

Dashboard

Quick navigation for the new Aquila v4 Dashboard.

- [AQUILA v4. Dashboard](#)

AQUILA v4. Dashboard

Overview

This is the new and improved dashboard of the **AQUILA**, where it might seem confusing than the old dashboard. It contains a lot of information with each module, metrics, and its domains. Basically, an overview of monitoring on what are the things that need help and the things that are required to do for the daily operations.



Cyber Way Points

Let's start with this section, **Cyber Way Points** section is where the different task list is located for each module, such as **Cyber Training**, **Culture & Awareness** and other modules with assigned task and its details.

Cyber Way Points

60

Total Tasks

23

In Progress

34

Due Soon

3

Overdue

Q Search

Immediate

Task List

60 Tasks

Establish Network Segmentation

Zero Trust Architecture

Due Date: 2 days ago

Overdue

Not Yet Started

Conduct Phishing Awareness Training

Data Governance & Privacy

Due Date: 2 days ago

Overdue

In Progress

Deploy Intrusion Detection System

Data Governance & Privacy

Due Date: 2 days ago

Overdue

In Progress

Perform Security Audit

Cyber Resilience

Due Date: 2 days

Due Soon

In Progress

Evaluate Firewall Configuration

In Progress

Conduct Phishing Awareness Training

Module: Cyber Training, Culture & Awareness

Domain: Zero Trust Architecture

In Progress

Details

Subtasks

Attachments

Comments

Activity

Description

Reach out to all department heads to confirm their current contact details. Ensure updates are documented in the standard contact format and confirm acknowledgment.

People

Assignee

Accountable

John Doe

John Doe

Details

Complexity

Priority

Planned Start Date

Planned End Date

Actual Start Date

Actual End Date

Cost

Estimated Cost

Relation

Content Security Policy (CSP) Header Not Set

Delete Task

Edit Task

Overall Cyber Posture

Cyber Posture reflects all combined cybersecurity health across each domain and its management for security operations.

Overall Cyber Posture

51%

Overall Cyber Posture

Consolidated view of cybersecurity posture and maturity across all domains.

51%

As of October 25, 2025

Current Status At Risk

Some domains show early gaps. Controls exist but require focus to prevent risks from accumulating.

What is Overall Cyber Posture

Overall Cyber Posture reflects the organization's combined cybersecurity health across all ten domains. It shows how well controls, risk management, and security operations are performing, and whether capabilities are balanced, sustainable, and aligned with business objectives.

Cross-Domain Performance Overview

Click on domain icon to view Cross-Domain Performance

Overall Cyber Posture Levels

Each level represents the organization's overall cybersecurity maturity and risk exposure based on the combined performance of all domains.

Needs Attention

0-25%

At High Risk

26-50%

At Risk

51-75%

Optimal

76-100%

What affects in cyber?

Multiple domains are operating well below acceptable thresholds. Control gaps, delayed execution, or unmanaged risks are widespread.

What affects in business?

High likelihood of security incidents or operational disruption. Leadership lacks reliable assurance over cybersecurity readiness.

Example

Several domains consistently at At High Risk with unresolved critical KPIs.

What affects in cyber?

Domain weaknesses are accumulating faster than improvements. Risks are known but not being addressed at sufficient speed.

What affects in business?

Security teams may be reactive rather than proactive. Governance and execution gaps begin affecting business confidence.

Example

Repeated delays in remediation, incomplete initiatives, or weak governance follow-through.

What affects in cyber?

Core security capabilities exist but lack consistency across domains. Improvements are visible but uneven.

What affects in business?

Security posture is manageable but fragile. Targeted failures could cascade into broader risk.

Example

Strong performance in some domains offset by persistent weaknesses in others.

What affects in cyber?

Most domains meet or exceed expected maturity thresholds. Risks are controlled and continuously monitored.

