# WORK WITH ALERTS

Digital Threat Monitoring (DTM) continuously ingests documents from the deep and dark web to search for mentions of topics or entities that you designate in Monitors. When content in a collected document matches the conditions that you define in one of your Monitors, an Alert is created. The new Alert is displayed in the DTM **Alerts** tab.

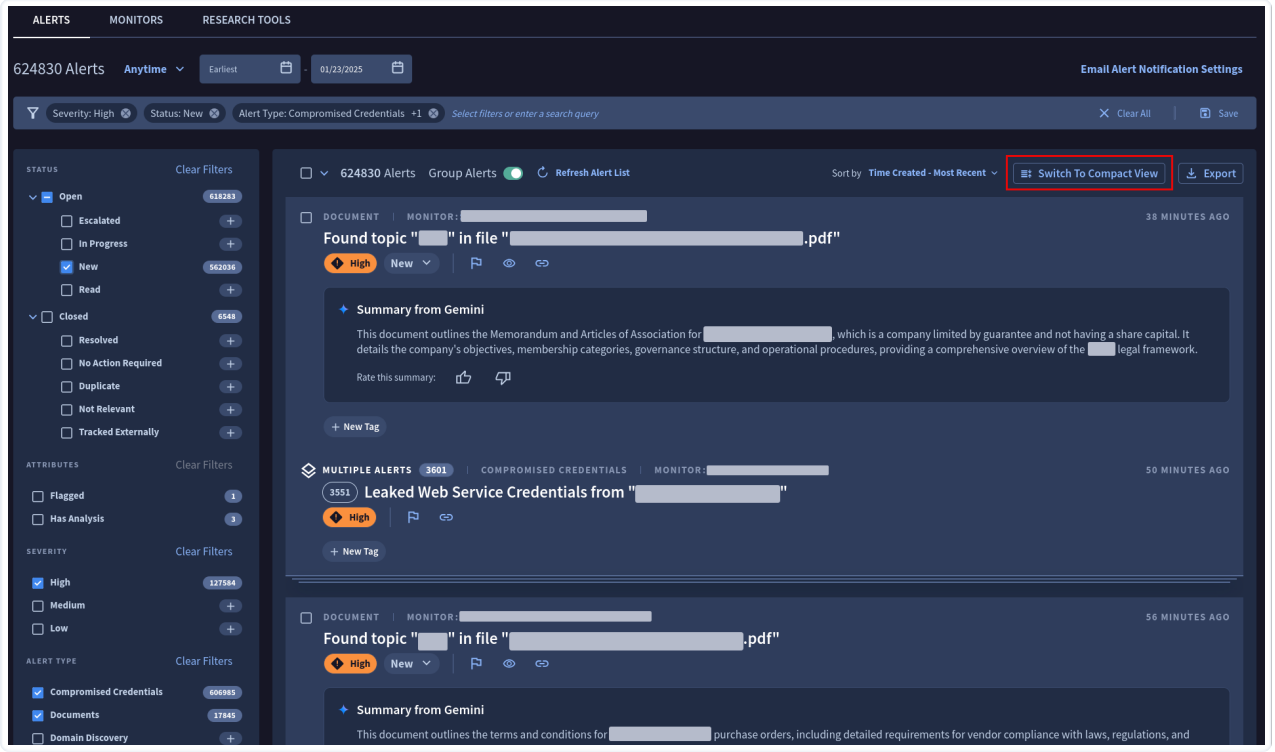
DTM provides numerous capabilities to filter and triage these Alerts to help you focus on the ones that matter most. You can update and enrich Alerts directly in DTM during your investigation to further streamline response and mitigation efforts across your organization.

Email notifications can be sent when Alerts are created or modified. For more information, see **Configuring DTM Email Notifications** (https://docs.mandiant.com/home/dtm-email-notifications).

## View Alerts

To view Alerts in DTM:

1. Sign into the **Mandiant Advantage Threat Intelligence (MATI) platform** (https://advantage.mandiant.com/).
2. Click the **Digital Threat Monitoring** tab to see the **Alert List** of all Alerts.




