

Agentic Penetration Testing

AI-driven testing that validates real-world exposure around-the-clock, not once a year

Why Sekuro

Attackers don't test your defences once a year, so why should your penetration testing stop there? Operating at machine speed, our Agentic Penetration Testing service augments our experienced Offensive Security team. Gain valuable insights across your environment scanning your attack surface continuously.

Built by cybersecurity professionals with decades of first-hand offensive security experience, our service focuses precisely where it adds the most impact. We deliver high-value findings that validate deeper exploration; not informational noise. The result is automated testing that reflects how attackers operate today: fast, continuous, unconstrained by the cloud and supply chains. Protect your attack surfaces that traditional black-box testing was never scoped to cover.

Service Overview

We deploy AI agents to scan your attack surface continuously, on demand, removing the 'next available resource' scheduling constraints that limit traditional annual testing. Agents run exploitation and validation at machine speed, while our human experts concentrate their time on exploring and confirming high-value findings, ensuring depth where it matters most. Set budgets to meter usage according to your requirements, and scale testing from a single assessment to many concurrent tests for continuous, real-world validation of your security posture.

Deploy individually or unlock deeper insights combined with Agentic Vulnerability Management and Agentic Security Operations Centre through our SekuroOne platform. The result is a hyper-intelligent, evidence-based view of your risk exposure that strengthens over time.

Key Benefits

- Validate your exposure every day with continuous, unlimited testing using agentic AI.
- Scale agentic capacity to run multiple concurrent tests, with zero scheduling limitations.
- Reserve human expertise for high-value findings, maximising the value of every expert hour.
- Automatically feed findings into Agentic Vulnerability Management so exploitable conditions are tracked and remediated.
- Set budgets to your testing requirements with flexible, metered billing.
- Extend coverage beyond traditional black-box scope to cloud, supply chain, and AI attack surfaces.

Our Approach

Scoping and Planning

Define objectives, scope, and rules of engagement aligned to your business priorities, risk tolerance, and operational requirements.

Agentic Exploitation

Agents safely assess and validate exploitable weaknesses at machine speed, running concurrently across your environment.

Human-Led Deep Dive

Our experienced offensive security practitioners focus their expertise on exploring and validating high-value findings identified by the agents.

Continuous Reconnaissance

Agents continuously map exposed assets and attack surfaces, viewing your environment from a real attacker's perspective.

Integrated Findings Handling

Automatically feed validated, exploitable findings into Agentic Vulnerability Management so nothing is tracked in isolation or lost.

Reporting and Remediation Guidance

Deliver clear, risk-based findings with actionable remediation guidance for both technical and executive audiences, backed by continuous evidence rather than a single test cycle.