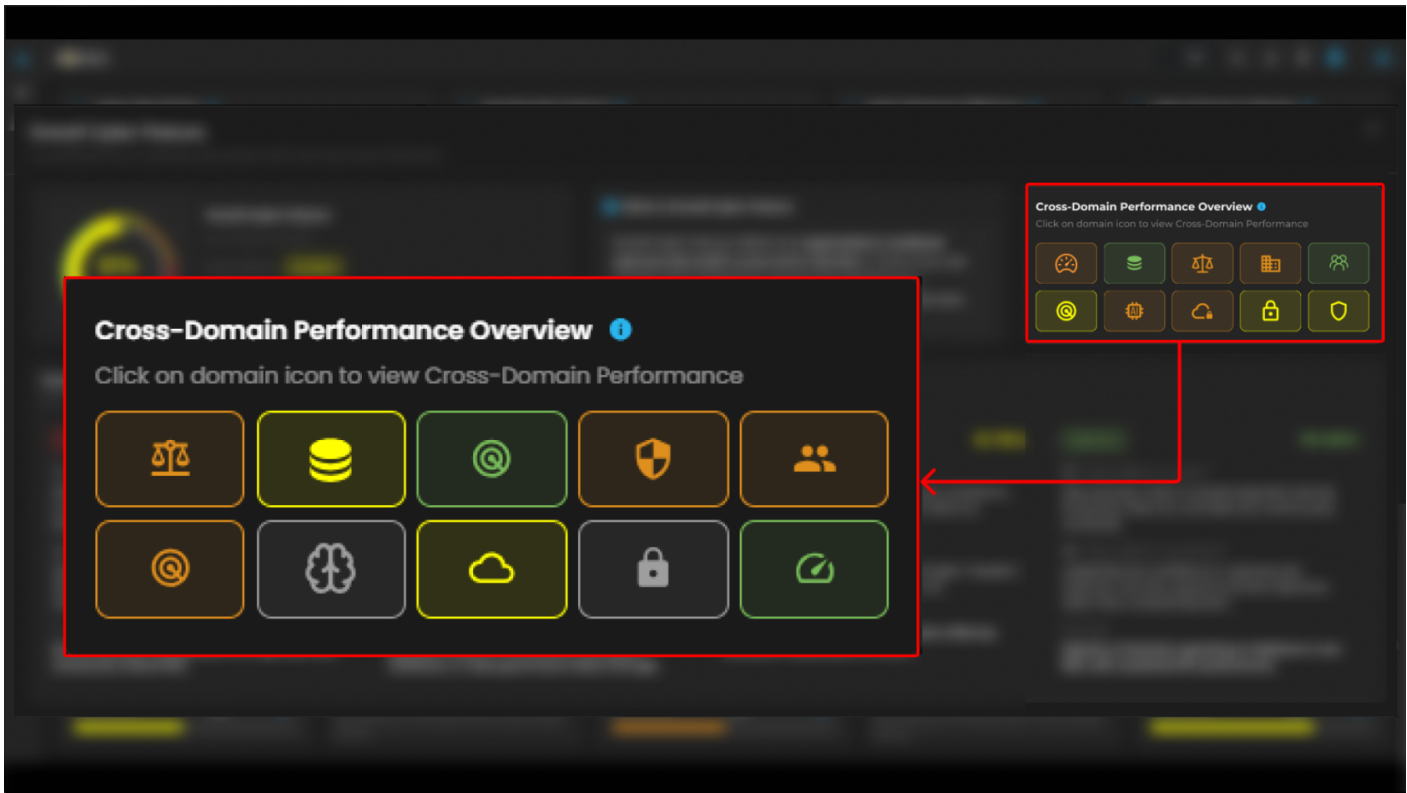
What affects in business?

Leadership has confidence in cybersecurity readiness. Security supports business objectives rather than constraining them.

Example

Majority of domains operating at Optimal or Low Risk with sustained KPI performance.

Clients can also access "Cross-Domain Performance Overview" to navigate different modules that are assigned for each button.



