CYBERDISE FEATURE CATALOGUE

Version 19.02.2024

TABLE OF CONTENTS

INTRODUCTION

What is Cyberdise? On the one hand, it is a platform for **sending phishing simulations and smishing** exercises. On the other hand, Cyberdise contains a learning management system with prepared **cybersecurity awareness training (SAT),** which can be used to train employees on cybersecurity risks. The solution, which can also be installed locally, is completed by a 'phishing report button' and various AI features.

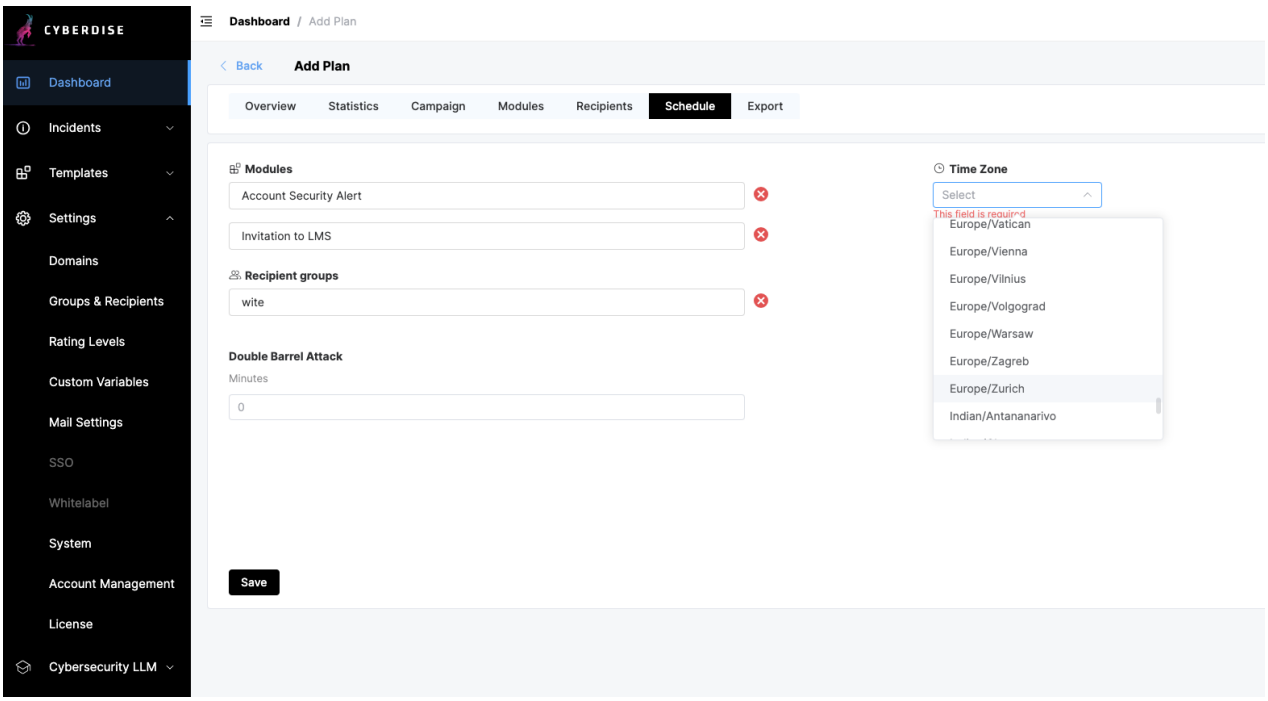
About the Company: Cyberdise was launched in 2023 by a group of founders in the cybersecurity awareness industry to bring better cybersecurity awareness training and testing solutions to the market. Cyberdise is a comprehensive, AI-powered platform and software that can be used to sustainably train and test an organization's employees against cyber risks.

Adress (HQ): Cyberdise AG, Poststrasse 26, 6300 Zug, Switzerland. Further information can be found at www.cyberdise-awareness.com

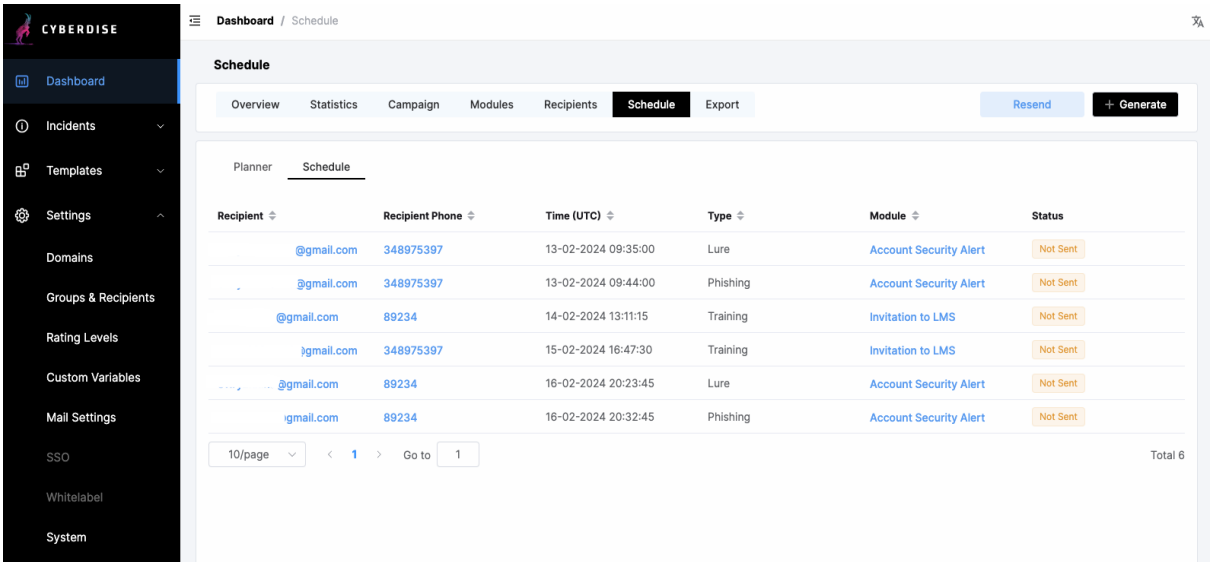
Contact: For further inquiries please call +41 41 511 78 10 or send an email to sales@cyberdise.io

GENERAL FEATURES

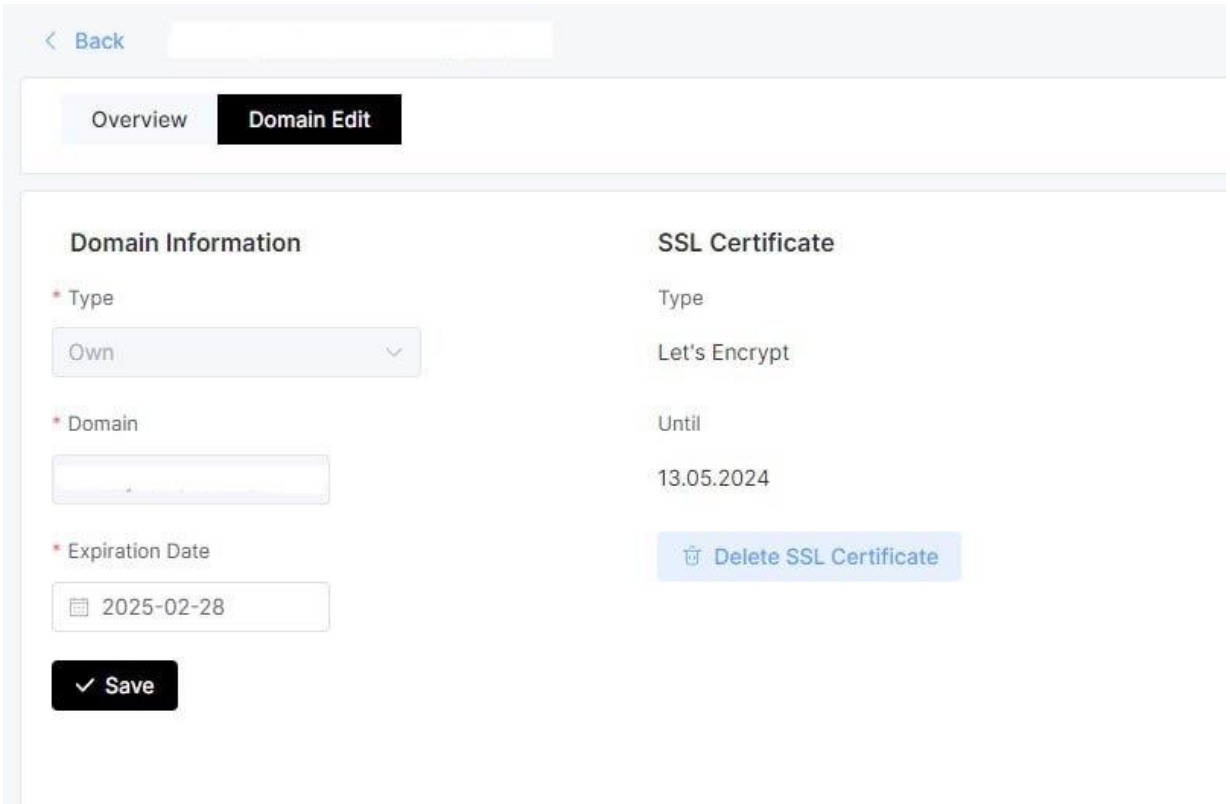
Multi Timezone Campaign Scheduler: You can serve recipients who are in different time zones in the same campaign.



