SIEM HOME LAB – PREM PERSONAL NETWORK

I have assembled a home lab using a Kali virtual machine and Elastic SIEM. I used the Elastic Beats agent to transfer data from the Kali virtual machine to the SIEM; Nmap was used to generate security events on the Kali VM; and the Elastic web interface was used to query and analyze the logs in the SIEM. In order to detect security incidents, I also designed an alert and a dashboard to visualize security occurrences.

Using the help of this home lab, I can acquire and hone the skills required for efficient security monitoring and incident response using Elastic SIEM. By following these steps, I can enhance my security monitoring abilities and obtain practical experience with utilizing a SIEM, which will help me become a great security analyst or engineer.

Prerequisites

Before we get started, make sure you have the following:

1. VirtualBox or VMware
2. Basic knowledge of Linux and virtualization software.

Overview of the tasks

- Set up a free Elastic account.
- Install the Kali VM.
- Set up the Linux virtual machine's Elastic Agent to gather logs and send them to the SIEM.
- Generate security events on the Kali VM.
- Query to find the security events in the Elastic SIEM.
- Create a Dashboard to visualize security events.
- Create alerts for security events.

Task 1: Set up an Elastic Account

1. Sign up for a free trial to use Elastic Cloud at https://cloud.elastic.co/registration
2. Once you have an Elastic account, log in to the Elastic Cloud console at https://cloud.elastic.co.
3. Click on “Start your free trial.”
4. When choosing the deployment type, click the "Create Deployment" button and choose "Elasticsearch."
5. Select the deployment size and region that best suit your requirements, then click "Create Deployment."
6. Wait for the configuration to complete.
7. Once the deployment is ready, click “continue.”

Task 2: Setting up the Linux VM

1. Download the Kali Linux VM from the official Kali website at https://www.kali.org/get-kali/#kali-virtual-machines.
2. Using the Kali VM file, create a new virtual machine (VM) in your favourite virtualization software, like VMware or VirtualBox.
3. Start the VM and follow the on-screen prompts to install Kali.
4. After installation is finished, use "kali" as the login and password to access the Kali virtual machine (VM).

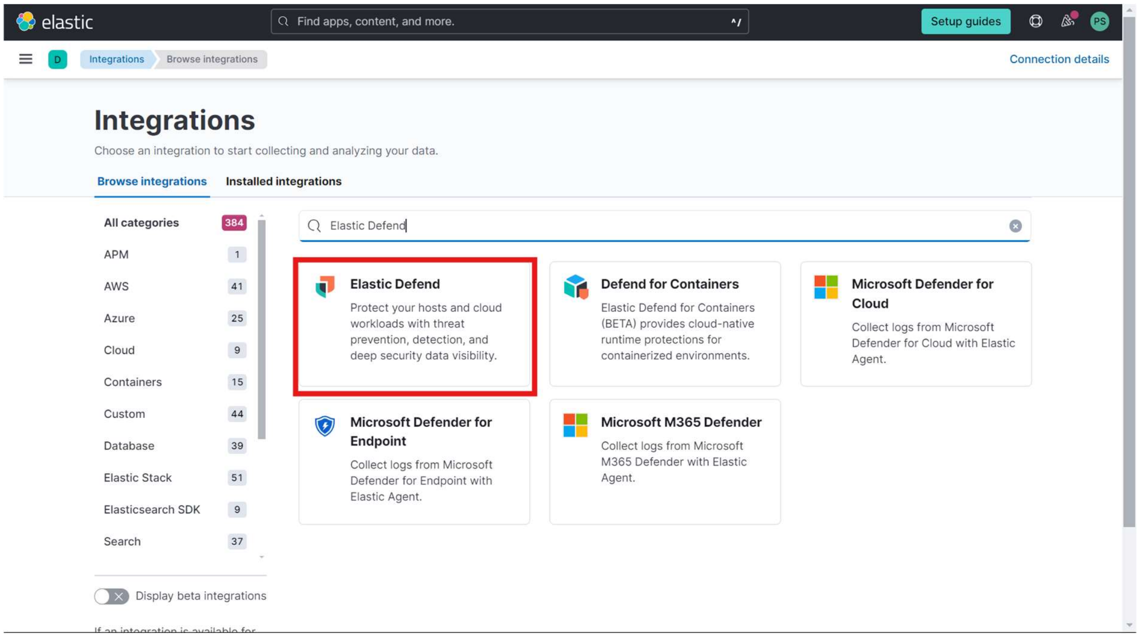
Task 3: Setting up the Agent to Collect Logs

To gather and transmit data to a centralized system for analysis and monitoring, software called an agent is placed on a device, such as a server or endpoint. Security-related events from your endpoints are gathered and forwarded to your Elastic SIEM instance via an agent in the context of the platform.

To set up the agent to collect logs from your Kali VM and forward them to your Elastic SIEM instance, follow these steps:

1. To access the Integrations page, log in to your Elastic SIEM instance, click the Kibana main menu bar in the upper left corner, and then choose "Integrations" from the bottom menu.
2. Search for "Elastic Defend" and click on it to open the integration page.
3. To install the agent on your Kali VM, click "Install Elastic Defend" and adhere to the installation instructions on the integration page. Paste that command into the Kali terminal (command line).
4. You will receive a notification stating that the "Elastic Agent has been successfully installed" after the agent has been installed, which may take several minutes. It may take a few minutes for the logs to show up in the SIEM, but it will begin automatically gathering and transmitting data to your Elastic SIEM server.
5. You can verify that the agent has been installed correctly by running this command: **sudo systemctl status elastic-agent.service**

Note: Before continuing, make sure your Kali is online by pinging google.com if you receive a problem when installing the agent.



Choose an integration to start collecting and analyzing your data.

