RISKIQ®

RiskIQ External Threats®

Detect and Respond to Digital Threats

Business is Embracing Digital—so are Cybercriminals

As business evolves and moves more processes and interactions online, cybercriminals are exploiting digital channels to launch new types of attacks.

Detecting threats across the vastness of the internet is a daunting task. With hundreds of thousands of new web pages created every day, on top of the billions that already exist, understanding which websites, apps, and social profiles are a threat to your business at any given time, and how threat actors are leveraging them, is critical to protecting your organization. However, to make sense of it all, your organization requires massive scale data collection and sophisticated analysis.

RiskIQ External Threats® software automates the detection, monitoring, and remediation of digital threats posed by malicious actors to your organization, employees, and customers. Utilizing virtual user technology, advanced machine learning, and petabytes of RiskIQ internet data, External Threats finds fraudulent websites, domains, social profiles, and mobile apps as they emerge, determines their threat severity, and empowers security teams to take action to mitigate the specific risks.

External Threats provides organizations the capability to monitor digital channels and detect advanced threats like:

- Domain and subdomain typosquatting
- Phishing
- Social media accounts impersonating companies or executives
- Leaked data published in the open or posted for sale
- Fake or modified mobile apps harvesting user credentials or distributing mobile malware
- Brand tarnishment or misuse in scams
- Attack planning in deep and dark web forums

How Does RiskIQ Detect External Threats?

External Threats uses virtual user technology as it crawls the internet, experiencing websites, social media profiles, and mobile apps just like a real user does. RiskIQ virtual users visit websites from thousands of IP addresses originating from around the world, using different browser and device types. This technique allows us to evade obfuscation techniques used by advanced threat actors seeking to cover their tracks and detect attacks targeted only to specific groups of users.

Features

- Industry-leading coverage of web, mobile, and social digital channels
- Built-in workflow for efficient threat mitigation and management
- Monitor threats over time to track changes in risk severity
- Automatic enrichment to contextualize threats to your environment
- Robust API access and easy integrations with other security tools
- Flexible policy framework and granular controls to customize and fine-tune detection

Benefits

- Comprehensive detection of threats to your business, brand, and customers
- Group large volumes of data by key risk factors to focus on high priority threats to the business and scale your security program
- Fast triage and takedown of threats with automated tracking and follow-up
- Seamless communication across teams regarding threat status

External Threats Modules:

- Domain threats
- Mobile threats
- Social brand threats
- Social executive threats
- Phishing
- Brand tarnishment
- Data leakage
- Deep and dark web monitoring

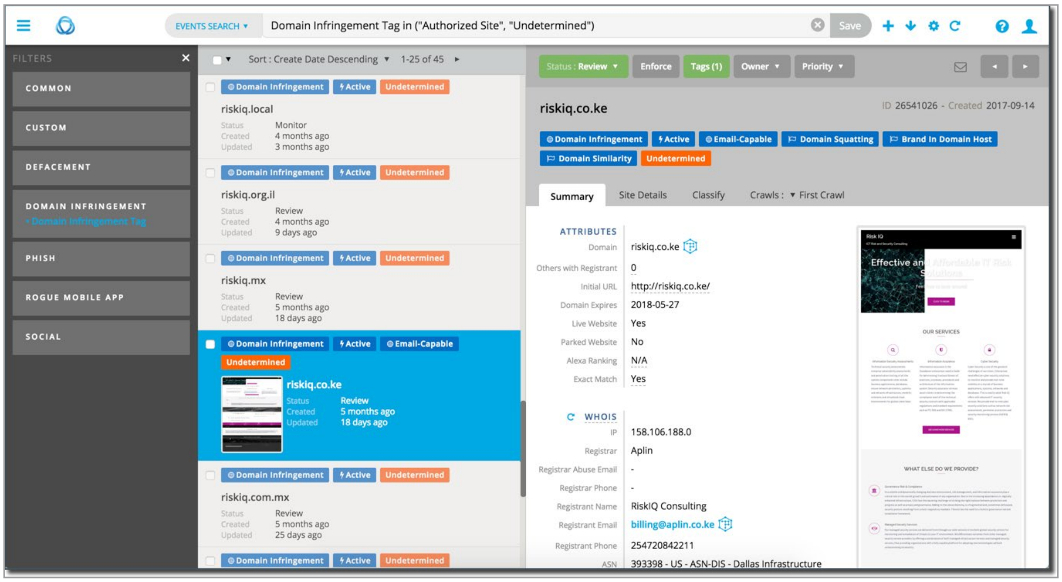
External Threats Dashboard and Reporting

