Questions & Answers

How/Where is my data stored?

We store your data in a database hosted on Azure in a datacenter in Europe. To further increase security, every customer has its own database.

Is my data shared with other parties in any way?

We do not by any means provide other parties except Microsoft with access to the information stored in our databases or gained through the assessment process. Additionally, we do not sell, forward or by other means provide access to your data to any other party. The cooperation with Microsoft follows the limitations outlined in their documentation.

Note that this does not provide Microsoft with more access to your data as they already have due to you using their services.

How does C-Ray get the data from my Cloud Environment?

C-Ray gets the data needed for the assessments from the Microsoft Graph API and Exchange Online PowerShell. To make it work you need to give certain permissions to C-Ray.

Which permissions does C-Ray need to create an assessment?

C-Ray needs permissions for the Microsoft Graph API and the Exchange Online PowerShell. During the first Registration C-Ray will ask you to grant these permissions.

Needed permissions for Graph API:

- Directory.Read.All
- RoleManagementPolicy.Read.Directory
- RoleManagement.Read.All
- Agreement.Read.All
- AccessReview.Read.All
- CrossTenantInformation.ReadBasic.All

Detailed Information regarding the Graph API permissions you can find here.

The needed permission for Exchange Online allows C-Ray to manage the organization's Exchange environment, such as mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles to the apps service principal.

C-Ray requires the role *Global Reader*, which therefore needs to be assigned to the corresponding Enterprise Application / Service Principal in your Azure Active Directory. If this role is not assigned, C-Ray can only perform checks on the Azure Active Directory.

How does a security assessment by C-Ray look like?

A finished security assessment is provided as a report in PDF format. All the findings are described in detail in your language including risk assessment, remediation effort and remediation instructions.

An example-report with one finding can be found here.

Can I delete data about my environment?

Yes, whenever you delete an assessment, all data created for this assessment is deleted as well. Additionally, we only stored data required for user authentication and access agreements. If you want to have all data deleted, please reach out to us via the contact form. Note that deletion of all data will lead to a full reset of your profile and we have no means of restoring data once deleted.

How is the data about my environment used?

The data is only used for the creation of your security reports. While performing the assessment, we collect anonymized metadata for statistical purposes (like the amount of assessments performed, counter per vulnerability and weakness etc.). This helps us focusing our improvement efforts on those weaknesses and vulnerabilities which occur most often. As these metadata are not linked to your environment and collected in a fully anonymized form, they cannot be deleted.