Incident report analysis

Summary	In May 2023, Tesla experienced a data breach caused by an insider who leaked sensitive information to the German news outlet Handelsblatt. The breach involved the unauthorized release of 23,00 internal documents, 100 GB of personal identifiable information (PII) belonging to both former and current employees.
Identify	It was discovered that two former employees breached the IT security and data protection policies, accessing and disclosing 23,000 internal documents and 100 GB of confidential data. This breach resulted in the exposure of personally identifiable information (PII) of 75,735 former and current Tesla employees
Protect	Strong access control should be implemented through a blend of policy, technology, and training. This approach includes adhering to the Principle of Least Privilege, ensuring that users have only the access necessary for their roles. Regular audits should be conducted to identify and address any unauthorized access, while clear data access policies must be established and enforced to govern how and when data can be accessed.
Detect	Implementing a SIEM solution enhances the ability to continuously monitor network activity, detect unusual behavior, and provide real-time alerts for suspicious actions. It centralizes log data, allowing for quick identification of how breaches occur and supports incident response by automating actions to minimize damage. Additionally, it helps detect insider threats and ensures compliance with security regulations.
Respond	To address a data breach effectively, begin by identifying the scope of the incident to determine what data has been compromised and how it was accessed. Next, contact the appropriate authorities. Ensure clear, accurate, and

	timely communication with all stakeholders and customers, providing them with detailed information about the breach and its potential impact.
Recover	Review the incident response process to identify both strengths and areas for improvement. Record and analyze the details of the breach to refine future security strategies and response plans. Maintain open lines of communication with customers, partners, and regulatory bodies to uphold trust and credibility. Additionally, focus on recovering data and ensuring that it is restored securely.