RISKIQ® partnered with Microsoft

Boosting Cloud-Native Investigations with Security Intelligence

Challenges:

Today, security teams require a full 360-degree view of their digital attack surface to better detect threats and defend their enterprise. This means having continuous visibility of their organization's internal network, their internet presence, and awareness of the systems and entities with which your users and systems interact. All enterprises are in various stages of digital transformation—moving workloads to the cloud, adopting SaaS applications, automating development operations, utilizing microservices, and switching to serverless architectures—making monitoring and managing an enterprise's digital attack surface increasingly tricky. This digital sprawl further reinforces the need for 360-degree visibility and context as the key to every enterprise security team's ability to detect, investigate, and respond to threats.

Solution:

RiskIQ PassiveTotal™ integrates with Microsoft Defender and Azure Sentinel to seamlessly combine internal endpoint telemetry with petabytes of external Internet security intelligence collected by RiskIQ over more than a decade. Layering internet intelligence on top of endpoint data in one location provides crucial context to internal incidents. This context helps security teams know if they've been breached, as well as understand how internal assets interact with external infrastructure to block or prevent attacks.

Integrating Microsoft and RiskIQ intelligence in a single platform accelerates and enriches incident response via automation and team collaboration and opens new avenues of research. Security teams can identify and block new threat infrastructure that's part of attacks against their organization that they wouldn't otherwise know existed. This added visibility helps them identify gaps between the internet infrastructure they can see connected to their endpoints and the infrastructure they can't, giving them a detailed picture of their attack surface— just as attackers see it.

Key Take-aways:

- Seamlessly enrich endpoint telemetry with petabytes of Internet security intelligence
- Improve detection of malware & malicious communication
- Accelerate investigations and incident response
- Enable continuous digital attack surface visibility
- Provide unmatched internet security intelligence

> “RiskIQ's massive data collection capabilities enable incident responders to act quickly and with conviction, With this integration which ties together internal endpoint data with external infrastructure and layers on pertinent OSINT, the paradigm for time to response and remediation has certainly shifted.”
>
> **Alon Rosental**
> Principal Group Program Manager, Microsoft Defender for Endpoint at Microsoft Corp.

About RiskIQ

RiskIQ is the leader in digital attack surface management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. Learn how at: www.riskiq.com

Use Cases / Business Value:

- **Accelerate Threat Detection and Investigation.** RiskIQ PassiveTotal aggregates the most comprehensive internet security intelligence and automatically correlates with and enriches Microsoft Defender's intelligence and insight.
- **Empower Collaboration and Reduce Remediation Time.** RiskIQ PassiveTotal enables enterprise security teams to seamlessly collaborate on threat investigations or incident response engagements by providing a shared, 360-degree context.
- **Proactively Manage and Protect Your Digital Attack Surface.** Gain complete visibility into your externally facing assets, compare that against Microsoft endpoint coverage, and assure that all of your assets are managed and protected.

Key Capabilities:

RiskIQ PassiveTotal merges external internet intelligence directly with Microsoft solutions and telemetry in order to give analysts a complete picture. Analysts can download Microsoft reports, explore OSINT data, pivot on related indicators and identify overlap between malicious actors.

RiskIQ PassiveTotal leverages the Microsoft Defender to automatically search internal endpoints for a specific indicator being queried or pivoted on. Having this information overlaid with external intelligence from RiskIQ means analysts save time and can stay focused on their investigation.

RiskIQ PassiveTotal brings over 10 years and multiple petabytes of external internet intelligence directly to the analyst in a simple-to-use interface. Investigations can be created and artifacts added in order to track response and completeness of the clean-up efforts.

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com