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

Mis à jour le 09/10/2026

S'inscrire

Formation DFIR-IRIS : plateforme collaborative

2 jours (14 heures)

Présentation

DFIR-IRIS est une plateforme open source collaborative dédiée à la réponse aux incidents et aux investigations numériques. Elle permet aux équipes SOC, CSIRT et DFIR de centraliser les informations d'un incident, organiser les preuves et indicateurs de compromission et coordonner les différentes étapes d'une investigation.

Notre formation DFIR-IRIS vous permettra de maîtriser la plateforme afin de structurer et centraliser vos investigations de cybersécurité, depuis la qualification initiale d'un incident jusqu'à sa clôture.

Vous apprendrez à créer et organiser des dossiers d'investigation, gérer les tâches et responsabilités des analystes, documenter les événements puis centraliser les preuves et indicateurs de compromission (IOC) nécessaires à l'analyse.

La formation vous permettra également de construire des timelines, d'enrichir les informations collectées avec des sources de Threat Intelligence et d'exploiter les possibilités d'intégration avec l'écosystème SOC afin d'accélérer les investigations.

Vous découvrirez enfin comment automatiser certaines opérations avec l'API DFIR-IRIS, standardiser les procédures de traitement des incidents et produire des rapports permettant de conserver une trace exploitable des investigations et actions de remédiation.

À l'issue de cette formation, vous serez capable de centraliser, conduire et documenter une investigation de cybersécurité avec DFIR-IRIS, tout en améliorant la collaboration et la traçabilité au sein de vos équipes de réponse aux incidents.

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

Objectifs

- Prendre en main et administrer les principales fonctionnalités de DFIR-IRIS
- Créer et structurer des dossiers d'incident et d'investigation
- Centraliser les preuves, IOC, événements et timelines d'une investigation
- Organiser le travail collaboratif entre analystes SOC, CSIRT et DFIR
- Enrichir les investigations avec des sources de Threat Intelligence
- Intégrer et automatiser DFIR-IRIS dans un environnement SOC
- Documenter les actions de réponse et produire des rapports d'investigation

Public visé

- Analystes SOC
- Analystes et consultants DFIR
- Analystes forensic
- Membres d'équipes CSIRT et CERT
- Ingénieurs cybersécurité
- Responsables de la réponse aux incidents

Pré-requis

- Connaissances des fondamentaux de la cybersécurité
- Compréhension des principales étapes de la réponse aux incidents
- Notions sur les logs, alertes et indicateurs de compromission (IOC)
- Une première expérience en SOC, investigation ou sécurité opérationnelle est recommandée

Pré-requis techniques

- Un ordinateur équipé d'un navigateur web récent
- Une connexion Internet stable
- Accès à un environnement de laboratoire DFIR-IRIS fourni ou préparé pour la formation

Programme de notre formation DFIR-IRIS : gestion collaborative des incidents de cybersécurité

[Jour 1 - Matin]

Prendre en main DFIR-IRIS et organiser la réponse aux incidents

- Découvrir DFIR-IRIS et son positionnement dans un environnement SOC, CSIRT et DFIR
- Comprendre l'architecture de la plateforme et les principaux composants d'une investigation
- Prendre en main l'interface, les dossiers, les utilisateurs, les groupes et les droits d'accès
- Créer et structurer un cas d'investigation à partir d'un incident de sécurité
- Organiser les tâches, responsabilités et informations nécessaires au travail collaboratif

- Comprendre les principes de traçabilité et de gestion des données d'investigation
- Atelier pratique : créer un dossier d'incident, organiser l'équipe d'investigation et structurer les premières actions de réponse.

[Jour 1 - Après-midi]

Centraliser les preuves, IOC et informations d'investigation

- Collecter et organiser les éléments de preuve associés à un incident
- Enregistrer et qualifier les indicateurs de compromission (IOC) : adresses IP, domaines, URL, fichiers et hashes
- Documenter les événements et construire une timeline d'investigation
- Relier les éléments techniques aux événements et informations du dossier
- Utiliser les notes, tâches et commentaires pour faciliter la collaboration entre analystes
- Structurer les données afin de conserver une investigation lisible, traçable et exploitable
- Atelier pratique : enrichir un incident à partir d'IOC, preuves et événements puis reconstruire les premières étapes d'une compromission.

[Jour 2 - Matin]

Conduire et enrichir une investigation avec DFIR-IRIS

- Construire une méthodologie d'investigation collaborative depuis la qualification jusqu'à la remédiation
- Exploiter les informations du dossier pour identifier les systèmes, utilisateurs et actifs concernés
- Enrichir les indicateurs avec des sources et outils de Threat Intelligence
- Comprendre les possibilités d'intégration avec MISP et les services d'enrichissement externes
- Organiser les informations nécessaires à l'analyse de la chaîne d'attaque
- Suivre les actions de confinement, d'éradication et de remédiation dans le dossier
- Atelier pratique : conduire une investigation à partir d'une alerte, enrichir les IOC et déterminer le périmètre de compromission.

[Jour 2 - Après-midi]

Intégrer, automatiser et restituer les investigations

- Comprendre les possibilités d'intégration de DFIR-IRIS avec les outils SOC, SIEM, EDR et Threat Intelligence
- Exploiter l'API et les mécanismes d'automatisation pour enrichir les dossiers et réduire les tâches répétitives
- Standardiser les procédures, modèles et informations nécessaires au traitement des incidents
- Construire des rapports permettant de restituer les éléments techniques et les actions réalisées

- Clôturer un incident en conservant les preuves, décisions et enseignements nécessaires au retour d'expérience
- Appliquer les bonnes pratiques de gouvernance, sécurité et contrôle des accès à la plateforme
- Atelier pratique : traiter un incident complet, de son ouverture à son enrichissement, sa remédiation et la production du rapport final.

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg