AI Security Bootcamp for Leaders – Half-Day Workshop Agenda

Theme: "Leading AI Securely: Risk, Governance, and Trust"

This half-day format provides a focused, high-impact AI security session tailored to executive leadership responsibilities

Morning Session: Understanding AI Security Risks and Leadership Imperatives

8:30 AM – 8:45 AM | Welcome and Opening Remarks

- Workshop objectives and security leadership context
- Quick participant introductions

8:45 AM – 9:15 AM | AI Security Landscape Overview

- Key AI-specific cybersecurity risks including adversarial attacks, data poisoning, model inversion, and prompt injection
- Business impact and reputational risks of AI security failures

9:15 AM – 9:45 AM | Strategic AI Risk Management

- Leadership role in AI threat modeling and vulnerability management
- Aligning AI security risks with organizational risk frameworks

9:45 AM – 10:15 AM | AI Governance and Ethical Security

- Building trustworthy AI: transparency, fairness, compliance
- Governance frameworks and executive accountabilities

10:15 AM – 10:30 AM | Energizer Break

Late Morning Session: Actionable Leadership for Secure AI Adoption

10:30 AM – 11:15 AM | Case Study: Navigating an AI Security Breach

- Scenario-based exercise on decision-making, communication, and mitigation
- Lessons for crisis readiness and stakeholder management

11:15 AM – 11:45 AM | Executive Workshop: Developing a Secure AI Roadmap

- Guided breakout work to identify priority security controls and governance steps
- Peer feedback and facilitator guidance

11:45 AM – 12:00 PM | Closing and Commitment

- Summary of key takeaways
- Leadership pledge for fostering an AI security culture
- Resources and next steps