Course Project

About the final course project and assessment

Introduction

You have gained new knowledge and skills in cybersecurity concepts and mitigation strategies during the last few weeks. Now, it is time to demonstrate this learning by completing the course project and graded assessment.
But first, let's explore what you can expect and discover how to set yourself up for success.

Demonstrating your mastery

The final course project serves as a culmination of your learning journey, allowing you to demonstrate your ability to navigate cybersecurity threat vectors and apply effective mitigation strategies. It will enable you to practice what you've learned and showcase your understanding, while the graded assessment will evaluate your mastery of the key learning objectives covered in the course.

What to expect from the course project

In the course project, you will be tasked with creating a comprehensive security strategy for a business enterprise, leveraging your knowledge and skills acquired throughout the course. Drawing upon your understanding of the active threat landscape, types of cyberattacks, encryption, and security and compliance concepts, you will practice applying your knowledge to a real-world scenario.
More specifically, you will demonstrate your ability to:

- Identify potential security threats.
- Identify and assess risks.
- Develop countermeasures for identified risks and threats.
- Design a data protection strategy.
- Create an incident response plan.

Overall, the course project aims to enhance your skills in security analysis, strategy development, risk assessment, data protection, and incident response in the context of cybersecurity.

What to expect from the graded assessment

The graded assessment is a final measure of mastery of the course objectives. Rest assured that the assessment will cover only the topics you have learned throughout the course. It allows you to apply your knowledge and demonstrate your understanding in a controlled setting.
The assessment will take approximately 1 hour and 30 minutes, and a passing score of 80% is required. You can retake the quiz if needed, bearing in mind that the questions will vary each time. Make sure to review the feedback provided on your answers and focus on areas that require further attention.

How to prepare for success

To prepare for the final assessment and course project, here are some tips to guide you:

- Revisit key learning material: Review the course materials, including videos, readings, and resources, to reinforce your understanding of the concepts covered.
- Review knowledge checks and module quizzes: Take the time to revisit the knowledge checks and module quizzes you completed throughout the course. Focus on areas where you may have struggled or need further clarification and use the feedback provided to identify areas that require additional attention.
- Review exercises: Take advantage of the hands-on exercises you've completed and review the exemplary material. This can help inform your application of key skills in the final course project.
  - Exemplar: Initial protective measures
  - Exemplar: Walling off
- Seek additional resources: If you feel the need for further exploration, consider referring to the different additional resources available in each lesson.

Final thoughts

The exercise and graded assessment are your chance to demonstrate the depth of your understanding and the practical application of your skills. Remember that this journey has equipped you with the knowledge necessary to complete this final chapter of cybersecurity threat vectors and mitigation.

The finish line is in sight, and success awaits those ready to embrace the final challenge. Good luck!

Final course project: Security strategy

Introduction

This exercise provides an opportunity to apply your theoretical knowledge in a practical, real-world scenario. By completing this exercise, you will gain hands-on experience in conducting a security analysis, identifying potential threats, assessing their risks, and formulating effective countermeasures.

Scenario

Sam's Scoops has experienced substantial expansion. Operating across multiple locations, Sam's Scoops deals with sensitive customer data, including credit card information, addresses, and personal details.

The growing workforce, now over 250 employees, work in diverse departments. An emerging concern is that some of these employees bring their personal computers to the office, potentially introducing new vulnerabilities into the company's network.

Given the rising complexity of cyber threats, Sam's Scoops is increasingly exposed to potential risks like phishing, ransomware, and DDoS attacks. Furthermore, data breaches are an ever-looming threat that could impact the company's reputation and financial stability.

Objective

Your task is to conduct a comprehensive security analysis and develop a detailed security strategy report for Sam's Scoops. The strategy should address the evolving threats that the company could encounter and outline suitable solutions for risk mitigation and data protection.
Use the knowledge gained from this course and previous courses to develop this strategy report.

Instructions

Follow the steps below to create a comprehensive security strategy report for Sam's Scoops. Remember, the content is the primary concern, and you are free to design the report in a format that works for you.

Step 1: Identify all potential threats

Identify all potential threats, internal and external, that Sam's Scoops might face. Consider the risk employees pose by using personal computers in the office and the external threats of cyberattacks.

Step 2: Evaluate risks

Evaluate the risk associated with each identified threat. Assess the likelihood of each threat occurring and consider the potential impact of each on Sam's Scoops' business operations. Then, prioritize the threats based on the risk assessment.

Step 3: Develop countermeasures for each threat

To mitigate risks, develop a set of countermeasures for each threat. This can encompass technological solutions, policy changes, and employee training.

Step 4: Design a comprehensive data protection strategy

Design a comprehensive data protection strategy, taking into account secure data storage and transmission, regular data backups, and robust access control measures.

Step 5: Develop a phishing avoidance strategy

Identify anti-phishing solutions and propose solutions to enhance employee phishing awareness.

Step 6: Create a personal device policy

Create a personal device policy to manage and mitigate the security risks associated with employees using personal devices in the shop.

Step 7: Implement MFA and biometric security measures

Outline a strategy for implementing MFA and biometric security measures across all relevant systems. This should ensure that only authorized personnel can access sensitive data, reducing the risk of unauthorized access.

Step 8: Create an incident response plan

Create an incident response plan that enables Sam's Scoops to respond to and recover from security incidents effectively. Include immediate response steps, long-term recovery strategies, and measures to prevent future occurrences.

Step 9:Propose a plan for continuous monitoring and improvement

Propose a plan for continuously monitoring, reviewing, and improving security measures to help ensure that Sam's Scoops can adapt and respond to the evolving threat landscape.

Conclusion

Ensure your report is comprehensive, well-structured, and easy for all stakeholders to understand. Keep the tone professional, clear, and precise. Your aim is to provide a roadmap that secures Sam’s Scoops operations and customer data from potential threats.