Blue Team: Summary of Operations

Report by: Amisha Mehta

Table of Contents

Network Topology

The following machines were identified on the network:

- Azure VM
    - **Operating System**: WIndows 10 Pro
    - **Purpose**: Hyper V Host
    - **IP Address**:192.168.1.100
- Target 1
    - **Operating System**:Debian GNU/ Linux 8
    - **Purpose**: Expose Vulnerable Wordpress Server
    - **IP Address**:192.168.1.110
- Capstone
    - **Operating System**: Ubuntu 18.04.1
    - **Purpose**: Filebeat and Metricbeat are installed and will forward logs to the ELK machine.
    - **IP Address**:192.168.1.105
- ELK
    - **Operating System**: Ubuntu 18.04.4
    - **Purpose**: Holds Kibana Dashboards
    - **IP Address**:192.168.1.100
- Kali
    - **Operating System**: Kali Linux
    - **Purpose**: Used for Pentesting
    - **IP Address**:192.168.1.90

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:

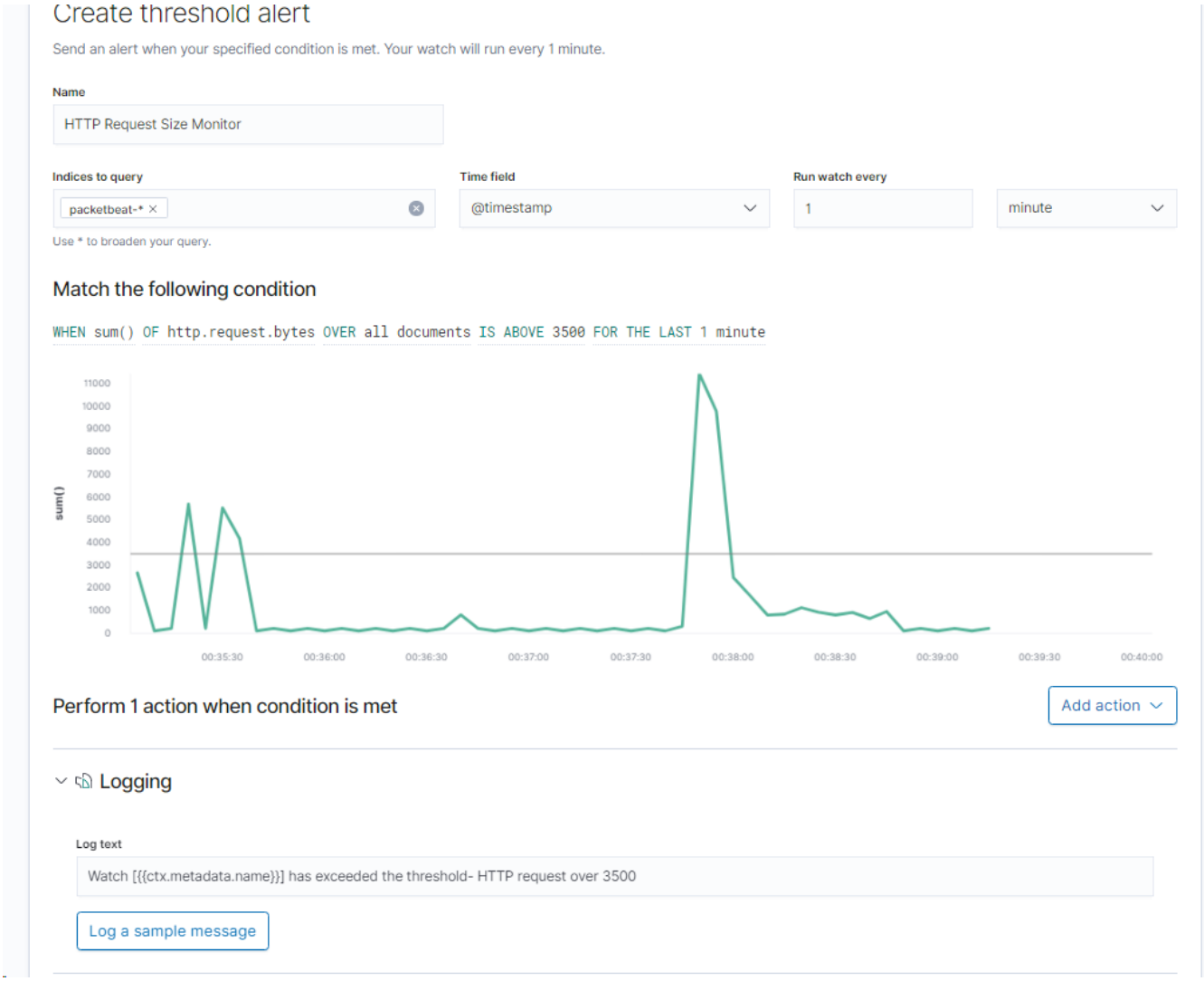
Monitoring the Targets

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

HTTP Request Size Monitor

Alert 1 is implemented as follows:

- **Metric**: When sum () of http.request.bytes over all documents
- **Threshold**: is above 3500 for the last 1 minute
- **Vulnerability Mitigated**: DoS Attack or code injection in HTTP request.
- **Reliability**: Alert has a medium reliability and there is a possibility for large non-malicious HTTP request. Alert could create false positives.

