Advanced SOAR Automation

SOAR Components: Orchestration (connectors to tools), Automation (scripts/playbooks), Response (containment actions).

Playbook design principles: idempotent steps, clear decision trees, logging & retry, safe default actions.

Sample Playbook: Auto-block phishing IP: 1) On Wazuh alert, query IP reputation (OTX/VirusTotal). 2) If reputation == malicious, call CrowdSec API to block IP. 3) Create TheHive case and attach IOCs. 4) Notify Slack/email and close automated task.

Pseudo-playbook representation: (IF alert.type == 'phishing') -> check_reputation(ip) -> if malicious: block_ip(ip) -> create_case(iocs) -> notify().

Testing & Validation: Run simulated alerts and assert the playbook performed expected actions (IP blocked, case created).