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

Mis à jour le 13/05/2025

S'inscrire

Formation certification Blue Team Level 1

All-In-One : Préparation & Examen inclus au tarif

2 jours (14 heures)

Présentation

Notre formation Certification Blue Team 1 vous permettra de valider vos compétences pratiques et techniques en sécurité défensive et de faire votre entrée dans le monde de la cybersécurité. La Blue Team Level 1 (BTL1) est la certification « junior » 100 % pratique délivrée par l'organisme britannique Security Blue Team.

Notre programme de formation cible les profils disposant de 0 à 2 ans d'expérience qui veulent démontrer leurs compétences défensives en environnement SOC de niveau 1.

À l'issue de cette formation, vous saurez identifier, exploiter et documenter les vulnérabilités et proposer des solutions pour renforcer et d'optimiser la sécurité informatique d'une organisation.

Objectifs

- Maîtriser les 5 grands domaines défensifs évalués par BTL1 (phishing, TI, DFIR, SIEM, IR)
- Savoir produire des rapports clairs et exploitables pour les équipes de sécurité
- Pouvoir passer l'examen BTL1

Public visé

- Analystes SOC junior ou aspirants
- Toute personne souhaitant fair ses premiers pas en cybersécurité

Pré-requis

- Il n'y a aucun prérequis nécessaire pour suivre la formation qui vous préparera au passage de l'examen

Programme de notre Formation Certification Blue Team Level 1

Fondamentaux & Vie d’un SOC

- Rôles blue-team : analyste N1 / N2, threat intel junior, forensique débutant
- Modèles OSI, devices réseau & segmentation de base
- Sécurité poste / serveur : durcissement, anti-malware, journalisation
- Soft-skills SOC : gestion du stress, priorisation alertes
- Présentation du parcours BTL1 : 330 leçons, 23 labs, 4 mois d’accès

Phishing Analysis & Email Threats

- Typologies d’attaque : BEC, drive-by, vishing, credential-harvesting
- Collecte d’artefacts : en-têtes, pièces jointes, sandboxes web
- Outils IOC : VirusTotal, URLscan, CyberChef, PhishTool
- Contremesures : SPF, DKIM, DMARC & playbooks de réponse
- Rédaction d’un rapport d’incident phishing conforme BTL1

Digital Forensics & Threat Intelligence

- Artefacts Windows : EVTX, Registry, JumpLists, $MFT
- Analyse mémoire & disque : Volatility, Autopsy, FTK
- PCAP & détection C2 : Wireshark, Suricata rules
- Modèles de veille : stratégique, opérationnelle, tactique
- Plateformes MISP / OpenCTI : ingestion, enrichissement, diffusion IoC

SIEM, Détection & Monitoring

- Splunk : requêtes stats, transaction, tableaux de bord SOC
- ELK & Sigma : corrélation cross-log, déploiement de règles
- Construction d’alertes ATT&CK (ex. T1059 PowerShell)
- KPIs SOC : MTTR, MTTD, faux positifs, coverage MITRE
- Automatisation basique : scripts Python & playbooks SOAR starter

Attaques Windows & Active Directory

- Introduction à Active Directory
- Kerberoasting, DCSync, Pass-the-Ticket
- Création de règles de détection personnalisées
- Analyse de scripts PowerShell malveillants

Incident Response

- Workflow NIST : préparation ? containment ? eradication ? recovery
- Simulation “24 h exam” : gestion du temps, evidence locker, sauvegarde notes
- Stratégies open-book : structure de notes, bookmarks, checklist navigateur
- Analyse post-mortem & retake planning
- Perspectives post-BTL1 : BTL2, CySA+, GCIA, eJPT Blue

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.