The background is a blue-tinted image of a person in a business suit holding a smartphone. Overlaid on this image are various white digital graphics, including lines, circles, and icons like a padlock and a lightbulb, suggesting a high-tech or digital theme.

D3.1 Digital Learning Platform and Teaching Tools v1

Set up the Digital Learning Platform and Teaching Tools for the online masters programme

Table of Contents

About the Digital4Security project.....	4
The Digital4Security Consortium	4
Document control information	6
Digital Learning Platform and Teaching Tools	7
Introduction	7
Objectives.....	7
Launch of the Digital Learning Platform and Teaching Tools.....	8
Student access.....	8
Technical architecture	9
Middleware Moodle data structure	10
Simplified entity relationship diagram.....	11
Chosen LMS — Moodle.....	13
Moodle framework.....	14
Moodle information architecture.....	16
Moodle user interface design	16
Moodle homepage	21
Accessibility.....	26
Academic access	28
Synchronous (real-time) learning.....	30
Asynchronous (self-paced) learning	30
Third party services	30
Platform Video Tool.....	31
Word processing software.....	31
Intelliboard	31
H5P interactive content	31
Flip (formerly Flipgrid).....	31
Miro.....	31

Video streaming platform	31
MOSS	31
Proctored (timed) exams	32
Labs	32
Full Fabric	33
Full Fabric	33
Digital4Security admissions process and candidate lifecycle with FULL FABRIC.....	36
Admissions/enrolment process narrative	39
Step 1.....	39
Step 2	39
Step 3.....	40
Step 4.....	40
Step 5	43
Step 6.....	43
Step 7	43
Step 8.....	43
Step 9.....	44
Step 10	44
Step 11	44
Transcript.....	45
Payment plan.....	45
Selecting courses:	45
Tuition payment.....	46
Student Enrolled.....	46
Full Fabric API Introduction.....	46
Emails	54
Applicant accesses the admissions' portal:	55
Applicant creates an account/logs in:.....	55
This is what the applicant will see once logged in:	56
Admissions Criteria Page:	57
Eligibility PASS:	58

Hosting.....	59
Technical Support	61
GDPR	62

About the Digital4Security project

Digital4Security is a groundbreaking pan-European master's programme aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. With funding of almost €10 million from the European Union, this four-year initiative is led by a Consortium of 34 partners spanning 14 countries. This industry-driven programme will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

WP3 is responsible for the programme development and setup. This deliverable *T3.1: Set up the digital learning platform and tools for the online cybersecurity master's programme, Output 14: (Digital Teaching Tools and Platform)* aims to develop and deploy a Digital Learning Platform that integrates all technical solutions needed to provide an adaptive, cohesive experience for all stakeholders involved. Every component, from content management, data processing, security governance, task and process automation, reporting, and insights to the basics of communication and collaboration, will be implemented in the system.

The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide.

No.	Role	Short name	Partner	Country
1	COO	POLITEHNICA BUCHAREST	NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST	RO
2	BEN	SA	SCHUMAN ASSOCIATES SCRL	BE
3	BEN	Ataya	ATAYA & PARTNERS	BE
4	BEN	POLIMI	POLITECNICO DI MILANO	IT
5	BEN	CMIP	POLSKI KLASZTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	PL
6	BEN	Contrader	CONTRADER SRL	IT
7	BEN	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	IE
8	BEN	indiepics	INDEPENDENT PICTURES LIMITED	IE

9	BEN	MATRIX	MATRIX INTERNET APPLICATIONS LIMITED	IE
10	BEN	PROFIL KLETT	PROFIL KLETT D.O.O.	HR
11	BEN	ServiceNow	SERVICENOW IRELAND LIMITED	IE
12	BEN	UNIBS	UNIVERSITA DEGLI STUDI DI BRESCIA	IT
13	BEN	UDS	UNIVERSITY OF DIGITAL SCIENCE GGMBH	DE
14	BEN	SKILLNET	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	IE
15	BEN	IT@CORK	IT@CORK ASSOCIATION LIMITED LBG	IE
16	BEN	ADECCO TRAINING	ADECCO FORMAZIONE SRL	IT
17	BEN	UNI KO	UNIVERSITAT KOBLENZ	DE
18	BEN	BRNO UNIVERSITY	VYSOKÉ UCENÍ TECHNICKÉ V BRNĚ	CZ
19	BEN	MTU	MUNSTER TECHNOLOGICAL UNIVERSITY	IE
20	BEN	DIGITAL SME	EUROPEAN DIGITAL SME ALLIANCE	BE
21	BEN	DIGITALEUROPE	DIGITALEUROPE AISBL*	BE
22	BEN	MRU	MYKOLO ROMERIO UNIVERSITETAS	LT
23	BEN	UNIRI	SVEUCILISTE U RIJEKI	HR
24	BEN	NASK	NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA - PAŃSTWOWY INSTYTUT BADAWCZY	PL
25	BEN	UNIR	UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	ES
26	BEN	NCI	NATIONAL COLLEGE OF IRELAND	IE
27	BEN	TERAWE	TERAWE TECHNOLOGIES LIMITED	IE
28	BEN	CY CERGY PARIS	CY CERGY PARIS UNIVERSITE	FR
29	BEN	BANCO SANTANDER	BANCO SANTANDER SA	ES
30	BEN	CYBER RANGES	CYBER RANGES LTD	CY
31	BEN	RED OPEN S.R.L.	RED OPEN S.R.L.	IT
32	BEN	VMU	VYTAUTO DIDŽIOJO UNIVERSITETAS	LT
33	AP	FHG	FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG EV	DE
34	AP	Pearson Benelux	Pearson Benelux BV	NL

Document control information

Project	Digital4Security
Document title	D3.1 Digital Learning Platform and Teaching Tools v1
Work Package number	WP3
Deliverable number	D3.1
Lead beneficiary	Matrix Internet
Project coordinator:	National University of Science and Technology POLITEHNICA Bucharest (NUSTPB)
Dissemination level	Sensitive — limited under the conditions of the Grant Agreement
Authors	Fionnuala Mahon, Timea, Brian Power, Tomas Herink, Matrix Internet
Reviewers	Conor McCaffrey, Matrix Internet (1st level review) POLITEHNICA Bucharest and SA (2nd level review) POLITEHNICA Bucharest (final review)
Description	Set up the Digital Learning Platform and Teaching Tools for the online masters programme
Status	Final
Delivery date	10.10.2024
Due date	31.10.2024
Approval date:	31.10.2024

Revision history

Version	Date	Modified by	Comments
1	10.10.2023	Fionnuala Mahon, Matrix Internet	Draft for QA review
2	31.10.2023	Brian Cochrane, SA Bogdan Costel Mocanu, Politehnica Bucharest	QA reviewers
3	31.10.2023	Florin Pop, Politehnica Bucharest	Final review
4	31.10.2023	Giuseppe Ditaranto, Fionnuala Mahon, Matrix Internet	Final review and layout

Digital Learning Platform and Teaching Tools



Introduction

T3.1 objective: The aim of T3.1 was to design, develop and deploy the Digital4Security Digital Learning Platform, connecting it to the project website www.digital4security.eu. This platform will be the central hub for promoting the programme, recruiting students and onboarding participants from across Europe.

The Consortium has chosen Moodle LMS, integrated with the Full Fabric system, for end-to-end management of admissions, enrolments, and CRM. This setup combines open-source and commercial tools to provide a seamless experience for students. Once registered in the platform students can undertake their online lessons, select and register for events, and manage all aspects of their programme progress all within this one platform.

Moodle's advanced analytics will support the evaluation of key metrics like course enrolment, admissions, engagement, and dropout rates. A variety of tools were identified to support both real-time (synchronous) and on-demand (asynchronous) learning, ensuring a well-rounded educational experience.

The backend will provide full programme management facilities for administrators and faculty. The portal will be fully responsive and accessible, optimised for use on multiple devices and different screen resolutions.

Objectives

The Digital Learning Platform was designed with the following key objectives in mind:

- A goal of developing an online master's programme that is highly accessible, affordable and convenient, ensuring it can reach the widest range of students from diverse demographics, backgrounds and countries;
- to design a sustainable and scalable European master's programme platform that minimises financial requirements and investment for participating higher education institutions (HEIs).

Launch of the Digital Learning Platform and Teaching Tools

The platform is being iteratively designed, developed, deployed and refined to support the delivery of the master's programme. It is being released in phases:

- Demo;
- Pilot;
- Version 1.0. The Digital Learning Platform and Teaching Tools will offer online training materials, certifications, and resources for the train-the-trainer programme to support the related goals and deliverables D3.2, D3.3, D3.4 and D3.5 for Work Package 3.

