

Subject: Multiple login failures for the same User | Unknown Severity | Non-Actionable | host\_4

Hi Team,

Multiple login failures for the same User detected from 41.234.160.62 to 105.253.27.136.

Security Alert Details:

SOC Analyst Triage Comments:

- The alert indicates a potentially serious security issue.
- The activity was detected between source IP 41.234.160.62 and destination IP 105.253.27.136.
- Immediate investigation is required to determine the cause and mitigate any potential damage.

Verifications Required:

Review related logs for anomalies and potential misconfigurations.

Recommended Next Steps:

Initiate incident response protocols and isolate affected systems if necessary.

Sincerely,

SOC Team