TechOwl SHIELD

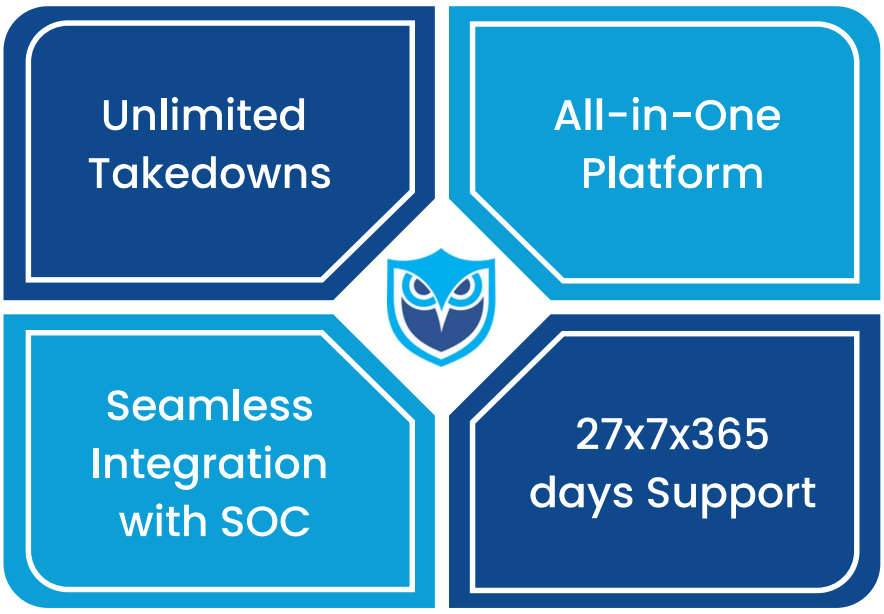
DATA SHEET

TechOwl SHIELD
Attack Surface Monitoring

Overview

TechOwl SHIELD is a comprehensive digital protection suite designed to safeguard brands and individuals from online threats. Leveraging advanced detection technologies and expert response teams, SHIELD monitors and mitigates risks such as impersonation, data leaks, brand abuse, and dark web exposure across digital platforms. From phishing takedowns to identity enforcement, Techowl SHIELD ensures robust defense in today's complex cyber landscape.

