CYBER QUANT

Release Notes Version 4.30

AUGUST 2024

Introduction

We are excited to announce the release of Cyber Quant Version 4.30, which features enhancements to improve customer experience and enrich cybersecurity assessments. This version includes a cutting-edge web interface for the Control Maturity Analysis - CyMA, which empowers and facilitates an organization's assessment analysis. Below delves into this and other features:

Key Highlights of Cyber Quant Version 4.30

Cyber Quant Methodology Enhancements: This release introduces new capabilities that strengthen the CQ Assessor with advanced customization and analytics features. Key updates include:

- **Indicator Analysis:** The new indicators analysis window offers customers the analytics capability of the CyMA desktop tool in the Cyber Quant Portal. Now, customers can review the control indicators and their descriptions. Additionally, customers can mark indicators and controls as relevant or irrelevant, overwrite their score, and visualize their maturity score through this new interface. This interface, in addition to grouping indicators into their respective controls, also offers the option of filtering by control category, standard (if applicable), technology, and environment allowing a quick search of indicators.

- **Standards and Frameworks Interface:** Cyber Quant now offers a straightforward approach to working with the supported standards and frameworks. The new view, included as part of the assessment journey, allows customers to add, remove, or replace standards from an existing evaluation with a single click.

- **Standards Breakdown Dashboard:** Cyber Quant can now visualize a breakdown of the mapped standards, frameworks, and regulations in an individual dashboard that is reachable from the assessment dashboard. This new view allows customers to understand the evaluation results in detail from the perspective of a particular standard, along with actionable recommendations.

- **User Interface Enhancements:** Cyber Quant has enhanced its methodology by adding detailed explanations for each widget in the results dashboard. We have also introduced a new glossary widget that provides definitions for the terminology used in Cyber Quant. Additionally, the portal offers information on the "help me decide" widget for each question in the questionnaire menu and a glossary in the assets and technology menu.
  This new feature aims to help clients quickly find and understand the dashboard results, become familiar with the terminology, and find guidance when configuring and answering a questionnaire.

- **Dashboard Enhancements:**
  - **Recommendations:** We've extended the feature from CQ Lite reports (version 4.29) to CQ Essentials. The Control Gap Analysis section in the Dashboard now includes a new widget with recommendations. This guides customers to a window where they can find recommendations for identified gaps during assessments. Additionally, a new integration tab allows customers to open a ticket in ServiceNow Platform and implement the recommendations for identified gaps.
  - **RiskRecon Widget:** To enrich the integration experience between Cyber Quant and RiskRecon customers, a new Risk Recon widget is added to the Cyber Quant dashboard. The widget displays metrics such as Risk Recon rating, security domain rating, industry rating, and companies related to this company's domains.

- **New Standards and Frameworks:** NIST CSF 2.0 has been added to expand the coverage of security standards and frameworks, giving organizations options and flexibility on what to evaluate. NIST CSF 2.0 Comprehensive Assessment based on the NIST CSF set of guidelines for mitigating cybersecurity risks published by the US National Institute of Standards and Technologies (NIST). NIST CSF 2.0 can be assessed in two ways:
  - CQ Essentials 500+ Questionnaire can be used to leverage the already existing mapping between Cyber Quant Security Framework and NIST CSF 2.0.
  - NIST CSF 2.0 CMMI-Based Assessment, which leverages the CMMI-based questionnaire to identify gaps in their cybersecurity capabilities, measure their maturity level, and progress toward achieving higher levels of cybersecurity resilience.

Technical Integrations: Cyber Quant enhances its technical analysis capabilities by adding more integrations through API to streamline the assessment process. This release enables integration with Qualys SCA and improves integration with Microsoft Azure and AWS.

Additionally, as a part of our regular maintenance, the CF integration template has been updated with new simulation payloads reflecting the latest threat actors and attack methods based on current and predicted cyber threat trends observed on Cyber Insights.

Updated CIS-CAT Pro Assessor support to version 4.43, enabling Cyber Quant to integrate more technologies and benchmark versions.

Threat Intelligence Enhancements (powered by Cyber Insights): Cyber Insights has enhanced its threat intelligence source maintenance, integrating 147 new sources and phasing out outdated ones for improved accuracy. The Cyber Insights Thesaurus has been enriched with 886 new entities, and 1,047 new entity synonyms; an update that will provide visibility into emerging threat actor groups and attack tools. .