The DTM Alerts dashboard

### Group Alerts

Alerts can be grouped into buckets based on similarity using the Group Alerts feature. Alert grouping is not available for all Alert Types. See **Group Alerts** (https://docs.mandiant.com/home/dtm-group-alerts) for more information.

Mandiant

### Summary from Gemini

This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to **Support.** (https://docs.mandiant.com/home/mandiant-support-cases)

Each Alert overview provides you with a variety of information including a **Summary from Gemini**. This summary blurb is AI generated.

- The AI **Summary from Gemini** is only available in the Standard View (which is your view when you see the **Switch To Compact View** option).
- **Summary from Gemini** is not available for all alert types. Summaries are only available for the following alert types:
  - Documents
  - Emails
  - Forum Posts
  - Messages
  - Pastes
  - Web Content
- If you want to turn off the AI **Summary from Gemini**, submit a **support** (https://docs.mandiant.com/home/mandiant-support-cases) request.

### Alert Details

Select any Alert to view additional information beyond what's displayed in the **Alert List.**


Your view varies depending on the **Alert Type** of the Alert you have selected. Still, all Alerts have a similar workflow for exploring the context surrounding where the monitored content was found in the source material.

- The **Overview** tab includes the following sections:
  - **Characterization**: Details about the **Content**, **Language**,**Type**, and **Threat** associated with the Alert.
  - **Source Information**: Information about the source document that matched the Monitor conditions.
  - **Content**: Details about where matched or discovered content was found in the source document.
- The **Entities** tab shows a consolidated view of all the Entities that were either matched or discovered in the document.

- The < >**Raw (JSON)** tab provides the option to download the entire Raw JSON as a TXT file.

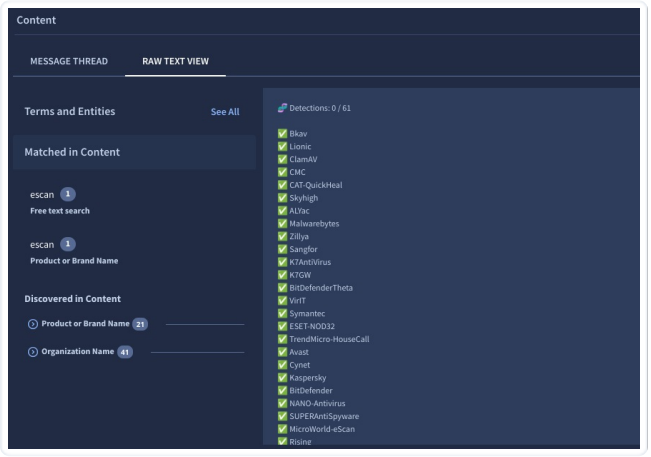
---

### Alert Deep Dive

The following example is specific to a **Message** Alert.

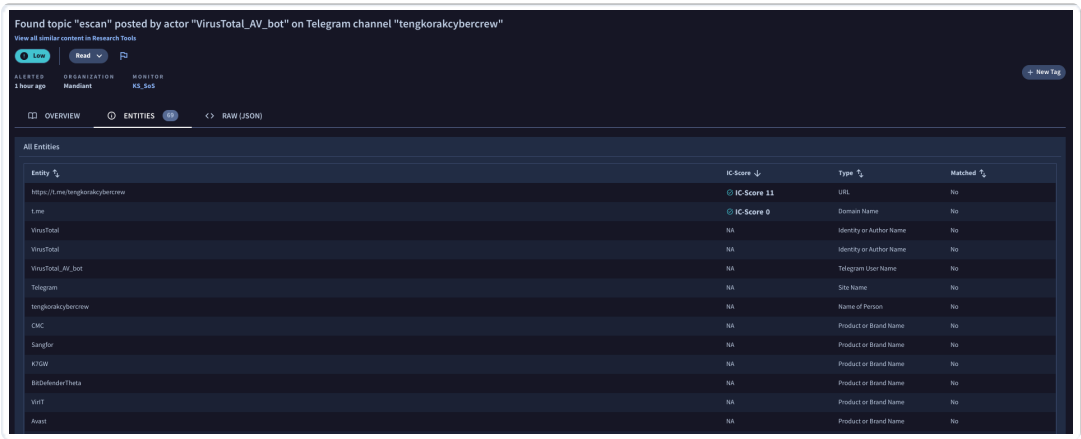
- In the **Content** section of the **Overview** tab:
  - Select the **Message Thread** tab to view the complete message thread, with the option to **Scroll to Highlighted Message**.