Student access

Students will engage with the system at different stages of their journey. We have developed multiple access points to facilitate this:

1. Information gathering

At the initial stage, users will collect details about the programme, such as eligibility requirements and pricing. The general public will be able to get all necessary information at <https://digital4security.eu>.

2. Application process

When prospective students are ready to apply, they will follow the application link on the website, which directs them to the Full Fabric student enrolment platform. The application process will be hosted at <https://my.digital4security.eu>, which will also serve as the main student dashboard.

3. Interacting as a student

By default, students will access the whole platform via <https://my.digital4security.eu>, which will link to individual courses hosted on the LMS at

<https://learn.digital4security.eu>.

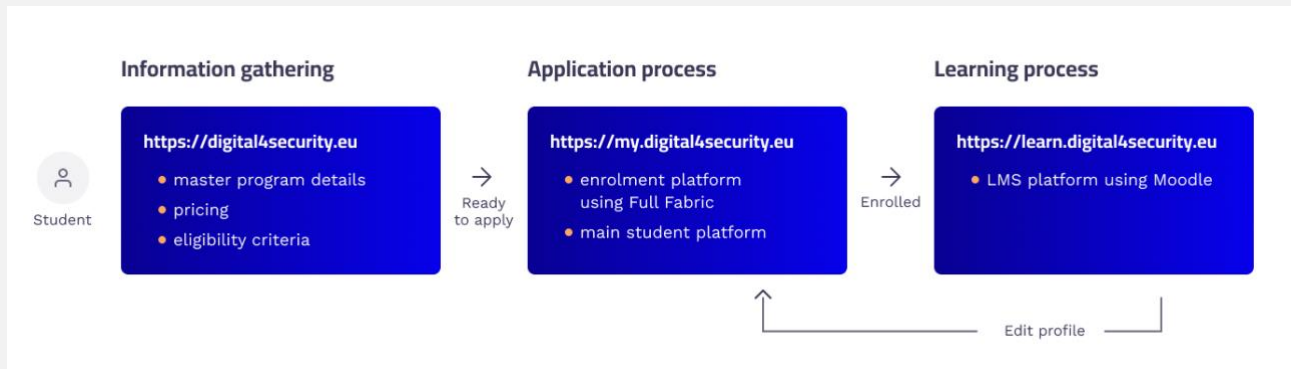


Figure: Student access flow and process.

Technical architecture

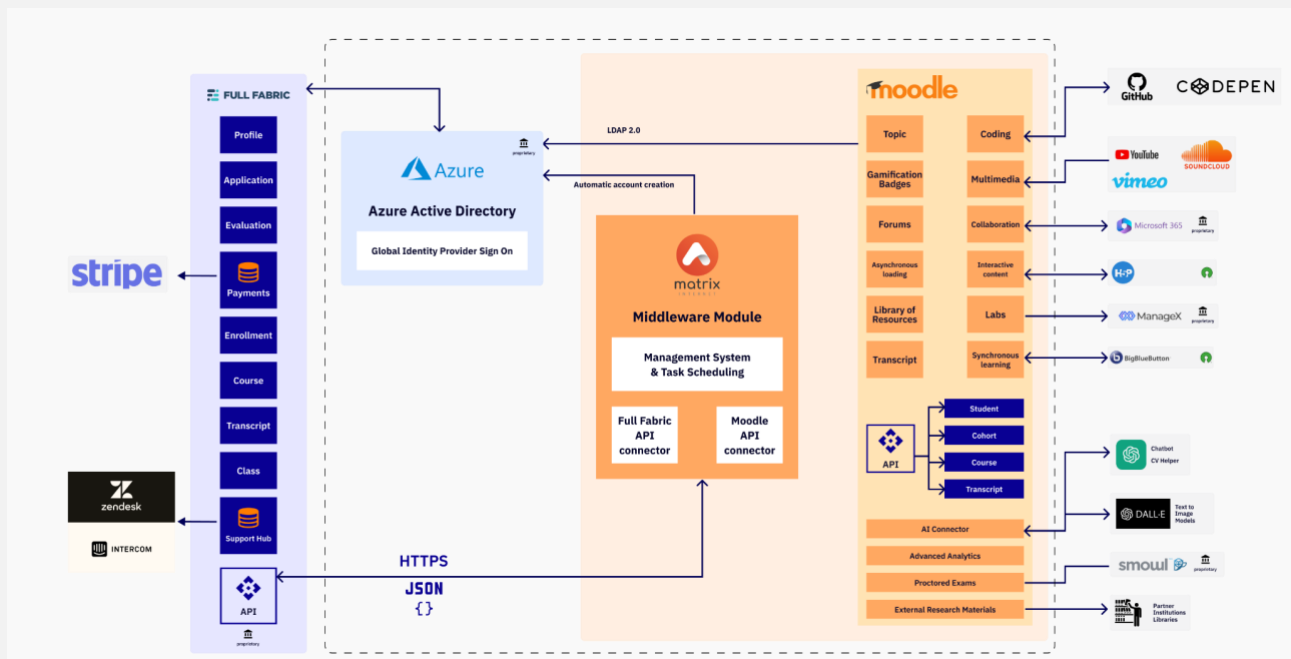


Figure: Architecture design of the learning platform.

This technical architecture diagram illustrates the system's various components and how they interconnect.

1. The system has three main components:
 - a. Full Fabric:

- i. Student Information System;
 - ii. Admissions;
 - iii. CRM.
- b. LMS system:
 - i. A Moodle instance hosted on a primary web server;
 - ii. A bespoke middleware facilitating seamless integration and single sign-on (SSO) functionality between Full Fabric and Moodle to facilitate user accounts and SSO.
- c. A variety of chosen third-party components, modules and plugins will provide much of the necessary interactive functionality.

Middleware Moodle data structure

A bespoke middleware application facilitates:

- Communication and data mapping between Moodle and Full Fabric;
- Scheduling of synchronisation tasks;
- Monitoring and alerting.

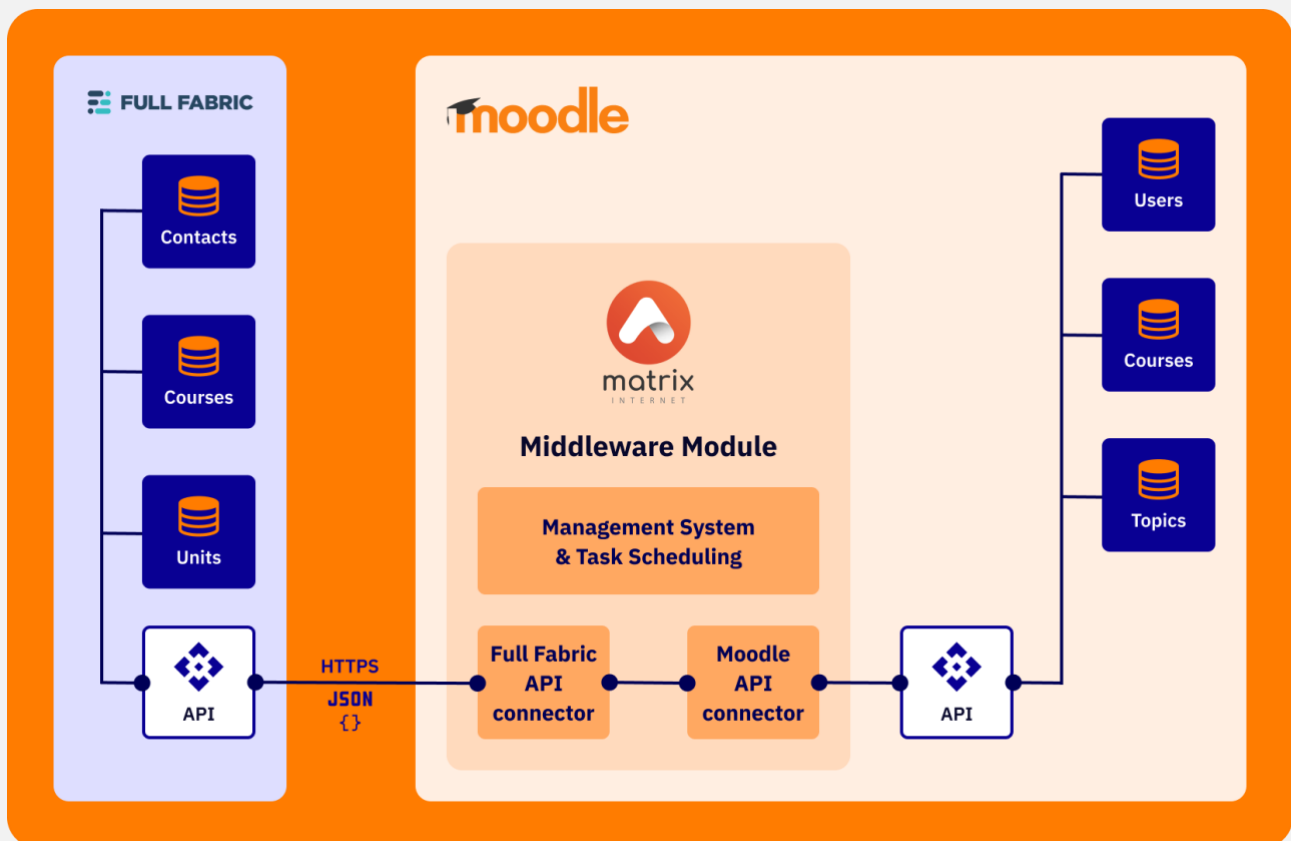


Figure: Middleware module (management system & task scheduling).

The diagram above highlights the key components that must be synchronised between the two systems — the Full Fabric CRM and Student Information System, and the Moodle LMS.

It demonstrates a direct mapping between the main entities in both systems, making them well-suited for integration and ensuring a smooth student experience. The Matrix Middleware Application, highlighted in orange in the diagram, will maintain data synchronisation between the systems and ensure all relevant users are notified about their access to the LMS.

Simplified entity relationship diagram

The following elements need to be synchronised between Full Fabric and Moodle.

1. Profiles > Users
 - a. User data will be synchronised daily overnight, starting the night after their initial application, days before they become students. If an applicant does not convert to a student, personal data will be deleted or anonymised after a specified period, as agreed.

2. Class > Cohort
 - a. Cohorts will be synchronised daily overnight.
3. Courses > Courses and Units
 - a. Empty courses will be created in Moodle overnight for content population.
4. Units > Topic
 - a. Topics will be synchronised together with Courses

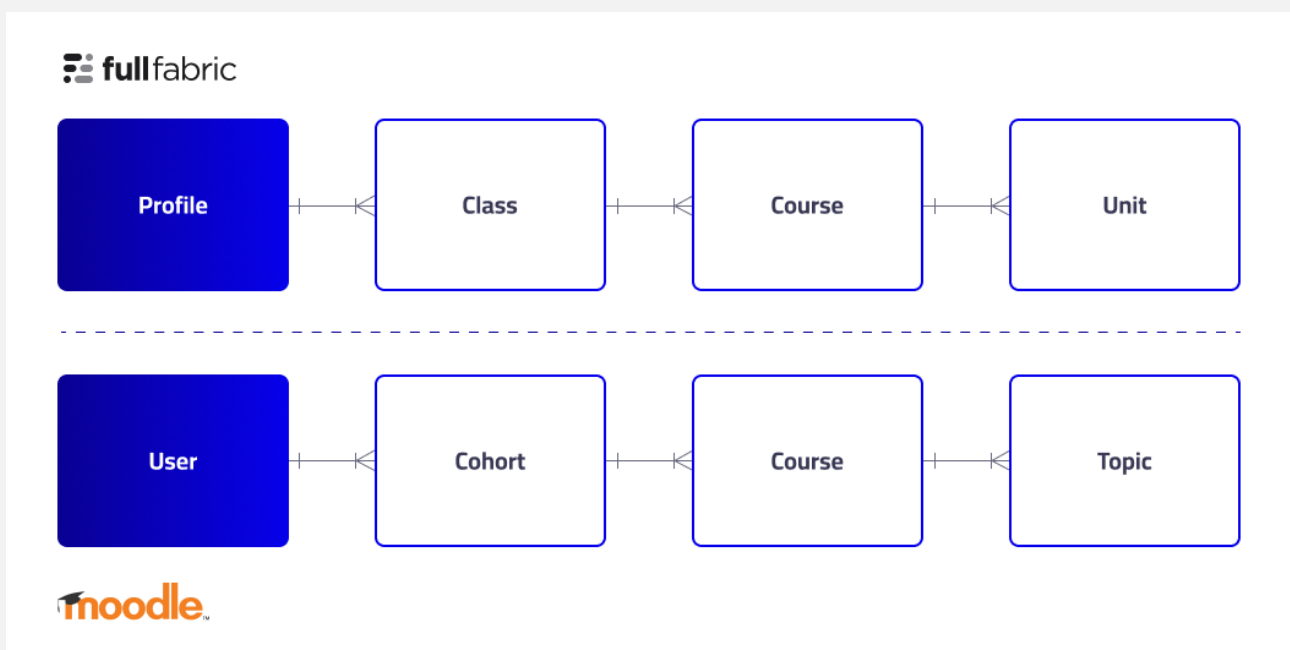


Figure: Simplified entity relationship diagram

Note: Courses map to courses, however, on Moodle courses will actually be called “modules” (for the purposes of this document and to show the mappings we will continue to refer to them as courses LMS.



Chosen LMS — Moodle

The Consortium has chosen Moodle as the platform for delivering the Digital4Security master's. It is one of the world's most widely used learning management systems, with large-scale installations that demonstrate its scalability. Many of our academic partners are already familiar with Moodle, as it is used regularly in their institutions, which reduces the learning curve.

Key features of Moodle include:

- User-friendly and designed with a user-centric approach;
- Comprehensive accessibility system to accommodate users with special requirements, so they can easily navigate and use the platform;
- Facilitates collaborative learning;
- Offers powerful analytics and reporting tools;
- Extensible with a global community of developers;
- Highly modular and open source;
- Supports a wide variety of plugins and integrations.

As of October 2024, Moodle had more than [155,753 active sites](#) registered across 239 countries, with nearly 430 million users.

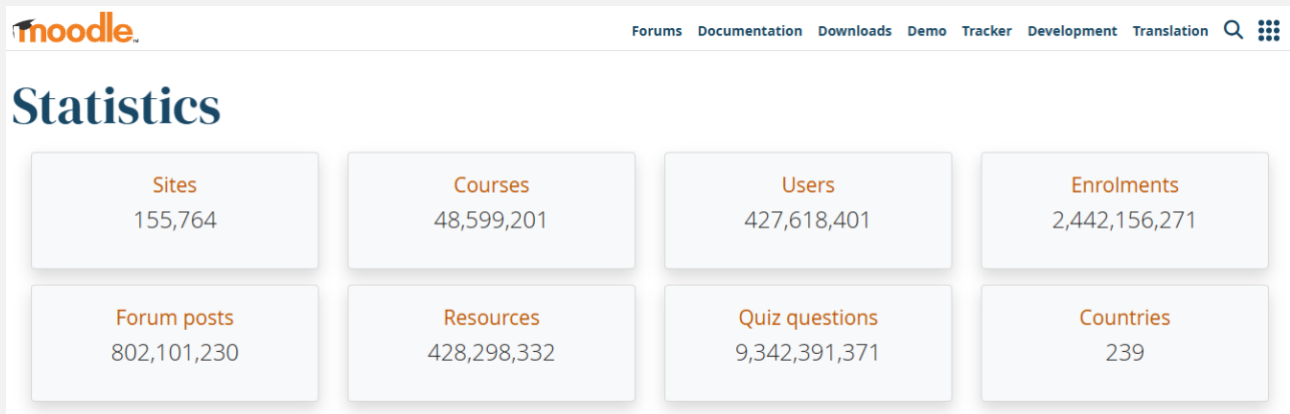
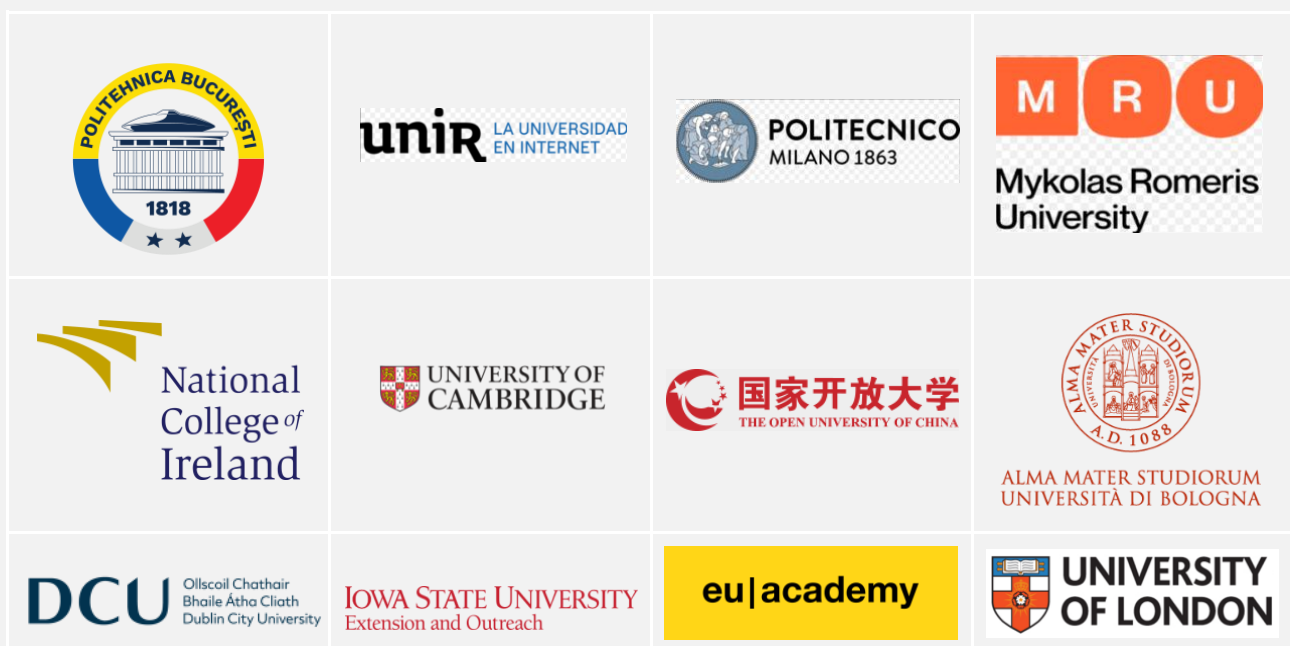


