

# Blue Team: Summary of Operations

## Table of Contents

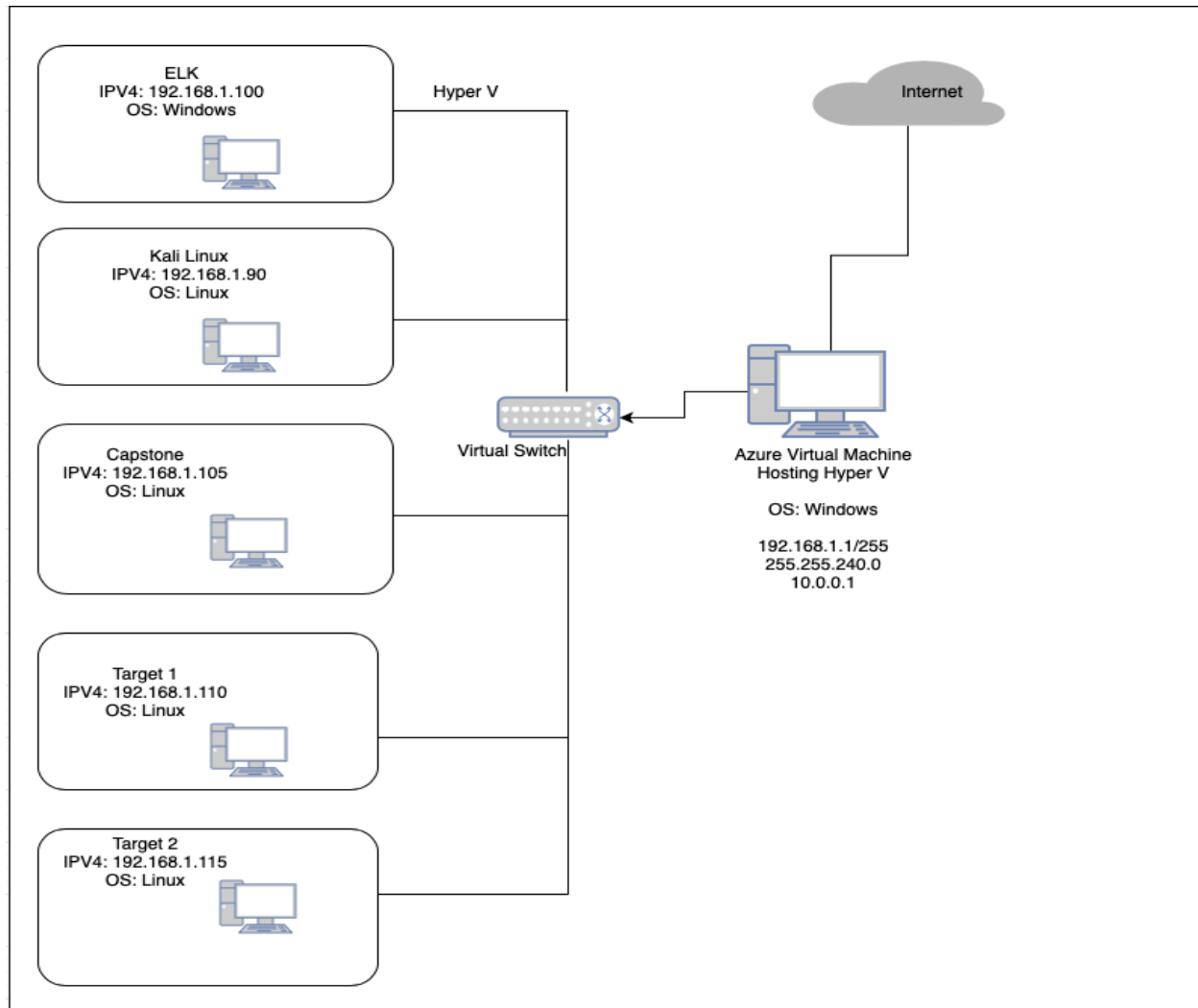
- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior
- Suggestions for Going Further

## Network Topology

The following machines were identified on the network:

- Name of VM 1- Capstone
  - o **Operating System:**Linux
  - o **Purpose:** Filebeat and Metricbeat are installed and will forward logs to the ELK machine. This VM is in the network solely for the purpose of testing alerts.
  - o **IP Address:** **Capstone:** 192.168.1.105
- Name of VM - ELK
  - o **Operating System:**Windows
  - o **Purpose:** It holds the Kibana dashboards
  - o **IP Address:** **ELK:** 192.168.1.100
- Name of VM 3- Kali
  - o **Operating System:**Linux
  - o **Purpose:** A standard Kali Linux machine used in the penetration test
  - o **IP Address:** **Kali:** 192.168.1.90
- Name of VM 4- Target 1
  - o **Operating System:** Linux
  - o **Purpose:** Exposes a vulnerable WordPress server. Sends logs to ELK
  - o **IP Address:** **Target 1:** 192.168.1.110

Including a Gliffy or draw.io diagram is optional but highly encouraged.



