Scenario 4: Initial Detection of Potential Security Incident

Date: **July 28th, 2024**	**Entry:** # 1
Description	Initial Detection of Potential Security Incident
Tool(s) used	• **Playbook:** Initial Response Protocol for Phishing Incidents
The 5 W's	• **Who:** An unknown malicious actor. • **What:** A Phishing Email Claiming Data Theft. • **Where**: Ecommerce organization (Remote Email Access). • **When**: Activity was observed at 3:13 p.m. JST, July 28th, 2024. • **Why**: Preliminary Assessment - Financial Gain (Cryptocurrency Demand) On July 28th, 2024, at approximately 3:13 p.m. JST, an employee reported receiving a suspicious email from an external email address. The email claimed that the sender had successfully stolen customer data and demanded $25,000 in cryptocurrency in exchange for not releasing the data to public forums. Initially, the employee assumed the email was spam and deleted it. However, this incident marked the beginning of a significant security event. Upon reflection, it's clear that the initial response relied heavily on employee vigilance, highlighting the need to explore automated detection tools for early threat identification.
Additional notes	**Immediate Actions and Preventative Measures:** • Notified Level 2 SOC Analyst to escalate the incident.

	• Initiated Playbook for Phishing Incidents to guide the response.
	• **Considerations for Future Prevention:**
	  ○ Enhance Employee Training on Phishing Detection and Response.
	  ○ Review and potentially enhance Email Filtering Mechanisms to catch similar threats.

Reflections for Scenario 4	• The reliance on employee action for initial detection underscores the importance of comprehensive security awareness training.

Follow-Up Actions	• Review of Email Security Protocols within the next two weeks. • Inclusion of Advanced Phishing Detection Techniques in the next training cycle for employees.