Escalation Email – High Priority Incident

File Name: 1.4_Escalation_Role_Play_Email.pdf
Created by: Abhishek Tiwary – SOC Analyst (Tier 1)

A. Email Details

Field	Value
To:	Tier 2 Security Operations Team
From:	SOC Analyst (Abhishek Tiwary)
Subject:	URGENT: High Priority Incident (INC-004) – SMB Brute-Force – CONTAINMENT CONFIRMED

B. Email Body (Approx. 100 words)

Subject: URGENT: High Priority Incident (INC-004) – SMB Brute-Force – CONTAINMENT CONFIRMED

Hi Tier 2 Team,

We have an active, high-priority brute-force attack (MITRE ATT&CK ID: T1110) targeting our Windows 10 VM (Victim IP: 10.178.124.51).

The CrowdSec agent detected repeated failed login attempts on Port 445. The attacker's IP was instantly banned by the Firewall Bouncer. **Containment has been verified successfully via a failed ping test.** The threat is contained, but the risk remains high until eradication is complete.

Please review the Windows Event Logs for failed login attempts and advise on next steps for policy hardening (e.g., account lockout review) to prevent future brute-force attacks.

Thanks,
Abhishek Tiwary
SOC Analyst (Tier 1)