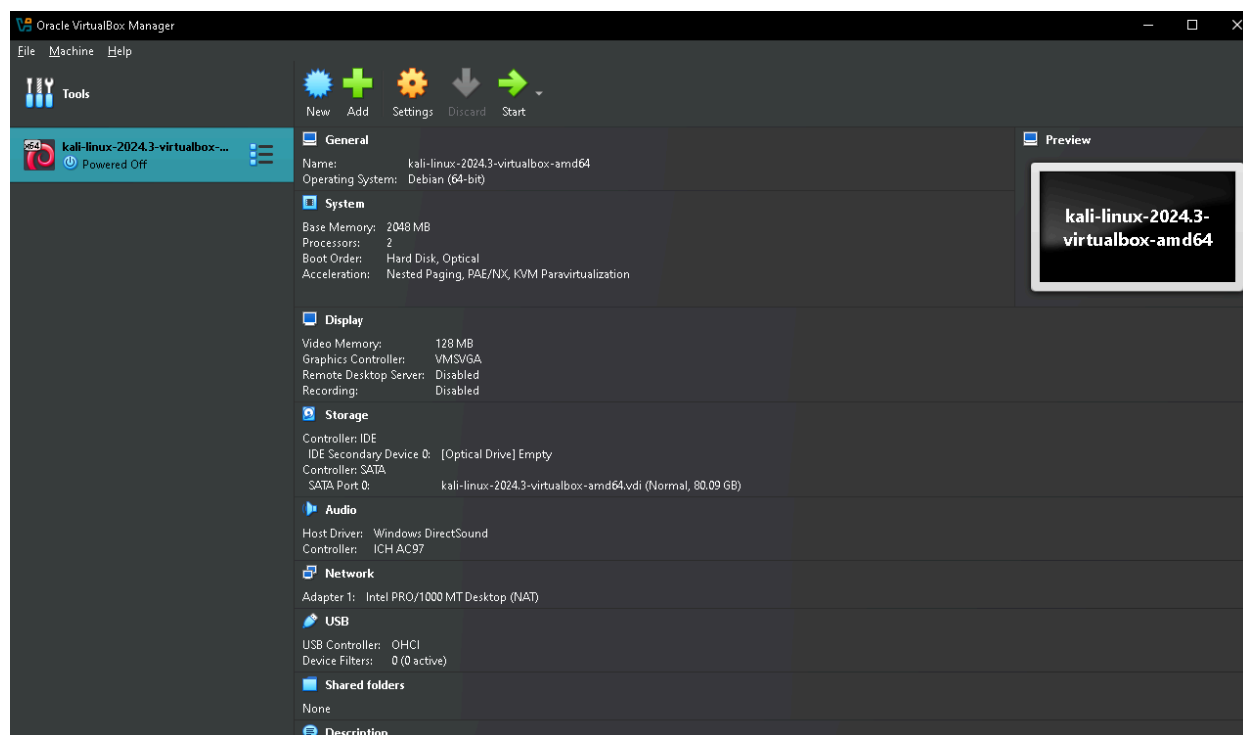


First, I installed a Kali Linux virtual machine into Oracle's VirtualBox:



Next, I install the Elastic Cloud agent through the Kali terminal:

```
(kali㉿kali)-[~/Desktop]
└─$ sudo curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://687d5af1ce2b4a28a0304c6fbeb3c396.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFBRsXk0Y0JuQXg5M2YxVXc5VmM6czBqdEk3Y3VUX2VEaV90d0hmejNxQQ==
[sudo] password for kali:
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload   Total   Spent    Left   Speed
0          0    0     0    0     0      0      0  --:--:--  --:--:--  --:--:-- 
0          0    0     0    0     0      0      0  --:--:--  --:--:--  --:--:-- 
0  407M    0  346k    0     0   214k      0  0:32:20  0:00:01  0:32:19  214
0  407M    0 1695k    0     0   567k      0  0:12:14  0:00:02  0:12:12  567
```


Once the agent was successfully installed, I ran a few nmap scans to generate some security events to log:

Once logs started being collected, I created a Dashboard. For the visualization, I include the Timestamp on the horizontal axis, and the count of records on the vertical axis:

Horizontal axis



Data

Functions 

Date histogr...

Intervals •

Filters

Top values •

Field

@timestamp



☒ Include empty rows

Vertical axis



Data

Method

Quick function

Formula

Functions

Average •

Count

Counter rate •

Cumulative sum

Differences

Last value •

Maximum •

Median •

Minimum •

Moving aver...

Percentile •

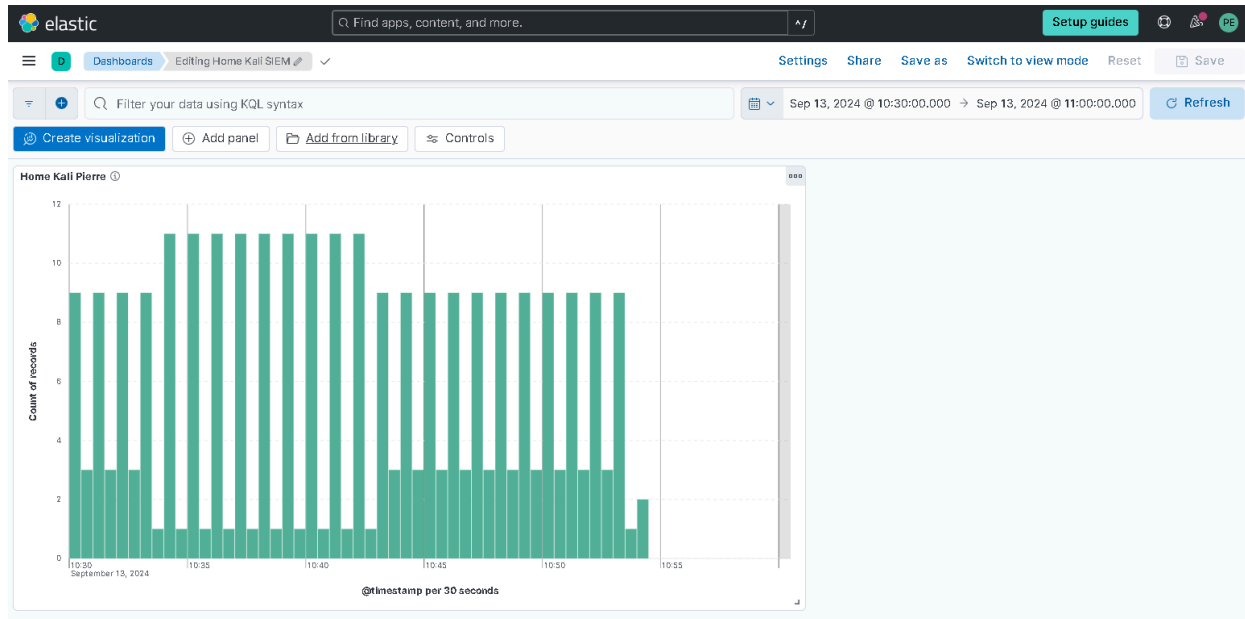
Percentile rank •

Standard deviation

Sum •

Unique count •

For the visualization type, I chose a bar stack, resulting in this dashboard:



Next, I start setting up an alert. Here I create a rule with a custom query **event.action: "nmap_scan"** :

The screenshot shows the Elastic Security console interface. The top navigation bar includes the Elastic logo, a search bar, and links for 'ML job settings' and 'Add integration'. The left sidebar contains a 'Security' section with a list of items: Dashboards, Rules (selected), Alerts, Attack discovery, Findings, Cases, Timelines, Intelligence, and Explore. The main content area is titled 'Edit rule settings' and includes a 'Rule preview' button. Below the title are tabs for 'Definition', 'About', 'Schedule', and 'Actions'. The 'Definition' tab is active, showing a 'Rule type' section with a 'Custom query' option selected. The 'Source' section indicates the rule uses 'Index Patterns' and provides a list of patterns: 'apm-*transaction*', 'auditbeat-*', 'endgame-*', 'filebeat-*', 'logs-*', 'packetbeat-*', 'traces-apm*', 'winlogbeat-*', and '*elastic-cloud-logs-*'. The 'Custom query' section shows the query 'event.action: "nmap_scan"'.

elastic

Find apps, content, and more.

Security Rules Detection rules (Sl... Nmap Scan Edit

ML job settings Add integration

Security

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Timelines

Intelligence

Explore

Back to Nmap Scan

Edit rule settings

Rule preview

Definition About Schedule Actions

Definition

Rule type

Custom query
Use KQL or Lucene to detect issues across indices.

Selected

Source

Use Kibana [Data Views](#) or specify individual [index patterns](#) as your rule's data source to be searched.

Index Patterns Data View

Index patterns

apm-*transaction* x auditbeat-* x endgame-* x filebeat-* x logs-* x packetbeat-* x

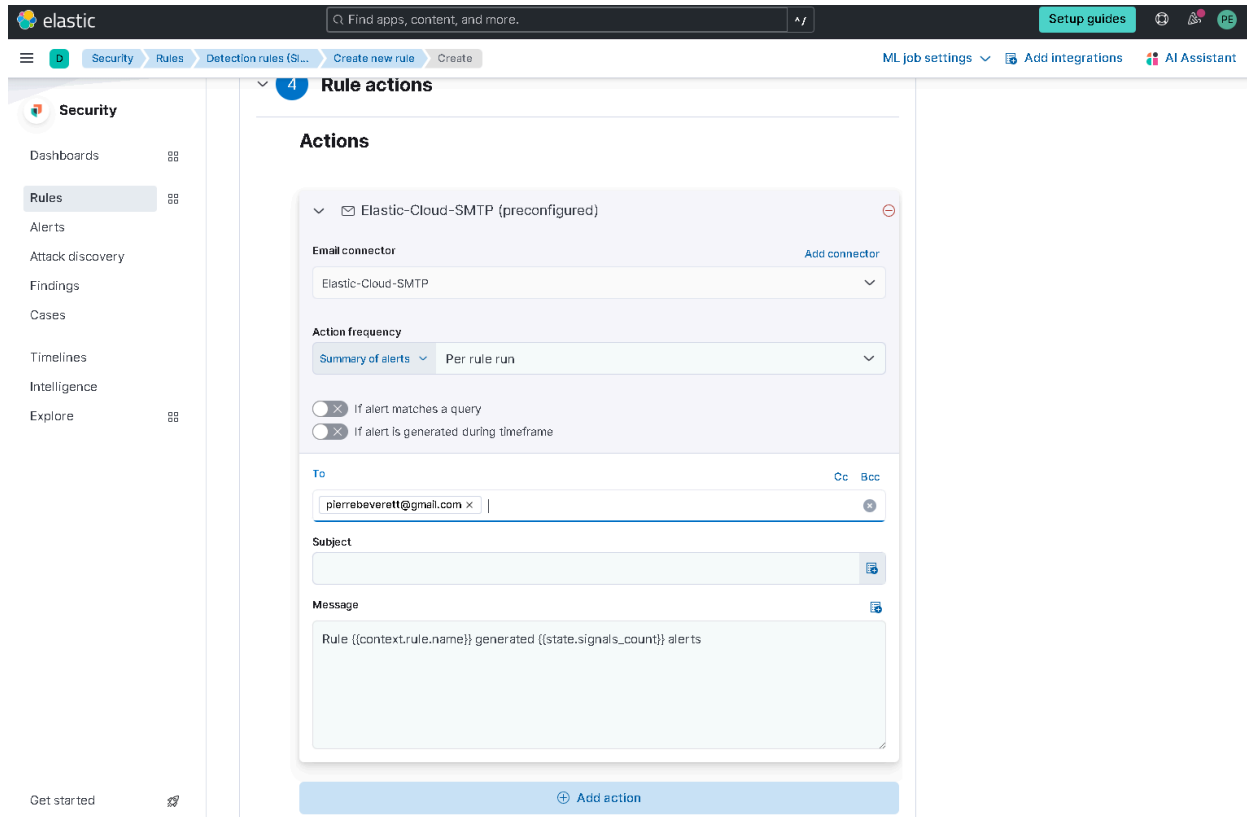
traces-apm* x winlogbeat-* x *elastic-cloud-logs-* x

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query [Import query from saved timeline](#)

event.action: "nmap_scan"

Finally, I configure what action is taken when the rule is triggered. In this case, an email will be sent to the recipient:



The alert is configured and running:

