Incident Ticket Draft (High Priority – SMB Brute Force)

A. Ticket Fields

Ticket Field	Value (Based on Capstone Data)	Notes
Incident ID	INC-2025-10-004	Mock ID (2025's 4th incident)
Date/Time	11 Oct 2025, 14:20 IST	Use your actual attack start time
Severity / Priority	HIGH	Active SMB brute-force attack
Status	Contained	Attack stopped due to CrowdSec ban
Assignee	SOC Analyst / Tier 1 (Abhishek Tiwary)	Your role

B. Incident Description

Field	Content
Title	[HIGH] Active Brute-Force Attempt Detected on SMB (Port 445)
Incident Type	Brute Force (MITRE ATT&CK ID: T1110)
Affected Asset	Windows 10 Victim VM (IP Address: 10.178.124.51)
Indicators of Compromise (IOCs)	• Source IP: 10.178.124.51 (Attacker IP) • Protocol: SMB (Port 445) • Event Type: Multiple Failed Login Attempts (Windows Event ID 4625)
Action Taken	The attacker IP was automatically detected by the CrowdSec Agent and instantly banned for 4 hours by the Firewall Bouncer. Containment verified via failed ping test.

C. Verification Section

Action	Status	Proof
Detection Confirmed	YES	CrowdSec scenario successfully triggered.
Containment Applied	YES	Ping test from attacker IP to victim IP failed.

Prepared by: Abhishek Tiwary – SOC Analyst (Tier 1)
Date: 11 Oct 2025