Figure: Moodle statistics according to <https://stats.moodle.org>.

Among the universities using Moodle are *POLITEHNICA* Bucharest, our project coordinator, UNIR, Politecnico Milano, National College of Ireland and MRU, all members of our Consortium.



Moodle framework

Moodle¹ is an open-source learning management system (LMS) designed to provide educators, administrators and learners with a secure and integrated environment for creating personalised learning experiences. It has been customised to meet the needs of Digital4Security. We have enhanced the system by integrating several third-party tools and plugins, adding interactive elements and AI-driven features. The Moodle LMS platform will be built out as follows:

¹ <https://moodle.org>

- Technical architecture (outline in previous section);
- Information architecture;
- User interface design for key pages;
- Assets for landing pages and modules;
- Setup and deployment of Moodle infrastructure;
- Integration of third-party plugins and licences;
- User access and administration;
- Moodle on-boarding and training;
- QA and testing.

Moodle information architecture

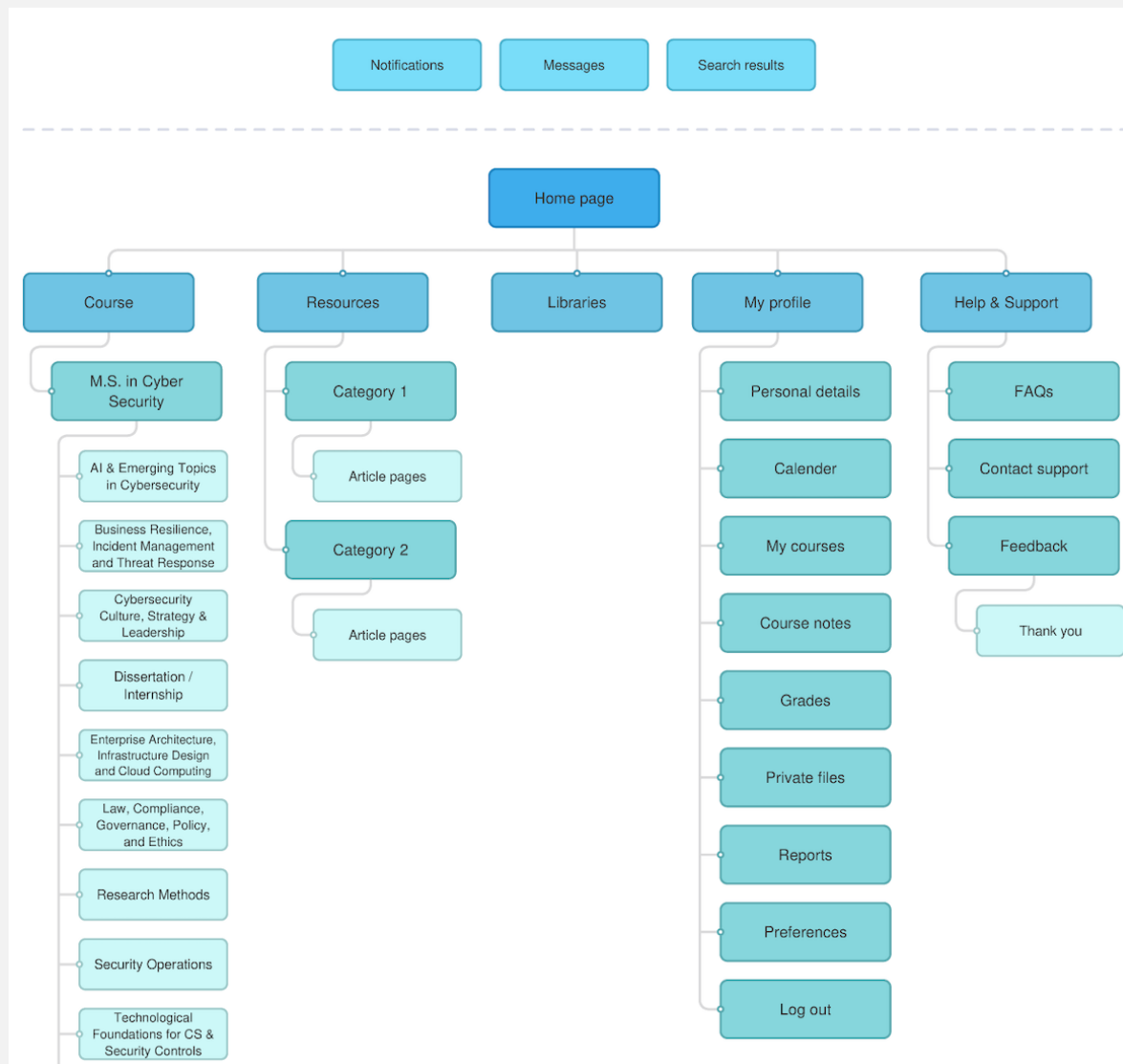


Figure: Information architecture of the Moodle LMS key pages which will include all modules.

Moodle user interface design

The design team created design components, assets and designs for the Moodle platform based on the project branding and accessibility best practices.

