**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:

* Captstone
  + **Operating System**: Linux
  + **Purpose**: a vulnerable target that will test alerts as it is being attacked. Filebeat and Metricbeat are installed and will forward logs to the ELK machine.
  + **IP Address**: 192.168.1.105
* ELK
  + **Operating System**: Linux
  + **Purpose**: logs are forwarded from Capstone and holds the Kibana dashboards.
  + **IP Address**: 192.168.1.100
* Kali
  + **Operating System**: Linux
  + **Purpose**: used for penetration testing.
  + **IP Address**: 192.168.1.90
* Target 1
  + **Operating System**: Linux
  + **Purpose**: exposes a vulnerable Wordpress server.
  + **IP Address**: 192.168.1.110

**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:

* Excessive HTTP Errors
* HTTP Request Size Monitor
* CPU Usage Monitor

**Monitoring the Targets**

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

**Excessive HTTP Errors**

WHEN count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400  
FOR THE LAST 5 minutes

Alert 1 is implemented as follows:

* **Metric**: HTTP status code
* **Threshold**: above 400 for the last 5 minutes
* **Vulnerability Mitigated**: Client error responses, including unauthorized access.
* **Reliability**: If traffic baseline is low, high reliability. If the traffic baseline is high, low reliability.

**HTTP Request Size Monitor**

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

Alert 2 is implemented as follows:

* **Metric**: HTTP range request
* **Threshold**: all documents above 3500 for the last 1 minute
* **Vulnerability Mitigated**: Partial content requests.
* **Reliability**: Low reliability, too much information to be conclusive.

**CPU Usage Monitor**

WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

Alert 3 is implemented as follows:

* **Metric**: Percentage of CPU time spent by the process since the last update.
* **Threshold**: above 0.5 for the last 5 minutes
* **Vulnerability Mitigated**: It helps mitigate CPU usage over 50% for an extended period  
  of time.
* **Reliability**: Medium reliability, depends on flow of traffic.

**Suggestions for Going Further**

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:

* OpenSSH
  + **Patch**: Rather than a patch, implement a password policy that is stronger. One of the most common ways a hacker can break into computers is to guess a password. The user must be educated to create passwords that are NOT simple or commonly used.
  + **Why It Works**: Access was gained onto the vulnerable web server by simply “guessing” the password. By implementing a stronger password policy, hackers will not be able to gain access so easily.
* rpcbind
  + **Patch**: Remove the service. If the service is really needed, apply access limitation to port 111 on a firewall.
  + **Why It Works**: Removing the service would remove the vulnerability so it could not be exploited.
* NetBIOS
  + **Patch**: It is suggested that NetBIOS is bad and should be killed. But there are some patches that Microsoft has issued. Specifically, one for NetBIOS Name Server Protocol Spoofing.
  + **Why It Works**: It works on Windows NT or Windows 2000 computers to ignore spoofed name conflict datagrams.