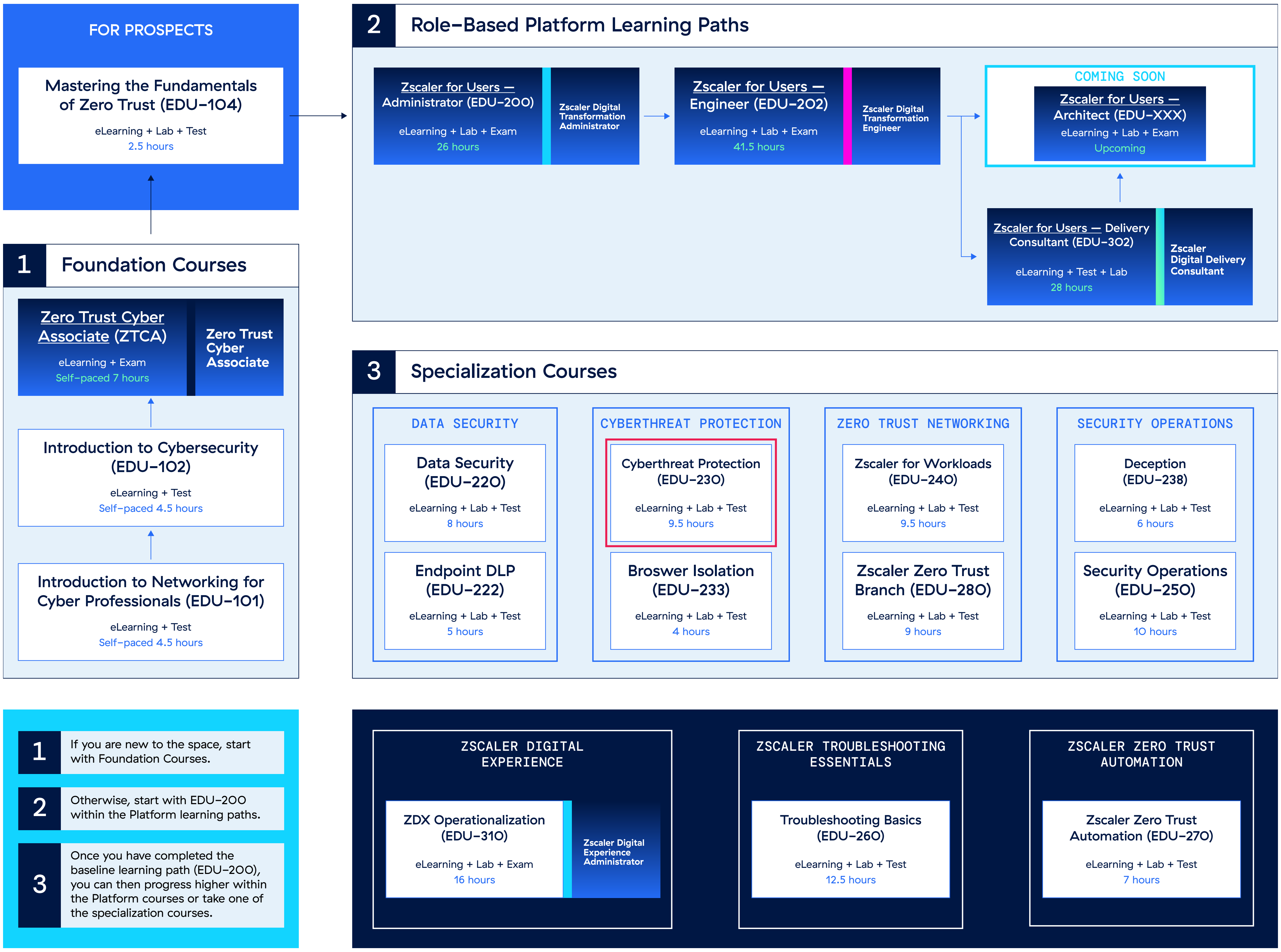
Zscaler Cyber Academy

Cyberthreat Protection (EDU-230)

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

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.

