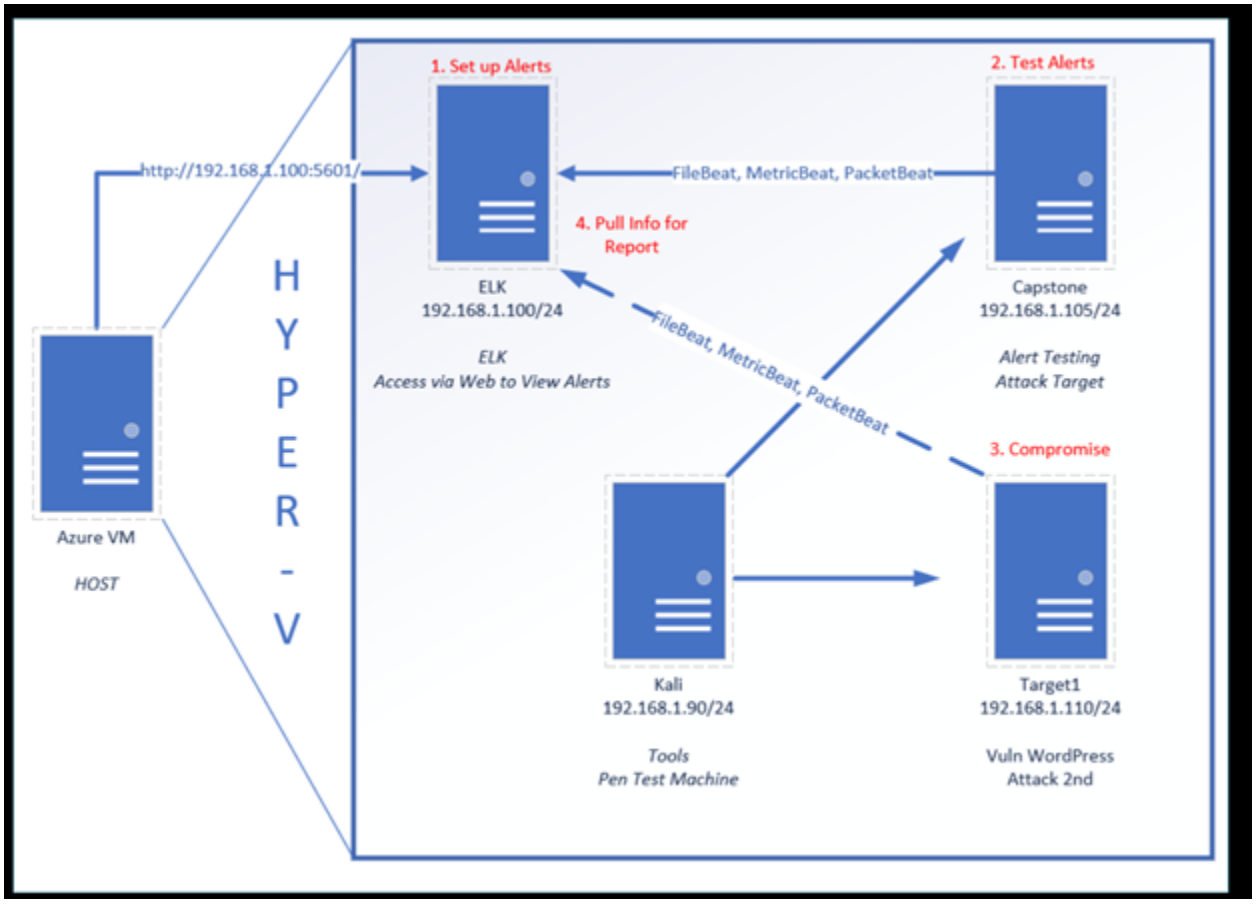
Blue Team: Summary of Operations

By

Darrel Mills Cybersecurity Specialist

- Network Topology



Network Topology

The following machines were identified on the network:

Network: Machines: Name of VM 1
Address Range: 192.168.1.0/24 IPv4: 192.168.1.1
Netmask: 255.255.255.0 OS: Microsoft Windows 10
Gateway: 10.0.0.1 Hostname: ML-RefVm-684427

Azure Host Machine

_____

Machine: Name of VM 2
IPv4: 192.168.1.90
OS: Kali Linux 5.4.0
Hostname: Kali

(Attack Machine)

_____

Machine: Name of VM 3
IPv4: 192.168.1.100
OS: Ubuntu Linux
Hostname: Elk Stack

_____

Machine: Name of VM 4
IPv4 192.168.1.110
OS: Linux 3.16.0-6-amd64
Hostname: Target1

_____

Machine: Name of VM 5
IPv4: 192.168.1.115
OS: linux 3.16.0-6-amd64
Hostname: Target2

-Description of Targets

The target of this attack was: `**Target 1` (IP Address 192.168.1.110).**
Target 2 (IP Address 192.168.1.115)

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:

Monitoring the Targets

Darrel Mills Blue_Team_SOC monitored the Traffic to these services and should be very careful, and has implemented the alerts below:

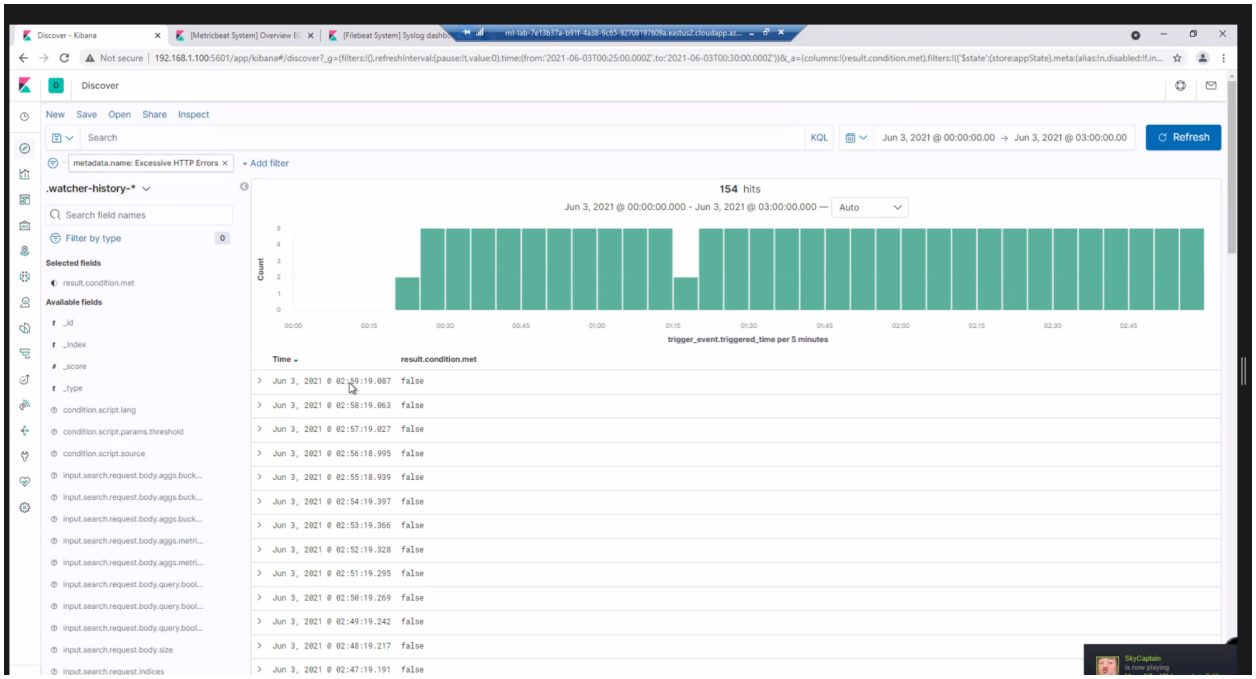
Name of Alert 1

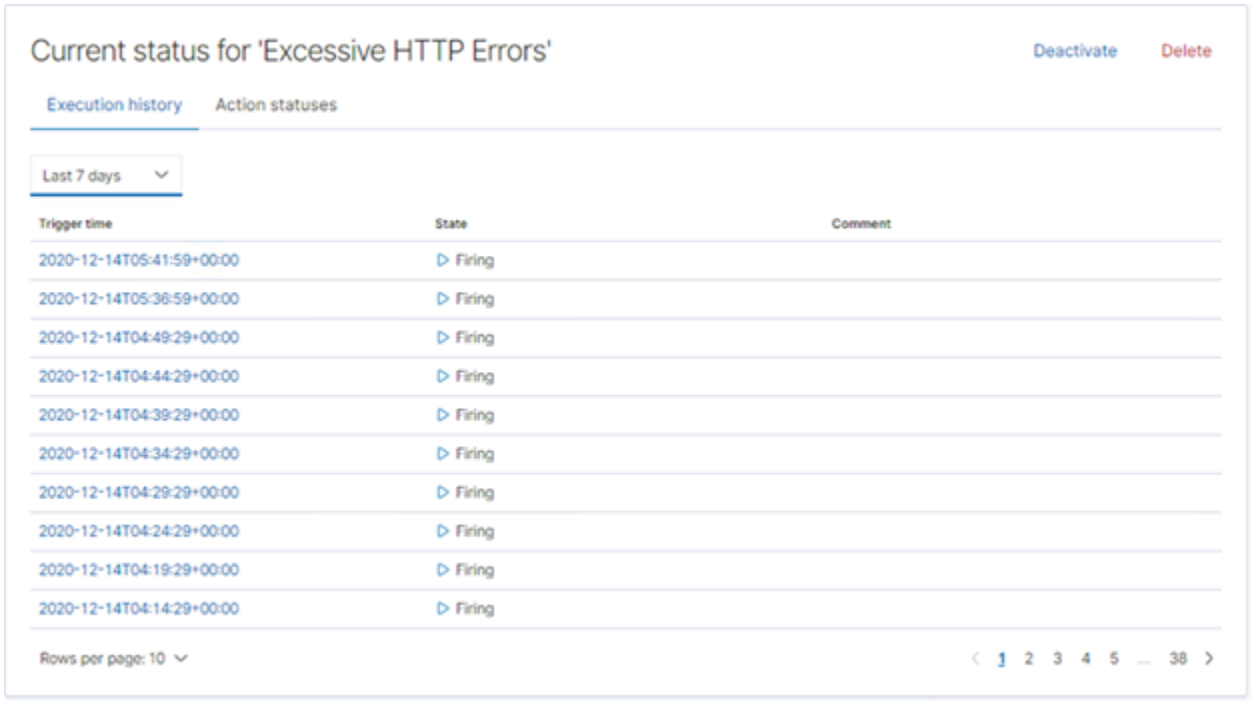
Kibana Watcher Alert 1:
Answer: **Excessive HTTP Errors**
Report was done by: Darrel Mills Cybersecurity Specialist
Alert 1 is implemented as follows: packetbeats
Answer: **Brute Force.**

