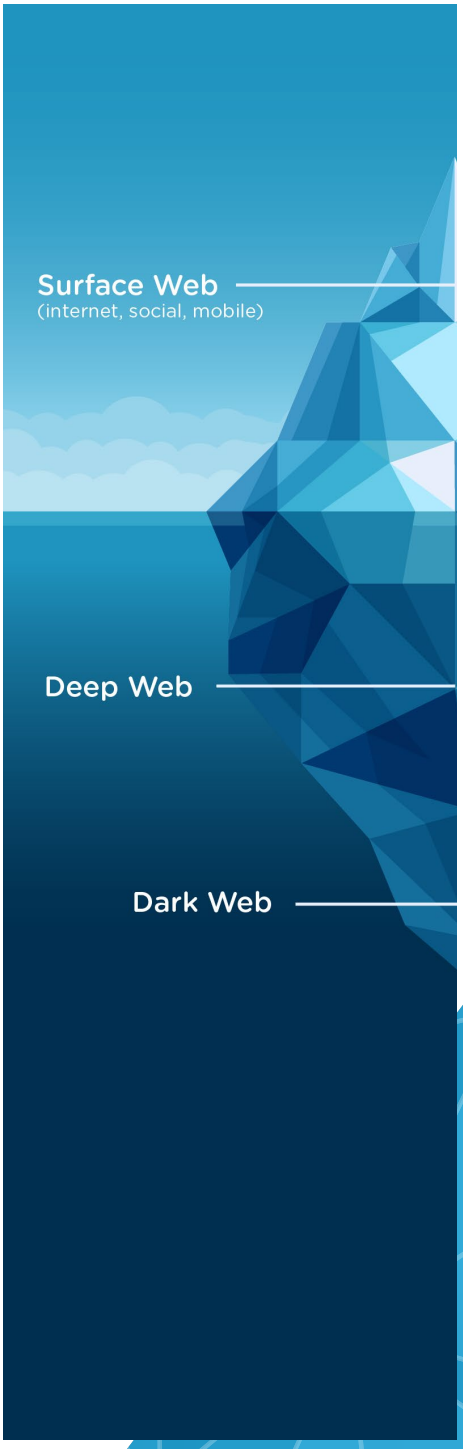
RISKIQ® partnered with FLASHPOINT

Digital Risk Protection Across the Open, Deep, and Dark Web

360 degree visibility to detect targeted threats against your organization

RiskIQ External Threats® automates the detection, monitoring, and remediation of digital threats posed by malicious actors to your organization, employees, and customers. A key piece of protecting your organization from digital risk outside the firewall is visibility across the surface web, the deep web, and the dark web. Each of these realms requires specialized technology to adequately detect threats so that security operations teams can take the appropriate action.

Like the visible part of an iceberg, the surface web is only one part of the digital risk equation. RiskIQ has remained the leader in targeted threat detection across the surface web, social media platforms, and mobile application marketplaces for almost a decade. RiskIQ provides security operations teams with the visibility, intelligence, and insight to find and shut down threat actors, their campaigns, and the infrastructure they use. This capability, coupled with deep and dark web visibility lets teams understand other attack types and even preempt them by seeing dark web forum conversations targeting an organization.



Deep and Dark Web Module and Partnership with Flashpoint

RiskIQ has partnered with Flashpoint, the leader in business risk intelligence, to search across deep and dark web forums where threat actors may be collaborating about impending attacks, planning campaigns, disclosing information about your organization or customers, or selling or discussing a data breach related to your business.

Traditional web crawling technology is blind to the deep and dark web since it operates in a separate realm from the surface web. Crawlers designed for the deep and dark web to surface discussions and pages are similarly blind to the surface web. Flashpoint compliments the internet-scale data provided by RiskIQ by giving access to forum data, enabling teams to proactively uncover references to your business, brand, or executives. The appearance of any keywords of interest create new events in External Threats.

Actioning the Intelligence

Web pages on the internet, social media profiles, and mobile applications that are threats to an organization can be removed from their respective platforms, and RiskIQ has built-in workflows to help manage the takedown processes. For the deep and dark web, though, awareness of the threat is key to preempt an attack, or to fortify your defenses in preparation.

Using RiskIQ and the Deep and Dark Web module in External Threats, customers get access to and awareness of discussions of targeted threats against them on the dark web, and using this intelligence, be prepared for an attack campaign based on those discussions. For example, threat actors may discuss a phishing campaign against a global payments provider on the dark web. As an External Threats customer, the discussion would appear as an event in External Threats, enabling the security team to be on high alert that there may be an imminent attack. Further, if an attack is actually launched, External Threats Anti-Phishing would find the page setup to phish users for their credentials, and automatically block that URL via Microsoft SmartScreen and Google Safe Browsing.

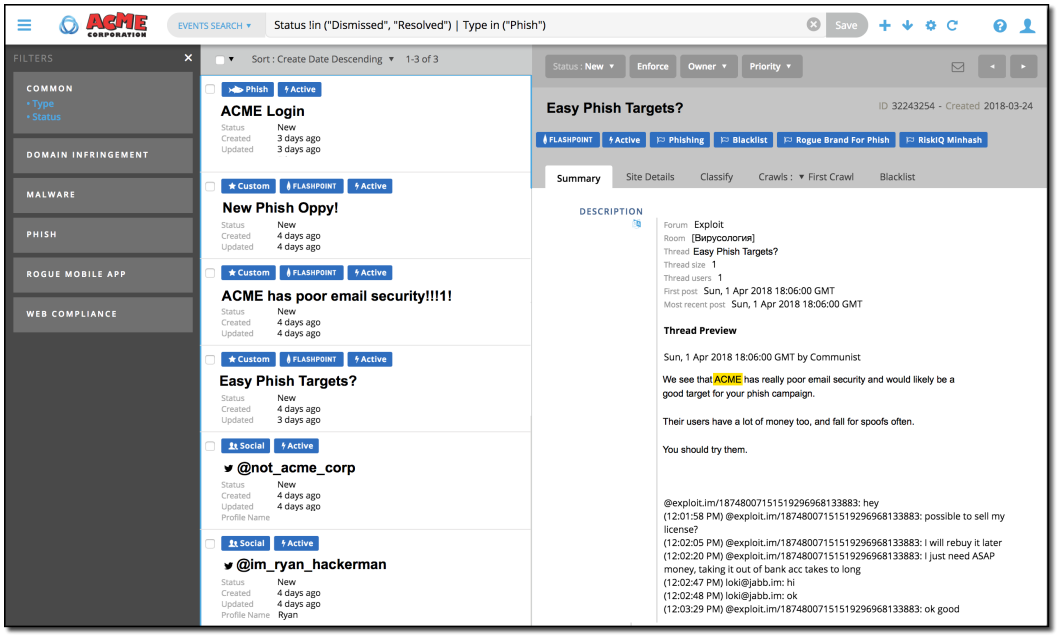


Fig 1 - Screenshot of External Threats with Dark Web alerts and a follow-on Phish campaign

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com