+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 01/07/2025

S'inscrire

Formation certification CCZT

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

Plongez dans l'univers du Zero Trust avec notre formation dédiée à la certification CCZT de la Cloud Security Alliance. Ce parcours structuré couvre toutes les étapes d'un programme Zero Trust : de la cartographie des surfaces à protéger jusqu'à l'automatisation des contrôles et à la réponse aux incidents. Il vous prépare intégralement à l'examen officiel CCZT.

Vous débuterez par la prise en main des référentiels Zero Trust de référence (NIST 800-207, CISA Roadmap) et du Prep Kit CCZT. Vous apprendrez à identifier vos actifs critiques, définir les « protect surfaces » et bâtir une feuille de route Zero Trust alignée sur vos exigences RGPD et ISO 27001.

La formation se poursuit avec la mise en œuvre opérationnelle : stratégies IAM "least privilege", intégration GitOps/OPA, supervision centralisée des journaux et création de tableaux de bord de risque Zero Trust. Vous orchestrerez également un pipeline DevSecOps capable de bloquer toute dérive de configuration.

Comme pour toutes nos formations, celle-ci vous sera présentée avec les toutes dernières actualisations pour le passage de la certification CCZT.

Objectifs

- Assimiler les 7 piliers Zero Trust définis par la Cloud Security Alliance.
- Savoir cartographier les "protect surfaces" et bâtir une feuille de route Zero Trust.
- Concevoir puis déployer une architecture Zero Trust sur des environnements hybrides et multicloud.
- Automatiser les contrôles et la surveillance pour un pilotage COMEX.
- Orchestrer la réponse aux incidents dans un contexte Zero Trust.

Public visé

- Responsable cybersécurité
- Architecte cloud
- Consultants GRC
- Chef de projet cloud

PRÉ-REQUIS

- Bases de sécurité informatique : pare-feu, chiffrement, IAM, réseaux

Programme de notre formation CCZT

Origines & Fondamentaux Zero Trust

- Genèse du concept : John Kindervag et la stratégie “Never Trust, Always Verify”
- Principes NIST 800-207 : policy engine, policy enforcement, trust algorithm
- Terminologie clé : protect surface, explicit verification, continuous monitoring
- Différences périmètre traditionnel vs. Zero Trust Edge
- Cadre de référence de la Cloud Security Alliance (CSA ZT Working Group)

Vision Stratégique & Gouvernance ZT

- Alignement business : objectifs, sponsors, parties prenantes
- Rôles & responsabilités : comité Zero Trust, RACI, budget et KPIs/KRIs
- Intégration réglementaire : RGPD, ISO 27001/17, FedRAMP, SecNumCloud
- Roadmap 18 mois : quick wins vs. chantiers structurants
- Atelier : Prioriser les initiatives Zero Trust (matrice valeur/effort)

Gestion du Risque & Maturité Zero Trust

- Méthode de cartographie des actifs et données critiques
- Évaluation du risque latéral et attaques d’identité
- ZT Maturity Model (CISA, Gartner ZTX) : auto-diagnostic organisationnel
- Heat-map risques cloud : impact/probabilité & plans de remédiation
- Outils de mesure continue : scorecards, tableaux de bord COMEX

Architecture Zero Trust (ZTA)

- Plans de contrôle, de données et de gestion
- Micro-segmentation réseau : overlay SD-WAN, ZTNA, proxy inversé
- Conception d’un Policy Decision Point (PDP) et Policy Enforcement Point (PEP)
- Intégration multi-cloud : AWS PrivateLink, Azure Private Link, Identity Broker
- Atelier : Schématiser l’architecture cible sur Draw.io

Software-Defined Perimeter & Accès Confiance Zéro

- Concepts CSA SDP : mutual TLS, cloaking, posture device
- Modèles d’authentification contextuelle : MFA, FIDO2, risk-based access
- Autorisation dynamique : ABAC, policy OPA/Rego, tags de sécurité
- Déploiement d’une passerelle ZTNA open-source (OpenZiti / Cloudflare Tunnel)
- Atelier : Publier un service interne via SDP et tester l’isolation

Identity, Devices & Micro-Segmentation

- Stratégies “least privilege” : rôle, attribut, identité de workload
- Gestion du cycle de vie des identités (CIEM, SCIM)
- Validation de posture des terminaux : EDR, Device Health Attestation
- Micro-segmentation Kubernetes : Cilium/eBPF, policies réseau, service mesh
- Atelier : Pipeline GitOps : push d’une policy OPA et validation CI/CD

Observabilité, Automation & DevSecOps

- Journalisation unifiée : SIEM/SOAR multicloud, UEBA, deception tokens
- Télémétrie en temps réel : metrics, traces, events et score Zero Trust
- Automatisation IaC / GitOps : Terraform, Ansible, politiques de contrôle
- Scans sécurité : SAST, SCA, SBOM continu, contrôle de dérive
- Optimisation des coûts (FinOps) dans une posture Zero Trust

Réponse aux Incidents & Amélioration Continue

- Runbooks IR Zero Trust : isolation segment, rotation secrets, forensics cloud
- Exercices de chaos engineering : test de résilience et fail-open/close
- Gestion des dérives de configuration : drift detection & auto-remediation
- Boucle PDCA : audit, revue KPI, mise à jour politiques et scripts
- Tableaux de bord d’amélioration de maturité ZT trimestriels

Préparation à l’Examen CCZT & Prochaines Étapes

- Structure officielle de l’examen : 60 QCM, 120 min, open-book, seuil 80 %
- Stratégiques de révision : banque de questions, indexation des supports
- Examen blanc chronométré et débrief personnalisé
- Plan de montée en compétence : CCZT ? CCSK / CCSP / Spécialités Cloud
- Communauté CSA : Circle, Slack alumni, webinars d’actualisation

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.