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

Mis à jour le 23/06/2025

S'inscrire

Formation StrangeBee : TheHive

3 jours (21 heures)

Présentation

Maîtrisez TheHive pour structurer, automatiser et optimiser votre gestion des incidents de sécurité. Cette formation vous accompagne pas à pas dans la mise en œuvre d'un SOC moderne, en exploitant pleinement la puissance de TheHive.

Vous apprendrez à installer, configurer et sécuriser TheHive, à créer des alertes et des cas, à coordonner les actions de réponse avec Cortex, et à automatiser l'enrichissement et la remédiation des incidents via des analyseurs et des répondeurs personnalisés.

Vous saurez intégrer les sources de renseignement, cartographier les menaces selon MITRE ATT&CK, produire des rapports exploitables et piloter l'activité du SOC grâce à des tableaux de bord et indicateurs avancés.

Vous serez également formé à la sécurisation des accès, à la conformité, à la gouvernance des données sensibles et à la mise à l'échelle dans un environnement cloud, multi-tenant ou hybride.

Comme pour toutes nos formations, elle se déroulera sur ma toute dernière version de l'outil TheHive

Objectifs

- Comprendre l'architecture technique de TheHive, Cortex et MISP pour construire une plateforme intégrée de gestion des incidents de sécurité
- Installer, configurer et sécuriser une instance TheHive on-premise ou cloud, en appliquant les bonnes pratiques d'administration et de conformité
- Créer, enrichir et automatiser les cas d'incident à l'aide des alertes, des tâches, des observables et des modules Cortex
- Intégrer les sources de renseignement pour renforcer l'analyse, la corrélation et la réponse aux menaces

- Superviser l’activité du SOC via des tableaux de bord, des KPIs personnalisés et des exports de rapports en Markdown ou HTML
- Déployer TheHive dans une architecture scalable, et orchestrer sa maintenance avec des outils DevOps et des API REST

Public visé

- Analystes SOC
- **Analystes Cybersécurité**
- Ingénieur en sécurité
- Administrateur Réseau

Pré-requis

- Connaissances de base sur les APIs REST
- Maîtrise des environnements Linux et des lignes de commande

Programme de la formation TheHive

Introduction à TheHive et son écosystème

- Architecture modulaire
- Modèle open source et offres commerciales
- Cortex : moteur d’analyse automatisée
- MISP : plateforme de renseignement sur les menaces
- Intégration MITRE ATT&CK, SIEM, outils EDR

Installation et Configuration Initiale

- Environnement système (Linux, Docker, PostgreSQL, Java)
- Réseau, dépendances, sécurité
- Méthodes : Docker Compose vs installation manuelle
- Configuration initiale (fichiers application.conf)
- Sécurisation de base (HTTPS, reverse proxy, comptes)
- Interface admin (UI/CLI/API)
- Création des utilisateurs et gestion des rôles
- Sauvegardes, logs, supervision

Gestion des alertes

- Sources : SIEM, CTI, MISP, API, emails

- Parsing et templates d’alerte
- Fusion et corrélation automatique

Cases

- Création manuelle et automatique de cas
- Structure : tâches, observables, logs
- Priorisation, tags, TLP, PAP, status

Collaboration

- Travail en équipe sur un cas
- Notifications internes
- Dashboards en temps réel

Cortex et automatisation de la réponse

- Rôle de Cortex dans l’enrichissement
- Analyseurs vs Responders
- Architecture et API
- Configuration d’un analyseur (Docker, API keys)
- Enchaînement automatique d’analyses
- Automatiser les actions correctives
- Bonnes pratiques d’orchestration

Exploitation avancée & bonnes pratiques SOC

- Playbooks de classification
- Analyse contextuelle automatisée
- Scénarios d’incidents types
- Mapping des observables aux TTPs
- Recherches et visualisation des techniques
- Détection et tracking de campagnes
- Suivi des cas : durée de traitement, statut, types
- Export CSV, API, reporting Markdown/HTML
- Intégration avec Grafana, Elastic…

Sécurité, audit et conformité

- RBAC (rôles, profils personnalisés)
- SSO (SAML, OIDC), MFA
- Logs d’audit
- Gestion du chiffrement
- Restrictions réseau, IP whitelisting
- Sécurité applicative (CSP, sécurité API)
- ISO 27001, SOC 2, RGPD

- Confidentialité (TLP 2.0), accès aux logs
- Retention et anonymisation

Personnalisation et intégrations

- Modèles d’alertes, de cas, de tâches
- Utilisation des macros et champs dynamiques
- Génération de rapports automatisés
- SIEM : Splunk, QRadar, Sentinel, ELK
- EDR : Crowdstrike, SentinelOne, XDR
- CTI : MISP, Anomali, ThreatConnect
- Utilisation de l’API REST pour automatisation
- Scripts Python (Hive4py)
- Webhooks et connecteurs personnalisés

Déploiement Cloud & montée en charge

- Présentation de l’offre SaaS de StrangeBee
- Avantages : haute dispo, maintenance, certif SOC2
- Accès via portail StrangeBee
- Monosite vs multisite
- Multi-tenant pour MSSP
- Load balancing, cluster, PostgreSQL HA
- Logs et métriques
- Intégration Prometheus/Grafana
- Alerting et gestion de la scalabilité

Labs pratiques

- Mise en place d’un cas d’incident complet
- Création d’alertes, enrichissement, réponse automatisée
- Collaboration en équipe simulée

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.