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

Mis à jour le 19/08/2026

S'inscrire

Formation Secator

1 jour (7 heures)

Présentation

Secator est un framework et une CLI open source française développés par Freelabz pour automatiser les outils de reconnaissance et de pentest. Grâce à ses workflows YAML, ses options unifiées et ses résultats structurés, Secator accélère la conduite d'évaluations de sécurité reproductibles.

Notre formation Secator vous permettra de maîtriser l'utilisation opérationnelle de cet outil afin d'orchestrer des phases de reconnaissance, de cartographie et d'identification de vulnérabilités sur des périmètres explicitement autorisés.

Vous apprendrez à installer et configurer Secator, à exécuter des tâches unitaires, des workflows et des scans, puis à exploiter les outils intégrés tels que subfinder, httpx, naabu, nuclei et katana.

À l'issue de la formation, vous serez en mesure de définir des cibles, de paramétrer les options de scan, de contrôler le rythme des requêtes et d'interpréter des sorties normalisées pour prioriser vos investigations.

Cette formation aborde également la création de workflows YAML, l'enchaînement des tâches, le filtrage des résultats et les bonnes pratiques de traçabilité afin de produire des analyses plus fiables et adaptées à un contexte professionnel.

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

Objectifs

- Installer et configurer Secator dans un environnement de test dédié

- Exécuter des tâches, workflows et scans sur des cibles autorisées
- Paramétrer les options de reconnaissance, de vitesse et de filtrage
- Interpréter les résultats structurés et prioriser les éléments à investiguer
- Créer un workflow YAML simple pour automatiser une chaîne de reconnaissance

Public visé

- Pentester
- Consultant cybersécurité
- Analyste sécurité
- Ingénieur sécurité offensive
- Bug bounty hunter

Pré-requis

- Connaissances des phases d'un test d'intrusion et du cadre d'autorisation
- Maîtrise des commandes courantes sous Linux
- Notions de reconnaissance réseau, web et DNS
- Connaissances de base des formats JSON et YAML

Pré-requis techniques

- Poste équipé de Kali Linux récent ou d'une distribution Linux compatible, native ou en machine virtuelle
- Processeur 64 bits, 8 Go de RAM minimum et 20 Go d'espace disque disponible
- Python 3 et Git installés, avec les droits nécessaires pour installer les dépendances
- Terminal, éditeur de texte ou IDE compatible YAML
- Connexion Internet stable, sans filtrage bloquant les téléchargements et les cibles de laboratoire autorisées

Programme de notre formation Secator

[Jour 1 - Matin]

Prise en main et automatisation de la reconnaissance

- Positionnement de Secator dans une démarche de pentest, cadre légal, périmètre autorisé et règles de sécurité opérationnelle
- Architecture de la CLI, concepts de tâches, workflows, scans et formats de résultats unifiés
- Installation, vérification de l'environnement et découverte des commandes essentielles de Secator
- Exécution de tâches de reconnaissance avec subfinder, dnsx, httpx et naabu
- Paramétrage des cibles, des options globales, des limites de débit et des options propres aux outils intégrés

- Atelier pratique : réaliser une chaîne de reconnaissance sur un périmètre de laboratoire autorisé, identifier les sous-domaines, services exposés et endpoints accessibles

[Jour 1 - Après-midi]

Workflows YAML et exploitation des résultats

- Lecture et analyse des sorties structurées, types de résultats, exports et critères de qualification des découvertes
- Utilisation des workflows existants pour le crawling, la recherche de contenus et l'identification de vulnérabilités avec katana, ffuf et nuclei
- Structure d'un fichier YAML, définition des tâches, entrées, options, tags et filtrage des résultats
- Enchaînement des traitements, réutilisation des résultats comme cibles et introduction aux exécutions parallèles
- Bonnes pratiques de contrôle de charge, de validation manuelle, de journalisation et de restitution des résultats
- Atelier pratique : exécuter le workflow, filtrer les résultats et produire une synthèse de constats priorisés

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.