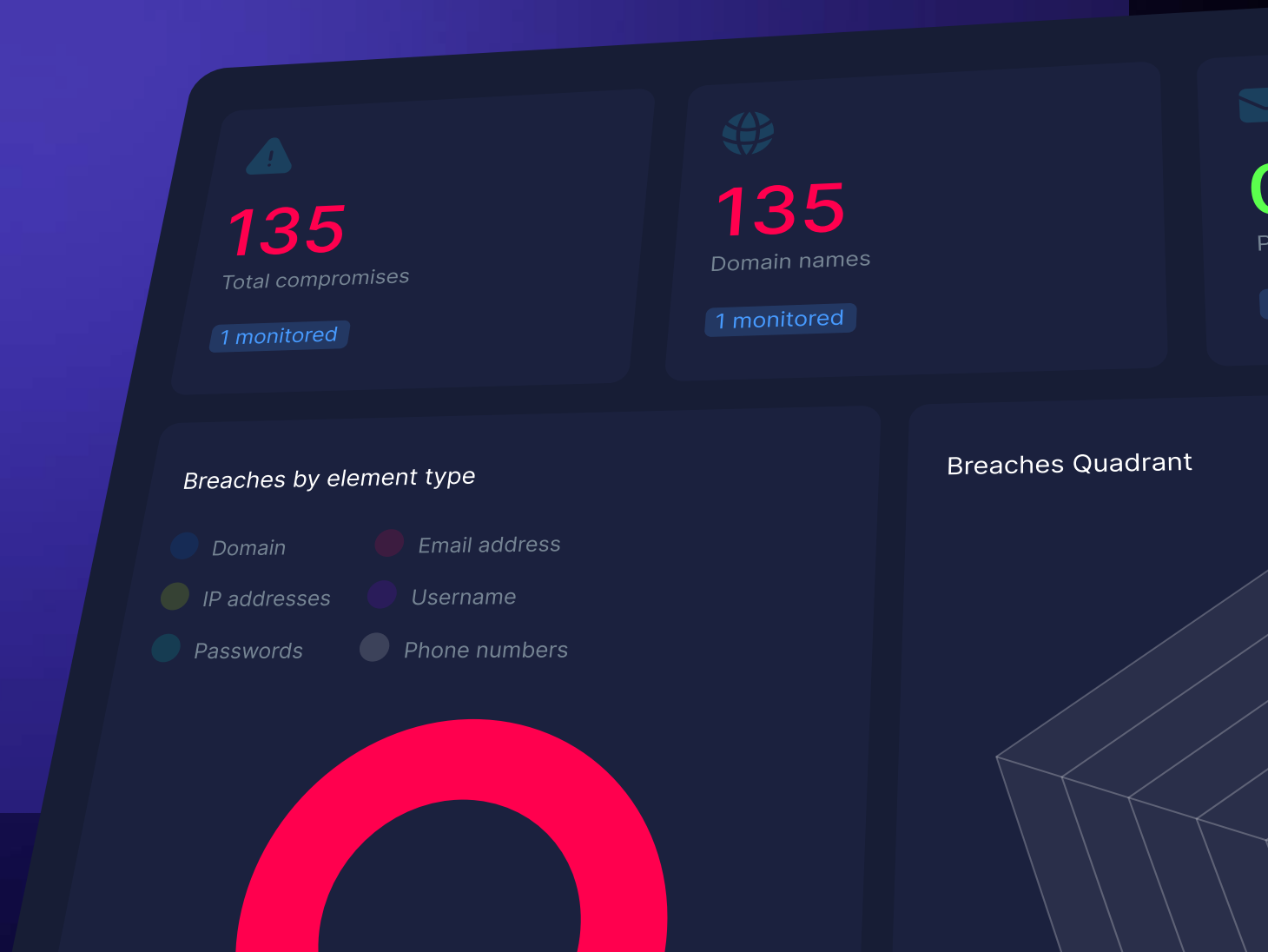




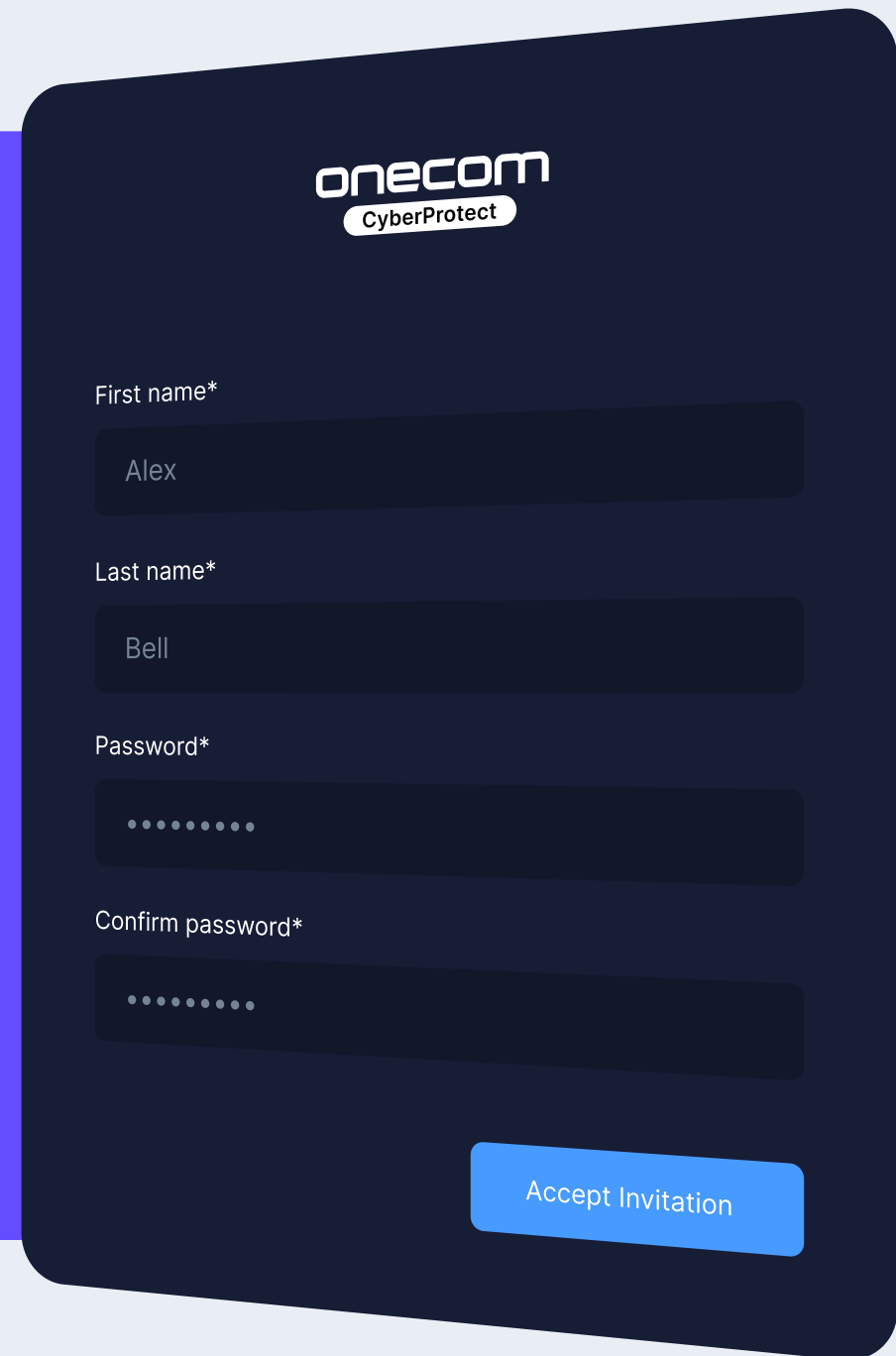
# User Guide

Mastering Onecom Cyber Protect's features and functionalities



# Activating your account

Following the receipt of an invitation to access CyberProtect either by Onecom or a member of your organisation, click the link in the email and enter your first name, last name and password choice.



The screenshot shows a dark-themed mobile application interface for account activation. At the top right is the 'onecom CyberProtect' logo. Below it are four input fields: 'First name\*' with the text 'Alex', 'Last name\*' with the text 'Bell', 'Password\*' with masked characters, and 'Confirm password\*' with masked characters. At the bottom right is a blue button labeled 'Accept Invitation'.

Email\*

alex@company.com

Password\*

.....

