Cyber Incident Management Module

Overview:

Cyber Incident Management with Extended Detection and Response (XDR) and Managed Detection and Response (MDR) provides comprehensive protection against cyber threats by continuously monitoring and analyzing an organization’s digital environment. XDR integrates data from various security sources, such as endpoints, networks, and cloud environments, to detect and correlate threats more effectively. MDR offers 24/7 monitoring, management, and incident response. Together, these tools enable rapid identification and mitigation of potential threats, helping to reduce the impact of cyber incidents and ensure the security of organizational assets.

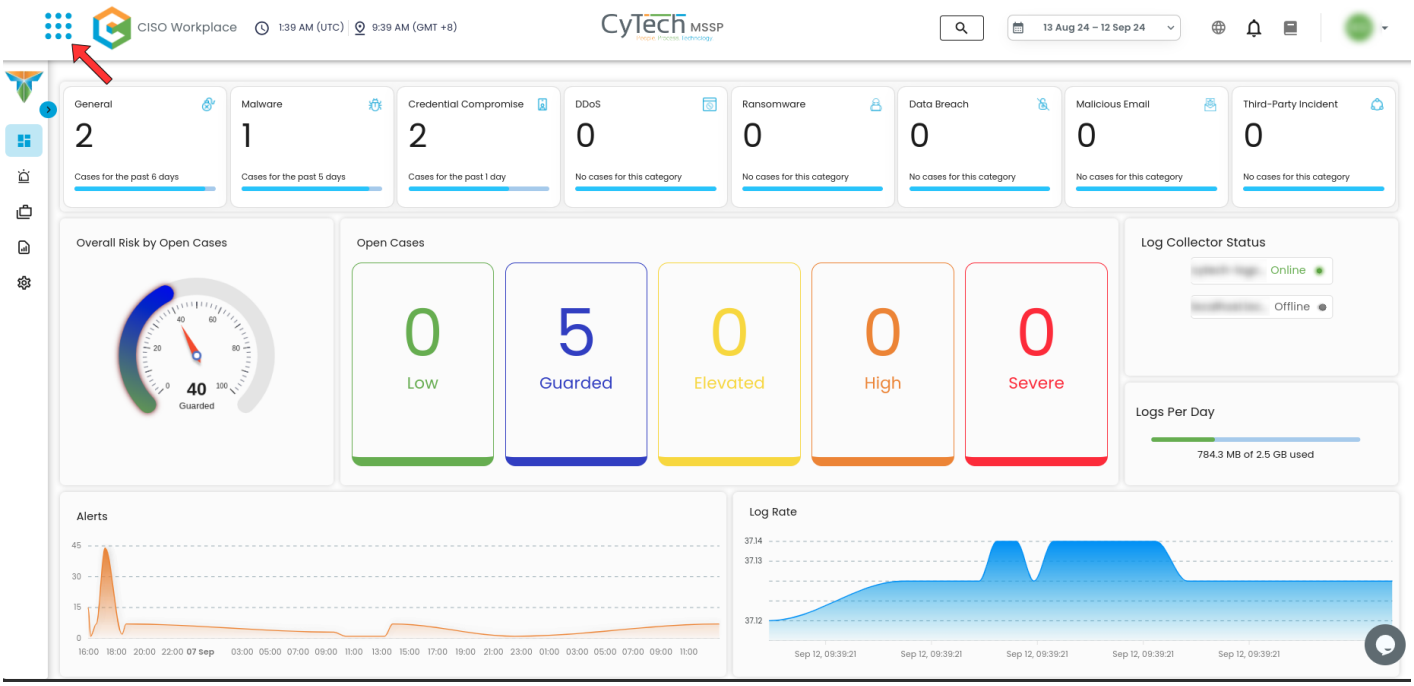
Pre-Installation Steps:

To ensure a smooth start, please complete the following steps:

