INFOSECTRAIN | CSA cloud security alliance®

CCZT

Certificate of Competence in Zero Trust

Training

Course Highlights

16-Hour Instructor-led Training

Learn from Industry Experts

Highly Interactive & Dynamic Sessions

Access to Recorded Sessions

Extended Post Training Support

Career Guidance and Mentorship

Mock Interview Tips and Techniques

Immersive Learning

Practical Examples from Real-world Case Studies

About Course

The **Certificate of Competence in Zero Trust (CCZT)** Training Course from InfosecTrain offers an in-depth exploration of the Zero Trust security model. The course is designed to provide participants with a comprehensive understanding of **Zero Trust Architecture (ZTA)**, its principles, and real-world use cases. Key topics include the fundamentals of Software-Defined Perimeter (SDP), developing a Zero Trust strategy, and effective planning and implementation.

Participants will learn how to evaluate their organization's current security posture, define the protect and attack surfaces, and develop a target architecture tailored to Zero Trust principles. The course also focuses on practical strategies for Zero Trust adoption, covering risk management, policy development, and implementation considerations, preparing participants for the **CCZT exam.**

Course Objectives

- Understand the foundational principles, components, and benefits of Zero Trust Architecture (ZTA).
- Identify key use cases for applying Zero Trust in various IT environments.
- Explore Software Defined Perimeter (SDP) technology and its deployment models.
- Develop a Zero Trust strategy, including key tactics and organizational buy-in.
- Plan Zero Trust adoption through gap analysis, scope definition, and business cases.
- Design a Zero Trust target architecture, including protected surfaces and policies.
- Assess implementation considerations for effective Zero Trust deployment.
- Manage and monitor Zero Trust deployments to align with security goals.

Target Audience

- C-Suite Executives, Managers, and Decision-makers
- Security Engineers, Architects, Analysts, and Administrators
- Compliance Managers
- Anyone involved in planning/implementing Zero Trust

Pre-Requisites

No formal experience is required, although CSA recommends having basic cloud and security experience (e.g., CCSK).

Exam Information

Exam Name	**CCZT Exam**
Exam Duration	120 minutes
Number of Questions	60
Exam Format	Multiple-choice Questions
Passing Score	80%
Exam Language	English

Course Content

Module 1 Introduction to Zero Trust Architecture

Context of ZTA

- ✓ History of ZT

Definitions, Concepts, and Components of ZT

- ✓ Definition of the ZT Concept
- ✓ Tenets
- ✓ Design Principles
- ✓ Pillars
- ✓ Components & Elements

Objectives of Zero Trust

- ✓ Technical Objectives
- ✓ Business Objectives

Benefits of Zero Trust

- ✓ Reduced Risk of Compromise
- ✓ Increased Trustworthiness of Access
- ✓ Increased Visibility &amp; Analytics
- ✓ Improved Compliance
- ✓ Additional Benefits

Planning Considerations ZTA

- ✓ Organizational & Technical Planning
- ✓ Risks of Project Implementation

Implementation Options of ZTA

- ✓ NIST Approach to ZT
- ✓ Software-Defined Perimeter
- ✓ Zero Trust Network Access

Zero Trust Use Cases

- ✓ Micro-Segmentation
- ✓ Software as a Service & ZT
- ✓ Hybrid, Multi-Cloud, & ZT
- ✓ Operational Technology
- ✓ 5G

Module 2 Introduction to Software Defined Perimeter

Software-Defined Perimeter History, Benefits, & Concepts

- ✓ SDP Definition & Function
- ✓ SDP Principles
- ✓ Relationship Between SDP & ZT
- ✓ History of SDP
- ✓ Technology Benefits of SDP
- ✓ Business Benefits of SDP

Traditional Architecture Issues and SDP Solutions

- ✓ Concerns SDP Addresses
- ✓ Threats SDP Protects Against
- ✓ SDP & Industry Adopted Solutions

Core Tenets, Underlying Technologies, and Architecture

- ✓ SDP Core Tenets
- ✓ Underlying Technology
- ✓ SDP Architecture Components
- ✓ SDP Secure Workflow

The Basics of SDP Deployment Models

- ✓ Architectural Considerations
- ✓ Deployment Models

Module 3 Zero Trust Strategy

Levels of Strategy

- ✓ Organizational Strategy - The Ultimate Goal
- ✓ Cybersecurity Strategy - Zero Trust
- ✓ IT Strategy & Technology
- ✓ Tactics
- ✓ Operations

Zero Trust Drivers and Buy-In

- ✓ The Value of Zero Trust
- ✓ Risk Management as a Driver
- ✓ Create a Case for Zero Trust
- ✓ Leadership Buy-In

Tactics for Zero Trust

- ✓ Zero Trust Design Principles
- ✓ Zero Trust Maturity Model
- ✓ The Five Steps for Zero Trust Implementation

Zero Trust and Operations

- ✓ Cultural & Organizational Shift
- ✓ Training & Education
- ✓ Regulatory & Compliance Shift
- ✓ Legacy Systems & Infrastructure
- ✓ Usability & Friction

Module 4 Zero Trust Planning

Starting the Zero Trust Journey

- ✓ Module Assumptions
- ✓ Initial Considerations

Planning Considerations

- ✓ Stakeholders
- ✓ Technology Strategy
- ✓ Business Impact Assessment
- ✓ Risk Register
- ✓ Supply Chain Risk Management
- ✓ Organizational Security Policies
- ✓ Architecture
- ✓ Compliance
- ✓ Workforce Training

Scope, Priority, and Business Case

- ✓ Prerequisite to Understanding the Protect Surface
- ✓ Scope
- ✓ Priority
- ✓ Development of a Business Case for ZT Planning
- ✓ Use Case Examples

Gap Analysis

- ✓ Determine Current State
- ✓ Determine the Target State
- ✓ Create a Roadmap to Close the Gaps
- ✓ Requirements

Define the Protect Surface and Attack Surface

- ✓ Identify the ZTA Protect Surface
- ✓ Identify the Attack Surface
- ✓ Illustration of Protect Surface & Attack Surface
- ✓ Protect & Attack Surface Considerations

Document Transaction Flows

- ✓ Example Transaction Flow: eCommerce
- ✓ Transaction Discovery: Functional Analysis & Tooling

Define Policies for Zero Trust

- ✓ The Policy
- ✓ The Policy Workflow
- ✓ Policy Considerations & Planning
- ✓ Continual Improvement
- ✓ Automation & Orchestration

Developing a Target Architecture

- ✓ Identity Considerations
- ✓ Device & Endpoint Considerations
- ✓ Network & Environment Considerations
- ✓ Workload & Application Considerations
- ✓ Data Considerations
- ✓ Visibility & Analytics Capability Considerations

- ✓ Automation & Orchestration Capability Considerations
- ✓ Governance Capability Considerations
- ✓ Examples of Zero Trust Architecture

Module 5 Zero Trust Implementation

Continuing the ZT Journey

- ✓ Training Assumptions

ZT Project Implementation Considerations

- ✓ Gap Analysis Report
- ✓ Aligning Information Security Policies with ZT
- ✓ Migration from Existing Architectures to ZTA
- ✓ Managed Service & In-House Implementation

Implementation Preparation Activities

- ✓ Defining ZT Project Deliverables
- ✓ Communicate ZT Change to Users
- ✓ Create an Implementation Checklist

ZT Target Architecture Implementation

- ✓ Zero Trust Pillars & Cross-Cutting Capabilities
- ✓ Transaction Flow Architecture Review
- ✓ Testing
- ✓ Continual Improvement
- ✓ Project Closure

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on