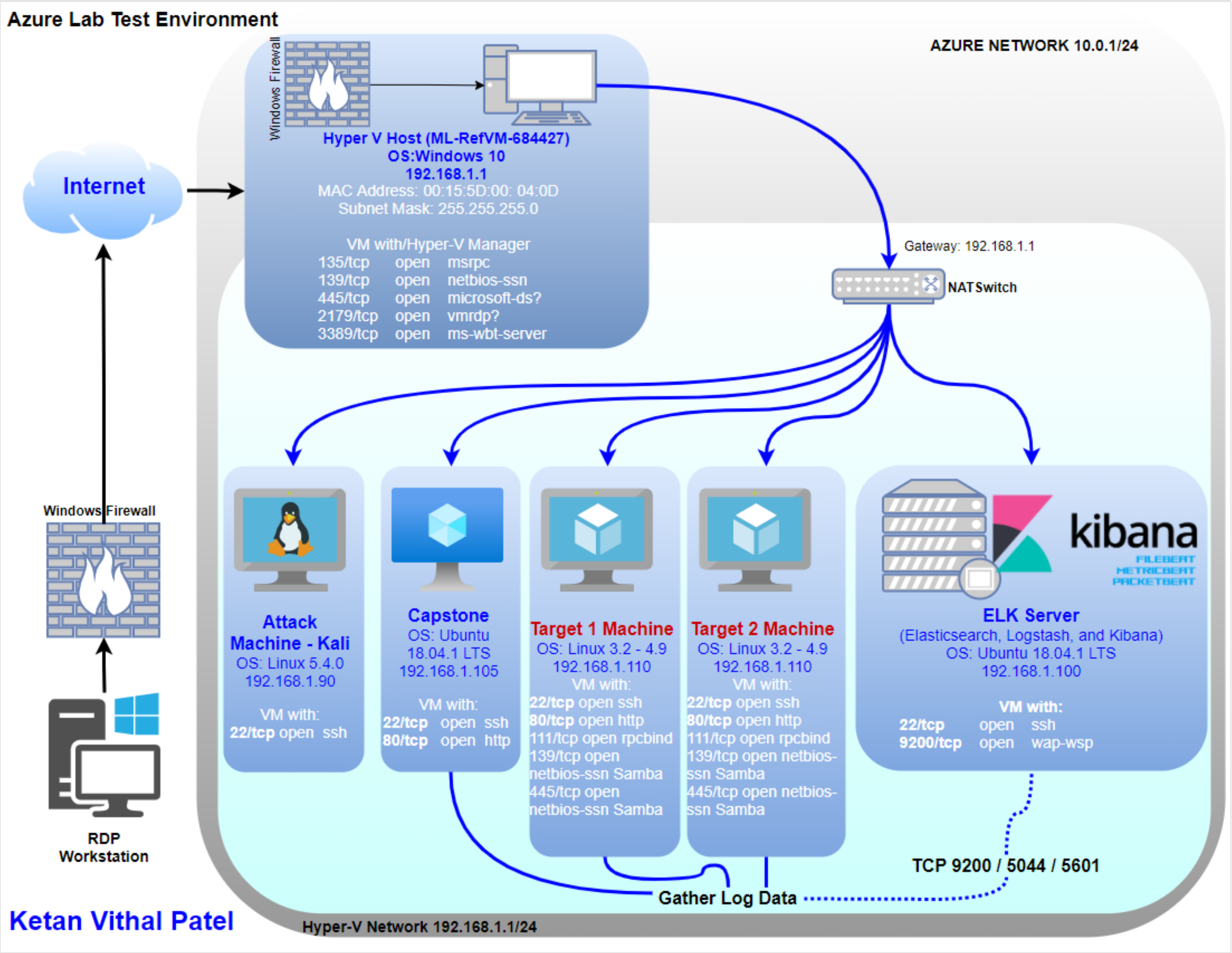
Blue Team: Summary of Operations

By:Ketan V. Patel

Table of Contents

Network Topology

The following machines were identified on the network:



