Updated on 01/07/2025

Sign up

CCZT certification training

ALL-IN-ONE : EXAM INCLUDED IN PRICE

2 days (14 hours)

Presentation

Immerse yourself in the world of Zero Trust with our training course dedicated to the Cloud Security Alliance's CCZT certification. This structured course covers every stage of a Zero Trust program: from mapping the areas to be protected to automating controls and incident response. It fully prepares you for the official CCZT exam.

You'll start by familiarizing yourself with the Zero Trust reference frameworks (NIST 800-207, CISA Roadmap) and the CCZT Prep Kit. You'll learn how to identify your critical assets, define "protect surfaces" and build a Zero Trust roadmap aligned with your RGPD and ISO 27001 requirements.

The training continues with operational implementation: "least privilege" IAM strategies, GitOps/OPA integration, centralized log supervision and Zero Trust risk dashboard creation. You'll also orchestrate a DevSecOps pipeline capable of blocking any configuration drift.

As with all our training courses, this one will be presented with the latest updates for CCZT certification.

Objectives

- Assimilate the 7 Zero Trust pillars defined by the Cloud Security Alliance.
- Map "protect surfaces" and build a Zero Trust roadmap.
- Design and deploy a Zero Trust architecture in hybrid and multi-cloud environments.
- Automate controls and monitoring for COMEX management.
- Orchestrate incident response in a Zero Trust context.

Target audience

- Cybersecurity managers
- Cloud architect
- GRC consultants
- Cloud project managers

PREREQUISITES

- IT security basics: firewalls, encryption, IAM, networks

CCZT training program

Zero Trust origins and fundamentals

- Genesis of the concept: John Kindervag and the "Never Trust, Always Verify" strategy
- NIST 800-207 principles: policy engine, policy enforcement, trust algorithm
- Key terminology: protect surface, explicit verification, continuous monitoring
- Differences between traditional perimeter and Zero Trust Edge
- Cloud Security Alliance Framework (CSA ZT Working Group)

ZT Strategic Vision & Governance

- Business alignment: objectives, sponsors, stakeholders
- Roles & responsibilities: Zero Trust committee, RACI, budget and KPIs/KRIs
- Regulatory integration: RGPD, ISO 27001/17, FedRAMP, SecNumCloud
- 18-month roadmap: quick wins vs. structuring projects
- Workshop: Prioritizing Zero Trust initiatives (value/effort matrix)

Zero Trust Risk & Maturity Management

- Method for mapping critical assets and data
- Lateral risk assessment and identity attacks
- ZT Maturity Model (CISA, Gartner ZTX): organizational self-diagnosis
- Heat-map cloud risks: impact/probability & remediation plans
- Continuous measurement tools: scorecards, COMEX dashboards

Zero Trust Architecture (ZTA)

- Control, data and management plans
- Network micro-segmentation: SD-WAN overlay, ZTNA, reverse proxy
- Policy Decision Point (PDP) and Policy Enforcement Point (PEP) design
- Multi-cloud integration: AWS PrivateLink, Azure Private Link, Identity Broker
- Workshop: Drawing the target architecture on Draw.io

Software-Defined Perimeter & Zero Trust Access

- CSA SDP concepts: mutual TLS, cloaking, posture device
- Contextual authentication models: MFA, FIDO2, risk-based access
- Dynamic authorization: ABAC, OPA/Rego policy, security tags
- Deploying an open-source ZTNA gateway (OpenZiti / Cloudflare Tunnel)
- Workshop: Publish an internal service via SDP and test isolation

Identity, Devices & Micro-Segmentation

- Least privilege" strategies: role, attribute, workload identity
- Identity lifecycle management (CIEM, SCIM)
- Endpoint posture validation: EDR, Device Health Attestation
- Kubernetes micro-segmentation : Cilium/eBPF, network policies, service mesh
- Workshop: GitOps pipeline: OPA policy push and CI/CD validation

Observability, Automation & DevSecOps

- Unified logging: SIEM/SOAR multicloud, UEBA, deception tokens
- Real-time telemetry: metrics, traces, events and Zero Trust score
- IaC / GitOps automation: Terraform, Ansible, control policies
- Security scans: SAST, SCA, continuous SBOM, drift control
- Cost optimization (FinOps) in a Zero Trust posture

Incident Response & Continuous Improvement

- Zero Trust IR runbooks: segment isolation, secret rotation, cloud forensics
- Chaos engineering exercises: resilience testing and fail-open/close
- Configuration drift management: drift detection & auto-remediation
- PDCA loop: audit, KPI review, policy and script updates
- Quarterly ZT maturity improvement dashboards

CCZT Exam Preparation & Next Steps

- Official exam structure: 60 MCQs, 120 min, open-book, 80% threshold
- Review strategies: question bank, media indexing
- Timed mock exam and personalized debriefing
- Upgrade plan: CCZT ? CCSK / CCSP / Cloud Specialties
- CSA community: Circle, Slack alumni, update webinars

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning at training start

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.