Elastic Defend

Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

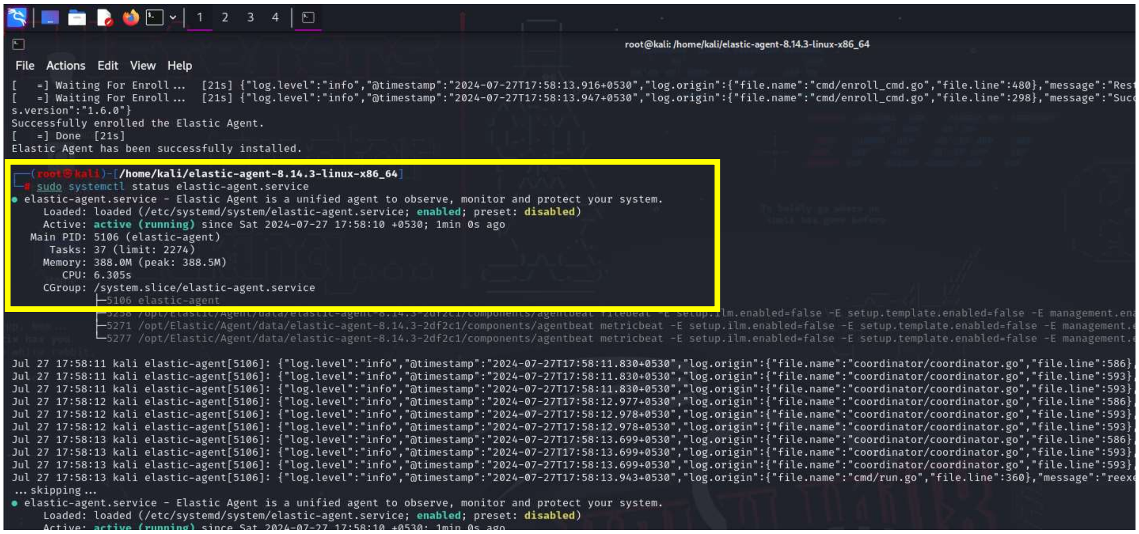
Defend for Containers
Elastic Defend for Containers (BETA) provides cloud-native runtime protections for containerized environments.

Microsoft Defender for Cloud
Collect logs from Microsoft Defender for Cloud with Elastic Agent.

Microsoft Defender for Endpoint
Collect logs from Microsoft Defender for Endpoint with Elastic Agent.

Microsoft M365 Defender
Collect logs from Microsoft M365 Defender with Elastic Agent.

If an integration is available for



1
2
3
4
root@kali: /home/kali/elastic-agent-8.14.3-linux-x86_64
File Actions Edit View Help

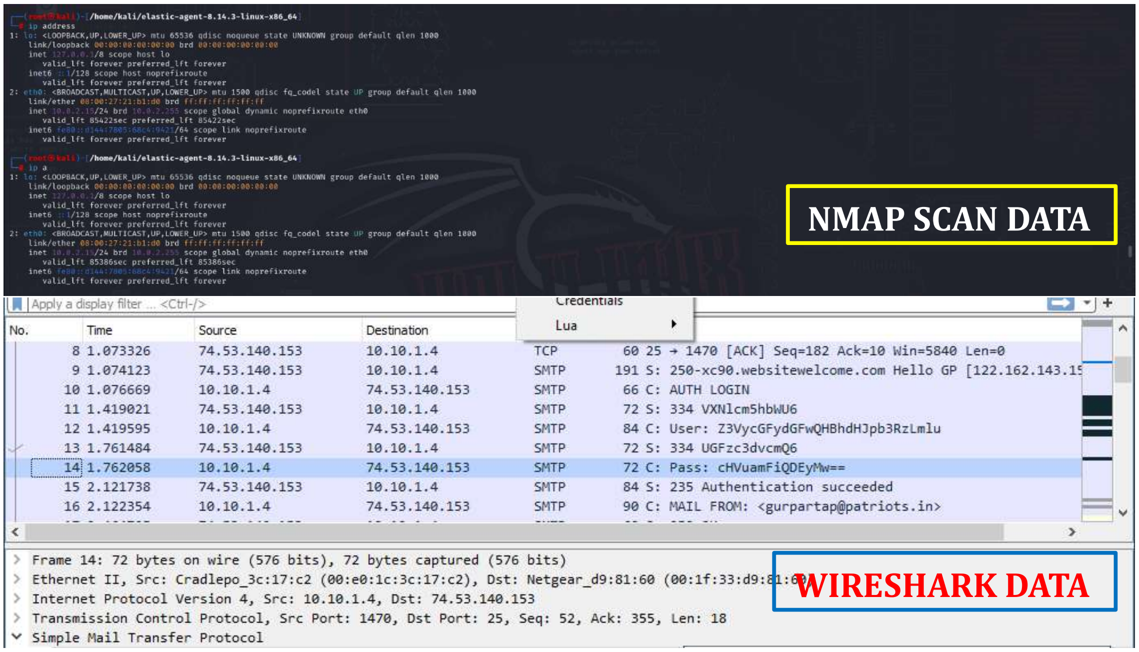
```
[   =] Waiting For Enroll ...  [21s] {"log.level":"info","@timestamp":"2024-07-27T17:58:13.916+0530","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":480},"message":"Rest
[   =] Waiting For Enroll ...  [21s] {"log.level":"info","@timestamp":"2024-07-27T17:58:13.947+0530","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":298},"message":"Succ
s.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[   =] Done  [21s]
Elastic Agent has been successfully installed.

┌──(root㉿kali)-[/home/kali/elastic-agent-8.14.3-linux-x86_64]
└─# sudo systemctl status elastic-agent.service
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
     Active: active (running) since Sat 2024-07-27 17:58:10 +0530; 1min 0s ago
   Main PID: 5106 (elastic-agent)
      Tasks: 37 (limit: 2274)
     Memory: 388.0M (peak: 388.5M)
        CPU: 6.305s
     CGroup: /system.slice/elastic-agent.service
             ├─5106 elastic-agent
             ├─5258 /opt/Elastic/Agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat filebeat -E setup.ilm.enabled=false -E setup.template.enabled=false -E management.ena
             ├─5271 /opt/Elastic/Agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat metricbeat -E setup.ilm.enabled=false -E setup.template.enabled=false -E management.e
             └─5277 /opt/Elastic/Agent/data/elastic-agent-8.14.3-2df2c1/components/agentbeat metricbeat -E setup.ilm.enabled=false -E setup.template.enabled=false -E management.e

Jul 27 17:58:11 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:11.830+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":586},
Jul 27 17:58:11 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:11.830+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":593},
Jul 27 17:58:11 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:11.830+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":593},
Jul 27 17:58:12 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:12.977+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":586},
Jul 27 17:58:12 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:12.978+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":593},
Jul 27 17:58:12 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:12.978+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":593},
Jul 27 17:58:13 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:13.699+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":586},
Jul 27 17:58:13 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:13.699+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":593},
Jul 27 17:58:13 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:13.699+0530","log.origin":{"file.name":"coordinator/coordinator.go","file.line":593},
Jul 27 17:58:13 kali elastic-agent[5106]: {"log.level":"info","@timestamp":"2024-07-27T17:58:13.943+0530","log.origin":{"file.name":"cmd/run.go","file.line":360},"message":"reexe
... skipping ...
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
     Active: active (running) since Sat 2024-07-27 17:58:10 +0530; 1min 0s ago
```

