CCZT Curriculum

Certificate of Competence in Zero Trust (CCZT) Course Outline

Overview

The Certificate of Competence in Zero Trust (CCZT) is the industry’s first, most authoritative, vendor-neutral Zero Trust training and certificate program that delivers mainstream best practices for developing and implementing a Zero Trust philosophy. Covering 5 domains of Zero Trust knowledge, the CCZT provides an in-depth understanding of Zero Trust architecture, the drivers, benefits, and how to plan for adoption.

Introduction to Zero Trust Architecture

List of Figures
Course Intro
Course Structure
Course Learning Objectives

Content

1 Context of ZTA
1.1 History of ZT
2 Definitions, Concepts, & Components of ZT
2.1 Definition of the ZT Concept
2.2 Tenets
2.3 Design Principles
2.4 Pillars
2.5 Components & Elements
3 Objectives of ZT
3.1 Technical Objectives
3.1.1 Establishing a Protective Framework
3.1.2 Reduce Management Overhead
3.1.3 Reduce Attack Surface
3.1.4 Reduce Complexity
3.1.5 Enforces the Principle of Least Privilege
3.1.6 Improved Security Posture & Resilience
3.1.7 Improved Incident Containment & Management
3.2 Business Objectives
3.2.1 Risk Reduction
3.2.2 Compliance Management

© Copyright 2024, Cloud Security Alliance. All rights reserved.

3.2.3 Organizational Improvements
4 Benefits of ZT
4.1 Reduced Risk of Compromise
4.1.1 Reduced Attack Surface & Impact Radius
4.1.2 Reduced Ability to Move Laterally
4.1.3 Reduced Time to Detect & Contain Breaches
4.2 Increased Trustworthiness of Access
4.3 Increased Visibility & Analytics
4.4 Improved Compliance
4.5 Additional Benefits
5 Planning Considerations for ZTA
5.1 Organizational & Technical Planning
5.1.1 Understand Your Needs
5.1.2 Identify Key Stakeholders
5.1.3 Assemble a Team
5.1.4 Define Current State
5.1.5 Set Goals
5.1.6 Define the Use Cases
5.1.7 Develop Collaboration Plan
5.2 Risks of Project Implementation
6 Implementation Options of ZTA
6.1 NIST Approach to ZT
6.2 Software-Defined Perimeter
6.2.1 Description
6.2.2 Compliance with ZT Principles
6.2.3 Implementation Options
6.2.3.1 Service Initiated (Cloud-to-Cloud)
6.2.3.2 Collaboration Across Boundaries
6.2.4 Characteristics
6.3 Zero Trust Network Access
6.3.1 Description
6.3.2 Compliance with ZT Principles
6.3.3 Implementation Options
6.3.4 Advantages
6.3.5 Disadvantages
6.4 Google BeyondCorp
6.4.1 Description
6.4.2 Compliance with ZT Principles
6.4.3 Implementation Options
6.4.3.1 Service Initiated (Remote Application Access)
6.4.4 Advantages
6.4.5 Disadvantages
7 ZT Use Cases
7.1 Remote Access & VPN Replacement

© Copyright 2024, Cloud Security Alliance. All rights reserved.

7.1.1 Use Case Description
7.1.2 Security Risks
7.1.3 ZT Mitigation of Risks
7.1.3.1 User Experience Impact
7.2 Micro-Segmentation
7.2.1 Use Case Description
7.2.1.1 Types of Micro-Segmentation
7.2.2 Security Risks
7.2.3 ZT Mitigation of Risks
7.2.4 Limitations & Dependencies
7.3 Software as a Service & ZT
7.3.1 Use Case Description
7.3.2 Security Risks
7.3.3 ZT Mitigation of Risks
7.3.4 Limitations & Dependencies
7.4 Hybrid, Multi-Cloud, & ZT
7.4.1 Use Case Description
7.4.2 Security Risks
7.4.3 ZT Mitigation of Risks
7.4.4 Limitations & Dependencies
7.5 Operational Technology
7.5.1 Use Case Descriptions: CPS, IoT, IIoT, ICS \
7.5.1.1 IoT & IIoT
7.5.1.2 Industrial Control Systems
7.5.2 Security Risks
7.5.3 ZT Mitigation of Risks
7.5.4 Limitations & Dependencies
7.6 5G
7.6.1 Use Case Description
7.6.2 Security Risks
7.6.3 ZT Mitigation of Risks
7.6.4 Limitations & Dependencies

Ancillaries

Conclusion
Glossary

Introduction to Software-Defined Perimeter

List of Figures
Course Intro
Course Structure
Course Learning Objectives

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Content

1 SDP History, Benefits, & Concepts
- 1.1 SDP Definition & Function
- 1.2 SDP Principles
- 1.3 Relationship Between SDP & ZT
- 1.4 History of SDP
  - 1.4.1 The Origination of SDP
  - 1.4.2 The Business Case for SDP
- 1.5 Technology Benefits of SDP
  - 1.5.1 Reduced Attack Surface
  - 1.5.2 Authenticate & Authorize Before Access
  - 1.5.3 Centralized Organizational IAM Security
  - 1.5.4 Open Specification
- 1.6 Business Benefits of SDP
  - 1.6.1 Enhances Existing Cybersecurity Investments
  - 1.6.2 Cost Reduction & Labor Savings
  - 1.6.3 Reduces Compliance Scope

