Blue Team: Summary of Operations

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 to attack Target Machines
    - **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 3: ELK
    - **Operating System**: Linux (Ubuntu 18.04.1 LTS)
    - **Purpose**: Gather information from Targets 1 and 2 using Metricbeat, Filebeat, and Packetbeat
    - **IP Address**: 192.168.1.100
- Name of VM 4: Target 1
    - **Operating System**: Linux 3.2-4.9
    - **Purpose**: VM with WordPress vulnerable web server
    - **IP Address**: 192.168.1.110
- Name of VM 5: Target 2
    - **Operating System**: Linux 3.2-4.9
    - **Purpose**: VM with WordPress vulnerable web server
    - **IP Address**: 192.168.1.115
- Name of VM 6: Hyper V Manager
    - **Operating System**: Windows 10
    - **Purpose**: Platform for running all the machines listed above
    - **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:

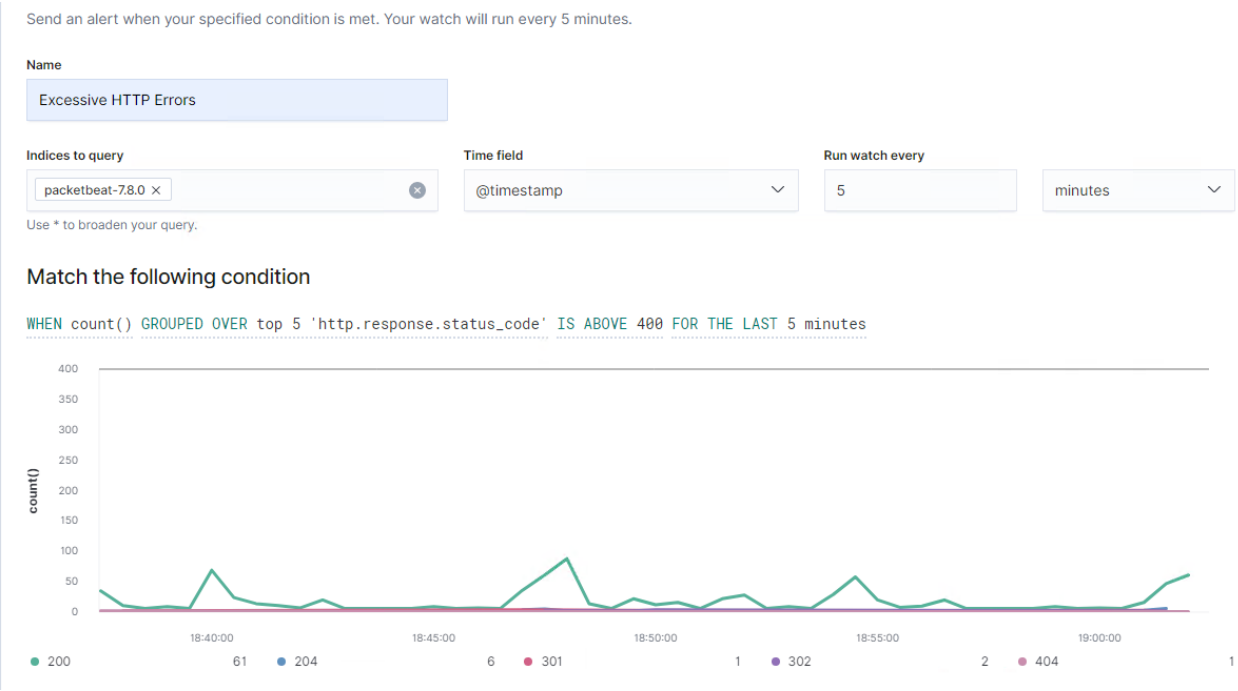
Monitoring the Targets

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

Excessive HTTP Error

Excessive HTTP Errors is implemented as follows:

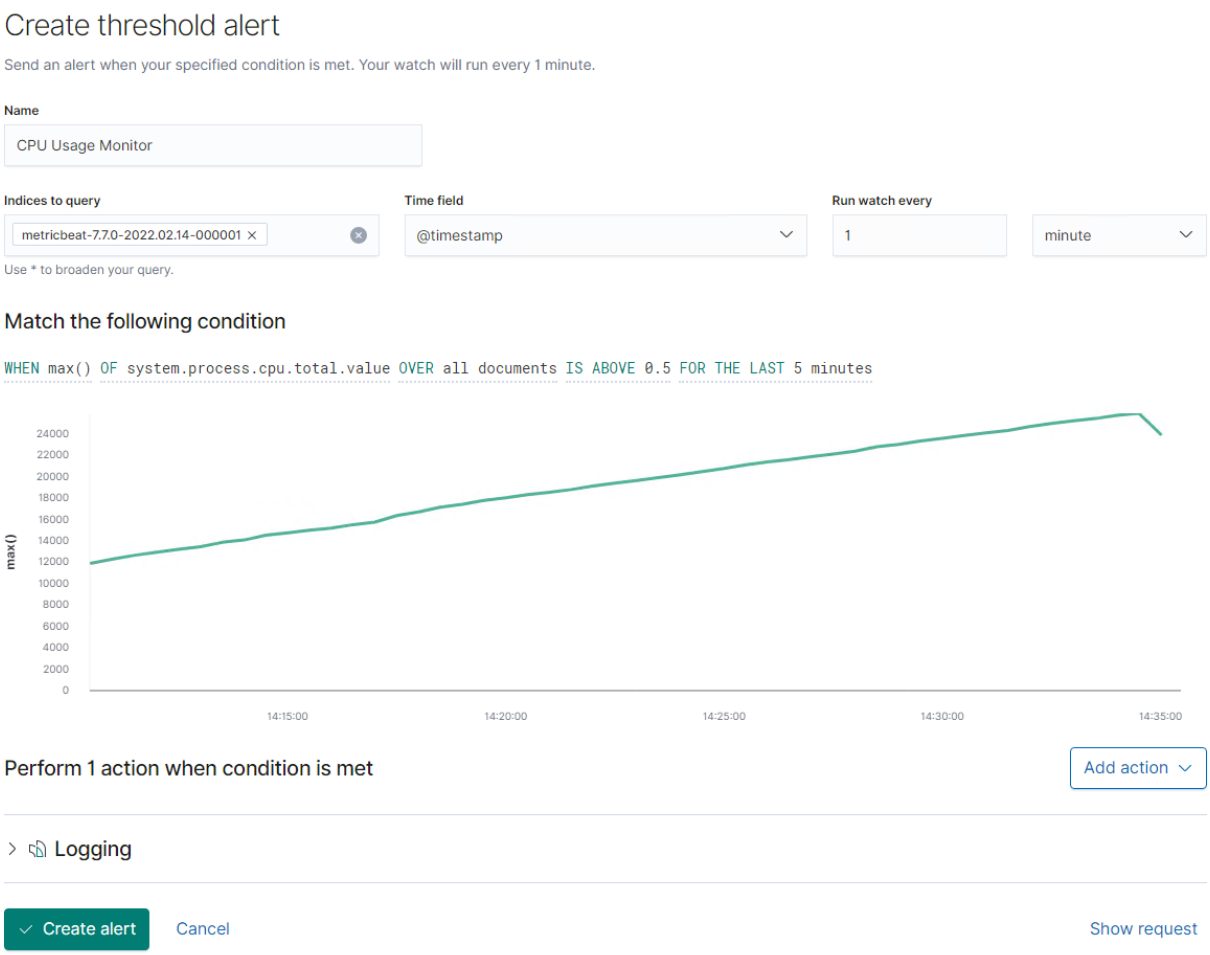
- **Metric**: Packetbeat: http.response.status_code > 400
- **Threshold**: grouped http response status codes above 400 every 5 minutes
    - When count() GROUPED OVER top5 ‘http.response.status_code’ is above 400 for the last 5 minutes
- **Vulnerability Mitigated**:
    - Intrusion detection/prevention for attacks
    - IPS should block any suspicious IP’s
    - Account management can be used to lock or request user accounts to change passwords every 60 days
    - Filter and subsequently disable or close port 22
- **Reliability**: This alert is not likely to create excessive amounts of false positives while identifying brute force attacks. Reliability is Medium



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**: CPU usage percentage is controlled. An alert is triggered if the CPU remains at or above 50% consistently for 5 minutes. This helps identify Virus or Malware
- **Reliability**: This can certainly generate a significant amount of false positives whenever the CPU has to increase usage past 50% during any processing. This, however, does have a High reliability



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**: Control over the number of http request sizes via a filter allows for further identification and subsequently protection against DDOS attacks.
- **Reliability**: This alert does not generate excessive false positives because DDOS attacks commonly submit requests across seconds and not typically across minutes. This is a medium reliability.

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-7.8.0-2022.02.14-000001 ×

Use * to broaden your query.

Time field

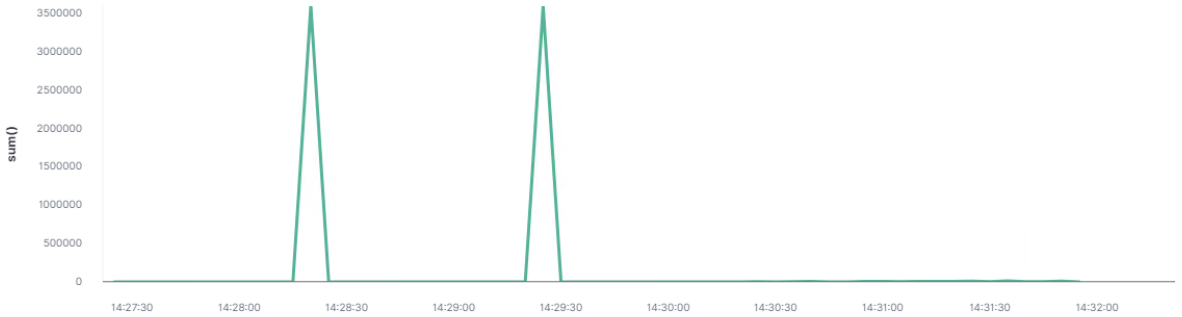
@timestamp

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

Add action

Logging

Create alert Cancel Show request