AI SECURITY ASSESSMENT

THE CHALLENGE

AI tools can help employees work faster and give organizations new ways to use information. They can also make sensitive data easier to discover, introduce new integrations and automated actions, and produce responses that require verification. Understanding these risks starts with knowing which AI systems are in use, what they can access, and how people rely on them. Risks vary by deployment: an employee assistant may expose broadly shared files, while a custom agent may connect to business systems or perform actions with elevated permissions.

OUR APPROACH

TruSec Consulting works with your team to define an assessment around your AI use cases and priorities. The scope may include commercial platforms such as Microsoft Copilot, ChatGPT, and Claude, as well as custom applications and agents. We identify the systems and data in scope, review relevant controls, and perform agreed testing to support practical risk reduction. We work with stakeholders to establish appropriate testing boundaries, identify the access and documentation needed, and focus on scenarios that matter to the organization.

ASSESSMENT SERVICES

AI GOVERNANCE AND INVENTORY

Identify AI tools and use cases, review policies and oversight, and assess access, monitoring, vendor dependencies, and third-party risks.

AI APPLICATION SECURITY TESTING

Assess agreed applications for prompt injection, information disclosure, and insecure handling of AI-generated output and downstream actions.

DATA ACCESS AND CONFIGURATION

Review data access, sharing, and configuration. Separately scoped cloud and network testing can address AI hosting, storage, and exposure.

AGENTS AND INTEGRATIONS

Review connected tools, agent permissions, authorization boundaries, and controls over automated actions, including approvals where applicable.

TESTING AND REVIEW

Depending on the agreed scope, we may review a sample of user roles, configurations, data sources, and application workflows. Hands-on scenarios can examine whether sensitive information is exposed, safeguards respond as intended, and connected actions remain within their authorized boundaries. Testing is coordinated with your team and tailored to the environment and available access. Provider-owned infrastructure may require a review of available assurance documentation.

ENGAGEMENT AND DELIVERABLES

Start with discovery and scoping or a focused assessment of an existing platform or application. We provide a report of observed risks, supporting findings, and prioritized recommendations tailored to the agreed scope. Findings identify the affected systems, potential impacts, and practical next steps. Results can be discussed with technical and business stakeholders to support remediation planning. Follow-on testing and remediation validation can be defined as needed.