RiskIQ provides an intuitive dashboard for monitoring the internet for External Threats across all threat-types and channels, as well as tracking on-going mitigation efforts and successful resolution.

- On-demand executive summary reports and a snapshot of the current state of an organization's global presence and threats against it
- Custom reports and data drill-down with key metrics include:
    - Event generation for a specific period
    - Current review status and status change history
    - Event uptime until resolution and time elapsed during each stage of the threat lifecycle
    - Events by website, app store, and social network
    - Brands associated to events
    - Geographic distribution of events

When virtual users arrive at a page, they capture and catalog everything that happens when that page is loaded. The perspective of a virtual user provides visibility into embedded resources in a site, drive-by downloads, or other malicious scripts or redirects. This allows you to capture data for forensic analysis and accurately identify, monitor, and mitigate digital threats against you across the internet.

Virtual users execute over a billion http requests per day. Additionally, RiskIQ has integrations with all major social media platforms, hundreds of app stores around the world, and analyzes millions of newly created domain names and hostnames daily to enable visibility and fast, comprehensive response to threats.



Domain Infringement Tag in ("Authorized Site", "Undetermined")

Sort : Create Date Descending 1-25 of 45

Domain Infringement | Active | Undetermined
riskiq.local
Status Monitor
Created 4 months ago
Updated 3 months ago

Domain Infringement | Active | Undetermined
riskiq.org.il
Status Review
Created 4 months ago
Updated 9 days ago

Domain Infringement | Active | Undetermined
riskiq.mx
Status Review
Created 5 months ago
Updated 18 days ago

Domain Infringement | Active | Email-Capable | Undetermined
riskiq.co.ke
Status Review
Created 5 months ago
Updated 18 days ago

Domain Infringement | Active | Undetermined
riskiq.com.mx
Status Review
Created 5 months ago
Updated 25 days ago

Domain Infringement | Active | Undetermined

riskiq.co.ke
ID 26541026 - Created 2017-09-14

Domain Infringement | Active | Email-Capable | Domain Squatting | Brand In Domain Host | Domain Similarity | Undetermined

ATTRIBUTES

Domain	riskiq.co.ke
Others with Registrant	0
Initial URL	http://riskiq.co.ke/
Domain Expires	2018-05-27
Live Website	Yes
Parked Website	No
Alexa Ranking	N/A
Exact Match	Yes

WHOIS

IP	158.106.188.0
Registrar	Aplin
Registrar Abuse Email	-
Registrar Phone	-
Registrant Name	RiskIQ Consulting
Registrant Email	billing@aplin.co.ke
Registrant Phone	254720842211
ASN	393398 - US - ASN-DIS - Dallas Infrastructure

Fig. 1: External Threats user interface showing event details, screenshots, and event history.

Easy Mitigation and Response Workflow

Once threats are detected, they must be addressed—and fast. RiskIQ provides in-app workflow to easily assign ownership, add notes and tags, get feedback from other business units, and automatically generate and send takedown notifications or content removal requests to the appropriate parties.

RiskIQ has direct relationships with some of the largest hosting providers, social networks, and mobile app stores. The platform also integrates into Google Safe Browsing and Microsoft SmartScreen to enable automated blocking of phishing pages to 95% of internet users across the internet to neutralize phishing threats while the site is being taken down.

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

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com