Task 4: Generating Security Events on the Kali VM

You can create some security-related events on your Kali virtual machine (VM) to confirm that the agent is operating as intended. We can use a tool like Nmap and Wireshark to accomplish this. A free and open-source tool for network administration, exploration, and security auditing is called Nmap (Network Mapper). Its purpose is to identify hosts and services on a computer network, generating a network "map" in the process. Nmap may be used to find out what operating system and software are installed on a target system, check hosts for open ports, and obtain further network information. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

To run an Nmap scan, follow these steps:

1. Install Nmap on the Linux VM if you're not using Kali, Nmap already comes preinstalled in Kali. Open a new Terminal and run this command to install it: **sudo apt-get install nmap.**
2. Run a scan on Kali machine by running the command: **sudo nmap <vm-ip>**. You can also run a scan of your host machine if you place your Kali VM on a "bridged" network.
3. This scan generates several security events, such as the detection of open ports and the identification of services running on those ports. Run a few more Nmap scans ("**nmap -sS <ip address>**", "**nmap -sT <ip address>**", "**nmap -p- <ip address>**"etc..



```
┌──(root㉿kali)-[/home/kali/elastic-agent-8.14.3-linux-x86_64]
└─# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85422sec preferred_lft 85422sec
    inet6 fe80::d144:7805:68c4:9421/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali/elastic-agent-8.14.3-linux-x86_64]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85386sec preferred_lft 85386sec
    inet6 fe80::d144:7805:68c4:9421/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
No.    Time        Source           Destination
     8 1.073326    74.53.140.153    10.10.1.4        TCP      60 25 → 1470 [ACK] Seq=182 Ack=10 Win=5840 Len=0
     9 1.074123    74.53.140.153    10.10.1.4        SMTP    191 S: 250-xc90.websitewelcome.com Hello GP [122.162.143.15
    10 1.076669    10.10.1.4        74.53.140.153    SMTP     66 C: AUTH LOGIN
    11 1.419021    74.53.140.153    10.10.1.4        SMTP     72 S: 334 VXNlcm5hbWU6
    12 1.419595    10.10.1.4        74.53.140.153    SMTP     84 C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
    13 1.761484    74.53.140.153    10.10.1.4        SMTP     72 S: 334 UGFzc3dvcmQ6
    14 1.762058    10.10.1.4        74.53.140.153    SMTP     72 C: Pass: cHVuamFiQDEyMw==
    15 2.121738    74.53.140.153    10.10.1.4        SMTP     84 S: 235 Authentication succeeded
    16 2.122354    10.10.1.4        74.53.140.153    SMTP     90 C: MAIL FROM: <gurpartap@patriots.in>

> Frame 14: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60)
> Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
> Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 52, Ack: 355, Len: 18
˅ Simple Mail Transfer Protocol
```

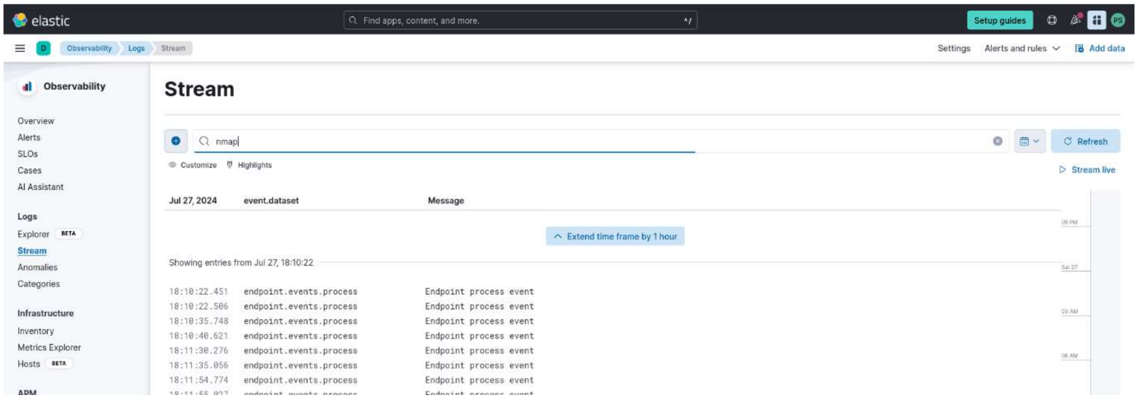
Task 5: Querying for Security Events in the Elastic SIEM

We can now begin searching through and examining the SIEM's logs after moving data from the Kali VM.

