Scenario 4 Ongoing Analysis: Incident Escalation and Root Cause Analysis

Date: **July 29th, 2024**	**Entry:** # 2
Description	Incident Escalation and Root Cause Analysis
Tool(s) used	• **Vulnerability Scans** • **Penetration Testing** • **Analysis of Access Control Mechanisms**
The 5 W's	• **Who:** Same unknown malicious actor. • **What:** Forced Browsing Attack via E-commerce Web App Vulnerability • **Where**: Organization's E-commerce Platform. • **When**: Initial Access - Undetermined; Second Email - July 29th, 2024 • **Why**: Financial Gain through Data Exfiltration and Extortion. July 29th, 2024 marked a significant escalation of the security incident. The same employee received a second email from the malicious actor, this time including a sample of the stolen customer data and increasing the cryptocurrency demand to $50,000. This development prompted an immediate response from the security team, leading to the identification of a vulnerability in the e-commerce web application. The root cause analysis revealed that the vulnerability allowed the attacker to perform a forced browsing attack, modifying the order number in the URL string of a purchase confirmation page to access and exfiltrate customer transaction data.
Additional	**Containment, Eradication, and Recovery Efforts:**

notes	• Immediate patching of the identified vulnerability to prevent further exploitation. • Enhanced monitoring for similar attack vectors to ensure no additional breaches occurred. • **Preventative Measures to Enhance Security Posture:** ○ Regular Vulnerability Scans and Penetration Testing to identify and address potential vulnerabilities proactively. ○ Implementation of Allowlisting for Specified URLs to enhance access control and prevent unauthorized access. ○ Enhanced Security Awareness Training for All Employees, focusing on the importance of timely reporting of suspicious activities.

Reflections for Scenario 4 Ongoing Analysis	• The delay between the initial phishing email and the security team's involvement is a critical area for process improvement.

Follow-Up Actions	• Comprehensive Review of Vulnerability Management Practices to ensure proactive identification and remediation of vulnerabilities. • Enhanced Security Awareness Training Scheduled for the next quarter, with a focus on early detection and reporting.