Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
  - **Operating System**:Linux
  - **Purpose**: Virtual Machine
  - **IP Address**:192.168.1.100

- Target 1
  - **Operating System**:Linux
  - **Purpose**: Apache Web Server
  - **IP Address**:192.168.1.110

Description of Targets

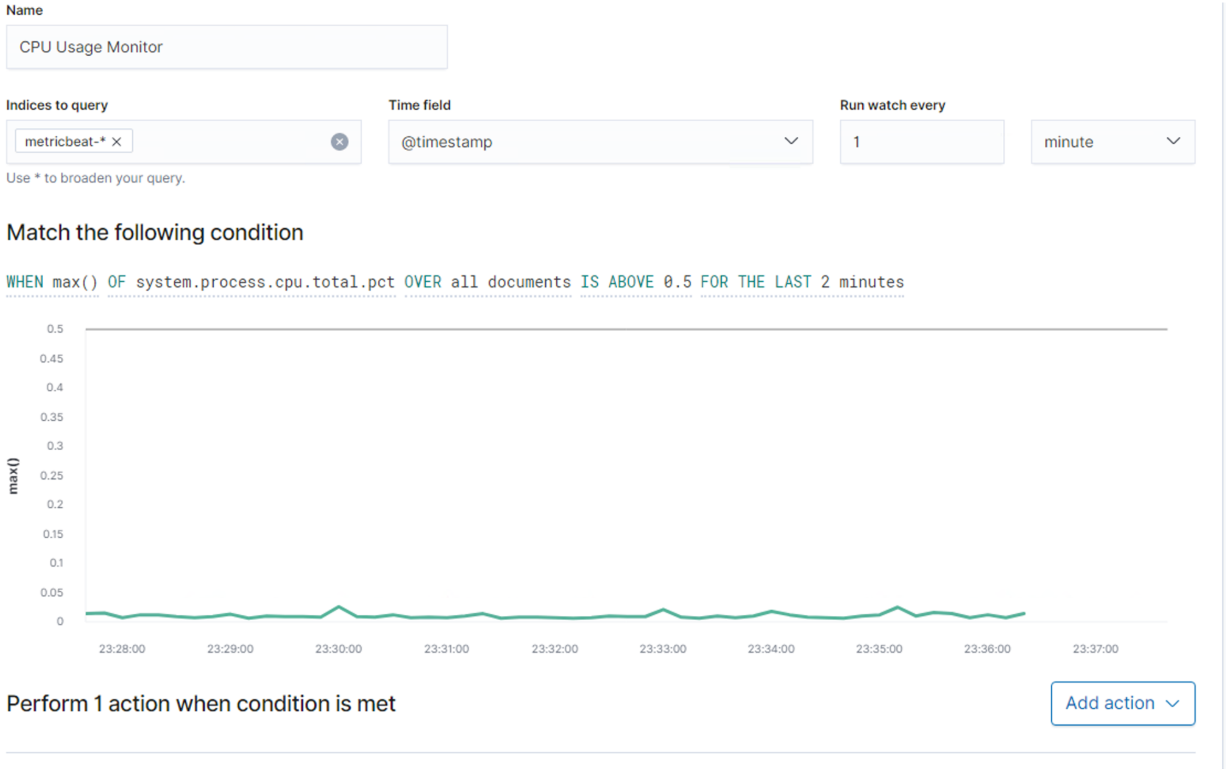
The target of this attack was: Target 1 Raven !92.168.1.110

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:

CPU Usage



Name

CPU Usage Monitor

Indices to query

metricbeat-*

Use * to broaden your query.

