Incident handler's journal

Maria Audu

Date: July 20, 2022	**Entry:** #1
Description	***Alert Ticket Update*** *Ticket Status: Investigating* *A phishing alert was triggered after an employee downloaded an email attachment whose SHA256 hash was previously verified as malicious.* *I am escalating the ticket because the email attachment was confirmed to be malicious and was successfully downloaded onto the employee's device. The sender details were suspicious, and the email content contained indicators of phishing. Because the file hash matches a known malicious hash, additional investigation and remediation by higher-level SOC staff is required.*
Tool(s) used	Email security gateway / alert system (for detecting the phishing email)
The 5 W's	**Who:** The incident was triggered by an employee who opened a phishing email and downloaded the attached file. **What:** A malicious email attachment was downloaded; file hash matches known malware. **When:** At the date/time listed in the alert ticket (from email timestamp and alert timestamp). **Where:** Occurred on the employee's workstation within the company's internal network. **Why:** The employee interacted with a phishing email designed to deliver malware. ●
Additional notes	The alert is legitimate, severe, and requires escalation. 1.