Additionally, an API has been introduced to facilitate data export and integration with external platforms, expanding Cyber Insights' functionality and accessibility. This feature allows customers with a Cyber Insights license to integrate the data output from Cyber Insights into their own systems and platforms efficiently, improving user experience and accessibility. Additionally, the API provides research functionality not included in the Cyber Insights web interface through an endpoint allowing query by multiple points of view for an easier comparison.

Resolved Issues—This release fixes and improves several functions in the Cyber Quant Platform and its components.

What's new?

Methodology enhancements

Indicator Analysis

The CyMA web interface improves the customer experience by offering a comprehensive view of technical indicators and enriching evaluation analysis. Customers can now access an interface with various analysis options, including filters by grouped controls, products, and technologies to refine their view and access a detailed context for each indicator (Image 1). They can also instantly override control and indicator maturity levels if there's a need to tweak values calculated by the system.
This feature is available for assessment types that involve technical integrations.

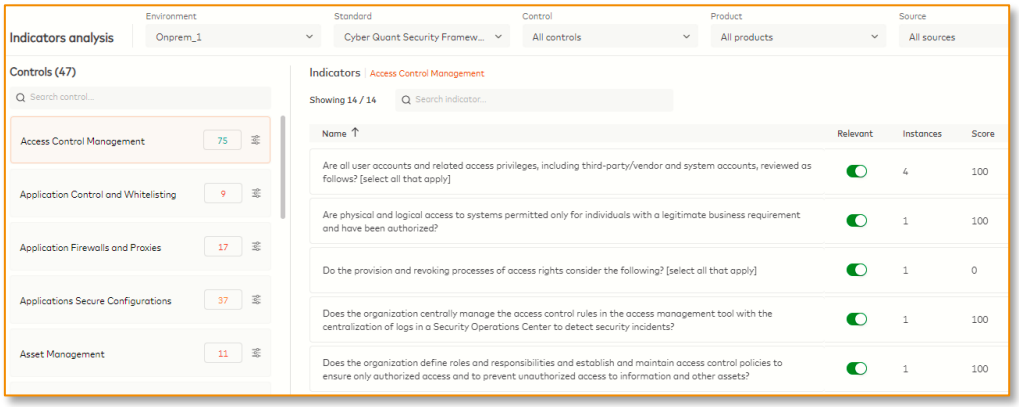


Image 1. Indicators view

A new side box will appear by clicking on each indicator (image 2), offering additional details, such as the indicator's description, technology sources, and specific information on the indicator's evaluation. This information will help the customer understand what was assessed and provide remediation guidance.

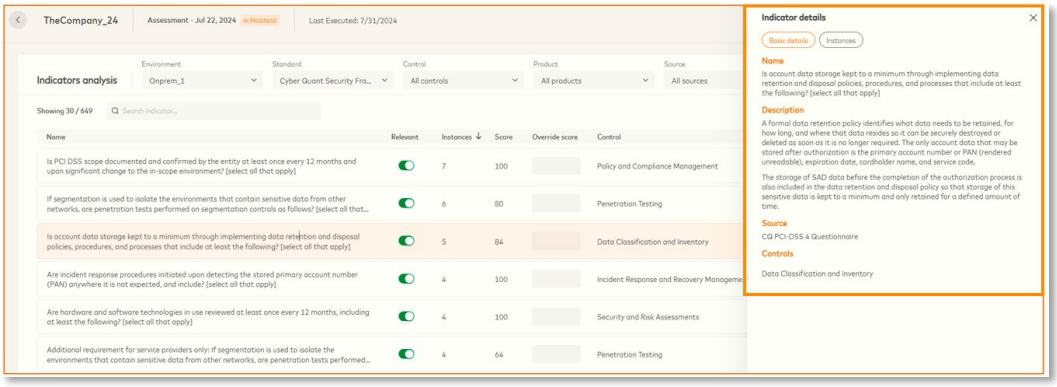


Image 2. Indicators detail side box

Control Management Options:

The hierarchy of control indications is established as follows (image 3):

- **Not relevant:** indicates that it does not apply to the assessment context and, therefore, does not receive a maturity score.
- **Control does not exist**: It has not yet been implemented and is assigned a score of zero to reflect its absence.
- **Edited:** It is a control modified or customized to fit the organization's specific needs, reflecting a maturity level tailored to the implementation.

