

BRANDEFENSE AND THREAT INTELLIGENCE PRODUCT OVERVIEW

Phishing Monitoring • **Attack Surface** Brandefense offers phishing domain monitoring services to Application Service Management (ASM) help you protect your brand and which is a tech-update notification & customers from phishing attacks. attack-surface discovery platform. continuous monitoring of the internet for new domains related , to your brand and take action to have their takedown. Vulnerability Management ı Fraud Monitoring Vulnerability Management service periodically tests your infrastructure Obtain and respond against and web applications. You'll be fraudulent activities notified in case of any vulnerability so that you can take precautions without encountering an attack. Blackhole Engine **Threat Intelligence** closely related to the threats that your organization faces and

The tool gathers intelligence that is closely related to the threats that your organization faces and provides news and other different threat information to help your team get ready for the same threats. After the threat collection process, our technology enriches the data. Our Cyber Threat Intelligence Service generates early alarms for many kinds of attacks that ability to affect our customers through its network.

The Brand Monitoring service scans the internet constantly to find any shared, compromised, leaked data about your company. You will be aware of any situation that may harm your company's brand value.

Brand Monitoring

The tool gathers intelligence that is closely related to the threats that your organization faces and provides news and other different threat information to help your team get ready for the same threats. After the threat collection process, our technology enriches the data. Our Cyber Threat Intelligence Service generates early alarms for many kinds of attacks that ability to affect

our customers through its network.







VULNERABILITY ASSESSMENT AND PENETRATION

QT Global Software has a dedicated team to conduct comprehensive security assessments of systems, applications (web, desktop, cloud, and mobile), and network infrastructure to identify vulnerabilities and potential entry points for cyberattacks. Through rigorous testing methodologies in static/manual and dynamic ways, we simulate real-world attack scenarios to uncover security loopholes and various weaknesses and provide actionable security countermeasures and remediations to fortify the cyber defense through a defense-in-depth approach.



