CyTech AQUILA - Cyber Incident Management (CIM): Dashboard

Overview:

Cyber Incident Management (CIM) is the **end-to-end process of preparing for, detecting, analyzing, responding to, and recovering from cybersecurity incidents** (such as malware infections, data breaches, insider threats, or DDoS attacks).

The goal is to **minimize damage, reduce recovery time, and prevent future incidents**.

Key Features:

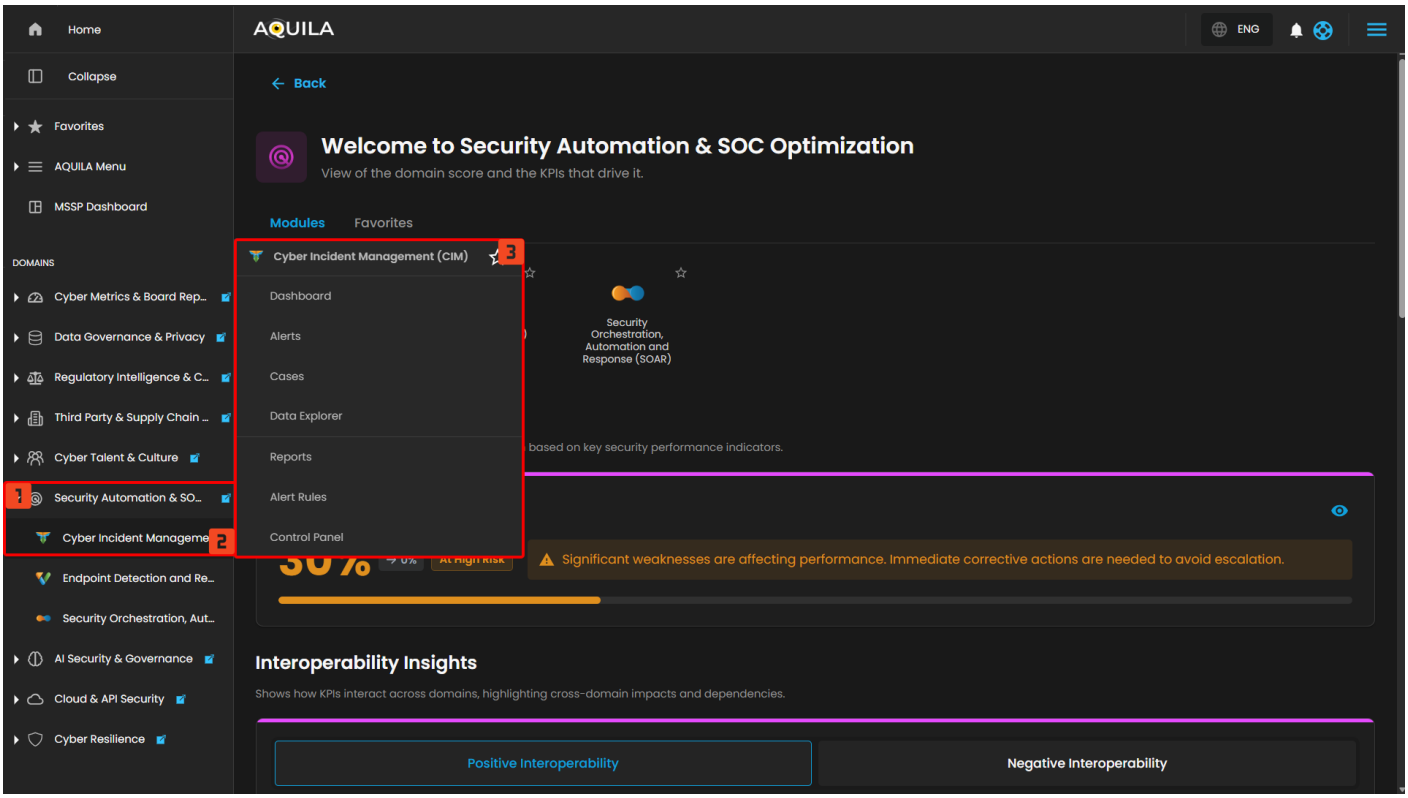
- **Dashboard** - Real-time view of alerts, cases, and overall security status.
- **Alerts** - Notifications when suspicious activity is detected.
- **Cases** - Track and manage incidents from start to finish.
- **Data Explorer** - Investigate logs and find root causes.
- **Reports** - Summaries for management, compliance, and lessons learned.
- **Alert Rules** - Define what should trigger an alert (custom detection logic).
- **Settings** - Configure integrations, access, and workflows.

Pre-requisites:

1. **Access to CyTech - AQUILA**
   - Only users assigned the **"Owner"** or **"Admin"** role can access the Log Collector installation resources within the platform.

> **To navigate to CIM Module please follow the instructions below:**

Step 1: Log in to CyTech - AQUILA. *click here* --> usdc.cytechint.io
Step 2: In the left column click Security Automation & SOC Optimization -> Cyber Incident Management (CIM) -> Dashboard



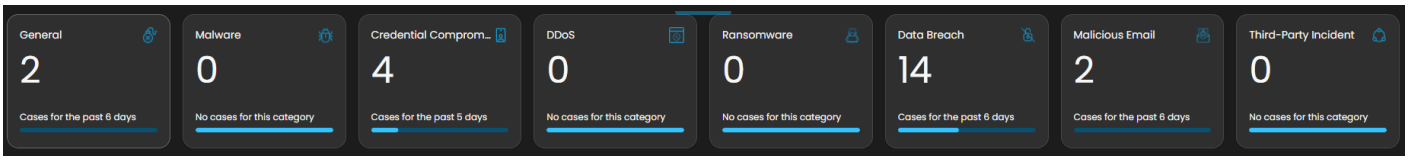
Cyber Incident Management (CIM): Dashboard

The **Main Dashboard** serves as the central hub for viewing all critical and relevant data associated with this module. It provides a consolidated interface where key **metrics**, **updates**, and **operational insights** are displayed for quick reference and effective monitoring.

