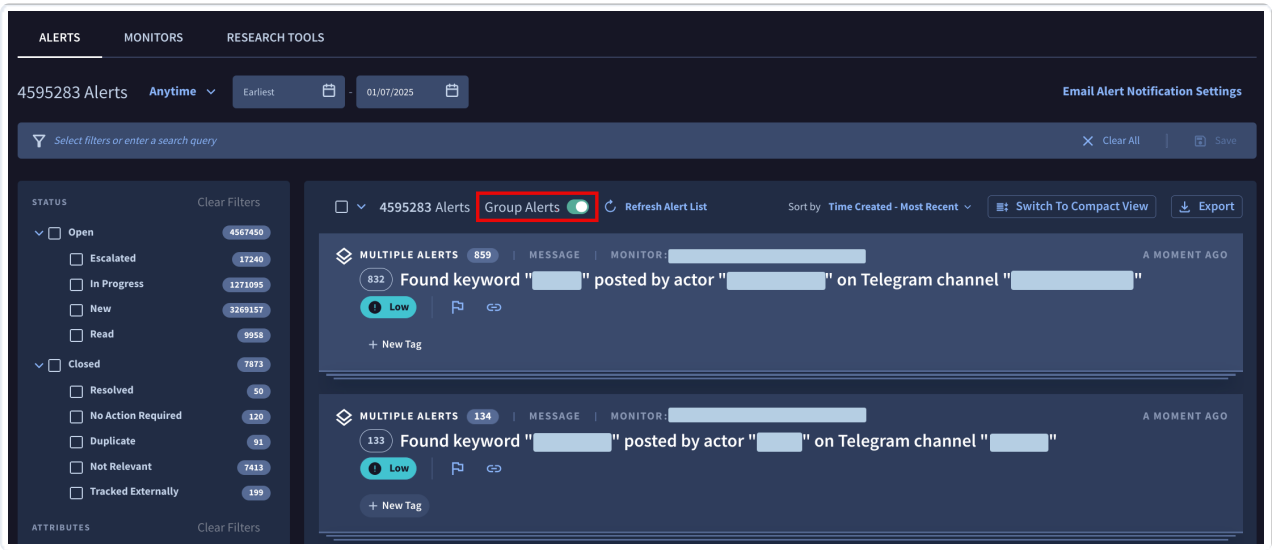
GROUP ALERTS

In Digital Threat Monitoring (DTM), similar Alerts can be grouped. This makes it easier for users to triage a large volume of related Alerts. They can determine when they have already investigated a case, track how the case is evolving, and view related findings.

To group Alerts, in Digital Threat Monitoring (DTM), toggle the **Group Alerts** setting to on.



DTM Alerts dashboard showing two buckets of grouped Alerts

The following restrictions exist for Alert grouping:

- Alerts are grouped per Alert Type, and grouping is only available for the following Alert Types:
  - Documents
  - Emails
  - Forum Posts
  - Messages
  - Pastes
  - Web Content
- Alerts are grouped on a per-Monitor basis. Alert buckets are unique to a single monitor, and there are not any alert buckets that contain child Alerts from multiple monitors.
- There is a fixed look-back time of 60 days. This means that if an alert bucket has not been updated in 60 days, a new bucket is created to group Alerts.

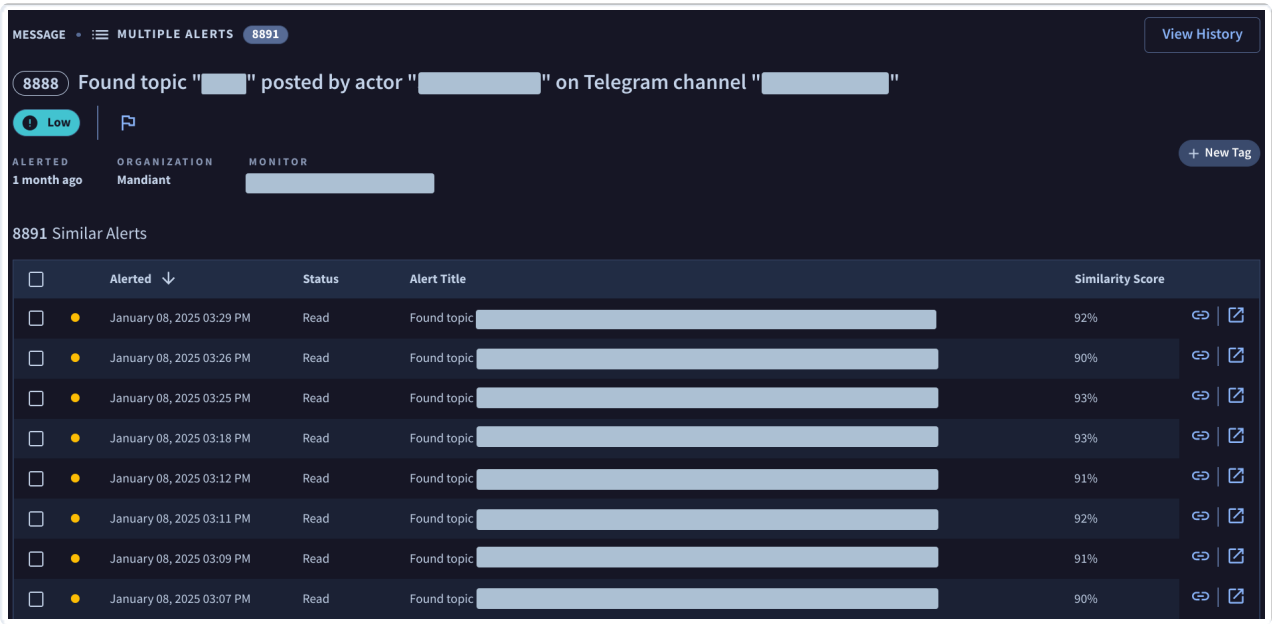
Similarity Score

Each Alert in DTM has a Similarity Score. Similarity Score is calculated by reviewing the document that generated the Alert and comparing the textual content to other alert documents. Therefore, similarity is a computation of how similar the content is between the documents that triggered Alerts. If a Similarity Score is 90% or higher in relation to another Alert, those Alerts are grouped together.

Alert buckets

When you select a bucket of grouped Alerts, you are presented with a table of Alerts that have been grouped together. This table includes a row for each Alert, along with a Similarity Score to let you know how closely related each Alert is to

the title Alert of the bucket.



An alert bucket view showing a table with multiple Alerts

Alert buckets are limited to 10,000 Alerts. Once a bucket exceeds 10,000 Alerts, a new bucket is created for additional Alerts that are similar. Therefore, you could see more than one alert bucket for the same set of similar content.