PASTA threat modeling worksheet

Stages	Sneaker company
I. Define business and security objectives	**Business Requirements** ● *The application should make it easy for users to sign-up, log in, manage their accounts, and make transactions* ● *Proper payment handling and data privacy are important for the business*
II. Define the technical scope	**Application Technologies** ● *API* ● *PKI* ● *AES* ● *SHA-256* ● ***SQL*** SQL should be prioritized for security because it manages the application's database. Steps should be made to ensure that SQL is properly configured to facilitate the business in fulfilling its data handling objective.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	**Threat Types** ● *A business employee that does not have proper data use privileges could submit unauthorized queries to the database, making him an insider threat* ● *An employee from a rival e-commerce company could corrupt the database or steal sensitive information, like trade secrets, from it*
V. Vulnerability analysis	V**ulnerabilities** ● *If the input for the login form is not handled correctly, a threat actor could slip in some malicious code that could trigger an exfiltration of the login data* ● *Similarly, an attacker could use SQL injection against the payment form of the website to collect payment card information of customers and spy on their transactions*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	**Security Controls** ● *Prepared statements* ● *Input sanitization* ● *Input validation* ● *User training*