Incident handler's journal

Date: October 30, 2023	**Entry: 1**
Description	Providing details about a security incident at a small healthcare clinic
Tool(s) used	No tools used
The 5 W's	Capture the 5 W's of an incident. • The threat is malicious actors, a well known and organized group. • The company's critical files were encrypted in a ransomware attack. • 9:00 AM on Tuesday. • A small U.S. health care clinic. • The company's employees fell victim to a sophisticated and targeted phishing attack through email allowing the group access to the company systems where they deployed ransomware specific malware.
Additional notes	What kind of training would prevent any future phishing attacks? Should we increase the frequency of auditing user privileges? This would be to ensure most phishing attacks don't give access to the entire system if they work.

Date: October 31, 2023	**Entry: 2**
Description	Providing details about an investigation into a malicious file using VirusTotal

Tool(s) used	Sha256 hash to get file unique fingerprint, VirusTotal to analyze
The 5 W's	Capture the 5 W's of an incident. • Malicious actor(s) • An employee opened an email attachment which deployed malware? • 1:11 PM. • At a financial service company • The employee was not properly trained in awareness of phishing techniques, and the attachment was password protected, baiting them into executing it.
Additional notes	Taking a unique fingerprint of the file using sha256 is a good strategy every security analyst should use. Taking note of this specific malware for future security analysts at the organization is a good practice. Having documentation of specific malware could help them in the future.

Date: November 1, 2023	**Entry: 3**
Description	Using playbook to complete investigation of incident involving a malicious file
Tool(s) used	Phishing incident response playbook
The 5 W's	Capture the 5 W's of an incident. • A malicious actor known as Def Communications using the email address: 76tguyhh6tgftrt7tg.su • An alert was sent out due to a potential malware download from an email attachment? • 1 PM

	• The incident occurred in the employee's inbox at the organization's place of business. • The employee clicked on the email attachment believing the claim that it was password protected to view and inadvertently downloaded malware onto their computer.
Additional notes	The body of the email has multiple typos, and the email address is unrecognizable. The email is pushing for the attachment to be used. Given confirmation that attachment is malicious, the procedures were followed and the ticket was escalated. A L2 SOC was notified of the situation.

Date: November 2, 2023	**Entry: 4**
Description	Reviewing the final report of major security incident
Tool(s) used	Security Incident Final Report
The 5 W's	Capture the 5 W's of an incident. • A malicious actor • Employee was contacted for ransom of stolen customer data • 3:13 PM October 22, 2023 • Employee received email with sample of customer data and increase in ransom demand • The cause was a vulnerability in the ecommerce web application that was exploited using a forced browsing attack to access customer transaction data

Additional notes	What kind of vulnerability scans should be introduced? What can be done to discover future similar vulnerabilities before they are used by threat actors? Can we prevent all future forced browsing attacks on the platform?

Reflections/Notes: These entries represent different parts of the Incident Response lifecycle. Documentation is important and all activities related to these events have been recorded here. In reflection these activities were very interesting and I learned a lot. I wouldn't say it was challenging because the incidents were very obvious and the solutions were as well. My understanding of incident detection and response has gone from no understanding to proficient because of the activities described in this journal. I really enjoyed learning about SIEM tools and hope to use them soon in my career.