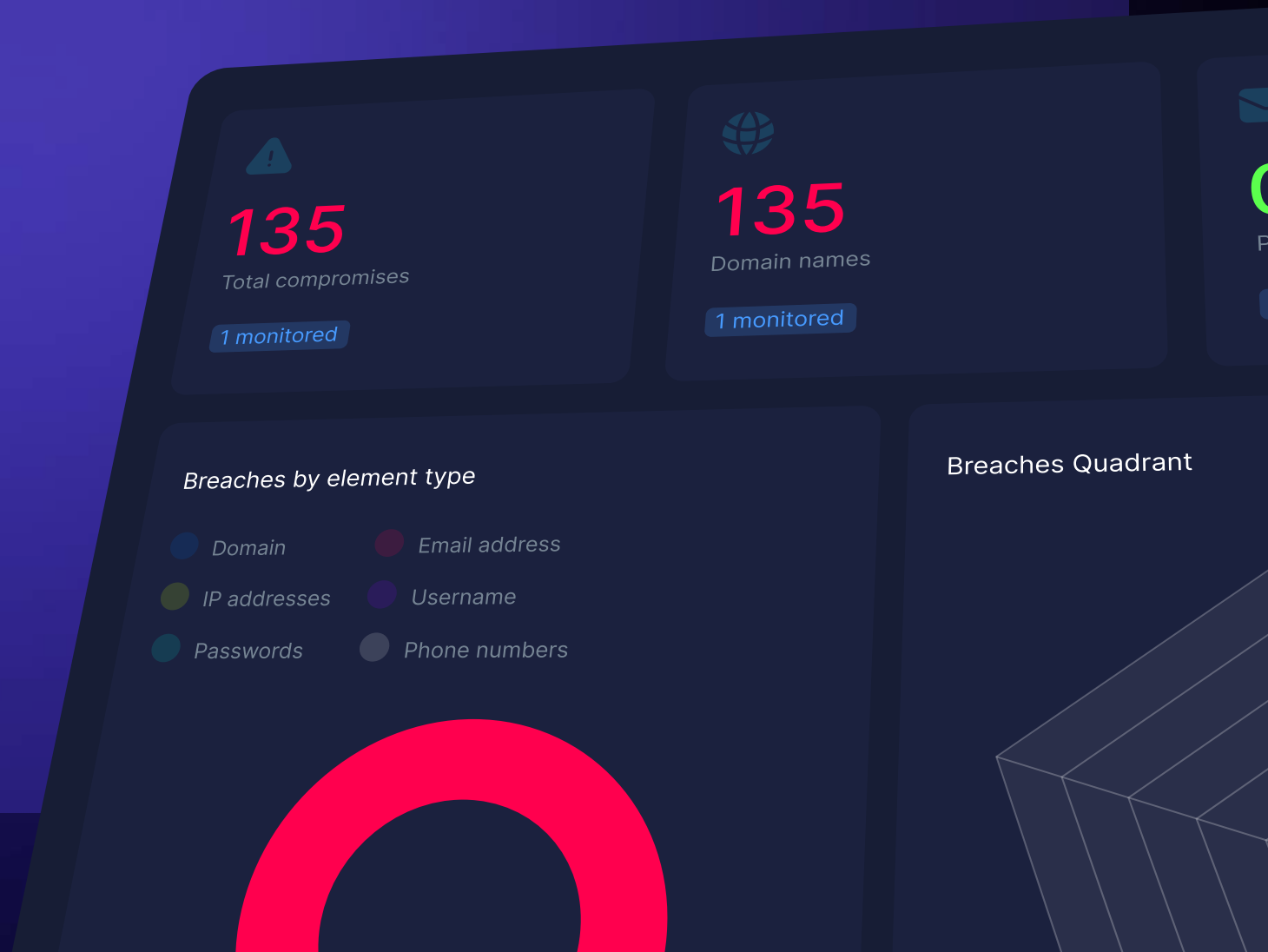
onecom
CyberProtect

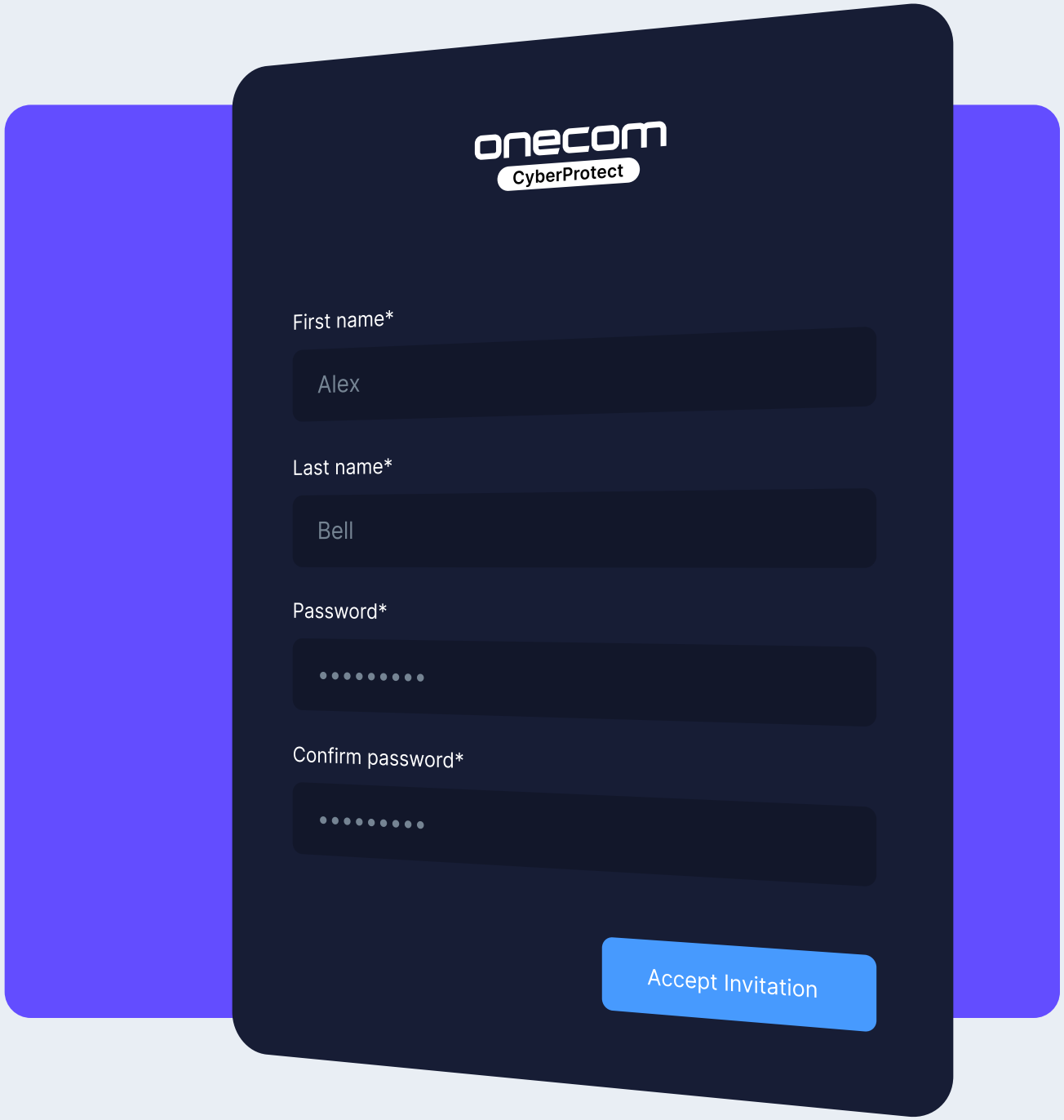
User Guide

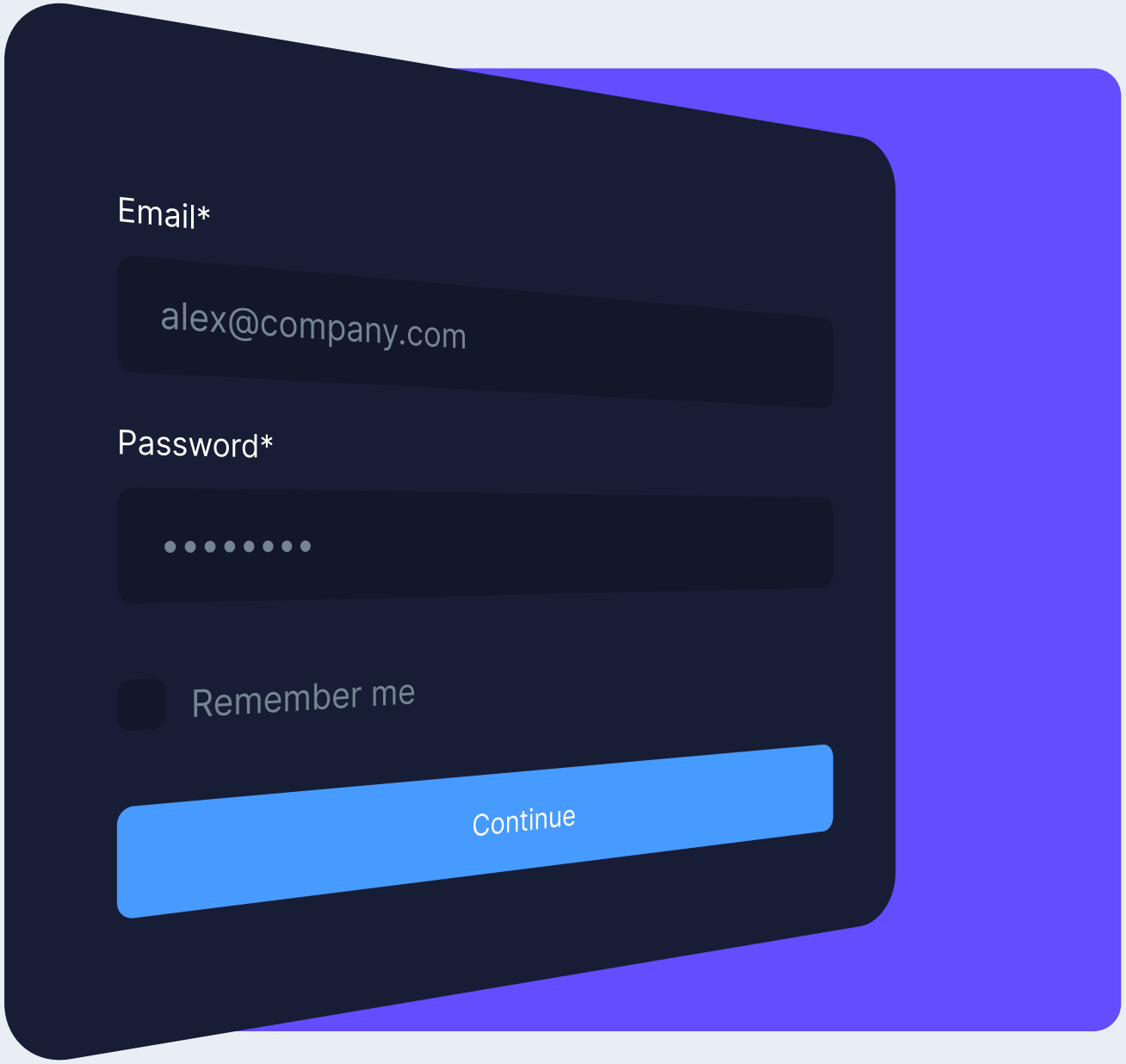
Mastering Onecom Cyber Protect's features and functionalities



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.





Logging in to the platform

