AI CERTs®

Executive Summary

Certification

TABLE OF CONTENTS

Introduction

The AI+ Security Practitioner certification equips you with the skills to apply artificial intelligence in cybersecurity and strengthen modern security practices. You will learn how to use AI-driven approaches to identify threats, improve security operations, and support proactive risk management.

Through this certification, you will explore key AI security concepts, including threat detection, vulnerability assessment, security automation, and responsible AI practices. You will gain practical expertise in leveraging AI technologies to enhance security decisions, protect digital environments, and develop effective solutions for emerging cybersecurity challenges.

This certification thoroughly covers topics such as:

- Computing, Linux, and Operating System Foundations
- Networking Fundamentals and Traffic Analysis
- Python for Security and Automation
- Cybersecurity Foundations and Threat Landscape
- Cryptography, Authentication, and Identity Security
- Introduction to Artificial Intelligence and Machine Learning
- AI Applied to Security Detection and Threat Hunting
- AI Security, LLM Security, and Responsible AI
- Offensive Security for AI Systems
- Security Operations, Incident Response, and Malware Analysis
- Governance, Compliance, and Ethical AI Security
- Capstone Project: AI-Driven Security Operations and Defense

Certification Prerequisites

- **Basic understanding of AI and cybersecurity concepts:** Familiarity with fundamental AI principles, security terminology, and common cybersecurity practices.
- **Knowledge of security operations:** Understanding of basic threat detection, risk management, vulnerability assessment, and incident response processes.
- **Familiarity with networking and infrastructure concepts:** Awareness of networks, systems, cloud environments, and common security controls.
- **Understanding of data protection principles:** Basic knowledge of privacy, compliance requirements, secure data handling, and cybersecurity best practices.

- **Basic programming and automation awareness**: Familiarity with scripting concepts, automation workflows, and how AI can support security operations.
- **Understanding of responsible AI and security governance:** Awareness of AI risks, ethical considerations, bias, transparency, and the importance of human oversight.
- **Comfort with AI-powered security tools:** Basic understanding of using AI technologies for threat analysis, security monitoring, and decision support.

Who Should Enroll?

- **Cybersecurity Professionals:** Those who want to enhance their security skills by applying AI techniques for threat detection, analysis, and response.
- **Security Analysts:** Those who work with security monitoring, incident investigation, vulnerability assessment, and AI-assisted security operations.
- **IT Professionals:** Those who want to understand how AI can strengthen infrastructure protection, risk management, and security workflows.
- **Network and System Administrators:** Those who manage digital environments and want to use AI tools to improve security monitoring and protection.
- **Risk and Compliance Professionals:** Those who want to explore AI-driven approaches for security governance, compliance management, and risk assessment.
- **Ethical Hackers and Security Researchers:** Those who want to apply AI capabilities to identify vulnerabilities, analyse threats, and improve defensive strategies.
- **AI and Technology Professionals:** Those who want to understand the security challenges of AI systems and implement safer AI solutions.
- **Security Managers and Decision Makers:** Those who want to leverage AI insights to improve cybersecurity strategies, operational efficiency, and organizational resilience.
- **Professionals Interested in AI Security:** Those who want to build foundational expertise in combining artificial intelligence with modern cybersecurity practices.

Certification Goals and Learning Outcomes

- Understand AI and Cybersecurity Fundamentals: Build a strong foundation in AI concepts, security principles, and the role of artificial intelligence in strengthening modern cybersecurity practices.
- Apply AI for Threat Detection and Analysis: Use AI-driven techniques to identify threats, analyse security events, detect anomalies, and support faster incident response.
- Perform AI-Enhanced Risk and Vulnerability Management: Leverage AI capabilities to assess risks, identify vulnerabilities, and improve security assessment processes.
- Implement AI-Powered Security Automation: Explore how AI can automate security workflows, streamline monitoring activities, and improve operational efficiency.
- Secure AI Systems and Applications: Understand AI-specific security risks and apply best practices to protect AI models, applications, and data environments.
- Apply Responsible AI and Security Governance: Implement ethical AI practices, manage security risks, support compliance, and maintain transparency in AI-driven security operations.
- Develop AI-Based Cybersecurity Solutions: Apply learned concepts through practical scenarios to design effective AI-powered approaches for addressing real-world security challenges.

