Escalation to Tier 2

On 2025-08-18 at 14:00 UTC, Wazuh detected suspicious activity targeting the Samba service on the Metasploitable2 host, originating from source IP 192.168.159.138. At 14:01 UTC, the alert was classified as high severity and mapped to MITRE ATT&CK technique T1210 (Exploitation of Remote Services). SOC analysis confirmed abnormal Samba behavior consistent with the usermap_script vulnerability. At 14:10 UTC, containment actions were initiated by isolating the affected virtual machine and blocking the attacker IP using CrowdSec. No persistence, lateral movement, or data exfiltration was observed. The incident was escalated to Tier 2 at 14:15 UTC for further review and validation.