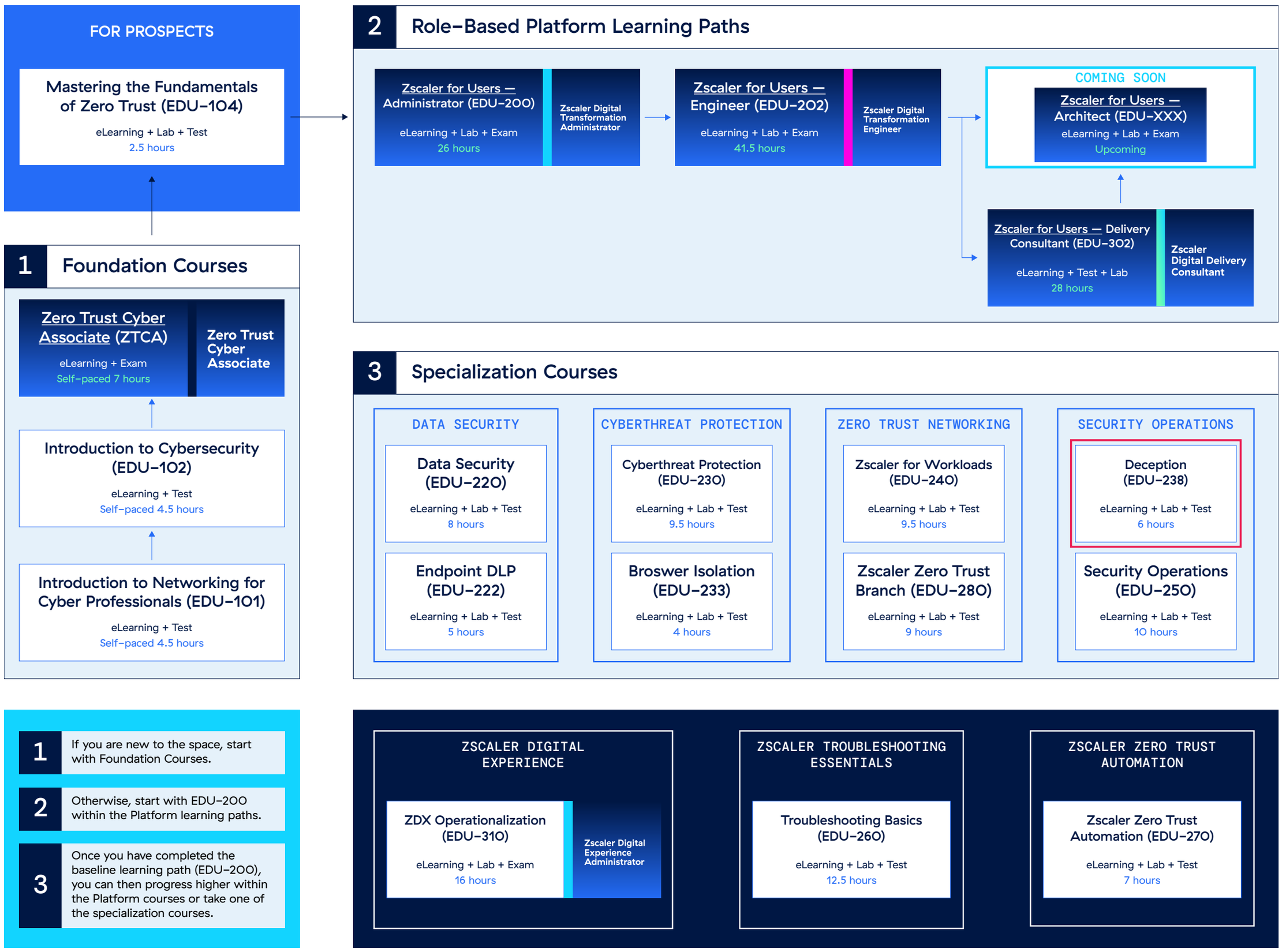
Zscaler Cyber Academy

Deception (EDU-238)

COURSE OUTLINE

Zscaler Cyber Academy Catalog

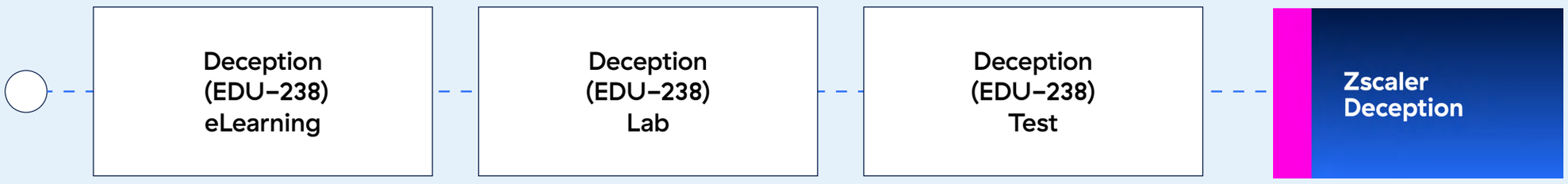


Deception (EDU-238) Learning Journey Map

The recommended path for the Deception learning journey is to complete the e-learning course and then take the hands-on labs. Once these are completed, you can sign up for the certificate test. You will have 45 minutes to answer its 20 questions, with 3 re-tests. Upon passing the test, you'll earn the Deception Certificate.

