PENTESTERRA
SEE THE REAL RISK

ATTACK SURFACE | THREAT INTELLIGENCE | SUPPLY CHAIN | HUMAN RISK

DISCOVER.
ENRICH.
ANTICIPATE.
STAY AHEAD.

ORGRECON MODULE

OSINT & Public Exposure Intelligence

People. Companies. Context. Real risks from the open internet.

Transform public data into actionable security intelligence. Discover what attackers can find, correlate the dots, and understand your real external exposure — before it's exploited.

COMPREHENSIVE
Data collection from multiple open sources

FAST
From seconds to minutes

ACTIONABLE
Enriched profiles and risk insights

NON-INTRUSIVE
Passive OSINT only

WHAT WE ENRICH

TURN PUBLIC DATA INTO A COMPLETE PICTURE.

Company Information
- Basic info & description
- Industry, size, location
- Subsidiaries & relations
- News & funding rounds

People & Profiles
- Employees & executives
- Roles & bios
- Social media profiles
- Personal interests (opt-in)
- Social engineering insights

Domains & Infrastructure
- Domains & subdomains
- IP ranges & hosting
- Open ports & services
- DNS / MX / SPF / DMARC
- Cloud providers & tech stack

Leaks & Threat Intelligence
- Breached data & credentials
- Mentions in dark web
- Malware & threat actor links
- Ransomware victim references
- Risk correlations (IPs, certificates)

HOW IT WORKS

FROM OPEN SOURCES TO ACTIONABLE INTELLIGENCE.

1. **Collect** — Gather data from public sources
2. **Enrich** — Correlate and analyze with AI
3. **Score** — Calculate real exposure risk
4. **Visualize** — Clear, intuitive results
5. **Monitor** — Keep tracking for new threats

OPEN SOURCES. REAL INSIGHTS. STRONGER SECURITY.

Prioritize real risks. Reduce human risk. Strengthen your security posture.

EXPLORE ORGRECON →

PENTESTERRA

OSINT & ATTACK SURFACE INTELLIGENCE

Intelligence That Gets Reused, Not Filed Away

A company is not just a domain. A person is not just an email. Pentesterra gathers company context, technology, exposed attack surface, and people intelligence into one reusable profile - passively - and feeds it into phishing, pentest, and reporting.

Passive

No active scanning, no target permission required

Company + People

Down to a per-person deep profile

Bulk

Upload and monitor thousands of organizations

WHY NOW

A pentest, an acquisition, or a supplier review is coming up, and nobody has pulled together what's publicly knowable about the target yet. Attackers already assemble this picture by hand. If your own team hasn't done it first, the phishing pretext, the exposed subdomain, or the leaked credential shows up in an incident report instead of an assessment.

WHAT THE MODULE DOES

Company-Level Intelligence

One profile per organization: what it does, the products it ships, likely tech stack, infrastructure and attack surface, and business/regulatory context. Passive and semi-passive collection - no active scanning required.

- → Business context, products, likely tech stack
- → Domains, subdomains, CIDR ranges, cloud footprint
- → Public signals: leaks, dark-web mentions, threat-actor interest
- → One deduplicated company record, updated on each run

People Intelligence

Who the people are, what roles they hold, and the public professional context around them - including the personal detail that makes a social-engineering assessment realistic instead of a guess.

- → Roles, seniority, org structure
- → Professional context, personal interests, hobbies, and public social-media footprint (opt-in)
- → Emails and identity data tied to the company record
- → On-demand deep profiling for named high-value individuals

Reusable, Not a Dead-End Report

OSINT is gathered so it can be reused. The same intelligence layer feeds phishing scenario design, pentest prioritization, social-engineering validation, and the "why this matters" section of the final report.

- → Feeds phishing and social-engineering simulation directly - the interests and context gathered here become the pretext
- → Informs pentest scope, likely tech, and attack paths
- → Adds business-impact context to findings
- → Shared across modules, not siloed per assessment

Discovery and Monitoring at Scale

Add companies in bulk, discover related entities, and keep them monitored. When the knowledge base updates, added companies are re-checked automatically, and you get alerts on new exposure.

- → Bulk upload and company discovery
- → Near-real-time re-checks as intelligence updates
- → Monitoring and alerting for tracked organizations
- → Suited to supplier, portfolio, and M&A due-diligence use

WHY THIS MATTERS FOR THE REST OF THE PLATFORM

The personal interests, hobbies, and public posts collected here aren't a side detail - they're the single biggest lever for phishing-simulation realism. A pretext built from a target's actual conference talk, side project, or recent post converts very differently from a generic "reset your password" email. Pentesterra's Phishing Simulation module draws on this profile directly.

FREQUENTLY ASKED QUESTIONS

Is Pentesterra OSINT passive?

Collection is passive and semi-passive - public sources, certificate transparency, DNS, leak and dark-web data, and professional context. No active scanning or authenticated access required.

What is "deep person profiling"?

An on-demand profile for a single named individual: role, seniority, professional context, interests, public footprint, and identity data - triggered per person rather than bundled into a whole-company scan.

How does OSINT connect to the rest of the platform?

It is the shared intelligence layer. Phishing simulation uses it to build context-aware, personalized scenarios; pentest modules use it to prioritize and understand likely technology; reporting uses it to explain business impact.

Can I use this to assess suppliers or acquisition targets?

Yes. Upload companies in bulk, run passive checks quickly, and keep them monitored - fitting third-party risk, portfolio monitoring, and pre-acquisition due diligence without needing permission to scan.

Build your first intelligence profile

Start from a company name or domain - no target permission required.

info@pentesterra.com
pentesterra.com/osint