- Name of VM 1 **Kali**
  - Operating System: **Linux 5.4.0**
  - Purpose: **Used as attacking machine**
  - IP Address: **192.168.1.90**
- Name of VM 2 **Capstone**
  - Operating System: **Linux (Ubuntu 18.04.1 LTS)**
  - Purpose: **Used as a testing system for alerts**
  - IP Address: **192.168.1.100**
- Name of VM 2 **ELK**
  - Operating System: **Linux (Ubuntu 18.04.1 LTS)**
  - Purpose: **Used for gathering information from the victim machine using Metricbeat, Filebeats, and Packetbeats**
  - IP Address:**192.168.1.100**
- Name of VM 2 **Target 1**
  - Operating System: **Linux 3.2 - 4.9**
  - Purpose: **The VM with WordPress as a vulnerable server**
  - IP Address:**192.168.1.110**
- Name of VM 2 **Target 2**
  - Operating System: **Linux 3.2 - 4.9**
  - Purpose: **The VM with WordPress as a vulnerable server**
  - IP Address:**192.168.1.115**
- Name of VM 2 **Hyper V Manager**
  - Operating System: **Windows 10**
  - Purpose: **Contains the vulnerable machines and the attacking machine**
  - IP Address:**192.168.1.1**

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:

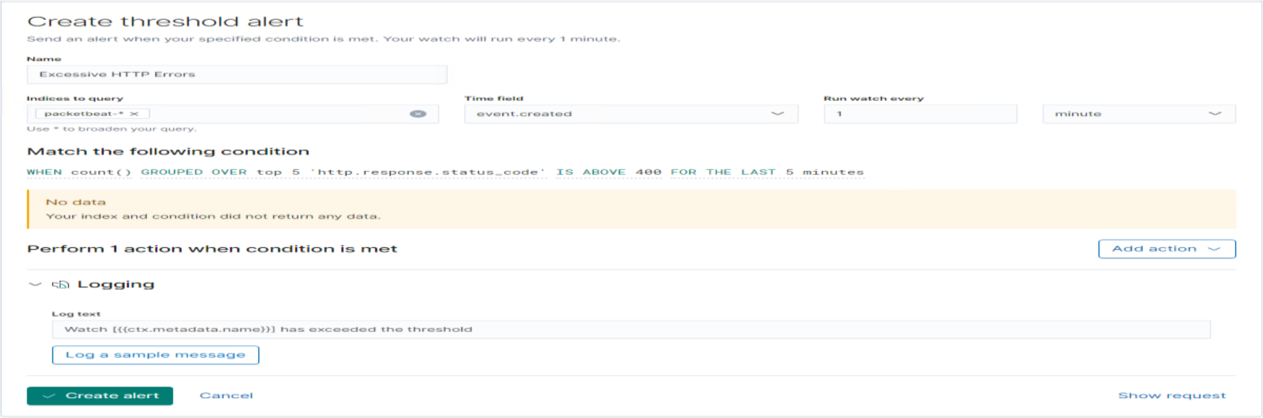
Monitoring the Targets

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:** Packetbeat: http.response.status_code > 400
- **Threshold:** grouped http response status codes above 400 every 5 minutes
  - When count() GROUPED OVER top5 'http.response.status_code' is above 400 for the last 5 minutes
- **Vulnerability Mitigated:**
  - Used intrusion detection/prevention for attacks
  - IPS would block any suspicious IP's
  - Utilize Account Management to lock or request user accounts to change the passwords every 60 days
  - Filter and disable or close port 22
- **Reliability:** This alert will not generate an excessive amount of false positives identifying brute force attacks. Medium



Create threshold alert

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

Name: Excessive HTTP Errors

Indices to query: packetbeat-*

Use * to broaden your query.

