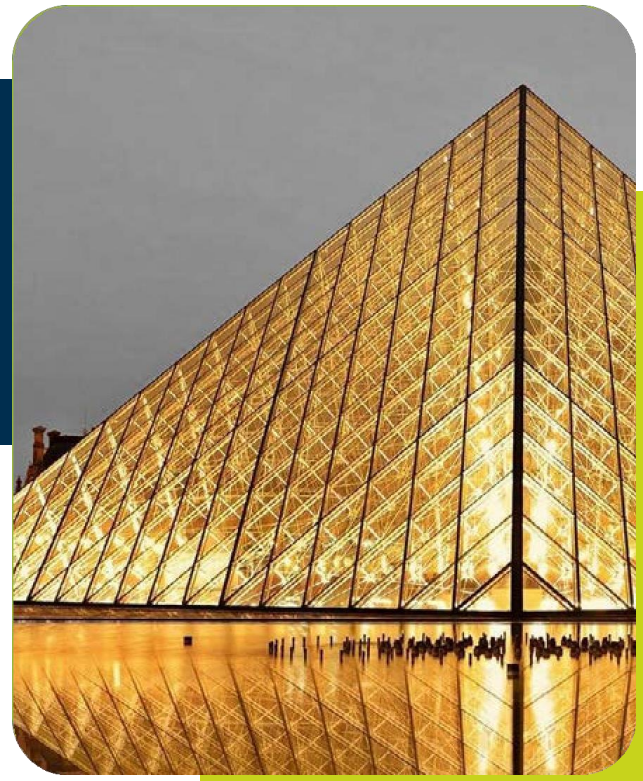
DARKIVORE

BY POTECH

WE ARE **A CYBERSECURITY TECHNOLOGY VENDOR** WITHIN THE POTECH GROUP.

Headquartered in Paris, France. Our mission it to empower organisations with the tools and expertise to navigate the complex digital landscape with confident



DARKIVORE
BY POTECH

Thidesoft offers TACIVOAR, DARKIVORE and OCTIVORE, three engineering masterpieces that harness AI, Machine Learning, and cutting-edge technology to protect internal & cloud assets, hunt the web for potential threats targeted at businesses, and respond to security incidents.

DISARM CYBERTHREATS AT THE SOURCE

Cutting-edge comprehensive Cyberthreat Intelligence and Digital Risk Protection Platform

KNOWLEDGE, AT THE FIRST LINES OF DEFENSE

A SIEM++ solution, empowering organizations by allowing them full control of their IT and Cloud infrastructures.

NEXT GENERATION SIRP SOLUTION

A scalable SIRP platform with the OMNI-reach needed to deal with a barrage of security incidents that require immediate attention

CHAT ROOMS & MESSAGING APP

EXPOSED CLOUD ASSETS

PHISING FORMS

DOMAIN NAME SERVERS

SOCIALMEDIA & DEEPFAKES

DARK WEB MARKETPLACES

HACKER SPACES/FORUMS

DARKIVORE

BY POTECH

Darkivore is a cutting-edge Cyber Threat Intelligence and Digital Risk Protection platform designed to proactively neutralize cyber-attacks such as data breaches, brand impersonation, and phishing scams.

IMPERSONATION & SOCMINT

Leverage Social Media Intelligence (SOCMINT) to eliminate risks of VIP/brand impersonation, scams, account takeovers, and fraud attempts.

TACTICAL CYBERTHREAT INTELLIGENCE

Gather indicators from open-source intelligence (OSINT) major threat feeds, CSIRT advisories, and deep/dark web platforms to counter potential harmful events targeting the organization.

ATTACK SURFACE & VULNERABILITY INTELLIGENCE

Automate Passive Recon and Enumeration process to quantify and reduce the attack surface while identifying threat vectors or vulnerabilities that affect your organization.

COPYRIGHT AND TRADEMARK

Neutralise any infringement of copyright and trademark, whether targeting brand images, media content, or exclusive services and products.

3RD PARTY CLOUD AND SECURITY

Map and protect large amounts of data stored with third parties, software (Saas) providers, and cloud computing platforms.

DIGITAL FOOTPRINT PROTECTION

Safeguard digital footprints, both passive and active. By identifying and cleansing these traces, protect against reputational costs, identify theft, business email compromise (BEC), and spamming.

