DARK WEB MONITORING AND THREAT EXPOSURE MANAGEMENT

Data sheet

Who is Flare?

Flare was founded to empower organizations to proactively detect and remediate exposure across the clear & dark web, providing organizations with the equivalent of an automated cyber reconnaissance team.

HOW IT WORKS

Flare acts as your business's digital security bloodhound, sniffing out threats lurking on the dark web. It scans for leaked credentials, stolen data, and suspicious activity, alerting you to potential breaches before they happen. This allows you to proactively address risks and make informed security decisions to protect your company's reputation and data.

BOOK A DEMO

CYBER RETALIATOR SOLUTIONS

www.CyberRetaliatorSolutions.com

IN-DEPTH DOMAIN MONITORING

Delivers the information analysts need to positively identify and action malicious domains including screenshots, favicon updates, SSL registration, and more.

LAYERED GITHUB LEAK DETECTION

Maps relations between different assets such as commits, users, domains, and repositories for precise identification of leaks.

AUTONOMOUS TAKEDOWNS

Effortlessly action takedown requests, streamline security operations, and reduce risk in a cost-effective model.

ROBUST INTEGRATIONS

Easily integrate with SIEM, SOAR, and ticketing systems for alignment with existing security workftows.

SIMPLE LICENSING

Unlimited users, full API access, and straightforward product options to suit business needs and minimize confusion.

USE CASES

- Safeguard sensitive data
- Maintain compliance
- Protect your developers
- Rapidly detect PHI leaks
- Map your external attack surface
- Monitor the dark web for threats
- Understand the Attack Surface
- Effective Prioritization and remediation of Security breaches
- Proactive Monitoring for effective identification of risks