Remember me

Continue

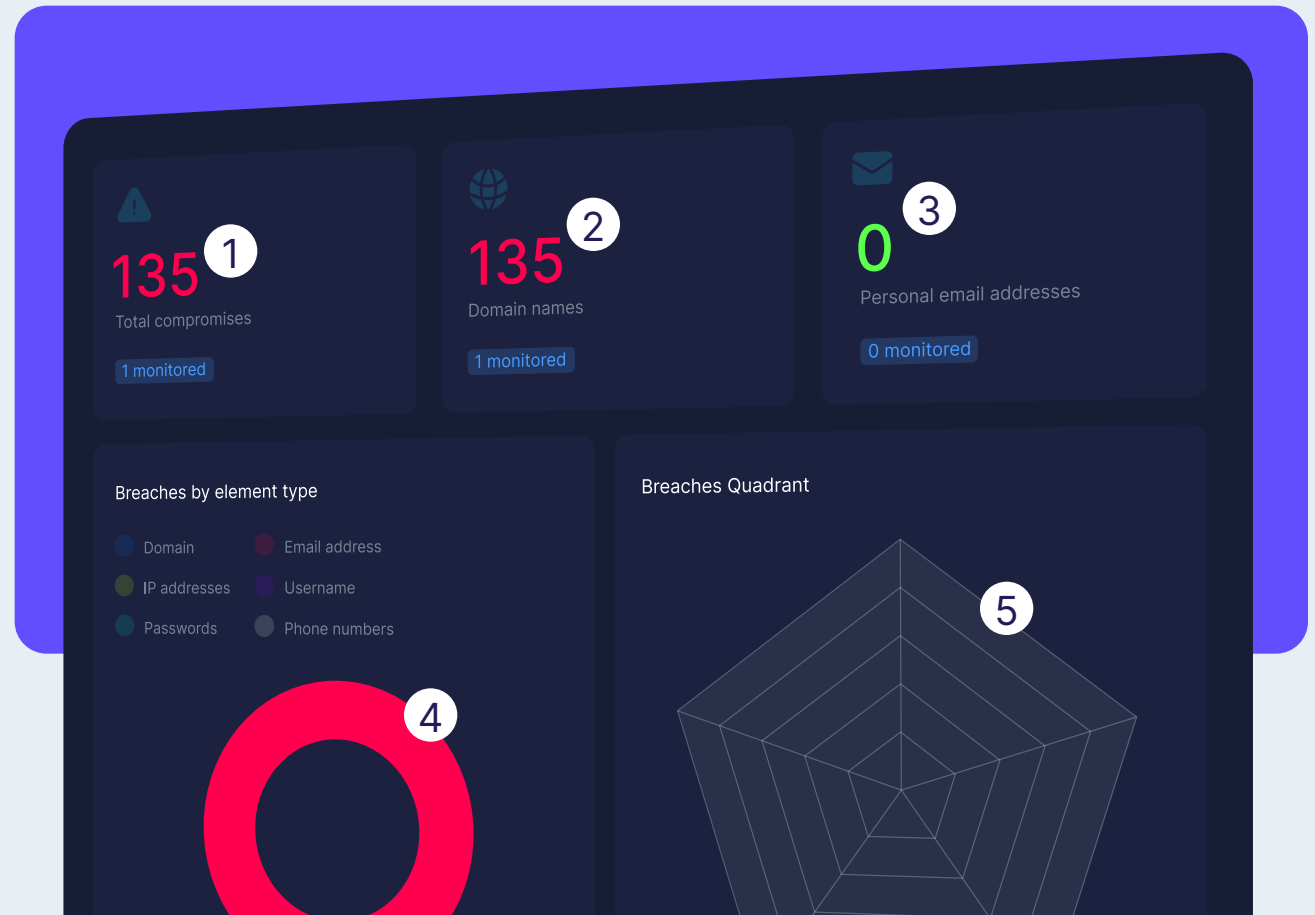
## Logging in to the platform

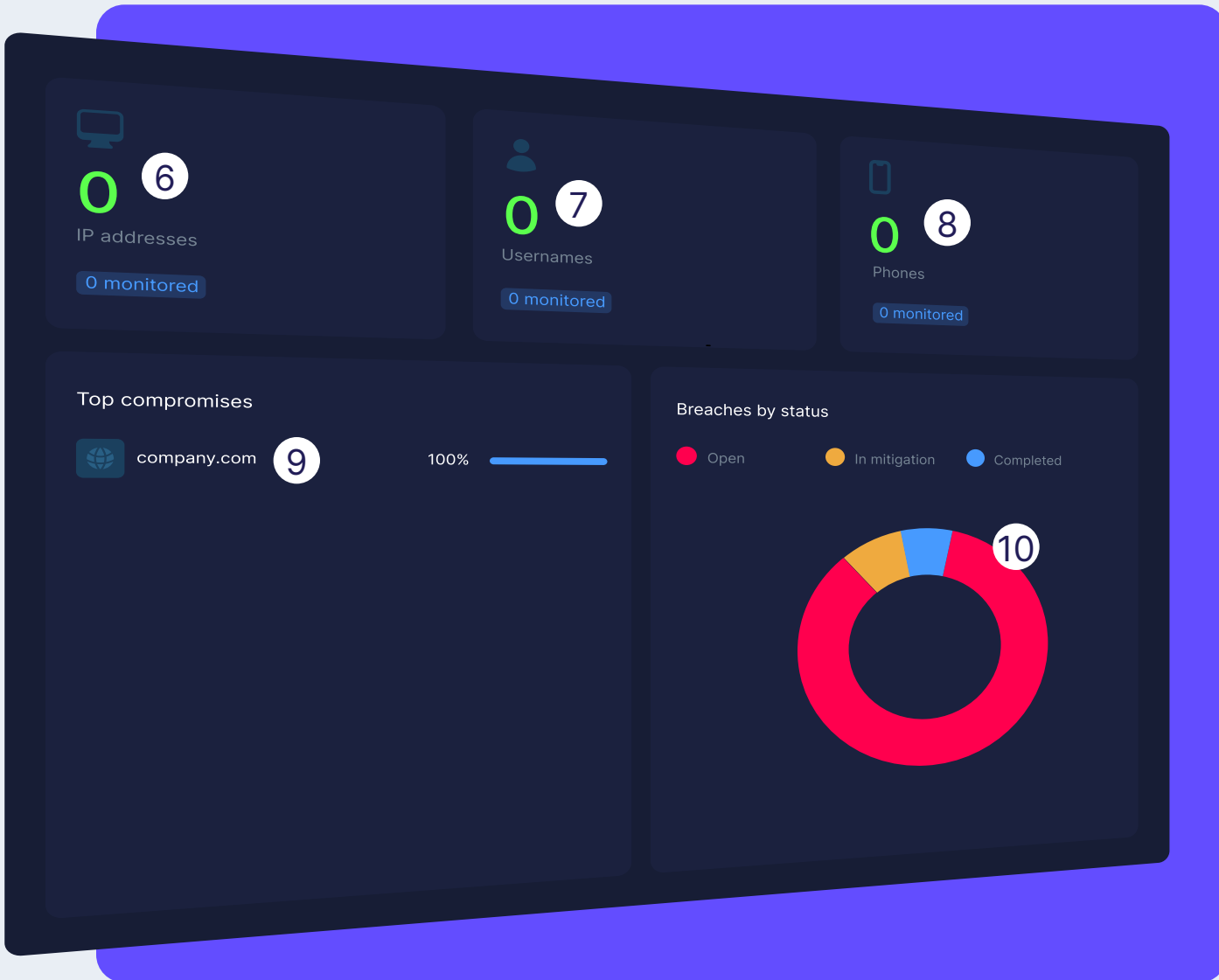
Click [Sign In](#) to be taken to the login page and enter the email address to which you received the invitation link, and the password set in the previous step. You can tick the [Remember me](#) check box to save entering your details next time you login.