The Impact of AI on Modern Security Practices

AI is significantly transforming modern cybersecurity practices across the globe, reshaping how security threats are detected, analyzed, prevented, and managed. In North America, which commands 28.8% of the AI market, organizations are integrating AI into cybersecurity operations to enhance threat detection, incident response, vulnerability management, security monitoring, and automated defense strategies. This adoption helps security teams analyze large volumes of security data, identify emerging threats, improve decision-making, and respond to cyber incidents with greater speed and efficiency.

In the Asia-Pacific region, holding 25% of the market, AI is enabling more adaptive cybersecurity processes, such as real-time threat intelligence analysis, behavioral monitoring, automated investigations, and faster security response. This allows cybersecurity teams to detect suspicious activities, strengthen digital protection, improve security visibility, and develop more proactive defense strategies across rapidly expanding technology environments.

Europe, with 24.3% of the AI market, places strong emphasis on the secure and responsible use of AI in cybersecurity. Organizations focus on compliance, data protection, transparency, and responsible AI practices while implementing AI-powered security solutions. This ensures that threat detection, risk assessment, security automation, and AI-assisted decision-making remain trustworthy, accountable, and aligned with regulatory expectations.

Emerging markets in the Middle East, Africa, and Latin America are steadily adopting AI in cybersecurity, with growth rates of 2.4% and 5.4%, respectively. This adoption is improving security operations, strengthening threat monitoring capabilities, supporting automated analysis, and enabling organizations to enhance their protection against evolving cyber threats.

Australia, experiencing a growth rate of 14.1%, is increasingly leveraging AI for cybersecurity operations to streamline threat detection, improve incident response, enhance security investigations, and support data-driven risk management. This reflects the growing role of AI in helping cybersecurity professionals work more efficiently, identify vulnerabilities faster, and strengthen digital resilience.

This global shift highlights how AI, combined with cybersecurity expertise through AI+ Security Practitioner skills, is strengthening modern security practices by improving threat intelligence, automation, detection accuracy, incident response, risk management, and overall cyber resilience across organizations and regions.

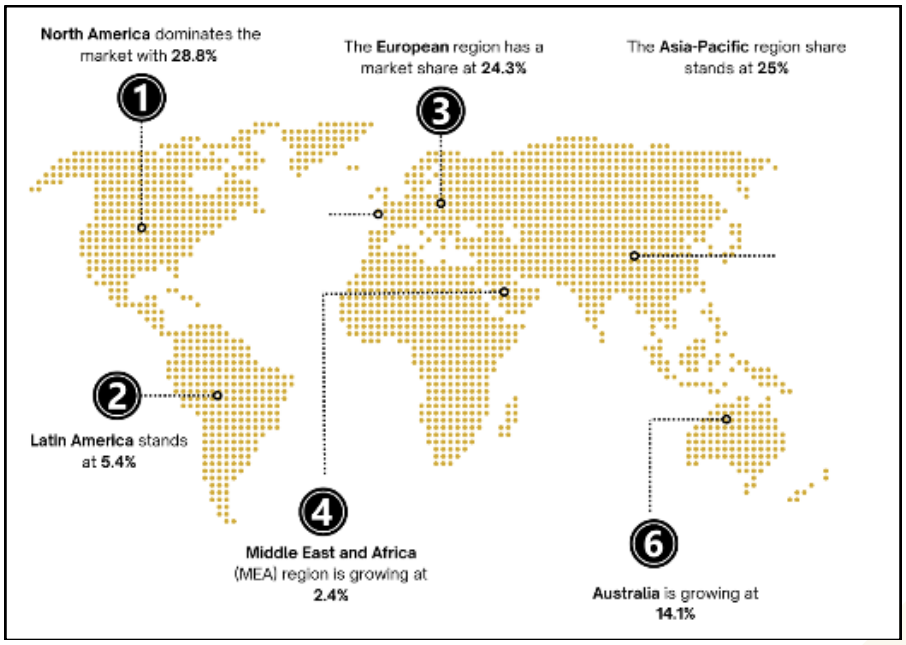

Figure 1: Market Share of AI from a Regional Perspective

What is Next for AI?

AI is moving toward more intelligent, adaptive, and autonomous cybersecurity capabilities, transforming how organizations detect, analyze, and respond to evolving threats. The next stage of AI will help security professionals identify suspicious behavior, analyze massive volumes of security data, automate threat investigations, predict potential attacks, and strengthen defense strategies through advanced AI-driven solutions. AI-powered security platforms will increasingly support Security Operations Centers (SOCs) by improving alert prioritization, enhancing threat intelligence analysis, assisting incident response, and enabling faster decision-making. As cyber threats become more complex, the focus will shift from reactive defense to proactive security, where AI helps organizations anticipate risks, identify vulnerabilities, and build stronger digital resilience.

The future of AI security will also bring more advanced AI systems capable of supporting security workflows from detection to response. AI agents will assist professionals by investigating alerts, correlating threat information, analyzing vulnerabilities, and recommending or executing security actions under appropriate controls. For this course, that future connects directly to skills such as AI-based threat detection, LLM security, AI threat modeling, adversarial testing, AI red teaming, security automation, governance, and responsible AI practices. Learners will need to balance automation with human expertise, especially when managing AI risks, protecting sensitive data, validating AI decisions, and maintaining security compliance. The next phase of AI in cybersecurity will belong to professionals who can combine security knowledge, AI capabilities, ethical decision-making, and practical defense strategies to create secure, resilient, and intelligent cybersecurity environments.

How AI Can Transform Security Practices

AI can transform cybersecurity practices by enabling security teams to move from traditional reactive approaches to intelligent, proactive, and automated defense strategies. With AI-powered security capabilities, professionals can analyze large volumes of security data, detect emerging threats, automate investigations, and improve decision-making while strengthening protection across digital environments.

Below are a few transformative ways :

Figure 2: How AI Can Transform Security Practices

With AI+ Security Practitioner skills, security professionals can combine artificial intelligence with cybersecurity expertise to build faster, smarter, and more resilient defense capabilities.

How AI Addresses Current Challenges in Cybersecurity

Modern cybersecurity teams face increasing challenges such as rapidly evolving threats, massive volumes of security data, sophisticated attack techniques, and the need for faster response. AI helps address these challenges by enhancing threat detection, automating security processes, improving analysis, and enabling professionals to build stronger and more proactive defense strategies.

Here's an overview of common challenges and how AI offers practical solutions:

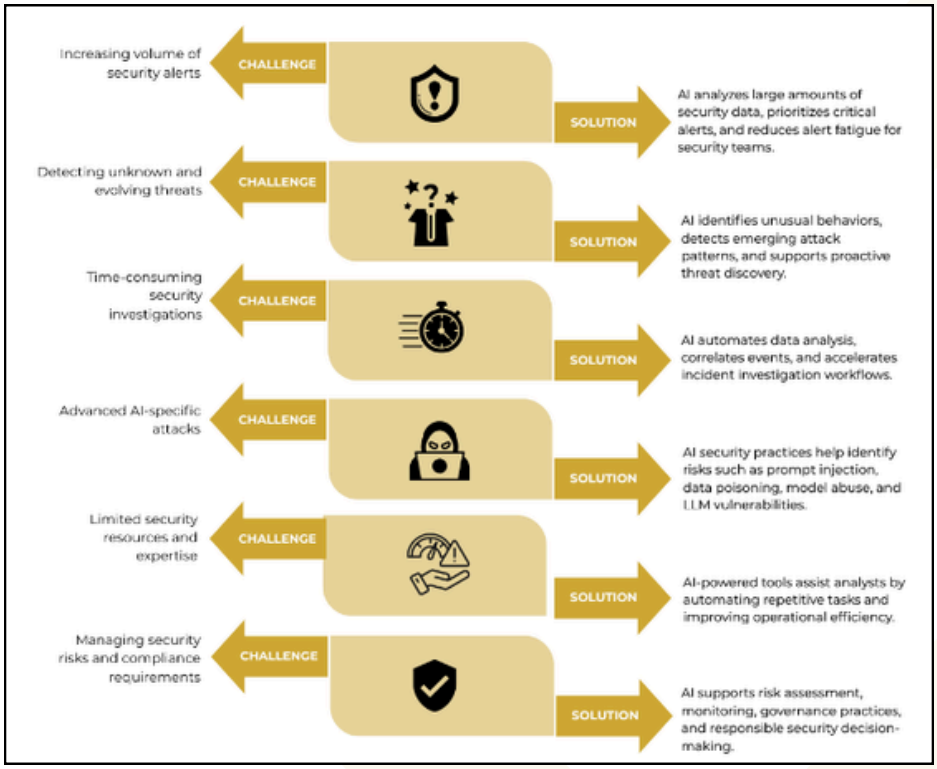

Figure 3: How AI Can Address the Current Security Challenges

With AI+ Security Practitioner skills, cybersecurity professionals can overcome modern security challenges by combining AI capabilities with human expertise to create more adaptive, efficient, and resilient defense environments.

How AI Adoption is Transforming Security Across Industries

Artificial intelligence is transforming security practices across industries by enabling faster threat detection, intelligent risk analysis, automated responses, and proactive protection against emerging cyber threats. In the financial services industry, AI is used to detect fraudulent transactions, identify unusual customer behavior, strengthen identity verification, and protect digital banking platforms from sophisticated cyberattacks. In healthcare, AI helps secure sensitive patient data by monitoring network activity, detecting unauthorized access, and supporting compliance with data protection regulations while protecting connected medical devices. The manufacturing sector is adopting AI-driven security solutions to safeguard industrial control systems, IoT devices, and smart factories from cyber threats that can disrupt production operations. In retail and e-commerce, AI improves security by detecting payment fraud, analyzing customer behavior patterns, preventing account takeovers, and protecting online platforms from automated attacks. The government and public sector use AI to enhance national cybersecurity efforts, monitor critical infrastructure, identify threats in real time, and improve incident response capabilities. Across these industries, AI is shifting security from a reactive approach to a proactive defense model, helping organizations predict threats, reduce response times, and build more resilient digital environments.

How to Integrate AI into Security Workflows

Integrating AI into cybersecurity workflows helps security teams improve threat visibility, automate complex processes, and make faster, more accurate decisions. By applying AI-driven security techniques, professionals can enhance threat detection, streamline investigations, strengthen incident response, and improve overall security operations across modern digital environments.

Below are the Key Steps to integrate AI into security workflows:

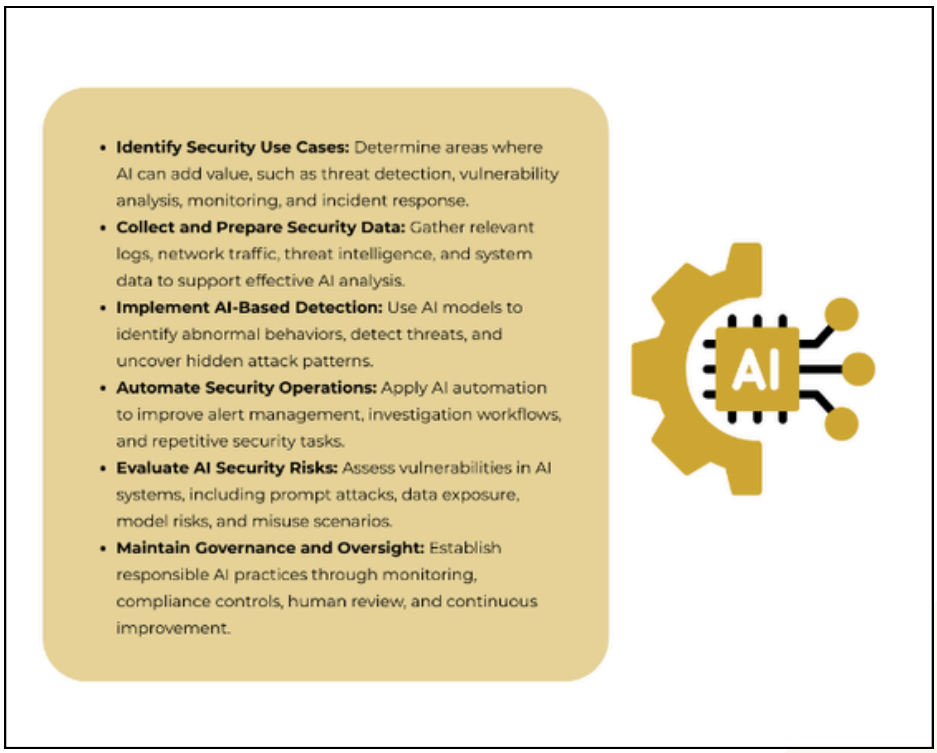

Figure 4: Key Steps to Integrate AI into Security Workflows

Integrating AI into cybersecurity workflows enables organizations to build smarter defence strategies, improve operational efficiency, and create more resilient security environments.

Module 1: Computing, Linux, and Operating System Foundations

A strong understanding of computing systems and operating environments is essential for building effective cybersecurity skills. Before exploring advanced security and AI-driven defence techniques, professionals need to understand how hardware, software, operating systems, Linux environments, and access controls work together to support secure digital infrastructures.

In this module, you will learn the fundamentals of computer systems, operating systems, and Linux administration. You will explore Linux commands, file systems, user management, permissions, authentication concepts, and access control mechanisms. You will also understand how these foundational concepts support cybersecurity operations and AI security practices.

Module 2: Networking Fundamentals and Traffic Analysis

Modern cybersecurity depends on understanding how systems communicate and how data moves across networks. A strong foundation in networking enables security professionals to identify suspicious activities, analyse traffic patterns, and understand how attackers exploit network communication channels.

In this module, you will learn essential networking concepts, including IP addressing, MAC addresses, ports, protocols, DNS, TCP/IP communication, and network security fundamentals. You will explore how firewalls, IDS/IPS, VPNs, and network monitoring techniques help protect digital environments and support threat detection.

Module 3: Python for Security and Automation

Automation is becoming increasingly important in cybersecurity as organizations manage growing volumes of security data and complex operations. Python provides security professionals with the ability to automate repetitive tasks, analyse information, and build efficient security workflows.

In this module, you will learn Python programming fundamentals, including variables, conditions, loops, functions, modules, file handling, and error management. You will also explore how Python is applied in security operations through log analysis, automation scripts, data processing, and AI-powered security workflows.

Module 4: Cybersecurity Foundations and Threat Landscape

Understanding cybersecurity fundamentals is essential for identifying risks, protecting digital assets, and responding effectively to modern cyber threats. As organizations face increasingly sophisticated attacks, security professionals must understand common attack methods, vulnerabilities, and defensive strategies.

In this module, you will learn core cybersecurity principles, including the CIA Triad, threats, vulnerabilities, risks, attack surfaces, defence-in-depth strategies, and security controls. You will also explore common cyber threats such as malware, phishing, ransomware, social engineering, and industry security frameworks.

Module 5: Cryptography, Authentication, and Identity Security

Protecting sensitive information and managing user identities are critical components of modern cybersecurity. Strong cryptographic techniques and identity security practices help organizations prevent unauthorized access, maintain trust, and protect valuable digital assets.

In this module, you will learn cryptography fundamentals, including encryption, hashing, digital signatures, and TLS security. You will also explore authentication methods, identity management, access controls, password security, multi-factor authentication, and common identity-related security risks.

Module 6: Introduction to Artificial Intelligence and Machine Learning

Artificial Intelligence and Machine Learning are transforming cybersecurity by enabling faster detection, improved analysis, and intelligent decision-making. Understanding how AI models learn and operate is essential for professionals working at the intersection of cybersecurity and emerging technologies.

FIn this module, you will learn AI, Machine Learning, and Deep Learning fundamentals. You will explore supervised, unsupervised, and reinforcement learning approaches, machine learning lifecycle concepts, datasets, features, labels, model evaluation, and the role of AI in modern cybersecurity applications.

Module 7: AI Applied to Security Detection and Threat Hunting

As cyber threats become more advanced, security teams need intelligent methods to analyse large volumes of data and identify hidden risks. AI-powered detection and threat hunting techniques help organizations improve visibility, reduce response time, and strengthen security operations.

In this module, you will learn how AI supports security detection through behavioral analytics, anomaly detection, machine learning-based detection, detection engineering, and threat intelligence. You will also explore threat hunting approaches, MITRE ATT&CK mapping, IOC analysis, and AI-assisted SOC operations.

