## PASTA worksheet

|  |  |
| --- | --- |
| **Stages** | **Sneaker company** |
| **I. Define business and security objectives** | *The app needs a secure connection for make pay transactions and chatting with the provider, that implicit the backend will be complex and will need high compute processing. GDPR must be obligated in this case, the app will handle PII and SPII from users and sellers.* |
| **II. Define the technical scope** | List oftechnologies used by the application:   * *API* * *PKI* * *AES* * *SHA-256* * *SQL*   Starting with AES and SHA-256 as methods of cryptography are essential to secure the communications transactions, salting and hashing SQL queries and content in this way SQL injections and session hijacking will reduce the impact on server´s performance. PKI is part important of the cryptography methods, described previously, all connections will be secured and hardly can be decrypted and finally. API are the endpoint that needs to be protected with all the infrastructure described. |
| **III. Decompose application** | When the user made a query to app the connection to database is with a PKI with SHA-256 and AES cryptographic methods the session is encrypted. Now in case that session is compromised exist other layer to protection and SQL queries are salting and hashing reducing collision hashing, rainbow hashing or extraction of PII and SPII. |
| **IV. Threat analysis** | *Internal threats*   * *Employees* * *Business partners*   *External threats*   * *Competitors* * *Hackers* |
| **V. Vulnerability analysis** | *-Misconfigured PKI*   * *Out-dated libraries* * *Expose environment keys* * *No salting* * *No hashing* |
| **VI. Attack modeling** | Threat actors can exploit our vulnerabilities using phishing strategi in a user not all attacks need be DoS or brute force. Hackers can use prepared statements in the form login or in the API. |
| **VII. Risk analysis and impact** | * MFA * IAM * Least privilege * Passwords policies * GDPR compliance * Limiting server’s area |