Notable Highlights



Brand Protection

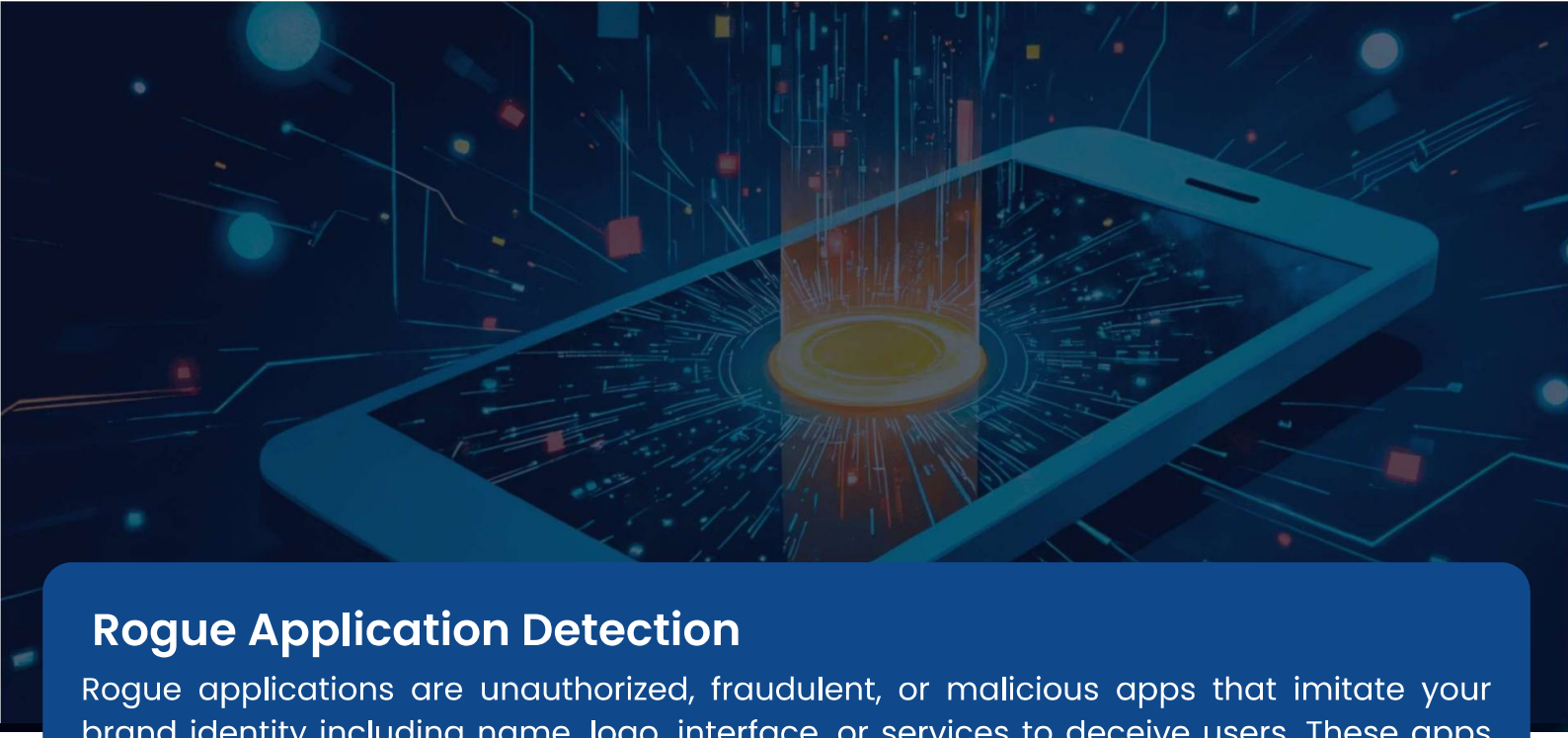
In today's digital landscape, your brand faces constant threats from fake apps and phishing sites to impersonated profiles. TechOwl SHIELD Brand Monitoring helps organizations proactively detect and eliminate such risks across the web, code repositories, and social media platforms to protect trust and reputation

Key Features

Rogue Application Detection	Tracks and flags unauthorized or fake mobile applications impersonating your brand.
Code Repository Scanning	Monitors platforms like GitHub, GitLab, Bitbucket for exposed code, credentials, or sensitive brand assets.
Phishing Domain Monitoring	Identifies domains mimicking your website or brand name to deceive users.
Keyword Threat Monitoring	Detects risky mentions of your brand, product, or executive names across public and semi-public sources.
Social Media Threat Detection	Spots fake profiles, impersonated pages, or posts abusing your brand identity.
Website Impersonation Watch	Finds lookalike websites designed to mislead customers or partners.

Use Case

An international organization uncovered a rogue mobile app and a phishing domain that were misleading its customers and partners. Thanks to TechOwl SHIELD Brand Monitoring, the malicious app was swiftly removed from the web, while the phishing domain was disabled through a coordinated takedown. Real-time alerts enabled the organization to promptly issue public warnings, reinforcing digital trust and protecting its reputation from further damage



