

# AI Security Rapid Assessment

Identify priority AI security risks and define a practical 90-day action plan in 7-10 business days.

## ENGAGEMENT SNAPSHOT

**Duration:** 7-10 business days

**Investment:** \$8K-\$10K fixed fee

**Scope:** Focused review of 3-5 priority AI use cases, platforms, or workflows

**Format:** Rapid technical assessment for direct or partner-led delivery

## Typical Challenges

- Limited visibility into enterprise AI usage and shadow AI
- Sensitive or regulated data exposed to AI tools and platforms
- Unclear governance, ownership, and approval of AI use cases
- Third-party AI and model providers introducing unknown risk
- AI-enabled workflows deployed without technical security validation

## Assessment Focus Areas

- AI / GenAI inventory and priority use cases
- Data flows, sensitive-data exposure, and trust boundaries
- Identity, privilege, non-human identities, and access controls
- LLM, RAG, API, model/provider, and agentic AI security
- Logging, monitoring, incident readiness, and governance alignment

## Technical Methodology

**Hands-on technical assessment - not a paper audit.** Symosis combines stakeholder workshops with architecture review, targeted configuration validation, and open-source discovery/analysis tooling where appropriate.

### 1. Discover & Scope

Identify 3-5 priority AI use cases, systems, data sources, owners, and technical artifacts.

### 2. Architecture & Config Review

Review architecture, data flows, trust boundaries, identity, logging, and relevant platform configurations.

### 3. Technical Validation

Use open-source discovery/analysis tooling and targeted control checks to validate exposure and key security gaps.

### 4. Prioritize & Roadmap

Rank findings by business impact, exploitability, and effort; define practical remediation actions.

## Assessment Approach

| 1               | 2                       | 3                | 4                    | 5                  |
|-----------------|-------------------------|------------------|----------------------|--------------------|
| <b>Discover</b> | <b>Review</b>           | <b>Validate</b>  | <b>Prioritize</b>    | <b>Roadmap</b>     |
| AI landscape    | Architecture + controls | Technical checks | Risk-ranked findings | 90-day action plan |

Focused, technically grounded assessment for rapid AI risk identification and prioritization.

## Deliverables

- Executive AI risk summary
- Key findings and risk themes
- Priority architecture and control gaps
- Practical remediation recommendations
- 90-day action plan and executive readout

## Business Value

- Identify the most important AI security gaps quickly
- Improve visibility into AI usage and sensitive-data exposure
- Reduce third-party and access-control risk
- Support FY27 planning and governance readiness
- Provide leadership with a defensible action plan

## Why Symosis

**Engineering-Led:** Technical, architecture-aware assessments. | **Senior-Led:** Experienced practitioners lead the work. | **AI + Cybersecurity:** Governance, architecture, engineering, and security. |

**Enterprise Experience:** Fortune 500, technology, healthcare, and regulated environments.

**Scope note:** Focused assessment of selected AI use cases; not a full ISO/IEC 42001 certification assessment, enterprise-wide discovery program, source-code review, or penetration test. Partner delivery available.