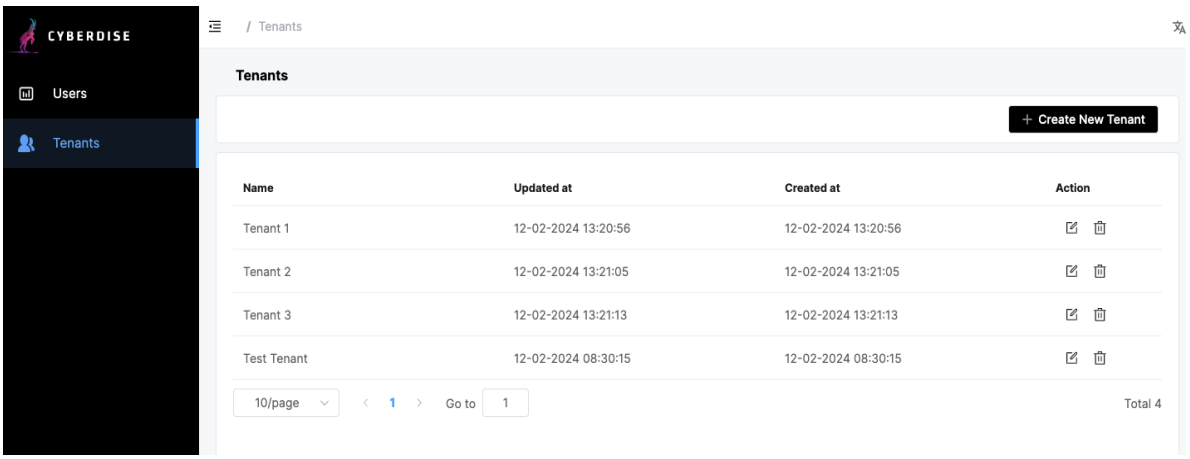
Delivery Randomizer: The crucial element for achieving effective and lasting awareness among employees is to enhance their understanding at random intervals. Conducting numerous campaigns simultaneously and at random is one of the most effective strategies for training employees.



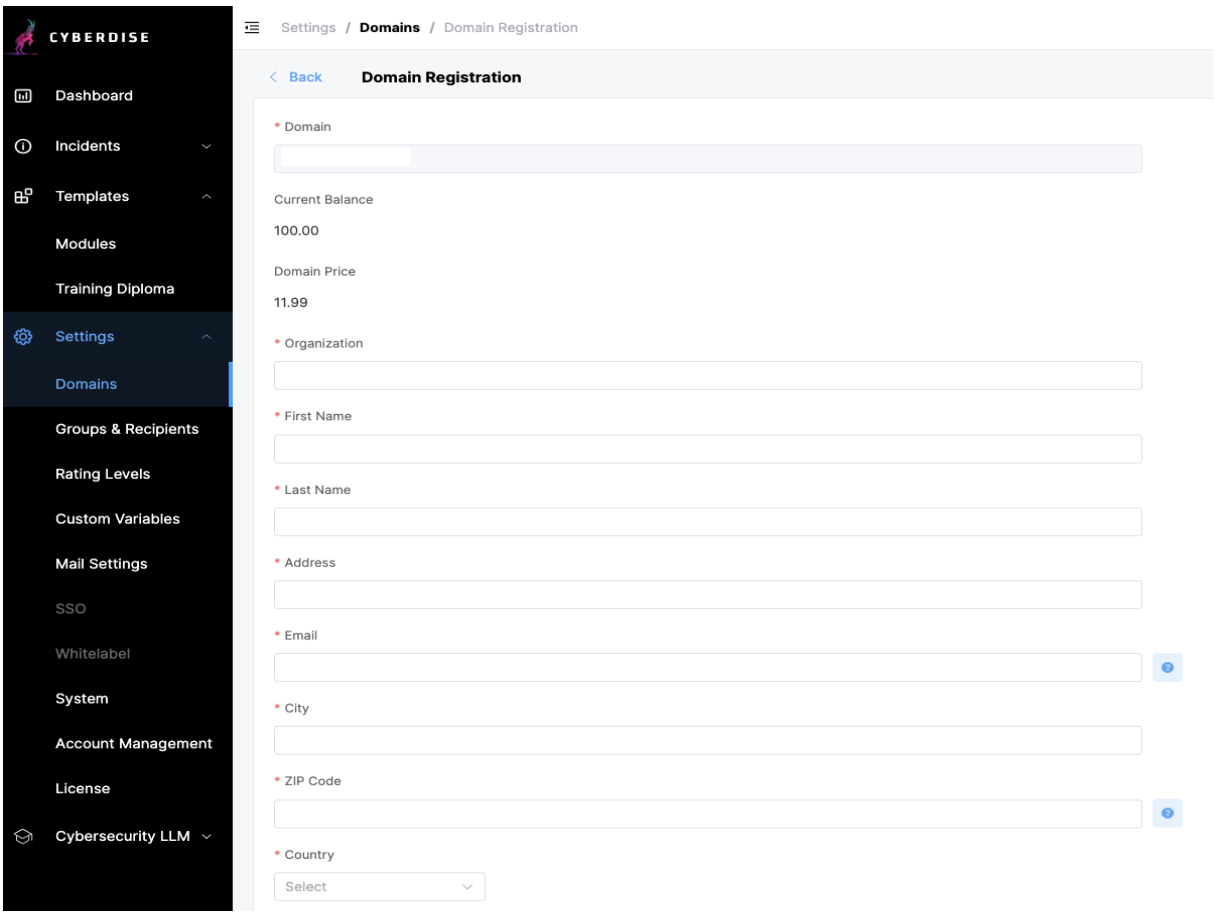
SSL Certificates: Allows automatic creation of official and trusted certificates for administrative backends and campaigns. If you choose to use SSL for your campaign, you can generate a custom certificate or certificate signing request (CSR) for the domain you want to use. Of course the import of own official trusted certificates is also supported.



Multitenancy: "Tenants" can refer to different companies, departments, or groups which have an associated campaign in Cyberdise. These customers can be used, for example, to allow campaign-specific access or to create customer-specific analysis.

