# OSAI

- Reconnaissance for AI Targets
- Attacking AI Agents
- Attacking Multi-Agent Systems & A2A Protocol
- Exploit RAG Pipelines
- Attacking Embeddings
- Attacking Model Context Protocol and Tool Surfaces
- Supply Chain Attacks on AI/ML Systems
- AI Infrastructure and Deployment Exploits
- Threat Modeling for AI-Enabled Targets
- Assembling The Pieces - Capstone Red Team Engagement

# Reconnaissance for AI Targets

# Attacking AI Agents

# Attacking Multi-Agent Systems & A2A Protocol

# Exploit RAG Pipelines

# Attacking Embeddings

# Attacking Model Context Protocol and Tool Surfaces

# Supply Chain Attacks on AI/ML Systems

# AI Infrastructure and Deployment Exploits

# Threat Modeling for AI-Enabled Targets

# Assembling The Pieces - Capstone Red Team Engagement