Time field

@timestamp

Run watch every

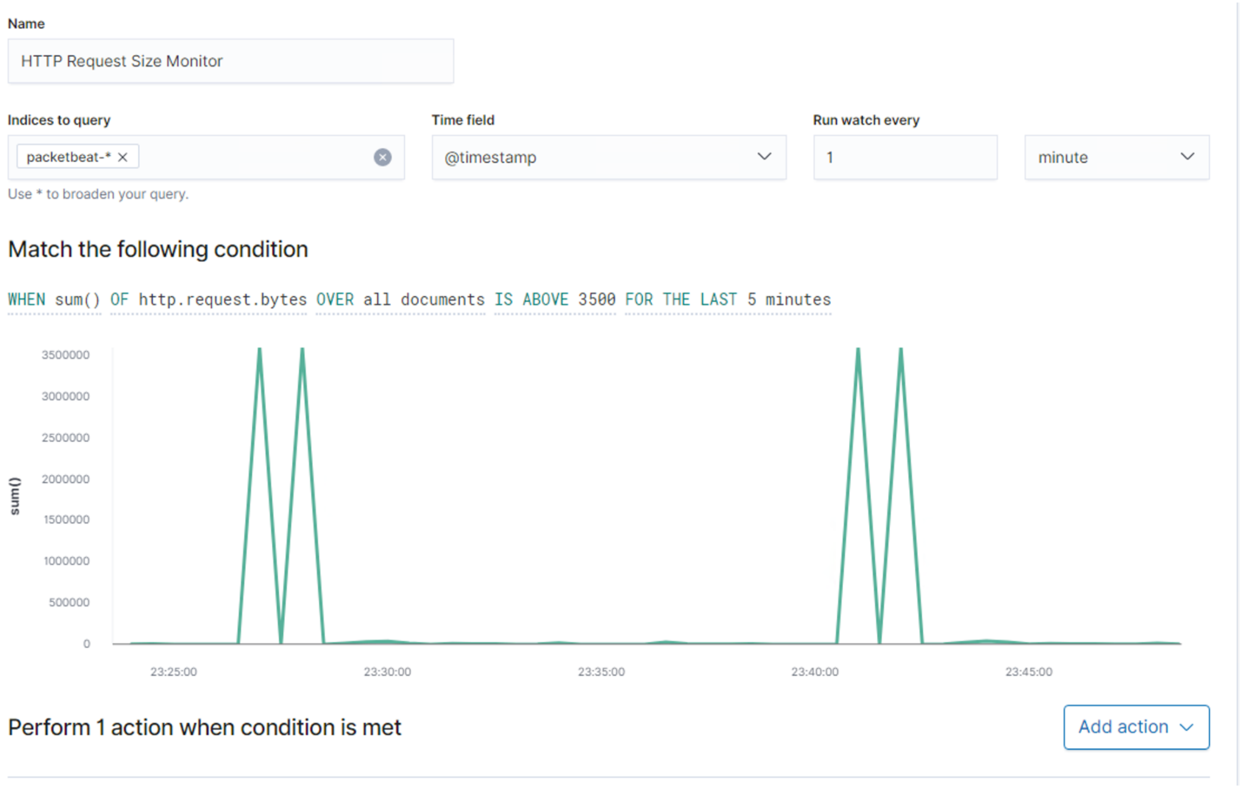
1 minute

Match the following condition

```
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 2 minutes
```

Perform 1 action when condition is met

HTTP Request Size Monitor



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

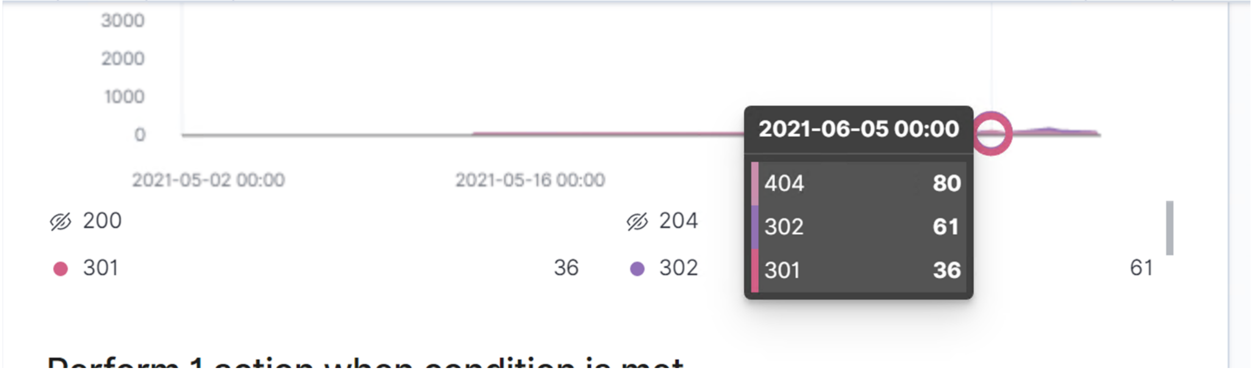
```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 5 minutes
```

