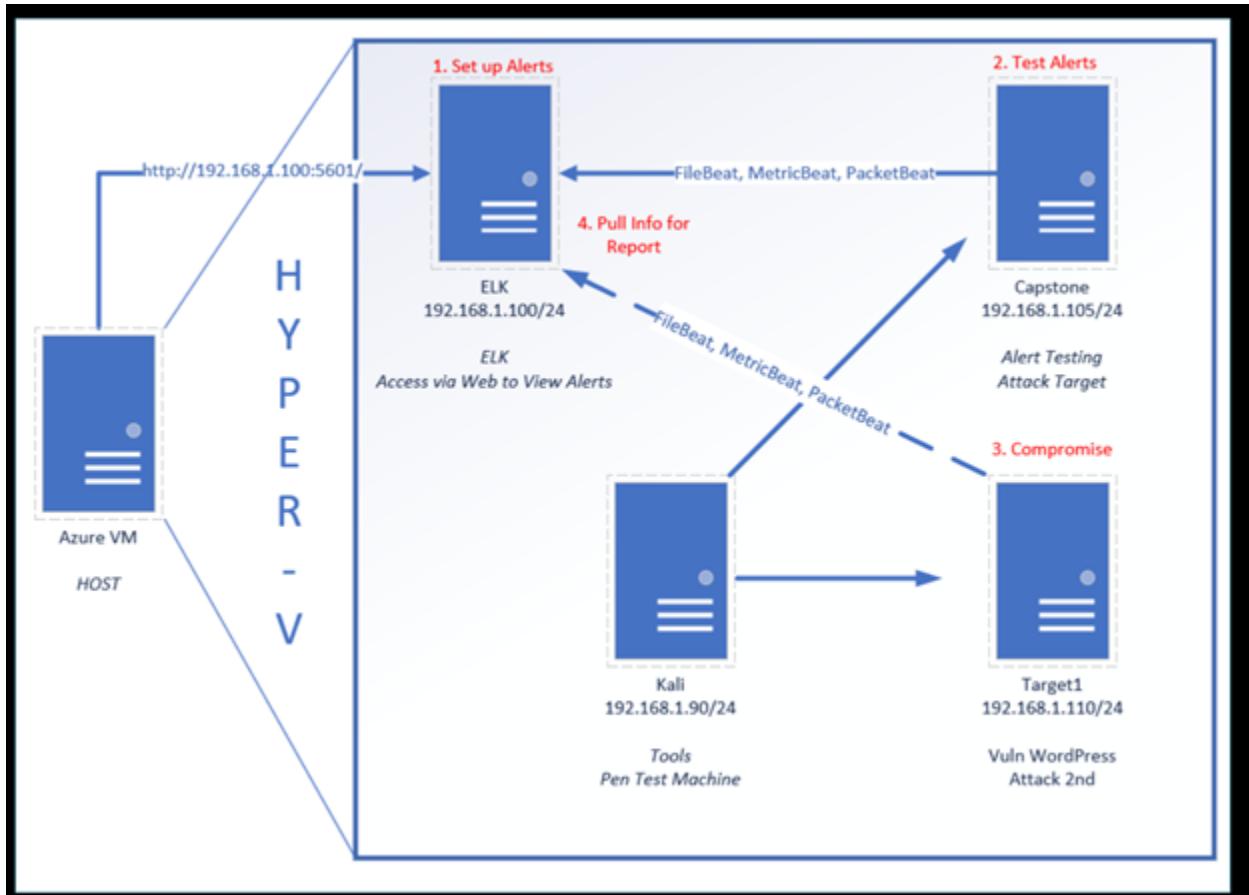


# Blue Team: Summary of Operations

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

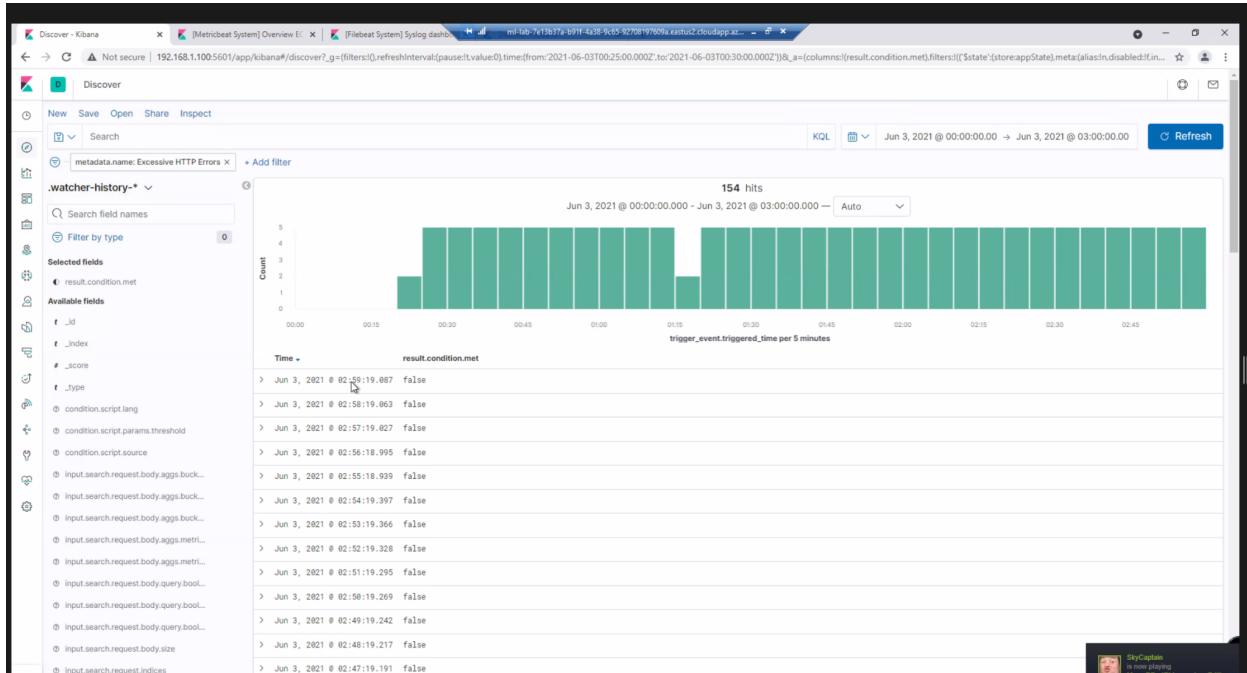
Alert 1 is implemented as follows: packetbeats

