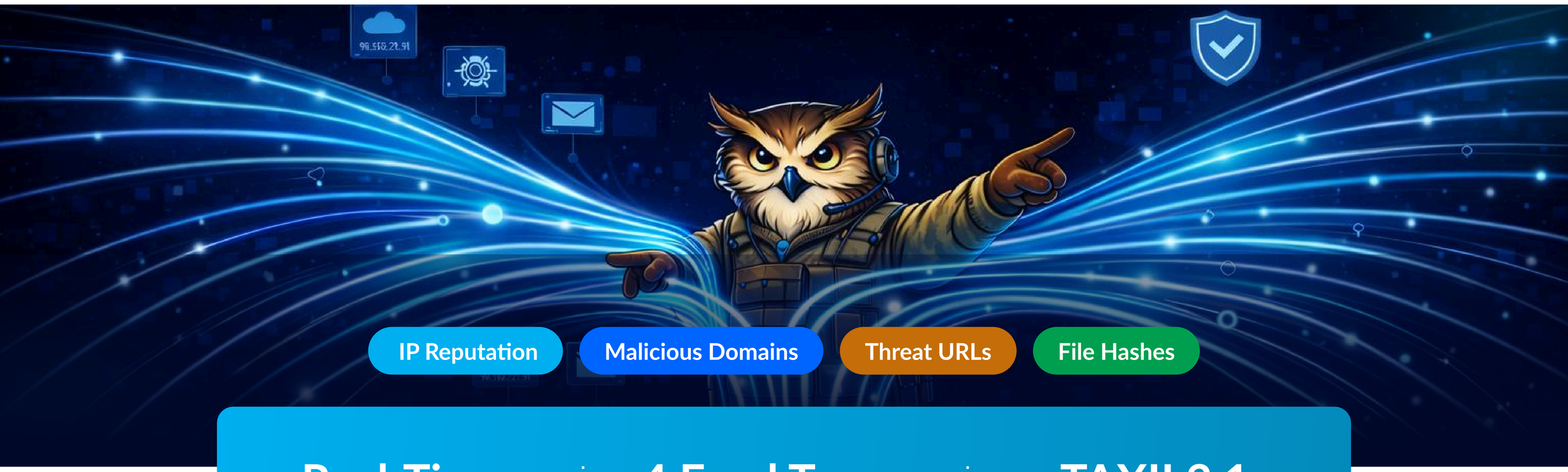
TechOwl
THREAT PULSE

KNOW THE THREAT.
BEFORE IT KNOWS YOU.

Curated, real-time threat intelligence - delivered as TAXII feeds directly into your security tools the moment a new indicator is confirmed.



Real-Time
IOC delivery - the moment a threat is confirmed

4 Feed Types
IPs, Domains, URLs & File Hashes - one subscription

TAXII 2.1
Industry-standard delivery into your existing tools

THE CHALLENGE

Threats Change Every Hour. Your Intelligence Shouldn't Be Days Behind.

Your SIEM, firewall, and endpoint tools are only as good as the intelligence feeding them. Stale indicators, unvalidated feeds, and manually curated blocklists leave dangerous gaps - gaps that active threat actors are already exploiting.

Without fresh, accurate, and contextually rich threat intelligence flowing continuously into your defenses, you're reacting to yesterday's threats - while today's attackers move freely through the spaces in between.

Stale Intelligence Is Dangerous

Threat actors rotate infrastructure constantly. An IP or domain that was safe yesterday may be actively malicious today - and your tools won't know.

Integration Is A Manual Burden

Pulling threat data from multiple sources, formatting it, and importing it into security tools consumes analyst hours that should be spent on actual threats.

Noise Drowns Out Signal

Low-quality open-source feeds flood security teams with unvalidated indicators, wasting analyst time and desensitizing teams to real alerts.

THE SOLUTION

ThreatPulse - Curated IOC Intelligence, Delivered Automatically

TechOwl ThreatPulse is a curated threat intelligence feed service that delivers validated, high-fidelity Indicators of Compromise directly into your security infrastructure via industry-standard TAXII 2.1 feeds - automatically, continuously, and without manual intervention.

Every indicator is validated and context-enriched before it reaches your tools - so your defenses act on intelligence that's accurate, relevant, and ready to use.

