Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Scenario 1 (US health company ransomware)

1. A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.
2. The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files.
3. An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key

Date: Tuesday 9a.m.	**Entry:** 1
Description	Several employees computers were infected through phishing by ransomware software.
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. ● **Who**? Group of unethical hackers. ● **What**? A ransomware security incident ● **When** did the incident occur? Tuesday 9 a.m. ● **Where**? US health care company ● **Why** did the incident happen? Employee open attached file in phishing email from unethical hacker. After gaining access, the attackers launched their ransomware on the company, encrypting critical files. The attacker`s motivation is financial, because ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. Should the company pay the ransom for decryption key? 2. How could the health care company prevent an incident like this from occurring again?

Scenario 2 (Finance company, analyze an artifact using VirusTotal and Pyramid of Pain)

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

You retrieve the malicious file and create a SHA256 hash of the file. Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

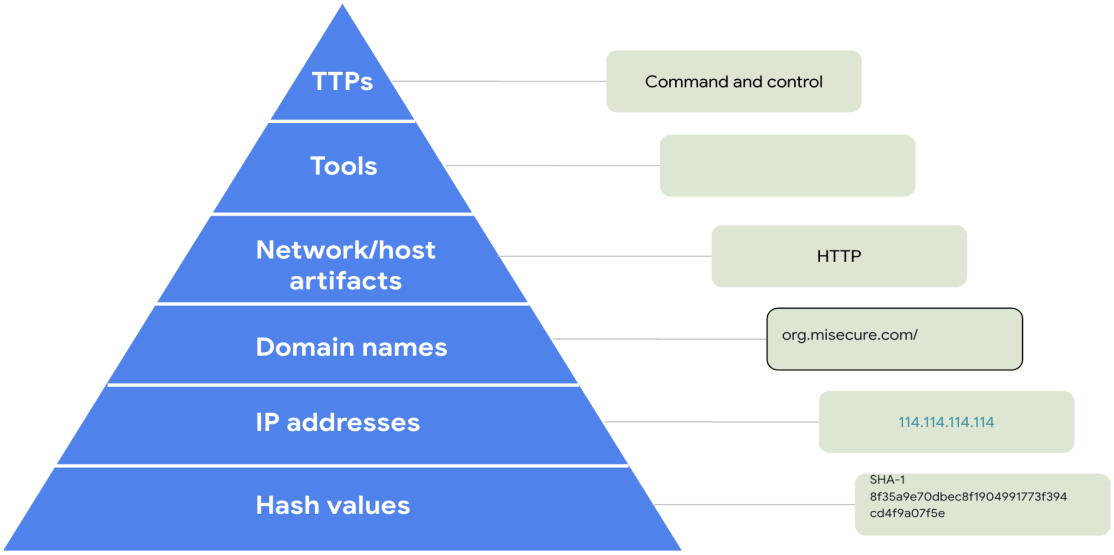
Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West
Attachment: filename="bfsvc.exe"



Date: 07.20.2022	**Entry:** 2
Description	Suspicious file downloaded on employee computer via email phishing attachment.
Tool(s) used	VirusTotal for detect attachment file.
The 5 W's	Capture the 5 W's of an incident. • **Who**? Unethical group BlackTech • **What**? Phishing with malware attachment • **When**? 07.20.2022 • **Where**? US financial company • **Why**? Gathering information and control environment
Additional notes	1. What damage can cause this malware? 2. How company can prevent an incident in future? 3. Should we consider impoving security awareness training so that

	employees are careful with what they click on?

Scenario 3 (Review final report and use incident handler to take notes)

Final report

Date: 12.28.2022 7:20pm, PT	**Entry:** 3
Description	Unauthorized access to PII and fuinancial information. (100.000$)
Tool(s) used	-
The 5 W's	Capture the 5 W's of an incident. • **Who**? Unknown hackers • **What**? Data breach • **When**? Steel date unknown, detection date 12.28.2022 • **Where**? US finance organization • **Why**? Vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform **a forced browsing attack (directory traversal)** and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.
Additional notes	1. Are secure coding practices, such as input validation and output encoding, followed consistently across our web applications to prevent forced browsing attacks? 2. Are our web applications regularly tested for vulnerabilities, including forced browsing, to identify and address any potential weaknesses?

Scenario 4 (Intestigate security incident involving phishing)

You are a security analyst at a financial services company. You receive an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: **`signin.office365x24.com`**. You need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. You will use Chronicle to investigate this domain.

Date: 2023-01-31	**Entry:** 4
Description	Asset ‘emil-palmar-pc’ lost his credentials by phishing website
Tool(s) used	- Chronicle SIEM Tool
The 5 W's	Capture the 5 W's of an incident. ● **Who**? Unknown hacker ● **What**? Phishing website, signin.office365x24.com ● **When**? 2023-01-31 ● **Where**? Singapur ● **Why**? Gain user credentials thorough phishing
Additional notes	1. Does any another employees post their credentials to this website?

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

TEMPLATE

Date: Record the date of the journal entry.	**Entry:** #
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.

The 5 W's	Capture the 5 W's of an incident. • **Who**? • **What**? • **When**? • **Where**? • **Why**?
Additional notes	Include any additional thoughts, questions, or findings.