SANS

Analyst Program

Product Review

Get the Risk Out! How to Manage Third-Party Cyber Risk

Written by **Dave Shackleford**

October 2022

cyber GRX

Introduction

Most organizations rely on third parties to provide important services and capabilities, often not realizing that third-party vendors are as vulnerable to advanced attacks as the organizations are. The increasing level of access and integration within host organization environments can present risks and potential new avenues of compromise. To manage these risks, host organizations must adapt their security procedures to include vendors, partners, and even customers. In addition, to secure the third party as much as possible, organizations must closely evaluate their own people, processes, and technology.

Third-party breaches may occur in many different ways. A software manufacturer could be breached via malware that modifies source code, which the software manufacturer then distributes to enterprises that use the software. This exact scenario played out with SolarWinds in 2020–2021.[1] Or perhaps an attacker steals a vendor's credentials, giving the thief remote access to an enterprise the vendor partners with or provides support to, which then leads to infiltration of the enterprise network from an already trusted source (the vendor network). Repeatedly, we've seen trusted access come back to bite us, whether from vendors, partners, or other third parties that organizations work with on a regular basis. We need to do a better job at securing our networks and assets from third parties that, although trusted to some extent, may still represent a significant risk to our organizations just by virtue of being connected or providing software or services to us.

We need more effective risk management for vendors and service providers that we employ in our environments or that we use to provision business services (such as cloud providers, for example). Defining critical vendors and service providers (as well as partners) represents a starting point. From there we need to carefully evaluate which types of assets and data that the third-party organizations and solutions will interact with.

With more organizations focusing on the third party than ever before, it's time to take a hard look at what third-party products and services we have, what third-party providers can access, and what types of behaviors vendors and service providers exhibit during the course of business. With the third party firmly in the crosshairs of adversaries, there's no better time than now to focus on third-party risk and third-party security.

In this paper, SANS reviews a leading third-party cyber risk management solution: the CyberGRX Exchange. We highlight several critical features and services that any organization could benefit from immediately.

The CyberGRX team provisioned an account for us that included a variety of associated third-party solutions and services. When you start off with CyberGRX, you then add any third-party vendors and services that you work with. (This was already done and configured for us.) We found the interface easy to navigate. We could also easily access the CyberGRX Knowledge Base, which contains a multitude of instructional articles, FAQs, and deeper explanations on core topics. This Knowledge Base is organized by user flow and searchable by keywords.

---

[1] "What SolarWinds Taught Us About Third-Party Risk Management," SANS Institute, www.sans.org/webcasts/solarwinds-taught-about-third-party-risk-management-118980/

Building and Managing a Cyber-Relevant Third-Party Portfolio

After we acclimated to the interface, we started to review the portfolio of vendors and third parties associated with our account. Within the CyberGRX ecosystem, this Portfolio Management Table (PMT) enables users to see and manage all third parties added to their portfolio along with details about each third party's assessment status. By clicking the Company Name, users get quick access to their Vendor Profile Pages. The Reports Available metric highlighted on this screen quickly shows you the proportion of your portfolio that already has assessment data available to request as desired (see Figure 1).

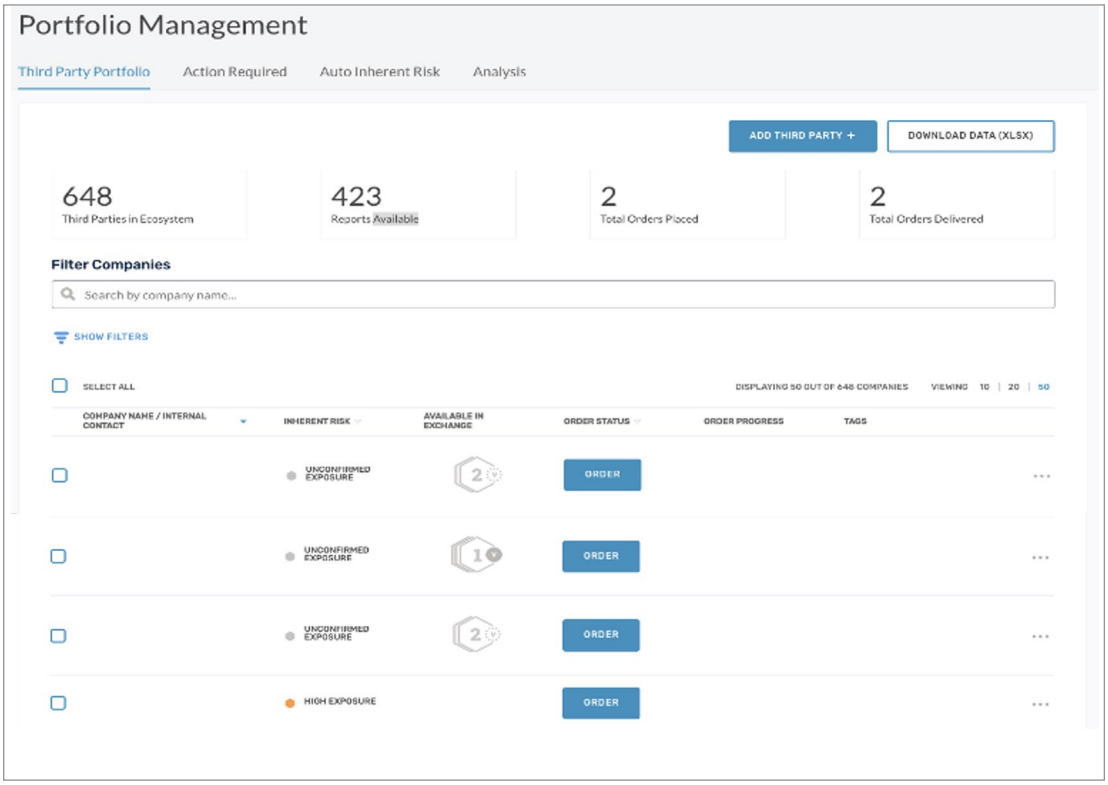

Figure 1. Portfolio Management Table Overview

We requested available risk-analysis reports for data insights into any of our third-party companies and services. Filters and correlating columns in the PMT help users further understand which level reports are available (those labeled as Available in Exchange), and which orders/data access requests have been responded to by the third party (Order Status). PMT also enables users to track the progress of new assessments they have requested (Order Progress), among other things. This function can facilitate easier portfolio management and more accurate communication to internal stakeholders about the status of their requested vendor, known risks with vendors, and more. See Figure 2 for available filtering options.

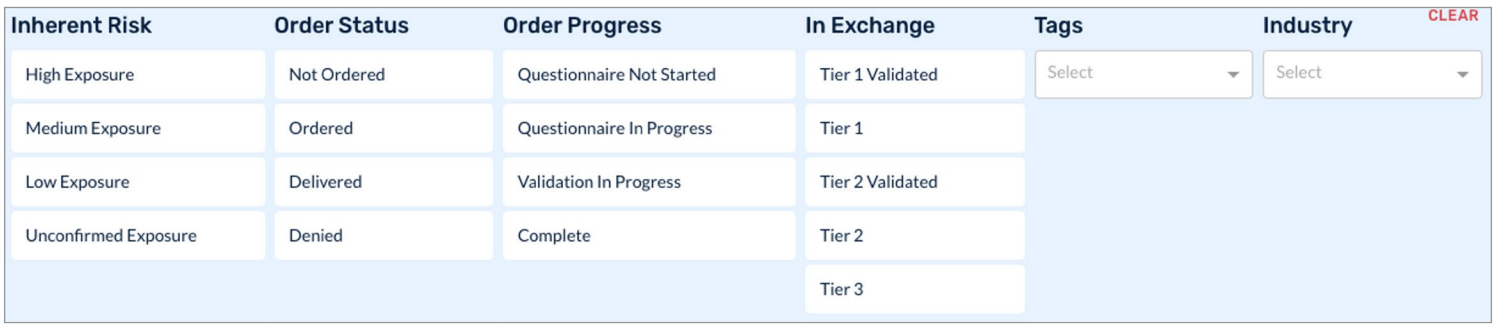

Figure 2. Portfolio Management Filtering

Although we didn't fully assess the CyberGRX Exchange, more than 200,000 vendors are listed there, each with a risk profile and associated risk data, and at least 12,000 (at the time of this writing) that had a completed risk assessment with detailed information readily available. From the main PMT interface, clicking the Available in Exchange icon displays information about a third party's completed assessment, including the questionnaire submission date. This enables organizations to decide whether the available data is acceptable or if an update to the assessment is needed (see Figure 3).

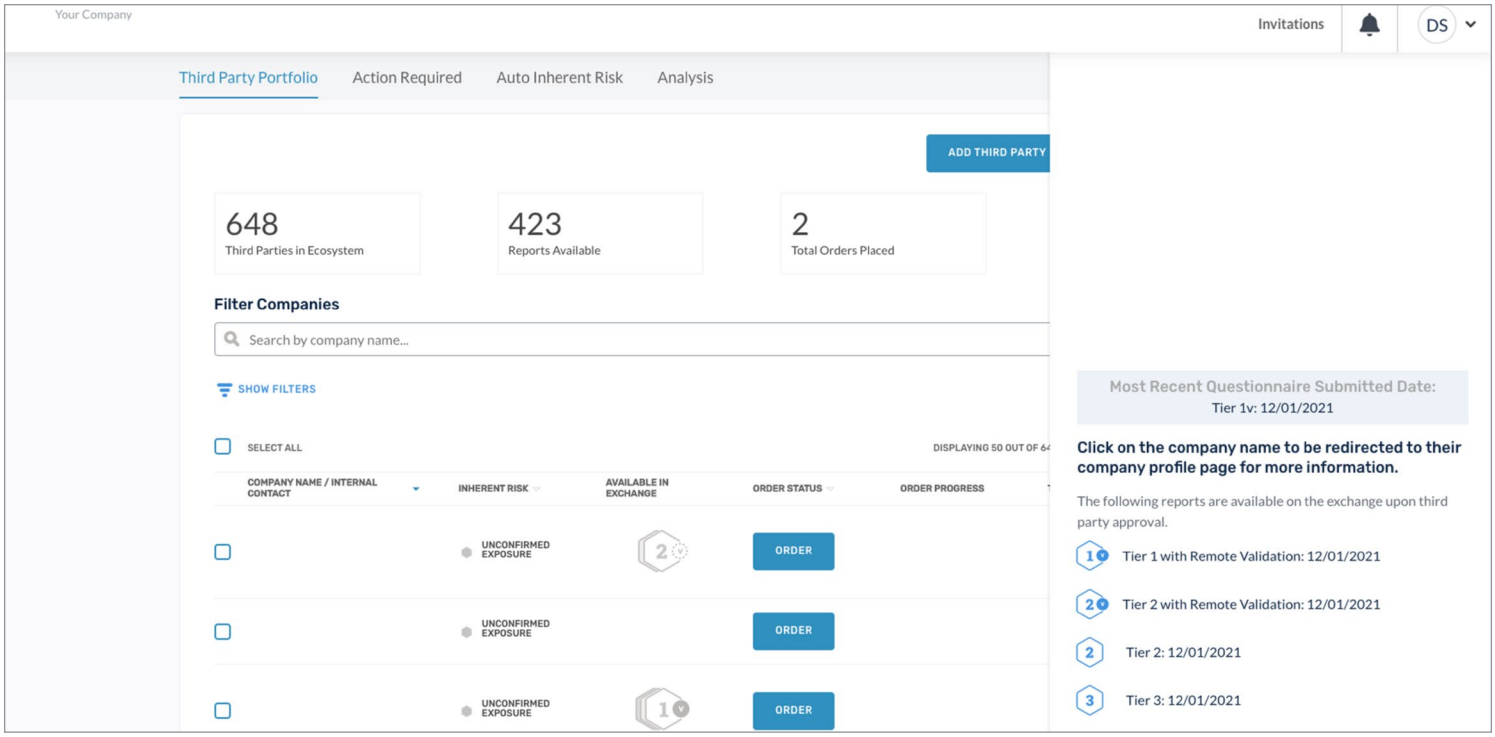

Figure 3. Risk Assessments Available for Review

In addition, if an Assessment Owner is provided under the company name, the user can see whether the third party has registered on the CyberGRX Exchange, which can facilitate more effective communication between customers and their third parties. If the third party has registered, the table displays the most relevant third-party user and the user's role. Customers can click the username to send an email to that user when necessary.

Pre-Assessment Portfolio Analysis and Third-Party Prioritization

The CyberGRX portfolio risk-analysis capabilities are particularly innovative, especially with regard to third parties that a customer wants to consider working with. A set of pre-assessment–impact questions help to determine potential business exposure if the organization seeks to associate with a given third-party organization. In the main Portfolio Management screen, the Auto Inherent Risk tab shows auto-populated answers to the eight Impact Assessment questions that help calculate the Business Exposure level (high, medium, or low) a specific third party has to the user based on their relationship. This feature further refines the contextualized pre-assessment analysis provided by CyberGRX. Here, users can edit or confirm the auto-populated answers for any non-confirmed third parties and see the aggregate risk scoring for their entire portfolio. We selected a random group of third parties in the listed catalog within our account on which to perform this overall risk review, and Figure 4 shows the simple scoring dashboard across all of them in tandem.

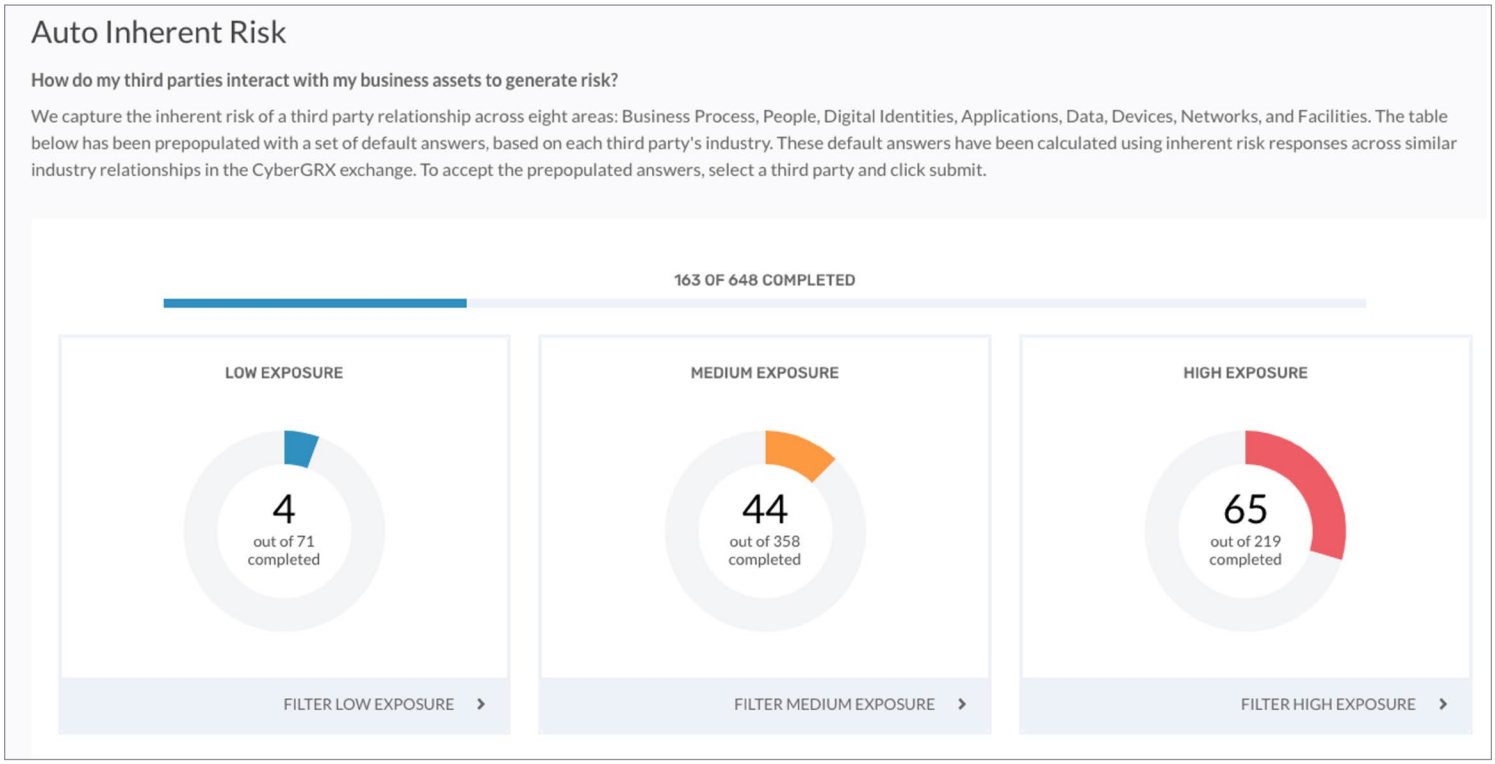

Figure 4. Auto Inherent Risk in Aggregate Across Third Parties

Figure 5 shows the menu to edit any third-party score derived by CyberGRX so that risk scoring can be adjusted on a subjective and more granular basis. (The name of the third party is redacted in Figure 5.)

In addition, the Analysis tab in Figure 6 provides a portfolio view that helps users better prioritize activities and allocate resources to the riskiest third parties based on Likelihood and Impact as well as both confirmed Business Exposure (solid circles) and non-confirmed Business Exposure (outlined circles). Along with the Auto Inherent Risk section of the platform, this can help companies prioritize which third parties to review more closely (covered in the CyberGRX Predictive Risk Profile section of this paper) and/or which assessments to request first. See Figure 6 on the next page for a risk-scoring breakdown in our sample portfolio.

