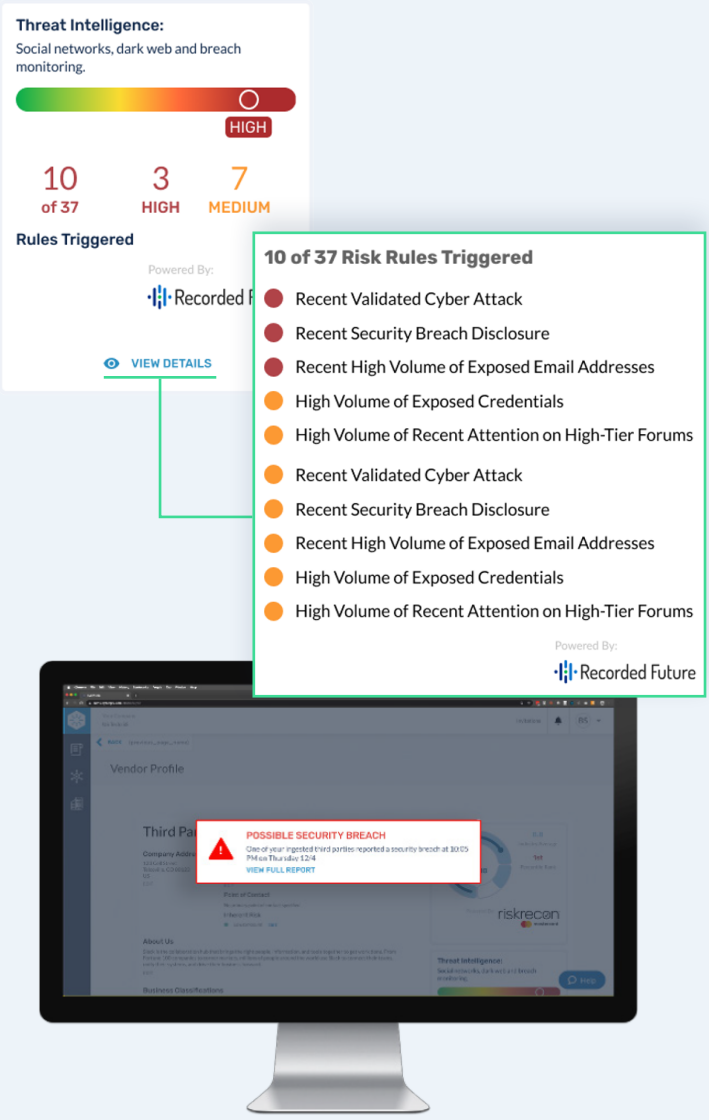
Risk Monitoring and Alerting Rules Overview

CyberGRX Risk Monitoring and Alerting

Data breaches are inevitable and having rapid notification of a potential breah or alert is critical to effectively manage your third-party ecosystem. While organizations focus on performing risk assessments which require a high degree of manual effort and are focused on a single point in time, having knowledge of the changing attack patterns on the dark web as well as visibility into exposed assets and credentials can help to quickly predict the likelihood of a breach.

Most companies end up finding out about a potential risk exposure of one of their third parties in a news headline. With our new Risk Monitoring & Alerting capabilities, you will have visibility and receive alerts to third-party risk alerts within your portfolio in near real-time. In addition, you'll have the vital information and context needed to assess the possible impact on your business and collaborate with the affected third party to assess and manage the risk.



Recorded Future Threat Intelligence data and breach notification in the CyberGRX platform.

How it Works

Recorded Future uses patented machine learning and natural language processing to automatically collect, analyze and categorize information into 40 risk rules. The applicable rules and corresponding alert methods that will be triggered within the CyberGRX platform to notify on potential risk exposures on third parties include:

Rule #	Risk Rule	Risk Category	Alert Method
1	Recent Security Breach Disclosure	Breach or Incident Reporting	In-Platform
2	Recent Validated Cyber Attack	Breach or Incident Reporting	In-Platform
3	High Volume of Exposed Credentials	Leaked Credentials	In-Platform
4	Historical Security Breach Disclosure	Breach or Incident Reporting	In-Platform & Email
5	Historical Validated Cyber Attack	Breach or Incident Reporting	In-Platform & Email
6	Recent Attention on Ransomware Extortion Websites	Breach or Incident Reporting	In-Platform
7	Recent Single-Document Email Address Exposure	Leaked Credentials	In-Platform

Third-Party Risk Rules

Third-party risk rules can trigger at three bands: High, Moderate, and Informational. These bands represent a level of externally observable threat or risk. Each triggered rule has a criticality, a rule name, an evidence string, and a mitigation string.

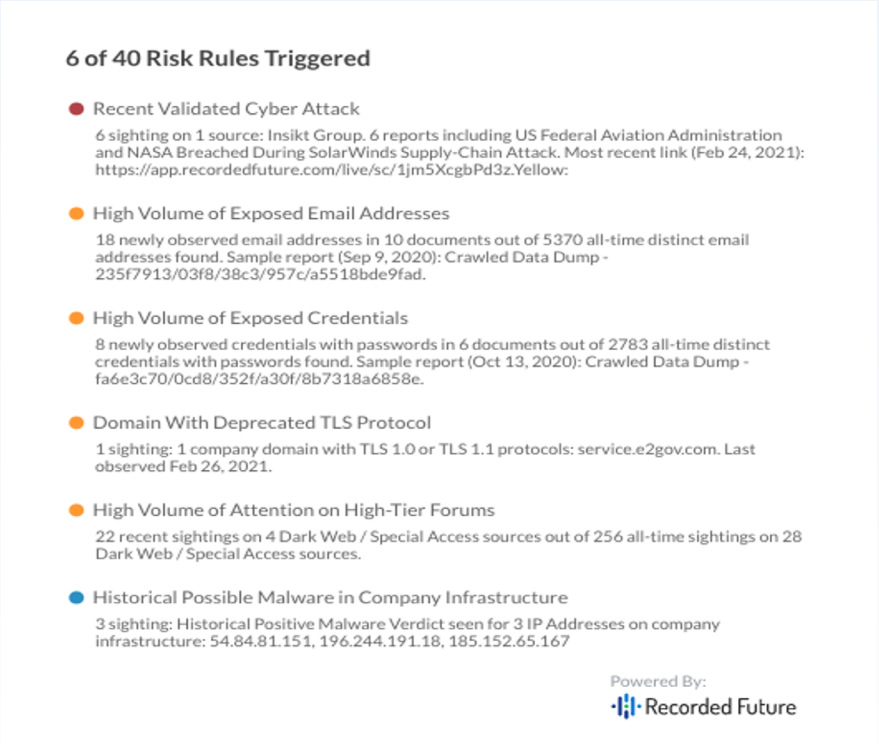
High (65-99): Observed high indicators of high severity threats and elevated cyber risk

Moderate (25-64): Observed over time indicators of moderate threats and cyber risk

Informational (5-24): Important for general situation awareness

Members will see a Risk Summary for each third-party profile with a summary of impacted rules for probing and investigation. Third parties can also view a detailed list of the risk rules triggered in order to help drive proactive mitigation and issue tracking.

CyberGRX is at the forefront to meet the increasing criticality and complexity of the third-party cyber risk landscape, moving past traditional approaches like static assessments or stand-alone security ratings. By building out comprehensive and real-time risk intelligence profiles for third parties, organizations can be confident to make rapid, risk-reducing decisions.



The third party view of the Recorded Future widget

For more information on CyberGRX third-party risk intelligence and the Recorded Future integration, visit our website at:

www.cybergrx.com/platform/predictive-risk-profiles

Cyber GRX