AVERTIUM

CONTINUOUS PENETRATION TESTING

Most organizations test security once a year. Attackers test it every day.

Avertium's Continuous Penetration Testing risk reduction engine continuously lessens the likelihood and impact of a real-world breach. Our programmatic approach closes the gap between point-in-time assessments and real-world danger by recurringly validating how controls perform as environments, vulnerabilities, and attacker techniques change.

As infrastructure, configurations, applications, and identities evolve, annual testing quickly becomes stale. A continuous model helps organizations identify newly introduced weaknesses, validate exploitability, and focus remediation on the attack paths that matter.

Turn pen testing services into an integrated, outcome-driven offensive security program with Avertium's Continuous Penetration Testing.

WHEN IT MAKES SENSE:

- Your environment changes faster than annual testing can keep up.
- You need to understand what is truly exploitable, not just what appears on a scan.
- You want to test what happens after initial access, including identity abuse and lateral movement.
- You need to validate that existing security truly works under pressure.
- You operate in a controlled industry + need ongoing evidence of security effectiveness.
- You want to show improvement in security maturity and risk reduction.

WHY IT MATTERS

Avertium provides real-world view that connects initial access, attacker movement, and business impact into a measurable path to risk reduction:

- **Governance-first adoption:** Identify new weaknesses as your infrastructure, applications, identities, and configurations change instead of waiting for the next annual test.
- **Identification of real attack paths earlier:** Prioritize what is actually exploitable and focus remediation on the attack paths that could lead to material business impact.
- **Strengthen audit readiness:** Build dated, repeatable evidence that illustrates operating effectiveness over time.
- **Give leadership a clearer risk story:** Provide executive-ready reporting that shows how risk is changing and where improvement is happening.

DELIVERABLES

1) Recurring testing results
with reproduction details and prioritized remediation guidance.

2) Attack-path narratives
that show how single weaknesses can combine into business impact.

3) Executive-ready summaries
with clear risk statements, trends, and program outcomes.

4) Trendable program metrics
with reproduction details and prioritized remediation guidance.

5) Memorandum-style updates
when urgent issues arise, such as newly exploitable vulnerabilities.

WHAT'S INCLUDED

Organizations get the benefit of weekly external penetration testing to monitor changing risk on a continuous basis, supported by a quarterly deep dive that examines higher-impact attak paths, internal weaknesses, and opportunities to strengthen detection and response:

Continuous External Penetration Testing: Recurring testing of internet-facing assets to identify and validate exploitable weaknesses and emerging attack paths.

Social Engineering Assessment: Validate human risk, identity controls, and awareness effectiveness through phishing and related attack techniques.

Internal Penetration Testing: Simulate an assumed-breach scenario to test lateral movement, privilege escalation, and access to sensitive systems or data.

Purple Team Exercise: Validate detection, alerting, and response while improving controls during the engagement.

Customized Targeted Assessments: Focus testing on critical applications, workflows, crown-jewel assets, or high-impact attack paths aligned to business risk.

WHY AVERTIUM

Avertium turns recurring testing into a security program that helps organizations lower breach risk over time. Our experts join recurring validation, human-led attack logic, remediation guidance, and measurable reporting to turn penetration testing from a compliance event into an ongoing source of guidance and assurance.

- → **Human expertise backed by 25+ years of penetration testing experience:** Delivers certified technical depth, expert-powered creativity and intuition, and proven adaptability to the evolving cybersecurity threat landscape.
- → **Continuous, attack-pack-focused validation:** Validates security as threats evolve with deeper testing across identity, cloud, privilege escalation, and real-world attack paths - not just isolated vulnerabilities at one single moment in time.
- → **Effectiveness vs. compliance-only:** Measures how well your defenses actually prevent, detect, and contain attacker activity, rather than simply confirming that controls are present for audit or compliance purposes.
- → **Built-in detection validation:** Includes purple teaming and detection engineering to validate SOC and XDR performance, helping ensure alerts fire as expected and analysts can respond effectively.
- → **Remediation validation included:** Goes beyond basic reporting with detailed, guided remediation support and follow-up validation to confirm issues have been properly addressed and risk has been meaningfully reduced.

ABOUT AVERTIUM

Avertium **is an AI security and compliance leader,** delivering comprehensive solution to mid-market and enterprise customers. Our unique “Assess, Design, Protect” approach 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.