Incident Handler's Journal

Date: September 3, 2025	**Entry:** #001
Description	Several employees from a small U.S. health clinic reported they were unable to use their computers to access files like medical records. Business ops shut down due to employee's inability to access needed files and software to perform their job function. Some employees shared that a ransom note was displayed on their computers stating all company files were encrypted by an organized group of unethical hackers. The note demanded a large sum of money in exchange for the decryption key.
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who caused the incident?** – An organized group of unethical hackers who target organizations in healthcare and transportation industries. • **What happened?** – Ransomware security incident: attackers were able to gain access to the company's network by using targeted phishing emails sent to several employees of the company. These phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. One access was gained, ransomware was deployed, encrypting critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. • **When did the incident occur?** – The security incident occurred on Tuesday at 9:00 AM.

	• **Where did the incident happen?** – The security incident occurred on the healthcare company's employee work computers. • **Why did the incident happen?** – Compensation appears to be the motive behind the hackers' ransom note in exchange for decrypting the company's critical files.
Additional notes	1. Conversations should begin regarding preventing a security incident of this magnitude from occurring again. 2. Should the company oblige the hackers' request and pay the ransom?

Date: September 9, 2025	**Entry:** #002
Description	The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed, and a thorough investigation has been conducted.
Tool(s) used	Splunk, Firewalls

The 5 W's	Capture the 5 W's of an incident. • **Who caused the incident?** – An organized group of unethical hackers who target organizations in healthcare and transportation industries. • **What happened?** – An employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it. On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000. On the same day, the employee notified the security team, who began their investigation into the incident. Between December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft. • **When did the incident occur?** – Approximately 3:13 p.m., PT, on December 22, 2022 • **Where did the incident happen?** – The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. • **Why did the incident happen?** – The attackers motivation was money due to the ransom requested.

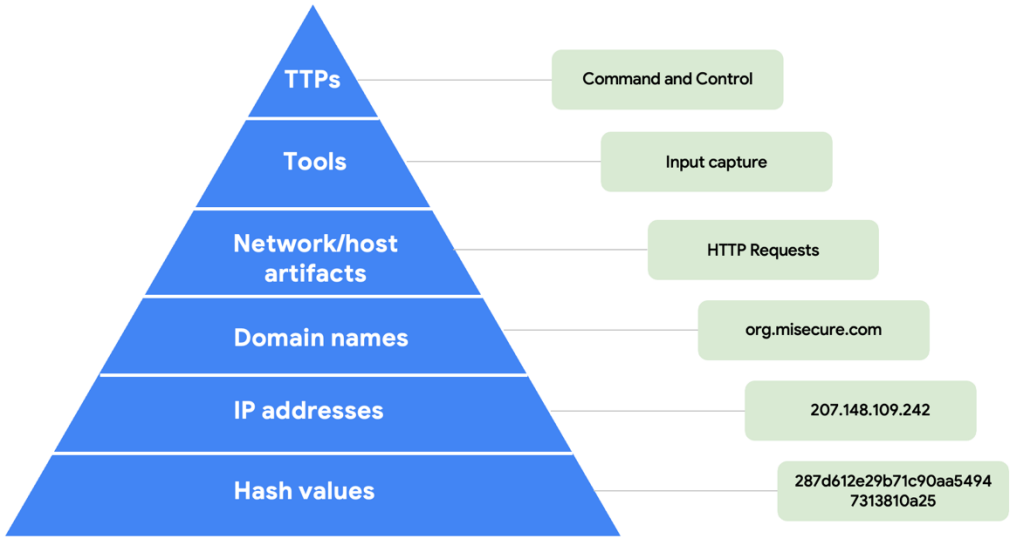
Additional notes	To prevent future recurrences, we are taking the following actions: 3. Perform routine vulnerability scans and penetration testing. 4. Implement the following access control mechanisms: a. Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. b. Ensure that only authenticated users are authorized access to content.

Reflections/Notes: The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident. After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source showing an exceptionally high volume of sequentially listed customer orders.

Date: September 5, 2025	**Entry:** #003
Description	Examining alerts, logs and rules with Suricata via Linux bash shell
Tool(s) used	Suricata is an open-source intrusion detection system (IDS), intrusion prevention system (IPS), and network analysis tool.
Details	After learning the three different components of signature analysis: action, header, and rule options, this detection method allowed me to break down a Suricata signature to better understand the various alerts that may be relayed to a security analyst and how to read a signature based on the output information.

Additional notes	I learned that there is no one-size-fits-all approach to creating and modifying rules. This is because each organization's IT infrastructure differs. Security teams must extensively test and modify detection signatures according to their needs.

Date: September 8, 2025	**Entry:** #004
Description	Investigating a Suspicious File Hash
Tool(s) used	VirusTotal is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content, such as malware.
Details	After investigating the sample file hash using VirusTotal, it's been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.
Additional notes	Using the "Pyramid of Pain," I was able to connect the Indicators of Compromise (IoC) with information from VirusTotal. Attached is a screenshot showing the correlation:


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Command and Control
Input capture
HTTP Requests
org.misecure.com
207.148.109.242
287d612e29b71c90aa5494 7313810a25