Zscaler Cyber Academy

Security Operations (EDU-250)

COURSE OUTLINE

Zscaler Cyber Academy Catalog

FOR PROSPECTS

Mastering the Fundamentals of Zero Trust (EDU-104)
eLearning + Lab + Test
2.5 hours

1 Foundation Courses

Zero Trust Cyber Associate (ZTCA)
eLearning + Exam
Self-paced 7 hours
→ Zero Trust Cyber Associate

Introduction to Cybersecurity (EDU-102)
eLearning + Test
Self-paced 4.5 hours

Introduction to Networking for Cyber Professionals (EDU-101)
eLearning + Test
Self-paced 4.5 hours

2 Role-Based Platform Learning Paths

Zscaler for Users — Administrator (EDU-200)
eLearning + Lab + Exam
26 hours
→ Zscaler Digital Transformation Administrator

→ **Zscaler for Users — Engineer (EDU-202)**
eLearning + Lab + Exam
41.5 hours
→ Zscaler Digital Transformation Engineer

COMING SOON
Zscaler for Users — Architect (EDU-XXX)
eLearning + Lab + Exam
Upcoming

Zscaler for Users — Delivery Consultant (EDU-302)
eLearning + Test + Lab
28 hours
→ Zscaler Digital Delivery Consultant

3 Specialization Courses

DATA SECURITY
- Data Security (EDU-220)
  eLearning + Lab + Test
  8 hours
- Endpoint DLP (EDU-222)
  eLearning + Lab + Test
  5 hours

CYBERTHREAT PROTECTION
- Cyberthreat Protection (EDU-230)
  eLearning + Lab + Test
  9.5 hours
- Broswer Isolation (EDU-233)
  eLearning + Lab + Test
  4 hours

ZERO TRUST NETWORKING
- Zscaler for Workloads (EDU-240)
  eLearning + Lab + Test
  9.5 hours
- Zscaler Zero Trust Branch (EDU-280)
  eLearning + Lab + Test
  9 hours

SECURITY OPERATIONS
- Deception (EDU-238)
  eLearning + Lab + Test
  6 hours
- Security Operations (EDU-250)
  eLearning + Lab + Test
  10 hours

ZSCALER DIGITAL EXPERIENCE
- ZDX Operationalization (EDU-310)
  eLearning + Lab + Exam
  16 hours
  → Zscaler Digital Experience Administrator

ZSCALER TROUBLESHOOTING ESSENTIALS
- Troubleshooting Basics (EDU-260)
  eLearning + Lab + Test
  12.5 hours

ZSCALER ZERO TRUST AUTOMATION
- Zscaler Zero Trust Automation (EDU-270)
  eLearning + Lab + Test
  7 hours

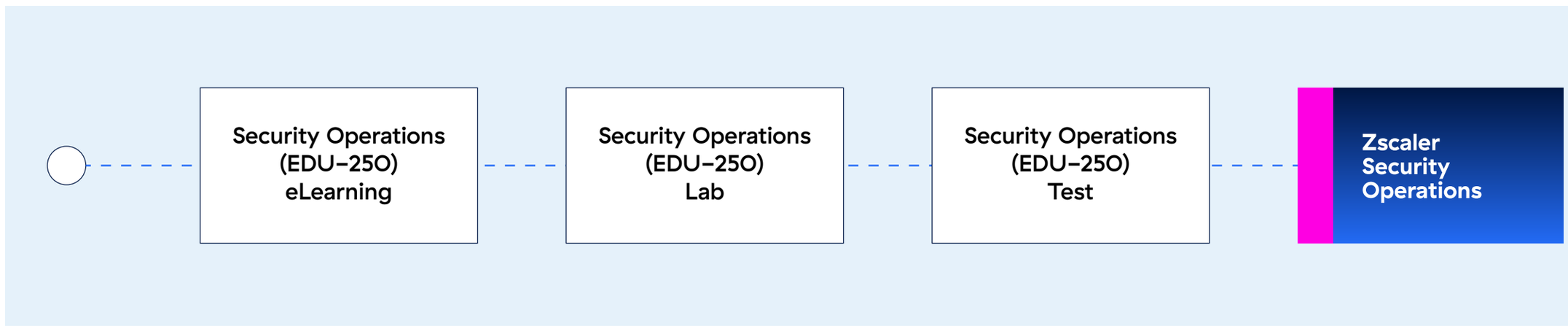
1. If you are new to the space, start with Foundation Courses.
2. Otherwise, start with EDU-200 within the Platform learning paths.
3. Once you have completed the baseline learning path (EDU-200), you can then progress higher within the Platform courses or take one of the specialization courses.