## Description of Targets

The target of this attack was: **Target 1** - IP: 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:

- 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:

**Name of Alert 1- Excessive HTTP Errors** - HTTP response error status code (this alert is detecting excessive amount of HTTP errors)

The Excessive HTTP Errors Alert is implemented as follows: packetbeat  
WHEN count() GROUPED OVER top 5 'http.response.status\_code' IS ABOVE 400 FOR THE LAST 5 minutes

- **Metric:** HTTP Errors
  - **Threshold:** 400+ HTTP errors within 5 minutes
  - **Vulnerability Mitigated:** Brute Force Attacks. Resource Usage Issues.
  - **Reliability:** High reliability.
- The alert for **Excessive HTTP Errors** was set up for a threshold of 400 errors over the last 5 minutes. Based on the results found, the reliability of the alert is valid as the alert was triggered which is shown below:

```

{
  "messages": {
    "metadata": {
      "name": "Excessive HTTP Errors",
      "watcherui": {
        "agg_type": "count",
        "index": "packetbeat-*",
        "term_field": "http.response.status_code",
        "term_size": 5,
        "threshold": 400,
        "threshold_comparator": ">",
        "time_field": "@timestamp",
        "time_window_size": 5,
        "time_window_unit": "m",
        "trigger_interval_size": 1
      }
    }
  }
}
```

metadata.watcherui.threshold_comparator	>
metadata.watcherui.time_field	@timestamp
metadata.watcherui.time_window_size	5
metadata.watcherui.time_window_unit	m
metadata.watcherui.trigger_interval_size	1
metadata.watcherui.trigger_interval_unit	m
metadata.xpack.type	threshold
node	mkfRONI8Teu-NE4WaojMQ
result.actions	{       "id": "logging_1",       "type": "logging",       "status": "success",       "logging": {         "logged_text": "Watch [Excessive HTTP Errors] has exceeded the threshold of above 400 status codes in last 5 minutes"       }     }
result.condition.met	true
result.condition.status	success
result.condition.type	script
result.execution_duration	16
result.execution_time	Jun 3, 2021 @ 02:59:40.998
result.input.payload._shards.failed	0
result.input.payload._shards.skipped	0
result.input.payload._shards.successful	2
result.input.payload._shards.total	2
result.input.payload.aggregations.bucketAgg.buckets	{       "doc_count": 205697,       "key": 404     },     {       "doc_count": 82,       "key": 200     }   }

**Name of Alert 2 - HTTP Request Size Monitor** - Total size in bytes of the request (body and headers).

The HTTP Request Size Monitor Alert is implemented as follows:

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

- **Metric:** HTTP Request Size
- **Threshold:** 3500+bytes within 1 minute
- **Vulnerability Mitigated:** DOS (Denial of Service) Attacks
- **Reliability:** High Reliability
- The alert for **HTTP Request Size Monitor** was set up for a threshold above 3500 bytes for 1 minute. Based on the results found, the alert was not triggered based on threshold parameters. In the near future, we will review these threshold parameters for possible false positives or negatives.

⌘ metadata.name	HTTP Request Size Monitor
⌘ metadata.watcherui.agg_field	http.request.bytes
⌘ metadata.watcherui.agg_type	sum
⌘ metadata.watcherui.index	metricbeat-*
# metadata.watcherui.term_size	5
# metadata.watcherui.threshold	3,500
⌘ metadata.watcherui.threshold_comparator	>
⌘ metadata.watcherui.time_field	@timestamp
# metadata.watcherui.time_window_size	60
⌘ metadata.watcherui.time_window_unit	s
# metadata.watcherui.trigger_interval_size	1
⌘ metadata.watcherui.trigger_interval_unit	m
⌘ metadata.xpack.type	threshold
⌘ node	mkfRONI8Teu-NE4WaaojMQ
[-] result.actions	⚠
🕒 result.condition.met	false
⌘ result.condition.status	success
⌘ result.condition.type	script
# result.execution_duration	1
📅 result.execution_time	Jun 3, 2021 @ 02:59:23.459
🕒 result.input.payload._shards.failed	⚠ 0
🕒 result.input.payload._shards.skipped	⚠ 0
🕒 result.input.payload._shards.successful	⚠ 1
🕒 result.input.payload._shards.total	⚠ 1
🕒 result.input.payload.aggregations.metricAgg.value	⚠ 0
🕒 result.input.payload.hits.hits	⚠

