QOMPLX:CYBER

Q:SCAN for Supply Chains

Score the cyber risk posture of your suppliers

Find and Fix Your Third-party Cyber Risks — Every Day

All organizations rely on vendors and third parties to support their business. These suppliers provide a wide range of goods and services such as payroll processing, infrastructure hosting, physical security, maintenance, and software, not to mention less glamorous but essential services such as catering and copier repair. Most organizations have third-party risk management ("TPRM") or vendor oversight teams that manage the cradle-to-grave lifecycle of vendor activities, including sourcing, due diligence, contracting, onboarding, fulfillment, continuous monitoring and offboarding.

Suppliers of every size and in every sector are increasingly taking their businesses online. As they do, they create opportunities for bad actors to find new vulnerabilities and exploit them, gaining access to the financial accounts, personal information, or intellectual property that your organization has required them to protect. Because attackers prize efficiency as much as businesses do, they look for paths of least resistance. In many cases, the best way to gain access to a target's sensitive data is to compromise its supply chain, or to infiltrate the IT systems of a key vendor. For example, in 2013, attackers caused $220 million in damages to the retailer Target by initially targeting Fazio Mechanical, a humble HVAC vendor.

As cyber risks remain elevated, third-party risk management teams need to continuously monitor their suppliers' processes to minimize the likelihood of third-party cyber breaches. Organizations need repeatable, data-driven solutions that create clean, accurate vendor masters and automate error-prone manual risk-rating processes.

Solution

Q:SCAN for Supply Chains is a new way for your third-party risk management team to visualize the security of your entire vendor base. Q:SCAN for Supply Chains uses open-source intelligence ("OSINT") collection and analysis techniques to look for high-risk signals that would be valuable to attackers. Q:SCAN for Supply Chains complements existing vulnerability scanning and tabletop processes your vendor risk management team has already implemented.

Q:SCAN for Supply Chains passively scans the Internet domains of your suppliers to identify key risk signals that can indicate they may have a poor security posture, or may be prone to mishandling the information you have entrusted to their care. Q:SCAN detects misconfigured or missing email security settings, inadequate use of cryptography, exposed Internet services and other key signals of poor domain health. To provide advanced analytics, Q:SCAN also checks a range of public and proprietary

databases including lists of data breaches breaches, historical cyber events, IP reputation databases, disclosed vulnerabilities, cyber attack tools and known threat actors.

To help your third-party risk management team understand which suppliers need to improve their public security postures, Q:SCAN for Supply Chains organizes key cyber risk signals by vendor tier and by categories that include technical security, configuration, data and information management, process and activity, and documentation. Q:SCAN for Supply Chains creates an overall risk score for each supplier using the familiar metaphor of a "credit score," with scores ranging from zero to 850.

Q:SCAN for Supply Chains runs continuously, delivering alerts to you by email when particular vendor scores change. You are in full control about when and how you are alerted. To help you take action, QOMPLX experts are available to provide guidance and recommendations whenever you need it.

Benefits

Without Q:SCAN for Supply Chains	With Q:SCAN for Supply Chains
Your third-party risk team has poor visibility into the cyber risks in your supply base.	Q:SCAN for Supply Chains analyzes high-risk signals that attackers may seek to exploit in your supply chain. You control which domains to scan for each vendor.
Your knowledge about your suppliers' true security practices are limited to what they told you in their initial vendor assessment forms.	Q:SCAN for Supply Chains delivers the "ground truth" about suppliers' external internet exposures, not the sunshine and fluff that they want you to believe.
Your tabletop exercises and vulnerability scanning tools don't give you the full picture of risk for your high-risk suppliers.	Q:SCAN for Supply Chains looks at a wide range of public and proprietary databases to provide advanced analytics that identify whether your suppliers have been cited in breaches, cyber events or IP address reputation lists.
Your third-party risk management team screens suppliers prior to onboarding them, but needs help continuously monitoring them.	Q:SCAN for Supply Chains scans your vendors' internet presences continuously for weaknesses and exposures, alerting you to conditions that suggest poor internal controls.

Key Features

Q:SCAN for Supply Chain's key features include:

- **Detailed Risk Exposure Alerts**. Q:SCAN for Supply Chains alerts you about vendor external exposures including data breach citations, presence on IP reputation lists, observed malware databases, externally observable vulnerabilities and exposed ports.

- **Periodic Reporting for On-going Risk Assessment and Trend Analysis**. Q:SCAN for Supply Chains provides high-resolution visualization of your entire supply chain's external security posture by vendor tier, and of the "portfolio risk" these suppliers represent. Reports run on-demand, or on a periodic schedule you choose.
- **Granular Access Control Management**. Q:SCAN for Supply Chains role-based access control (RBAC) secures access to configurations and scan data, and optionally integrates with your organization's Single-Sign-On (SSO) system via SAML 2.0.
- **Convenient API Access**. Q:SCAN for Supply Chains's secure RESTful API allows engineers to initiate scans, query status and to download data and reports, enabling you to integrate Q:SCAN for Supply Chains into vendor risks monitoring and reporting systems.

Ready to learn more about *Q:Scan*? Contact us today.

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

Why QOMPLX®

QOMPLX provides the essential data, tools, and services customers need to identify, contain, and fix their most critical risks. Our SaaS-based analytics infrastructure is provided by QOMPLX:OS, an enterprise operating system that powers QOMPLX's decision platforms in cybersecurity, insurance underwriting, and quantitative finance. Headquartered in Reston, VA, QOMPLX, Inc. also has offices in New York and London. More information about QOMPLX can be found at https://www.qomplx.com/.