CYBER INSURANCE

Online Guide for **Pen Protect**

Pen underwriting

Logging in to Pen Protect

Simply visit **penprotect.ai**

From here you can

- **Activate** your account on your first visit
- **Sign in** to your account

Pen Protect Guide

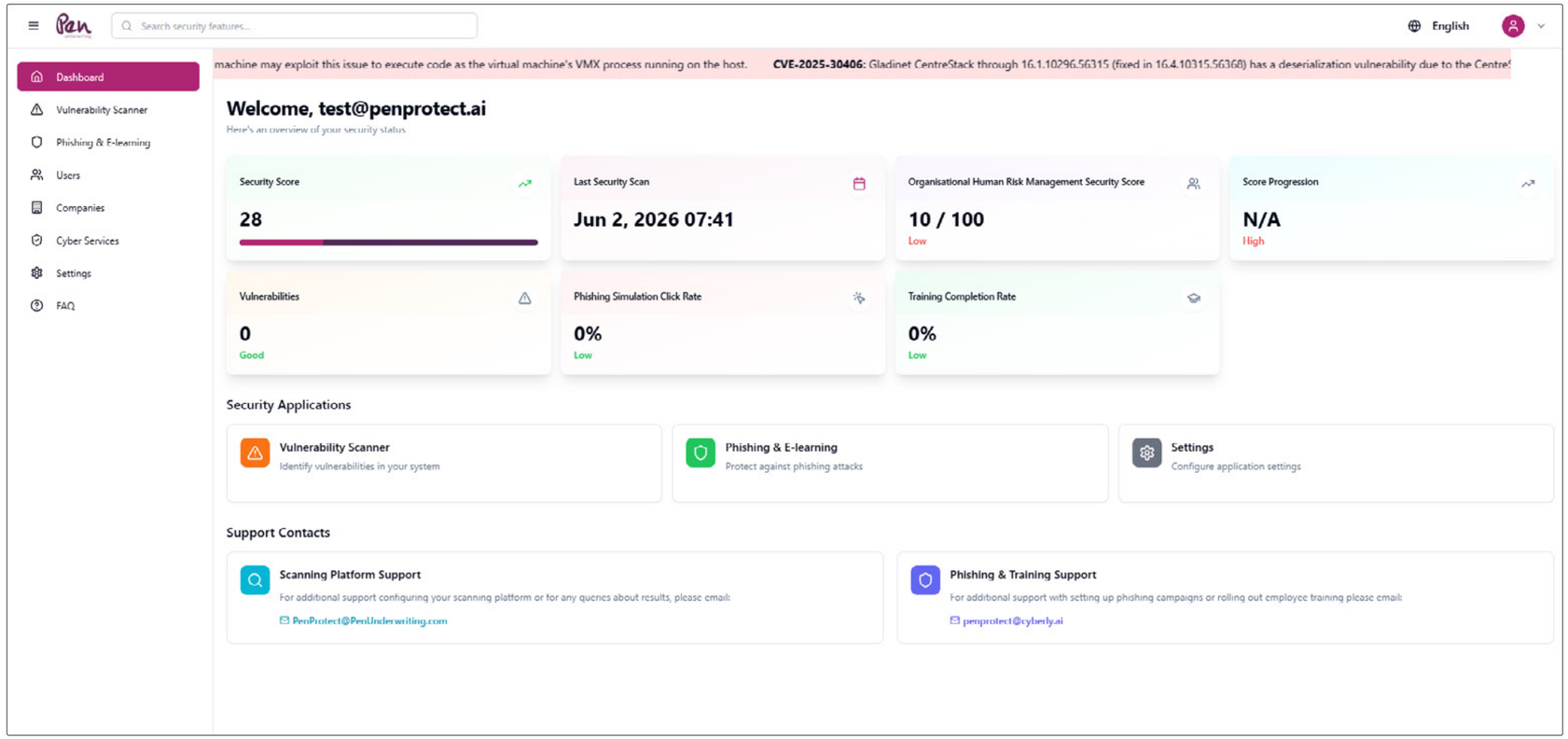
Your Dashboard

Here you'll find a summary of your vulnerability scan.

Your Vulnerabilities

As soon as you log in to Pen Protect, you'll see your organisation's

- overall security score
- total vulnerabilities
- recent scan history
- phishing simulation employee click rate
- employee training completion rate
- your overall human risk score



Pen Protect Guide

Your Pen Protect Menu

On the left-hand side of any Pen Protect page you can access your navigation menu.

Dashboard

This is your homepage, with tiles displaying some key vulnerability metrics.

Vulnerability Scanner

Visit the vulnerability scanner to add your IP addresses/domains and review your results in full.

Phishing & E-learning

Use this tool to roll out training and phishing campaigns to your workforce.

Users

This is where you can view all admin users of the Pen Protect platform.

Companies

View your company details and add new users.

Settings

Make changes to the appearance of the dashboard, including language and light/dark mode.

FAQ

This section holds the answers to some of the more frequently asked questions, for anything else please contact penprotect@penunderwriting.com.