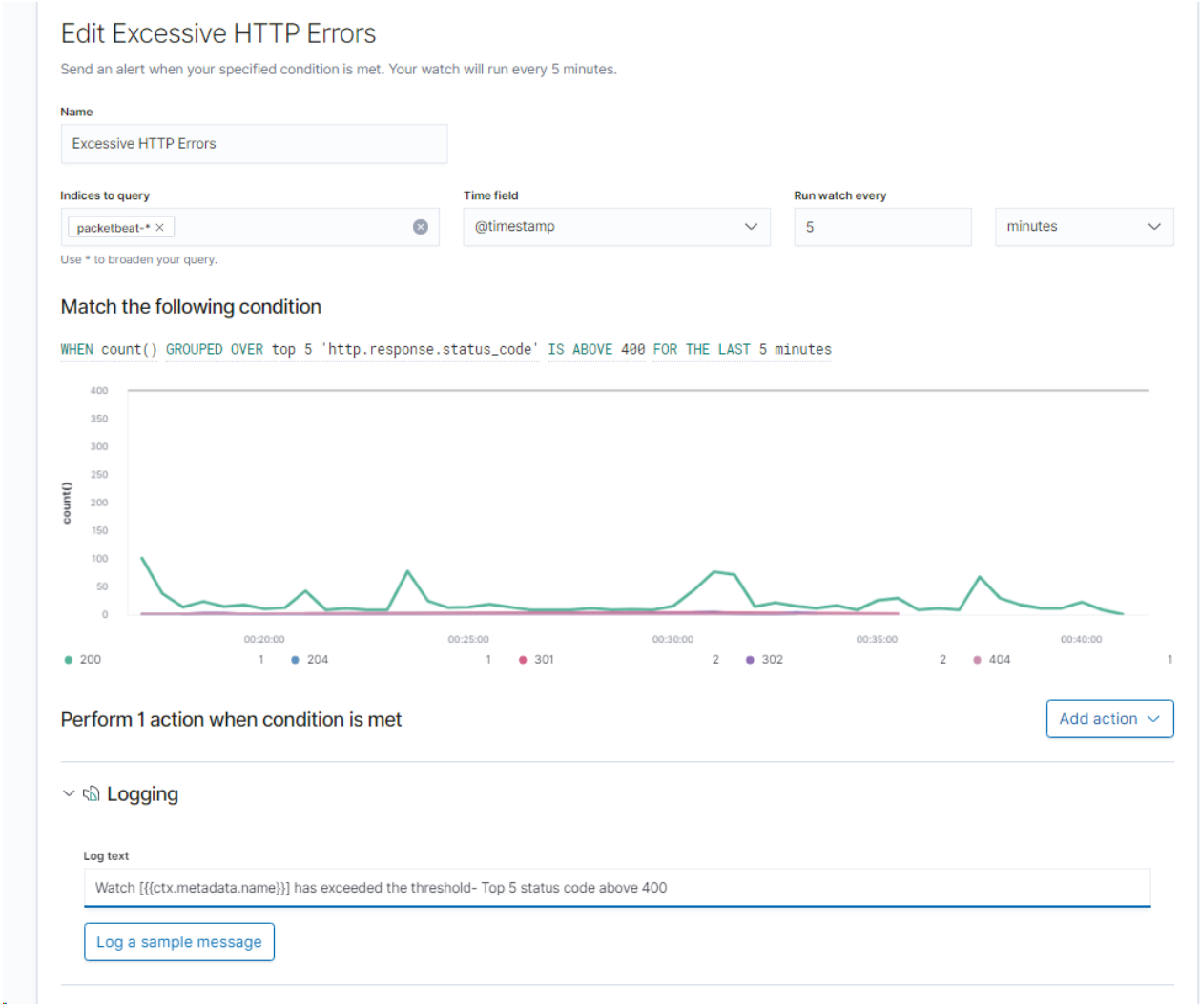


Excessive HTTP Errors

Alert 2 is implemented as follows:

- **Metric**:When count grouped over top 5 http.request.status.code
- **Threshold**: is above 400 for the last 5 minutes
- **Vulnerability Mitigated**: Brute Force Attack

- **Reliability**: 400+ codes are concerning client and server errors. Measuring by 400 error codes will filter out normal responses. This alert is highly reliable.



CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: When max of system.process.cpu.total.pct
- **Threshold**: is above .5 for the last 5 minutes
- **Vulnerability Mitigated**: Malware or viruses taking up resources.
