Insider Threat Detection Report

Generated on: 2025-12-15 20:18:33.283913

Summary of Findings:

User: alice

- Odd-hour login

Risk Score: 30

User: invalid

- Brute-force (5 failures)

Risk Score: 50

User: user

- Excessive sudo usage (3 times)

Risk Score: 40

Recommendations:

- Investigate high-risk users

- Apply least privilege principle

- Enable multi-factor authentication

- Perform continuous monitoring of authentication logs

- Conduct periodic security audits