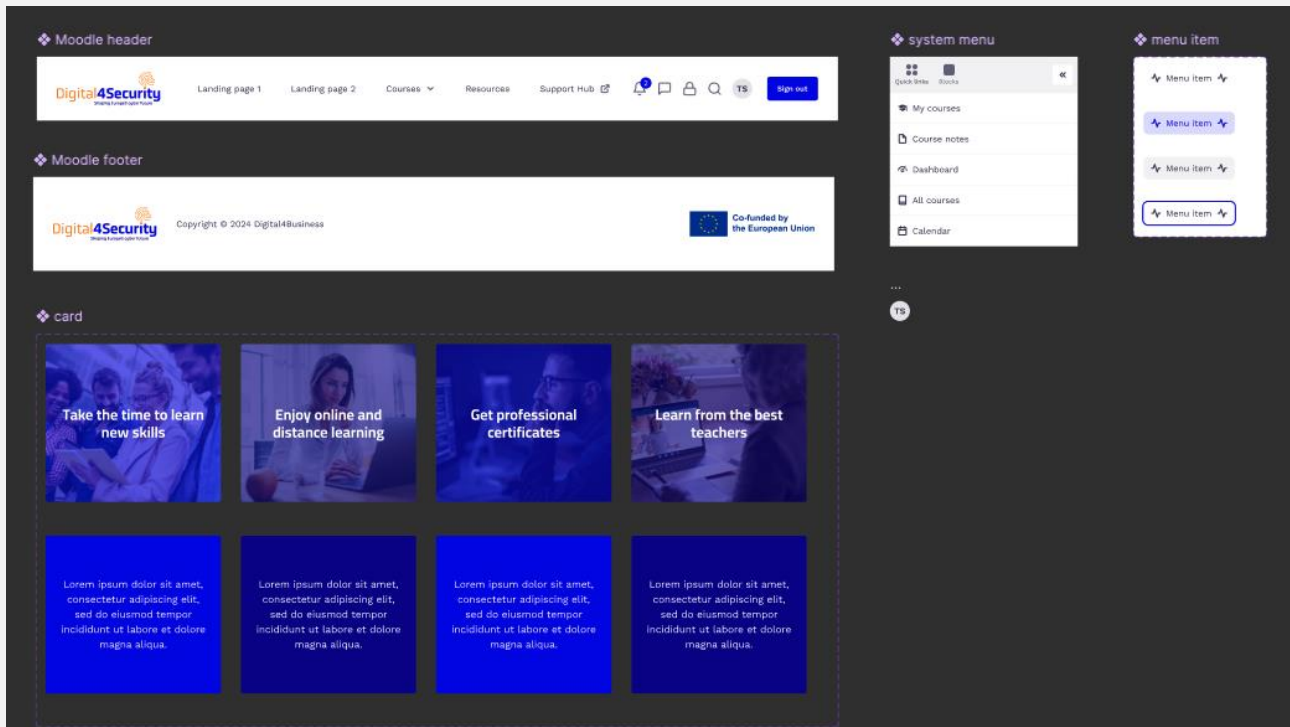


Figure: a series of assets were created to populate the Moodle LMS platform.

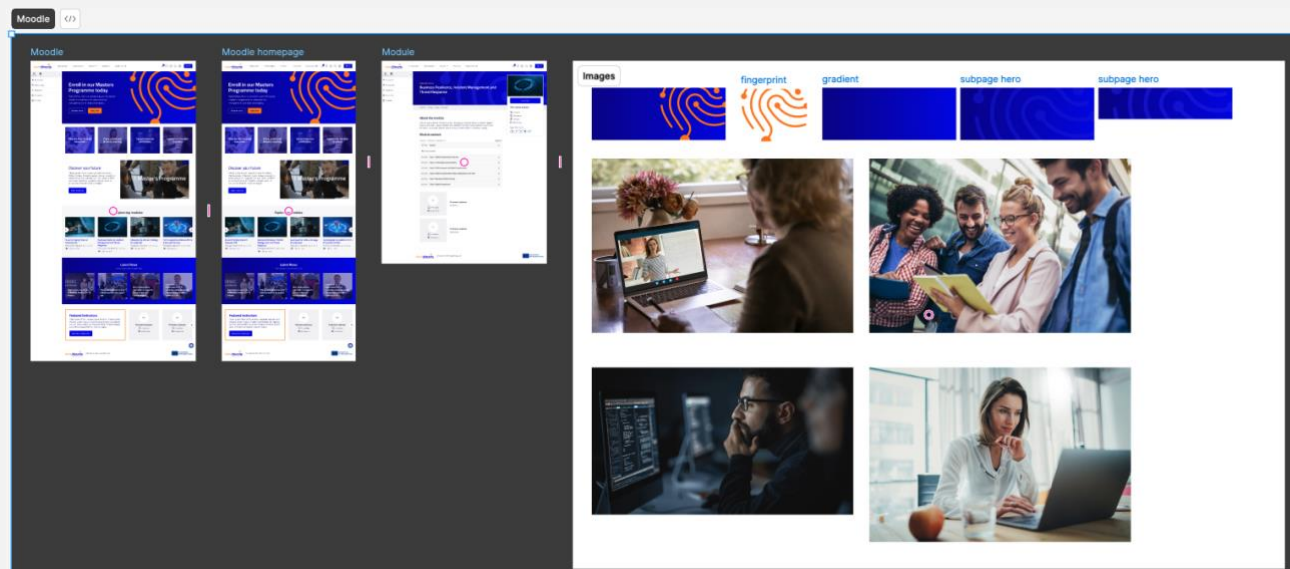


Figure: UI design assets for implementation in the Moodle LMS platform.

Colours

Our design system leverages a purposeful set of color styles as the perfect starting point for any brand or project. When it comes to color, contrast is critical for ensuring text is legible. We've added [WCAG 2.1](#) contrast ratios to our color system so you can make sure you're designing with accessibility in mind.

Primary colours

These are the main colors that make up the majority of the colors used in the design system.

Primary D4S Orange

The primary color is your "brand" color, and is used across all interactive elements such as buttons, links, inputs, etc. This color can define the overall feel and can elicit emotion.

2.58	AAA 9.72
500 #FF7C00	300 #FFA861

Primary Blue

AAA 16	AAA 9.51	AAA 14.66	AAA 18.51
200 #DEDEFF	500 #0600EB	600 #090093	700 #000056

Gradient

AAA 9.51
Gradient

Base

AAA 21:1
White #FFFFFF

D4S Slate

AAA 19.55	AA 11.11	AA 5.27	AAA 13.29	AAA 16.87	AAA 18.94	AAA 19.79
500 #07072B	400 #393955	300 #6A6A8D	200 #CDCDD5	100 #E6E6EA	50 #F3F3F4	10 #F8F8F9

Secondary colours

Along with primary colors, it's helpful to have a selection of secondary colors to use in components such as pills, alerts and labels. These secondary colors should be used sparingly or as accents, while the primary colors should take precedence.

Light blue

AAA 16
500 #DEDEFF

Yellow

AAA 12.1
500 #FFB800

Figure: Digital4Security project brand colours.

Mandatory modules

AI and Emerging Topics in Cybersecurity



Business Resilience, Incident Management and Threat Re...



Cybersecurity Culture, Strategy & Leadership



Elective modules

Automation of Security Tasks and Data Analytics



Crisis Communication



Risk Management of Cyber-Physical Systems



Figure: assets were created for each of the master's modules.