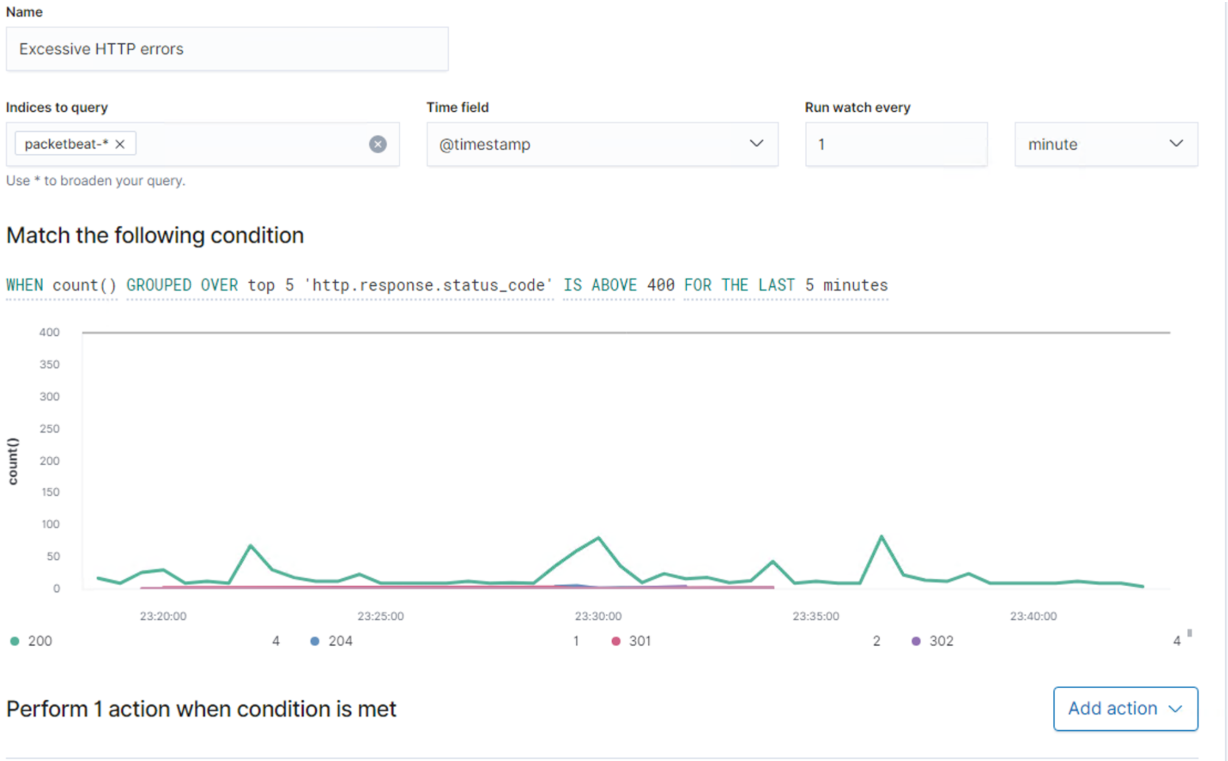
Perform 1 action when condition is met

Metric: packetbeat

- **Threshold**: 3500
- **Vulnerability Mitigated**: Denial of service. Downtime servers
- **Reliability**: high