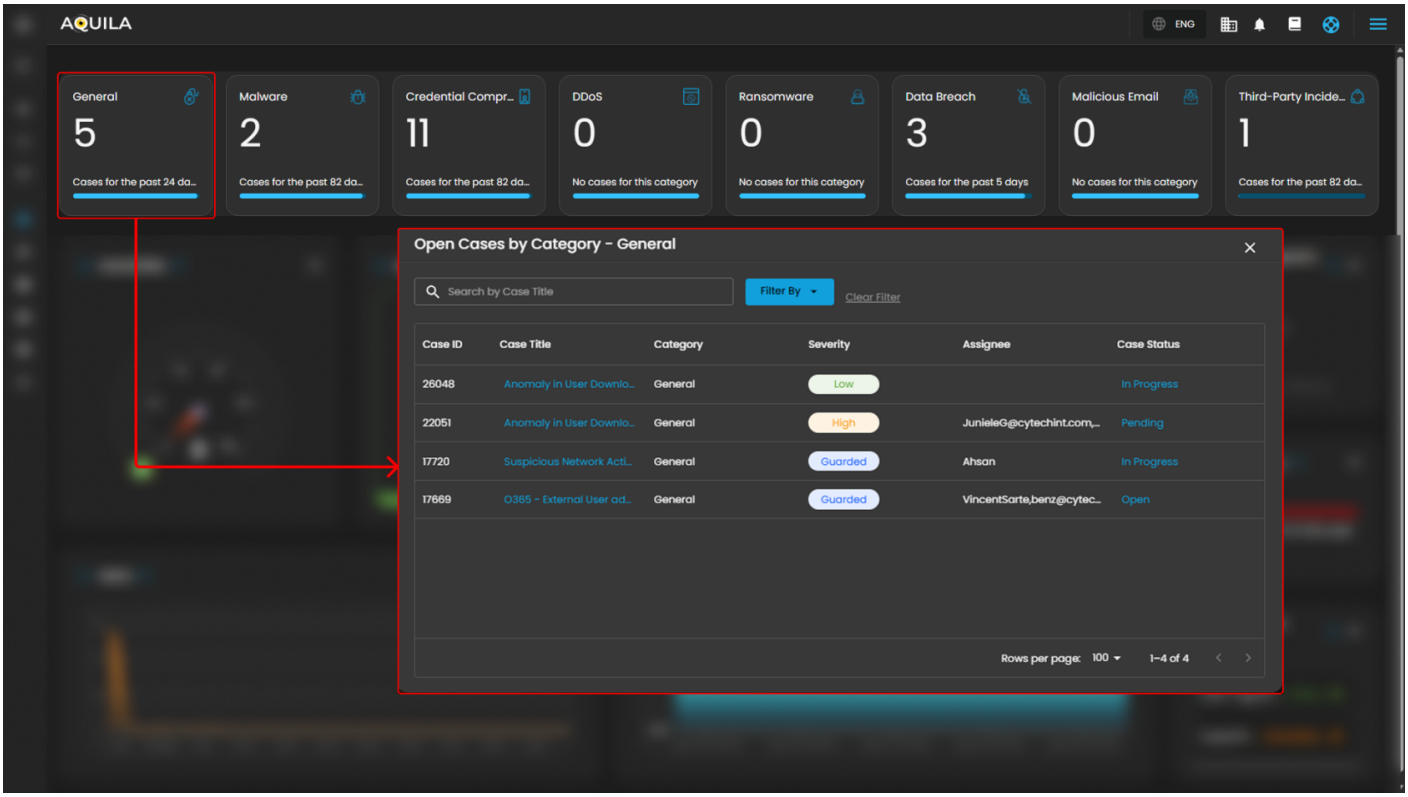


Case Categories

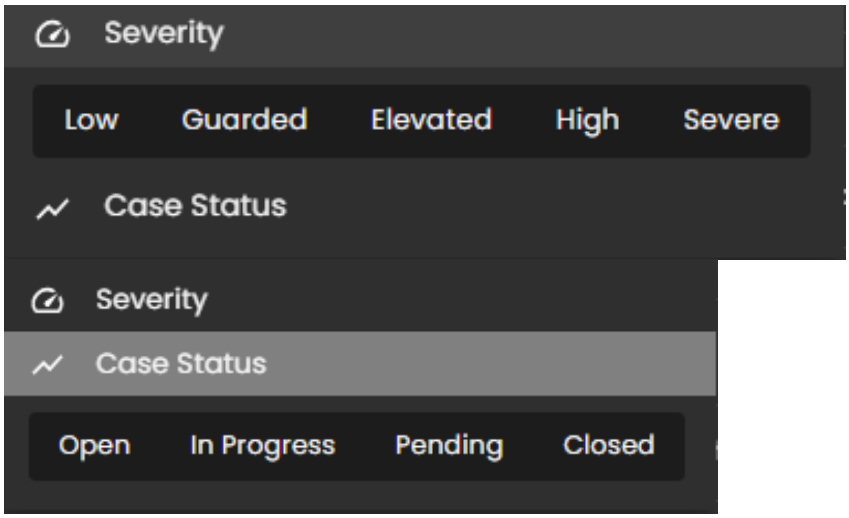
This panel displays and categorizes all cases within your environment that are currently open or in progress. It presents a structured view based on case categories, offering a clear summary of ongoing activity. This allows for efficient tracking, prioritization, and management of active investigations.



