



partnered with

**Microsoft**

# RiskIQ Intelligence for Microsoft Security Solutions

## Enhancing your Security Operations with Petabytes of Internet Intelligence

### Challenges: Staying Ahead of Digital Transformation

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 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 architecture—making monitoring and managing an enterprise's digital attack surface increasingly difficult. This digital sprawl further reinforces the need for 360-degree visibility and context as the key to every enterprise security team's ability to timely detect, investigate, and respond to threats.

### Solution: Accelerate Investigations, Eliminate Threats

RiskIQ Intelligence integration combines and enriches Microsoft's Security Ecosystem and Azure Sentinel with petabytes of external Internet security intelligence collected by RiskIQ over more than a decade. Connecting RiskIQ's Internet Intelligence Graph with Microsoft's Security solutions provide crucial external context to all internal IOC's and incidents. This context helps security teams understand how internal assets interact with external infrastructure so they can better detect and prevent attacks and know if they've been breached.

Integrating RiskIQ intelligence into Microsoft Azure Sentinel's cloud-native SIEM platform accelerates and enriches incident response via automation, 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.

### Use Cases / Business Value:

- Accelerate Threat Detection and Investigations.** RiskIQ Intelligence with Microsoft Security suite brings the most comprehensive internet security intelligence data set and automatically correlates and enriches Microsoft Azure Sentinel's insights, analytics, and dashboards.

### Key Take-aways:

- Accelerate triage efforts by fusing data from RiskIQ Internet Intelligence Graph with Microsoft Azure Sentinel alerts and incidents
- Gain deeper visibility into threats in your environment by applying RiskIQ Threat Intelligence within your Microsoft Azure Sentinel Analytics
- Automate response efforts and keep teams informed using RiskIQ Playbooks to decorate incidents with enrichment content
- Build your own orchestration pipelines using the RiskIQ Flow Connector and Microsoft Logic Apps

### Search, Correlate, and Enrich Microsoft with the following

#### Data Sets:

- Passive DNS
- WHOIS
- SSL Certificates
- Web Components
- Trackers
- Host Pairs
- Cookies

"RiskIQ is the first security intelligence solution to deliver automated incident enrichment within Microsoft Sentinel, giving practitioners the ability to tap into petabytes of current and historic internet intelligence to inform and automate their security operation programs."

**Jason Wescott**  
Principal Product Manager  
Microsoft Cloud + AI Security

- **Proactively Defend Your Organization from Attackers.** Uncover hidden facets of an attacker's infrastructure, proactively block this malicious infrastructure, and set monitors on branded terms to be alerted when elements are found that may be targeting your brand.
- **Automate Your Security Operations.** Leverage the RiskIQ Flow Connector to extend published playbooks or create your own. Build complex workflows that automate mundane or tedious security tasks to save your team time and resources.

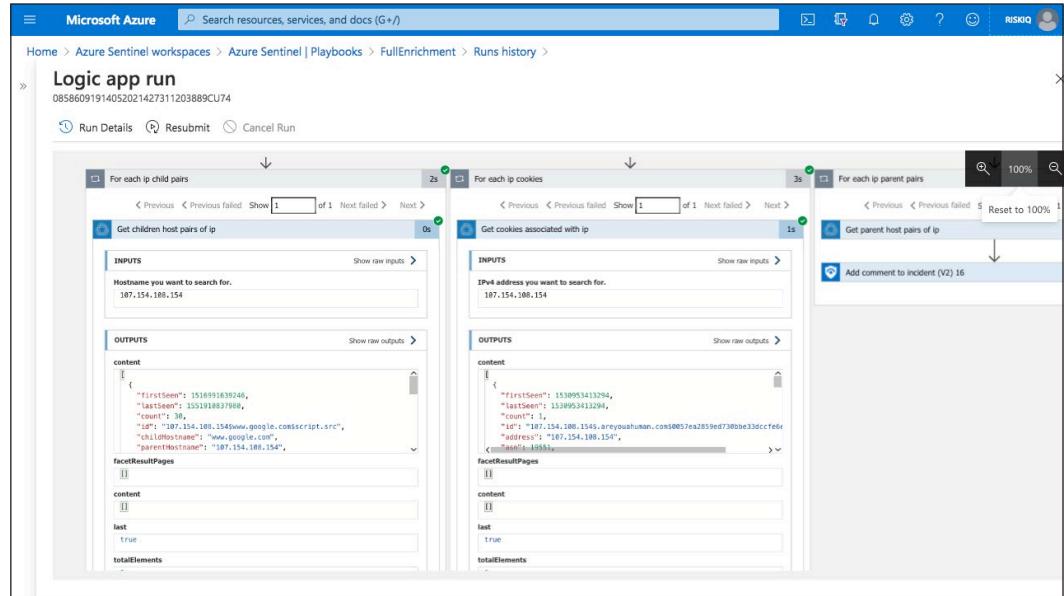
## Better Defend Your Organization from Attackers

