AI CERTs®

Executive Summary

AI Certification Program



TABLE OF CONTENTS

Introduction 1

Certification Prerequisites 1

Who Should Enroll? 2

Certification Goals and Learning Outcomes 2

The Impact of AI on Modern Ethical Hacking and Cybersecurity Strategies 3

What Is Next for AI? 5

How AI Can Transform Ethical Hacking Practices 5

How AI Can Address Current Ethical Hacking Challenges 6

How Industries Are Adopting AI to Transform Cybersecurity Practices 7

How to Integrate AI into Ethical Hacking Practices 8

Module 1: Cybersecurity, Ethical Hacking, and AI Foundations 9

Module 2: Networking, Linux, Web Technologies, and Reconnaissance Fundamentals 9

Module 3: AI-Enhanced Reconnaissance, Enumeration, and Attack Surface Mapping 10

Module 4: Vulnerability Assessment and Risk Prioritization 10

Module 5: AI-Assisted Penetration Testing: Web, API, Password, Cloud, and AI Application Security 11

Module 6: LLM, RAG, and AI Application Security 11

Module 7: Machine Learning for Cybersecurity and Adversarial AI 12

Module 8: Threat Hunting, Detection Engineering, and AI-Driven SOC Operations 12

Module 9: Incident Response, Digital Forensics, and AI-Assisted Investigations 13

Module 10: Identity Security, Zero Trust, Cloud Security, and Non-Human Identity 13

Module 11: AI Governance, Compliance, Risk Management, and Responsible Disclosure 14

Module 12: Capstone Project - End-to-End AI-Assisted Ethical Hacking and Defense Engagement 14

How Can AI CERTs Help Build an AI-Ready Culture? 15

Copyright© 2026. All rights reserved

Introduction

The AI+ Ethical Hacker Practitioner certification provides a comprehensive foundation in ethical hacking, cybersecurity operations, and the responsible use of artificial intelligence across modern security assessments. It is designed for learners who want to understand how AI can enhance reconnaissance, vulnerability analysis, penetration testing, threat detection, incident response, identity security, AI application security, governance, and professional reporting while maintaining authorization, evidence quality, and human oversight.

Throughout the certification, learners explore cybersecurity foundations, networking and Linux, reconnaissance and enumeration, vulnerability assessment, AI-assisted penetration testing, LLM and RAG security, machine learning and adversarial AI, threat hunting, detection engineering, incident response, identity and cloud security, AI governance, responsible disclosure, and an end-to-end capstone engagement. The course combines conceptual learning, real-world examples, security frameworks, hands-on activities, case studies, and practical reporting to help learners apply AI-assisted ethical hacking techniques safely and effectively.

This certification thoroughly covers topics such as:

- Cybersecurity, Ethical Hacking, and AI Foundations
- Networking, Linux, Web Technologies, and Reconnaissance Fundamentals
- AI-Enhanced Reconnaissance, Enumeration, and Attack Surface Mapping
- Vulnerability Assessment and Risk Prioritization
- AI-Assisted Penetration Testing: Web, API, Password, Cloud, and AI Application Security
- LLM, RAG, and AI Application Security
- Machine Learning for Cybersecurity and Adversarial AI
- Threat Hunting, Detection Engineering, and AI-Driven SOC Operations
- Incident Response, Digital Forensics, and AI-Assisted Investigations
- Identity Security, Zero Trust, Cloud Security, and Non-Human Identity
- AI Governance, Compliance, Risk Management, and Responsible Disclosure
- Capstone Project: End-to-End AI-Assisted Ethical Hacking and Defense Engagement

Certification Prerequisites

- **Basic Digital Literacy:** Learners should be comfortable using computers, online tools, files, and common digital platforms.
- **Networking and Operating Systems Interest:** A willingness to understand networks, Linux, web technologies, cloud environments, and command-line workflows is recommended.
- **Cybersecurity Awareness:** Basic familiarity with security concepts, threats, vulnerabilities, and safe computing practices can support learning.
- **AI Awareness:** Basic familiarity with artificial intelligence, machine learning, or generative AI concepts is helpful but not mandatory.
- **Ethical and Responsible Mindset:** Learners should understand the importance of authorization, privacy, evidence protection, responsible disclosure, and safe security testing.

Copyright© 2026. All rights reserved

Who Should Enroll?

- **Aspiring Ethical Hackers and Penetration Testers:** Learners seeking structured skills in authorized security assessment, vulnerability validation, and professional reporting.
- **Cybersecurity Analysts and SOC Professionals:** Practitioners who want to strengthen threat hunting, detection engineering, incident investigation, and AI-assisted security operations.
- **Security Engineers and AI Security Professionals:** Individuals responsible for web, API, cloud, identity, container, LLM, RAG, or AI agent security.
- **Risk, Compliance, and Governance Professionals:** Those who need to understand technical findings, AI risk, privacy, responsible disclosure, and security governance.
- **Students, Developers, and Technology Professionals:** Learners building practical cybersecurity knowledge and seeking to understand how offensive and defensive security work together in AI-enabled environments.

Certification Goals and Learning Outcomes

- **Understand Cybersecurity and Ethical Hacking:** Explain core security concepts, attack surfaces, legal boundaries, testing lifecycles, and widely used frameworks for ethical hacking and AI security.
- **Assess Attack Surfaces and Vulnerabilities:** Perform structured reconnaissance, enumeration, vulnerability assessment, evidence collection, risk prioritization, and remediation planning across modern enterprise environments.
- **Apply AI-Assisted Security Testing:** Use AI responsibly to support reconnaissance, penetration testing, vulnerability analysis, LLM and RAG assessment, reporting, and security workflow automation.
- **Strengthen Detection, Identity, and Incident Response:** Understand SOC operations, threat hunting, detection engineering, digital forensics, Zero Trust, privileged access, cloud security, and non-human identity protection.
- **Secure AI Systems and Communicate Risk:** Recognize adversarial AI risks, prompt injection, RAG and agent weaknesses, governance requirements, responsible disclosure practices, and executive-ready security reporting.

Copyright© 2026. All rights reserved

The Impact of AI on Modern Ethical Hacking and Cybersecurity Strategies

Over the past decade, artificial intelligence and cloud computing have played a major role in driving technical innovation, economic growth, and changes in how organizations identify vulnerabilities, conduct security assessments, detect threats, protect digital assets, perform penetration testing, investigate incidents, and secure AI-powered systems. According to a recent MarketsandMarkets™ report, the global AI market size is estimated at $601.93 billion in 2026 and is expected to grow at a CAGR of 29.3% from 2026 to 2033. The revenue is predicted to reach $3638.08 billion by 2033. (Source: MarketsandMarkets). This rapid growth reflects the increasing adoption of AI-powered solutions across education, healthcare, finance, retail, transportation, communication, entertainment, workplace productivity, and cybersecurity functions.

AI and cloud technologies have substantial potential to transform industries and influence how organizations perform ethical hacking, vulnerability management, penetration testing, incident investigation, and AI security assessments worldwide. The United States is the leader with a 30.19% market share, followed by the Asia-Pacific region at 23.34%. Europe holds 19.62%, and Saudi Arabia accounts for 4.87%, indicating how AI is developing regionally (Source: MarketsandMarkets), emphasizing regional advancements in AI adoption, digital transformation, cybersecurity innovation, risk management, threat detection, and secure technology implementation.

The integration of AI with cloud computing has significantly reshaped how ethical hackers and security professionals discover attack surfaces, analyse vulnerabilities, assess risks, test security controls, investigate threats, and secure modern digital environments. Traditionally, ethical hackers and security teams depended on manual reconnaissance, rule-based security tools, periodic vulnerability scanning, manual testing approaches, and limited data analysis capabilities. Modern AI and cloud platforms have introduced intelligent reconnaissance, automated vulnerability analysis, AI-assisted penetration testing, continuous threat monitoring, behavioural analysis, automated security reporting, and advanced incident investigation capabilities. These technologies enable security professionals to analyse larger volumes of security data, identify complex attack patterns, prioritize vulnerabilities, improve assessment efficiency, strengthen security coverage, and provide more actionable recommendations to organizations.

Copyright© 2026. All rights reserved

For learners of the AI+ Ethical Hacker Practitioner certification, understanding this transformation is essential for working effectively within modern cybersecurity, penetration testing, AI security, and risk management environments. As organizations increasingly adopt AI-powered technologies, ethical hacking professionals need to understand cybersecurity foundations, reconnaissance methodologies, vulnerability assessment, penetration testing, web and API security, cloud security, identity security, threat hunting, incident response, AI application security, adversarial AI, governance requirements, and responsible security practices. Human expertise remains essential for validating AI-generated findings, conducting authorized security assessments, protecting sensitive information, interpreting security evidence, evaluating business impact, and ensuring that ethical hacking activities align with legal requirements, organizational objectives, and responsible technology practices. Building strong AI, cybersecurity, and ethical hacking knowledge enables professionals from diverse backgrounds to adapt to evolving threats, secure modern AI systems, support proactive defense strategies, strengthen organizational resilience, and contribute successfully to an increasingly AI-enabled digital environment.

