AGENTIC AI SECURITY · POWERED BY ORY

Agentic AI Security Workshops

À la carte 90-minute workshops for AI agent and non-human identity governance

OVERVIEW

AI agents are already running on static keys and broad permissions.
And most teams can't say how many they have.

Numberline helps organizations apply Zero Trust thinking to agentic AI programs, while Ory provides the identity, token, and policy controls needed to operate agents securely.

Each focused 90-minute module can be run on its own or combined into a customized four-session day, onsite or remote.

6	4	2
90-MINUTE WORKSHOPS	WORKSHOPS = 1 FULL DAY	DELIVERY MODES ONSITE / REMOTE

ENGAGEMENT PATH

Workshops map to four phases — pick any combination or run them in sequence.

PHASE 01	PHASE 02	PHASE 03	PHASE 04
Assess	**Design**	**Control**	**Operate**
Agent inventory • Risk	Architecture • Use cases	Policy • Integration	Governance • Response

WORKSHOP PORTFOLIO

Each 90-minute workshop stands alone or combines into a four-session engagement.

WORKSHOP 01 · Assess phase

Agentic AI Taxonomy & Risk Deep Dive

Inventory current and planned AI agents and expose static-key, over-permissioning, and governance risk.

WORKSHOP 02 · Design phase

Agent Architecture & Design

Define the target design for Ory Agent Security, integrated with your identity stack and MCP servers.

WORKSHOP 03 · Design phase

Agent Use Case Design & Review

Clarify what agents may and may not do, where humans remain in the loop, and how delegation should work.

WORKSHOP 04 · Control phase

Agent Authorization & Policy Configuration

Design Ory Agent Security capability-token and permission policies for secure agent actions.

WORKSHOP 05 · Control phase

Agent Framework & Application Integration

Plan agent plugins, MCP server, audit instrumentation, staged rollout, and kill-switch patterns.

WORKSHOP 06 · Operate phase

Governance, Audit & Incident Response

Create the governance model, anomaly monitoring approach, revocation workflow, and incident runbook.

SAMPLE FULL-DAY BUNDLES

Example four-workshop combinations, tailored to the client's architecture, priorities, and maturity.

BUNDLE A

Agent Security Foundations

Best for teams starting their agent program

01 Agentic AI taxonomy
02 Agent architecture & design
03 Agent use case design
04 Agent authorization & policy

BUNDLE B

Build & Operate

Best for teams ready to implement

01 Agent architecture & design
02 Authorization & policy
03 Framework & app integration
04 Governance & incident response

BUNDLE C

Risk-Led Rollout

Best for risk and compliance-driven programs

01 Agentic AI taxonomy
02 Agent use case design
03 Authorization & policy
04 Governance & incident response

WHO SHOULD ATTEND

- CISO and Security leadership
- IAM and identity teams
- Security architects
- AI and app engineering leads
- AI and platform engineering leads
- Risk and compliance teams
- SOC / incident response teams

CLIENT OUTCOMES

- ✓ Clarity on where AI agents introduce new identity and authorization risk
- ✓ A practical design for secure agent interactions and permissions
- ✓ A prioritized action plan for rollout, governance, and incident response

DELIVERABLES

- Workshop readout with agent-specific findings and recommendations
- Target-state guidance for Ory Agent Security usage
- Prioritized next-step roadmap for secure agent rollout

NOT SURE WHERE TO START?

Let's plan it together

Tell us where you are today and we'll set up a free 30-minute planning call to pick the right workshops for your team.

Contact Numberline
info@numberlinesecurity.com