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

Mis à jour le 15/07/2026

S'inscrire

Formation CrowdStrike Falcon

2 jours (14 heures)

Présentation

CrowdStrike Falcon est une plateforme de sécurité cloud-native conçue pour renforcer la protection des endpoints, accélérer la détection et simplifier la réponse aux menaces. Avec son agent léger, ses capacités NGAV et son approche unifiée de la sécurité, elle aide les équipes à stopper les attaques modernes avec efficacité.

Notre formation CrowdStrike Falcon vous permettra d'aller au-delà de la prise en main pour maîtriser les usages opérationnels essentiels d'une console de sécurité moderne.

Vous apprendrez à structurer une stratégie de prévention, à comprendre le fonctionnement des politiques, à exploiter la télémétrie et à interpréter les alertes pour mieux qualifier les incidents.

Vous verrez également comment piloter les détections, affiner les règles de protection, gérer les remédiations et organiser une supervision cohérente dans un contexte de production.

À l'issue de la formation, vous serez en mesure de déployer une exploitation plus robuste de CrowdStrike Falcon, de réduire le bruit opérationnel et de renforcer la posture de sécurité de votre environnement.

Cette formation aborde enfin les bonnes pratiques de paramétrage, de suivi et d'administration pour fiabiliser l'usage quotidien de la plateforme et soutenir les équipes SOC et administration sécurité.

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

Objectifs

- Comprendre l'architecture et le positionnement de CrowdStrike Falcon.
- Configurer les principaux mécanismes de prévention et de protection endpoint.
- Analyser les alertes et exploiter la télémétrie pour qualifier les menaces.
- Gérer les politiques, les exceptions et les actions de remédiation.
- Structurer une exploitation opérationnelle adaptée à un contexte SOC ou administration sécurité.

Public visé

- Analyste SOC
- Administrateur sécurité
- Ingénieur cybersécurité
- Responsable sécurité des systèmes d'information
- Technicien support sécurité

Pré-requis

- Connaissances de base en cybersécurité et en protection des postes de travail.
- Compréhension des principes de Windows et de l'administration système.
- Notions sur les malwares, les journaux et l'analyse d'incidents.
- Expérience préalable avec une console de sécurité ou un EDR appréciée.

Pré-requis techniques

- Un ordinateur récent avec navigateur à jour et ressources suffisantes pour les démonstrations.
- Une connexion Internet stable en Wi-Fi ou Ethernet pour accéder aux environnements distants.
- Un environnement de travail autorisant l'usage d'une console web sécurisée et des outils de supervision.
- Un micro et un casque recommandés pour les sessions à distance et les ateliers collaboratifs.

Programme de notre formation CrowdStrike Falcon

[Jour 1 - Matin]

Fondamentaux de la plateforme

- Comprendre le rôle de CrowdStrike Falcon dans une stratégie de protection des endpoints.
- Identifier les composants clés, dont le capteur, la console et la logique cloud-native.
- Différencier prévention, détection et réponse dans un flux opérationnel.
- Découvrir les grandes familles de modules et leur contribution à la sécurité.
- Appréhender la logique de centralisation des événements et des alertes.
- Atelier pratique : prise en main guidée de l’interface, repérage des espaces de navigation et lecture d’un premier tableau de bord.

[Jour 1 - Après-midi]

Déploiement et protection initiale

- Préparer le déploiement du capteur sur différents postes de travail.
- Comprendre les principes de politique de prévention et de ciblage des groupes.
- Analyser les options de configuration liées à la protection temps réel.
- Gérer les exclusions, les exceptions et les impacts métier.
- Suivre l’état d’installation et vérifier la remontée de télémétrie.
- Atelier pratique : paramétrage d’une politique de base et validation de son application sur un jeu de machines de test.

[Jour 2 - Matin]

Détection et investigation

- Lire une detection et comprendre ses indicateurs principaux.
- Interpréter les informations de contexte, de processus et d’historique d’exécution.
- Relier les événements à une logique de chaîne d’attaque.
- Qualifier le niveau de criticité et prioriser les actions.
- Exploiter les éléments utiles à l’investigation pour documenter un incident.
- Atelier pratique : analyse d’alertes réelles ou simulées, puis rédaction d’un premier diagnostic opérationnel.

[Jour 2 - Après-midi]

Réponse opérationnelle et exploitation avancée

- Mettre en œuvre les actions de remédiation adaptées au contexte.
- Gérer le cycle de vie d’une alerte, de l’ouverture à la clôture.
- Exploiter les bonnes pratiques de suivi, de priorisation et de traçabilité.
- Structurer une exploitation quotidienne pour limiter le bruit et gagner en efficacité.
- Identifier les points d’attention pour l’administration et la supervision à long terme.
- Atelier pratique : traitement complet d’un incident, depuis la qualification jusqu’à la clôture et au compte rendu.

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.