# **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:

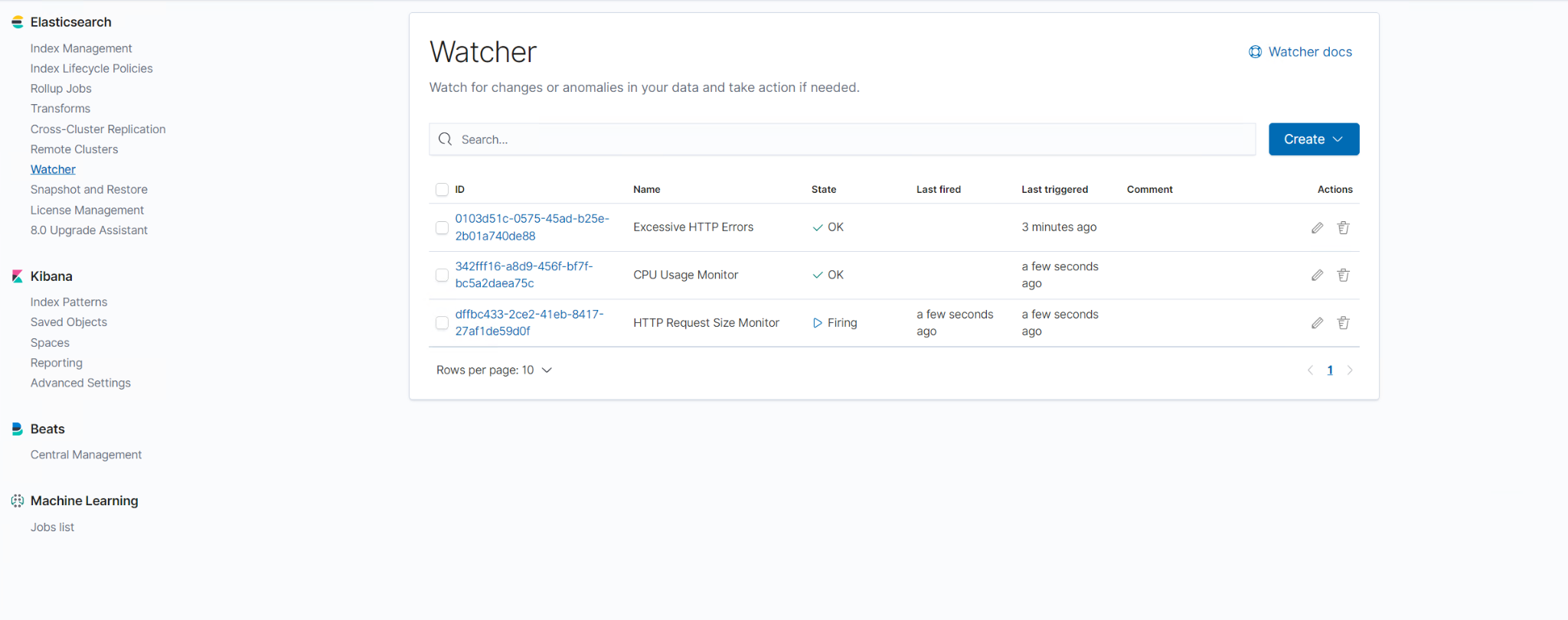
* Name of VM 1: KALI
  + **Operating System**: Kali Linux
  + **Purpose**: Attacking machine
  + **IP Address**: 192.168.1.255
* Name of VM 2: WordPress Server
  + **Operating System**: Debian GNU/Linux 8
  + **Purpose**: Target machine of Kali machine
  + **IP Address**: 192.168.1.110
* Name of VM 3: ELK server
  + **Operating System:** Ubuntu 18/Linux 4
  + **Purpose:** Monitor traffic during attack
  + **IP Address:** 192.168.1.100