01

COLLECT

Techowl continuously aggregates threat data from global sources - tracking malicious IPs, domains, URLs, and file hashes in real time.

02

VALIDATE

Every indicator is validated & false-positive filtered before publication - so tools receive only confirmed, actionable intelligence.

03

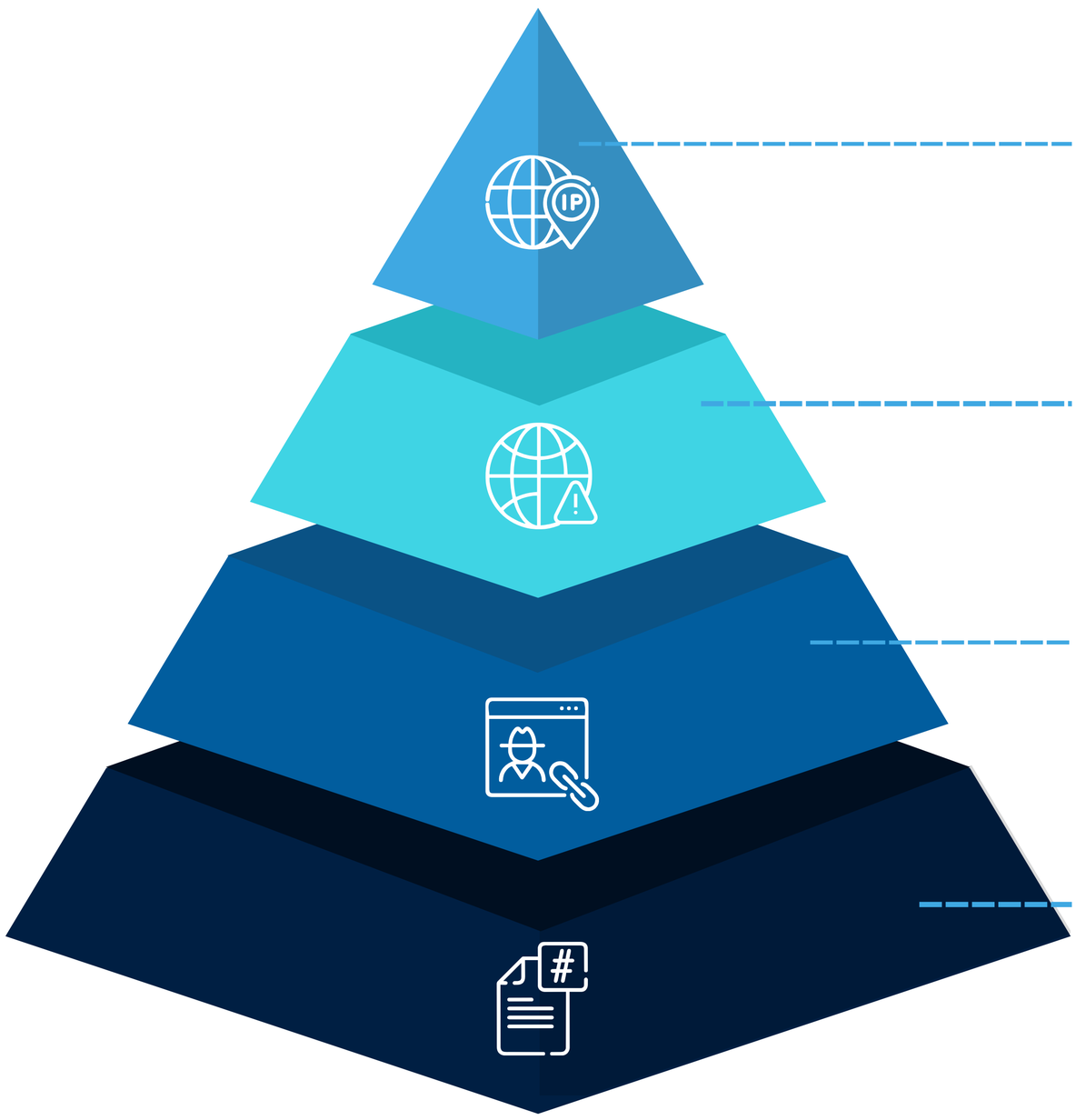
DELIVER

Fresh IOCs are pushed to your SIEM, firewall, and security tools via TAXII 2.1 - automatically, the moment they are confirmed.

