Title: Escalation to Tier-2

Summary:

On 18 September 2025 at 14:00 UTC, Wazuh generated a high-priority alert for a Samba usermap_script exploit against host 192.168.1.100. Source IP 192.168.1.101 established a reverse Meterpreter session to 192.168.1.50:4444 and created /tmp/pwned.txt. Immediate containment: isolated VM and applied CrowdSec/iptables block on 192.168.1.101. Collected artifacts: Wazuh alert JSON, Metasploit session logs, attack.pcap, and /tmp/pwned.txt with recorded MD5/SHA256 hashes. Request Tier-2: perform full disk and memory imaging of 192.168.1.100, detailed timeline and root-cause analysis, and review network captures for potential lateral movement. Preserve chain-of-custody for all artifacts and contact SOC on-call for coordination and evidence transfer immediately upon request by leadership.