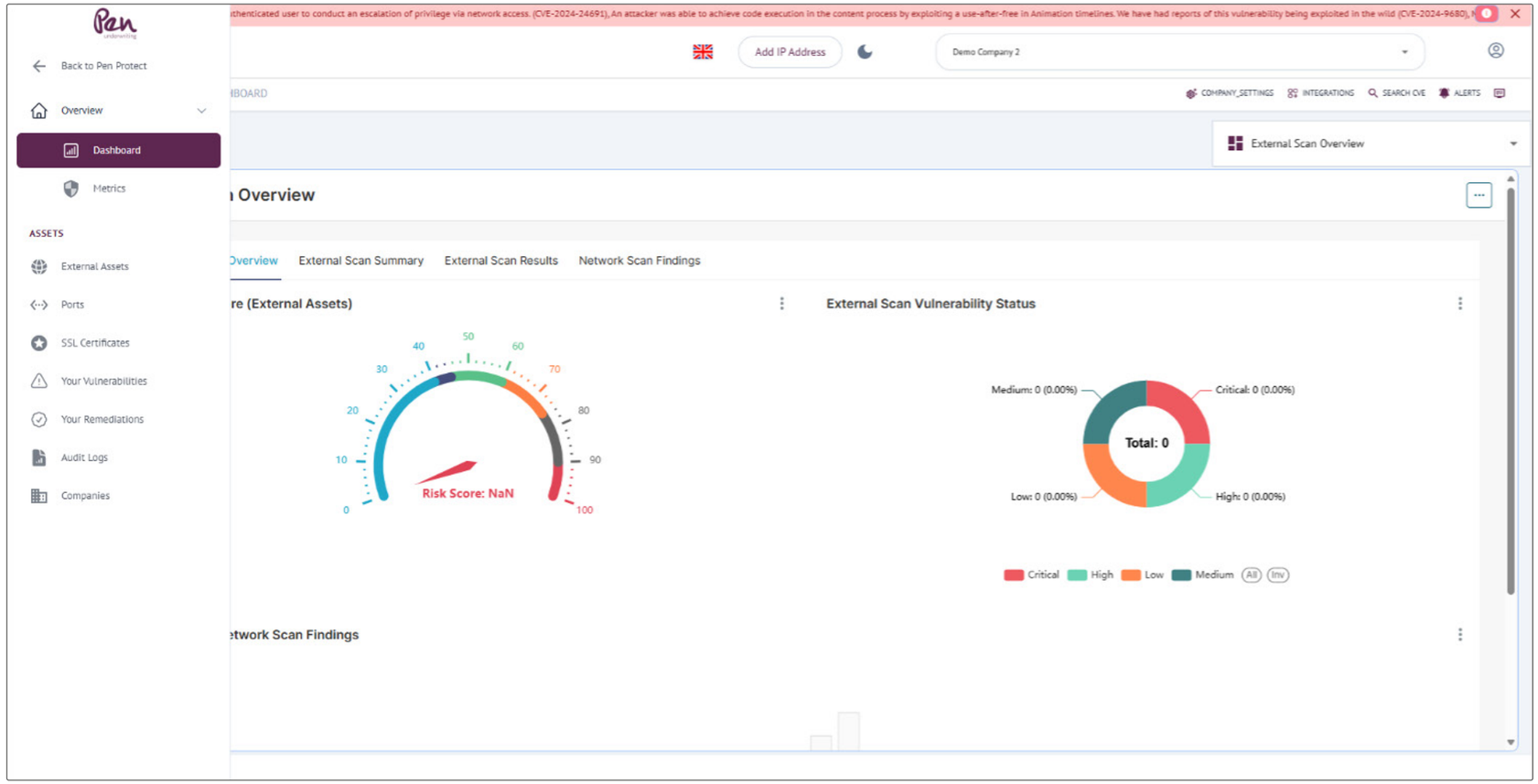
Pen Protect Guide

Vulnerability scanning – set up and results

Dashboard

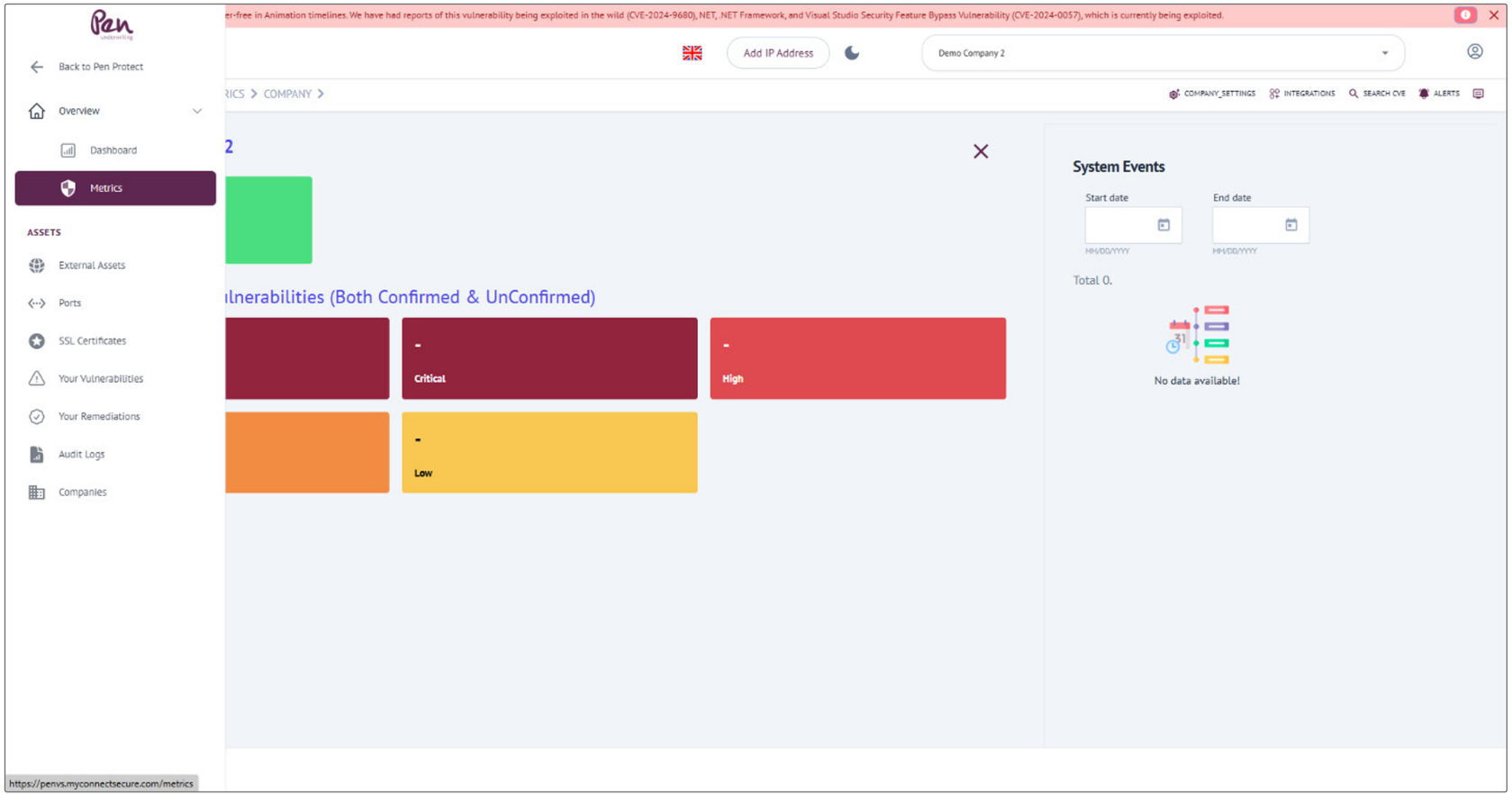
Your overview of vulnerability scans will display

- assets being scanned
- average risk score
- vulnerability trends graph



Metrics

This breaks down your external scan vulnerabilities by severity – from critical to low.



External Assets

Results – Here is a detailed list of each Internet Protocol (IP) or domain, and its specific vulnerabilities, remediation options, open and insecure ports and the status of any SSL or TLS certificates. You'll see which certificates are valid, expired or due to expire soon.

Configuration – Here you can add new assets to Pen Protect. Click '**Configurations**' and selecting '**Add**'.

- allocate a **name** for your asset to identify diRerent IP addresses, this could be based on locations or business purpose for example.
- choose one of three **address types**
- **Static IP**: any singular IP addresses, and will follow the format of 192.168.0.0
- **IP Range**: a block of IP addresses, and will look like this 191.168.2.1-192.168.2.100
- **Domain**: any web domains and should be shown in this format xyz.com
- select the scope of your scan, from the following scan profiles:
  - **Quick scan**

