RISKIQ® partnered with CROWDSTRIKE

Providing Security Teams with 360-degree Visibility of Their Adversaries

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 a continuous visibility of their organization's internal network, their presence outside the firewall, and awareness of which systems and entities your users and systems are interacting with. 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 a serverless architectures—making monitoring and managing an enterprise's digital attack surface increasingly difficult. This digital sprawl further reinforces the need for a 360-degree visibility and context as the key to every enterprise security team's ability to to timely detect, investigate, and respond to threats.

Solution:

RiskIQ Illuminate™ for CrowdStrike integrates with Falcon 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 understand how internal assets interact with external infrastructure so they can block or prevent attacks and know if they've been breached.

Integrating CrowdStrike 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 what they can't, which gives 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 has been a core component and integral part of CrowdStrike's Threat Research operations for years. RiskIQ Illuminate now seamlessly enriches CrowdStrike Falcon with RiskIQ's unmatched internet intelligence empowering security teams to accelerate investigation and better protect their enterprise."

Adam Meyers
VP of Threat Research
Crowdstrike

About Crowdstrike

CrowdStrike® Inc., a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: www.crowdstrike.com

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 Illuminate aggregates the most comprehensive internet security intelligence and automatically correlates with and enriches CrowdStrike Falcon's intelligence and insight.
- **Empower Collaboration and Reduce Remediation Time.** RiskIQ Illuminate 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 CrowdStrike endpoint coverage, and assure that all of your assets are managed and protected.

Key Capabilities:

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

RiskIQ Illuminate leverages the CrowdStrike ThreatGraph 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 Illuminate 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®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com