AVERTIUM

PENETRATION TESTING SERVICES

Avertium's expert-led penetration testing uncovers and mitigates vulnerabilities within your organization's IT infrastructure through tailored, real-world attack simulations. Our seasoned professionals deliver realistic assessments and detailed, actionable reports to help you strengthen defenses before attackers strike.

IT'S IN OUR DNA

Avertium has been conducting superior, high-value pen testing for more than 25 years. Drawing on decades of experience, Avertium combines deep technical knowledge, cybersecurity expertise and extensive experience to deliver comprehensive assessments today.

AVERTIUM'S PEN TESTING SERVICES

Avertium's hands-on penetration testing services feature skilled ethical hackers that simulate real-world cyberattacks, uncovering vulnerabilities that automated tools might miss:

- Internal Penetration Test
- External Penetration Test
- Network Penetration Test
- Web Application Test
- Mobile Application Test
- Purple Team
- Red Team
- Social Engineering/Physical Penetration Test

A PROCESS THAT SERVES YOU

SCOPING & PLANNING: TAILORED TO BUSINESS CONTEXT

Emulates realistic threat scenarios relevant to your organization beginning with a thorough discovery phase to understand your business operations, risk posture, and compliance needs.

TESTING EXECUTION: EXPERT LED, REAL-WORLD SIMULATION

blends manual techniques and advanced tools to simulate adversary behavior, including privilege escalation, lateral movement, and chained vulnerabilities exploitation.

REPORTING: ACTIONABLE, BUSINESS-ALIGNED INSIGHTS

Concludes with a thorough report designed for both technical & non-technical stakeholders, providing valuable insight and helping to drive internal buy-in for the detailed recommended remediation.

PEN TESTING AND SECURE AI ADOPTION

AI systems can introduce new attack surfaces and unique risks. Pen testing ensures that your existing security measures (like access controls, encryption, and monitoring) are effective against real-world scenarios that target AI components. Our pen testers simulate these threats to uncover model exposure, API vulnerabilities, data leakage and more.

WE PROVIDE WHAT IT TAKES

By partnering with Avertium, you can ensure your organization is well-protected against cyber threats and can thrive in an always-on, connected world:

1. **Expert Analysis:** Our certified penetration testers go beyond automation, using creative strategies to uncover complex attack paths, chained vulnerabilities, and unique business logic flaws.
2. **Customized Testing:** We tailor our testing to your specific business and environment needs, exposing blind spots where threats like zero-days, privilege escalation, and chained exploits may gain access.
3. **Realistic Scenarios:** Because attackers are human, your defenses should be tested by humans, too. Avertium simulates real-world threats to reveal how your systems would fare against actual adversaries.
4. **Comprehensive Risk Mitigation:** Taking a proactive approach helps you to prepare for, respond to, and mitigate the impact of potential threats, equipping your organization to handle real-world cyberattacks.
5. **Compliance:** Fulfills mandates and recommended best practice guidance for PCI DSS, HITRUST, CIS, FISMA, HIPAA, SOC 2, and more, ensuring that your organization meets industry standards and regulatory requirements.
6. **Detailed Reporting:** Our comprehensive reports deliver clear findings, a risk assessment, and actionable remediation steps to help you understand and address vulnerabilities.

MODERN THREATS REQUIRE MORE

Adaptive threat actors require adaptive defenders

Automated tools follow predefined rules, but attackers can be innovative - chaining vulnerabilities in creative ways, exploiting business logic flaws, and mimicking insider threats and social engineering.

Context matters, and only experts understand it

A skilled tester can prioritize vulnerabilities based on real-world impact, understand the nuances of your environment, and identify risks that scanners miss, like misconfigurations or insecure workflows.

Compliance is not enough, resilience is the goal

Regulations and cyber insurance may require pen testing, but a check-the-box approach alone won't stop a breach. Organizations must address compliance *and* risk.

ASSESS, DESIGN, PROTECT INTEGRATED CYBERSECURITY STRATEGY

A high-quality penetration test should bolster your overall security program:

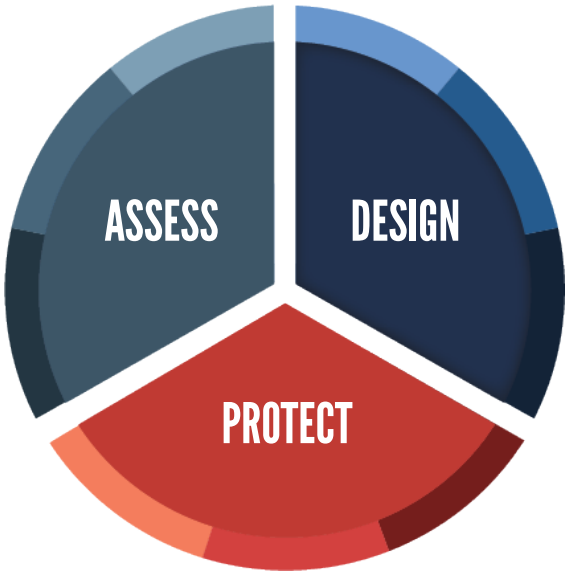
Function	Role of Pen Testing
Vulnerability Management	Validate and prioritize vulnerabilities.
Incident Response	Test detection and response capabilities.
Security Architecture	Reveal design flaws and misconfigurations.
Threat Intelligence	Inform test scenarios based on current threats.

Avertium's signature Assess, Design, Protect approach lays a streamlined and strategic path that evolves with you to apply pen testing findings across your cybersecurity defenses:

Assess: Employ Avertium's pen testing services to assess your defenses' effectiveness and determine how to best protect against emerging threats.

Design: Apply findings from pen testing to plan and architect systems that are both secure and serve your organization's needs.

Protect: Execute secure configurations and deploy managed security to detect and disrupt attacks, 24/7.



ABOUT AVERTIUM

Avertium is a cyber fusion and MXDR leader, delivering comprehensive security and compliance services to mid-market and enterprise customers. Our unique "Assess, Design, Protect" methodology addresses and improves security strategy, reduces attack surface risk, strengthens compliance, and provides continuous threat protection. Avertium maximizes customer security investments and enables customers to focus on growth, innovation, and business outcomes, while assuring that their security infrastructure is resilient and adaptive to evolving threats. That's why customers trust Avertium to deliver better security, improved compliance, and greater ROI.