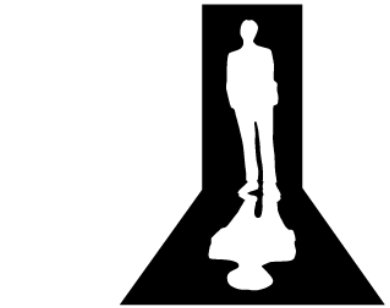


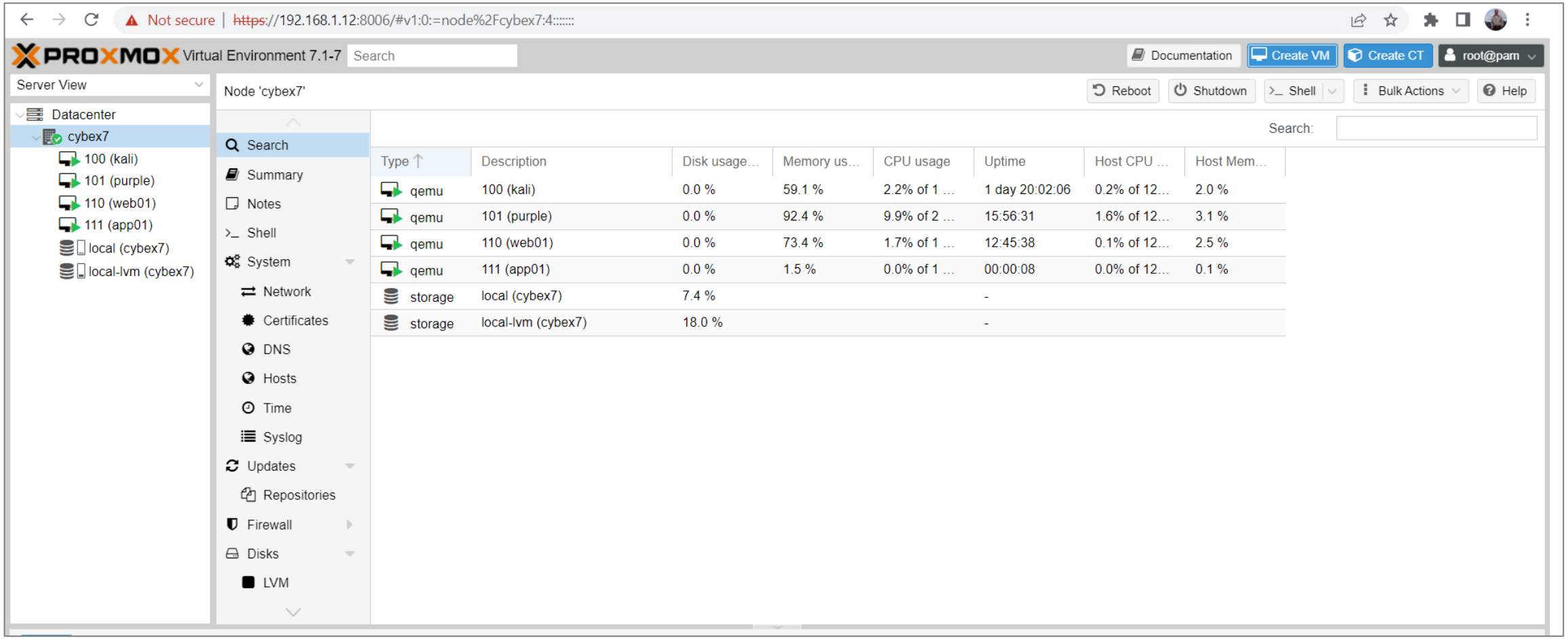

# SOC200 CHALLENGE LAB
# ADVERSARY VILLAGE

# WORKSHOP LAB

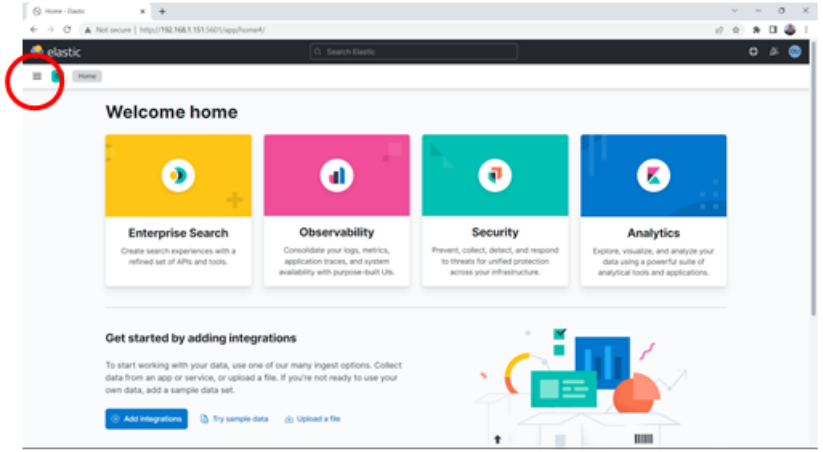
Intel NUC Platform  (12 cpu  64Gb/512Gb)

| | | |
|---|---|---|
| proxmox | VMM | https://192.168.1.12:8006 |
| kali | Attacker | |
| purple | SIEM | https://192.168.1.101:5601 |
| web01 | DMZ Proxy server and web | |
| app01 | Internal applications server | |

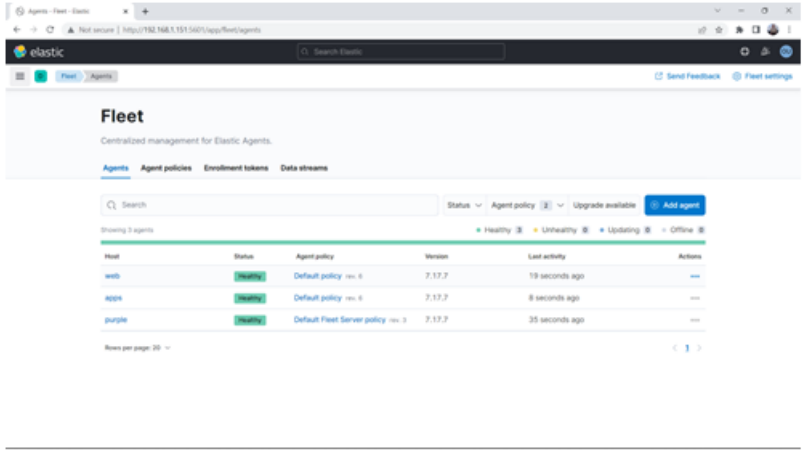
## FOR MORE INFORMATION OR TO GIVE FEEDBACK


Not secure | https://192.168.1.12:8006/#v1:0:=node%2Fcybex7:4::::::
PROXMOX Virtual Environment 7.1-7
Search
Documentation
Create VM
Create CT
root@pam
Server View
Node 'cybex7'
Reboot
Shutdown
Shell
Bulk Actions
Help
Datacenter
cybex7
100 (kali)
101 (purple)
110 (web01)
111 (app01)
local (cybex7)
local-lvm (cybex7)
Search
Summary
Notes
Shell
System
Network
Certificates
DNS
Hosts
Time
Syslog
Updates
Repositories
Firewall
Disks
LVM
Search:
Type
Description
Disk usage...
Memory us...
CPU usage
Uptime
Host CPU ...
Host Mem...
qemu 100 (kali) 0.0 % 59.1 % 2.2% of 1 ... 1 day 20:02:06 0.2% of 12... 2.0 %
qemu 101 (purple) 0.0 % 92.4 % 9.9% of 2 ... 15:56:31 1.6% of 12... 3.1 %
qemu 110 (web01) 0.0 % 73.4 % 1.7% of 1 ... 12:45:38 0.1% of 12... 2.5 %
qemu 111 (app01) 0.0 % 1.5 % 0.0% of 1 ... 00:00:08 0.0% of 12... 0.1 %
storage local (cybex7) 7.4 % -
storage local-lvm (cybex7) 18.0 % -