WHAT YOU RECEIVE

Four Feed Types. One Continuous Stream of Confirmed Threats.

ThreatPulse delivers four distinct, independently subscribable IOC feeds - each focused on a specific threat indicator type, validated for accuracy, and enriched with context that makes every indicator immediately actionable.



IP Reputation Feed

Continuously updated list of confirmed malicious IP addresses - including C2 servers, scanners, botnet nodes, and known attacker infrastructure - with threat category and geolocation context.

Malicious Domain Feed

Verified malicious domain indicators covering phishing sites, C2 domains, malware distribution points, and newly registered suspicious domains - updated as the threat landscape shifts.

Threat URL Feed

Confirmed malicious URLs actively used in phishing campaigns, malware delivery, and credential harvesting - ready to block at the proxy and web gateway level.

File Hash Feed

SHA256, MD5, and SHA1 hashes of confirmed malware samples - enabling rapid detection of known malicious files across endpoints, email, and cloud storage environments.

HOW IT'S DELIVERED

Plug Into Your Security Stack - Without a Single Line of Code

ThreatPulse delivers all IOC feeds via TAXII 2.1 - the industry-standard protocol for automated threat intelligence sharing. Your SIEM, firewall, threat intelligence platform, or security orchestration tool connects once, and from that moment forward, fresh indicators flow in automatically.

No manual downloads. No CSV imports. No scheduled scripts. Just a continuous, authenticated feed of confirmed threats - ready for your tools to act on the moment they arrive.

TAXII 2.1 Native Delivery

Industry-standard protocol ensures compatibility with leading SIEMs, TIPs, firewalls, and SOAR platforms - without custom integrations or middleware.

STIX 2.1 Structured Format

All indicators are delivered in STIX 2.1 format - providing rich, machine-readable context including threat type, category, first seen, and last seen timestamps.

Continuous Automatic Updates

Your connected tools receive new indicators the moment they are validated and published. No polling intervals, no stale data windows, no manual refresh cycles.

Authenticated & Encrypted

All feed connections are authenticated and encrypted in transit - ensuring only authorized systems can consume your organization's threat intelligence subscription.

WHERE IT CONNECTS

Feeds Your Existing Security Tools - Instantly

ThreatPulse is designed to integrate with the security infrastructure your team already operates - not to replace it. A single TAXII connection is all it takes to start enriching your defenses with curated, real-time threat intelligence.

SIEM Platforms

Enrich detection rules and alert context with real-time IOC correlation.

SOAR & Orchestration

Trigger automated playbooks the moment a confirmed IOC is detected in your environment.

Firewalls & Gateways

Automatically block confirmed malicious IPs, domains, and URLs at the perimeter.

Threat Intel Platforms

Aggregate ThreatPulse feeds alongside other intelligence sources for unified analyst context.

BUSINESS OUTCOMES

What Changes When Your Intelligence Is Always Current

Threats Blocked Before They Reach Your Environment

Real-time IOCs flowing into your firewall and security tools mean known malicious infrastructure is stopped at the perimeter - automatically.

Analyst Time Spent On Real Threats, Not Feed Management

Automated TAXII delivery eliminates the manual effort of sourcing, validating, and importing threat data - freeing your team for higher-value work.

Alerts Enriched With Confirmed Threat Context

Every IOC match in your SIEM comes with validated intelligence - not a raw indicator, but a confirmed threat with category, first seen, and context attached.

Dramatically Reduced False Positive Noise

Validated, false-positive-filtered feeds mean your detection tools fire on confirmed threats - not on aged, unverified indicators from low-quality open sources.

Faster Detection And Response When It Matters

When a confirmed malicious IP or domain appears in your logs, your team already knows it's a real threat - cutting investigation time significantly.

Intelligence That Keeps Pace With The Threat Landscape

Continuous updates mean your defenses reflect the threat landscape as it exists right now - not as it existed last week or last quarter.

