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

Mis à jour le 27/11/2023

S'inscrire

Formation Zero Trust Security

3 jours (21 heures)

PRÉSENTATION

Zero Trust Security est un modèle de cybersécurité stratégique conçu pour protéger l'ensemble des actifs et des environnements numériques d'une entreprise. De plus en plus hétérogénes, ces écosystèmes sont généralement constitués de mixte entre clouds publics et privés, d'applications SaaS, d'environnements DevOps et de processus robotiques automatisés (APR).

Fondé sur le principe de « Never Trust, Always Verify », il vise à protéger les environnements numériques en s'appuyant sur quatre piliers : segmentation du réseau, prévention des mouvements latéraux, prévention des menaces sur la couche L7 et simplification du contrôle granulaire des accès utilisateurs.

Basé sur le logiciel BeyondCorp, il s'agit d'un des moyens les plus efficaces pour les entreprises de contrôler l'accès à leurs réseaux, applications et données.

Il intègre un large éventail de techniques de prévention, notamment l'authentification et l'analyse comportementale, la micro-segmentation, la sécurité des terminaux et les contrôles de moindre privilège, pour dissuader les attaquants potentiels et limiter leur accès en cas de violation.

À la suite de notre formation Zero Trust Security, vous saurez évaluer le modèle de sécurité déjà existant d’une entreprise et mettre en œuvre un nouveau réseau zéro-confiance au sein de l’entreprise.

OBJECTIFS

- Identifier les défis de la conception traditionnelle du réseau
- Comprendre la nécessité d'un accès réseau à Zero Trust
- Décrire les implications du changement d'environnement et du Cloud
- Identifier les caractéristiques de l'accès réseau à Zero Trust
- Savoir comment mettre en œuvre l'accès réseau du Zero Trust

PUBLIC VISÉ

- Développeurs
- Ingénieurs de sécurité informatique
- Professionnels en cybersécurité

Prérequis

- Connaissance de base des concepts de mise en réseau
- Connaissance de base en sécurité d'entreprises
- Connaissance de base des technologies de l'information (TI)

Programme de notre formation Zero Trust Security

Principes fondamentaux du Zero-Trust

- Qu'est-ce que le Zero Trust ?
- Quelques définitions du Zero Trust
- Ne jamais faire confiance, toujours vérifier
- Principes du Zero Trust
- Piliers du Zero Trust
- Contexte historique du Zero Trust

Pourquoi avons-nous besoin du Zero Trust ?

- Pièges de la sécurité périmétrique
- Transformation numérique
- L'état du Zero Trust
- Étude de cas : De SolarWinds à Zero Trust

Zero Trust Architecture

- Le modèle d'architecture Zero Trust (ZTA) du NIST
- Exemple de solutions ZTA réelles
- Approches de l'architecture ZTA du NIST
- Modèles de déploiement ZTA du NIST

Piliers architecturaux Zero Trust

- Pilier de sécurisation des utilisateurs et de l’identité
- Sécurisation des appareils Pillar
- Sécurisation du Pilier Réseau et Environnement
- Pilier Sécurisation des applications et des charges de travail
- Sécurisation du pilier des données
- Composants fondamentaux

- Rassembler tout le monde
- Étude de cas : Colonial Pipeline

Conception d’une architecture Zero Trust

- Il n’y a pas de moyen simple d’atteindre le Zero Trust
- Principes de conception Zero Trust
- La méthodologie de conception Zero Trust en cinq étapes
- Les cinq étapes de Forrester vers le Zero Trust

Migration vers le Zero Trust

- Élaboration d’une analyse de rentabilisation pour le Zero Trust
- Le défi du changement
- Créer une équipe Zero Trust
- Tirer parti de la courbe de mise en œuvre du Zero Trust

Exploration des cas d’utilisation du ZTA

- VPN-Less mise en œuvre
- Segmentation Est-Ouest
- Accès sécurisé De n’importe où
- Authentification et autorisation conditionnelles
- Microsoft ZTA étape par étape
- Exploration de la feuille de route Zero Trust de Cloudflare

Modèles de maturité Zero Trust

- Modèle de maturité Zero Trust de la NSA
- Modèle de maturité Microsoft Zero Trust
- Modèle de maturité Zero Trust de la CISA
- Dod Target et activités avancées Zero Trust

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.