Cybersecurity Consulting

Penetration Testing Services

Outside groups constantly probe for weakness and exploitability of your infrastructure. Don't let adversaries to dictate your security strategy, get your Pentest done.

Cyber incidents create significant levels of **financial impact** and **loss of trust.** The resiliency of an organization, more than ever, is directly aligned to the effectiveness of their cybersecurity defenses.

Penetration testing is a process to **continuously evaluate** the security investments from outside-in and help organization to proactively focus on the **prevention** and recovery plans before it is too late.

95% of breaches could be prevented (source: ISOC)[1]

Do you need PenTesting services?

- Are you safe from zero-day attacks?
- Is your wireless network secure and hardened enough against cyberattacks?
- Do you know if your intrusion detection capabilities are effective and where are your weakest controls?

[1] www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/

Trusted partner for your **Digital Journey**

Atos

Identify your weakest spots & remediate

Network mapping

Visualize all devices on the network

Real-world scenario simulation

Run simulation tests for malware, DDoS attacks and other known cybersecurity threats

Regulatory Compliance

Evaluate compliance requirements, identify and remediate anomalies to strengthen organization's compliance

A flexible and comprehensive approach to penetration testing services

Atos penetration testing strategy leverages and employs agile principles and an incremental approach to develop flexible options that align to the organization needs and goals.

Atos uses a systematic and well-structured testing process that identifies and prioritizes vulnerabilities and remediation activities to drive next steps supported by the Atos global pool of skilled and certified pentesting experts.

The key aspects of the Pentesting services are:

- Tied to outcomes / goals / objectives
- Customized to address pressing needs and top threats
- Engaging key players, right sized, at each test phase
- Clearly and timely communicated to authorized parties
- Delivering immediate briefing on critical findings

The initial discussion focuses on the evaluation and and preparation of the testing scenarios required to assess and successfully manage risks.

The next step in the process is to run various attack scenarios - including but not limited to – mimic an external actor, malicious insider, someone with limited access. Pentesting assessments of the infrastructure are performed using an approach that is common across all testing scenarios: discover weaknesses, identify the vulnerabilities and attempt to exploit.

Atos coordinates with key stakeholders, to gain permissions and consensus to perform a controlled exploit of the identified vulnerability and to identify the extend of the exposure and impact.

The results of penetration testing should be used to quantify risks, highlight the control gaps and prioritize investments. This approach eliminates the identified risks and strengthens the effectiveness of a well-rounded cybersecurity program.

Prepare

Evaluate and define the scope, objective and testing scenarios required.

Analyze

Initiate scans and attempt exploits. Investigate the results of the Pentest to identify vulnerabilities, verify and validate the weakness.

Advise

Examine results, perform gap analysis against enterprise policy, security governance program, publish reports and summary.

Roadmap

Device guidance and roadmap to strengthen the security governance, protect critical assets and safeguard investments.

Key characteristics and deliverables

Scan

- Wired Network scans
- Wireless Network scans
- Web-Application scans
- External and Internal scans
- Cloud Infrastructure scans
- Social Engineering/ Phishing scans
- Blind Scans

Assessments

- Remote assessments
- On-site assessments
- Manual and Technical assessments
- Vulnerability assessments

Methods

- Black Box Test
- Network Mapping
- Mimic external attacker
- Real-world test scenarios

