ergo:·

# Threat-Led *Penetration Services*

Penetration tests have traditionally provided a detailed and useful assessment of technical and configuration vulnerabilities, often within isolation of a single system or environment. However, they do not assess the full scenario of a targeted attack against an entire entity (including the complete scope of its people, processes and technologies).

To provide an appropriate level of assurance that an organisation's key financial services assets and systems are protected against technically competent, resourced and persistent adversary attacks, Ergo offer Threat Led Penetration Testing (TLPT) based on the TIBER-EU framework aligned to the EU Digital Operational Resilience Act (DORA)

An intelligence-led red team test mimics the tactics, techniques and procedures (TTPs) of advanced threat actors who are perceived by threat intelligence as posing a genuine threat to entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack – either by malicious outsiders or by staff – on an entity's information security arrangements (i.e. its people, processes and technologies).

The core objective for Ergo in performing the TLPT will be on testing and improving your key elements of cyber resilience with a heavy focus on reporting the methodology employed in order to provide a customer the learning opportunities that the testing provides.

## Key *benefits*

- Non-biased assessment of your security posture
- Identify physical, hardware, software and human vulnerabilities
- Measure your defence systems response capabilities to a cyber attack
- Enables smart and focused cyber security investments
- Demonstrate DORA, NIS2 and other regulatory compliance

> *Article 26 of the Digital Operational Resilience Act requires financial entities to conduct a threat-led penetration test based on the TIBER_EU framework at least every three years. These tests must cover critical functions and be performed on live production systems.*

## What *you get*

- End-to-end security assessment
- A comprehensive report with industry best-practice recommendations
- Technical details of the vulnerabilities and recommended solutions
- Long-term recommendations for efficient cyber defence investment

# Ethical Hacking to *Prevent Potential Intrusions*

Our Red Team uses a systematic, repeatable and reproducible testing methodology to fully assess the ability of any type of organisation's cyber defence capabilities through a simulated cyber-attack.

Phase 1
## Pre-Engagement Interactions

- Define the scope and rules of engagement
- Establish lines of communication

Phase 2
## Reconnaissance

- Intelligence gathering
- Target delection
- Footprinting
- Targeted threat intelligence report

Phase 3
## Attack Delivery

- Deliver payloads
- Compromise targeted assets
- Obtain foothold
- Record findings and observations

Phase 4
## Command and Control

- Escalate privileges
- Lateral movement
- Data extraction

Phase 5
## Analysis, Reporting and Support

- Generate report
- Remediation advice
- Report opportunities for improvement
- Offer support