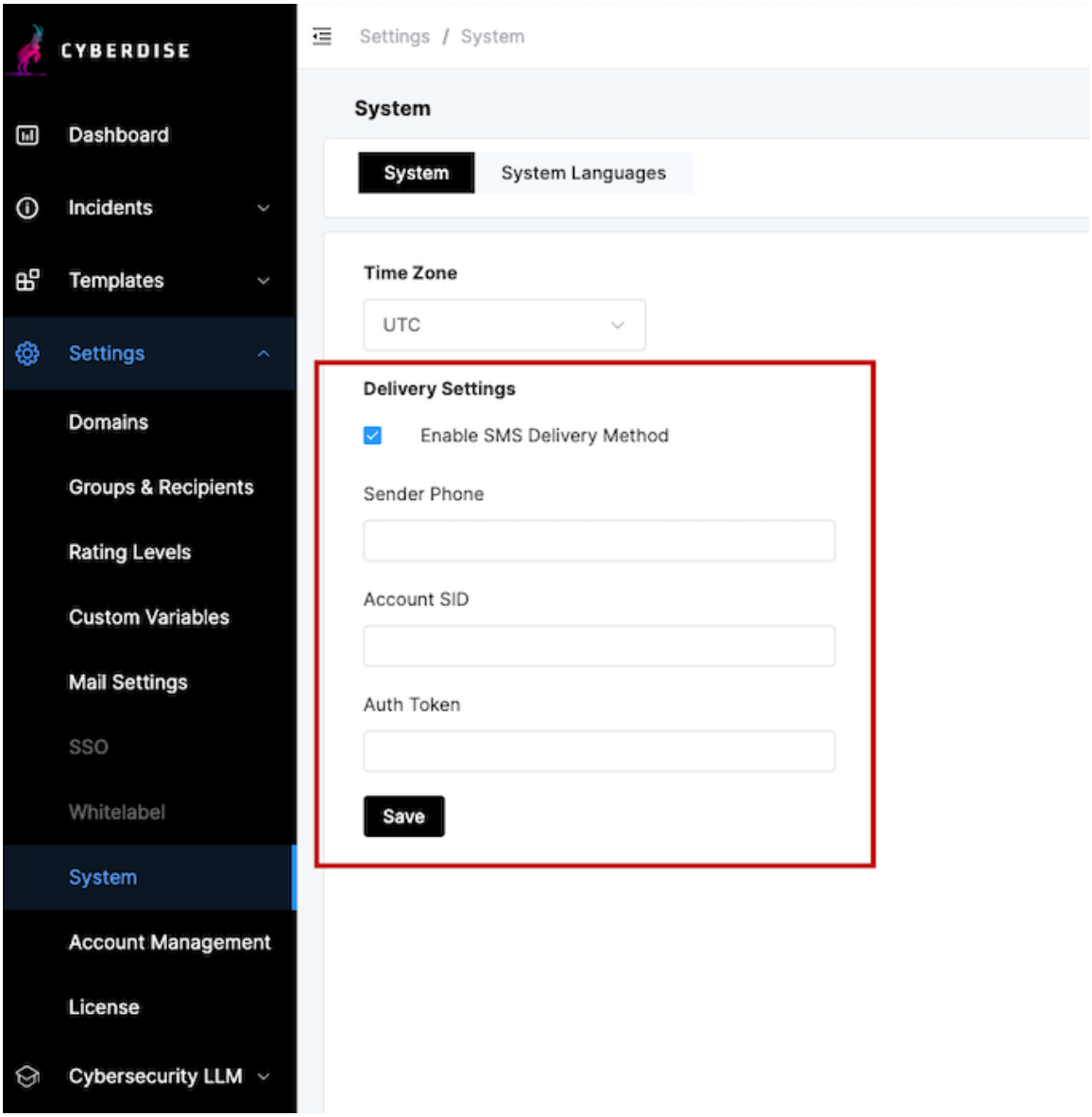


DNS Domain API: Purchase any number of domain names directly through Cyberdise for your phishing exercises or awareness training. Have Cyberdise automatically generate the relevant DNS records (including SPF, MX, Wildcard A-Record, and Whois protection) for you. Maintain and extend the domains you have purchased directly in Cyberdise.

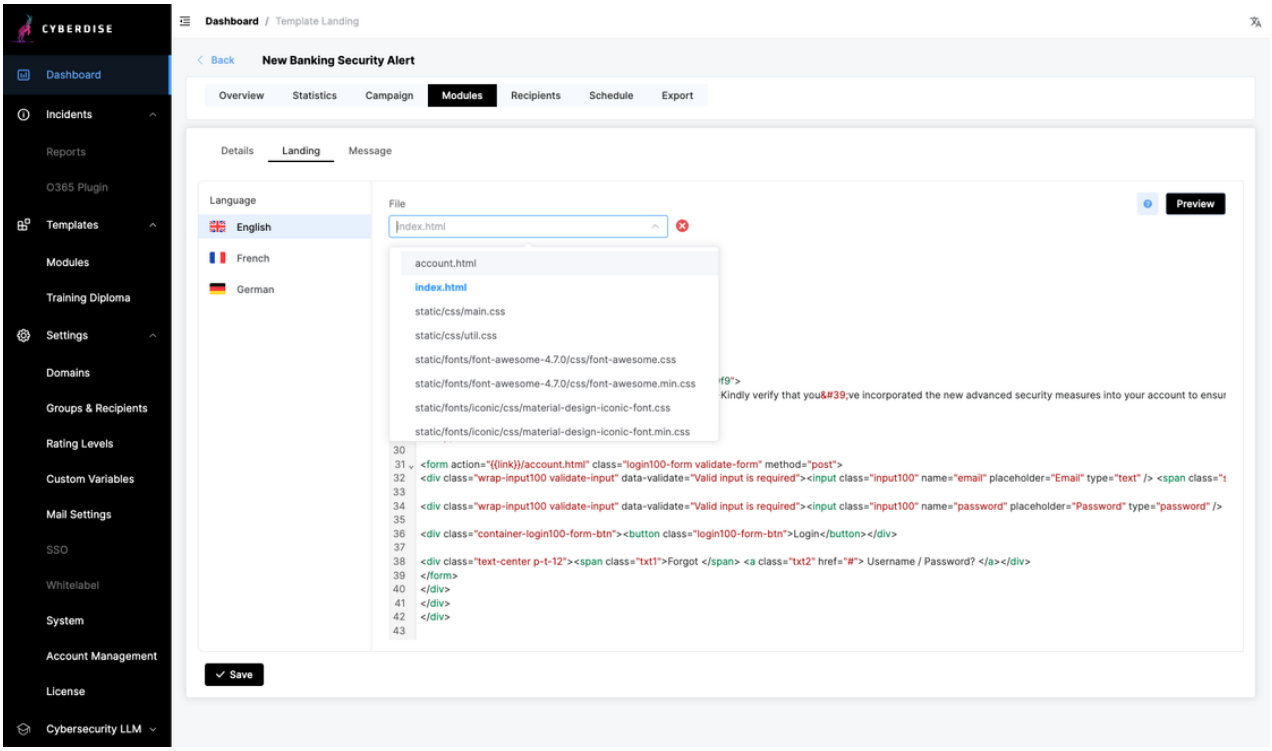


ATTACK EXERCISE & AWARENESS TRAINING

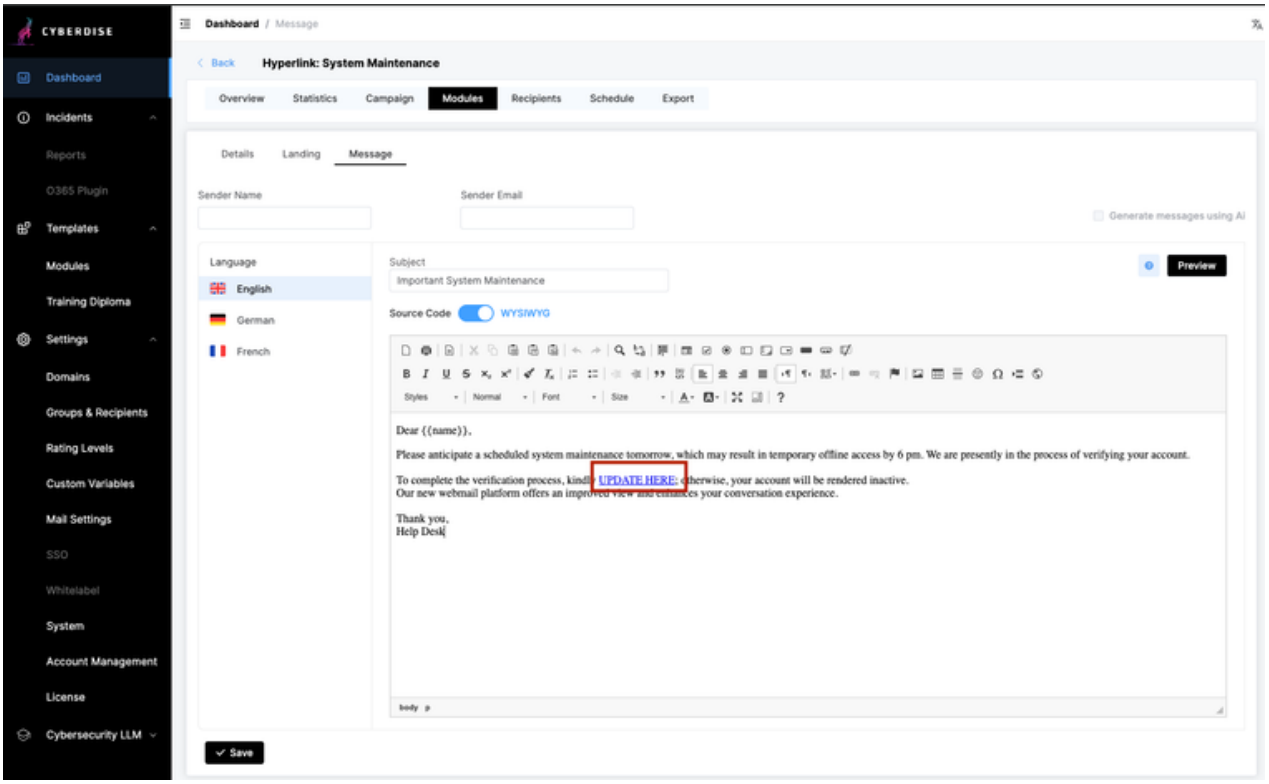
Smishing: is essentially "SMS-based phishing." In this approach, cybercriminals engage in "phishing" activities by sending deceitful text messages instead of emails, aiming to dupe the recipient into opening an attachment loaded with malware or clicking on a harmful link.