- **Reliability**: This alert is highly reliable in not only will it catch malicious software or programs using cpu but can also show where cpu usage can be improved.

Send an alert when your specified condition is met. Your watch will run every 5 minutes.

Name

CPU Usage Monitor

Indices to query

metricbeat-* ×

Time field

@timestamp

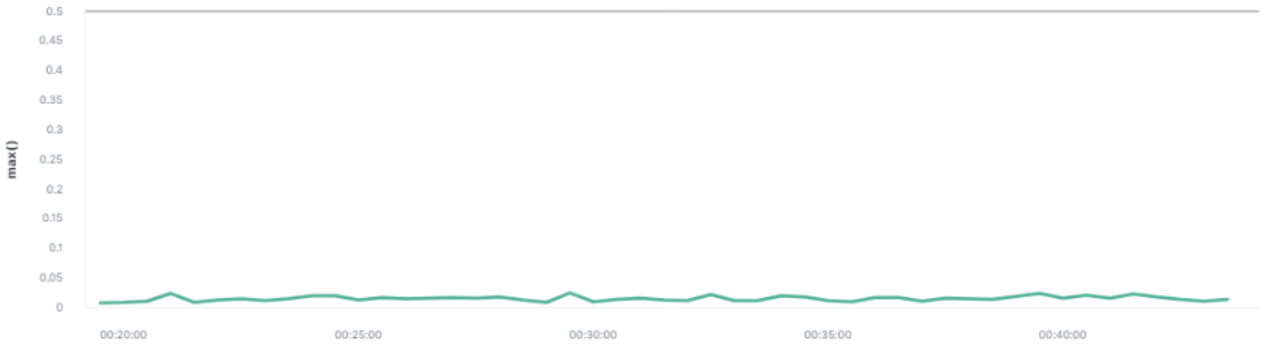
Run watch every

5 minutes

Use * to broaden your query.

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

Add action

Logging

Log text

Watch [{{ctx.metadata.name}}] has exceeded the threshold -CPU usage over .5

Log a sample message

Create alert Cancel Show request