

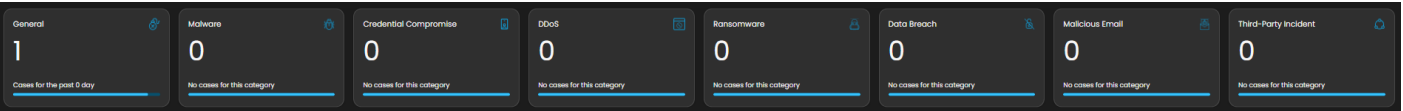
Cyber Incident Management (SIEM and XDR)

Welcome to the **Cyber Incident Management** module.

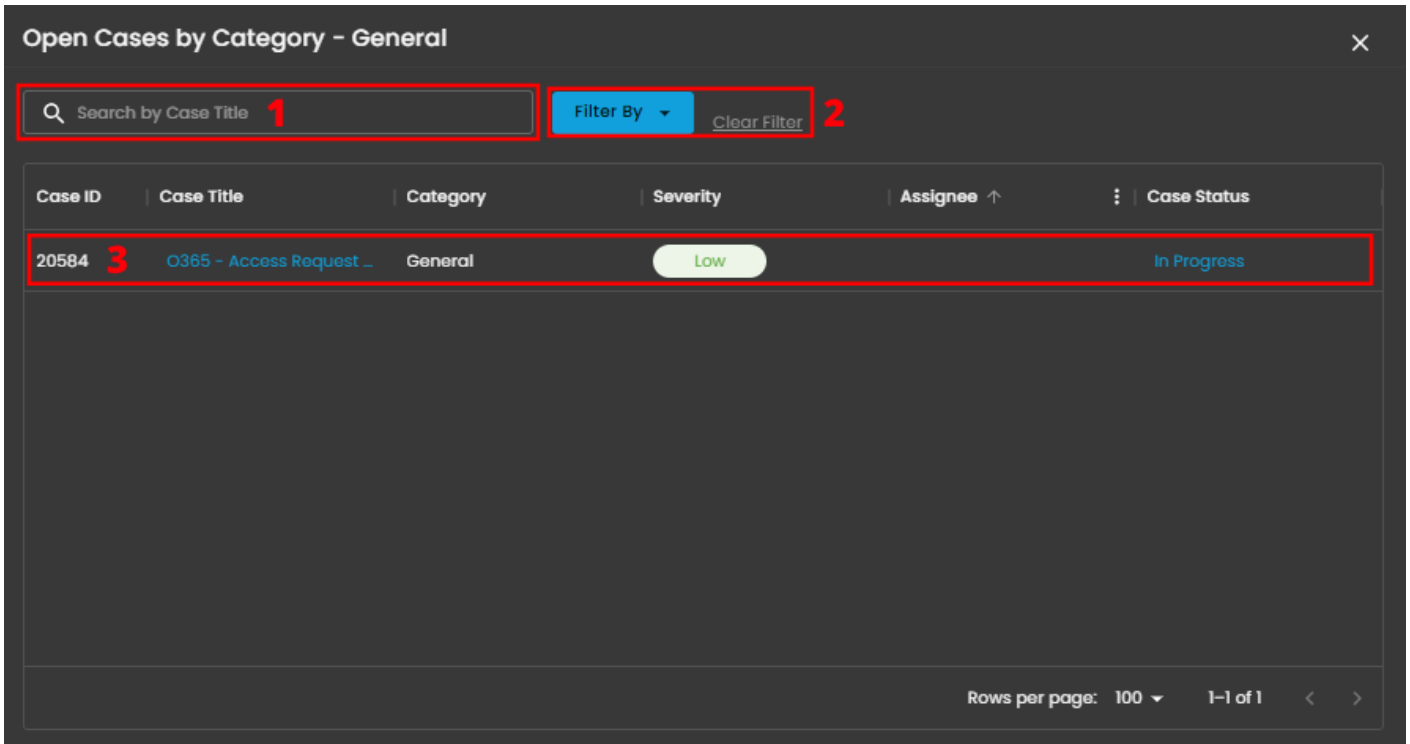
The Main Dashboard serves as the central hub for viewing all critical and relevant data associated with this module. It provides a consolidated interface where key metrics, updates, and operational insights are displayed for quick reference and effective monitoring.



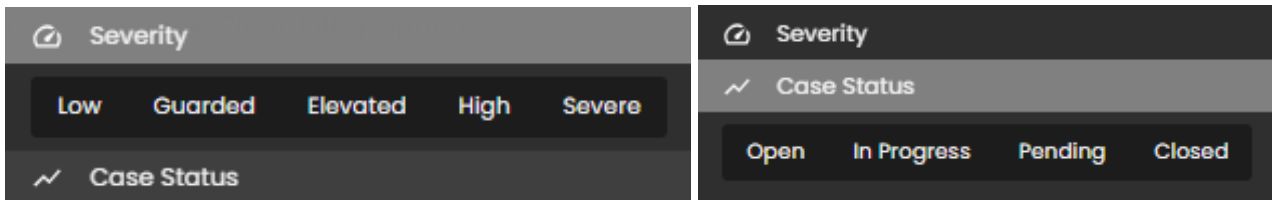
This panel displays and categorizes all cases within your environment that are currently open or in progress. It presents a structured view based on case categories, offering a clear summary of ongoing activity. This allows for efficient tracking, prioritization, and management of active investigations



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



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.

Revision #2

Created 27 May 2025 18:39:49 by Darryl Espancho

Updated 27 May 2025 23:25:05 by Darryl Espancho