Q:SCAN
Product Solutions Brief

Introduction

Built from the ground up with organizational risk scoring for performance measurement in mind, Q:SCAN is a large scale, highly performant, data-driven cyber exposure measurement platform that is tailored to deliver "ground truth" by taking advantage of the latest open source intelligence (OSINT) collection and analysis techniques. It can be used standalone or to complement vulnerability scanning efforts.

Conceived by our team of leading OSINT and web-scale data extraction experts, backed by our team of experienced data scientists with decades of practical experience in government and private industry, Q:SCAN enables security control experts to map indicators from open-source information to probable deviation from desired maturity levels.

Leveraging the performance offered by the sector-leading cloud infrastructure, Q:SCAN delivers on-demand and scheduled risk measurement reports for organizations in just a few moments. QOMPLX:OS underpinnings also allow for tracking, change and anomaly detection, event-driven alerting, forecasting and even simulation modeling to help clients understand, prioritize, and mitigate their organization-specific risk exposure.

Key Features

Periodic reporting for ongoing risk assessment and trend analysis. Organizational performance is measured and indexed on a configurable periodic basis (e.g. daily, weekly, monthly) to provide high-resolution visualization of details and trend analysis.

Risk scoring threshold monitoring: When observed security scoring thresholds are exceeded, real-time risk scoring notifications are made available via email and the secure Q:SCAN portal. Email notifications do not include sensitive information, while the full details of the reason(s) for scoring change are presented in the secure portal. The discoveries that triggered the scoring changes are prioritized and can be sorted as required by severity and asset type. Additional notifications through additional communications channels (e.g. Slack) are also optionally configurable.

Detailed risk exposure alerts: Performance alerts can also be delivered using a highly available secure portal protected by multi-factor authentication. Immediate alerts for data breach, IP reputation, malware, vulnerabilities and exposed ports are available, as well as on-demand or scheduled reporting options.

Granular access control management: User privilege administration is achieved with a role-based access control (RBAC) methodology. Roles and organizational view privileges are assigned on a per-user/per-organization basis. Roles include a read-only view to a specific collection of monitored organizations.

Convenient API-based accessibility: To support automation and third-party integration efforts, secure RESTful API access is available to transmit data and reports as needed.

Approach and Methodology

Q:SCAN's approach is to enumerate a company's external assets by using open source intelligence and footprinting techniques as an attacker would to collect information about security posture as viewed from outside the network perimeter. The data sets collected are considered risk signals that when fed into the scoring engine produce an overall risk score.

Collected signals may include but are not limited to the following:

- Domain and subdomains
- DNS Records
- DMARC
- SPF
- DNSSEC
- Zone Transfers
- Open Ports
- Exposed Services
- Malware Indicators and Reputation
- Web Application Headers
- Emails associated with know public breach records
- TLS Certificate health
- Cyber Enrichment Datasets

Q:SCAN leverages several open and proprietary aggregated datasets to enrich the raw data collected from Q:SCAN with known breach, reputation, and vulnerability data. This contextualized enrichment enables sophisticated analytics for cybersecurity risk exposure and mitigation with Q:CYBER and operational risk exposure and coverage with RubiQon.

Breach Data

The Breach Records database provides a core data set for supporting historical breach record search and exploration based on matching emails and domains. Raw and derived data from actual breaches is characterized and cataloged to support standardized threat intelligence enrichment, including security rating influence, 3rd- and 4th-party risk assessment, and sector-specific trends such as known attack tactics, breach magnitudes, losses, etc.

Event Data

The Event database is intended to capture a list of cyber-related events which can be queried directly for many details about event properties and attributes based on meta-data from SEC filings, press releases, news reports, Internet Relay Chat (IRC) channels etc.

Reputation Data

The Reputation database ingests, harmonizes, and indexes open source and paid reputation data feeds used by QOMPLX to determine if intellectual property and/or domains have been associated with known malicious activity such as the spread of malware or otherwise may be compromised.

Vulnerability & Exploit Database

The Vulnerability & Exploit database catalogs critical data ingested from open source and commercial vulnerability and exploit data feeds to inform network risk scoring, threat intelligence (including advanced attack path planning), and risk modeling efforts (such as the ability to track, predict, and alert on changes to vulnerability and exploit trends across cyber and insurance use cases).

Threat Actor Database

The Threat Actor database maps known threat actors with their tactics, techniques, and procedures (TTPs) as well as their known breach details. This information is particularly helpful for organizations typically targeted by certain threat actors to identify and block likely threat vectors.

Tool Database

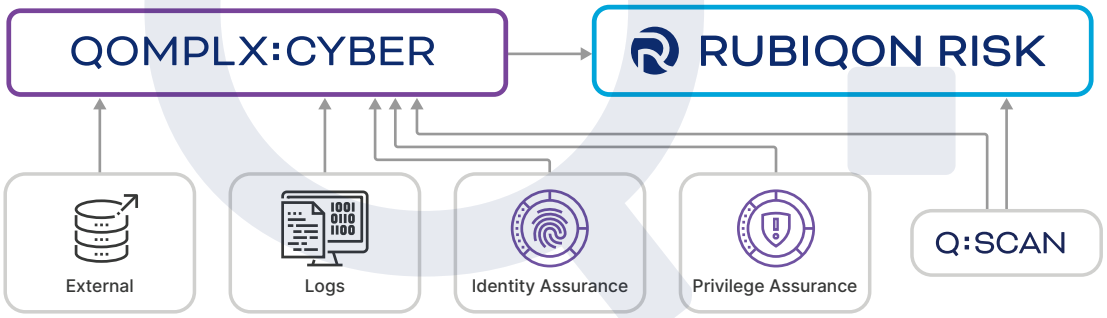
The Tool database collects metadata associated with both offensive and defensive security and software tools to link their usage to specific cyber events, cyber controls, cyber kill chain stages, and threat actors.

Internet Infrastructure Health Database

The Internet Infrastructure Health database captures public internet infrastructure state information to normalize and contextualize historical breach events, breach data sets, and insurance/economic loss estimates to better reflect reality. For example, a widespread Distributed Denial-of-Service (DDoS) attack can be an important part of understanding the "state" of the environment under which a given breach may have occurred.

Q:SCAN in the QOMPLX Ecosystem

Data from Q:SCAN and the Cyber Enrichment Datasets form one half of the signals needed to measure real cyber risk for an organization by providing a clear understanding of the external exposures. Q:CYBER provides the second half by providing real-time monitoring of internal exposures. Mapping both internal and external signals to an organizational threat model identifies the true cyber risk that a company should apply mitigations against. Pairing threat model findings with known mitigations allows RubiQon to assess a company's actual cyber risk at any given time.



QOMPLX Risk Management Ecosystem

Risk Signal Collection

- Q:SCAN results
- External logs
- Internal logs
- Identity Assurance data
- Privilege Assurance data

Contextual Risk Enrichment Databases

- Breach data
- Event data
- Reputational data
- Vulnerability & Exploit data
- Threat Actor data
- Security Tool metadata
- Internet Infrastructure Health data

Cyber Risk Management

Q:CYBER

- Integration
- Customization
- Monitoring
- Response
- Forensics
- Optimization

Operational Risk Management

RUBIQON RISK

- Exposure assessment
- Bespoke coverage
- Risk reduction incentives
- Claims and loss adjustment