2 Traditional Architecture Issues & SDP Solutions
- 2.1 Concerns SDP Addresses
  - 2.1.1 The Shifting Perimeter
  - 2.1.2 The IP Address Challenge
  - 2.1.3 Integrating Security Controls
- 2.2 Threats SDP Protects Against
  - 2.2.1 CSA's Egregious 11
  - 2.2.2 Verizon's DBIR
  - 2.2.3 OWASP IoT Top 10
  - 2.2.4 OWASP Top 10
  - 2.2.5 Server Exploitation Threats
  - 2.2.6 Hijacking Threats
  - 2.2.7 Other Threats
- 2.3 SDP & Industry Adopted Solutions
  - 2.3.1 Network Access Control
  - 2.3.2 Virtual Private Network
  - 2.3.3 Identity & Access Management
    - 2.3.3.1 SDP & Identity Lifecycle Management
    - 2.3.3.2 SDP & Open Authentication Protocols
  - 2.3.4 Next Generation Firewall

3 Core Tenets, Underlying Technologies, & Architecture
- 3.1 SDP Core Tenets
- 3.2 Underlying Technology
  - 3.2.1 Drop-All Firewall
  - 3.2.2 Separate Control & Data Planes

© Copyright 2024, Cloud Security Alliance. All rights reserved.

3.2.3 Mutual Transport Layer Security
3.2.4 Single Packet Authorization
3.2.4.1 SPA Benefits
3.2.4.2 SPA Limitations
3.3 SDP Architecture Components
3.3.1 Initiating Hosts
3.3.2 SDP Client
3.3.3 Accepting Hosts
3.3.4 Controller
3.3.5 Gateway
3.4 SDP Secure Workflow
4 The Basics of SDP Deployment Models
4.1 Architectural Considerations
4.1.1 Existing Network Topologies & Technologies
4.1.2 Monitoring & Logging Systems
4.1.3 Application Release & DevOps
4.1.4 User Experience
4.1.5 Onboarding
4.1.6 Device Validation
4.2 Deployment Models
4.2.1 Client-to-Gateway Model
4.2.2 Client-to-Server Model
4.2.3 Server-to-Server Model
4.2.4 Client-to-Server-to-Client Model
4.2.5 Client-to-Gateway-to-Client Model
4.2.6 Gateway-to-Gateway Model

Ancillaries

Conclusion
Glossary

Zero Trust Strategy

List of Figures
Course Intro
Course Structure
Course Learning Objectives

Content

1 Levels of Strategy
1.1 Organizational Strategy - The Ultimate Goal

© Copyright 2024, Cloud Security Alliance. All rights reserved.

1.2 Cybersecurity Strategy - Zero Trust
1.2.1 Key Tenets of Zero Trust
1.2.2 Strategic Alignment & Operational Integration
1.3 IT Strategy & Technology
1.4 Tactics
1.5 Operations
2 Zero Trust Drivers & Buy-In
2.1 The Value of Zero Trust
2.2 Risk Management as a Driver
2.2.1 Board-Level Risk Management & Zero Trust Alignment
2.2.2 Evolving Threat & Risk Landscape
2.3 Create a Case for Zero Trust
2.4 Leadership Buy-In
3 Tactics for Zero Trust
3.1 Zero Trust Design Principles
3.1.1 Focus on Business Outcomes
3.1.2 Design from the Inside Out
3.1.3 Determine Who & What Needs Access
3.1.4 Inspect & Log Traffic
3.2 Zero Trust Maturity Model
3.2.1 Zero Trust Maturity Model in Practice
3.2.2 CISA-Based Maturity Model
3.3 The Five Steps for Zero Trust Implementation
3.3.1 Step 1: Define Your Protect Surface(s)
3.3.2 Step 2: Map & Prioritize the Transaction Flows
3.3.3 Step 3: Build a Zero Trust Architecture
3.3.4 Step 4: Create Zero Trust Policy
3.3.5 Step 5: Monitor & Maintain the Network
4 Zero Trust & Operations
4.1 Cultural & Organizational Shift
4.2 Training & Education
4.3 Regulatory & Compliance Shift
4.3.1 Regional Regulations
4.4 Legacy Systems & Infrastructure
4.5 Usability & Friction
4.5.1 User Experience
4.5.2 Site Reliability Engineering
4.5.2.1 Monitoring & Understanding System Compromises
4.5.2.2 Resource & Component Management

Ancillaries

Conclusion
Glossary

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Acronym List

Zero Trust Planning

List of Figures
Course Intro
Course Structure
Course Learning Objectives

Content

1 Starting the Zero Trust Journey
- 1.1 Module Assumptions
- 1.2 Initial Considerations

2 Planning Considerations
- 2.1 Stakeholders
  - 2.1.1 Stakeholder Responsibilities
  - 2.1.2 Stakeholder Communications
- 2.2 Technology Strategy
- 2.3 Business Impact Assessment
- 2.4 Risk Register
- 2.5 Supply Chain Risk Management
- 2.6 Organizational Security Policies
- 2.7 Architecture
- 2.8 Compliance
- 2.9 Workforce Training

3 Scope, Priority, & Business Case
- 3.1 Prerequisite to Understanding the Protect Surface
  - 3.1.1 Data & Asset Discovery & Inventory
  - 3.1.2 Data & Asset Classification
  - 3.1.3 Entities/User Discovery
- 3.2 Scope
- 3.3 Priority
- 3.4 Development of a Business Case for ZT Planning
- 3.5 Use Case Examples
  - 3.5.1 Role Based Access Control for Internal Staff
  - 3.5.2 Remote Access
  - 3.5.3 Services Accessed Using Mobile Devices
  - 3.5.4 Third-Party Service Providers with Remote Access
  - 3.5.5 Staff Access to Assets in Hybrid Environments
  - 3.5.6 SaaS & PaaS
  - 3.5.7 Application Release & DevOps
  - 3.5.8 Industrial Control Systems, Operational Technology, & Internet of Things

© Copyright 2024, Cloud Security Alliance. All rights reserved.

4 Gap Analysis
4.1 Determine Current State
4.2 Determine the Target State
4.3 Create a Roadmap to Close the Gaps
4.4 Requirements
5 Define the Protect Surface & Attack Surface
5.1 Identify the ZTA Protect Surface
5.2 Identify the Attack Surface
5.3 Illustration of Protect Surface & Attack Surface
5.4 Protect & Attack Surface Considerations
6 Document Transaction Flows
6.1 Example Transaction Flow: eCommerce
6.2 Transaction Discovery: Functional Analysis & Tooling
6.2.1 Collecting Data
6.2.2 Discovery of Known & Unknown Transactions
6.2.2.1 Transaction Inventory
6.2.2.2 Transaction Records
6.2.3 Monitoring & Analytics
6.2.4 Identifying Anomalies & Edge Cases
7 Define Policies for Zero Trust
7.1 The Policy
7.2 The Policy Workflow
7.3 Policy Considerations & Planning
7.4 Continual Improvement
7.5 Automation & Orchestration
8 Developing a Target Architecture
8.1 Identity Considerations
8.2 Device & Endpoint Considerations
8.3 Network & Environment Considerations
8.4 Workload & Application Considerations
8.5 Data Considerations
8.6 Visibility & Analytics Capability Considerations
8.7 Automation & Orchestration Capability Considerations
8.8 Governance Capability Considerations
8.9 Examples of Zero Trust Architecture

Ancillaries

Conclusion
Glossary

Zero Trust Implementation

List of Figures

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Course Introduction
Course Structure

Content

1 Continuing the ZT Journey
  1.1 Training Assumptions
2 ZT Project Implementation Considerations
  2.1 Gap Analysis Report
  2.2 Aligning Information Security Policies with ZT
  2.3 Migration From Existing Architectures to ZTA
  2.4 Managed Service & In-House Implementation
3 Implementation Preparation Activities
  3.1 Defining ZT Project Deliverables
  3.2 Communicate ZT Change to Users
  3.3 Create an Implementation Checklist
    3.3.1 Organization’s Governance
    3.3.2 Compliance
    3.3.3 Risk Management
    3.3.4 Operational Requirements
    3.3.5 Visibility & Analytics Integration
    3.3.6 Vulnerability Scanning & Patch Management
    3.3.7 Change Management Process
    3.3.8 Problem Management Process
    3.3.9 Incident Management
    3.3.10 Business Continuity Planning & Disaster Recovery
    3.3.11 Training & Awareness Programs
4 ZT Target Architecture Implementation
  4.1 Zero Trust Pillars & Cross-Cutting Capabilities
    4.1.1 Identity
      4.1.1.1 PDP Identity
    4.1.2 Applications & Workloads
    4.1.3 Networks & Environments
      4.1.3.1 Initial Client Authentication Request
      4.1.3.2 Authentication Request/Validation Request
      4.1.3.3 Decision Transmission
      4.1.3.4 Session Establishment or Termination
      4.1.3.5 Micro-Segmentation
      4.1.3.6 PEP Installation & Access Configuration
    4.1.4 Data
    4.1.5 Devices
      4.1.5.1 Deploying Agent-Based Access
      4.1.5.2 Deploying Agentless Access
    4.1.6 Visibility & Analytics

© Copyright 2024, Cloud Security Alliance. All rights reserved.

- 4.1.7 Automation & Orchestration
- 4.1.8 Governance
  - 4.1.8.1 ZT Policies
- 4.2 Transaction Flow Architecture Review
  - 4.2.1 Transaction Flow Mapping
  - 4.2.2 Converting Flow Maps to Transaction Lists
- 4.3 Testing
- 4.4 Continual Improvement
- 4.5 Project Closure

Ancillaries

Conclusion
Glossary
Acronym List

Learn More about CCZT

To learn more about the CCZT course structure, benefits, and available classes, visit https://cloudsecurityalliance.org/education/cczt.

© Copyright 2024, Cloud Security Alliance. All rights reserved.