Rogue Application Detection

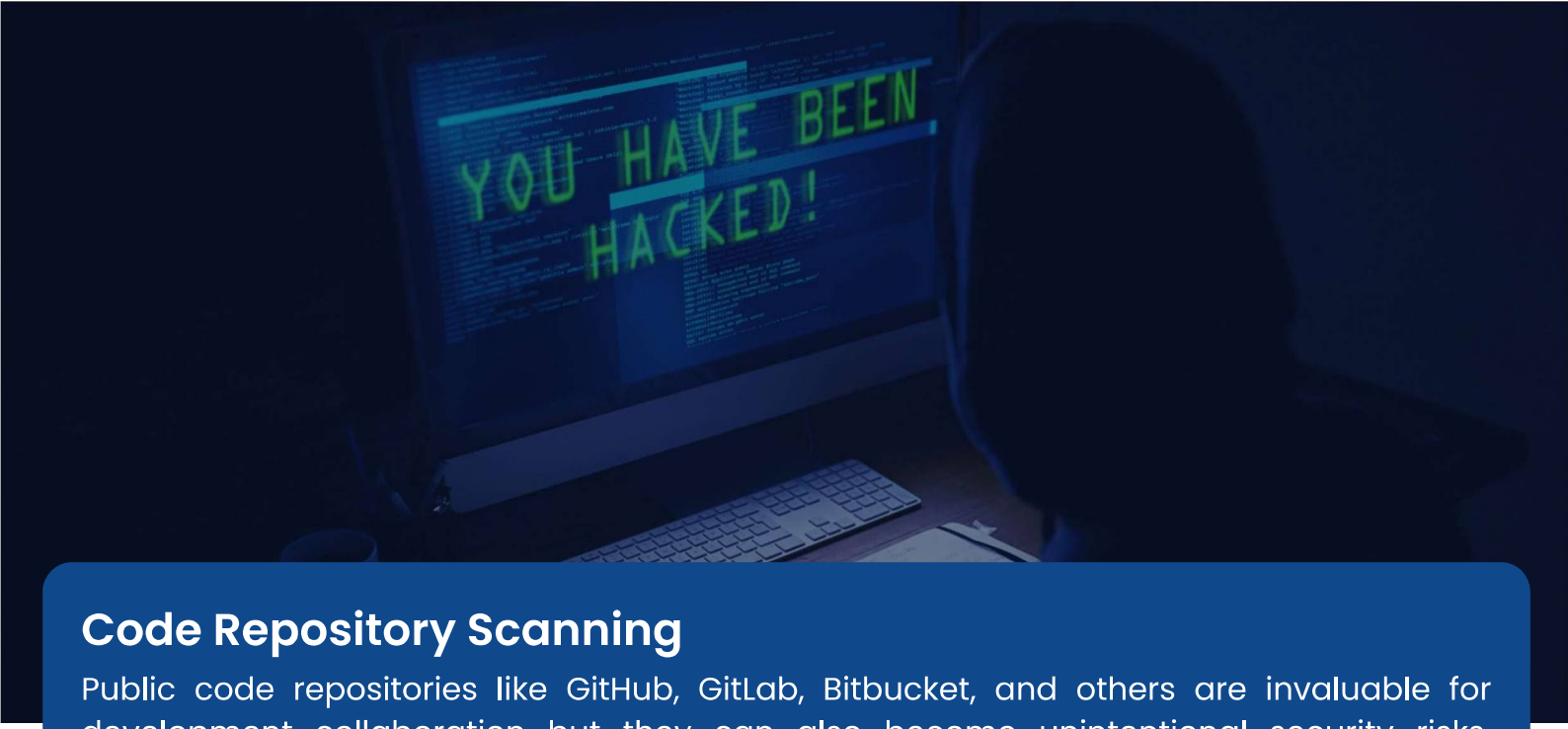
Rogue applications are unauthorized, fraudulent, or malicious apps that imitate your brand identity including name, logo, interface, or services to deceive users. These apps are often distributed via third-party app stores, lesser-known Android markets, or sometimes even official platforms like Google Play and Apple App Store. Their intent ranges from phishing and malware distribution to financial scams and surveillance. Since mobile apps are a primary touchpoint for users today, the presence of a rogue app can significantly erode trust and cause irreversible brand damage.

Associated Threats:

- Unauthorized use of brand assets
- Malware injection and credential harvesting
- Customer data theft and financial fraud
- Drastic loss of brand reputation and trust
- Legal and regulatory liabilities

How TechOwl SHIELD Helps:

TechOwl SHIELD scans hundreds of app marketplaces, global, regional, and unofficial to identify apps mimicking your brand. Our intelligent detection engine flags rogue applications using visual, metadata, and code-level indicators. With Unlimited Takedowns, we go beyond detection: our team initiates and follows through on legal and procedural takedowns globally, ensuring these malicious apps are removed swiftly and without limit so your brand remains uncompromised.



