CyberEdu AI SOC Report

Log:


```
{
  "timestamp": "2025-05-12T14:03:00Z",
  "event": "failed_login",
  "user": "student01",
  "ip_address": "192.168.1.56",
  "location": "Lab-PC-03"
}
```


GPT Analysis:

Incident Analysis:

1. **Type of Incident**: Brute-force Attack
2. **Risk Level**: Medium
3. **Explanation**: The log indicates a "failed_login" event, suggesting that someone, possibly an unauthorized individual, atte
4. **Prevention/Response Recommendation**:
   - Implement account lockout policies to prevent multiple failed login attempts.
   - Enforce strong password policies and encourage the use of multi-factor authentication.
   - Monitor login attempts closely for any further suspicious activity and consider blocking the source IP address if repeated fa