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

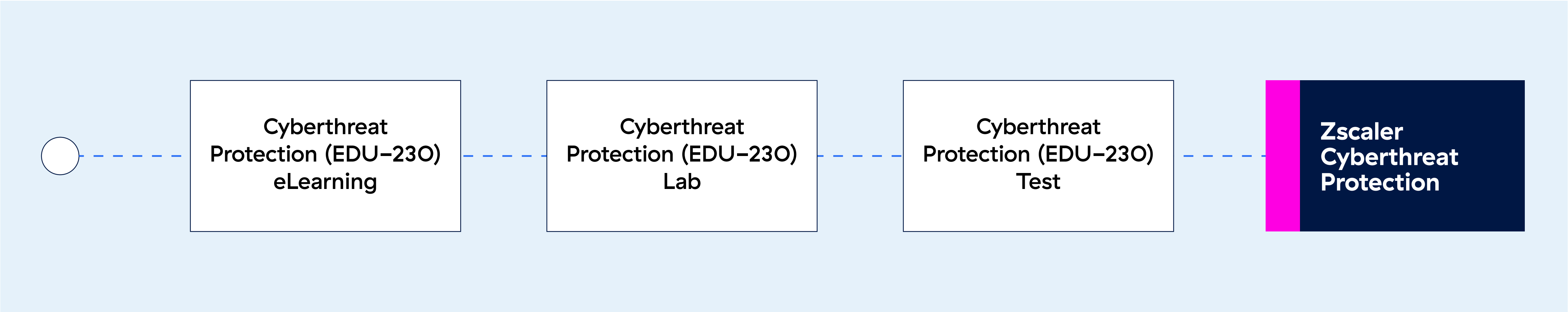
Zscaler Zero Trust Automation (EDU-270)
eLearning + Lab + Test
7 hours

EDU-230 Learning Journey Map

The recommended path for the Cyberthreat Protection 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 90 minutes to answer its 50 questions, with 3 re-tests. Upon passing the test, you'll earn the Cyberthreat Protection Certificate.

OUR LEARNING PATH

Cyberthreat Protection (EDU-230) Learning Path


Cyberthreat Protection (EDU-230) eLearning
Cyberthreat Protection (EDU-230) Lab
Cyberthreat Protection (EDU-230) Test
Zscaler Cyberthreat Protection

LEARNING OUTCOMES

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

- Explain cybersecurity, types of attack surfaces, and the different stages involved in a cyber attack framework
- Discuss the types of cyberattacks and malware, and how Zscaler holistically stops them
- List the malicious file protection capabilities that Zscaler offers through the malware protection configuration
- Identify Zscaler's Advanced Threat Protection capabilities and the options to utilize to configure the capability
- Describe and explain Cloud Sandbox, IPS, Deception, ITDR, Private AppProtection, and Browser Isolation
- Configure Advanced Threat Protection capabilities
- Discover how to configure Zscaler products and services to defend against attacks
- Recognize the cyber functions Zscaler has in place to analyze organizational risk and defend against cyber attacks

eLearning Details

Prerequisites	None
Proficiency	Intermediate
Description	This course will give you an in-depth understanding of the holistic cyberthreat protection that Zscaler offers including the importance of cybersecurity, the different types of cyber threats, and how to utilize Zscaler products and capabilities including Malware Protection, Advanced Threat Protection, Sandbox, Intrusion Prevention System (IPS), Deception, Identity Threat Detection and Response (ITDR), App Protection, and Browser Isolation to protect from these threats.
Duration	6 hours
Type	Self-paced
Completion criteria	Complete the eLearning
Available language(s)	English
Price per set	Free

eLearning Outline

Topics	Sub Topic
The Current State of Cybersecurity	• Cybersecurity: The Invisible War We're All Fighting • The Expanding Attack Surface: Why Every User Is a Target • AI: The New Double-Edged Sword in Cybersecurity • Types of Modern Cyberattacks: Beyond Malware • Some of the Most Dangerous Cyber Attacks
What is Cybersecurity?	• Cybersecurity Overview • Need for Cybersecurity • Attack Surface
Stages of a Cyberattack Framework	• Attack Surface Identification • Initial Compromise • Lateral Movement • Data Theft and Exfiltration
Types of Cyberattacks	• Malware • Phishing • Distributed Denial-of-Service (DDoS) • Man-in-the-middle (MITM) • SQL Injection • Insider Threat • Cryptojacking
How the Zscaler Zero Trust Exchange Platform Stops Cyberattacks	• The structure from connectivity services up to digital experience services. • Zscaler cyberthreat protection products and capabilities.
SSL Inspection	• SSL Inspection Overview • How does SSL Inspection Work? • Features that Depend on SSL/TLS Inspection • How Is SSL Inspection Deployed? • Root CA Enrollment • Granular Policy Framework for Effective Exemption Management • SSL Inspection: Pilot Ruleset • QUIC Protocol • Block QUIC (RFC 9000) to Avoid Blind Spots (UDP:443) • Applications with Customer Truststores: What are they? • What is Certificate Pinning/Hardcoded certificates? • Hardcoded Certificates: How to Identify? • Hardcoded Certificates: What to do about them? • Policy Types and Recommendations

