RETAIL & CONSUMER | AI SECURITY & GOVERNANCE

Establishing an AI security program for a retail supercenter chain

A retail supercenter operating more than 250 stores across the United States, with over 70,000 team members, engaged **Optiv Consulting** to stand up the governance, controls, and security needed to adopt AI safely at scale.

SECTOR	FOOTPRINT	PEOPLE	FRAMEWORKS
Retail supercenter	**250+ US stores**	**70,000+**	**NIST AI RMF, OWASP**

THE CHALLENGE

AI was expanding quickly across the business, and its growing footprint meant any new security program would carry significant change impact for customers and employees. The client needed to secure AI deliberately, with governance, controls, and clear ownership in place before adoption outpaced oversight.

OUR APPROACH

- Built a multi-workstream plan integrating Security Risk Management, Application Security, and Security Operations.
- Ran stakeholder discovery to sequence the work around interdependencies, availability, and effort.
- Developed an Integrated Compliance Framework drawing on the NIST AI RMF, OWASP AI Exchange, and NIST Privacy Framework.
- Recommended tooling across governance, risk profiling, and software composition analysis, including ServiceNow, Veracode, and Azure DevOps.

5 program segments

Risk management, SDLC, threat modeling, AI test cases, and AI security operations

BUSINESS RESULTS

- Delivered an executive readout mapping current and future state across the five program segments.
- Produced detailed deliverables the client could act on immediately, including tooling recommendations.
- Set the foundation for an ongoing engagement to expand the AI program.