DevSecAI

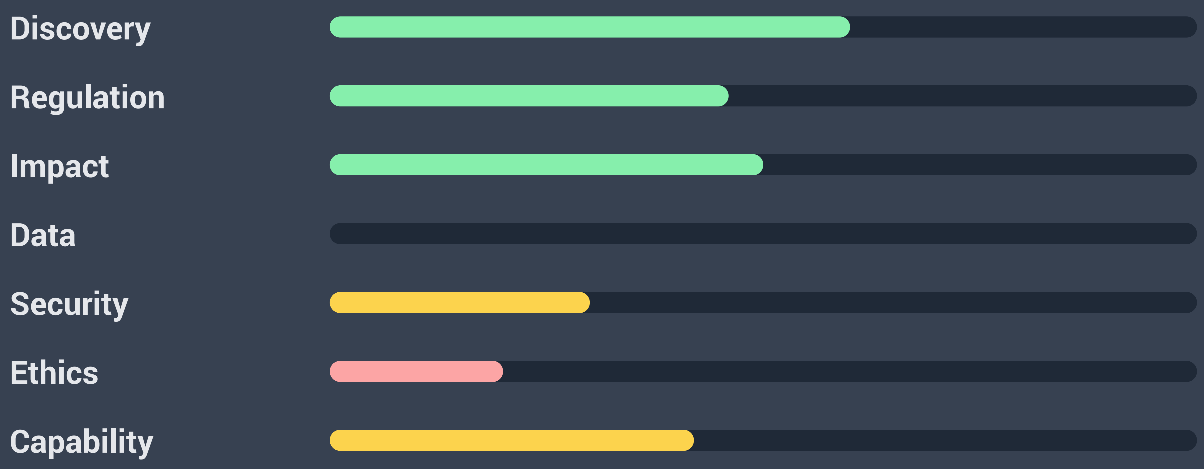
Security Assessment Report

Overall AI Security Maturity

Level: Developing

Basic AI security policies are in place, but significant gaps remain. Your organisation should focus on formalising processes and expanding controls.

Key Domain Insights



Priority Recommendations

1. AI Asset & Risk Discovery

These two services will provide a discovery of AI systems and tooling across your organisation and an evaluation of the associated risk impact. This will give you a centralised AI tooling view, allowing you to prioritise your AI risks in line with regulation.

2. Comprehensive AI Security Maturity Assessment

Conduct a full AI Security Maturity Assessment aligned to the DSAIF that is repeatable and will be taught to your teams to use themselves. Coupled with the AI Tool Secure Config Review, this will highlight your AI security gaps and vulnerabilities across your organisation including within AI models and their deployment. The maturity improvements and risks will be documented and tracked in an AI Risk Tracker that is automated.

3. AI Threat Landscape & Strategic Roadmap

Understanding the global AI threat actors that will exploit your AI systems and how they do it is essential to remaining on the front-foot and will provide the context to the AI Security Strategy. The Security Strategy will provide a deliberate view of your approach to AI security as the business embraces AI. This will be finalised with a one-year and three-year roadmap to improve maturity and mitigate risks aligned to achieving your strategy and improve your overall AI security maturity score.

4. AI Security Implementation Program

Putting in place the following tools and capabilities: ML Model Data Poisoning Scanners and testers, ML Inference scanners, AI Threat modelling Workshops, DevSecAI Champions program, ML Data Tagging, Pre Trained Model assessments, AI Security training workshops, Data Anonymisation and Masking, ML security performance monitoring, Adversarial Attack Detection and more.

Next Steps

Contact DEVSECAI for a comprehensive AI security roadmap tailored to your organisation's specific needs, priorities, and budget constraints.