

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:

Based on the log provided, let's analyze it according to the given tasks:

1. Incident Type: This log indicates a "failed login" event, which suggests that someone with the username "student01" attempted to log in.
2. Risk Level: The risk level for this incident would be assessed as Medium. While a single failed login attempt may not pose a significant threat, it could be a precursor to a more serious attack.
3. Explanation: In simple terms, this log shows that someone using the username "student01" tried to log into a system from the IP address 192.168.1.56, located at Lab-PC-03.
4. Prevention/Response Recommendation: To mitigate the risk of unauthorized access in the future, it is recommended to implement strong password policies, multi-factor authentication, and regular security updates.