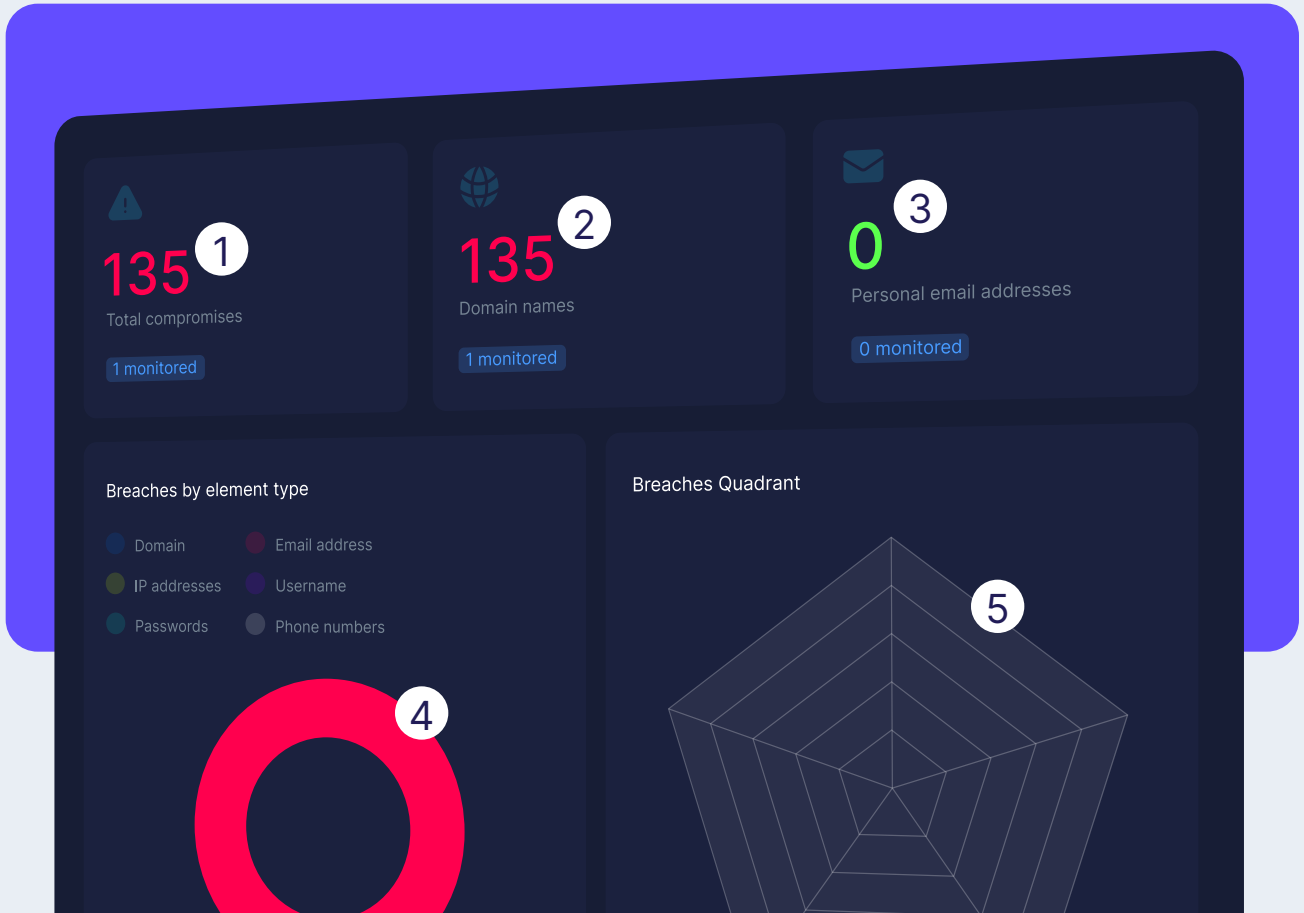
Click Sign In to be taken to the login page and enter the email address to which you received the invitation link, and the password set in the previous step. You can tick the Remember me check box to save entering your details next time you login.