    Duration approximately 30 minutes

    Quick scans look at the most commonly used 1,000 ports as per the Internet

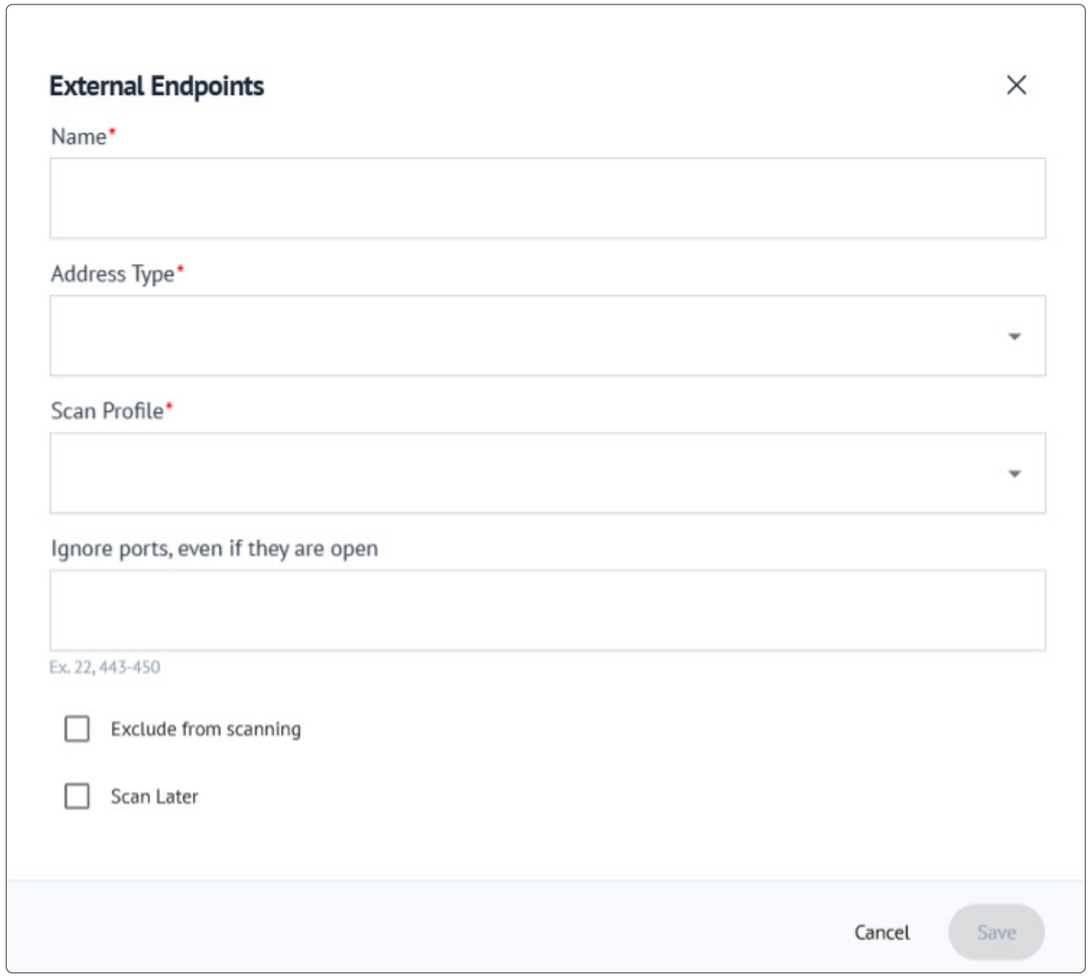
    Assigned Numbers Authority (IANA).
  - **Detailed scan**

    Duration approximately 90 minutes

    Detailed scans look at the most commonly used 3,500 ports as per the IANA.
  - **Deep scan**

    Duration approximately 3 hours

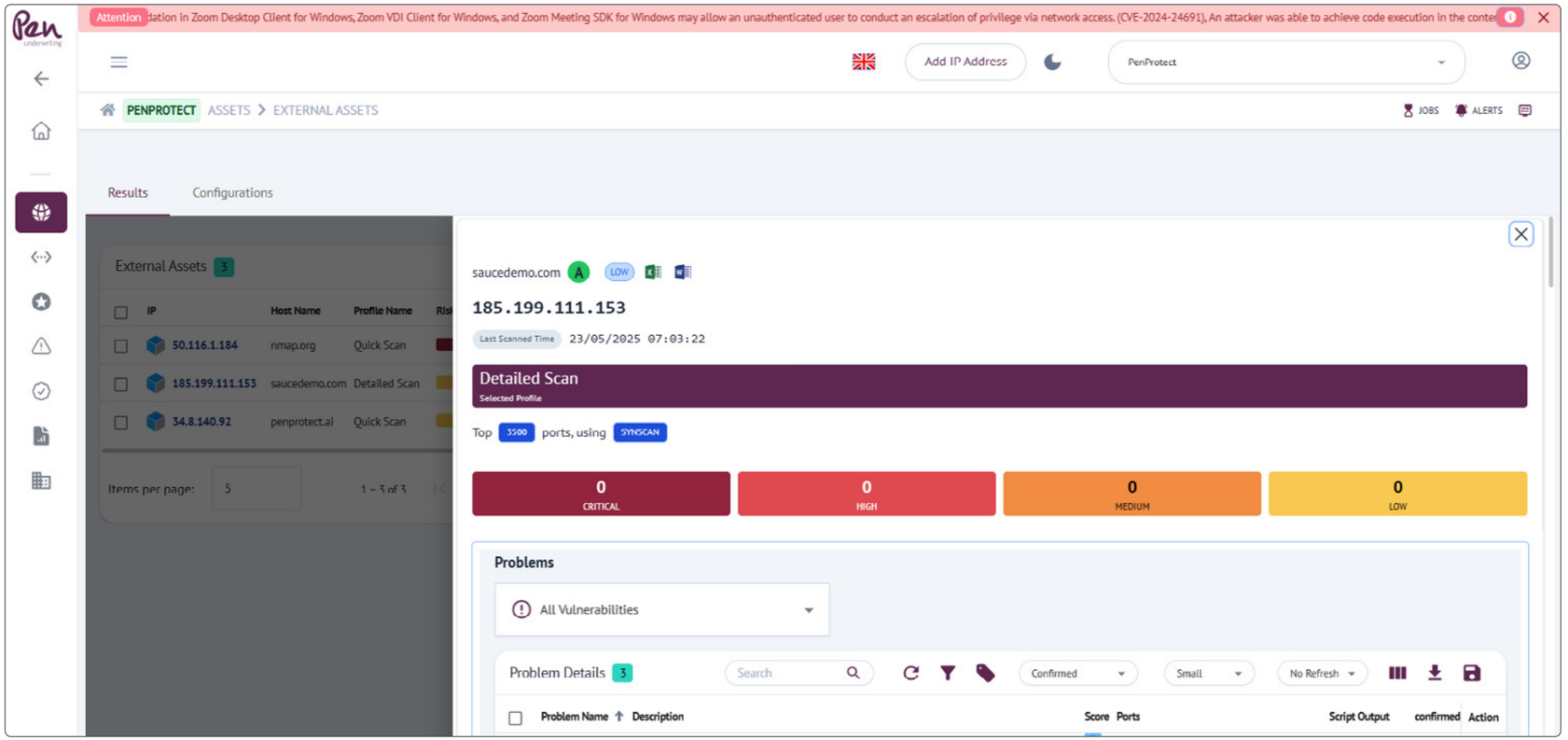
    This scan profile looks at all 65,535 ports.



