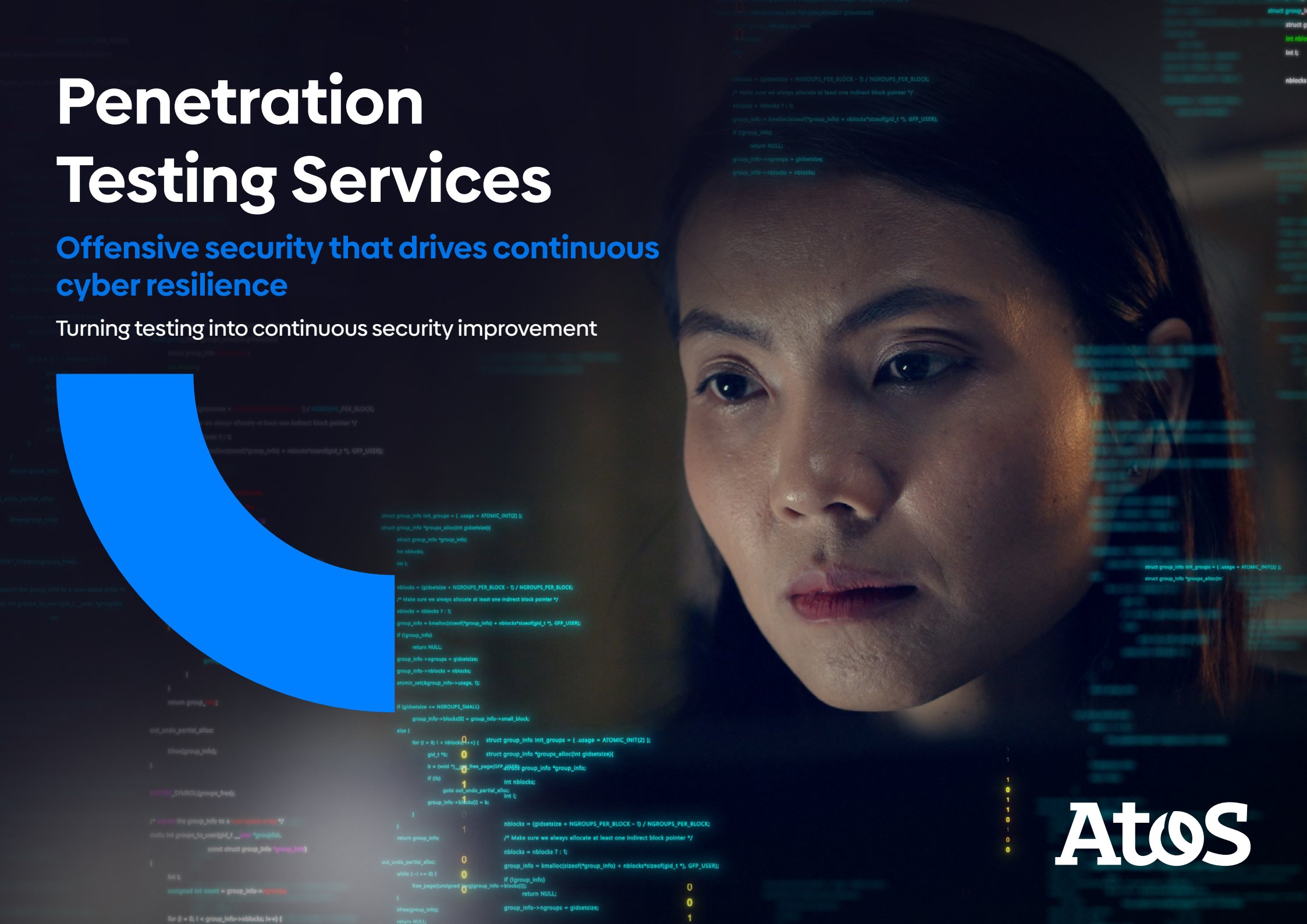
Penetration Testing Services

Offensive security that drives continuous cyber resilience

Turning testing into continuous security improvement



Penetration testing is no longer a point-in-time assessment.

