RISKIQ® partnered with Phantom™

Orchestrating Digital Risk Protection

Automate key tasks associated with triaging and understanding digital threats

As organizations continue to grow their digital presence, their security teams have to deal with exponentially more threats. To address them, security operations and analyst teams need access to details about threats and their associated infrastructure and then tools necessary to block and eliminate them.

RiskIQ provides access to internet-scale intelligence and insight into the connections between assets on the internet, giving security operations and analyst teams the information they need to understand suspicious activity and indicators of compromise (IOC) and identify the tactics, techniques, and procedures of adversaries.

Phantom automates and orchestrates incident response processes based on event enrichment provided by RiskIQ. Using Phantom playbooks, security operations teams can create custom, automated workflows to trigger IOC investigation, block threats and related infrastructure, and understand ownership of suspicious infrastructure.

Fig 1 - The above picture is showing a phantom playbook that is utilizing RiskIQ to enrich information that was initially observed by the organization's internal security products. The playbook performs analytics and data enrichment utilizing RiskIQ internet data sets. This allows for decisions to be made and the appropriate actions to be taken.

Integration Benefits

- Reduce the number of tools required to triage and mitigate risk
- Optimize operations and analysis processes within and between teams
- Automate the decision making and enrichment processes with no additional resources

About Phantom

Phantom is the leading Security Operations Platform. It integrates your team, processes, and tools together. Work smarter, respond faster, and strengthen your defenses with Phantom. Learn how at: https://phantom.us.

About RiskIQ

RiskIQ is the leader in attack surface management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. Learn how at: https://www.riskiq.com

Conclusion

Phantom allows for institutional knowledge to be preserved and automated. Seasoned analysts can create playbooks that utilize RiskIQ integration for their organization with confidence that junior analysts will perform security investigations more efficiently and at a higher skilled level.

RISKIQ®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com