Annual Pen Testing vs PTaaS vs Autonomous Pentesting



01 Annual Pen Testing



Key characteristics

- Manual testing by security experts
- Time-bound assessment
- Detailed findings and remediation report
- Limited visibility between tests

Best for:
Annual security reviews and compliance requirements.

02 PTaaS



Key characteristics

- On-demand or recurring testing
- Centralized findings dashboard
- Collaboration with security experts
- Retesting and remediation tracking

Best for:
Teams needing more frequent testing and streamlined remediation.

03 Autonomous Pentesting



Key characteristics

- Frequent, repeatable security testing
- Automated attack-path validation
- Faster feedback after environmental changes
- Scalable testing with reduced manual effort

Best for:
Organizations seeking scalable, ongoing security validation.

Evaluation Criteria	Annual Pen Test	PTaaS	Autonomous Pentesting
Testing frequency	Scheduled	On-demand or recurring	Frequent or continuous, depending on configuration
Primary approach	Expert-led manual testing	Platform-enabled testing, often expert-led	Automated attack simulation and validation
Speed of feedback	After assessment	Faster access to findings	Rapid feedback between runs
Scalability	Limited by testing scope and resources	Platform-supported	High for repeatable testing
Human expertise	Central to testing	Often integrated	Expert oversight varies by solution
Ideal outcome	Periodic assurance	Streamlined testing and remediation	Repeatable validation at scale

www.ampcuscyber.com | letsconnect@ampcuscyber.com