Creating an Incident

https://campus.barracuda.com/doc/79463562/

This functionality is available only with Barracuda Email Protection Premium and Premium Plus plans. To upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

Incident Response enables you to remediate emails based on criteria you provide. You can also remediate incidents based on User-Reported Emails and Geographical Insights. This process is also known as Manual Remediation. The system can address some incidents through Automatic Remediation.

Note that after you remediate an email in any way, that email will only be visible from within the incident on the Incidents page. The email will no longer appear in searches, on the location map, or in user-reported emails.

To use the Incident Response wizard to identify a new incident:

1. Log into Incident Response.
2. On the **Incidents** page, click **Create Incident**.
3. On the **Create Incident** page, enter criteria in one or more of the fields, then click **Search Messages**.

   For more information on searching with the **Email Subject**, see Searching for Messages.
   You can set default values for options within this wizard. See Manual Remediation Settings for details.

   - **Sender Email** – Search by sender name or domain name.
   - **Email Subject** – Search by full words in the subject line.
     - Select **Match exact phrase** (this is the default) to return only messages that include your search terms together, in the exact order shown in the Email Subject search field.
       - Example: searching for "fw: respond to invoices" would return results that include `fw: respond to invoices please`, but not `fw: please respond to invoices`.
     - If you *do not* select **Match exact phrase**, it will return messages that contain *any* of your search terms and words *related* to your search terms.
       - Example: searching for "fw: respond to invoices" would return results that include `fw: hello` and `invoiced customer` and `to the moon`.
   - **Message Body Text** – Search for full words in the message body. Words related to your search terms are also automatically searched.
   - **Message Body URL** – Search for emails that contain the URL entered here.
   - **Attachment Name** – Search for known or suspected malicious attachments by name. By default, words related to your search terms are also automatically searched. If you do not know the specific attachment name, you can search for the attachment type, like `txt` or

    `pdf`.
    - **Date** – Select from the Last 12 hours, Last 24 hours, Last 2 days, Last 7 days, or Last 30 days.
    - **Include emails that Barracuda Networks' Impersonation Protection moved to the Junk folder** – Select to search emails already flagged as suspicious by Impersonation Protection. (Available if you configured Impersonation Protection to send suspicious emails to users' Junk email folder.)

   Some or all of the search criteria fields are completed automatically if you are creating an incident from certain locations including user-reported emails or message log emails.

4. The **Review Messages** page displays all matching results for the entered criteria. Note that you can see whether an email was **Inbound**, addressed to someone in your organization, or **Outbound**, sent from someone in your organization.

   Optionally click the **View Message** (✉) icon to view a copy of an email in question, along with its header, attachment, and threat detail information. Threat details include DMARC, SPF, and DKIM information.
   Click **Back** to return to the **Review Messages** page.
5. If your search returned too many emails, click **Refine Search** to better target the suspicious mails. Return to Step 3, described above. Otherwise, proceed to Step 6.
   Click **Review Remediation Options**. On the **Incident Remediation - User Options** page, if needed, select one or more actions that affect users.
    - **Delete selected emails** *permanently* from affected users' inboxes. Note that you also have the option to delete the selected emails and turn on continuous remediation later when reviewing the incident in the Reviewing Incidents page.
        - **Turn on continuous remediation** for this incident to enable Incident Response to continuously search for emails matching your search criteria (from Step 3 above) for 72 hours. If matching emails are found, they will be added to the incident and Incident Response will attempt to delete them. After 72 hours, the feature automatically turns itself OFF.
          You must select **Delete selected emails** if you want to use continuous remediation.
    - **Send a warning email alert** to the affected users. Click **Edit Email Alert** to customize the message.
    - **Send incident summary** to your security team for tracking purposes. To change the recipient of the summary, from the Menu, select **Settings**. See Manual Remediation Settings.

   Optionally, add one or more custom Tags to this incident so you can easily identify it later. Click in the **Tags** field, type a tag, then press **Enter**. Repeat this process for additional tags. For more information, refer to the Tags section in Reviewing Incidents.
6. On the **Incident Remediation - Policy Options** page, if needed, select one or more actions that affect policies, then click **Next.**
    - **Add a sender policy to Quarantine/Block emails** – Adds a global policy in Barracuda Email Gateway Defense under **Sender Policies**. You can choose to add either a quarantine or block policy in two different ways:
        - *by sender* sets the policy for the unique sender(s) of these emails.
        - *by domain* sets the policy for all unique sending domain(s) of these emails.

If you include a comment, it will show alongside the new policy in Barracuda Email Gateway Defense.

  - `Added by Incident Response` will be included with the new policy if the comment field is left blank.

- **Block all user web traffic for domains contained in links** – Adds block exception policies for linked domains in your Barracuda CloudGen Access account, if you have an account. You can learn more about Incident Response and Creating Policies With Barracuda CloudGen Access.

  If you do not already have a CloudGen Access account, follow the **Learn More** link on the **Incident Remediation - Policy Options** page to sign up for a free 30 day trial.

7. Click **Remediate**. Note that some actions might take several minutes to complete. Review the suggested additional actions, including asking your end users to watch a video about suspicious emails from Security Awareness Training.

   > You can also remediate without selecting any of the actions above. Review and investigate the incident before deleting the emails in the Reviewing an Incident page.

8. Click **Close**.

Figures

1. mailPreview.png