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

Mis à jour le 20/08/2026

S'inscrire

Formation HolmesGPT

1 jour (7 heures)

Présentation

HolmesGPT est un agent SRE open source conçu pour accélérer l'investigation des incidents de production grâce à l'intelligence artificielle, aux métriques, aux logs et aux traces.

Notre formation HolmesGPT vous permettra de prendre en main cet outil d'investigation assistée afin de réduire le temps consacré au diagnostic des alertes et d'améliorer la qualité des premières analyses réalisées par les équipes d'exploitation.

Vous apprendrez à installer et configurer HolmesGPT, à sélectionner un fournisseur de modèles de langage, puis à connecter les sources d'observabilité utiles, notamment Kubernetes, Prometheus, les plateformes cloud et les outils de journalisation.

La formation vous permettra également de structurer des requêtes efficaces, d'interpréter les rapports générés et de recouper les hypothèses avec les données techniques disponibles. Vous saurez exploiter les investigations conversationnelles pour qualifier un incident, identifier les causes probables et préparer les actions de remédiation.

Enfin, vous aborderez les principes de sécurité, les permissions en lecture seule, la gouvernance des accès et l'automatisation des contrôles de santé. Vous disposerez ainsi d'une démarche opérationnelle pour intégrer HolmesGPT dans un processus SRE fiable et maîtrisé.

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

Objectifs

- Comprendre le positionnement de HolmesGPT dans une démarche SRE et d'observabilité.
- Installer et configurer HolmesGPT avec un fournisseur de modèles de langage.

- Connecter les sources de télémétrie nécessaires à l'investigation des incidents.
- Conduire une investigation assistée à partir d'une alerte Prometheus ou Kubernetes.
- Interpréter les résultats, valider les hypothèses et appliquer les principes de sécurité d'accès.

Public visé

- Ingénieur SRE
- Ingénieur DevOps
- Administrateur système
- Ingénieur plateforme
- Responsable observabilité

Pré-requis

- Expérience de l'exploitation d'applications en production.
- Connaissance des principes de supervision, de logs et de gestion d'incidents.
- Pratique des commandes de base sous Linux.
- Connaissances opérationnelles de Kubernetes et de Prometheus.

Pré-requis techniques

- Poste sous Linux, macOS ou Windows 11 avec environnement terminal disponible.
- Ordinateur disposant de 8 Go de RAM minimum et d'une connexion Internet stable.
- Installation de Python 3.10 ou version ultérieure et de Git.
- Accès à un environnement de démonstration Kubernetes et à une instance Prometheus, ou environnement fourni par le formateur.

Programme de notre formation HolmesGPT

[Jour 1 - Matin]

Fondamentaux et mise en place de HolmesGPT

- Positionnement de HolmesGPT dans les pratiques SRE, l observabilité et la réponse aux incidents.
- Architecture de l agent : interface conversationnelle, appels aux outils, fournisseurs de modèles et collecte de contexte.
- Installation et configuration initiale : variables d environnement, clés d accès, choix du modèle et modes d exécution.
- Connexion des données d exploitation : Kubernetes, Prometheus, logs, traces et services cloud.
- Sécurisation des investigations : RBAC, accès en lecture seule, périmètre des données et validation humaine.
- Atelier pratique : installer et configurer HolmesGPT, connecter un environnement Kubernetes de démonstration et réaliser une première requête de diagnostic.

[Jour 1 - Après-midi]

Investigation d incidents et industrialisation des contrôles

- Formulation d une investigation : contexte d alerte, symptômes observés, questions de suivi et exploitation des runbooks.
- Analyse croisée des métriques, des logs et des traces pour construire une hypothèse de cause racine.
- Lecture critique des rapports HolmesGPT : preuves collectées, limites des résultats, validation des hypothèses et priorisation des actions.
- Utilisation des alertes Prometheus, investigation conversationnelle et préparation d une réponse d incident exploitable.
- Introduction au mode opérateur : contrôles de santé planifiés, détection proactive et intégration dans les processus d exploitation.
- Atelier pratique : investiguer une alerte Prometheus simulée, identifier les éléments de preuve et rédiger une synthèse de diagnostic ; Atelier pratique : définir un contrôle de santé planifié, puis évaluer son périmètre, ses permissions et ses critères de validation.

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.