Triage Simulation Table (Mock SSH Brute-Force Alert)

File Name: 3.1_Triage_Simulation_Table.pdf
Prepared by: Abhishek Tiwary – SOC Analyst (Tier 1)
Date: 11 Oct 2025

A. Triage Simulation Table

Column	Data Entry	Notes
Alert ID	002	Mock Alert ID
Description	Brute-force SSH Attempts	Indicates an attack targeting the SSH service
Source IP	192.168.1.100	Mock attacker IP address
Priority	Medium	SSH brute-force is typically medium unless targeting a critical server
Status	Open / Assigned	Triage has started and the case is assigned for further analysis
MITRE Technique	T1110 (Brute Force)	Classification as per MITRE ATT&CK framework