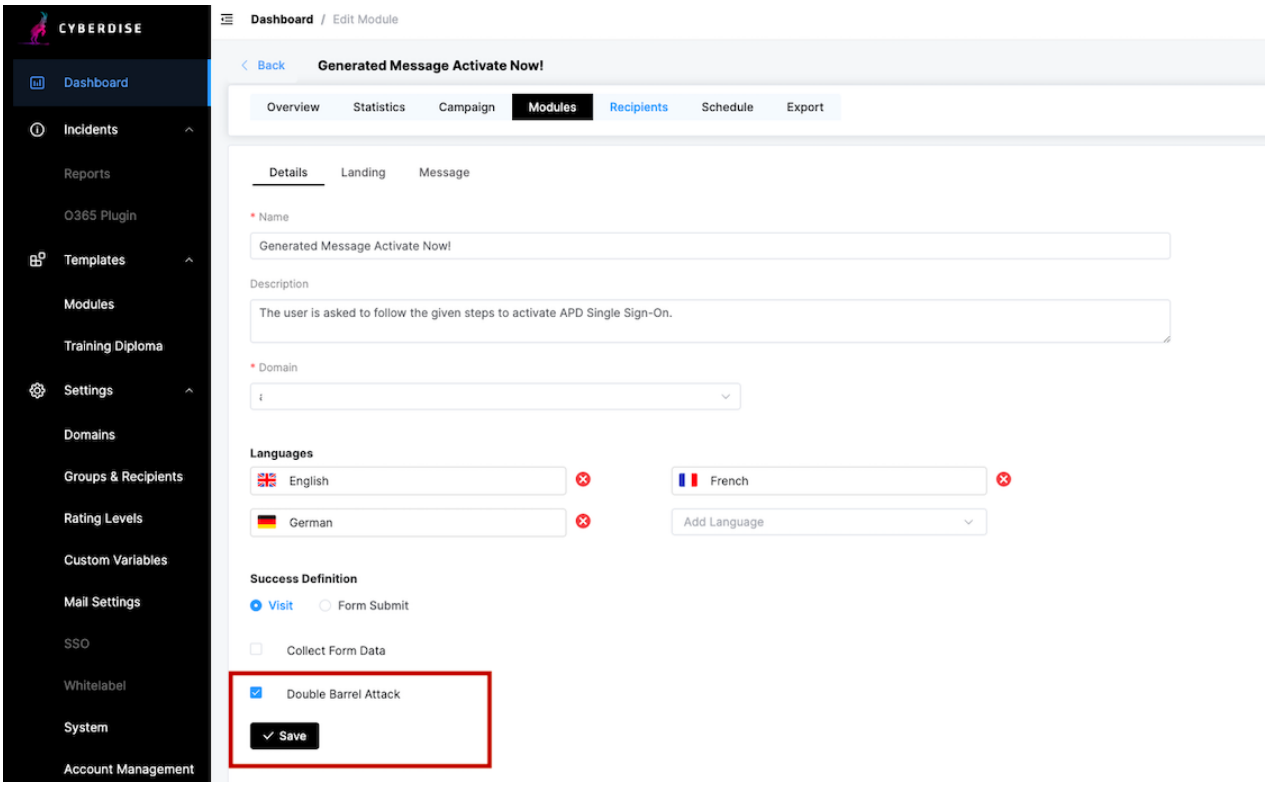
Data Entry Phishing Exercises: Data entry attacks can include one or more web pages that intercept the input of sensitive information. The available web pages can be easily customized with a Cyberdise content editor. Additional editing tools allow you to quickly set up functions such as log-in forms, download areas, etc. without HTML knowledge.



Hyperlink Exercises: A hyperlink-based campaign will send users an e-mail that contains a randomized tracking URL.



Double barrel: This feature makes it possible to send multiple phishing e-mails in each campaign, with the first benign e-mail (the Lure) containing nothing malicious and not demanding a reply from the recipient.



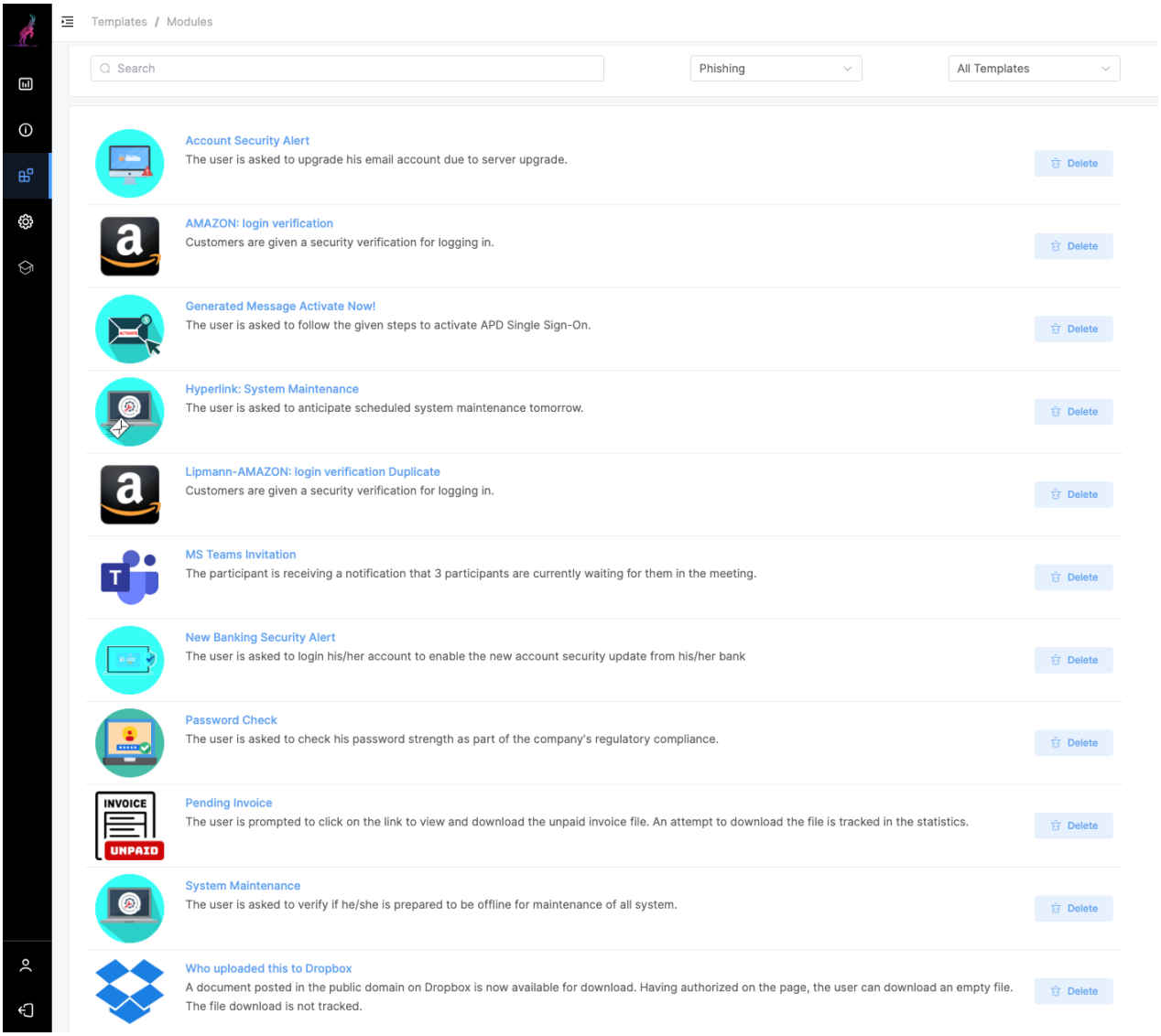
Java-Based Exercises: Java-based phishing exercises/attacks allow the Cyberdise operator to integrate a trusted applet within the file-based or mixed attack templates provided in Cyberdise and to measure their execution by the user.

Data Entry Validation: Data Entry Validation Toolkit In phishing simulations, false positives must be prevented for log-in fields (e.g., logging with invalid syntax). The company guidelines may also forbid the transmission of sensitive data such as passwords. For this purpose, Cyberdise provides a flexible input filtering engine that offers a suitable solution for every requirement.

Mobile-Responsive Format: Many of Cyberdise's built-in modules are available in a mobile-responsive format that gives your users the flexibility to take the training on any type of connected device.

Video Customization: Send us your company logo and we will include it in the training videos. You want another language? No problem. We will set the video to play in the language you prefer. You want a different scene? Simply download the video scripts and mark the desired changes.

