Subject: Multiple login failures for the same User | High | Actionable | host_39

Hi Team,

Multiple login failures for the same User detected from 244.179.137.146 to 206.140.150.87.

Security Alert Details:

SOC Analyst Triage Comments:

- This alert indicates High severity, suggesting a potential security risk.
- The event was triggered from IP address 244.179.137.146 targeting 206.140.150.87, possibly indicating suspicious activity.
- Immediate action is recommended. This may involve isolating affected systems, performing root cause analysis, and reviewing access controls.

Verifications Required:

Check server logs for unauthorized access or misconfiguration.

Recommended Next Steps:

Investigate further and apply necessary mitigations.

Sincerely,

SOC Team