EDU-250 Learning Journey Map

The recommended path for the Security Operations 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 20 minutes to answer its 10 questions, with 3 re-tests. Upon passing the test, you'll earn the Security Operations Certificate.

OUR LEARNING PATH

Zscaler Zero Trust Automation (EDU-270) Learning Path



LEARNING OUTCOMES

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

- Explain the core principles and importance of cyber risk management in today's digital landscape
- Understand Risk Management platform offerings
- Identify key risk factors impacting an organization's security posture using Risk360
- Analyze comprehensive risk insights using the Zscaler Data Fabric for Security
- Explain how Zscaler UVM enhances the organization's vulnerability assessment and remediation processes
- Describe the strategic benefits of the Zscaler EASM solution
- Recognize the strategic importance of deploying Zscaler Deception technology
- Explain the role of Zscaler ITDR in enhancing detection and mitigation of identity-based threats
- Identify potential future security breaches using Zscaler Breach Predictor
- Implement advanced vulnerability management techniques using Zscaler UVM
- Develop strategies for continuous monitoring and management of the external attack surface using EASM
- Integrate ITDR capabilities with other security solutions for a comprehensive defense strategy
- Develop proactive defense mechanisms based on breach prediction insights and scenarios

eLearning Details

Prerequisites	None
Proficiency	Intermediate
Description	The Security Operations course explores Zscaler's products and solutions designed to enhance your organization's security posture through comprehensive security operations strategies. It covers foundational principles of risk management, including threat identification, assessment, and mitigation, with insights into Zscaler's Risk360, how Zscaler Data Fabric and UVM revolutionizes vulnerability management, an overview of Zscaler EASM, and finally we will focus on Deception: Architecture and Use Cases and explore how ITDR continuously monitors the Active Directory (AD) domain for any identity-based threats, and Breach Predictor, detailing their capabilities, use cases, and contributions to a robust cybersecurity strategy.
Duration	5 hours
Type	Self-paced
Completion criteria	Complete the eLearning
Available language(s)	English
Price per set	Free

eLearning Outline

Topics	Sub Topic
Introduction to Security Operations	• Zscaler — Four Comprehensive and Integrated Solutions • What is Risk Management? • Key Steps of Risk Management • Types of Risk • A Challenging Risk Landscape • Key Capabilities to Effectively Manage Risk • Zscaler's Comprehensive Security Operations Suite • Zscaler's Integrated Security Portfolio

Topics	Sub Topic	
Exposure Management	Intro to CTEM	• Why focus on exposure management? • What is CTEM? Why does it Matter? • Why is exposure management challenging?
Zscaler's Exposure Management Solutions	Zscaler's approach to exposure Management	• Separate solutions powered by one Data Fabric • Which use case is each solution designed to solve • How does the data fabric power better exposure management • Why context matters for better exposure prioritization
	Data Ingestion	• Configuring data sources — connector vs anysource • Configuring data source mapping — adding field mapping, using python scripts, adding fields to an entity if they are missing
Asset Exposure Management	Deduplicated Asset Inventory	• Using the asset view — to search for an asset, click into it and seeing details across sources • Asset Inventory Dashboard — report on inventory • Coverage & Gap — report on coverage gaps or overlaps
	Policies & Policy Violations	• What are policy rules & vioations? • Configuring policy rules • Working with policy violations — setting SLAs, assignees, creating tickets • Reporting on policy Compliance

Topics	Sub Topic	
Security Operations Product and Services	Zscaler Risk360	• Why Handling Risk is Important? • Risk360 and Its Key Capabilities • Risk360: Data Driven Risk Management • How Risk360 Works • Risk360 Platform Benefits • Contributing Factors to the Organizational Risk score • Challenges / Problem Statement • Solution: Zscaler Risk360 • How Does it Help? • How Risk360 Identifies and Assesses 4 Stages of Attack? • Risk Factors • Annotated Risk Score Trend Chart • Mapping to Security Risk Framework
	Risk360 Alert	• Alerts and Its Benefits • Alerts: Principles and Practices • Configuring Customized Alerts • Best Practices
	Financial Analysis	• Financial Analysis in Risk360 • Loss Exceedance • Understanding Loss Exceedance In Risk360
Zscaler Unified Vulnerability Management (UVM)	Introduction to Vulnerability Management	• What is Vulnerability Management? • Key Characteristics of Vulnerability Management • Vulnerability Management versus Risk Management • Why Organizations Need Both • Vulnerability Management → Exposure Management • How Zscaler UVM Efficiently Address Vulnerability and Exposure Management

