SOEBIT Cybersecurity AI Foundation SCAIF

1 day edition

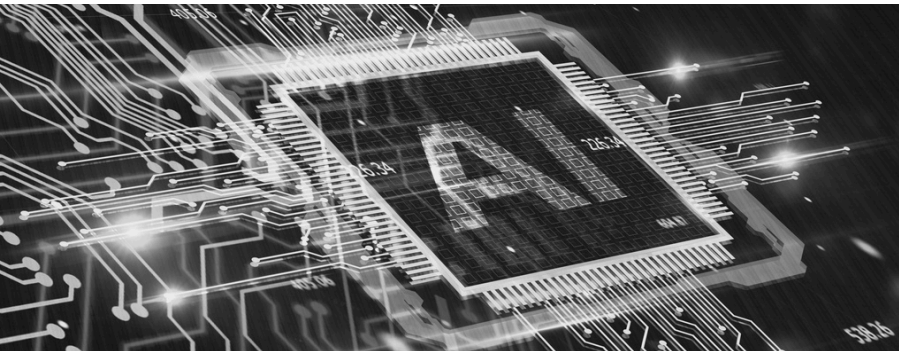
Course Overview

The SOEBIT Cybersecurity AI Foundation (SCAIF) training course delivers a comprehensive and practical introduction to the convergence of cybersecurity and artificial intelligence.
This course explains the fundamentals of cybersecurity and AI, covering key concepts such as machine learning, deep learning, generative AI, large language models (LLMs), and AI agents. It also introduces how AI is applied across cybersecurity domains including threat detection, incident response, malware analysis, and offensive security.

Participants develop a strong conceptual foundation in how AI and cybersecurity intersect, where AI provides advantages over traditional approaches, and how it introduces new risks such as adversarial manipulation, prompt injection, model theft, and data leakage. The course also addresses governance, risk management, and responsible AI use in security contexts.
By the end of this program, learners gain the knowledge required to evaluate AI-driven security solutions, participate in informed technical and strategic discussions, and understand organizational readiness for AI adoption in cybersecurity.

Course agenda

- Module 1: Introduction to Cybersecurity and AI
- Module 2: Artificial Intelligence Fundamentals
- Module 3: Generative AI, LLMs, and Modern AI Systems
- Module 4: AI in Cybersecurity
- Module 5: Security risks and attacks against ai
- Module 6: Securing AI systems
- Module 7: AI governance, risk and responsible use
- Module 8: Current trends and practical applications



PREREQUISITES

No prior cybersecurity, AI, advanced mathematics, or programming experience is required.

training@soebit.com
+31 6 107 55 479 (NL)
+91 95469 23827 (IN)
https://soebit.com

Why should you attend?

As artificial intelligence becomes deeply embedded in cybersecurity tools and operations, understanding its capabilities, limitations, and risks has become essential for both technical professionals and decision-makers. AI introduces powerful new defenses, but also expands the attack surface and creates new categories of vulnerabilities. Many organizations struggle to separate realistic AI security opportunities from hype, leading to misaligned investments or unpreparedness for emerging threats such as AI-powered phishing, deepfakes, and autonomous cyber operations. This course enables participants to clearly understand how AI operates in cybersecurity, what it can and cannot do today, and how organizations can approach AI-driven security in a structured and informed manner.

Who should attend?

This course is ideal for professionals across technical and non-technical roles, including:

- Students, beginners, and early-career professionals building foundational knowledge of cybersecurity and AI
- Managers and decision-makers responsible for security strategy, innovation, or long-term risk planning
- Engineers, architects, and researchers interested in AI and cybersecurity concepts and applications
- Information security professionals seeking to enhance their knowledge of AI-driven threats and defenses
- Professionals involved in R&D, innovation programs, or advanced computing initiatives
- Anyone responsible for understanding the business, security, or strategic implications of AI in cybersecurity

What You Will Learn

By completing this course, you will be able to:

- Understand the fundamental concepts and principles of cybersecurity and AI
- Explain how AI, machine learning, deep learning, generative AI, and LLMs operate
- Describe how AI is applied to threat detection, threat intelligence, and incident response
- Identify common applications and limitations of AI in cybersecurity
- Recognize the impact of AI on offensive and defensive security operations
- Assess organizational readiness for AI adoption in cybersecurity

Key Skills Gained

- Cybersecurity and AI conceptual literacy
- Understanding of AI/ML models, GenAI, and LLM fundamentals
- Threat detection and security monitoring awareness
- AI risk and attack surface analysis
- Human-AI collaboration in security operations
- Informed evaluation of AI-driven security claims and use cases

Career Benefits

After completing this course, you will be better prepared to:

- Participate confidently in AI and cybersecurity discussions and initiatives
- Support informed security and technology decisions
- Assess AI-related security risks and opportunities
- Contribute to organizational AI security readiness planning
- Navigate emerging opportunities and limitations of AI in cybersecurity

training@soebit.com
+31 6 107 55 479 (NL)
+91 95469 23827 (IN)
https://soebit.com