Penetration Testing Overview (2025 Edition)

A penetration test (pentest) is a controlled attack carried out by a third-party security expert, using the same techniques that a hacker would use. It is considered by the security community to be among **the best investments you can make** in your overall security program.

Type	Traditional Pentest	Crowdsourced Pentest	PTaaS (Pentesting as a Service)	Red Teaming	Security Pursuit SNAP
What is it?	Scheduled, deep-dive project testing for vulnerabilities.	Continuous vulnerability discovery via a vetted hacker community.	Launch pentests anytime through a dashboard; integrates with vulnerability management.	Full-scope, real-world attack simulation against your defenses.	Customized traditional pentesting with frequent, vulnerability testing and pentesting.
Attack Vectors	Defined: networks, web apps, wireless, social engineering.	Broad scope; commonly web apps, APIs, and cloud targets.	Primarily web apps, APIs, networks based on provider.	Any vector: technical, physical, social engineering, phishing.	Predefined based on client priorities; covers varied attack vectors.
Goal	Find and exploit vulnerabilities; rank risks; deliver detailed reporting.	Continuously identify vulnerabilities with diverse researcher input.	Provide rapid, repeatable security validation; ideal for DevOps cycles.	Breach defenses stealthily to test detection and response capabilities.	Identify, rank, and update vulnerabilities; keep reports constantly current.
Timeline	2-4 weeks.	Ongoing, 24/7.	Immediate scheduling; flexible.	1-2 months engagement window.	Recurring based on client needs.
Strengths	Deep, focused, customizable; easy to scope and budget.	Fresh perspectives; diverse techniques; continuous feedback.	Fast launch; integrates into CI/CD; frequent validation.	Highest realism; ideal for advanced security testing.	Frequent, client-tuned assessments; highly actionable reporting.
Weaknesses	Static "point-in-time" view; needs regular repetition.	Quality control; expensive; low hanging fruit; can promote hackers.	Shallow depth compared to manual pentests; quality varies by provider.	Potential operational disruptions; depends heavily on Red Team skill.	Higher cost vs. one-off tests due to frequency and customization.
Best Fit For	Companies formalizing security practices; compliance-driven organizations.	High-risk or high-profile companies needing continuous testing.	SaaS developers; companies needing security embedded in software release pipelines.	Mature SOC teams aiming to test detection and response readiness.	Mature organizations wanting continuous updates for customers, BODs, or auditors.
Best Quote	"Best investment to uncover hidden risks."	"Better to get hacked by friends than foes."	"Security testing as fast as our DevOps cycle."	"Prove your security team can stop real threats."	"Stay current and control the process on your terms."
Reporting	Detailed remediation plans; executive summaries.	Real-time dashboards; variable reporting depth.	Dashboards with immediate findings and remediation tips.	Results vary depending on Red Team outcomes; can be minimal or extensive.	Fully customized reporting updated regularly to match client priorities.
Security Pursuit	☑			☑	☑

Contact Security Pursuit for more information on our customized penetration testing services. **Email:** sales@securitypursuit.com