Upon selecting a category, a new window will automatically open, displaying all cases associated with the selected category.



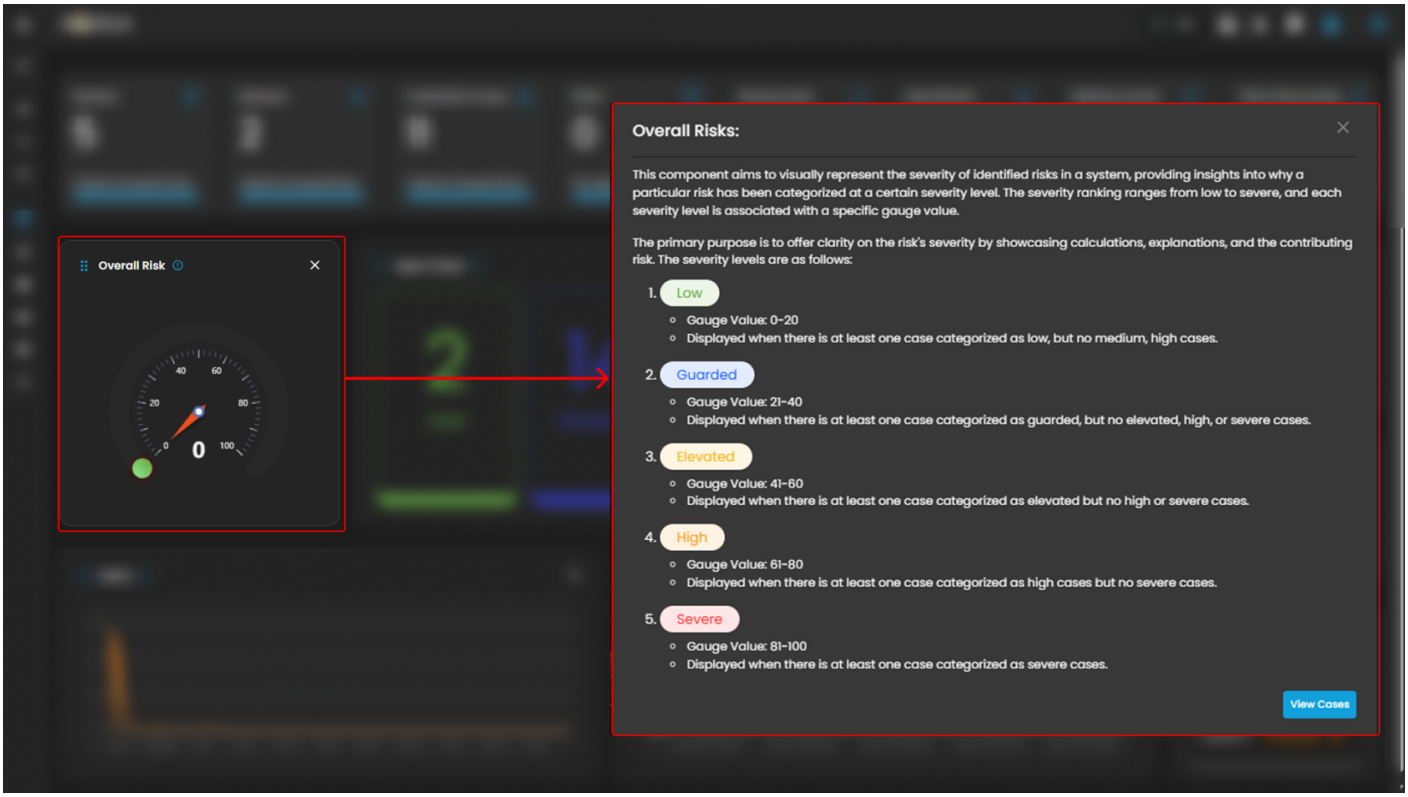
1. **Search Bar:** The search bar enables users to locate a specific case by entering the exact case title. Simply type the desired title into the search field to quickly retrieve relevant results.
2. **Filter By & Clear Filter:** This feature enables users to refine the list of cases by applying filters based on Severity and Case Status. Use the Filter By option to display only the cases that match specific criteria. To remove all applied filters and return to the full list of cases, use the Clear Filter option.



3. **Case Details:** To access the investigation section of a case, double-click on the case entry. This action will automatically redirect you to the detailed investigation interface for further analysis and review.

