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

Mis à jour le 11/09/2026

S'inscrire

Formation Certification TryHackMe SEC1

Présentation

La Formation Certification TryHackMe SEC1 prépare à la certification officielle Cyber Security 101 (SEC1), une validation pratique des fondamentaux en cybersécurité. Vous apprendrez à analyser, investiguer et sécuriser des environnements simulés grâce à des laboratoires hands-on orientés situations réelles.

Cette formation vous permet de préparer méthodiquement l'examen Cyber Security 101 (SEC1), conçu pour valider des compétences opérationnelles plutôt que la simple restitution de connaissances. Vous travaillerez les fondamentaux des systèmes, des réseaux, de la sécurité offensive et de la sécurité défensive.

Vous apprendrez à utiliser la ligne de commande sous Linux et Windows, à interpréter des flux réseau, à identifier des vulnérabilités web et à comprendre les mécanismes de protection des identités, des mots de passe et des postes de travail.

La préparation aborde également l'analyse de journaux, les principes de supervision SOC, la réponse aux incidents, l'initiation à l'analyse de malwares et les outils essentiels de diagnostic. Chaque notion est mise en application dans des scénarios progressifs proches du format de certification.

À l'issue de la formation, vous serez en mesure d'aborder l'examen pratique avec une méthode claire, de résoudre des tâches techniques en environnement contrôlé et de démontrer les compétences fondamentales validées par la certification Cyber Security 101 (SEC1).

Objectifs

- Comprendre le périmètre et le déroulement de la certification Cyber Security 101 (SEC1)
- Utiliser les commandes essentielles sous Linux et Windows
- Analyser les principaux protocoles réseau, paquets et journaux de sécurité
- Identifier des vulnérabilités web et appliquer une démarche de test encadrée

- Réaliser les étapes fondamentales d'investigation, de détection et de réponse à incident
- Se préparer à résoudre des scénarios pratiques dans l'environnement TryHackMe

Public visé

- Analyste cybersécurité junior
- Analyste SOC junior
- Administrateur système junior
- Technicien support informatique
- Étudiant en cybersécurité

Pré-requis

- Connaissances de base des postes de travail et des systèmes d'exploitation
- Notions élémentaires de réseaux TCP/IP et d'adressage IP
- Familiarité avec la navigation web et la gestion de fichiers
- Première approche de la ligne de commande Linux ou Windows

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou version ultérieure, de macOS ou d'une distribution Linux récente
- Navigateur Google Chrome ou Mozilla Firefox à jour
- Connexion Internet stable, autorisant l'accès aux laboratoires en ligne et sans filtrage de sécurité bloquant
- Compte personnel TryHackMe actif
- Écran avec une résolution minimale de 1366 x 768 et 8 Go de mémoire vive recommandés

Programme de notre formation TryHackMe SEC1

[Jour 1 - Matin]

Comprendre la certification et les fondations cyber

- Découverte de la certification Cyber Security 101 (SEC1), de son positionnement débutant et de ses compétences évaluées
- Présentation du format pratique : scénarios, tâches techniques, questions associées et gestion de la fenêtre d examen
- Panorama des métiers, des équipes Red Team, Blue Team et des workflows d investigation
- Rappels sur les systèmes d exploitation, les fichiers, les processus, les utilisateurs et les droits
- Prise en main de l environnement de laboratoire TryHackMe et méthodologie de résolution d une tâche
- Atelier pratique : explorer un laboratoire guidé, identifier les éléments d un système et collecter les premières informations utiles

[Jour 1 - Après-midi]

Systèmes, ligne de commande et gestion des accès

- Fondamentaux de Linux : arborescence, navigation, recherche de fichiers et permissions
- Fondamentaux de Windows : comptes, services, système de fichiers et commandes usuelles
- Utilisation progressive des shells, des redirections et des commandes de consultation
- Compréhension des utilisateurs, groupes, privilèges et mécanismes d authentification
- Bonnes pratiques pour relever des preuves techniques et formuler une réponse précise lors de l examen
- Atelier pratique : réaliser une investigation guidée sous Linux et Windows pour retrouver des informations, comptes et droits d accès

[Jour 2 - Matin]

Réseaux et analyse de trafic

- Révision des notions TCP/IP, adressage, ports, services et flux réseau
- Lecture des protocoles courants : DNS, HTTP, HTTPS, SSH et SMB
- Principes de sécurité réseau : segmentation, filtrage, chiffrement et protocoles sécurisés
- Initiation à la capture et à l interprétation de paquets avec Wireshark et tcpdump
- Découverte de l énumération de services avec Nmap dans un cadre autorisé
- Atelier pratique : analyser une capture réseau, identifier les services exposés et repérer un échange anormal

[Jour 2 - Après-midi]

Cryptographie, mots de passe et sécurité web

- Comprendre les rôles du chiffrement, du hachage, des clés et des certificats
- Différencier authentification, autorisation, gestion des sessions et protection des identifiants
- Identifier les attaques par dictionnaire et force brute, ainsi que les mesures de protection adaptées
- Découvrir le fonctionnement d une application web : requêtes, réponses, paramètres, cookies et formulaires
- Reconnaître les vulnérabilités web fondamentales et adopter une démarche de test responsable avec Burp Suite
- Atelier pratique : observer des requêtes web, identifier une faiblesse simple et proposer une mesure corrective

[Jour 3 - Matin]

Sécurité offensive et investigation défensive

- Comprendre les phases d une démarche offensive : reconnaissance, énumération, exploitation et post exploitation
- Découvrir les outils fondamentaux d énumération, de recherche de contenu et d accès distant dans un laboratoire contrôlé
- Introduction aux principes d exploitation de vulnérabilités et aux limites éthiques et légales des tests
- Fondamentaux de la défense : journaux, alertes, indicateurs de compromission et supervision SOC
- Premières étapes de triage : qualifier un événement, collecter les preuves et prioriser une investigation
- Atelier pratique : mener un scénario de détection, corréler des journaux et produire un premier diagnostic d incident

[Jour 3 - Après-midi]

Révision ciblée et mise en situation de certification

- Révision des domaines essentiels : systèmes, réseaux, sécurité web, outils offensifs et opérations défensives
- Initiation à l analyse de malwares : types de menaces, comportements observables et précautions de manipulation
- Utilisation de données techniques : journaux, fichiers, hash, URL et indicateurs de compromission
- Méthode de résolution d un scénario : lire le contexte, tester, vérifier, documenter et répondre
- Stratégie de préparation à l examen Cyber Security 101 (SEC1) : organisation, gestion du temps et contrôle des réponses
- Atelier pratique : réaliser une mise en situation de certification combinant analyse système, réseau, web et investigation défensive

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.