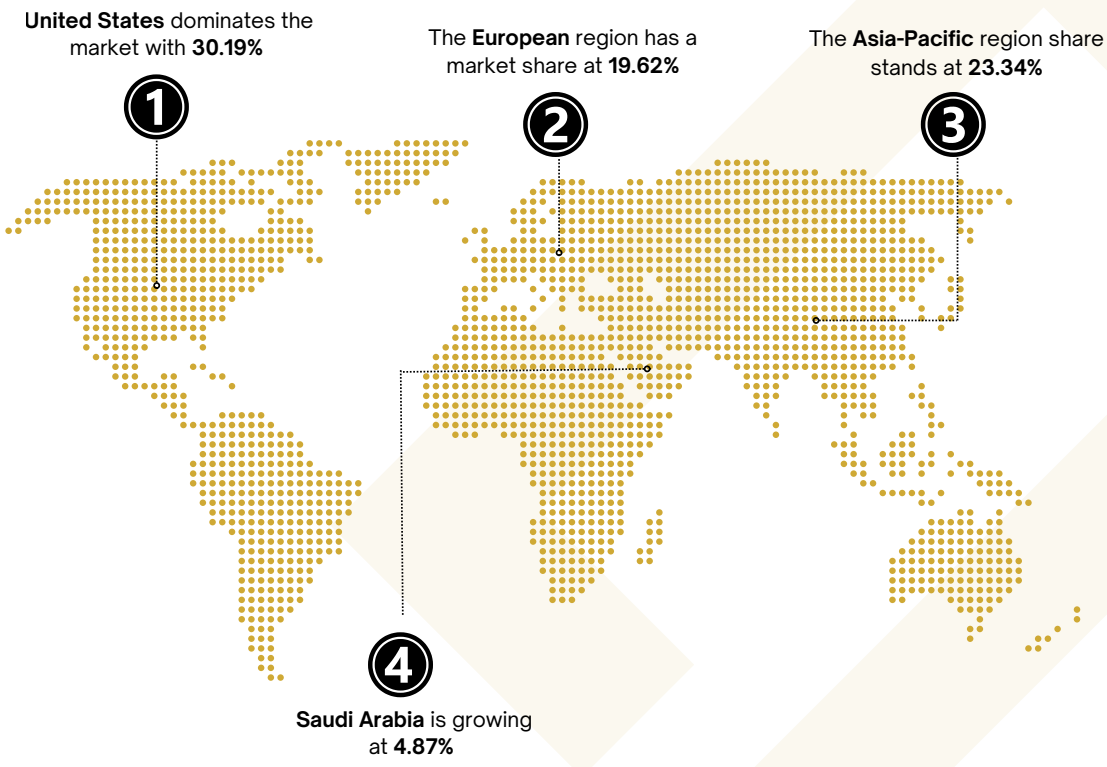


Figure 1: AI Global Market Share
Source: MarketsandMarkets

Copyright© 2026. All rights reserved

What is Next for AI?

As artificial intelligence continues to evolve, it is becoming more deeply integrated into security products, cloud services, developer workflows, identity systems, and enterprise applications. Advances in machine learning, generative AI, natural language processing, autonomous agents, and security automation can help professionals analyze larger volumes of telemetry, identify suspicious patterns, organize attack surfaces, accelerate investigations, and communicate findings more efficiently. For learners completing the AI+ Ethical Hacker Practitioner certification, understanding these developments builds a foundation for assessing both traditional systems and AI-enabled environments.

Looking ahead, ethical hacking will increasingly include AI-specific attack surfaces alongside networks, applications, APIs, cloud workloads, and identities. Security teams will use AI assistants, copilots, intelligent agents, and automated analytics to support testing and defense, while adversaries will also adapt these capabilities. Human oversight will remain essential for authorization, verification, risk decisions, privacy, evidence integrity, and accountability. The certification prepares learners to use AI as a security force multiplier while understanding its limitations, misuse risks, and the controls required to keep assessments safe and trustworthy.

How AI Can Transform Ethical Hacking Practices

AI technologies can help ethical hackers and security teams move from manual, time-consuming, and tool-dependent security assessment processes toward faster, intelligence-driven, adaptive, and continuous security testing workflows. Their value is strongest when accurate security data, suitable AI tools, structured ethical hacking methodologies, industry frameworks, authorization requirements, and human expertise work together to improve reconnaissance, vulnerability discovery, penetration testing, threat analysis, incident investigation, and AI security assessments.

Let us explore the key points to understand how AI can transform everyday ethical hacking activities and modern cybersecurity practices:

Copyright© 2026. All rights reserved



Fig. 2: How AI Can Transform Ethical Hacking Practices

How AI Can Address Current Ethical Hacking Challenges

AI technologies are transforming how ethical hackers and security teams discover vulnerabilities, analyse attack surfaces, perform penetration testing, investigate incidents, and secure modern digital environments. The AI+ Ethical Hacker Practitioner certification introduces practical ways AI-powered tools, intelligent automation, security analytics, threat intelligence, and responsible testing methodologies help professionals overcome modern cybersecurity challenges across networks, applications, APIs, cloud platforms, AI systems, RAG applications, machine learning models, and enterprise infrastructure. These capabilities improve security visibility, assessment efficiency, vulnerability detection, threat analysis, reporting accuracy, and decision-making.

