2.1

Incident 1: Data Leak Incident

* Threat Agent: Hacker
* Threat: Unauthorized access to data storage systems
* Vulnerability: Inadequate cybersecurity measures
* Exploit: Breach via weak network defenses

Incident 2: System Downtime Due to Cyberattack

* Threat Agent: Attacker
* Threat: Distributed Denial-of-Service (DDoS) attack
* Vulnerability: Insufficient DDoS protection
* Exploit: Overwhelm servers with traffic

Incident 3: GPS System Hacked

* Threat Agent: Hacker
* Threat: Exploitation of software vulnerabilities
* Vulnerability: Failure to update and secure software
* Exploit: Injection of malicious code into GPS software

Incident 4: Unauthorized Access to Fleet Management System

* Threat Agent: Hacker
* Threat: Breach of authentication protocols
* Vulnerability: Weak passwords and lack of multi-factor authentication
* Exploit: Access through credential stuffing or brute force attacks

2.2

Incident 1: Data Leak Incident

Impact: Confidentiality & Integrity

* + Confidentiality: Unauthorized access to sensitive data compromises privacy.
  + Integrity: Potential alteration or corruption of data by unauthorized parties.

Incident 2: System Downtime Due to Cyberattack

Impact: Availability

* + Availability: DDoS attacks render systems unavailable, disrupting services.

Incident 3: GPS System Hacked

Impact: Integrity & Availability

* + Integrity: Malicious code can alter GPS data, leading to inaccurate tracking.
  + Availability: System manipulation may cause service disruptions.

Incident 4: Unauthorized Access to Fleet Management System

Impact: Confidentiality & Integrity

* + Confidentiality: Unauthorized access exposes sensitive fleet information.
  + Integrity: Unauthorized parties may alter schedules or vehicle assignments.