



APATÉ

ANTI-PHISHING & ABUSE THREAT ERADICATION

Take Threats Down Before They Strike.

Continuous brand protection & rapid phishing-infrastructure takedown — outside your perimeter, at machine speed.



<2 hr fastest takedown



<24 hr average takedown



Fully managed
zero added headcount



OJK · BI · PDP
compliance-aligned



OVERVIEW

APATÉ is an enterprise Digital Risk Protection platform that guards your brand, customers and executives beyond the corporate firewall — pairing automated threat hunting with a relentless global enforcement network.



Global takedown framework

Direct pipelines to registrars, hosts & social networks.



Rapid time-to-mitigation

Disrupts attacker architecture in hours, not weeks.



Zero operational overhead

Fully managed, continuous validation loop.



PROBLEMS WE SOLVE



Exploding look-alike domains

Typosquatted & homograph domains harvest credentials and financial data.



Social & VIP impersonation

Fake support channels and executive profiles drive whaling and fraud.



Rogue mobile apps

Fake apps on third-party stores steal banking tokens and inject spyware.



Regulatory pressure

OJK, BI & PDP Law mandate active technical measures against digital fraud.



CORE CAPABILITIES

01 EXTERNAL THREAT INTELLIGENCE



Typo-squat & homograph detection

Fuzzy-match ML scans thousands of daily domain registrations for look-alikes.



Deep & dark web crawling

Monitors forums, closed channels & paste sites for leaks and phishing kits.



Phishing lure analysis

Sandboxed crawlers profile live lures and extract attacker infrastructure.

02 GLOBAL ENFORCEMENT & TAKEDOWN



Direct registrar & ISP integration

Automated cease & desist notices and takedown demands to hosts and DNS registries via established legal pathways.



Malicious binary takedown

Flags and coordinates removal of rogue Android & iOS apps masquerading as your official enterprise apps.

KEY BENEFITS



Protect brand trust

Customers reach only verified assets — fewer fraud incidents.



Cut response costs

Neutralize threats at source; less SOC triage.



Relentless execution

Escalates up the hierarchy so threats stay down.



Full visibility

Executive dashboard: MTTD, alerts & takedown history.



HOW IT WORKS — THE TAKEDOWN LIFECYCLE



01

Detect

Continuous scanning of DNS logs, the web, dark web & app stores for brand abuse.



02

Analyze

Sandboxed crawlers profile phishing lures and extract attacker infrastructure markers.



03

Enforce

Automated C&D notices to registrars, hosts, social networks & app marketplaces.



04

Verify

Escalation loop confirms permanent removal and logs audit-ready evidence.

The APATÉ loop never stops — detect, analyze, enforce, verify, repeat.



WHAT APATÉ TAKES DOWN



Look-alike domains



Phishing landing pages



Rogue social profiles



Fake mobile apps



Dark-web leaks



IDEAL USE CASES



Banking & Finance



Government & Public



Critical Infra & Energy



Healthcare & Hospitals



Retail & E-Commerce



Telecom & Networks



WHY APATÉ?



Proactive, not reactive

Compliance firefighting becomes machine-speed mitigation.



Built-in enforcement network

Direct pipelines to registrars, hosts & app marketplaces.



Audit-ready by design

Full-lifecycle logs for board & regulator reporting.



Globally validated

Proven across banking & critical infrastructure.

RESOLUTION TIME TO TAKEDOWN

<2 hr fastest

<24 hr average



Schedule a live brand-threat assessment

See APATÉ detect and take down threats — live, with our engineering team.



sales@ptdts.co.id



www.ptdts.co.id



Jakarta, Indonesia