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



Current status for 'Excessive HTTP Errors'			Deactivate	Delete
Execution history		Action statuses		
<a href="#">Last 7 days</a>				
Trigger time	State	Comment		
2020-12-14T05:41:59+00:00	<span>▶ Firing</span>			
2020-12-14T05:36:59+00:00	<span>▶ Firing</span>			
2020-12-14T04:49:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:44:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:39:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:34:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:29:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:24:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:19:29+00:00	<span>▶ Firing</span>			
2020-12-14T04:14:29+00:00	<span>▶ Firing</span>			
Rows per page: 10				
◀ 1 2 3 4 5 ... 38 ▶				

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.**

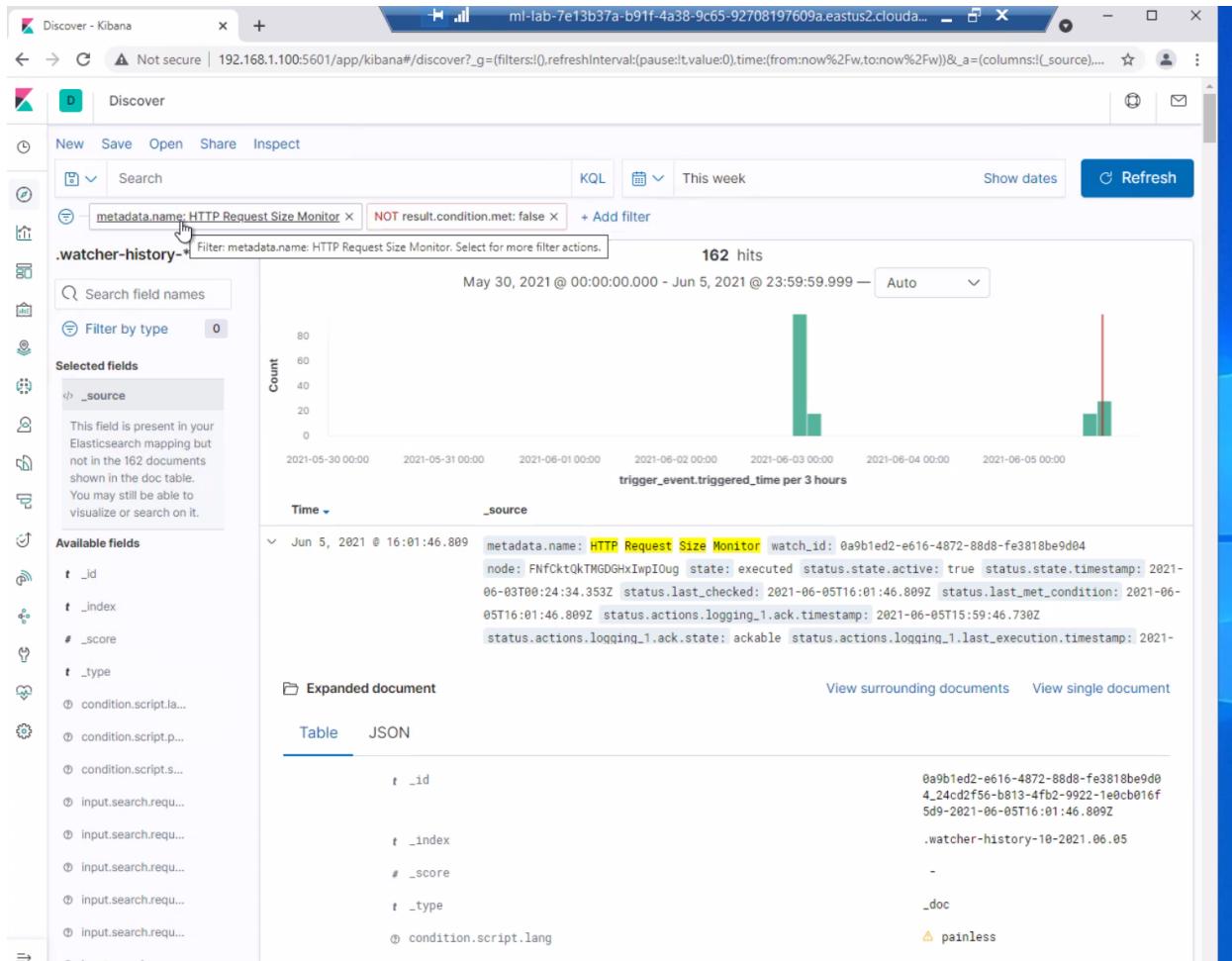
**Answer: And a high reliability for this alert is high due to the alert being triggered when there is a sudden influx bytes request because threshold is met**

Report was done by: Darrel Mills Cybersecurity Specialist

## CVE-2017-0777 OPEN SSH PORTS VULNERABLE

Current status for 'HTTP Request Size Monitor'			Deactivate	Delete
Execution history	Action statuses	Comment		
Last 7 days				
Trigger time	State	Comment		
2020-12-14T05:41:59+00:00	▶ Firing			
2020-12-14T05:40:59+00:00	▶ Firing			
2020-12-14T05:39:59+00:00	▶ Firing			
2020-12-14T05:38:59+00:00	▶ Firing			
2020-12-14T05:37:59+00:00	▶ Firing			
2020-12-14T05:36:59+00:00	▶ Firing			
2020-12-14T05:35:59+00:00	▶ Firing			
2020-12-14T05:34:59+00:00	▶ Firing			
2020-12-14T05:33:59+00:00	▶ Firing			
2020-12-14T05:32:59+00:00	▶ Firing			
Rows per page:	10		< 1 2 3 4 5 ... 189 >	

⌚	result.execution_ti...	t node
⌚	⌚ result.input.payload...	[:] result.actions
⌚	⌚ result.input.payload...	⌚ result.condition.met
⌚	⌚ result.input.payload...	t result.condition.status
⌚	⌚ result.input.payload...	t result.condition.type
⌚	⌚ result.input.payload...	# result.execution_duration
⌚	⌚ result.input.payload...	Jun 5, 2021 @ 16:02:46.836
⌚	⌚ result.input.payload...	⌚ result.execution_time
⌚	⌚ result.input.payload...	⌚ result.input.payload._shards.failed
⌚	⌚ result.input.payload...	⌚ result.input.payload._shards.skipped
⌚	⌚ result.input.payload...	⌚ result.input.payload._shards.successful
⌚	⌚ result.input.payload...	⌚ result.input.payload._shards.total
⌚	⌚ result.input.payload...	⌚ result.input.payload.aggregations.metricAgg.value
⌚	⌚ result.input.payload...	⌚ result.input.payload.hits.hits
⌚	⌚ result.input.payload...	⌚ result.input.payload.hits.max_score
⌚	⌚ result.input.payload...	⌚ result.input.payload.hits.total
⌚	⌚ result.input.payload...	⌚ result.input.payload.timed_out
⌚	⌚ result.input.payload...	⌚ result.input.payload.took
⌚	⌚ result.input.search...	⌚ result.input.search.request.body.aggs.metricAgg.sum.field
⌚	⌚ result.input.search...	⌚ result.input.search.request.body.query.bool.filter.range.timestamp.format
⌚	⌚ result.input.search...	strict_date_optional_time  epoch_millis
⌚	⌚ result.input.search...	⌚ result.input.search.request.body.query.bool.filter.range.timestamp.gte
⌚	⌚ result.input.search...	2021-06-05T16:02:46.530Z -1m
⌚	⌚ result.input.search...	⌚ result.input.search.request.body.query.bool.filter.range.timestamp.lte
⌚	⌚ result.input.search...	2021-06-05T16:02:46.530Z
⌚	⌚ result.input.search...	⌚ result.input.search.request.body.size
⌚	⌚ result.input.search...	t result.input.search.request.indices
⌚	⌚ result.input.search...	⌚ result.input.search.request.rest_total_hits_as_int
⌚	⌚ result.input.search...	true
⌚	⌚ result.input.search...	⌚ result.input.search.request.search_type
⌚	⌚ result.input.search...	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**

Current status for 'CPU Usage Monitor'

Execution history Action statuses

Last 7 days

Trigger time	State	Comment
2020-12-14T05:41:59+00:00	▷ Firing	
2020-12-14T05:36:59+00:00	▷ Firing	
2020-12-14T04:49:29+00:00	▷ Firing	
2020-12-14T04:44:29+00:00	▷ Firing	
2020-12-14T04:39:29+00:00	▷ Firing	
2020-12-14T04:34:29+00:00	▷ Firing	
2020-12-14T04:29:29+00:00	▷ Firing	
2020-12-14T04:24:29+00:00	▷ Firing	
2020-12-14T04:19:29+00:00	▷ Firing	
2020-12-14T04:14:29+00:00	▷ Firing	

Rows per page: 10 < 1 2 3 4 5 ... 38 >

Discover

New Save Open Share Inspect

Search NOT result.condition.met: false result.condition.met: true + Add filter

KQL Jun 5, 2021 @ 15:30:00.000 → Jun 5, 2021 @ 16:00:00.000 Refresh

.watcher-history-\*

Count Jun 5, 2021 @ 15:30:00.000 - Jun 5, 2021 @ 16:00:00.000 — Auto 8 hits

Time \_source

Jun 5, 2021 @ 15:46:40.378 watch\_id: dd858150-68f7-4765-ae09-357c02ac90d8 node: FNFCkt0kTMGDGhIepIOg state: executed status.state.active: true status.state.timestamp: 2021-06-03T00:22:46.948Z status.last\_checked: 2021-06-05T15:46:40.378Z status.last\_met\_condition: 2021-06-05T15:46:40.378Z status.actions.logging\_1.ack.state: ackable status.actions.logging\_1.last\_execution.timestamp: 2021-06-05T15:46:40.378Z status.actions.logging\_1.last\_successful\_execution.timestamp: 2021-06-05T15:46:40.378Z status.actions.logging\_1.last\_successful\_execution.successful: true status.actions.logging\_1.last\_successful\_execution.timestamp: 2021-06-05T15:46:40.378Z status.actions.logging\_1.last\_successful\_execution.successful: true status.execution\_state: executed status.version: -1 trigger\_event.type: schedule trigger\_event.triggered\_time: Jun 5, 2021 @ 15:46:40.378Z

