## PASTA worksheet

* 2-3 business objectives
* 2-3 technology requirements
* 2 potential threats
* 2 system vulnerabilities
* 4 defenses that limit risk

|  |  |
| --- | --- |
| **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 sneaker company’s goal(s) are:   * drive profits & ROI * grow brand awareness * increase market share   In order for their app to do business and process transactions, it will have to do back-end processing of payments so it will need necessary technologies:   * Mobile Payment SDKs (e.g. Apple Pay, Google Pay) * Payment Gateway (e.g. Stripe, Paypal, Square) * Backend Payment Process System (e.g. Braintree, Ayden) |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *User Authentication* * *API Integration* * *Fraud Detection Tools* * *DB Management* * *Payment Gateway*   Write **2-3 sentences** (40-60 words) that describe why you choose to prioritize that technology over the others.   * **User Authentication:** Secure users to safely login and authenticate using MFA or OAuth 2.0 * **Fraud Detection:** USe tools like Sift & Riskified to detect & prevent fraud transactions * **APIs:** Connect with 3rd party services such as banks, shipping services, and etc to complete order fulfillment |
| **III. Decompose application** | [Data Flow Diagram](https://docs.google.com/presentation/d/1wpDtJO1sjNDZ-GeZ_y-0e74Us0kg4laEFOls8gBrhhs/edit?usp=sharing) |
| **IV. Threat analysis** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.   * Insider Threat(s) * Phishing & Social Engineering |
| **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?*   Issues in codebase which could lead to issues such as SQL Injection include:   * Weak password policies * No MFA   Weaknesses in databases include:   * lack of authentication steps in place * lack of enforcement in role-based access control (RBAC) * not enough audits & reviews. |
| **VI. Attack modeling** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| **VII. Risk analysis and impact** | List **4 security controls** that you’ve learned about that can reduce risk.   * MFA * Strong passwords/passphrases * Can use Access Badges w/ RFID chip at Work |