Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- ELK
    - **Operating System**: Ubuntu 18.04
    - **Purpose**: ELK server
    - **IP Address**: 192.168.1.100
- Target 1
    - **Operating System**: Debian GNU/Linux 8
    - **Purpose**: WordPress Host
    - **IP Address**: 192.168.1.110
- Capstone
    - **Operating System**: Ubuntu 18.04
    - **Purpose**: Vulnerable Web Server
    - **IP Address**: 192.168.1.105
- Kali
    - **Operating System**: Debian Kali 5.4.0
    - **Purpose**: Attack Machine
    - **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:

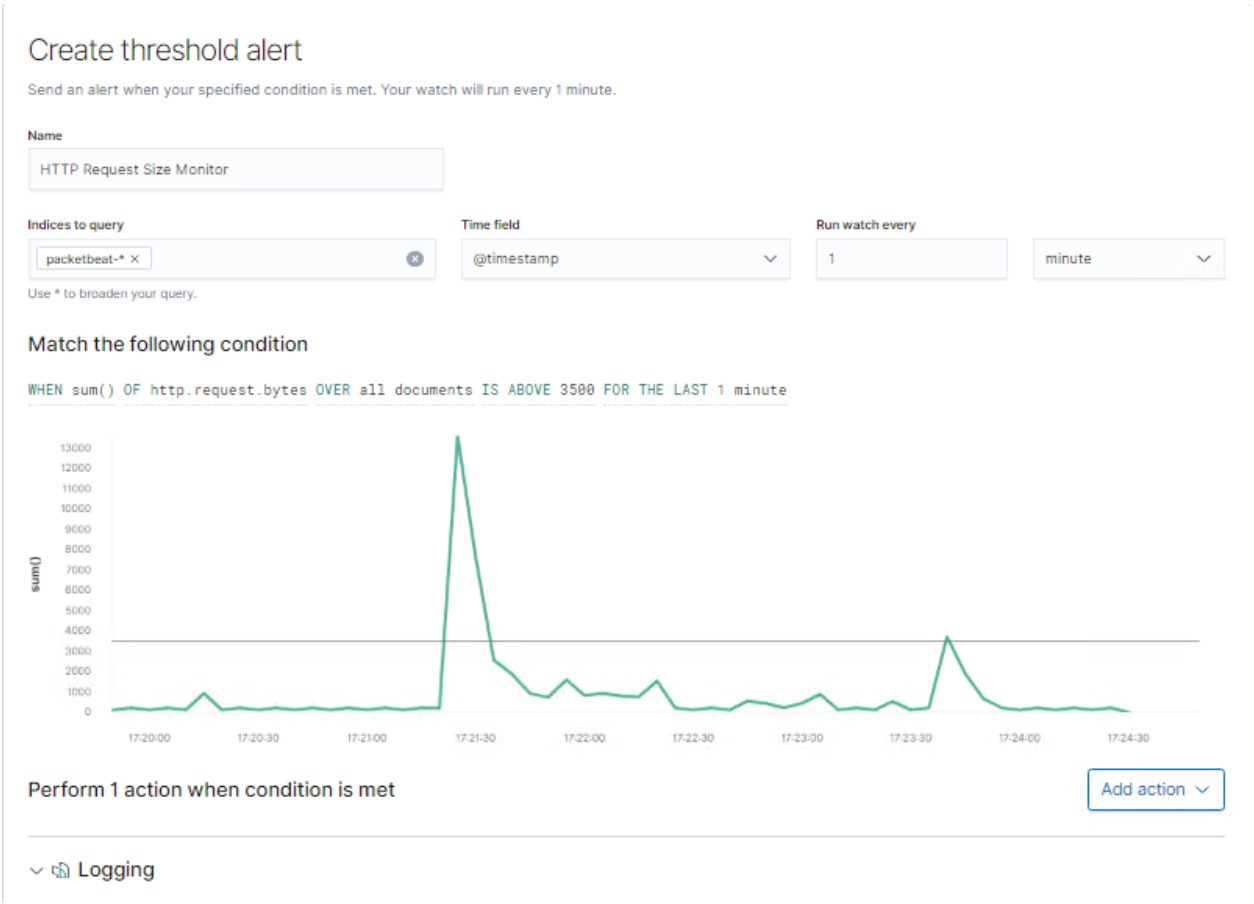
Monitoring the Targets

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

HTTP Request Size Monitor

HTTP Request Size Monitor 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**: High traffic events such as XSS attacks and Ddos attacks
- **Reliability**: I would rate this as medium reliability as it could flag a malicious script running, or code injection event. However there is a possibility that it will also flag non-malicious high HTTP request events.