To do this, follow these steps:

1. To see the logs from the Kali virtual machine, within your Elastic Deployment, click the three horizontal line menu icon in the top-left corner and select the "Logs" option under "Observability."
2. In the search bar, enter a search query to filter the logs. For example, to search for all logs related to Nmap scans, enter the query: event.action:“**nmap_scan**” or **process.args: “sudo**”.
3. Click on the “Search” button to execute the search query.
4. The results of the search query will be displayed in the table below. You can click on the three dots next to each event to view more details.

Note: You can learn more about how security incidents are found, looked into, and handled in real-world settings by creating and examining various security event types in Elastic SIEM, such as the one above, or by creating authentication failures caused by a user entering the wrong password or trying to log in to SSH with the wrong password.

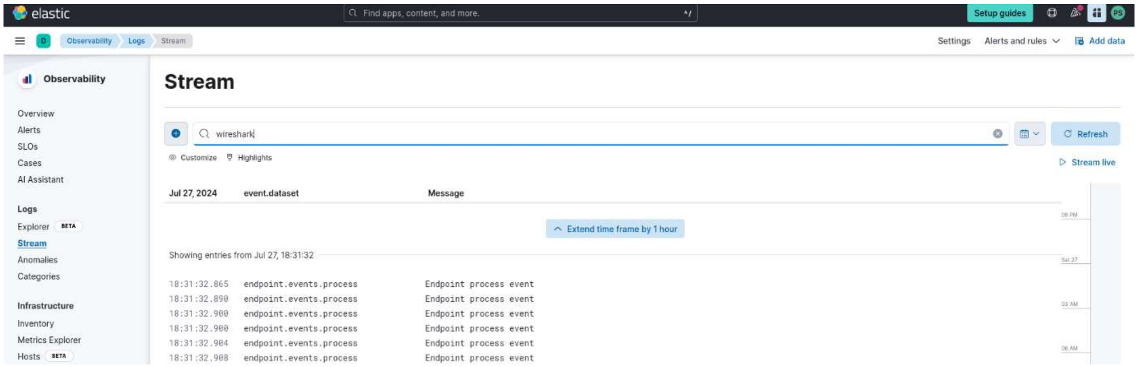


Search: nmap

Showing entries from Jul 27, 18:10:22

```
Jul 27, 2024   event.dataset             Message
18:10:22.451   endpoint.events.process   Endpoint process event
18:10:22.506   endpoint.events.process   Endpoint process event
18:10:35.748   endpoint.events.process   Endpoint process event
18:10:40.621   endpoint.events.process   Endpoint process event
18:11:30.276   endpoint.events.process   Endpoint process event
18:11:35.056   endpoint.events.process   Endpoint process event
18:11:54.774   endpoint.events.process   Endpoint process event
```

NMAP SCAN DATA



Search: wireshark

Showing entries from Jul 27, 18:31:32

```
Jul 27, 2024   event.dataset             Message
18:31:32.865   endpoint.events.process   Endpoint process event
18:31:32.890   endpoint.events.process   Endpoint process event
18:31:32.900   endpoint.events.process   Endpoint process event
18:31:32.900   endpoint.events.process   Endpoint process event
18:31:32.904   endpoint.events.process   Endpoint process event
18:31:32.908   endpoint.events.process   Endpoint process event
```

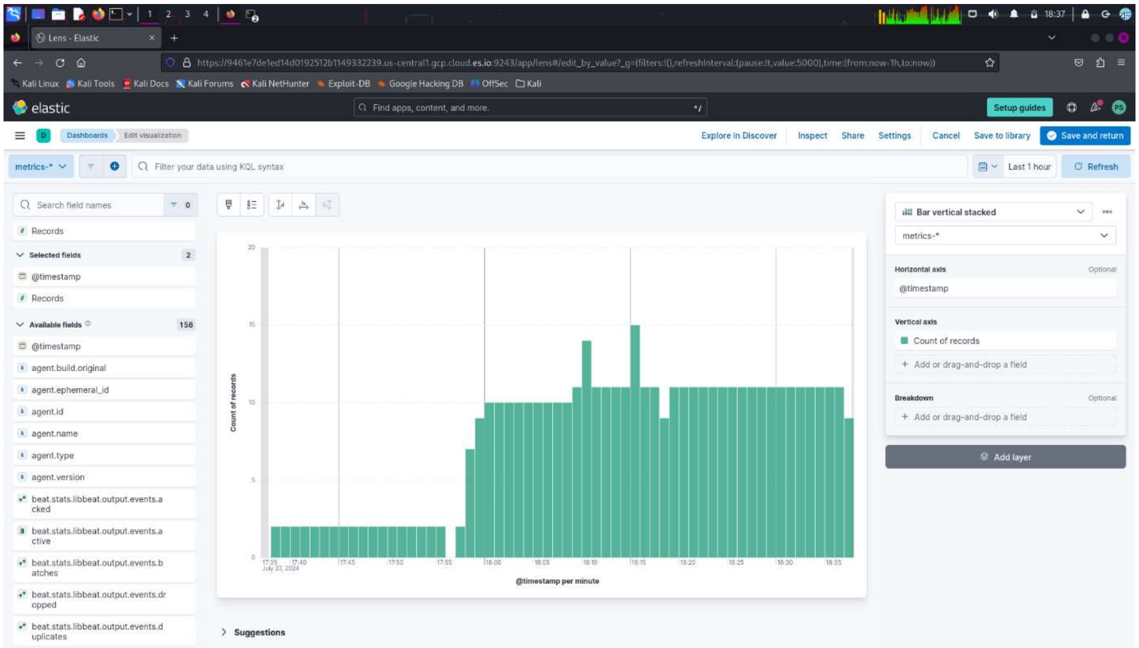
WIRESHARK SCAN DATA

Task 6: Create a Dashboard to Visualize the Events

You can also use the visualizations and dashboards in the SIEM app to analyze the logs and identify patterns or anomalies in the data.

Here's how you can do that:

1. Navigate to the Elastic web portal at https://cloud.elastic.co/.
2. Click on the menu icon on the top-left, then under "Analytics," click on "Dashboards."
3. Click on the "Create dashboard" button on the top right to create a new dashboard.
4. Click on the "Create Visualization" button to add a new visualization to the dashboard.
5. Choose the visualization kind you desire, either "Area" or "Line." A chart displaying the number of incidents over time will be produced as a result.
6. Choose "Timestamp" for the horizontal field and "Count" for the vertical field type in the "Metrics" section of the visualization editor on the right. This will display the number of occurrences over time.
7. Click on the "Save" button to save the visualization and then complete the rest of the settings.



https://9461e7de1ed14d0192512b1149332239.us-central1.gcp.cloud.es.io:9243/app/lens#/edit_by_value?_g=(filters:!(),refreshInterval:(pause:!t,value:5000),time:(from:now-1h,to:now))

Bar vertical stacked

metrics-*

Horizontal axis: @timestamp

Vertical axis: Count of records

Task 7: Create an Alert

Alerts are an essential component of a SIEM that help identify security events and quickly address them. Alerts can be set up to perform particular actions when predetermined criteria are fulfilled, and they can be generated using established rules or bespoke queries.

Here are the steps:

1. Click on the menu icon on the top-left, then under "Security," click on "Alerts."
2. Click on "Manage rules" at the top right.
3. Click on the "Create new rule" button at the top right.
4. Under the "Define rule" section, select the "Custom query" option from the dropdown menu.

5. Establish the rules' conditions under "Custom query." The following query can be used to find Nmap scan events. All events that match the action "**nmap_scan**" will be matched by this query. Next, select "Continue."

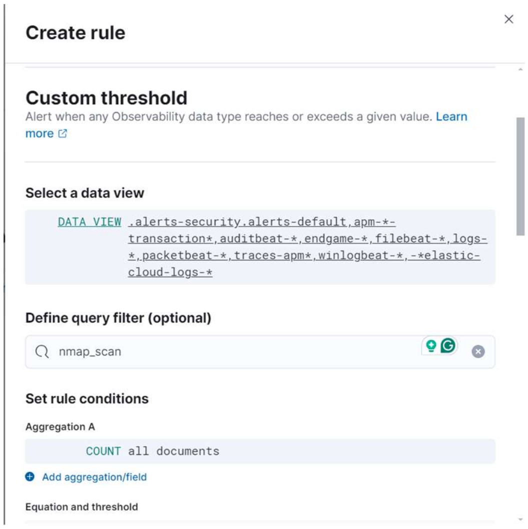
6. Under the "About rule" section, give your rule a name and a description (Nmap Scan Detection).

7. You can prioritize warnings according to their importance by setting the alert's severity level. Click "Continue" after maintaining all other default settings under "Schedule rule."

8. Choose the action you wish to perform when the rule is activated from the "Actions" section. You have the option to start a custom webhook, start a Slack chat, or send an email notification.

9. Finally, click the "Create and enable rule" button to create the alert.

Note: After creating the alert, it will keep an eye out for Nmap scan events in your logs. The alarm will sound and the chosen action will be carried out if a Nmap scan event is found. Under "Security," go to the "Alerts" section to view and manage your notifications.



Create rule

Custom threshold

Alert when any Observability data type reaches or exceeds a given value. Learn more

Select a data view

DATA VIEW .alerts-security.alerts-default,apm-*-transaction*,auditbeat-*,endgame-*,filebeat-*,logs-*,packetbeat-*,traces-apm*,winlogbeat-*,-*elastic-cloud-logs-*

Define query filter (optional)

nmap_scan

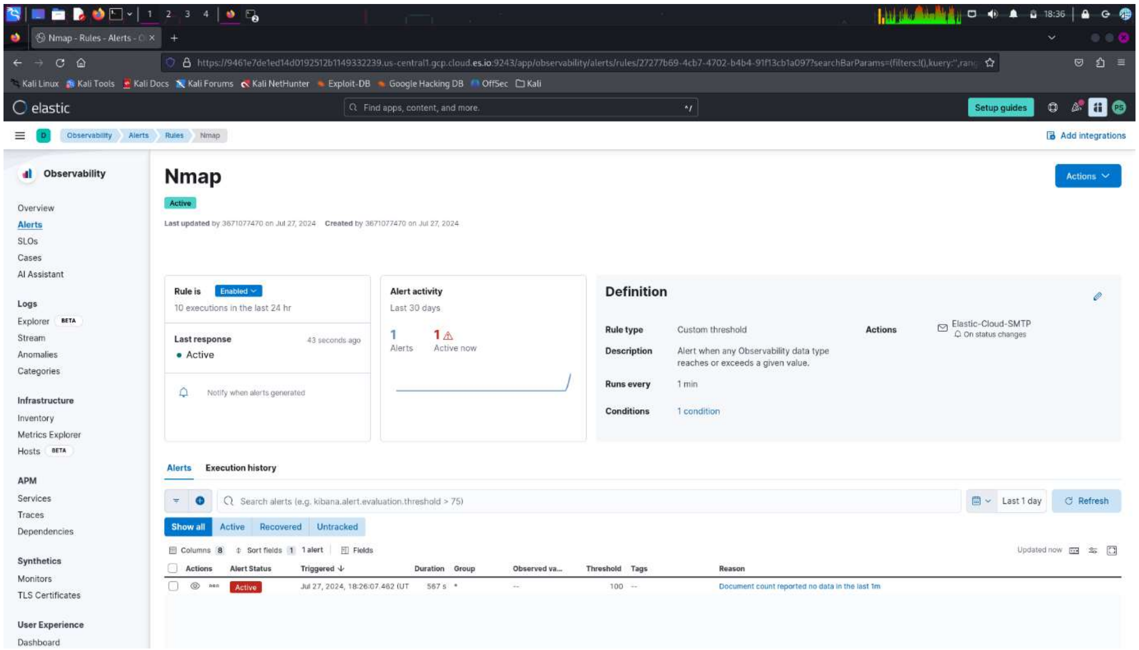
Set rule conditions

Aggregation A

COUNT all documents

Add aggregation/field

Equation and threshold



Nmap

Active

Last updated by 3671077470 on Jul 27, 2024   Created by 3671077470 on Jul 27, 2024

Rule is Enabled

10 executions in the last 24 hr

Last response 43 seconds ago

● Active

Notify when alerts generated

Alert activity

Last 30 days

1 Alerts   1 ⚠ Active now

Definition

Rule type: Custom threshold

Description: Alert when any Observability data type reaches or exceeds a given value.

Runs every: 1 min

Conditions: 1 condition

Actions: Elastic-Cloud-SMTP — On status changes

Alerts | Execution history

Search alerts (e.g. kibana.alert.evaluation.threshold > 75)   Last 1 day   Refresh

Show all | Active | Recovered | Untracked

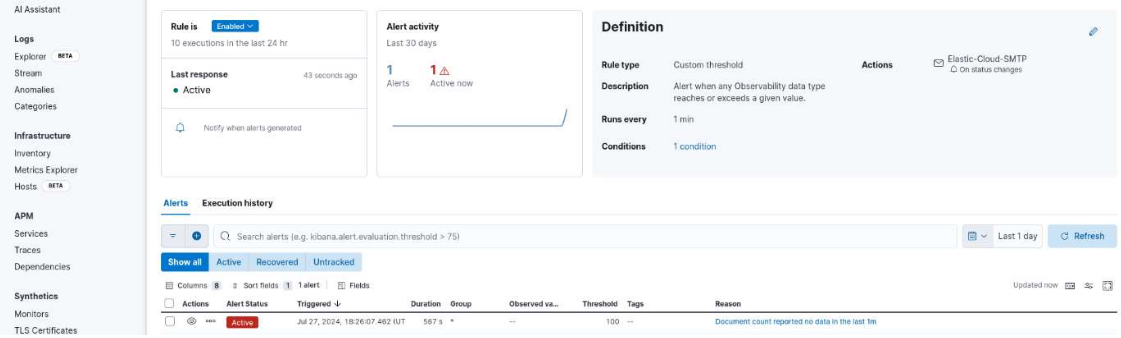
Columns 8   Sort fields 1   1 alert   Fields   Updated now

Actions	Alert Status	Triggered ↓	Duration	Group	Observed va...	Threshold	Tags	Reason
	Active	Jul 27, 2024, 18:26:07.462 (UT	567 s	*	--	100	--	Document count reported no data in the last 1m

Additional Observations :

- In order to use Anomaly detection, Data Frame Analytics, Dashboard Management, Data Visualizations, and other features on your deployment, you can also build Machine Learning models.

- You may locate your rule operating on the specified path and receiving the triggered actions on the main dashboard under the alerts part of the observability section.



Rule is Enabled
10 executions in the last 24 hr

Last response 43 seconds ago
Active

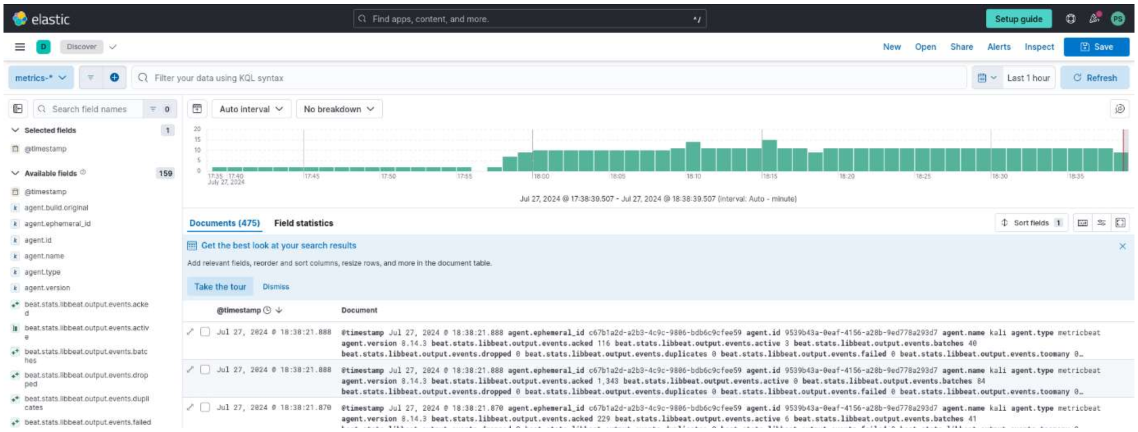
Notify when alerts generated

Definition

Rule type	Custom threshold	Actions	Elastic-Cloud-SMTP On status changes
Description	Alert when any Observability data type reaches or exceeds a given value.		
Runs every	1 min		
Conditions	1 condition		

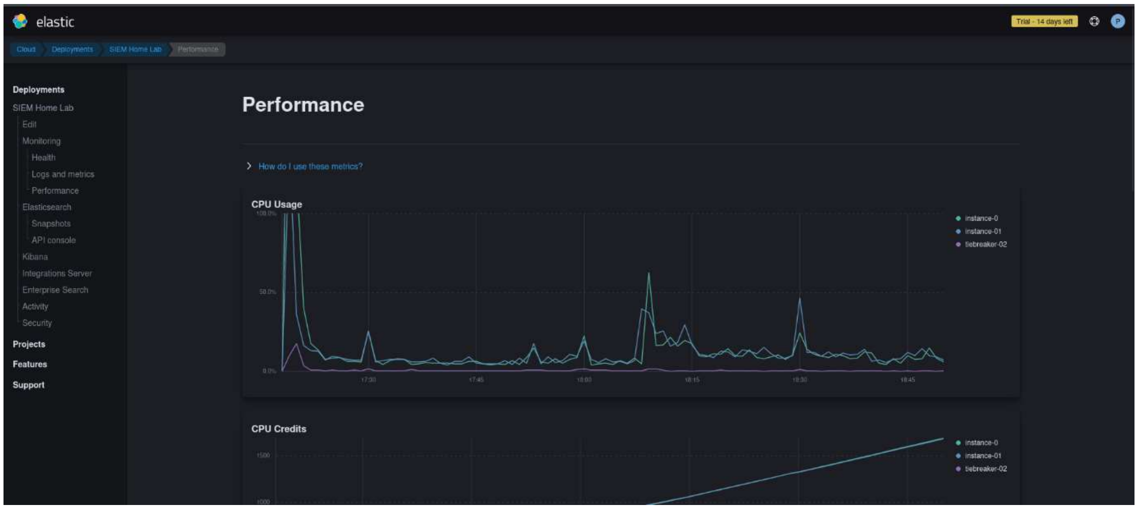
Actions	Alert Status	Triggered	Duration	Group	Observed va...	Threshold	Tags	Reason
	Active	Jul 27, 2024, 18:26:07.462 (UT	567 s	*	--	100	--	Document count reported no data in the last 1m

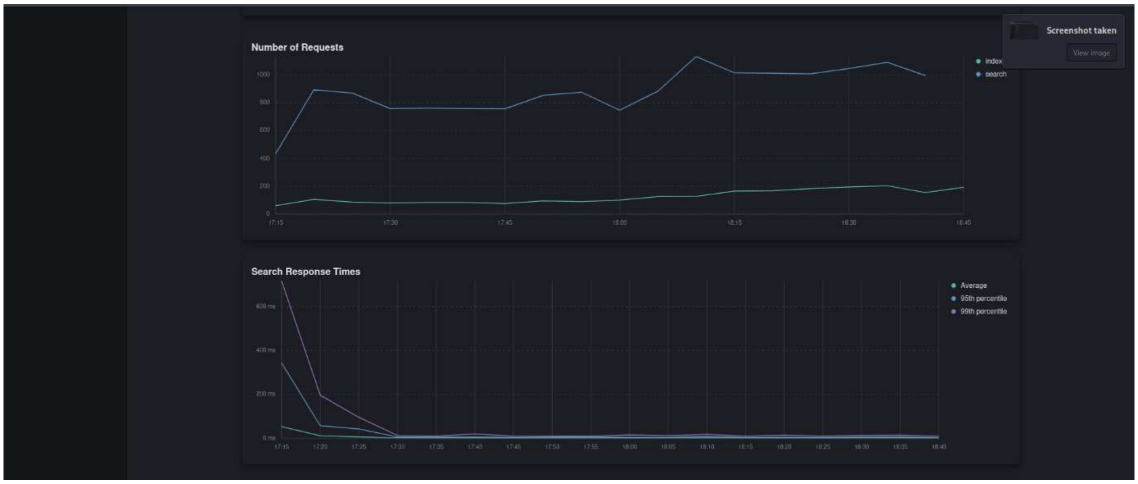
- You can filter out specific events from the stream section by using the timestamps and actions completed as a collaborative log found in the discover sections. These logs will be used to create a pictorial representation of the occurrences.


elastic
Find apps, content, and more.
Setup guide
Discover
New
Open
Share
Alerts
Inspect
Save
metrics-*
Filter your data using KQL syntax
Last 1 hour
Refresh
Search field names
Selected fields 1
@timestamp
Available fields 159
@timestamp
agent.build.original
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
beat.stats.libbeat.output.events.acked
beat.stats.libbeat.output.events.active
beat.stats.libbeat.output.events.batches
beat.stats.libbeat.output.events.dropped
beat.stats.libbeat.output.events.duplicates
beat.stats.libbeat.output.events.failed
Auto interval
No breakdown
20
15
10
5
0
17:35
17:40
July 27, 2024
17:45
17:50
17:55
18:00
18:05
18:10
18:15
18:20
18:25
18:30
18:35
Jul 27, 2024 @ 17:38:39.507 - Jul 27, 2024 @ 18:38:39.507 (interval: Auto - minute)
Documents (475)
Field statistics
Sort fields 1
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

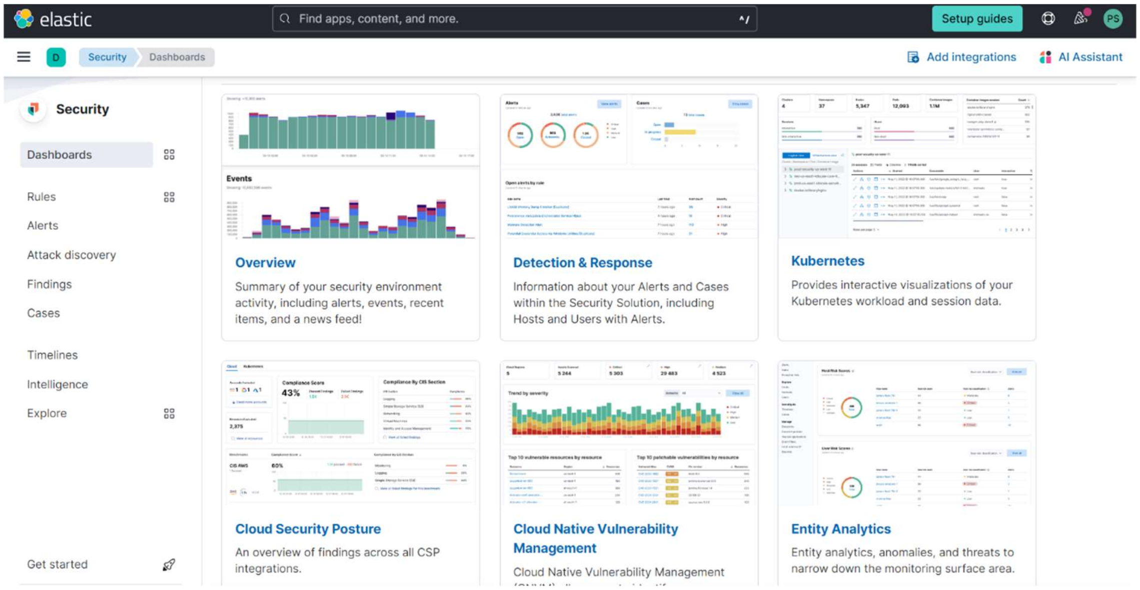
```
@timestamp              Document
Jul 27, 2024 @ 18:38:21.888  @timestamp Jul 27, 2024 @ 18:38:21.888 agent.ephemeral_id c67b1a2d-a2b3-4c9c-9806-bdb6c9cfee59 agent.id 9539b43a-0eaf-4156-a28b-9ed778a293d7 agent.name kali agent.type metricbeat
                             agent.version 8.14.3 beat.stats.libbeat.output.events.acked 116 beat.stats.libbeat.output.events.active 3 beat.stats.libbeat.output.events.batches 40
                             beat.stats.libbeat.output.events.dropped 0 beat.stats.libbeat.output.events.duplicates 0 beat.stats.libbeat.output.events.failed 0 beat.stats.libbeat.output.events.toomany 0…
Jul 27, 2024 @ 18:38:21.888  @timestamp Jul 27, 2024 @ 18:38:21.888 agent.ephemeral_id c67b1a2d-a2b3-4c9c-9806-bdb6c9cfee59 agent.id 9539b43a-0eaf-4156-a28b-9ed778a293d7 agent.name kali agent.type metricbeat
                             agent.version 8.14.3 beat.stats.libbeat.output.events.acked 1,343 beat.stats.libbeat.output.events.active 0 beat.stats.libbeat.output.events.batches 84
                             beat.stats.libbeat.output.events.dropped 0 beat.stats.libbeat.output.events.duplicates 0 beat.stats.libbeat.output.events.failed 0 beat.stats.libbeat.output.events.toomany 0…
Jul 27, 2024 @ 18:38:21.870  @timestamp Jul 27, 2024 @ 18:38:21.870 agent.ephemeral_id c67b1a2d-a2b3-4c9c-9806-bdb6c9cfee59 agent.id 9539b43a-0eaf-4156-a28b-9ed778a293d7 agent.name kali agent.type metricbeat
                             agent.version 8.14.3 beat.stats.libbeat.output.events.acked 229 beat.stats.libbeat.output.events.active 6 beat.stats.libbeat.output.events.batches 41
```

- Numerous performance data, like CPU Usage, CPU Credits, Number of Inbound Requests, Search Response Time, and so forth, are available on your deployment's Main Page. You will receive a comprehensive analysis of the performance and health of your deployment from these indicators.





- You can compute your data quality, Kubernetes, entity analytics, and detection and response data using a variety of pre-defined dashboards found under the security area. Additionally, you may design a custom dashboard to track the actions that are triggered by your deployment and conduct technical analysis.



Overview

Summary of your security environment activity, including alerts, events, recent items, and a news feed!

Detection & Response

Information about your Alerts and Cases within the Security Solution, including Hosts and Users with Alerts.

Kubernetes

Provides interactive visualizations of your Kubernetes workload and session data.

Cloud Security Posture

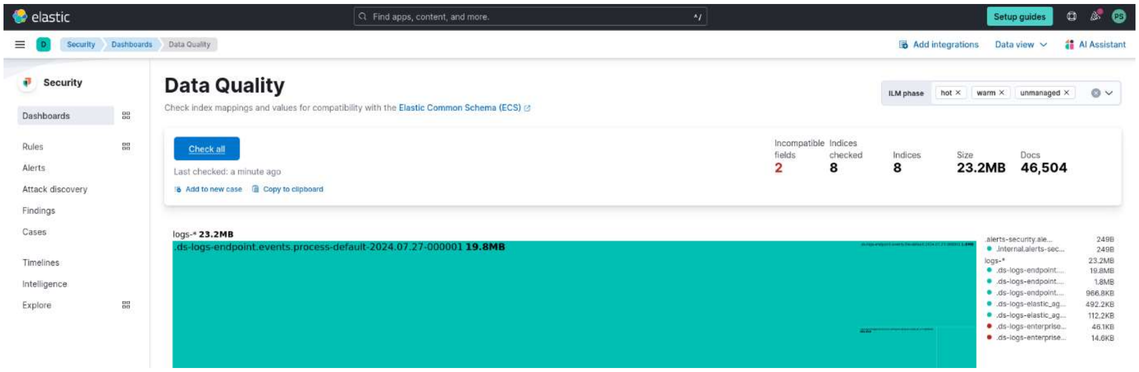
An overview of findings across all CSP integrations.

Cloud Native Vulnerability Management

Cloud Native Vulnerability Management

Entity Analytics

Entity analytics, anomalies, and threats to narrow down the monitoring surface area.



Data Quality

Check index mappings and values for compatibility with the Elastic Common Schema (ECS)

Last checked: a minute ago

Incompatible fields	Indices checked	Indices	Size	Docs
2	8	8	23.2MB	46,504

logs-* **23.2MB**

.ds-logs-endpoint.events.process-default-2024.07.27-000001 **19.8MB**

.alerts-security.ale...	249B
● .internal.alerts-sec...	249B
logs-*	23.2MB
● .ds-logs-endpoint....	19.8MB
● .ds-logs-endpoint....	1.8MB
● .ds-logs-endpoint....	966.8KB
● .ds-logs-elastic_ag...	492.2KB
● .ds-logs-elastic_ag...	112.2KB
● .ds-logs-enterprise...	46.1KB
● .ds-logs-enterprise...	14.6KB