## PASTA worksheet

| **Stages** | **Sneaker company** |
| --- | --- |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *App will process transaction have several payment options for a smooth checkout process* * *It will do lot of backend processing because there are many features* * *There will be 2 industries measure will be followed 1st will be GDPR and 2nd will be PCI DSS* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *Application programming interface (API)* * *Public key infrastructure (PKI)* * *SHA-256* * *SQL*   I will first apply PKI because it is an encryption framework that secures the exchange of online information. The mobile app uses a combination of symmetric and asymmetric encryption algorithms: AES and RSA. AES encryption is used to encrypt sensitive data, such as credit card information. RSA encryption is used to exchange keys between the app and a user's device. |
| **III. Decompose application** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| **IV. Threat analysis** | List **2 types of threats** in the PASTA worksheet that are risks to the information being handled by the application.   * *The internal Threat would be if encryption got decrypted it will be a loss App authentication process can be also decompremise* * *External threats would if any employee will be phished so the app will be also at risk if employee device is compromised then the also could be* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * [*CVE-2025-3342*](https://www.cve.org/CVERecord?id=CVE-2025-3342)  ***LLM02:2023 - Data Leakage*** |
| **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** | * We can secure the app from data breach * We can secure the app from sql injection * We can limit the access of employees * We can make use Api , Pki, And Hash for making it more secure from the backend * We can update regularly the database for exploits or viruses and and conduct a vulnerability assessments and app auditing |