Time field: event.created

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
```

No data

Your index and condition did not return any data.

Perform 1 action when condition is met

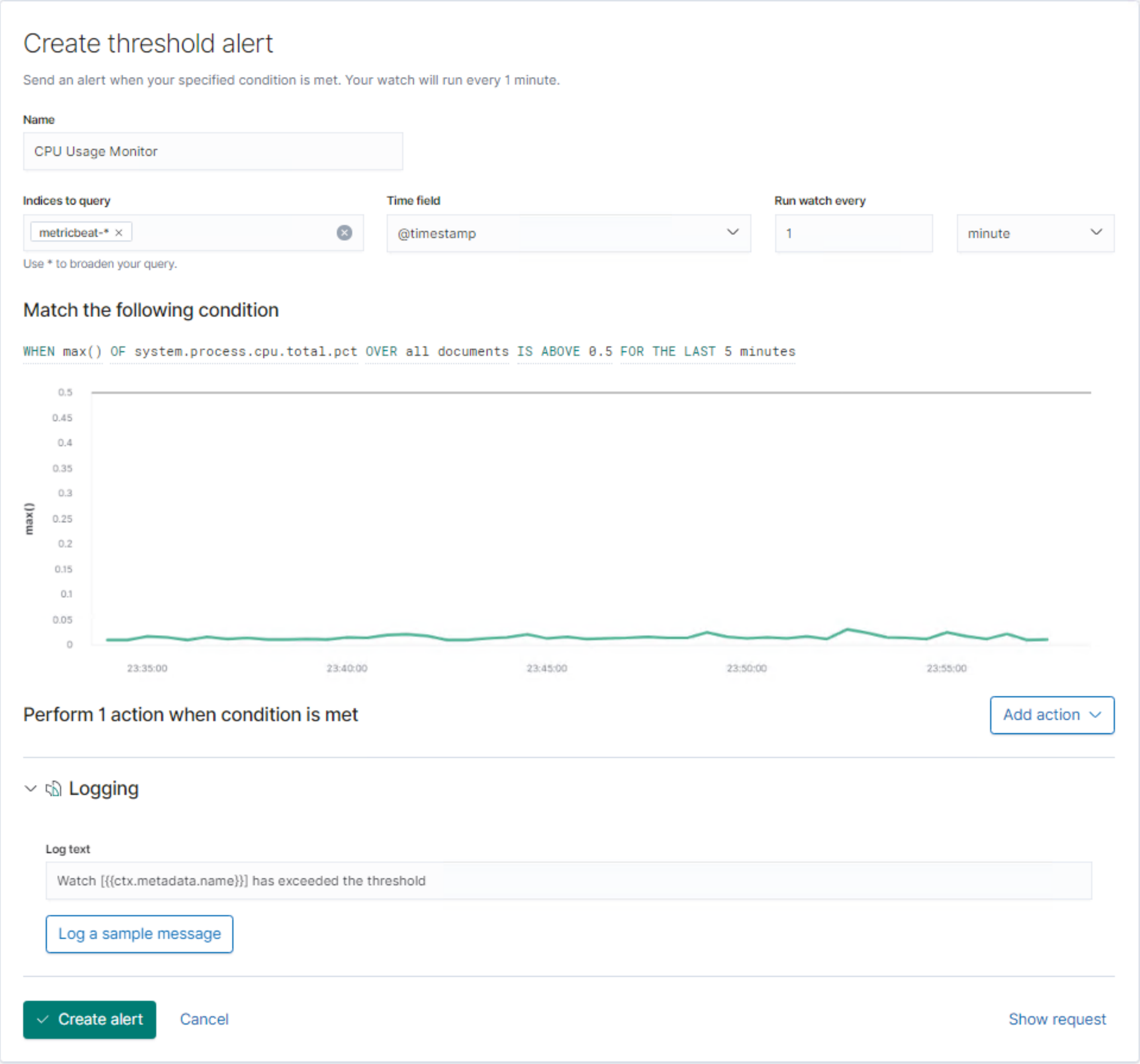
Logging

Log text: Watch [{{ctx.metadata.name}}] has exceeded the threshold

CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric:** Metricbeat: system.process.cpu.total.pct
- **Threshold:** The maximum cpu total percentage is over .5 in 5 minutes
  - WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated:** Controlling the CPU usage percentage at 50%, it will trigger a memory alert only if the CPU remains at or above 50% consistently for 5 minutes. Virus or Malware
- **Reliability:** Yes, this alert can generate a lot of false positives due to CPU spikes occurring when specific integrations are initiated at the start of processing. High



