

New Module (July 19): SOAR

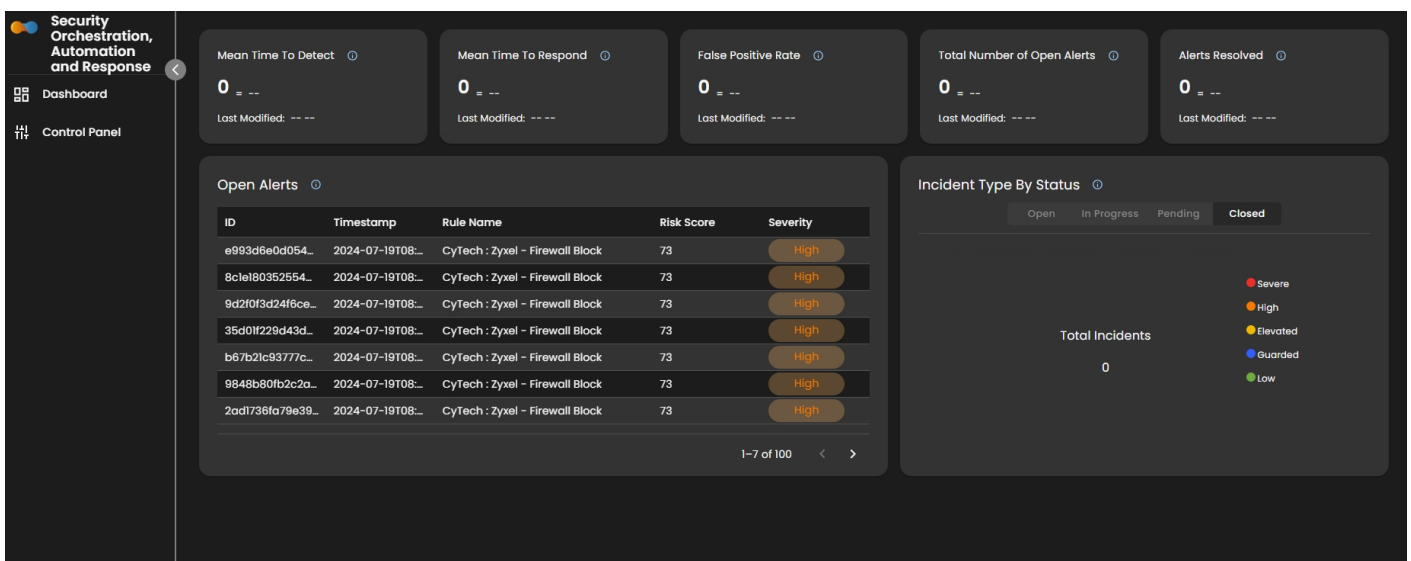
☐ New Module Release

We've just dropped a new module: **SOAR (Security Orchestration, Automation and Response)**

☐ New Features:

Dashboard

- **Dashboard supports the following:**
 - Mean time to respond with history comparison
 - User can now see their respond time data
 - User can also see the comparison from yesterday
 - False positive rate with history comparison
 - User can now see their false positive time data
 - User can also see the comparison from yesterday
 - Total open alerts
 - User can now see their total open alerts
 - Total resolved alerts
 - User can now see their total resolved alerts
 - Open Alerts
 - Case Resolution Time Analysis:
 - Partially Supported



- **Dashboard Limitations:**
 - Mean time to respond with history comparison

- User can only see the comparison from yesterday
- Total open alerts
 - Query limited to only 100, proper implementation to support large sets of alerts is not yet complete
- Total resolved alerts
 - Query is limited to only 100, proper implementation to support large sets of alerts is not yet completed.
- Open Alerts
 - Query limited to 100
- Incident Type By Status
 - Not Yet Supported
- False positive rate with history comparison
 - User can only see the comparison from yesterday