In a threat landscape defined by constant change, organizations must continuously validate how well their defenses withstand real attacks. Traditional penetration testing ends with a vulnerability report. Atos goes further - converting offensive findings into measurable security improvement.

Our Penetration Testing Services simulate real-world adversaries across modern attack surfaces, including networks, cloud environments, Operational Technology (OT) and IoT infrastructures, human factors, and AI systems. The insights gained directly enhance your ability to detect, respond, and recover.

With Atos penetration testing, your organization can:

- Identify real attack paths before adversaries exploit them
- Validate detection and response capabilities under realistic conditions
- Prioritize remediation based on business impact
- Reduce risk continuously - not just at audit time.

Penetration testing becomes a strategic driver of operational resilience.

Expert-led offensive testing across your digital ecosystem

Atos delivers comprehensive penetration testing designed to uncover exploitable weaknesses, challenge assumptions, and strengthen defenses across the full attack surface.

1. Network Penetration Testing

Assess your IT infrastructure through controlled simulations reflecting authentic attacker behavior.
Outcome: Clear visibility into real attack paths and strengthened preventive controls.

2. Cloud Penetration Testing

Identify vulnerabilities and privilege escalation paths across AWS, Azure, GCP, and containerized platforms.
Outcome: Reduced exposure caused by misconfiguration and excessive permissions.

3. IoT and OT Penetration Testing

Evaluate embedded systems and industrial environments using OT-safe methodologies.
Outcome: Increased resilience across safety-critical and operational technology systems.

4. Social Engineering

Simulate phishing, vishing, impersonation, and physical access scenarios.
Outcome: Reduced human risk and improved organizational preparedness.

5. AI Penetration Testing

Secure AI-driven applications against prompt injection, data leakage, and abuse scenarios.
Outcome: Confidence to scale AI initiatives securely.

6. Application Security Testing (including Code Review)

Test business applications and APIs using modern techniques aligned with OWASP and MITRE standards. Combine dynamic testing with secure code reviews (white-box) to uncover deeper vulnerabilities and insecure coding practices.
Outcome: Reduced application risk, improved code quality, and stronger protection of critical digital business processes.

Embedded in the Atos 360° Cybersecurity Lifecycle

Atos Penetration Testing is fully integrated into a lifecycle-driven approach, ensuring findings lead to sustained improvement rather than isolated fixes.

Prevent

Identify architectural weaknesses, misconfigurations, and exposure paths before exploitation.

Detect

Where applicable, assess whether SOC and MDR services recognize real attacker techniques.

Respond

Evaluate incident response processes, escalation paths, and coordination under attack conditions.

Improve

Prioritize remediation and retest to confirm measurable progress.

Optional integration with Atos Managed Security Services ensures that offensive insights strengthen day-to-day defensive operations.

Turning findings into operational readiness

Many providers deliver findings. Atos delivers operational readiness.

What sets Atos apart:

- Realistic adversary-led testing across IT, OT, cloud, and AI
- Integration with Managed Detection and Response (MDR) services
- Business-aligned remediation and risk prioritizationt
- Validation of SOC and MDR detection capabilities
- A shift from compliance-driven testing to continuous resilience

Atos empowers organizations to move beyond vulnerability discovery toward proactive, intelligence-driven defense.

Start turning testing into resilience

Whether you require a focused penetration test or a lifecycle-driven improvement program, Atos supports you every step of the way - from prevention to detection, response, and continuous improvement.

Ready to validate your real-world-exposure?

- Discuss your testing objectives with our experts.
- Build a continuous resilience roadmap.

About Atos:

Atos is a global leader in digital transformation and cybersecurity, delivering end-to-end protection across governance, risk and compliance, identity and access management, cloud security, managed detection and response, and offensive security - helping organizations innovate securely and build lasting resilience.

About Atos Group

Atos Group is a global leader in digital transformation with c. 56,000 employees and annual revenue of c. €7.2 billion (at the go-forward perimeter), operating in 54 countries under two brands - Atos for services and Eviden for products and systems. European number one in cybersecurity and a leader in cloud, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is listed on Euronext Paris.

Find out more about us

atos.net
atos.net/career

Let's start a discussion together

Cys-JG

Atos