PENETRATION TESTING & ADVERSARIAL SIMULATION

Test your defenses *against the cyber attacks happening today.*

ATOM's approach is informed by more than 300 cybersecurity incidents managed over the past six years. We combine rigorous manual testing with targeted tools to uncover what automated scanning alone can miss, then show how each vulnerability could be exploited, what an attacker could reach, and what needs to change.

EVERY ENGAGEMENT FOLLOWS A CLEAR PATH

- **Scope & rules of engagement**
- **Reconnaissance**
- **Threat-informed testing**
- **Controlled exploitation**
- **Clear reporting**

Built for Your Environment

SECTOR-SPECIFIC ENGAGEMENTS

Critical Infrastructure & OT/ICS

Controlled testing of IT, OT, and industrial control environments that identifies risk while protecting critical operations and uptime.

Managed Service Providers

Testing for MSP infrastructure and customer environments, with passthrough services that extend your offering without a dedicated practice.

Private Enterprises

Customized testing for startups through Fortune 500 companies, protecting sensitive data, intellectual property, critical systems, and operations.

Medical Device Manufacturers

Testing connected devices and their ecosystems, from software and cloud to hardware and UART/JTAG, mapped to FDA premarket cybersecurity expectations.

Public Entities

Testing for school districts, counties, and other public organizations, phased around operational and budget requirements.

TESTING SURFACES

- **Azure Cloud**
- **AWS Cloud**
- **Oracle Cloud**
- **AI Integrations**
- **On Premise**
- **Networks**
- **Applications**
- **Endpoint Protections**
- **Remote Workforce**

Schedule your free consultation.

Email **info@theatomgroup.com**

COMPLIANCE & CYBER INSURANCE

Independent testing that supports these requirements

CMMC | NIST 800-171 | NIST 800-53 | SOC 2 | HIPAA | GDPR | PCI DSS | FDA 510(k) | Insurance

MULTIPLE ATTACKER PERSPECTIVES

The Art and the Science

No two environments are identical. ATOM evaluates security from different attacker perspectives.

Black Box

No prior knowledge or internal access, simulating an external attacker targeting your perimeter.

Grey Box

An authenticated user's view, evaluating segmentation, privilege escalation, lateral movement, and compromised-account impact.

White Box

Access to source code, architecture, and credentials to uncover weaknesses not visible from outside.

FOR TECHNICAL TEAMS AND LEADERSHIP

What Good Testing Looks Like

Executive Findings
Risk in terms leadership can act on

→

Technical Evidence
Detailed proof with remediation guidance

→

Structured Retesting
Verify fixes actually worked

Clear documentation of methodology, findings, risk, and remediation supports conversations with auditors, customers, insurers, and other stakeholders. **Retesting of remediated vulnerabilities for up to 180 days is included with every engagement.**

FOR MATURE SECURITY PROGRAMS

Advanced Adversarial Testing

Red Team Operations

Objective-based simulations using real-world tactics across people, processes, and technology to evaluate how you detect and respond to an active attacker.

Purple Team Engagements

Our offensive team works with your defenders to validate detections, tune SIEM and EDR tools, test response procedures, and drive measurable improvement.

Ready to Test Your Defenses?

Contact ATOM to scope an engagement built around your environment, risk profile, and testing objectives.

CONTACT
603-501-0003
info@theatomgroup.com
www.theatomgroup.com