Task 2: Security Alert Monitoring & Incident Response

Objective

Monitor simulated security alerts using a SIEM tool, identify suspicious activities, classify incidents, and draft an incident response report.

Project Specifications

🛠️Task Description

- Use a SIEM platform to monitor and analyze security events.
- Identify suspicious behaviors and correlate them with potential incidents.
- Classify incidents based on severity and category.
- Draft an incident response report with findings and recommendations.

🕐Skills Gained

- Log analysis
- Alert triage
- Incident classification
- SOC (Security Operations Center) operations fundamentals

🧰Tools & Technologies

- **SIEM Tools**: Elastic Stack (ELK), Splunk Free Trial
- **Data**: Sample log files

📦Deliverables

- An **incident response report** containing:
- Alert analysis
- Incident classification
- Remediation recommendations