Moodle homepage

The Moodle LMS will be publicly accessible via learn.digital4security.eu

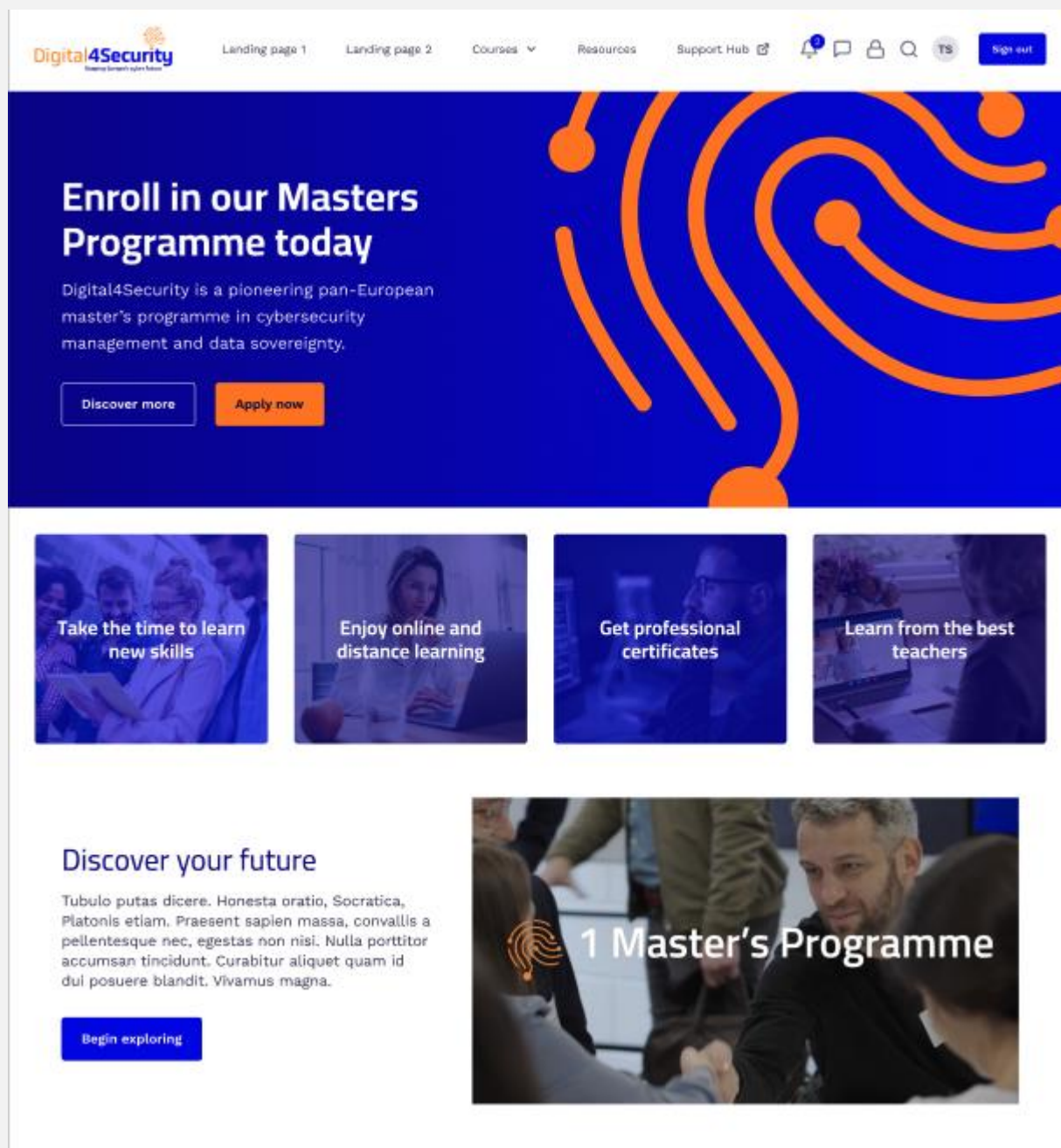


Figure: UI design mockup of the proposed Moodle LMS homepage.

Explore top modules



AI and Emerging Topics in Cybersecurity
Firstname Lastname (and 1 more)
🎓 1 🕒 May 2024



Business Resilience, Incident Management and Threat Response
Firstname Lastname (and 6 more)
🎓 1 🕒 May 2024



Cybersecurity Culture, Strategy & Leadership
Firstname Lastname (and 5 more)
🎓 1 🕒 May 2024



Technological Foundations for CS & Security Controls
Firstname Lastname (and 15 more)
🎓 1 🕒 May 2024

Latest News

Visit our blog to read the latest news



Digital4Security at the
CYBERSEC Forum 2024 in
Poland



The growing importance of
cybersecurity in the digital
age



Why cybersecurity
education is crucial for
Europe's digital
transformation



Launching
Digital4Security: A
groundbreaking European
master's programme in
cybersecurity

Featured Instructors

Tubulo putas dicere. Honestas oratio, Socratica, Platonis etiam. Praesent sapien massa, convallis a pellentesque nec, egestas non nisi. Nulla porttitor accumsan tincidunt. Curabitur aliquet quam id dui posuere blandit. Vivamus magna.

[Become an instructor](#)

MA

Firstname Lastname

📅 4 modules
🎓 50 students

MA

Firstname Lastname

📅 4 modules
🎓 50 students

Figure: UI design of the proposed Moodle LMS homepage.

The Consortium can feature key modules they want students to sign up for, directly on the Moodle homepage, as shown below:



Figure: UI design of the proposed Moodle LMS homepage displaying top modules.

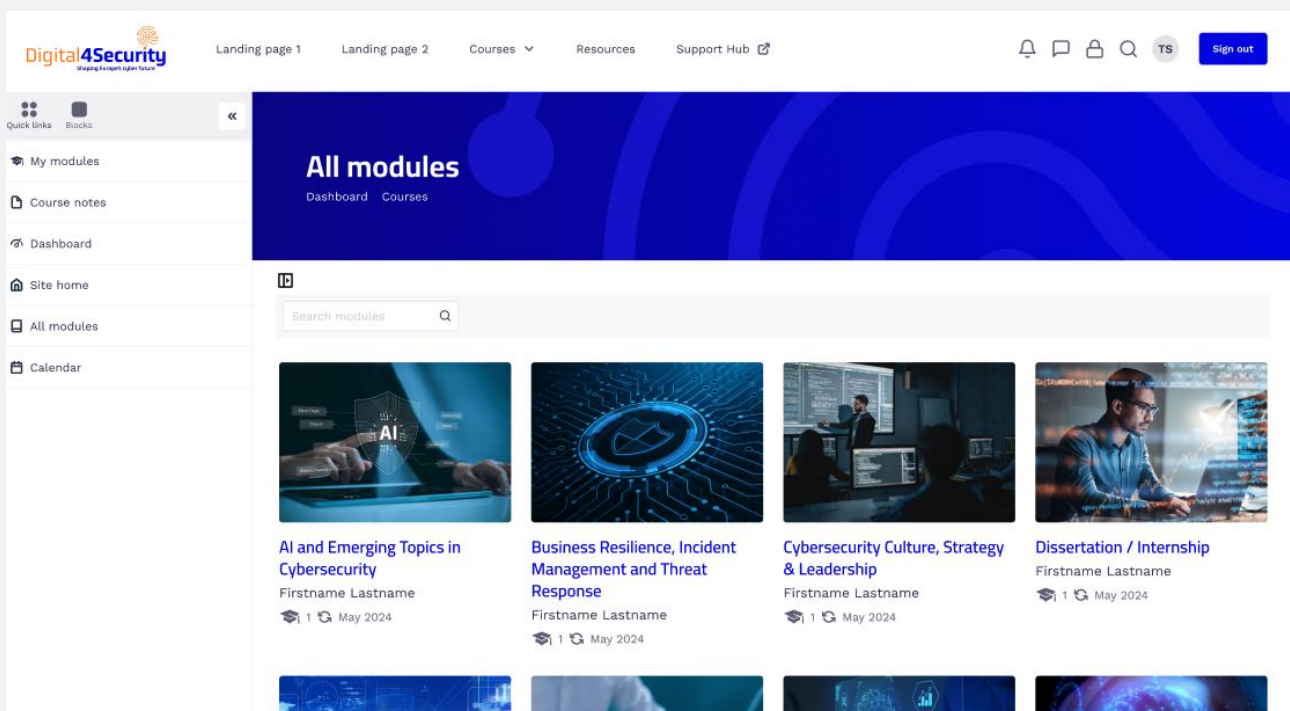


Figure: UI design of how Moodle will display when students are logged in.