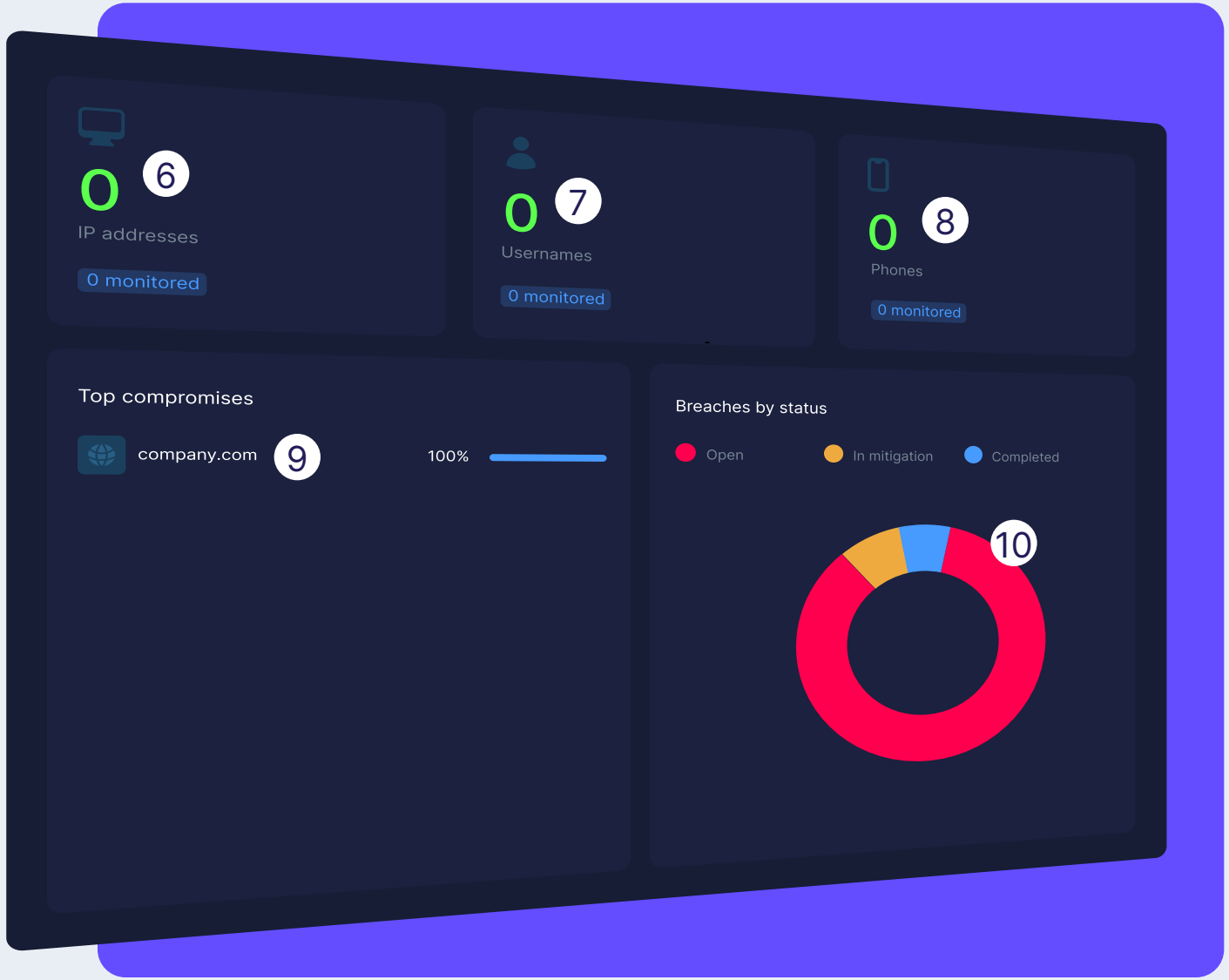
Dark Web Monitoring

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





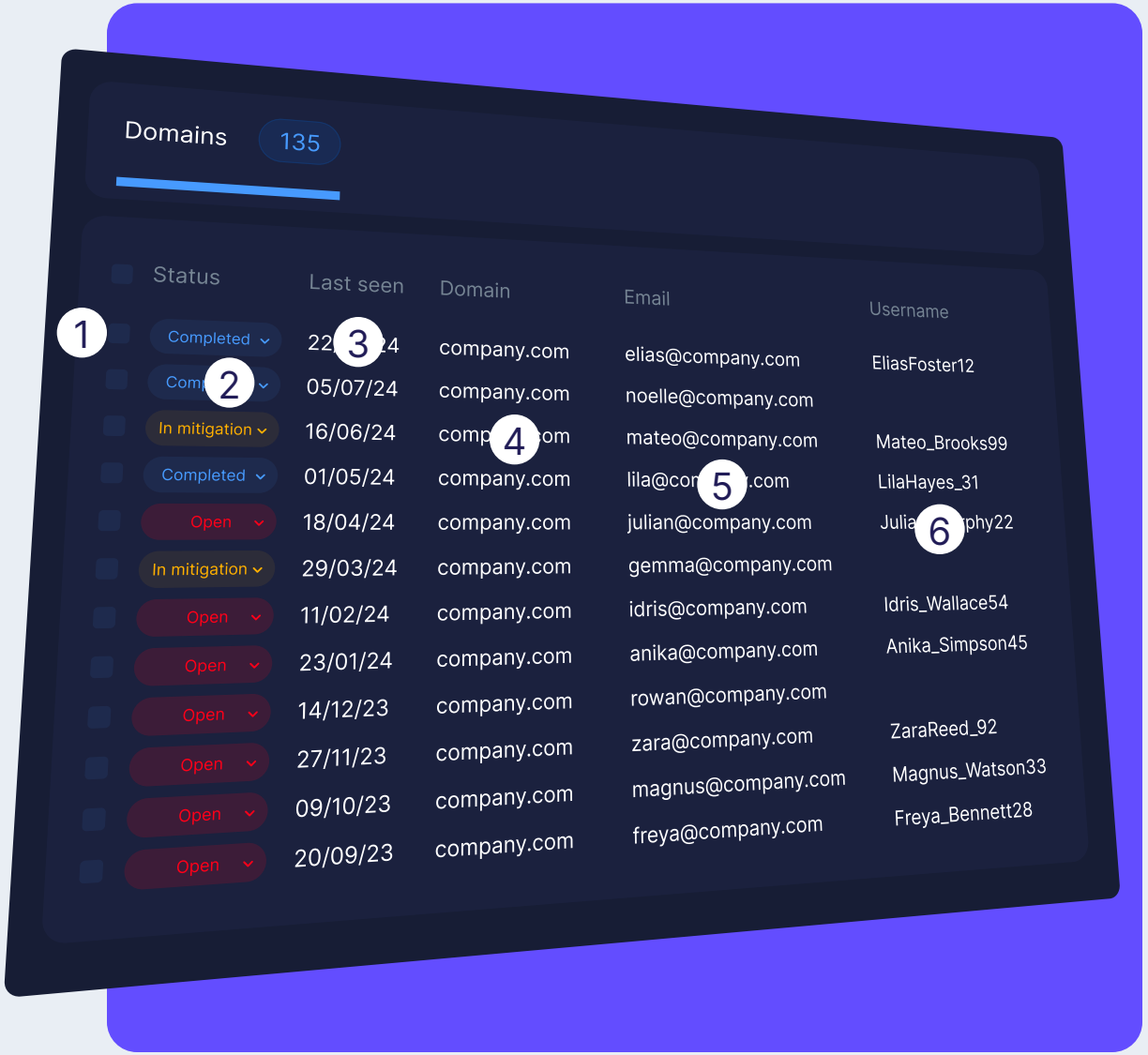
6 Breaches found against monitored IP addresses

