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

Mis à jour le 30/09/2025

S'inscrire

Formation Certification TryHackMe SAL1

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

TryHackMe SAL1 est une certification pratique dédiée aux centres d'opérations de sécurité (SOC). Elle valide les compétences d'un Analyste SOC Junior en matière de triage, investigation et réponse aux incidents dans un environnement simulé.

Notre formation TryHackMe SAL1 vous permettra de maîtriser la collecte et la normalisation de logs, la détection et l'enrichissement des alertes, l'investigation dans un SIEM et la réponse aux incidents.

Vous apprendrez à utiliser des outils concrets pour analyser le trafic, identifier des indicateurs de compromission (IOC), automatiser des tâches via des scripts et produire des rapports d'incident exploitables.

Vous serez en mesure de conduire des investigations complètes, d'automatiser des actions répétitives et de préparer la réussite de l'examen SAL1. La formation inclut un examen blanc intégral corrigé afin de vous mettre dans les conditions réelles de certification.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version du contenu officiel TryHackMe et privilégie une approche résolument pratique et opérationnelle.

Objectifs

- Comprendre le rôle et les missions d'un Analyste SOC niveau 1
- Maîtriser l'usage d'un SIEM pour trier et enrichir des alertes
- Détecter des menaces grâce à la Threat Intelligence et aux IOC
- Conduire la réponse aux incidents et rédiger des rapports clairs
- Se préparer efficacement à l'examen SAL1 via un examen blanc

Public visé

- Analystes SOC juniors
- Techniciens sécurité
- Équipes IT/OPS

Pré-requis

- Connaissances de base en réseau et systèmes
- Notions d’exploitation de logs

Programme de formation TryHackMe SAL1

[Jour 1 - Matin]

Fondamentaux SOC et contexte

- Rôle d’un Analyste SOC : missions, périmètre et interactions
- Cycle d’un incident : détection, triage, escalade, remédiation
- Panorama des outils SOC : SIEM, EDR, NDR, ticketing
- Rappels réseau essentiels
- Atelier pratique : Prise en main de l’environnement et triage d’alertes simples.

[Jour 1 - Après-midi]

Collecte et normalisation des logs

- Sources de logs : endpoints, réseau, applications, cloud
- Formats courants : Syslog, CEF, JSON, champs clés
- Normalisation et enrichissement
- Qualité de données : bruit, duplication, priorisation des événements
- Atelier pratique : Ingestion et parsing de jeux de logs dans un SIEM de démo.

Outils et workflow d’investigation

- Recherches dans un SIEM : filtres, corrélations, agrégations
- Pivoting et timeline : IP, utilisateur, hôte, application
- Conservation des preuves et chain of custody
- Méthodologie d’investigation orientée hypothèses
- Atelier pratique : Conduite d’une mini-enquête et production d’un court compte-rendu.

[Jour 2 - Matin]

Détection des menaces et cas d’usage

- Signatures vs détection comportementale (UEBA, règles)
- Use cases : phishing, brute force, exfiltration, mouvements latéraux
- Écriture et tuning de règles (réduction des faux positifs)
- Tableaux de bord et KPI de détection
- Atelier pratique : Créer et tester des règles d’alerte dans le SIEM.

[Jour 2 - Après-midi]

Malware triage et forensic basique

- Analyse statique vs dynamique : principes et limites
- Collecte d’artefacts endpoint (processus, persistance, services)
- Indicateurs d’infection : IOC fichiers, réseau, registre
- Bonnes pratiques de sandbox et sécurité des manipulations
- Atelier pratique : Triage d’un binaire suspect et extraction d’IOC.

Threat Intelligence et enrichissement

- Sources TI (open-source, commerciales) et intégration au SOC
- IOC & TTP : utilisation et limites opérationnelles
- Playbooks d’enrichissement
- Priorisation des menaces et cartographie MITRE ATT&CK
- Atelier pratique : Enrichir une alerte et qualifier la sévérité avec Threat Intelligence.

[Jour 3 - Matin]

Réponse aux incidents et escalade

- Processus d’escalade : critères, canaux, responsabilités
- Containment, eradication, recovery : stratégies et pièges
- Communication opérationnelle et reporting en temps de crise
- Exercices tabletop et rôles RACI
- Atelier pratique : Simulation d’un incident avec phases d’escalade.

[Jour 3 - Après-midi]

Monitoring Cloud et sécurité des journaux

- Spécificités cloud et journaux natifs
- Détections typiques : clés compromises, dérives IAM
- Centralisation et rétention des logs cloud
- Contraintes de conformité et segmentation des environnements
- Atelier pratique : Investigation d’événements cloud anormaux.

Forensics réseau et capture de trafic

- Outils de capture (tcpdump, Wireshark) : filtres et lecture
- Reconstruction de flux et inspection HTTP/DNS/TLS
- Détection d’exfiltration et canaux non standard
- Mise en relation du trafic réseau avec les journaux applicatifs
- Atelier pratique : Analyse d’une trace pcap et extraction d’IOC.

[Jour 4 - Matin]

Automatisation et orchestration

- Concepts SOAR : playbooks, jobs, actions automatisées
- Cas d’usage : enrichissements, blocages, quarantaines
- Chaîne SIEM - SOAR - ITSM et traçabilité
- Mesure d’efficacité : MTTR, faux positifs, couverture
- Atelier pratique : Créer un playbook d’automatisation simple.

[Jour 4 - Après-midi]

Langages et scripts utiles pour l’analyste

- Scripts Python/PowerShell pour triage et extraction
- Automatisation d’enrichissements via API
- Bonnes pratiques de scripting sécurisé
- Gestion des erreurs et rollback
- Atelier pratique : Écrire un script d’enrichissement d’alertes.

Gestion des vulnérabilités et corrélation

- Vulnérabilité vs incident : complémentarités SOC
- Intégration des scans vuln dans le SIEM
- Corrélation vulnérabilité - événements et priorisation risque
- Stratégies de remédiation et communication
- Atelier pratique : Croiser un scan et des alertes pour prioriser.

[Jour 5 - Matin]

Reporting et amélioration continue

- Rédiger un rapport lisible pour technique et métier
- KPI SOC : SLI/SLO, MTTR, taux de faux positifs
- Post-mortem et retour d’expérience
- Construire un catalogue de playbooks et runbooks
- Atelier pratique : Produire un rapport post-incident complet.

[Jour 5 - Après-midi]

Mise en production des compétences

- Du labo au poste : checklist d’intégration en SOC
- Continuité opérationnelle, documentation et handover
- Outillage open-source et parcours de certification complémentaires
- Plan de progression pour un Junior SOC
- Atelier pratique : Bâtir un plan d’intégration et de montée en compétences.

Préparation à l’examen SAL1

- Structure et attentes de l’examen SAL1
- Stratégies de gestion du temps et de priorisation
- Check-list de révision : SIEM, logs, IOC, TTP, cloud, scripts
- Bonnes pratiques de rédaction et qualité des livrables
- Atelier pratique : Passage de l’examen blanc + correction

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.