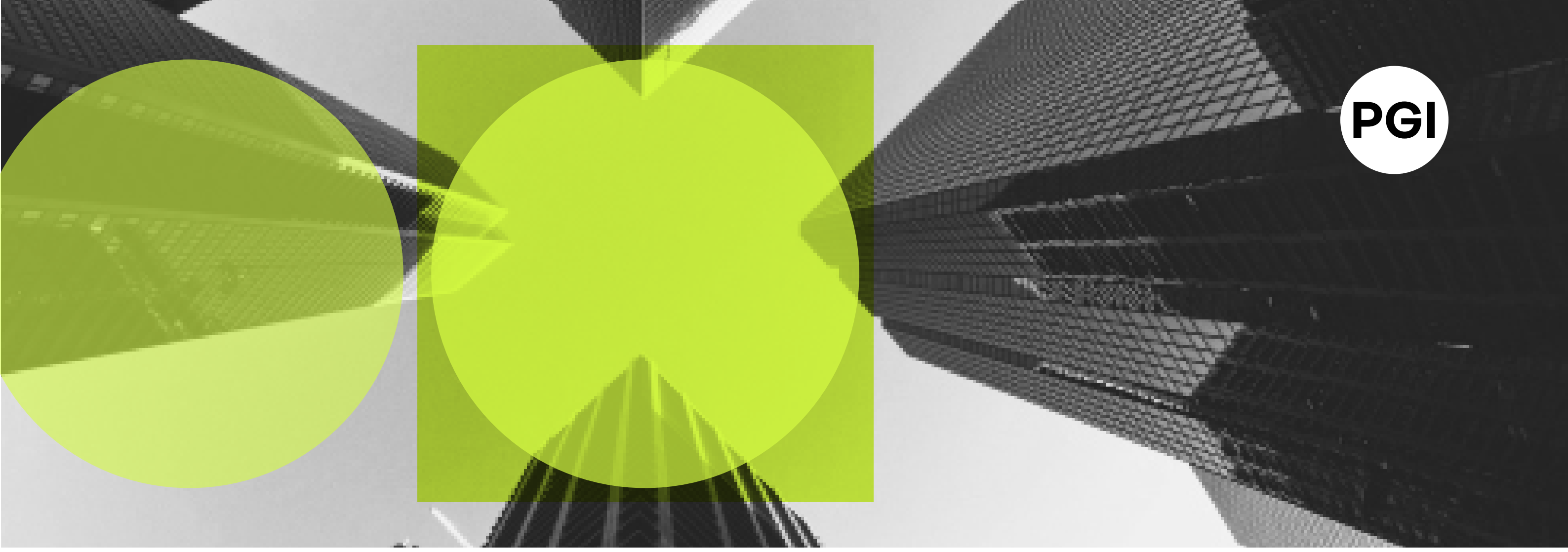

# Intelligence-Led Penetration Testing

## Setting a new standard for mitigating digital risk exposure

Our Intelligence-Led Penetration Testing combines **digital risk intelligence** with penetration testing to uncover your **full risk landscape**, including what attackers can discover about your organisation and exploit.

## Why it matters

Modern cyber-attacks don’t start with technical exploits—they start with information. Using OSINT (Open-Source Intelligence), attackers identify key personnel, uncover exposed Personal Identifiable Information (PII), and build detailed pictures of internal structures. This information can be exploited through social engineering and other malicious attacks, to cause **operational, financial, or reputational damage.**

Traditional penetration testing effectively evaluates your technical controls, but if you're not assessing your **public digital footprint**, you're leaving a major gap in your defences.

## Our two-phase approach

### 1 Digital Risk Assessment (DRA)

Using advanced OSINT techniques, we uncover what threat actors can learn about your organisation from public sources, including:

- Exposed personal or sensitive employee data
- Digital footprints that can be leveraged in social engineering attacks
- Publicly available technical or structural information

### 2 Penetration Testing

Equipped with the findings from the DRA, we perform a simulated attack to identify and exploit weaknesses within your internal systems and networks to analyse real-world impact.

This allows us to:

- Conduct a fully informed penetration test to assess real-world vulnerabilities
- Use findings from the DRA to help identify and exploit vulnerabilities in the context of your organisation
- Correlate findings between digital exposure and technical weaknesses to understand how an attacker might leverage these vulnerabilities against your organisation.

## The benefits of Intelligence-Led Penetration Testing

- **Advanced threat simulation:** Simulates real-world adversaries using both external intelligence and internal technical testing.
- **Contextual risk analysis:** Connects public exposure with technical gaps to map out likely attack paths.
- **Prioritised remediation:** Targeted recommendations to reduce both digital exposure and technical vulnerabilities.
- **More efficient security testing:** The DRA insights streamline our penetration testing, focusing effort where attackers would, for a cost-effective security solution.

## What you get

- **Comprehensive risk report:** A side-by-side view of digital exposure and technical vulnerabilities.
- **Actionable insights:** Practical, prioritised remediation steps to strengthen your defences.
- **Unified security posture:** A holistic view of your digital risk landscape.

> “Your security testing might only be telling you half the story.”

**Barry Sadler**
PGI’s Head of Penetration Testing

## How PGI does things differently

By combining technical and intelligence expertise with a deep understanding of modern business operations, PGI are setting a new standard for digital threat mitigation, helping our clients stay resilient against today’s most sophisticated evolving threats.

Our Intelligence-Led Penetration Testing provides your organisation with the most up-to-date and comprehensive security testing available.