Tema 6 Managementul riscurilor

Planul de răspuns la incidente pentru **SecureHealth Systems Inc.** integrează platforma **TheHive** pentru a optimiza gestionarea incidentelor de securitate, asigurând conformitate cu HIPAA și eficiență operațională. Iată adaptarea pe etape:

**1. Echipa de Răspuns la Incidente (IRT) în TheHive**

**Structura și colaborare:**

* Acces centralizat în TheHive pentru toți membrii IRT, cu roluri definite (Coordonator, Expert Securitate, Legal, Comunicare).
* **Notificări în timp real** prin sistemul de alertă integrat, cu asignare automată de task-uri în funcție de competențe .

**2. Pregătire și Configurare**

**Politici în TheHive:**

* Crearea de **template-uri standardizate** pentru tipuri comune de incidente (ex: breșă de date, ransomware).
* Integrare cu **MISP** pentru sincronizare automată a indicatorilor de compromitere (IOCs) și evenimente .

**Instrumente automate:**

* **Cortex** pentru analize automate de observabile (ex: verificare hash în VirusTotal, geolocalizare IP).
* Conectare la SIEM (Splunk) pentru import alertă direct în TheHive ca caz nou .

**3. Identificare și Analiză**

**Detectare și triaj:**

* Alertă din TheHive la primirea evenimentelor din MISP sau SIEM.
* Clasificare automată a severității folosind reguli predefinite (ex: număr de sisteme afectate, tip de date expuse) .

**Analiză colaborativă:**

* Adăugare observabile (IP-uri, fișiere suspecte) în cazul creat, cu analiză paralelă prin Cortex.
* Marcarea IOCs relevanți pentru export în MISP sau blocare în firewall .

**4. Limitare și Eliminare**

**Automatizări prin TheHive:**

* Executare **playbook-uri** predefinite pentru izolarea sistemelor (ex: deconectare server via API).
* Trimitere automată de comenzi către CrowdStrike pentru ștergere malware .

**Documentare în timp real:**

* Înregistrarea tuturor acțiunilor în jurnalul cazului, cu atașare dovezi (screenshot-uri, log-uri) .

**5. Recuperare și Raportare**

**Restabilire automatizată:**

* Generare raport de restaurare din backup cu verificare integritate prin Cortex.
* Monitorizare continuă a sistemelor recuperate timp de 72h prin integrare cu Nessus .

**Raportare conformă:**

* Export raport final în format HIPAA direct din TheHive pentru trimitere către **Oficiului pentru Drepturile Civile (OCR)**
* Arhivare caz în baza de date centrală cu tag-uri pentru audit viitor .

**6. Îmbunătățiri Post-Incident**

**Root Cause Analysis:**

* Identificare lacune folosind **metrica timpului de răspuns** din dashboard-ul TheHive.
* Actualizare template-uri de cazuri pe baza lecțiilor învățate .

**Simulări și training:**

* Creare scenarii de atac în TheHive pentru exersarea procedurilor.
* Tracking al performanței echipei prin rapoarte de progres .

**Exemplu practic de utilizare TheHive în ransomware:**

1. **Alertă automată**: TheHive primește notificare de la SIEM despre criptare masivă.
2. **Caz creat automat**: Template-ul "Ransomware" activează task-uri predefinite (izolare, analiză).
3. **Analiză Cortex**: Fișierul ransomware este trimis la Sandbox prin integrare directă.
4. **Playbook executat**: Serverul afectat este deconectat prin integrare cu API-ul VMware.
5. **Raport final**: Documentarea întregului proces este exportată ca PDF pentru audit .