Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

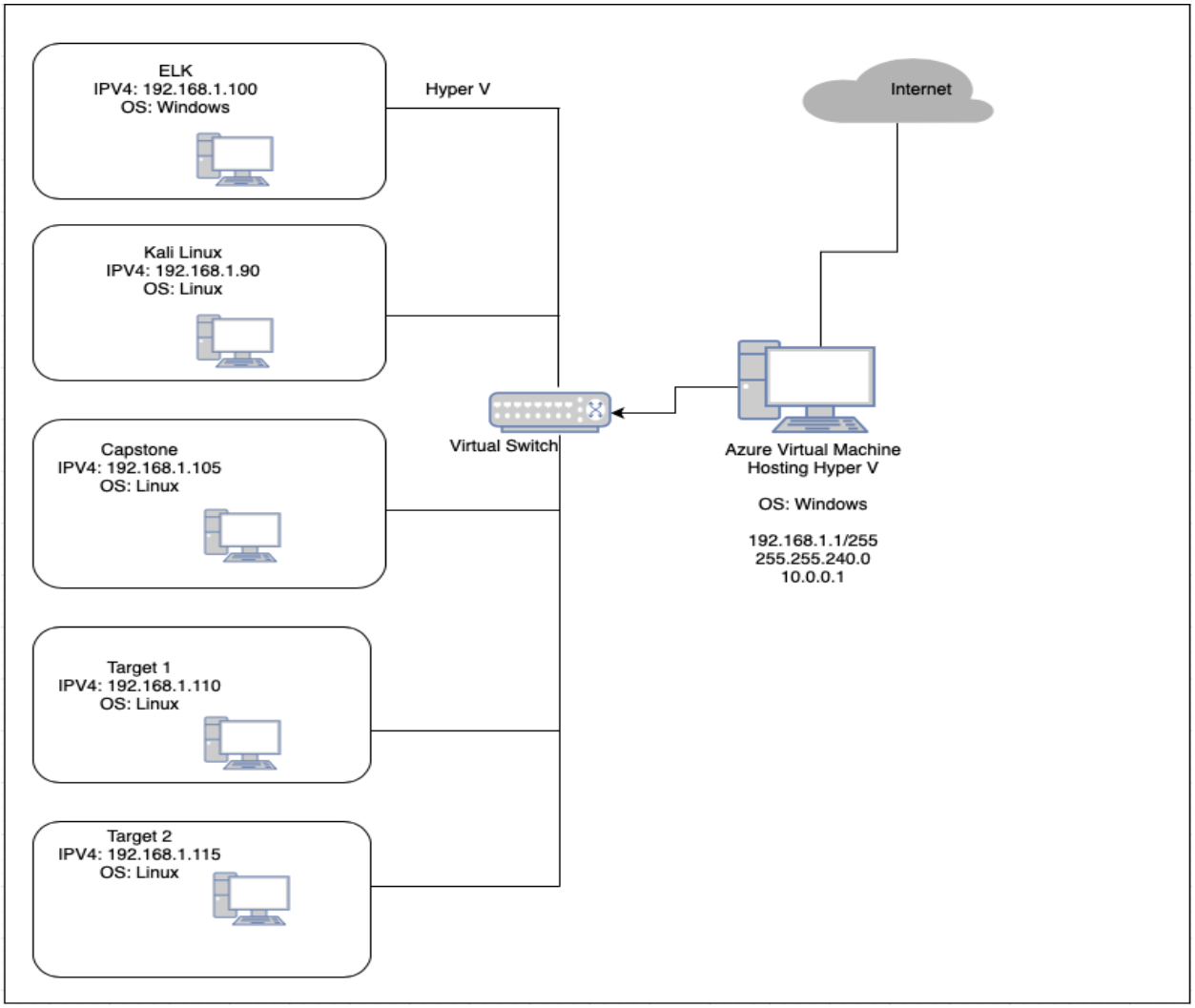
- Name of VM 1- Capstone
  - **Operating System**:Linux
  - **Purpose**: Filebeat and Metricbeat are installed and will forward logs to the ELK machine. This VM is in the network solely for the purpose of testing alerts.
  - **IP Address**: **Capstone**: 192.168.1.105