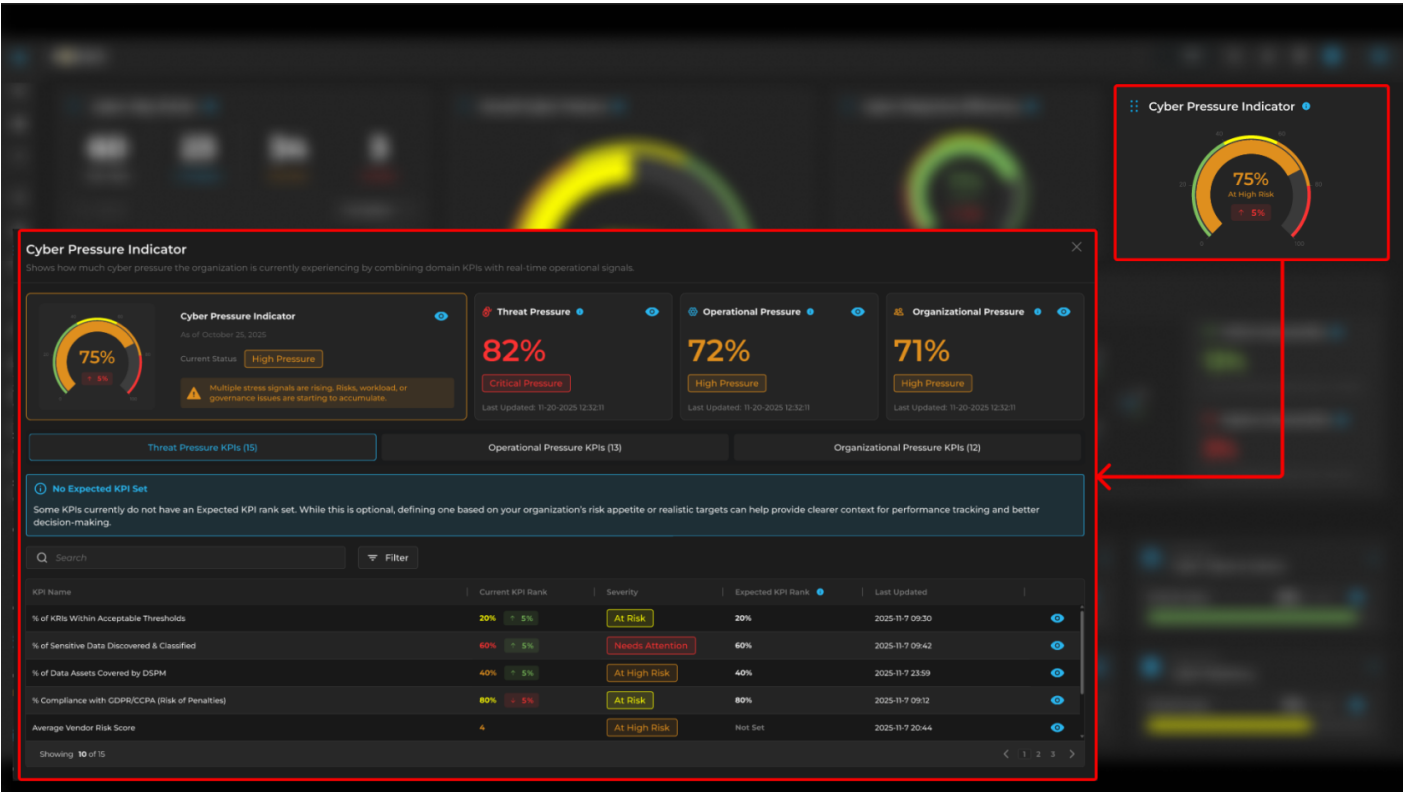
Cyber Response Efficiency

This section shows **Mean Time to Detect (MTTD)**, **Mean Time to Respond (MTTR)** and **Metrics** for response efficiency on cyber incident on how well your organization takes incident.



