

CyberEdu AI SOC Report

Log:

```
{  
  "timestamp": "2025-05-12T18:02:47Z",  
  "event": "powershell_execution",  
  "user": "student02",  
  "command": "powershell -enc aGVsbG8gd29ybGQ=",  
  "location": "Lab-PC-07"  
}
```

GPT Analysis:

****Incident Analysis:****

1. ****Type of Incident:**** Powershell Execution
2. ****Risk Level:**** High
3. ****Explanation:**** The log shows that a user named "student02" executed a Powershell command which translates to "hello v
4. ****Prevention/Response Recommendation:****
 - Ensure that users have the necessary permissions to execute Powershell commands only for legitimate purposes.
 - Monitor and analyze Powershell activity on systems to detect any suspicious or unauthorized commands.
 - Implement application whitelisting to restrict the execution of unauthorized scripts or commands.
 - Regularly update and patch systems to prevent vulnerabilities that could be exploited through Powershell attacks.