OUR LEARNING PATH

Deception (EDU-238) Learning Path



LEARNING OUTCOMES

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

- Explain what Zscaler Deception is and how it works
- Describe the value of Deception, including the challenges it solves and the benefits it provides
- Identify Deception's unique points of differentiation
- Monitor and analyze the activities of attackers
- Orchestrate automated workflows, notifications, and response rules
- Use prebuilt decoys and datasets to deploy effective Deception campaigns
- Gain visibility into credential misuse, entitlement exposures, and privilege escalation activities in Active Directory
- Identify advanced account settings, and user & roles management
- Recognize support options and how to access the help portal

eLearning Details

Prerequisites	Basic knowledge of Cybersecurity, Decoys
Proficiency	Intermediate
Description	The Zscaler Deception course is for internal Zscaler employees, customers, and partners. It is aimed at technical individuals responsible for proposing, architecting, deploying, and supporting the Zscaler Deception solution. This course provides an overview of how Deception uses lures and decoys to detect and disrupt cyberthreats that bypass traditional defenses. You will dive into the Zscaler's critical capabilities, benefits, the pains it solves, and the initiatives that are driving adoption. You will also gather insight into the unique differentiating value the product brings.
Duration	4 hours
Type	Self-paced
Completion Criteria	Complete the eLearning and Exam
Available Language(s)	English
Price per Seat	Free

eLearning Outline

Topics	Sub Topic

Current State of Cyberthreat Security	• Introduction to Deception
	• Security Challenges Posed by Cyberthreats
	  • Key Values of Deception
	  • What Sets Zscaler Deception Apart

Zscaler Deception	• Zscaler Deception Architecture
	  • Integration with ZPA
	  • Zscaler Deception Admin Portal
	  • Types of Decoys
	• Key Features and Benefits
	• How Deception Works
	• Deception Use Cases

Topics	Sub Topic
Investigate	• Investigate Overview • ThreatParse • Incidents

Orchestrate	• Orchestrate Overview
	• Orchestrate Rules
	• Integration Types
	  • Enrichment Integrations
	  • Containment Integrations
	  • SIEM Integrations
	• API Token Management
	  • Describe Use Cases for API access to Deception
	  • Describe API token details
	• Event Template
	  • Types of Event Template
	  • Template Settings
	• Service Connectors
	  • Usage of Service Connectors for SIEM Integration
	  • Service Connector Settings

Miragemaker	• Miragemaker Overview
	• Dataset Types
	  • Static Application Datasets
	  • Vulnerable Application (CVE) Datasets
	  • Dynamic Application Datasets
	  • SCADA/IoT Datasets
	  • Keyword Datasets
	  • Custom Service Datasets
	  • File Datasets and File Template
	• High-Interaction Containers
	• ThreatParse Rules

Topics	Sub Topic

Deceive	• Deceive Overview/Menu
	  • Start and Stop Decoys
	  • View Deployment Logs
	• Types of Decoys
	• Threat Intelligence (TI) Decoys
	• Network Decoys
	  • Internal Network Decoys
	  • Zero Trust Network Decoys
	• Active Directory (AD) Decoys
	  • User and Attributes
	  • Triggers
	  • Domains
	• Landmine Decoys
	  • Landmine Policies
	  • Landmine Agents
	  • Landmine Settings
	  • Landmine Update Phase Groups
	  • Landmine Safe Processes
	• Cloud Deception
	  • Deployment of Deception in Azure
	  • Deployment of Deception in AWS
	• MITM Detection
	• Deceive Settings
	  • Blocklist Management
	  • Hash Password Settings
	  • Hostname Resolution Settings
	  • Decoy Groups Management

ITDR	• ITDR Dashboard
	• Change Detection
	• ITDR for AD
	  • Scan Agents Settings Management
	  • Issue Safelist
	  • Object Safelist
	  • Change Detection Safelist

Topics	Sub Topic

Deception Settings	• Virtual Machine Settings
	  • Interface Settings
	  • Decoy Connector Settings
	  • Aggregators Settings
	  • Service Backend Settings
	• User and Roles Management
	  • User Management
	  • Role Management
	  • SSO Management
	  • Support User Management and Alert Notifications
	  • Login and Password Settings
	• Logs
	  • Audit Logs
	  • Debug Logs
	  • System Messages
	• Network Settings
	  • Allowed IPs Management
	• Advanced Settings
	  • Verify License Information
	  • Event Data and Evidence Management
	  • Log File Retention Settings
	  • Kill Switch Function (Account Deactivation)
	  • Debugging Settings
	• Account Settings
	  • Profile Settings
	  • Notification Preferences
	• Support Options
	  • Submit a Ticket
	  • Access Help Portal

Hands-On Lab Details

Prerequisites	Deception (EDU-238) – eLearning
Proficiency	Intermediate
Description	The Deception (EDU-238) lab provides students with the opportunity to acquire the essential skills necessary for safeguarding sensitive corporate data using Zscaler's Deception solution. Through this lab, students can gain proficiency in utilizing Deception to identify compromised users, prevent lateral movement, and effectively combat human-operated ransomware attacks.
Duration	3 hours
Type	Self-paced hands-on lab
Completion Criteria	Complete all hands-on labs
Available Language(s)	English
Price per Seat	$300 (1 credit)

Lab Outline

Task	Sub Task
Lab 1: Connect to the Virtual Lab	• Log into Client Connector and verify Deception service is running on endpoint
Lab 2: Navigate the Deception Admin Portal	• Investigate Threats • View Orchestrate Functions • View Miragemaker Options • View Deceive Functions • Check ITDR Posture • View Deception Settings
Lab 3: Investigate Pre-Breach connaissance Activity	• Conduct DNS brute force attack • Identify and respond to pre-breach reconnaissance
Lab 4: Lure Adversary to Decoys and Contain via ZPA	• Conduct post-breach attack from a compromised windows VM • Investigate and respond to post-breach attack

Certificate Exam Details

Prerequisites	Deception (EDU-238) Lab
Duration	45 minutes
Test Format	20 multiple-choice questions
Available Language(s)	English

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**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

Zero Trust Everywhere