

CyberEdu AI SOC Report

Log:

```
{  
  "timestamp": "2025-05-12T10:22:34Z",  
  "event": "failed_login",  
  "user": "admin",  
  "ip_address": "203.0.113.45",  
  "attempts": 12,  
  "location": "Server-01"  
}
```

GPT Analysis:

****Incident Analysis:****

1. ****Type of Incident:**** Brute-force Attack
2. ****Risk Level:**** Medium
3. ****Explanation:**** The log indicates a "failed_login" event where the user "admin" attempted to log in from the IP address "203.0.113.45" with 12 attempts.
4. ****Recommendation:**** To prevent brute-force attacks, it is essential to implement strong password policies, enable account lockout, and monitor for suspicious activity.

If you have any further questions or need more clarification, feel free to ask!