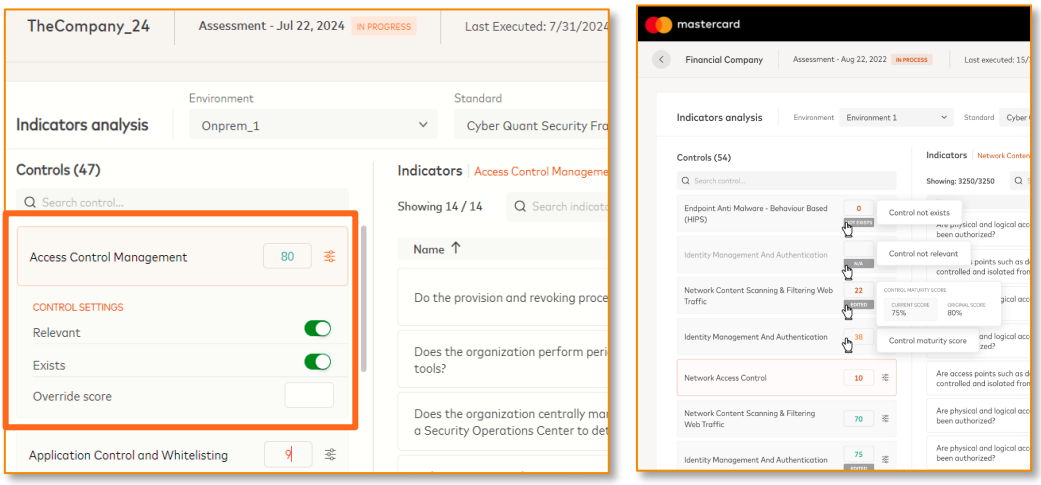


Image 3. Management options

Standards and Frameworks Interface

Manage Standards

Now, customers can quickly add or remove standards in our assessments. In the CQ Assessment Portal, a new Standards and Frameworks menu is available (Image 4); by selecting it, a new menu will appear, showing all standards and frameworks supported by Cyber Quant. To include a standard for an in-progress assessment, choose the assessment you wish to include (Image 5) and, with a single click, incorporate it into your company's evaluation.
This feature is designed to give more transparency on how CQ supports standards and frameworks, provides efficiency, and smoothens the customer experience in an evaluation process.

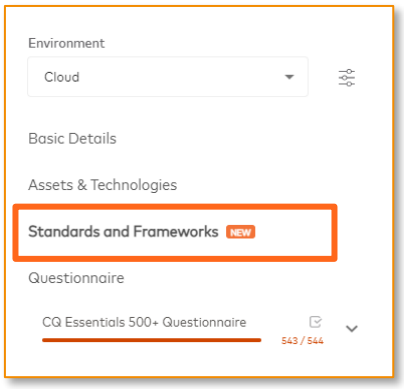


Image 4. Standards and Frameworks menu

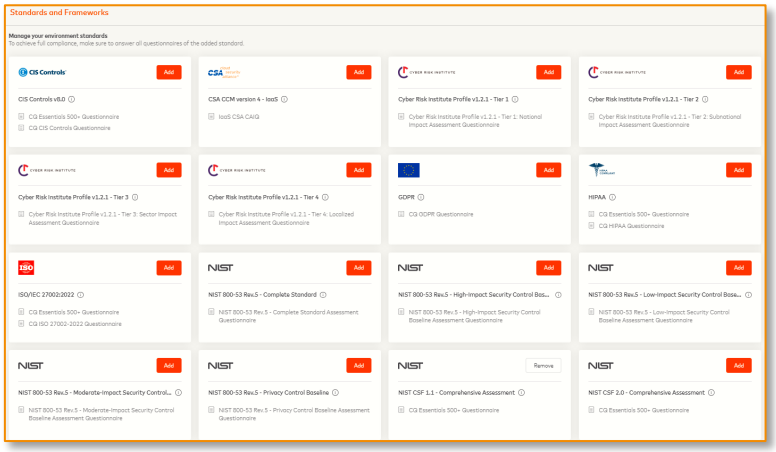


Image 5. Add / Remove standards

Standards Breakdown Dashboard

With the introduction of this new functionality, customers will be able to analyze the standards and framework results in detail (Images 6 and 7). This will facilitate in-depth control and analysis of associated indicators. Additionally, the recommendation feature included in this release will be available for this analysis, providing customers with a fully described dashboard to examine results thoroughly.

