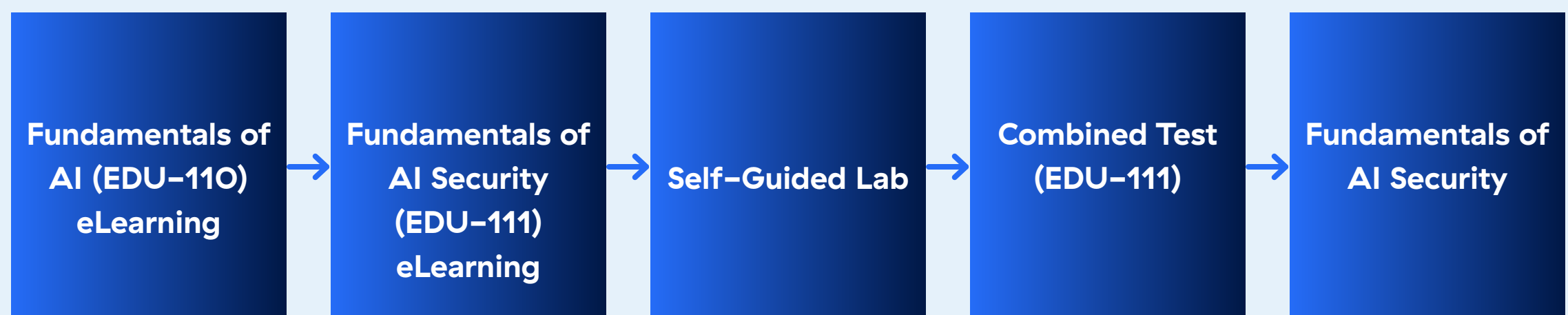


EDU-111 Learning Journey Map

The recommended path for Fundamentals of AI Security (EDU-111) is to complete the Fundamentals of AI (EDU-110) eLearning course first, then complete this eLearning course. Once both courses are complete, work through the self-guided lab to apply what you have learned. You can then take the combined test, which covers content from both EDU-110 and EDU-111. Upon passing, you will earn a completion certificate.

OUR LEARNING PATH



→ [Download Fundamentals of AI Security \(EDU-111\) Data Sheet](#)

LEARNING OUTCOMES

Once you complete this course, you will be able to:

- Describe how attackers use AI to enhance phishing, malware, and other cyber threats
- Explain how AI changes the data security risks organizations must manage
- Recognize why Shadow AI and legacy controls create visibility and control gaps
- Explain the purpose of the Zscaler AI Security Framework in securing AI adoption
- Recognize how AI Governance promotes safe usage policies



eLearning Details

Prerequisites	Fundamentals of AI (EDU–110)
Proficiency	Foundational
Description	In this course, you will explore how attackers weaponize AI, how data risks and Shadow AI expand the attack surface, and how organizations can respond using the Zscaler AI Security Framework.
Duration	65 Minutes
Type	Self–Paced
Completion Criteria	Complete the eLearning
Available Language(s)	English
Price per Set	Free

eLearning Outline

Topics	Sub Topics
Module Overview	• Introduction
How Attackers Weaponize AI	• How Attackers Weaponize AI • Phase 1: Reconnaissance • Phase 2: Access • Phase 3: Lateral Movement • Phase 4: Action
How Defenders Fight Back	• How Defenders Fight Back • Prompt Engineering Best Practices for Security • When Attackers Manipulate Your AI • Defending Against Adversarial Prompts • Key Defensive Mindset
The AI Data Security Challenge	• The AI Data Security Challenge • Why Traditional Security Fails • What Are We Risking?
Shadow AI and Why Legacy Controls Fail	• The Rise of Shadow AI • When AI Makes Things Up (Hallucination)



Topics	Sub Topics
Zscaler AI Security Framework	• Securing Your AI Transformation with Zscaler (three pillars) • The Framework in Action
From Detection to Debrief	• Detection • Investigation • Correlation • Response • Containment • Analysis • Hunting • Debrief • The Shift: From Reactive to Proactive

Self-Guided Lab Details

Prerequisites	Fundamentals of AI Security (EDU-111) eLearning Course
Proficiency	Foundational
Description	Practice what you learned in the course using a virtual lab environment. You will test how prompt design influences LLM behavior, evaluate data exposure risk when using public AI tools, and use AI to analyze a suspicious web log entry.
Duration	2 Hours
Type	Self-Paced Hands-On Lab
Completion Criteria	Complete all lab exercises
Available Language(s)	English
Price per Set	Free



Lab Outline

Task	Sub Task
Lab O: Connect to the Virtual Lab Environment	- EnvironmentTask O.1: Verify Lab Access - Task O.2: Use the Lab Clipboard
Lab 1: The Jailbreak Challenge	- Task 1.1: Enter a Direct Prompt - Task 1.2: Submit a Role-Play Prompt
Lab 2: The Helpful Intern	Task 2.1: Share Sensitive Data with a Public AI Tool
Lab 3: The Analyst’s Assistant	Task 3.1: Prompt the AI to Identify Attack Type and Risk Level

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.



Act Fast.
Stay Secure.