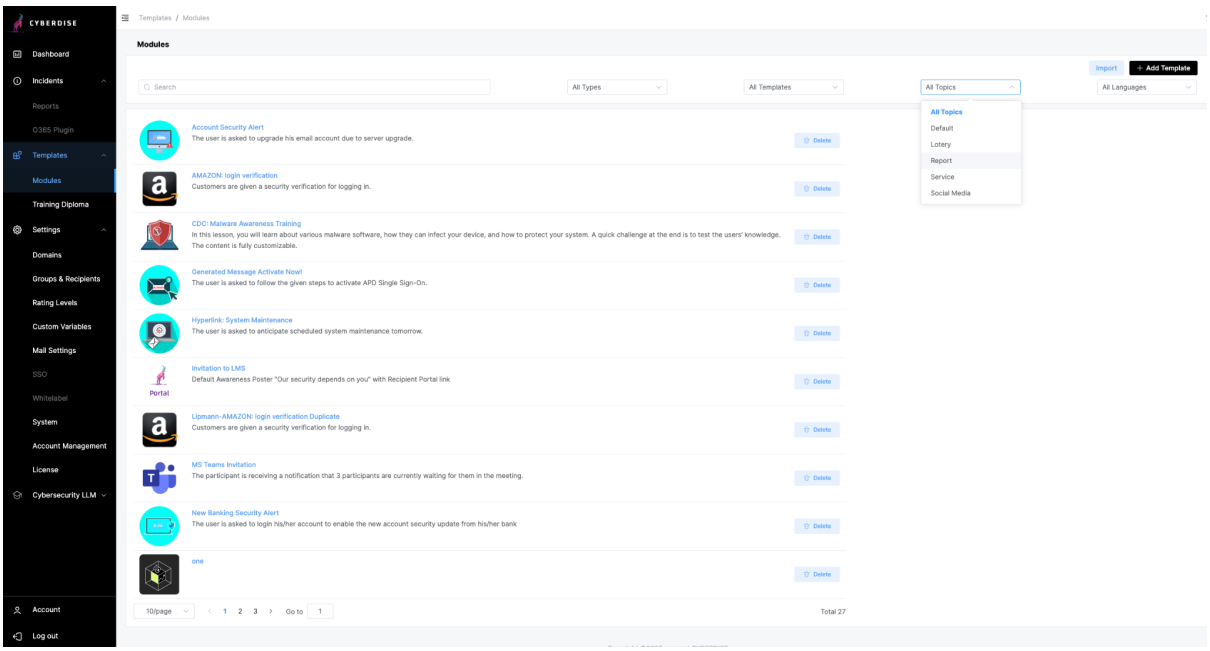
Muiltilingual Phishing Exercise Library: Cyberdise comes with predefined phishing templates in different languages in the categories of data entry (templates with a website), file-based (e-mails or websites with a file download), hyperlink (e-mails with a link), mixed (combination of data entry and download), and portable media.



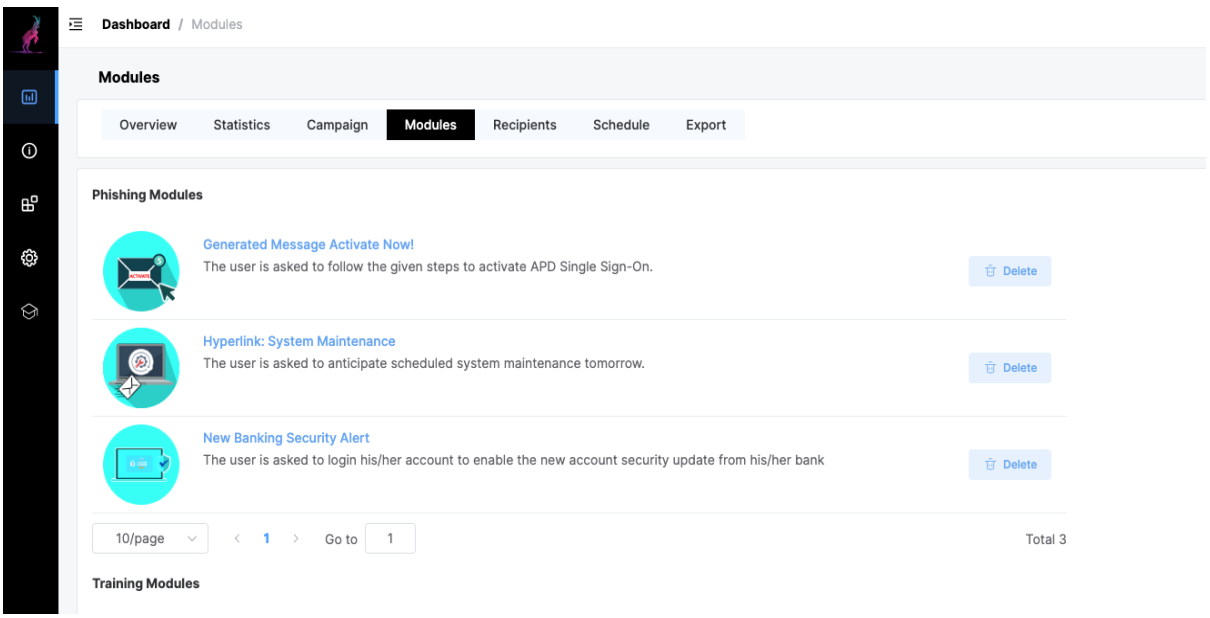
Website Cloner: Quickly create highly professional landing pages for your campaigns. Clone existing websites and add additional layers with data entry fields, files for download, and more. Please note that pages to be copied that contain a lot of Javascript can often only be copied inadequately. Cyberdise does not offer support for working with the cloning feature itself.

Custom Homepage Creation for the Phishing Exercise: users with a better technical understanding could use their browser to call the domain or IP address associated with the randomly generated phishing link. To prevent error messages from appearing or the end user from even coming to the login area of the admin console, you can create generic "homepages" within Cyberdise for the domains used in the phishing simulation.

Topical And Division Specific Exercise Templates: Attack templates are available for specific topics or divisions.



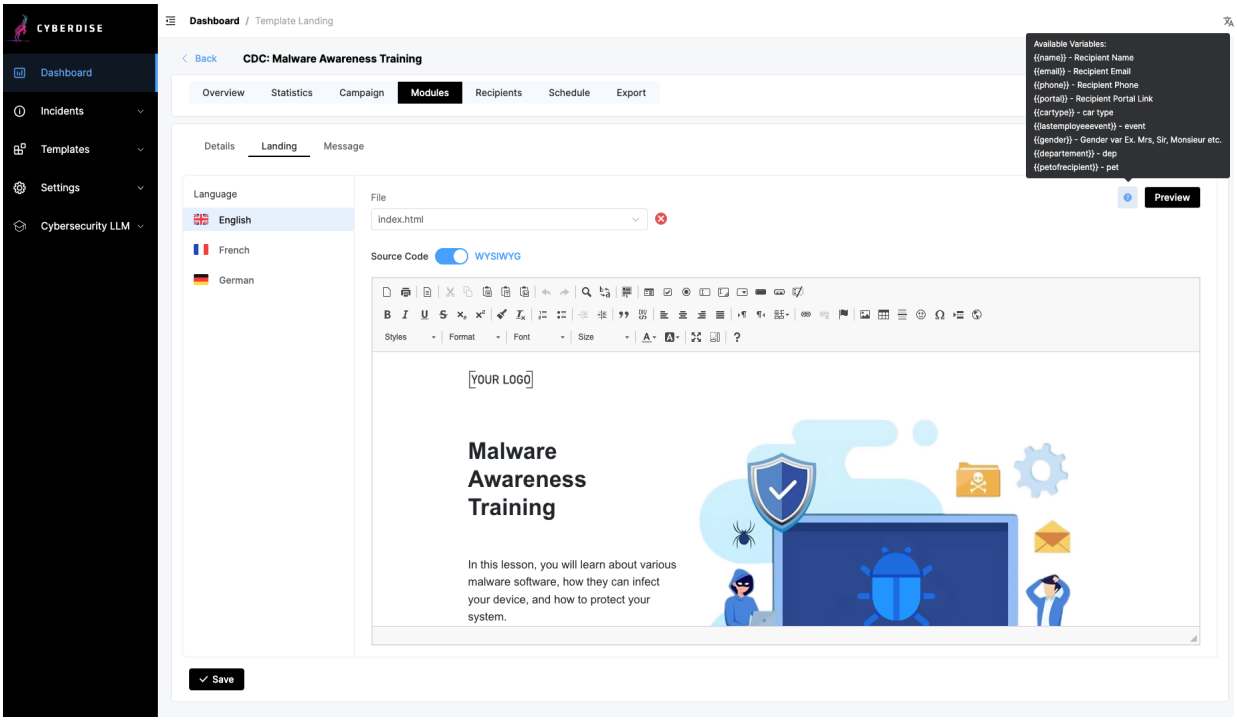
Multi Template Usage: Cyberdise offers the option to utilize multiple simulated phishing templates within a single campaign. Mix various types (hyperlink, file-based, etc.) with different topics to achieve the broadest possible risk coverage and gain a deeper understanding of employee vulnerabilities. When combined with our scheduling randomizer, complex phishing patterns can be executed over an extended period.



