

TAKEDOWN SERVICES

Detection flags threats. Takedowns remove them.

Fake domains, impersonation accounts, and rogue apps don't go away just because you found them. Styx Intelligence combines AI-powered workflows and analyst support to remove them.

The threat landscape

Every detected threat stays live and does damage until someone acts on it. These threats span your domains, social presence, app stores, and job boards at the same time, and each one keeps putting you at risk for as long as it's up.

The existing tools gap

Many tools stop at the alert. Acting on it means opening a case yourself, gathering evidence, and waiting while the threat stays live. Every Styx client gets a dedicated analyst who helps prioritize and take down active threats.

Takedown Services · Alerts

Open actions 21

CP-VR-4671	Lookalike domain registered Domain takedown · Open	CRITICAL	Aug 11
TP-HI-9	Phishing page cloning login Website takedown · Open	CRITICAL	Aug 09
CP-VR-4670	Fake support account removed Social takedown · Open	LOW	Aug 05
TP-HI-8	Unauthorized mobile app listing App takedown · Open	HIGH	Aug 04
CP-VR-4669	Unauthorized job posting Brand risks · Open	INFO	Jul 29

TAKEDOWN SUMMARY · CP-VR-4669

Status: Submitted to host

Detected	100%
Evidence gathered	82%
Takedown filed	58%
Content removed	26%

Recommendation: expedite removal request and continue monitoring for reposts of the same content.

Illustrative sample data

CAPABILITIES

Every active threat removed, tracked 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.

- Evidence gathered and takedowns filed with the host on your behalf
- Status of every case visible, so you always know where it stands



Impersonation & social takedown

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

- Fake support and executive accounts taken down
- Fraudulent job postings misusing your company name removed



App & data exposure takedown

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

- Rogue apps removed from official and third-party app stores
- 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.

- Dedicated analyst for complex and hard-to-remove threats
- Removed threats stay on watch, and reposts are actioned again

01

Protect customers from apps you didn't publish

Unauthorized apps impersonating your brand are removed before they spread malware or steal data.

02

Stop attackers from copying your site

Sites mimicking your domain are taken down before customers mistake one for the other.

03

Protect job seekers from fraud in your name

Fraudulent listings misusing your company name are removed before they hurt your reputation.

CONNECTED IN STYX INTELLIGENCE

Iris AI Assistant · New

Ask plain-language questions about open cases, takedown status, and active threats.

Brand Monitoring

Detects the fake domains, phishing pages, and brand misuse that feed straight into takedowns.

Social & News Monitoring

Flags impersonation accounts and fake profiles across social platforms for removal.

Less risk, less manual work.

Styx removes the manual chase of filing, escalating, and following up on takedowns, so detected threats actually come down.

Talk to Us

styxintel.com