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

- Unlimited Takedowns
- All-in-One Platform
- Seamless Integration with SOC
- 27x7x365 days Support

Security Assessment

Your digital perimeter is only as strong as its weakest link. Misconfigured apps, forgotten subdomains, and exposed ports create silent vulnerabilities. TechOwl SHIELD's Security Assessment offers continuous, non-intrusive monitoring to identify gaps before attackers do.

Key Features

Vulnerability Detection	Identify known CVEs, unpatched services, and outdated software across exposed assets.
Open Port Discovery	Discover and analyze open ports that could act as entry points for attackers.
Application Misconfiguration Scanning	Detect common mistakes like exposed admin panels, default credentials, or missing headers.
SSL/TLS Health Check	Ensure HTTPS configurations are secure with valid certificates, proper cipher suites, and no deprecated protocols.
Dead Domain Monitoring	Detect unused or expired domains/subdomains that could be hijacked or abused for phishing.

Use Case

A company unknowingly left an old, unused subdomain pointing to their live infrastructure, an oversight that could have allowed attackers to hijack the subdomain for phishing, malware delivery, or brand impersonation. Fortunately, TechOwl SHIELD's continuous domain monitoring identified this takeover risk early. By flagging the vulnerable subdomain in time, SHIELD enabled the organization to decommission it before it could be exploited, effectively preventing a potential security incident and safeguarding the company's brand reputation.

Vulnerability Detection

Vulnerabilities are flaws or weaknesses in systems, applications, or software code that attackers can exploit to compromise the confidentiality, integrity, or availability of data. These can arise from outdated software versions, unpatched security flaws, misconfigurations, or insecure coding practices. In enterprise environments, even a minor vulnerability can provide a foothold for an attacker to infiltrate deeper systems. Exploitable vulnerabilities are often cataloged in public databases like CVE, making them low hanging fruit for cybercriminals. Regular assessment and patching are critical to maintain a strong security posture.

Associated Threats:

- Remote code execution and system compromise
- Privilege escalation and lateral movement
- Data breaches via known CVEs
- Regulatory non-compliance (e.g., OWASP Top 10)

How TechOwl SHIELD Helps:

TechOwl SHIELD performs comprehensive vulnerability scanning across your infrastructure and applications, correlating findings with CVE databases and real-time threat feeds. We prioritize vulnerabilities based on severity and exploitability, offering tailored remediation steps. This proactive detection helps organizations patch issues before they are exploited. SHIELD also integrates with your existing systems for timely alerting and status tracking. Our reports are aligned with regulatory frameworks like OWASP Top 10 and PCI-DSS, helping you stay compliant.

Open Port Discovery

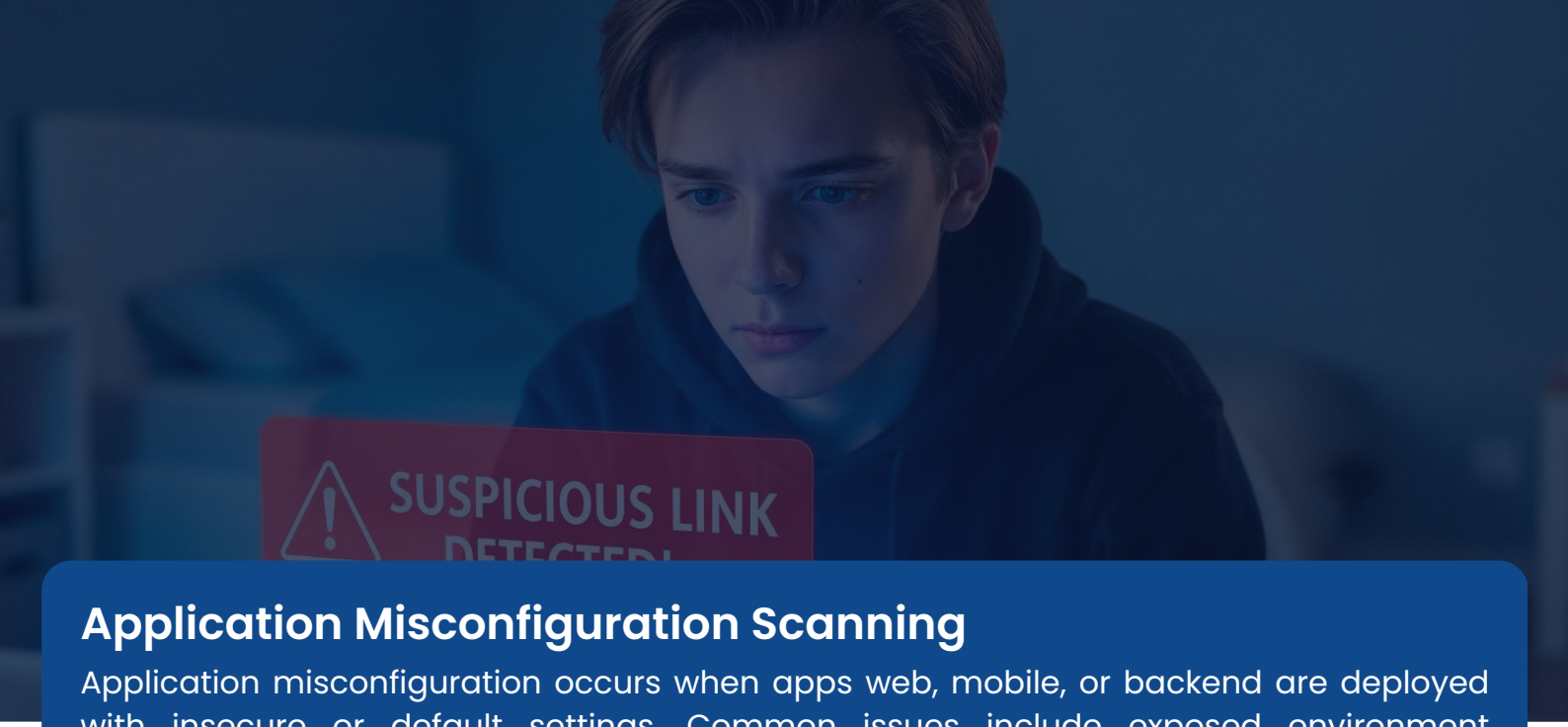
Open ports are communication gateways that allow external access to services running on your systems. While necessary for legitimate services like web servers or email, open ports can be exploited if improperly secured or unnecessary. Attackers routinely scan the internet for open ports to identify vulnerabilities or poorly protected services. Exposed services like RDP, FTP, or database ports can become easy entry points for brute-force attacks or malware injection. Unmanaged open ports significantly widen the organization's attack surface.

