Blue Team: Summary of Operations

Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets

Network Topology

Fill out the information below.

The following machines were identified on the network:

Name of VM 1: Kali

- Operating System: Linux
- Purpose: To find the flags and passwords and other penetration test
- IP Address: 192.168.1.90

Name of VM 2: Target 1

- Operating System: Target 1
- Purpose: To expose a vulnerable WordPress server
- IP Address: 192.168.1.110

Name of VM 3 : Capstone

- Operating System: Terminal
- Purpose: Sends Filebeat and Metricbeat logs to the ELK machine and solely for testing alerts.
- IP Address: 192.168.1.105

Name of VM 4: ELK

- Operating System: Terminal
- Purpose: To send the Kibana dashboard and holds the elk docker container.
- IP Address: 192.168.1.100

Description of Targets

TODO: Answer the questions below.

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

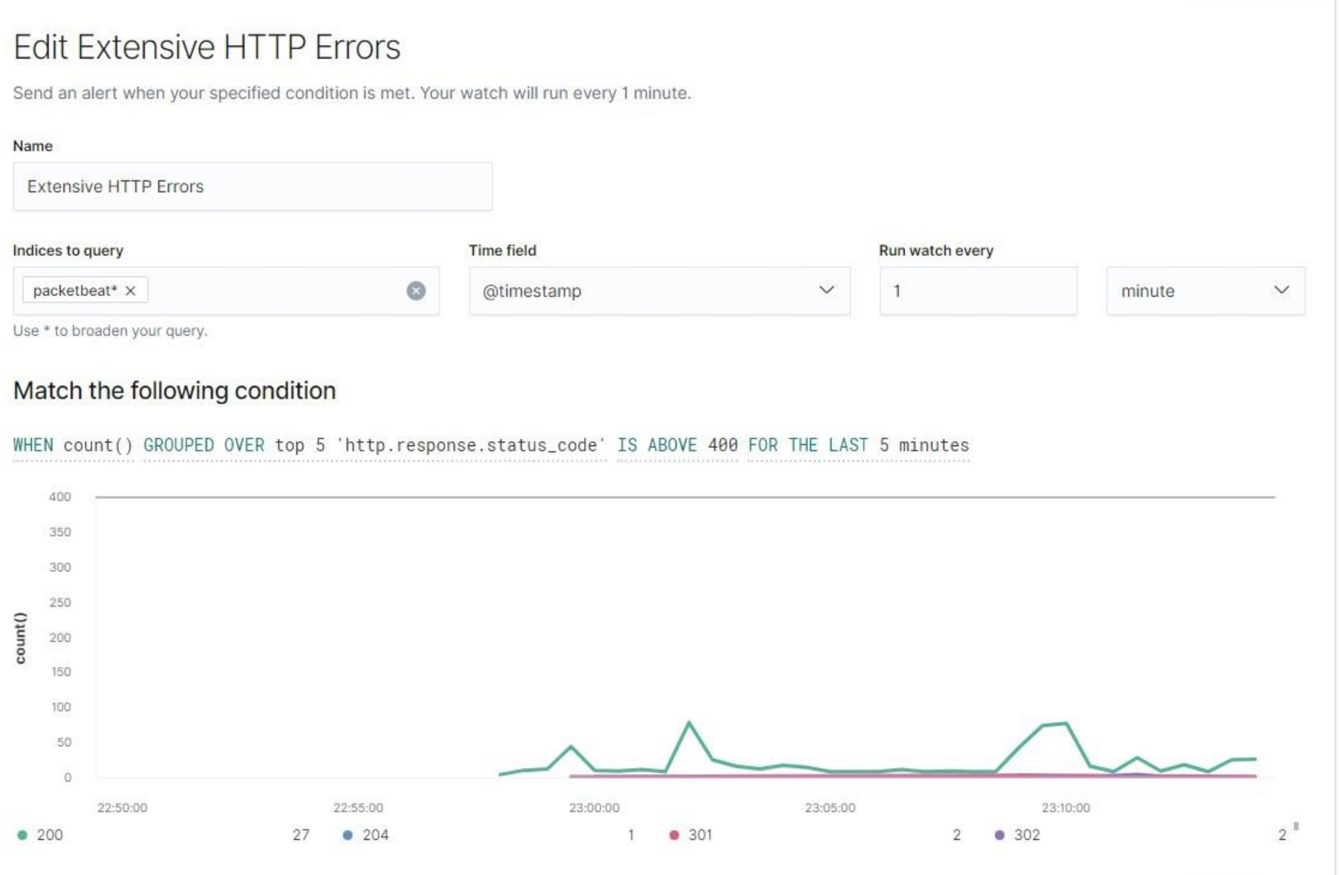
Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

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

Name of Alert 1

- Extensive HTTP Errors is implemented as follows:
- Metric: When count of http response status code goes above 400.
- Threshold: 400 For The Last 5 Minutes.
- Vulnerability Mitigated: HTTP Response Status Code.
- Reliability: Generates 100 at maximum so I say reliability as LOW.\
- Screenshot:



Edit Extensive HTTP Errors

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

Extensive HTTP Errors

Indices to query

packetbeat* ×

Use * to broaden your query.

