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

Dark Web Threats

The dark web is a breeding ground for leaked corporate credentials, sensitive data, and insider information, often traded or sold without your knowledge. TechOwl SHIELD's Dark Web Monitoring keeps a constant watch, identifying and alerting you to any data leak tied to your organization before it's weaponized.

Key Features

Credential Exposure Monitoring	Tracks exposed email IDs, usernames, and passwords.
Infected System Monitoring	Monitor organization-specific compromised devices.
Deep & Dark Web Coverage	Leverages crawlers and intel feeds across hard-to-reach sources.
Card Leaks	Monitor Credit card and Debit card leak over the darkweb

Use Case

A technology company unknowingly had its employee credentials leaked on a hacker forum after a phishing campaign. With TechOwl SHIELD's Dark Web Monitoring, the breach was flagged in real-time. The security team quickly reset exposed credentials, enforced MFA, and launched awareness training neutralizing the threat before any damage occurred.

Credential Exposure Monitoring

Credential leaks involve the exposure of employee or customer usernames, passwords, and email addresses typically obtained through data breaches, phishing, or malware infections.These credentials are often sold, traded, or dumped on dark web marketplaces, paste sites, and breach forums. Attackers use them to gain unauthorized access, initiate account takeovers, or move laterally across systems using password reuse.

Associated Threats:

- Account Takeover (ATO) attacks
- Business Email Compromise (BEC)
- Data theft and lateral movement inside networks
- Identity fraud and impersona -tion
- Credential stuffing attacks using leaked logins

How TechOwl SHIELD Helps:

TechOwl SHIELD continuously monitors breach dumps, pastebins, darknet markets, and leak forums for exposed credentials linked to your domains and employees. Our automated engine validates data (e.g., hash types, passwords) and alerts your security team in real-time. Each leak is enriched with breach source, timestamp, and exposure details enabling quick mitigation like password resets, MFA enforcement, and SOC response.

Infected System Monitoring

Infected systems are organizational assets (devices, IPs, endpoints) compromised by malware, bots, RATs (Remote Access Trojans), or ransomware often part of command and control (C2) networks. These infected machines are commonly observed through malware telemetry, dark web logs, and threat actor infrastructure dumps.

Associated Threats:

- Active malware infections and data exfiltration
- Inclusion in botnets or DDoS attacks
- Persistent backdoors for future intrusions
- Ransomware triggers or extortion threats
- Reputational damage and compliance violations

How TechOwl SHIELD Helps:

TTechOwl SHIELD correlates telemetry data from threat feeds, dark web marketplaces, sinkhole traffic, and blacklists to detect infected endpoints tied to your organization's IPs orinfrastructure. We provide details like malware path, infection timestamp, and geo-location, Host name, OS used empowering your security teams to isolate and remediate infected systems before they escalate.

