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 breach.
- The event was triggered from IP address 244.179.137.146 targeting 206.140.150.87, indicating unusual network activity.
- Immediate response is needed to isolate the affected systems and perform a detailed analysis.

Verifications Required:

Investigate network traffic logs and check for unauthorized access.

Recommended Next Steps:

Isolate affected systems and conduct a thorough investigation.

Sincerely,

SOC Team