## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | Make **2-3 notes** of specific business requirements that will be analyzed.   * *The app will process monetary transactions* * *The app has to search and filter the inventory in the backend to return search results* * *The app must adhere to PCIDSS guidelines* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   APIs are generally third-party programs used to solve specific problems. While this increases productivity, care must be taken to verify the authenticity of the authors and the program before using. If not, it becomes a possible attack surface. |
| **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.   * *Broken user access controls* * *Unencrypted data in storage and transit* |
| **V. Vulnerability analysis** | List **2 vulnerabilities** in the PASTA worksheet that could be exploited.   * *Users with more access than necessary can cause malicious actors to attack the systems.* * *Data that is not encrypted in storage or transit becomes vulnerable to man-in-the-middle attacks whereby anyone who listens to the packets can read all data.* |
| **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** | * *User access must follow the principle of least privileges* * *Users must have separation of duties. No one user must possess critical power to damage the systems.* * *Data must be encrypted and verified using cryptography and hashing* * *Passwords must follow the NIST standards to ensure strength* |