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

Mis à jour le 14/08/2026

S'inscrire

Formation Gatewatcher

2 jours (14 heures)

Présentation

Gatewatcher est une plateforme NDR pensée pour offrir une visibilité réseau complète, une détection avancée et une réponse rapide face aux menaces. Avec ses moteurs d'analyse, sa contextualisation des alertes et son approche orientée décision, Gatewatcher aide les équipes cyber à mieux prioriser et à mieux agir. Notre formation Gatewatcher vous permet de prendre en main les fondamentaux opérationnels de la plateforme pour exploiter efficacement ses capacités de détection, d'analyse et de pilotage des incidents. Vous apprendrez à comprendre l'architecture de la solution, à interpréter les événements réseau, à qualifier les alertes et à structurer une investigation cohérente dans un contexte SOC. La formation couvre également la mise en œuvre des principaux usages de surveillance, la lecture des indicateurs de compromission, l'exploitation des fonctions de priorisation et les bonnes pratiques de traitement des menaces. À l'issue de ces 2 jours, vous serez en mesure d'utiliser Gatewatcher avec méthode pour renforcer la détection des menaces, améliorer la réactivité de vos équipes et contribuer à une posture de sécurité plus robuste.

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

Objectifs

- Comprendre le positionnement de Gatewatcher dans une stratégie de NDR.
- Identifier les composants clés de la plateforme et leurs usages opérationnels.
- Analyser les alertes et les signaux faibles pour qualifier une menace.
- Structurer une investigation réseau à partir des données disponibles dans la solution.
- Exploiter les fonctions de priorisation pour améliorer le traitement des incidents.
- Appliquer les bonnes pratiques d'exploitation pour un usage quotidien en environnement SOC.

Public visé

- Analyste SOC
- Ingénieur cybersécurité

- Responsable sécurité des systèmes d'information
- Administrateur sécurité
- Consultant cybersécurité

Pré-requis

- Connaissances de base en réseaux et en adressage TCP/IP.
- Compréhension des principes de cybersécurité et de la supervision de sécurité.
- Pratique d'un SOC, d'un outil de supervision ou d'une solution de détection.
- Notions sur les journaux, les événements et les indicateurs de compromission.
- Expérience d'exploitation d'une console d'administration ou d'analyse de sécurité.

Pré-requis techniques

- Ordinateur récent avec navigateur web à jour et ressources suffisantes pour les démonstrations.
- Connexion Wi-Fi ou Ethernet stable pour accéder aux environnements de formation.
- Accès à un poste avec droits de connexion autorisant l'usage de la console de démonstration si fournie.
- Casque et micro recommandés pour les sessions à distance et les ateliers collaboratifs.
- Si un environnement de test est utilisé, disposer des identifiants et accès transmis en amont.

Programme de notre formation Gatewatcher

[Jour 1 - Matin]

Fondamentaux de la plateforme

- Positionnement de Gatewatcher dans une stratégie de NDR et de détection des menaces.
- Lecture de l’architecture fonctionnelle, des rôles des composants et des flux d’information.
- Compréhension des notions de visibilité réseau, de contextualisation et de priorisation.
- Présentation des types de signaux exploités pour détecter des activités suspectes.
- Panorama des usages en SOC et des cas d’emploi les plus courants.
- Atelier pratique : cartographier les composants de la solution et relier chaque brique à son rôle opérationnel.

[Jour 1 - Après-midi]

Exploration des alertes

- Navigation dans l’interface et repérage des zones utiles à l’analyse.
- Lecture d’une alerte, compréhension du contexte et identification des éléments déterminants.
- Différenciation entre bruit, signal faible et événement exploitable.
- Utilisation des filtres, des vues et des critères de recherche pour affiner l’analyse.
- Premiers réflexes de qualification pour orienter correctement le traitement.
- Atelier pratique : analyser un ensemble d’alertes et classer les événements selon leur niveau de criticité.

[Jour 2 - Matin]

Investigation et corrélation

- Méthode d’investigation à partir d’un indicateur, d’une alerte ou d’un comportement anormal.
- Exploration des relations entre hôtes, flux et objets observés dans la plateforme.
- Corrélation des signaux pour reconstituer une séquence d’attaque possible.
- Lecture des indices utiles à la qualification d’une menace connue ou inconnue.
- Organisation d’une investigation reproductible et exploitable par une équipe de sécurité.
- Atelier pratique : mener une investigation guidée à partir d’un scénario d’attaque simulé.

[Jour 2 - Après-midi]

Exploitation opérationnelle

- Structuration du traitement des incidents et des priorités d’action.
- Utilisation des fonctions de pilotage pour accélérer la prise de décision.
- Bonnes pratiques de suivi, de documentation et de restitution des analyses.
- Intégration de la solution dans une démarche de supervision quotidienne.
- Conseils d’industrialisation pour fiabiliser l’usage en environnement de production.
- Atelier pratique : construire un mini-processus de traitement d’incident à partir d’un cas d’usage métier.

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.