# USING THE SIEM



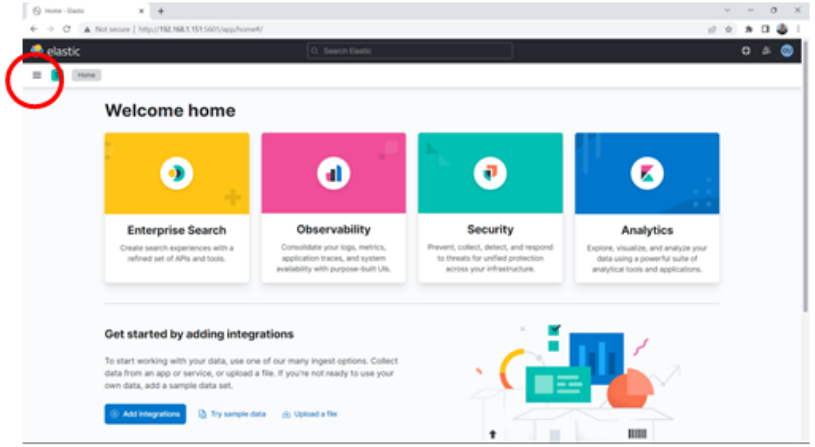

Click and select Management > Fleet



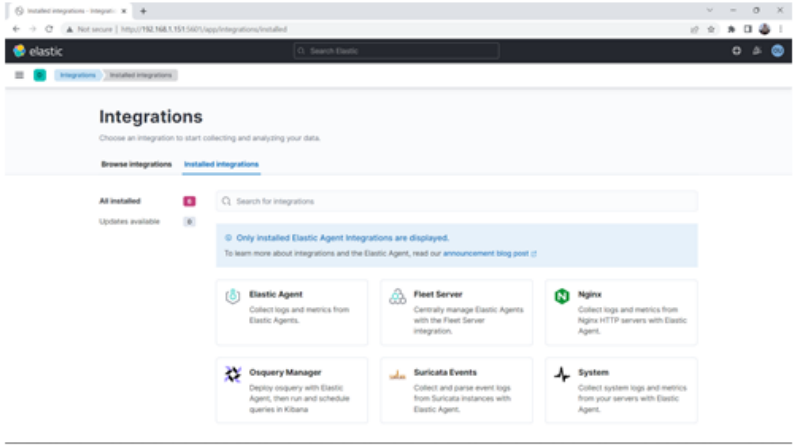

Here we see the hosts being monitored

# WHAT IS A SIEM??

A SIEM collects logs from hosts being monitored and presents them for review. It provides search capabilities and  may also allow searches to be stored for regular use as alerts.  The ELK SIEM uses the term “Integrations” to mean the set of logs it collects.  For example, the *System* integration is the basic system logs (syslogs). On Linux these are in /var/log/syslog, on Windows hosts, we use Sysmon to generate syslogs. ELK also has some special logs it knows about such as *Nginx* proxy logs and Suricata IDS events.




Click and select Management > Integrations

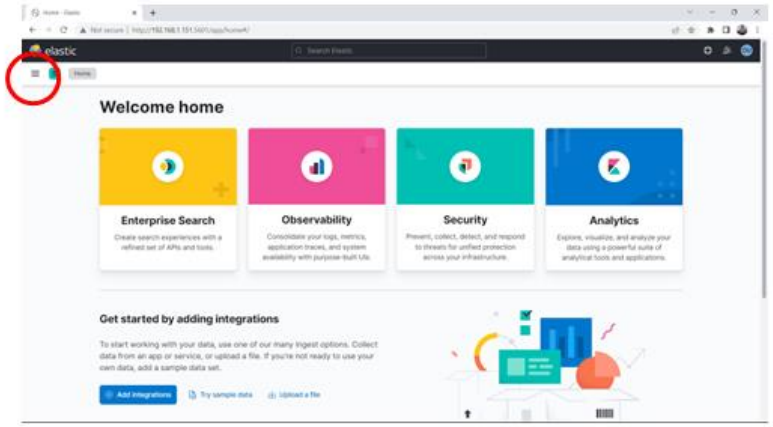



Here we see the log sets being collected

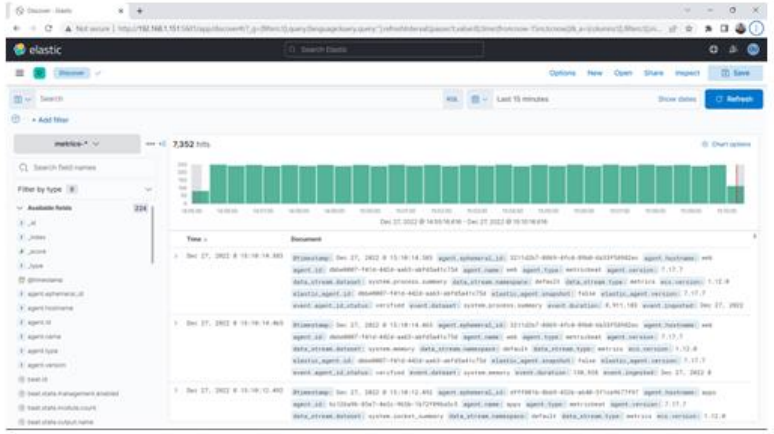
# HOW DO WE MONITOR LOGS?

ELK provides a monitoring screen which we get to by selecting *Discover*. Below the top Ribbon is the main SOC Analyst search controls. We can enter a search in Kibana Query Language (KQL) in the left hand box and can set the time period of what we see below in the right hand panel. If we make changes we press *Refresh* to apply them.

The left hand lower panel provides the list of fields that can be used for searching and for the log display. Note there are two main kinds of logs that ELK collects: metrics and logs. We need to select *logs-**