### **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:

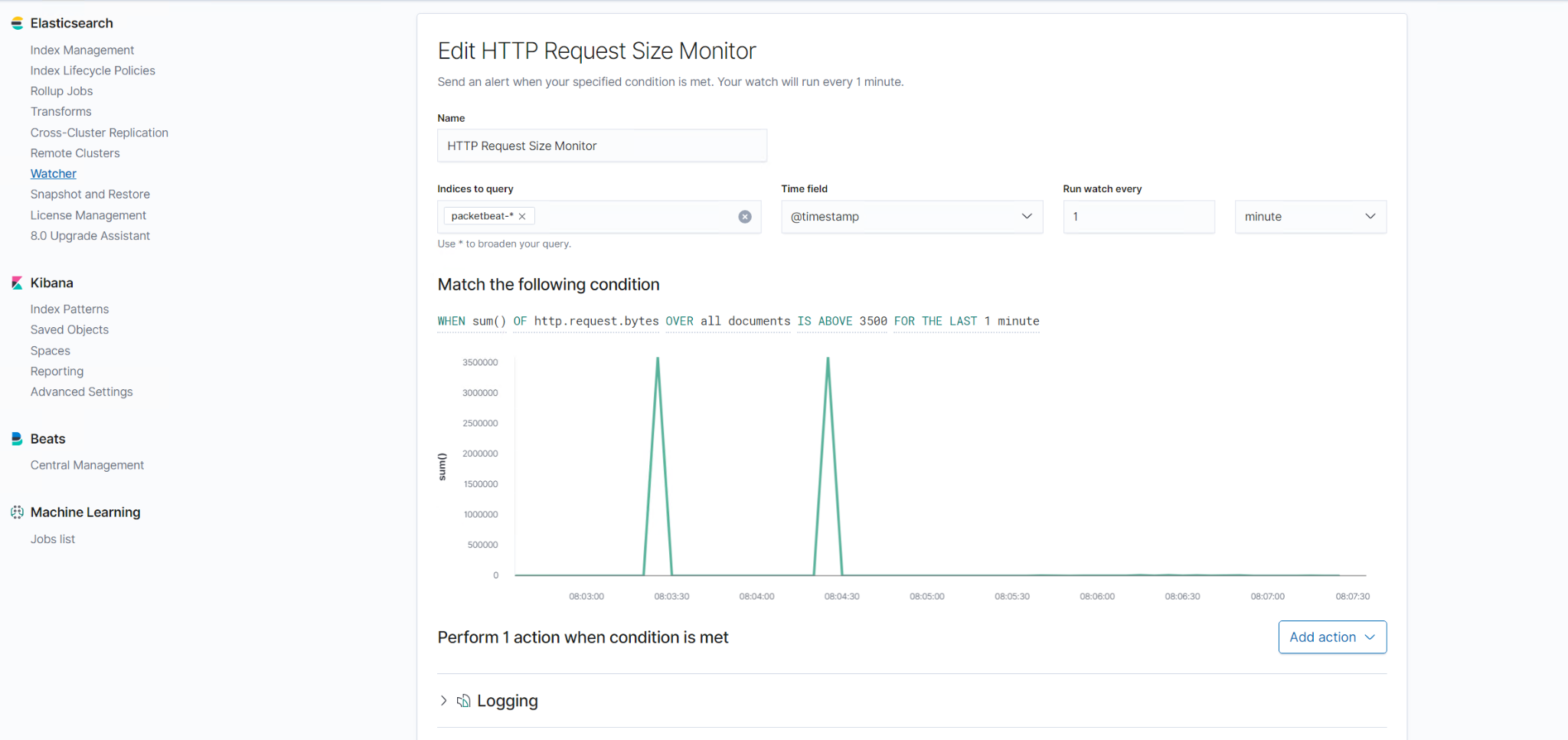
#### 

#### 

#### **Name of Alert 1**

Alert 1 is implemented as follows:

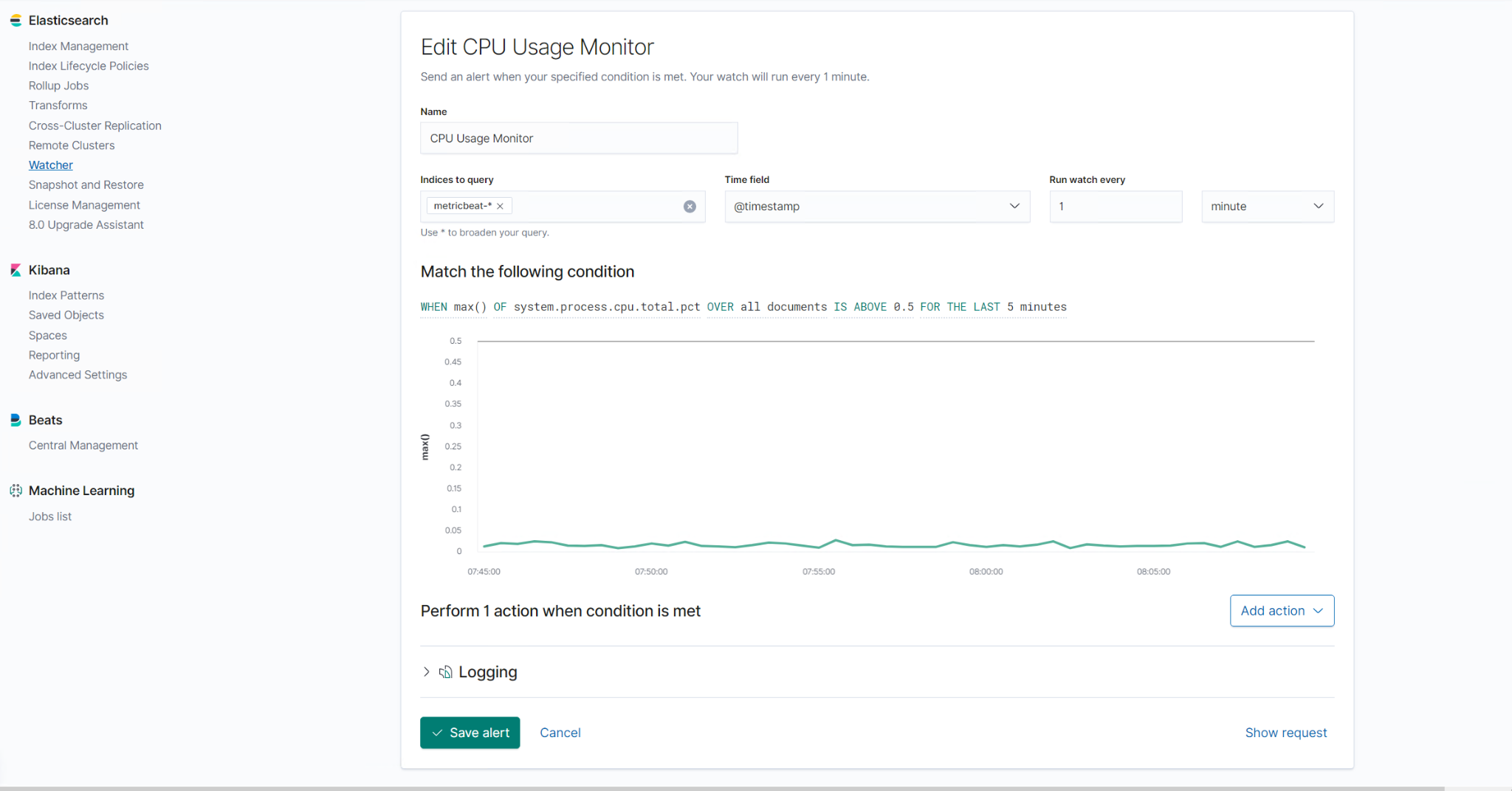
* **Metric**: HTTP Request Size Monitor
* **Threshold**: 3500
* **Vulnerability Mitigated**: Size of HTTP Requests in bytes
* **Reliability**: The alert fires more than average making it have Low reliability



#### **Name of Alert 2**

Alert 2 is implemented as follows:

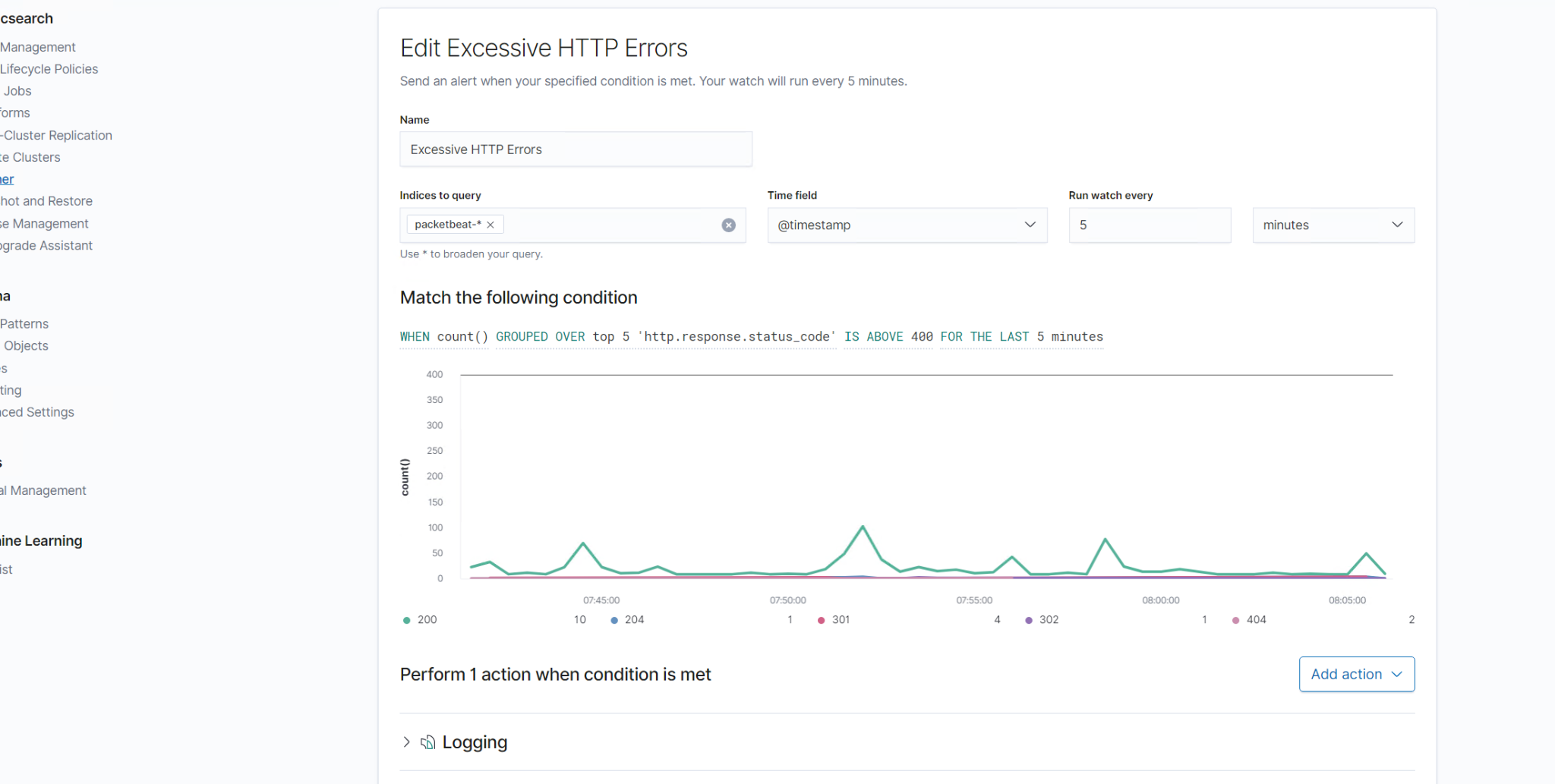
* **Metric**: CPU Usage Monitor
* **Threshold**: Above 0.5
* **Vulnerability Mitigated**: System Process Usage, Higher usage higher risk
* **Reliability**: This alert triggers less often making it have High reliability.



#### **Name of Alert 3**

Alert 3 is implemented as follows:

* **Metric**: Excessive HTTP Errors
* **Threshold**: Above 400
* **Vulnerability Mitigated**: HTTP response status error or success
* **Reliability**: Triggers less often but enough to make medium reliability.

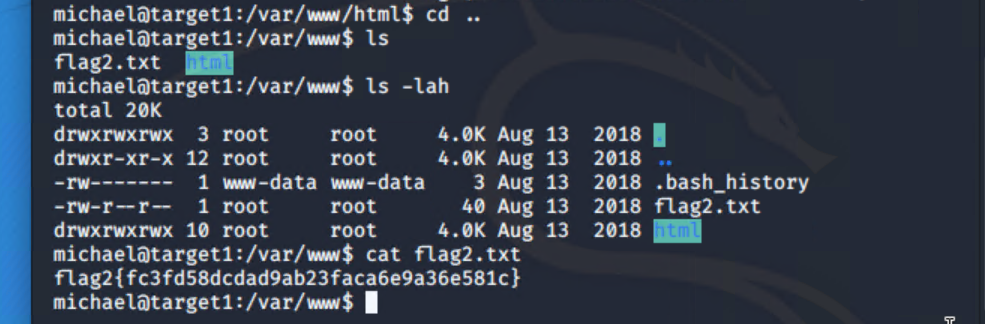


### **Suggestions for Going Further (Optional)**

* 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: Users should not be able to access files that they are not permitted to



* + **Patch**: Chmod to 700, this gives only root read and write access.
  + **Why It Works**: If only root has read and write access to these files then it acts like another layer of security because the attacker first has to elevate his/her privileges to access the files.
* Vulnerability 2: Important information is accessible in plaintext on html pages on wordpress website.
  + **Patch**: Get a hold of developers on site and notify them of the problem.
  + **Why It Works**: If they patch the error then users cannot openly access hashed passwords and other information to use in other attacks or to further an attack.
* Vulnerability 3: ssh
  + **Patch**: You can disable this issue by accessing the /etc/ssh/ssh.conf file as the root user and adding AllowGroups Wheel root
  + **Why It Works**: This will disable ssh access to anyone who does not have root privileges.