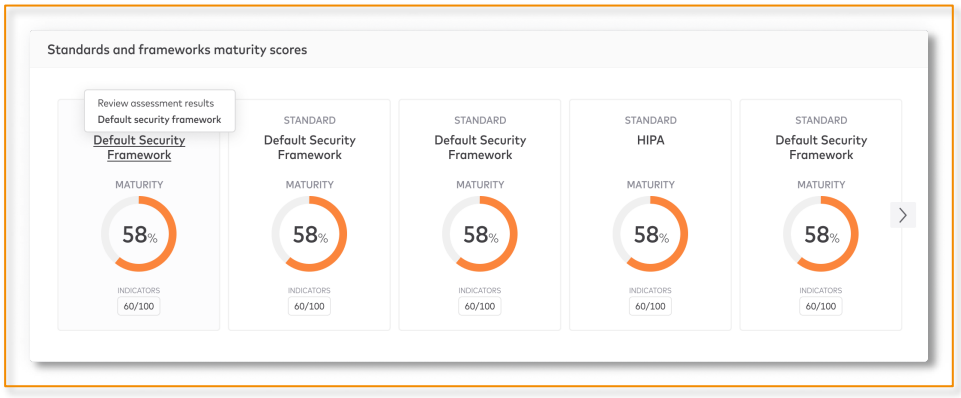
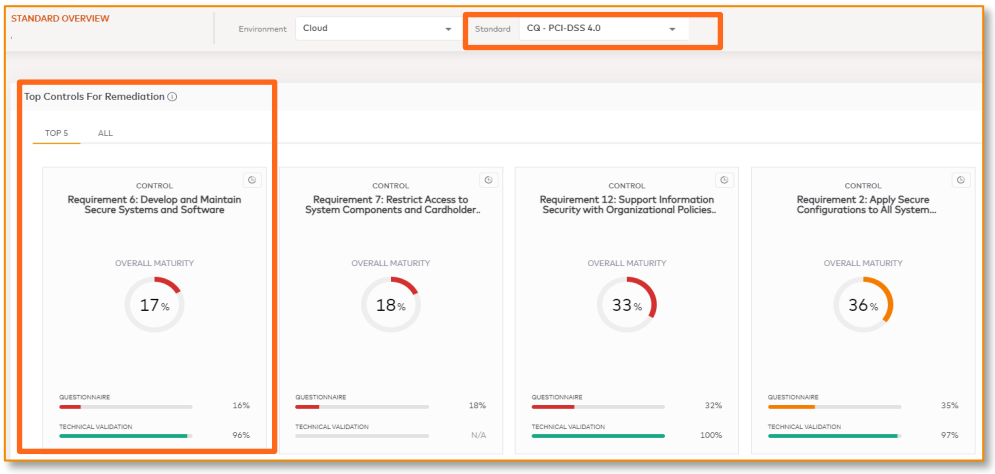
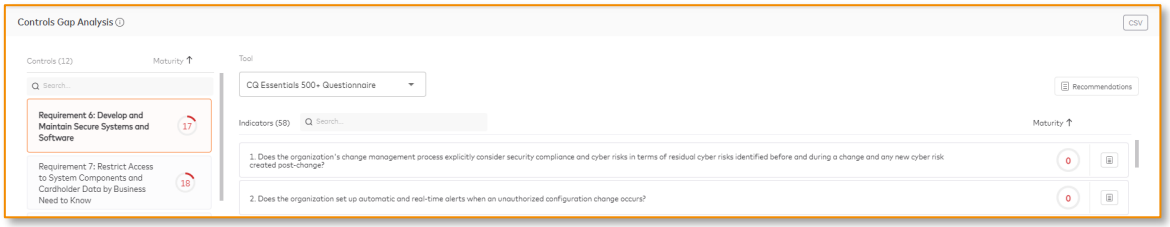


