Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
  - **Operating System**: Kali GNU/Linux Rolling
  - **Purpose**: Attack machine
  - **IP Address**: 192.168.1.90
- Target 1
  - **Operating System**: Debian GNU/Linux 8
  - **Purpose**: Target VM that has a vulnerable WordPress server exposed and sends logs to ELK
  - **IP Address**: 192.168.1.110
- ELK
  - **Operating System**: Ubuntu 18.0.4
  - **Purpose**: Access via web to view alerts
  - **IP Address**: 192.168.1.100
- Capstone
  - **Operating System**: Ubuntu 18.04.4
  - **Purpose**: Alert testing / attack target
  - **IP Address**: 192.168.1.105

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:

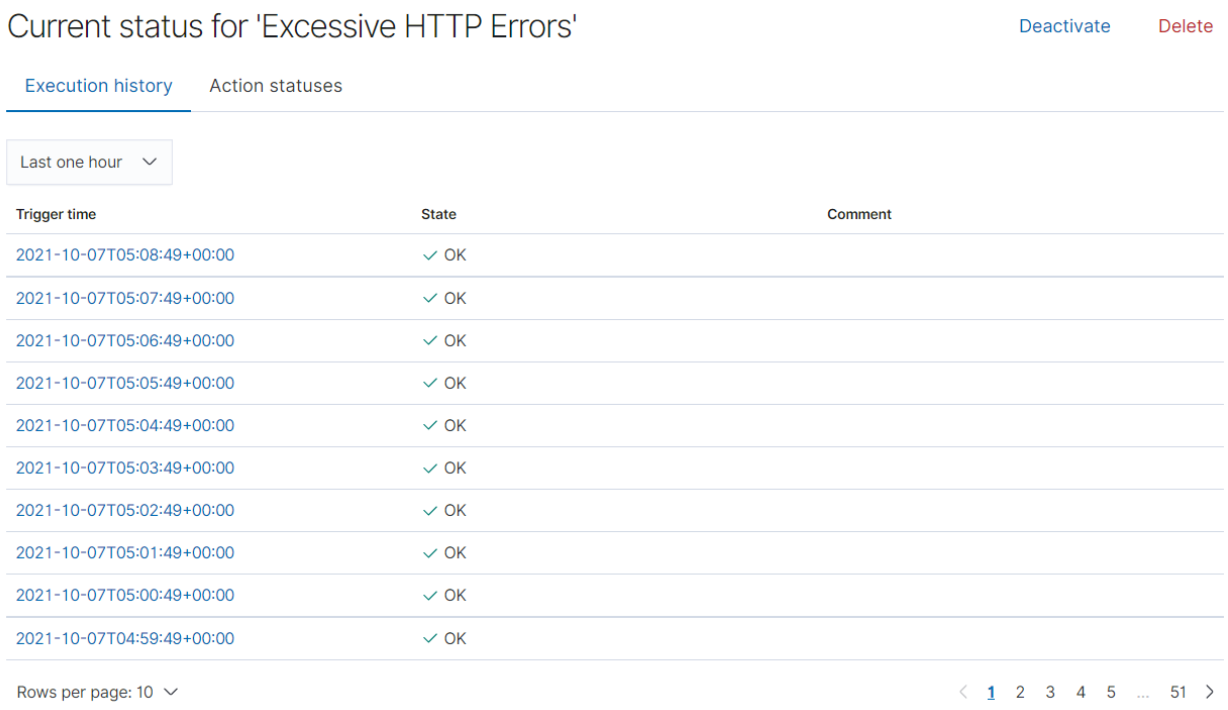
Monitoring the Targets

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

Alert 1: Excessive HTTP Errors

Alert 1 is implemented as follows:

- **Metric**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold**: IS ABOVE 400
- **Vulnerability Mitigated**: Overload of requests from possible DDoS attacks
- **Reliability**:
    - **Does this alert generate lots of false positives/false negatives?** This alert has a threshold set to “is above 400.” This threshold provides sufficient space to avoid alert fatigue and notify only when HTTP errors are above 400.
    - **Rate as low, medium, or high reliability:** This alert is highly reliable. The threshold will only alert for above normal amounts of HTTP errors and indicate that we should investigate.

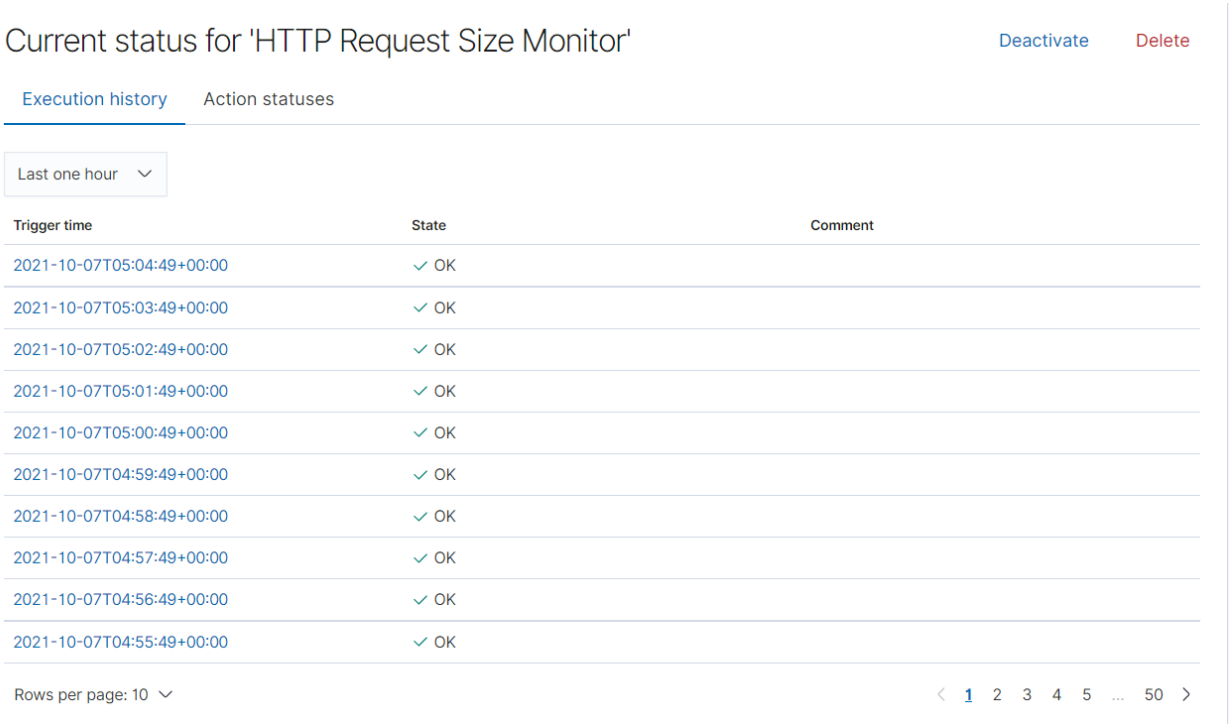


Alert 2: HTTP Request Size Monitor

Alert 2 is implemented as follows:

- **Metric**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

- **Threshold**: IS ABOVE 3500
- **Vulnerability Mitigated**: HTTP request smuggling
- **Reliability**:
    - **Does this alert generate lots of false positives/false negatives?** This alert has a threshold set to “is above 3500.” This threshold provides sufficient space to avoid alert fatigue and notify only when HTTP request size exceeds 3500.
    - **Rate as low, medium, or high reliability:** This alert is highly reliable. The threshold will only alert for above normal amounts of HTTP requests and indicate that we should investigate in order to avoid DOS.



Alert 3: CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Threshold**: IS ABOVE 0.5
- **Vulnerability Mitigated**: system crash
- **Reliability**:
    - **Does this alert generate lots of false positives/false negatives?** This alert has a threshold set to “is above 0.5.” This threshold provides sufficient space to avoid alert fatigue and notify only when CPU usage is above 0.5.
    - **Rate as low, medium, or high reliability:** This alert is highly reliable. The threshold will only alert for above normal amounts of CPU usage and indicate that we should investigate in order to avoid system crash. When a system

crashes, there is a core dump of its internal state and if the core-dump is not secured, then unauthorized users could access it.