

DARK WEB MONITORING & DATA LEAKAGE

Keep your credentials off the dark web

Credentials, source code, and confidential files end up on the dark web every day. Styx Intelligence finds them before someone uses them against you, and covers exposure from your own cloud and code in the same view.

The threat landscape

Leaked credentials, proprietary code, and confidential files circulate on dark web forums and marketplaces, often for months before anyone notices. None of it requires a direct breach, just something of yours sitting where you're not watching.

The existing tools gap

Most teams find out about a leak after it's been used, and lean teams don't have the analyst hours to watch the dark web manually. Styx runs those scans continuously, so exposure is caught while there's still time to reset access or contain it.

CAPABILITIES

Everything of yours that leaks, watched in one place



Credential & financial exposure

Continuously monitors for exposed employee, executive, and customer credentials and stolen credit card numbers tied to your brand.

- Coverage across forums, breach dumps, and marketplaces
- Alerts include the source, affected account, and recommended action, such as a forced reset



Dark web forums & marketplaces

Tracks the criminal marketplaces, forums, and chat rooms where stolen documents, financial data, and corporate access are traded.

- Mentions of your brand, employees, or data flagged early
- Fraud and insider threats surfaced before they become incidents



Cloud & infrastructure exposure

Scans AWS, GCP, and Azure for exposed storage buckets, and flags misconfigurations and insider leaks before an attacker finds them.

- Publicly exposed cloud storage buckets
- Leaked internal configs, VPN details, secrets, and credentials



Proprietary data & IP leakage

Monitors code repositories, file-sharing platforms, and dark web forums so your competitive advantage doesn't leak unnoticed.

- Leaked source code and secrets committed to repositories
- Trade secrets and internal documents published where they shouldn't be

01

Reset access before it's exploited

Catching a stolen credential early means resetting access on your terms, not after an account takeover.

02

See the threat before it's a breach

Early visibility into what's already circulating turns a future incident into a threat you've handled.

03

Close exposure before attackers find it

An exposed asset will be found eventually. Closing the gap first means your team finds it, not an attacker.

CONNECTED IN STYX INTELLIGENCE

Iris AI Assistant · New

Ask plain-language questions about leaked credentials, exposures, and your risk posture.

Executive Protection

Monitor for leaked personal data, impersonation accounts, and targeted threats against your leaders.

Third Party Vendor Risk

See the external exposure of vendors and partners connected to your business.

Less risk, less manual work.

Styx watches the forums, marketplaces, and cloud surfaces your team can't monitor manually, and alerts you while there's still time to contain the exposure.

Talk to Us

styxintel.com



Dark Web & Data Leakage · Overview

Digital Risk Score **730**

DARK WEB — MARKETS, FORUMS & CHAT ROOMS

Monitored User Accounts
Emails seen in external sources

1,136

Credential Snippets
Passwords with identifiers

289

Data Breaches
Active campaigns detected

13

Other Mentions
Forums & marketplaces

3

DATA LEAKAGE — YOUR OWN INFRASTRUCTURE & CODE



Illustrative sample data