AI/ML

AI Safety & Security Training

Understanding operational concerns and risks of AI-based systems

While many professionals are somewhat familiar with AI and ML concepts, there remains a significant gap in understanding the specific dangers and risks these technologies pose. Our course is tailored to fill this gap, providing a comprehensive understanding of AI safety and security that goes beyond basic knowledge to practical, actionable insights.

Module 1:	AI/ML Fundamentals
Module 2:	Operations and Pipeline
Module 3:	Vulnerabilities and Remediation
Module 4:	Risk Assessment and Threat Model
Module 5:	Mitigations, Controls, and Risk Reduction

Our Training

- Expert-led training
- On-site or virtual
- Group discounts

Our training mainly consists of five modules, featured on the left, tailored to your company's needs.

Designed For

- Cybersecurity experts
- Data scientists
- Software engineers
- IT professionals

Enhance your knowledge and awareness of AI safety, security, risks, and mitigations

Now scheduling for Summer and Fall 2024!

SCHEDULE A MEETING WITH TRAIL OF BITS

ABOUT TRAIL OF BITS

Since 2012, Trail of Bits has helped secure some of the world's most targeted organizations and devices. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code.

www.trailofbits.com

AI/ML | Application Security | Blockchain | Cryptography | Research & Engineering