RISKIQ®

Discovery Limited Takes a Proactive Approach to Attack Surface Management with RiskIQ

About Discovery Limited

Discovery Limited is a South African-founded financial services organisation that operates in the healthcare, life assurance, short-term insurance, savings, and investment products and wellness markets. Founded in 1992, Discovery is guided by a clear core purpose—to make people healthier and to enhance and protect their lives. The company has expanded its operations globally and currently serves over 5 million clients across South Africa, the United Kingdom, the United States, China, Singapore, and Australia.

Challenges

Over recent years, Discovery's diversification activities, including the creation of a retail banking subsidiary and expanded global operations, resulted in a rapidly growing Internet presence and increased cyber risk. While they had some elements of brand protection in place, they recognised the need to better understand what was happening outside of their network:

- Across the assets they own that were visible on the Internet and therefore visible to malicious actors.
- Assets they didn't own that infringed on any of Discovery's brands and could potentially be used in targeted campaigns against their organisation and their customers.

In early 2018 Discovery began evaluating the market for Attack Surface Management (ASM) solutions. Their key requirements included comprehensive visibility into their owned assets and infringing assets across web, mobile, and social platforms. The solution needed to provide group-level visibility and operating company-level visibility, serving the group CISO and his team and the CISOs and SOC teams supporting the different subsidiaries. Finally, to operationalise ASM within their existing team structure, the intelligence provided had to integrate with their existing SOC tools and practices. Apart from technical considerations, the security operations team also required additional support to evaluate and respond to brand infringement threats.

Challenges

- Growing breadth and complexity of Internet exposed assets
- Detecting and responding to threats targeting Discovery brands and customers
- Resource constraints within the security team

Solution Benefits

- Living inventory of Internet exposed assets to drive various use cases
- Integration with Splunk for security operations workflows and reporting
- Detection and managed remediation of brand infringing assets across web, mobile and social platforms

> "… RiskIQ is the "spotlight" that removes the traditional dark spaces where the bad guys hide."
>
> – Zaid Parak
> CISO
> Discovery Limited

The RiskIQ Solution

After evaluating the market, Discovery selected the RiskIQ Illuminate® Platform as the foundation for their Attack Surface Management program. RiskIQ's breadth of coverage and ability to address all essential requirements made it the clear choice for the group CISO, subsidiary CISOs, and the security operations teams. Discovery have implemented the following Illuminate modules:

- **RiskIQ Digital Footprint®:** continuous discovery of all of Discovery's owned assets visible on the Internet. RiskIQ virtual users regularly engage with these assets as real users would to understand the subcomponents, services, and relationships of site elements and highlight anything requiring further investigation or remediation. Assets are tagged by organisational structure to provide relevant asset views for both group and subsidiary teams.
- **RiskIQ External Threats®:** brand security across the internet. RiskIQ detects the appearance of brand-infringing domains, brand infringing mobile apps in over 150 app stores, brand infringing social media accounts across the major social media platforms, and phishing sites leveraging Discovery's brands. RiskIQ provides a fully managed service to triage generated events and take down infringing assets.
- **RiskIQ PassiveTotal®:** used by security operations to conduct additional investigations into suspicious indicators and their connection to threat actor infrastructure.

As Splunk is used pervasively in the security operations centre, RiskIQ's Splunk integration allows security operations personnel to directly access RiskIQ data in Splunk to drive automation through playbooks and provide Splunk dashboards and reporting at all levels.

Key considerations included:

- Automated and continuous discovery of digital assets exposed on the Internet
- Curation of this asset inventory to provide views to support group functions as well as subsidiary security teams
- Detection of brand infringing assets across all Internet platforms; web, mobile and social and support in managing and responding to infringement events
- Integration with Splunk to support operational playbooks and multi-level reporting

The Results

Discovery have successfully deployed an Attack Surface Management platform underpinned by RiskIQ Illuminate. Security teams now have visibility of their existing Internet assets as well as any new assets that are deployed. Various use cases have been implemented both in RiskIQ and Splunk to automatically address areas of weakness across their footprint, with additional use cases planned. Brand infringing assets are automatically detected and triaged by the RiskIQ customer success team. Confirmed violations are sent to Discovery for review and takedown approval, with RiskIQ handling the takedowns and ensuring that the violating URLs are sent to Google Safe Browsing and Microsoft Smartscreen to warn users from visiting those locations.

“We believe we cannot achieve our Core Purpose without fiercely guarding our member’s data and protecting their digital lives,” said Zaid Parak, Discovery’s CISO. “To this end, RiskIQ is the “spotlight” that removes the traditional dark spaces where the bad guys hide.”

Conclusion

The RiskIQ Illuminate Platform provides organisations with ‘outside the firewall’ visibility to discover unknowns in their digital attack surface and identify threats targeting their organisation and their customers. This actionable intelligence can be used by security teams to address a wide range of security operations use cases to strengthen security and reduce overall cyber risk.

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

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com