Results

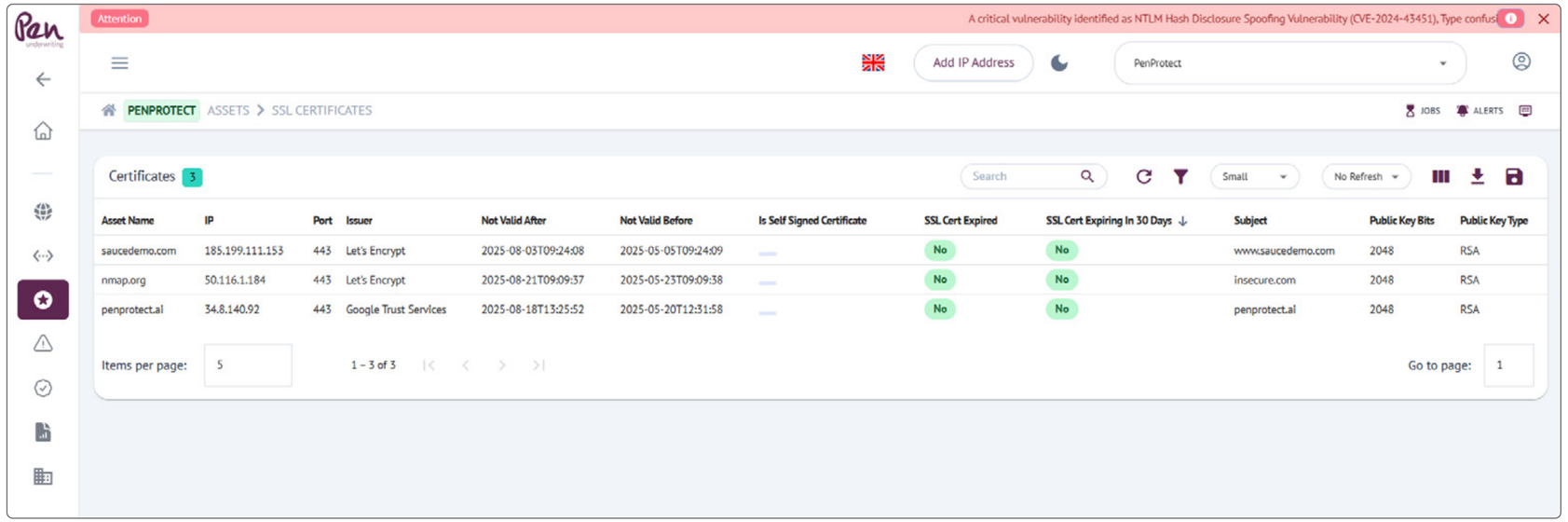
You can see the scan results for each domain/IP address.

Click the domain/IP address, to show the specific details for each, including problems, remediations, open and insecure ports and any SSL or TLS certificates.



SSL Certificates

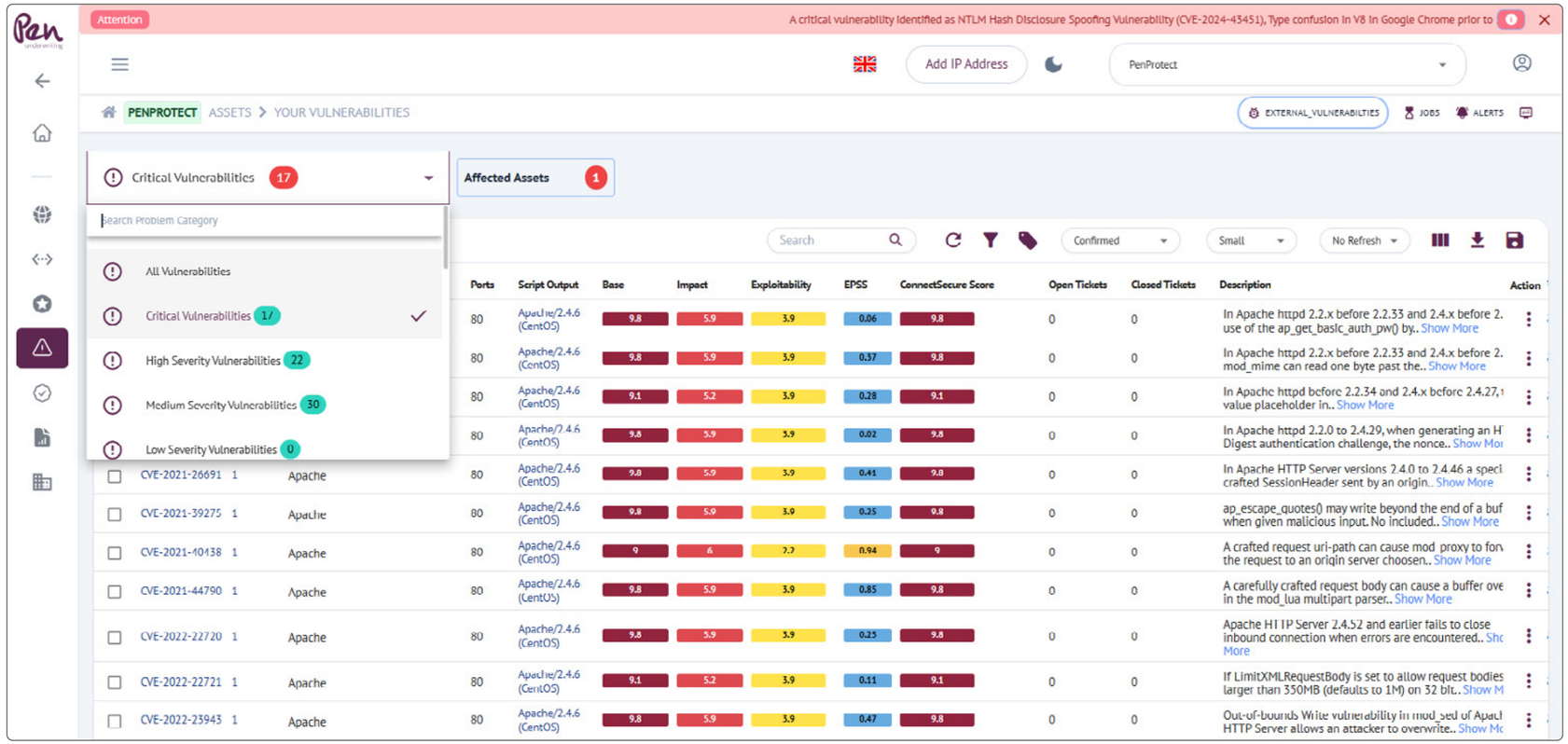
Here are all the SSL certificates across all your external assets in Pen Protect. You'll be shown the IP address and corresponding port, the date the certificate is valid to, if it has expired and if it is expiring in the next 30 days.



Your Vulnerabilities

Pen Protect can help you remediate your vulnerabilities too. Click '**Your vulnerabilities**' on the left-hand menu to see all your organisation's discovered vulnerabilities, including For each vulnerability is given an identifier known as a common vulnerabilities and exposure (CVE) and a code for the year the CVE is found, a software name for the service eRected, the port the service is running from and finally a score.