# Navigating the dashboard

Once you're logged in you will be presented with your dashboard that contains details of any breaches found against your monitored asset.

- 1 Total breaches found, totalled from all monitored assets
- 2 Breaches found against monitored domains
- 3 Breaches found against monitored personal domains
- 4 Breaches by asset type
- 5 Quadrant of breaches by asset type



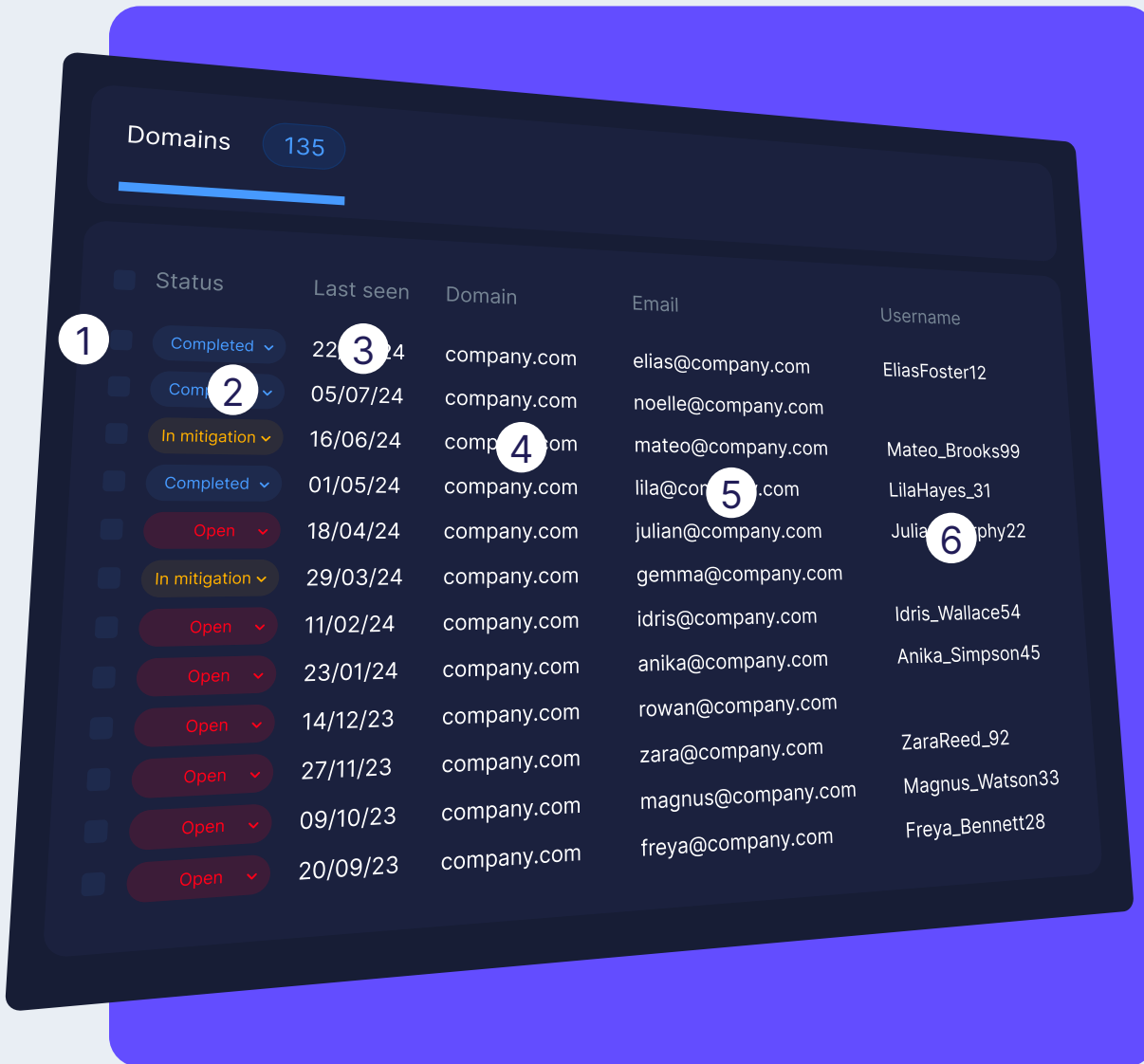


- 6 Breaches found against monitored IP addresses
- 7 Breaches found against monitored usernames
- 8 Breaches found against monitored phone numbers
- 9 Top assets breached
- 10 Breaches by mitigation status

# Identified breaches

Below the dashboard is then a breakdown listing all of the breaches and key information contained within the identified breach.

