QOMPLX:CYBER

Q:SCAN

Score your external security posture

Present the very best version of yourself to the internet

Your organization uses the internet to conduct all kinds of business. You have public websites, email servers, infrastructure, and business applications, running in your own data centers, in the cloud, and on partner platforms. You have people—lots of people—working in their professional capacities but also living their lives outside of work. This unique mix of public and private resources all produce signals that attackers seek to understand and exploit, and that customers use to judge the health of your security program.

Nothing invites theft like a broken window. How you appear to others sends powerful signals about how you should be treated. With internet security as with life, appearances matter. And the consequences can be severe: cyber criminals are continually seeking to steal data, damage reputations, and extort ransoms. But even the most opportunistic digital thief knows basic economics: rattle doorknobs to find houses to rob. Look for signals that suggest poor habits. Survey targets to find the easiest ways in.

Solution

Q:SCAN is a new way for your cybersecurity team to see your organization's security the way outsiders see it. Q:SCAN uses open-source intelligence ("OSINT") collection and analysis techniques to look for high-risk signals that are valuable to attackers. Q:SCAN can be used all by itself, or it can complement the vulnerability scanning tools you are already using.

Q:SCAN passively scans your internet domains to identify key risk signals that can indicate your organization may have a poor security posture. 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 organization understand how it can improve its public security posture, Q:SCAN organizes key cyber risk signals by categories including technical security, configuration, data and information management, process and activity, and documentation. Q:SCAN creates an overall risk score for your organization using the familiar metaphor of a "credit score," with scores ranging from zero to 850.

Q:SCAN runs on demand or on a schedule of your choosing, delivering it to you by email alert after each scan or when your scores change. To help you take action, QOMPLX experts are available to provide guidance and recommendations whenever you need it.

Benefits

Without Q:SCAN	With Q:SCAN
Your organization has poor visibility into how attackers see your organization.	Q:SCAN analyzes high-risk signals that attackers may seek to exploit. You have complete control over which domains to scan.
Your vulnerability scanning tools don't give you the full picture.	Q:SCAN looks at a wide range of public and proprietary databases to provide advanced analytics that identify whether your company or its employees have been cited in breaches, cyber events or IP address reputation lists.
You spend too much time fending off questions from customers about your security program.	Q:SCAN helps you get ahead of customers' third-party risk management teams by identifying external weaknesses, reducing the time and money your staff needs to spend on inquiries.
Your organization's reputation is damaged by third-party reports that attribute risks to assets you do not own.	Q:SCAN offers an accurate analysis of your internet-facing presence by scanning assets linked to your domain. Q:SCAN does not guess what assets "might" belong to your organization.

Key Features

Q:SCAN's key features include:

- **Detailed risk exposure alerts**. Q:SCAN alerts you on 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 provides high-resolution visualization of your organization's external security posture. Reports run on-demand or on a schedule you choose.
- **Granular access control management**. Q:SCAN's 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's secure RESTful API allows engineers to initiate scans, query status and to download data and reports, enabling you to integrate Q:SCAN into your security monitoring systems and reporting.
- **Attack Surface Monitoring.** Discover, map, monitor, and report your global Internet-facing attack surface.

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

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

Ready to learn more about QOMPLX:CYBER?
Contact us today.

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

Why QOMPLX®

QOMPLX harnesses data to provide unified visibility into cyber risks and trust in identity. QOMPLX solutions reduce cyber risk and attack surfaces by mapping exposures and performing real-time detection of attacks. This approach increases network observability by closing the largest remaining gaps in cybersecurity: identity verification, cross-tool data fusion, and data interoperability. QOMPLX defends some of the world's most renowned brands by re-establishing trust for client organizations, assuring authentication, and enabling confident security decisions.

For more information, visit **qomplx.com** and follow us **@QOMPLX**.