- **Metric**: **This packetbeat measures the excessive HTTP errors such as 4xx and 5xx series errors**
- **Threshold**: **Alert is instructed to run a watch every 5 minutes**
- **Vulnerability Mitigated**: **Brute force The alert sends a trigger when the count is above 400 Status response codes in a 5 minute window.**

- **Reliability**Medium from some of the False negatives, but if we compare this alert to the others it shows a Brute Force attack. : Does this alert generate lots of false positives/false negatives? False negative and the reliability is medium due to all the alerts compiling data would keep brute force at check..**

Malicious Git HTTP Server For **CVE-2017-1000117 39**

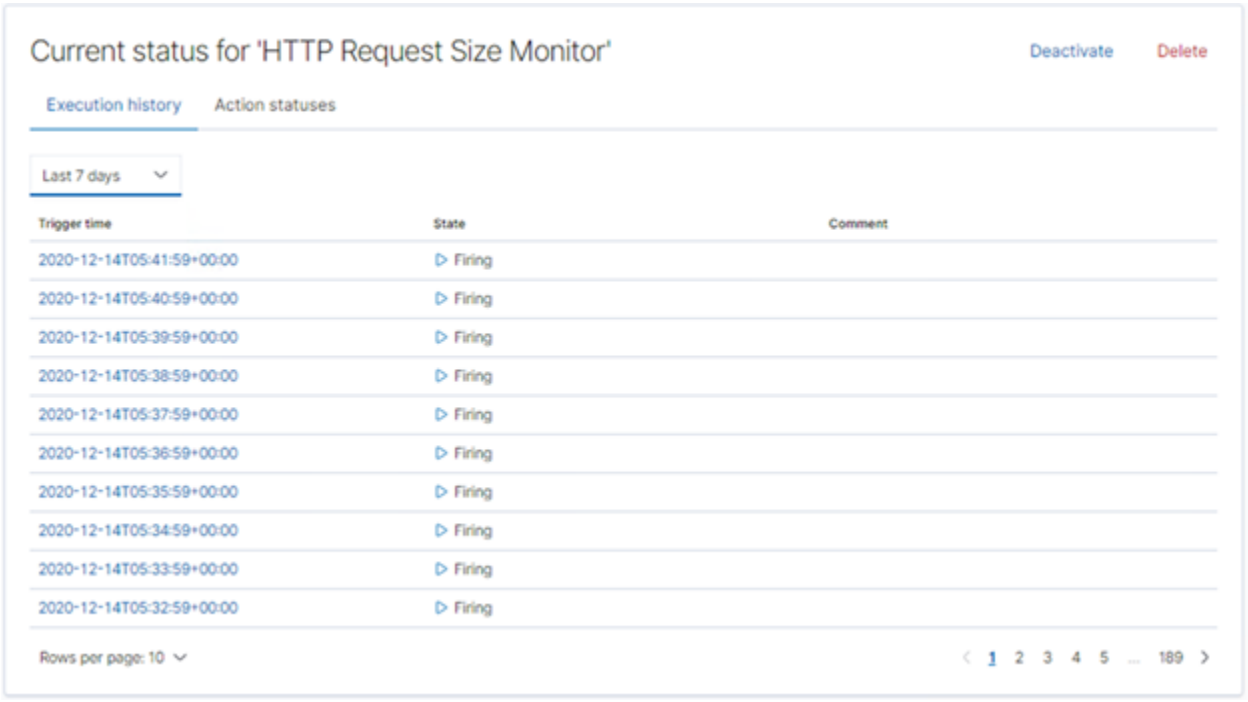


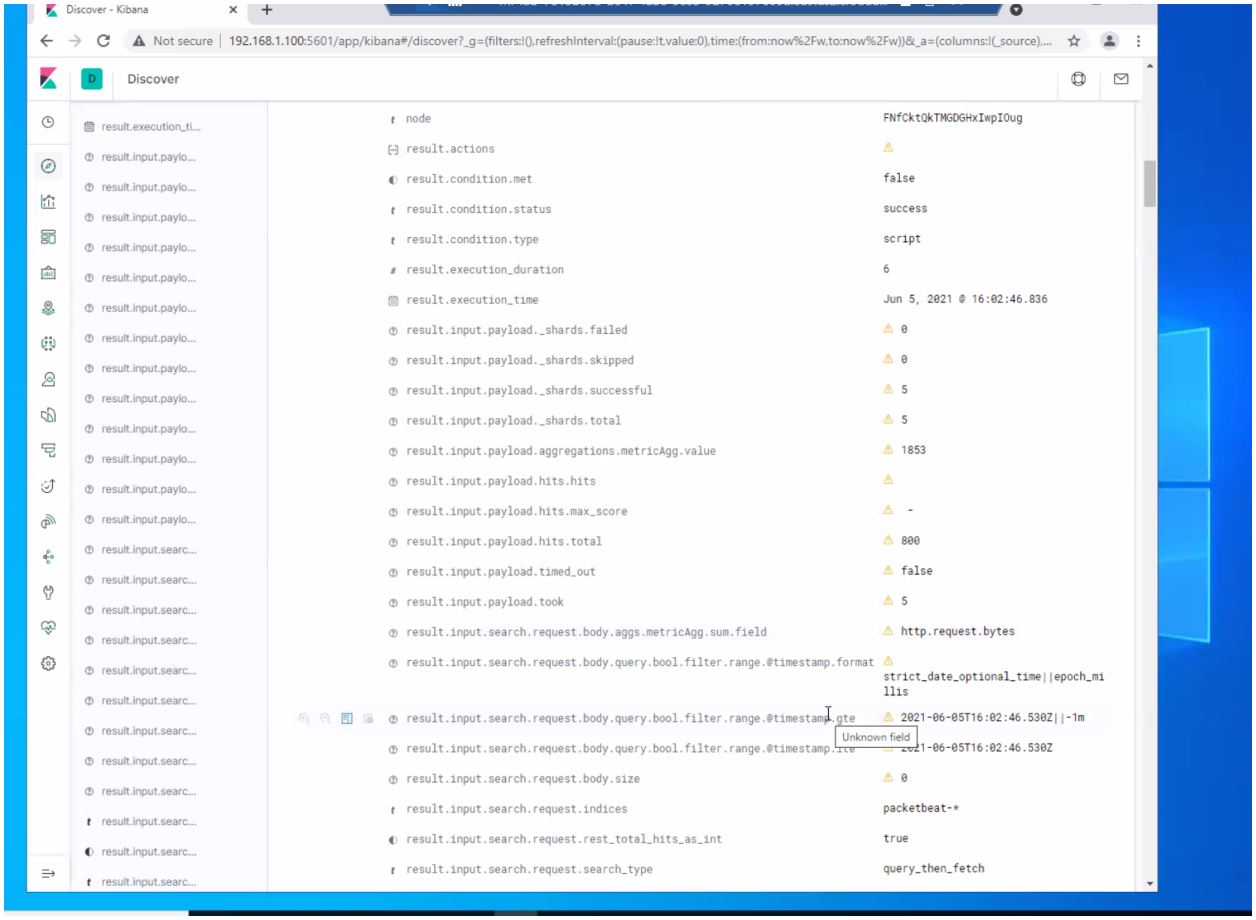


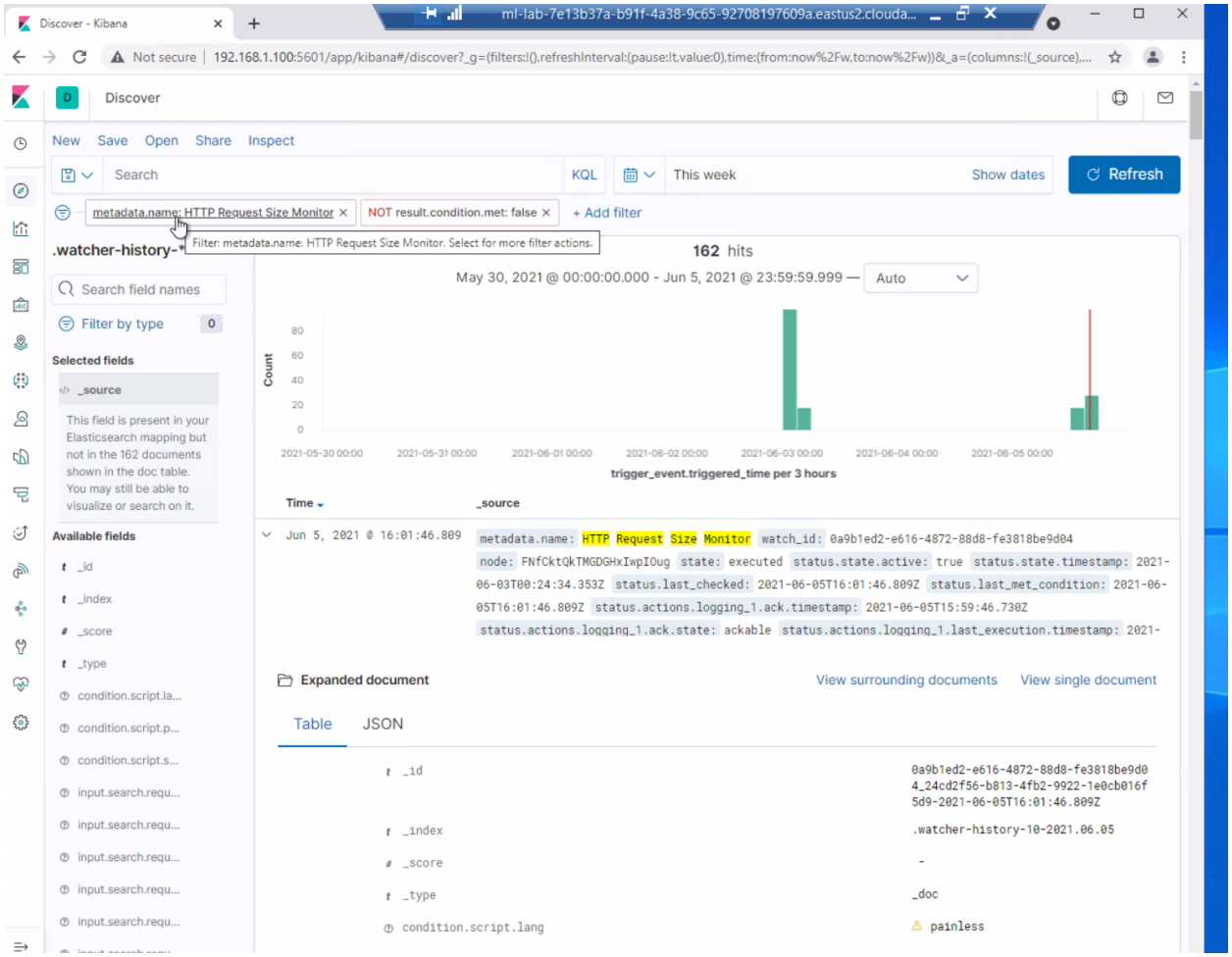
Name of Alert 2

Kibana Watcher Alert 2: **HTTP requests size monitor**
Alert 2 is implemented as follows: **packetbeat**
- **Metric**:
Answer: **This packetbeats measures the quantity of HTTP request for documents**
- **Threshold**:
Answer: **Alert is instructed to run a watch every 1 minute**
- **Vulnerability Mitigated**:
Answer: **The alert sends a trigger when the sum total of HTTP request for all documents is above 3500 request in a 1-minute window**
- **Reliability**
Answer: **HIGH**
Rate as low, medium, or high reliability.

Answer: And a high reliability for this alert is high due to the alert being triggered when there is a sudden influx bytes request because threshold is met
Report was done by: Darrel Mills Cybersecurity Specialist
CVE-**2017-0777 OPEN SSH PORTS VULNERABILE**




Discover - Kibana
Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now%2Fw,to:now%2Fw))&_a=(columns:!(_source),...