Time field

@timestamp

Run watch every

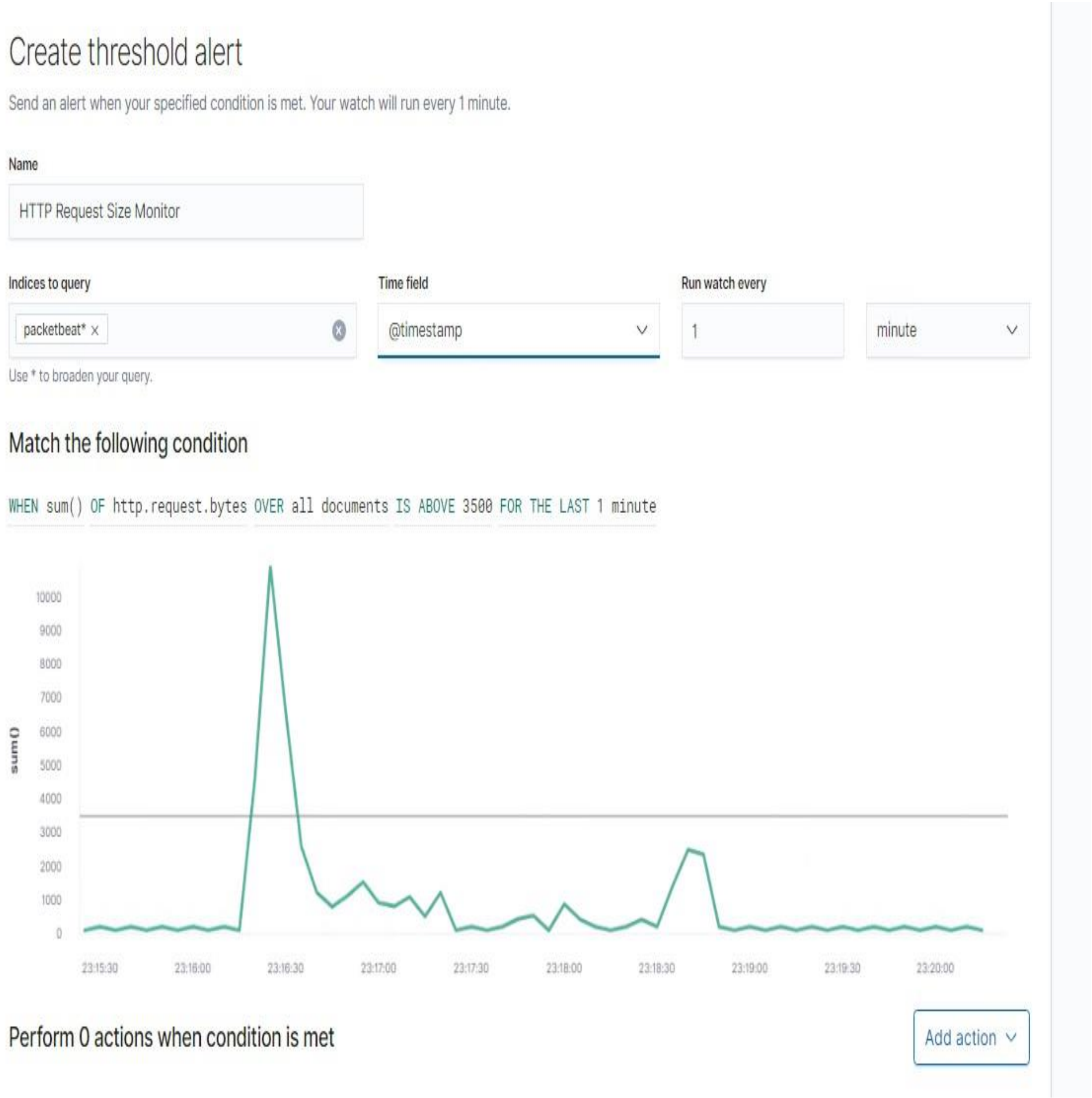
1 minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

