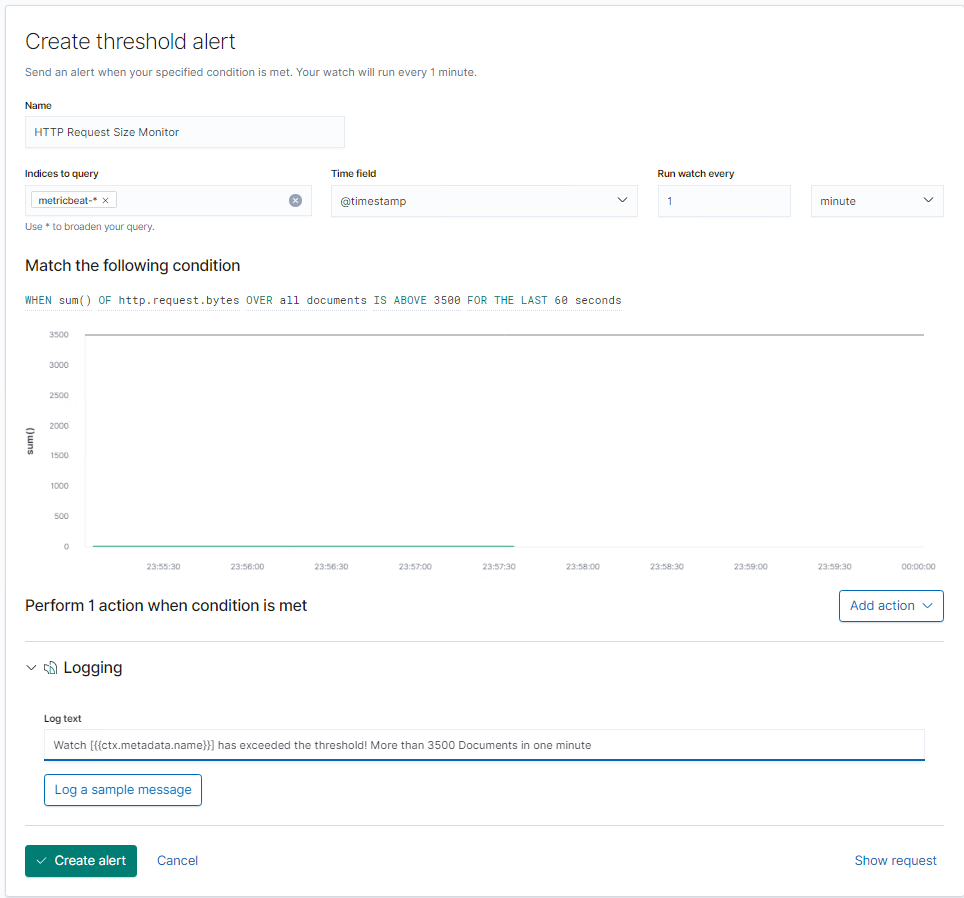
The HTTP Request Size Monitor is implemented as follows:

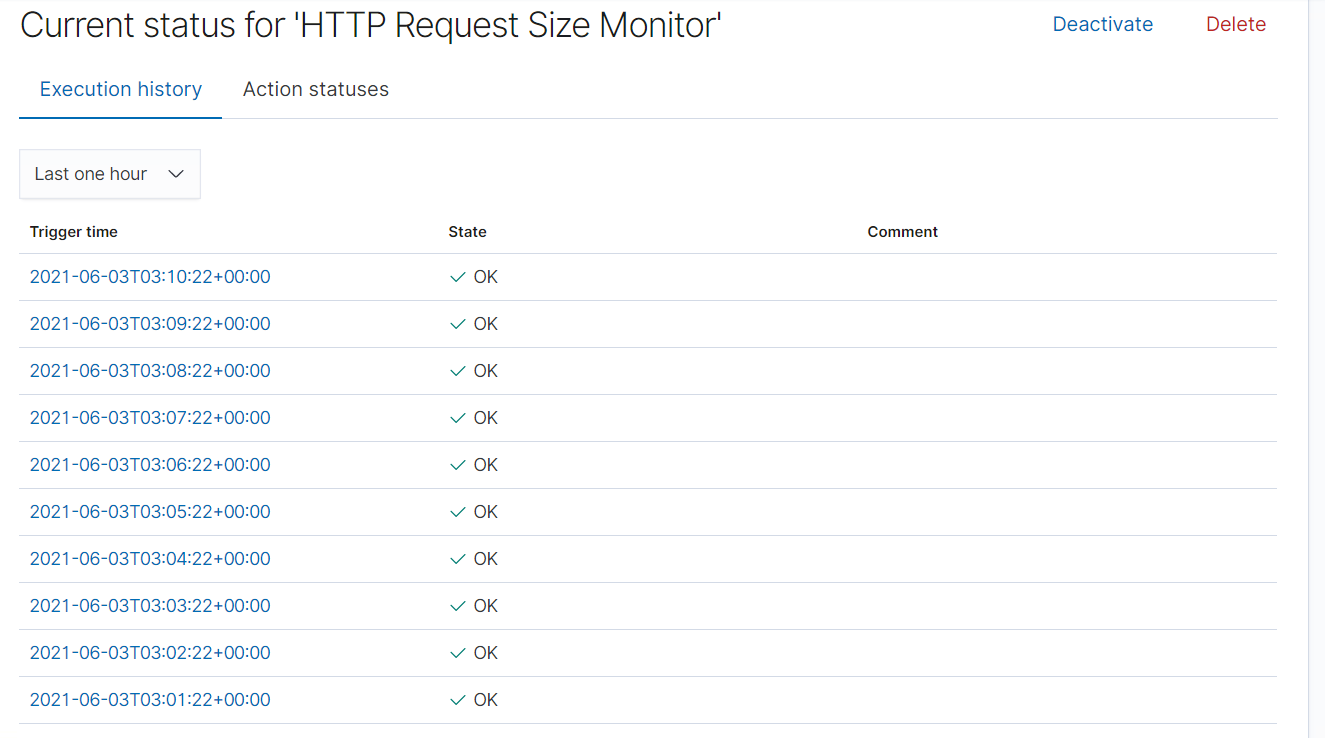
- Metricbeat

- When packet size exceeds 3500 bytes in the last 1 minute

- Vulnerability Mitigated: Possible exfiltration and infiltration of data/files either malicious or not given packet size

- Reliability: Low - because there could be files downloaded onto or off the platform. A typical image file would be around 11.8 Kilobytes (11,800 bytes).





#### Excessive HTTP Errors

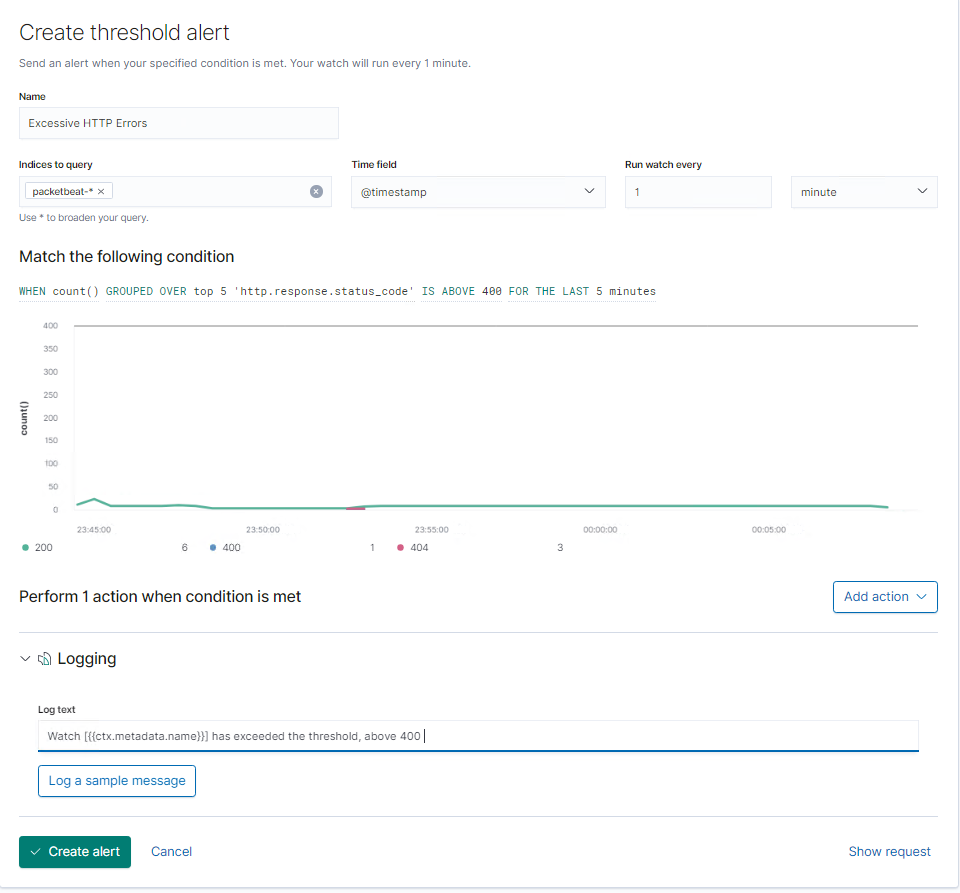
Excessive HTTP Errors are implemented as follows:

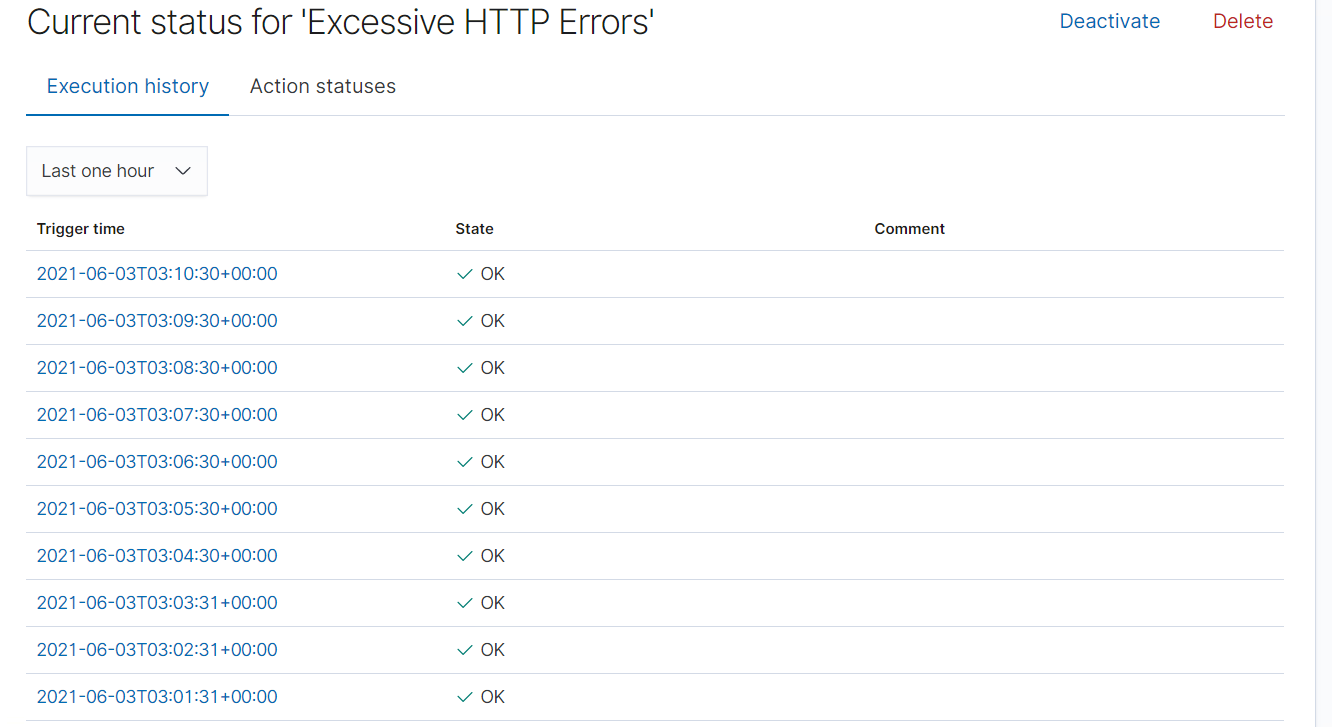
- Packetbeat

- HTTP Responses are over 400 in the last 5 minutes (if there are more files being downloaded from your website or onto your website, it means that there are going more HTTP requests being displayed.)

- Vulnerability Mitigated: Bad user experience, DDOS Attacks, WP Scans

- Reliability: Medium Reliability





### Suggestions for Going Further (Optional)

\_TODO\_:

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain \_how\_ to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

- Vulnerability 1

- \*\*Patch\*\*: TODO: E.g., \_install `special-security-package` with `apt-get`\_

- \*\*Why It Works\*\*: TODO: E.g., \_`special-security-package` scans the system for viruses every day\_

- Vulnerability 2

- \*\*Patch\*\*: TODO: E.g., \_install `special-security-package` with `apt-get`\_

- \*\*Why It Works\*\*: TODO: E.g., \_`special-security-package` scans the system for viruses every day\_

- Vulnerability 3

- \*\*Patch\*\*: TODO: E.g., \_install `special-security-package` with `apt-get`\_

- \*\*Why It Works\*\*: TODO: E.g., \_`special-security-package` scans the system for viruses every day\_