  - Click the **Raw Text View** tab to view specific identifiers that have been located throughout the source document.
    - **Matched in Content** lets you highlight the section of the content where text specified in the Monitor conditions has been detected. Click each term to highlight it within the content.
    - **Discovered in Content** shows additional identifiers that were discovered in the Document. Click each term to highlight it within the content.




- Click the **Entities** tab to obtain a consolidated view of all the entities that were either matched or discovered in the Document. The table also displays the following:
  - **IC-Score**: If available, the Indicator Confidence Score (IC-Score) of the entity is listed. For more information, see **Understanding IC-Score (https://docs.mandiant.com/home/understanding-ic-score)**.
  - **Type**: The matched topic or entity name of each entity is shown. For more information, see **DTM Monitor & Research Tools Fields (https://docs.mandiant.com/home/dtm-monitor-fields)**.
  - **Matched**: Indicates whether the entity was matched to the Monitor conditions:

- **Yes**: The entity explicitly matched a condition defined in a Monitor.
- **No**: The entity didn't match a Monitor condition but was discovered in the Document as a known Entity or Topic identifier.




> The **Entities** tab header displays the total count of entities present in the document.

- The raw JSON can be downloaded for external use. To download, select the **Raw (JSON)** tab, then click **Download**.

> To help read the raw JSON interactively, the **Fold line** option is provided to collapse JSON objects, if desired.


- Optional: To look at similar content, click **View all similar content in Research Tools** . This step creates a new Research Tools query.

> This functionality is not supported for Compromised Credentials, Domain Discovery, or Shop Listings alert types.

## Filter Alerts

DTM provides several ways to help you filter out extraneous Alerts and focus only on Alerts of interest:

1. Sign into the **Mandiant Advantage Threat Intelligence (MATI) platform (https://advantage.mandiant.com/)**.
2. Select the **Digital Threat Monitoring** tab.

3. Select the **Alerts** tab.
    - Optional: Specify a time period to be applied to all additional filters.
    - Enter a search query in the **Add a Filter** bar.

      > Lucene syntax is supported for search queries. For more information, see **Lucene Queries in DTM (https://docs.mandiant.com/home/dtm-lucene-queries)**.

    - Select filters from the nested **Filter By** menu in the **Add a Filter** bar.
    - Select one or more filter checkboxes in the **Filters** pane.
4. Click **Clear All** to remove all filters.
5. Click **Save** to make the new filtered view your default view upon login.

---

### Filter descriptions

The **Filters** pane displays all available filters and subfilters at a glance:

- **Status**: Filter Alerts based on their status within the broader categories of **Open** or **Closed**.
    - **Open**: Alerts that are new or currently being worked.
        - **Escalated**: An analyst has completed their investigation of the Alert and escalated to the Customer, a third party, or another Mandiant organization for further action.
        - **In Progress**: The Alert is actively being triaged.
        - **New**: The Alert has not been viewed and therefore no triage has been performed.
        - **Read**: The Alert has been viewed but no additional action has been logged.

          > This status is automatically applied when a New Alert has been opened by any user.

    - **Closed**: Alerts that have been triaged and require no further action.
        - **Resolved**: The Alert has been triaged and the underlying cause has been addressed.

          > This status is applied to all Alerts that were marked Closed in previous releases of DTM.