Name of Alert 2

- HTTP Request Size Monitor is implemented as follows:
- Metric: when sum of request size goes above 3500.
- Threshold: 3500 Last 1 Minutes.
- Vulnerability Mitigated: Sum of Request Size Exceed the threshold.
- Reliability: as per the report, Five times the result exceeds the threshold set by 1500 values, so I say reliability as MEDIUM
- Screenshot:



Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

HTTP Request Size Monitor

Indices to query: packetbeat* ×

Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

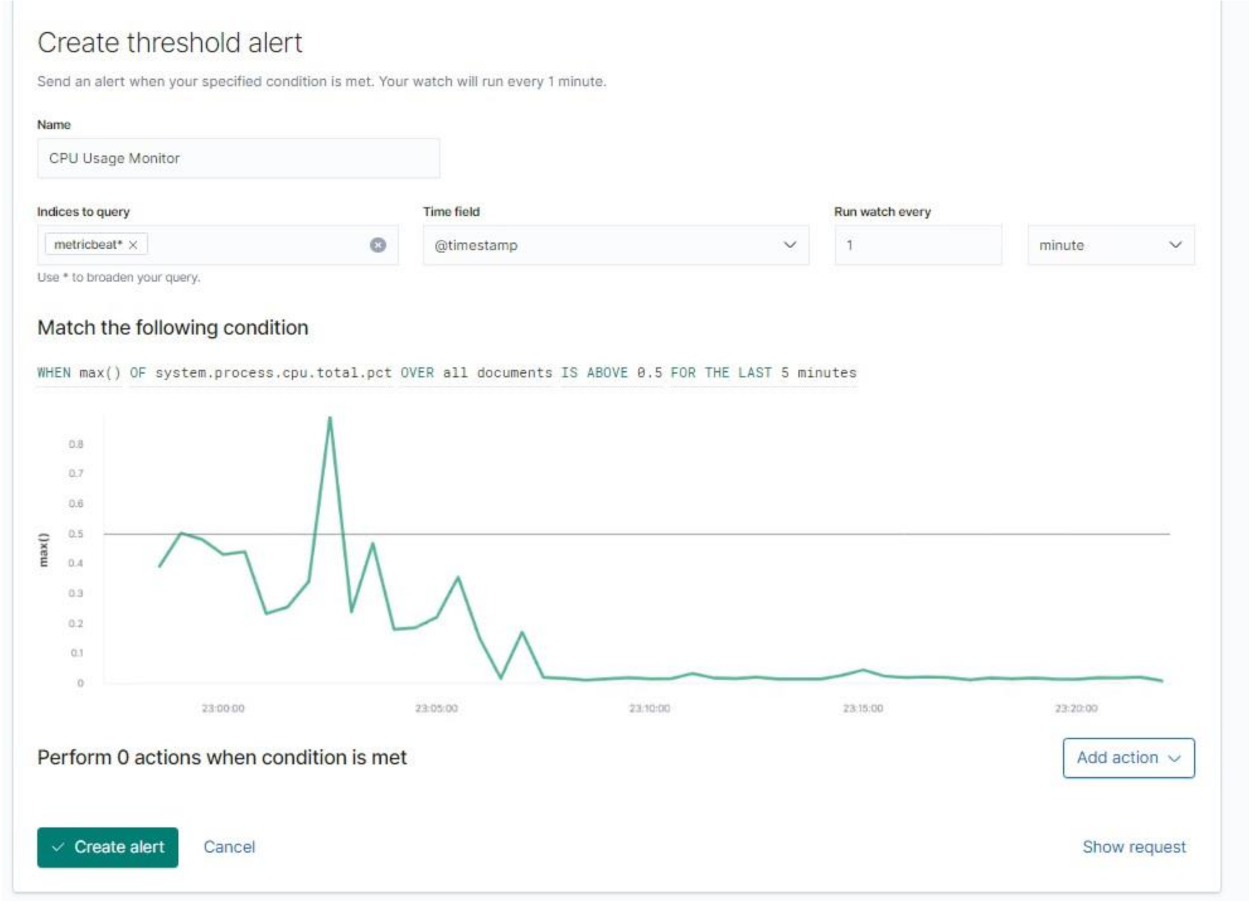
Match the following condition

```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
```

Perform 0 actions when condition is met

Name of Alert 3

- CPU Usage Monitor is implemented as follows:
- Metric: when maximum number of processes running on cpu goes above 0.5.
- Threshold: 0.5
- Vulnerability Mitigated: Maximum System Processes Running on CPU Every Minute.
- Reliability: Reliability is LOW in this alert, because all the cpu usage goes way below 0.5.
- Screenshot:



Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name: CPU Usage Monitor

Indices to query: metricbeat* ×

Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

Match the following condition

```
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
```

Perform 0 actions when condition is met