TheHive Project

# ****TheHive Project – Notes****

### **Task 1: Room Outline**

* TheHive is an **open-source Security Incident Response Platform (SIRP)**.
* Purpose: streamline **Incident Response (IR)**, **DFIR**, and **SOC operations**.
* Integrated with: Cortex (for automated analysis) and MISP (for threat intel sharing).
* Supports collaboration between SOC analysts, IR teams, and threat hunters.

### **Task 2: Introduction**

* Developed by **TheHive Project** (community-driven, open-source).
* Designed to help security teams manage and respond to incidents efficiently.
* Provides:
  + **Case management** (track investigations).
  + **Collaboration tools** (multiple analysts working on same case).
  + **Automation & enrichment** (via Cortex analyzers).
* API-driven → can integrate with SIEMs, SOAR, threat intel feeds.

### **Task 3: TheHive Features & Integrations**

**Core Features:**

* **Cases & Tasks** → central unit of work (incidents, investigations).
* **Observables** → artifacts (IPs, hashes, domains, files, etc.) tied to a case.
* **Collaboration** → analysts can assign tasks, add comments, and track progress.
* **Search & Correlation** → link related cases and observables.
* **Dashboards & Metrics** → overview of active cases, response time, workload.

**Key Integrations:**

* **Cortex** → runs analyzers on observables (VirusTotal, WHOIS, sandboxing, etc.).
* **MISP (Malware Information Sharing Platform)** → import/export IOCs, enrich investigations.
* **SIEM / EDR tools** → forward alerts directly into TheHive for case creation.

### **Task 4: User Profiles & Permissions**

* Role-based access control (RBAC) ensures proper separation of duties.
* **User Profiles:**
  + **Admin** → manage users, org settings, integrations.
  + **Analyst** → create and investigate cases, run analyzers.
  + **Read-only** → view cases/observables, but cannot modify.
* Permissions can be customized per organization.

### **Task 5: Analyst Interface Navigation**

* **Dashboard/Home** → overview of cases, metrics, activity feed.
* **Cases Tab** → list of active/closed investigations.
* **Case View** →
  + Details (title, description, severity).
  + Tasks (step-by-step investigation actions).
  + Observables (IP, domain, hash, file).
  + Comments/Collaboration section.
* **Alerts** → incoming events/IOC feeds from SIEM, IDS, etc.
* **Search** → filter by case, task, observable, tag.
* **Integration Panel** → trigger Cortex analyzers or MISP queries from observables.

### **Task 6: Room Conclusion**

* TheHive is a **centralized, collaborative incident response platform**.
* Strength lies in **automation**, **integration with Cortex & MISP**, and **analyst collaboration**.
* Helps reduce **MTTD** (Mean Time to Detect) and **MTTR** (Mean Time to Respond).
* Widely used in SOCs, CERTs, and DFIR teams.

