Activity Overview

In this activity, you will review the details of a security incident and document the incident using your incident handler's journal. Previously, you learned about the importance of documentation in the incident response process. You've also learned how an incident handler's journal is used to record information about security incidents as they are handled.

Throughout this course, you can apply your documentation skills using your incident handler's journal. With this journal, you can record information about the experiences you will have analyzing security incident scenarios through the course activities.

By the time you complete this course, you will have multiple entries in your incident handler's journal that you can use as a helpful reference to recall concepts and tools.

Scenario

Review the following scenario.

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their jobs.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in the healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers could gain access to the company’s network by using targeted phishing emails, which were sent to several company employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company could not access critical patient data, causing major disruptions in its business operations. The company was forced to shut down its computer systems and contact several organizations to report the incident and receive technical assistance.