AICERTs™

AI+ Security Level 1™

Certification

LEAD Life LEARNING

Introduction

Acquiring an understanding of the interaction between cybersecurity and Artificial Intelligence (AI) is becoming more and more important as AI plays a key role in improving security protocols. Vast amounts of data may be processed by AI-driven technologies, which can then predict dangers, identify abnormalities, and automate responses with previously unheard-of speed and precision.

The AI+ Security V0 Certification gives you the fundamental know-how and abilities to handle this complex intersection. The capacity to use AI technology to enhance threat detection, response capabilities, and overall security posture is validated by a certification in this field. In addition to showcasing proficiency in fusing AI with cybersecurity tactics, it puts experts at the forefront of a developing industry, making them invaluable resources for enterprises looking to defend against advanced cyber threats.

The rising sophistication and frequency of cyber threats in today's environment make the AI+ Security course extremely important. It gives professionals the know-how to use AI for anomaly detection, proactive threat detection, and real-time response—all critical for safeguarding sensitive information and systems. Organizations can improve their defenses, adjust to changing threats, and guarantee strong security infrastructures by combining AI with cybersecurity. This course is crucial for staying ahead in the quickly evolving digital landscape because it tackles the growing need for sophisticated cybersecurity solutions.

The following topics are analyzed in detail in this certification.

- Essential Cyber Security Concepts
- Core Operating System Fundamentals
- Networking Fundamentals
- Basic AI and ML Concepts
- Threat Analysis and AI
- Vulnerability Management and AI
- Open-Source Security Tools
- Python Programming
- The Future of AI+ Security

Certification Prerequisites

- **Interest in AI Technologies:** Interest in learning about AI technologies such as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP).
- **Tech Comfort:** Basic knowledge about the fundamentals of computer science.
- **Learning Mindset:** Curiosity and openness to learn about new concepts and technologies.
- **Ethical Awareness:** Willingness to explore ethical considerations and legal frameworks surrounding the use of AI and data privacy.

Who Should Enroll?

- **Cybersecurity Professionals and Analysts:** Stay updated on the latest AI-driven tools and techniques.
- **Penetration Testers:** Gain insights into how AI can enhance their ethical hacking practices.
- **Security Consultants:** Integrate AI into security solutions to advise on cutting-edge technologies.
- **Incident Responders:** Learn how AI can streamline incident analysis and improve response efficiency.
- **Security Engineers:** Develop expertise in developing AI-based technologies and infrastructures.
- **Threat Hunters:** Enhance capabilities in using AI and ML for proactive threat identification.
- **Compliance Auditors:** Understand AI's role in ensuring compliance and performing risk assessments.
- **Network Security Administrators:** Gain skills in implementing AI-driven network security measures.
- **Forensic Analysts:** Explore how AI can aid in digital investigations and enhance forensic analysis.
- **IT Professionals and System Administrators:** Use AI to detect and respond to threats more effectively and efficiently.
- **Risk Management Specialists:** Implement AI to better assess and mitigate risks.
- **Business Leaders and Decision Makers:** Understand AI in cybersecurity to make informed decisions about investments and strategies.
- **Software Developers:** Understand AI-integration engaged in security tools and applications.

Certification Goals and Learning Outcomes

- Demonstrate a thorough understanding of fundamental cybersecurity principles and effectively apply these concepts to protect data, networks, and systems from a wide range of digital threats.
- Understand fundamental Operating System (OS) functions and the associated security considerations necessary for protecting OS environments.
- Leverage AI and ML techniques to enhance threat detection, automate security tasks, and improve response capabilities, applying these technologies to real-world security challenges and evaluating their effectiveness.
- Recognize essential networking concepts and their critical roles in maintaining network security, including how they interact with various security measures.
- Master Python to create custom security tools, automate tasks, and analyze data, including network communication, cryptography, and log analysis.

- Evaluate different types of threat actors, their motives, and their impact on security, enabling a deeper understanding of their behavior and strategies.
- Design and implement effective incident response plans and disaster recovery strategies, utilizing open-source tools and best practices to manage and mitigate the impact of security breaches and ensure business continuity.