Code Repository Scanning

Public code repositories like GitHub, GitLab, Bitbucket, and others are invaluable for development collaboration but they can also become unintentional security risks. Developers often accidentally commit sensitive credentials, API tokens, or proprietary logic to these platforms. In other cases, attackers may create fake repositories or fork your code to distribute malware. These exposures, when linked to your brand, can be exploited by cybercriminals to gain network access, tamper with code, or launch supply chain attacks.

Associated Threats:

- Hardcoded credentials and API key leakage
- Unauthorized access to internal systems
- Malicious forks or fake dev repos
- Backdoors introduced into the supply chain
- Compromised developer trust

How TechOwl SHIELD Helps:

TechOwl SHIELD performs deep scanning across all major public code repositories, monitoring for your brand mentions, project forks, and sensitive data leaks. Our AI-drivenengine detects exposure patterns (like AWS keys, SSH passwords, etc.) and alerts you instantly. We also offer takedown coordination and remediation guidance to prevent exploitation.

Phishing Domain Monitoring

Phishing domains are fraudulent web addresses crafted to resemble your company's legitimate websites. These domains are often used in deceptive email campaigns or search engine traps to lure users into entering personal, financial, or login information. Cybercriminals may tweak characters (e.g., amazon.com, google.net) or register similar looking domains to carry out scams. These domains tarnish your online reputation and directly affect customer security.

Associated Threats:

- Fake login pages for credential harvesting
- Malware distribution and scam pages
- Loss of SEO performance and domain reputation
- Legal or customer service fallout
- BEC (Business Email Compromise) via spoofed domains

How TechOwl SHIELD Helps:

TechOwl SHIELD monitors DNS registrations, WHOIS data, and MX record to proactively detect suspicious or lookalike domains related to your brand. Our real-time alerts and threat categorization ensure swift visibility. With Unlimited Takedowns included, our team collaborates with domain registrars, hosting providers, and CERT authorities worldwide to remove phishing domains as many times as needed protecting your digital perimeter without additional costs or restrictions.

Keyword Threat Monitoring

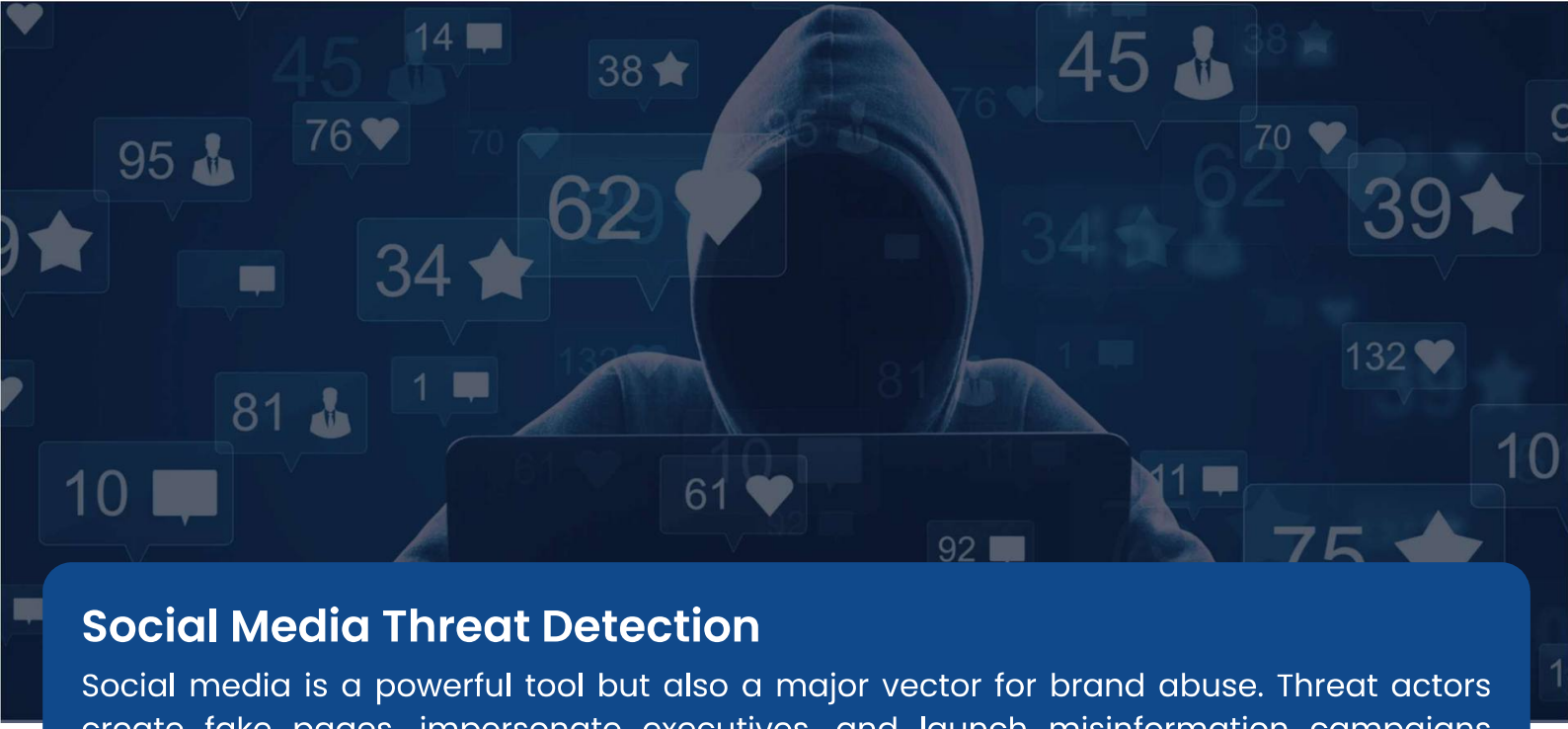
Your brand name, products, and executive identities are often discussed on various platforms including underground forums, surface web chatter, social media, and dark web markets. These keyword mentions may be the first indicator of targeted attacks, impersonation plans, or scam campaigns. Monitoring this chatter provides an early warning system against upcoming cyber threats or brand misuse.