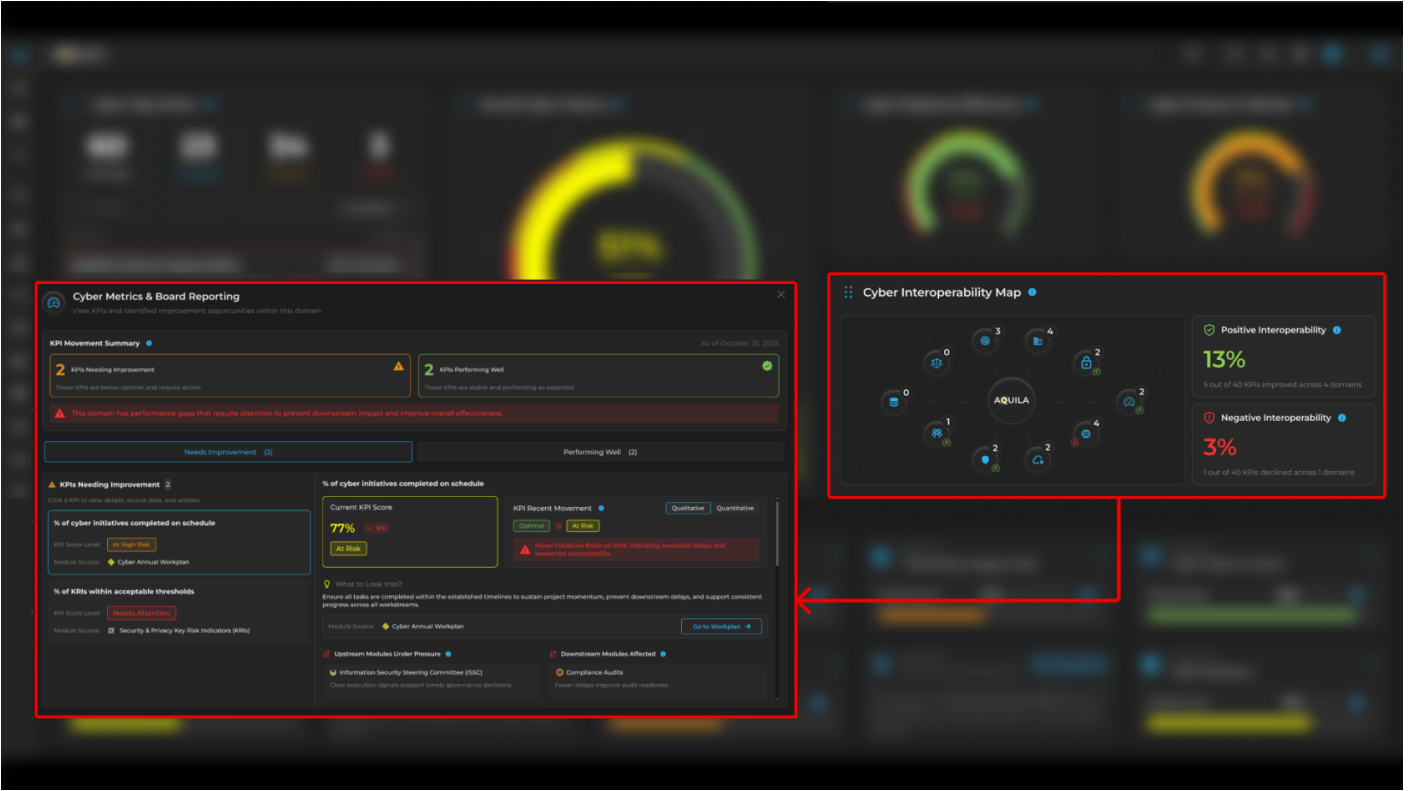
Cyber Pressure Indicator

This section shows combined KPI with real-time operational signals. It also shows list of KPI with their "Severity" and "Expected KPI Rank"

