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

Mis à jour le 02/09/2026

S'inscrire

# Formation Certification Blue Team Level 2

## Présentation

La Formation Certification Blue Team Level 2 prépare les professionnels de la cybersécurité à la certification officielle Blue Team Level 2 (BTL2), un examen pratique centré sur l'investigation avancée, la détection et la réponse aux incidents.

La certification Blue Team Level 2 (BTL2) valide des compétences opérationnelles attendues dans un centre de supervision de sécurité. Son parcours couvre l'analyse de malwares, le threat hunting, l'exploitation avancée d'un SIEM et la gestion des vulnérabilités dans des scénarios proches des situations rencontrées en entreprise.

Notre formation vous permettra de structurer votre préparation à l'examen, de consolider votre méthode d'investigation et de mobiliser les outils adaptés pour collecter, corréler et qualifier les preuves techniques. Vous apprendrez à transformer des journaux, artefacts et indicateurs en conclusions exploitables par les équipes de sécurité.

Vous développerez une approche rigoureuse de l'analyse statique et dynamique, de la recherche de comportements suspects et de la cartographie des techniques adverses. Les mises en situation vous aideront à prioriser les actions, à documenter vos constats et à produire un rapport d'incident clair et défendable.

À l'issue de la formation, vous serez en mesure d'aborder l'examen Blue Team Level 2 (BTL2) avec une méthode fiable, tout en renforçant vos capacités d'analyste SOC de niveau intermédiaire. La préparation associe révision des domaines évalués, exercices pratiques et entraînement à la restitution professionnelle des résultats.

## Objectifs

- Comprendre le périmètre de compétences évalué par la certification Blue Team Level 2 (BTL2).
- Analyser des fichiers suspects par des techniques d'analyse statique et dynamique.

- Conduire des investigations de threat hunting à partir de journaux et d'indicateurs de compromission.
- Exploiter un SIEM pour rechercher, corréler et qualifier une activité malveillante.
- Évaluer des vulnérabilités et prioriser les mesures de réduction du risque.
- Produire un rapport d'investigation structuré, exploitable et adapté au contexte de l'examen.

## Public visé

- Analyste SOC
- Analyste cybersécurité
- Analyste réponse à incident
- Threat Hunter
- Consultant cybersécurité

## Pré-requis

- Expérience pratique de l'investigation d'incidents de sécurité.
- Connaissances opérationnelles de Windows et de ses principaux artefacts système.
- Maîtrise des fondamentaux des réseaux TCP/IP, des journaux et des protocoles courants.
- Capacité à interpréter des événements dans un SIEM et à manipuler des indicateurs de compromission.
- Connaissances de base en analyse de malwares et en gestion des vulnérabilités.

## Pré-requis techniques

- Poste de travail sous Windows 10 ou Windows 11, avec droits d'installation des outils nécessaires.
- Configuration recommandée : processeur 4 cœurs, 16 Go de RAM et 50 Go d'espace disque disponible.
- Solution de virtualisation installée, telle que VMware Workstation ou VirtualBox, capable d'exécuter une machine virtuelle.
- Navigateur récent, tel que Google Chrome, Microsoft Edge ou Mozilla Firefox.
- Connexion Internet stable, sans filtrage bloquant les laboratoires, téléchargements d'outils ou services d'analyse.

## Programme de notre formation Blue Team Level 2

### [Jour 1 - Matin]

#### Cadre de certification et méthodologie SOC

- Positionnement de la certification Blue Team Level 2 (BTL2) et compétences évaluées.
- Organisation des quatre domaines : malware analysis, threat hunting, advanced SIEM et vulnerability management.
- Déroulement d une investigation, de la qualification initiale à la restitution des résultats.

- Priorisation des alertes, gestion des preuves et construction d une chronologie d incident.
- Lecture d un scénario de compromission et identification des livrables attendus pour l examen.

[Jour 1 - Après-midi]

## Fondamentaux de l investigation avancée

- Collecte et qualification des indicateurs de compromission : hachages, domaines, adresses IP et artefacts hôtes.
- Analyse des événements Windows, des processus, des services et des mécanismes de persistance.
- Exploitation des journaux réseau et des traces DNS, HTTP et authentification.
- Structuration d hypothèses d investigation et validation par recoupement des sources de télémétrie.
- Atelier pratique : analyser un jeu de journaux hôte et réseau afin d établir une première chronologie de compromission.