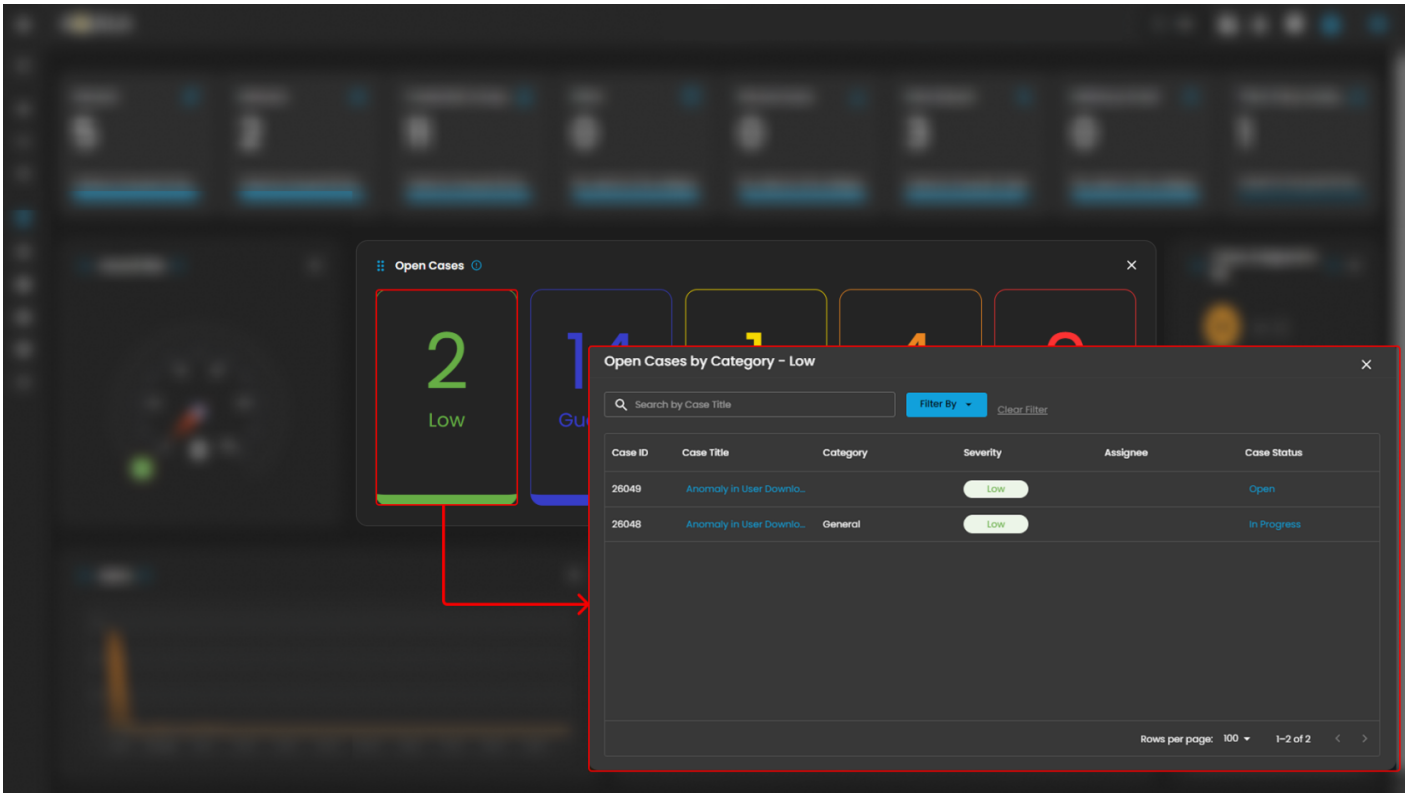
Overall Risk

Displays system risk severity levels on a scale from **Low** to **Severe** (**0 - 100**), explaining the rationale behind risk classifications and showing the highest severity level present in the system. Clicking on the gauge allows you to view more details about.



Open Cases

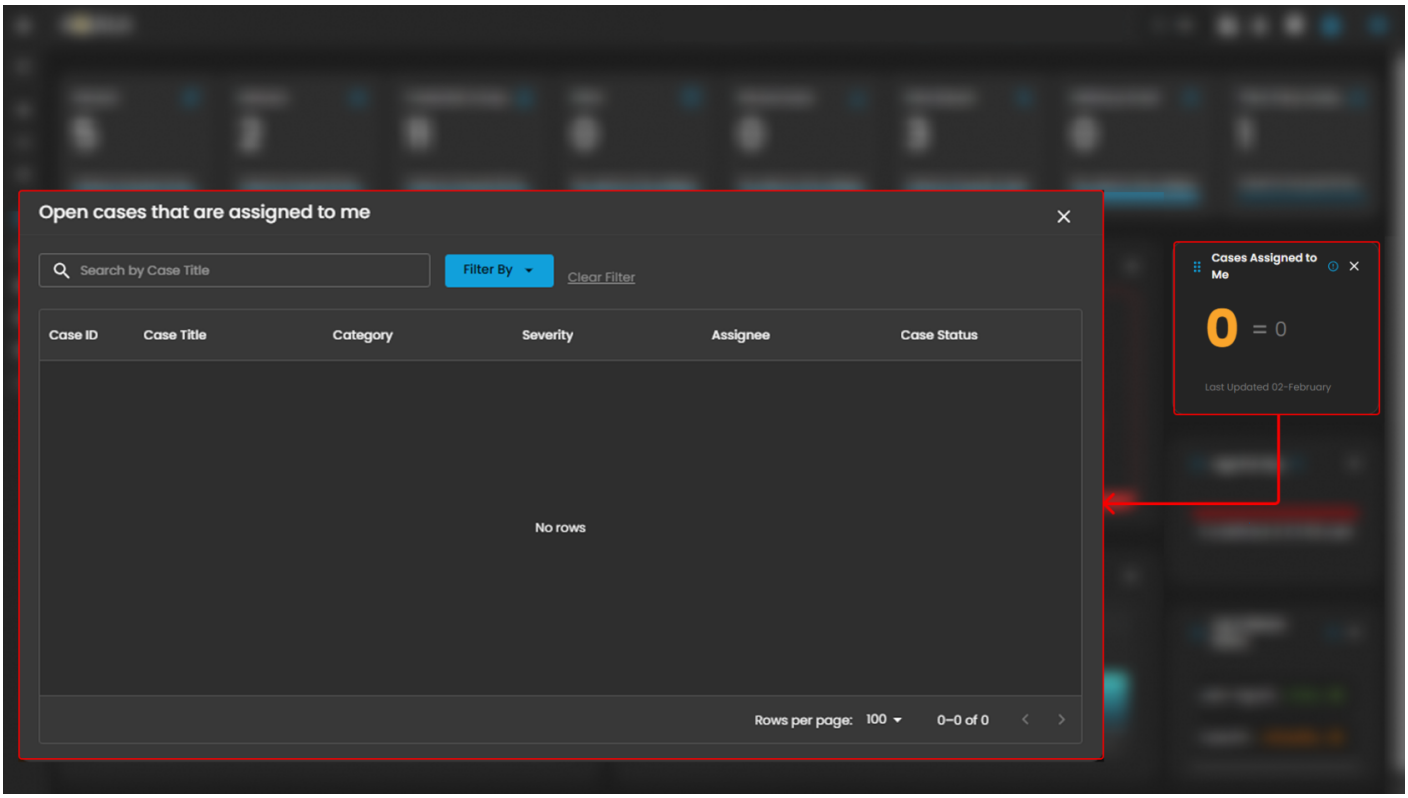
Displays the total number of open cyber incident cases, categorized by severity, that are currently being investigated.



