Zero Trust Training Curriculum Overview

Introduction

Building on the foundational principle of Zero Trust that no part of a computing and networking system can be implicitly trusted, including the humans operating it, CSA is developing a course to give you the knowledge and skills necessary to implement a Zero Trust strategy and reduce risk. Covering eight areas of Zero Trust knowledge, the Zero Trust Training (ZTT) will outline how to put measures in place to provide assurance that the systems and their components operate appropriately and are continuously verified. ZTT enables you to understand and implement Zero Trust principles into business planning, enterprise architectures and technology deployments.

Zero Trust Training Curriculum

The ZTT curriculum will cover eight areas of Zero Trust knowledge. Each area is composed of one or more training module(s) and will include a Study Guide and self-paced eLearning training that is approximately 60-90 minutes within each training module. Instructor-led training will be offered in the future, and a CSA exam and certificate for ZTT will be made available at a later date.

Eight Areas of Zero Trust Knowledge

- Zero Trust Strategy & Governance, Risk and Compliance
- Zero Trust Architecture
- Zero Trust Planning & Implementation
- Visibility, Analytics & Monitoring
- Identity
- Data, Assets, Applications and Services (DAAS)
- Device Security
- Applications and Workloads

Learning Objectives for Each Area of Knowledge

Zero Trust Strategy & Governance, Risk and Compliance

This area of Zero Trust knowledge includes modules that cover Zero Trust Strategy, Governance, Risk Management and Compliance.

- Understand the organization's current state
- Identify strategies that drive Zero Trust implementation approaches and identify core strategic principles for Zero Trust implementation
- Identify how a company's Zero Trust strategy supports the IT strategy and business goals
- Identify critical cultural, organizational and technical gaps for implementing a Zero Trust approach
- Identify the key components of the organization's Zero Trust Governance Framework
- Summarize how Zero Trust Governance Framework supports the organizational Risk Posture
- Summarize how Zero Trust Governance Framework supports the organizational Compliance Program
- Identify the key security controls to sustain an organizational Zero Trust driven approach to Governance, Risk and Compliance
- Identify key use cases, evaluate where each use case falls on the Zero Trust maturity scale, and approaches to prioritization

Zero Trust Architecture

This area of Zero Trust knowledge includes modules that cover SDP, ZTNA, Cloud Native / Containers / Microservices based Architectures.

- Fundamental components and architectural approaches in a Zero Trust environment
- Summarize the foundational components of an Software Defined Perimeter (SDP) Architecture
- Identify the key SDP features, technologies, deployment/architectural approaches and components
- Identify the difference between SDP and ZTNA
- Summarize the foundational components of Cloud Native / Containers / Microservices based Architecture
- Identify the key features, technologies, deployment/architectural approaches and components of a Cloud Native / Containers / Microservices based Architecture
- Explain how Zero Trust and DevSecOps can work together

Zero Trust Planning & Implementation

This area of Zero Trust knowledge includes modules that cover Zero Trust Planning and Implementation, a Zero Trust Maturity Model and Zero Trust use cases.

- Demonstrate understanding of the key considerations to be performed during the planning of a Zero Trust approach
- Identify the key steps for the implementation of the Zero Trust approach
- Understand effective internal communication and phase-wise plan for deployment
- Explain how to select the appropriate set of requirements and scope a Zero Trust approach
- Demonstrate understanding of how to map organizational data flows within the scope of the Zero Trust approach
- Demonstrate understanding of how to create Zero Trust policies
- Demonstrate understanding of the continual improvement process
- Demonstrate understanding of Zero Trust project risk management
- Demonstrate understanding of the Zero Trust Maturity Model
- Explain how the Maturity Model supports an organization's medium/long-term Zero Trust goal
- Summarize some of the common Zero Trust use cases

Visibility, Analytics & Monitoring

This area of Zero Trust knowledge includes modules that cover the foundational concept of asset discovery, logging, monitoring, analytics, security orchestration and automation.

- Demonstrating understanding of the role of Visibility, Analytics and Monitoring in a Zero Trust Architecture
- Explain asset inventory
- Summarize approaches for asset discovery
- Demonstrate understanding of security and network logging
- Security feeds and configuration alerts
- Demonstrate understanding of strategies for logs collection
- Demonstrate understanding of security analytics, automation and orchestration
- Demonstrate the methods for integration of baselines
- Explain the usage of Artificial Intelligence and Machine Learning in A&O and V&A

Identity

This area of Zero Trust knowledge includes modules that cover IAM foundational concepts, IAM security threats, vulnerabilities and risks, enhanced identity governance approaches and IAM best practices, Zero Trust Policy recommendations and Security Controls for IAM.

- Demonstrate understanding of IAM Components & Workflow
- Explain Directories

- Summarize key standards
- Demonstrate understanding of Authentication, Authorization and Accounting (AAA)
- Explain Single Sign-On (SSO), Multi-Factor Authentication (MFA) and Privileged Access
- Demonstrating understanding of the role of IAM in a Zero Trust Architecture
- Identify IAM security threats, vulnerabilities, and risks
- Identify IAM security and compliance best practices
- Identify Zero Trust Policy recommendations and Security Controls for IAM
- Mitigating controls for common identity-based attacks

Data, Assets, Applications and Services (DAAS)

This area of Zero Trust knowledge includes modules that cover the challenges and threats related to DAAS, DAAS best practices, Zero Trust Policy recommendations and Security Controls for DAAS.

- Demonstrate understanding of organizing principles of data
- Summarize major categories of data
- Demonstrating understanding of the role of DAAS in a Zero Trust Architecture
- Demonstrate understanding of Encryption & Key Management
- Summarize Data models (categories of data within common systems)
- Explain data protection principles and techniques
- Context around applying least privilege & Zero Trust principles to different data models
- Identify DAAS security threats, vulnerabilities, and risks
- Identify DAAS security and compliance best practices
- Identify Zero Trust Policy recommendations and Security Controls for DAAS

Device Security

This area of Zero Trust knowledge includes modules that cover Device Security challenges and threats, Device Security best practices, Zero Trust Policy recommendations and Security Controls for Device Security.

- Summarize the foundation of Device Security / Endpoint protection
- Understand the role of Device Security in a Zero Trust Architecture
- Identify Device Security threats, vulnerabilities and risks
- Identify Device Security and compliance best practices
- Identify Zero Trust Policy recommendations and Security Controls for Device Security
- Understand how different types of devices integrate with a Zero Trust Architecture

Applications and Workloads

This area of Zero Trust knowledge includes modules that cover APIs, Applications and Workloads challenges, threats and best practices, Zero Trust Policy recommendations and Security Controls for APIs, Applications and Workloads.

- Demonstrate understanding of the SPI model
- Summarize API, Application and workload categories and main characteristics
- Explain DevOps and DevSecOps
- Demonstrate understanding of the role of APIs Application and Workloads in a Zero Trust Architecture
- Identify APIs, Applications & Workload threats, vulnerabilities and risks
- Identify API, Application & Workload security and compliance best practices
- Identify Zero Trust Policy recommendations and Security Controls for APIs, Applications & Workloads

For more information about the ZTT curriculum or to learn more about CSA's Zero Trust program, visit cloudsecurityalliance.org/zt/ or contact zt@cloudsecurityalliance.org.