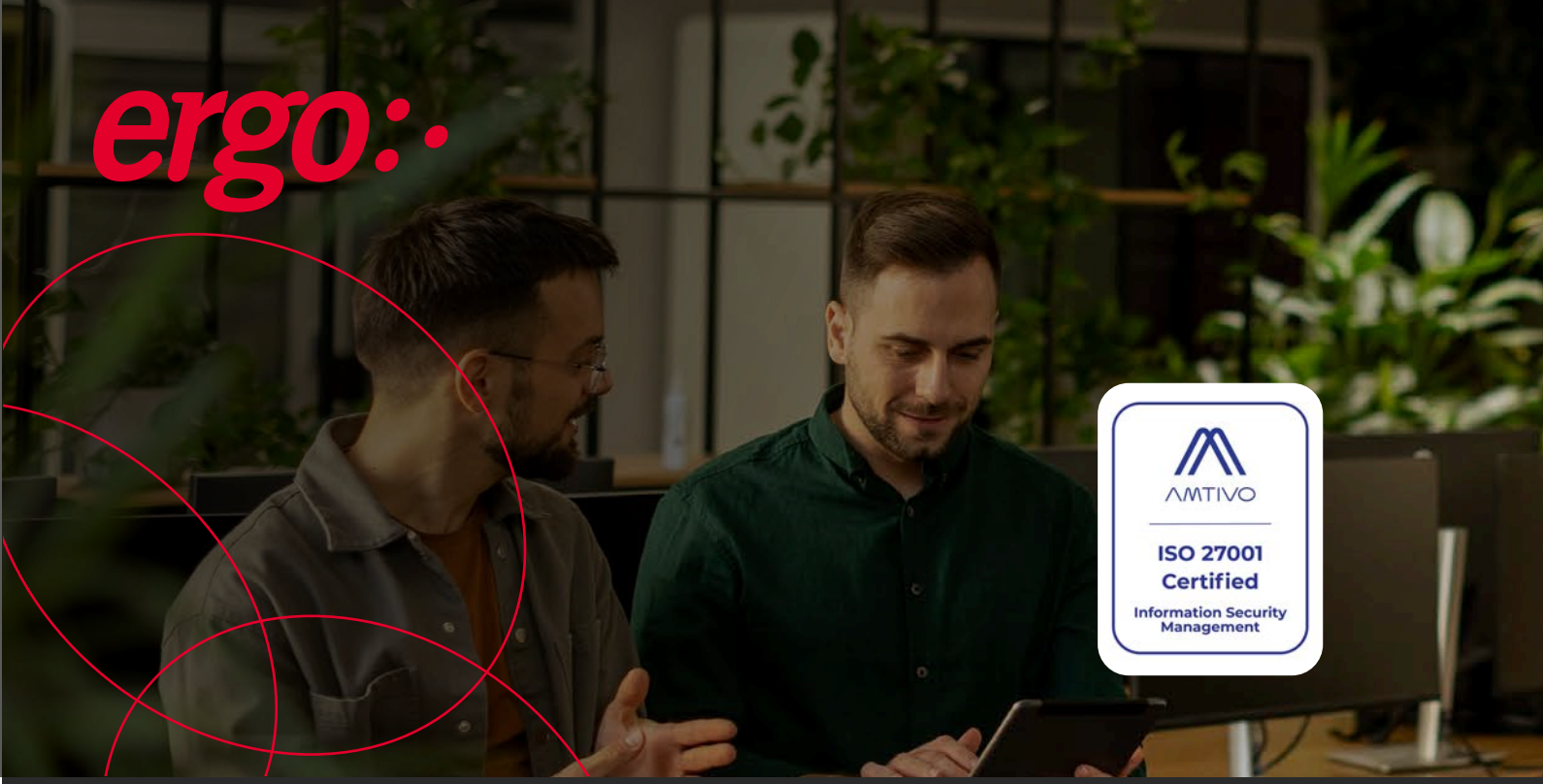
# Deliverables

At the end of the Red Team Operations process we provide our customers with an extensive report and recommendations to effectively eliminate the detected threats:

- Targeted Threat Intelligence Report which sets out the attack scenarios.
- The final report will have an executive summary and details of all findings, including specifics such as the affected resources, evidence of the successful hack, proposed remediation and will prioritise findings according to their criticality to allow you to plan forward.
- In addition to delivering the report we will facilitate a review workshop of results to do a deep dive on the report and ensure alignment among stakeholders.
- Long-term strategic advice that will help in avoiding repetition of vulnerabilities.
- Actionable recommendations to remediate the revealed security issues.

# Reasons to *choose Ergo*

- More than 15 years' experience in the field
- Committed to deliver quality
- TIBER-EU aligned
- Flexible pricing policy around our clients' needs
- Custom reports to plan your security strategy further
- Our team of ethical hacking experts possess the accreditations, skills and experience to identify threats.




# About *Ergo*

Ergo has helped IT leaders excel at the intersection of business and technology for over three decades, becoming Ireland's largest privately-owned IT services company with offices in the UK, Europe, North America and New Zealand. Providing bespoke, insights-led advice, expert implementation and proactive managed services, Ergo enables organisations to become more agile, more efficient, more compliant and better equipped for long-term growth.

By recommending a strategy of proactive IT investment that aligns with each client's unique business needs, Ergo has steered clients away from risk and towards reward. Cloud is the destination, where continual cost optimisation and performance improvements are service fundamentals for Ergo, where the IT estate becomes a hub for innovation and the driver for business transformation.

## Contact us

*ergotechnologygroup.com*
info@ergotechnologygroup.com
+353 1 884 3200

*Connect with us*