# Recorded Future® Third-Party Threat Intelligence Insights

CyberGRX incorporates industry-leading third-party cyber risk management with threat intelligence

CyberGRX is on a mission to map the cybersecurity profile of every organization around the globe. What began as the world's first global risk exchange populated by proprietary risk assessment data has evolved into a sophisticated, third-party risk insight platform. The latest innovation within the CyberGRX platform is the integration of Recorded Future's third-party intelligence, providing a real-time view of third-party cyber risks.
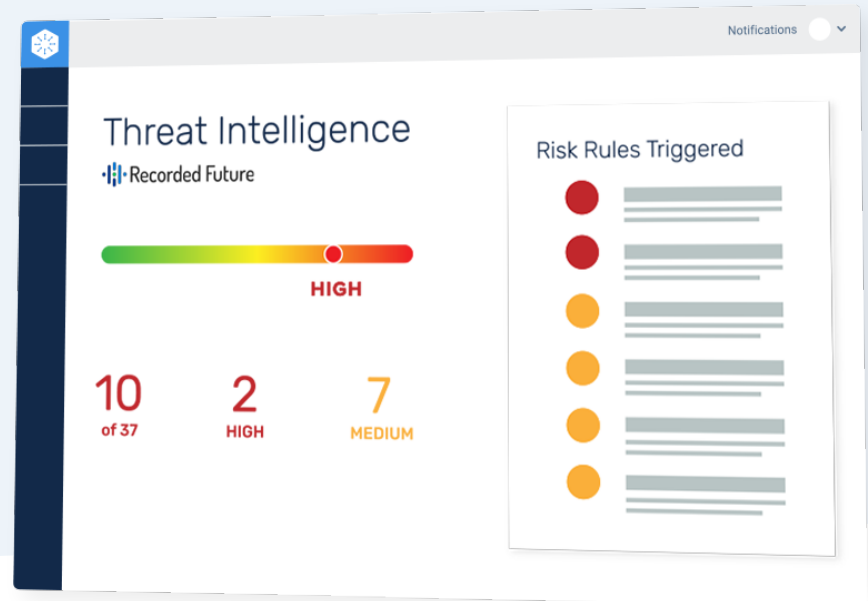
Having a single pane view of proven and contextualized datasets helps alleviate resource constraints, allowing customers to focus more on third parties that pose a higher risk to the organization. Real-time visibility into third-party data being transacted in the Deep and Dark Webs – such as data leakage, domain abuse, ransomware extortion, C2C comms, and breach Intelligence – can not only help with third-party risk management but the additional threat intelligence can improve the quality and defensibility of other cyber security programs.

Recorded Future third party intelligence data is available to both enterprise users and third parties at no additional charge to provide a collaborative environment in which to address risk and mitigation strategies.

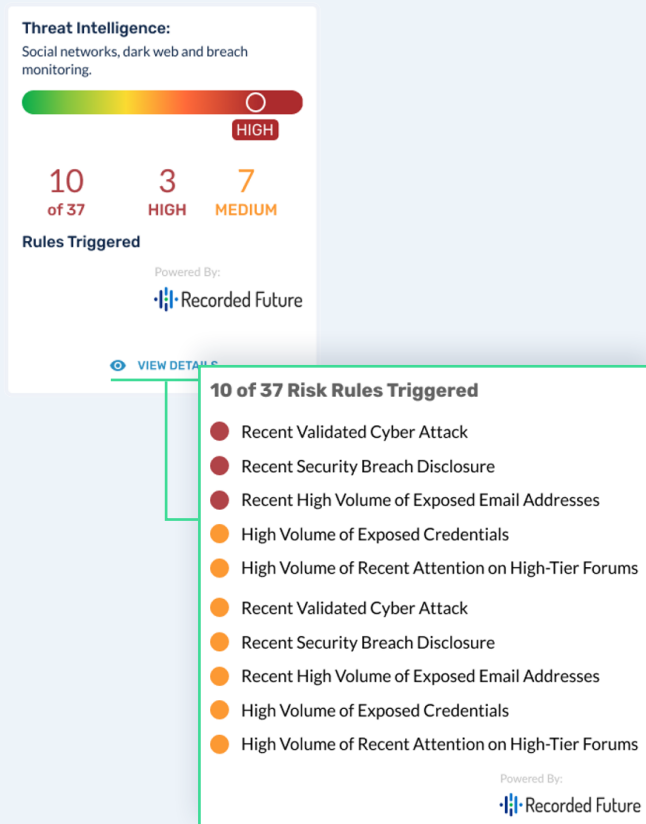## Benefits of Recorded Future Intelligence Integration

- Know when a third party has been exposed – Access risk monitoring intelligence within the CyberGRX platform

- Increase your attack surface visibility – Better predict the likelihood of a breach and allow for predictive mitigation strategies with knowledge of your entire third-party ecosystem and your levels of exposure within it

- Monitor of vendor risk profiles continuously – Gain access to unique finished threat intelligence through additional datasets from Recorded Future including advanced threat hunting, detection and validation, and deep/ dark & social web investigation.

The Enterprise view of the Recorded Future® widget

CyberGRX Risk Monitoring

Data breaches are inevitable and getting instant awareness of a breach is critical to managing the supply chain ecosystem in today's landscape. 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 to exposed assets and credentials can predict the likelihood of a risk exposure.

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

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

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

Enterprise users will see a Risk Summary widget for each third-party profile with a summary of impacted rules for probing and investigation. Third parties will receive the Risk Summary widget with a detailed view 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 threat 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 the CyberGRX integration of Recorded Future third party intelligence and the rest of the CyberGRX Global Third Party Cyber Security Exchange Platform, please visit our website at:

www.cybergrx.com/platform/identify-prioritize

Cyber GRX