- level of severity
- CVE identifier, this is a common vulnerabilities and exposure identifier and a code for the year the CVE is found
- a software name for the aRected service and
- port details
- and a vulnerability score

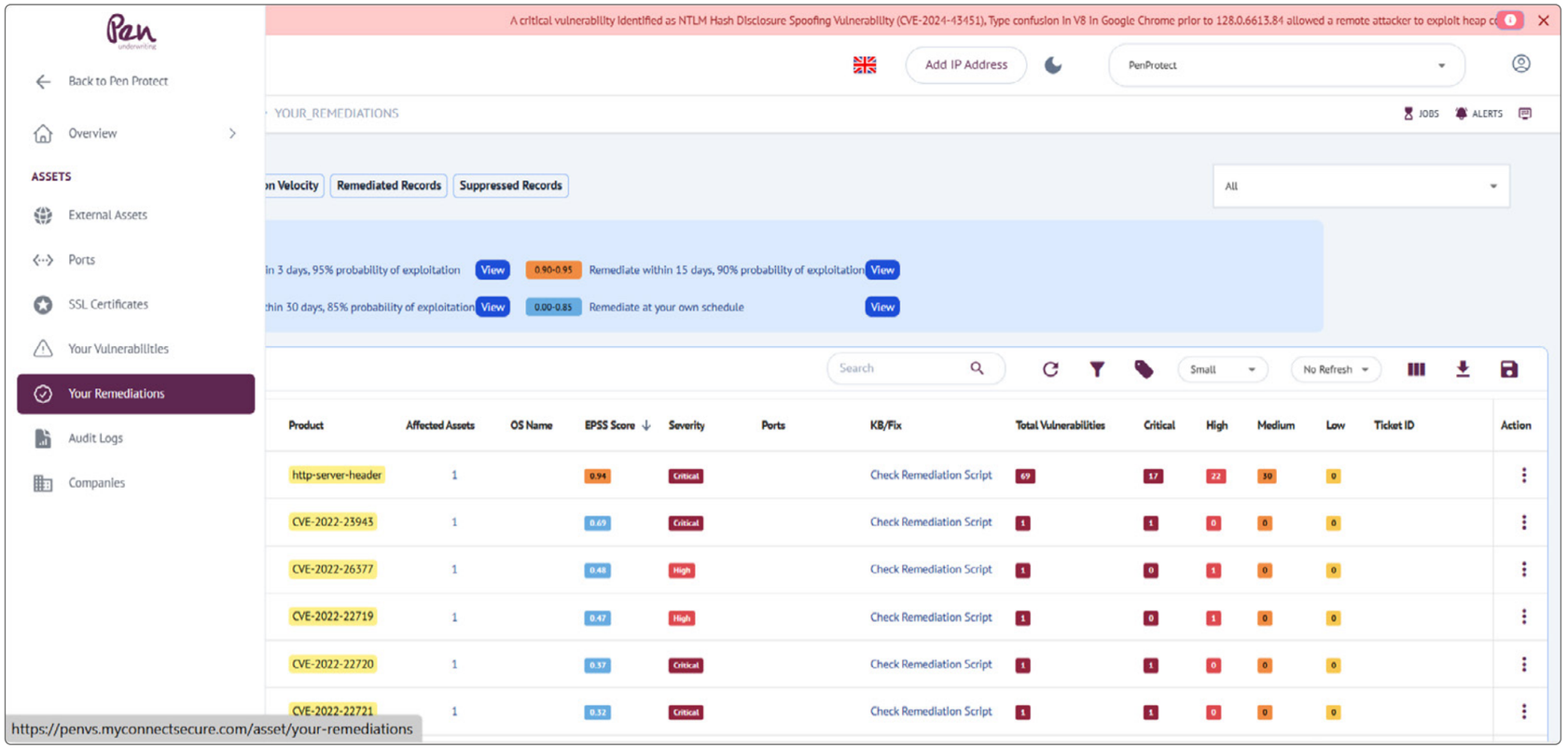


Your Remediations

If you select ‘Your Remediations’, you’ll see recommended fixes for your vulnerabilities.

Including

- the CVE for the vulnerability needing to be remediated
- aRected assets which, once selected, will show the domain/IP address
- an Exploit Prediction Scoring System (EPSS) score
- vulnerability severity
- total vulnerabilities the remediation will resolve
- and in some cases, a fix, called check remediation script.



Pen Protect Guide

Managing your human risks with phishing and e-learning

Dashboard

Managing human risks is key to your cyber risk management. Pen Protect can deliver training for your team and run phishing simulations to test your employees understanding and behaviours.

The dashboard displays various statistics and metrics based on employees' behaviours.

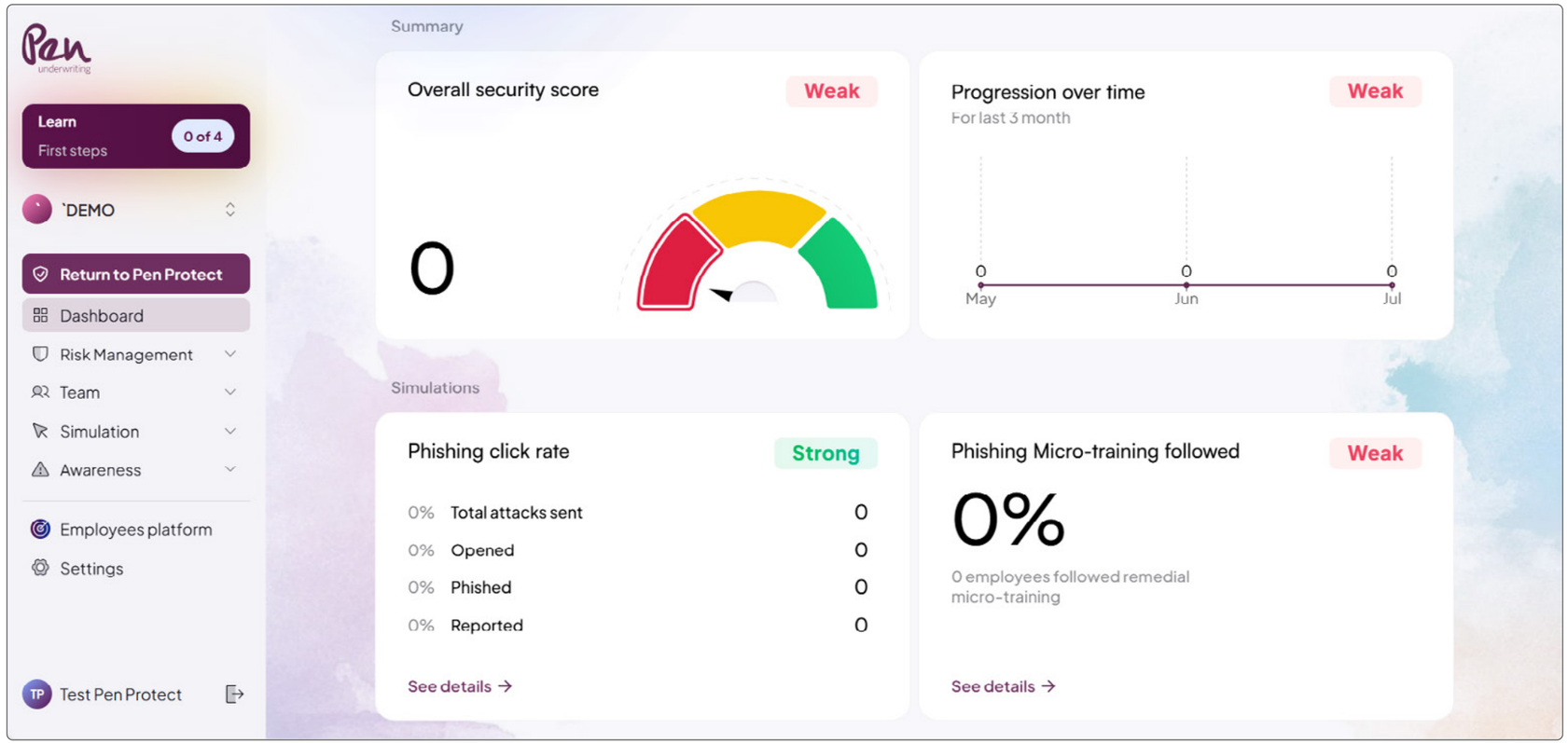
- **Simulations**
  The results from phishing simulations including click rates, who opened a specific phishing email, who gave credentials and who reported.

