

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.

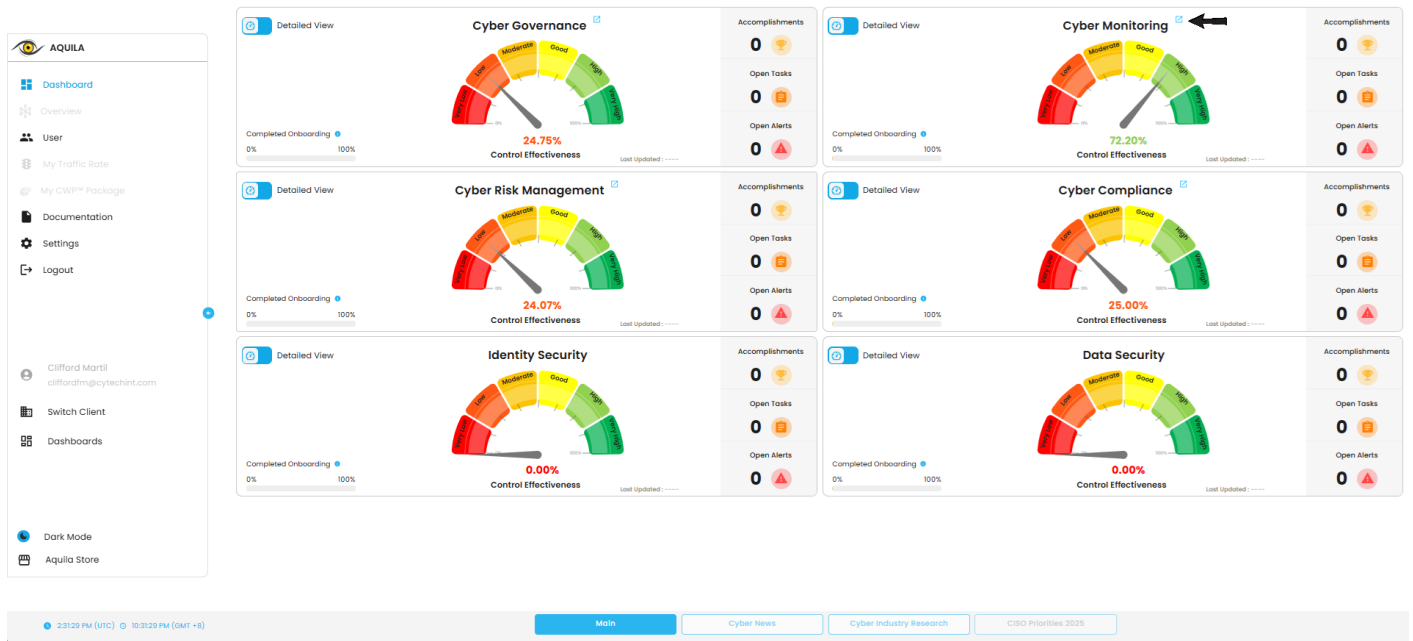
Pre-Installation Steps:

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

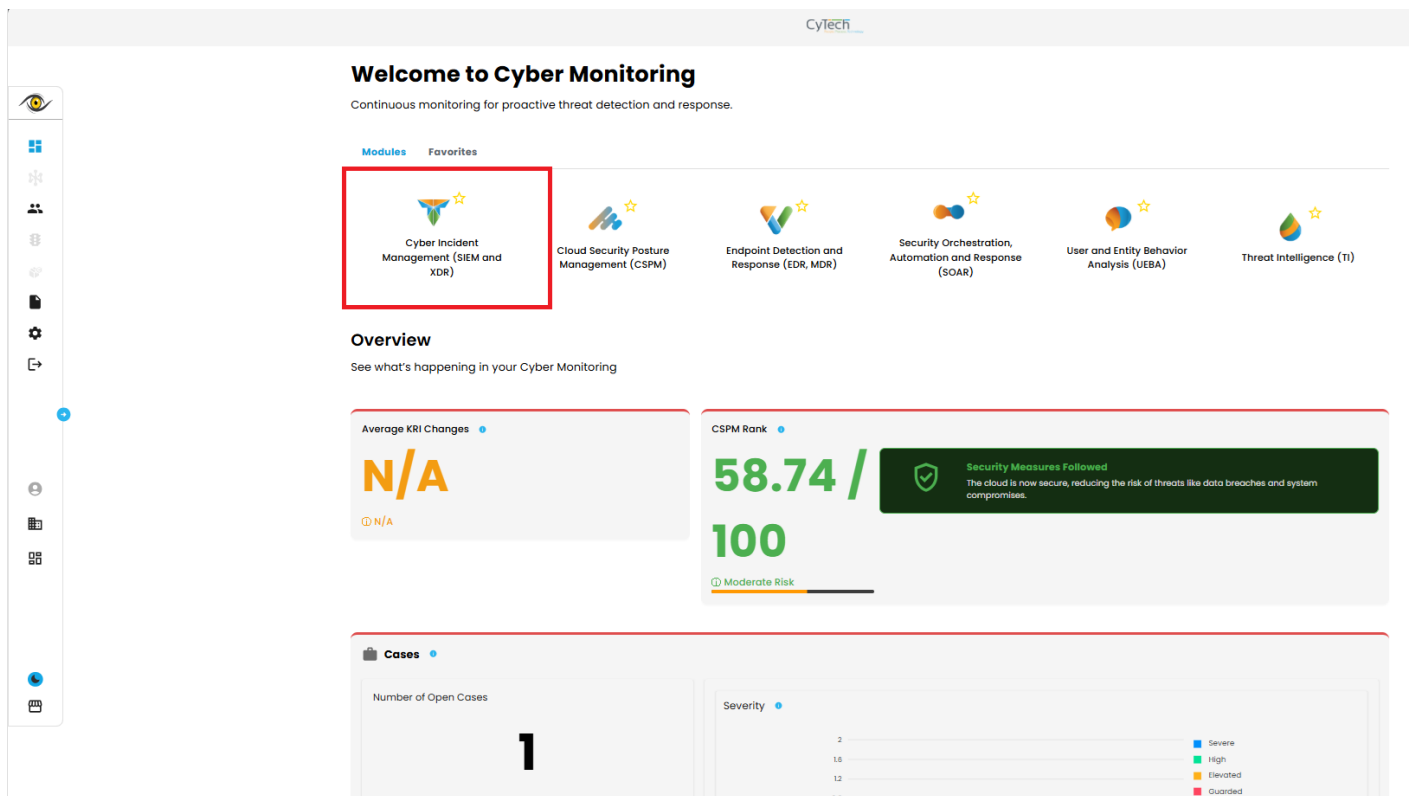
1. Pre-Installation Questionnaire: Kindly fill out the questionnaire <https://forms.office.com/r/MNvfCj3q8E>, which will help us customize the platform to your specific requirements.
2. The CISO Workplace Log Collector shall be installed as a VM (Virtual Machine).
The host for this VM can be a Windows 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:

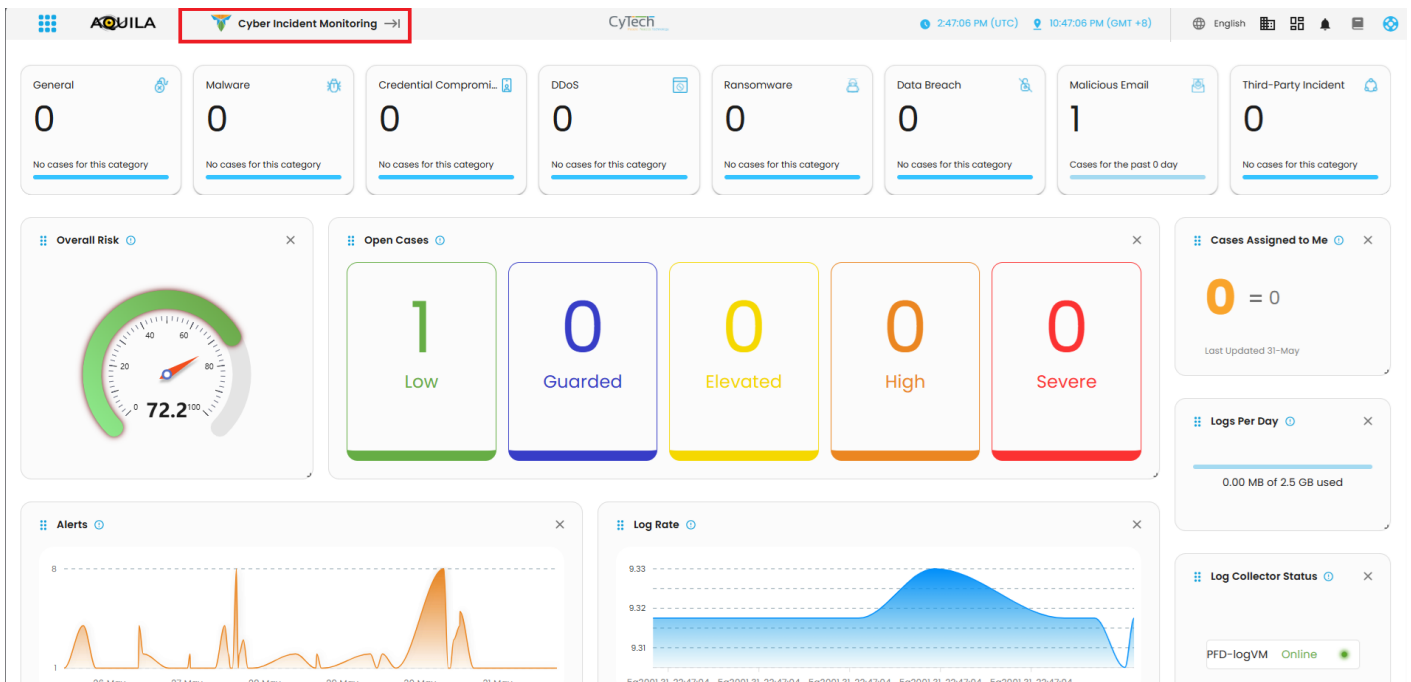
- To show all the different modules, click on the menu icon. 



