CYART

inquiry@cyart.io

www.cyart.io

Phishing Response Playbook Summary

This simplified playbook demonstrates manual phishing alert response using TheHive and CrowdSec. The suspicious IP 192.168.1.102 was first verified through external threat intelligence sources such as VirusTotal and OTX. Upon confirmation, the IP was manually blocked via CrowdSec to prevent further malicious activity. This workflow showcases end-to-end incident handling without automated SOAR tools.

Playbook Step	Status	Notes
Check IP	Success	IP 192.168.1.102 verified as malicious via VirusTotal/OTX
Block IP	Success	IP 192.168.1.102 manually blocked using CrowdSec (cscli ban)