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

Mis à jour le 26/08/2026

S'inscrire

Formation CNAPP avec Prisma Cloud

2 jours (14 heures)

Présentation

Prisma Cloud est une plateforme CNAPP conçue pour sécuriser les applications, les identités et les charges de travail sur des environnements multicloud. Avec la visibilité de bout en bout, le contrôle des risques et la remédiation guidée, vous structurez une sécurité cloud cohérente, du code à l'exécution.

Cette formation CNAPP avec Prisma Cloud vous permet d'aller au-delà des fondamentaux pour maîtriser les enjeux opérationnels de la sécurité cloud en environnement hybride et multicloud.

Vous apprendrez à comprendre l'architecture de Prisma Cloud, à exploiter les capacités de CSPM,CIEM,CWPP et IaC security, puis à organiser la détection des risques, la priorisation des alertes et la remédiation.

La formation vous amènera aussi à sécuriser les charges de travail, à analyser les mauvaises configurations, à renforcer la gouvernance des accès et à industrialiser des pratiques DevSecOps adaptées aux usages cloud.

À l'issue de ce parcours, vous serez en mesure de piloter une démarche CNAPP plus robuste, d'améliorer la posture de sécurité globale et de préparer une exploitation orientée production et conformité.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre les principes d'une approche CNAPP et le positionnement de Prisma Cloud.

- Identifier et prioriser les risques liés aux configurations, aux identités et aux charges de travail cloud.
- Exploiter les briques CSPM,CIEM,CWPP et IaC security dans une logique de bout en bout.
- Mettre en place une lecture opérationnelle des alertes, des politiques et des remédiations.
- Appliquer les bonnes pratiques de sécurisation DevSecOps et de gouvernance multicloud.

Public visé

- Ingénieur sécurité cloud
- Architecte cloud
- Analyste SOC
- DevSecOps
- Administrateur cloud

Pré-requis

- Connaissance des fondamentaux de la sécurité cloud et des concepts IaaS,PaaS et SaaS.
- Pratique d'un environnement AWS,Azure ou Google Cloud.
- Compréhension des notions d'identités, de rôles et de permissions dans le cloud.
- Notions de base en DevOps et en déploiement d'applications cloud-native.

Pré-requis techniques

- Ordinateur récent avec navigateur web à jour et ressources suffisantes pour les démonstrations.
- Connexion Wi-Fi ou Ethernet stable pour les accès console et les ateliers.
- Accès à un environnement cloud de démonstration ou à des comptes de test selon le contexte pédagogique.
- Casque et micro recommandés pour les sessions à distance et les échanges en atelier.
- Éditeur de texte ou IDE standard pour consulter des extraits de configuration et de code.

Programme de notre formation CNAPP avec Prisma Cloud

[Jour 1 - Matin]

Fondations CNAPP et architecture Prisma Cloud

- Comprendre le rôle d'une plateforme CNAPP dans la sécurisation du cycle de vie cloud.
- Positionner Prisma Cloud dans une stratégie de sécurité multicloud et hybride.
- Identifier les grands blocs fonctionnels, de la visibilité à la remédiation.
- Découvrir les notions de CSPM, CIEM, CWPP et IaC security.
- Lire l'organisation générale des actifs, des risques et des politiques de sécurité.
- Atelier pratique : prise en main de l'interface et repérage des principaux tableaux de bord.

[Jour 1 - Après-midi]

Posture de sécurité et conformité

- Analyser les mauvaises configurations les plus fréquentes sur les environnements cloud.
- Comprendre la logique de conformité, de contrôle continu et de cartographie des écarts.
- Explorer les politiques de sécurité et leur impact sur la priorisation des risques.
- Étudier la lecture des alertes, des scores et des niveaux de criticité.
- Relier posture de sécurité, gouvernance et exigences opérationnelles.
- Atelier pratique : qualification d'un ensemble de findings et construction d'un plan de remédiation.

[Jour 2 - Matin]

Identités, workloads et détection

- Approfondir la gestion des identités et des permissions avec CIEM.
- Comprendre l'exposition des charges de travail, des conteneurs et des environnements serverless.
- Relier la détection des menaces à la visibilité sur les actifs cloud.
- Examiner les usages de CWPP pour renforcer la protection runtime.
- Structurer une lecture orientée investigation et réduction du bruit d'alerte.
- Atelier pratique : analyse d'un scénario de risque combinant identité, workload et exposition cloud.

[Jour 2 - Après-midi]

Industrialisation et remédiation

- Intégrer la sécurité dans les chaînes DevSecOps et les workflows de livraison.
- Exploiter les contrôles sur l'IaC pour prévenir les erreurs avant déploiement.
- Organiser la remédiation manuelle ou guidée selon le niveau de criticité.
- Mettre en place des pratiques de suivi, de reporting et d'amélioration continue.
- Préparer une exploitation durable, adaptée aux contraintes de production et de conformité.
- Atelier pratique : conception d'un workflow de sécurisation de bout en bout, du code au cloud.

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.