INTELLIGENCE QUALITY

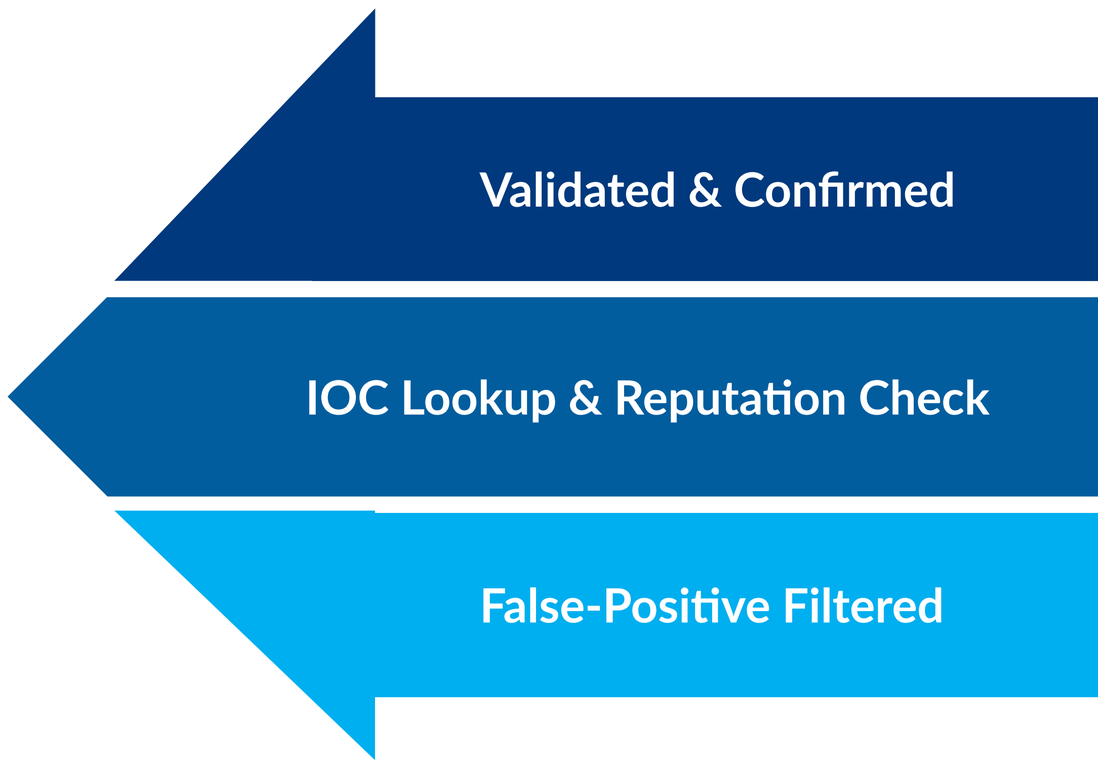
Not Just Indicators - Context That Makes Them Actionable

A raw IP address or domain name tells your team that something may be suspicious. ThreatPulse tells them what it is, how confident the assessment is, when it was first seen, how active it currently is, and what kind of threat it represents - so every alert comes with the context needed to act decisively.

01 Every IOC is verified before delivery. No unvetted community submissions. No automated-only sourcing. Only confirmed, actionable threat indicators reach your tools.

02 Analysts can manually query any IP, domain, URL, or file hash against the ThreatPulse database - instantly checking reputation and threat context for active investigations.

03 Indicators associated with legitimate infrastructure, CDNs, or known safe services are excluded before publication - protecting your team from wasted investigations.



IOC LOOKUP & THREAT HUNTING

Search Any Indicator. Get an Answer in Seconds.

ThreatPulse isn't just an automated feed. It's also an on-demand threat intelligence lookup tool - giving your analysts the ability to query any indicator of compromise directly and get an immediate, evidence-backed reputation verdict.

Whether you're investigating an alert, triaging a suspicious connection, or proactively hunting for threats in your environment - simply enter the indicator and ThreatPulse tells you exactly what it knows about it.

Enter any IP, Domain, URL, or File Hash

185.220.101.44 | malicious-update.com | /login.php | 8f3a9c4d...

Malicious - C2 Infrastructure | Phishing Domain | Malware Delivery URL | Known Malware Hash

IP Lookup

Check any IP address against the ThreatPulse database - see if it's a known C2 server, botnet node, scanner, or malicious actor infrastructure.

Domain Lookup

Query any domain for known malicious classification - phishing, C2, malware distribution, or newly registered suspicious domains.