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

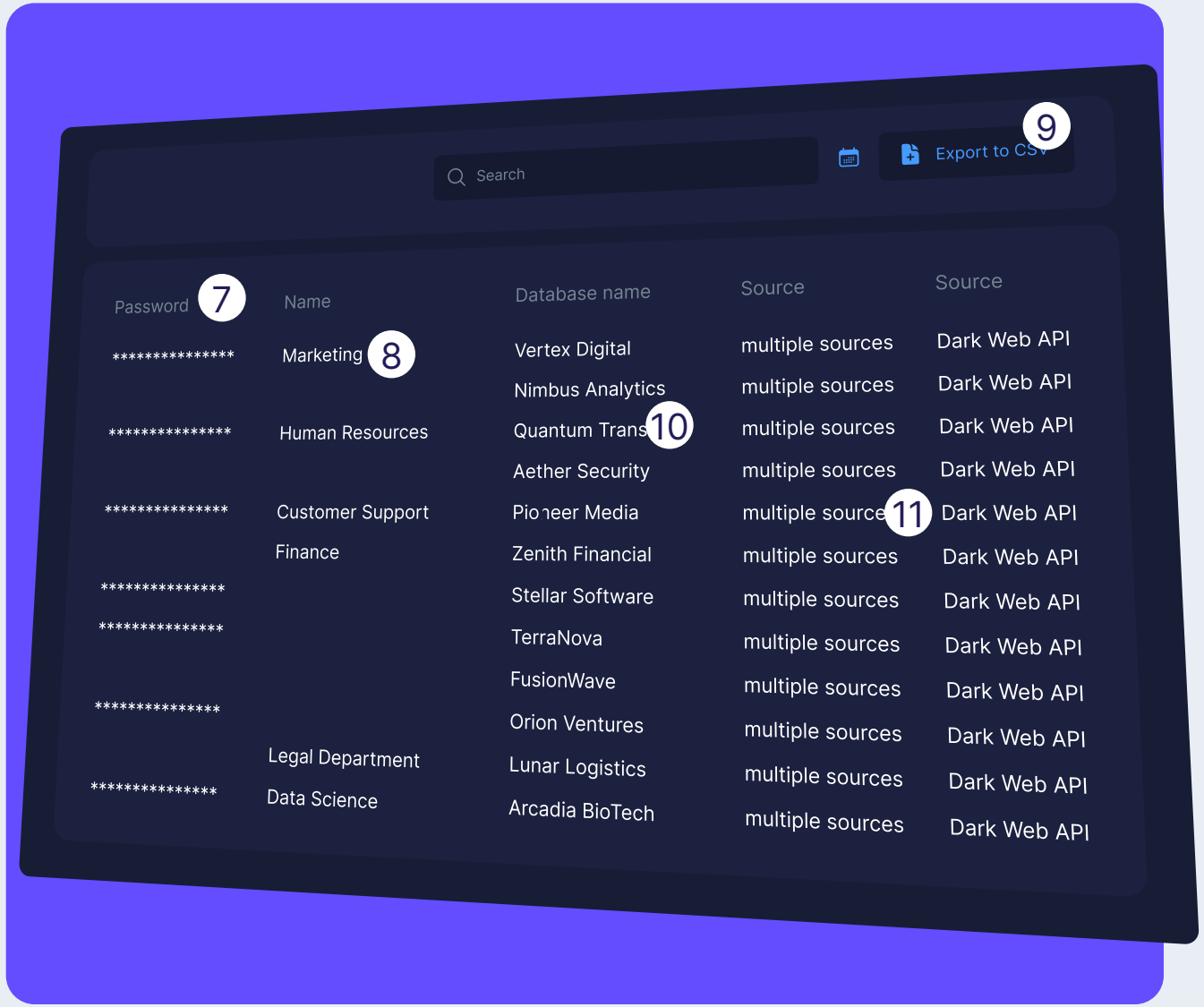
7 If a password was in the breach it will show here