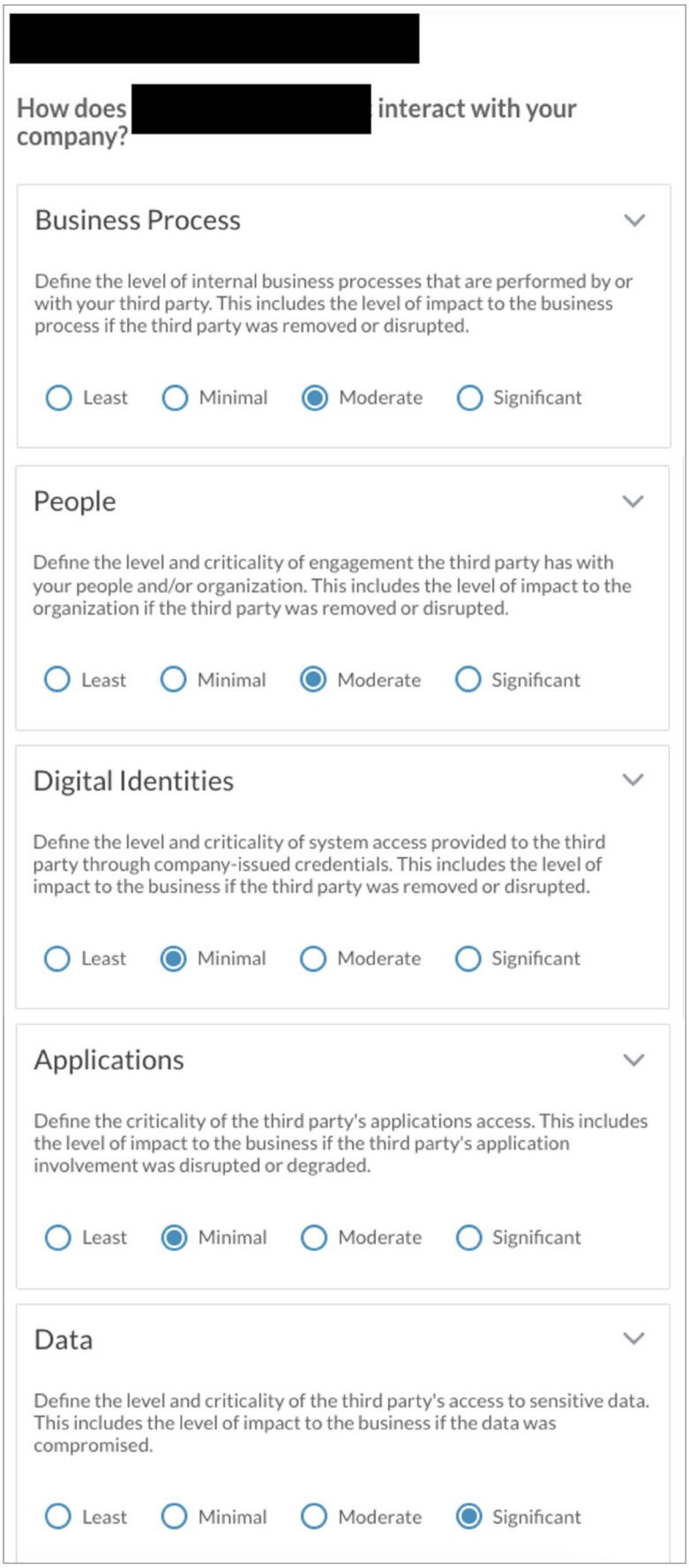

Figure 5. Modifying and Tuning Risk Scoring in CyberGRX

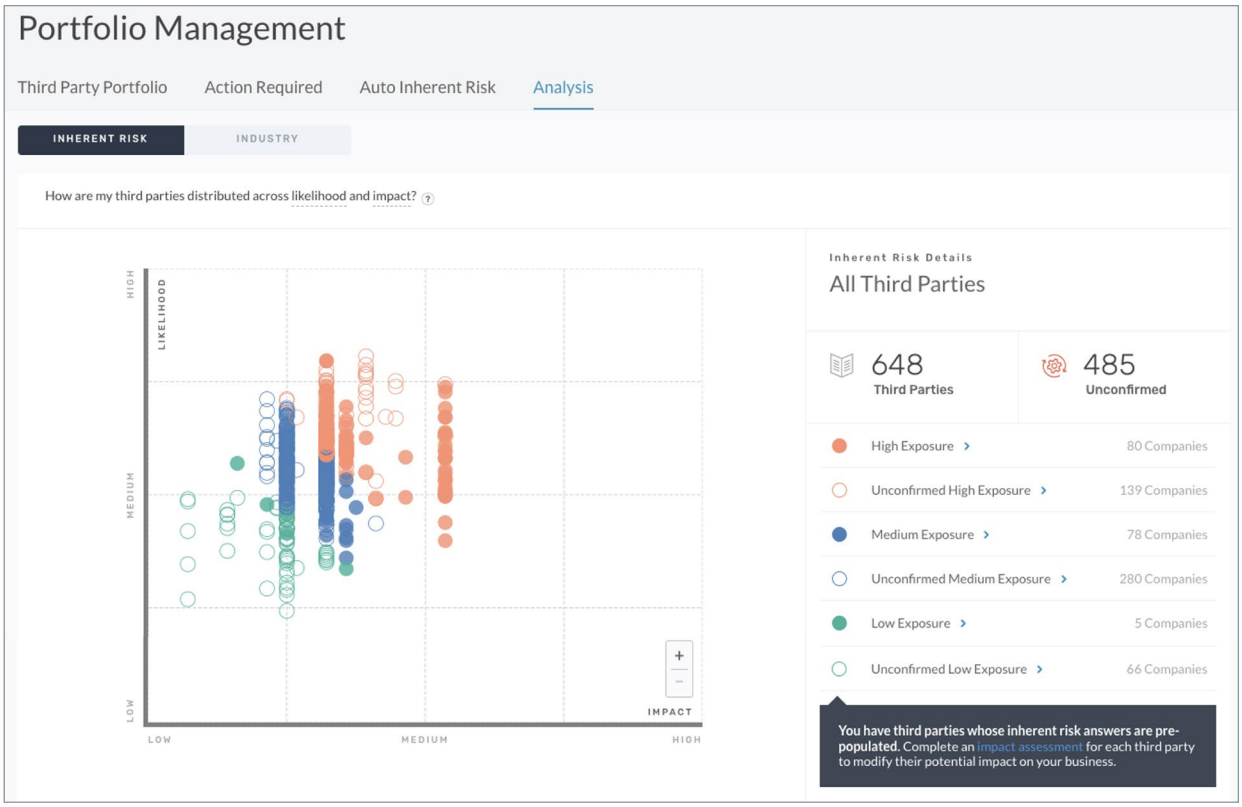

Figure 6. Risk-Analysis Breakdown for Third Parties

In addition, CyberGRX does a great job at categorizing industries represented in our third-party portfolio, as shown in the second section of the Analysis tab, which we can filter to either Likelihood or Impact (see Figure 7).

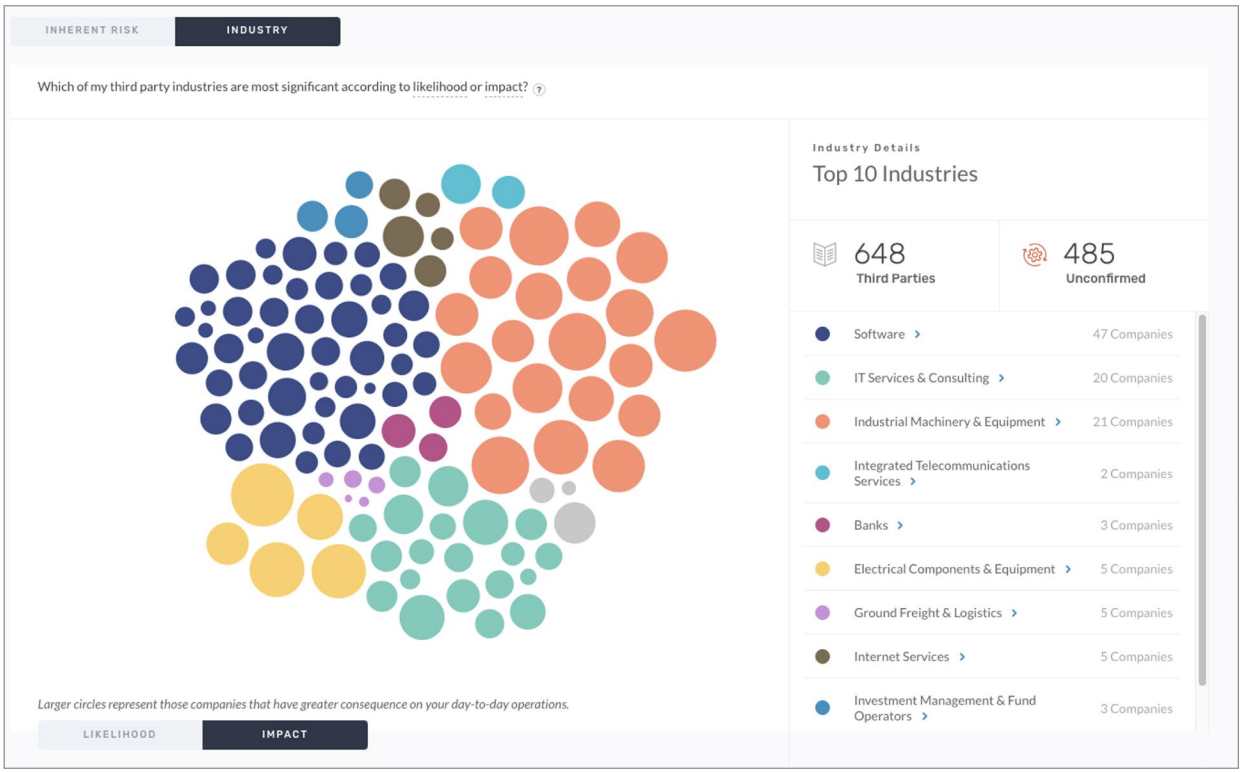

Figure 7. Industry Impact Analysis

The Industry Impact Analysis screen could provide analysts with a quick, easy visual of the most impactful and likely risks within their third-party portfolio, classified by industry or vertical.

