Formation StrangeBee : TheHive

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	SBTH
Durée	3 jours (21h)
Tarif	2 190 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

- du 8 au 10 décembre 2025
- du 2 au 4 février 2026
- du 30 mars au 1er avril 2026
- du 8 au 10 juin 2026
- du 3 au 5 août 2026
- du 28 au 30 septembre 2026
- du 23 au 25 novembre 2026

PARIS

- du 8 au 10 décembre 2025
- du 2 au 4 février 2026
- du 30 mars au 1er avril 2026
- du 8 au 10 juin 2026
- du 3 au 5 août 2026
- du 28 au 30 septembre 2026
- du 23 au 25 novembre 2026

VOIR TOUTES LES DATES

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

| Analystes SOC
| Analystes Cybersécurité
| Ingénieur en sécurité
| Administrateur Réseau

Prérequis

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

Programme de la formation

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

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.