ANTI-PHISHING

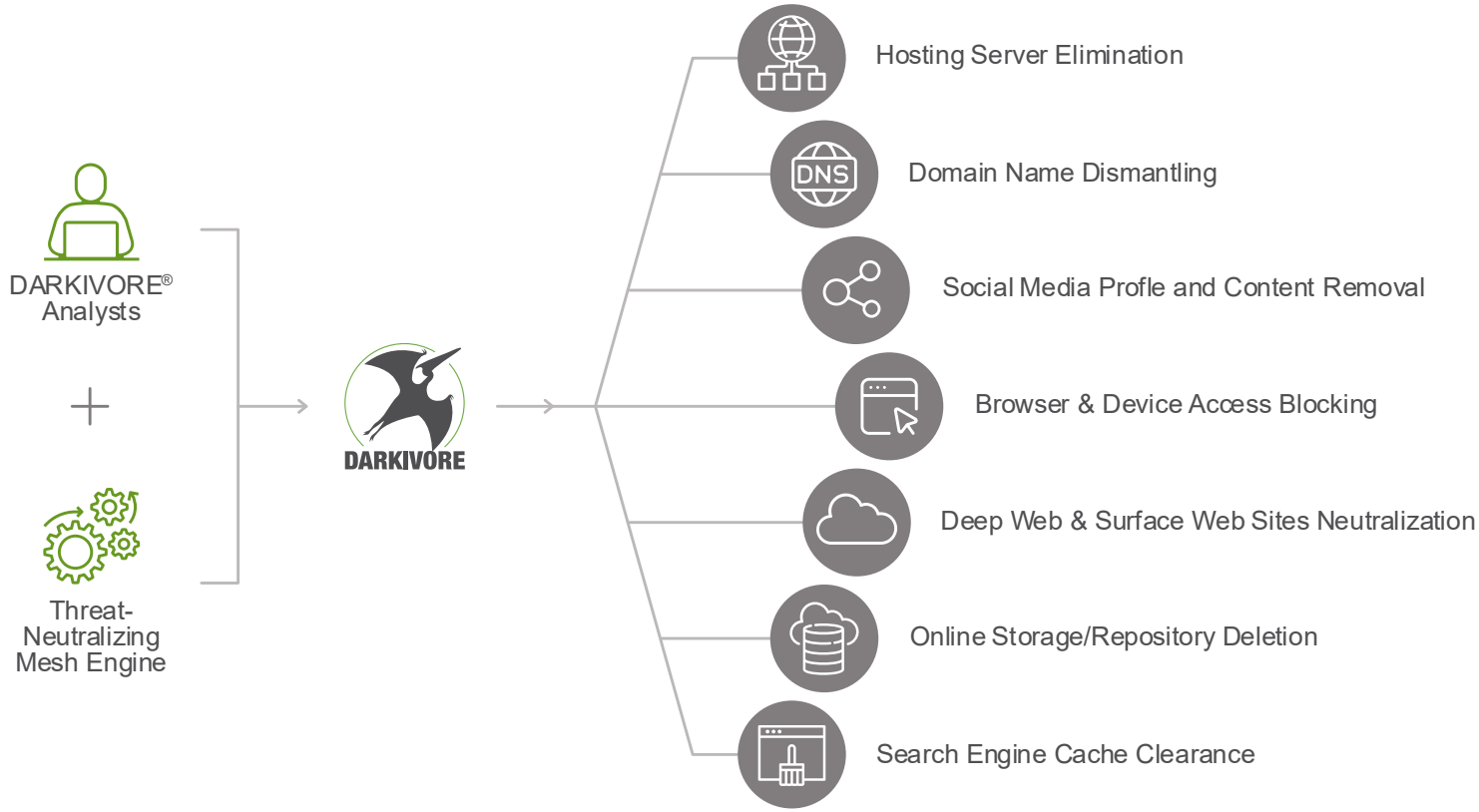
Detect, analyze, and take down phishing domains, bogus apps, spooled subdomains, and fake web forms to protect our human factor in addition to your customers data.

DATA BREACH PROTECTION

Monitor the deep and dark web for leaks retrieving compromised and sensitive information such as credentials stuffing, financial leaks, credit card data, source codes, and configuration files relevant to your business.

DARKIVORE® leverages active takedown services (on hourly, daily and weekly basis) to eradicate external threats targeting organizations.

This is done while covering a wide spectrum of threat sources, events and behaviors including illegitimate impersonation, malicious content, phishing, fake domains, social media scams and attackers' infrastructure.



DARKIVORE IN NUMBERS

+20,000
Prevented data breaches

15%
Increase in average business valuation

DARKIVORE
BY POTECH

+150,000
Yearly takedowns, potential threats neutralized

$2.31M
Average Cost of Fraud prevented

$450M
Avoided potential damages from data leakage and cyber attacks

95%
Reduction in threats

FULL LICENSE - FEATURES

This all-in-one license integrates full-spectrum intelligence services with a robust suite of breach, incident, and takedown response capabilities, providing complete protection for your brand, digital assets, and online presence .