When you click on a category, you will see all the cases that fall under that severity level. For example, as shown in the image above, selecting the “**Guarded Severity**” category will display all cases labeled as guarded severity.

Cases Assigned to Me

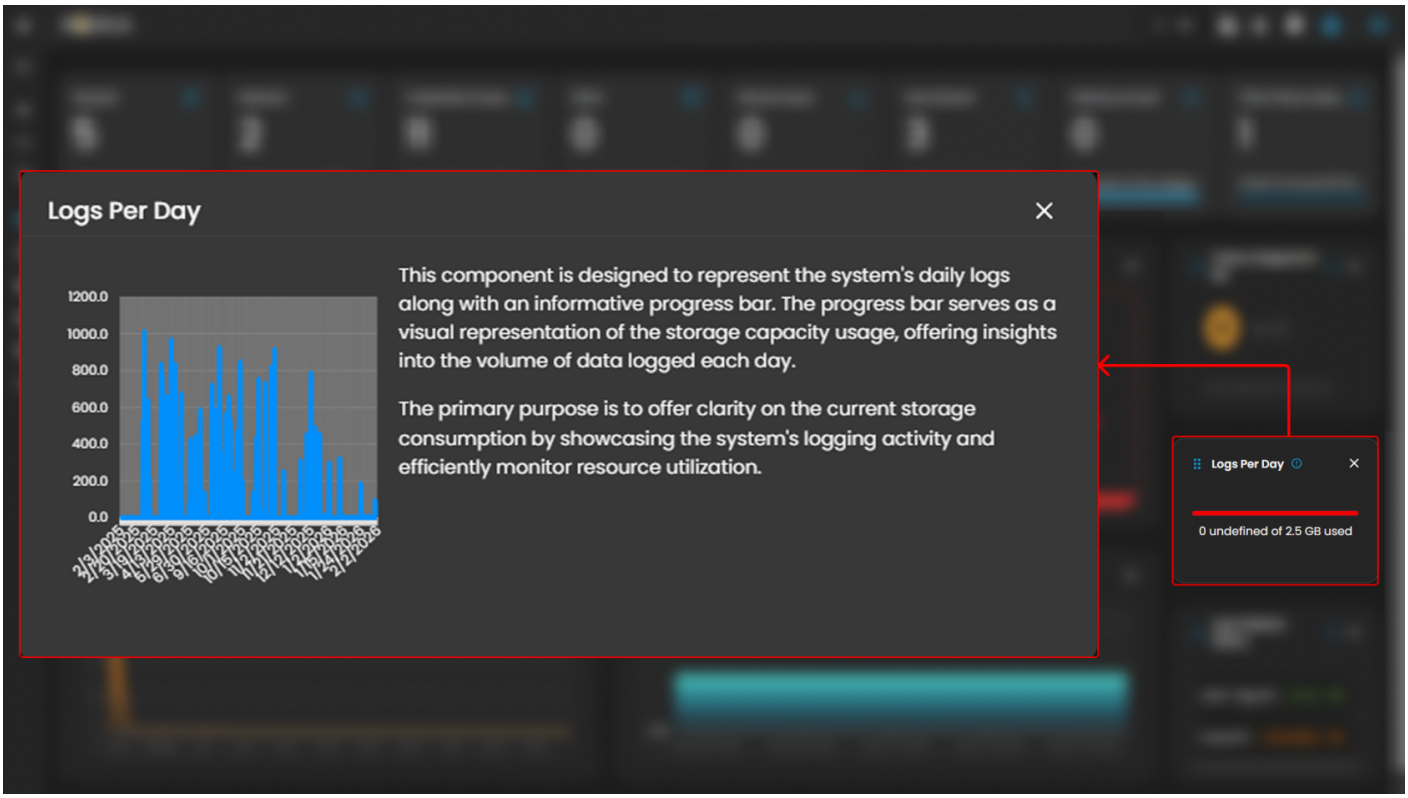
Shows the number of cyber incident cases specifically assigned to you for investigation and resolution. Clicking on it will open up a small window that will show all the cases assigned under you.