Image 6. *Standards and framework breakdown*





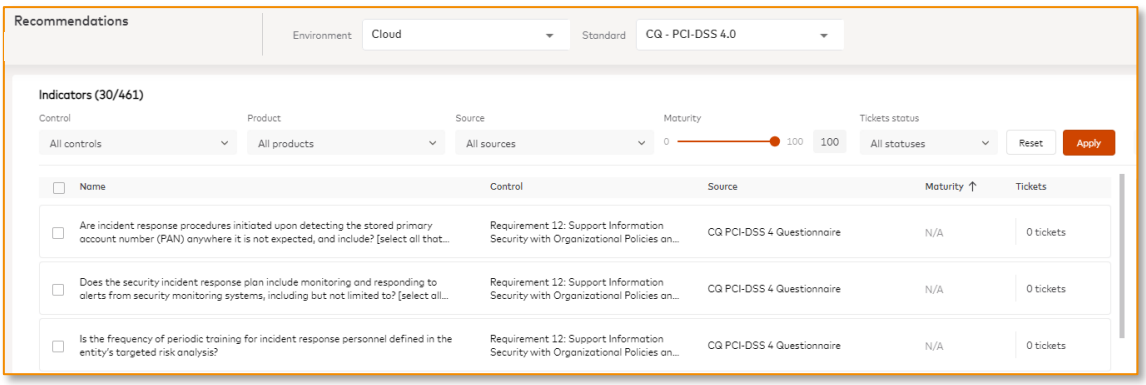


Image 7. Standards and framework detailed dashboard

User Interface Enhancements

Glossary

Customers can easily find and understand Cyber Quant terminology in the new glossary on the main dashboard (image 8). This glossary explains key concepts, terminologies, and components of Cyber Quant. Additionally, the glossary can be found in the "Assets & Technologies" menu in the Assessment Portal (image 9), where customers can access information on various classifications for these items. This ensures that customers can access essential definitions and classifications in multiple locations within the platform, making it easier to use. In addition, customers will find glossary descriptions for all the cyber metrics presented in the results Dashboard (image 10).

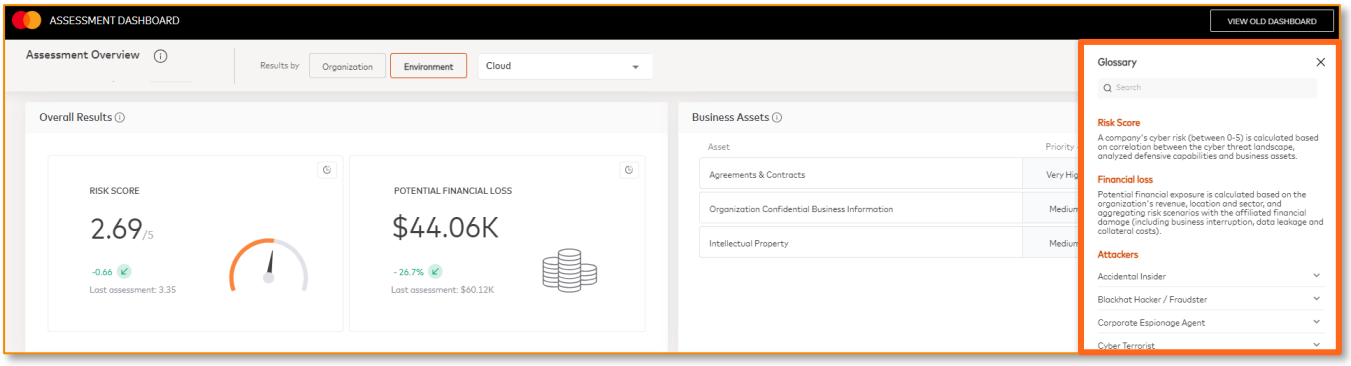


Image 8. Glossary side box in the Dashboard

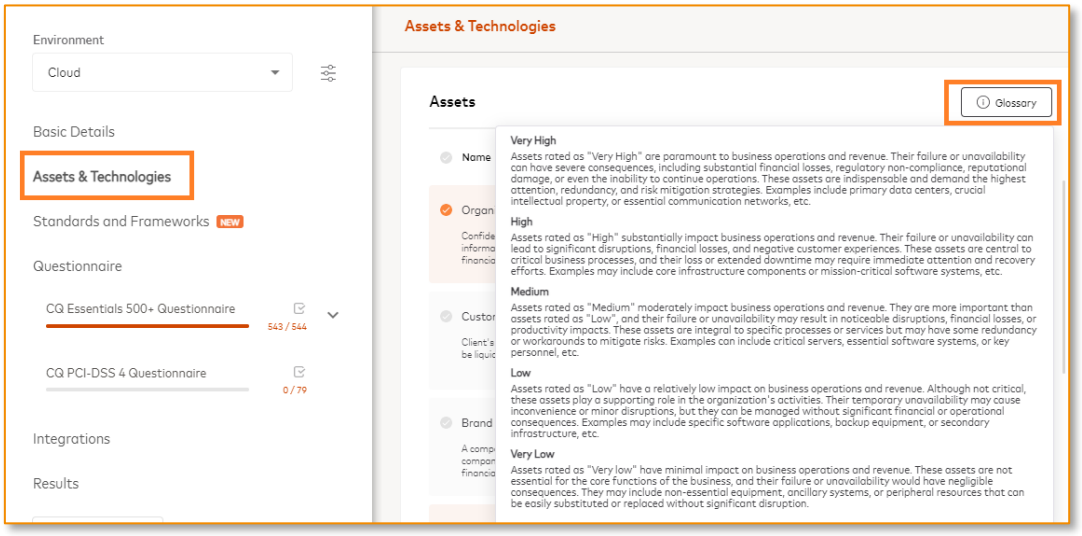


Image 9. Glossary in the assessment portal

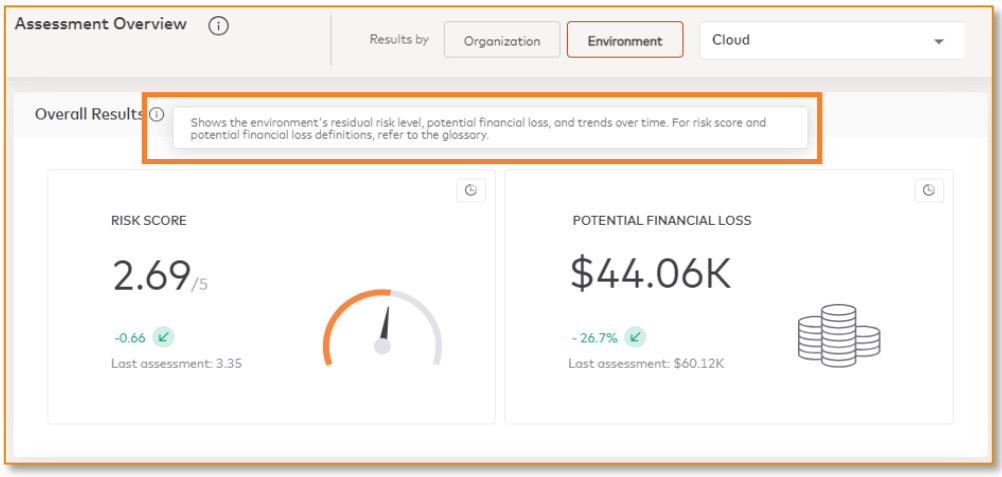


Image 10. Glossary description in the results dashboard

Questionnaire menu enhancements

Customers now have two more functionalities available to enrich and facilitate their experience during the evaluation process:

- New questionnaire update available: This function will notify you when a new version of the questionnaire is available.
- Update questionnaire: Upon clicking the button, the new version of the questionnaire is loaded. The capability is applicable across all types of questionnaires, including customer-created surveys as well as maturity and risk assessment questionnaires. When customers access their custom questionnaires, they can easily update them to incorporate the latest changes and enhancements, ensuring that all assessments, whether standard or custom, are consistently up to date.

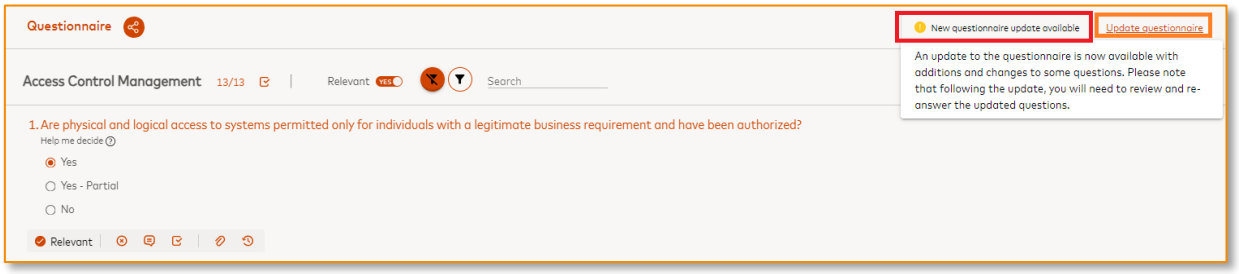


Image 12. Update questionnaire button

Dashboard Enhancements

Recommendations

Cyber Quant offers customers comprehensive recommendations view that helps to address all identified gaps. The recommendations are based on the controls in the case of Cyber Quant Lite assessments and individual indicators maturity scores in Cyber Quant Essentials assessments. This enables customers to follow a specific end-to-end process, implementing actions and then simulating the outcomes to accurately reduce risk and maturity scores.

Furthermore, Cyber Quant integrates with the ServiceNow platform, expediting the remediation process by enabling customers to create ServiceNow tickets directly from these recommendations, ensuring efficient follow-up and resolution. This can be performed in bulk or for each individual recommendation. For more information about ServiceNow integration, please visit our knowledge base website.

Additionally, users can export these recommendations out of Cyber Quant to work on the recommendations outside of the platform or to export them to a third-party platform.

Customers can access the new Recommendations window from the Dashboard result in the Controls Gap Analysis section (images 13, 14).

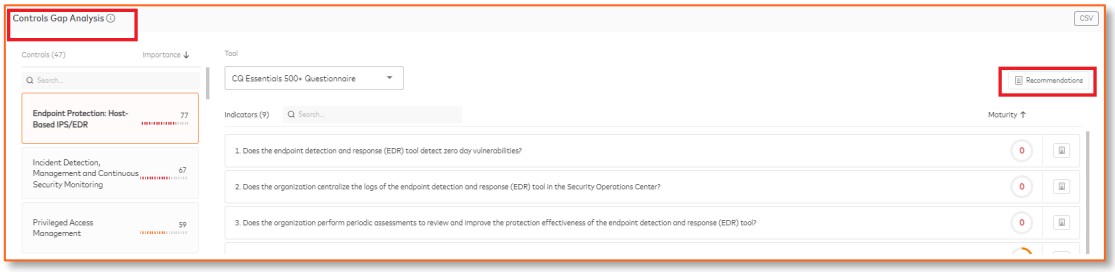


Image 13. The recommendation menu in the Control Gap Analysis section - Dashboard

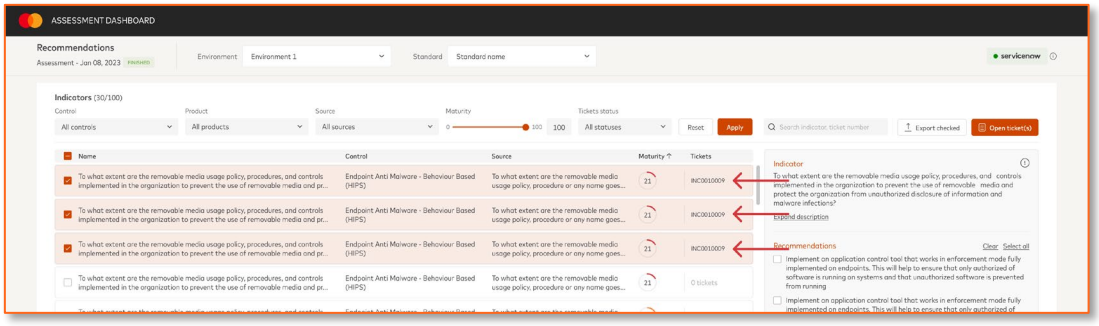


Image 14. Recommendations window & ServiceNow connection

Risk Recon Widget

The new RiskRecon widget is designed to maximize the utility of the data gathered during assessments by providing a tailored and in-depth view. It enables customers to incorporate multiple domains. The dashboard identifies pertinent companies for each domain and displays their information directly within the widget (image 14). The dropdown menu can accommodate various companies, simplifying the process of comparison.

The dashboard features a comprehensive suite of tools, including the RiskRecon Rating, which provides clear insights into the company's associated risk. It also includes Domain Ratings to evaluate the specific risk of each added domain, Industry Ratings to compare your company's ratings against industry benchmarks, and a historical view (image 15) of Risk Recon's risk ratings to track trends over time.

