Reviewing Incidents

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

The **Incidents** page displays all incidents for your Barracuda Forensics & Incident Response account, along with the suspicious email associated with each incident.

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 Barracuda Forensics & 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 recommends Barracuda PhishLine.
  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 Barracuda Forensics & 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. 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. Select the **Email** tab to view the following information. Click **Export to CSV** to export this data.
   - 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

6. A paper clip displays if the email has an attachment. You can see the attachment when you view the email.
7. Click the **Sample Email** icon to view a copy of the email in question, along with its header information, threat details, and attachments, if any.
8. Select the **Users** tab to view users involved in this incident and whether they:
   - **Clicked on a link** within the email – Requires that Link Protection in Barracuda Email Security Service is turned ON when the email is received.
     Undetected: Barracuda Email Security Service does not process internal emails, so they appear as **Undetected** in Barracuda Forensics & Incident Response.
   - **Opened** the email
   - **Replied to** the email or **Forwarded** the 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 Barracuda Forensics & Incident Response to be able to detect whether a user replied to or forwarded one of the specific messages.
9. 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.
10. 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.

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

Figures