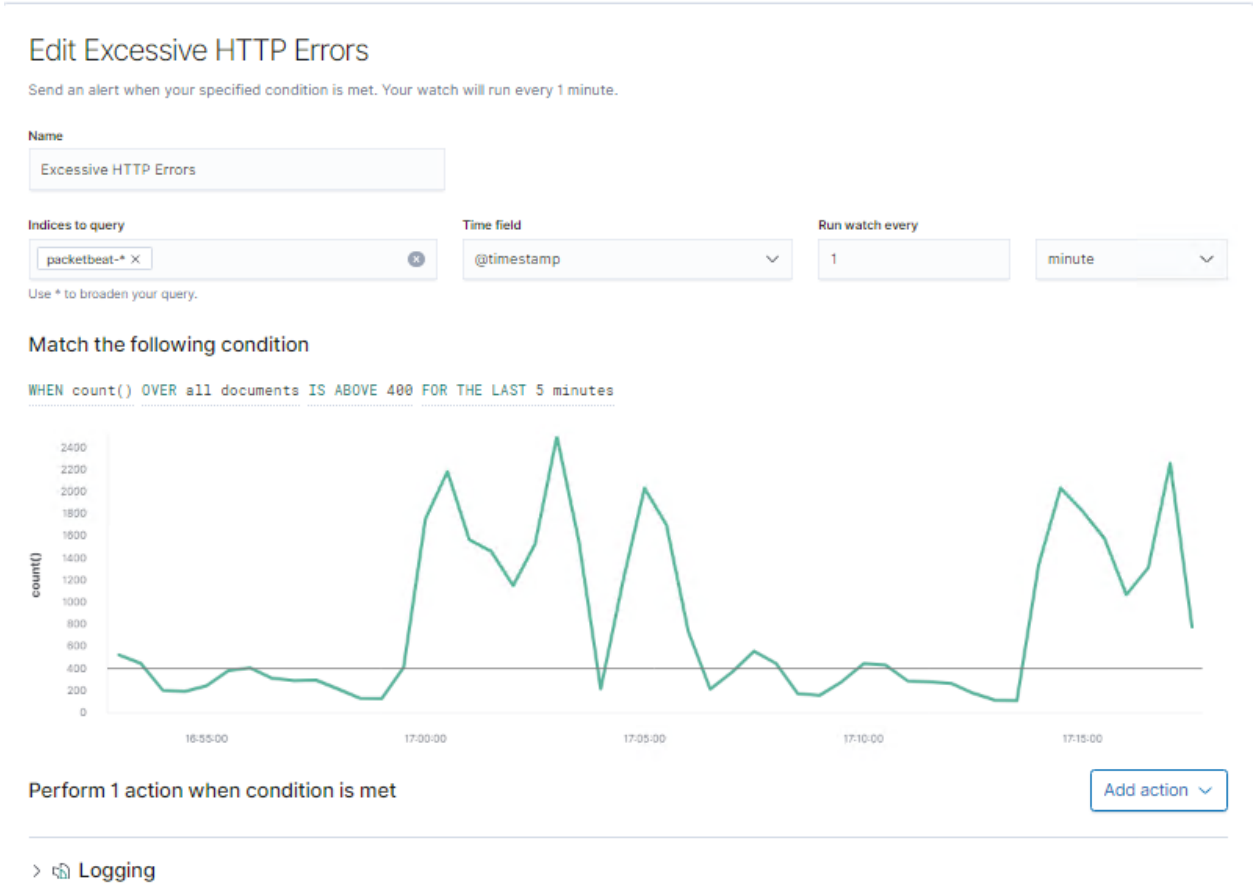


Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

- **Metric**: WHEN count() OVER all documents
- **Threshold**: IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Enumeration

- **Reliability**: I would rate this as high reliability as it will only flag high numbers of HTTP errors in a short period of time which usually happens during brute force attacks.



CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents
- **Threshold**: IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: TODO
- **Reliability**: I would rate this as medium reliability as it could flag an event such as john the ripper running. However it could also flag a non malicious event that requires high CPU usage. This alert is also very dependent on system resources and its reliability can fluctuate from system to system.

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

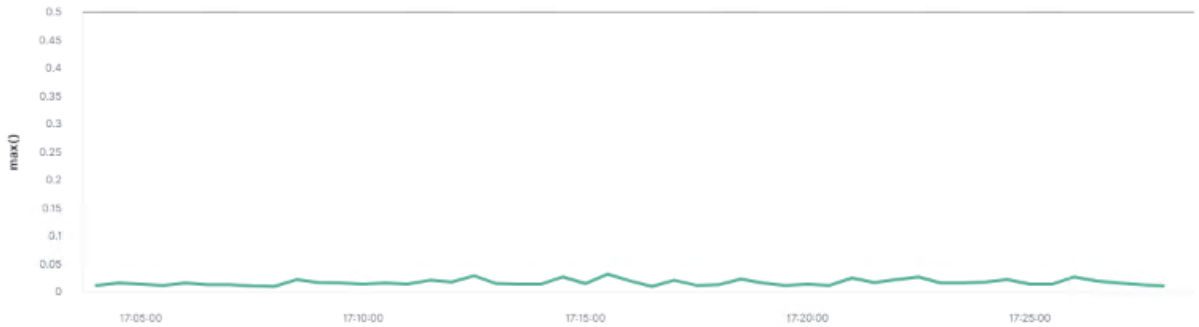
Run watch every

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

Add action

Logging