

Task 16: Incident Response Report & Incident Timeline Document

1. Incident Response Report

An incident response report documents the identification, analysis, and handling of a security incident. It provides details about the type of attack, affected systems, response actions taken, and final resolution. The purpose of an incident response report is to minimize damage, recover quickly, and prevent future incidents by improving security measures and response strategies.

Field	Details
Incident Type	Malware Attack
Date Detected	10 Feb 2026
Affected Systems	2 user computers and 1 server
Impact	Slow system performance and data risk
Action Taken	Isolated systems and removed malware
Status	Resolved and secured

2. Incident Timeline Document

An incident timeline document records the sequence of events during a security incident. It helps investigators understand how the incident occurred, how quickly it was detected, and how effectively it was resolved. Maintaining a clear timeline improves future response planning and strengthens overall cybersecurity preparedness.

Time	Event
09:00 AM	Suspicious activity detected
09:30 AM	IT team notified
10:00 AM	Affected systems isolated
11:00 AM	Malware removed
12:00 PM	Systems restored and monitored