- 1 Multiple breach selection for bulk mitigation status changes
- 2 Status of the mitigation
- 3 When the breach was last seen on the dark web
- 4 The domain that was breached
- 5 If an email was in the breach it will show here
- 6 If a username was in the breach it will show here



Status	Last seen	Domain	Email	Username
<input type="checkbox"/> Completed	22/07/24	company.com	elias@company.com	EliasFoster12
<input type="checkbox"/> Completed	05/07/24	company.com	noelle@company.com	
<input type="checkbox"/> In mitigation	16/06/24	company.com	mateo@company.com	Mateo_Brooks99
<input type="checkbox"/> Completed	01/05/24	company.com	lila@company.com	LilaHayes_31
<input type="checkbox"/> Open	18/04/24	company.com	julian@company.com	JuliaMophy22
<input type="checkbox"/> In mitigation	29/03/24	company.com	emma@company.com	
<input type="checkbox"/> Open	11/02/24	company.com	idris@company.com	Idris_Wallace54
<input type="checkbox"/> Open	23/01/24	company.com	anika@company.com	Anika_Simpson45
<input type="checkbox"/> Open	14/12/23	company.com	rowan@company.com	
<input type="checkbox"/> Open	27/11/23	company.com	zara@company.com	ZaraReed_92
<input type="checkbox"/> Open	09/10/23	company.com	magnus@company.com	Magnus_Watson33
<input type="checkbox"/> Open	20/09/23	company.com	freya@company.com	Freya_Bennett28

- 7 If a password was in the breach it will show here
- 8 Name contained within the breach
- 9 Filter and export options
- 10 The breached database your data was contained in
- 11 Where in the dark web your data was found

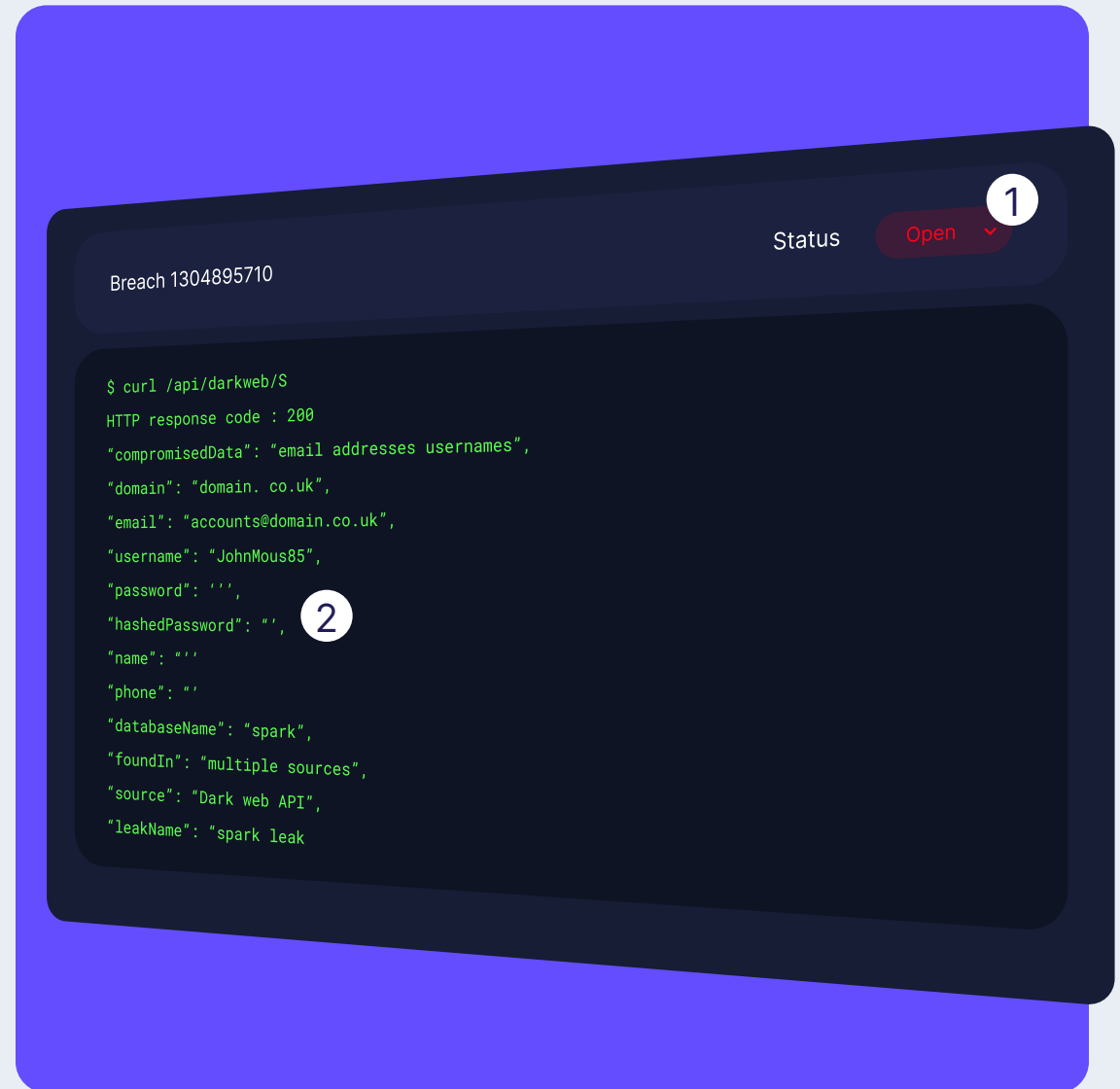
The screenshot shows a dark-themed web interface for analyzing data breaches. At the top right, there is a search bar and an 'Export to CSV' button. The main content is a table with five columns: Password, Name, Database name, Source, and Source. The table lists various departments and their associated databases and sources. Numbered callouts (7-11) point to specific elements: 7 points to the Password column header, 8 to the Marketing department name, 9 to the Export to CSV button, 10 to the Quantum Trans database name, and 11 to the Dark Web API source for Pioneer Media.