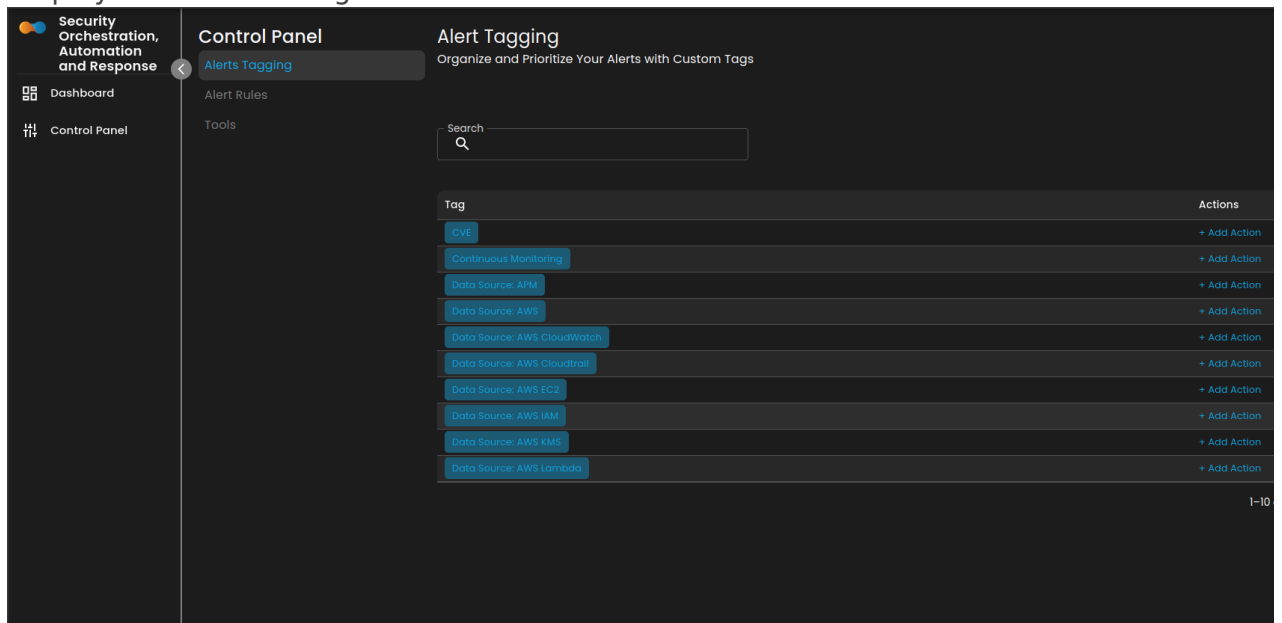
- **Dashboard Known Issues:**

- For features with history comparison, it needs at least 2 historical data in order to be able to perform a comparison.

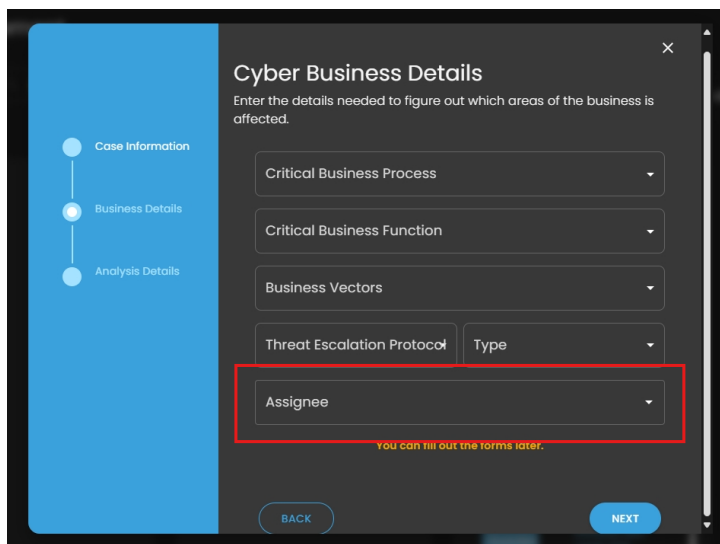
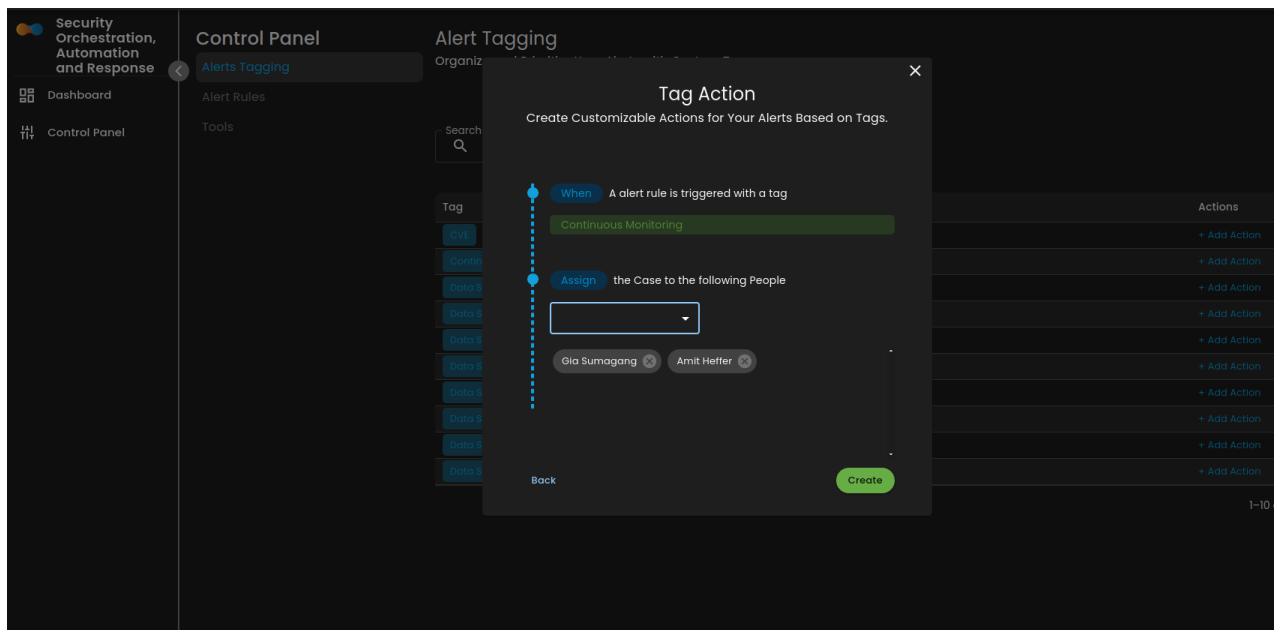
SOAR Configuration

