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

Updated on 27/06/2025

Sign up

StrangeBee Training : TheHive

3 days (21 hours)

Presentation

Master TheHive to structure, automate and optimize your security incident management. This step-by-step course guides you through the implementation of a modern SOC, taking full advantage of the power of TheHive.

You'll learn how to install, configure and secure TheHive, create alerts and cases, coordinate response actions with Cortex, and automate incident enrichment and remediation via custom analyzers and responders.

You'll be able to integrate intelligence sources, map threats according to MITRE ATT&CK, produce usable reports and manage SOC activity using advanced dashboards and indicators.

You will also be trained in securing access, compliance, governance of sensitive data and scaling in a cloud, multi-tenant or hybrid environment.

As with all our training courses, it will be run on my latest version of TheHive.

Objectives

- Understand the technical architecture of TheHive, Cortex and MISP to build an integrated security incident management platform.
- Install, configure and secure an on-premise or cloud TheHive instance, applying good administration and compliance best practices
- Create, enrich and automate incident cases using alerts, tasks, observables and Cortex modules
- Integrate intelligence sources to strengthen analysis, correlation and response to threats

- Monitor SOC activity via dashboards, custom KPIs and Markdown or HTML report exports
- Deploy TheHive in a scalable architecture, and orchestrate its maintenance with DevOps tools and REST APIs

Target audience

- SOC analysts
- **Cybersecurity analysts**
- Security engineers
- Network administrators

Prerequisites

- Basic knowledge of REST APIs
- Knowledge of Linux environments and command lines

TheHive training program

Introduction to TheHive and its ecosystem

- Modular architecture
- Open source model and commercial offerings
- Cortex: automated analysis engine
- MISP: threat intelligence platform
- MITRE ATT&CK integration, SIEM, EDR tools

Installation and Initial Configuration

- System environment (Linux, Docker, PostgreSQL, Java)
- Network, dependencies, security
- Methods: Docker Compose vs. manual installation
- Initial configuration (application.conf files)
- Basic security (HTTPS, reverse proxy, accounts)
- Admin interface (UI/CLI/API)
- User creation and role management
- Backups, logs, supervision

Alert management

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

- Alert parsing and templates
- Automatic merging and correlation

Cases

- Manual and automatic case creation
- Structure: tasks, observables, logs
- Prioritization, tags, TLP, PAP, status

Collaboration

- Teamwork on a case
- Internal notifications
- Real-time dashboards

Cortex and response automation

- Cortex's role in enrichment
- Analyzers vs. Responders
- Architecture and APIs
- Analyzer configuration (Docker, API keys)
- Automatic chaining of analyses
- Automating corrective actions
- Orchestration best practices

Advanced exploitation & SOC best practices

- Classification playbooks
- Automated contextual analysis
- Typical incident scenarios
- Mapping observables to TTPs
- Search and visualization of techniques
- Campaign detection and tracking
- Case tracking: processing time, status, types
- CSV export, API, Markdown/HTML reporting
- Integration with Grafana, Elastic...

Security, audit and compliance

- RBAC (roles, personalized profiles)
- SSO (SAML, OIDC), MFA
- Audit logs
- Encryption management
- Network restrictions, IP whitelisting
- Application security (CSP, API security)
- ISO 27001, SOC 2, RGPD

- Confidentiality (TLP 2.0), access to logs
- Retention and anonymization

Customization and integration

- Alert, case and task templates
- Use of macros and dynamic fields
- Automated report generation
- SIEM: Splunk, QRadar, Sentinel, ELK
- EDR: Crowdstrike, SentinelOne, XDR
- CTI: MISP, Anomali, ThreatConnect
- Use of REST API for automation
- Python scripting (Hive4py)
- Webhooks and custom connectors

Cloud deployment & scalability

- Presentation of StrangeBee's SaaS offering
- Benefits: high availability, maintenance, SOC2 certification
- Access via StrangeBee portal
- Monosite vs multisite
- Multi-tenant for MSSP
- Load balancing, clustering, PostgreSQL HA
- Logs and metrics
- Prometheus/Grafana integration
- Alerting and scalability management

Hands-on labs

- Setting up a complete incident case study
- Alert creation, enrichment, automated response
- Simulated team collaboration

Companies involved

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the format selected. This

questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check that skills have been correctly acquired.

Certification

A certificate will be awarded to each trainee who completes the training course.