

STEP 1: Mock Alert Identification

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

STEP 2: Initial Triage Analysis

- Alert indicates multiple failed SSH login attempts.
- Activity occurred within a short time window.
- No successful authentication recorded.
- Source IP **192.168.1.100** is a private internal IP.
- Initial severity assessed as **Medium**.

STEP 3: Triage Notes (Analyst Observation)

- Possible brute-force pattern detected.
- Source is internal, not an external attacker.
- Could be caused by:
 - User password mistakes
 - Misconfigured automation or script
- No immediate impact observed.

STEP 4: Threat Intelligence Validation (Browser-Based)

4.1 VirusTotal Lookup

- Checked IP: **192.168.1.100**
- Result:
Identified as private/internal IP
 - No malware or malicious reputation
 - No detections by security vendors

4.2 AlienVault OTX Lookup

- Checked IP: **192.168.1.100**
- Result:
No threat pulses
 - No IOC associations
 - Not linked to known attacks or campaigns

STEP 5: Threat Intelligence Conclusion

- Internal IPs do not appear in global threat databases.
- No evidence of malicious activity.
- Alert does not match known brute-force campaigns.

STEP 6: 50-Word Threat Intelligence Summary

The IP address 192.168.1.100 was verified using VirusTotal and AlienVault OTX and showed no malicious reputation or associated threat activity. As the address is internal, it is not present in threat intelligence feeds. The brute-force alert is likely a false positive caused by repeated login attempts.