

Subject: Multiple login failures for the same User - Windows | Unknown Severity | Non-Actionable |
host_78

Hi Team,

Multiple login failures for the same User - Windows detected from 174.8.117.222 to 69.146.196.41.

Security Alert Details:

SOC Analyst Triage Comments:

- The alert indicates a potentially serious security issue.
- The activity was detected between source IP 174.8.117.222 and destination IP 69.146.196.41.
- 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