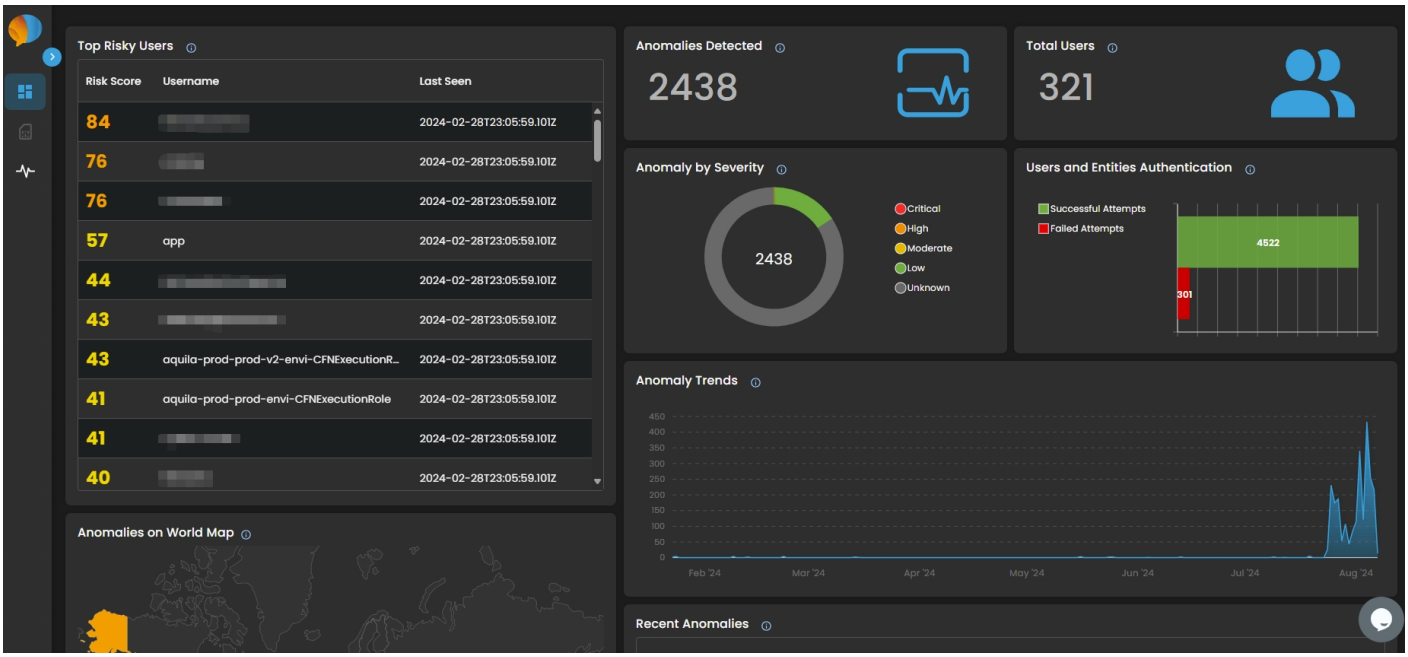
New Module (August 30): User and Entity Behavior Analysis

◫ New Module Release

We’ve just dropped a new module: **User and Entity Behavior Analysis**

◫ New Features:

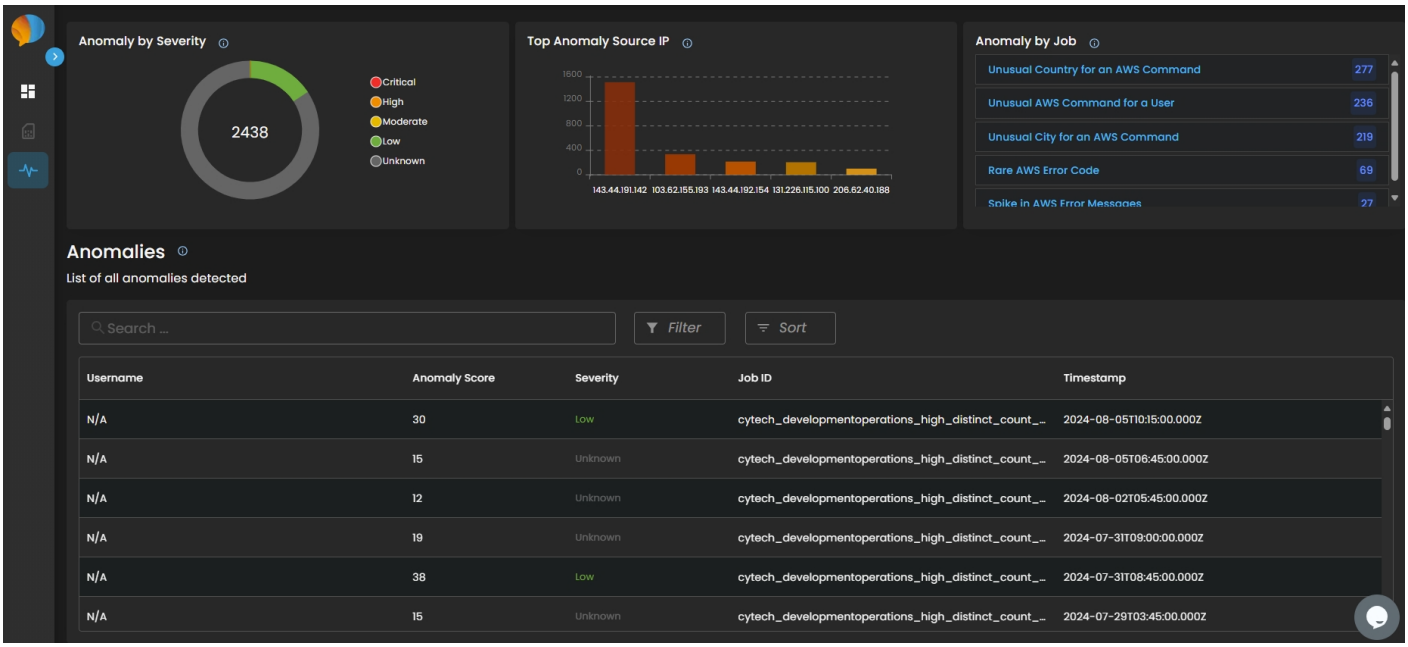
1) Dashboard



- Top Risky Users
  - Users can now see risky users in descending order
  - Risk score are colored according to their severity
- Anomalies on World Map
  - Users can now see the countries where anomalies originated from

- Anomalies Detected
    - Users can view the total number of anomalies detected
- Total Users
    - Users can view the total number of users detected
    - Limitation: the data presented is not yet filtered by space or client.
- Anomaly by Severity
    - Users can view the total number of anomalies per severity
    - The data will be presented as donut chart where it will show the breakdown of anomalies per severity
- Users and Entities Authentication
    - Users can view the total number of failed and successful attempts in authentications for the whole organization
- Anomaly Trends
    - Users can now view the total number of anomalies per day.
    - The data will be presented as line chart where it will show the timeline and fluctuations of data throughout the time range.
- Recent Anomalies
    - Users can now view the recent anomalies detected by the module.

2) Anomalies Page



- Anomaly by Severity
  - Users can now see the countries where anomalies originated from (same from the dashboard)
- Top Anomaly Source IP
  - Users can now see which IP have the most anomalies
- Anomaly by Job
  - Users can now see which job had the most anomalies detected
- Anomalies
  - Users can view the list of all anomalies detected so far

◫ Known Issue:

- Anomaly by Job
  - There is a count discrepancy when comparing the total between Anomaly by Job vs Anomalies Detected or Anomaly by Severity.
  - This is because of the different query used retrieving the data. The Anomaly by Job used filter where it only gets documents with anomaly_score greater than 0. The other components did not have this one yet.

◫ To be supported:

- Users and Entities Page
- Dashboard "Rabbit Hole" Support

◫ Limitations

- Total Users
  - The data presented is not yet filtered by space or client

- Anomaly Trends

    - Remarks: The reason why the data only starts with August 2024 is we deactivated the Jobs that were active since the start of the year because they collected anomalies and put them in a single index regardless of the space or client the anomaly originated from. This caused challenges in retrieving filtered data and we have to create separate jobs for each client to combat this issue.
- Recent Anomalies
    - Sometimes the field/data expected by backend and frontend from elastic is not provided (e.g., username). This was handled by the backend to display “N/A” instead. Investigation is yet to start for this one.

Revision #3
Created 30 August 2024 02:47:29 by Aldion Pueblos
Updated 30 August 2024 03:26:32 by Aldion Pueblos