Topics	Sub Topic	
Zscaler Unified Vulnerability Management (UVM)	Data Fabric for Security	• Zscaler Data Fabric and UVM • Introduction to Data Fabric • Connecting the Data • Need for Data Mapping • Data Unification • Key Capabilities of the Data Fabric for Security • The Zscaler Approach • Zscaler Data Fabric for Security
	Unified Vulnerability Management	• Operationalize your Data to solve UVM • UVM Portal Walkthrough
Breach Predictor		• What is Breach Predictor? • Breach Predictor Architecture • BP Process Flow • How BP Works? • IOC Detection: URL Fuzzy Matching • Kill Chain Reconstruction • Breach Predictor Use Cases
Zscaler EASM		• Zscaler EASM • Zscaler EASM: Key Features and Benefits • Zscaler EASM: Use Cases • Understanding Assets in EASM • Asset Discovery • Benefits of Asset Discovery • How Asset Discovery Works • Setting up Asset Discovery • Lookalike Domains • EASM Findings Page Overview — Filtering & Customization
Zscaler DECEPTION & ITDR	Deception	• Deception in a Zero Trust Architecture • Zero Trust + Deception • Disrupting Advanced Attacks with Deception • Deception Standalone Architecture • Using Deception with ZPA • Designed for the Zero Trust Exchange • Deception Use Cases

Topics	Sub Topic	
Zscaler DECEPTION & ITDR	Zscaler ITDR	• Identity–Based Attacks • Why is ITDR Crucial? • What is Zscaler ITDR? • Benefits of Zscaler ITDR • ITDR Dashboards
	Identity Threat Detection and Response (ITDR) — Demos	• ITDR Threat Detection Policies • Identity Change Detection • Entra ID Change Detection • Scanning an Active Directory

Hands–On Lab Details

Proficiency	Intermediate
Duration	4 hours
Type	Instructor–led hands–on lab
Price per set	$600 (2 credits)

Lab Outline

Task	Sub Task
Lab 1: Navigating to the Risk360 Portal	Task 1.1: View Risk360 Dashboard
Lab 2: View Reports in Risk360	Task 2.1: View CISO Board report, Attach Surface Report, Cybersecurity Maturity
Lab 3: Viewing Assets in Risk360	Task 3.1: View Asset Page (Overview, Distribution of Assets by Authentication Status, Authenticated Assets, Risky Asset Inventory)
Lab 4: Analyzing Risk with MITRE ATT&CK and NIST CSF	Task 4.1: Analyzing Risk MITRE ATT&CK Framework
	Task 4.2: Analyzing Risk with NIST CSF
Lab 5: Understanding Financial Risk in Risk 360	Task 5.1: Exploring Financial Risk Page

Task	Sub Task
Lab 6: Navigating to the External Attack Surface Management Portal	Task 6.1: View EASM Dashboard
Lab 7: Adding Discovery Profiles	Lab 7.1: Adding Discovery Profile
Lab 8: Navigating the Deception Portal	Task 8.1: Viewing Events on the Investigate Dashboard
	Task 8.2: Explore Orchestrate Menu in Deception Dashboard
Lab 9: Exploring Zscaler UVM	Task 9.1: Ingest Data from Many different Sources
	Task 9.2: Customize Scoring to meet your Organization's Needs
	Task 9.3: Explore Findings
	Task 9.4: Operationalize Risk Findings
	Task 9.5: Understanding Tickets
	Task 9.6: Exploring Remediation Dashboard
	Task 9.7: Understanding Risk Dashboard
	Task 9.8: Build Your Own Dashboard
Lab 10: Exploring Zscaler Asset Exposure Management	Task 10.1: Understanding Assets and Findings
	Task 10.2: Understanding Asset Inventory
	Task 10.3: Understanding Policies

Certificate Exam Details

Prerequisites	Security Operations Portfolio (EDU-250) — eLearning
Duration	30 minutes
Test format	15 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**

zscaler™

Zero Trust Everywhere