Topics	Sub Topic
DNS Security	• DNS Security Overview • Zscaler DNS Security • DNS and Zscaler Threat Protection • DNS and Zscaler Enhanced Security Posture • Newly Registered & Observed Domains • Newly Revived Domains
Malware Protection	• Types of Malware • Common Delivery Mechanisms • Phishing (detailed explanation) • Exploit kits (detailed explanation) • Watering Hole (detailed explanation) • Pre-existing Compromise • Malicious file protections: • Options to block various types of malware, including spyware, adware, viruses, trojans, worms, and more. • Antivirus signatures and MD5 hashes used in malware identification. • Detection / Protection via Content Scanning • AI/ML to identify malicious files • Industry-Leading AV, Signature-Based Detection • ZIA Policy Design — Malware Policy • Policy Types and Recommendations — Malware Protection
Advanced Threat Protection	• Overview • Command and Control Channels • Zscaler Advanced Threat Protection • Zscaler Advanced Threat Protection Overview • Protection via URL Categories • Newly Registered and Observed Domains • Newly Revived Domains • Advanced Threat Protection: C2, Phishing • Advanced Threat Protection: Malicious Active Content & Server Side Vulnerabilities • Advanced Threat Protection: Anonymizers and P2P • PageRisk Engine detection via Webpage and Domain Features • AI-powered Phishing Detection • AI-powered C2 Detection • Key Differentiator • Advanced Threat Protection Configuration — Demo • Policy Types and Recommendations — Advanced Threat Protection

Topics	Sub Topic
Cloud Sandbox	• Overview • What is Zscaler Cloud Sandbox? • How does Cloud Sandbox Work? • AI-Driven Quarantine Effect of Cloud Sandbox • Cloud Sandbox Workflow • AI Instant Verdict Quarantine: Use Case • Cloud Sandbox Analysis Flow • Cloud Sandbox Policies • Example Cloud Sandbox policies • Granular Policies • Full coverage policy • Policies with risk tolerance • Complete visibility into Malware behavior • Zscaler Cloud Sandbox • Sandboxed File Flow per Policy • ZIA Policy Design — Sandbox Policy • Standard vs Advanced Cloud Sandbox
Intrusion Prevention System (IPS)	• Overview • Integrating IPS with the Zero Trust Exchange • Intrusion Prevention for all Web & Non-web Applications • Granular IPS Policy by IPS Category • Custom IPS SignaturesEvasive Traffic on Non-Standard Ports

Topics	Sub Topic

Deception	• What are Decoys?
	• Pot of Gold Scenario
	• Deception: Use Cases
	• Why Zscaler Deception?
	• Zscaler Deception Workflow
	  ◦ How Deception Works?
	  ◦ Zero Trust + Deception
	  ◦ Simplified Architecture
	  ◦ Decoys Supported
	  ◦ Investigate Dashboard
	  ◦ ThreatParse
	  ◦ ThreatParse Page
	  ◦ Orchestrate
	  ◦ Attacker Score
	  ◦ Cutting off Access based on Attack Score
	  ◦ Containment
	  ◦ MirageMaker
	  ◦ Vulnerable Application Datasets (CVE DataSheet)
	  ◦ Deceive
	  ◦ Landmine
	  ◦ Policy
	  ◦ Selection Criteria
	  ◦ Defense Evasion and Privilege Escalation
	  ◦ Advanced Deception Capabilities
	  ◦ Network Decoys
	• Set up a Zscaler Deception Campaign
	  ◦ Deploy Strategy
	  ◦ Deploy Network Strategy
	  ◦ Network Decoys

Zscaler ITDR	• Overview
	• What is Zscaler Identity Threat Detection and Response (ITDR?)
	• How it works
	• Extending Zero Trust with Zscaler Identity Protection
	  ◦ Zscaler ITDR Demo
	  ◦ Identity Risk Summary
	  ◦ Identity Posture
	  ◦ Endpoint Credential Exposure
	  ◦ Change Detection

