SOAR Playbook - Auto-Block Phishing IP

SOAR Playbook: Phishing Auto-Block

Trigger: Wazuh phishing alert

Step 1: Pull alert metadata

Step 2: Query IP/domain reputation (OTX/VirusTotal)

Step 3: If malicious, block via CrowdSec and add firewall rule

Step 4: Create TheHive case and attach IOCs

Step 5: Notify stakeholders and log actions