Click and select Discover

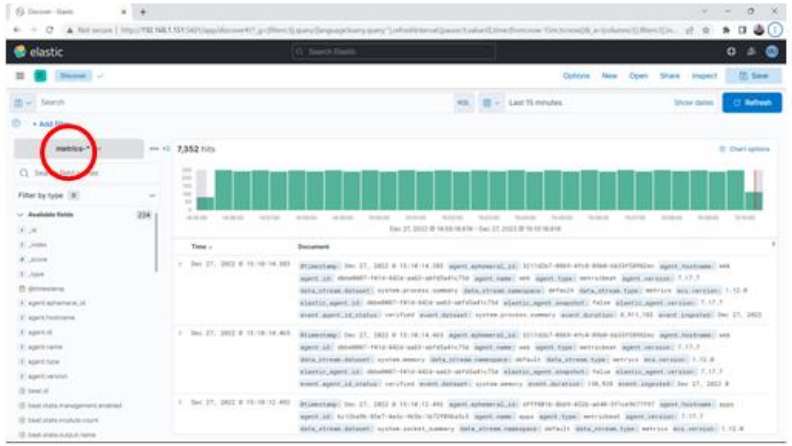



Here we see the logs that have been collected

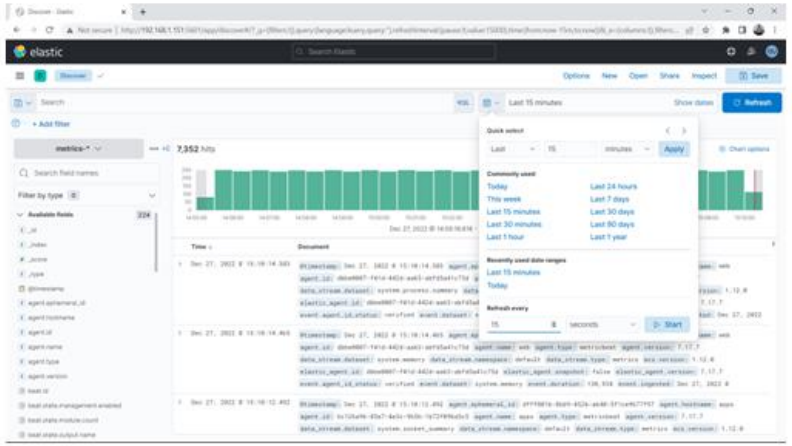
# REAL TIME MONITORING

In a production environment many millions of logs are collected every hour so looking for individual logs is problematic. An analyst has two key strategies: he/she can watch logs as they are being collected and look for changes in traffic patterns that might indicate an event of interest; or they can monitor alerts which have been set up in advance to detect certain types of log.  One form of event which is useful to monitor is IDS alerts which flag known malware or suspicious traffic.

To set the Discover screen into real time mode, select the clock dropdown, set the refresh rate, and press *Start*.



Click and select logs-*



Click the clock and change to 15 seconds, then press Start

# WHAT ARE WE LOOKING FOR?

There are two forms of *detection*: signature detection, where the signature of a known piece of malware is detected; and anomaly detection, where something out of the pattern of normal behaviour is detected.

The approach for this workshop is to:

(a) Understand the normal traffic flow

(b) Watch for changes in the pattern of traffic which may be an “anomaly”

(c) Check logs from the start of the anomaly to determine what is happening

(d) As we begin to understand an anomaly, refine our search to anomaly-specific logs of interest

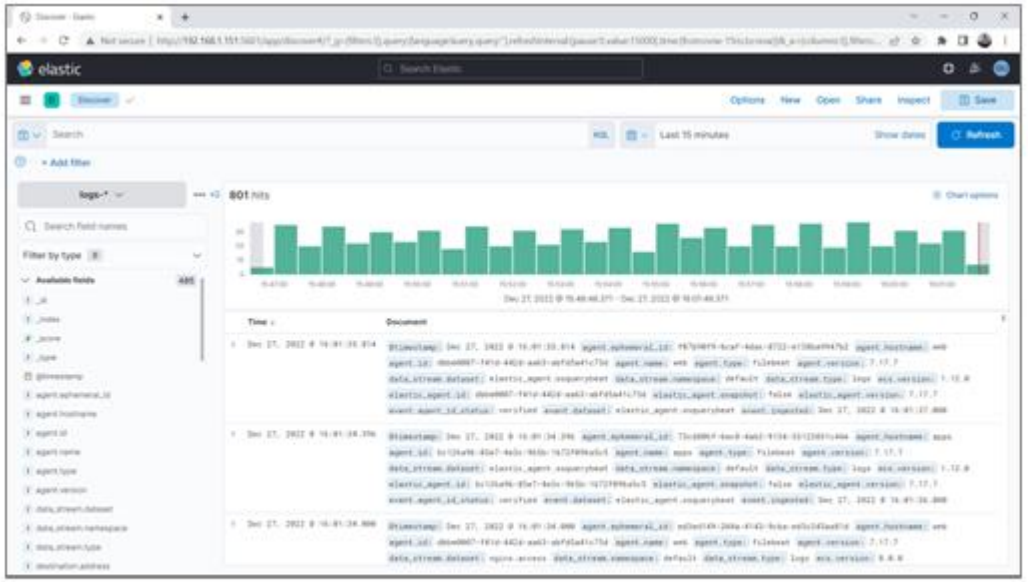
(e) Check logs for specific indicators of attack