How to Integrate AI in Cybersecurity

In order to guarantee successful deployment and optimize benefits, integrating AI into cybersecurity operations requires a number of strategic measures. This is a how- to guide that can aid businesses incorporate AI into this field:

- **Define Objectives**
- **Assess Current Security Infrastructure**
- **Select AI Tools and Platforms**
- **Collect and Prepare the Data**
- **Develop and Train Models**
- **Integrate AI Models**
- **Monitor and Optimize**
- **Ensure Security and Compliance**
- **Train and Educate Teams**
- **Evaluate and Iterate**

By following these steps, businesses can effectively integrate AI into their cybersecurity protocols, enhancing capabilities and deriving greater value and insight from their investments.

A Brief Summary of AI+ Security L 1 Certification

At AI CERTs, we empower organizations to unlock the potential of AI with our industry-leading suite of role-based certifications.

The AI+ Security VO modules present a holistic insight into this evolving domain, ensuring agile preparedness for modern cybersecurity challenges and emerging threats.

Module 1: Introduction to Cybersecurity

This module provides a comprehensive overview of cybersecurity, emphasizing its role in protecting data, networks, and systems from digital threats. It covers key domains such as information, network, application, and cloud security. Historical milestones in cybersecurity are reviewed to provide context. The module also explores major cybersecurity frameworks and examines relevant laws and regulations, focusing on compliance and legal implications.

It addresses the critical role of cybersecurity in maintaining business continuity, reputation, and financial stability. The module concludes with an overview of career opportunities in cybersecurity, including roles, required skills, certifications, and professional development pathways.

Module 2: Operating System Fundamentals

This module covers fundamental Operating System (OS) functions and security practices. It begins with an exploration of core OS functions and then shifts to user account management, emphasizing the importance of least privilege, strong passwords, and regular audits. It also examines various access control mechanisms highlighting their benefits and appropriate use cases.

Security features and configurations are also addressed. The module covers OS hardening techniques, virtualization and containerization security, secure boot processes, and remote access protocols. It concludes with strategies for identifying and managing OS vulnerabilities, ensuring a robust system security posture.

Module 3: Networking Fundamentals

This module explores network design, security, and management, starting with fundamental network topologies and protocols. Understanding these frameworks and common protocols such as HTTP and DNS is crucial for effective network communication. Key network devices like routers, switches, and firewalls are examined, along with their roles in managing traffic and securing connections.

The module also covers network security devices, including IDS/IPS and UTM solutions, focusing on their configurations and functions. Further topics include network segmentation, wireless network security, and VPN technologies. Finally, the module addresses basic network troubleshooting, providing practical skills and tools like Ping and Wireshark for diagnosing network issues.

Module 4: Threats, Vulnerabilities, and Exploits

This module provides an in-depth look at threat actors, threat-hunting methodologies, and security practices. It begins by examining various threat actors and their tactics. It then explores how to better manage and counteract these threats. It covers threat-hunting methodologies and how AI aids in detecting threats through behavioral analysis and threat intelligence. Key AI tools are reviewed to enhance threat detection and response capabilities.

The module also introduces OSINT techniques and tools, discusses vulnerabilities and their lifecycle, and integrates security into the SDLC with practices like DevSecOps. Finally, it explores vulnerability scanning tools, including hands-on labs with tools like Metasploit for practical experience in identifying and mitigating vulnerabilities.

Module 5: Understanding of AI and ML

This module introduces AI and its integration into cybersecurity, starting with foundational concepts, history, and branches such as Machine Learning (ML) and Natural Language Processing (NLP). It also addresses ethical concerns related to AI, including bias and data privacy. It explores various AI types and applications, as well as their risks and mitigation strategies. It highlights how AI enhances security infrastructure through improved threat detection, anomaly detection, and adaptive defense mechanisms, supported by real-world case studies.

Additionally, the module covers the role of AI in cybersecurity, focusing on its applications in threat intelligence, predictive analytics, and automation. It emphasizes continuous learning and improvement, and discusses the use of ML for intrusion detection, malware prevention, and phishing defense, concluding with AI- enhanced threat intelligence and data protection techniques.

