RISKIQ® 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 their 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 provides 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.

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 including dynamic reputation scores
- 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

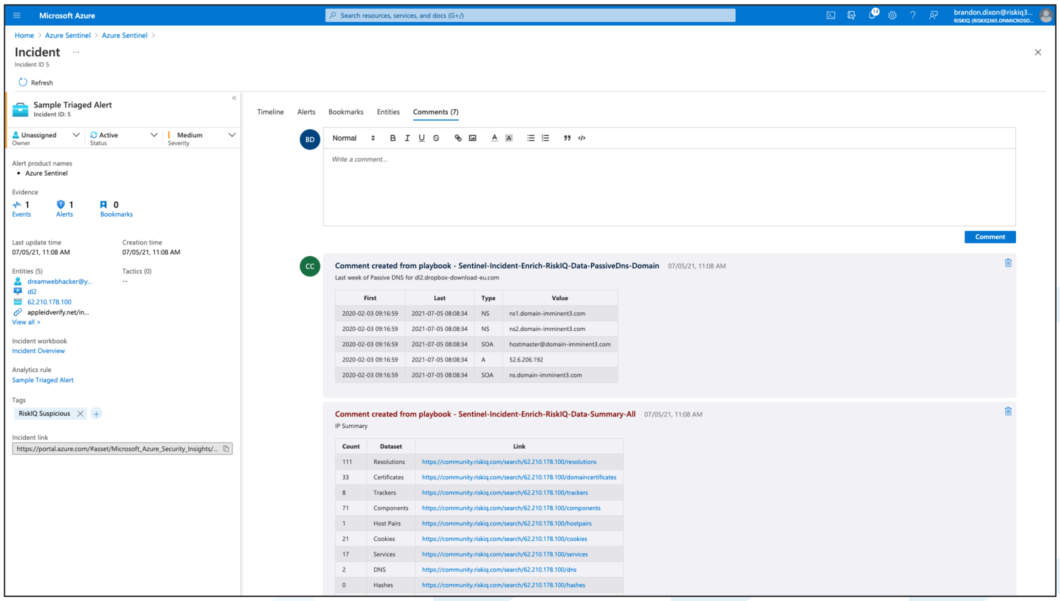
Use Cases / Business Value:

- **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.
- **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



Incident
Incident ID 5

Sample Triaged Alert
Incident ID: 5

Unassigned
Owner

Active
Status

Medium
Severity

Alert product names
- Azure Sentinel

Evidence
1 Events
1 Alerts
0 Bookmarks

Last update time
07/05/21, 11:08 AM

Creation time
07/05/21, 11:08 AM

Entities (5)
dreamwebhacker@y...
dl2
62.210.178.100
appleidverify.net/in...
View all >

Tactics (0)
--

Incident workbook
Incident Overview

Analytics rule
Sample Triaged Alert

Tags
RiskIQ Suspicious

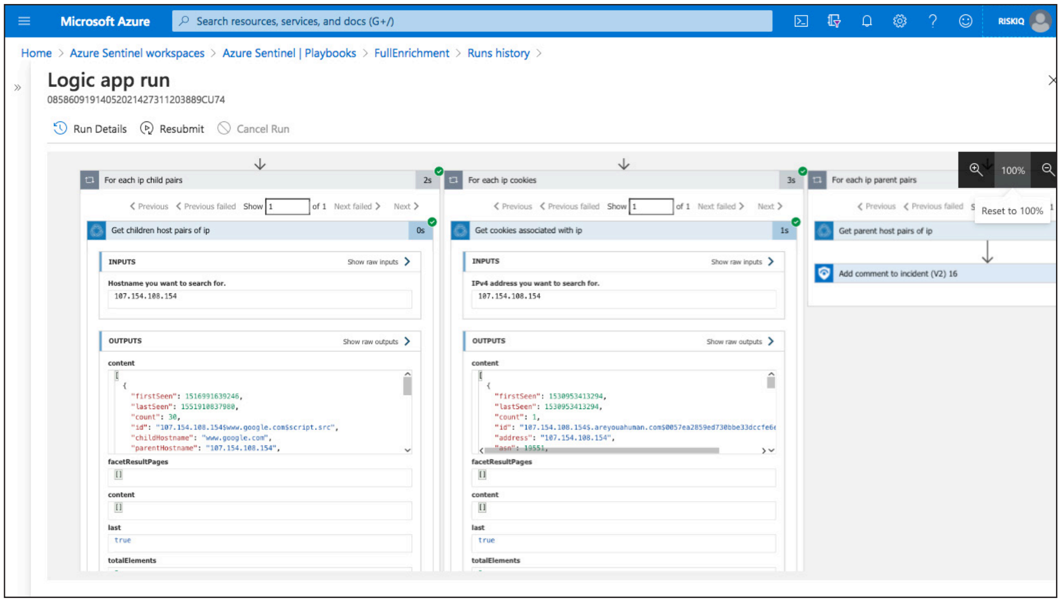
Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...

Comment created from playbook - Sentinel-Incident-Enrich-RiskIQ-Data-PassiveDns-Domain 07/05/21, 11:08 AM
Last week of Passive DNS for dl2.dropbox-download-eu.com

First	Last	Type	Value
2020-02-03 09:16:59	2021-07-05 08:08:34	NS	ns1.domain-imminent3.com
2020-02-03 09:16:59	2021-07-05 08:08:34	NS	ns2.domain-imminent3.com
2020-02-03 09:16:59	2021-07-05 08:08:34	SOA	hostmaster@domain-imminent3.com
2020-02-03 09:16:59	2021-07-05 08:08:34	A	52.6.206.192
2020-02-03 09:16:59	2021-07-05 08:08:34	SOA	ns.domain-imminent3.com

Comment created from playbook - Sentinel-Incident-Enrich-RiskIQ-Data-Summary-All 07/05/21, 11:08 AM
IP Summary

Count	Dataset	Link
111	Resolutions	https://community.riskiq.com/search/62.210.178.100/resolutions
33	Certificates	https://community.riskiq.com/search/62.210.178.100/domaincertificates
8	Trackers	https://community.riskiq.com/search/62.210.178.100/trackers
71	Components	https://community.riskiq.com/search/62.210.178.100/components
1	Host Pairs	https://community.riskiq.com/search/62.210.178.100/hostpairs
21	Cookies	https://community.riskiq.com/search/62.210.178.100/cookies
17	Services	https://community.riskiq.com/search/62.210.178.100/services
2	DNS	https://community.riskiq.com/search/62.210.178.100/dns
0	Hashes	https://community.riskiq.com/search/62.210.178.100/hashes


Microsoft Azure
Search resources, services, and docs (G+/)
RISKIQ
Home > Azure Sentinel workspaces > Azure Sentinel | Playbooks > FullEnrichment > Runs history >
Run Details
Resubmit
Cancel Run
For each ip child pairs
2s
For each ip cookies
3s
For each ip parent pairs
Previous
Previous failed
Show 1 of 1
Next failed
Next
Get children host pairs of ip
0s
Get cookies associated with ip
1s
Get parent host pairs of ip
Add comment to incident (V2) 16
100%
Reset to 100%
INPUTS
Show raw inputs
OUTPUTS
Show raw outputs

Logic app run

085860919140520214273112O3889CU74

Hostname you want to search for.

107.154.108.154

content

```
[
  {
    "firstSeen": 1516991639246,
    "lastSeen": 1551910837980,
    "count": 30,
    "id": "107.154.108.154$www.google.com$script.src",
    "childHostname": "www.google.com",
    "parentHostname": "107.154.108.154",
```

facetResultPages

[]

content

[]

last

true

totalElements

IPv4 address you want to search for.

107.154.108.154

content

```
[
  {
    "firstSeen": 1530953413294,
    "lastSeen": 1530953413294,
    "count": 1,
    "id": "107.154.108.154$.areyouahuman.com$0057ea2859ed730bbe33dccfe6e
    "address": "107.154.108.154",
    "asn": 19551,
```

facetResultPages

[]

content

[]

last

true

totalElements

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