RAPID7

DATA SHEET

Threat Command

Third-Party Risk Assessment

To reduce risk, security teams must have continuous visibility into clear, deep, and dark web threats facing third-party vendors. Supply chain threats can result in exposure to your organization, as digital assets may be compromised via vendor data leaks.

Solution Overview

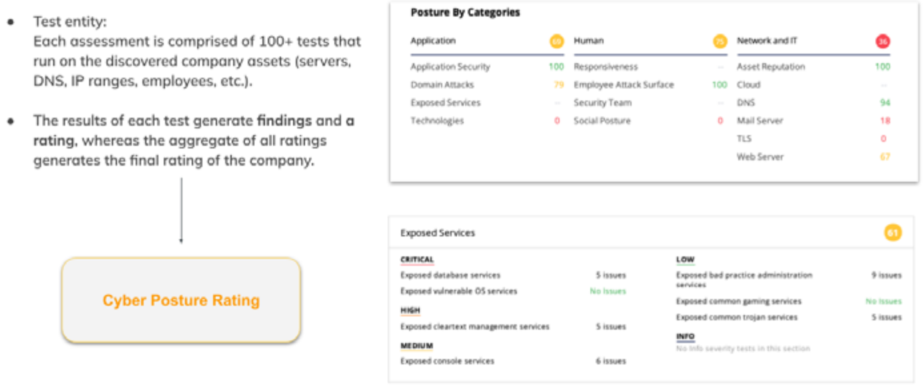
Rapid7's Third-Party Risk Assessment solution leverages best-in-class threat intelligence capabilities to give security professionals contextual understanding of vendor threats. It is designed to augment existing security solutions with additional data for increased visibility and due diligence.

Third-Party Risk Assessment is a fully automated, non-intrusive vendor risk assessment that rates organizations by mapping risks against their digital footprints. The tool evaluates your third-party attack surface through the analysis of externally available data. Every assessment performs hundreds of tests, such as collecting information on exposed assets and checking for evidence of security best practices, to provide a comprehensive view of a vendor's digital perimeter. Tests are performed across:

- **Network & IT:** Web, email, DNS servers, TLS protocols, asset reputation, cloud solutions, and other exposed services
- **Application:** Web applications, CMS, domain attacks, etc.
- **Human:** Employee attack surface, social posture, presence of a dedicated security team, etc.

Risk Assessment Reports

Risk Assessment Reports (available in 12 to 72 hours upon request), provided by our security risk management software partner, evaluate the vendor's external attack surface. The assessment delivers a bottom-line **Cyber Risk Rating** reflecting all findings related to the vendor, including a **Cyber Posture Rating** (based on external attack surface assessment).



- Test entity:
  Each assessment is comprised of 100+ tests that run on the discovered company assets (servers, DNS, IP ranges, employees, etc.).
- The results of each test generate findings and a rating, whereas the aggregate of all ratings generates the final rating of the company.

Posture By Categories

Application	69	Human	75	Network and IT	36
Application Security	100	Responsiveness	--	Asset Reputation	100
Domain Attacks	79	Employee Attack Surface	100	Cloud	--
Exposed Services	--	Security Team	--	DNS	94
Technologies	0	Social Posture	0	Mail Server	18
				TLS	0
				Web Server	67

Exposed Services 61

CRITICAL		LOW	
Exposed database services	5 issues	Exposed bad practice administration services	9 issues
Exposed vulnerable OS services	No Issues	Exposed common gaming services	No Issues
HIGH		Exposed common trojan services	5 issues
Exposed cleartext management services	5 issues	INFO	
MEDIUM		No Info severity tests in this section	
Exposed console services	6 issues		

TESTS AND RATING METHODOLOGY

The Risk Assessment Report

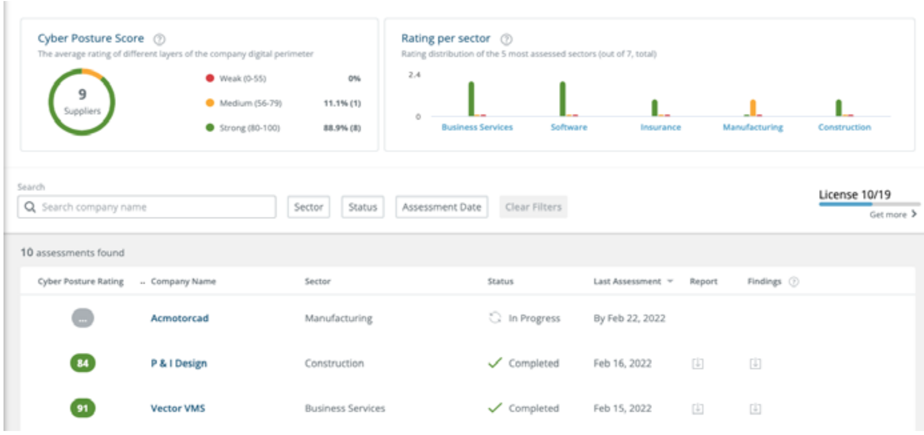
- Overview and Third-Party Relationships
- 360-degree Cyber Posture Rating
- Posture by Test Category
- Industry Range
- Dark Web Mentions
- Test Categories Drilldown

Solution Features

- Organization ratings based on mapping risks against digital footprints
- Evaluation of third-party attack surface
- Hundreds of tests including information collected on exposed assets, evidence of security best practices, etc.

Solution Benefits

- Rapid identification of third parties with high-risk external threat profiles
- Faster, smarter decisions that enable better security across third-party ecosystem



10 assessments found

Cyber Posture Rating	Company Name	Sector	Status	Last Assessment	Report	Findings
...	Acmotorcad	Manufacturing	In Progress	By Feb 22, 2022		
84	P & I Design	Construction	✓ Completed	Feb 16, 2022	⤓	⤓
91	Vector VMS	Business Services	✓ Completed	Feb 15, 2022	⤓	⤓

RISK ASSESSMENT DASHBOARD

Methodology

To generate the Risk Assessment Report, data is collected from asset reputation feeds and light probes, and tests are performed on discovered assets. Data from publicly available and proprietary resources contributes to the organization's cyber resilience ratings across each layer of the vendor's digital perimeter: **Network & IT, Application, and Human.**

The rating for each category is an aggregation of findings derived from all tests performed within the category. Weighting of the tests is based on objective parameters including comparisons to trusted companies and breached companies, and ratings distribution within an industry. Additionally, the assessment checks vendor compliance with leading regulatory requirements.

Network and IT

- Asset reputation
- DNS
- Exposed services
- Mail server
- TLS
- Web server

Application

- Application security
- Domain Attacks
- Technologies

Human

- Responsiveness
- Employee attack surface
- Security team
- Social posture

PRODUCTS

insightCloudSec | insightIDR | Threat Command
insightVM | insightAppSec | insightConnect

SUPPORT

Customer Portal | Call +1.866.380.8113

To learn more or start a free trial, visit:
https://www.rapid7.com/try/insight/