Playbook Summary

The Phishing IP Auto-Block Playbook is a robust, automated incident response solution built within **Splunk Phantom**. Its primary function is to rapidly detect and neutralize phishing threats. The playbook initiates by automatically fetching the suspicious IP address from incoming alerts (e.g., from Wazuh) and then performing an immediate reputation check against threat intelligence sources. If the IP is confirmed as malicious, the playbook seamlessly integrates with **CrowdSec** to deploy an immediate block, preventing further communication from the malicious entity (e.g., 192.168.1.102). Concurrently, to ensure comprehensive incident tracking and analyst engagement, a detailed incident ticket is automatically generated and pushed to **TheHive**, summarizing the actions taken and flagging the case for human review. This end-to-end automation significantly reduces the mean time to respond (MTTR) to phishing incidents, enhancing overall security posture.