Security Vulnerabilities Scenarios with AI

Assignment

40m - 1h

Status | Incomplete

Scenario #1

Imagine you're responsible for the cybersecurity of a small online retail company. This company stores customer data, processes online payments, and has an internal employee network. Your task is to make sure the digital assets are safe!

Consider the different aspects of the company's operations and technology.

What are the potential weak points where a cyber attack could occur?

Be sure to consider the three types of security controls that should be in place: Technical controls, physical controls and administrative controls.

This could include things like:

- data storage
- website security
- payment systems
- employee access to sensitive information.

Toggle Answer

Based on the vulnerabilities you've identified, think about what kinds of threats could exploit these weaknesses.

This could include things like:

- code injection attacks
- DDOS attacks
- unencrypted information
- insider threats.

Toggle Answer

Make a list of some of the threats that you anticipate the organization may face based on the company profile and the weak points you listed above.

Reflect on how AI might assist in this scenario. How could it help in:

- detecting unusual activities
- analyzing large volumes of data for suspicious patterns
- or prioritizing risks based on their severity

Toggle Answer

Watch the following demonstration about how to use the AI tool ChatGPT to search for security recommendations based on your company's profile.

Cyber - Scenario #1

Lighthouse Labs

02:02

For this demo, the cybersecurity analyst used AI to research the company profile and quickly identify some of the company's main risk factors.

In particular, three main pieces of information give us clues as to the most likely vulnerabilities that this company will face:

1. It is an online company, meaning it was a website we needed to secure.
2. As an online retail store, we will need to worry about secure payment and secure storage of customer data.
3. We have an internal employee network we need to secure.

> Whenever you are doing a security assessment, you should build a company/application profile to evaluate each component of the company for potential risks/vulnerabilities.

Then, you can take this information and do research and analysis using tools like ChatGPT, as demonstrated below:

Cyber - Scenario #2

Lighthouse Labs

01:57

Reflection

Think back to the AI demo video you just watched. Remember how AI was used to identify, analyze, or mitigate cybersecurity threats.

Consider the following questions:

- How did AI contribute to solving the cybersecurity challenges?
- Were there any limitations or challenges in the AI's approach?
- Could anything have been done differently or more effectively?
- Where does AI excel, and where is human judgment still very important?

> In this reflection, try to go beyond just summarizing the demo.
>
> Challenge yourself to think about the broader implications of AI in cybersecurity: How might reliance on AI shape the future of cyber defence?

Scenario #2

You're the cybersecurity analyst for 'MD Clinic', a healthcare provider that offers both in-person and telehealth services. The clinic uses electronic health records (EHRs), online appointment booking systems, and a remote health platform for virtual consultations. Your task is to assess and strengthen the cybersecurity posture of the clinic.

Write down some of the possible vulnerabilities that may be present based on their business model.

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

Now, try using an AI tool to analyze the listed vulnerabilities in the MD Clinic scenario. See how it can assist in identifying and prioritizing these cybersecurity risks.

Mark Completed

Previous
Vulnerability Severity

How well did this activity help you to understand the content?

Let us know how we're doing

W05D2

Tue Jul 23

- Vulnerability Concepts
- Common Vulnerabilities and Exploits (CVE) List
- Vulnerability Severity
- Security Vulnerabilities Scenarios with AI

› Other (1)

W05D2 Schedule »