8 Name contained within the breach

9 Filter and export options

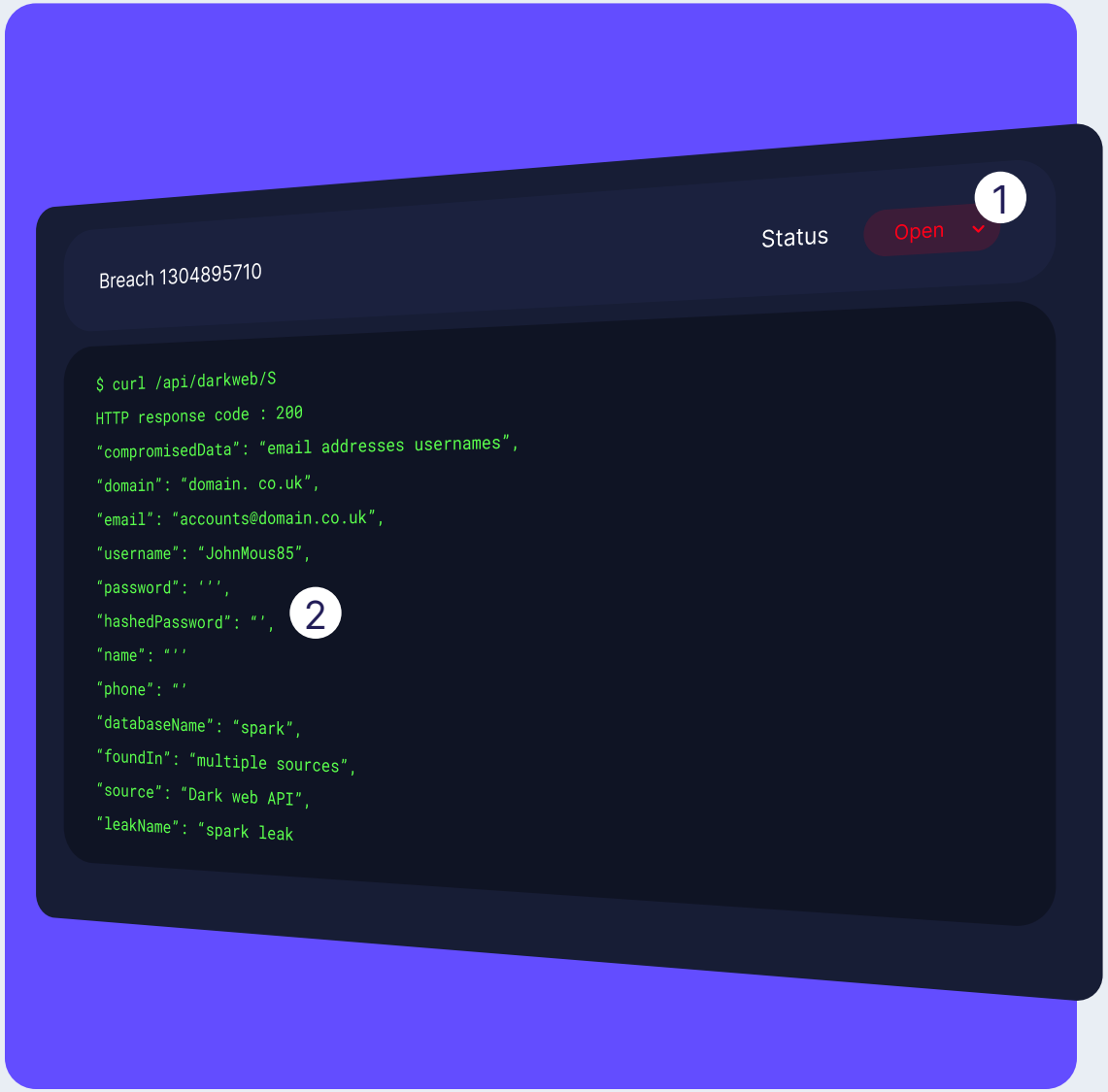
10 The breached database your data was contained in

11 Where in the dark web your data was found



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

3 Detailed description of the breach

4 Categorised 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

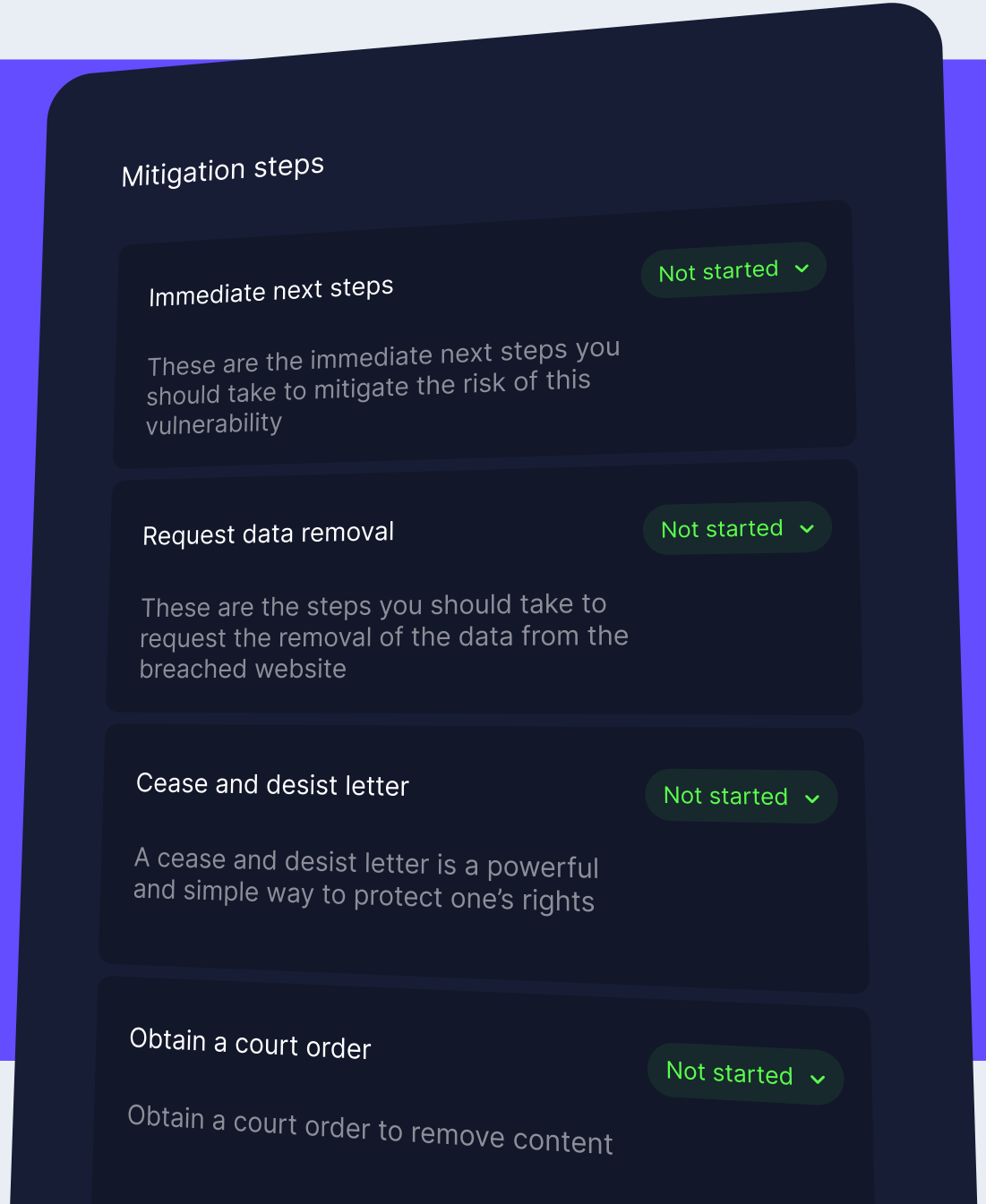
14 Where on the dark web it was found

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.



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.

ID Guard

Navigating the dashboard

1. Breakdown of impersonation threats by your mitigation status
2. Breakdown of number of threats by Fuzzer

Below the dashboard is then a breakdown listing all of the potential impersonation threats and key information contained within the identified entry

3 Your mitigation status

4 When the threat was found

5 The domain that is being impersonated

6 The identified impersonation threat

7 The Perceptual Hash, how close it is to the original

8 The type of Fuzzer

9 Number of DNS NS entries

10 Number of Mail Exchange entries

11 Number of IP address entries

3 Status	4 Found date	5 Domain	6 Threat	7 Phash	8 Fuzzer	9 DNS NS	10 Mail Exchange	11 IPV4
Open	22/08/24	company.com	company.dk	17%	TLD swap	1	1	1
Open	05/07/24	company.com	cornpany.co.uk	17%	Replacement	1	1	0
In mitigation	16/06/24	company.com	company.es	17%	TLD swap	1	0	1
Completed	01/05/24	company.com	compny.co.uk	17%	Omission	1	0	1
Open	18/04/24	company.com	be.company.co.uk	17%	Subdomain	1	1	0
In mitigation	29/03/24	company.com	company.det	17%	TLD swap	1	0	1

Types of Fuzzer threats

TLD Swap

Top-level domains in the domain name are swapped. Swapping top-level domains may have limited impact on domain security, and severity would depend on the context.

