Alert Classification System

Alert ID	Alert Name	Type	Priority	MITRE Technique	MITRE Tactic
INC-004	SMB Brute-Force Attempt on Port 445	Brute-Force Attack	High	**T1110**(Correct)	Credential Access
002	Firewall Ban Triggered	Defensive Action	Medium	N/A	N/A
003	Failed Login Attempts (Windows Event Logs)	Authentication	High	T1110	Credential Access
004	Post-Attack Containment Validation (Ping Fail)	Containment	Info	N/A	N/A

Alert Prioritization Using CVSS

Alert Name	CVSS Score	Severity	Reason
SMB Brute-Force (Port 445)	**8.0**	**High**	Network-based, repeated auth attempts, lateral movement risk
Attacker IP Auto-Banned	4.5	Medium	Mitigated quickly, reduced exposure
Failed Windows Logins	7.5	High	Indicates active unauthorized access attempt
Containment Verified	0.0	Informational	No risk post-isolation

Final Incident Priority: HIGH
Because risk of lateral movement still exists until logs are reviewed and policy hardened.