URL Lookup

Verify any URL's threat status - instantly know if it's been observed in active phishing or malware delivery campaigns.

Hash Lookup

Submit any file hash (SHA256, MD5, SHA1) to check if it matches a known malware sample in the ThreatPulse database.

1

Instant Reputation Verdict

Know within seconds whether an indicator is clean, suspicious, or confirmed malicious - no waiting, no manual research.

2

Full Threat Context Per Indicator

See threat category, first observed date, associated campaign type, and geographic origin - everything your analyst needs to make a confident decision.

3

Accelerate Active Investigations

During an incident, analysts can rapidly validate every suspicious indicator from logs, alerts, and endpoint telemetry - cutting investigation time dramatically.

4

Proactive Threat Hunting Support

Hunt through your environment with confidence - any IOC you surface can be instantly cross-referenced against ThreatPulse before you escalate or remediate.

GOVERNANCE & COMPLIANCE

Threat Intelligence as a Demonstrable Security Control

Regulators and security frameworks increasingly expect organizations to demonstrate that their defenses are informed by current, external threat intelligence - not just internal telemetry. ThreatPulse provides the evidence that your detection capabilities are continuously enriched with validated IOC data.

Compliance Support

- Demonstrates active threat intelligence integration
- Supports detection control effectiveness evidence
- Validates that IOC monitoring is continuous, not periodic
- Provides documented feed sources for audit review
- Strengthens incident response readiness posture
- Supports NIST CSF Detect and Respond functions

Governance Value

- Proves defenses are informed by external intelligence
- Supports BFSI, Healthcare & regulated sector requirements
- Demonstrates proactive, not reactive, threat posture
- Gives boards evidence that detection is continuously enriched
- Reduces regulatory risk from undetected known threats
- Satisfies threat intelligence program expectations in audits

WHY THREATPULSE

Curated Intelligence vs Generic Feeds - The Difference Is Everything

Free and open-source threat feeds exist. But unvalidated, stale, and noisy intelligence does more harm than good - flooding your tools with false positives and burying the signals that matter. ThreatPulse is built around quality, not volume.

CAPABILITY	GENERIC THREAT FEEDS	TECHOWL THREATPULSE
Free / open-source threat feeds	✓	✓ Curated, validated & enriched
Real-time IOC updates	✗	✓
IP reputation intelligence	Limited	✓ Full context & enrichment
Malicious domain feeds	Limited	✓ Continuously updated
URL threat intelligence	✗	✓
File hash (malware) feeds	✗	✓
TAXII 2.1 / STIX 2.1 delivery	✗	✓ Native, plug-and-play
Validated & false-positive filtered	✗	✓
IOC context enrichment (type, category, first seen)	✗	✓
Direct SIEM & firewall integration	Limited	✓ Automated

WHO IT'S FOR

For Every Security Team That Needs Intelligence It Can Actually Trust

SOC Teams

Enrich detections and reduce investigation time with confirmed, contextual IOC data in every alert.

BFSI Sector

Meet intelligence-led security requirements with validated, industry-grade IOC feeds.

Threat Hunters

Hunt against a continuously refreshed set of confirmed indicators from active global threat infrastructure.

Regulated Sectors

Demonstrate that detection capabilities are continuously enriched with external threat intelligence.

MSSPs

Deliver curated IOC intelligence to multiple clients through a single, scalable TAXII subscription.

ECOSYSTEM

Part of the TechOwl Security Platform

ThreatPulse feeds directly into the TechOwl ecosystem - combining live threat intelligence with cloud posture management, domain protection, human risk simulation, and malware analysis under one unified security partnership.

TechOwl SHIELD — Attack Surface Monitoring

TechOwl DMARC SHIELD — Email Trust Assurance

TechOwl VENDOR SHIELD — Third-Party Risk Intelligence

TechOwl CLOUD SHIELD — Cloud Security Visibility

TechOwl PHISH SHIELD — Employee Risk Readiness

TechOwl THREAT PULSE — Threat Signal Intelligence

TechOwl THREATLAB — Advanced Threat Detonation

Start Receiving Live Threat Intelligence Today.

Connect ThreatPulse to your security stack in minutes. One TAXII endpoint. Four feed types.
Continuous, validated IOC intelligence - from the moment you're live.

sanchita@techowl.com