Scenario

You recently joined the security team as a level-one security operation center (SOC) analyst at a mid-sized retail company. Along with its physical store locations, your company also conducts operations in e-commerce, which account for 80% of its sales.

You are spending your first week of training becoming familiar with the company's security processes and procedures. Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, your team is working to prevent incidents like this from happening again. This breach happened before you began working at the company. You have been asked to review the final report.

To gain an understanding of the incident's life cycle, your goals for your review are as follows:

Goals and Answers

Goal 1: Identify exactly what happened.

- The organization experienced a data breach where an individual gained unauthorized access to customer personal identifiable information (PII) and financial data, affecting approximately 50,000 customer records.

Goal 2: Identify when it happened.

- The security incident occurred on December 28, 2022, at 7:20 p.m. PT, with initial signs of compromise noted on December 22, 2022, when an employee received an email from the attacker.

Goal 3: Identify the response actions that the company took.

- The company responded by collaborating with the security team to investigate the breach, disclosing the incident to affected customers, and providing free identity protection services. Also, routine vulnerability scans and penetration testing were implemented to prevent future recurrences.

Goal 4: Identify future recommendations.

- To prevent similar incidents, the organization recommends performing routine vulnerability scans and penetration testing, access control mechanisms like allowlisting, and ensuring that only authenticated users have access to sensitive content.