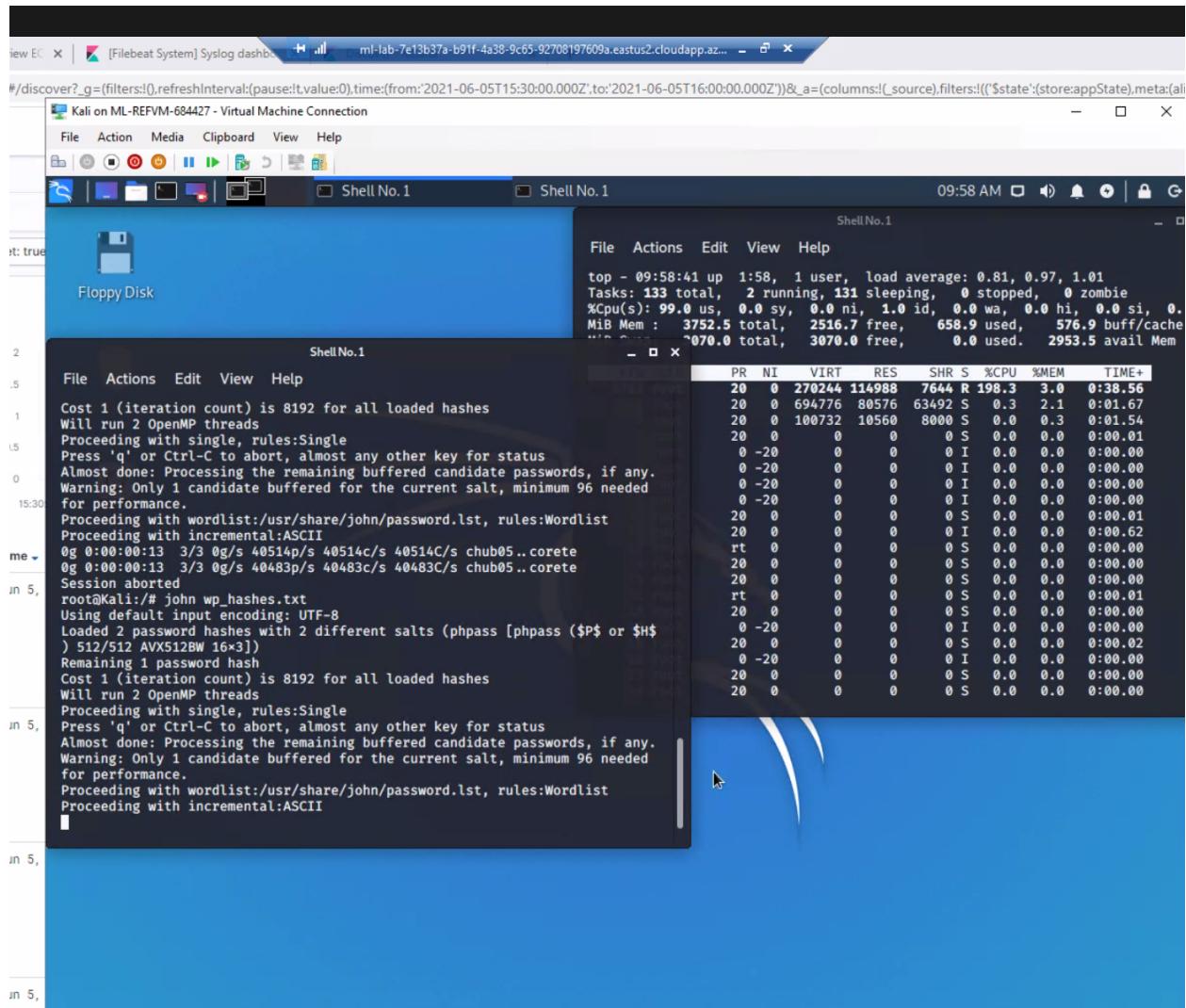
Expanded document

Table JSON

\_id \_index \_score \_type condition.script.lang condition.script.params.threshold condition.script.source input.search.request.body.aggs.bucket... input.search.request.body.aggs.bucket... input.search.request.body.aggs.meter... input.search.request.body.aggs.meter... input.search.request.body.query.bool... input.search.request.body.query.bool... input.search.request.body.query.bool... input.search.request.body.query.bool... input.search.request.body.size

dd858150-68f7-4765-ae09-357c02ac90d8\_8af5e846-eca0-41b0-923d-bc03120e3d1e-2021-06-05T15:46:40.378Z .watcher-history-10-2021.06.05 - \_doc painless 400 ArrayList arr = ctx.payload.aggregations.bucketApp.buckets; for (int i = 0; i < arr.length; i++) { if (arr[i].d

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

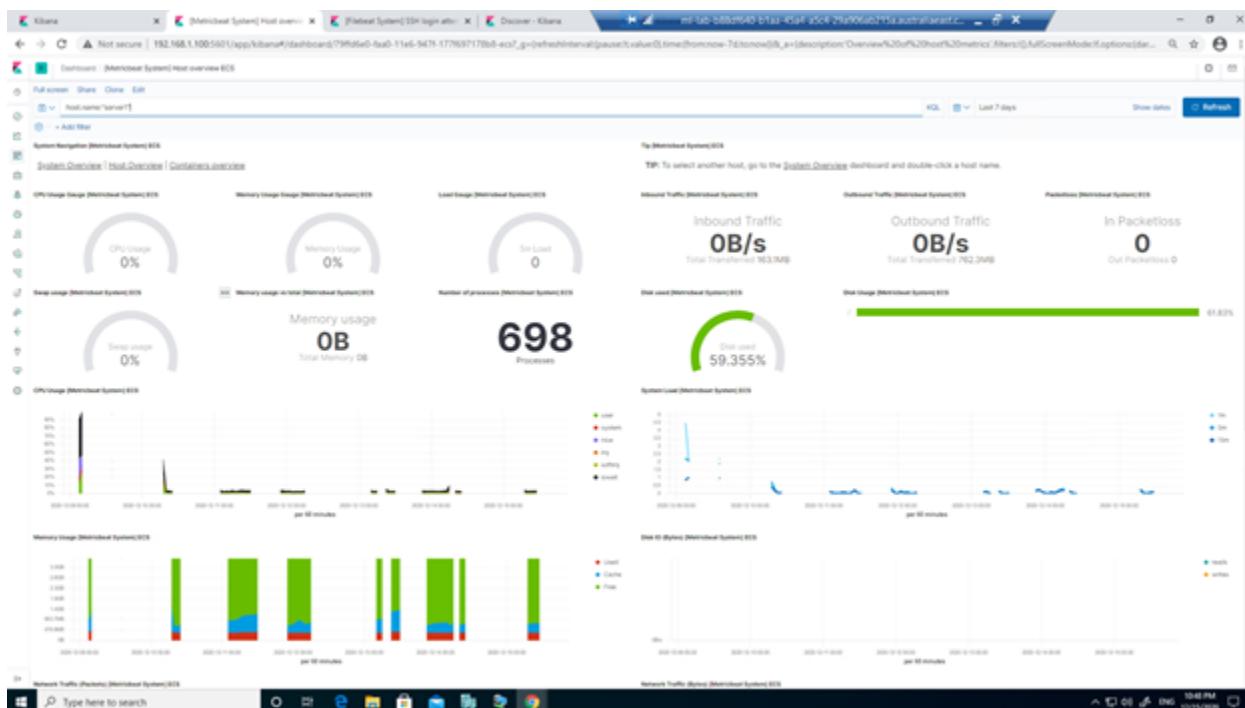
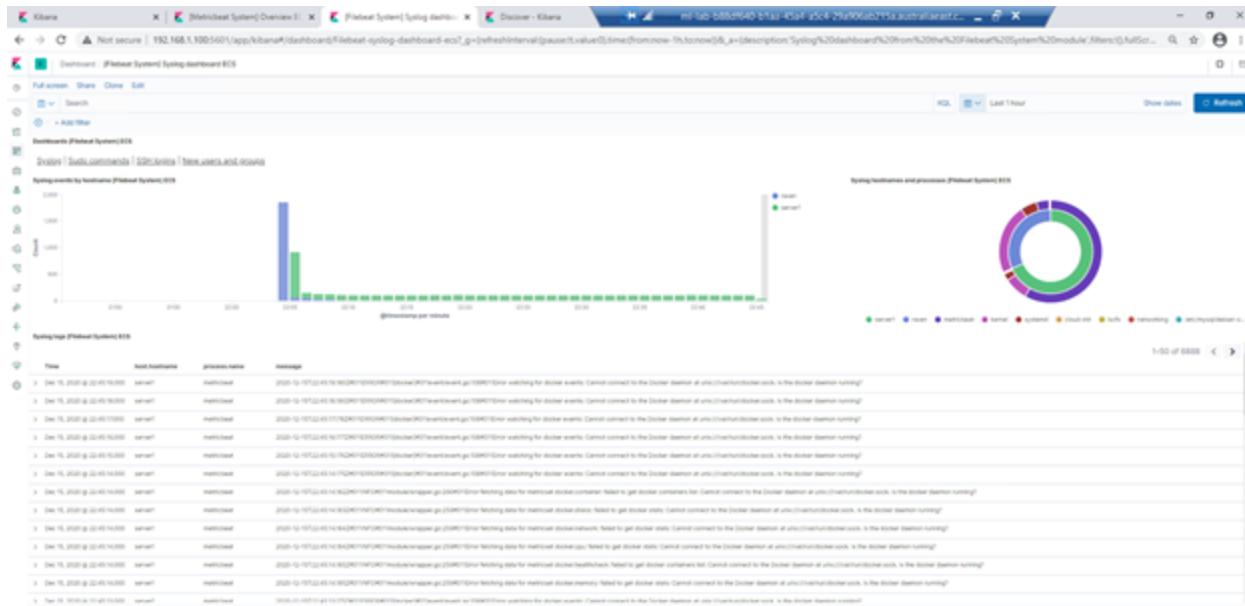
<https://wordpress.org/support/article/updating-wordpress/#one-click-update> or [https://wordpress.org/download/to\\_install](https://wordpress.org/download/to_install)

