PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	• *Maintaining confidentiality, integrity and availability of customer data is a top priority.* • *We need to streamline sign-up, log in and account management tools to improve user experience.* • *Making sure customers have multiple payment options as well as ensuring clear and fast checkout.*
II. Define the technical scope	List of technologies used by the application: • *API* • *PKI* • *AES* • *SHA-256* • *SQL* SQL should be prioritized above all others because of the risk of SQL injection attacks against the application. We need to make sure all user input options on the application have adequate controls in place to prevent such an attack, as well as check for flaws within the programs code base.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	• *Social engineering attacks aimed at our employees' to obtain access to company assets.* • *SQL injection attacks, including in-band, out-of-band and inferential.*
V. Vulnerability analysis	• *Inadequate coding on our user input fields could allow attackers to compromise them with malicious code.* • *Authentication would be vulnerable if an employee fell prey to a social engineering attack.*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis	Prepared statements and input sanitization on our input fields

and impact	coding to address our SQL injection vulnerabilities. Training for employees' on phishing and social engineering attacks. Multi-factor authentication (MFA) and single sign-on (SSO) to streamline customer login process.

Data flow diagram

Note: This data flow diagram represents a single process. Data flow diagrams for an application like this are normally much more complex.

Sample attack tree

Note: Applications like this normally have large, complex attack trees with many branches.