CyberEdu AI SOC Report

Log:

{
  "timestamp": "2025-05-12T14:15:02Z",
  "event": "email_received",
  "subject": "Your password has expired!",
  "sender": "support@micros0ft-secure.com",
  "attachment": "reset-password.html",
  "recipient": "student@academy.edu",
  "location": "Inbox-Student01"
}

GPT Analysis:

Based on the log provided, the incident type is likely a phishing attempt.

1. Incident Type: Phishing
2. Risk Level: Medium
3. Explanation: In this incident, the email subject is crafted to create a sense of urgency by claiming that the recipient's passwo
4. Prevention/Response Recommendation:
   - **Prevention:** Educate users about recognizing phishing emails, encourage them to verify sender addresses before clickin
   - **Response:** If a user has interacted with the email or attachment, advise them to change their password immediately, re