URL Shortening: URL shorteners can be used by cyber criminals to hide the real target of a link, such as phishing or infected websites. For this reason, Cyberdise offers the possibility to integrate different shortener services within a phishing or smishing campaign.

Skill-Based Campaigns: Skill-based phishing campaigns serves individual phishing exercises based on the current skill level (rating) of the employee.

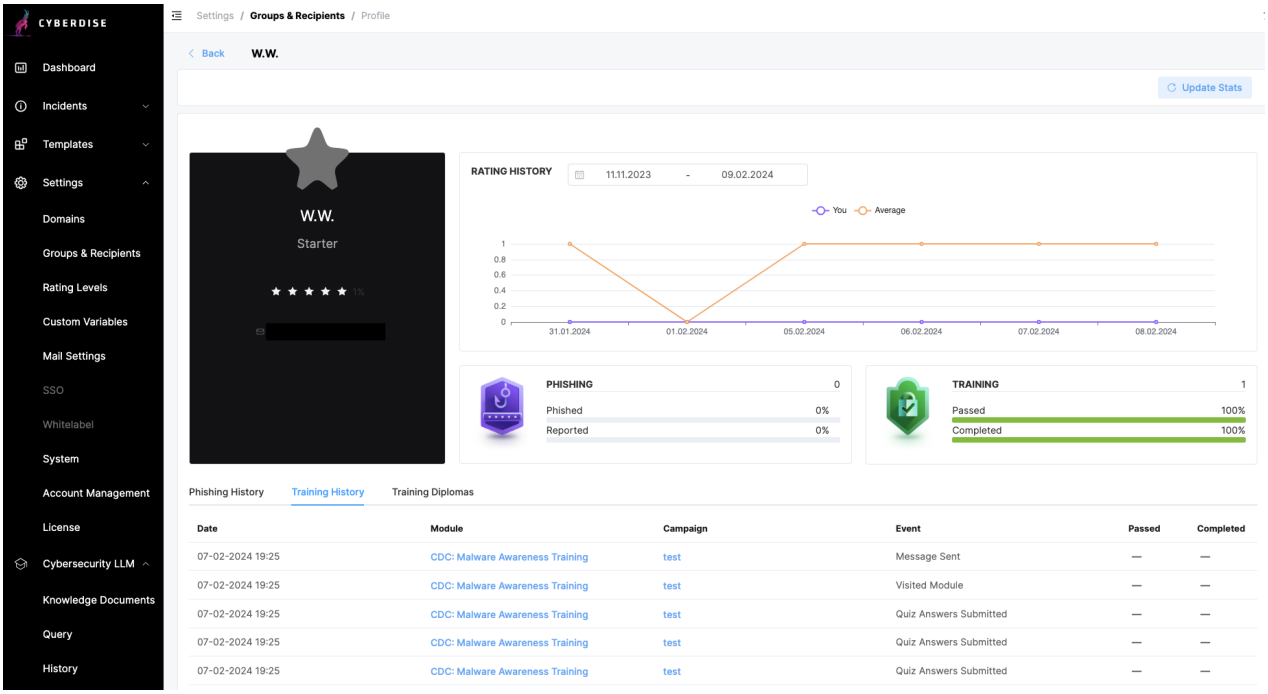
Spear Phishing Simulation Exercises: The Spear Phish Tailoring works with dynamic variables (gender, time, name, e-mail, links, messages, division, country, etc.) which you can use in landing and message templates. Create as much individual variables you need.



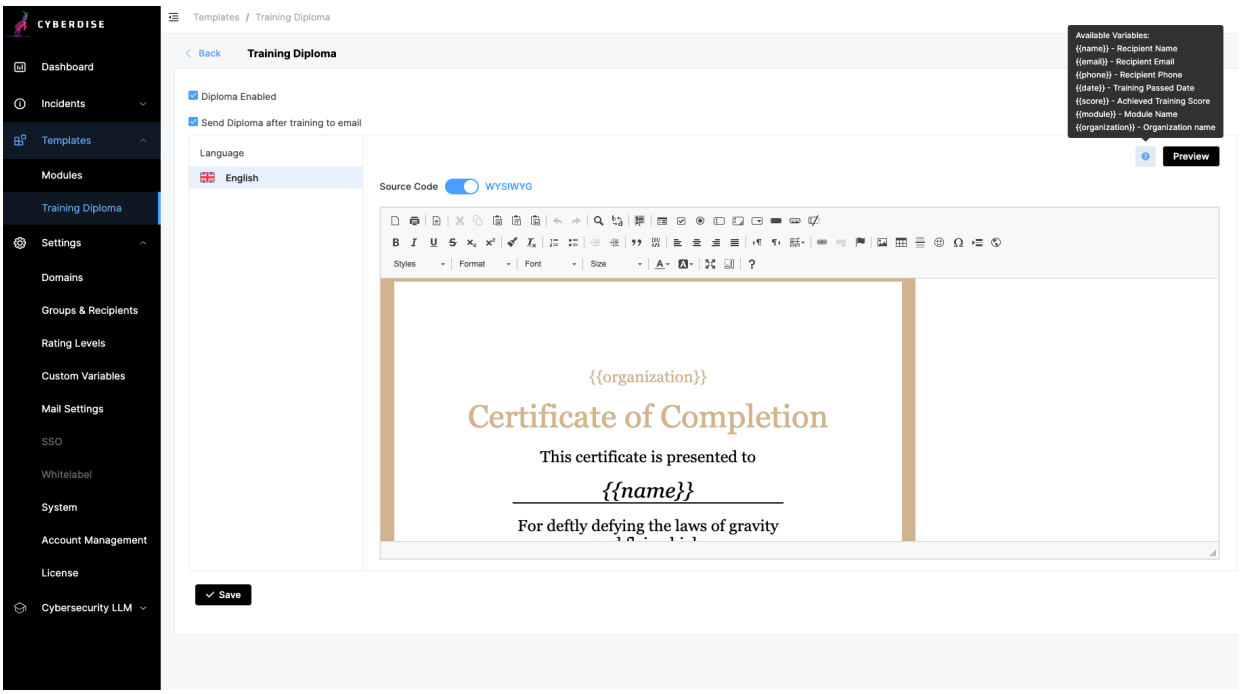
DKIM / S / MIME Support For Phishing E-Mails: Digital signatures for emails: Send signed phishing simulation mails (s/mime). Use DKIM to get a better sender score

Skill-Based E-Learning: Train your employees according to their required skills. Measure employee abilities and enable friendly competition between colleagues (gamification).Based on the ranking profiles of each end user, the system can automatically provide them with multiple training sessions. The ranking profiles are based, among other factors, on the user's behavior in phishing simulations. This ensures that users who are repeated offenders receive different training content from those who click on an attack simulation for the first time.

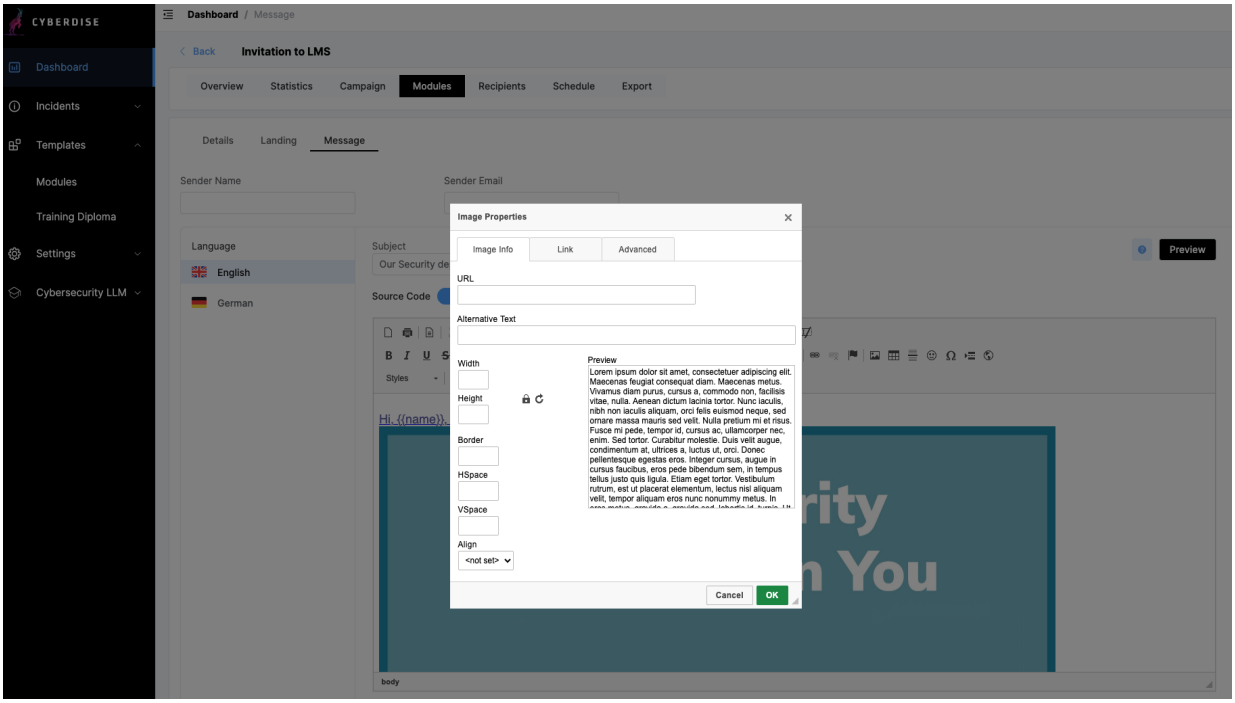
Learning Management System (LMS) functionality: Gives each employee permanent access to a personalized training homepage that features your own courses specifically tailored for them. On this homepage they can view their performance statistics, resume or repeat training, create course certificates, and compare their results with other departments or groups.



