Subject: Multiple login failures for the same User - Windows | High | Actionable | host_57

Hi Team,

Multiple login failures for the same User - Windows detected from 136.67.219.152 to 153.108.153.144.

Security Alert Details:

SOC Analyst Triage Comments:

- This alert indicates High severity, suggesting a potential security breach.
- The event was triggered from IP address 136.67.219.152 targeting 153.108.153.144, 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