        - **No Action Required**: The Alert has been reviewed and explicitly determined to require no action.
        - **Duplicate**: The Alert is duplicative of another Alert that is already being investigated.
        - **Not Relevant**: The Alert is valid based on matched Monitor conditions but is not a cause for concern and requires no action.
        - **Tracked Externally**: The Alert is being triaged in another system outside of DTM.
- **Attributes**: Filter based on Alert-specific properties that can be manually enabled to aid in further investigation or mitigation efforts.
    - **Flagged**: Alerts selected for follow-up using the **Flag for follow-up** feature.
    - **Has Analysis**: Alerts that have been reviewed by an analyst.
- **Severity (https://docs.mandiant.com/home/dtm-alert-severity-definitions-and-examples)**: Filter Alerts according to their Severity (High, Medium, or Low). Severity scoring models combine data science and Mandiant expertise to help you prioritize response efforts and resources. The Severity score identifies how urgently actionable an alert is based on factors such as the following:
    - Degree of potential damage
    - Ease and likelihood of exploitation

    - Number of false positives in a typical environment

- **Alert Type**: Filter on Alert Type, which is based on the type of source Document that matched a Monitor condition.
    - **Compromised Credentials**: Specific user account logins and passwords detected in compromised credentials data collected from the deep and dark web.
        - **Group Alerts** (https://docs.mandiant.com/home/dtm-group-alerts): Click the **Group Alerts** toggle to the on or off position, depending on whether you want to group or ungroup Alerts.
    - **Documents**: Includes the following file types:
        - docx
        - xlsx
        - PDF
        - ppt/pptx
        - rtf
        - ppsx
        - odf
    - **Domain Discovery**: Newly registered domains detected in open source DNS record databases such as **WhoisDS** (https://www.whoisds.com/) and **ZoneFiles** ().
    - **Emails**: Phishing, spam, or communications including sensitive information.
    - **Forum Posts**: Posts in cybersecurity forums on the deep and dark web.
    - **Messages**: Chat messages in cybersecurity groups using messaging services such as Telegram.
    - **Pastes**: Content that is pasted to websites that let users store and share plain text data such as code snippets, configuration files, or scripts.
    - **Shop Listings**: Items for sale on the deep and dark web, especially stolen payment cards and known hosts for attacker access.
    - **Tweets**: Messages from the Twitter microblogging site with a focus on cybersecurity relevance.
    - **Web Content**: Cybersecurity-based information collected from the open internet.

- **Monitors**: Filter Alerts based on specific Monitors that you've created.

### Triage and add Analysis to Alerts

DTM offers numerous features to update Alerts during your investigation to streamline response, mitigation, and auditing efforts.

The following capabilities can be performed in the **Alerts List** view or by selecting specific Alerts and updating each directly:

- Flag Alerts
- Bulk Edit Alerts
- Add tags to Alerts

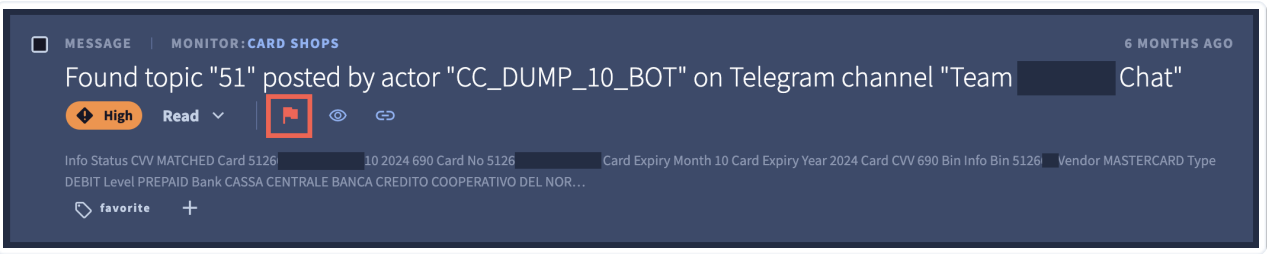
The following capabilities can only be performed by selecting specific Alerts and updating each directly:

- Add Analysis
- View History

---

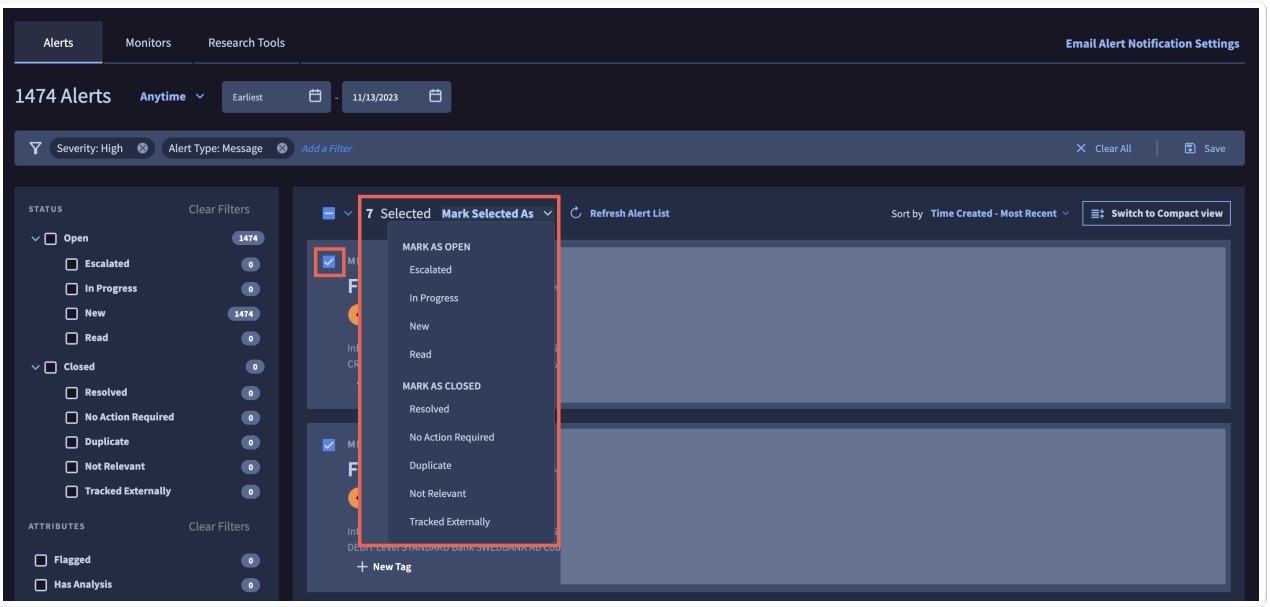
#### Flag Alerts

This feature lets you flag Alerts for easy reference or to be filtered for later follow up. Click **Flag for follow-up** to designate Alerts for follow up.



