PENTESTERRA

OSINT INTELLIGENCE

Do You Know Your Target Before an Attacker Does?

OSINT intelligence on companies and people - passively gathered, reused across phishing, pentest, and reporting, not a dead-end report.

IN SHORT

A passive collection of publicly available information about a company and the people who work there - domain, likely tech stack, exposed surface, roles, public interests (opt-in) - no permission to scan required. Feeds directly into phishing simulation, pentest scope, and the business-impact context in the final report.

Passive

No active scanning, no target permission required

Company + People

Down to a per-person deep profile

Bulk

Thousands of organizations uploadable and monitored

THE SITUATION TODAY

WHO YOU ARE

You're the security, OSINT, or pentest lead of an organization that needs to gather the public context on a target - your own or a third party's - before a pentest, an acquisition, or a supplier review.

WHAT HAPPENED

A pentest, an acquisition, or a supplier review is coming up, and nobody has pulled together what's publicly knowable about the target yet.

WHY IT HURTS

Attackers already assemble this picture by hand. If your own team hasn't done it first, the exposed subdomain or the leaked credential shows up in an incident report instead of an assessment.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want one reusable profile - not information scattered across different tools that nobody ever puts together.

THE SOLUTION

An OSINT Intelligence service: company profile (likely tech stack, exposed surface, business context) and people intelligence (roles, professional context, opt-in public interests), gathered passively and reused throughout the rest of the assessment.

WHY IT'S DIFFERENT

You're not buying another OSINT tool that spits out a list of domains. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know. And the personal interests and public activity gathered 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 or side project converts very differently from a generic email.

CONCRETE PROOF

The result is a complete PDF report with the company and people profile collected, reusable throughout the rest of the assessment. If broader gaps come up, we propose additional services: phishing simulation, vulnerability assessment, penetration testing.

Reusable

Feeds phishing, pentest, and reporting

Bulk + Monitoring

Automatic re-check on every KB update

Opt-In

Personal interests collected only with consent

WHAT'S ACTUALLY INCLUDED

Not a list of domains - a reusable company and people profile shared across the whole platform.

Company-Level Intelligence

One profile per organization: what it does, likely tech stack, infrastructure and attack surface, business/ regulatory context.

- 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.

- Roles, seniority, org structure
- Professional context, personal interests, and public social 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

The same intelligence layer feeds phishing, pentest, and reporting.

- Feeds phishing scenario design directly
- 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.

- 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

PENTESTERRA

OSINT INTELLIGENCE

WHAT YOU GET

- ✓ A complete PDF report with the company and people profile collected
- ✓ Attack surface, tech stack, and business context of the target
- ✓ Professional context and public interests (opt-in) of key people
- ✓ Intelligence reusable for phishing simulation, pentest, and reporting
- ✓ Continuous monitoring with alerts on new exposure

HOW IT WORKS

1

We define the scope

A company, a supplier, or a whole portfolio - we set the scope together.

2

We collect passively

No active scanning, no permission required to start.

3

We build the profile

Company and key people, with public interests collected only with consent.

4

We deliver the report

A complete PDF, reusable throughout the rest of your assessment.

Find out what's already publicly known about your target

A complete report, ready to present to clients, auditors, or your board.

Request your OSINT Intelligence →

info@pentesterra.com · pentesterra.com/osint