

AI Security Assessment & Roadmap

Move forward with confidence grounded in a clear, practical pathway and a pragmatic view of your AI security posture

Why Sekuro

AI adoption shouldn't be held back by unanswered security questions. We'll deliver the clarity you need to move forward, not just another report that gathers dust. Our strategy, governance and offensive security experts work as one to deliver a complete picture across every security domain your AI adoption touches. Findings are unified across multiple vendors in one coordinated engagement.

We deliver a dual capability in one engagement, both securing your AI adoption and using AI to strengthen your security operations. Whether you're rolling out Copilot, Claude, Agent 365, a custom chatbot, or an in-house model, our approach is tailored to fit your unique environment.

Service Overview

Security foundations must be on point before scaling AI services consumption, building agents to automate processes, or embedding AI into your development pipeline. Our AI security assessment reveals where your posture stands today, whether AI visibility and controls are adequate, and what must be addressed before adoption goes further. Optional governance and offensive security assessments include ISO 42001 Gap Assessment and LLM/AI Offensive Security Testing. Engagements are tailored to your organisation's size, from small business to large enterprises with complex, multi-platform environments. We revise our assessment process continuously as AI develops, so you are assessed against frontier capability as it arrives.

KEY BENEFITS

- Understand your AI security posture across all the domains that matter, not just the obvious ones.
- Receive tailored findings for specific roles, including a board-ready executive summary.
- Build a roadmap around your actual environment and priorities to enable immediate action.
- Surface the highest-severity vulnerabilities in your AI deployments.
- Get a clear baseline and a practical path towards AI certification readiness.
- Receive a shared, aligned plan that covers both AI consumption and AI development.

Our Approach

Discovery

Gather insights from identity and data owners and your security operations team to gain a complete picture of what's in place, what's in motion, and where the exposure sits.

Security Posture Assessment

Evaluate your controls and assess AI-specific risk across ten domains: governance, privacy, people, identities, endpoints, networks, infrastructure, applications, data, and analytics.

Governance Requirements

Assess your AI governance framework against ISO 42001 to measure maturity across policy, accountability structure, and risk management practices. Identify the gaps and define a practical path to close them.

Adversarial Testing

Test your AI deployments against the techniques most likely to cause real harm—including prompt injection, data exfiltration, jailbreaks, and privilege escalation through agent identities. Audit what your AI agents can actually access and flag where permissions go beyond what they need.

Report and Roadmap

All findings come together in a maturity heatmap, a target future state, and a prioritised multi-year roadmap. Effort, priority, and technology recommendations are mapped to each initiative, delivered alongside a current state assessment and an executive summary your leadership team can take straight to the board.