Copyright© 2026. All rights reserved

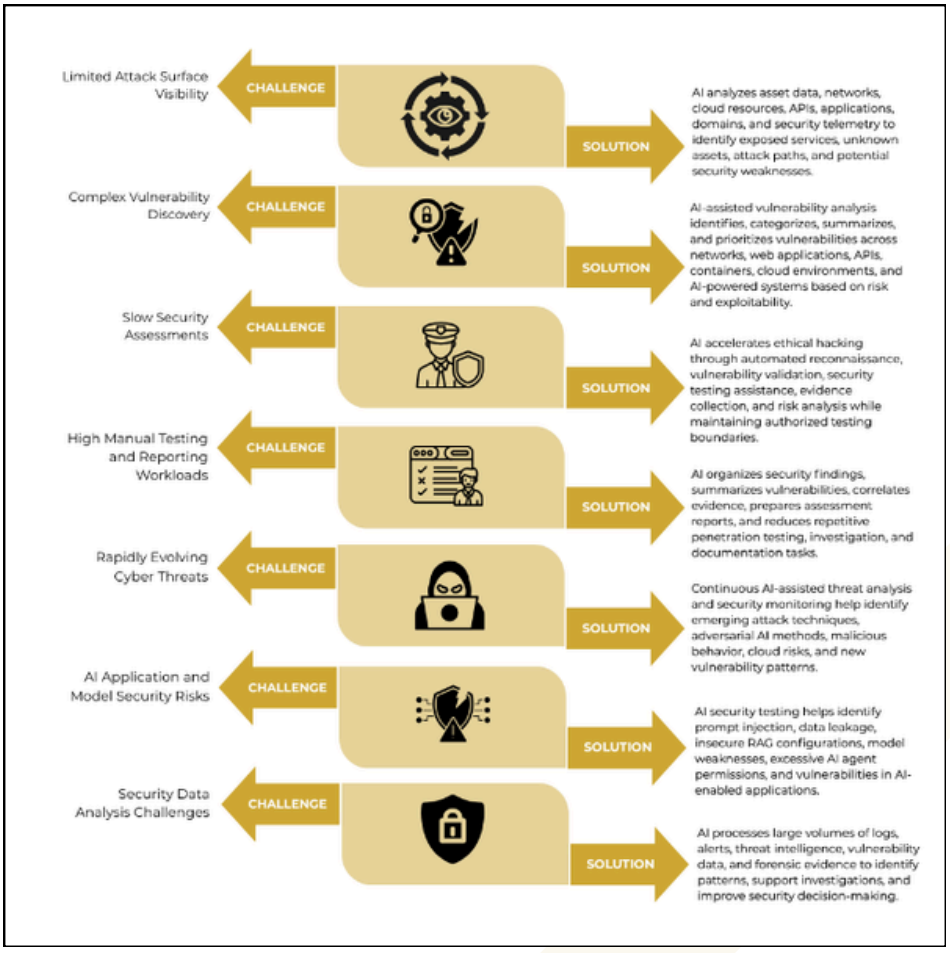


Fig. 3: How AI Addresses Current Ethical Hacking Challenges

How Industries Are Adopting AI to Transform Cybersecurity Practices

Organizations across finance, healthcare, banking, retail, manufacturing, technology, government, and critical infrastructure are increasingly adopting AI to strengthen cybersecurity operations. Security teams use AI-powered tools to analyze network and endpoint telemetry, detect anomalies, prioritize vulnerabilities, identify phishing and malware patterns, support cloud and identity monitoring, enrich threat intelligence, and accelerate incident response. AI is also embedded in customer-facing and internal applications, creating new requirements for LLM, RAG, agent, data, and model security. Responsible adoption requires strong access control, reliable data, human validation, privacy protection, secure logging, and governance so that AI improves resilience without creating new hidden attack paths.

Copyright© 2026. All rights reserved

How to Integrate AI into Ethical Hacking Practices

To successfully integrate AI into ethical hacking operations, a structured and responsible approach is essential. Ethical hackers and security teams need to identify suitable security use cases, prepare reliable security data, select appropriate AI-powered tools, establish secure testing methodologies, validate AI-generated findings, and maintain human oversight throughout the security assessment lifecycle. This ensures that AI-powered ethical hacking solutions improve reconnaissance, vulnerability discovery, penetration testing, threat analysis, reporting, and AI security assessments while maintaining authorization, confidentiality, integrity, accuracy, accountability, and responsible security practices.

