Q:CYBER

Q:SCAN
Technical Specifications

See & score your external security posture the way attackers do

---

Find and Fix External Exposures Faster with Q:SCAN

Q:SCAN enables cybersecurity teams to see their organization's security the way outsiders see it using open source intelligence (OSINT) collection and analysis techniques to search for high-risk signals that are valuable to attackers. It can be used alone or with vulnerability scanning tools you may already be using.

Approach and Methodology

Q:SCAN passively scans your internet domains to identify key risk signals that can indicate your organization may have a poor security posture. It creates an overall risk score for your organization similar to a credit score, where scores range from zero to 850 and higher scores indicate better security posture.

Q:SCAN uses open and proprietary aggregated datasets to enrich the raw data it collects with known breach, reputation, and vulnerability data. This contextualized enrichment is used to create sophisticated analytics for cybersecurity risk exposure. Customers can use Q:SCAN's insights to inform the controls implemented in Q:CYBER, or to determine cyber insurance coverage with RubiQon Risk.

Q:SCAN analyzes the following cyber risk signals to measure your organization's external exposures and to help you mitigate any threats. Signals include the following:

KEY SIGNALS ANALYZED BY Q:SCAN

- Domains and subdomains
- DNS Records
- DMARC
- SPF
- Zone Transfers
- Open Ports
- Exposed Services
- TLS Certificate health
- Malware Indicators and Reputation
- Web Application Headers
- Advanced Analytics datasets (see below)
- Emails associated with known public breach records

Advanced Analytics Datasets

In addition to the risk signals that can be directly observed from your domains and associated infrastructure, Q:SCAN offers advanced analytics that incorporate data from public and proprietary information datasets. These datasets provide additional context that helps your cybersecurity team identify additional exposures.

- ### Historical Breach Dataset
  The Historical Breach Dataset contains curated information on historical breach record searches. Q:SCAN checks whether your domains have been included in prior cyber breaches, and categorizes raw and refined data that you can use for threat assessments.

- ### Reputation Dataset
  The Reputation Dataset assimilates, harmonizes, and indexes open source and paid reputation data feeds to determine whether IP addresses associated with your domains have been associated with known malicious or compromised activity.

- ### Vulnerability & Exploit Dataset
  The Vulnerability & Exploit Dataset is an archive of exploits and vulnerable software[1]. It catalogs vulnerabilities in open source and commercial software to inform network risk scoring, threat intelligence, and risk modeling efforts.

Ready to learn more about *QOMPLX's Q:SCAN solution*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX is the cloud-native leader in risk analytics. We help organizations around the world make intelligent business decisions and better manage risk through our advanced, proprietary risk cloud. We are the leaders at rapidly ingesting, transforming, and contextualizing large, complex, and disparate data sources through our data factory in order to help organizations better quantify, model, and predict risk in areas including cybersecurity, insurance, and finance. For more information, visit qomplx.com and follow us @QOMPLX.

[1] Exploit Database (EDB)