Logs Per Day

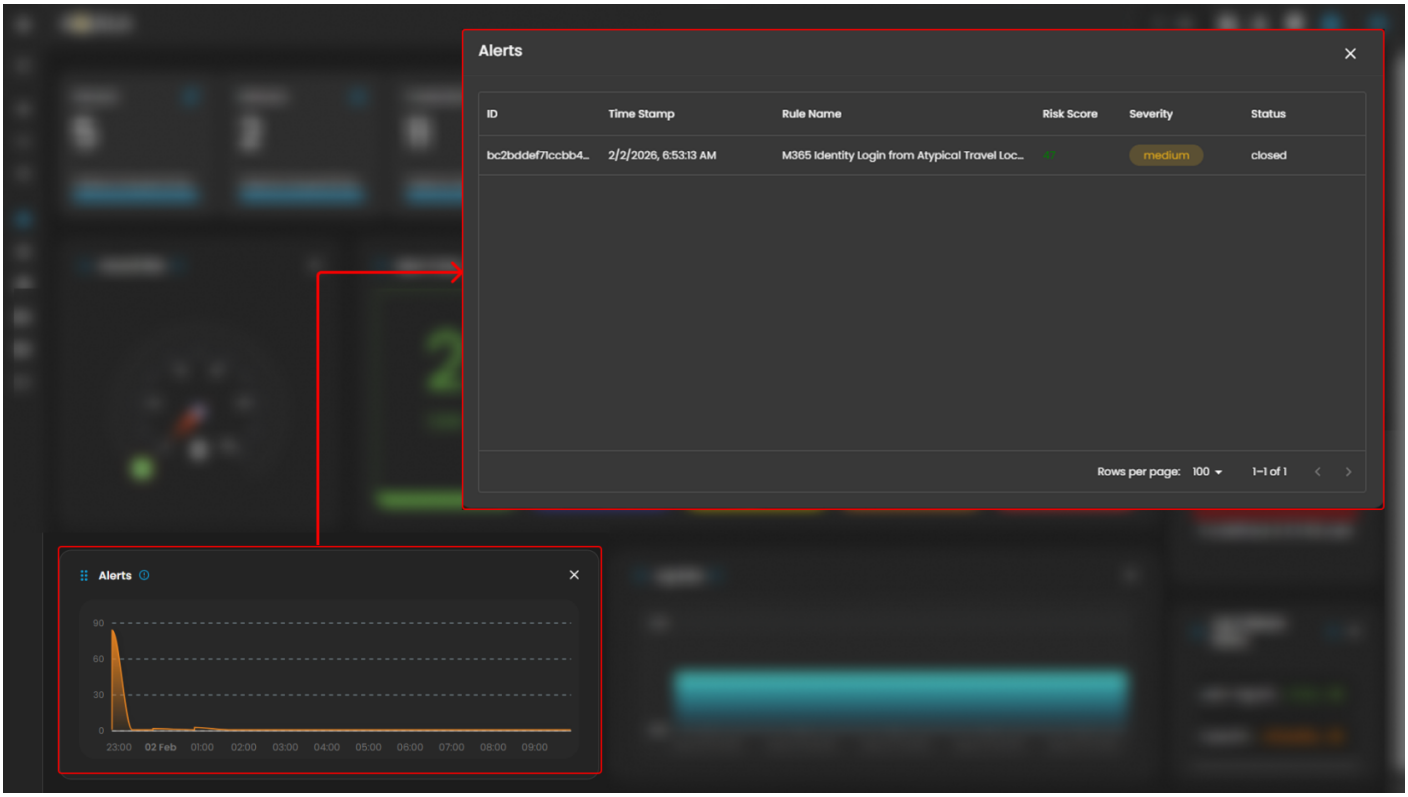
Displays daily system logs with a progress bar that tracks storage capacity usage, providing clear insights into daily logging volume and resource consumption.

When you click on it, a small window will appear displaying a graph.



