**Blue Team: Summary of Operations**

**Table of Contents**

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

**Network Topology**

The following machines were identified on the network:

Name of VM 1: Target 1

* Operating System: Linux
* Purpose: Check for vulnerabilities to exploit
* IP Address: 192.168.1.110

Name of VM 2: Target 2

* Operating System: Linux
* Purpose: Check for vulnerabilities to exploit
* IP Address: 192.168.1.115

**Description of Targets**

Two VMs on the network were vulnerable to attack: `Target 1` (192.168.1.110) and `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. 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 Errors**

Excessive HTTP Errors is implemented as follows:

* + Metric – http.response.status\_code
  + Threshold: Above 400 for the last 5 minutes
  + Vulnerability Mitigated: Brute force attacks or resource usage errors (bad logins)
  + Reliability: high reliability.

**HTTP Request Size Monitor**

HTTP Request Size Monitor is implemented as follows:

* + Metric: http.request.bytes
  + Threshold: above 3500 for the last 1 minute
  + Vulnerability Mitigated: Denial of Service Attacks or latency
  + Reliability: High reliability.

**CPU Usage Monitor**

CPU Usage Monitor is implemented as follows:

* + Metric: system.process.cpu.total.pct
  + Threshold: OVER all documents IS ABOVE 0.5 for the last 5 minutes
  + Vulnerability Mitigated: Resource management
  + Reliability: medium reliability.

**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. (I.E., 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: Brute Force or Invalid Login Attempts**

* + Patch: Invalid credentials or lockouts; whitelist or blacklist IP address ranges.
  + Why It Works:

**Vulnerability 2: Denial of Service or latency**

* + Patch: Implement a load balancer
  + Why It Works: Helps redirect traffic if a specific server is experiencing a large volume of traffic.

**Vulnerability 3: Resource Management**

* + Patch: Set levels of CPU usage alerts for high, medium
  + Why It Works: alerts will help to manage CPU usage and gives a heads up to address issues