Hewlett Packard Enterprise

Artificial Intelligence and Cybersecurity Essentials

H41KHS

Course ID	H41KHS
Duration	1 day
Format	ILT, VILT
View schedule, local pricing, and register	**View now**
Browse related courses	**View now**

This training focuses on the changing landscapes of cybersecurity with artificial intelligence including generative AI. It covers recommendations and guidelines along with scenarios on various attacks, exploits, vulnerabilities, and remedies.

5 reasons to choose HPE as your training partner

1. Learn HPE and in-demand IT industry technologies from expert instructors.
2. Build career-advancing power skills.
3. Enjoy personalized learning journeys aligned to your company's needs.
4. Choose how you learn: in-person, virtually, or on-demand—anytime, anywhere.
5. Sharpen your skills with access to real environments in virtual labs.

Explore our simplified purchase options, including HPE Education Learning Credits.

Audience

This course is ideal for business leaders, business professionals, and IT and security professionals looking to learn about AI-driven security.

Course objectives

After completing this course, you should be able to:

- Understand vulnerabilities, exploits, and attacks
- Discover how AI and generative AI are driving both defence and offense
- Differentiate between AI- and human-driven cybersecurity attacks
- Understand how to guard against AI-driven cyberattacks
- Identify and report security incidents
- Understand the ethical concerns of AI and cybersecurity

Detailed course outline

Module 1: A Recap—AI and Cybersecurity	• Key phrases and terminology	• The relationship between data, AI, and security
	• AI process, possibilities, and outcomes	• Why traditional controls are insufficient
Module 2: The Good, the Bad, and the Ugly	• The human to AI handover	• AI-enabled cyberattacks
	• Threats, vulnerabilities, and attacks	• The total blackout—what could happen
	• The business impact	
Module 3: Generative AI-Powered Modern Attacks	• The added risks	• Key takeaways
	• Modern attacks and concerns	
Module 4: Strategizing AI for Defense	• Detect, prevent, and recover with AI	• Protect your AI from falling victim
Module 5: From the Edge to Cloud	• The layered approach to secure AI	• HPE offerings for building AI with security
Module 6: How Do We Adopt Secure Practices While Using AI?	• Prevent and identify AI attacks	• Report an attack
	• Tools and technologies	
Module 7: Responsible AI and Governance	• Factors for responsible AI and governance	• The law and regulations

Learn more at

hpe.com/ww/learnAI

Follow us:

H41KHS A.00, August 2024

Hewlett Packard Enterprise