PASTA Threat Model for Snazzy Sneakers

Stages	Sneaker company
I. Define business and security objectives	Specific business requirements that will be analyzed: • *Users can create member profiles internally or by connecting external accounts, like Facebook or Google.* • *The application must maintain confidentiality of seller-shopper messaging interactions.* • *The application must comply with PCI-DSS.* • *The application must protect seller and shopper data, including financial transactions.*
II. Define the technical scope	List of technologies used by the application: • *Application programming interface (API)* • *Public key infrastructure (PKI)* • *SHA-256* • *SQL* API's should be prioritized because they facilitate the exchange of data between sellers, shoppers, and employees. This data is often sensitive. Particular attention should be paid to third party API's that are utilized. PKI will be necessary to protect payment data and other web application usage, as well as to comply with PCI-DSS. Client passwords will need to be stored securely as hashes with SHA-256. The databases that store all seller and shopper data will run on SQL.
III. Decompose application	Sample data flow diagram
IV. Threat analysis	List **3 types of threats** in the PASTA worksheet that are risks to the information being handled by the application. • *Code injection* • *Data exfiltration* • *Session hijacking*
V. Vulnerability analysis	List **3 vulnerabilities** in the PASTA worksheet that could be exploited. • *Lack of prepared SQL statements.*

	• *Third party code vulnerabilities.* • *Insecurely stored API tokens.*
VI. Attack modeling	Sample attack tree diagram
VII. Risk analysis and impact	List **5 security controls** that you've learned about that can reduce risk. • *Implement strong password policies and require employees to abide by them.* • *Utilize prepared SQL statements.* • *Regularly verify the security of third party API's.* • *Store passwords securely as SHA-256 hashes.* • *Enforce principle of least privilege.*