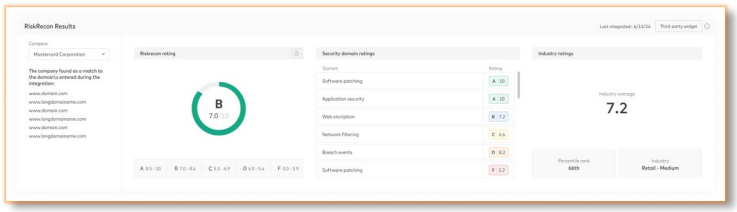


Image 14. RiskRecon Dashboard widget

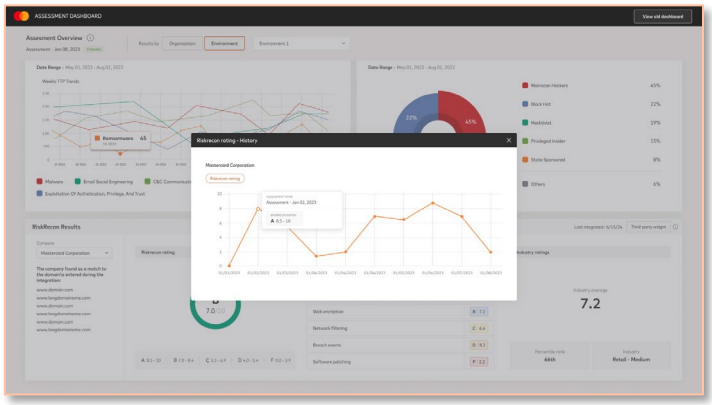


Image 15. RiskRecon Score History

New Standards and Frameworks

NIST CSF 2.0

By incorporating NIST CSF 2.0, the user can conduct a thorough assessment that evaluates both adherence to the NIST cybersecurity guidelines and the maturity of cybersecurity processes. This approach measures alignment with the comprehensive NIST framework, identifies gaps and tracks progress in cybersecurity capabilities, enabling continuous improvement and enhanced resilience.

Technical Integrations

Microsoft Azure Defender for Cloud & Regulatory Compliance

In this latest release, two Cyber Quant integrations for Microsoft Azure have been enhanced:

- Microsoft Azure CIS Security Best Practices integration now includes updated standards and supports API- and CyMA-based integration.
- Microsoft Azure Defender for Cloud / Regulatory Compliance integration has been updated with new standards and content and API-based integration capability.

AWS Resource Tagging Standard & CIS AWS Foundations Benchmark

The existing AWS API now includes comprehensive information on the AWS Resource Tagging Standard v1.0.0 and the CIS AWS Foundations Benchmark v3.0.0.

The AWS Resource Tagging Standard helps organizations implement a consistent tagging strategy across AWS resources, which is crucial for efficient resource management, cost allocation, and operational automation. Complementarily, the CIS AWS Foundations Benchmark v3.0.0 offers a set of security best practices for securing AWS accounts.

Qualys SCA

Qualys Security Configuration Assessment (SCA) is a powerful solution for ensuring an organization's IT assets are securely configured. It helps identify misconfigurations and compliance issues across various systems and applications. Integrating Qualys SCA into our platform provides a seamless connection that enables compliance scans and detailed reporting within Cyber Quant assessments, ensuring accuracy and adherence to the latest recommended practices. The robust features of Qualys SCA, such as automated scanning and continuous monitoring, offer invaluable insights for maintaining strong security postures and regulatory compliance.

CIS CAT Pro Assessor 4.43

We updated the coverage for CIS-CAT Pro Assessor to version 4.43. Adding support for the newer version enables Cyber Quant CyMA to assess additional technologies and versions. It also supports updates and refinements in CIS benchmarks for the given technologies.

Threat Intelligence Enhancements (powered by Cyber Insights)

Cyber Insights has significantly upgraded its threat intelligence source management by incorporating 105 new sources and systematically retiring outdated ones to enhance accuracy. This refinement ensures the platform provides the most relevant and up-to-date threat information. The Cyber Insights Thesaurus has been expanded with 886 new entities, enriching its comprehensive vocabulary and improving its ability to categorize and understand diverse threat indicators.

This release introduces a notable enhancement to the Cyber Insights menu, allowing customers to filter the threat landscape based on organization size, providing a more tailored and relevant view of potential threats according to their specific needs and scale.

New Cyber Insights API interface

The new API will allow customers to access Cyber Insights and the threat landscape by enabling seamless and direct integration with their existing systems and obtaining real-time analysis and data on cyber threats.
With this API, customers can customize alerts and reports to their specific needs, enhancing their ability to proactively respond to vulnerabilities and emerging threats. Furthermore, this API will facilitate the automation of processes and data-driven decision-making, representing a significant added value for customers seeking to optimize their

cybersecurity management. For more information about the Cyber Insights API integration, please consult the Cyber Insights - API article in the knowledge base.