<table>
<tr><th>Topics</th><th>Sub Topic</th></tr>
<tr><td>Private App Protection</td><td><ul>
<li>Overview</li>
<li>What Happens if App Protection is not Enabled?</li>
<li>Inline Inspection & Prevention for Private Applications</li>
<li>ZPA AppProtection</li>
<li>SSL Inspection Modes</li>
<li>Private AppProtection Flow Implementation</li>
<li>AppProtection Configuration</li>
</ul></td></tr>
<tr><td>Browser Isolation Overview</td><td><ul>
<li>Overview</li>
<li>Setting Up Zero Trust Threat Isolation
<ul>
<li>Browser Isolation for Public Applications</li>
<li>Granular Policy Control</li>
<li>AI-Powered Cloud Browser Isolation</li>
<li>Identifying Suspicious Domains</li>
<li>Browser Isolation + Unmanaged Devices + Identity Proxy = Isolation Proxy</li>
<li>Isolated SaaS Access from Unmanaged Devices</li>
<li>Browser Isolation for Private Applications</li>
<li>Ideal Enterprise Adoption of Browser Isolation</li>
<li>Granular Policy Control Demo</li>
</ul></li>
<li>Zscaler’s Browser Isolation
<ul>
<li>Zscaler’s Browser Isolation Safe Document Rendering</li>
<li>Content Disarm and Reconstruction (CDR): Flattened PDF Option in Isolation</li>
<li>Sandbox Integration with Isolation</li>
</ul></li>
<li>Browser Isolation Configuration
<ul>
<li>ZIA Isolation Profile Configuration</li>
<li>ZPA Isolation Profile Configuration</li>
</ul></li>
<li>Advanced Control Policies & Recommendations — Cloud Browser Isolation</li>
</ul></td></tr>
<tr><td>Detection and Response</td><td><ul>
<li>Overview</li>
<li>Alert Framework: Correlating Logs and Prioritize Alerts
<ul>
<li>The Correlation Engine</li>
<li>Export alerts from ZIA to SIEM products</li>
<li>Detection and Response Workflow</li>
<li>Alert Management</li>
<li>Alert Prioritization and Investigation</li>
<li>Impact Assessment and Remediation</li>
<li>Creating Custom Alert Rules</li>
<li>Alert Notifications</li>
</ul></li>
</ul></td></tr>
</table>

Hands–On Lab Details

Prerequisites	Cyberthreat Protection self paced e–learning course
Proficiency	Intermediate
Description	Practice what you learned in training using our remote lab. You'll configure secure internet access, isolate risky websites, inspect unknown files with Zscaler Sandbox, enforce safe access to web and SaaS apps using content filtering and access control, and extend zero trust with deception–based active defense.
Duration	4 hours
Type	Instructor–led hands–on lab
Completion criteria	Complete all hands–on labs
Available language(s)	English
Price per set	US $600 (2 credits)

Lab Outline

Task	Sub Task
Lab 1: Signing into ZIdentity landing page and Client Connector	• Test Cyber Risk Posture on Unprotected Device
Lab 2: Configuring SSL Inspection Policies	• Configure Forwarding Options • Enable SSL Inspection for All Destinations • Enable an SSL Exemption • Verify Zscaler CA Installation • Certificate Pinning Error
Lab 3: DNS Security	• Configure App Profile • Configure DNS control policy • DNS Insight Logs
Lab 4: URL Filtering and Cloud App Control	• View Threat Protection Configurations & Risk Reports • Configure URL Filtering Controls • Test End User Experience with URL Filtering • Configure Cloud App Control • Test End User Experience with Cloud App Control • Check Your Security Posture

Task	Sub Task
Lab 5: Configure Sandbox File Inspection and Set real time alerts	• Configure Sandbox Policies • Real-Time Alerts • View Sandbox Activity Report
Lab 6: Browser Isolation	• Build Isolation Profile • Implement Isolation Policy • Add URL/Cloud App Isolate Control Policies • Smart Browser Isolation
Lab 7: Deception-Based Active Defense	• Generate Recon Activity • Investigate Deception Alerts
Lab 8: ZPA Traffic Inspection via ZIA	• Provision an App Connector • Activate the App Connector • Add an Intranet Application • Add an Access Policy for the Intranet Application • Enable ZIA Inspected ZPA Apps

Certificate Exam Details

Prerequisites	Cyberthreat Protection Quiz
Duration	90 minutes
Test format	50 Objective Questions
Available language(s)	English
Price per attempt	US $300 (1 credit)

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