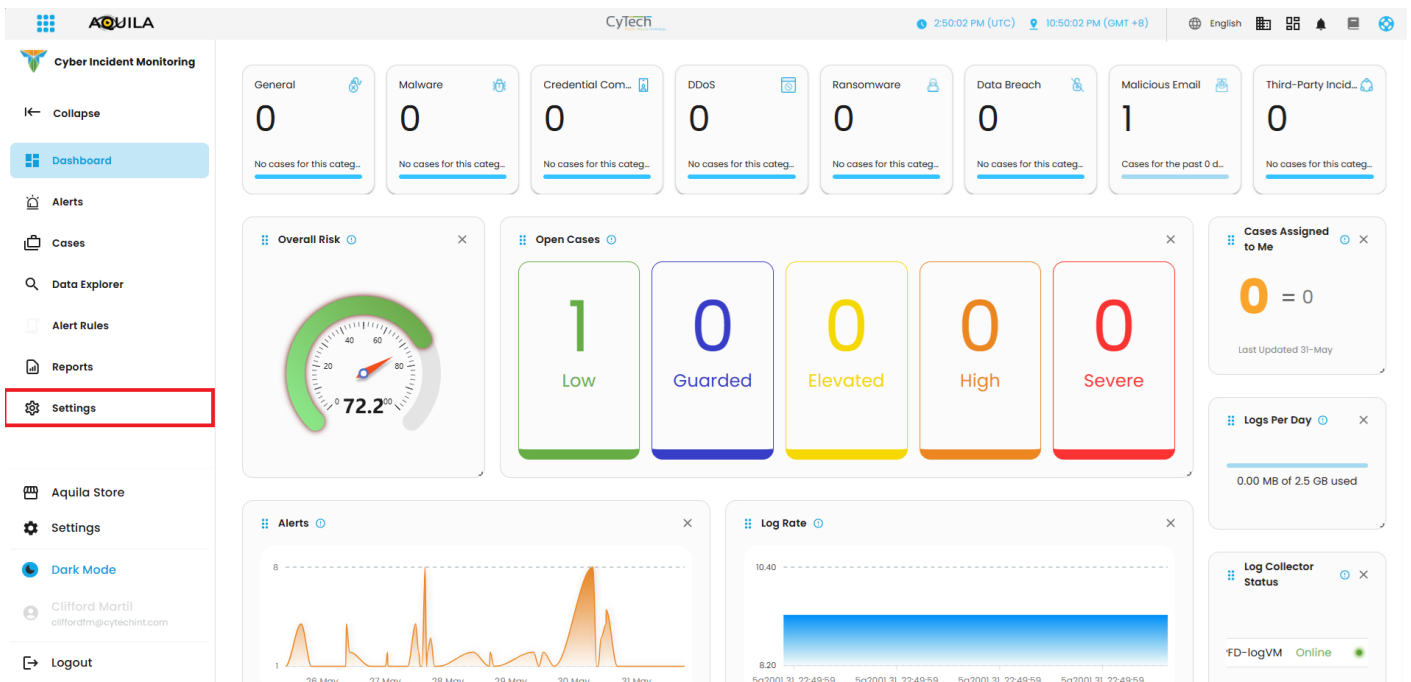
- Under Cyber Monitoring, click on Cyber Incident Management (SIEM, XDR)



- To **Display Dashboard**, click this



- Click on **Settings** to start the Log Collector installation and follow the instructions:



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

Cyber Incident Monitoring

Collapse

Dashboard

Alerts

Cases

Data Explorer

Alert Rules

Reports

Settings

Aquila Store

Settings

Dark Mode

Clifford Martil
cliffordm@cytechtint.com

Logout

Settings for CIMS

Notifications

Log Collector

Log Source

Alert Rules

Kanban

Access Control

Log Source

List of all Integrations for your agent.

Search Integration

List of Integrations

IPassword Events
1.30.2

Collect logs from IPassword with Elastic Agent.

Add to Agent

Abnormal Security...
1.0.1

Collect logs from Abnormal Security with Elastic Agent.

Add to Agent

Akamai logs
2.26.0

Collect logs from Akamai with Elastic Agent.

Add to Agent

Amazon Security L...
2.0.0

Collect logs from Amazon Security Lake with Elastic Agent.

Add to Agent

Apache logs and m...
1.26.0

Collect logs and metrics from Apache servers with Elastic Agent.

Add to Agent

Apache Spark metrics
1.3.0

Collect metrics from Apache Spark with Elastic Agent.

Add to Agent

Apache Tomcat
1.8.1

Collect and parse logs and metrics from Apache Tomcat servers with ...

Add to Agent

Elastic APM Integ...
8.15.0-preview-1716438434

Monitor, detect, and diagnose complex application performance issues.

Add to Agent

Arista NG Firewall...
1.2.0

Collect logs and metrics from Arista NG Firewall.

Add to Agent

Audit Logs
2.2.2

Collect logs from Atlassian Bitbucket with Elastic Agent.

Add to Agent

Audit Logs
1.26.1

Collect logs from Atlassian Confluence with Elastic Agent.

Add to Agent

Audit Logs
1.27.2

Collect logs from Atlassian Jira with Elastic Agent.

Add to Agent

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**](mailto:support@cytechint.com).

We're thrilled to work with you!

Revision #6

Created 21 October 2024 15:17:00

Updated 31 May 2025 15:25:02 by Clifford Martil