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 1 action when condition is met

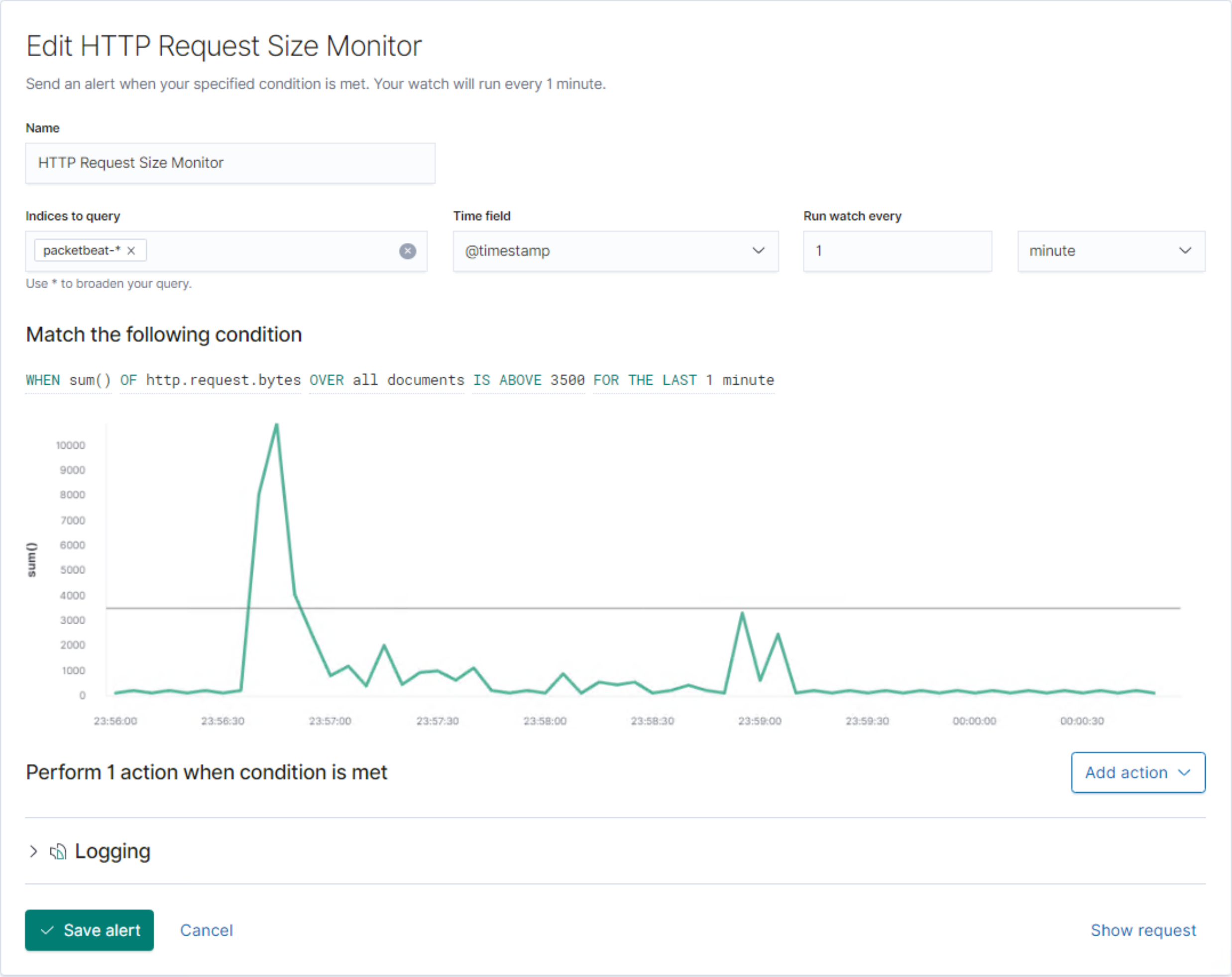
Logging

Log text: Watch [{{ctx.metadata.name}}] has exceeded the threshold

HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- **Metric:** Packetbeat: http.request.bytes
- **Threshold:** The sum of the requested bytes is over 3500 in 1 minute
    - When sum() of http.request.bytes OVER all documents is ABOVE 3500 for the LAST 1 minute
- **Vulnerability Mitigated:** By controlling the number of http request sizes through a filter, protection is enabled to detect or prevent DDOS attacks for IPS/IDS.
- **Reliability:** No, this alert doesn't generate an excessive amount of false positives because DDOS attacks submit requests within seconds, not within minutes. Medium



Edit HTTP Request Size Monitor

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 1 action when condition is met

Logging