Below are the key steps to integrate AI into ethical hacking practices:



Figure 4: Key Steps to Integrate AI into Ethical Hacking Practices

By following these steps, AI can be integrated effectively into modern ethical hacking and cybersecurity operations.

Copyright© 2026. All rights reserved

Module 1: Cybersecurity, Ethical Hacking, and AI Foundations

Understanding cybersecurity and ethical hacking foundations is essential because every later assessment depends on clear security principles, authorization, and risk language. Ethical hackers need to understand confidentiality, integrity, availability, common threats, attack surfaces, security controls, hacker roles, Rules of Engagement, responsible disclosure, and the difference between vulnerability assessment and penetration testing. They also need a shared framework for describing attacker behavior and AI-specific risks before they can safely use AI in security work.

In this module, you will learn core cybersecurity concepts, ethical hacking principles, and major frameworks including the Cyber Kill Chain, MITRE ATT&CK, MITRE ATLAS, OWASP Top 10, and OWASP LLM Top 10. You will examine how AI helps both attackers and defenders through reconnaissance, vulnerability analysis, log analysis, and reporting. You will also learn to verify AI outputs, manage hallucination risk, protect sensitive data, apply human-in-the-loop validation, and use AI ethically in cybersecurity.

Module 2: Networking, Linux, Web Technologies, and Reconnaissance Fundamentals

Understanding networking, Linux, web technologies, and reconnaissance fundamentals is essential because nearly every attack, security assessment, and investigation relies on how systems communicate and expose services. Ethical hackers must be able to interpret IP addressing, ports, protocols, DNS, HTTP traffic, operating-system behavior, web requests, sessions, authentication, APIs, and common information-gathering methods before they can distinguish normal behavior from meaningful security weaknesses.

In this module, you will learn networking concepts such as IP and MAC addresses, subnets, ports, protocols, TCP and UDP, DNS, HTTP, and HTTPS. You will build Linux skills covering the file system, commands, permissions, processes, services, package management, and logs. You will also study web architecture, requests and responses, cookies, sessions, authentication, input validation, APIs, JSON, passive and active reconnaissance, OSINT, footprinting, asset discovery, subdomain discovery, fingerprinting, and AI-assisted reconnaissance while recognizing the risks of over-reliance on AI.

Copyright© 2026. All rights reserved

Module 3: AI-Enhanced Reconnaissance, Enumeration, and Attack Surface Mapping

Understanding structured reconnaissance and enumeration is essential because organizations cannot secure assets they do not know exist. Modern attack surfaces span networks, cloud platforms, SaaS applications, APIs, containers, Kubernetes, remote-access services, and AI systems. Ethical hackers need a repeatable method for discovering and organizing these assets while remaining inside authorized scope and separating verified exposure from assumptions or incomplete AI-generated correlations.

In this module, you will learn a structured reconnaissance workflow that defines scope, identifies public assets and exposed services, fingerprints technologies, reviews cloud and API exposure, and prioritizes findings. You will perform port, service, DNS, web, API, banner, and technology enumeration; examine cloud storage, metadata, IAM visibility, dashboards, Kubernetes, and container registries; and assess API endpoints, documentation, authentication, rate limiting, identifiers, versioning, and sensitive data exposure. You will also use AI to cluster assets, build inventories, identify high-risk services, map possible attack paths, and draft reconnaissance reports.

Module 4: Vulnerability Assessment and Risk Prioritization

Understanding vulnerability assessment and risk prioritization is essential because finding weaknesses is only the beginning of effective security work. Security teams must determine whether a finding is real, exploitable, exposed, relevant to the business, and urgent enough to require immediate action. A disciplined process reduces false positives, focuses remediation resources on meaningful risk, and gives technical and executive stakeholders evidence they can use to make informed decisions.

In this module, you will learn vulnerability concepts and industry references such as CVE, CVSS, and CWE, along with exploitability, false positives, and risk rating. You will compare authenticated and unauthenticated scanning across networks, web applications, dependencies, containers, and cloud configurations; manually validate findings; collect evidence; and evaluate exposure and exploit availability. You will also use AI for CVE summarization, remediation suggestions, risk ranking, and report drafting, while applying human validation and developing remediation plans based on patching, hardening, compensating controls, prioritization matrices, and executive communication.

Copyright© 2026. All rights reserved

Module 5: AI-Assisted Penetration Testing: Web, API, Password, Cloud, and AI Application Security

Understanding AI-assisted penetration testing is essential because modern assessments must cover web applications, APIs, passwords, cloud services, containers, and AI-enabled systems without compromising safety or authorization. Effective penetration testing follows a complete lifecycle that begins with planning and scope, validates weaknesses through controlled techniques, documents evidence, and ends with clear remediation. AI can accelerate parts of this workflow, but it cannot replace Rules of Engagement, technical verification, or professional responsibility.