Associated Threats:

- Identity theft or impersonation attempts
- Threat actor planning and targeting discussions
- Fake listings of products or services under your name
- Negative publicity or black hat SEO campaigns
- Precursor signals to cyberattacks

How TechOwl SHIELD Helps:

Our platform scans millions of indexed pages across the open, deep, and dark web using proprietary keyword detection algorithms. You can define custom watchlists for brand names, executive identities, or critical product terms. SHIELD provides contextual analysis, source details, and risk scoring — enabling your teams to respond before the threat escalates.



Social Media Threat Detection

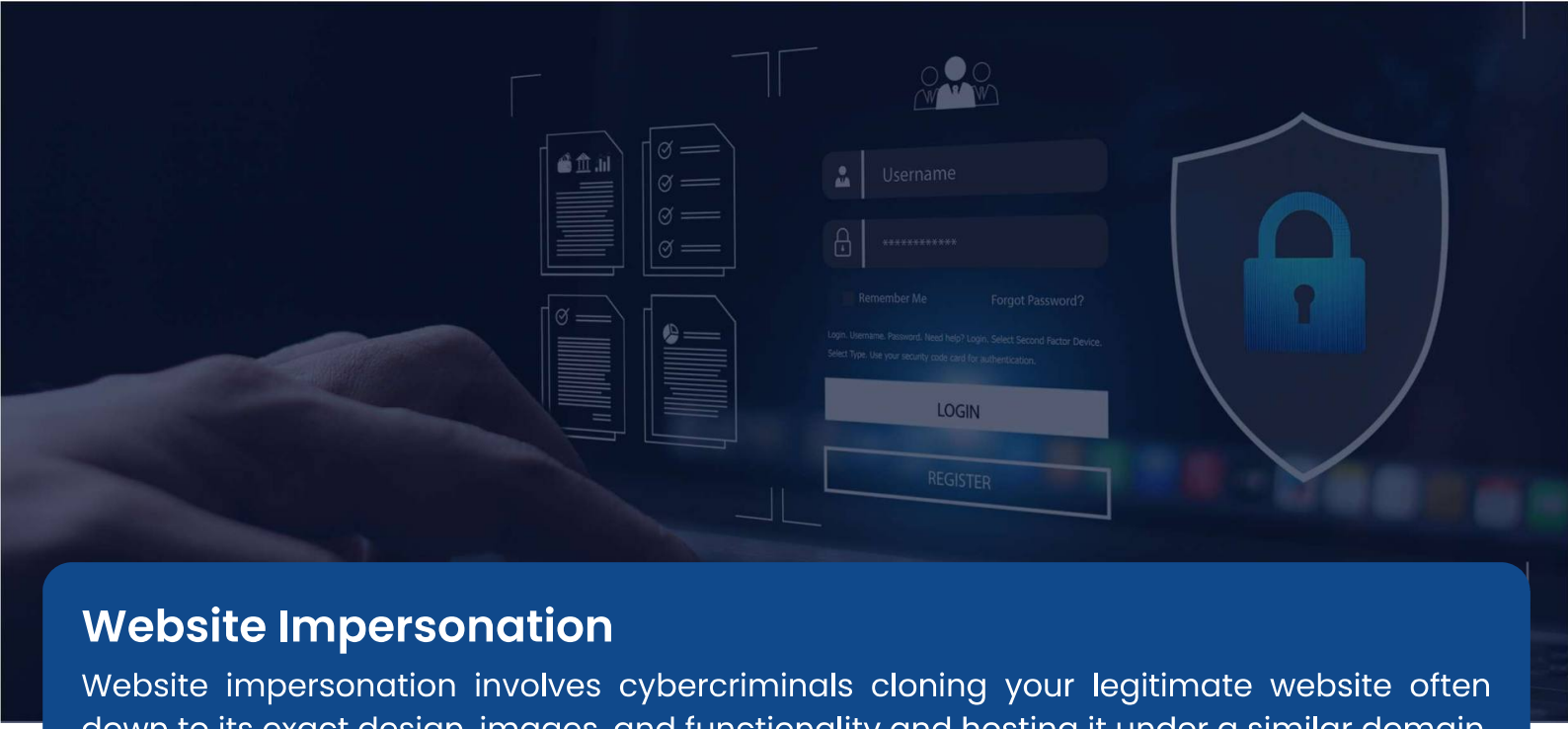
Social media is a powerful tool but also a major vector for brand abuse. Threat actors create fake pages, impersonate executives, and launch misinformation campaigns across platforms like Facebook, Instagram, Twitter, LinkedIn, and YouTube. These impersonations not only deceive customers but can also trigger compliance issues, scams, and coordinated reputational attacks.

Associated Threats:

- Executive impersonation and CEO fraud
- Fake job postings or scam giveaways
- Counterfeit product promotions
- Viral misinformation that harms your brand
- Misuse of customer queries for phishing

How TechOwl SHIELD Helps:

TechOwl SHIELD continuously monitors platforms like LinkedIn, Facebook, Instagram, Twitter, and emerging social channels for brand abuse, fake accounts, and harmful mentions. When malicious content is found, our platform not only notifies you but also initiatesUnlimited Takedowns submitting verified abuse claims and coordinating directly with social media platforms to remove impersonations, scams, or counterfeit content at scale, without limitation.



Website Impersonation

Website impersonation involves cybercriminals cloning your legitimate website often down to its exact design, images, and functionality and hosting it under a similar domain. These cloned sites are used to phish users, distribute malware, or host fake login portals. Such threats often bypass traditional security tools and lead to direct losses in customer data, revenue, and brand credibility.

Associated Threats:

- Cloned websites used for phishing
- Harvesting of user credentials
- SEO attacks through duplicate content
- Fake job portals or support pages
- Legal and compliance complications

How TechOwl SHIELD Helps:

TechOwl SHIELD uses website fingerprinting technology to detect lookalike and cloned versions of your domain. We continuously monitor changes in favicon, content layout, JS structures, and hosting data to uncover impersonation attempts. Once detected, we provide detailed forensic insights and initiate rapid takedown through legal, CERT, and hosting channel coordination.