TechOwl SHIELD

DATASHEET

TechOwl Shield Takedown Services

Safeguarding Your Digital Brand Presence
Across the Web, Social, and Cloud

Overview

In an era of rampant digital impersonation and cyber fraud, Techowl Shield's Takedown Services provide proactive monitoring and enforcement against any unauthorized, malicious, or infringing use of your brand, identity, or data. Our response team works globally to remove phishing websites, rogue applications, impersonating domains, fake social media profiles, code leaks, and more. .

Scope of Coverage

Channel	Examples
Websites	Phishing domains, website clones, fake login pages
Emails	Spoofed domains, phishing campaigns
Mobile Apps	Unauthorized Play Store / App Store listings, trademark-violating apps
Social Media & Professional Sites	Impersonation of executives, fake brand profiles, scam promotions
Public Repositories	Source code leaks on GitHub, Bitbucket, Pastebin
Cloud Storage	Leaked documents in "ready to download" public links

Scope of Coverage

Detection

Automated & manual brand monitoring using advanced threat intelligence and keyword logic.

Verification

Validation by Techowl's analyst team to confirm if content violates brand, copyright, or security.

Client Confirmation

Optional approval step before takedown (for sensitive cases).

Enforcement

Legal and technical removal using registrar, host, platform, or app store escalation.

Reporting & Closure

Incident report with timeline, evidence, case ID, and status provided.

SLA & Enforcement Commitment

Techowl commits to an annual ≥80% takedown success rate. Below is the detailed SLA matrix:

No.	Channel	Incident Type	Median Completion Time
1.	**Phishing Website**	Website clone or fake login	Within **3 business days**
		Phishing email campaign	Within **5 business days**
2.	**Website**	Copyright / IPR infringement	Within **7 business days** (IPR delays possible)
3.	**Social Media**	Brand impersonation, fake handles	Within **2-3 business days**
4.	**Mobile Apps**	Trademark-violating apps	Within **5-8 business days**
5.	**Code Repositories**	Public leaks (GitHub, Bitbucket, etc.)	Within **7 business days**
6.	**Professional Sites**	Fake executive or employee profiles	Within **10 business days**
7.	**Cloud Storage (Anonymous)**	Public breach links (read -to-download documents)	Within **7 business days**

Key Features

1. **Global Coverage**
   Works across all major platforms: web hosts, registrars, social networks,app stores, and more.

2. **Fast SLA Execution**
   Initiation within 2 hours for high-risk threats upon client confirmation.

3. **Confidential & Auditable**
   All takedown activity is logged, timestamped, and available in a downloadable report.

4. **Real-time Dashboard**
   View threat alerts, SLA timelines, evidence, and enforcement progress anytime.

5. **Email Alerts + Syslog Support**
   Integrate takedown events with your SIEM for central monitoring.

Sample Use Cases

Client Type	Use Case
Banking Institution	Daily phishing site takedowns and brand abuse cases targeting customers
E-commerce Platform	Takedown of fake coupon sites and fraudulent mobile apps
SaaS Provider	GitHub code leaks takedown and internal tool impersonation resolution
Media House	Removal of pirated content links and fake social pages

Why Choose Techowl Shield?

Features	Techowl Shield	Typical Provider
Takedown SLA Initiation	Within 2 hours	24–48 hours
Platform Coverage	7+ channel types	Limited (2–3 types)
Success Rate Commitment	≥80% yearly	No formal guarantee
Custom Rule Logic & Threat Tags	☑ Available	☒ Often Unavailable
Legal Template Support	☑ Included	☒ Extra or Unavailable
MSSP Integrations	☑ Syslog, API, Reports	☒ Rare