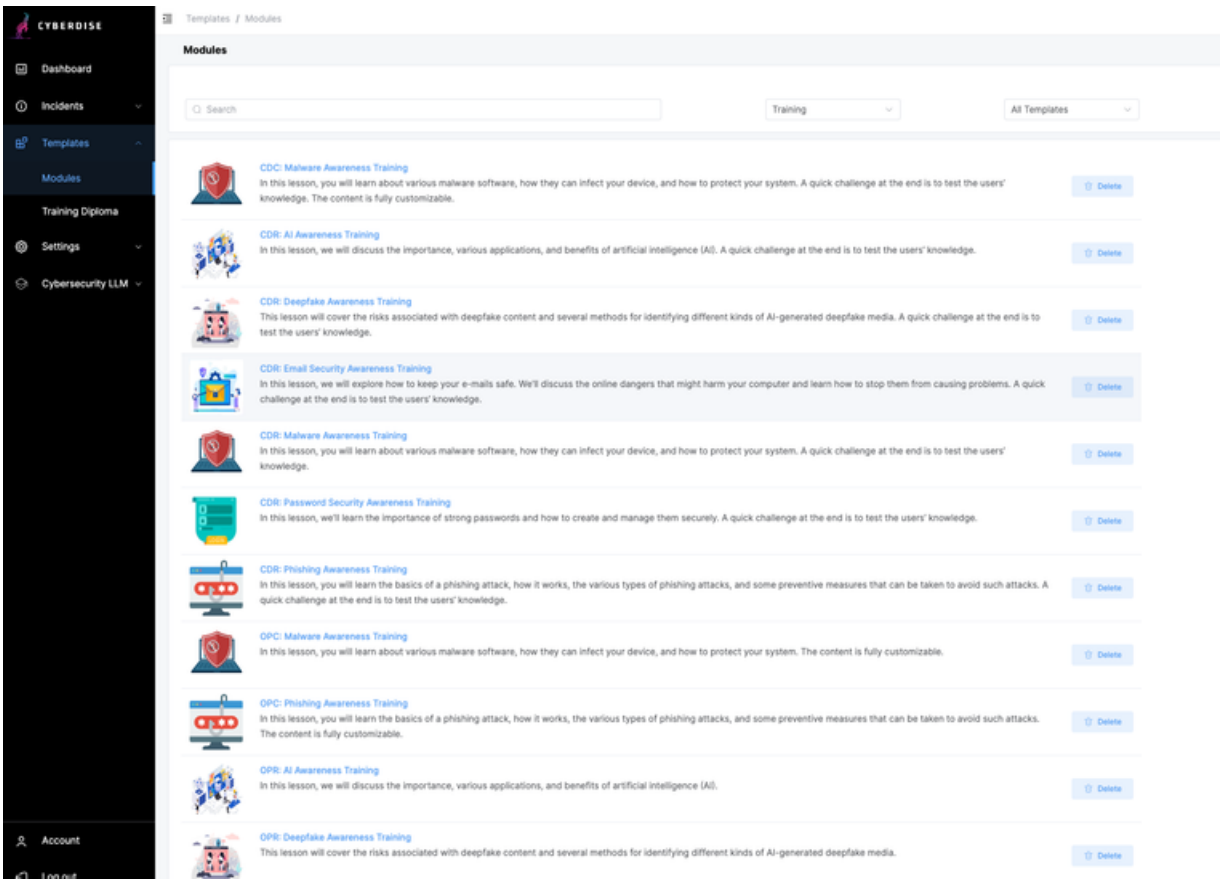
Training Diploma or Certificate: Certificates of e-Learning can be created and printed out by the user either directly within a training or inside the users LMS (Learning Management System).



E-Learning Authoring Toolkit: The e-Learning Authoring Toolkit (Adapt) allows the creation of individualized learning content. Drag and drop videos or any other rich media format, insert exams from pre-defined menus, create interactive e-learning content from scratch in a short time.



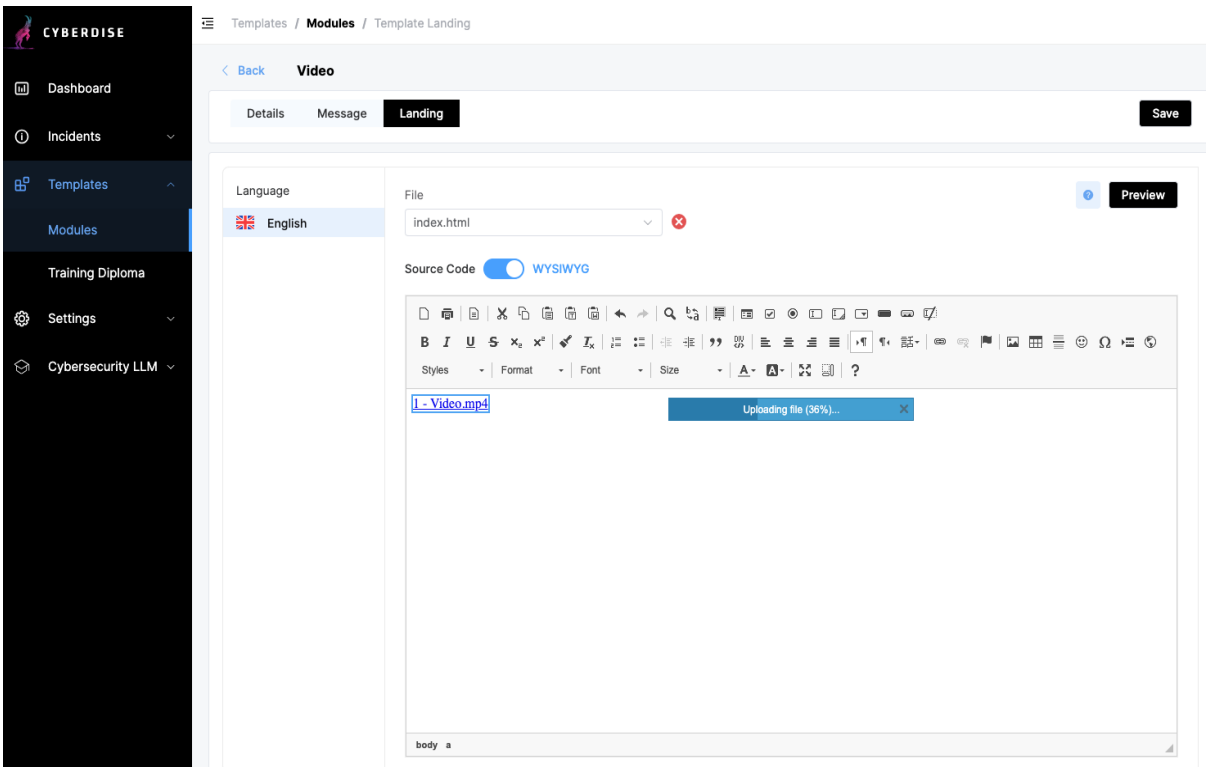
Training Library: contains a large selection of Cyberdise's regular e-learnings. The amount of available modules depends on the given license.



Static Training Support: Training content can also be published on static pages within Cyberdise or the intranet, giving the user permanent access to training content, independent of possible phishing exercises

Offline Training Support: Cyberdise is supplied with a series of editable templates (Adobe Photoshop or Illustrator files) for awareness training, such as posters, screensavers, fliers, etc.