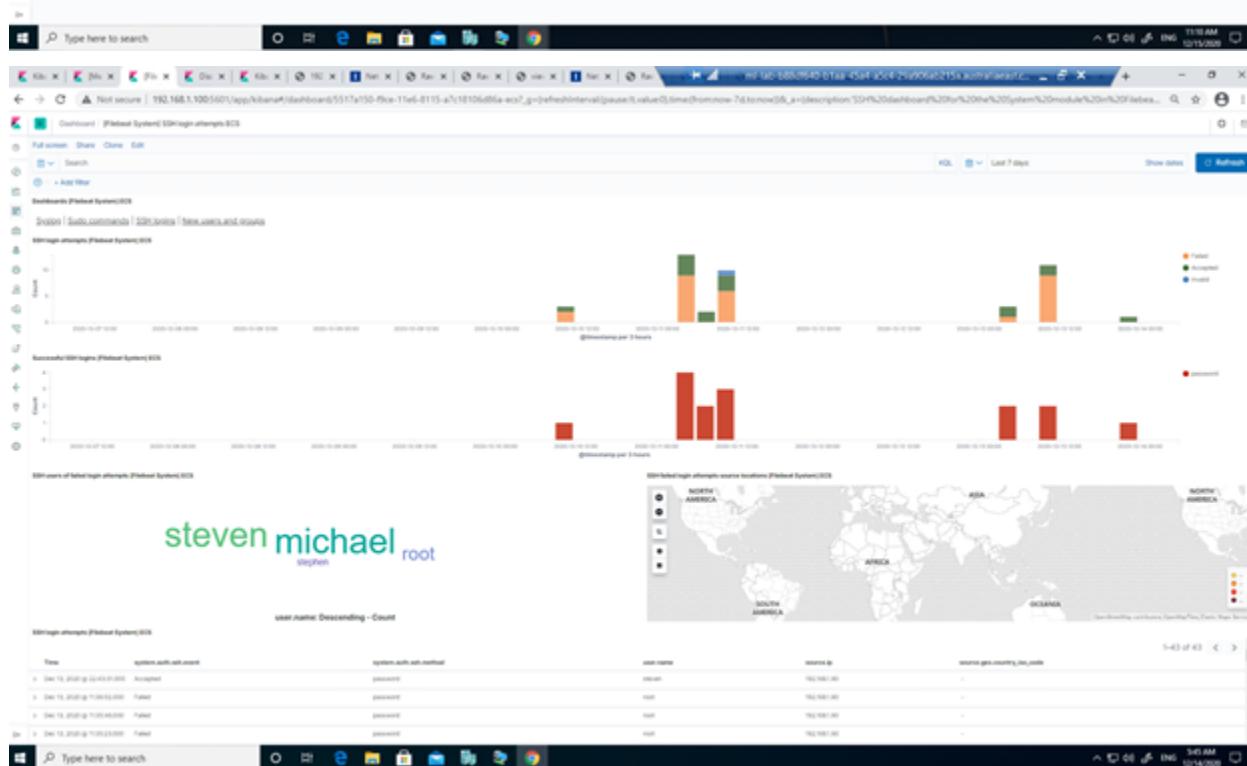
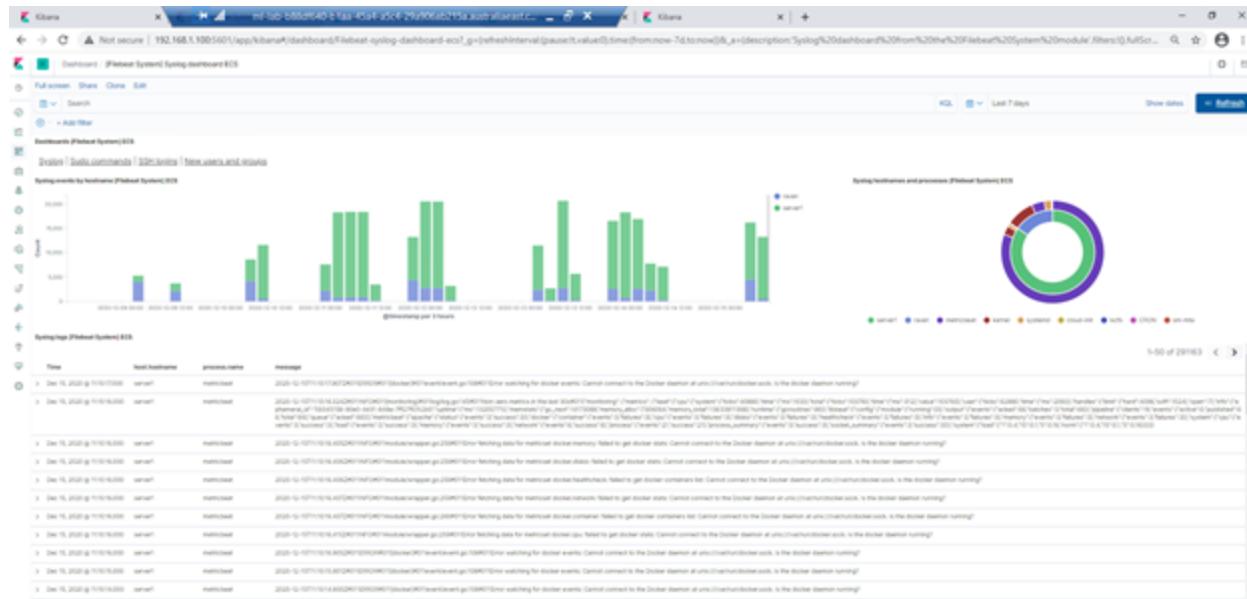
- **Why It Works\*\*:**

