Incidents

Armor Knowledge Base

Topics Discussed

To fully use this screen, you must have the following permissions assigned to your account:

- Read Security Offenses

The **Security Incidents** screen was deprecated on November 1, 2019.

To locate open or pending support tickets created prior to 11/1/19, that previously displayed on this screen, view the **Health Overview** screen. To learn more, see Health Overview Dashboard or ANYWHERE Health Overview Dashboard.

You can also view your open or pending support tickets in the **Armor Ticketing System (ATS).** To learn more, see Armor Support.

The **Incidents** screen displays security incidents detected by the Armor correlation engine. For each incident, the associated events that caused the detection are also provided.

All security incidents start as a detection, before being escalated by Armor's Security Operations Center (SOC). These escalated incidents are important, and you should take steps immediately to mitigate the threat.

Access the Incidents Screen

1. In the Armor Management Portal (AMP), click **Security**.
2. Click **Incidents**.

The default view is pre-filtered to display incidents only. Click **Filters + Settings** to adjust the view to also display detections.

Column	Description
ID	This is the unique ID of the security incident.
Summary	A brief description of the incident found.
Severity	There are four severity types: • Low • Medium • High • Critical
Tags	Armor will "tag" a detection with **Incident** if it requires security attention, and is a potential threat.
Events	A count of events that triggered a detection or incident in the Armor correlation engine.
Status	The current status of the incident or detection. • If an incident has a corresponding ticket, then the status of the ticket will display. • If a detection does not have a corresponding ticket, then the status will display **Closed.**

3. Expand the row to view the **First** and **Last Event Date.**

4. Click **Filters + Settings** to filter the data that displays in the table.
    a. Filter by **Severity**, **Tags**, or **Status**.
        i. Click **Apply Filters** to save your changes.
    b. In **Table Settings,** you can customize the view of your table.
    c. Click **Save Settings** to save your changes.

View Incident Details

1. In the Armor Management Portal (AMP), click **Security**.
2. Click **Incidents**.
3. Locate and select the incident that you want to view.

Incident Details

Field	Description
Full ID	This is the unique ID of the alert.
First Event Date	The date and time of the first event tracked for this alert.
Last Event Date	The date and time of the last event tracked for this alert.
Status	The status of the detection/incident.
Event Count	The total number of events tracked for this alert.
Categories	The categories used by Armor to group detections, based on the correlation rule(s) that triggered the detection and the associated events.

Event Details

Column	Description
Name	The descriptive name of the event.
Source IP	The source network address associated with the event.
Dest. IP	The destination network address associated with the event.
Timestamp	The date and time that the event occurred.
Log Source	The data source of the event log.
Category	The category assigned based on the correlation rule(s) that triggered the detection and the associated event.

4. Click **Filters + Settings** to filter the data that displays in the table.
    a. Click **Apply Filters** to save your changes.
5. In **Table Settings,** you can customize the view of your table.
    a. Click **Save Settings** to save your changes.

View Support Ticket Details

⚠ In order to view a ticket, you must be a member of the organization that the ticket was created in.

1. In the Armor Management Portal (AMP), click **Security**.
2. Click **Incidents**.
3. Locate and select the incident that you want to view.
4. Click **View Ticket**.
    a. The ticket details from the Armor Ticketing System (ATS) will open in a new window.

Close A Security Incident

Only Armor Support can close a security incident. However, after you have performed the troubleshooting tips suggested by Armor Support, simply enter a comment expressing your desire to close the ticket. Armor Support will verify and confirm that the security incident has been properly addressed, and then they will close the ticket.

Troubleshooting

If you do not see any data in the **Incidents** screen, consider that:

- Your account does not have any security incidents to display.
  - Armor is responsible for adding security-related incidents to this screen.
- You do not have permissions to view security incidents.
  - You must have the Read Security Alerts and Read Security Offenses permissions enabled to view security incidents in this screen. Contact your account administrator to enable this permission. To learn how to update you permissions, see Roles and Permissions.

Related Documentation

- ANYWHERE Detection Dashboard
- ANYWHERE Health Overview Dashboard
- ANYWHERE Protection Dashboard
- ANYWHERE Response Dashboard
- Armor Support
- Detection Dashboard
- Health Overview Dashboard
- Incidents
- Protection Dashboard
- Response Dashboard

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★½ 13 rates