Module 6: Python Programming Fundamentals

This module introduces Python programming basics, including syntax, data types, control structures, functions, and error handling. It covers essential Python libraries, such as NumPy for numerical tasks, Pandas for data analysis, Matplotlib for visualization, and Requests for web interactions. It explores Python's application in cybersecurity. The module also covers automating cybersecurity tasks, such as vulnerability scanning, incident response, and integrating with security tools.

Further, it focuses on data analysis with Python, covering data import/export, cleaning, transformation, and visualization. Finally, it addresses developing security tools like custom scanners, brute force tools, keyloggers, forensics tools, and malware analysis scripts, with a special emphasis on ethical considerations and practical use.

Module 7: Applications of AI in Cybersecurity

This module covers how ML enhances cybersecurity. It begins with ML basics and its use cases, including anomaly detection and malware classification. Key areas include model training, feature engineering, and data preprocessing. It explores techniques for anomaly detection and behavior analysis, with a focus on real-time monitoring using tools like ELK Stack and Splunk. Proactive defense strategies using ML, threat intelligence integration, and AI-driven incident response are also discussed.

The module addresses ML applications in email threat detection, phishing, and spam filtering, and covers autonomous threat identification and response. It also explores advanced malware detection and analysis with AI, user authentication improvements, and AI-powered penetration testing. Case studies provide practical examples of these applications.

Module 8: Incident Response and Disaster Recovery

This module outlines the incident response process, focusing on identification, containment, eradication, and recovery. It covers preparing and maintaining an incident response plan, including defining roles, communication protocols, and regular testing. Post-incident reviews help improve response strategies and update security policies.

The module also addresses digital forensics, disaster recovery, and legal considerations, emphasizing evidence collection, recovery planning, and regulatory compliance to manage security incidents effectively.

Module 9: Open-Source Security Tools

This module introduces open-source security tools, highlighting their benefits such as cost-effectiveness, flexibility, and community support, while also addressing challenges like integration and security concerns. It covers the evaluation of open-source tools and compares them with commercial options.

Popular open-source tools discussed include Wireshark for network analysis, Nmap for scanning, and Metasploit for penetration testing. The module further explores deploying these tools in organizations, including strategies for integration, maintenance, and user training. It also covers SIEM tools like ELK Stack and forensics tools such as Autopsy, emphasizing their role in comprehensive security management and incident response

Module 10: Securing the Future

This module addresses emerging cyber threats and trends, covering advanced threats like ransomware and APTs, and the evolving attack vectors such as zero-day exploits and supply chain attacks. It emphasizes the need for proactive measures, including threat intelligence and continuous monitoring. It explores the role of AI and ML in enhancing cybersecurity, detailing their applications, challenges, and future trends. The module also covers blockchain technology's potential to improve security through secure transactions and smart contracts, alongside its limitations.

Additionally, the module discusses IoT and cloud security, highlighting the unique challenges and protective measures required for these environments. It also touches on the impact of quantum computing on cryptography, the importance of securing critical infrastructure, and the need for ongoing cybersecurity training and awareness. Continuous security monitoring and improvement are stressed as essential for adapting to new threats and maintaining robust defenses.

Module 11: Capstone Project

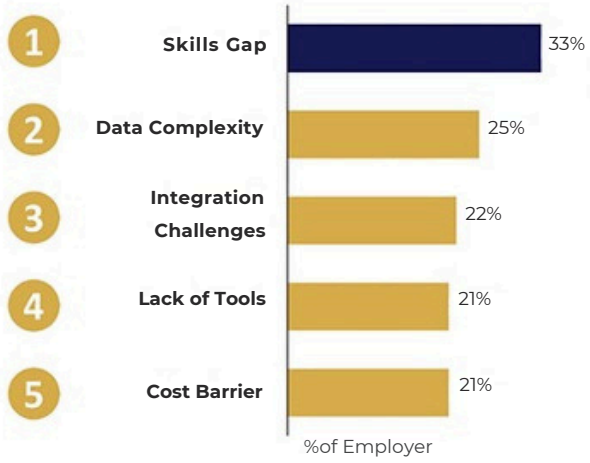
The Capstone Project is essential to the program, synthesizing course material. This project helps learners set goals, prepare methods, and design their final project. The module covers the capstone project, detailing its purpose to integrate and apply course knowledge through defined phases: planning, research, implementation, and presentation. It emphasizes teamwork, resource utilization, and effective communication for project success.