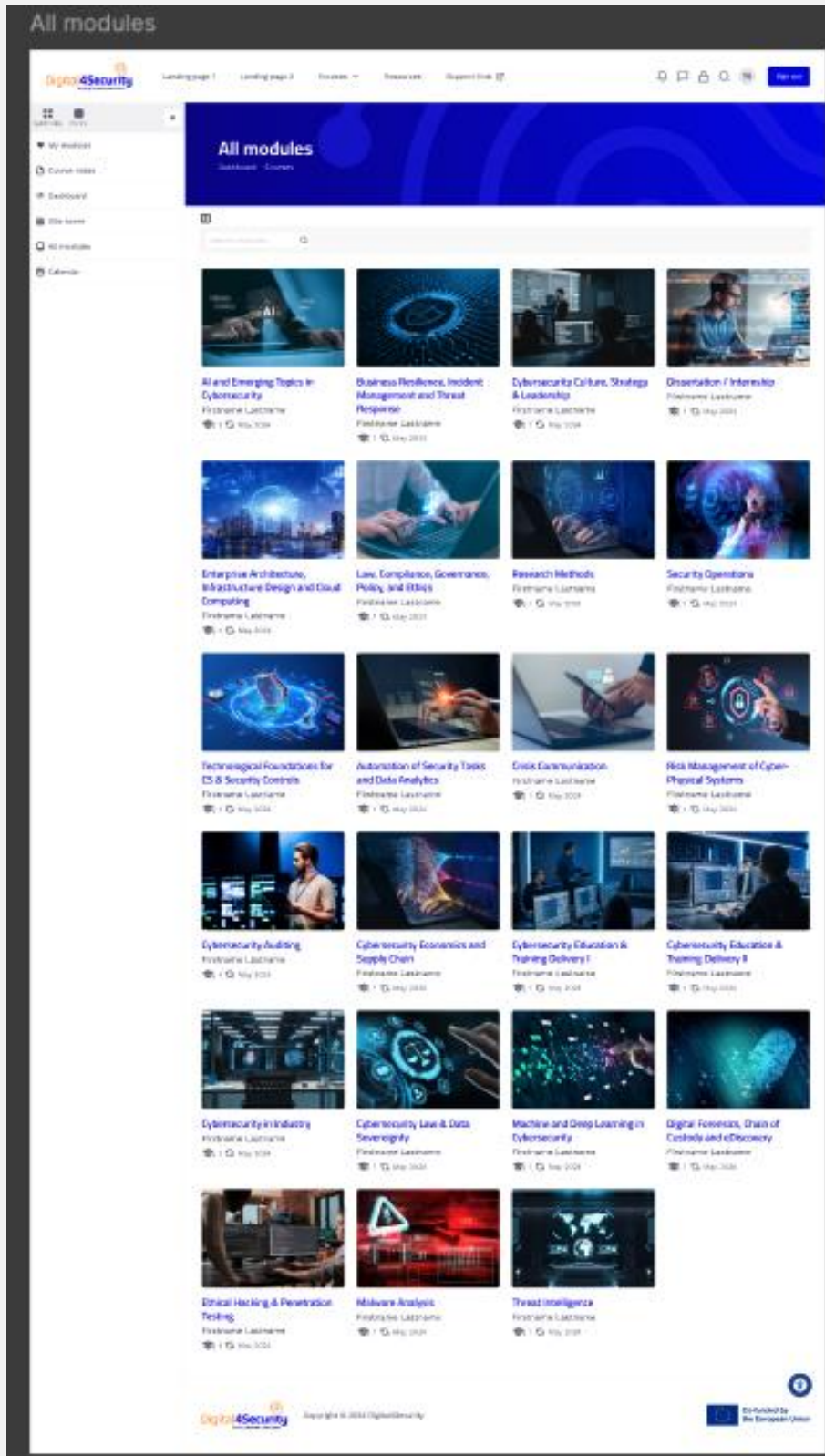


Figure: UI design of how all Moodles will display when students are logged in.

The screenshot displays the Moodle LMS interface for a user logged into the Digital4Security platform. The top navigation bar includes links for 'Landing page 1', 'Landing page 2', 'Courses', 'Resources', and 'Support Hub'. A sidebar on the left contains a 'My modules' section with links to 'Create notes', 'Dashboard', 'All modules', and 'Calendar'. The main content area features a blue header with the title 'Business Resilience, Incident Management and Threat Response' and a 'Create new' button. Below the header, there is a section titled 'About the module' with a paragraph of placeholder text. A 'Module content' section lists various topics under different sections, with a 'Expand all' link. On the right, a 'This module includes' sidebar lists 'Forums', 'Glossaries', 'Quizzes', and 'Resources', along with social sharing options. At the bottom, there are two user profile cards showing 'Firstname Lastname' and 'Resources'. The footer includes the Digital4Security logo, copyright information, and a 'Co-funded by the European Union' badge.

Figure: UI design of Module landing page when logged into the Moodle LMS.

Accessibility

In configuring Moodle, we implemented a comprehensive accessibility system to accommodate users with special requirements, so they can easily navigate and use the platform. We have included some images to demonstrate examples of some of the accessibility features available in the Digital4Security Moodle LMS.

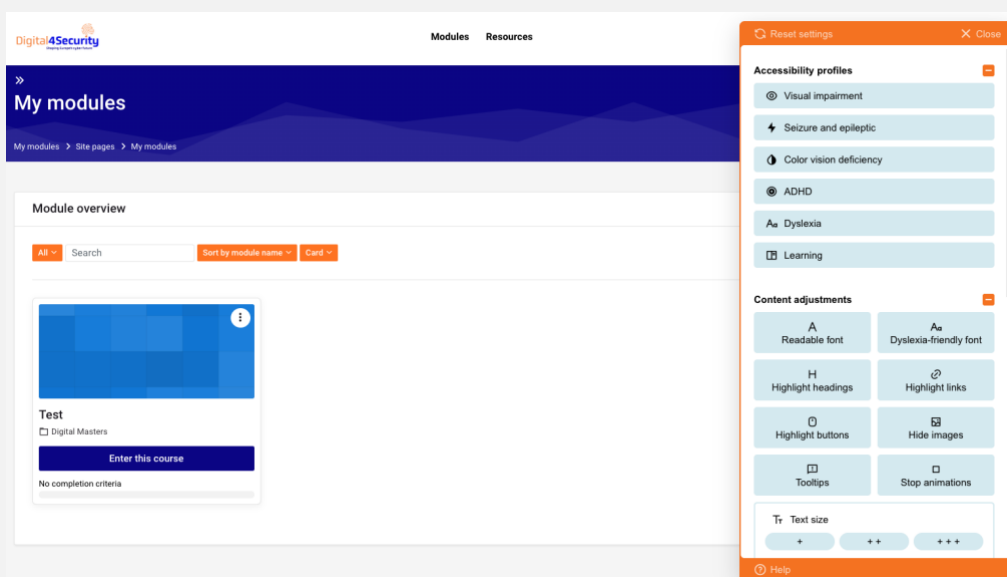


Figure: showing how the accessibility can be adjusted as required within the Moodle platform.

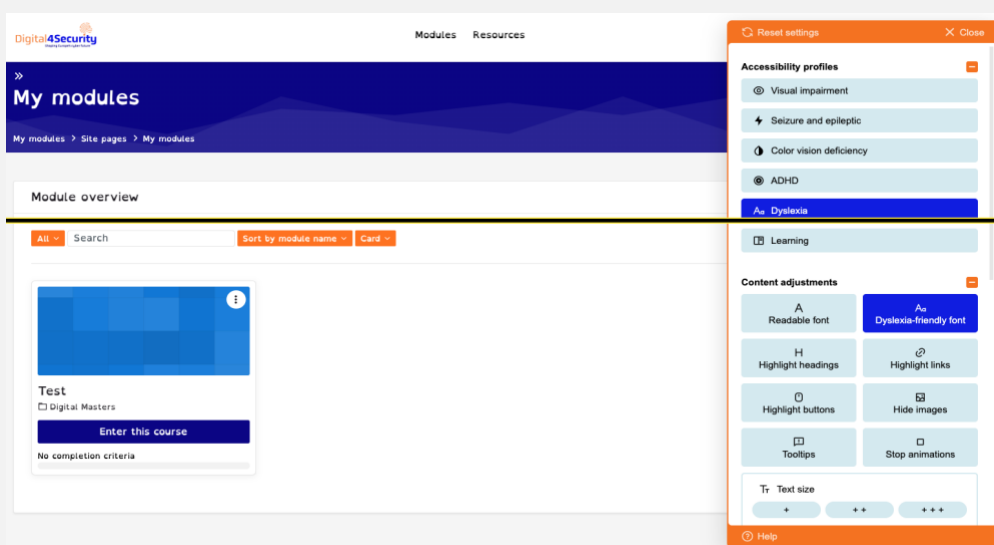


Figure: showing how the accessibility can be adjusted as required within the Moodle platform.

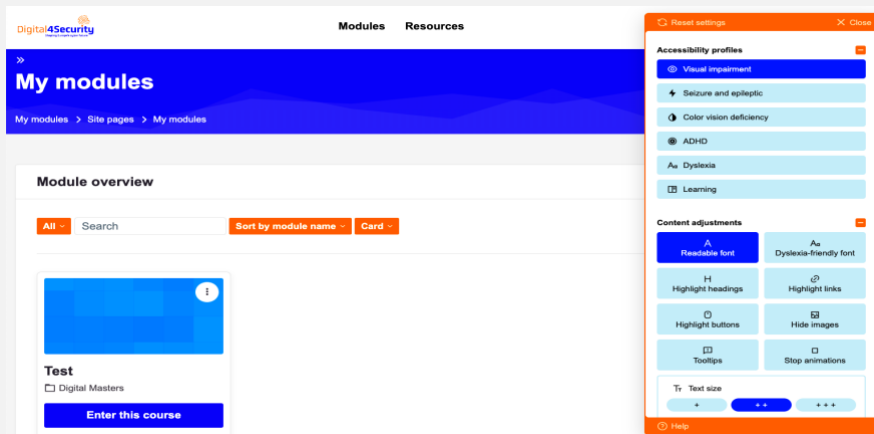


Figure: showing how the accessibility can be adjusted as required within the Moodle platform