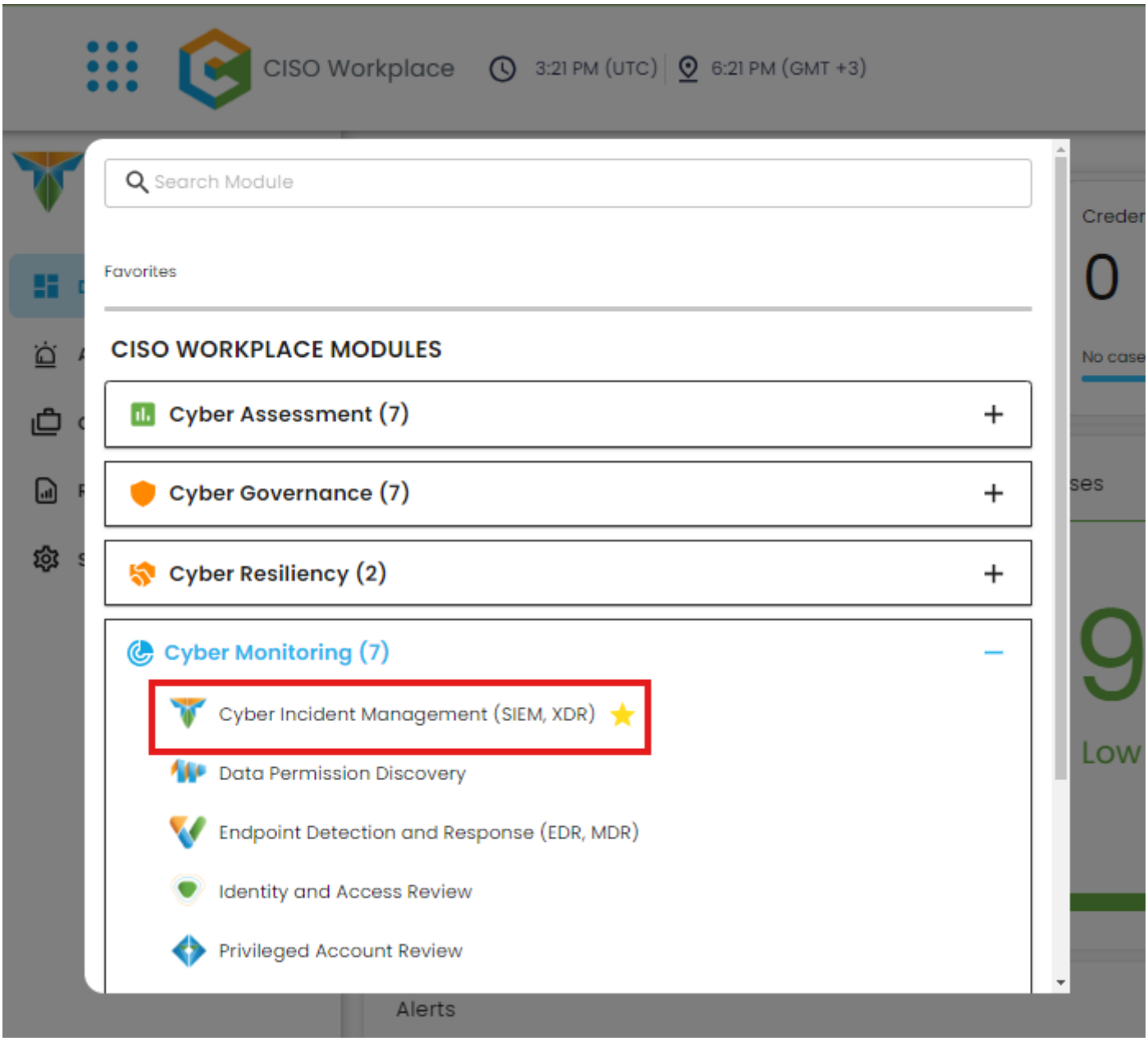
1. Pre-Installation Questionnaire: Kindly fill out the questionnaire https://forms.office.com/r/MNvfCj3q8E, which will help us customize the platform to your specific requirements.
2. The CISO Workplace Log Collector shall be installed as a VM (Virtual Machine).
   The host for this VM can be a Windows or Linux Machine.
   For the case of Syslogs, other machines (hosts) in your network will need to forward the logs to this Log Collector.
   A virtualizer will be necessary to be installed on the host machine.
   For Windows -- Virtualbox can be used.
   For Linux -- kvm can be used.

Navigate to Dashboard:

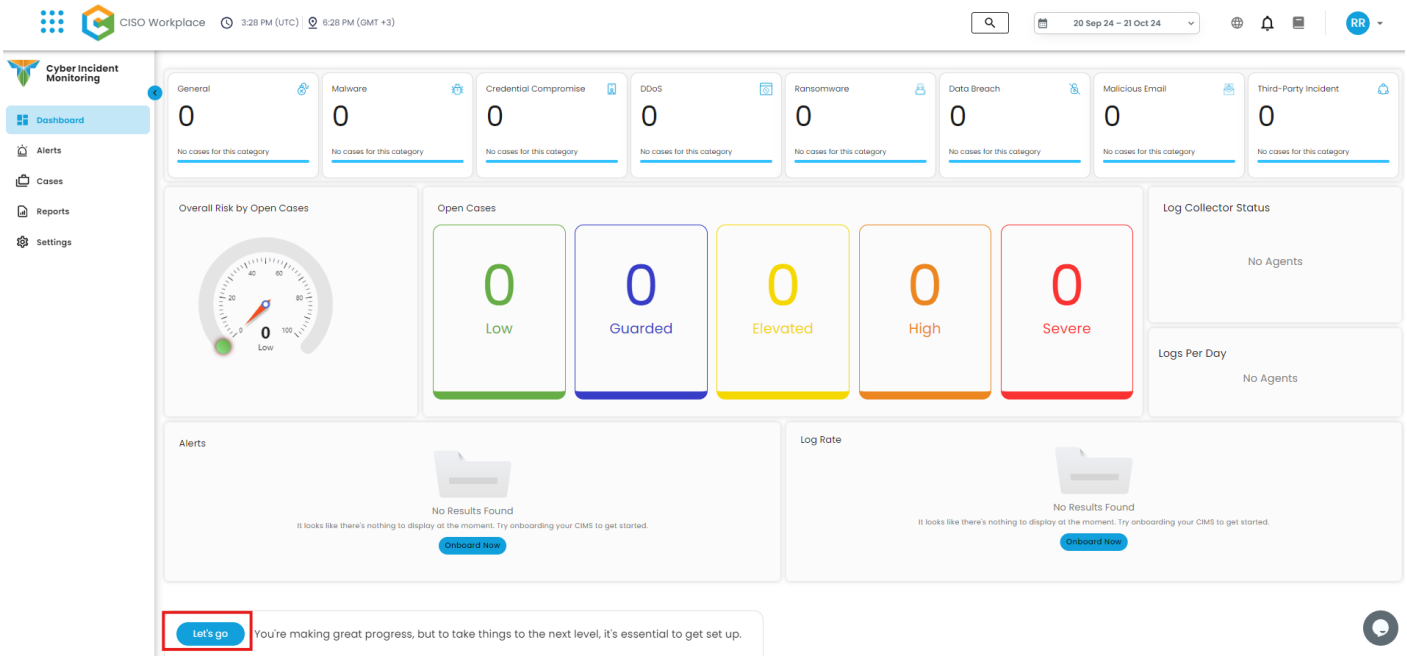
- To show all the different modules, click on the menu icon .



