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.

Data: 26 de Agosto, 2025	**Entrada:** #1
Descrição	Ataque de ransomware em uma clínica de saúde.
Ferramenta(s) utilizada(s)	Nenhuma. Incidente reportado pelo usuário.
Os 5 Qs (The 5 W's)	• **Quem causou o incidente:** Um grupo organizado de hackers antiéticos conhecido por visar o setor de saúde. • **O que aconteceu:** Um ataque de ransomware que resultou na criptografia de arquivos críticos e na paralisação completa das operações da clínica. • **Quando o incidente ocorreu:** Terça-feira, aproximadamente às 09:00. • **Onde o incidente ocorreu:** Na rede de computadores interna da clínica de saúde. • **Por que o incidente ocorreu:** Um e-mail de phishing direcionado com um anexo malicioso foi aberto por um funcionário. O objetivo dos hackers é o ganho financeiro através de extorsão via exigência de resgate.

Anotações Adicionais	• **Investigação**: A prioridade é determinar o escopo da violação e identificar se dados foram exfiltrados. • **Recomendação:** Não pagar o resgate, conforme as melhores práticas do setor. • **Próximos passos:** Ativar o Plano de Resposta a Incidentes (PRI) para iniciar os procedimentos de contenção, erradicação e recuperação. • **Recomendação de longo prazo:** Implementar treinamento de conscientização em segurança, utilizar filtros de e-mail avançados e criar uma política de backup robusta

---

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.

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.

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.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.