Brand Threat Report

As a RiskIQ customer, tokens or professional services, may be used for a RiskIQ Brand Threat Report that provides a detailed assessment of you, as our customer in the perspective of a threat actor. Whether the threat actor is sponsored by a nation-state, works for a criminal organization, is engaged in hacktivism, or hacks as a hobby.

RiskIQ's i3 analysts will use strategic intelligence to create these assessments much in the same way a threat actor would: by gathering as much internet intelligence about the customer as possible, then studying the vulnerabilities before deciding on a plan of attack.

The Brand Threat Report is neither a penetration test nor a red team exercise; rather, it represents preliminary reconnaissance related to the customer. RiskIQ i3 analysts will identify attack vectors in combination with the assets most likely to be exploited by a threat actor and then provide a tailored analysis.

In this vein, RiskIQ provides a snapshot of a customer's asset inventory and layers it with an analysis of the customer's risks and vulnerabilities. RiskIQ i3 analysts leverage RiskIQ's proprietary Digital Footprint® inventory to identify applications and digital assets a customer has exposed to the internet. Many corporate security teams are forced to deal with a blind spot consisting of hundreds, if not thousands, of unmanaged applications and digital assets from which cyberattacks can emerge. RiskIQ Brand Threat Reports aid our customers' in-house security teams' in understanding their organization's attack surface and how it can be exploited by threat actors.

In a Brand Threat Report, RiskIQ's i3 analysts review a customer's asset inventory and contextualize vulnerabilities specific to their digital footprint. They will then review the customer's history, factor in the current threat climate for the customer's industry, prioritize specific points of vulnerability, conduct a final, holistic analysis and ultimately write the final report. Lastly, RiskIQ analysts can provide a virtual briefing to present their findings and discuss mitigation recommendations.

The following are the most common components included in the final RiskIQ Brand Threat Report:

WHAT WE PROTECT:

1. Executive Summary
2. Background
3. Methodology
4. Disclaimer
5. Brief History of the Company
6. Nature of the Company
7. Global Threat Environment
8. Company's Infrastructure
9. Points of Vulnerability
10. Link Analysis
11. Assessment
12. Mitigation Strategies

The final RiskIQ Brand Threat Report provides a sample of the resources, tools, technology, and analytical prowess that RiskIQ, working in partnership with the customer, can bring to bear against today's full spectrum of ever-evolving threat actors.

RISKIQ®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com