Discover
result.execution_ti...
result.input.paylo...
result.input.searc...
node FNfCktQkTMGDGHxIwpIOug
result.actions
result.condition.met false
result.condition.status success
result.condition.type script
result.execution_duration 6
result.execution_time Jun 5, 2021 @ 16:02:46.836
result.input.payload._shards.failed 0
result.input.payload._shards.skipped 0
result.input.payload._shards.successful 5
result.input.payload._shards.total 5
result.input.payload.aggregations.metricAgg.value 1853
result.input.payload.hits.hits
result.input.payload.hits.max_score -
result.input.payload.hits.total 800
result.input.payload.timed_out false
result.input.payload.took 5
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 2021-06-05T16:02:46.530Z||-1m
Unknown field
result.input.search.request.body.query.bool.filter.range.@timestamp.lte 2021-06-05T16:02:46.530Z
result.input.search.request.body.size 0
result.input.search.request.indices packetbeat-*
result.input.search.request.rest_total_hits_as_int true
result.input.search.request.search_type query_then_fetch



Darrel Mills Blue_Team_SOC

Name of Alert 3

Report was done by: Darrel Mills Cybersecurity Specialist

Kibana Watcher Alert 3: CPU Usage Monitor

Alert 3 is implemented as follows: packetbeat

- **Metric:**

Answer: System Processes % threshold 50% usage This metric measures CPU usage

- **Threshold:**

Answer: Alert is instructed to run a watch every minute

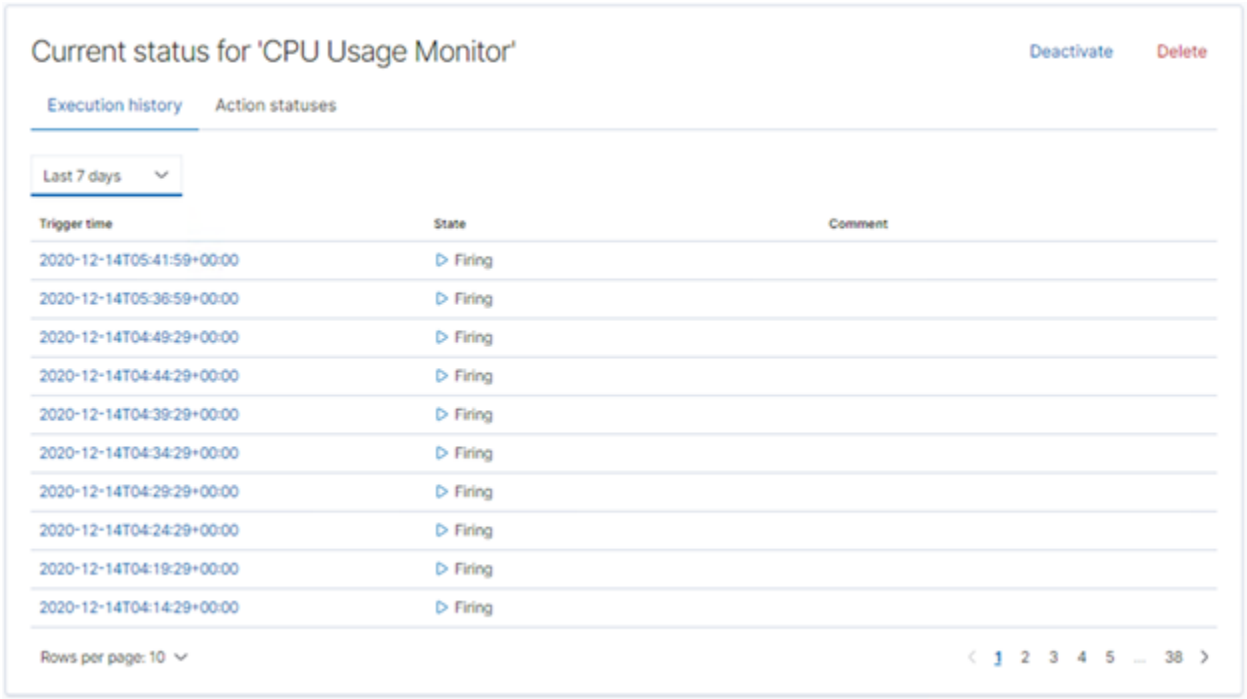
- **Vulnerability Mitigated:**

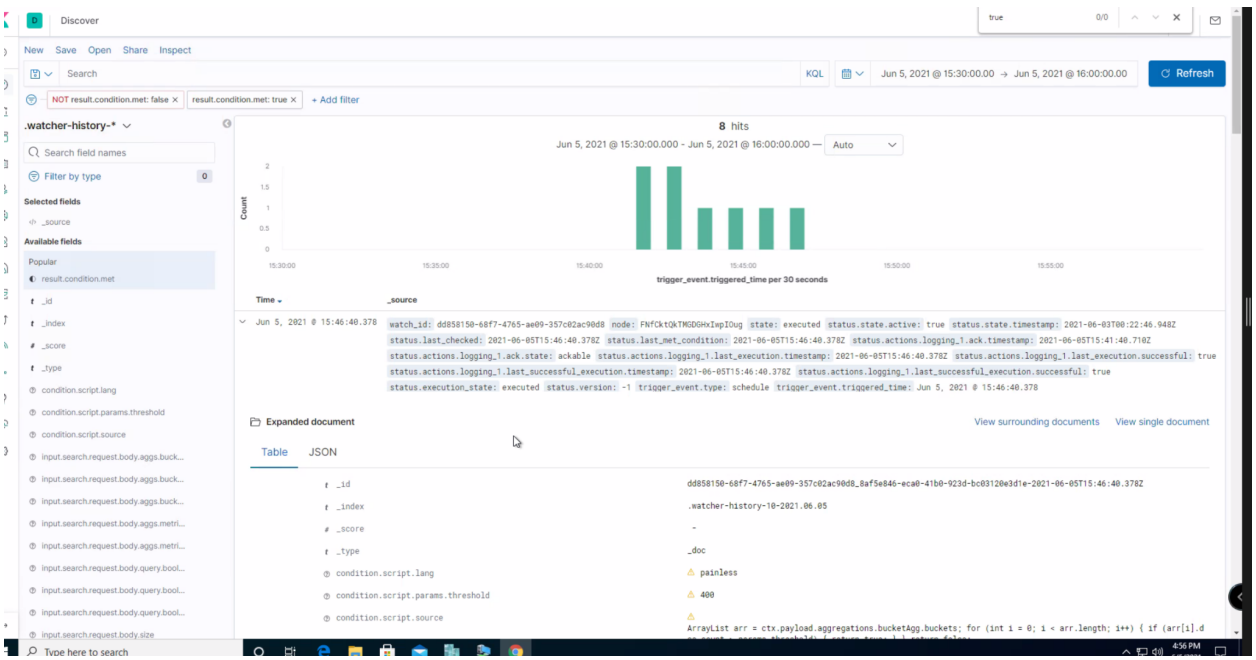
Answer: Brute Force The alert sends a trigger when the percentage of CPU usage is above 0.25 in a 5 minute window yes

