|  |  |
| --- | --- |
| Question | Prompt strategy |
| Name of application |  |
| Introduction of the business functions and general aspects |  |
| Contact person |  |
| Describe the main business purposes of the application. Companies or consumers in scope | Improve writing and translate into target language |
| Describe approximate number of users and where are they located, countries and region | Depending on regions there must be specific requirements. E.g. in EU follow GDPR, data should not be hosted outside of EU. In other countries less restrictions. In China and Russia data must be kept inside the same country. Add this information into the prompt and let GPT generate the controls. |
| Describe the level of confidentiality, integrity and availability. Examples for confidentiality: public, internal, confidential, secret. Example for availabilty: standard or critical. Example for integrity: standard or critical. If the app includes personal sensitive data such as credit card number, motion data, sexual preference etc.? All can be can also be implemented as check boxes. | Extract the information and use them across the entire prompting. E.g. this is a confidential application (public, internal, confidential, secret). Based on this classification recommend the corresponding controls.  Personal sensitive data -> strict controls |
| Kind of application: SaaS, completely Self developed, or individual coding based on existing products |  |
| Industry of the application (Example: automotive, health, public sector, financial, consumer, telecom, machinery, chemistry, service, consulting, education) | Ask if any industry specific security requirements are necessary. |
| Any certification available (e.g. SOC2 type2, ISO27001 etc.). | In case of SaaS the certification must be related to the SaaS software. In other cases the certification is related to the (cloud) hosting environment. Judge if the certification is available or not, and if it is sufficient. |

General application information

Authentication/authorization

|  |  |
| --- | --- |
| Question | Prompt strategy |
| Do you use a company wide SSO system or a built-in authentication of the application? | Say that company authorized SSO should always be preferred over the built-in authentication of the application. Only in the case of few users, it makes no sense to integrate SSO since it causes too much efforts. |
| What authentication mechanism is being used for the web application? Is it based on passwords, multi-factor authentication, or some other method? | Describe the company’s password policy, MFA etc. |
| Is account creation and management secure? | Describe a secure account creation and management process. Describe how to prevent unauthorized account creation or modification. |
| What authorization mechanism is being used for the web application? Describe technology | Based on the described technology, describe best practice according |
| Where are user credentials stored? Which programming language or framework is used. | Describe which function should be used based on the given programming language and framework. Mention hash and salt. |
| Is there any sort of rate limiting or account lockout policies in place to prevent brute force attacks? Name any products used if available | Describe the right account lockout policies and rate limiting mechanism based on the product, if any. |
| Does the system implement secure session management? Which product or technology is used? How are session tokens handled and protected? Name the technology | Describe how should session tokens be handled and protected based on the product or technology. Describe what is the best practice for secure session management. |
| How does the application manage user roles and permissions? Name all planned user roles. | Describe the user roles and their permissions in best practice. |
| Does the application have a secure password reset or account recovery mechanism? | Describe how a secure password reset or account recovery looks like. |
| Does the web application use micro services and name the products used for the micro services. | Describe the proper authentication this micro service. |

Application Architecture

|  |  |
| --- | --- |
| Question | Prompt strategy |
| Describe the main technology used for the application. Main framework, programming language, functions. | Improve the writing and translate into target language |
| Describe the technology of the frontend and used products | Figure out any known security weakness of the frontend technology and framework and describe the countermeasures. Consider also OWASP top 10 for mobile app. |
| Describe the technology stack of the middle layer and used products | Figure out any known security weakness of the middleware technology and framework and describe the countermeasures. Consider also OWASP top 10. |
| Describe the backend layer or used database | Figure out any known security weakness of the backend technology and framework and database, and describe the countermeasures. Consider also OWASP top 10. |
| Describe the relation between frontend, middle layer or backend. If any layer is not available, just skip. | Judge if it is a good architecture design. |
| Describe any library, dependencies used | Improve the writing and translate into target language. |
|  |  |
|  |  |

Cloud Architecture

|  |  |
| --- | --- |
| Question | Prompt strategy |
| Name of the cloud provider, e.g. Azure, AWS, GCP |  |
| Name all cloud resources used for this application such as VM, App service, container service, security groups, firewall, private link, database, application gateway, forward proxy, load balancer, security proxy, data storage, | Describe the hardening measures for every of this cloud resource depending on the classification. |
| Describe the relation between all the cloud resources | Judge if this is a good cloud security architecture design. Recommend security best practices for this cloud settings. |
| Describe if there are any connections between the cloud resources and company’s onprem environment | Judge if the connection is secure considering the classification. What is the preferred architecture? |
| Describe how the user can access the web application, from the internet, from company’s intranet. | Judge if the access is secure regarding the classification. |
| Describe monitoring and evaluation services | Judge if that is sufficient and mention that they should be connected to company’s central monitoring and SIEM solutions. |
| Describe the current cloud governance model | Judge if the cloud governance model is sufficient and recommend improvements. |
|  |  |

Final prompting:

Create a report with following structure:

Management summary and mention the business function briefly and the most critical controls.

Introduction of the business functions and general aspect description.

Describe authentication/authorization concept.

Describe the application architecture and its recommended controls.

Describe controls for cloud architecture.

Let general information such as application name, confidentiality etc. always be integrated in the following chapters.

A further chapter for visualization of the architecture (backlog).