ARCTIQ

Architect Security

Penetration Testing Offerings

Enterprise Security

Arctiq offers a comprehensive suite of penetration testing services designed to identify security vulnerabilities, assess risks, and provide actionable remediation strategies. Our penetration testing engagements simulate real-world attack scenarios to evaluate the security posture of your organization's network, applications, and systems. We ensure that our assessments are conducted safely and with minimal disruption to business operations.

Penetration Testing Services

Opportunistic Attacker Penetration Test	OBJECTIVE	Simulate an external attack targeting publicly accessible assets, identifying vulnerabilities and assessing risk exposure.
	KEY ACTIVITIES:	• Open-source intelligence (OSINT) reconnaissance • Scanning for publicly exposed services and potential entry points • Probing vulnerabilities for privilege escalation and data exposure • Selective exploitation of identified vulnerabilities • Optional social engineering campaign (email phishing, vishing)
	DELIVERABLES:	• Comprehensive report detailing identified vulnerabilities • Risk analysis and prioritized remediation guidance • Narrative walkthrough of testing methodology • Executive briefing with actionable security recommendations • Optional retest to verify mitigation
Compromised Insider Penetration Test	OBJECTIVE	Assess risks posed by a compromised internal system, such as malware infections or insider threats.
	KEY ACTIVITIES:	• Enumeration of internal network subnets and security zones • Unauthenticated and authenticated vulnerability scans • Active Directory privilege assessment • Adversarial simulation with optional command-and-control components
	DELIVERABLES:	• Executive summary of findings • Technical report detailing vulnerabilities and remediation steps • Replication guidance for security teams • Prioritized recommendations for security improvements • Final report with optional retesting within 8 weeks
Web, Mobile, and API Penetration Testing	OBJECTIVE	Identify and remediate vulnerabilities in web applications, mobile applications, and APIs to improve security resilience.

	KEY ACTIVITIES:	• Authenticated web application penetration testing
		• Assessment of the OWASP Top 10 vulnerabilities, including:
		  • Broken Access Control
		  • Injection attacks (SQLi, XSS, LDAP, etc.)
		  • Security misconfigurations and outdated components
		  • Insecure authentication mechanisms
		• Optional mobile application penetration testing aligned with OWASP Mobile Top 10

	DELIVERABLES:	• Detailed security findings with replication steps • Risk prioritization and mitigation guidance • Summary of identified vulnerabilities and remediation recommendations • Executive presentation of results • Optional retest within 8 weeks

Engagement Process

Each penetration test follows a structured methodology, ensuring thorough evaluation and clear communication throughout the engagement:

Project Initiation

- Kickoff meeting to define scope and objectives
- Identification of key stakeholders and roles
- Establishment of secure communication and reporting protocols

Assessment Execution

- Vulnerability identification and exploitation testing
- Real-world attack simulation aligned with latest threat tactics
- Compliance with ethical hacking and security best practices

Reporting and Knowledge Transfer

- Delivery of a comprehensive security report
- Remediation roadmap and security enhancement recommendations
- Optional final presentation and stakeholder debriefing

Retesting (Optional)

- Validation of security fixes within 8 weeks at no additional cost
- Update of reports to reflect improved security posture

Our consultants hold numerous security related designations including:

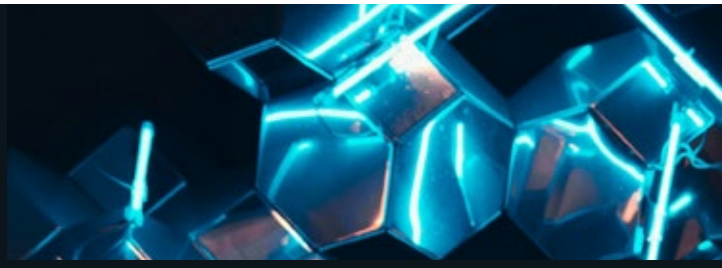
CISM Certified Information Security Manager

CISA Certified Information Systems Auditor

GPEN GWAPT GXPN GCIH OSCP OSWE CISSP

Why Choose Arctiq?

Our key differentiator is the depth of experience and knowledge that our IT security staff possess. Each of our security consultants has years of experience in conducting web application security assessments, vulnerability assessments, PCI audits and providing advisory services such as creating IT security policies, standards, guidelines and procedures.



Real-World Attack Simulation

We replicate actual cyber threats to provide actionable insights.

Expert Security Team

Our specialists bring deep expertise in threat analysis and remediation.

Actionable Reports

Clear, prioritized recommendations to strengthen your security defenses.

No Additional Cost to Retest

Validate fixes within 8 weeks at no extra charge.

Secure Your Business Today

Don't wait for a breach to test your security. Get in touch with Arctiq to schedule a penetration test and protect your organization from evolving cyber threats.

Book a Consultation