- Name of VM - ELK
  - **Operating System**:Windows
  - **Purpose**: It holds the Kibana dashboards
  - **IP Address**: **ELK**: 192.168.1.100

- Name of VM 3- Kali
  - **Operating System**:Linux
  - **Purpose**: A standard Kali Linux machine used in the penetration test
  - **IP Address**:**Kali**: 192.168.1.90

- Name of VM 4- Target 1
  - **Operating System**: Linux
  - **Purpose**: Exposes a vulnerable WordPress server. Sends logs to ELK
  - **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:

t	messages	
t	metadata.name	Excessive HTTP Errors
t	metadata.watcherui.agg_type	count
t	metadata.watcherui.index	packetbeat-*
t	metadata.watcherui.term_field	http.response.status_code
#	metadata.watcherui.term_size	5
#	metadata.watcherui.threshold	400
t	metadata.watcherui.threshold_comparator	>
t	metadata.watcherui.time_field	@timestamp
#	metadata.watcherui.time_window_size	5
t	metadata.watcherui.time_window_unit	m
#	metadata.watcherui.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-NE4WaaojMQ
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	⚠

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

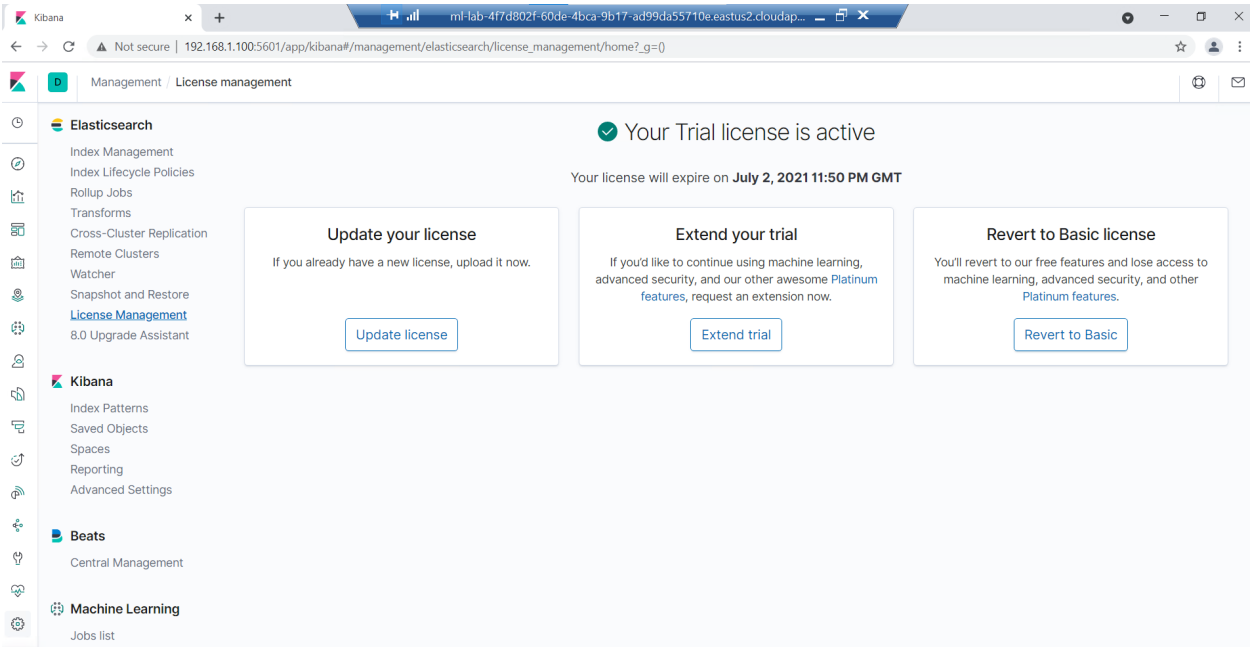
- The alert for **CPU Usage Monitor Alert** was set up for a threshold above 0.5 CPUs for 5 minutes. Based on the results found, the alert was not triggered based on threshold parameters. In the near future, we will review these threshold parameters for possible false positives or negatives.