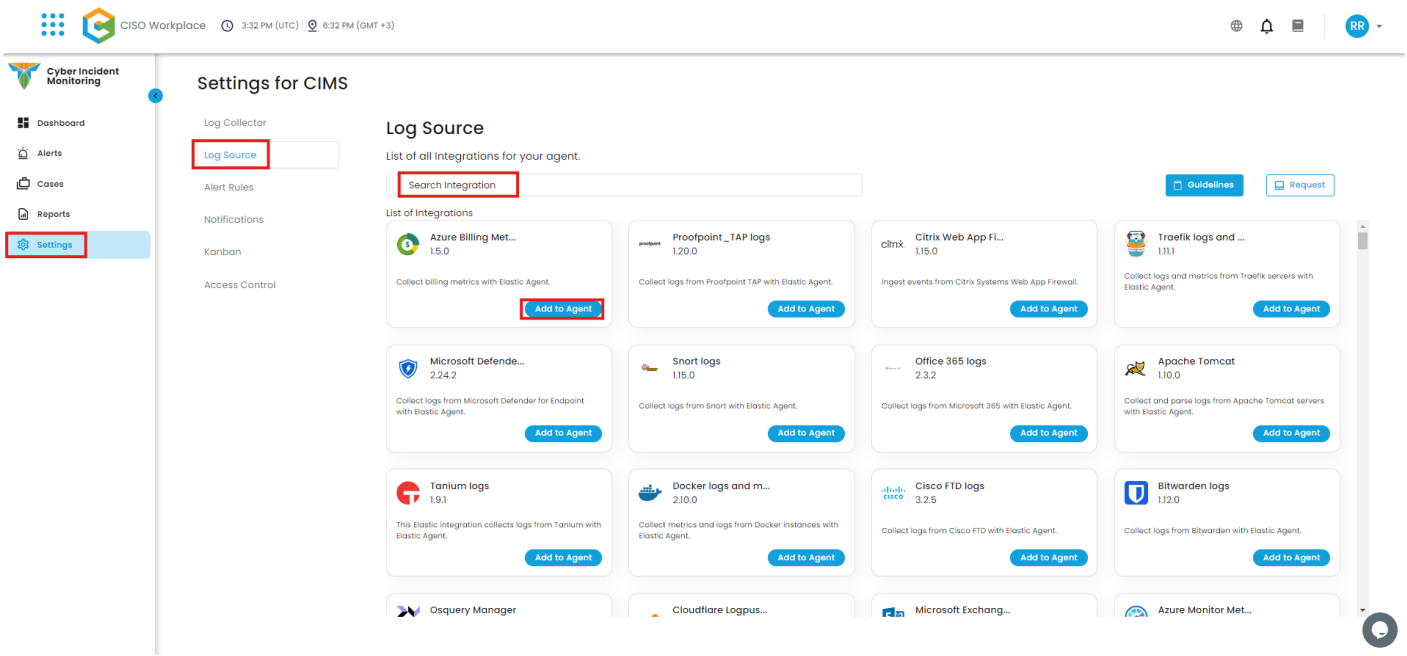
- Under Cyber Monitoring, click on Cyber Incident Management (SIEM, XDR)



- Click on **Let's go** to start the Log Collector installation and follow the instructions:



- **Install Log Source:**
  Go to settings > Log Source> Choose your desired source and follow the instructions.



Please notify us once you have completed these steps and we will start monitoring your environment.

If you have any questions, feel free to contact our support team at **support@cytechint.com**.

We're thrilled to work with you!

Revision #2
Created 21 October 2024 15:17:00 by Reut Rubinstein
Updated 21 October 2024 15:36:53 by Reut Rubinstein