Dictionary

Dictionary-based fuzzing relies on predefined words, making it less likely to be a significant security concern unless used creatively.

Character swap

Characters are added to the domain name. Adding extra characters to domain names is less likely to result in successful attacks unless users frequently mistype.

Vowel swap

Vowels in the domain name are swapped. This fuzzer targets vowel characters and may have limited impact unless specific user behaviour patterns are exploited.

Homoglyth

Similar looking characters are swapped in the domain name. Homoglyph attacks can be medium severity because they rely on visually similar characters from different scripts. These attacks may deceive users but require careful crafting.

Omission

Omission removes characters from domain names, which is less likely to result in successful attacks due to the need for specific user behaviour.

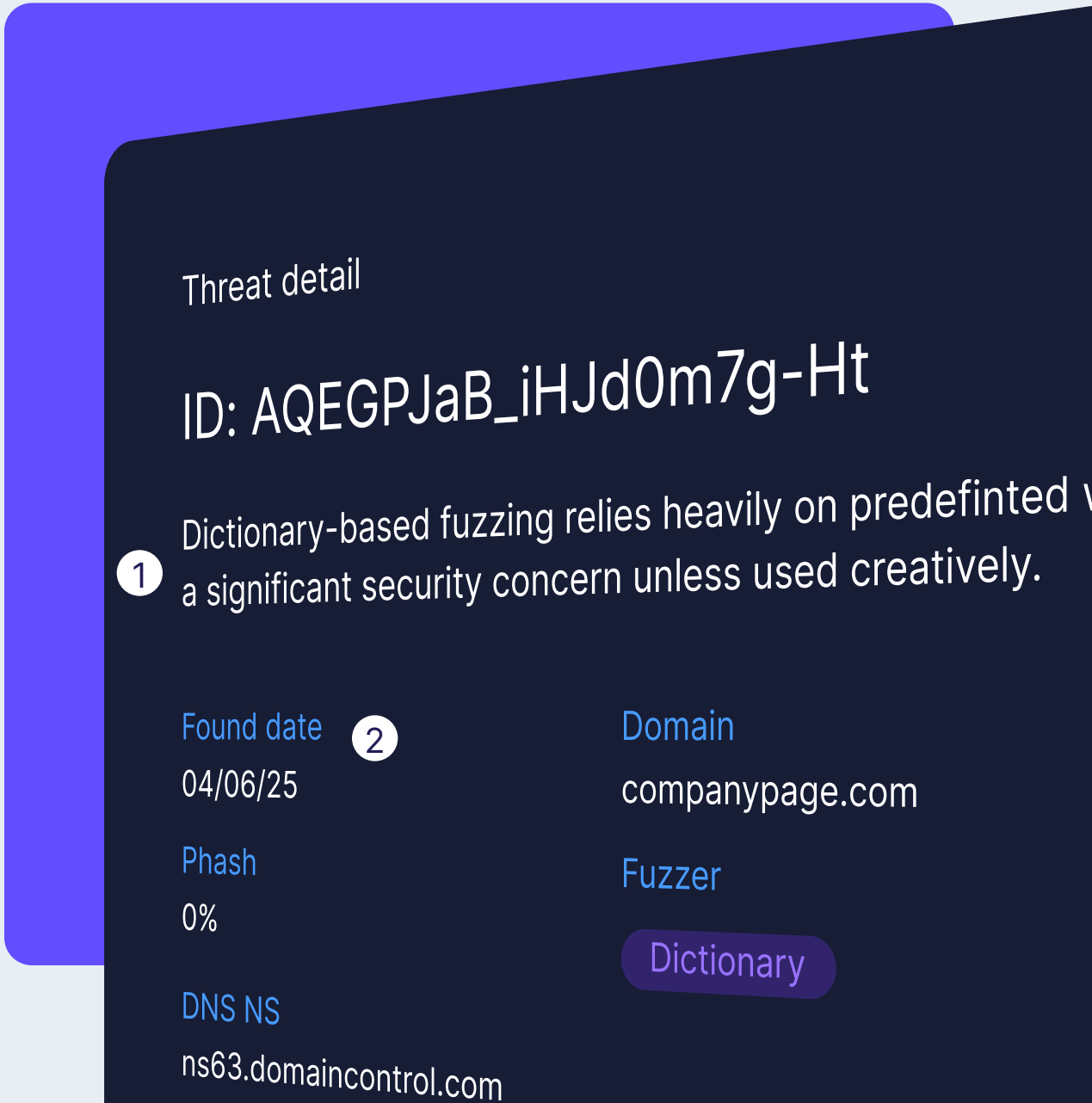
Insertion

Insertion adds characters within domain names, making it a lower severity fuzzer as it requires specific circumstances for successful attacks.

Understanding the Impersonation Threat

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

1. Detail about the type of Fuzzer used in this threat and the level of risk
2. When the threat was found



3 The Perceptual Hash, how close it is to the original

4 The registered DNS NS entry

5 The IPv4 address registered

6 The potential impersonating domain name

7 The type of Fuzzer

8 A status you can change to track your mitigation of the threat. Changing this will expand further information of mitigation advice

Mitigation options and tracking

When you change the status of the threat to In mitigation you are presented with some suggested mitigation steps that you can take to protect your business from potential impersonation attacks.

Respond to incidents quickly

Have a response plan ready for when a potentially harmful domain is detected. Include analysis of DNS logs and emails to find it users have been compromised. If users have been deceived, communicate openly about the incident, guide them on security measures, and assure them of steps taken.

Implement technical solutions

Use DNSSEC (Domain Name System Security Extensions) to ensure the domain's authenticity. Use Content Security Policies (CSP) to restrict where content can be loaded from, limiting the reach of phishing sites. Enable HSTS (HTTP Strict Transport Security) to ensure users connect to your site using HTTPS only.

Use trademark protections

Ensure you have trademarks in place for your brand and product names and keep monitoring domain registrars and take legal action against those infringing on your trademarks.

Partner with domain registries

Most domain registrars have an “abuse” contact email. Use it to report domains impersonating your brand. Establish a relationship with popular domain registrars and registries. Use this relationship to quickly act on malicious or suspicious domain registrations.

Register protective domains

Proactively register common misspellings or variations of your domain. Buy TLDs (.com, .net, .org, etc.) for your domain to prevent others from creating fake variations.