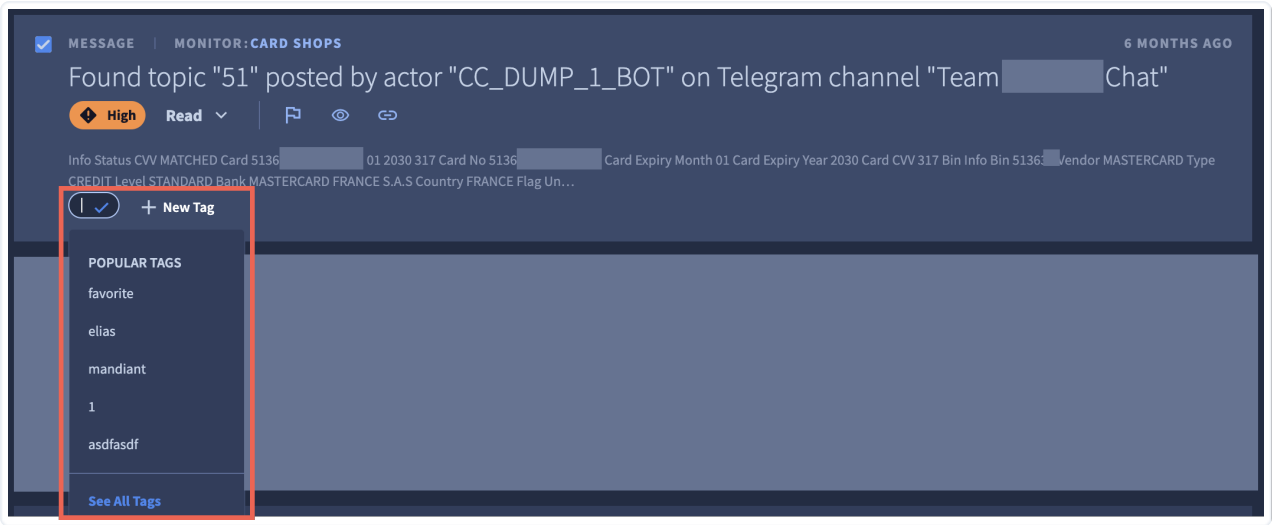

### Bulk edit Alerts

This feature streamlines Alert triage by letting you update the status of multiple Alerts at the same time. Select the Alerts to be updated and click **Mark Selected As** to update the status of all designated Alerts simultaneously.

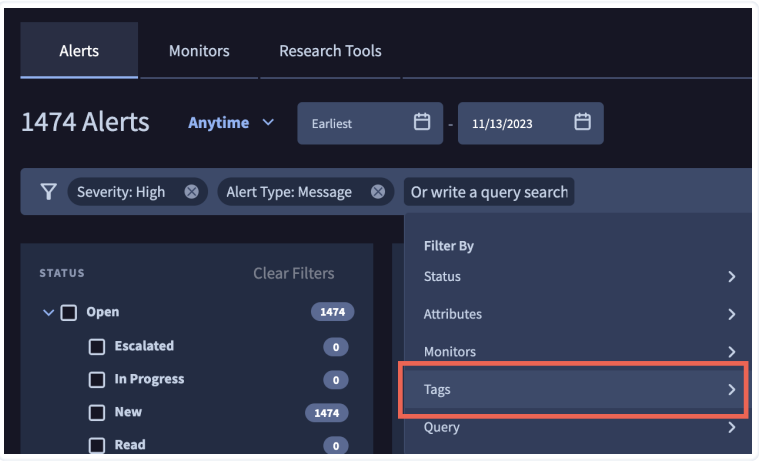



### Add Tags to Alerts

Tags are an simple way to correlate associated Alerts for easy reference, either by searching or filtering Alerts. Add tags to Alerts by clicking + **New Tag**. Enter a tag name to create a new tag, or select from the list of existing tags.



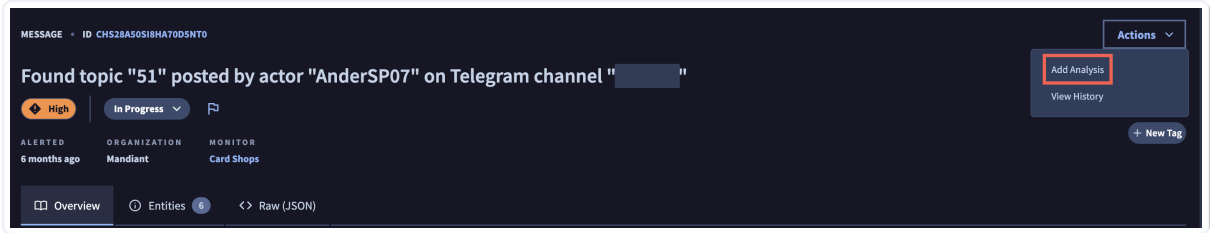

Tags can be used to filter Alerts by selecting **Tags** from the **Filter By** drop-down in the **+ Add a Filter** bar.




### Add an Analysis to an Alert

This feature lets you share additional information about the Alert and capture ongoing work to streamline the triage process. Perform the following workflow to add an Analysis to an Alert.