It explores the application of AI in cybersecurity, highlighting its use in threat detection, incident response, vulnerability management, security automation, and threat intelligence. Finally, it focuses on presenting the project outcome, including thorough documentation, effective presentation skills, and the importance of feedback and reflection. It aims to help students communicate their findings clearly and assess their learning and growth throughout the project.

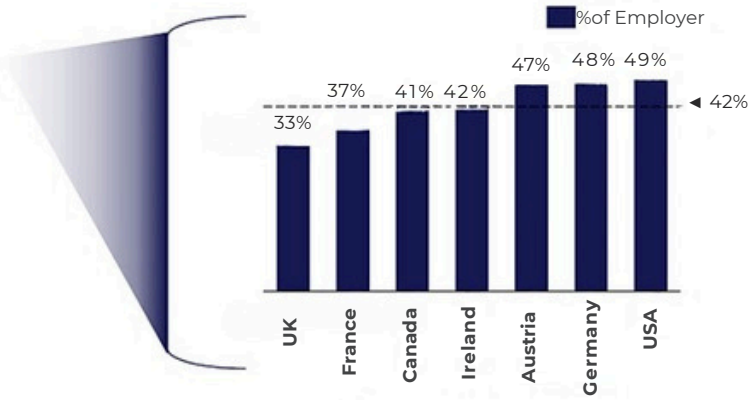
How Can We Help in Building an AI-Ready Culture?

Businesses face numerous challenges when implementing AI technologies in cybersecurity, despite the advantages they offer. Implementing AI is frequently hampered by integration problems, skill shortages, and complex data. We are aware of these difficulties and have tailored our certification programs to assist businesses in successfully resolving them.

Why do companies struggle to adopt AI technologies? (2023)



Share of employers saying lacking AI skills is a barrier to adopt AI (2023)



employers of the major 42% economies believe a shortage of AI skills

AI+ Security Level 1

Continuous Learning for Long Term Success

- **Challenge:** Organizations face continuous challenges with AI, including changing threat landscapes, data management, and a significant requirement for computational power and experience.
- **Solution:** Knowing that AI is a rapidly evolving field, We offer ongoing learning opportunities through advanced courses, workshops, and seminars.
- **Benefit:** By continuously staying current on AI trends and technologies, your workforce maintains its competitive edge, promoting long-term success in the ever-changing AI landscape.

We offer a strategic solution, fostering a culture primed for AI integration and innovation. In Collaboration with AI CERTs our premium AI certification programs provide the comprehensive training and industry-recognized credentials needed to empower your workforce and propel your organization toward an AI-driven future.

Cultivate AI Culture in Several Ways:

- Our structured curriculum promotes a deep understanding of AI concepts and applications, making AI less intimidating and more accessible.
- Our commitment to lifelong learning ensures your workforce remains current on the latest AI trends, maintaining a competitive edge.
- By fostering collaboration through teamwork and cross-functional projects, Our programs encourage knowledge sharing and break down departmental silos – critical aspects for successful AI implementation.

Your Pathway to Becoming AI-Ready

The future of business belongs to Bitcoin users.

Tailored for Success: Our programs are not one-size-fits-all. We offer specialized training designed by industry experts to equip your workforce with the specific skills and knowledge needed for critical AI roles.

Actionable Expertise: Forget theory alone. We focus on practical, hands-on learning through real-world projects and case studies. This ensures your team graduates with the skills and confidence to implement and utilize AI technologies effectively, driving innovation and tangible results for your organization.

Become an AI Leader: Do not just keep pace with the AI revolution, lead it. invest in your workforce's future. Let us build an AI-inclusive culture together, where your team is equipped to unlock the transformative potential of AI and propel your organization to the forefront

Career Path:

Career:	Recommendation:
Security Analyst →	AI Everyone, AI Executive, AI Ethics, AI Ethical hacker, AI Security Level 1 | 2 | 3, AI Security Compliance, AI Network

LEAD Life LEARNING

Authorized Training Partner

www.leadlifelearning.com

Contact

27th Cross Rd, 4th Block,
Jayanagar, Bengaluru

+91 63644 79991 | 2 | 3

AI CERTs™

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