Reviewing Incidents

https://campus.barracuda.com/doc/79463566/

The **Incidents** page displays all incidents for your Barracida account, along with the suspicious email associated with each incident.

When you first start using Incident Response, there are no incidents, so the main **Incidents** page has no data.

You can consider the **Incidents** page to be like a dashboard. Charts at the top of the page enable you to visualize the last six months of incidents and threats for your organization. Hover over a value in a chart to see the specific data.

- **Incidents Created** – Displays the number of incidents you created in the last six months. Data updated once per day.
- **Threats Remediated** – Displays the number of threats remediated by Incident Response in the last six months. Data updated once per day.
- **Top 5 Attacked Users** – Shows the five users in your organization who have received the most attacks. Data is updated once per day. You might consider evaluating why these users are attacked repeatedly and equip them with proper training in identifying threats and reporting them promptly. Barracuda Networks recommends Barracuda Networks Security Awareness Training.
  Note that if you have fewer than five users, fewer than five users are displayed.

Note that after an email has been remediated 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 review incidents:

1. Log into Incident Response.
2. In the left pane, click the menu (☰) icon to toggle the menu, and click **Incidents**.
3. On the **Incidents** page, locate the incident you want to investigate and click **View Incident**.
4. At the top of the page, view basic information about the incident, including your search criteria and how many messages were received by unique recipients. You can also view a list of remediation actions you chose to take on the reported incident displays.
   Note that you cannot turn on **Continuous Remediation** if you did not choose to delete messages when you created the incident.
5. Review, or optionally, add one or more custom **Tags** to this incident so you can easily identify it later. In the upper-right corner of the page, 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 below.
6. Select the **Emails** tab to view information about the emails involved in the incident.
   To focus on the information you want to find, you can choose to take the following actions:

        - **Sort**: Click a column heading to sort by that column. The first click sorts in ascending order. Click again to reverse the sort order to descending order. Click a different column heading to sort by that column instead. Note that you cannot sort by the **Status** column.
        - **Filter**: In a column heading, click the three dots ⋮ to specify filtering information for that column. Select whether you want a value to contain or *not* to contain the value you enter. Click **Filter** to apply the filter. You can apply filters to one or more columns. Columns with a filter applied display with a colored background. To clear a filter, click the three dots ⋮, then click **Clear**. Note that you can only filter the **Status** column by **Remediated**/**Not Remediated**. You cannot filter the **Received Date** column.

    Data displayed:

    - Dates emails were received
    - Whether the email was inbound (*to* your organization) or outbound (*from* your organization)
    - Sender emails
    - Affected Mailboxes (members of your organization affected by this incident)
    - Subjects
    - Status of actions taken, if any
      Status options include:

✅	Email successfully removed from the user's inbox, or User removed email from their inbox
❗	Email could not be removed from the user's inbox
↻✓	Email successfully removed from the user's inbox during Continuous Remediation
↻!	Email could not be removed from the user's inbox during Continuous Remediation
🕓	Actions pending
ⓘ	No remediation actions taken for this inbox/user

    A paper clip 📎 displays if the email has an attachment. You can see the attachment when you view the email.

7. Click **Delete Emails** to delete the emails after you have reviewed the incident. Note that this will not add sender policies in Email Gateway Defense or block traffic on Barracuda CloudGen Access. However, you can now enable Continuous Remediation after deleting emails.
8. Click **Export to CSV** to export all of the data – from all of the tabs – for this incident. Note: the check boxes on the left side have no effect on what data is exported. They are only used to Send a User List to Barracuda Security Awareness Training.
9. Click the plus icon ⊞ at the far left of a row to view a copy of the email in question, along with its header information, threat details, and attachments, if any.
10. Select the **Users** tab to view users involved in this incident and any actions they may have taken.
    - The check boxes on the left side are only used to Send a User List to Barracuda Security

    - Awareness Training.
    - **User type** can be either:
        - **Internal** – Part of your organization.
        - **External** – A recipient outside of your organization. Incident Response cannot detect whether External users interacted with messages and the *Clicked on links*, *Opened email*, *Replied to email*, and *Forwarded email* columns will be blank.
    - **Clicked on links** within the email – Requires that Link Protection in Email Gateway Defense is turned ON when the email is received.
        - **Undetected**: Email Gateway Defense does not process internal emails, so they appear as **Undetected** in Incident Response.
    - **Opened email**
    - **Replied to email** or **Forwarded email**
        - **Undetected**: Note that some values for **Replied to email** or **Forwarded email** might display as **Undetected**. This can happen if there is more than one email in an incident and it is not possible for Incident Response to be able to detect whether a user replied to or forwarded one of the specific messages.

11. Click **Create Training Group** to send a list of user email address you selected from the **Users** tab to Barracuda Security Awareness Training. See Send a User List to Barracuda Security Awareness Training for more information.
12. Select the **Threats** tab, if it is present. The **Threats** tab appears only for incidents that were resolved through automatic remediation. It displays:
    - **For malicious links**: The malicious URL that was included in the email, the type of attack the URL is identified to be, and the actual path of the malicious URL.
    - **For malicious attachments**: The attachment name, the category of malicious attachment, and any details about the attachment.
13. Select the **Clicked Links** tab. For one or more emails related to this incident, it displays:
    - **Received Date** – The date emails were received.
    - **Users Involved** – One or more users who received the emails.
    - **Message ID** – Barracuda Networks' unique identifier for emails.
    - **Subject** – The subject line of the emails.
    - **Clicked Link** – Whether the user clicked a link in the email.
    - **Clicked IP** – The target IP address of the link clicked by the user.
    - **Clicked User Agents** – Information associated with each user's browser that was used to click the link.

    Note that if one user in a group of multiple recipients clicks a link, this table displays that the link was clicked, but not necessarily by which recipient.
14. Click the **Incidents** breadcrumb at the top of the page, use the menu to select **Incidents**, or use your browser's Back button to return to the **Incidents** page.

Creating an Incident

Creating an incident is available only with Incident Response. For more information, see Overview of Email Protection Plans.

To create a new incident from within the **Incidents** page, refer to Creating an Incident.

Tags

You can add custom tags to your incidents to help you remember them later. For example, you might choose to add tags like *finance team* or *extortion attempt*. Tags are available in the following locations within Incident Response. You can only create and delete tags in certain locations.

Location/Action	Available	View Tags	Create/Delete Tags
Creating an incident	Premium and Premium Plus plans	✓	✓
Reviewing incident details	All plans	✓	✓
Reviewing table on the **Incidents** page	All plans	✓	

To create a tag:

Click in the **Tags** field and type a tag, then press **Enter**. Repeat this process for additional tags. You can use tags you defined previously by clicking in the **Tags** field and selecting from the Tags displayed in the list.

To delete a tag:

Click the associated **X** icon for that tag.

Tags can include up to 100 letters, numbers, and spaces.

Figures