Associated Threats:

- Unauthorized access to internal systems
- Exposure of sensitive services (e.g., RDP, SSH, databases)
- Lateral movement within the network
- Reconnais-sance and enumeration attacks

How TechOwl SHIELD Helps:

TechOwl SHIELD continuously scans your public-facing IP addresses and cloud assets to detect open, unprotected, or misconfigured ports. We identify risky exposures such as exposed admin consoles or unused legacy services and provide recommendations to restrict or close them. Our platform also monitors for changes in port status to detect unauthorized modifications. This real-time visibility allows IT teams to respond swiftly, harden perimeter security, and reduce the likelihood of external compromise.



Application Misconfiguration Scanning

Application misconfiguration occurs when apps web, mobile, or backend are deployed with insecure or default settings. Common issues include exposed environment variables, verbose error messages, directory listings, and lack of authentication on sensitive endpoints. Such misconfigurations are frequently exploited by automated tools and attackers during reconnaissance. These flaws are among the OWASP Top 10 security risks and often stem from lack of security validation during deployment or CI/CD pipelines.

Associated Threats:

- Data leakage and unauthorized access
- Exposure of API keys, credentials, and admin panels
- Bypass of authentication and access controls
- Increased likelihood of automated attacks (e.g., bots)

How TechOwl SHIELD Helps:

TechOwl SHIELD audits your applications for common misconfigurations, including overly permissive CORS settings, missing security headers, open debug panels, and exposed admin interfaces. Our scanner simulates attacker behavior to identify weak spots and offers clear, actionable remediation steps. This helps development and DevSecOps teams fix issues early in the lifecycle. SHIELD also supports recurring scans post-deployment to ensure changes or updates don't introduce new misconfigurations.

SSL/TLS Health Check

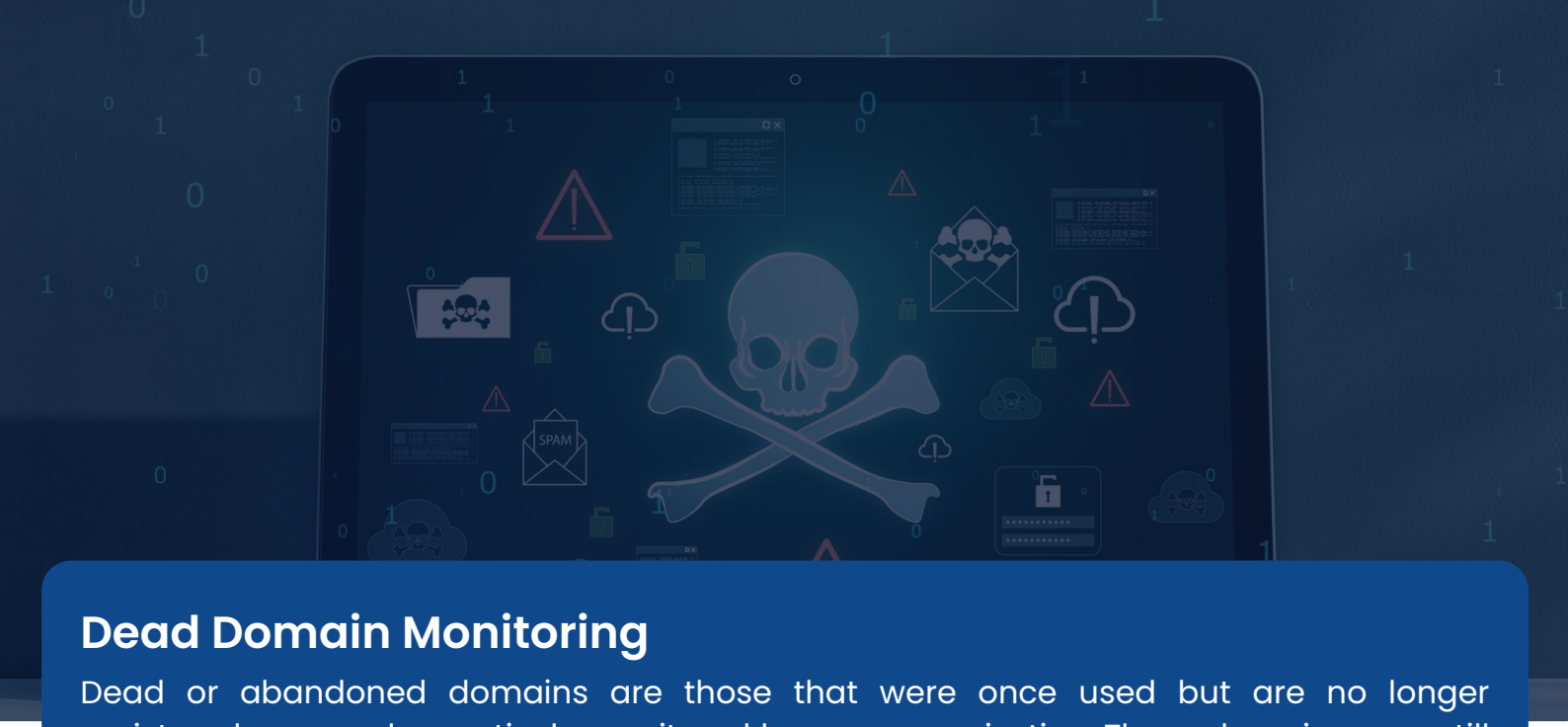
SSL certificates (now typically TLS) are vital for encrypting data between users and services. Expired, weak, or misconfigured SSL certificates not only pose security risks but also affect customer trust and service availability. Insecure protocols, deprecated cipher suites, or weak key lengths can be leveraged in man-in-the-middle (MitM) attacks. Google Chrome and other browsers now actively block or warn users when encountering insecure SSL configurations.

Associated Threats:

- Data interception via Man-in-the-Middle (MitM) attacks
- Loss of user trust due to certificate errors
- Downtime and service disruption
- Non-compliance with data protection standards

How TechOwl SHIELD Helps:

TechOwl SHIELD automatically scans your domains and subdomains for SSL issues. We check for expired certificates, weak encryption standards, incorrect hostname bindings, and outdated TLS versions. Our reports provide a risk-based breakdown of issues and industry best practices for correction. SHIELD also tracks renewal cycles, helping your team avoid unexpected expiries that can lead to website outages or loss of user trust. This ensures secure communication and compliance with standards like PCI-DSS and GDPR.



Dead Domain Monitoring

Dead or abandoned domains are those that were once used but are no longer registered, renewed, or actively monitored by your organization. These domains may still be linked in third-party systems, emails, or digital infrastructure, making them prime targets for domain hijacking. Attackers can re-register these domains and use them for phishing, malware delivery, or impersonation of your brand. This is a common tactic for social engineering campaigns targeting your employees or customers.

Associated Threats:

- Brand impersonation and phishing attacks
- Spoofing of legacy communication channels
- DNS hijacking and redirection to malicious sites
- Loss of control over historical assets

How TechOwl SHIELD Helps:

TechOwl SHIELD keeps an active watch on all domains associated with your brand, including those that have expired or are nearing expiry. We alert you if any are re-registered by unauthorized entities or show signs of misuse. Our platform also helps you maintain an updated domain inventory and guides you on reclaiming or securely retiring legacy assets. This mitigates the risk of impersonation, spoofed communication, and brand reputation loss.