Pre-Assessment Third-Party Analysis Using Predictive Risk Intelligence

One of CyberGRX's most powerful features is the Predictive Risk Profile, which is based on its proprietary Predictive Risk Intelligence model. This profile provides immediate insight into a specific third party's risk posture and provides users with better intelligence about a third party's potential risk before the third party completes an assessment by referring to the specific predictive data components. Users can identify or map which CyberGRX controls are most important to their organization and use the Predictive Data components to evaluate the likelihood of a given third party having coverage in those critical control areas. This insight enables more productive and collaborative conversations with third parties by allowing them to discuss more specific concerns, backed by data. It also enables users to make faster business decisions and/or remediation recommendations based on real data before the assessment is completed.

Predictive Risk Intelligence data components available in each Vendor Profile Page (VPP) include:

- Predicted Key Findings
- Predicted Maturity Score
- Predicted Coverage Score
- Predicted Residual Risk

Let's take a look at each of these components.

Predicted Key Findings

These are the summary risk findings that CyberGRX analyzes and presents as a core report for each vendor. Each of these findings has a more detailed breakdown and analysis available, and we can export each report as a full report in an Excel spreadsheet. See Figure 8.

Based on these findings, an organization may want to coordinate with the third party to further analyze and/or review their controls documented in each respective area shown in Figure 8.

Figure 8. Predicted Key Findings for a Third Party

Predicted Maturity Score

The predicted maturity score for an organization combines the documented and stated controls status provided by the third party with intelligence gathered and correlated by CyberGRX into a map of the overall third-party security maturity in the areas of core security practices, operational security, strategic security, privacy, and management. See Figure 9.

This map can fluctuate and change over time, providing a dynamic visualization of the complete security posture of a third-party organization.

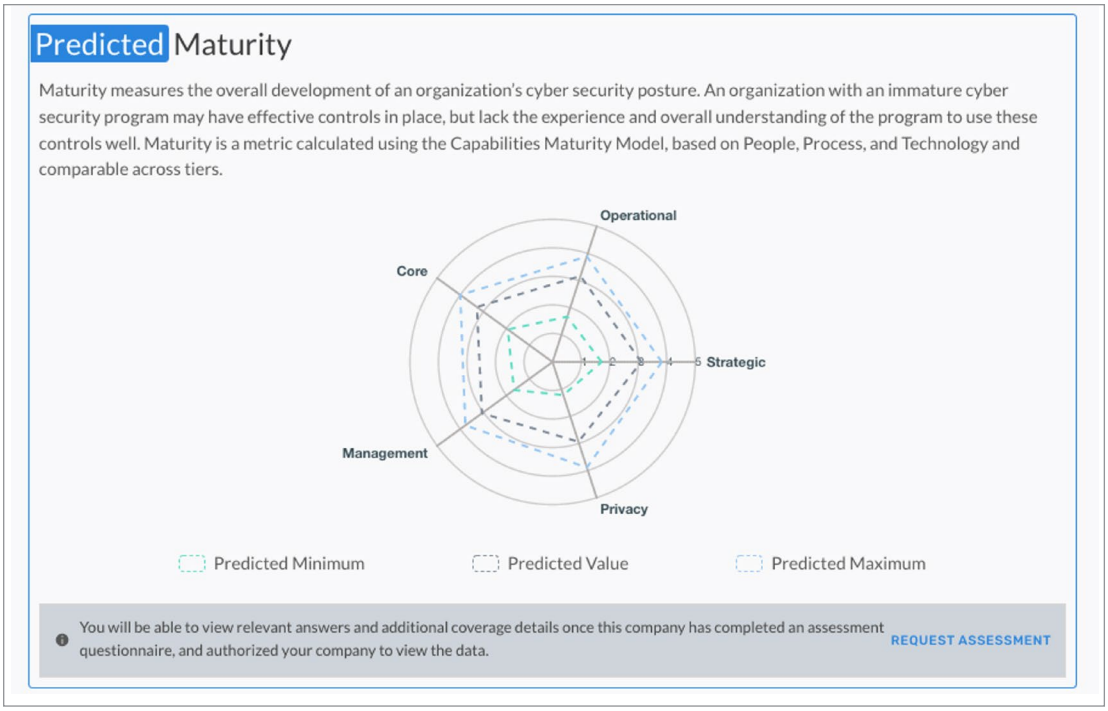

Figure 9. Predicted Maturity Score for a Third Party

Predicted Coverage Score

In conjunction with the predicted maturity score, the predicted coverage score breaks down each of the five categorized areas of security maturity with a ranking score and confidence level, as shown in Figure 10.

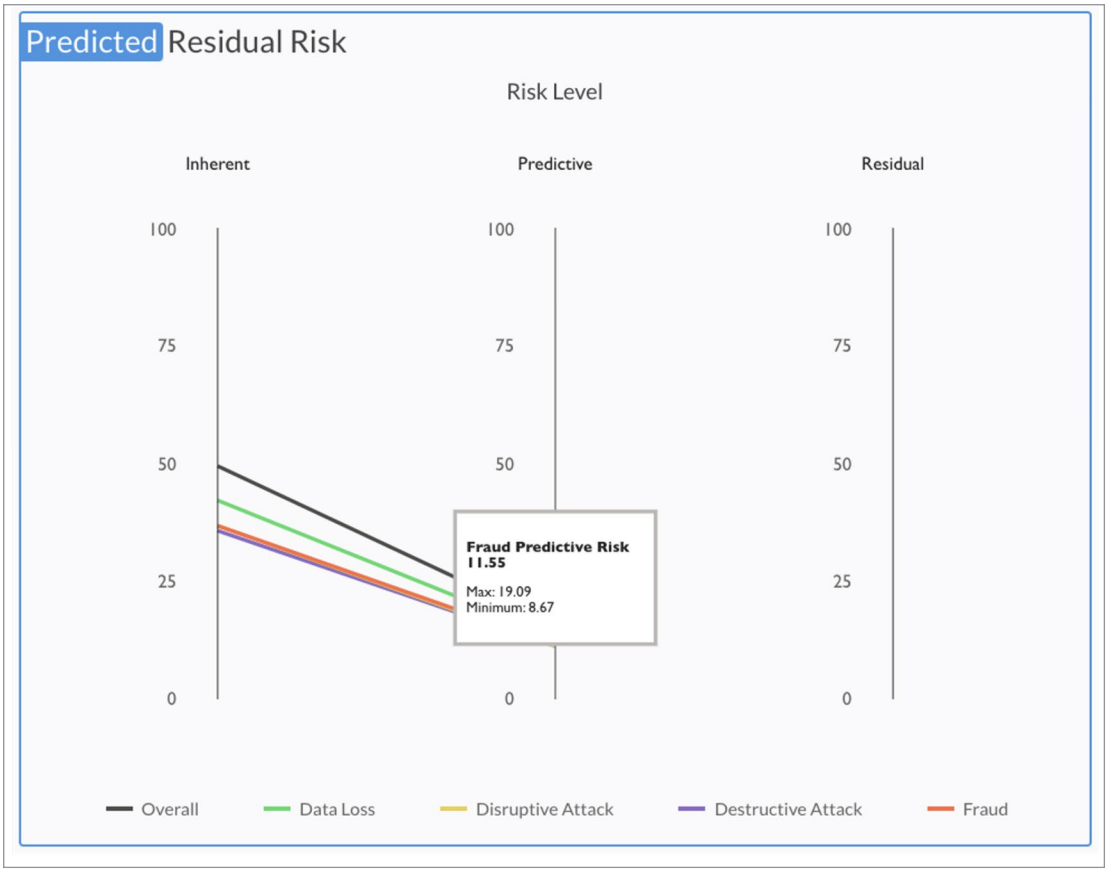

Figure 10. Predicted Coverage for a Third-Party Security Maturity Analysis

Predicted Residual Risk

Lastly, the predicted residual risk of an organization can help to demonstrate where a third party likely has some longer-term risks that may persist over time, based on documented controls and analysis by CyberGRX (see Figure 11).