Module 8: AI Security, LLM Security, and Responsible AI

The rapid adoption of generative AI and Large Language Models introduces new opportunities and security challenges. Understanding AI-specific risks is essential for designing secure AI applications and ensuring responsible technology adoption.

In this module, you will learn the fundamentals of LLMs, generative AI, AI copilots, and Retrieval-Augmented Generation (RAG). You will explore OWASP LLM security risks, including prompt injection, sensitive information disclosure, insecure outputs, and excessive agency. You will also understand responsible AI principles, governance, and human oversight.

Module 9: Offensive Security for AI Systems

Securing AI systems requires proactive testing to identify weaknesses before attackers can exploit them. Offensive security approaches help organizations evaluate AI applications, discover vulnerabilities, and strengthen their defences against emerging AI threats.

In this module, you will learn AI threat modelling concepts, attack surfaces, STRIDE methodology, adversarial AI techniques, and AI system attacks. You will also explore AI red teaming practices, security testing approaches, and methods used to improve AI system resilience.

Module 10: Security Operations, Incident Response, and Malware Analysis

Effective cybersecurity requires more than prevention; organizations must also detect, investigate, respond to, and recover from security incidents. Security Operations Centres (SOCs) use advanced tools and processes to manage threats and protect digital environments.

In this module, you will learn SOC operations, SIEM concepts, alert management, incident response lifecycle, detection workflows, and evidence handling. You will also explore malware analysis techniques, threat investigation methods, and how AI assists security teams in improving operational efficiency.

Module 11: Governance, Compliance, and Ethical AI Security

Technology alone cannot ensure secure AI adoption. Organizations require governance frameworks, compliance practices, and ethical principles to manage risks and maintain trust in AI-driven environments.

In this module, you will learn security governance, risk management, AI governance, compliance requirements, privacy principles, and responsible AI practices. You will explore how organizations establish policies, manage AI risks, protect sensitive data, and ensure secure and ethical technology usage.

Module 12: Capstone Project — AI-Driven Security Operations and Défense

Applying cybersecurity knowledge in realistic scenarios is essential for developing practical security expertise. The capstone project allows learners to combine technical skills, analytical thinking, and security decision-making in an enterprise environment.

In this module, you will complete an end-to-end AI security assessment by reviewing an enterprise environment, analysing threats, evaluating AI security risks, performing incident response activities, and preparing governance recommendations. You will apply concepts from the entire course to investigate security challenges and communicate findings through professional security reports.

How Can AI CERTs Help in Building an AI-Ready Culture?

While AI offers immense opportunities, businesses frequently encounter obstacles such as skill gaps, managing complex data, and integration challenges. At AI CERTs, we tackle these issues head-on with expertly crafted certifications, empowering organizations to build the expertise needed to overcome these barriers and unlock AI's full potential.

