Activity Overview

In this activity, you will practice using the Process of Attack Simulation and Threat Analysis (PASTA) threat model framework. You will determine whether a new shopping app is safe to launch.

Threat modeling is an important part of secure software development. Security teams typically perform threat models to identify vulnerabilities before malicious actors do. PASTA is a commonly used framework for assessing the risk profile of new applications.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You're part of the growing security team at a company for sneaker enthusiasts and collectors. The business is preparing to launch a mobile app that makes it easy for their customers to buy and sell shoes.

You are performing a threat model of the application using the PASTA framework. You will go through each of the seven stages of the framework to identify security requirements for the new sneaker company app.

PASTA worksheet

Stages	**Sneaker company**
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. *App will process transactions after users signing up App must process financial transactions. Industry regulations that need to be considered is PCI-DSS.*
II. Define the technical scope	List of technologies used by the application: ● *API* ● *PKI* ● *AES* ● *SHA-256* ● *SQL* APIs play a crucial role in enabling data exchange among customers, partners, and employees, making their prioritization essential. They manage sensitive information and bridge different users and systems.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. ● *SQL injection* ● *Session hijacking*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. ● *Broken API token* ● *Theft of session cookies*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **4 security controls** that you've learned about that can reduce risk. Patch update, principle of least privilege, SHA-256 and MFA