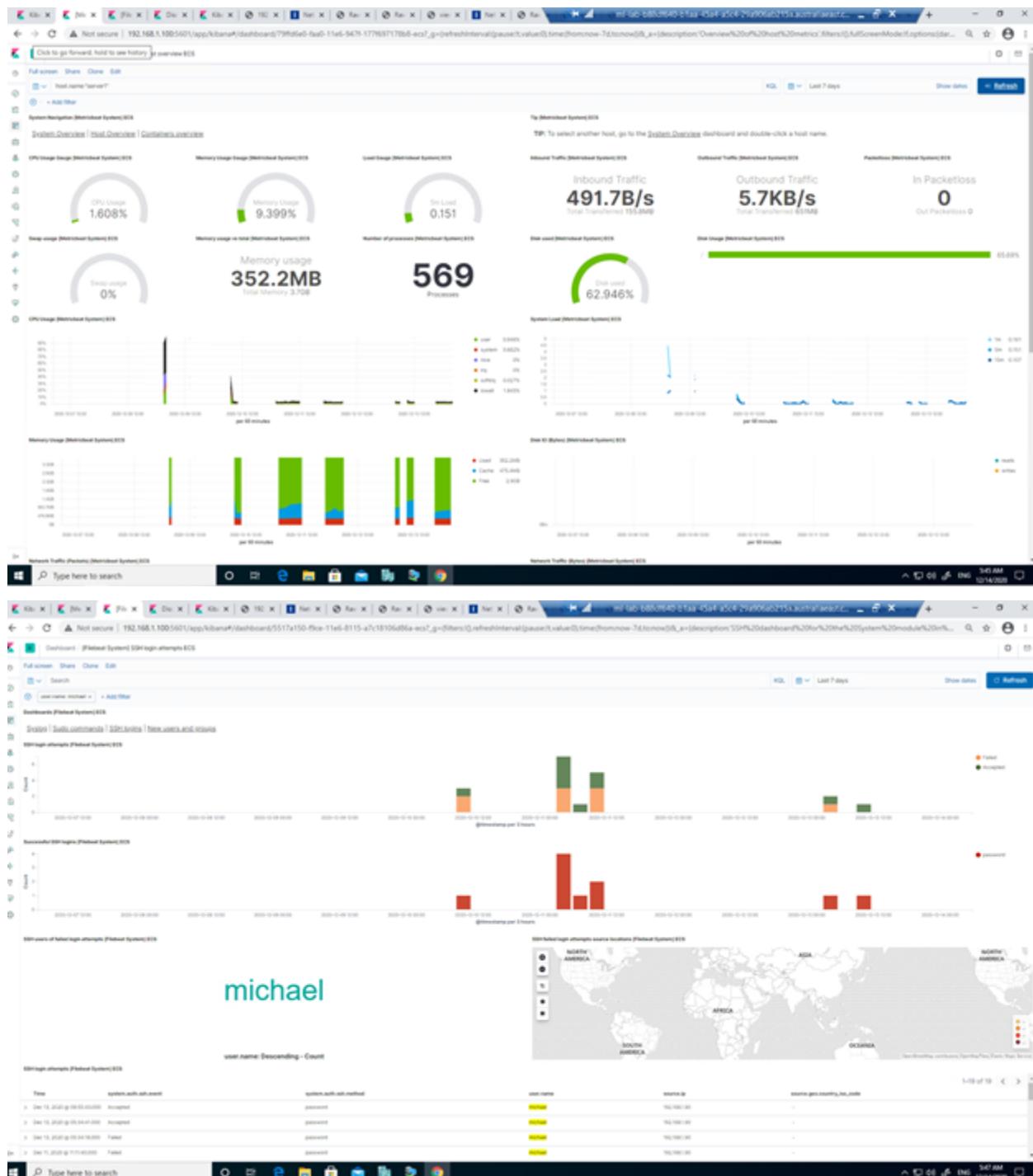
Report was done by: Darrel Mills Cybersecurity Specialist

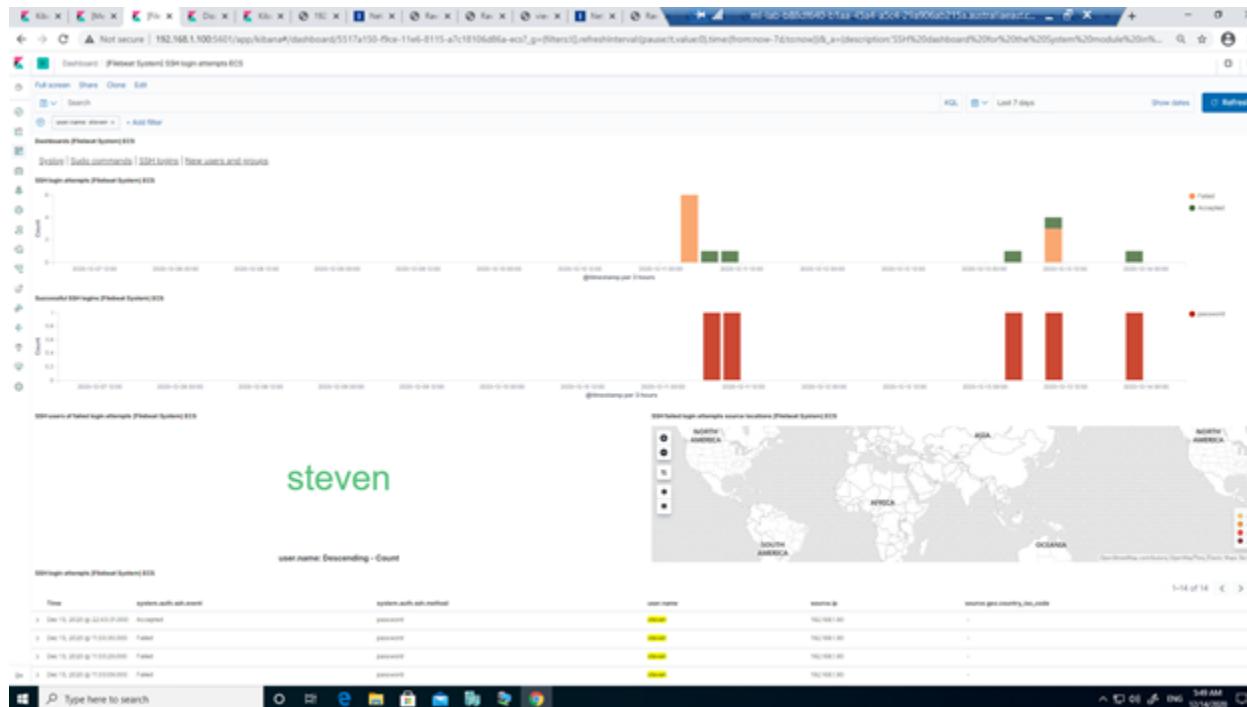
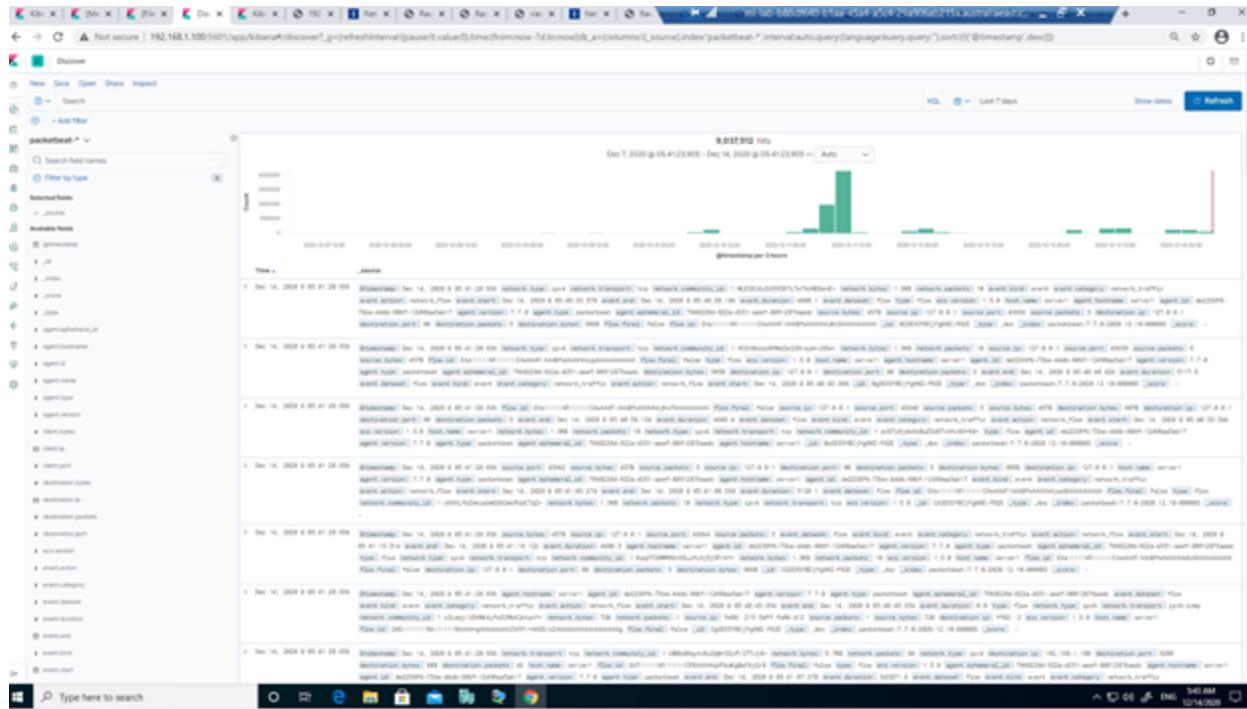
**Answer:** It is very important to update all critical infrastructure and company software, including WordPress, should be done on a regular basis. Company policy establishes that all assets are checked for updates either weekly, or monthly.checking,

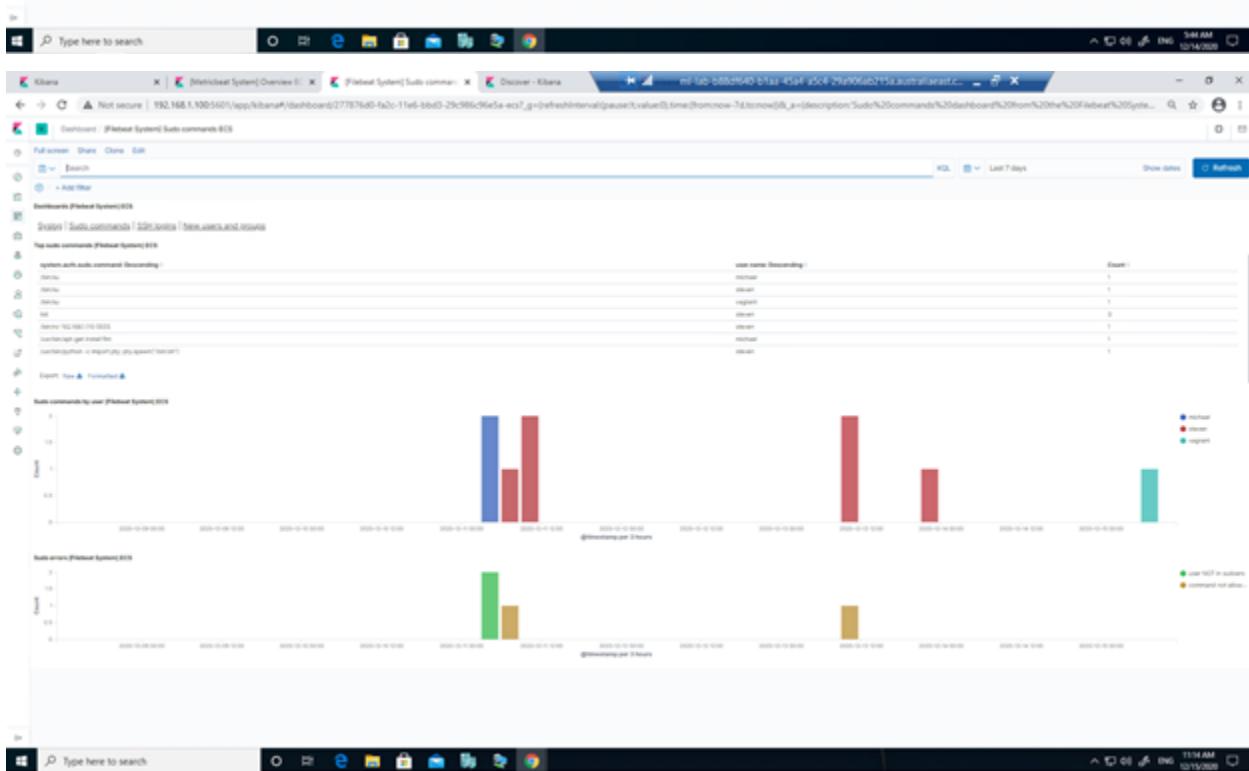
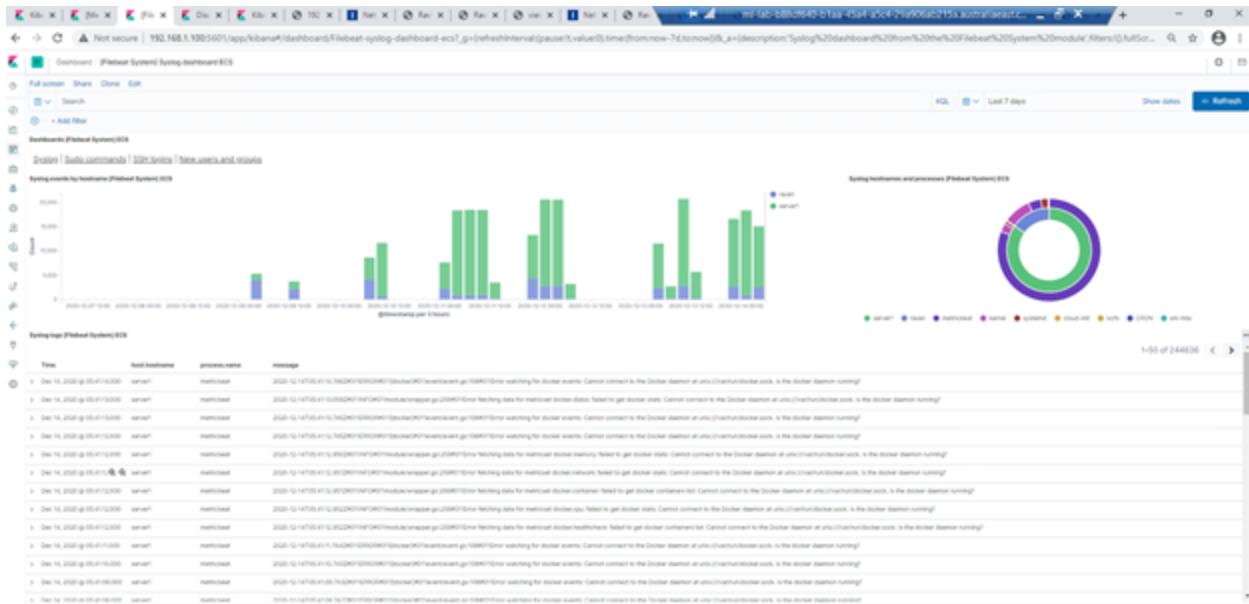
- Screenshot as evidence