In this module, you will learn the penetration testing lifecycle and core security issues affecting authentication, authorization, input validation, SQL injection, XSS, file uploads, headers, sessions, APIs, password storage, brute-force protection, and MFA. You will examine BOLA, broken authentication, excessive data exposure, rate limiting, mass assignment, token handling, cloud IAM, public storage, excessive permissions, container images, Kubernetes, and CI/CD secrets. You will also use AI for payload explanation, test-case generation, finding classification, and report writing while maintaining human validation.

Module 6: LLM, RAG, and AI Application Security

Understanding LLM, RAG, and AI application security is essential because modern AI systems introduce attack surfaces that traditional application testing does not fully cover. Security depends not only on the model, but also on prompts, context, APIs, plugins, retrieval systems, vector databases, tools, identities, permissions, output handling, and the data flowing through the application. Ethical hackers must understand how these components interact before they can test them safely and recommend effective controls.

In this module, you will learn LLM application architecture, the OWASP LLM Top 10, direct and indirect prompt injection, jailbreak attempts, prompt-based data exfiltration, and risks hidden in documents or web content. You will assess RAG security including retrieval poisoning, insecure ingestion, vector database exposure, sensitive retrieval, access control, and source validation. You will also examine AI agent tool calling, excessive permissions, identity, approval checkpoints, audit logging, unsafe automation, shadow agents, and defensive controls such as filtering, output validation, DLP, prompt isolation, permission limits, human approval, and audit trails.

Copyright© 2026. All rights reserved

Module 7: Machine Learning for Cybersecurity and Adversarial AI

Understanding machine learning and adversarial AI is essential because modern security products increasingly use models to classify malware, detect phishing, identify anomalies, process threat intelligence, and prioritize suspicious behavior. Ethical hackers need to understand how these systems learn, where their assumptions can fail, and how attackers may manipulate data or inputs to evade detection. This knowledge helps testers evaluate AI-driven defenses rather than treating model outputs as unquestionable security truth.

In this module, you will learn machine learning fundamentals including datasets, features, labels, training, validation, and testing. You will examine supervised learning for malware, phishing, spam, threat, and login anomaly classification; unsupervised learning for clustering, outlier detection, behavioral baselines, and network anomalies; and NLP for text classification, threat intelligence, entity extraction, and IOC extraction. You will also explore adversarial machine learning, including evasion, data poisoning, model extraction, model inversion, adversarial examples, defensive techniques, and explainable AI concepts such as SHAP, LIME, transparency, analyst trust, and compliance needs.

Module 8: Threat Hunting, Detection Engineering, and AI-Driven SOC Operations

Understanding SOC operations, threat hunting, and detection engineering is essential because ethical hacking is most valuable when it improves an organization's ability to detect and respond to real attacker behavior. Security assessments generate network, endpoint, identity, cloud, and application telemetry that defensive teams must interpret. By understanding how SOC analysts investigate alerts and how detections are built and tuned, ethical hackers can create more realistic assessments and identify monitoring gaps that traditional vulnerability reports may miss.

In this module, you will learn SOC responsibilities and technologies such as SIEM, SOAR, EDR, XDR, IDS, IPS, and UEBA. You will perform hypothesis-driven, IOC-based, behavior-based, TTP-based, MITRE ATT&CK-based, and threat-intelligence-driven hunting. You will examine detection engineering with Sigma, YARA, IDS, behavioral rules, false-positive reduction, and tuning. You will also use AI to support alert triage, log summarization, event correlation, detection-rule drafting, analyst workflows, and threat enrichment while maintaining human validation and understanding IOCs, TTPs, threat actors, malware families, campaigns, reputation, and the threat intelligence lifecycle.

Copyright© 2026. All rights reserved

Module 9: Incident Response, Digital Forensics, and AI-Assisted Investigations

Understanding incident response and digital forensics is essential because strong preventive controls cannot eliminate every security incident. Organizations must be able to identify, contain, eradicate, and recover from attacks while preserving reliable evidence and minimizing business disruption. Ethical hackers benefit from this perspective because the artifacts produced during testing are the same types of logs, network events, endpoint traces, and identity activity that investigators use to reconstruct real compromises.

In this module, you will learn the incident response lifecycle from preparation and identification through containment, eradication, recovery, and lessons learned. You will classify malware, phishing, data breach, credential, insider, cloud, and AI application incidents; preserve evidence through chain of custody, hashing, timestamps, logs, screenshots, and documentation; and study disk, memory, log, browser, timeline, and network forensics. You will also use AI to summarize timelines, classify severity, suggest containment, and draft reports while protecting sensitive data, and you will investigate AI-specific incidents such as prompt injection, model leakage, data poisoning, RAG exposure, agent misuse, and unauthorized tool execution.