HTTP Excessive Errors





Name

Excessive 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
```

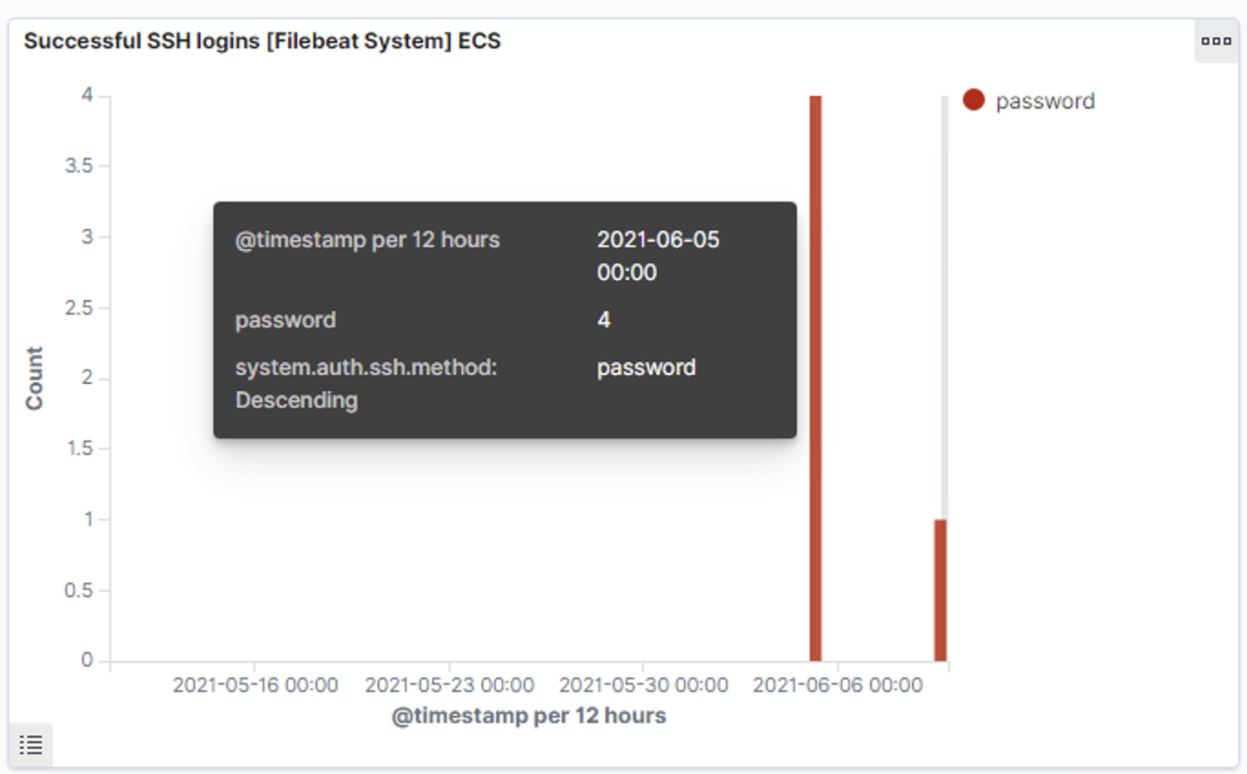
Perform 1 action when condition is met

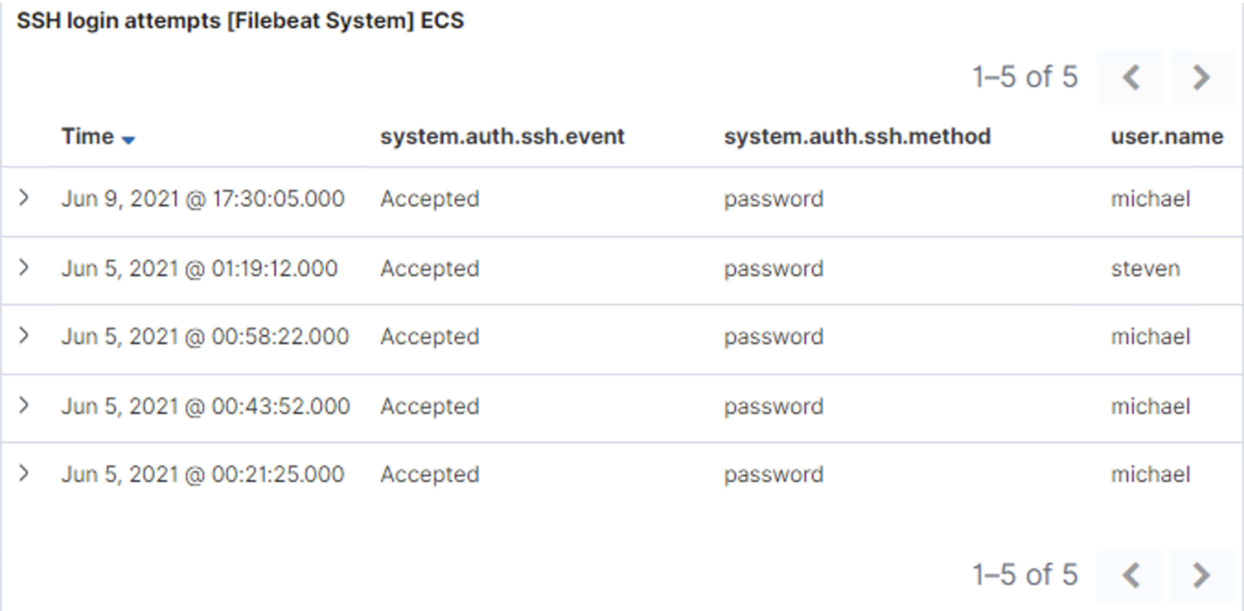
Metric: packetbeat

- **Threshold**: over 5
- **Vulnerability Mitigated**: error will show high count.
- **Reliability**: high

We had 80 eros indicating a brute force attack.

SSH Successful login attempts




SSH login attempts [Filebeat System] ECS

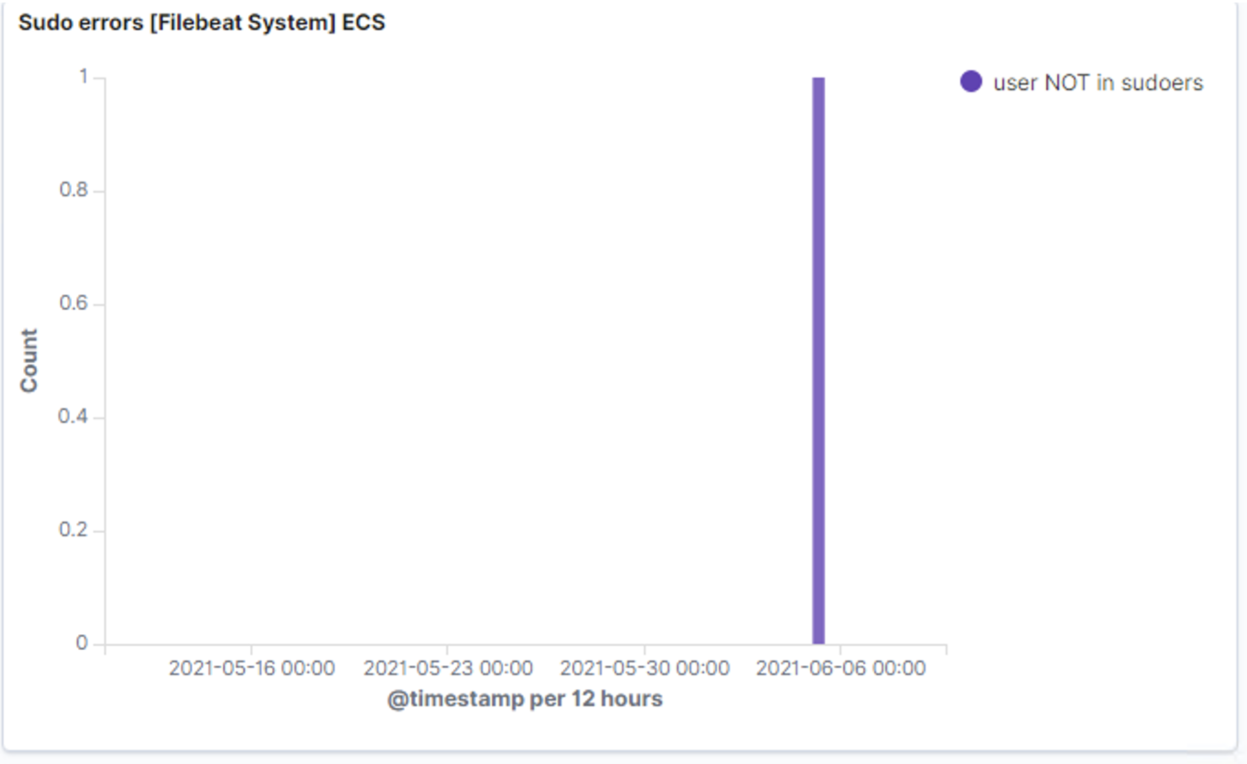
1–5 of 5

Time	system.auth.ssh.event	system.auth.ssh.method	user.name
Jun 9, 2021 @ 17:30:05.000	Accepted	password	michael
Jun 5, 2021 @ 01:19:12.000	Accepted	password	steven