metadata.name	CPU Usage Monitor
metadata.watcherui.agg_field	system.process.cpu.total.pct
metadata.watcherui.agg_type	max
metadata.watcherui.index	metricbeat-*
metadata.watcherui.term_size	5
metadata.watcherui.threshold	0.5
metadata.watcherui.threshold_comparator	>
metadata.watcherui.time_field	@timestamp
metadata.watcherui.time_window_size	2
metadata.watcherui.time_window_unit	m
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 @ 02:59:22.456
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	⚠ 0.247
result.input.payload.hits.hits	⚠
result.input.payload.hits.max_score	⚠ -

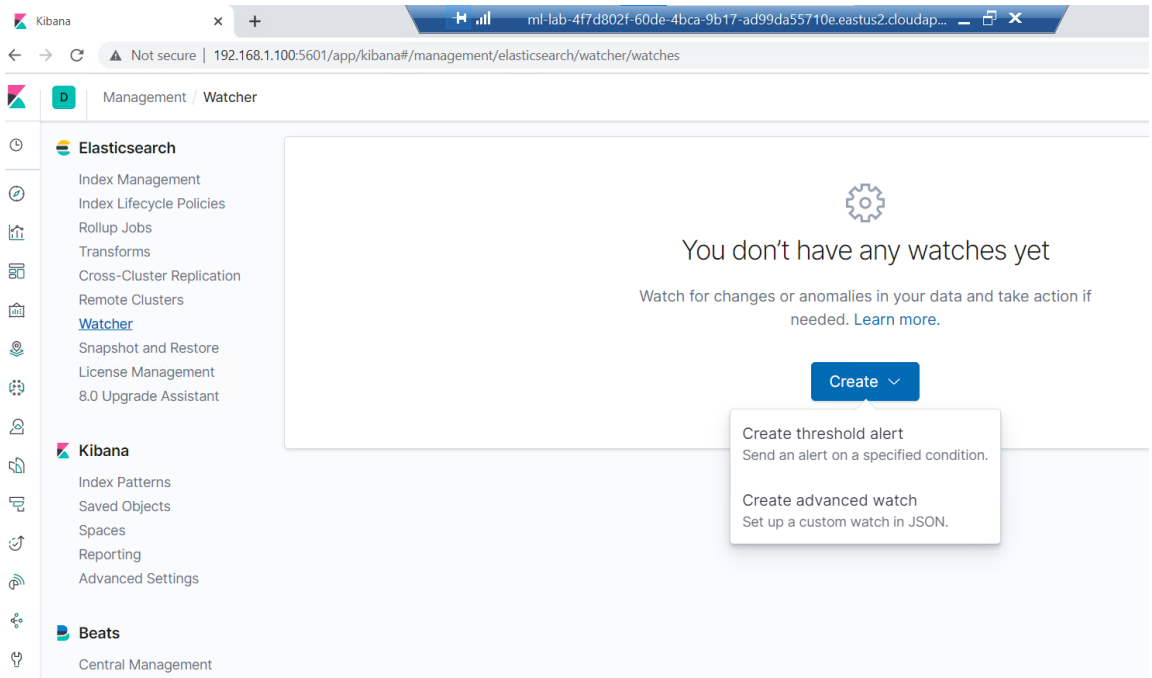
result.input.payload.hits.max_score	-
result.input.payload.hits.total	583
result.input.payload.timed_out	false
result.input.payload.took	1
result.input.search.request.body.aggs.metricAgg.max.field	system.process.cpu.total.pct
result.input.search.request.body.query.bool.filter.range.@timestamp.format	strict_date_optional_time||epoch_millis
result.input.search.request.body.query.bool.filter.range.@timestamp.gte	2021-06-03T02:59:22.343Z||-2m
result.input.search.request.body.query.bool.filter.range.@timestamp.lte	2021-06-03T02:59:22.343Z
result.input.search.request.body.size	0
result.input.search.request.indices	metricbeat-*
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
status.actions.logging_1.ack.state	awaits_successful_execution
status.actions.logging_1.ack.timestamp	2021-06-03T00:05:22.342Z
status.execution_state	execution_not_needed
status.last_checked	2021-06-03T02:59:22.456Z
status.state.active	true
status.state.timestamp	2021-06-03T00:05:22.342Z
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