RiskIQ's Internet Intelligence Graph brings the full-scope context to incidents and attack campaigns by identifying and linking related entities through multiple data sets, including active and passive DNS, WHOIS, SSL certificates, and other webpage content attributes. RiskIQ integration with Microsoft Azure Sentinel aggregates and correlates external threat actor intelligence with internal indicators data into a single platform, so analysts can spend their time focusing on threats, not data collection and correlation. With a combination of RiskIQ and Microsoft, security teams are able to quickly make decisions, accelerate investigations, orchestrate remediation actions, and block threat actors before they breach your enterprise.

## Screen Shots

The screenshot shows the Microsoft Azure Azure Sentinel Incidents page. On the left, there is an incident details card for "Crimeware Malware Delivery" (Incident ID: 3874). The card includes fields for Severity (High), Status (Active), and Owner (Unassigned). It also shows the incident link: [https://portal.azure.com/#asset/Microsoft\\_Az...](https://portal.azure.com/#asset/Microsoft_Az...). Below the link are sections for Tactics (empty), Tags (crimeware, loader), Last update time (06/23/20, 06:22 PM), Creation time (06/23/20, 06:17 PM), and Classification (N/A). At the bottom of the card is a blue "Investigate" button. On the right, there is a "Comments (15)" tab selected, showing 15 comments from user "Brandon Dixon" dated 06/23/20, 06:21 PM. Each comment includes a snippet of associated data and a link to view additional details.

Commenter	Date	Associated Data
Brandon Dixon	06/23/20, 06:21 PM	Associated SSL Certificates for dl2.dropbox-download-eu.com: 7 View additional details at <a href="https://community.riskiq.com/search/dl2.dropbox-download-eu.com/domaincertificates">https://community.riskiq.com/search/dl2.dropbox-download-eu.com/domaincertificates</a>
Brandon Dixon	06/23/20, 06:21 PM	Associated Cookies for dl2.dropbox-download-eu.com: 5 View additional details at <a href="https://community.riskiq.com/search/dl2.dropbox-download-eu.com/cookies">https://community.riskiq.com/search/dl2.dropbox-download-eu.com/cookies</a>
Brandon Dixon	06/23/20, 06:21 PM	Associated Cookies for 45.142.213.18: 16 View additional details at <a href="https://community.riskiq.com/search/45.142.213.18/cookies">https://community.riskiq.com/search/45.142.213.18/cookies</a>
Brandon Dixon	06/23/20, 06:21 PM	Associated Web Components for dl2.dropbox-download-eu.com: 5 View additional details at <a href="https://community.riskiq.com/search/dl2.dropbox-download-eu.com/components">https://community.riskiq.com/search/dl2.dropbox-download-eu.com/components</a>



## About RiskIQ, Inc.

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. With more than 75 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams, and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect the business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.

Visit <https://www.riskiq.com> or follow us on Twitter. Try RiskIQ Community Edition for free by visiting <https://www.riskiq.com/community/>

### RiskIQ, Inc.

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



**✉** sales@riskiq.net

**📞** 1 888.415.4447

**Learn more at [riskiq.com](https://www.riskiq.com)**

Copyright © 2020 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 06\_20