# Incident Response Report (SANS)

## 1. Objective

The objective of this task is to document a cybersecurity incident using a **professional SANS-style incident response report**.

## 2. Report Sections

### Executive Summary

A brief overview of the incident, impact, and resolution.

### Incident Timeline

Chronological sequence of events from detection to recovery.

### Detection and Analysis

Description of how the incident was detected and validated.

### Containment and Recovery

Steps taken to isolate affected systems and restore operations.

### Lessons Learned

Security gaps identified and recommended improvements.

## 3. Incident Response Flowchart

A flowchart was created using Draw.io showing:

***Detection → Analysis → Containment → Eradication → Recovery***

## 4. Conclusion

This report demonstrates the ability to document incidents in a structured and professional manner, aligning with industry best practices.