Title: Escalation Email – High Priority Incident

Date: 25 Nov 2025
Prepared by: Mayuri Sawle

To:
Tier 2 Security Operations Team
From: SOC Tier1 analyst
Subject: URGENT: High Priority Incident (INC-004) – SMB Brute-Force – Containment Confirmed

Hello Tier 2 Team,
We have a confirmed high-priority brute-force attack classified under MITRE ATT&CK T1110 targeting our Windows 10 VM at 192.168.1.129. CrowdSec detected hundreds of failed SMB login attempts on port 445, and the Firewall Bouncer automatically banned the attacker’s IP. Containment is verified through a failed ping test. Although the threat is contained, the risk remains high until full eradication is complete. Please review Windows Event Logs for authentication failures and recommend policy hardening steps, including account lockout thresholds and SMB exposure reduction.
Regards,
SOC Tier 1 Analyst