

Autonomous Threat Intelligence (ATI)

Detect impersonation, leaks, and brand abuse, before it spreads. OSINT Scanning



The Problem

Fake domains, impersonation attempts, leaked credentials, and executive exposure often appear on platforms outside your control.



The Shift

An autonomous system that detects and helps remove external threats: from spoofed assets to brand misuse and executive targeting.

What it Covers

ATI flags early-stage attacker activity including phishing infrastructure, spoofed domains, SSL certificate misuse, and breach chatter. It monitors forums, auction sites, grey noise, and infrastructure signals to detect intent in real time, not just after a breach.

What Makes It Different



Tracks auction sites, forums, and grey noise, not just breach dumps.



Flags attacker prep using SSL certs, infrastructure prep, and domain setups.



Builds user-level risk profiles from exposure and interest.



Identifies phishing domains before they go live.



Escalates real threats with analyst support when needed.

How it works

Track ➤ Detect ➤ Predict ➤ Escalate

What you get

Live alerts, no noise. Each threat is contextualised and risk-rated, with clear next steps. You get visibility without extra tooling, and support when a takedown or escalation is needed. No overhead. Just coverage.