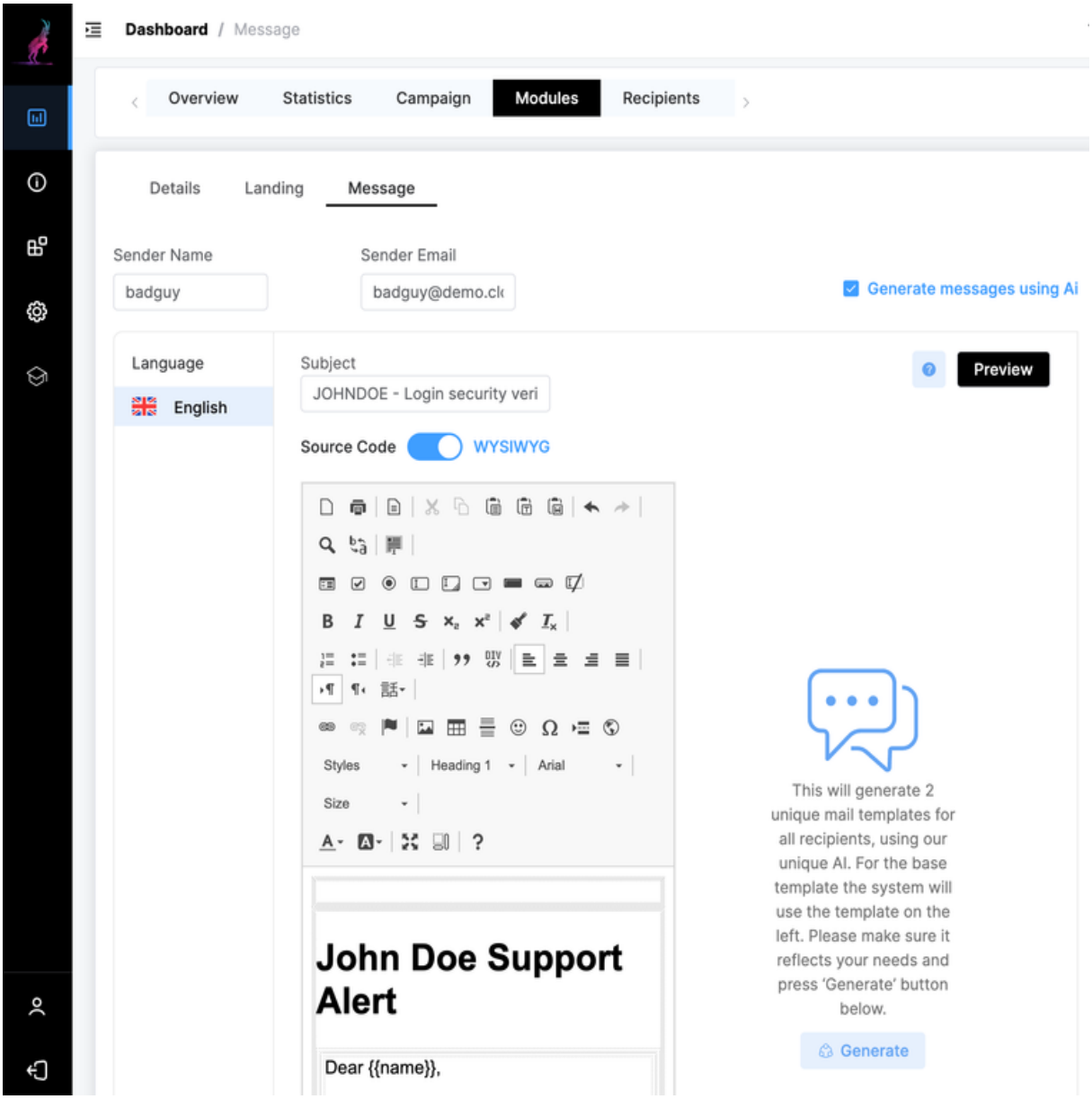
SCORM & Video Import/Export and Player: You can export Cyberdise videos and other training modules to your own LMS, intranet or similar. You can do it also the opposite way: import your own e-learnings, trainings and educational videos into Cyberdise.Use 3rd party Trainings also in Cyberdise using the SCORM interface and its SCORM Player. Track and report exam results like it would be a training module from Cyberdise.



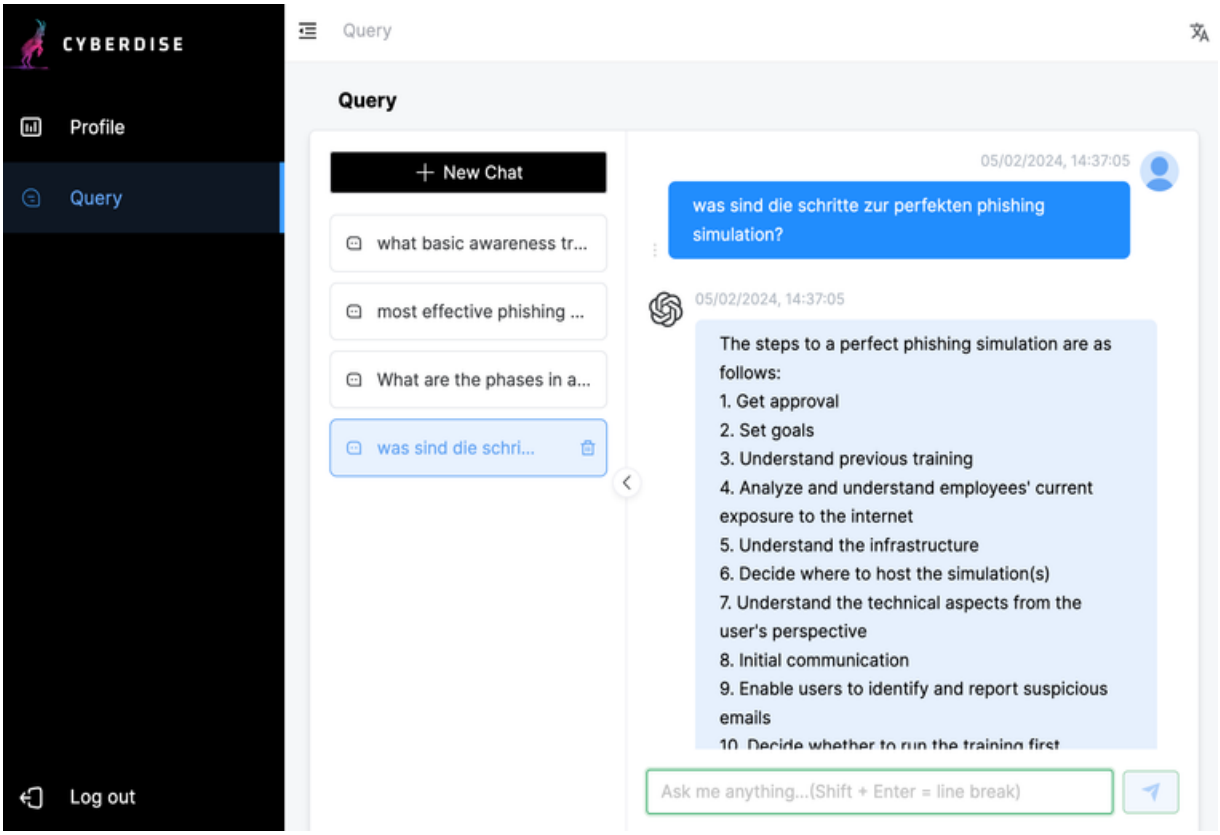
Dynamic Training Hints: The implemented dynamic hints allow your admin/operator to set markers within the attack templates that could indicate to your employees, inside the e-learning material, where the phishing attack may have been detected.

AI FEATURES

Phishing Exercise AI Assistant: The PEAA tailors simulated attacks according to your specific selections and needs. It generates personalized spear phishing simulation messages and also constructs an initial version of a landing page for the simulated attack, all based on your provided criteria.



Cybersecurity Chatbot: When it comes to cybersecurity, every company should first communicate its own policies and guidelines to its employees. Store your regulations and documents in Cyberdise LLM and allow your employees to ask questions with the help of the cybersecurity chatbot and have them answered based on your stored regulations, guidelines and documents!



Operator Chatbot: Ask the operator chatbot for help configuring awareness campaigns or setting up the system.

Custom Training Modules: Create individual training content tailored to your organization and employees, which is tailored to the current company context and, if desired, also includes exam questions that relate to your own guidelines.

Deep Fake Phishing Exercise: Create the most deceptive phishing scenarios with the help of advanced AI support. Train your best users with simulations with convincing and sophisticated messages and landing pages that have been created using deep fake techniques but are still recognisable as deceptive.

End of Document