Jun 5, 2021 @ 00:58:22.000	Accepted	password	michael
Jun 5, 2021 @ 00:43:52.000	Accepted	password	michael
Jun 5, 2021 @ 00:21:25.000	Accepted	password	michael

1–5 of 5

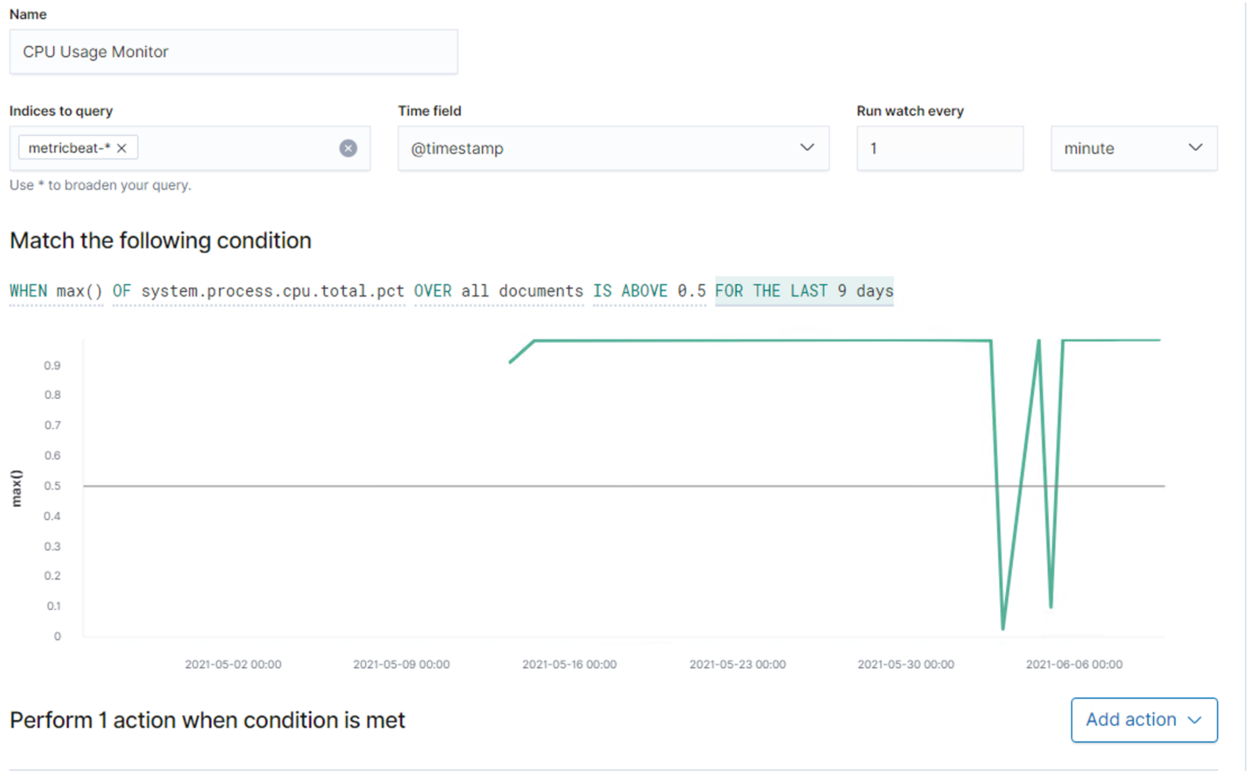
- **Metric**:
- **Threshold**: more than 1
- **Vulnerability Mitigated**: multiple login access
- **Reliability**: high reliability

Name of Alert 2 Sudo Command Errors



- **Metric**: filebeat
- **Threshold**: more than 1
- **Vulnerability Mitigated**: Unauthorized user
- **Reliability**: high

Alert - CPU Usage



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 9 days
```

Perform 1 action when condition is met

- **Metric**: packetbeat
- **Threshold**: over .5
- **Vulnerability Mitigated**:
- **Reliability**: high

Suggestions for Going Further

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

- Vulnerability 1 ssh login
    - **Patch**: Disable port 22 or ssh. Edit the configuration files to only allow root users to ssh.
    - **Why It Works**: It will prevent non root users from ssh into their servers.
- Vulnerability 2 Accessible files/ Privileges

    - **Patch**: change permissions
    - **Why It Works**: disables changing files, and executing such pythons
- Vulnerability
    - **Patch**: hide information better, encrypt it. Make stronger passwords. Update and fix developer bugs.
    - **Why It Works**: it'll reduce brute force attempts. Attackers will have a harder time.