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

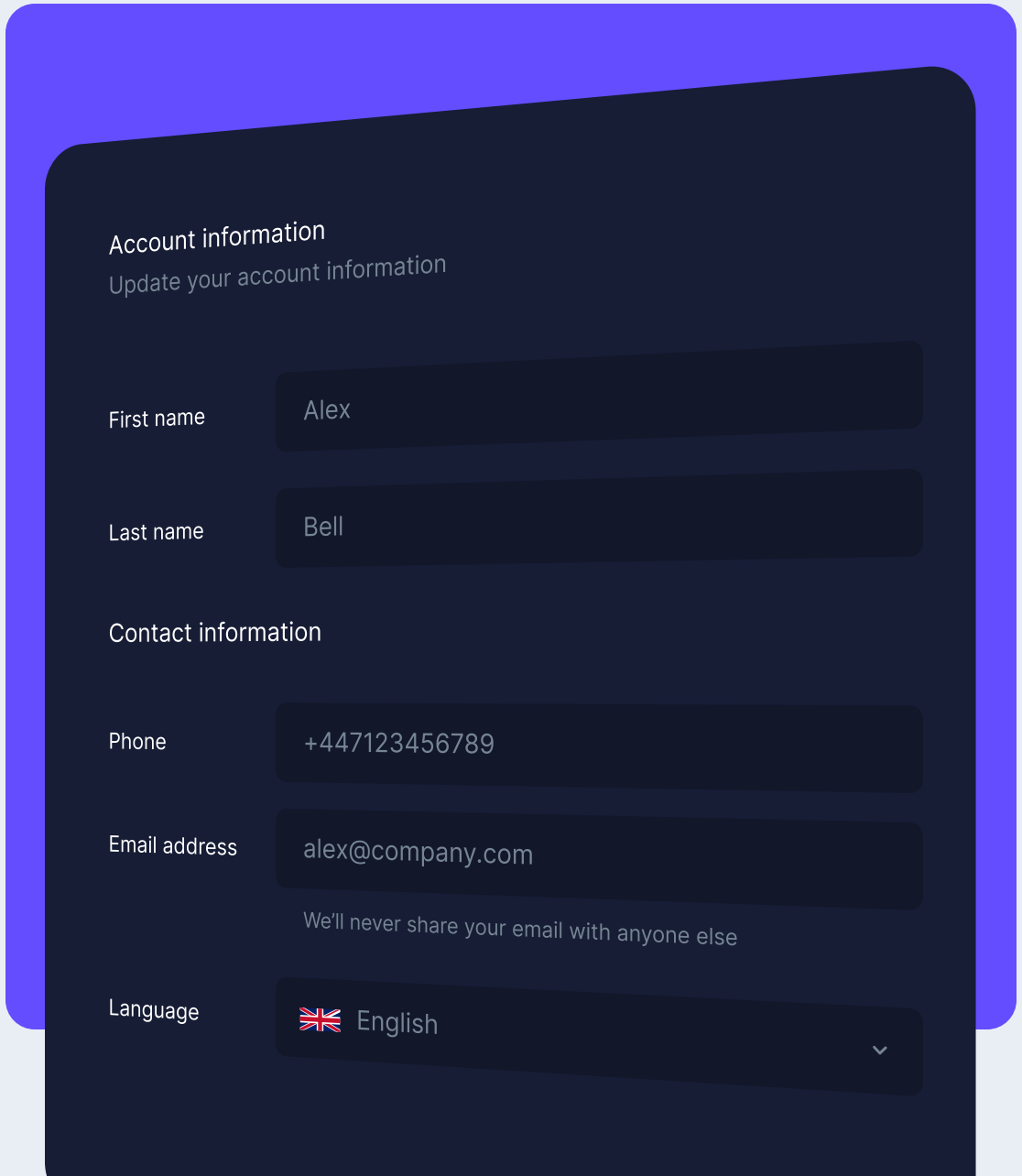
Account Management

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.

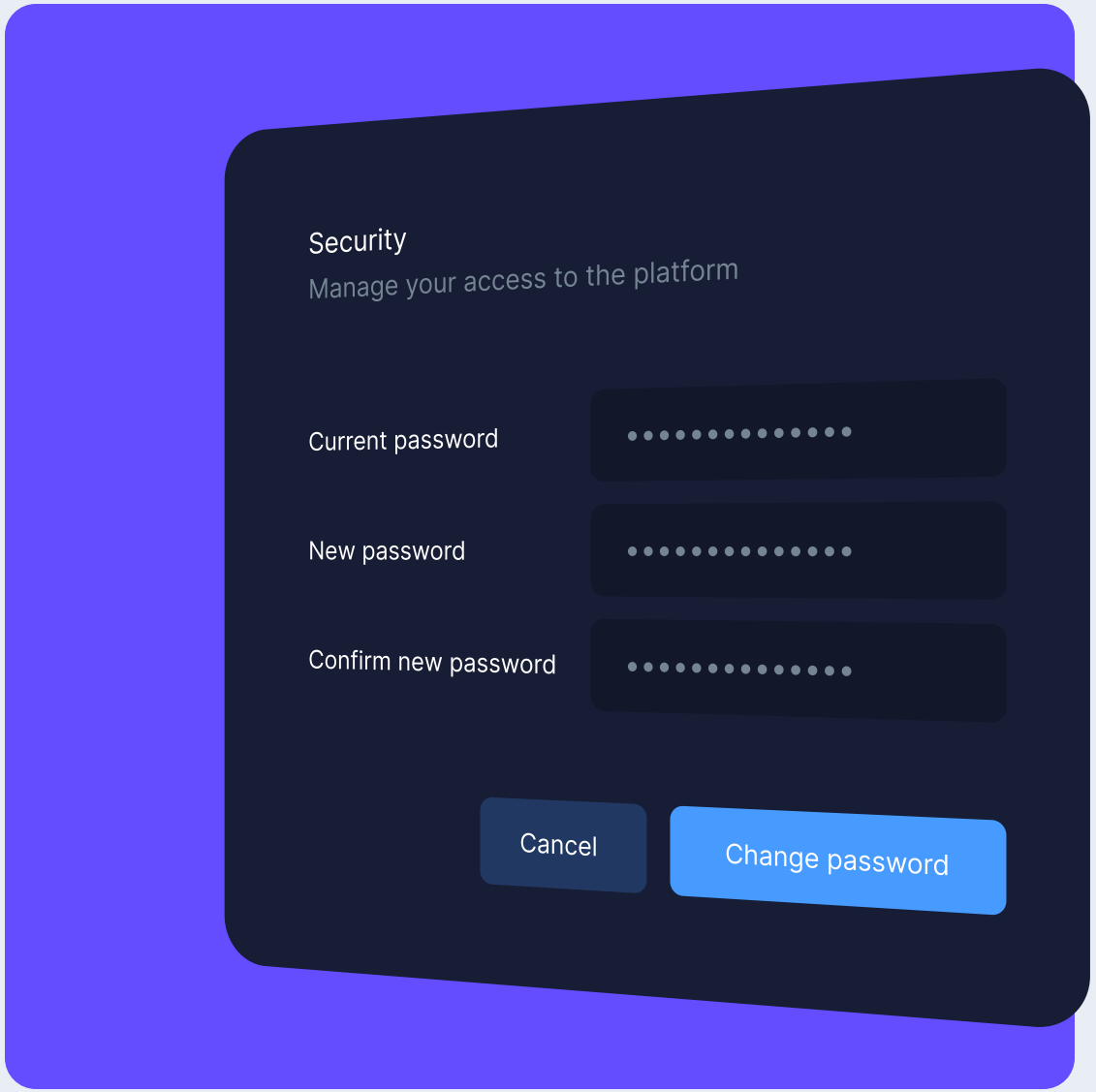


Changing your password

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.



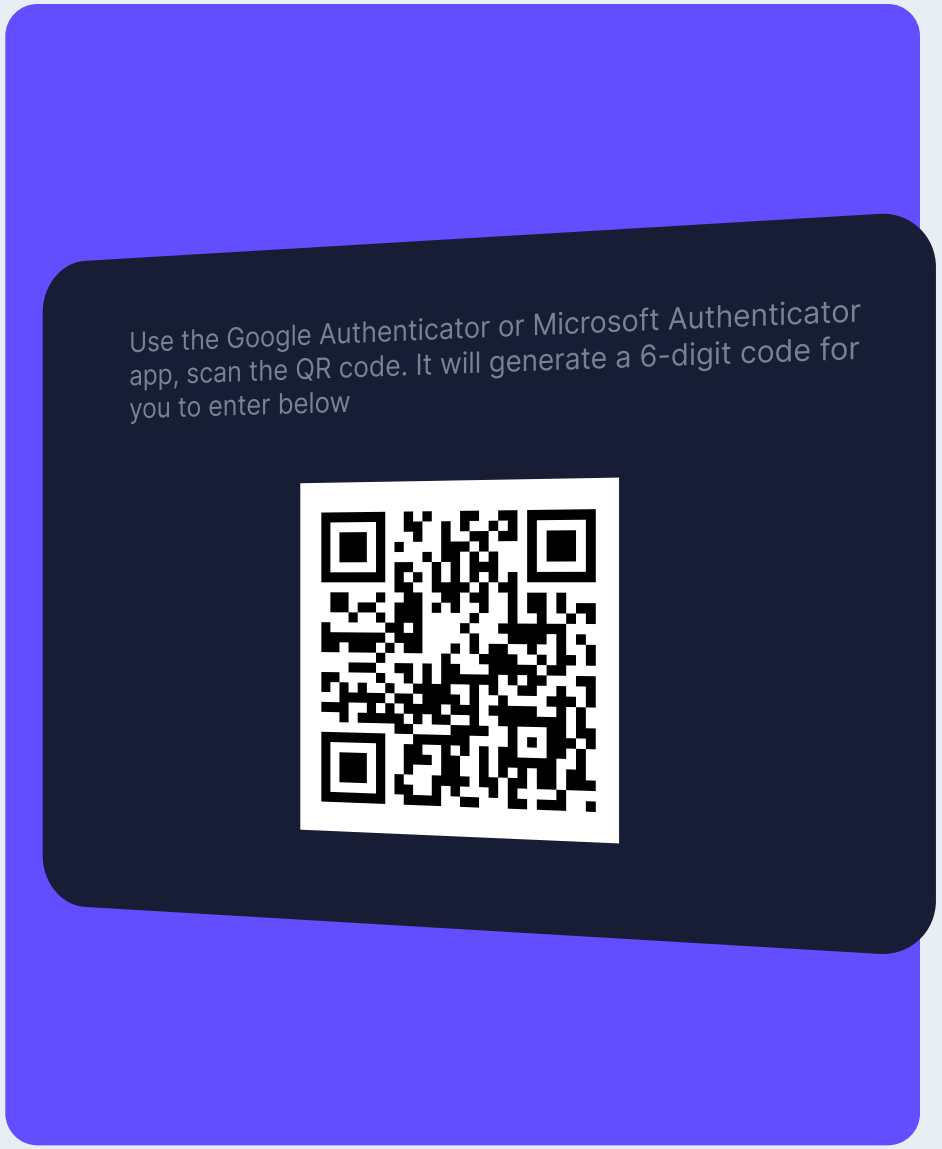
Setting up two-factor authentication

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.

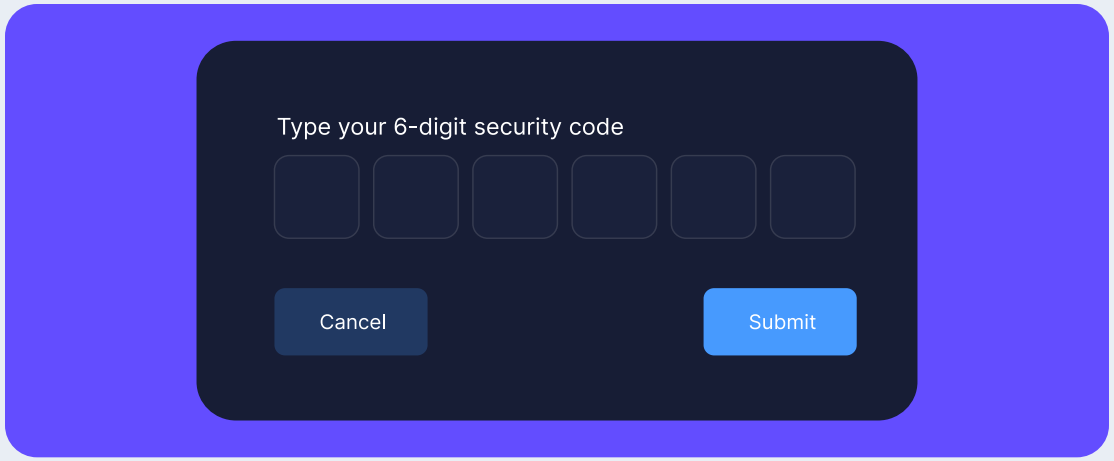
Step one

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



Step two

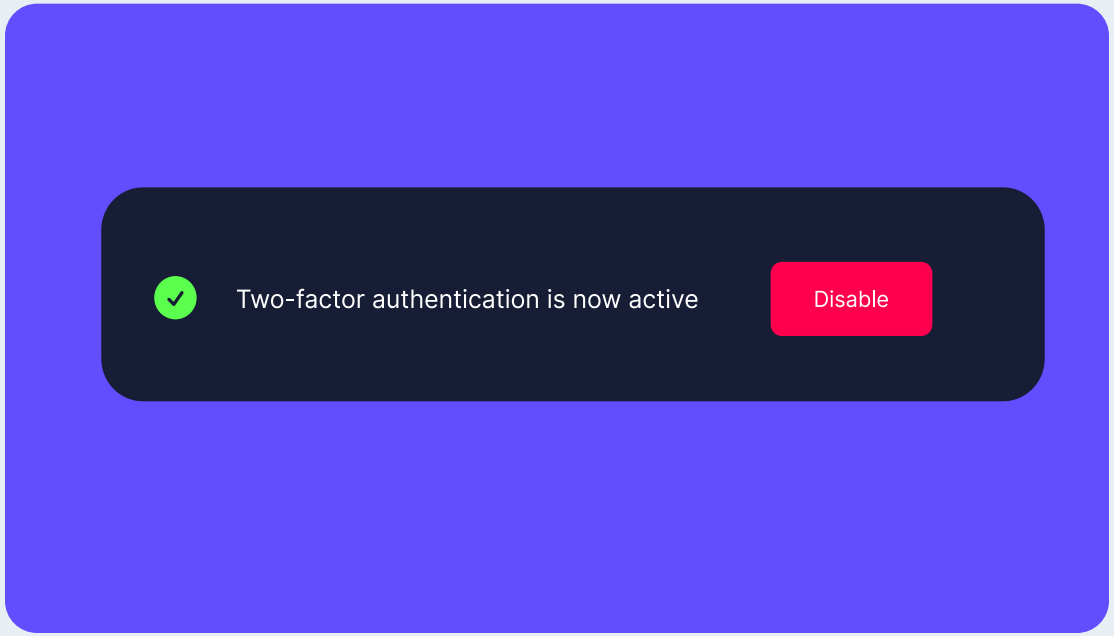
Once you have scanned the QR code, enter the current six (6) digit code to finish setting up two-factor authentication.



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

onecom
CyberProtect