LOOKINGGLASS

THIRD PARTY RISK MONITORING

PROTECT YOUR ORGANIZATION FROM VENDOR DATA BREACHES

Managing your organization's security posture is difficult without adding the complexity of third party vendors. Each third party opens the door for potential risk to your organization. As the list of vendors grows, exposure increases. Protecting this expanded attack surface requires expertise, infrastructure, and capabilities that few companies have the resources and budget to address.

LookingGlass™ Third Party Risk Monitoring is a cost-effective, risk-focused approach to managing and mitigating third party cyber risk. Our managed, continuous monitoring service includes human-review of all flagged incidents, as well as a point-in-time vendor risk report.

We enhance visibility into third party vulnerabilities by footprinting your third parties' networks to assess their cyber hygiene, such as open ports and misconfigured or expired certs – passively and unintrusively, without direct engagement with your third parties. Analysts use our dashboard to view risks so they can alert your security team of potential risks and suggest incident response - reducing time-to-action from 191 days[1] to a few, decisive moments.

Built-in reporting allows proper collection and easy metric delivery to organizational leaders, promoting visibility across the organization's security posture.

WHAT WE MONITOR

Structured Data:

- Malware hosting/distribution
- Virus/Botnet infection
- Command-and-Control activity
- Malicious/Scanning behavior
- Observed Spam
- Questionable Asset Use
- Phishing activity
- Emergent vulnerabilities
- Port and cert information

Unstructured Data:

- Reported breach of your vendor
- Suspicious domain registrations & spear phishing exposure

1 https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

FLEXIBLE DELIVERY OPTIONS

FEATURES	BENEFITS	SHARED SERVICE	HOSTED
Surface and Deep and Dark Web Data	Receive information from all corners of the Internet in a consumable and comprehensive product	✓	✓
Human-Vetting	Reduce false positives created by unvetted notifications	✓	✓
Port, Vulnerabilities, and Certification Information	Automatically monitor for inferred vulnerabilities, potentially open ports, and expired and/or misconfigured certificates	✓	✓
Near real-time alerting	Receive immediate notifications at time of discovery and continuously monitor all the items mentioned above, with customizable user and frequency settings	✓	✓
Baseline Attack Surface Report™	Historical look to establish a baseline for current security gaps	✓	✓
Threat Indicator Confidence™ (TIC) Score	Customizable scoring providing flexibility on what should/shouldn't trigger an alert	Not Customizable	✓
Service Manager	Have a question? Reach out to your service manager and ask	✓	✓
API Capabilities	Export data to consume elsewhere across your security organization	Not Available	

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass delivers unified threat protection against sophisticated cyber attacks for global enterprises and government agencies. Its comprehensive portfolio of managed services, threat platforms, machine-readable feeds, and automated threat response products – all supported by a global team of intelligence analysts – provides unprecedented visibility, response, and management of digital business risks. Prioritized, timely, and relevant cyber threat intelligence insights enable customers to take action across the different stages of the attack life cycle. Organizations of any size and level of security operations maturity leverage our 20+ years of tradecraft and investment in scalable, innovative solutions to protect their most valuable assets – brand, employees, customers, networks, and facilities.

Learn more at http://www.LookingGlassCyber.com