Deep & Dark Web Coverage

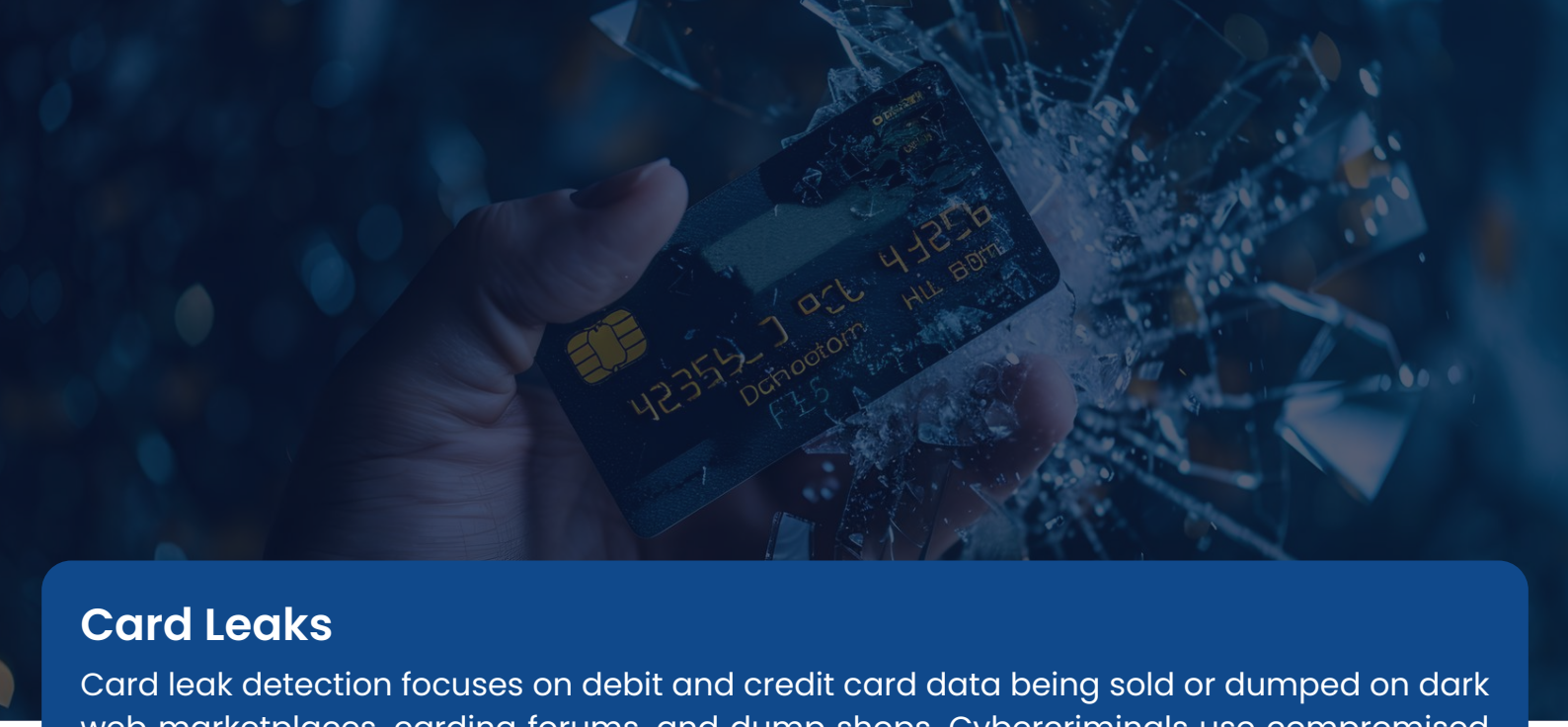
Dark Network Monitoring involves surveillance of underground chat forums, encrypted messaging boards (e.g., Telegram, IRC, XMPP), and darknet marketplaces where threat actors collaborate, trade exploits, and plan attacks. Discussions referencing your company, executives, assets, or digital footprint often precede targeted cyberattacks.

Associated Threats:

- Targeted ransomware or phishing campaigns
- Sale of internal access or credentials
- Infrastructure targeting (IP leaks, VPNs, portals)
- Brand and executive-specific threats
- Zero-day targeting or exploit trading

How TechOwl SHIELD Helps:

TechOwl SHIELD passively monitors hundreds of invite-only hacker forums, encrypted groups, and darknet marketplaces. Using AI-powered NLP and threat modeling, we flag anyconversation where your brand, executives, domains, or IPs are mentioned. Each alert comes with full context (actor profile, thread history, language translation) providing early warning before an attack is launched.



Card Leaks

Card leak detection focuses on debit and credit card data being sold or dumped on dark web marketplaces, carding forums, and dump shops. Cybercriminals use compromised PoS terminals, skimming devices, phishing kits, and data breaches to steal cardholder information. BIN-based monitoring lets banks proactively detect if cards issued under their bank identification numbers are part of any dark web sale.

Associated Threats:

- Financial fraud and unauthorized transactions
- Massive cardholder data exposure
- Regulatory penalties and PCI-DSS violations
- Trust erosion among banking customers
- Increase in fraud reimburse-ments and chargebacks

How TechOwl SHIELD Helps:

Exclusively for banks and NBFCs, TechOwl SHIELD offers BIN-based monitoring, where your issued BIN ranges (first 6–8 digits of card numbers) are continuously tracked across dark web sources. When card data matching your BINs is found, we provide actionable intelligence,including dump site source, compromised data (CVV, expiry, ZIP), and exposure level. Our insights help fraud prevention teams respond faster, block affected cards, and notify customers if needed.