

# Fixing Dashboard Mapping

Management → Kibana → Saved → Object

If any component of docker get updated, Kibana re-add all the dashboard. It is important to delete them by searching in the search bar: `cowrie dshield`.











Select and delete them all and download the current map and manually upload it in this same location. Go to this directory: <https://github.com/bruneaug/DShield-SIEM/tree/main/scripts>

The file to download is: `dshield_sensor_8.11.1.ndjson`

## Before you Delete

### Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated

<input type="checkbox"/>	Type	Title	Tags
<input type="checkbox"/>		DShield	
<input type="checkbox"/>		cowrie*	
<input type="checkbox"/>		DShield Sensor Map - Unique IP by Country	<span>DShield</span>
<input type="checkbox"/>		DShield Logs	
<input type="checkbox"/>		[Logs DShield Sensor] Overview	
<input type="checkbox"/>		DShield Sensor	
<input type="checkbox"/>		cowrie*	
<input type="checkbox"/>		DShield Sensor Map - Unique IP by Country	<span>DShield Sensor</span>
<input type="checkbox"/>		DShield Logs	<span>DShield Sensor</span>
<input type="checkbox"/>		.alerts-security.alerts-default,apm-*~transaction*,auditbeat-* endgame-*,filebeat-*,logs-*,packetbeat-*,traces- apm*,winlogbeat-*,-*elastic-cloud-logs-*	

## After you Imported the Updated Dashboard

The result will look like this after the JSON has been re-imported (6 Titles):

### Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

dshield cowrie

Type

Title

Tags

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

DShield

cowrie\*

DShield Sensor Map - Unique IP by Country

DShield

DShield Logs

[Logs DShield Sensor] Overview

I have also added cowrie\* in the first Title. By adding cowrie\*, it is now used by the Security → Rules to track threat intelligence matches by the SIEM part of Elastic. The minimum of 4 rules that are needed will also be listed in Management → Alerts and Insights → Rules

4 rules									
<input type="checkbox"/>	Name	Last run	Notify	Interval	Duration	P50	Success ratio	Last response	State
<input type="checkbox"/>	Threat Intel Hash Indicator Match Indicator Match Rule	3 Mar 22, 2024 10:52:14am 37 minutes ago		1 hr	00:02	00:02	100%	Succeeded	<span>Enabled</span>
<input type="checkbox"/>	Threat Intel IP Address Indicator Match Indicator Match Rule	3 Mar 22, 2024 10:52:17am 37 minutes ago		1 hr	00:00	00:00	100%	Succeeded	<span>Enabled</span>
<input type="checkbox"/>	Threat Intel URL Indicator Match Indicator Match Rule	3 Mar 22, 2024 10:52:20am 37 minutes ago		1 hr	00:00	00:00	100%	Succeeded	<span>Enabled</span>
<input type="checkbox"/>	Threat Intel Windows Registry Indicator Match Indicator Match Rule	3 Mar 22, 2024 10:52:17am 37 minutes ago		1 hr	00:00	00:00	100%	Succeeded	<span>Enabled</span>

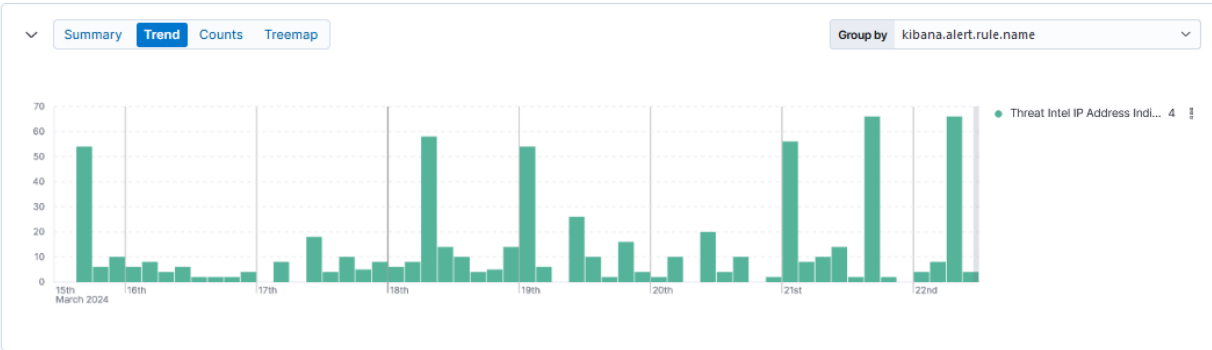
# Security → Alerts

## Alerts

Assignees

Manage rules

Status open 1 Severity User Host



Columns 1 field sorted 682 alerts Updated 10 seconds ago Additional filters Grid view Group alerts by: None

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name
<input type="checkbox"/>	Mar 22, 2024 @ 10:23:03.982	Threat Intel IP Address Indi...	critical	99	network event with source 192.168.25.28:8080, destination 84.54.51.37:...	—
<input type="checkbox"/>	Mar 22, 2024 @ 10:23:03.974	Threat Intel IP Address Indi...	critical	99	network event with source 84.54.51.37:59521, destination 192.168.25.2...	—
<input type="checkbox"/>	Mar 22, 2024 @ 10:23:03.965	Threat Intel IP Address Indi...	critical	99	network event with source 192.168.25.28:8080, destination 84.54.51.37:...	—
<input type="checkbox"/>	Mar 22, 2024 @ 10:23:03.956	Threat Intel IP Address Indi...	critical	99	network event with source 84.54.51.37:37594, destination 192.168.25.2...	—