DIGITAL RISK PROTECTION

BRAND PROTECTION

- IMPERSONATION & SOCMINT
- COPYRIGHT & TRADEMARK
- DIGITAL FOOTPRINT PROTECTION
- ANTI-PHISHING

ATTACK SURFACE & THREAT INTELLIGENCE

- DATA BREACH PROTECTION
- 3RD PARTY & CLOUD SECURITY
- ATTACK SURFACE & VULNERABILITY INTELLIGENCE
- TACTICAL CYBER THREAT INTELLIGENCE

DARKIVORE BY POTECH

FEATURES	DARKIVORE	SOCRADAR	CROWDSTRIKE	ZEROFOX	RECORDER FUTURE	CYBELANGEL	BLUELIV
PHISHING DOMAIN PROTECTION	✓	✓	Limited (cyber-squatting)	✓	Limited (newly created domains)	✓	✓
DATA LEAKAGE DEEP & DARK WEB SCAVENGING	✓	✓	✓	✓	✓	✓	✓
SUBDOMAIN SPOOFING DEFACEMENT WHALING / ONLINE FORM	✓	Limited	✗	✓	✓	✗	✗
SOCIAL MEDIA COVERAGE	✓	Limited reference to official content	Limited (focused on official referenced content)	✓	Limited local & regional social media presence	✗	limited focused on official references, lack of regional social media
UNLIMITED TAKEDOWN	✓	Limited	✗	Limited cost /takedown	Limited response time & frequency latency	Limited social media coverage	Limited no takedown service specified
TRADEMARK & COPYRIGHT (FOR E-MARKETPLACES)	✓	Limited to darkweb marketplace	Limited to darkweb marketplace	✓	Limited to darkweb marketplaces	✓	Limited to social media
MOBILE ROGUE APPS	✓	✓	Limited	✓	Limited direct monitoring of official app stores	✗	✓
ATTACK SURFACE MANAGEMENT	✓	✓	✓	✓	✓	Limited	✗

CASE STUDIES

// SUCCESS STORY : AUSTRALIAN SCHOOL

IMPERSONATION, IDENTITY THEFT, CYBERBULLYING

PROBLEM

1. A group of students at an Australian school created TikTok videos impersonating teachers and classmates as a prank.
2. The situation escalated into a cyberbullying campaign, with fake profiles spreading misinformation.
3. Cybercriminals exploited the chaos by creating fraudulent websites to steal personal data from parents and users.
4. The school struggled to manage the growing digital threats as traditional reporting methods were ineffective.

ACTION PLAN

DARKIVORE

Darkivore took control of the situation – stopping it before it worsened:

1. **Tracked impersonation attempts** and identified fake accounts in real time.
2. **Took down fraudulent websites** and removed malicious content from social media.
3. **Dismantled coordinated harassment campaigns** before they could escalate further.

RESULTS

1. Darkivore took down:
    - 35 fake TikTok accounts
    - 1 fake Instagram account
    - 3 fake websites
1. The school regained control over its digital presence.
2. Students and teachers felt safe to engage both online and in school once again

// SUCCESS STORY : LARGE MULTI-REGIONAL BANK

SOCMINT & ANTI-PHISHING CHALLENGE

PROBLEM

1. The Bank's customers were affected by external fraud attempts through Phishing and Social Media Scam attacks.
2. Executives were suffering from Identity Theft.
3. The customer brand and digital assets were facing reputational damage.
4. Sensitive data was divulged through unintentional leakage.
5. SOC, SIEM, EDR, DLP, NGFW, Pen Tests etc.. Were not pre-emptive enough.

ACTION PLAN

DARKIVORE

1. Took a proactive approach to enhance company security instead of simply reacting to attacks.
2. Implemented round-the-clock scanning of the surface, deep, and dark web
3. Provided customers with a real-time platform to :
   - Continuously monitor brand's digital footprint on all social media platforms
   - Track usage of brand domain & trade name on various platforms
   - Monitor the online exposure of key personnel

RESULTS

- **Take down of :**
  +9,000 fake pages on Social Media
  +1,500 malicious sites
  +25 rogue Mobile Application detected
- **Deactivation of** +500 fake WhatsApp groups & malicious members
- **Detected & Alerted customers for deactivation of** +2,500 Credit Card leaked
- **Reduced** malicious activities by 99% over 2 years time
- Provided regular weekly & monthly reports that included quantitative analysis of cyber threats and risks.

// SUCCESS STORY : LARGE MULTI-REGIONAL HEALTHCARE COMPANY

MALWARE DARK WEB DATA LEAKAGE

PROBLEM

1. Customers and Dev-Ops employee's data was compromised and sold on the dark/deep web.
2. Many password stuffing, and illegitimate access were detected on their platforms & VPN/PAM.
3. Initial Forensic investigations conducted by 3rd parties showed no sign of customer environment compromise.
4. Still their operations and online platforms were dramatically affected.
5. Cybersecurity teams were confused and overwhelmed.

ACTION PLAN

DARKIVORE

1. **24/7 scanned** the surface, deep and dark web.
2. **Analyzed** the data leakage : Malware installed on employees and end user's personal device that logs user credentials, outside the company's environment.
3. **Detected & Alerted** our client of the compromised users.

RESULTS

- Malware harvested other credentials (personal email & social media accounts) and was not targeting the company specifically.
- Data Leak took place outside the organization environment , company was relieved by the news.
- Client enforced remote access policies to protect their technical employees, changed their credentials immediately.
- Client informed their customers to change their credentials and alerted them about the attack targeting their personal devices.