[Jour 2 - Matin]

## Analyse statique de malwares

- Cadre de sécurité pour manipuler un fichier suspect dans un environnement isolé.
- Identification du type de fichier, de son empreinte, de sa structure et de ses métadonnées.
- Recherche de chaînes, d imports, de ressources et d artefacts utiles à la qualification.
- Extraction d indicateurs et détection de techniques d obfuscation ou de contournement.
- Création et validation de règles YARA pour caractériser une famille de malwares.

[Jour 2 - Après-midi]

## Analyse dynamique et comportements malveillants

- Préparation d une machine virtuelle de détonation et principes de confinement.
- Observation des processus, fichiers, clés de registre, tâches planifiées et connexions réseau.
- Analyse des communications de commande et contrôle et identification des comportements anormaux.
- Mise en relation des actions observées avec les tactiques et techniques MITRE ATT&CK.
- Atelier pratique : réaliser l analyse statique et dynamique d un échantillon contrôlé, puis produire les indicateurs et comportements observés.

[Jour 3 - Matin]

## Threat hunting fondé sur les hypothèses

- Principes du threat hunting et différence entre détection réactive et recherche proactive.
- Construction d hypothèses à partir du renseignement sur les menaces et des techniques adverses.
- Sélection des sources de données : endpoints, identité, réseau, messagerie et cloud.
- Recherche de signaux faibles, anomalies comportementales et pivots entre événements.
- Qualification des résultats, réduction des faux positifs et préparation des actions de réponse.

[Jour 3 - Après-midi]

## Investigation et détection dans le SIEM

- Recherche avancée dans un SIEM : filtres, agrégations, jointures et corrélations.
- Analyse des authentifications, élévations de privilèges, mouvements latéraux et exfiltrations.
- Conception de requêtes de détection alignées sur une hypothèse de compromission.
- Documentation des résultats et enrichissement des alertes avec le contexte utile aux analystes.
- Atelier pratique : mener une chasse aux menaces dans un SIEM à partir d une hypothèse liée à un mouvement latéral.

[Jour 4 - Matin]

## Détection avancée et amélioration continue

- Cycle de vie d une règle de détection : besoin, données, logique, tests et mise en production.
- Écriture et adaptation de règles Sigma pour normaliser les détections.
- Évaluation de la couverture de détection au regard de MITRE ATT&CK.
- Réduction du bruit, réglage des seuils et critères de priorisation des alertes.
- Mesure de l efficacité opérationnelle : qualité des données, couverture et délais de traitement.

[Jour 4 - Après-midi]

## Gestion des vulnérabilités orientée risque

- Cycle de gestion des vulnérabilités : découverte, évaluation, priorisation, correction et contrôle.
- Interprétation des résultats de scan et mise en contexte des scores CVSS.
- Prise en compte de l exposition, de l exploitabilité, des actifs critiques et des menaces actives.
- Construction d un plan de remédiation et suivi des exceptions de sécurité.
- Atelier pratique : prioriser un ensemble de vulnérabilités à partir des risques métier et rédiger un plan de remédiation.

[Jour 5 - Matin]

## Restitution et rapport d incident

- Structure d un rapport d investigation adapté aux attentes de la certification.
- Formalisation du périmètre, des sources examinées, de la chronologie et des preuves collectées.

- Présentation des indicateurs, techniques adverses, impacts potentiels et niveaux de confiance.
- Formulation de recommandations de confinement, d éradication, de remédiation et de détection.
- Relecture critique : précision technique, traçabilité des constats et clarté pour les décideurs.

[Jour 5 - Après-midi]

### Simulation de préparation à l examen

- Récapitulatif des domaines et des compétences clés de Blue Team Level 2 (BTL2).
- Stratégie de gestion du temps pour une investigation pratique étendue.
- Choix des outils, journalisation des actions et conservation des éléments de preuve.
- Autoévaluation des lacunes et plan de préparation individuel avant le passage de l examen.
- Atelier pratique : traiter un scénario de compromission de bout en bout, analyser les preuves et restituer un rapport synthétique de type examen.

## 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.