- **Security Awareness**
  Here you can review see the number of employees who have been assigned training, the percentage of training successfully passed, and percentage of courses not completed.

- **Reported Threats**
  This will show you how many phishing emails have been reported and for what reason.

- **Risky Behaviours**
  This identifies if a particular group or department is riskier than others or if particular employees are more likely to click the link than others.

Across the dashboard you can select '**more details**'.

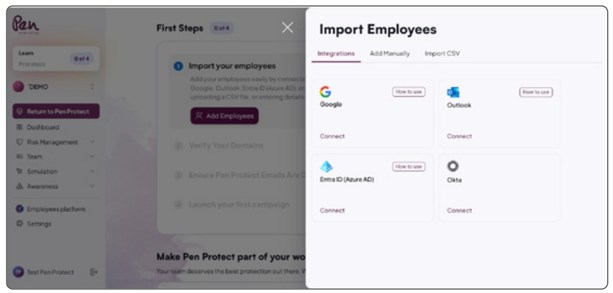


Creating Phishing Simulation Campaigns

Getting started is simple. Just four simple steps to setting up phishing simulation campaigns for your teams.

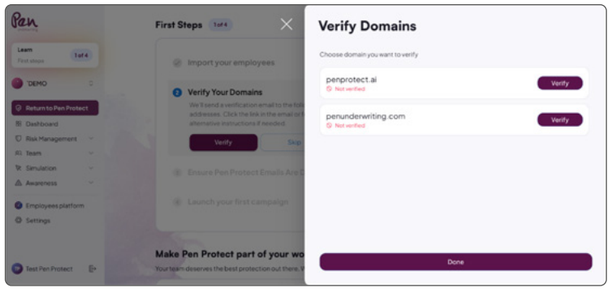
1. **Import your employees**

   You can add your employees to Pen Protect manually, via integration, or using the CSV import.



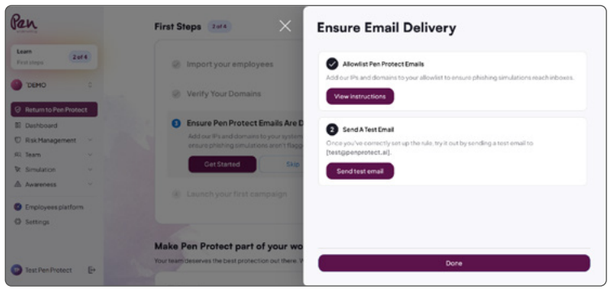
2. **Verify your domains**

   This ensures the phishing campaign and training emails reach your team without being blocked



3. **Ensure Pen Protect emails are delivered**

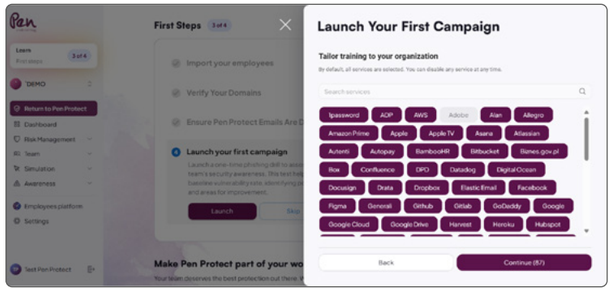
   Whitelist the email senders and send yourself a test of the phishing email.



4. **Launch your campaign**

   Select applicable services and software for your organisation.

   Choose one of Pen Protect's templates and launch your first phishing campaign.

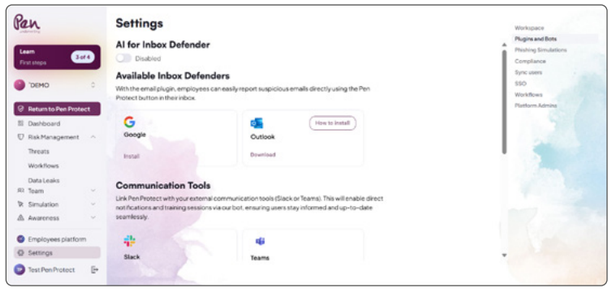


Risk Management

Threats

To stay ahead of cyber threats, you can install a reporting button so that employees can report any suspicious emails with just one click.

You'll be able to track how many phishing emails your teams are receiving and reporting.

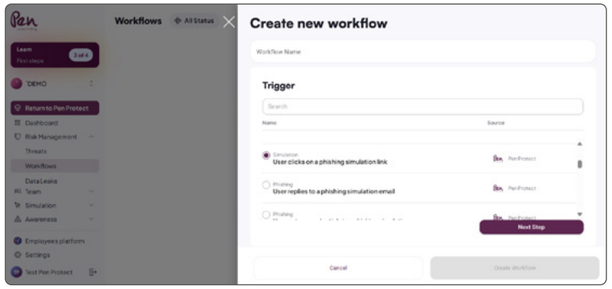


Workflows

You can automate follow- up actions using workflows, for example you can assign refresher training when a colleague clicks a phishing link.

1. Select '**set up workflow**' and '**new workflow**'
2. Choose your trigger event

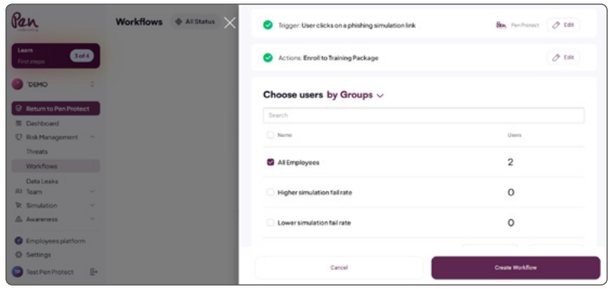
   In this example we have chosen '**User clicks on a phishing link**'. Add a '**title**' and select '**Next Step**'.



3. Choose your action or actions to select the next activity following the trigger event.

   If you select '**enrol to training package**', you will need to create a training package or select from one of the three already created training packages.

4. Choose your '**employee groups**' to who the actions will apply to and select '**create workflow**'



Data Leaks

Pen Protect's data leaks feature scans external online repositories to search for leaks relating to your domain or individual emails. You'll be notified here if you data appears in public leaks or on the dark web.

Click '**Activate**' to get started.