Not secure | 192.168.1.100:5601/app/kibana#/management/elasticsearch/watcher/watchers/\_list/\_go

### Watcher

Watch for changes or anomalies in your data and take action if needed.

	Name	Status	Last fired	Last triggered	Comment	Action	
94423217-95be-4b5d-4320- a6e8d958c1f0	CPU Usage Monitor	Fire	5 minutes ago	5 minutes ago			
9477a0a0-344b-4884-9052- ef1275e62820	Excessive HTTP Errors	Fire	5 minutes ago	5 minutes ago			
9477a0a0-344b-4884-9052- ef1275e62820	HTTP Request Size Monitor	Fire	a minute ago	a minute ago			

Rows per page: 10 < >

Management Watcher

- Elasticsearch
- Kibana
- Beats
- Machine Learning

Not secure | 192.168.1.100:5601/app/kibana#/management/elasticsearch/watcher/watch/94423217-95be-4b5d-4320-  
a6e8d958c1f0/status/\_list/\_go

### Current status for 'CPU Usage Monitor'

Execution history	Action statuses	Deactivate	Delete
Last 7 days			
Trigger time	Status	Comment	
2020-12-14T08:41:00+0000	Fire		
2020-12-14T08:36:00+0000	Fire		
2020-12-14T04:49:00+0000	Fire		
2020-12-14T04:44:00+0000	Fire		
2020-12-14T04:39:00+0000	Fire		
2020-12-14T04:34:00+0000	Fire		
2020-12-14T04:29:00+0000	Fire		
2020-12-14T04:24:00+0000	Fire		
2020-12-14T04:19:00+0000	Fire		
2020-12-14T04:14:00+0000	Fire		

Rows per page: 10 < 1 2 3 4 5 ... 38 >

Type here to search

Management Watcher Status

- Elasticsearch
- Kibana
- Beats
- Machine Learning

Not secure | 192.168.1.100:5601/app/kibana#/management/elasticsearch/watcher/watch/94423217-95be-4b5d-4320-  
a6e8d958c1f0/\_list/\_go

The screenshot shows the Elasticsearch Management interface with the 'Watcher' section selected. A table titled 'Current status for "Excessive HTTP Errors"' displays the following data:

Trigger time	State	Comment
2020-12-14T05:41:09+0000	▶ Pending	
2020-12-14T05:36:09+0000	▶ Pending	
2020-12-14T04:49:29+0000	▶ Pending	
2020-12-14T04:44:29+0000	▶ Pending	
2020-12-14T04:36:29+0000	▶ Pending	
2020-12-14T04:34:09+0000	▶ Pending	
2020-12-14T04:29:09+0000	▶ Pending	
2020-12-14T04:24:29+0000	▶ Pending	
2020-12-14T04:19:09+0000	▶ Pending	
2020-12-14T04:14:09+0000	▶ Pending	

At the bottom, there are buttons for 'Deactivate' and 'Delete', and a pagination control showing pages 1 through 30.

## Vulnerability 3 . HTTP source code disclosure

The screenshot shows the Elasticsearch Management interface with the 'Watcher' section selected. A table titled 'Current status for "HTTP Request Size Monitor"' displays the following data:

Trigger time	State	Comment
2020-12-14T05:41:09+0000	▶ Pending	
2020-12-14T05:40:19+0000	▶ Pending	
2020-12-14T05:39:09+0000	▶ Pending	
2020-12-14T05:38:09+0000	▶ Pending	
2020-12-14T05:37:09+0000	▶ Pending	
2020-12-14T05:36:09+0000	▶ Pending	
2020-12-14T05:35:09+0000	▶ Pending	
2020-12-14T05:34:09+0000	▶ Pending	
2020-12-14T05:33:09+0000	▶ Pending	
2020-12-14T05:32:09+0000	▶ Pending	

At the bottom, there are buttons for 'Deactivate' and 'Delete', and a pagination control showing pages 1 through 100.



Trigger time	Status	Comment
2020-12-14T05:41:59+0000	Pending	
2020-12-14T05:40:59+0000	Pending	
2020-12-14T05:39:59+0000	Pending	
2020-12-14T05:38:59+0000	Pending	
2020-12-14T05:37:59+0000	Pending	
2020-12-14T05:36:59+0000	Pending	
2020-12-14T05:35:59+0000	Pending	
2020-12-14T05:34:59+0000	Pending	
2020-12-14T05:33:59+0000	Pending	
2020-12-14T05:32:59+0000	Pending	

## 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**