

Risk Monitoring and Alerting Rules Overview

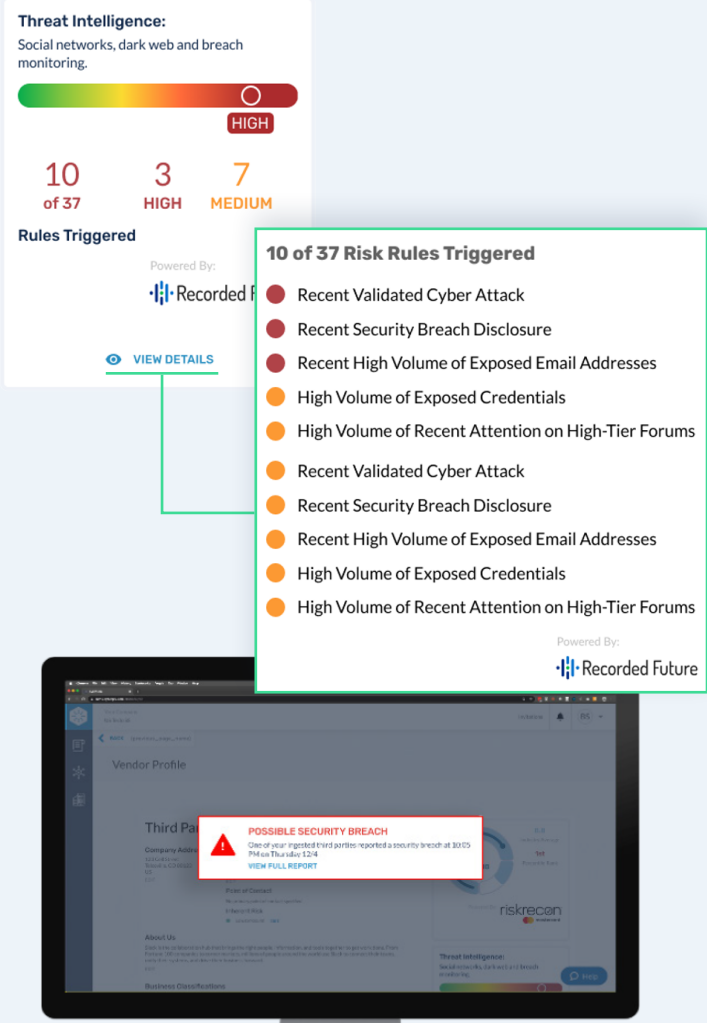
CyberGRX Risk Monitoring and Alerting

Data breaches are inevitable and having rapid notification of a potential breach 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.

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:



Threat Intelligence:
Social networks, dark web and breach monitoring.

10 of 37
3 HIGH
7 MEDIUM

Rules Triggered

Powered By: Recorded Future

[VIEW DETAILS](#)

10 of 37 Risk Rules Triggered

- Recent Validated Cyber Attack
- Recent Security Breach Disclosure
- Recent High Volume of Exposed Email Addresses
- High Volume of Exposed Credentials
- High Volume of Recent Attention on High-Tier Forums
- Recent Validated Cyber Attack
- Recent Security Breach Disclosure
- Recent High Volume of Exposed Email Addresses
- High Volume of Exposed Credentials
- High Volume of Recent Attention on High-Tier Forums

Powered By: Recorded Future

POSSIBLE SECURITY BREACH
One of our registered third parties reported a security breach at 30:25 PM on Thursday, 12/4.

[VIEW FULL REPORT](#)

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

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.

6 of 40 Risk Rules Triggered

- **Recent Validated Cyber Attack**
6 sighting on 1 source: Insikt Group. 6 reports including US Federal Aviation Administration and NASA Breached During SolarWinds Supply-Chain Attack. Most recent link (Feb 24, 2021): <https://app.recordedfuture.com/live/sc/1jm5XcgbPd3z.Yellow>
- **High Volume of Exposed Email Addresses**
18 newly observed email addresses in 10 documents out of 5370 all-time distinct email addresses found. Sample report (Sep 9, 2020): Crawled Data Dump - 235f7913/03f8/38c3/957c/a5518bde9fad.
- **High Volume of Exposed Credentials**
8 newly observed credentials with passwords in 6 documents out of 2783 all-time distinct credentials with passwords found. Sample report (Oct 13, 2020): Crawled Data Dump - fa6e3c70/0cd8/352f/a30f/8b7318a6858e.
- **Domain With Deprecated TLS Protocol**
1 sighting: 1 company domain with TLS 1.0 or TLS 1.1 protocols: service.e2gov.com. Last observed Feb 26, 2021.
- **High Volume of Attention on High-Tier Forums**
22 recent sightings on 4 Dark Web / Special Access sources out of 256 all-time sightings on 28 Dark Web / Special Access sources.
- **Historical Possible Malware in Company Infrastructure**
3 sighting: Historical Positive Malware Verdict seen for 3 IP Addresses on company infrastructure: 54.84.81.151, 196.244.191.18, 185.152.65.167

Powered By:
 Recorded Future

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