1. Select an Alert from **Alerts List.**
2. Choose **Add Analysis** from the **Actions** drop-down.




   An **Analysis** tab is automatically be added to the Alert.
3. Enter the **Intelligence Analysis** details using plain text or Markdown syntax.

   A preview of the rendered Markdown appears next to the **Intelligence Analysis** text field.

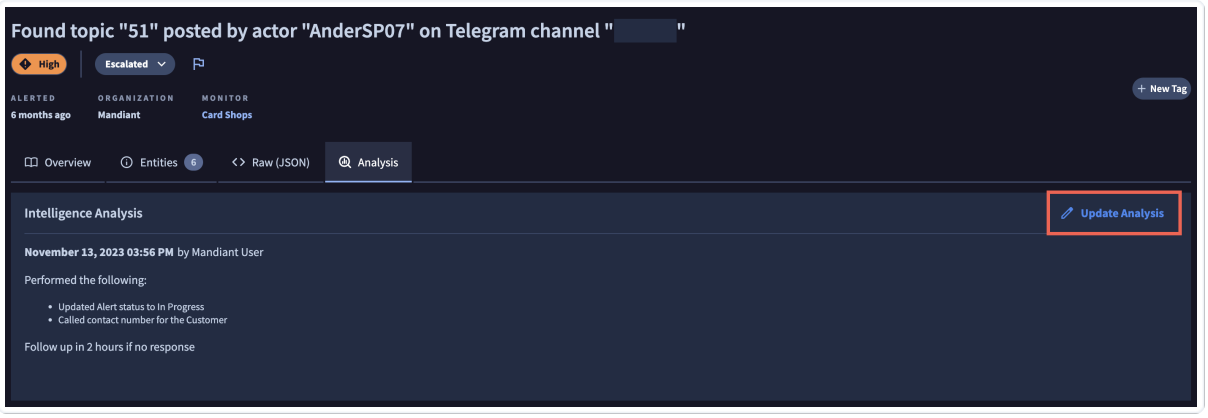
4. Include **Attachments** as needed.

   - There is a limit of five attachments per analysis.
   - Supported file types include: .doc, .docx, .xls, .xlsx, .pdf, .jpg, .png, .zip, .csv, or .txt files.
   - Maximum file size is 10 MB.

5. Click **Save**.


The following characteristics are applied to the Alert once an Analysis is added:

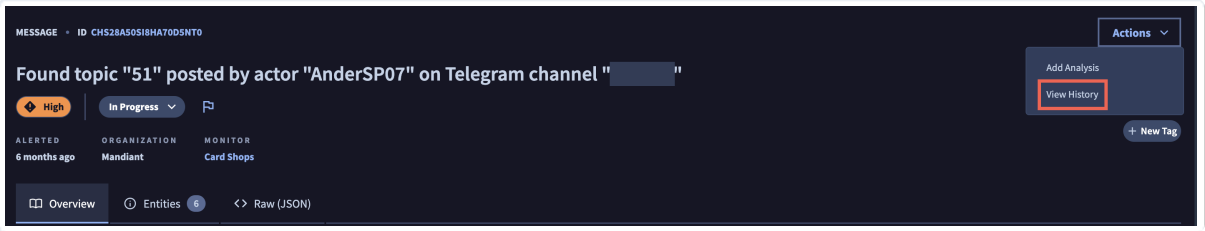
- The Alert is included in filter results when the **Attribute > Has Analysis** filter is selected.
- The status of the Alert is automatically updated to **Open > Escalated**.
- There is no built-in viewer for attachments, so they can only be viewed by downloading them and opening them in your viewer of choice.
- Any user in your DTM organization can update or delete an Analysis by clicking **Update Analysis**.




## View History of an Alert

DTM provides a clear audit trail of all modifications to an Alert. Perform the following workflow to view the history of updates to an Alert.

1. Select an Alert from **Alerts List**.
2. Choose **View History** from the **Actions** drop-down.




The **Alert History** modal is displayed, showing the date and timestamp for any of the following modification types and the user that made the changes:

- Status updates
- Addition or removal of tags
- Addition, update, or deletion of an Analysis