PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. • *Will the app process transactions?* • *Does it do a lot of back-end processing?* • *Are there industry regulations that need to be considered?* The application allows users to create member profiles either internally or by linking external accounts. Additionally, it facilitates financial transactions and must comply with PCI-DSS compliance standards.
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. APIs are like the connectors that enable different apps and systems to talk to each other. Since they handle a lot of sensitive data and link various users and systems together, they need to be given special attention. However, before picking one API over another, it's important to know which ones are being used. This is because APIs can be targeted by hackers more easily due to their extensive connections, making them potentially vulnerable to security risks.
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. • *What are the internal threats?* • *What are the external threats?*

	• Insider Threats: These involve malicious or negligent actions by individuals within the organization who have authorized access to the application and its data. Insider threats can include employees intentionally leaking sensitive information or accidentally exposing it through negligent actions. • External Attacks: These are threats originating from outside the organization, typically from malicious actors such as hackers or cybercriminals. External attacks can take various forms, including malware infections, phishing attacks, or direct exploitation of vulnerabilities in the
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. • *Could there be things wrong with the codebase?* • *Could there be weaknesses in the database?* • *Could there be flaws in the network?* Yes, there could be issues with the codebase, weaknesses in the database, or flaws in the network that could be exploited by attackers. It's crucial to identify and address these vulnerabilities to mitigate the risk of security breaches.
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. Four key security controls that help reduce risks are access control, encryption, intrusion detection and prevention systems (IDPS), and security patch management. Access control limits access to authorized users, encryption protects data from unauthorized access, IDPS monitors for suspicious activities, and security patch management ensures systems are updated with the latest protections against vulnerabilities.