- **Reliability:**

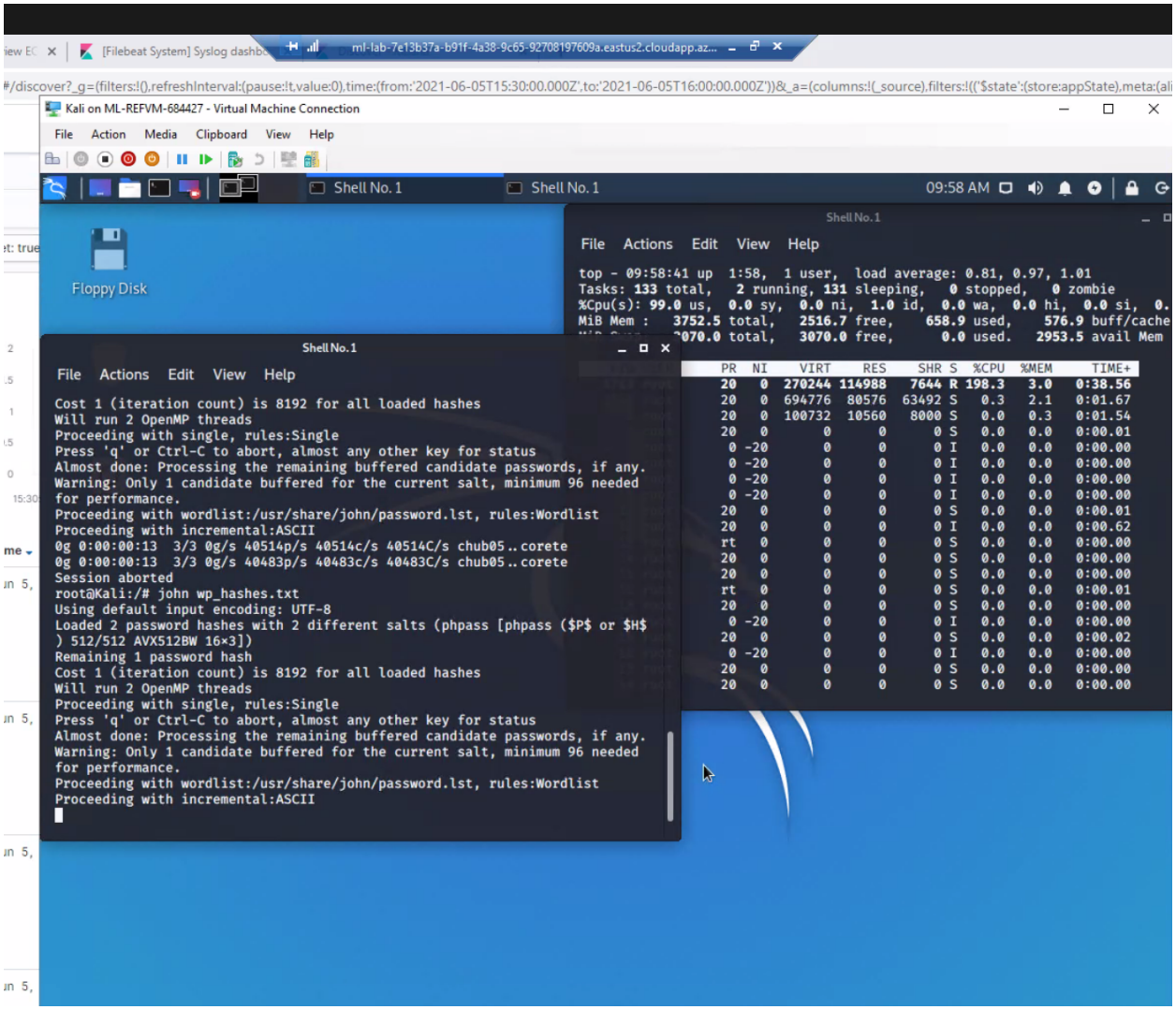
Answer: would high and find true during the attack triggers alerts accurately when CPU usage threshold is met..

CVE-2016-0778





V



The CPU jumps up after running the John the Ripper so therefore the alert is working and is high reliability.

Darrel Mills Blue_Team_SOC

Suggestions for Going Further :

The alerts Darrel Mills generated during the assessment suggest that this network has several active threats. The Network should be hardened against them in addition to keeping an eye on all the threats that occurred. The Blue Team suggests that IT implement the fixes below to protect the network.

- 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. E.g.,

implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain _how_ to implement each patch.

- **Vulnerability 1 SSH Access**

Answer: Patch: Upgrade your openssh to fix CVE-2016-0778

- **Patch:**

Answer: $ sudo apt-get update

- $ sudo apt-get install openssh-client openssh-server openssh-sftp-server`_

- **Why It Works:**

Answer: `special-security-package` scans the system for viruses every day_

-

- **Vulnerability 2 Wordpress out of date**

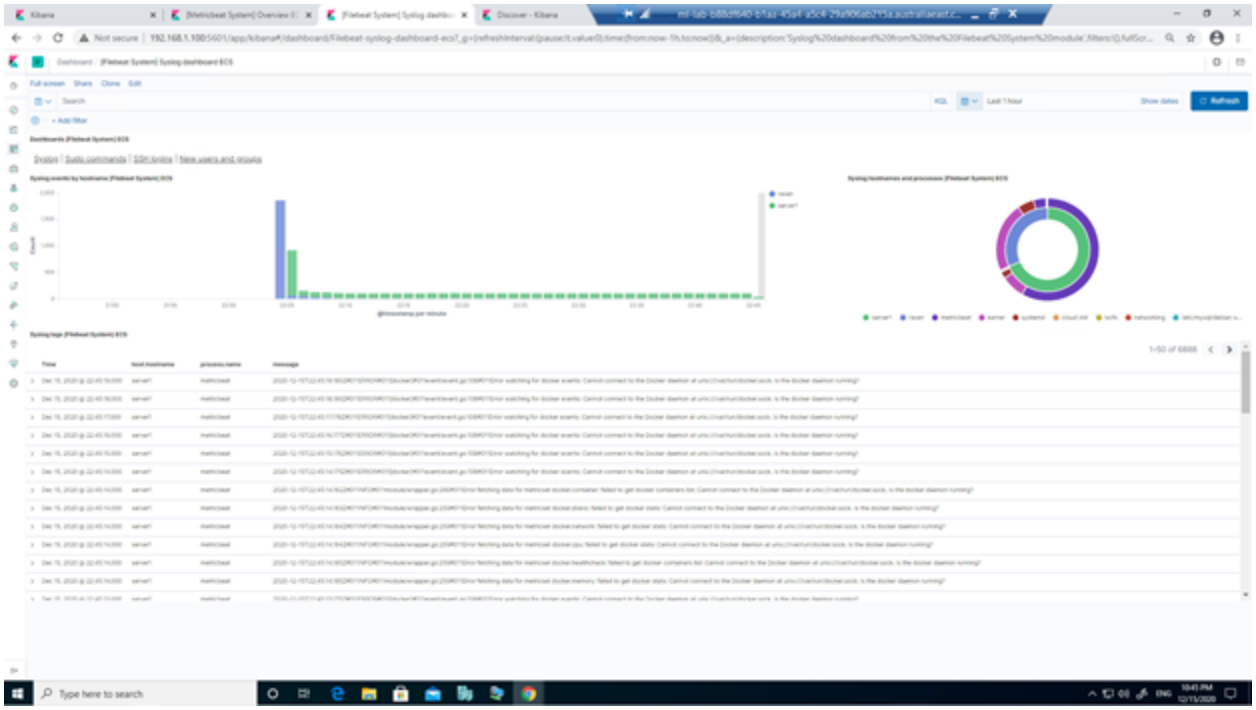
Answer: Patches below https://wordpress.org/support/article/updating-wordpress/#one-click-update or https://wordpress.org/download/,to_install

