Alert ID	**Description**	**Source IP**	**Priority**	**Status**
002	Brute-force SSH login attempts	192.168.1.100	Medium	Open

Triage Analysis

The alert indicates multiple failed SSH login attempts from a single external IP address.Such activity is commonly associated with brute-force attacks attempting unauthorized access.The affected system was reachable over SSH, but no successful login was observed.

Threat Intelligence Validation

The source IP address 192.168.1.100 was checked against AlienVault OTXand VirusTotal for known malicious activity. The IP did not showstrong malicious reputation but was associated with previous scanningbehavior. Based on this information, the alert was classified as suspicious but not immediately critical.

Final Triage Decision

The alert was confirmed as a true positive brute-force attempt.Since no successful authentication occurred and impact was limited, the priority was set to Medium. The IP was recommended for monitoring and potential blocking if repeated activity is observed.

Threat intelligence checks revealed no active exploitation linked to the source IP. However, historical scanning activity suggests potential malicious intent. Continuous monitoring and correlation with additional alerts is recommended before escalation.