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 (Failed Login Attempt).

2. **Risk Level:** Medium.

3. **Explanation:** Someone using the username "student01" attempted to log in from the IP address "192.168.1.56" multiple

4. **Prevention/Response Recommendation:**
   - Implement account lockout policies to prevent multiple login attempts after a certain number of failures.
   - Enforce strong password policies for all users to make it harder for attackers to guess passwords.
   - Monitor and analyze login attempts for unusual patterns or multiple failed login attempts from the same IP address.

Stay vigilant and ensure your systems are protected against brute-force attacks to safeguard sensitive information.