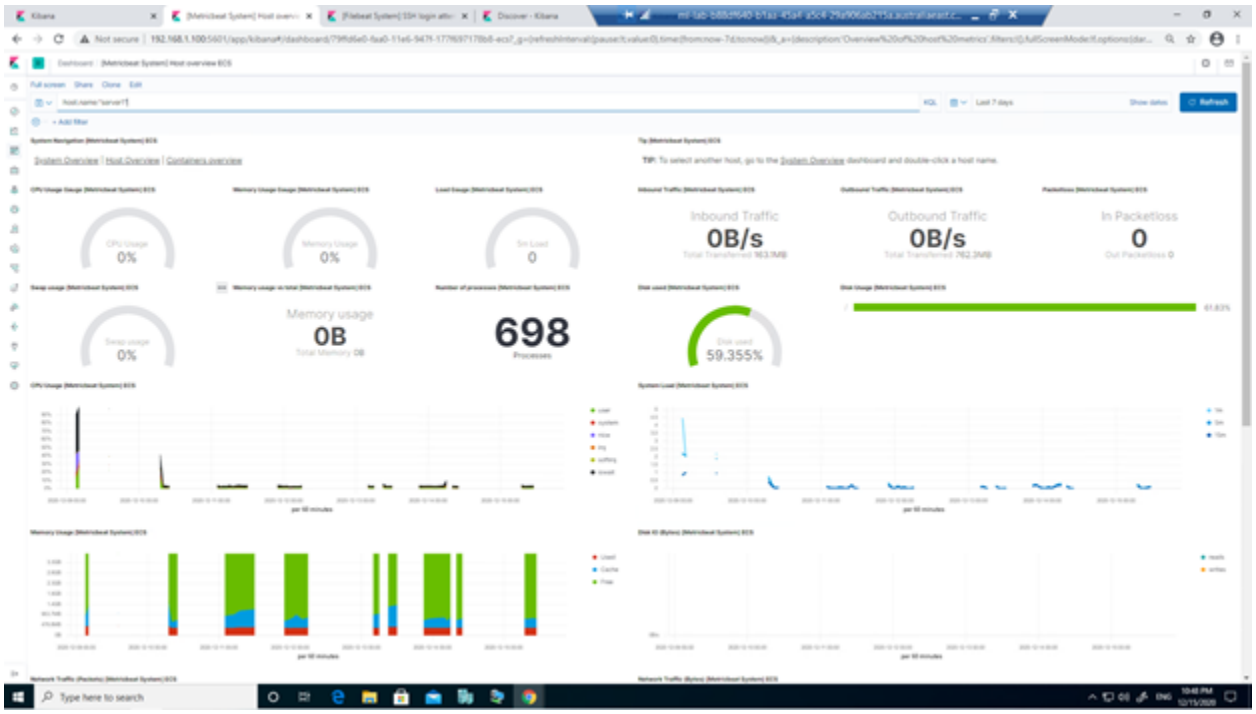
- **Why It Works:**

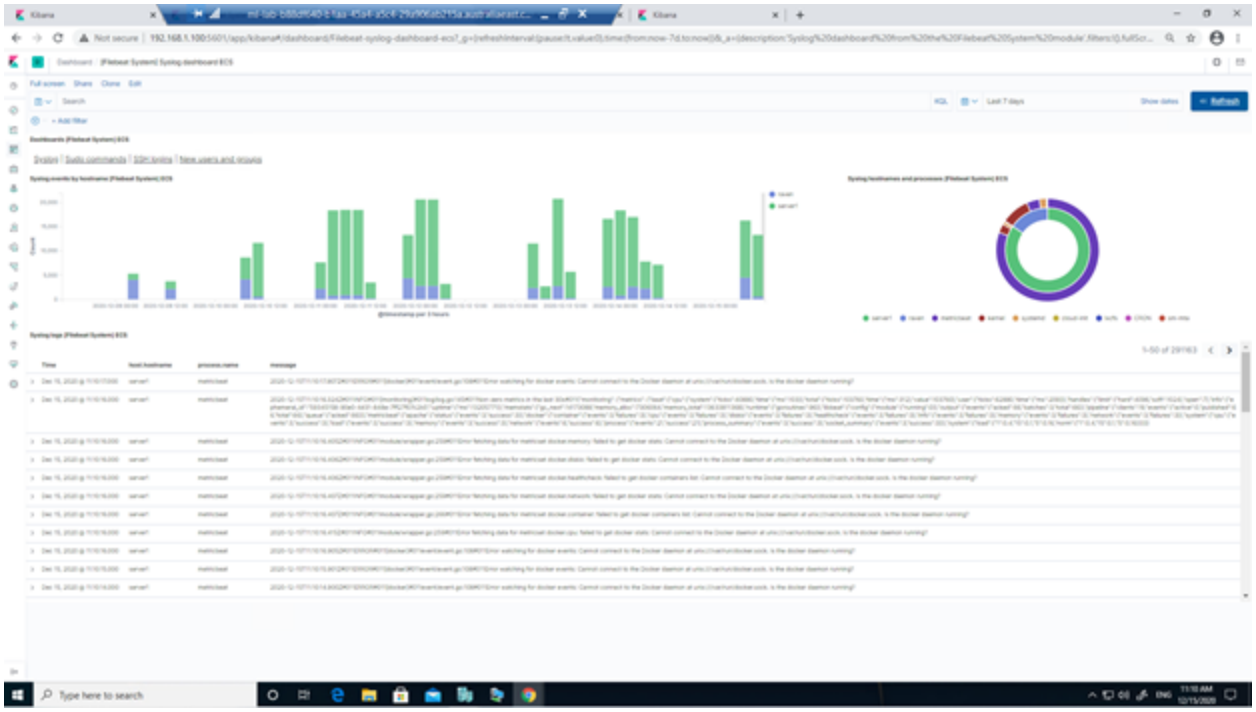
Report was done by: Darrel Mills Cybersecurity Specialist

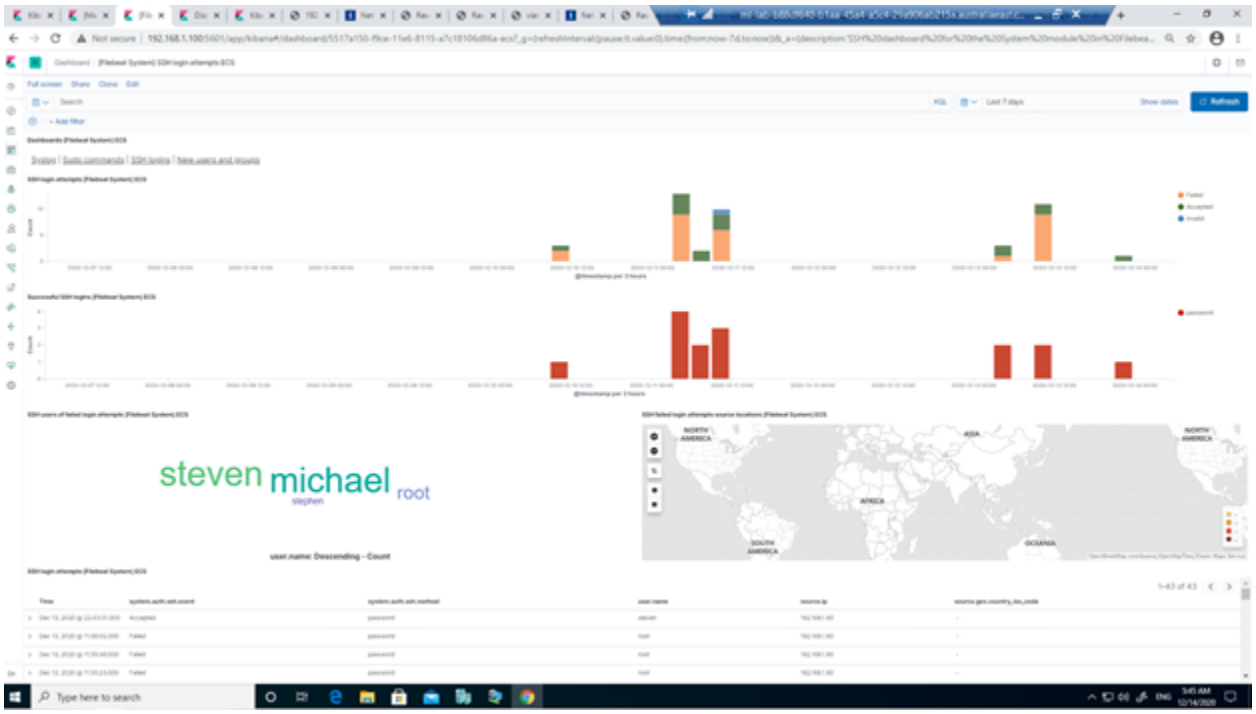
Answer: It is very important to update all critical infrastructure and company software, including WordPress, should be done on a regular basis. Company policy establishes that all assets are checked for updates either weekly, or monthly.checking,

