STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

# Dark Web Scans and Threat Intel Monitoring

# Cyber Solutions: The Challenge

Data breaches, ransomware attacks, cyber targeting, and phishing campaigns can expose organizations to high levels of online risk and unintended data exposure across the open, deep, and dark web.

Scanning and monitoring to identify online vulnerabilities is critical to understanding your risk profile and protecting corporate assets.

| SOLUTIONS FOR THREAT INTELLIGENCE | SOLUTIONS FOR CYBER DUE DILIGENCE |
|---|---|
| We can conduct scans and monitoring following a breach, ransomware incident, phishing, or credential-stuffing attack, business email compromise, insider threat, or other types of security events involving leaked sensitive data. | We can assess the online exposure of entities involved in mergers and acquisitions, portfolio company scans, or third-party risk assessments for suppliers and vendors. |

## How We Help

We utilize custom tools, proprietary databases, and commercial repositories to search across TOR, I2P, and Freenet anonymous network protocols, ransomware group sites, underground forums and marketplaces, threat actor chatrooms, paste-and-dump sites, social media, and open sources. Search parameters are developed using keywords enumerated across corporate domains, subdomains, credentials, and internet-facing IP addresses.

- **Deep and Dark Web Scans** provide a one-time snapshot of an organization's externally facing risk exposure, including searches for indicators of compromise, exposed data, leaked credentials, targeted malware, and typo-squatting instances.
- Threat Intel Monitoring offers continuous monitoring to detect threats related to malicious targeting and other forms of online activity vulnerabilities.

## Why Work with Stroz Friedberg?

**Stroz Friedberg, a LevelBlue company**, can partner with your organization at every stage of your risk journey to help you make better decisions and achieve sustainable cyber resilience. With decades of combined experience managing cyber risk and responding to critical threats, our global team of experts assists organizations in making decisions with clarity and confidence in a complex risk environment.

The Intelligence Group includes experienced analysts with decades of expertise in threat intelligence and open-source research for both public and private sectors across North America, EMEA, and APAC.

We hold industry certifications that include CAMS, CFE, CISSP, CompTIA Security+, CompTIA A+, CREST, GSEC, GCIH, GPEN, GCTI, OSCP, OSWP, OSSTMM, and Pen Test+.

STROZ FRIEDBERG
A LevelBlue Company

# About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

**Cybersecurity. Simplified.**

**levelblue.com/strozfriedberg**