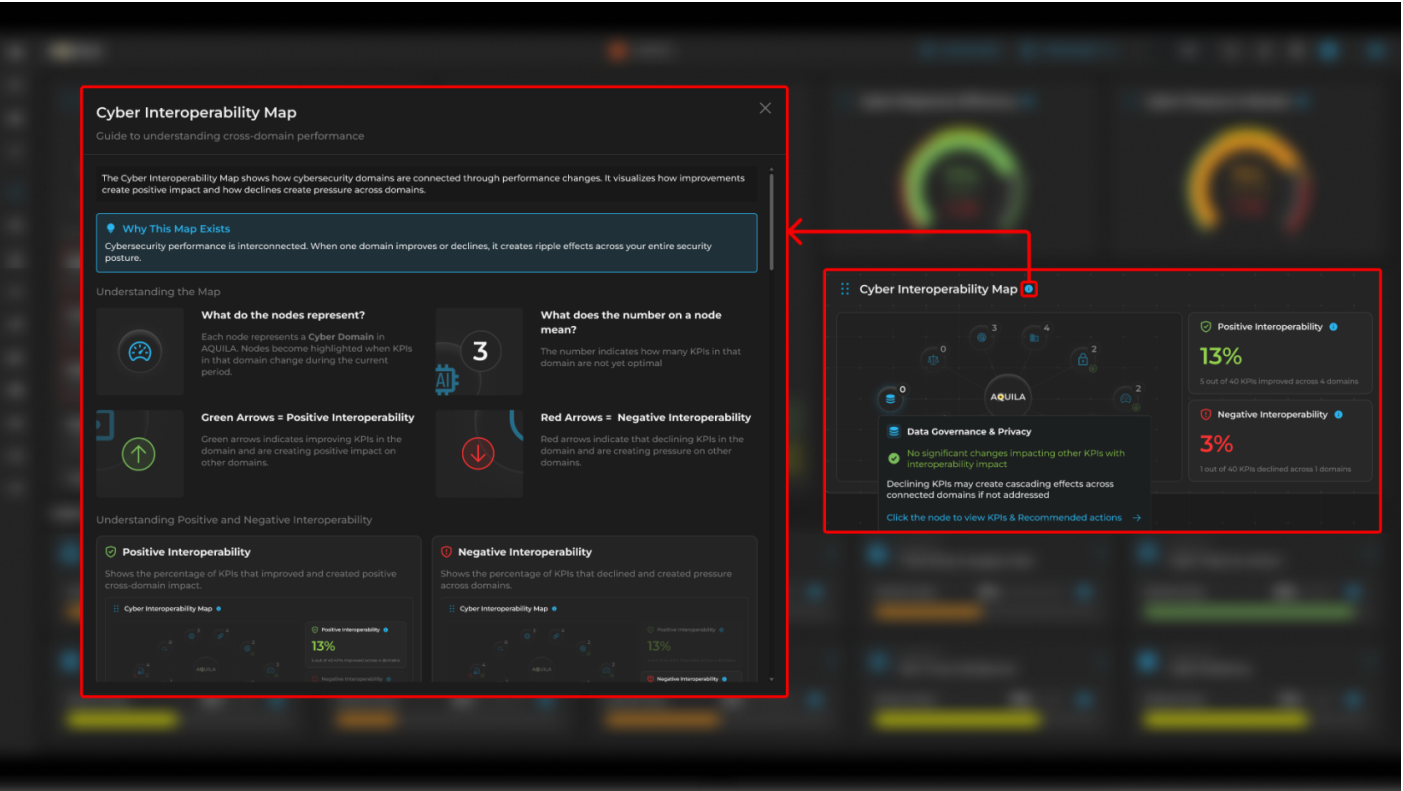


Cyber Interoperability Map

Cyber Interoperability Map is a section where, clients can see their performance of the KPI, and % of Cyber initiatives on schedule with their scoring.