- **SOAR configuration currently supports:**

- Alert Tagging
 - Display a list of alert tags

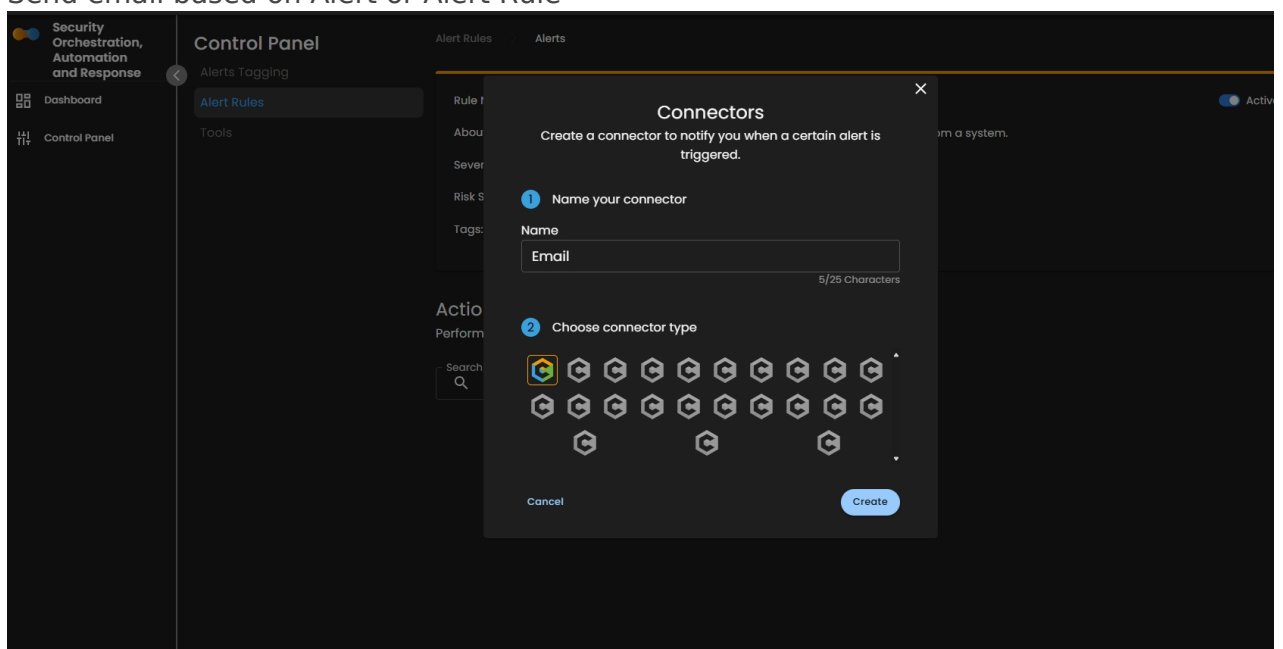


- Automatic assignee of a case based on the alert tags



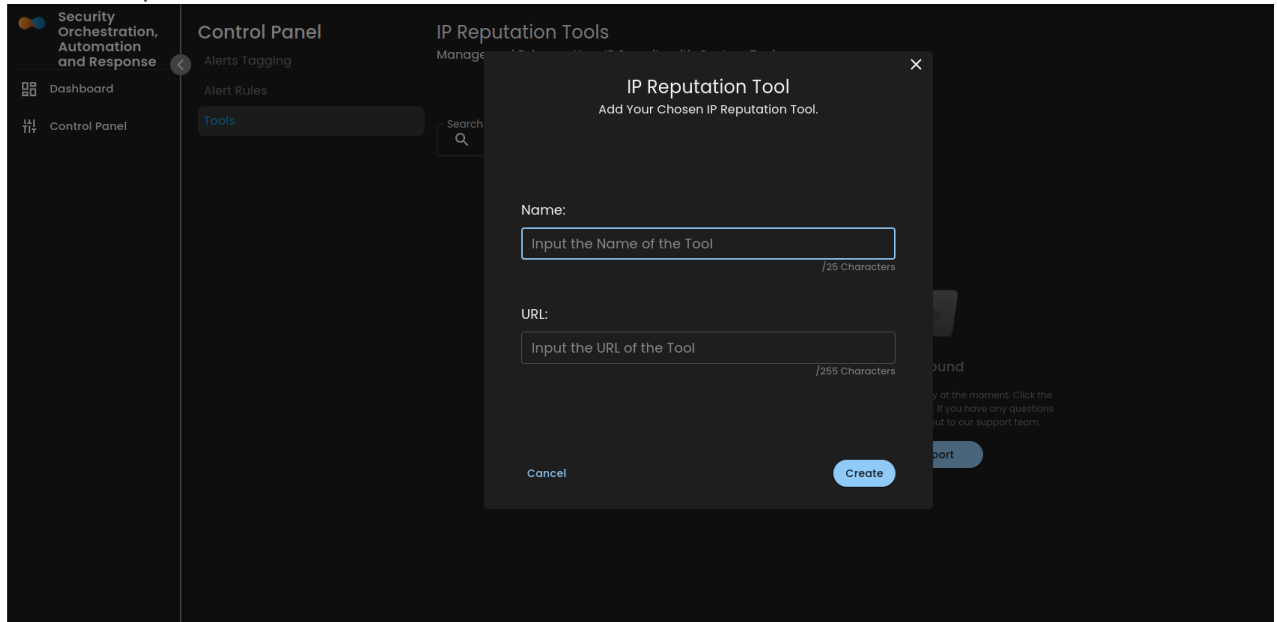
○ Connectors

○ Send email based on Alert or Alert Rule



○ Tools

- Add IP Reputation Tools



- **SOAR configuration Limitations:**

- Alert Tagging
 - Rule name characters length issue, characters must not be more than 25 characters
 - User can't modify or change alert tagging configuration
- Connector
 - User can't see the list of actions/connectors that has attached on a rule
 - Only Email Connector is currently supported. Other connectors such as Teams and etc.
- Tools
 - User can't edit IP Reputation tool
 - User can't delete IP Reputation tool added.
 - User can't view the list of IP Reputation tools

- **SOAR configuration Known Issues:**

- Alert Tagging
 - Assignee duplication issue when selecting multiple alerts to attach on a case in CIMS
- Connector
 - User can't create email connector with "for each alert and per rule" configuration

Revision #1

Created 12 July 2024 14:21:48 by Aldion Pueblos

Updated 19 July 2024 10:12:30 by Aldion Pueblos