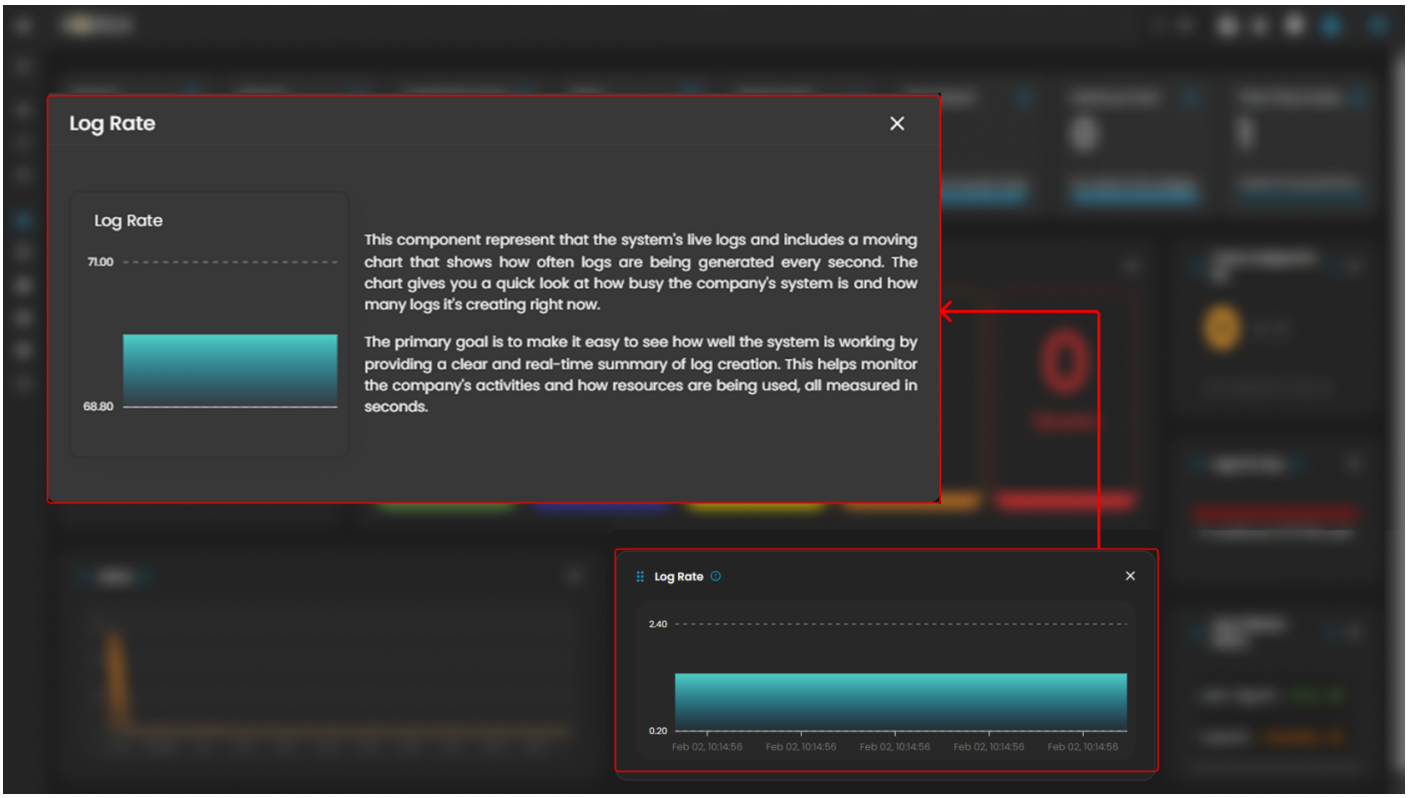
Alerts

Display the trends of the detections generated by the system, highlighting potential security incidents that require immediate attention. Clicking on a timeline will open up a small window that will show all the alerts that was recently triggered.



Log Rate

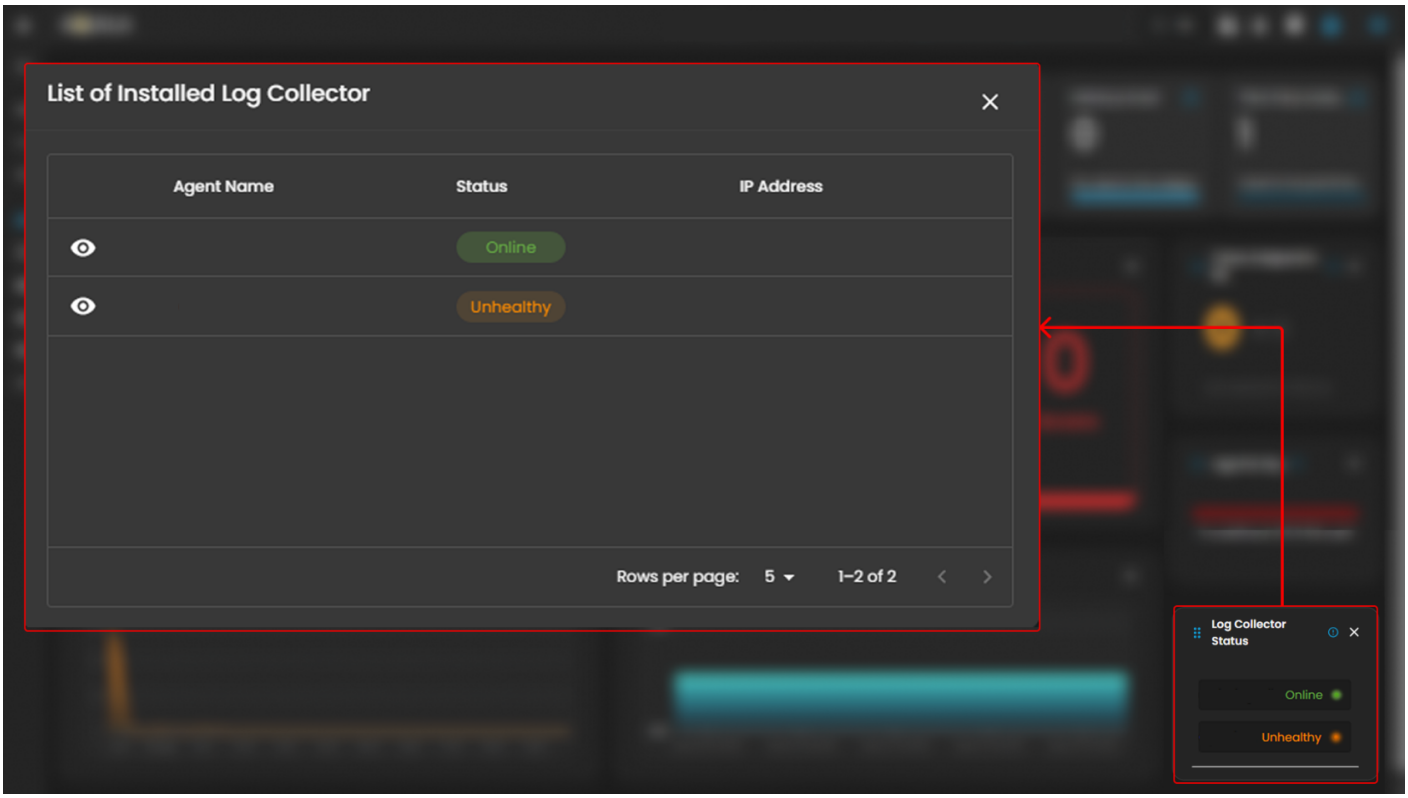
A real-time visualization to display system log generation frequency per second through a dynamic chart, enabling instant monitoring of system activity and resource utilization. Clicking on it will open up a small window that will show the detailed explanation.