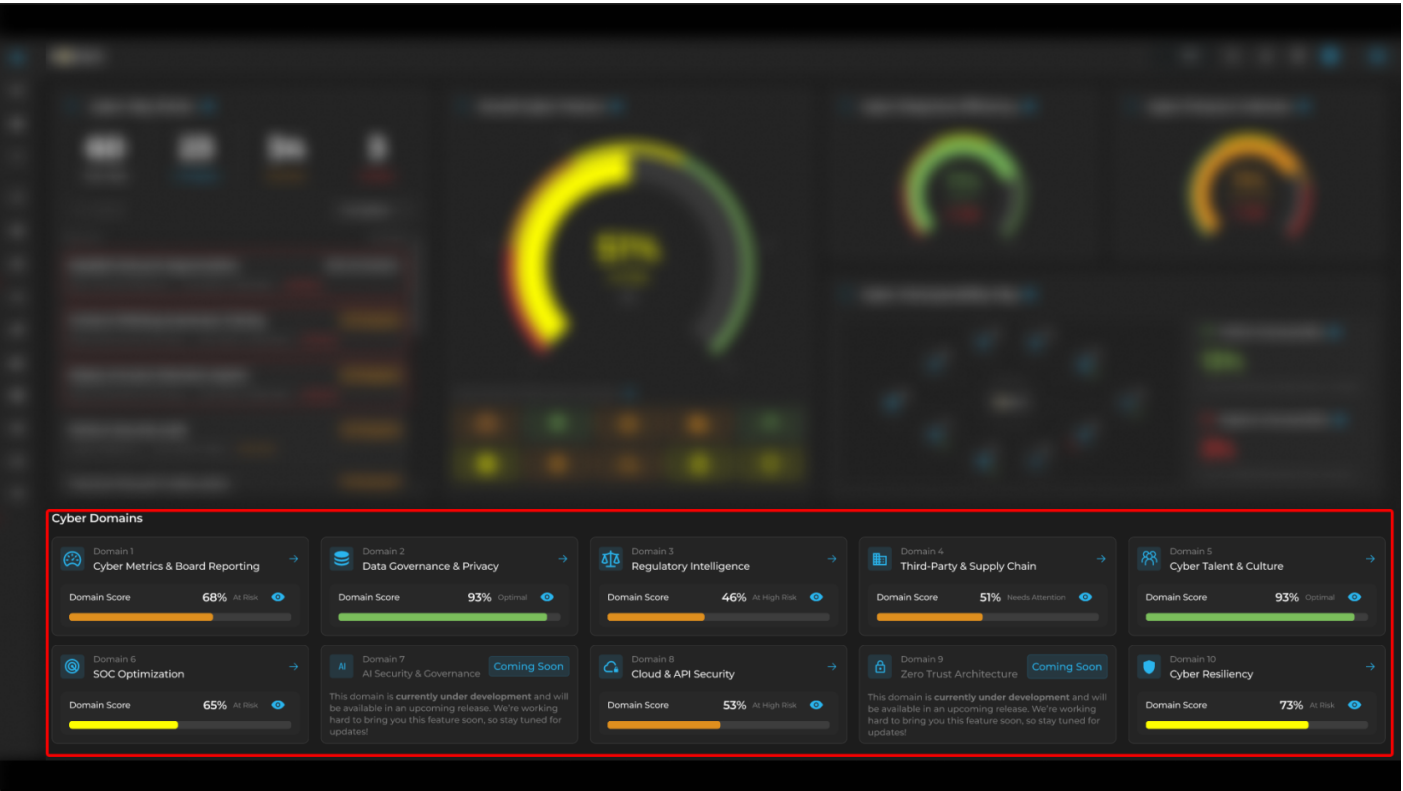


Users can also click the "!" icon to learn more about **Cyber Interoperability Map** and its usage.