In addition to the core graphing and reporting of overall risk (both stated and predicted), CyberGRX has partnered with several threat intelligence services to aid in providing reputation and independent industry analyses of third parties and their observed behaviors. The first integration is with Recorded Future, which provides third-party monitoring on social networks, the dark web, and breach monitoring. Figure 12 shows a risk-scoring breakdown of what Recorded Future has noted about this third party, along with the additional details of what contributed to the reported risk score.

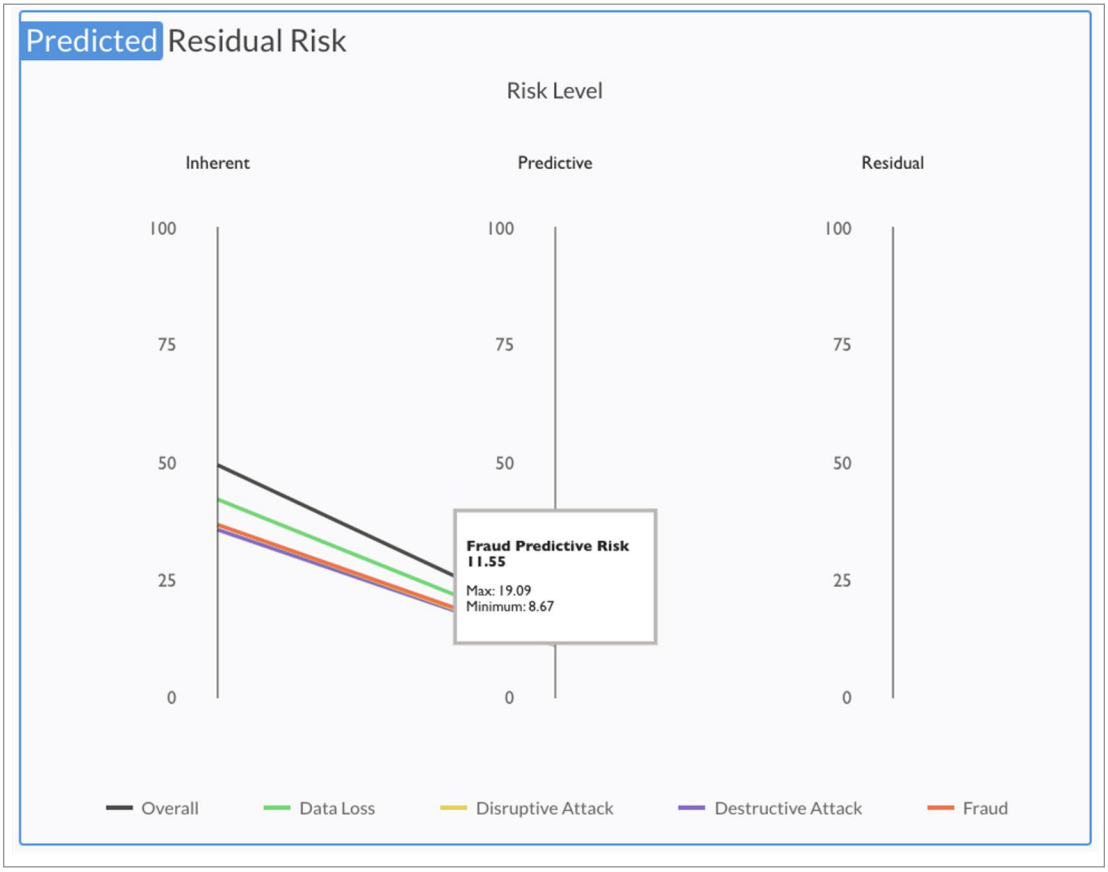

Figure 11. Predicted Third-Party Residual Risk

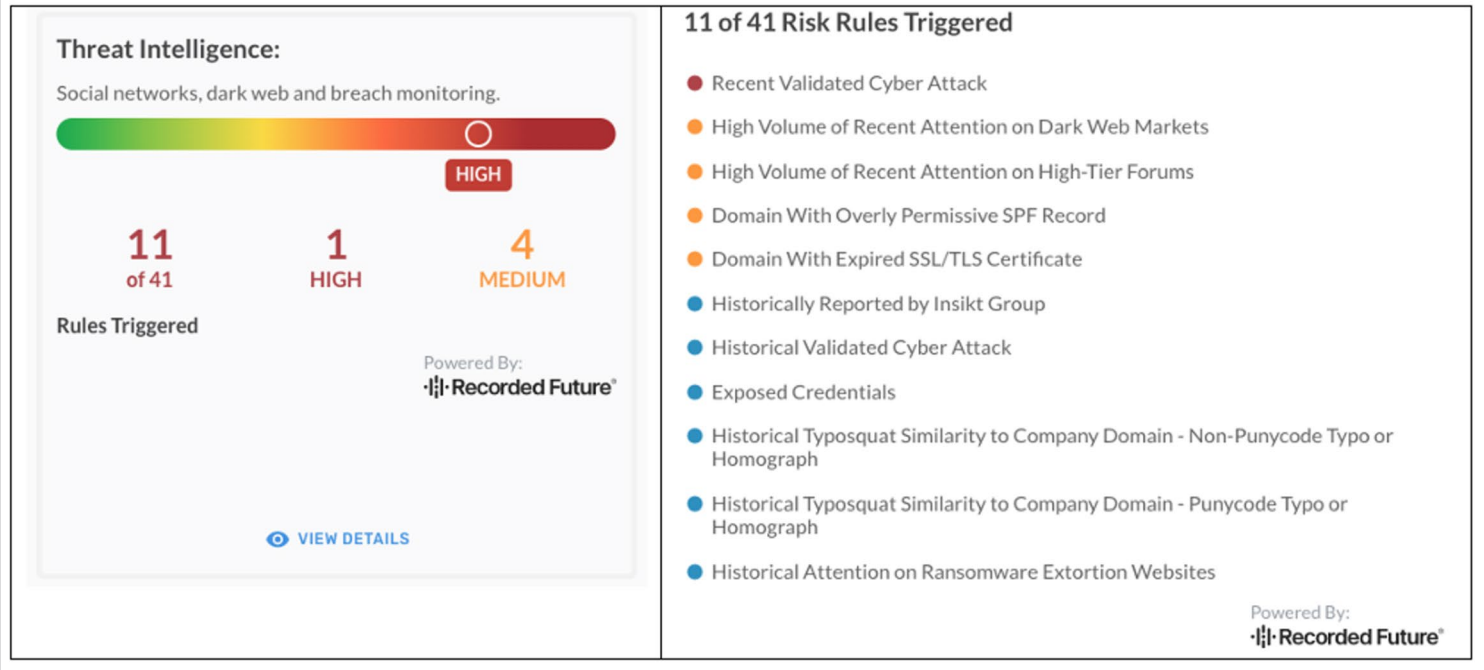

Figure 12. Recorded Future Threat Intelligence on Third Parties

CyberGRX performs continuous risk monitoring of all third parties in your portfolio and integrates the Recorded Future threat intelligence feature to determine whether any notable changes or events have occurred that likely warrant investigation or analysis. We configured the platform to send us a weekly summary (timing of this notification content adjustable as desired). CyberGRX then sent an email showing which potential events of interest had occurred, as well as the companies in the portfolio that had triggered some of the CyberGRX risk-analysis rules. See Figure 13 for an example.

The second threat intelligence provider that CyberGRX partners with is Risk Recon, which breaks the threat intelligence down into more finite categories of risk, including breach events, patching, email security, web application security, and more (see Figure 14).

These additional industry insights can help organizations ascertain what others are observing about a given third party, which helps elevate risk review and analysis beyond the stated and reported controls attestation provided by the third parties themselves.

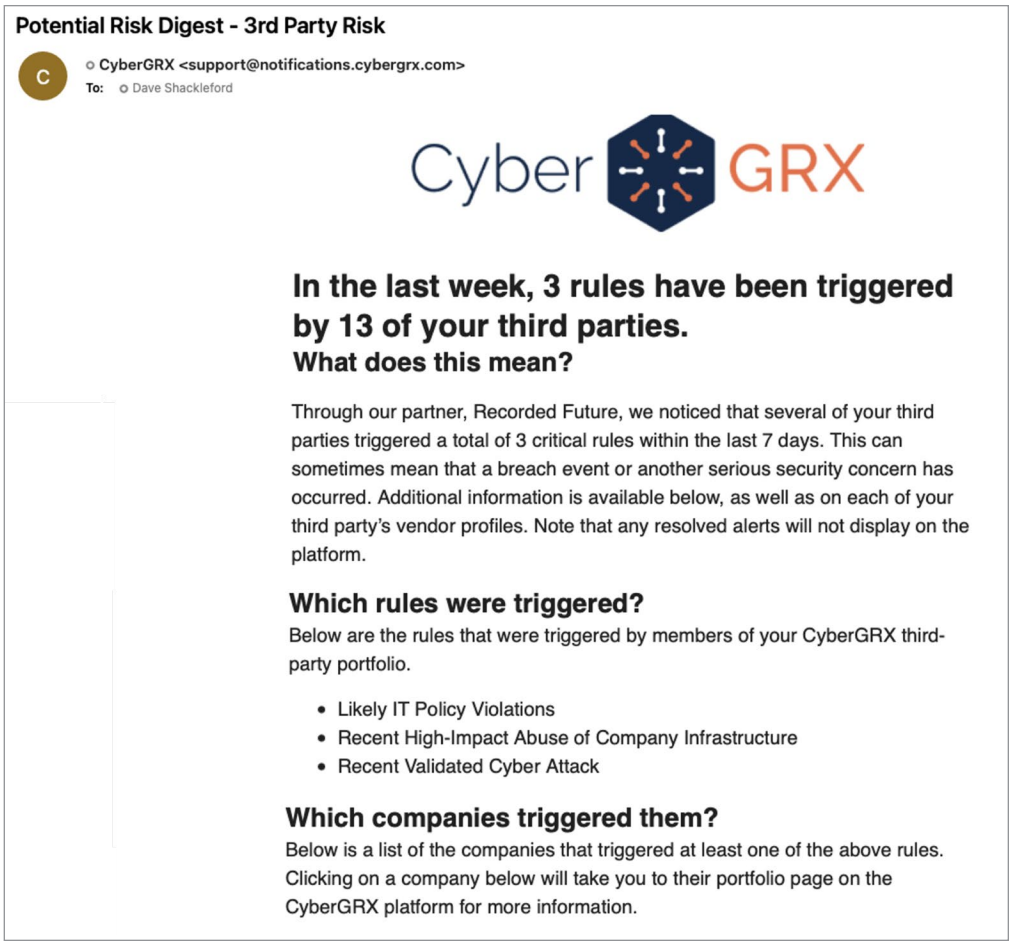

Figure 13. CyberGRX Continuous Risk Monitoring and Alerting

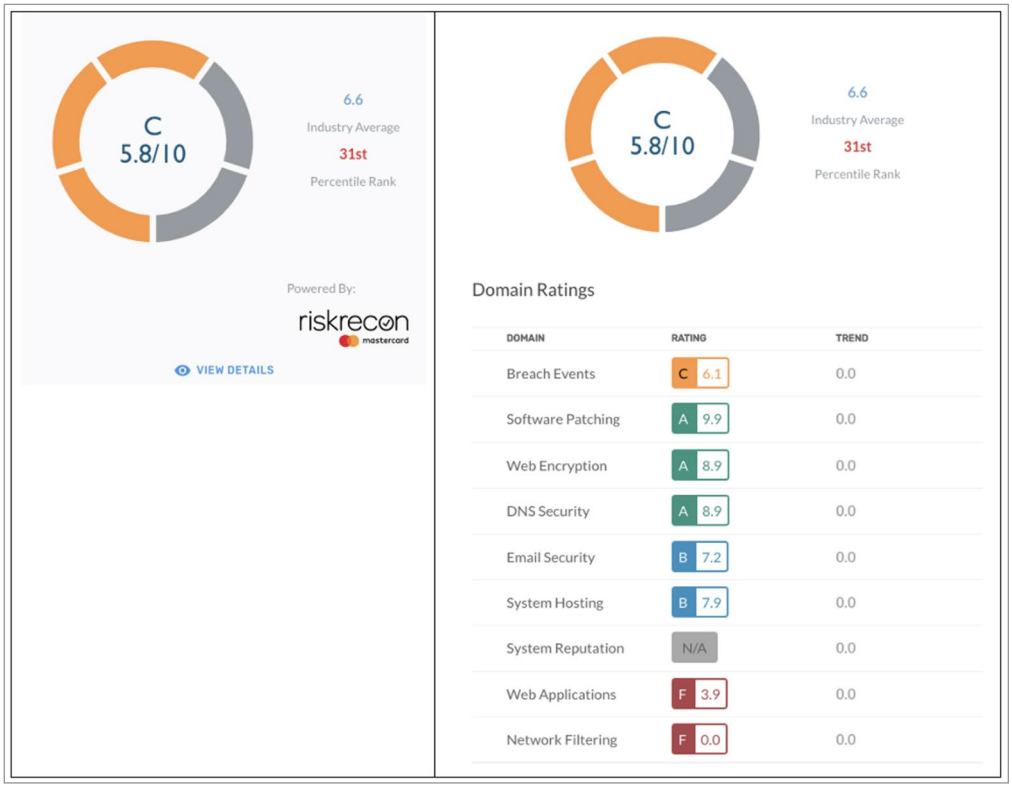

Figure 14. RiskRecon Threat Intelligence Scoring and Reporting

Third-Party Analysis Using Self-Attested Assessment Data

When a third party completes the CyberGRX Assessment and authorizes a requesting customer on the Exchange to have access to their assessment data, that data then becomes available in the customer's account, and various portfolio-level and individual vendor-level platform features enable analysis of it. We easily searched for this information in the main portfolio pane by filtering on Delivered under the Order Status (see Figure 15).

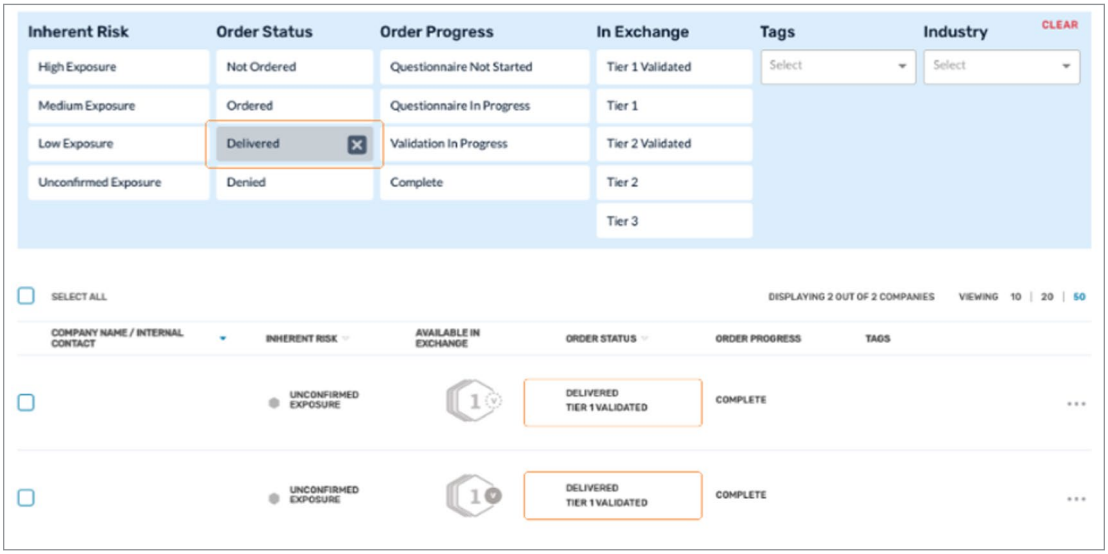

Figure 15. Third Parties with Completed Self-Assessments

This standardized dataset enabled by the CyberGRX assessment also enables customers to map the assessment answers to any other industry standard controls framework, custom framework, or event-specific threat profile. This function provides a crosswalk to existing programs using another framework, allows for immediate insights in the wake of a security event, and enables users to start analyzing data through the lens of their organization's specific critical controls that regulations, industry compliance standards, or internal standards may require. See Figure 16 for insight into the mapping process.

