PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	Make **2-3 notes** of specific business requirements that will be analyzed. • *Data privacy is a concern, must comply with PCI-DSS, PII, SPII, and GDPR regulations.* • *The users control their accounts* • *The app will process financial transactions* • *Back-end processing will occur*
II. Define the technical scope	List of technologies used by the application: • *Public key infrastructure (PKI)* • *Application programming interface (API)* • *Advanced encryption system (AES)* • *SHA-256 hash function* • *Structured Query Language (SQL)* Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others. PKI is an encryption framework that secures the exchange of sensitive online information. The mobile app employs a combination of symmetric and asymmetric encryption algorithms, namely Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). AES encryption ensures data remains securely encrypted during transmission and storage. On the other hand, RSA encryption secures the exchange of cryptographic keys between the mobile app and a user's device, establishing a trusted communication channel. Although API is a large attack surface, prioritizing the security of the PKI is essential to maintain the confidentiality and integrity of the exchanged information while safeguarding the privacy and trust of the app's users and partners.
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 attacks* • *Social engineering an employee who worked on the app*
V. Vulnerability analysis	List **2 vulnerabilities** in the PASTA worksheet that could be exploited. • *Lack of prepared statements* • *Lack of cybersecurity awareness training*
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. 1. *Data Sanitization or Masking of data,* 2. *Multi-Factor Authentication (MFA)* 3. *Incident Response Procedures,* 4. *Complex Password Policies,*