(f) Always focus on minimizing the number of logs we have to manually check

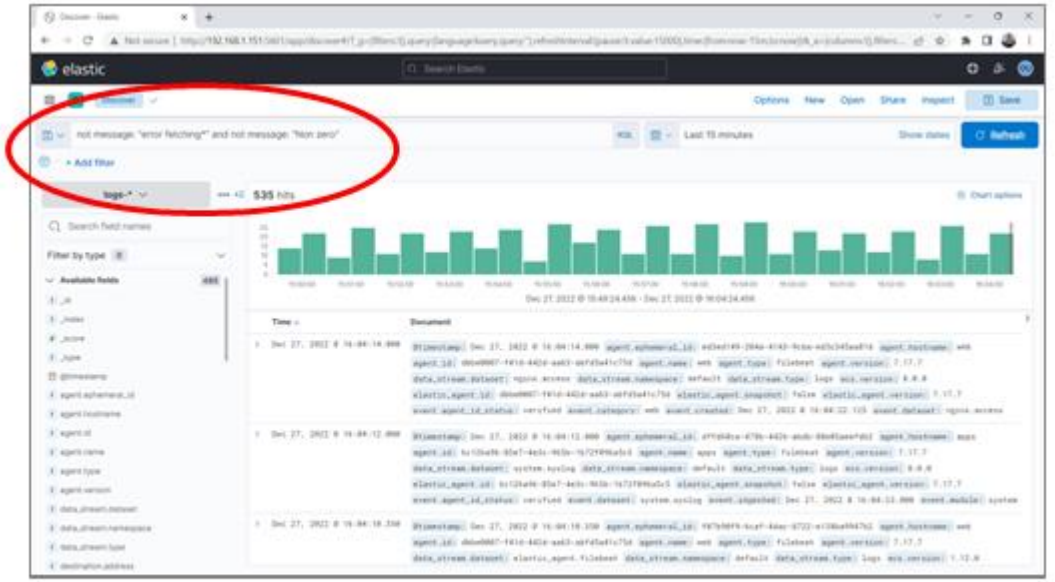
# REMOVING NOISE

Some log events are routine and we can ignore them.  It is useful to filter them out with a search.  In this example we have checked logs and identified some routine logs which are not of interest

not message: (“Error fetching*” or “Non zero”)