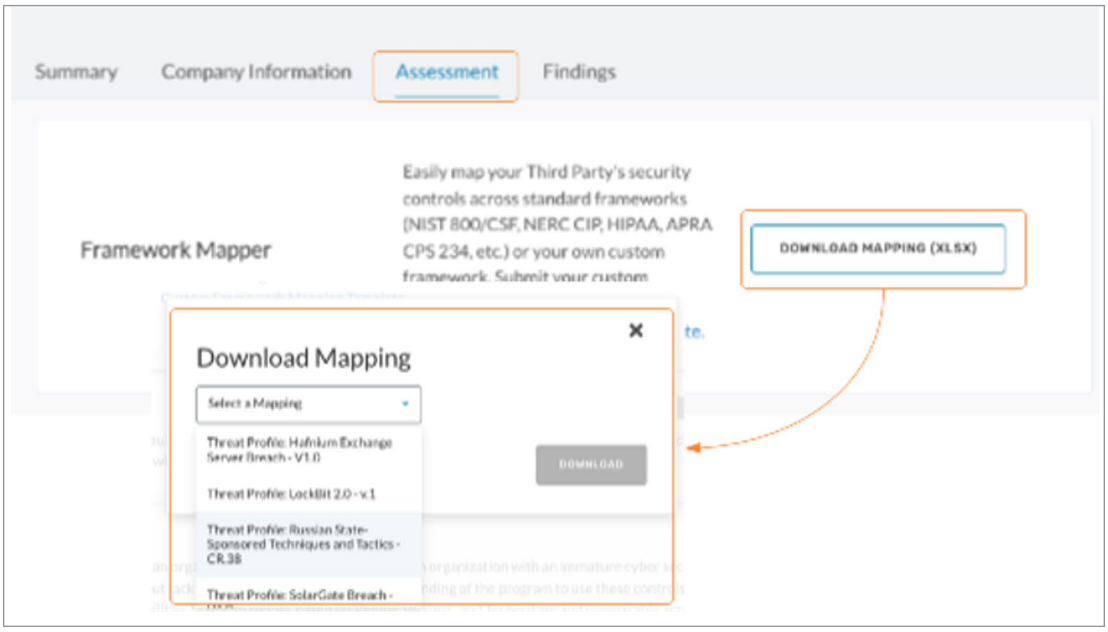

Figure 16. Exporting a Controls Mapping Report

For many risk and compliance teams, this controls mapping will prove invaluable and save an enormous amount of time tracking the state of controls for third parties. It proves especially valuable for analyzing the controls for a third party in light of known threat actor behaviors and campaigns.

CyberGRX has mapped its assessment controls with the MITRE ATT&CK® Framework, allowing any insights resulting from the assessment to be better communicated and understood thanks to the alignment provided by this widely adopted industry standard. Additionally, this framework enables users to drill into the use cases, tactics, and techniques associated with any identified gaps in a third party's coverage so that they can better understand how these gaps translate into exploitable vulnerabilities. The risk scores reported by CyberGRX are also contextually adjusted based on the relationship with the third party. The nature of this relationship can be edited by modifying the Business Exposure Questions, which would update the list of Findings in real time. See Figure 17 for an example of MITRE mapping.

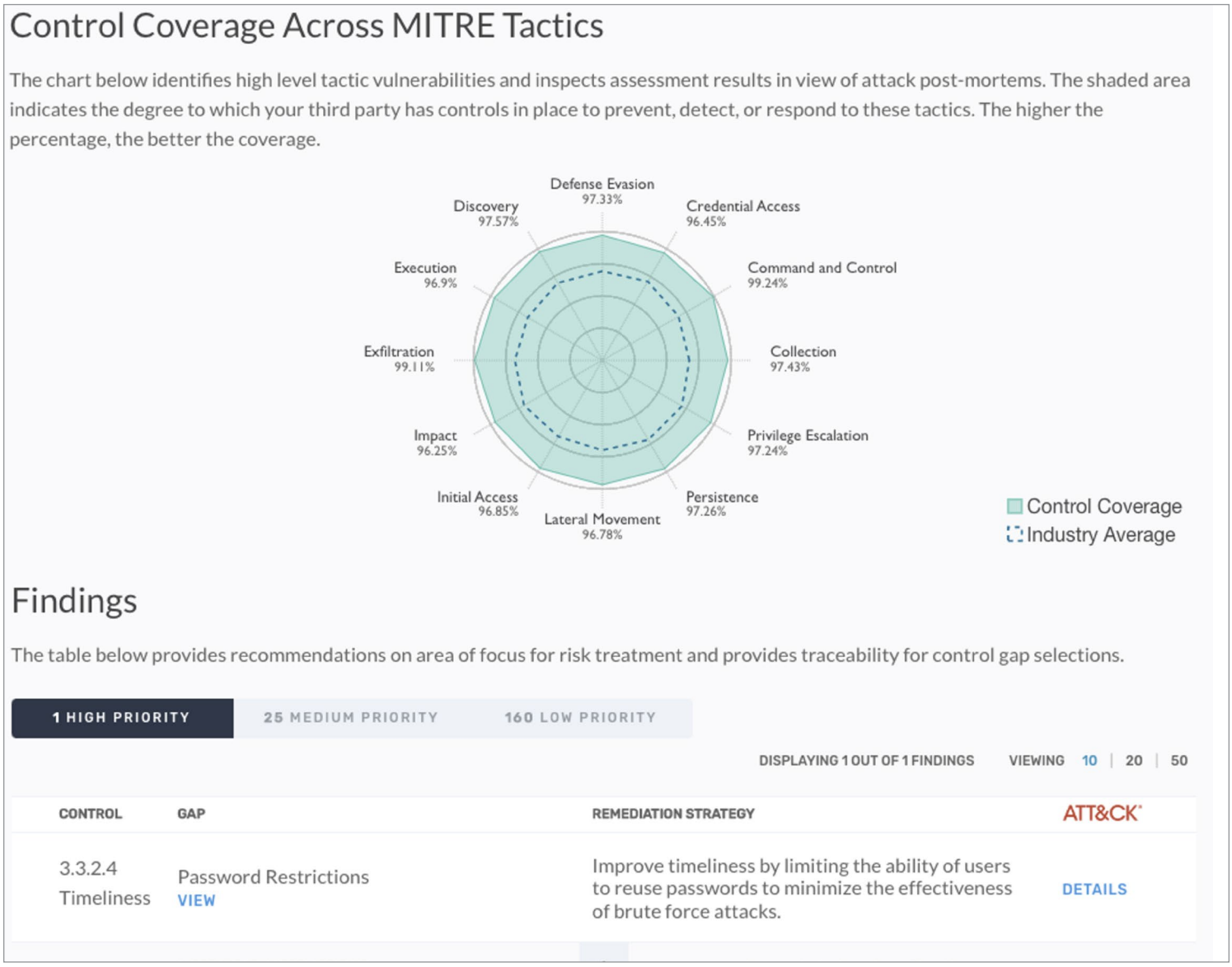

Figure 17. MITRE ATT&CK® Mappings for a Third Party

Last but not least, CyberGRX can provide automatic/scheduled validation or remote validation of any completed assessment. If customers want to review the evidence used to confirm the implementation of the critical controls, CyberGRX has enabled the sharing of raw documents used during the remote validation workflow. Requests to view these documents must be authorized by the third party, and access is limited to a period of time to ensure the security of sensitive information. Figure 18 shows an example of validated information from CyberGRX.