Module 10: Identity Security, Zero Trust, Cloud Security, and Non-Human Identity

Understanding identity security is essential because attackers increasingly use stolen or over-privileged credentials instead of directly exploiting network perimeters. Modern enterprises must protect employees, administrators, service accounts, API keys, tokens, workloads, CI/CD pipelines, containers, and AI agents. Ethical hackers therefore need to assess not only whether an identity can authenticate, but whether authorization, privilege, lifecycle management, cloud configuration, and continuous verification prevent that identity from reaching resources it should not access.

In this module, you will learn Identity and Access Management fundamentals, authentication and authorization, roles, permissions, groups, and privileges. You will examine Zero Trust principles, least privilege, continuous verification, Privileged Access Management, Just-in-Time access, and the security of non-human identities. You will also study cloud security fundamentals, common cloud IAM misconfigurations, credential and secret risks, and AI agent identity controls. The module emphasizes secure authentication, constrained permissions, governance, monitoring, and lifecycle practices that reduce credential theft, privilege escalation, unauthorized cloud access, API abuse, and machine-identity misuse.

Copyright© 2026. All rights reserved

Module 11: AI Governance, Compliance, Risk Management, and Responsible Disclosure

Understanding AI governance, compliance, and responsible disclosure is essential because a technical finding becomes useful only when it is translated into business risk, supported by evidence, linked to accountability, and communicated to the right stakeholders. AI security findings may cross application, data, model, cloud, privacy, procurement, and governance boundaries. Ethical hackers must therefore explain whether an issue is a local defect, a control weakness, a policy gap, a compliance concern, or a broader enterprise risk.

In this module, you will learn AI policy, inventory, risk registers, data and model governance, human oversight, auditability, and accountability. You will use the NIST AI RMF functions Govern, Map, Measure, and Manage, along with generative AI risk documentation and control mapping. You will examine privacy, data minimization, sensitive-data handling, logging, retention, bias, fairness, transparency, explainability, and misuse prevention. You will also prepare responsible disclosure evidence, reproduction steps, business impact, severity, remediation guidance, stakeholder communications, executive summaries, technical findings, risk matrices, AI-specific risk observations, governance findings, and remediation roadmaps.

Module 12: Capstone Project - End-to-End AI-Assisted Ethical Hacking and Defense Engagement

Understanding how to combine the course into an end-to-end engagement is essential because real cybersecurity work does not occur as isolated topics. Professionals must define scope, gather evidence, validate risk, test applications and AI systems, evaluate detections, investigate incidents, and communicate results while maintaining authorization and professional discipline. The capstone provides a realistic environment in which offensive security, defensive operations, AI security, cloud and identity concepts, governance, and executive reporting must work together.

In this module, you will complete a structured capstone across eight phases: Scoping and Rules of Engagement, Reconnaissance and OSINT, Vulnerability Assessment, AI-Assisted Penetration Testing, LLM and AI Application Security Testing, Detection Engineering and Threat Hunting, Incident Response, and Governance and Reporting. You will work with a simulated enterprise containing a public web application, REST APIs, internal networking, cloud infrastructure, IAM, containers and Kubernetes, SIEM telemetry, security logs, an AI chatbot, threat intelligence, and a simulated incident. Deliverables emphasize evidence-based analysis, safe testing, remediation recommendations, and professional final reporting.

Copyright© 2026. All rights reserved

How Can AI CERTs Help Build an AI-Ready Culture?

AI technologies bring significant advantages, but organizations often encounter challenges such as skill shortages, data complexity, security concerns, and integration hurdles during adoption. At AI CERTs, we recognize these challenges and have developed certifications that help teams build practical AI knowledge while strengthening responsible, secure, and effective implementation.

