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 risk.
- The event was triggered from IP address 136.67.219.152 targeting 153.108.153.144, 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