Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 01/02/2025	**Entry:** #4
Description	Mid-sized retail company. Along with its physical store locations, our company also conducts operations in e-commerce, which account for 80% of its sales.The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted.
Tool(s) used	Collaboration with public relations.
The 5 W's	• **Who**: employee received an email from an external email address (phising) • **What**: email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment • **Where**: Emails-onlilne • **When**:At approximately 3:13 p.m., PT, on December 22, 2022,

	December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer PII ● **Why**:the sender requested a $25,000 cryptocurrency payment. ⟶ later increased to $50,000
Additional notes	● Perform routine vulnerability scans and penetration testing. ● Implement the following access control mechanisms: ○ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. ○ Ensure that only authenticated users are authorized access to content. Employee meetings, email enhancements, MFA, and, least privilege protocols are all things that should be taken into accountability that will help employees and companies not go through this again.