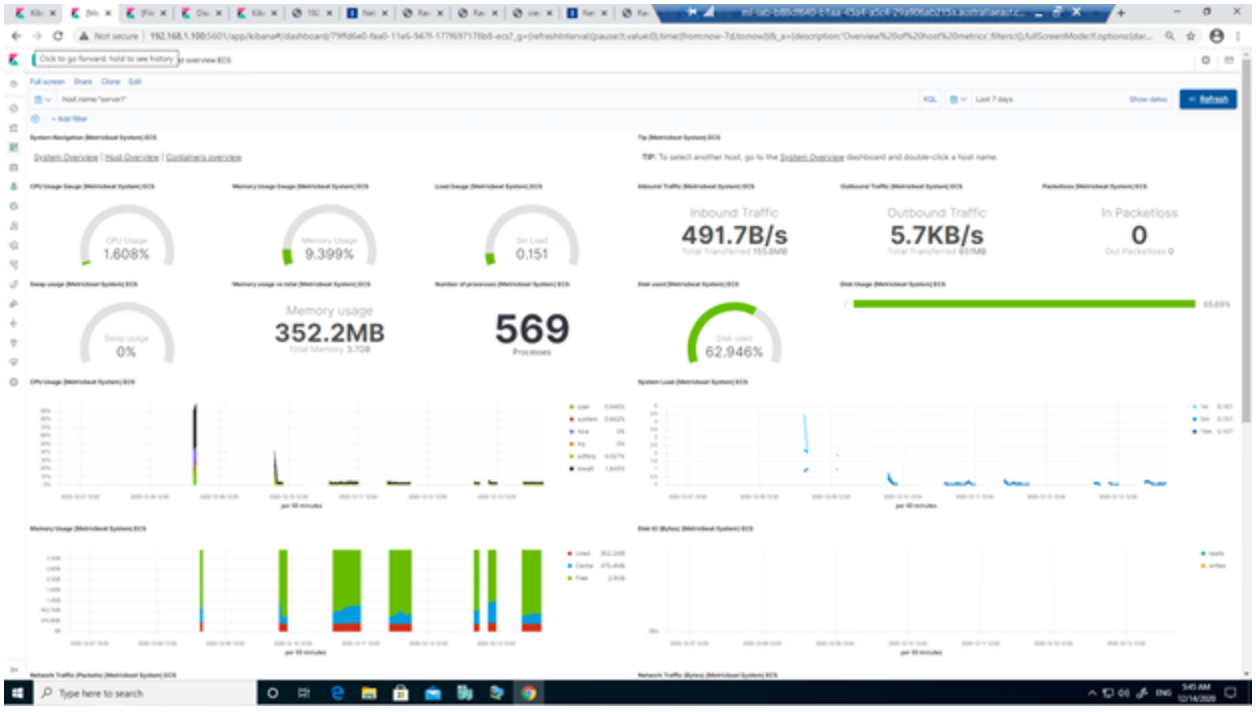
- **Screenshot as evidence**

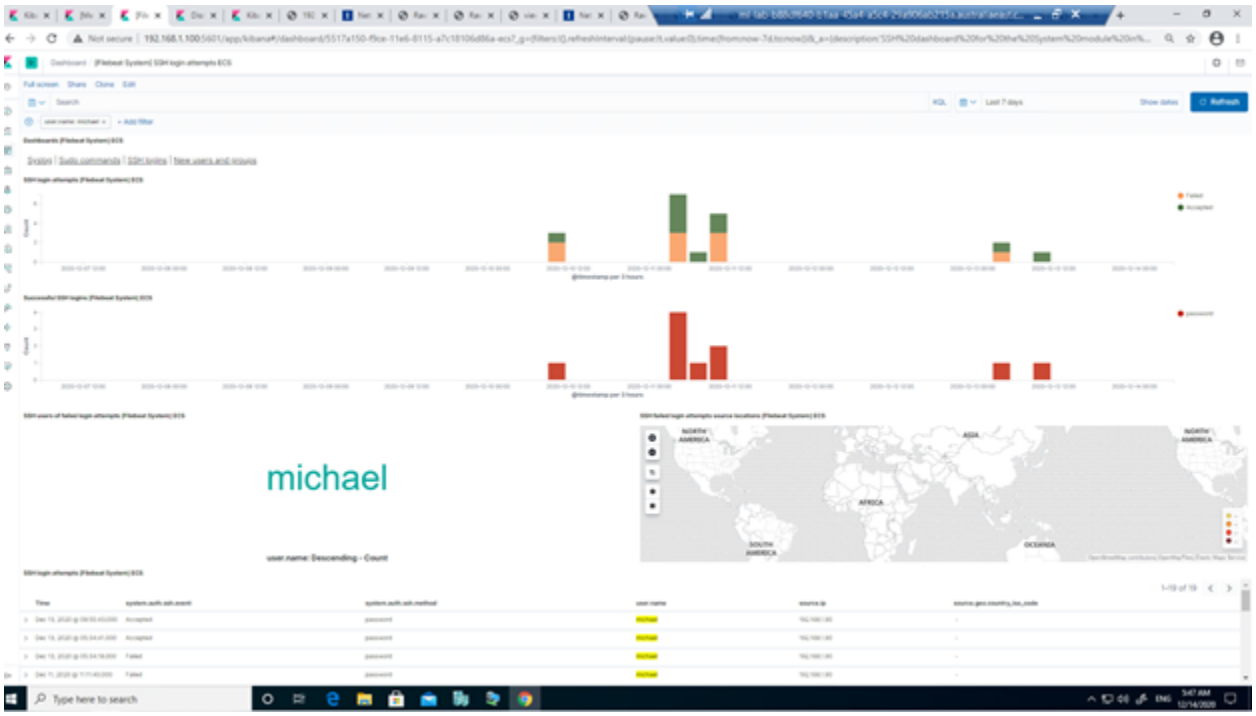


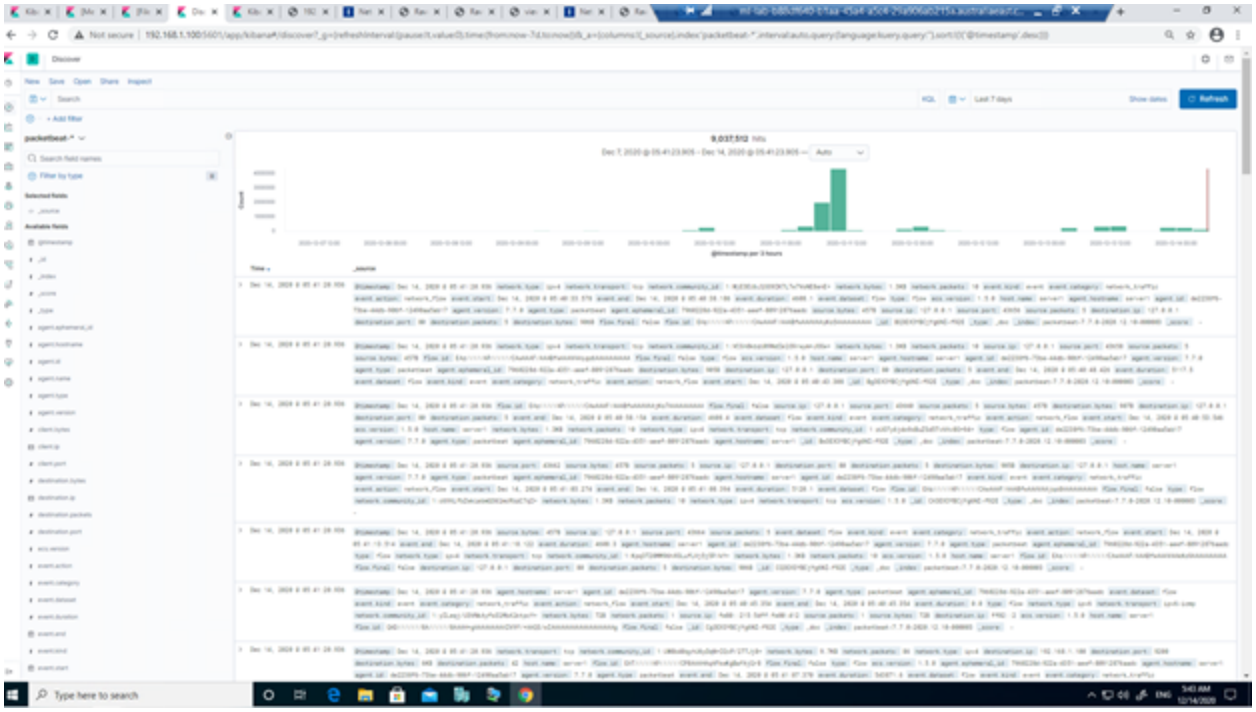


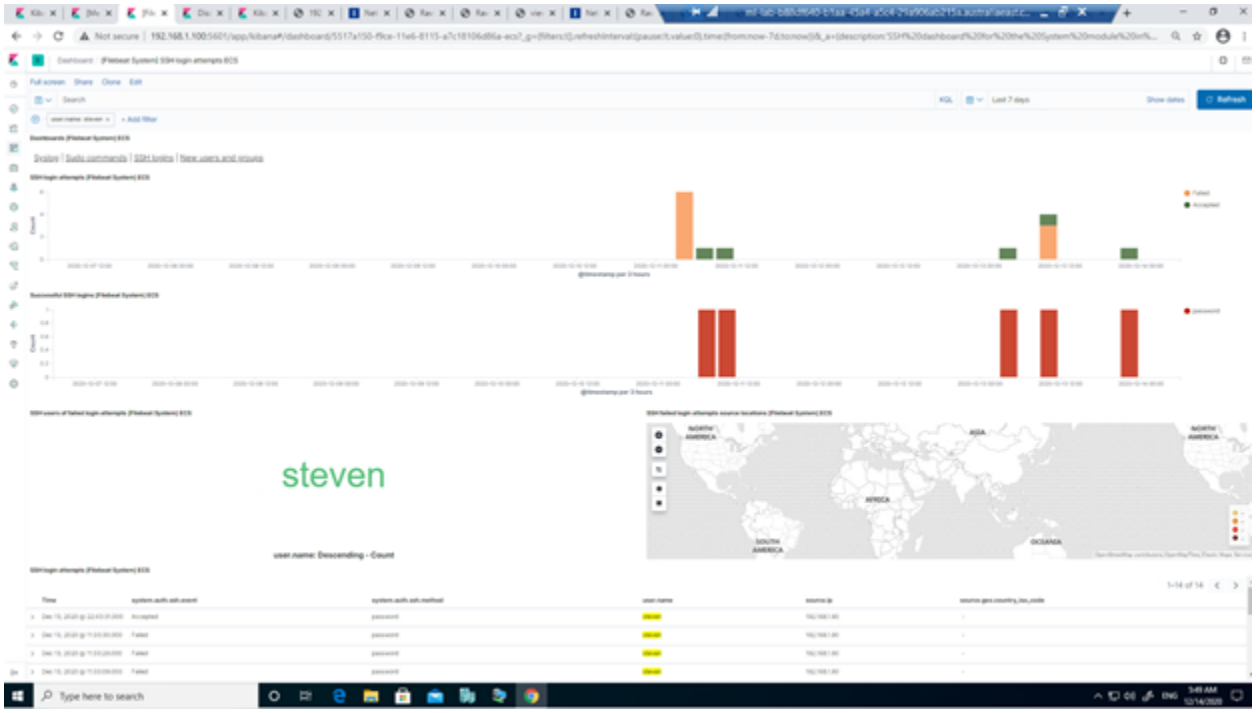