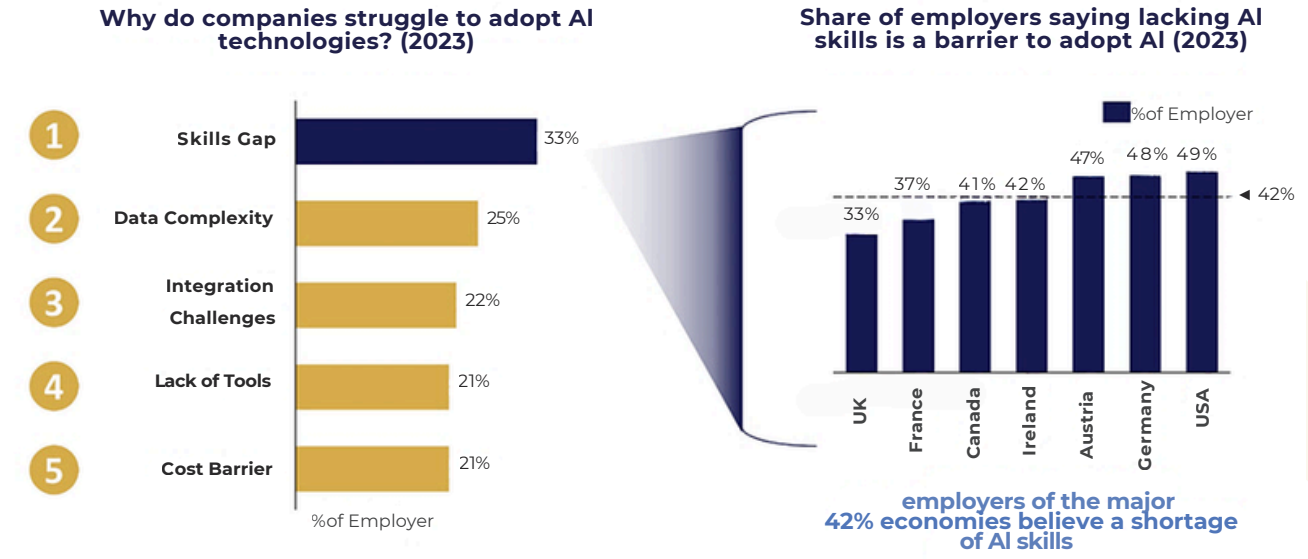

Figure 5: Factors driving the lack of adoption of AI Technologies
Source: OCED and IBM

Bridging the AI Skills Gap

- **Challenge:** Many cybersecurity professionals struggle to understand and apply AI-driven security solutions due to limited knowledge of artificial intelligence, machine learning, and AI-specific security concepts. This gap makes it challenging to effectively implement AI for threat detection, security automation, risk assessment, and modern cyber defense strategies.
- **Solution:** The AI+ Security Practitioner certification provides specialized training that bridges the gap between cybersecurity and artificial intelligence. This certification equips professionals with practical knowledge of AI fundamentals, threat detection, LLM security, AI risk management, security operations, and responsible AI practices to strengthen their cybersecurity capabilities.
- **Benefit:** By completing this training, cybersecurity professionals gain the skills to apply AI effectively in security operations, improve threat analysis, automate workflows, and respond to evolving cyber threats. Organizations benefit from stronger security teams, faster incident response, improved threat visibility, and enhanced cyber resilience.

Continuous Learning for Long Term Success

- **Challenge:** Security professionals often face difficulties keeping pace with rapidly evolving cyber threats and emerging AI technologies. Without hands-on knowledge of AI-powered security tools and techniques, teams may struggle to identify AI-specific risks, secure AI applications, and adapt to modern attack methods.
- **Solution:** The AI+ Security Practitioner certification provides comprehensive training on AI-driven cybersecurity practices, including machine learning applications, AI threat detection, LLM security, offensive AI security testing, SOC operations, governance, and incident response. The course prepares professionals to integrate AI into security workflows and address the challenges of modern cyber defense.
- **Benefit:** By developing AI security expertise, professionals can enhance their ability to detect threats, analyze security incidents, protect AI systems, and implement responsible security strategies. This enables organizations to build proactive defense capabilities, reduce security risks, and create a more resilient cybersecurity environment.

At AI CERTs, we provide a strategic approach to foster a culture of AI integration and innovation. Our AI certifications offer in-depth training and valuable recognition, empowering your employees to lead your organization into an AI-powered future.

AI CERTs Cultivate AI Culture in Several Ways:

- Our certification provides a clear and comprehensive introduction to AI fundamentals and applications, designed to make the learning experience easy and accessible.
- We ensure continuous learning opportunities to keep your team updated on emerging AI advancements, empowering your company to lead the industry.
- AI CERTs promote teamwork and knowledge sharing, fostering the critical collaboration needed for seamless AI adoption.

AI CERTs: Your Pathway to Becoming AI-Ready

The future of business belongs to Bitcoin users.

Tailored for Success: Our certifications are crafted to address your team's unique requirements, offering specialized training to equip them with the vital skills needed for key AI roles.

Actionable Expertise: Through hands-on learning with real-world projects and case studies, we enable your team to gain practical expertise and implement AI effectively to foster innovation and progress.

Become an AI Leader: Empower your team with AI CERTs to build an AI-driven culture, unlock cutting-edge technology, and drive your organization’s success.

AICERTs®

www.aicerts.ai

Contact

252 West 37th St., Suite 1200W
New York, NY 10018