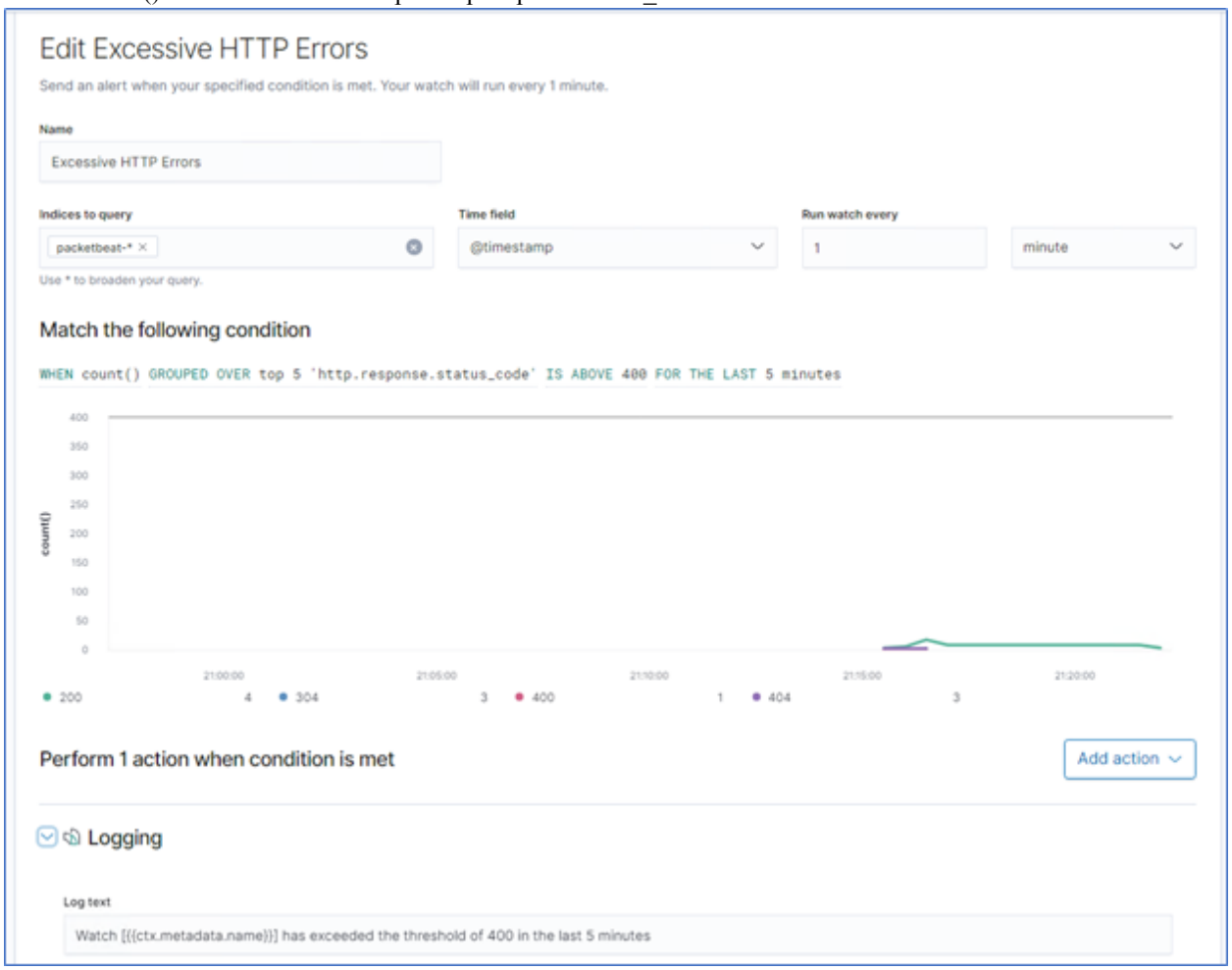


- Create a Threshold Alert:



