MILEVA SECURITY LABS

AI SECURITY WORKSHOPS

Do you know your organisation's AI risk?

Mileva Security Labs offers training and advisory services at the intersection of AI and cyber security. Our AI Security workshops help your organisation understand the strategic and technical considerations for securing AI systems.

Is your organisation compliant with AI standards and regulations?

While **94% of companies report using AI**, only **14% implement any AI security measures**. However, **100% of AI systems are vulnerable to disruption, deception and data exposure** - incidents that can result in significant financial losses, reputational damage, and regulatory penalties. In the face of increasing AI regulation, knowledge is our best defence.

Unsure where to start?

Our Intro to AI Primer is the launch point to secure your organisation’s AI future

INTRO TO AI PRIMER

Kickstart your AI Security journey with our introductory primer. This workshop is for you, regardless of your level in the organisation or technical proficiency. We'll demystify AI technologies and buzzwords, explore appropriate use, safety and security risks, review the policy and governance landscape, and discuss emerging trends.

Who it is for: everyone **How long it is:** 2 hours
What it is best for: a stand-alone workshop for general audiences, a lunch and learn, or as a primer before running the other workshops

WORKSHOPS

DISCOVER: UNDERSTANDING AI SECURITY

Explore the fundamental principles of AI security, real-world case studies, best practices, and emerging trends in the field. Leave with a deeper understanding of the unique challenges posed by AI security and the confidence to start discussions about organisational security measures to protect your AI-driven initiatives.

Who it is for: anyone who has an understanding of what AI is, and/or has attended Intro to AI
How long it is: 3 hours
What it is best for: ensuring everyone understands their obligations in adopting and implementing AI securely

DECIPHER: LEADING AI-DRIVEN ORGANISATIONS

Discover what it takes to lead your organisation in the realm of AI security. Explore real-world case studies and stay up-to-date with the ever-evolving landscape of AI-related regulations and compliance standards. Understand which AI risk management policies and framework your organisation should be implementing.

Who it is for: leaders and managers
How long it is: 3 hours
What it is best for: an extension to the Intro to AI, and Discover workshops, catered to leadership

DESIGN: INTRODUCING AI TO YOUR TEAM

Through case studies, participants explore suitable AI uses, learning about the Data Maturity model, change management theories, and strategies for scaling AI projects from pilot stages to full-scale operations while fostering an innovative culture. Interactive group activities encourage attendees to apply these insights directly. This workshop is a must-attend for those looking to strategically implement AI in their industry.

Who it is for: anyone whose team is considering introducing AI
How long it is: 3 hours
What it is best for: an extension to the Intro to AI, catered to non-technical teams considering third party AI tools

WORKSHOPS

DELIVER: BUILDING AI TO BE SECURE BY DESIGN

Tailored for technical managers and practitioners, dive deep into topics like model selection, data strategy, and deployment to ensure your AI systems are secure by design. Learn how to implement best practice AI safety techniques that minimise bias and maximise safety and alignment. Develop AI systems that are not only cutting-edge but also inherently secure, minimising risks and maximising impact.

Who it is for: technical managers, data scientists and developers
How long it is: 14 hours (2 days)
What it is best for: technical teams who want to ensure their AI systems are safe and secure by design

DETECT AND DEFEND: AI FOR SECURITY

Delve into the diverse applications of AI in security, explore real-world case studies, and dive deep into the strategies and technologies that enable us to leverage AI's capabilities effectively. From threat detection and anomaly analysis to intelligence gathering and decision support, AI is poised to revolutionise how we approach security challenges - learn how it can augment your teams safely and securely.

Who it is for: anyone who has attended Intro to AI, and works in security
How long it is: 3 hours
What it is best for: teams who work in security (or are security adjacent) who want to leverage AI safely and securely

HOW IT WORKS

Run each of our workshops as a stand-alone course, or bolt them together for maximum value

Package 1: Intro to AI + Discover: Understanding AI Security + Detect and Defend: AI for Security
8 hours (1 full day)
Great for teams who want to gain a holistic understanding of the intersection of AI and security - learn how to leverage AI for security, as well as how to ensure your AI is inherently secure

Package 2: Intro to AI + Discover: Understanding AI Security + Decipher: Leading AI-Driven Organisations
8 hours (1 full day)
Great for managers and leaders who want to go from 0 to 100 in what AI is, which AI risks exist, and how to implement AI securely in their organisations

Package 3: Discover: Understanding AI Security + Deliver: Building AI to be Secure by Design
17 hours (2.5 days)
Great for data science and development teams who are currently building AI products, and want to ensure they are implementing best practice in safety and security

Package 4: Intro to AI + Customisation
1-2 hours
Great for lunch and learns, seminars and keynote sessions at conferences. We offer customisation packages to deliver our ready-to-go Intro to AI primer in ways that best suit your organisation, incorporating specific case studies, tools, or changing session length

> *I never knew how easy it would be to implement AI attacks, Mileva's content is needed now more than ever*
> *- Global cybersecurity firm*

MILEVA
SECURITY LABS

Join the mission, and let's secure the future of AI together