Incident handler's journal

Date: 18/07/2024	**Entry: 1**
Description	Investigated a phishing alert with a malicious attachment..
Tool(s) used	Email analysis tools, Hash verification tool
The 5 W's	**Who caused the incident?** Def Communications <76tguyhh6tgftrt7tg.su> **What happened?** A phishing email with a malicious attachment was received. **When did the incident occur?** July 20, 2022, at 09:30:14 AM. **Where did the incident happen?** On the recipient's computer system. **Why did the incident happen?** The email aimed to trick the recipient into downloading a malicious attachment.
Additional notes	The email contained grammatical errors and an unusual attachment name. The attachment hash was confirmed malicious.

Date: 18/07/2024	**Entry: 2**

Description	First journal entry documenting a ransomware attack on a healthcare clinic caused by phishing emails containing malicious attachments
Tool(s) used	Antivirus software, Email filtering tools, Network monitoring tools, Ransomware detection tools, Incident response playbook.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers. • **What** happened? A ransomware attack encrypted critical files, disrupting business operations. • **When** did the incident occur? Tuesday morning at approximately 9:00 a.m. • **Where** did the incident happen? A small U.S. health care clinic specializing in primary-care services. • **Why** did the incident happen? The incident happened due to phishing emails containing malicious attachments that deployed ransomware.
Additional notes	The company shut down its computer systems and contacted several organizations for technical assistance. Key points to consider include enhancing employee training on phishing and improving email security protocols

Date: 18/07/2024	**Entry: 3**

Description	Splunk tool
Tool(s) used	SIEM software, platform that enables organizations to search, monitor, and analyze machine-generated data in real-time, providing valuable insights and operational intelligence.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	Used as SIEM to view data normalized and collected from logs in a centralized place, uses its own search processing language called SPL (Splunk Processing Language) for writing search queries. SPL is specifically designed to interact with machine data

Date: 18/07/2024	**Entry: 4**
Description	Google Chronicle
Tool(s) used	SIEM software, platform that enables organizations to search, monitor, and analyze machine-generated data in real-time, providing valuable insights and operational intelligence.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A

Additional notes	Used as SIEM to view data normalized and collected from logs in a centralized place, uses a query language called YARA-L (Yet Another Recursive Acronym - Language). YARA-L is specifically designed to query and analyze large volumes of security telemetry data efficiently.