7 Password	Name	Database name	Source	Source
*****	Marketing 8	Vertex Digital	multiple sources	Dark Web API
*****		Nimbus Analytics	multiple sources	Dark Web API
*****	Human Resources	Quantum Trans 10	multiple sources	Dark Web API
*****		Aether Security	multiple sources	Dark Web API
*****	Customer Support	Pioneer Media	multiple sources 11	Dark Web API
*****	Finance	Zenith Financial	multiple sources	Dark Web API
*****		Stellar Software	multiple sources	Dark Web API
*****		TerraNova	multiple sources	Dark Web API
*****		FusionWave	multiple sources	Dark Web API
*****		Orion Ventures	multiple sources	Dark Web API
*****	Legal Department	Lunar Logistics	multiple sources	Dark Web API
*****	Data Science	Arcadia BioTech	multiple sources	Dark Web API

# Understanding your breaches

From the list of breaches on the dashboard, when you click on one of the breaches it opens a new panel with more information of the breach than was listed on the dashboard, with options then to manage the breach and obtain further advice.

- 1 A status you can change for you to track your mitigation of this breach. Changing this will expand further information of mitigation advice
- 2 Depending on the type of breach, this area will either show the cURL or an image demonstrating the breach information





Description **3**

This breach information for emma@company.com has been scraped from Dark Web APIs. It was last seen on 2024-07-23 13:17:51.819493 on multiple sources, and is commonly identified as the lofox.com database. Due to the source of this data. The data compromised includes: email addresses, password hashes, full names, phone numbers, usernames

## Compromised data

Email addresses

Password hashes

Full names

Phone numbers

Usernames

**4**

## ID

13480572346

**5**

## Last seen

04/09/24

**10**

## Domain

company.com

**6**

## Email

emma@company.com

**11**

## Username

emma

**7**

## Password/hash

.....

**12**

## Name

Emma Stone

**8**

## Leak name

LoFox Leak

**13**

## Database name

LoFox.com

**9**

## Found in

Multiple sources

**14**

## Source

Dark Web API

## Victim domain

LoFox.com

**15**

## Distribution type

API redistribution

- 3** Detailed description of the breach
- 4** Categorized data that was breached
- 5** The ID our systems have given the breach
- 6** The impacted domain
- 7** The username contained in the breach
- 8** The person's or department's name contained in the breach
- 9** Which database was breached
- 10** When the breach was last seen on the dark web
- 11** The email address contained in the breach
- 12** The password contained in the breach
- 13** The name of the leak in which the data was contained within
- 14** Where on the dark web it was found
- 15** The domain name of the leak victim

# Mitigation options and tracking

When you change the status of the breach to In mitigation you are presented with some suggested mitigation steps that you can take to protect your systems and data from compromise.

Clicking into each one expands the information, and you can set a status against each one for you to track progress.

## Mitigation steps

### Immediate next steps

Not started ▾

These are the immediate next steps you should take to mitigate the risk of this vulnerability

### Request data removal

Not started ▾

These are the steps you should take to request the removal of the data from the breached website

### Cease and desist letter

Not started ▾

A cease and desist letter is a powerful and simple way to protect one's rights

### Obtain a court order

Not started ▾

Obtain a court order to remove content

### **Immediate next steps**

In here you'll find practical steps to take to mitigate the risk caused by this breach, we recommend these are carried out at a minimum.