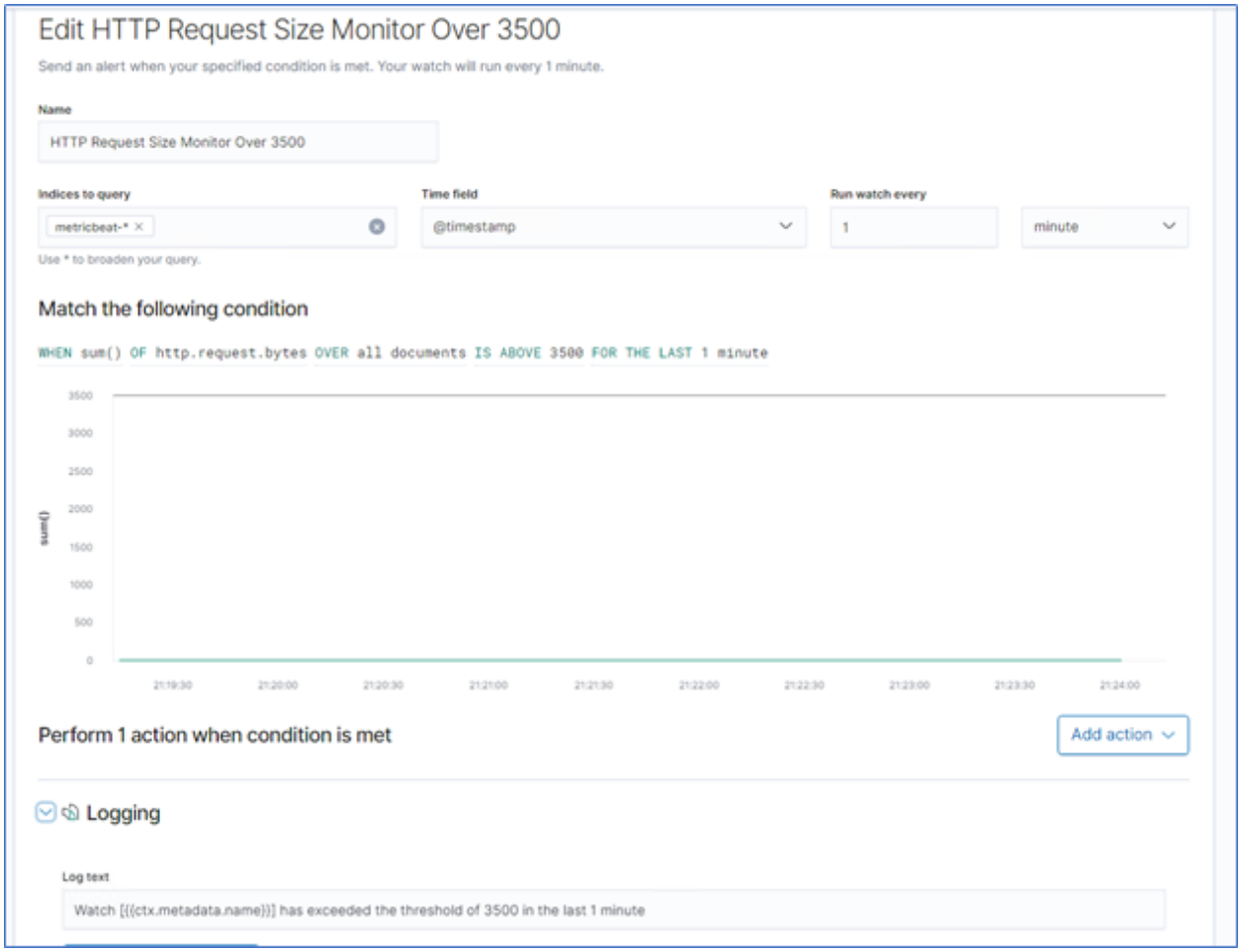
Excessive HTTP Errors Alert: packetbeat

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



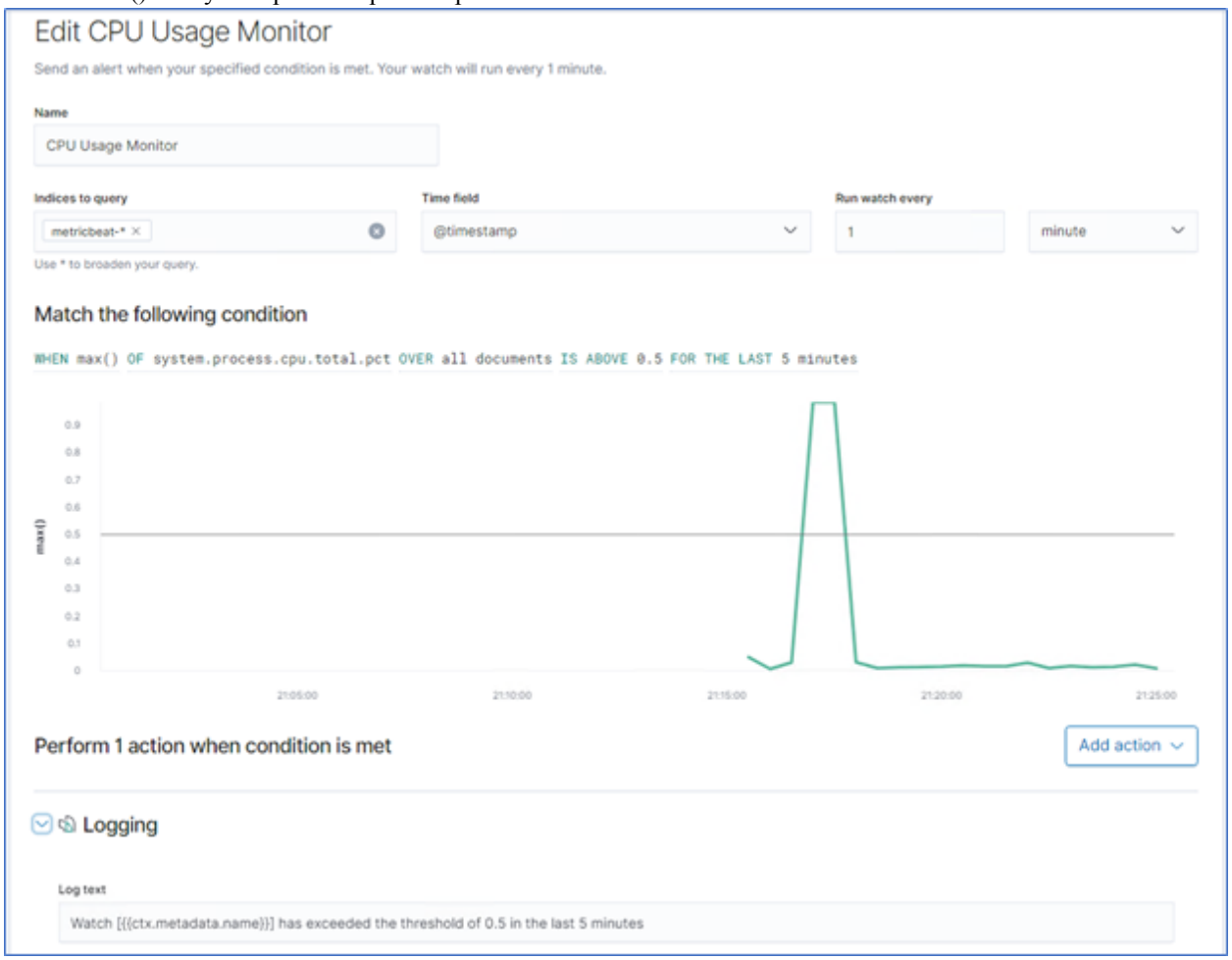
HTTP Request Size Monitor Alert: metricbeat

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



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