① result.input.payload.hits.hits	⚠
① result.input.payload.hits.max_score	⚠ -
① result.input.payload.hits.total	⚠ 266
① result.input.payload.timed_out	⚠ false
① result.input.payload.took	⚠ 1
① result.input.search.request.body.aggs.metricAgg.sum.field	⚠ http.request.bytes
① result.input.search.request.body.query.bool.filter.range.@timestamp.format	⚠ strict_date_optional_time  epoch_millis
① result.input.search.request.body.query.bool.filter.range.@timestamp.gte	⚠ 2021-06-03T02:59:23.207Z  -60s
① result.input.search.request.body.query.bool.filter.range.@timestamp.lte	⚠ 2021-06-03T02:59:23.207Z
① result.input.search.request.body.size	⚠ 0
† result.input.search.request.indices	metricbeat-*
① result.input.search.request.rest_total_hits_as_int	true
† result.input.search.request.search_type	query_then_fetch
† result.input.status	success
† result.input.type	search
† state	execution_not_needed
① status.actions.logging_1.ack.state	⚠ awaits_successful_execution
① status.actions.logging_1.ack.timestamp	⚠ 2021-06-03T00:00:21.650Z
① status.execution_state	⚠ execution_not_needed
① status.last_checked	⚠ 2021-06-03T02:59:23.459Z
① status.state.active	⚠ true
① status.state.timestamp	⚠ 2021-06-03T00:00:21.650Z
① status.version	⚠ -1

### Name of Alert 3 - CPU Usage Monitor

The CPU Usage Monitor Alert is implemented as follows:

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

- **Metric:** CPU Usage
- **Threshold:** Above 0.5 CPUs within 5 minutes
- **Vulnerability Mitigated:** DDoS (Denial of Service) Attacks
- **Reliability:** High Reliability
- The alert for **CPU Usage Monitor Alert** was set up for a threshold above 0.5 CPUs for 5 minutes. Based on the results found, the alert was not triggered based on threshold parameters. In the near future, we will review these threshold parameters for possible false positives or negatives.

<code>t metadata.name</code>	CPU Usage Monitor
<code>t metadata.watcherui.agg_field</code>	system.process.cpu.total.pct
<code>t metadata.watcherui.agg_type</code>	max
<code>t metadata.watcherui.index</code>	metricbeat-*
<code># metadata.watcherui.term_size</code>	5
<code># metadata.watcherui.threshold</code>	0.5
<code>t metadata.watcherui.threshold_comparator</code>	>
<code>t metadata.watcherui.time_field</code>	@timestamp
<code># metadata.watcherui.time_window_size</code>	2
<code>t metadata.watcherui.time_window_unit</code>	m
<code># metadata.watcherui.trigger_interval_size</code>	1
<code>t metadata.watcherui.trigger_interval_unit</code>	m
<code>t metadata.xpack.type</code>	threshold
<code>t node</code>	mkfRONI8Teu-NE4WaojMQ
<code>[~] result.actions</code>	⚠
<code>🔍 result.condition.met</code>	false
<code>t result.condition.status</code>	success
<code>t result.condition.type</code>	script
<code># result.execution_duration</code>	1
<code>📅 result.execution_time</code>	Jun 3, 2021 @ 02:59:22.456
<code>🔍 result.input.payload._shards.failed</code>	⚠ 0
<code>🔍 result.input.payload._shards.skipped</code>	⚠ 0
<code>🔍 result.input.payload._shards.successful</code>	⚠ 1
<code>🔍 result.input.payload._shards.total</code>	⚠ 1
<code>🔍 result.input.payload.aggregations.metricAgg.value</code>	⚠ 0.247
<code>🔍 result.input.payload.hits.hits</code>	⚠
<code>🔍 result.input.payload.hits.max_score</code>	⚠ -