### **Request data removal**

These are the steps you should take to request the removal of the data from the breached website. In here you'll also find a example letter template that you can use to help you get started.

### **Cease and desist letter**

If you have not been able to have your data removed following the data removal step above, a cease-and-desist letter is a powerful and simple way to protect one's rights. In here you'll also find a example letter template that you can use to help you get started.

### **Obtain a court order**

Failing an attempt at using the steps above to mitigate, a court order could be another step you take.

# Account management

You can update your personal details, contact information and change your password all within Account Settings.

## Updating your account information

Click on your initials in the top right corner of the screen, then select Account Information. In this section, you will be able to update your name, contact information and language preference.

### Account information

Update your account information

First name

Last name

### Contact information

Phone

Email address

We'll never share your email with anyone else

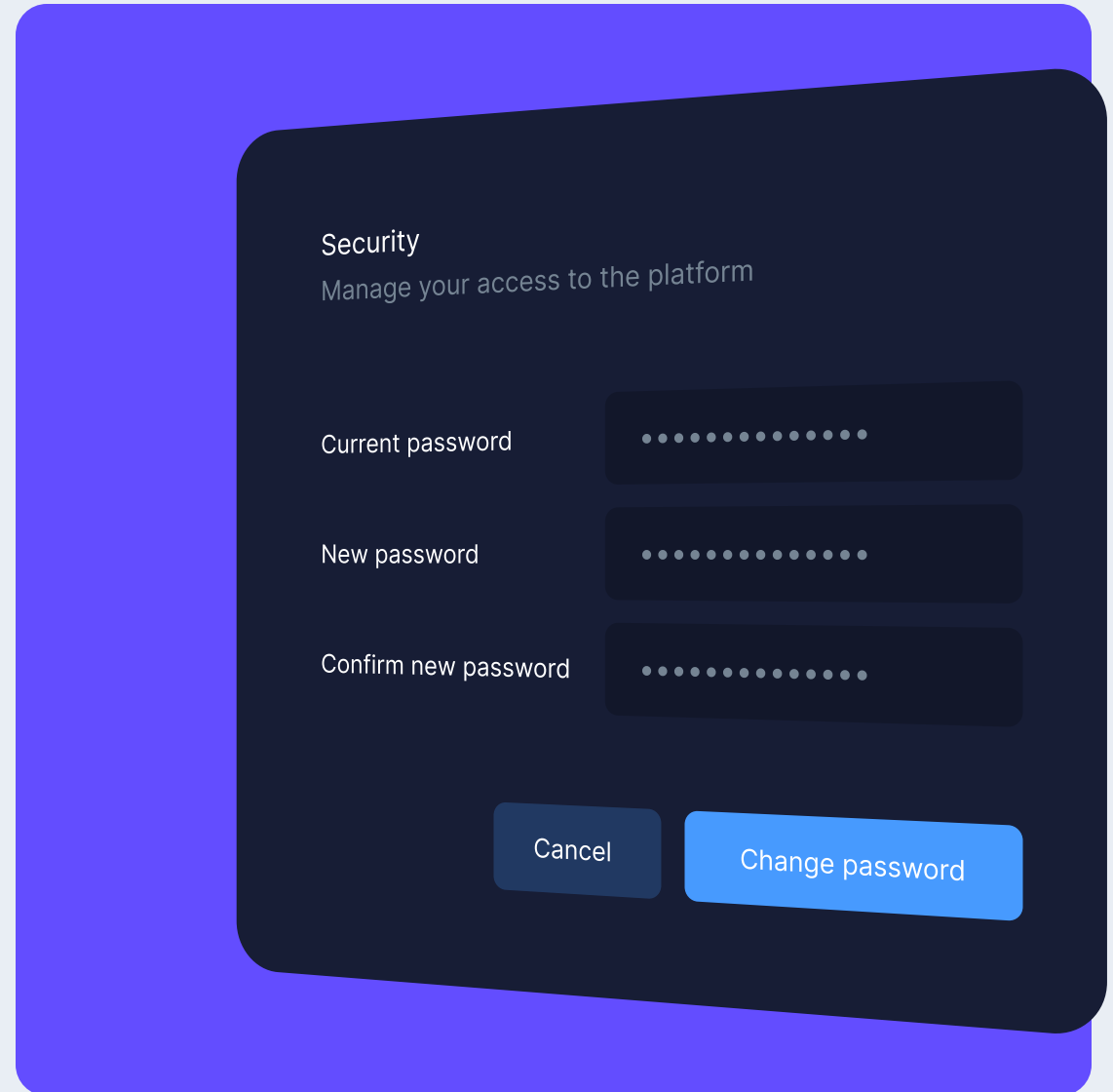
Language

## Changing your password

Click on your initials in the top right corner of the screen, then select [Security](#).

Next select [Reset Password](#) .

Enter the current password, and your desired new password (twice for confirmation) and select [Change password](#).



The screenshot displays a dark-themed user interface for the 'Security' section. At the top, the title 'Security' is followed by the subtitle 'Manage your access to the platform'. Below this, there are three input fields, each with a label and a masked password field (represented by dots): 'Current password', 'New password', and 'Confirm new password'. At the bottom of the form, there are two buttons: a dark blue 'Cancel' button and a bright blue 'Change password' button.