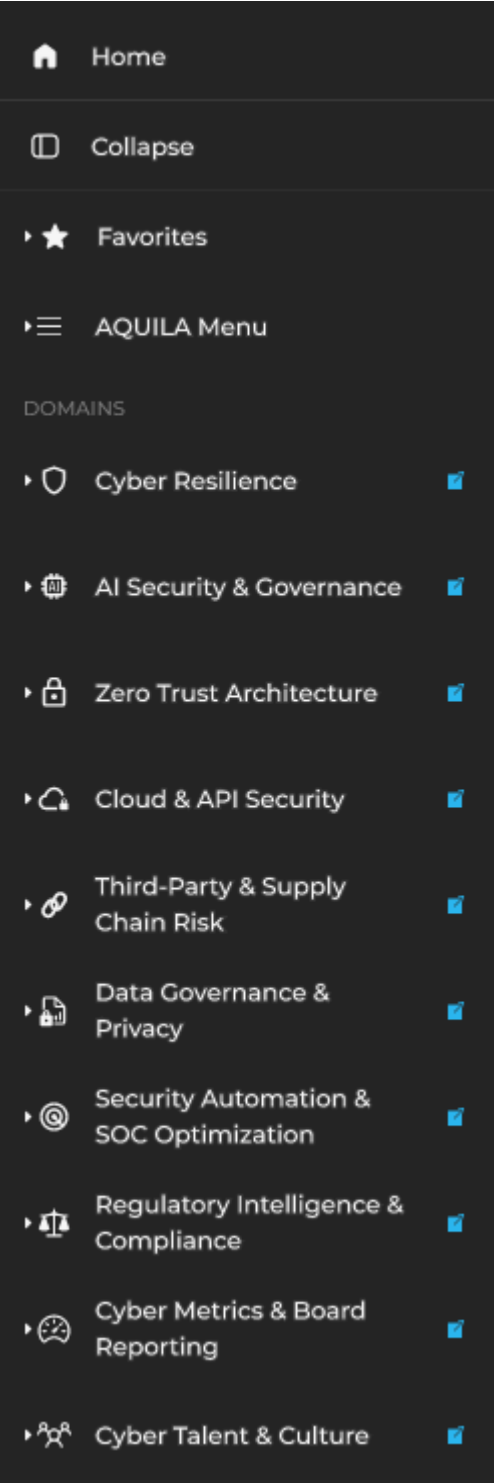
Cyber Domains

This section provides **Domain metrics** and **Domain scoring**, each of Domains contains modules that can be used as a navigation.





Clients can also use the side bar to navigate each module by pressing this icon .



“ Each module in the system contains several submodules that function as helpful and specialized tools for Cyber Security Operations. These submodules are designed to support different aspects of cybersecurity processes, enabling

organizations to manage threats, respond to incidents, and maintain operational security more effectively. For example, the Cyber Resilience module includes the Cyber Incident Management subdomain, which plays a critical role in supporting cyber investigations and case management. This subdomain provides structured processes and tools that allow security teams to document, analyze, and manage each investigation in an organized manner. Through these capabilities, cybersecurity professionals can track incidents, coordinate responses, maintain investigation records, and ensure that each case is handled systematically and efficiently.

The newly improved **AQUILA v4 Dashboard** serves as an essential tool for **Cyber Security Operations** by providing a comprehensive overview of the platform's modules and their current security status. Through its centralized interface, security teams can easily monitor and assess the overall condition of the system, including identified vulnerabilities and potential security risks. The dashboard highlights vulnerabilities that require remediation, allowing cybersecurity professionals to prioritize and address critical issues more efficiently. By presenting this information in a clear and organized manner, the **AQUILA v4 Dashboard** enables faster detection of threats, improved response times, and better decision-making for security operations. Ultimately, this enhanced visibility helps organizations strengthen their cybersecurity posture and maintain a proactive approach to threat management and incident response.

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