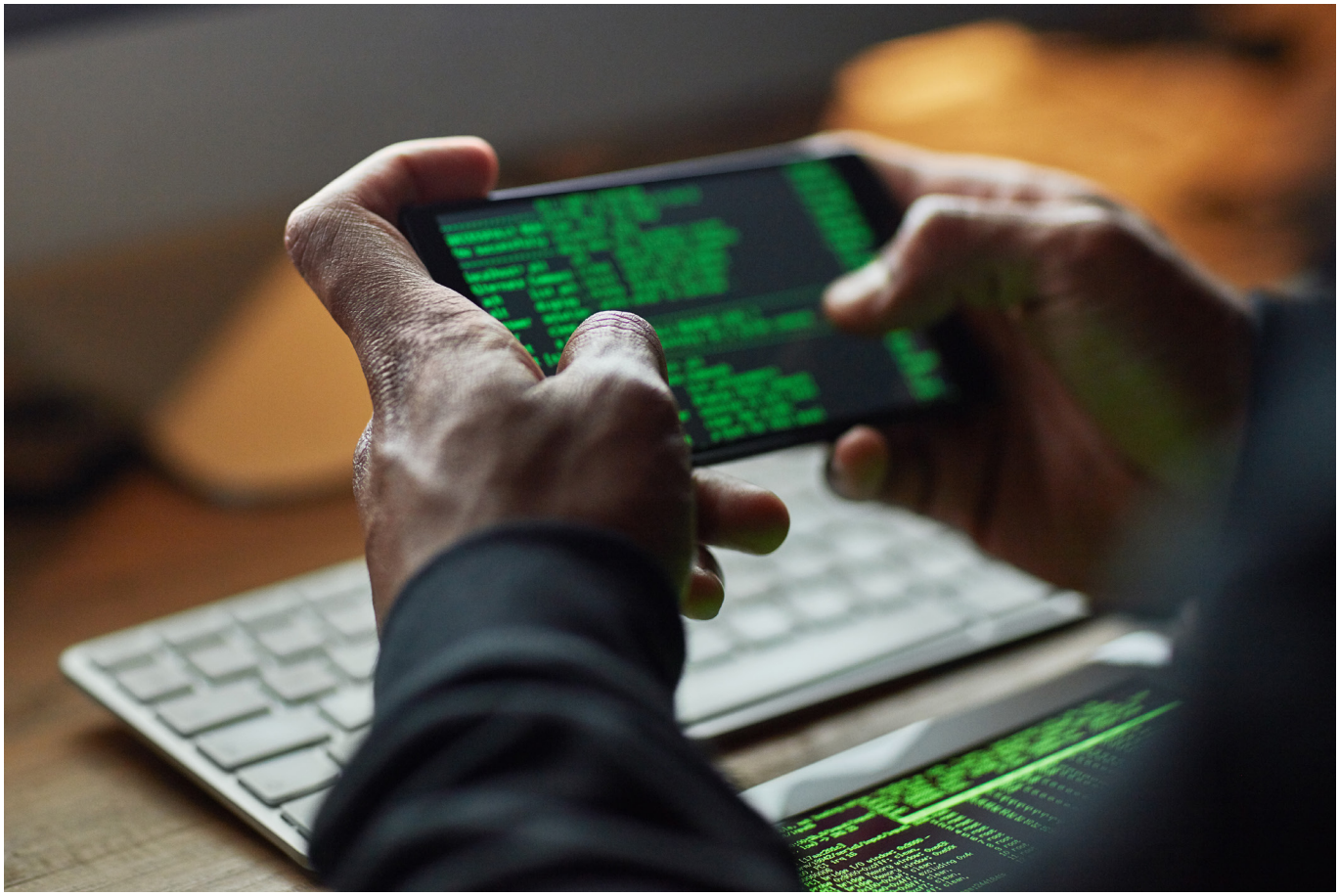
Deliverables

- Executive Summary
- Key Findings
- Plan of Action and Milestones
- Prioritized Recommendations
- Technical Report

Atos added value on penetration testing services

Atos penetration testing services provide insights and actionable intelligence into the strengths and weaknesses of deployed security controls and defenses. They benchmark organizations security posture to industry best practices and deliver prescriptive plan to protect enterprise data, assets and resources.

Atos cybersecurity experts support organizations in bringing operational alignment, consistency and efficiency to enterprise security governance and cybersecurity programs.



About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

For more information: atos.net/penetration-testing-services

CT-200904-MT-FS-Penetration Testing Services-en