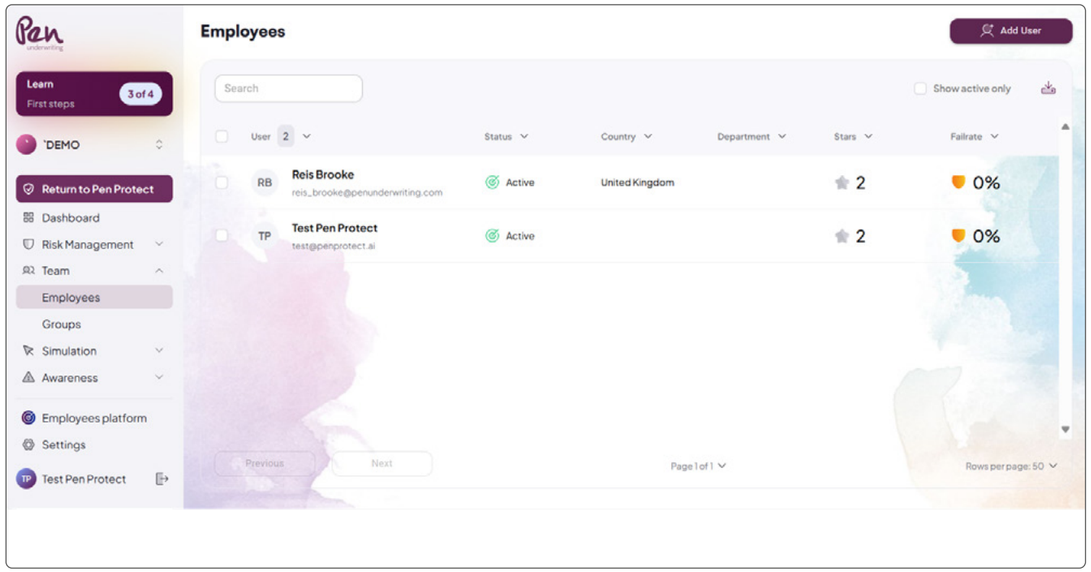
Team

In this section you can manage your employees and how they are grouped in Pen Protect.

You can easily view e-learning progress, group colleagues by department or their risk level, and target your phishing simulations campaigns accordingly.

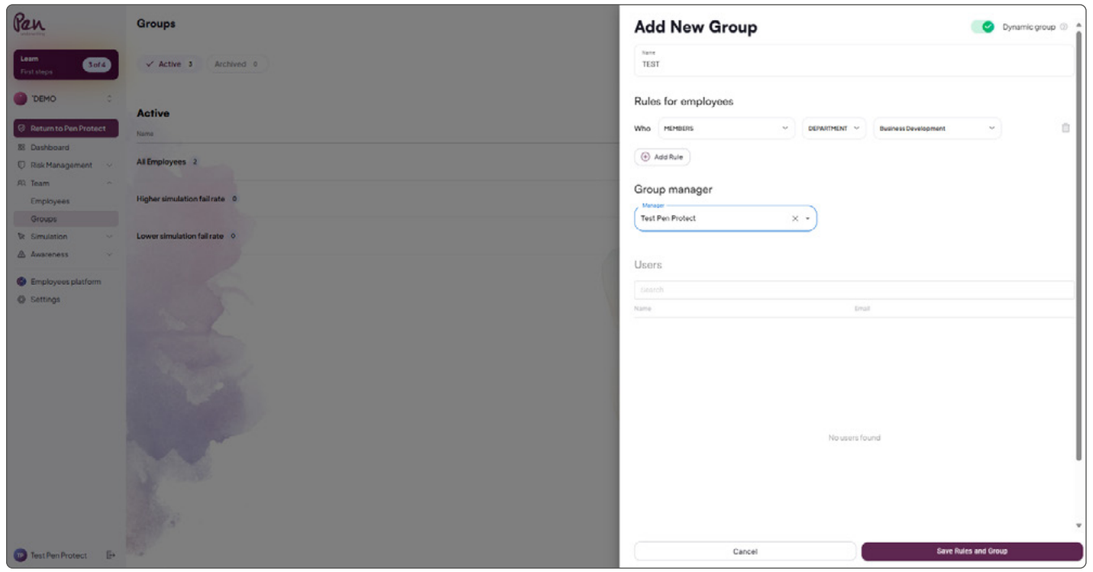
Employees

- Manually add more employees and view employee that have already been uploaded to Pen Protect.
- Pen Protect will show the country and corresponding department, with their number of training stars completed.



Groups

- Manually add more employees and view employee that have already been uploaded to Pen Protect.
- Pen Protect will show the country and corresponding department, with their number of training stars completed.



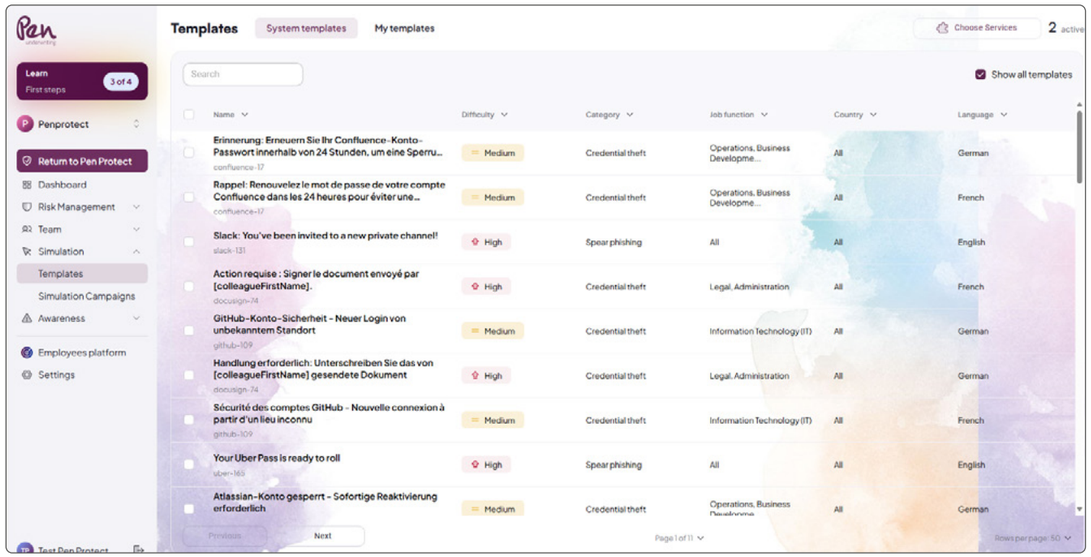
Simulations

You can create phishing simulation campaigns using our selection of templates or create your own.

You can schedule the dates of your campaign, define the post-phishing actions and track employee engagement.

Templates

Select '**Choose services**' to view all available phishing categories. You can adapt the template to make it as relatable as possible.



Simulation Campaigns

Here you can set up your phishing campaigns, view click rates, and other statistics for previous phishing campaigns.

1. Click '**new campaign**' at top right of the page, add your '**campaign name**' and select the group of employees that should receive the phishing campaign. Select '**Continue**'

2. Choose your preferred phishing simulation, from
   - Deepfake calls
   - SMS messages
   - AI generated email

   Pen Protect will generate the email automatically and create a personalised template for each user
   - Custom email

   Select a premade template(s) or create your own bespoke email template

3. Select when the simulation should run.
   Decide a starting date, and the duration that the simulation should rolled out.

4. Choose from two 'After-phish actions'
   - '**Skip login step**'

   Bypass the section where an employee provides credentials to become phished.
   - '**Skip Micro Learning**'

   Skip the redress training when an employee is phished.

5. Select '**save**' and your campaign will be rolled out to the chosen team

Awareness

This is where you can build training for your employees, either their first cyber training as they onboard, or ongoing refresher learning for your existing teams.

Training Topics

You can review the existing training, listed below, or create your own bespoke training.

Pen Protect's training topics include

- physical security
- privacy
- browsing the internet securely
- passwords
- social media and personal email
- social engineering
- working remotely / from home
- device security
- malware
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- System and Organization Controls 2 (SOC 2)
- and much more

Select '**view modules**' on each training topic to review, or the three dots on the right-hand side of the screen to either preview the training or edit and alter the training as you wish.