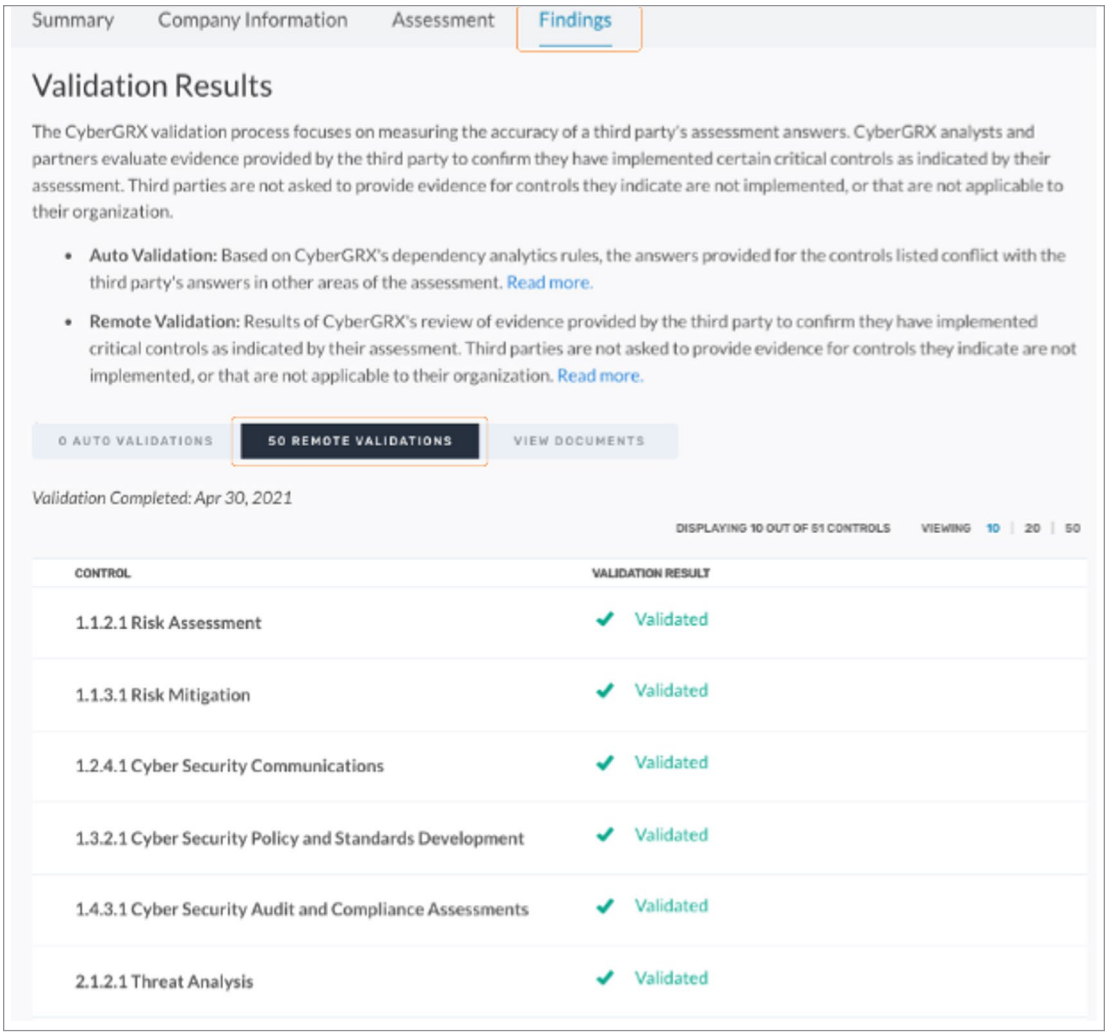

Figure 18. CyberGRX Controls Validation for a Third Party

Altogether, CyberGRX offers a comprehensive set of concrete and predicted risk-analysis reports and tools, augmented with continuous risk monitoring and alerting from industry partners Recorded Future and RiskRecon. Organizations can view their own company profile page to manage users on the account, adjust settings, and to gain visibility into their own Predictive Risk Profile so that they may understand how they are being presented to others viewing their company on the Exchange. Because our test account was a mock company (not a real one with legitimate business interests), we had minimal data presented here, but some basic risk scoring was available.

Enhanced Collaboration

The CyberGRX platform is intended to be a two-way sharing system: Customers may build their own company profiles and choose to share controls information with requesting parties, just as they would for their own third-party organizations.

Similarly, organizations can selectively choose to share their assessment information with other participants in the CyberGRX Exchange, as shown in Figure 19.

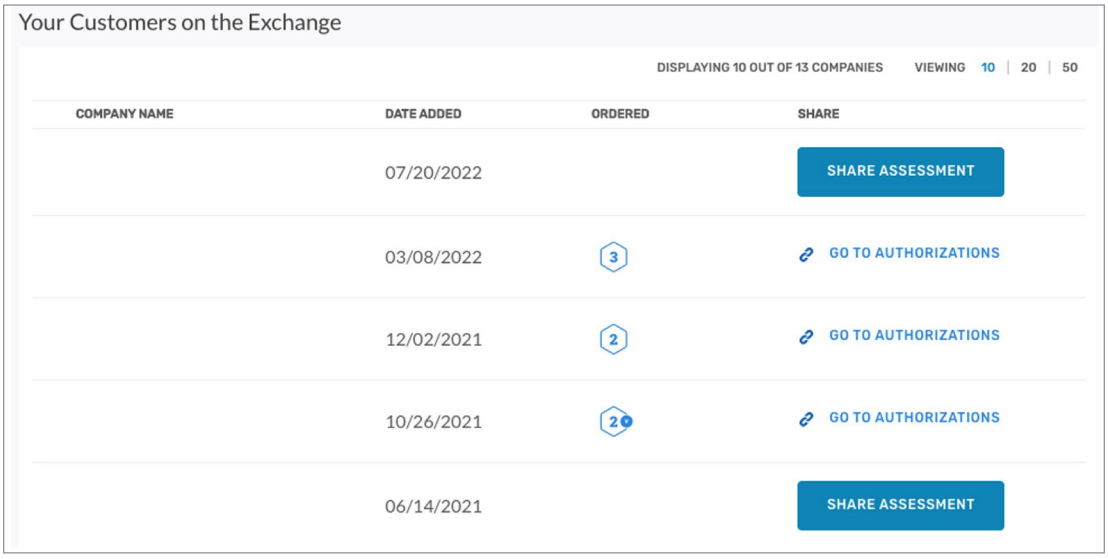

Figure 19. Sharing Organization Portfolios with Others

All organizations are encouraged to complete the CyberGRX Assessment to learn more about their own risk profiles and to save time and resources typically spent on repeatedly completing security control questionnaires. After completing the assessment, organizations can proactively share it with existing or prospective customers. Receiving customers do not need to be Exchange members to receive shared reports. This feature aims to promote assessment completion, data freshness, and Exchange interconnectivity, and we found this to be a novel and unique approach to facilitating coordination and collaboration among third parties (see Figure 20).

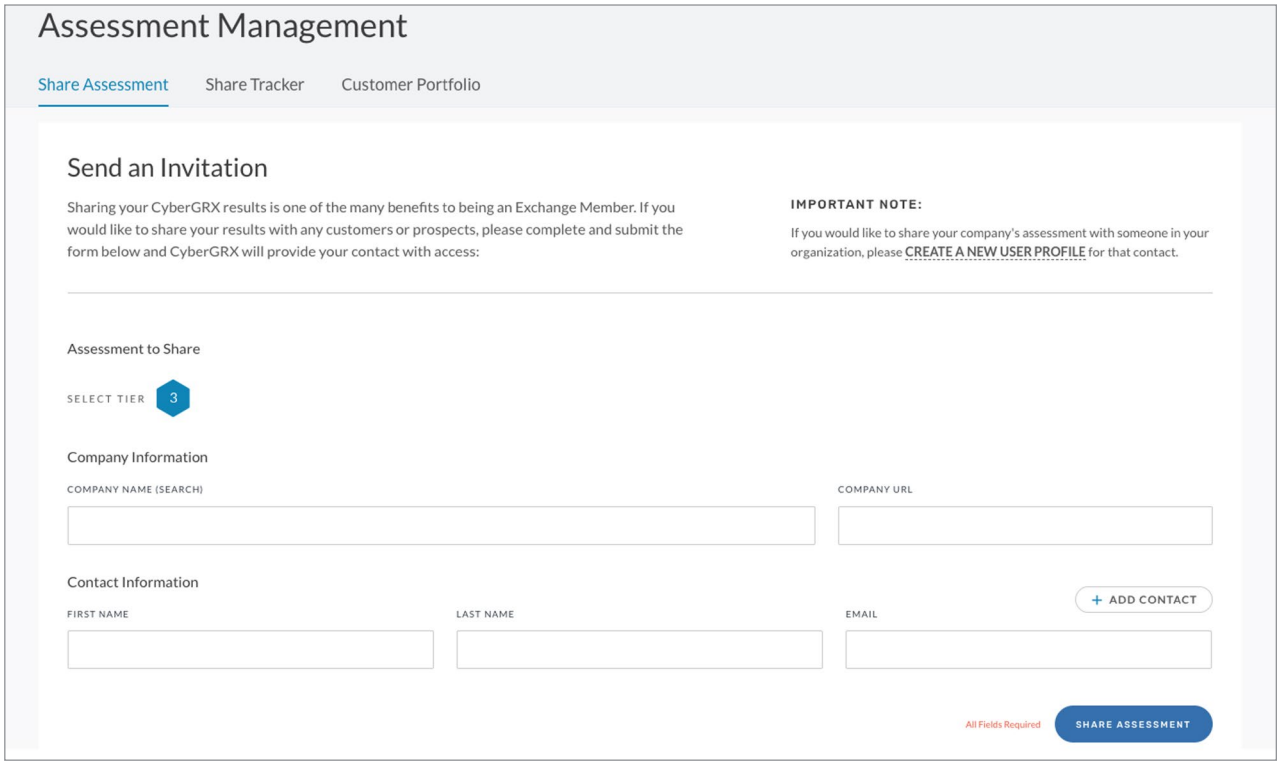

Figure 20. Upstream Sharing of Security Assessments

The platform also provides a public API as well as Excel downloads of critical data displayed in user accounts. These functions aim to improve communication and collaboration with internal stakeholders. These data-delivery methods allow for more contextualized data manipulation and analyses beyond what CyberGRX provides and allow integration with other tools to support users' end-to-end workflows. Download examples include:

- Portfolio Management Table
- Customer Action Required Table
- Individual Vendor Assessment Results
- First Party Assessment Results
- Framework Mapper Outputs

We did not explore all of these various download options because it was beyond the scope of this review, but we did note that many data export types were available.

Conclusion

Overall, we found the CyberGRX platform to be highly intuitive, easy to use, and capable of providing in-depth risk-analysis information for third parties while facilitating information exchange all the way around. The actual CyberGRX assessment questionnaire was easy to navigate, with simple multiple-choice questions in a web interface. The questionnaire results are easily shared and analyzed by any and all parties on the Exchange as well as parties outside the CyberGRX ecosystem.

With the significant increase in third-party risks and breaches we've seen in recent years, it's critical to make this type of third-party analysis and information sharing easier and more comprehensive. We believe that CyberGRX does exactly this. Incorporating external threat intelligence to add additional context and insight only makes the available datasets that much more comprehensive. Any organization could make use of this platform quickly and efficiently, and the reporting and analysis would prove useful to a broad variety of stakeholders, as well.

Sponsor

SANS would like to thank this paper's sponsor: