# Blue Team: Summary of Operations

## Table of Contents

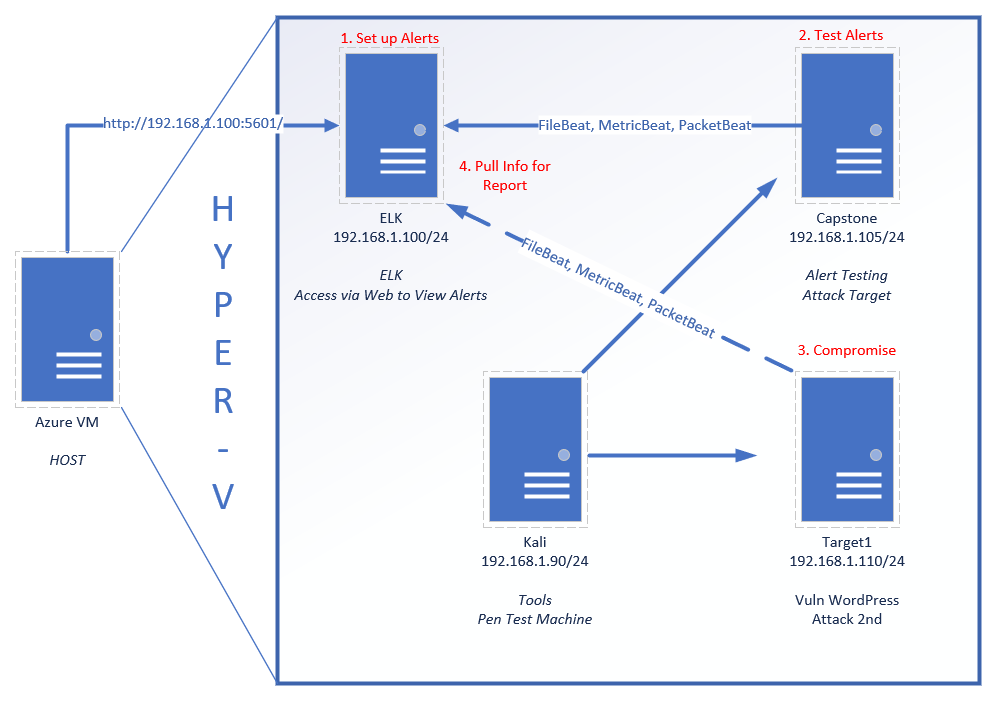
* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic and Behavior
* Suggestions for Going Further

## Network Topology

The following machines were identified on the network:

**[Target 1 - ravel.local]**

* Operating System: Windows 6.1
* Purpose: Webserver for Raven Security website
* IP Address: 192.168.1.110



## Description of Targets

Fill in the following:

* Two VMs on the network were vulnerable to attack:
  + Target 1 [192.168.1.110]
  + Target 2 [192.168.1.115]
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

## Monitoring the Targets

This scan identifies the services below as potential points of entry:

**Target 1**

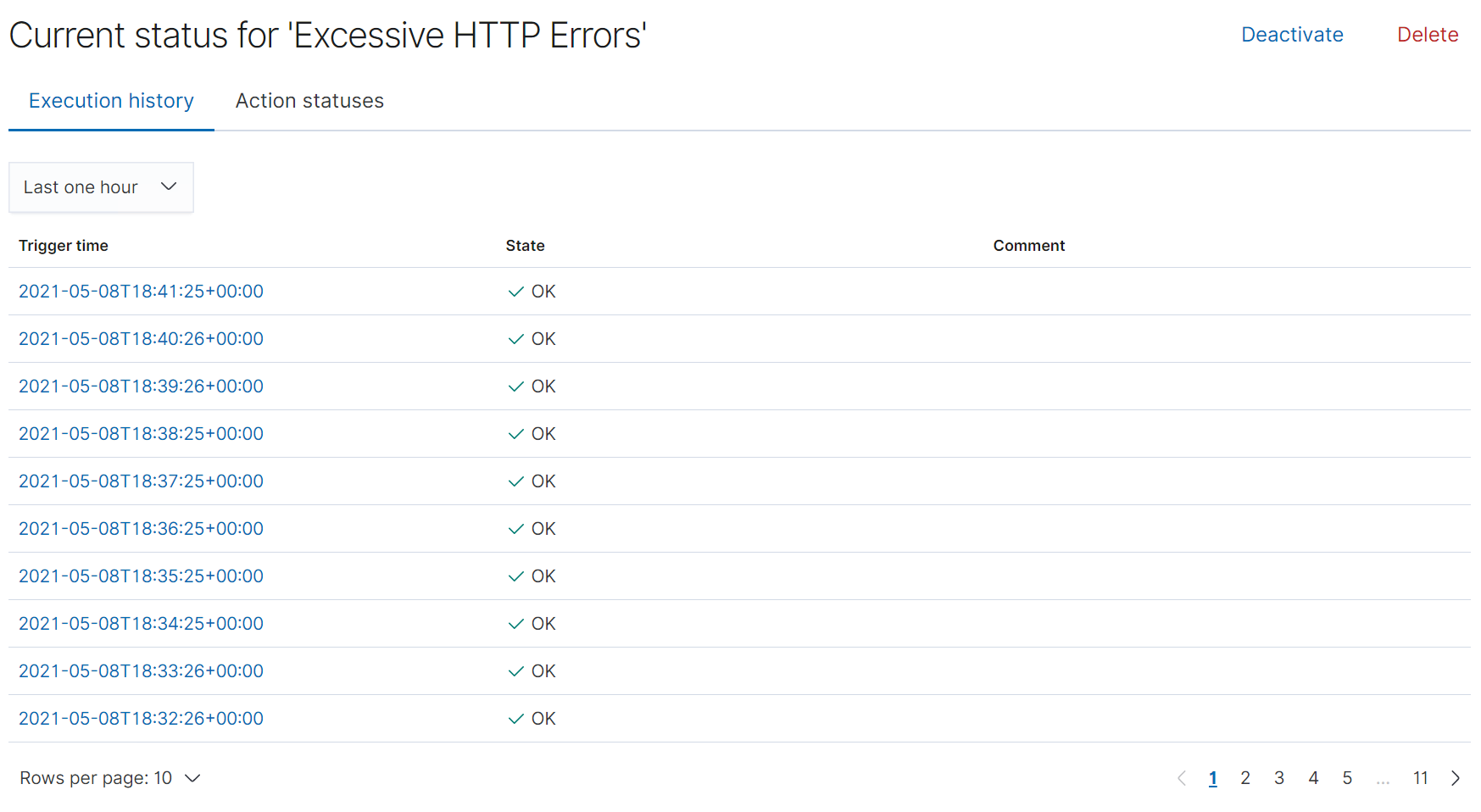
1. Rpcbind | Port 111
2. Netbios-ssn | Port 139
3. Microsoft-ds | Port 445

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below: (Note: Add at least three alerts. You can add more if time allows.)

**Excessive HTTP Errors**

Excessive HTTP Errors is implemented as follows:

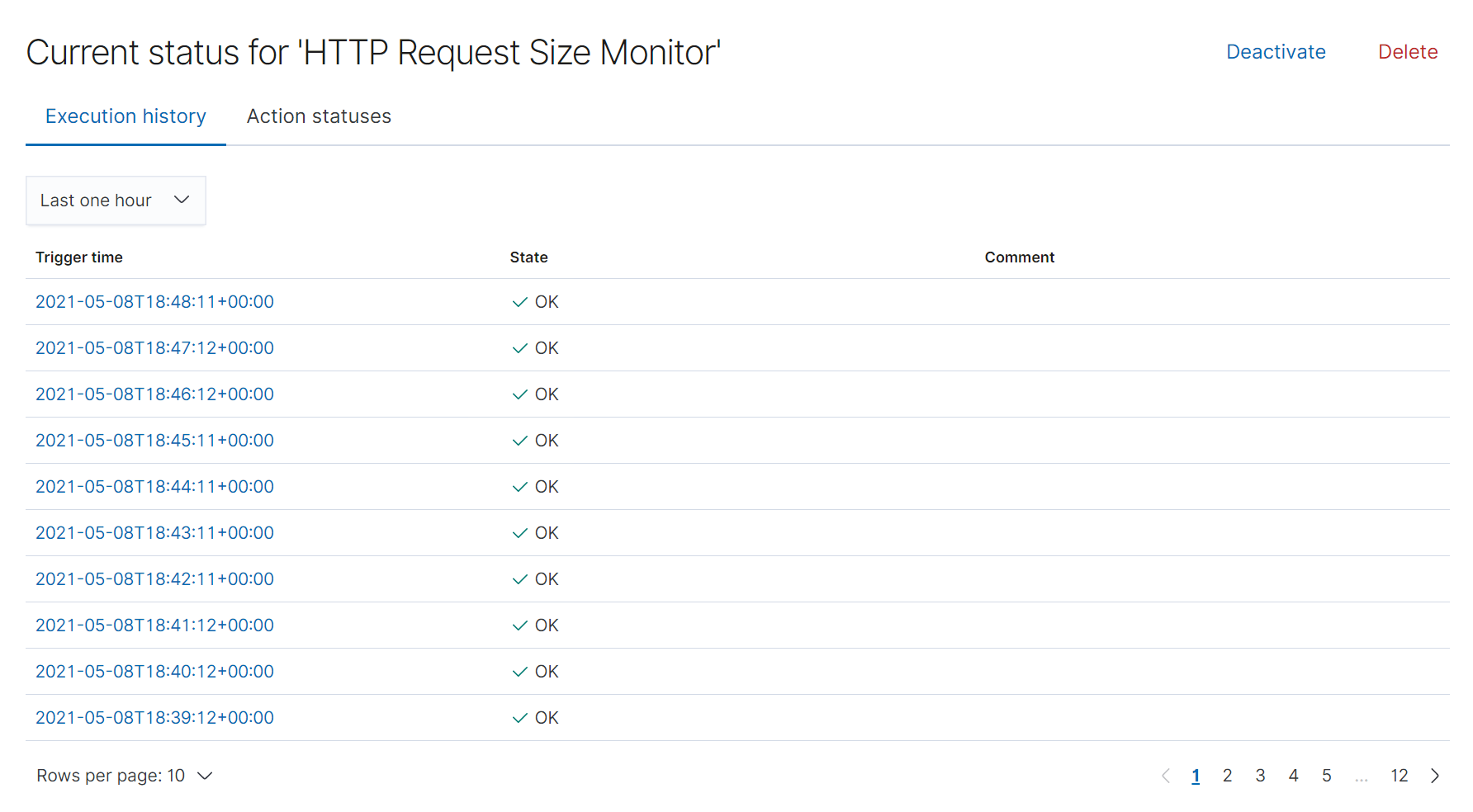
* Metric: Filebeat
* Threshold: WHEN count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes
* Vulnerability Mitigated: Brute Force Attacks
* Reliability: High | 7/10, could produce false positives



**HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

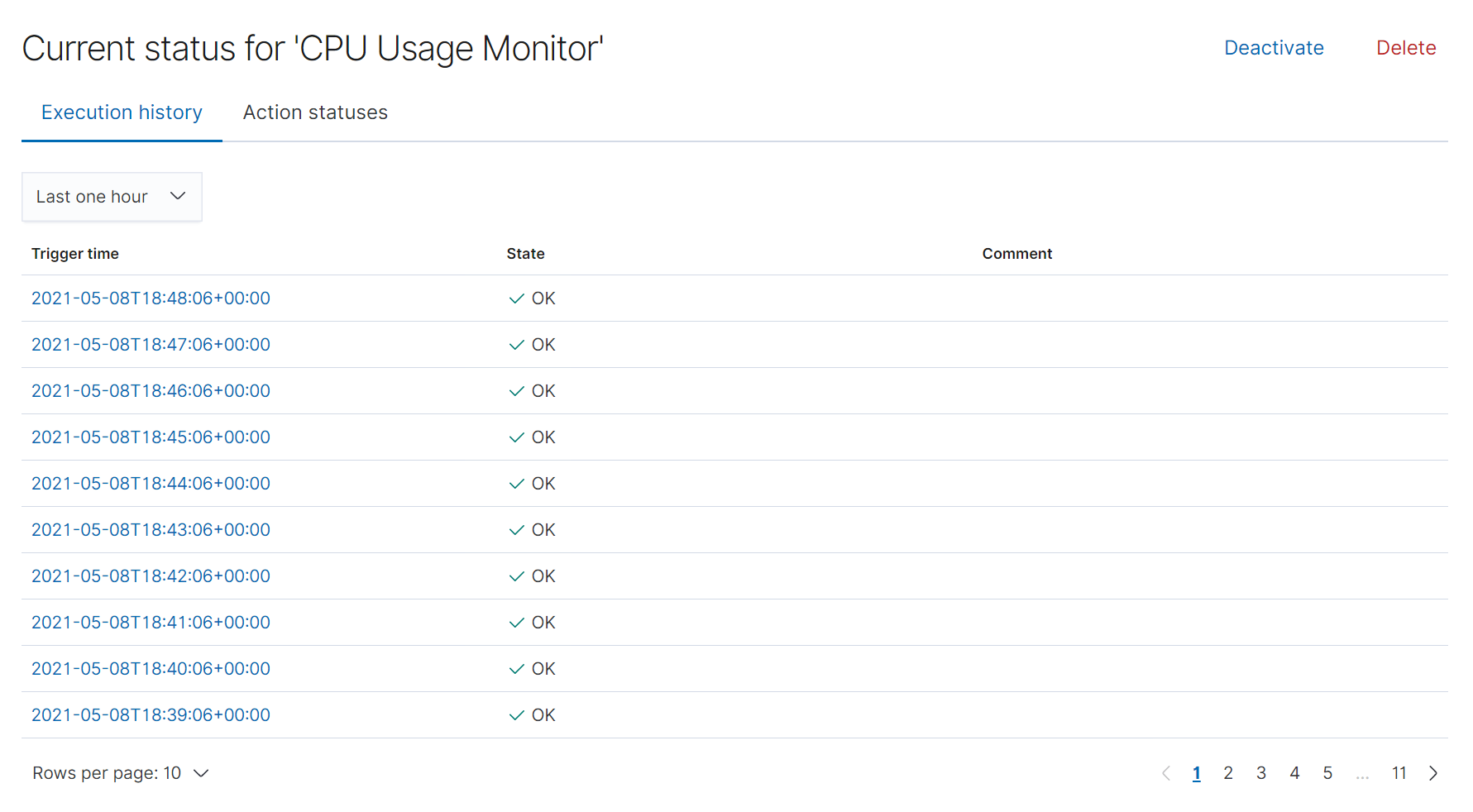
* Metric: FileBeat
* Threshold: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
* Vulnerability Mitigated: DDoS Attacks
* Reliability: High | 7/10, could produce false positives of users are requesting a lot of information.



**CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* Metric: MetricBeat
* Threshold: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
* Vulnerability Mitigated: Excessive CPU Usage
* Reliability: Medium | 5/10, the chance is greater that the CPU is just overload rather than an attack.



## 

## Suggestions for Going Further

**Suggest a patch for each vulnerability identified by the alerts above.** Remember: alerts only detect malicious behavior. They do not prevent it.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. 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 - Brute Force Attacks**

* Patch: Invalid Credentials Timeout /Lockout OR Limit activity/Whitelist to a specified IP address/range.
* Why It Works: It limits the number of attempts the attacker can commit. Only allows connections from trusted addresses.

**Vulnerability 2 - DOS Attacks**

* Patch: Install a Load Balancer.
* Why It Works: Distributes requests amongst a number of servers which lightens the traffic burden on each server.

**Vulnerability 3 - Excessive CPU Usage**

* Patch: Create different levels of alert for CPU Usage (ex. 25% / 50% / 75% / 90% / 100%).
* Why It Works: Different levels of alerts can help monitor CPU usage.