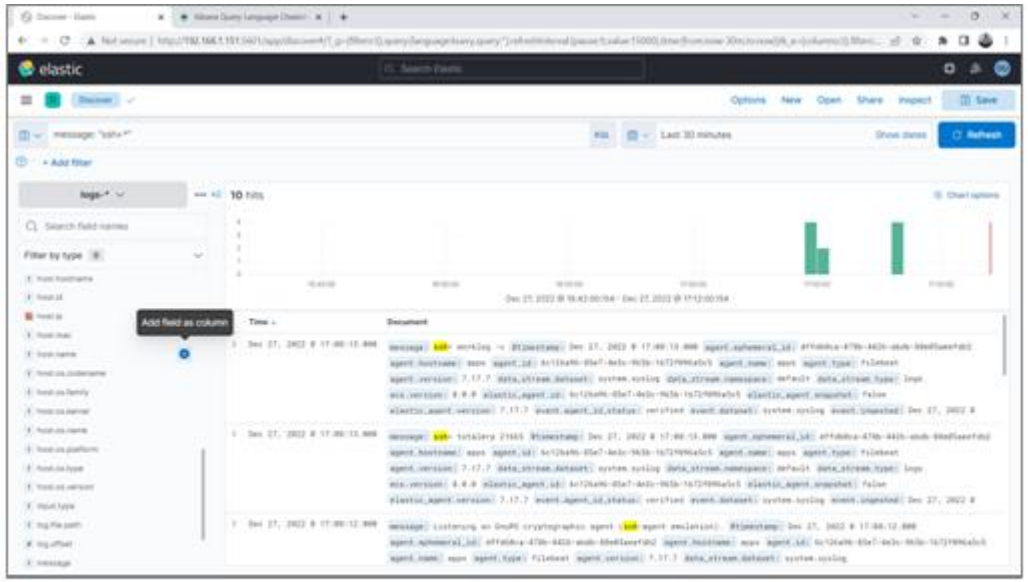
Noisy display



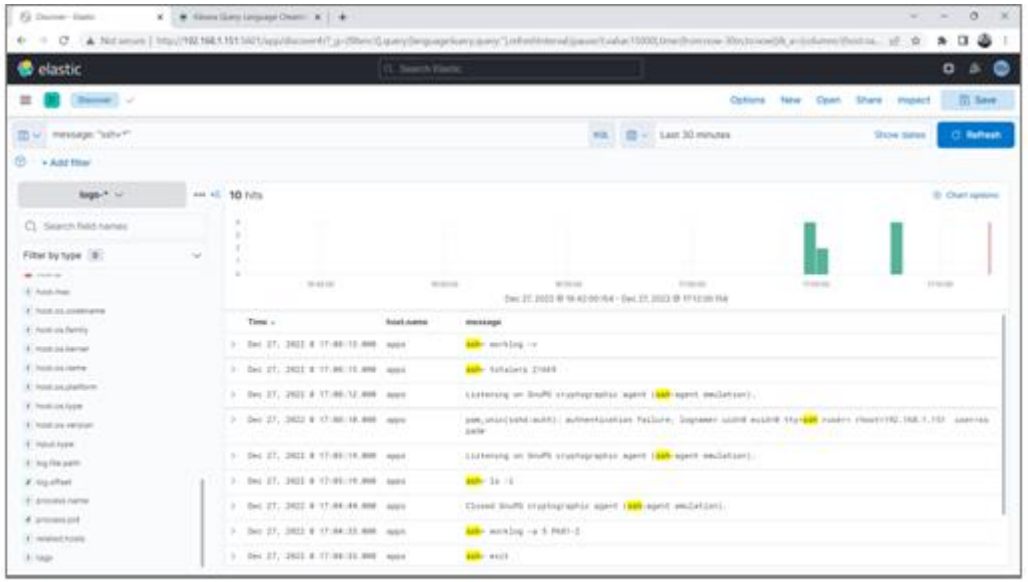
Removing noise

# FOCUSING OUTPUT

The default log display provides a lot of information, most of which we don't need. Using the field list on the left, click the plus symbol to add fields to the log display line.  If you decide you don't want a field, remove the field from the *Select Fields* list.  If you remove all selected fields, the default display will be used.




Default display




Field-focused display

# KIBANA QUERY LANGUAGE

KQL uses the field names that have been defined for the logs in the form of:

*fieldname: value*

*not fieldname: value*

Multiple expressions connected with *and* or *or*

logit.io

Kibana Cheat Sheet

**Term Search**

| | |
|---|---|
| **Keywords,** e.g. United Kingdom | Will return results containing the words 'United' and/or 'Kingdom'. |
| **Phrase,** e.g. "United Kingdom" | Returns results where the words 'United Kingdom' are presented together. |
| **OR keyword,** e.g. United OR Kingdom | Returns results where either the words 'United' **or** 'Kingdom' are present. |
| **AND keyword,** e.g. United AND Kingdom | Returns results where the words 'United' **and** 'Kingdom' are both present. |
| **+ keyword,** e.g. "United" +Kingdom | Returns results that contain the words 'United' but must also contain the word 'Kingdom'. |
| **- keyword,** e.g. "United" -Kingdom | Returns results that contain the words 'United' but must not include the word 'Kingdom'. |

**Field Search**

| | |
|---|---|
| **Field Search,** e.g. message: logit.io | Will return results that contain 'logit.io' under the field named 'message'. |
| **Field and Term OR,** e.g. message:(United or Kingdom) | Returns results containing either 'United' OR 'Kingdom' under the field named 'message'. |
| **Field and Term AND,** e.g. message:(United and logit.io) | Returns results containing 'United' and 'logit.io' under the field named 'message'. |
| **Exact Phrase Match,** e.g. message:"United Kingdom" | Returns results where the words 'United Kingdom' are presented together under the field named 'message'. |
| **_EXISTS_** e.g. _exists_:message AND NOT message:kingdom | Returns results with the field named 'message' but does not include results where the value 'kingdom' exists. |

**Wildcard Search**

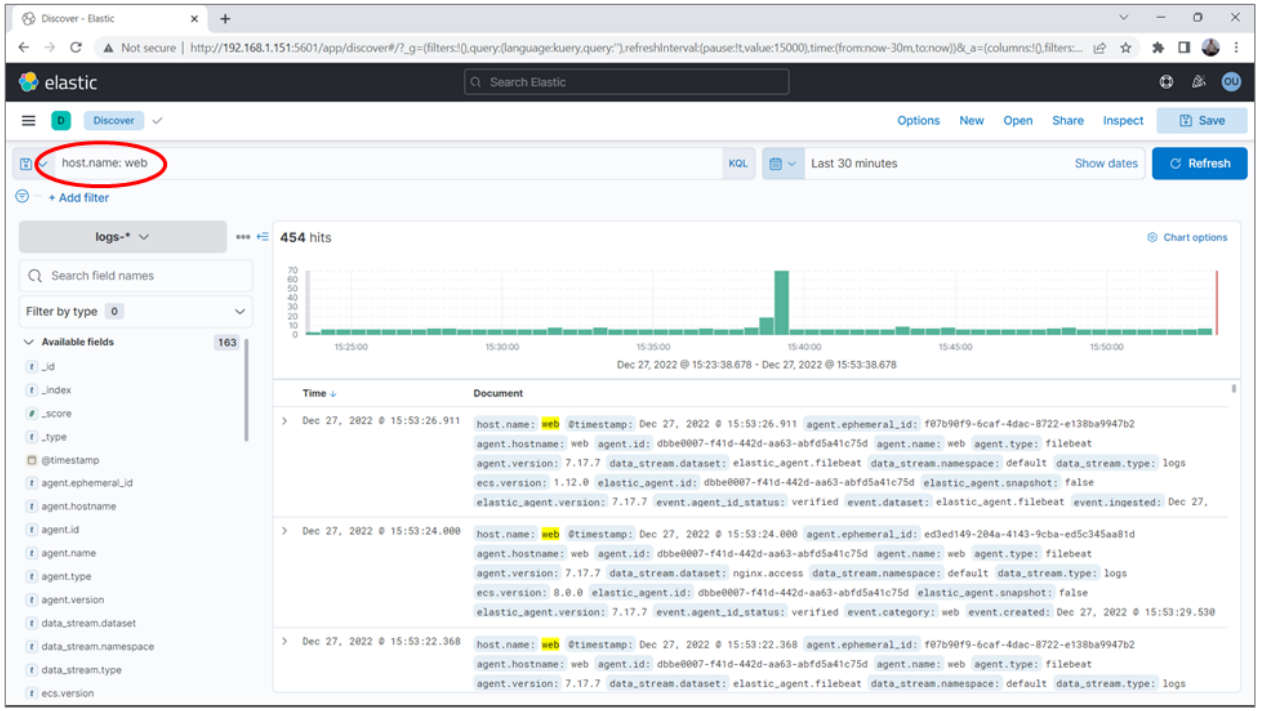
| | |
|---|---|
| **Multiple Characters,** e.g. United Kingdom | Searches for any number of characters before or after the word, e.g. Unite* will return United Kingdom, United States, United Arab Emirates. |
| **Single Characters,** e.g. "D?g" | Replaces single characters in words to return results , e.g. "D?g" will return 'Dig', 'Dog', 'Dug', etc. |
| **Fuzzy,** e.g. "Dog~" | Searches for a wider field of results such as words that are related to the search criteria, e.g. "Dog~" will return 'Dogs', 'Doe', 'Frog'. |
| **Proximity Wildcard Field,** e.g. Animal*:Dog | Searches against any field containing the specific word, e.g. searches for results containing the word 'Dog' within any fields named with 'Animal'. -Kibana V6.3 onwards only. |

**Range Search**

| | |
|---|---|
| **Inclusive Range,** e.g. [1 to 5] | Searches inclusive of the range specified, e.g. within numbers 1 to 5. |
| **Exclusive Range,** e.g. {1 to 5} | Searches exclusive of the range specified, e.g. between the numbers 1 and 5, so 2, 3 or 4 will be returned, but not 1 and 5. |
| **Larger Than,** e.g. age:>3 | Searches for numeric value greater than a specified number, e.g. greater than 3 years of age. |
| **Less Than,** e.g. age:<3 | Searches for numeric value less than a specified number, e.g. less than 3 years of age. |
| **Boost,** e.g. United^2 Kingdom | Prioritises results with the word 'United' in proximity to the word 'Kingdom' in a sentence or paragraph. The higher the value, the closer the proximity. |
| **Boost Phrase,** e.g. "United Kingdom" | Prioritises results with the phrase 'United Kingdom' in proximity to the word 'London' in a sentence or paragraph. The higher the value, the closer the proximity. |

# EXAMPLE SEARCH

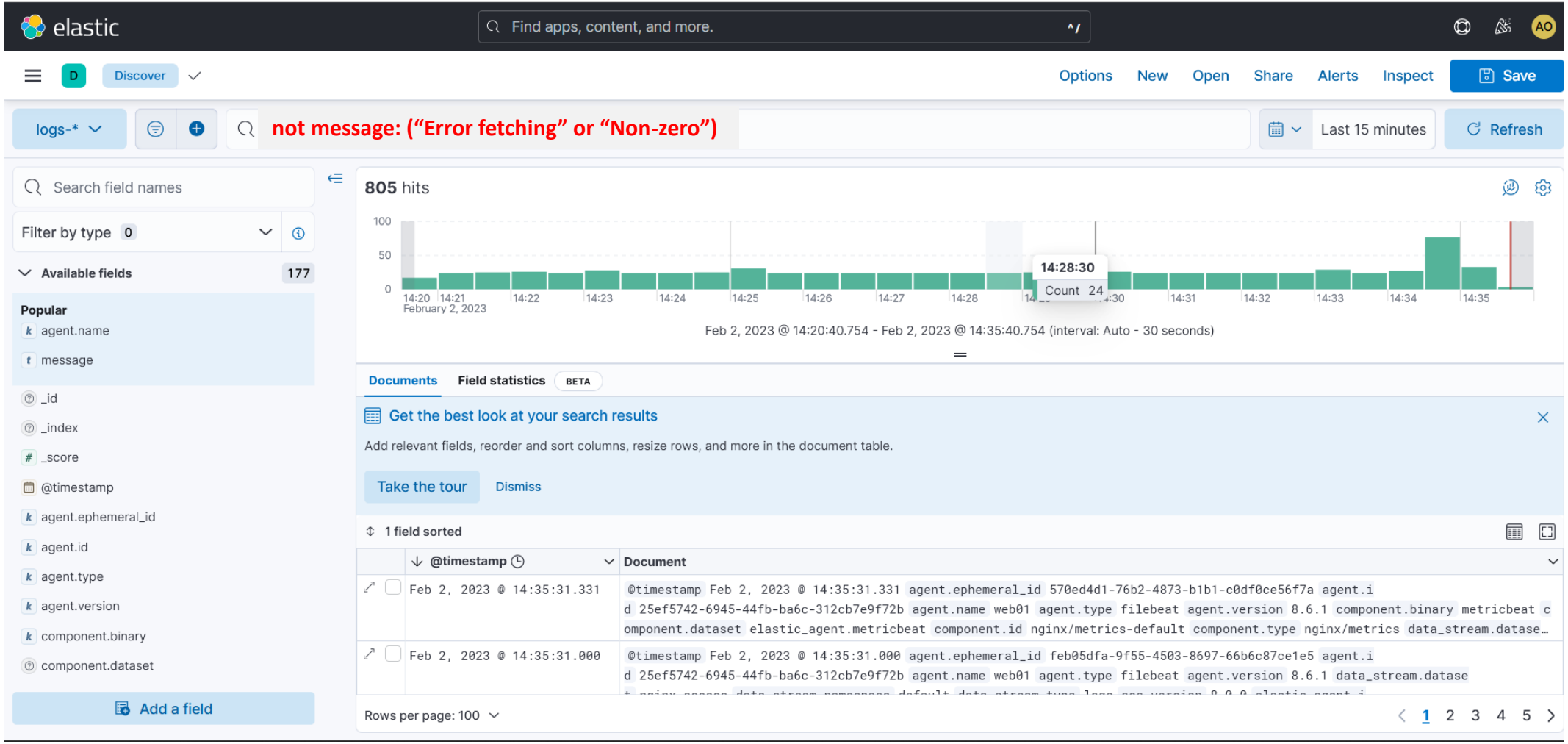
When an event occurs, let it run until you want to start analysis. Then *Stop* real time monitoring so you can focus on the static set of logs you have selected. Note the start and stop times of the event. Here we have stopped real time monitoring and are focusing in on logs from the web host using the KQL expression *host.name: web*.



# PRE-ATTACK

Connect to the SIEM https://192.168.1.101:5601

Monitor traffic for a couple of minutes and remove any noise.


elastic
Find apps, content, and more.
AO
D
Discover
Options
New
Open
Share
Alerts
Inspect
Save
logs-*
not message: (“Error fetching” or “Non-zero”)
Last 15 minutes
Refresh
Search field names
Filter by type 0
Available fields 177
Popular
agent.name
message
_id
_index
_score
@timestamp
agent.ephemeral_id
agent.id
agent.type
agent.version
component.binary
component.dataset
Add a field
805 hits
100
50
0
14:20
February 2, 2023
14:21
14:22
14:23
14:24
14:25
14:26
14:27
14:28
14:30
14:31
14:32
14:33
14:34
14:35
14:28:30
Count 24
Feb 2, 2023 @ 14:20:40.754 - Feb 2, 2023 @ 14:35:40.754 (interval: Auto - 30 seconds)
Documents
Field statistics
BETA
Get the best look at your search results
Add relevant fields, reorder and sort columns, resize rows, and more in the document table.
Take the tour
Dismiss
1 field sorted
@timestamp
Document
Feb 2, 2023 @ 14:35:31.331
@timestamp Feb 2, 2023 @ 14:35:31.331 agent.ephemeral_id 570ed4d1-76b2-4873-b1b1-c0df0ce56f7a agent.id 25ef5742-6945-44fb-ba6c-312cb7e9f72b agent.name web01 agent.type filebeat agent.version 8.6.1 component.binary metricbeat component.dataset elastic_agent.metricbeat component.id nginx/metrics-default component.type nginx/metrics data_stream.datase…
Feb 2, 2023 @ 14:35:31.000
@timestamp Feb 2, 2023 @ 14:35:31.000 agent.ephemeral_id feb05dfa-9f55-4503-8697-66b6c87ce1e5 agent.id 25ef5742-6945-44fb-ba6c-312cb7e9f72b agent.name web01 agent.type filebeat agent.version 8.6.1 data_stream.datase
Rows per page: 100
1 2 3 4 5

# ATTACK PHASE 1

I will launch the attack phase now.

We will:

- Monitor for anomalies
- Investigate anomalies
- Determine what has occurred

Notes from the SOC Manager:

- Local access on servers is under enhanced auditing. Records are tagged with *bash-audit*
- Remote access is under enhanced auditing. Records are tagged with ssh-audit.
- Connections to services on web/proxy are under enhanced logging.
- The Suricata IDS is running and produces eve logs. These can be helpful in detecting attacks, but has yet to be fine tuned.

# ELK WALKTHROUGH

**WORKSHOP CONCLUDES**

*Thank you!*