# Setting up two-factor authentication

Recommended

Within the Security area of Account settings (see changing your password steps on how to navigate there), you can setup two-factor authentication to further protect your access to our portal. We strongly recommend this for added security, using either the Google or Microsoft Authenticator apps.

## Step one

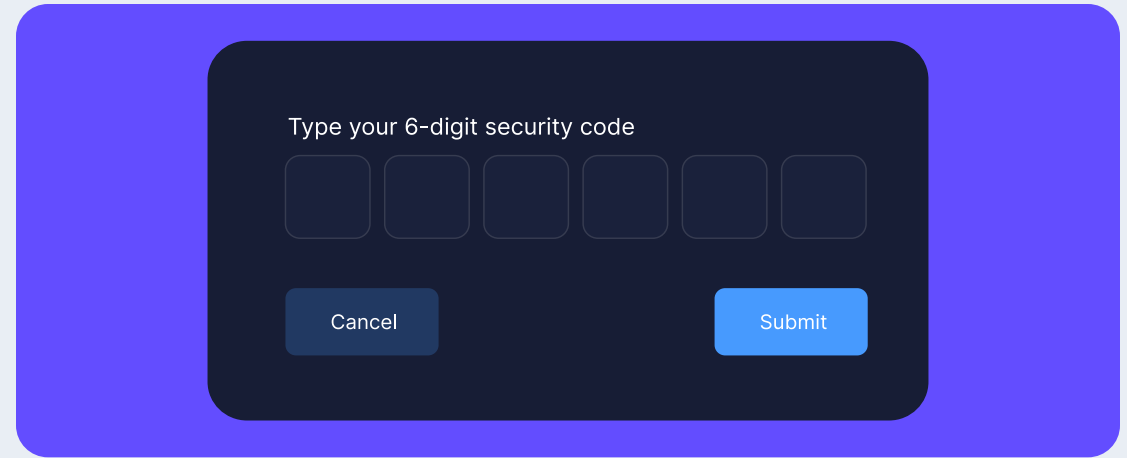
Click Enable, this will open a new window with a QR code to scan into your chosen authenticator app.

Use the Google Authenticator or Microsoft Authenticator app, scan the QR code. It will generate a 6-digit code for you to enter below



## Step two

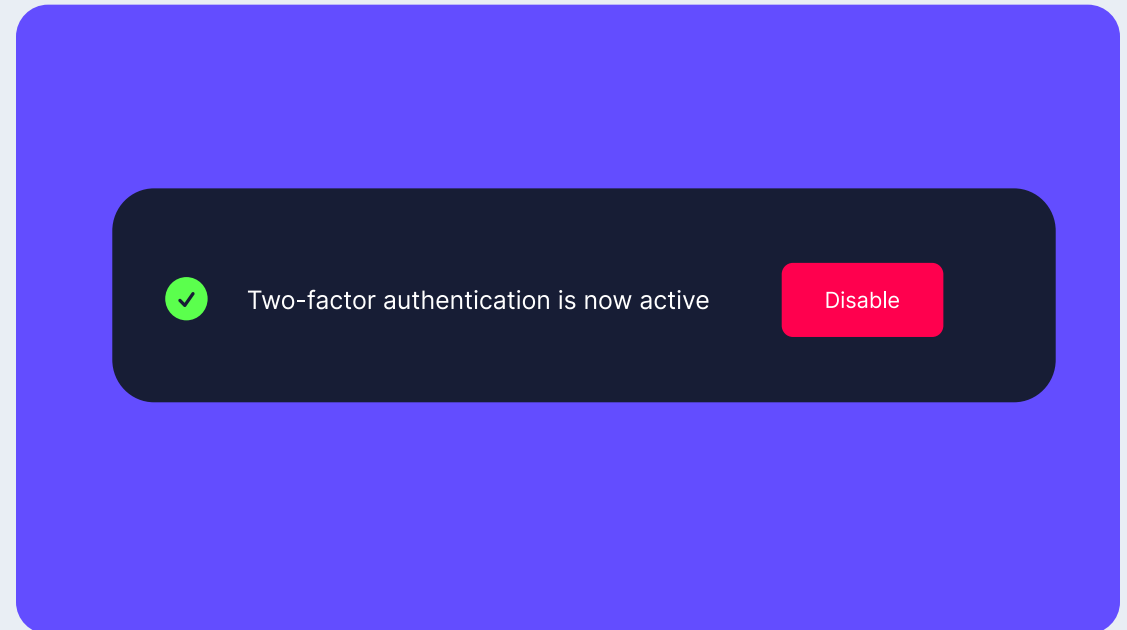
Once you have scanned the QR code, enter the current six (6) digit code to finish setting up two-factor authentication.



## Step three

The six (6) digit code will appear appear in your authenticator app as Onecom CyberProtect: [your email address].

You can later remove two-factor authentication by clicking Disable.



For further support, visit  
[onecomcyberprotect.com/support](https://onecomcyberprotect.com/support)