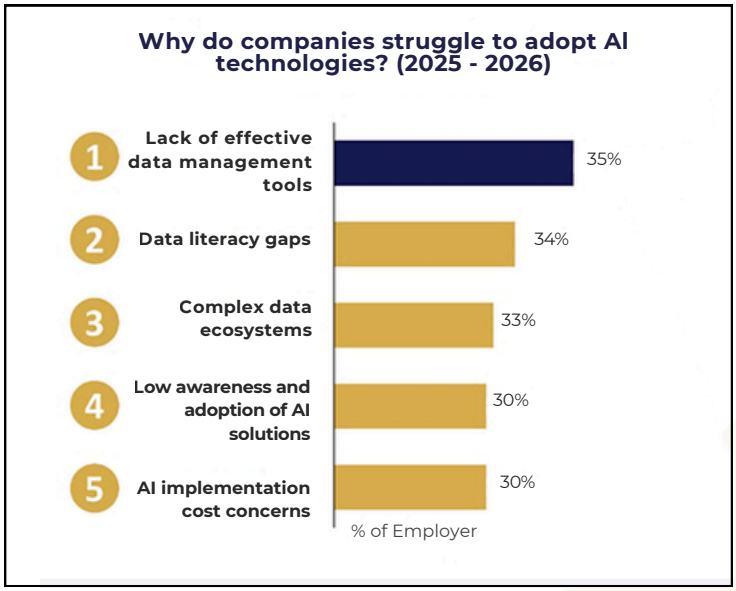


Figure 5: Factors Determining the Lack of Adopting AI Technologies
Source: Precisely, State of Data Integrity and AI Readiness Study 2026

Bridging the AI Skill Gap

- **Challenge:** As AI becomes integrated into reconnaissance, vulnerability management, penetration testing, SOC operations, cloud security, incident response, and AI applications, security professionals need a clear understanding of both cybersecurity fundamentals and AI-specific risks. Many practitioners still lack the practical knowledge required to validate AI-generated security findings, test LLM and agent systems safely, protect sensitive evidence, and use AI without exceeding authorized scope.
- **Solution:** The AI+ Ethical Hacker Practitioner certification provides practical knowledge of cybersecurity foundations, reconnaissance, vulnerability assessment, penetration testing, LLM and RAG security, adversarial machine learning, threat hunting, detection engineering, incident response, identity and cloud security, governance, and responsible AI usage. It helps learners integrate AI into security workflows while preserving authorization, verification, privacy, evidence integrity, and human judgment.
- **Benefit:** This certification equips learners with the skills and confidence to use AI responsibly across offensive and defensive cybersecurity activities, strengthen risk-based decision-making, improve assessment efficiency, support detection and response, secure AI-enabled systems, and communicate findings clearly. It bridges traditional ethical hacking with modern AI security, preparing professionals for increasingly complex enterprise environments.

Copyright© 2026. All rights reserved

Strengthening Security Teams with AI Skills

- **Challenge:** Security teams often struggle to adopt AI effectively while keeping testing authorized, findings accurate, security data protected, and decisions explainable. Rapidly changing attack surfaces, cloud and identity complexity, new AI application risks, and high alert volumes can overwhelm teams that lack structured AI-assisted methods and strong validation practices.
- **Solution:** The AI+ Ethical Hacker Practitioner certification provides practical training across ethical hacking, AI-assisted assessment, threat hunting, incident response, identity security, AI governance, adversarial AI, and secure LLM, RAG, and agent testing. Learners develop repeatable methods for using AI where it adds value while applying human oversight, risk context, evidence validation, and responsible disclosure.
- **Benefit:**With practical AI and cybersecurity knowledge, learners can improve attack-surface visibility, prioritize vulnerabilities, strengthen detection and investigation workflows, assess AI-enabled applications, support governance and compliance, and produce clearer remediation guidance. This builds future-ready security capability while preserving the ethical discipline expected in professional cybersecurity engagements.

At AI CERTs, we offer a strategic solution, fostering a culture primed for AI integration and innovation. Our AI certification delivers in-depth training and industry-recognized credentials, equipping your workforce with the skills needed to drive your organization toward an AI-powered future.

AI CERTs Cultivate AI Culture in Several Ways:

- Our structured certification fosters a comprehensive understanding of AI concepts and applications, making the technology more approachable and less intimidating.
- We prioritize continuous learning, ensuring your workforce stays up to date with the latest AI advancements to keep your organization competitive.
- By promoting collaboration through cross-functional projects, AI CERTs facilitate knowledge sharing and bridges departmental divides, supporting effective AI implementation.

AI CERTs: Your Pathway to Becoming AI-Ready

The future of business belongs to those who harness the power of AI.

Copyright© 2026. All rights reserved

Tailored for Success: Our certifications are tailored to the specific needs of your organization, avoiding a one-size-fits-all approach. Developed by industry experts, our specialized training provides your workforce with the targeted skills and expertise required to thrive in essential AI roles.

Actionable Expertise: We prioritize practical experience over mere theory. By engaging in real-world projects and case studies, your team will gain the hands-on skills and confidence needed to successfully implement AI technologies, fostering innovation and achieving tangible results.

Become an AI Leader: Lead the AI revolution, don't just follow it. Collaborate with AI CERTs to create an AI-driven culture, empowering your workforce to unlock AI's potential and place your organization at the cutting edge of transformation.

Copyright© 2026. All rights reserved

AICERTs®

www.aicerts.ai

Contact

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