Incident note

Title
Brute force suspected from 203.0.113.45

Time window
2026 02 01, 09 55 to 09 58 UTC

Suspect IP
203.0.113.45

Affected accounts observed
admin, root.

Evidence samples

```
2026 02 01, 09 55 32 Failed password for admin from 203.0.113.45
2026 02 01, 09 56 47 ERROR Possible injection attempt blocked from 203.0.113.45
2026 02 01, 09 57 56 WARN High authentication failure rate detected
```

Enrichment checks performed
VirusTotal for 203.0.113.45 returned no known hits.

Analysis short summary
Multiple failed login attempts from a single IP and concurrent web probes to login pages indicate likely automated credential stuffing or brute force. App warnings support suspicious behaviour but there is no confirmed compromise.

Decision and recommended action
Do not escalate to L2 at present given negative external reputation and no confirmed compromise. Increase monitoring and logging for this IP, set alert to notify on further attempts, block at firewall only if activity increases or new evidence appears.

Follow up
Monitor for 24 hours, escalate to L2 if threshold of 10 failed attempts per 15 minutes is reached

Owner
Jash Vaidya