Training Packages

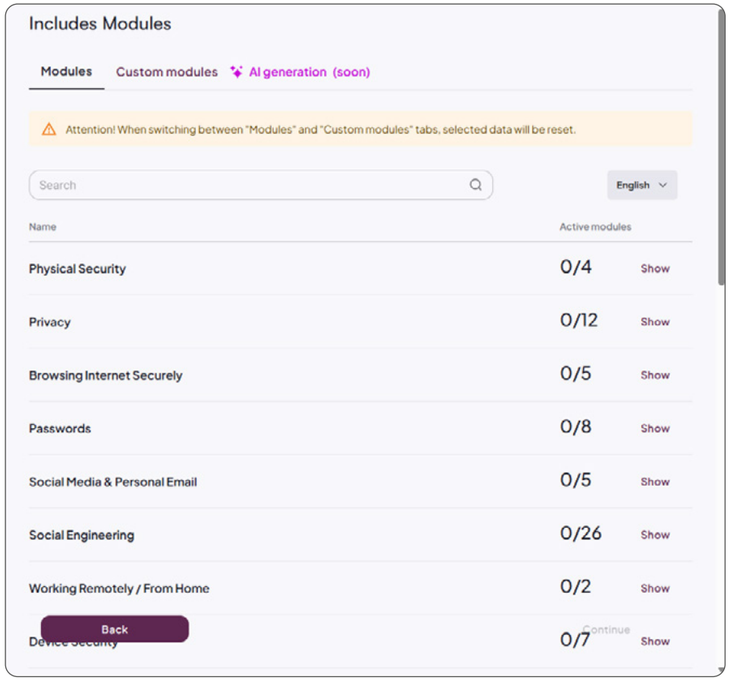
You can create bespoke training packages comprising of your chosen modules and create packages for specific business uses; for example, on-boarding new team members.

1. Select the '**New Training**' button

2. Define the training package details
   a. name your training package
   b. add a description
   c. choose whether the training is mandatory
   d. select how colleagues will be reminded to complete the training
   e. decide how long the training will be available for
   f. apply a deadline date, if appropriate

3. Decide the package's training contents.

   Selecting 'Show' for the topics you want to include, and use the slider to include the modules



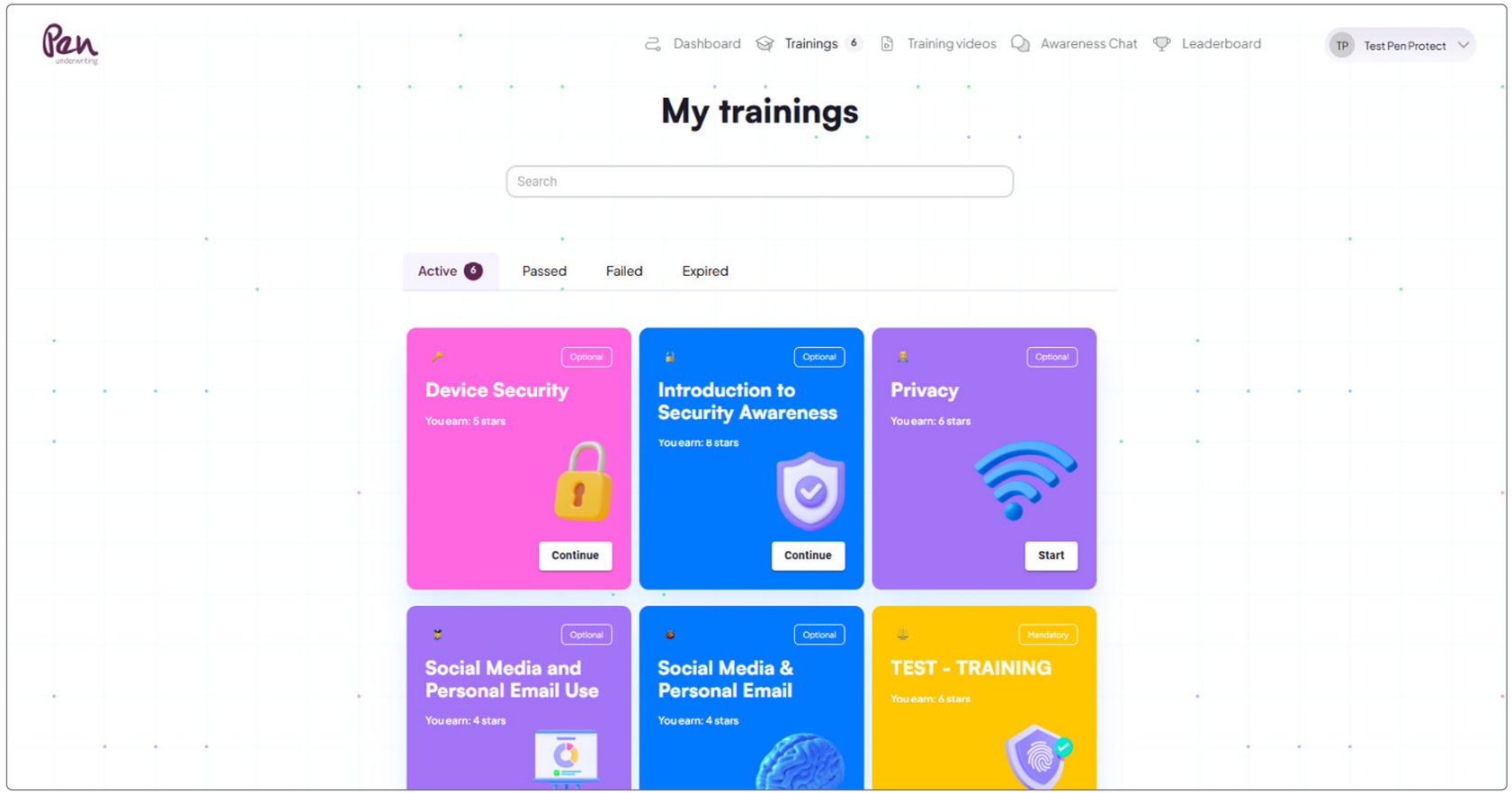
4. Select '**continue**' and choose the appropriate colleagues, and select 'continue' again

   The selected colleagues will be enrolled on to the training, based on the pre-defined criteria.

Employee Portal

Each employee can access their own part of the Pen Protect portal.

Here they can track their personal progress, phishing activities, review their upcoming and past training and access the chat function ‘Awareness Chat Room’ for quick answers to cyber security questions.



The sole purpose of this guide is to provide guidance on the issues covered. This guide is not intended to give legal advice, and, accordingly, it should not be relied upon. It should not be regarded as a comprehensive statement of the law and/or market practice in this area. We make no claims as to the completeness or accuracy of the information contained herein or in the links which were live at the date of publication. You should not act upon (or should refrain from acting upon) information in this publication without first seeking specific legal and/or specialist advice. Pen Underwriting Limited accepts no liability for any inaccuracy, omission or mistake in this publication, nor will we be responsible for any loss which may be suffered as a result of any person relying on the information contained herein.

penunderwriting.co.uk

Pen Underwriting Limited is authorised and regulated by the Financial Conduct Authority (FCA number 314493). Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company Number: 5172311.

www.penunderwriting.co.uk | FP221-2026 04032027

Pen underwriting