Escalation Case Summary

At 13:15 on 2025-08-18, Tier 1 escalated a High-priority case to Tier 2 following automated detection of suspicious Samba activity and confirmed phishing indicators. The escalation included IOCs (192.168.1.102, attacker-domain.example) and a short triage summary: abnormal privilege assignments and network exfil pattern. Tier 2 initiated deep-dive analysis, isolated the VM, and coordinated IP blocking. Outcome: attack contained in lab environment; case assigned remediation tasks and scheduled a lessons-learned review.