QOMPLX:CYBER

Monitor Your Cyber Risks

Let Q:CYBER Help Safeguard Your Security

Q:CYBER offers a comprehensive solution for organizations interested in defending Critical Controls Infrastructure, such as Active Directory and Kerberos, and turning back sophisticated attacks with applied data fusion.

Challenge

Modern cybersecurity teams face new threats and growing risks every day and must act quickly to proactively detect and prevent cyberattacks and other exposures. Attackers are finding it easier than ever to move laterally within organizations once they have established a foothold.

Although data lake efforts and security incident and event management (SIEM) tools were supposed to bring together multiple data sources and provide the security information needed to drive action, they fell short. Too many manual and complicated processes have been required and these outdated systems aren't modern event-oriented architectures with streaming analytics capabilities. Even a number of "next generation" SIEMs can't deliver what security teams really need, because traditional solutions don't really bring inside-out and outside-in security data together to provide an integrated view of enterprise security posture.

Solution

Q:CYBER offers a comprehensive solution for organizations interested in getting to ground truth in security. QOMPLX specializes in fusing together multiple security data feeds and uniquely defending Critical Controls Infrastructure like Active Directory and Kerberos and turning back sophisticated attacks and security challenges, such as:

- Attacks on Active Directory and other Critical Controls Infrastructure (CCI) undermine existing security and monitoring tools.
- Attacks on privileged accounts and lateral movement are a key stage in nearly every devastating cyber attack.
- Organizations struggle to assess their risk posture in time to address security lapses such as data breaches, IP theft, malware outbreaks and unpatched vulnerabilities or misconfigurations in public-facing IT assets.
- Managing high volume sources like Windows event logs and other high quality data sources that require careful management.

Q:CYBER

Benefits

Q:CYBER delivers all the capabilities of a truly modern cloud-native SIEM, from complete enterprise visibility and context to the range of analytics required to quickly protect networks and systems from attacks and other exposures. Our enterprise solution includes:

Privilege Assurance

Privilege Assurance helps companies map Active Directory and identity across the enterprise and proactively limit the BlastRadius score of a potential cyberattack.

Identity Assurance

Identity Assurance solution disrupts cyberattacks by detecting the techniques common to all large-scale breaches, including credential forgery and privilege escalation. Identity Assurance's detection and Active Directory monitoring capabilities are essential to keep your company's data secure.

Q:SCAN

Q:SCAN helps organizations map internet-facing attack surfaces to protect organizations' sensitive information for first and third party information security and risk programs.

Security Monitoring

Security Monitoring helps customers rapidly identify and contain attacks as they happen, by ingesting, parsing, normalizing, and monitoring logs from security tools and other sources, and by allowing customers to create their own rules, detections and analytics

D&B Cyber Risk Rating powered by QOMPLX

The D&B Cyber Risk Rating powered by QOMPLX combines the risk rating with financial impact scores to help you determine where you fall on the scale and how you can protect your business and your image.

Q:CYBER

Key Features

Let Q:CYBER's software bring you everything from complete visibility and context to the range of analytics required to quickly protect networks and systems from attacks and other exposures. Q:CYBER's features include:

- Support for mapping detections and controls against security frameworks such as MITRE ATT&CK, NIST, ISO, SOC, etc
- Identity validation as a service with metrics
- Identity systems monitoring with visibility on lateral movement pathways, assets, and privileges
- Validation of change management and configuration for identity and privilege
- Analysis of User/Entity behaviors, benchmarks, and anomalies
- Incident response capabilities for threat hunting and SOC teams
- Certified integrations with other tools like Splunk & Qradar with easy, API-based integrations and interoperability for any tool stack
- Big data platform tools for historical research on exploits, ad hoc queries, and detection performance

Ready to learn more about QOMPLX's *Q:CYBER suite of security solutions*? Contact us today.

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

Why QOMPLX®

QOMPLX makes it faster and easier for organizations to integrate all of the disparate data sources across the enterprise into a unified analytics infrastructure to make better decisions. This broader analytics infrastructure is provided through 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/.