

3- Create job wizard, select the kibana_sample_data_ecommerce index pattern.

elastic

Find apps, content, and more.

Machine Learning

Anomaly Detection

Create job

Machine Learning

Overview

Notifications

Memory Usage

Anomaly Detection

Jobs

Anomaly Explorer

Single Metric Viewer

Settings

Data Frame Analytics

Jobs

Results Explorer

Analytics Map

Model Management

Trained Models

Data Visualizer

File

Select data view or saved search

Search...

Types

Type

Title

[eCommerce] Orders

Kibana Sample Data eCommerce

<

1

>

4-7 -If you view the earlier dates in your results, you will see two critical anomalies - they appear red in both the line graph and the table of anomalies.

elastic

Find apps, content, and more.

Machine Learning

Anomaly Detection

Single Metric Viewer

Machine Learning

Overview

Notifications

Memory Usage

Anomaly Detection

Jobs

Anomaly Explorer

Single Metric Viewer

Settings

Data Frame Analytics

Jobs

Results Explorer

Analytics Map

Model Management

Trained Models

Data Visualizer

File

Single Metric Viewer

Dec 21, 2023 @ 01:04:19.000 → Jan 5, 2024 @ 11:21:05.057

Updating

average_total_price

Edit job selection

Detector

mean(taxful_total_price)

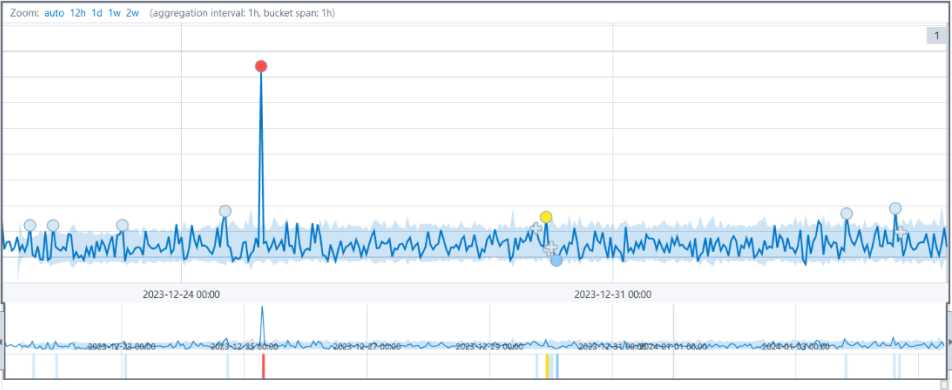
Forecast

Single time series analysis of avg taxful_total_price

show model bounds

annotations

Zoom: auto 12h 1d 1w 2w (aggregation interval: 1h, bucket span: 1h)



> Annotations Total: 1

Anomalies

Severity warning Interval Auto

Time	Severity	Detector	Actual	Typical	Description	Actions
> December 25th 2023	92	mean(taxful_total_price)	\$420.98	\$67.64	6x higher	
> December 29th 2023	46	mean(taxful_total_price)	\$127.61	\$70.58	2x higher	
> December 30th 2023	3	mean(taxful_total_price)	\$43.54	\$70.33	2x lower	
> December 21st 2023	< 1	mean(taxful_total_price)	\$111.83	\$68.56	2x higher	
> January 4th 2024	< 1	mean(taxful_total_price)	\$98.49	\$72.09	1.4x higher	
> January 3rd 2024	< 1	mean(taxful_total_price)	\$134.37	\$71.13	2x higher	
> December 23rd 2023	< 1	mean(taxful_total_price)	\$111.8	\$67.57	2x higher	
> December 24th 2023	< 1	mean(taxful_total_price)	\$139.33	\$68.29	2x higher	

Rows per page: 25

< 1 >

5-e- Create a new user named read_only_user

elastic

Find apps, content, and more.

Stack Management

Users

Create

Machine Learning

Watcher

Maintenance Windows

Security

Users

Roles

API keys

Role Mappings

Kibana

Data Views

Files

Saved Objects

Tags

Search Sessions

Spaces

Advanced Settings

Stack

License Management

Upgrade Assistant

Create user

Profile
Provide personal details.

Username
read_only_user

Full name
Read Only User

Email address
ayoub.guebli@univ-constantine2.dz

Password
Protect your data with a strong password.
nonprodpwd
Password must be at least 6 characters.

Confirm password
nonprodpwd

Roles
read_only × kibana_admin ×
[Learn what privileges individual roles grant.](#)

Create user Cancel

10-a- Under the Management heading, click on the Fleet section

elastic

Find apps, content, and more.

Fleet

Agents

Send feedback

Fleet

Centralized management for Elastic Agents.

Agents

Agent policies

Enrollment tokens

Data streams

Settings

Add Agent

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#)

Add Fleet Server

10-f- logs-* Data view

elastic

Find apps, content, and more.

Discover

New

Open

Share

Alerts

Inspect

Save

logs-*

Filter your data using KQL syntax

Last 15 minutes

Refresh

Search field names

0

Available fields

70

@timestamp

agent.build.original

agent.ephemeral_id

agent.id

agent.name

agent.type

agent.version

cloud.account.id

cloud.availability_zone

cloud.image.id

cloud.instance.id

cloud.instance.name

cloud.machine.type

cloud.project.id

cloud.provider

Add a field

191 hits

Break down by

Select field

100

80

60

40

20

0

11:14

11:15

11:16

11:17

11:18

11:19

11:20

11:21

11:22

11:23

11:24

11:25

11:26

11:27

11:28

January 6, 2024

Jan 6, 2024 @ 11:14:03.026 - Jan 6, 2024 @ 11:29:03.026 (interval: Auto - 30 seconds)

Documents

Field statistics

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

Document

Jan 6, 2024 @ 11:25:01.723

@timestamp

Jan 6, 2024 @ 11:25:01.723

agent.ephemeral_id

3aa8d8f7-0eaf-472d-8d22-de34dadfaa95

agent.id

150539f2-9c4b-4a75-b9b6-7fc9a85852fd

agent.name

DESKTOP-MNKGIVG

agent.type

filebeat

agent.version

8.10.4

component.id

fleet-server-default

component.state

HEALTHY

data_stream.dataset

elastic_agent

data_stream.namespace

default

data_stream.type

logs

ecs.version

8.10.0

Jan 6, 2024 @ 11:25:01.723

@timestamp

Jan 6, 2024 @ 11:25:01.723

agent.ephemeral_id

3aa8d8f7-0eaf-472d-8d22-de34dadfaa95

agent.id

150539f2-9c4b-4a75-b9b6-7fc9a85852fd

agent.name

DESKTOP-MNKGIVG

agent.type

filebeat

agent.version

8.10.4

component.id

fleet-server-default

Rows per page: 100

12

10-h- Enable the filtered rules of windows OS:

elastic

Find apps, content, and more.

ML job settings

Add integrations

AI Assistant

Security

Rules

Detection rules (SIEM)

Security

Dashboards

Rules

Alerts

Findings

Cases

Timelines

Intelligence

Explore

Get started

Manage

Rules

Add Elastic rules

Import value lists

Import rules

Create new rule

Installed Rules1027

Rule Monitoring1027

Rule name, index pattern (e.g., "filebeat-*"), or MITRE ATTÜC

Tags1

Last response3

Elastic rules (1027)

Custom rules (0)

Enabled rules

Disabled rules

Showing 1-20 of 452 rules

Selected 0 rules

Select

Search tags

Clear filters

Updated 3 seconds ago

On

Rule	Integrations	Tags	Score	Priority	Last run	Last response	Last updated	Notify	Enabled	
<input type="checkbox"/> Rule										
<input type="checkbox"/> Execution of File Written or Modif...	0/2 integrations	OS: Linux	21	High	50 minutes ago	Warn...	53 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Threat Intel Hash Indicator Match		OS: macOS	21	Criti...	49 minutes ago	Succ...	52 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Threat Intel Windows Registry In...		OS: Windows	21	Criti...	49 minutes ago	Succ...	52 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> PowerShell Script with Remote E...	0/1 integrations	Resources: Investigation Guide	21	Low	49 minutes ago	Warn...	52 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> PowerShell Script with Discovery...	0/1 integrations	Rule Type: BBR	21	Low	49 minutes ago	Warn...	52 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Threat Intel IP Address Indicator ...			99	Criti...	49 minutes ago	Succ...	52 minutes ago		<input checked="" type="checkbox"/>	...

Untitled timeline

<input type="checkbox"/> Threat Intel URL Indicator Match	3	99	Criti...	48 minutes ago	Succ...	51 minutes ago		<input checked="" type="checkbox"/>	...	
<input type="checkbox"/> Query Registry using Built-in Tools	0/1 integrations	6	21	Low	48 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> PowerShell Script with Password ...	0/1 integrations	7	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Execution of File Written or Modif...	0/2 integrations	7	73	High	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Binary Content Copy via Cmd.exe	0/1 integrations	7	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Potential Exploitation of an Unqu...	0/1 integrations	6	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Potential Process Injection from ...	0/1 integrations	8	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> WRITEDAC Access on Active Dire...	1/2 integrations	7	21	Low	47 minutes ago	Succ...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> WMIC Remote Command	0/1 integrations	6	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Unusual Process Execution on W...	0/1 integrations	6	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Office Test Registry Persistence	0/1 integrations	7	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> File or Directory Deletion Comma...	0/1 integrations	6	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Kirbi File Creation	0/1 integrations	6	21	Low	47 minutes ago	Warn...	51 minutes ago		<input checked="" type="checkbox"/>	...

Rows per page: 20

< 1 2 3 4 5 ... 23 >

The Question: as we see on the alerts table, we have 1 alert because of the rule “My First Rule”, and to see why we get this alert, we need to see this rule details, when we click on this rule,

The screenshot shows the Elastic Security Alerts page. The left sidebar has 'Alerts' selected. The main content area shows a filter for 'kibana.alert.severity: low'. The 'Alerts' section has a 'Summary' tab selected, showing a 'Severity levels' gauge with 'Low' at 1, an 'Alerts by name' table with 'My First Rule' at 1, and a 'Top alerts by' bar chart for 'host.name' showing 'desktop-mnvgivg' at 100%. Below this is a table with 1 alert:

Actions	@timestamp	Rule	Severity	Risk Score	Reason
[icon]	Jan 6, 2024 @ 15:01:07.629	My First Rule	low	21	event on desktop-mnvgivg created low alert My First Rule.

we get the details, and we see description about this rule, “This rule helps you test and practice using alerts with Elastic Security as you get set up. It’s not a sign of threat activity “ ,so this alert was just a test ,

The screenshot shows the 'My First Rule' details page. The left sidebar has 'Rules' selected. The main content area shows the rule name 'My First Rule' with a status 'Enable' and an 'Edit rule settings' button. Below this is a description: 'This rule helps you test and practice using alerts with Elastic Security as you get set up. It’s not a sign of threat activity.' The 'About' section shows the rule's author as 'Elastic', severity as 'Low', and risk score as '21'. The 'Definition' section shows the index patterns and custom query.

About

This rule helps you test and practice using alerts with Elastic Security as you get set up. It’s not a sign of threat activity.

Author Elastic

Severity Low

Risk score 21

Definition

Index patterns

- apm-*transaction*
- auditbeat-*
- endgame-*
- filebeat-*
- logs-*
- packetbeat-*
- traces-apm*
- winlogbeat-*
- *elastic-cloud-logs*

Custom query event.kind:event

Rule type Threshold