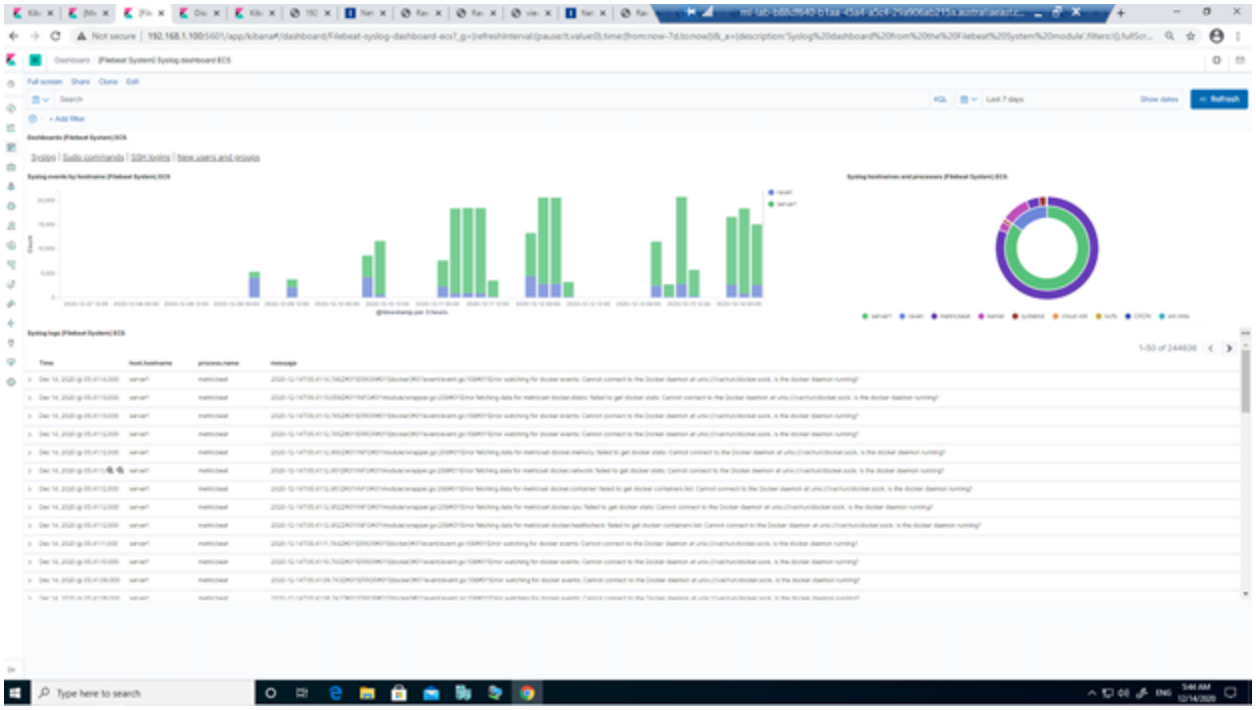

steven
michael
root
stephen

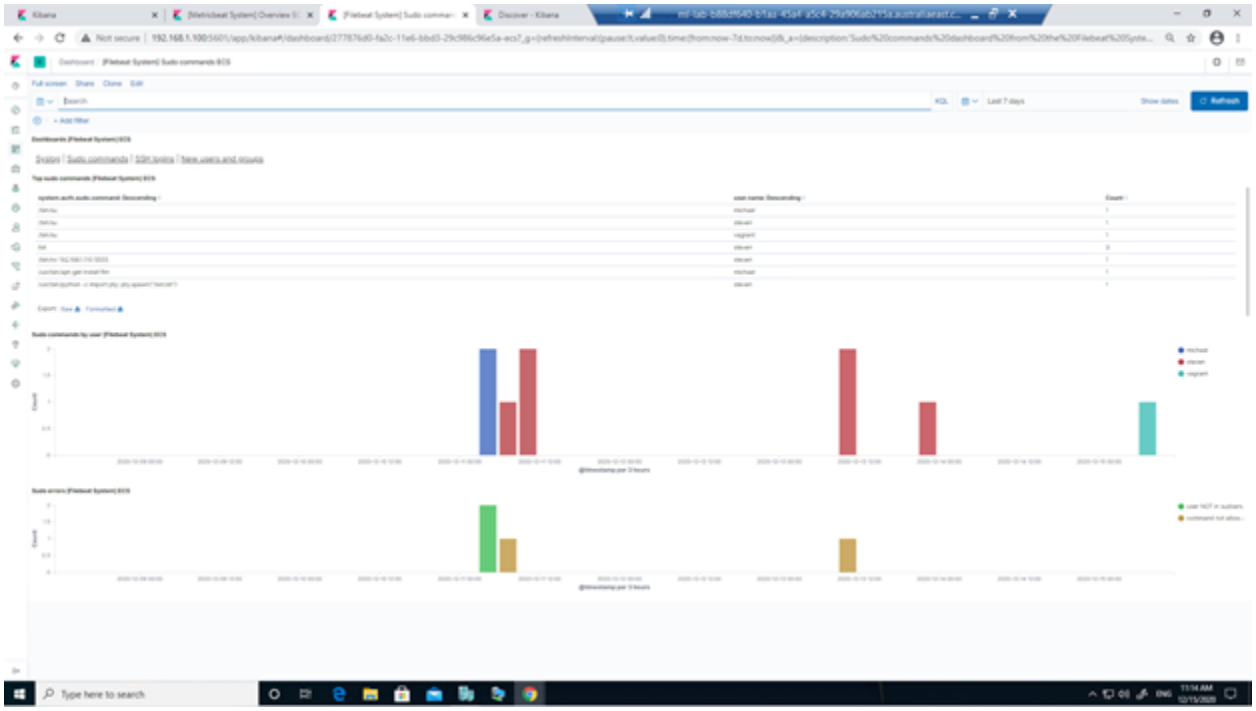

Inbound Traffic
491.7B/s
Outbound Traffic
5.7KB/s
In Packetloss
0
Memory usage
352.2MB
569
Processes
62.946%

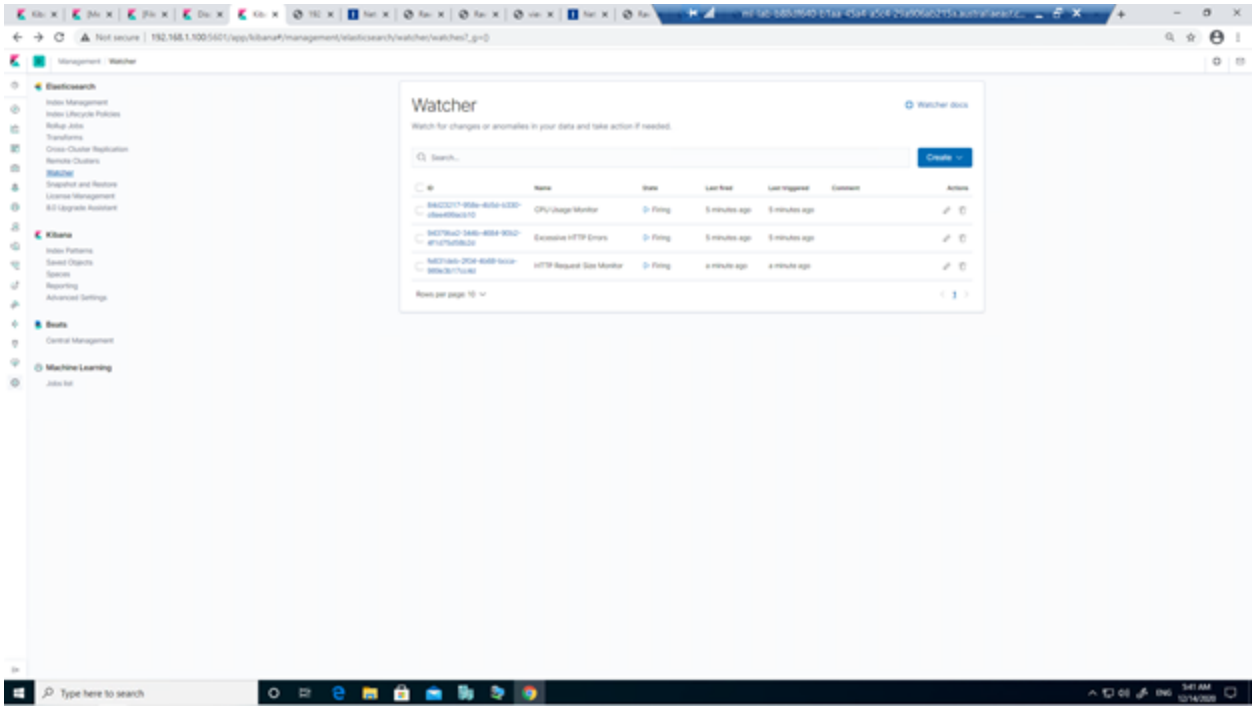

michael
user.name: Descending - Count

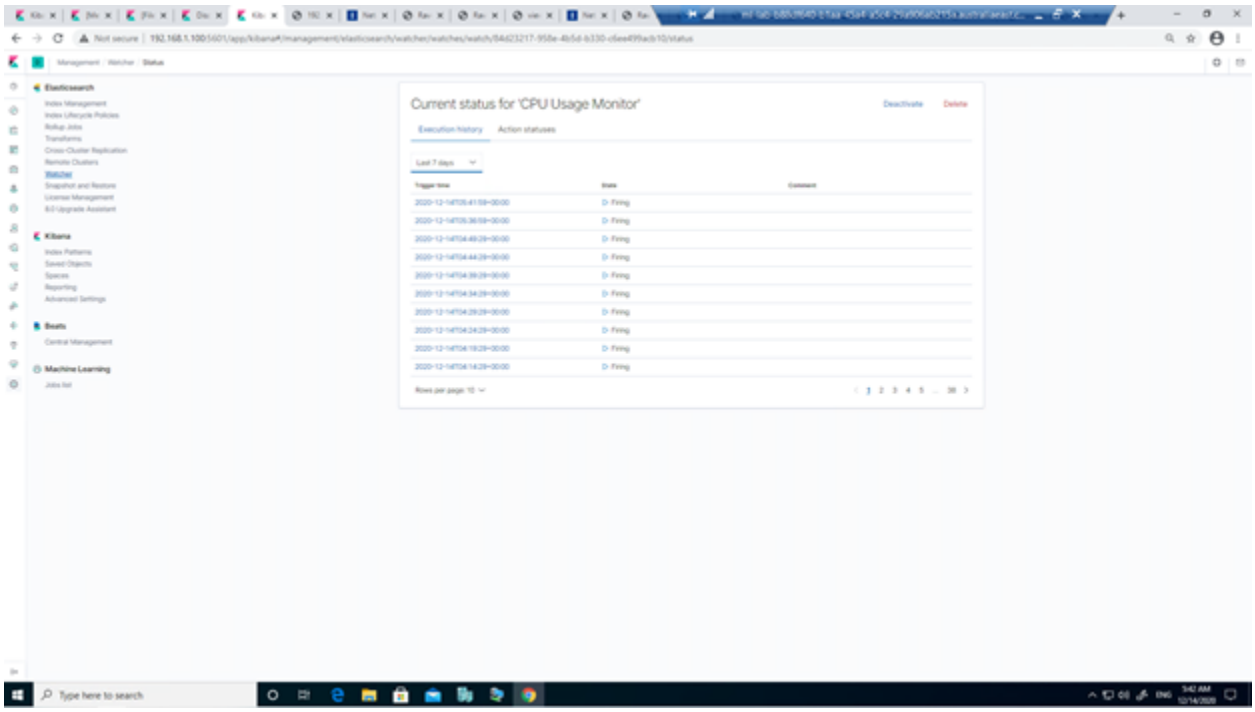


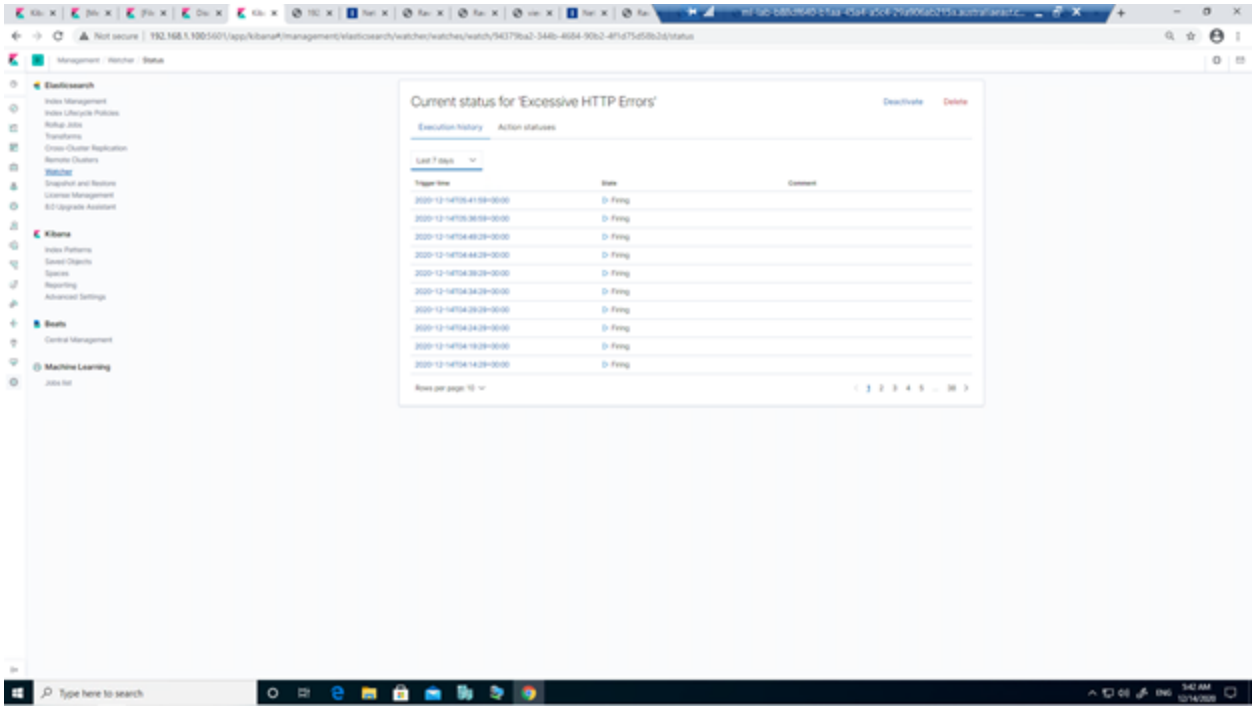

steven



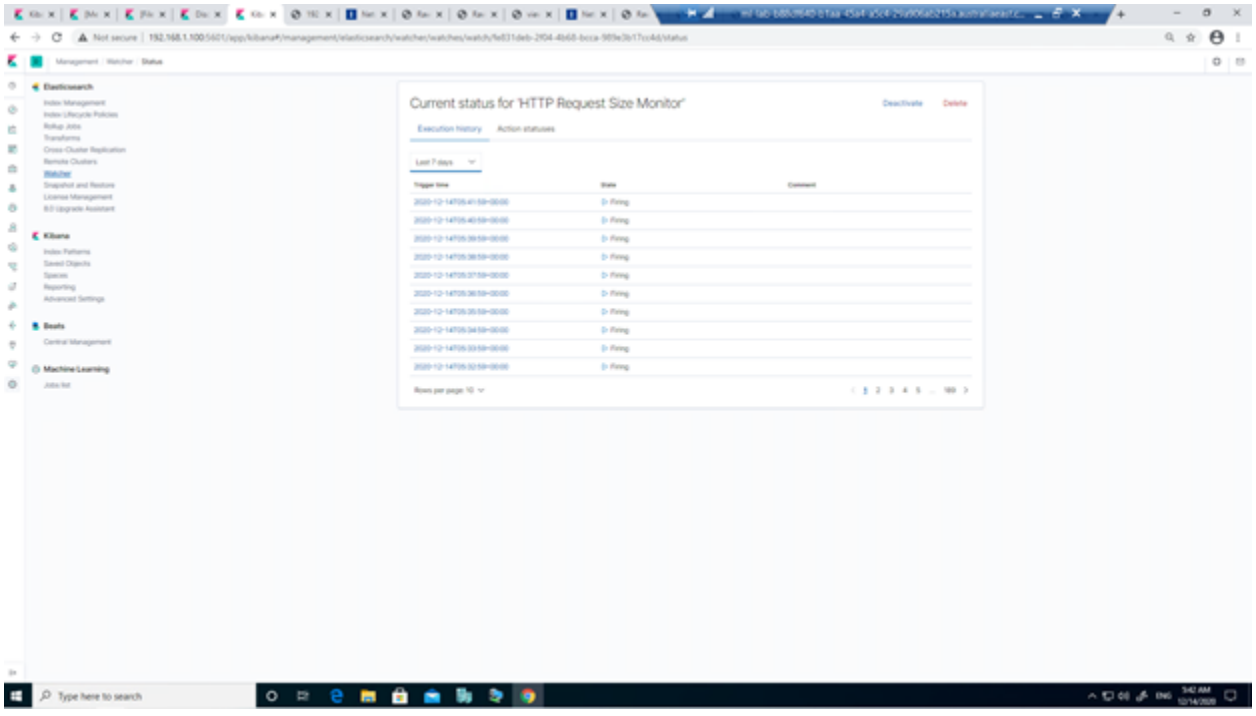


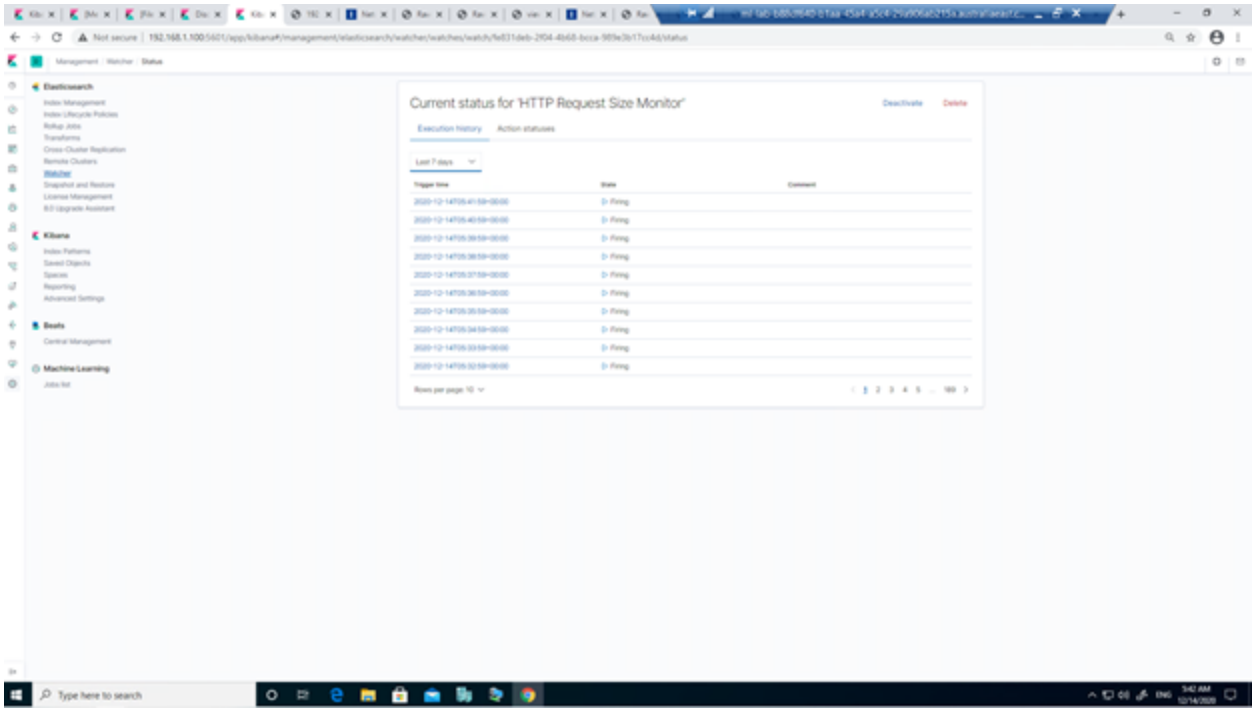

Watcher
Watcher docs
Watch for changes or anomalies in your data and take action if needed.
Create
CPU Usage Monitor
Excessive HTTP Errors
HTTP Request Size Monitor
Type here to search


Current status for 'CPU Usage Monitor'
Deactivate
Delete
Execution history
Action statuses
Type here to search



Vulnerability 3 . HTTP source code disclosure





Conclusion to reports done by: Darrel Mills Cybersecurity Specialist

Report was done by: Darrel Mills Cybersecurity Specialist

https://nvd.nist.gov/vuln/search

“Golden Nuggets”

By

Darrel Mills

We can start a revolution when we know what we stand against. Bad teams work in the same place. Good teams work together. To create change that lasts, we need to know what we stand for. The excitement comes from the achievement. Fulfillment comes from the journey that got you there. Our greatest test may not come from the path we travel to success. Our Greatest test is what we do with success once we find it. Leadership is not a rank or position to be attained. Leadership is a service to be given. Leadership is not about being in charge. Leadership is about taking care of those in your charge. Most of us live our lives by accident; we live as it happens. Fulfillment comes when we live our lives on purpose. May the Holy Spirit fill you with Volition and a “burning passion” to lead you; as you protect, mitigate, and defend, making each day a little safer place.

This Concludes the Defensive Blue Team Summary of Operations

By

Darrel Mills Blue_Team_SOC