

BRAND MONITORING & PROTECTION

Prevent brand attacks from outside your perimeter

Lookalike domains, fake apps, and phishing pages are real threats to your brand. Styx Intelligence finds the external threats wearing your name and shuts them down before your customers, partners, or employees see them.

The threat landscape

Brand attacks don't stop at one channel. A lookalike domain feeds a phishing campaign, a rogue app collects credentials under your name, and a fake job posting harvests applicants' personal data. It's one connected threat surface.

The existing tools gap

Most vendors make you buy a separate tool for each threat type, and those tools stop at detection. Styx pairs AI-powered detection with analyst-backed takedowns, all in one platform.

Brand Protection · Overview

Digital Risk Score **333**

High Severity Findings
Requiring attention

33

Overall Findings
Requiring attention

158

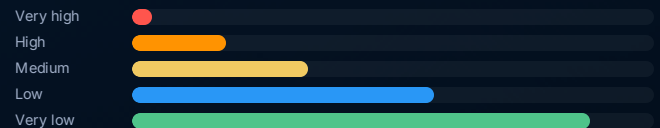
Suspicious Artifacts
On watchlist

781

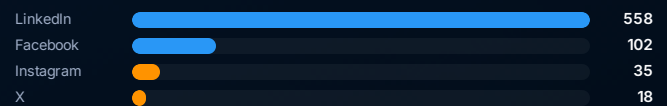
Response Actions
In progress / overall

21

DOMAIN IMPERSONATION — BY SEVERITY



IMPERSONATING ACCOUNTS — BY PLATFORM



Illustrative sample data

CAPABILITIES

Everything wearing your name, monitored in one place



Website & domain takedown

Finds phishing sites, lookalike domains, and clones of your legitimate site, then takes them down before a customer mistakes one for the real thing.

- Lookalike domains, cloned sites, and phishing infrastructure using your brand
- Counterfeit or unauthorized marketplace listings and misuse of your logos



Impersonation & social takedown

Removes fake social accounts impersonating your brand or executives before they're used in brand attacks.

- Coverage across LinkedIn, Facebook, Instagram, X, and other platforms
- Fraudulent job postings that misuse your company name to harvest applicant data



App & data exposure takedown

Identifies unauthorized apps distributing malware or stealing data under your brand, and acts on exposed sensitive information.

- Rogue mobile apps collecting credentials in your name
- Exposed sensitive data handled before it's used against you



Priority escalation

High-priority phishing and fraud cases skip the standard queue, so urgent threats never wait behind minor ones.

- Expedited takedown path for active phishing and fraud
- AI-powered detection with analyst triage before anything reaches remediation

01

One view of every external threat

Domains, social, disinformation, and exposed assets monitored from a single dashboard.

02

Cut response time from weeks to days

AI-powered takedowns and remediation workflows, with a dedicated analyst for complex threats.

03

Stop reacting, start prioritizing

Every threat is scored by risk, so your team focuses on what matters most.

CONNECTED IN STYX INTELLIGENCE

Iris AI Assistant · New

Ask plain-language questions about brand findings, impersonation, and takedown status.

Takedown Services

Automated and analyst-backed takedowns that remove what brand monitoring detects.

Disinformation Security

Track coordinated narratives targeting your brand, leaders, and customers before they spread.

Less risk, less manual work.

Styx replaces the patchwork of point tools and manual searching with one monitored view of everything wearing your name, plus the takedowns to shut it down.

Talk to Us

styxintel.com