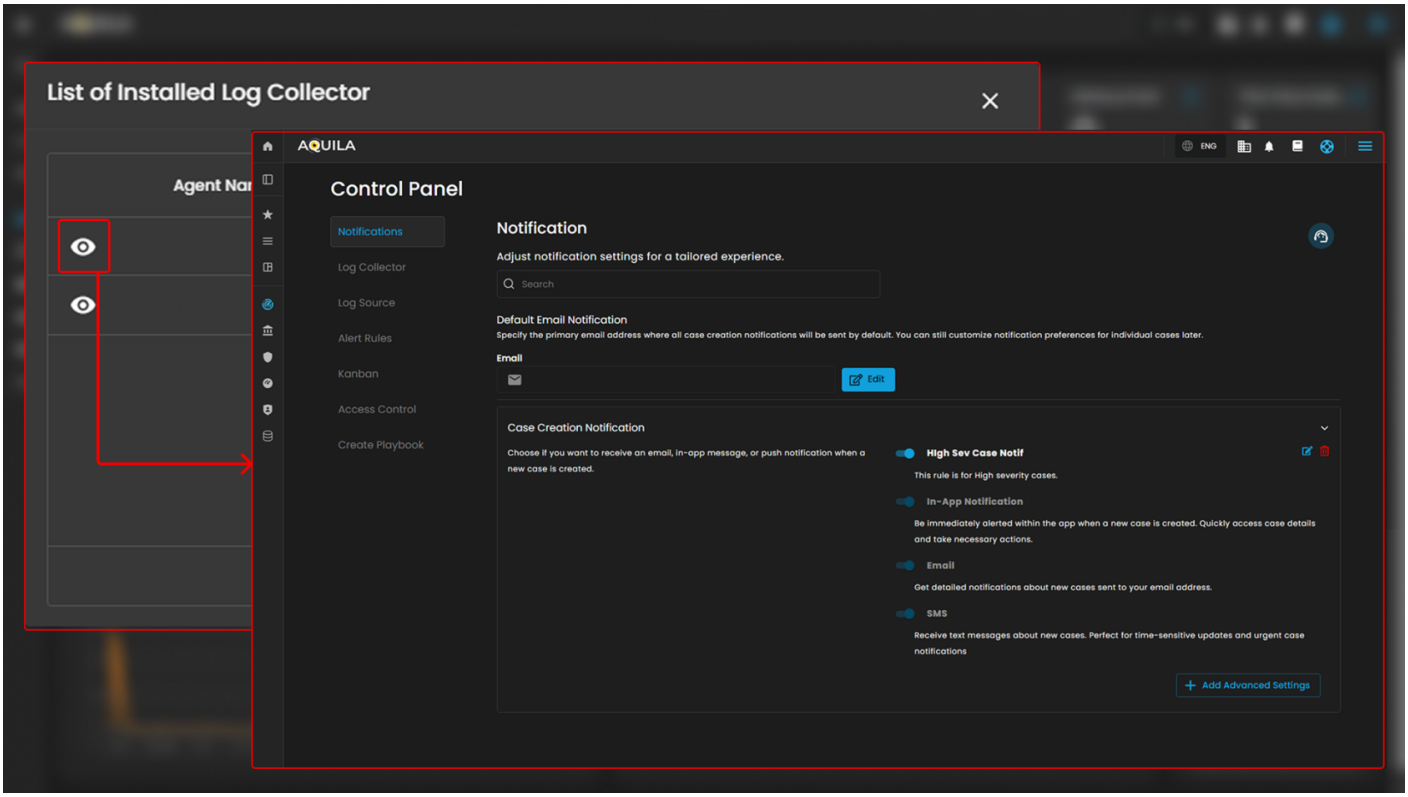
Log Collector Status

Indicates the current status of the log collector, ensuring that logs are being collected and monitored for any suspicious activity.

When you click on it, a small window will appear showing all installed **log collectors** along with their current **status**.



Click the **eye icon** next to the log collector name to go to the **Log Collector List** page.



In conclusion, this dashboard serves as a centralized operational interface that enhances cybersecurity case management by providing real-time visibility into alerts, active investigations, and unresolved cases. It enables security teams to systematically monitor alert statuses, track ongoing investigations, and identify open cases that have not yet been addressed. Through structured data visualization and status tracking, the dashboard improves workflow prioritization,

reduces response time, and ensures that no critical alerts are overlooked. Overall, it strengthens operational oversight, accountability, and incident response efficiency within the security environment.

> Please refer to the document for the next sub-module: **CyTech AQUILA - Cyber Incident Management (CIM): Alerts**

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #4
Created 13 February 2026 03:03:03
Updated 17 April 2026 03:30:24