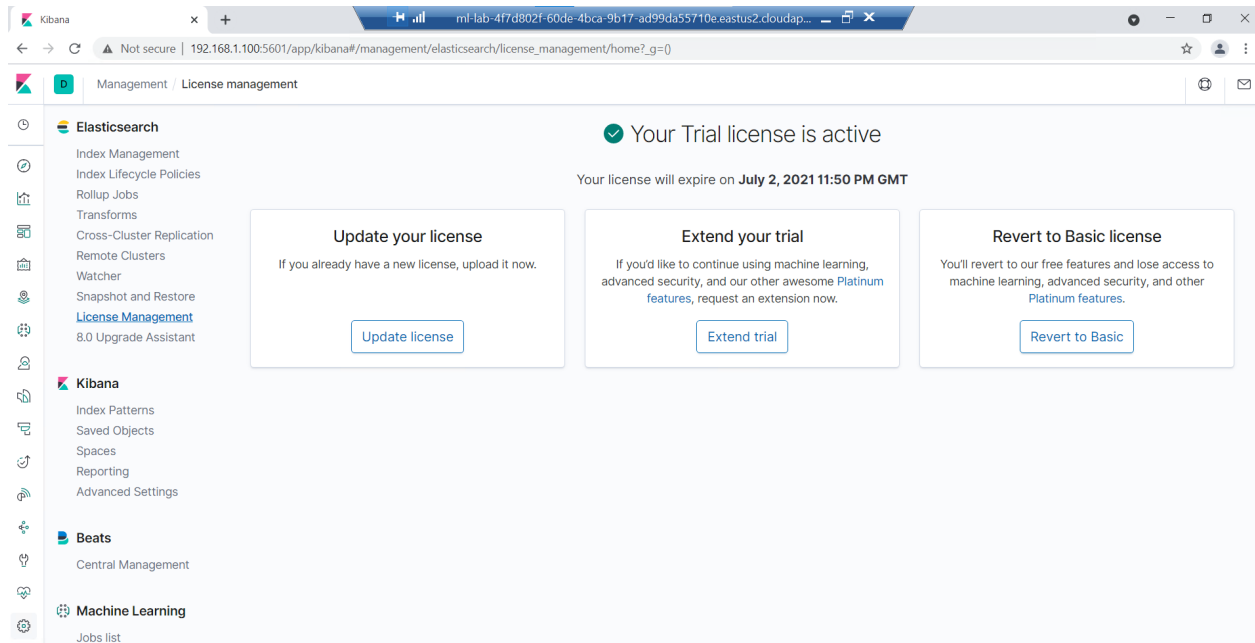
② result.input.payload.hits.max_score	⚠ -
② result.input.payload.hits.total	⚠ 583
② result.input.payload.timed_out	⚠ false
② result.input.payload.took	⚠ 1
② result.input.search.request.body.aggs.metricAgg.max.field	⚠ system.process.cpu.total.pct
② result.input.search.request.body.query.bool.filter.range.@timestamp.format	⚠ strict_date_optional_time  epoch_millis
② result.input.search.request.body.query.bool.filter.range.@timestamp.gte	⚠ 2021-06-03T02:59:22.343Z  -2m
② result.input.search.request.body.query.bool.filter.range.@timestamp.lte	⚠ 2021-06-03T02:59:22.343Z
② result.input.search.request.body.size	⚠ 0
† result.input.search.request.indices	metricbeat-*
④ result.input.search.request.rest_total_hits_as_int	true
† result.input.search.request.search_type	query_then_fetch
† result.input.status	success
† result.input.type	search
† state	execution_not_needed
② status.actions.logging_1.ack.state	⚠ awaits_successful_execution
② status.actions.logging_1.ack.timestamp	⚠ 2021-06-03T00:05:22.342Z
② status.execution_state	⚠ execution_not_needed
② status.last_checked	⚠ 2021-06-03T02:59:22.456Z
② status.state.active	⚠ true
② status.state.timestamp	⚠ 2021-06-03T00:05:22.342Z
② status.version	⚠ -1
📅 trigger_event.schedule.scheduled_time	Jun 3, 2021 @ 02:59:22.343
📅 trigger_event.triggered_time	Jun 3, 2021 @ 02:59:22.456
† trigger_event.type	schedule
† watch_id	c8979436-0a4d-47c8-87ec-18a3325dfae7

---

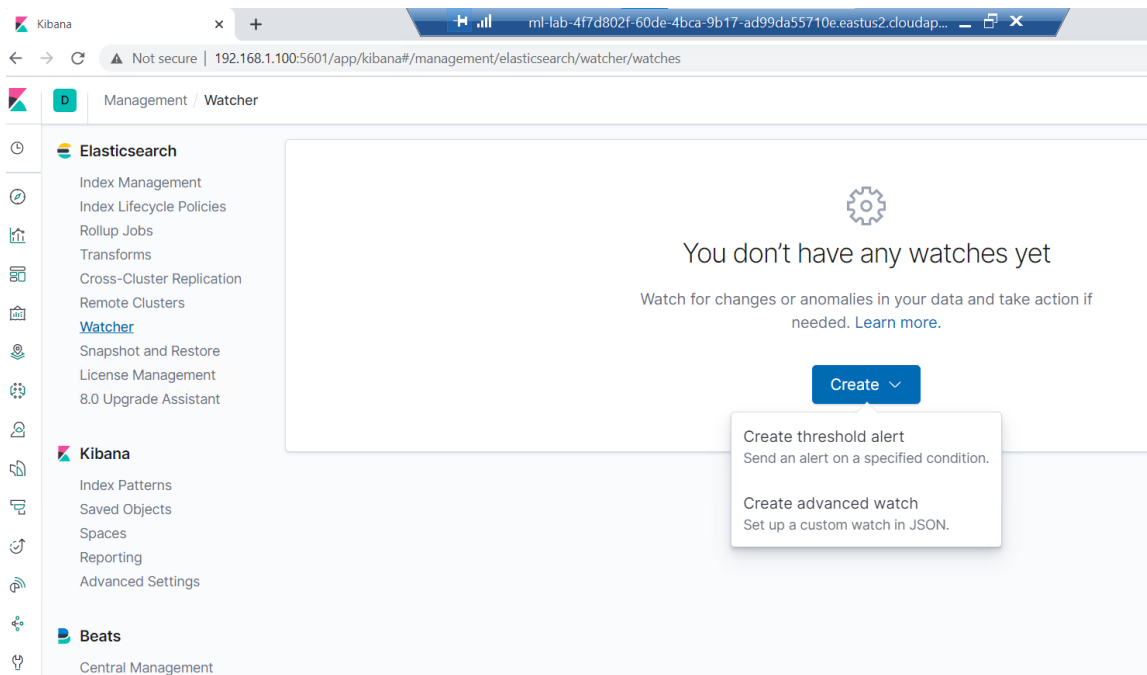


## Creating Alerts

- Create Free 30 Day Trial in Kibana



- Create a Threshold Alert:



## Excessive HTTP Errors Alert: packetbeat

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

### Edit Excessive HTTP Errors

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

Excessive HTTP Errors

Indices to query

packetbeat-\* ×

Time field

@timestamp ▼

Run watch every

1 ▼

minute ▼

Use \* to broaden your query.

#### 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 Add action ▼

☒ Logging

Log text

Watch [{{ctx.metadata.name}}] has exceeded the threshold of 400 in the last 5 minutes

## HTTP Request Size Monitor Alert: metricbeat

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

### Edit HTTP Request Size Monitor Over 3500

Send an alert when your specified condition is met. Your watch will run every 1 minute.

**Name**

HTTP Request Size Monitor Over 3500

**Indices to query**

metricbeat-\* X

**Time field**

@timestamp


**Run watch every**

1 minute

Use \* to broaden your query.

**Match the following condition**

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



**Perform 1 action when condition is met**

Add action

**Logging**

Log text

Watch [{{ctx.metadata.name}}] has exceeded the threshold of 3500 in the last 1 minute

## CPU Usage Monitor Alert: metricbeat

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

### Edit CPU Usage Monitor

Send an alert when your specified condition is met. Your watch will run every 1 minute.

**Name**

CPU Usage Monitor

**Indices to query**

metricbeat-\*

**Time field**

@timestamp


**Run watch every**

1 minute

Use \* to broaden your query.

**Match the following condition**

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



**Perform 1 action when condition is met**

Add action

☒ ☐ Logging

**Log text**

Watch [{{ctx.metadata.name}}] has exceeded the threshold of 0.5 in the last 5 minutes

This enables Filebeat, Metricbeat, and Packetbeat on the Target VM and forwards log

```
Target 1 on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help

Debian GNU/Linux 8 target1 tty1

target1 login: vagrant
Password:
Last login: Wed Jul  1 06:24:00 AEST 2020 on tty1
Linux target1 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vagrant@target1:~$ sudo -s
root@target1:/home/vagrant# /opt/setup
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.
See more: https://www.elastic.co/guide/en/elastic-stack-overview/current/xpack-ml.html
Loaded machine learning job configurations
Loaded Ingest pipelines
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
-
```