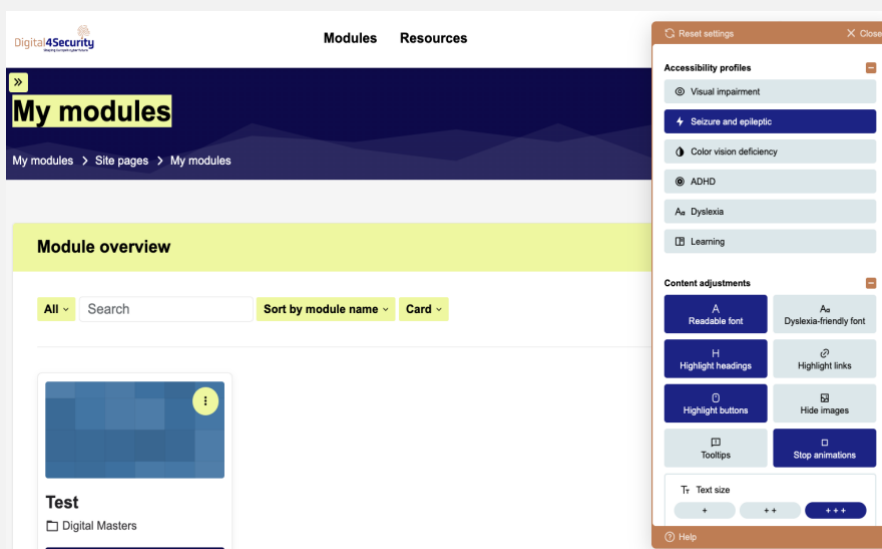


Figure: showing how the accessibility can be adjusted as required within the Moodle platform.

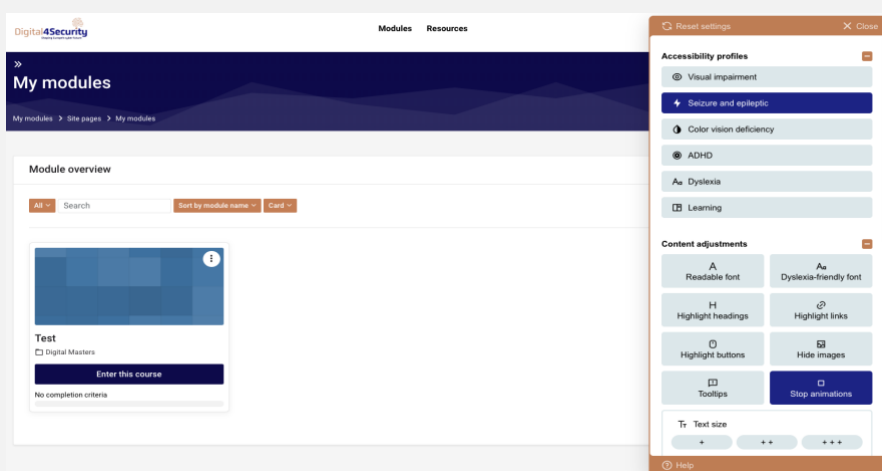


Figure: showing how the accessibility can be adjusted as required within the Moodle platform.

Academic access

Academic access is managed by the platform's development partner, granting access with the necessary permissions as needed, and upon request.

Here is a preview of the academic access of a lecturer assigned to Module as a teacher to be able to add the materials for each Module in Moodle:

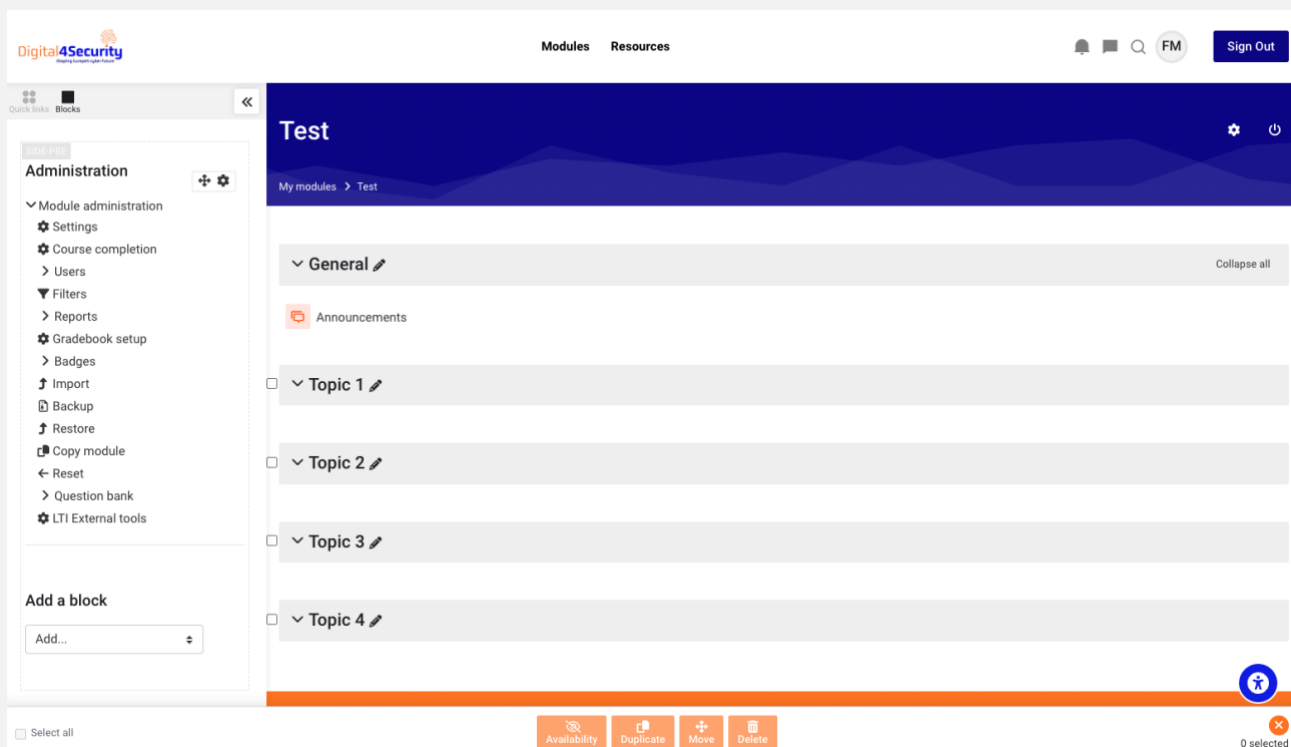


Figure: academic access to Moodle.

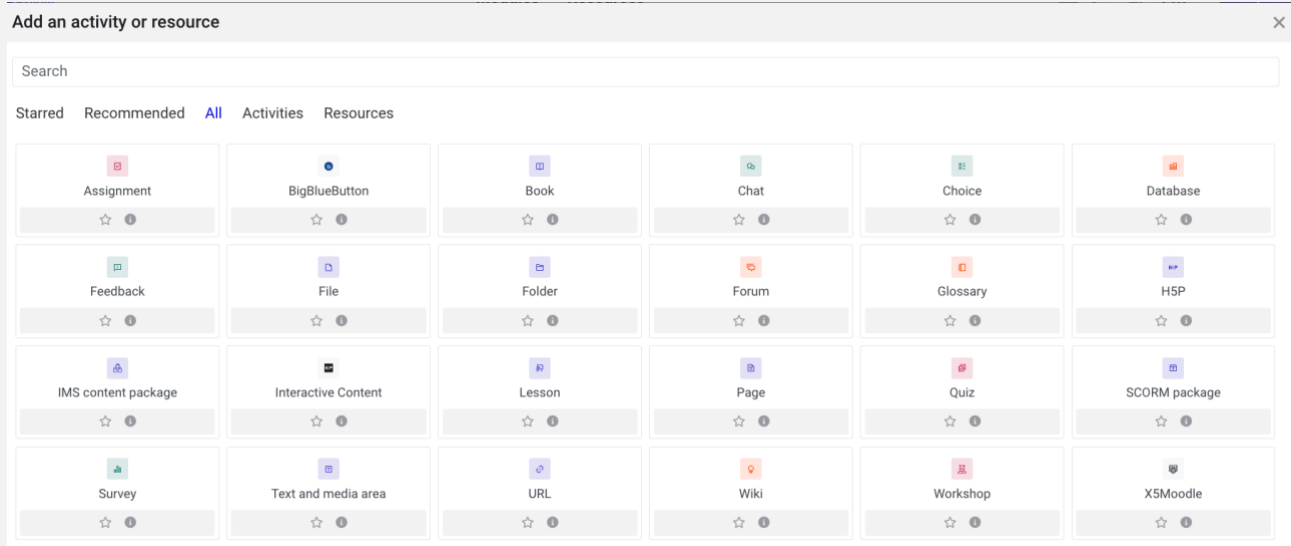
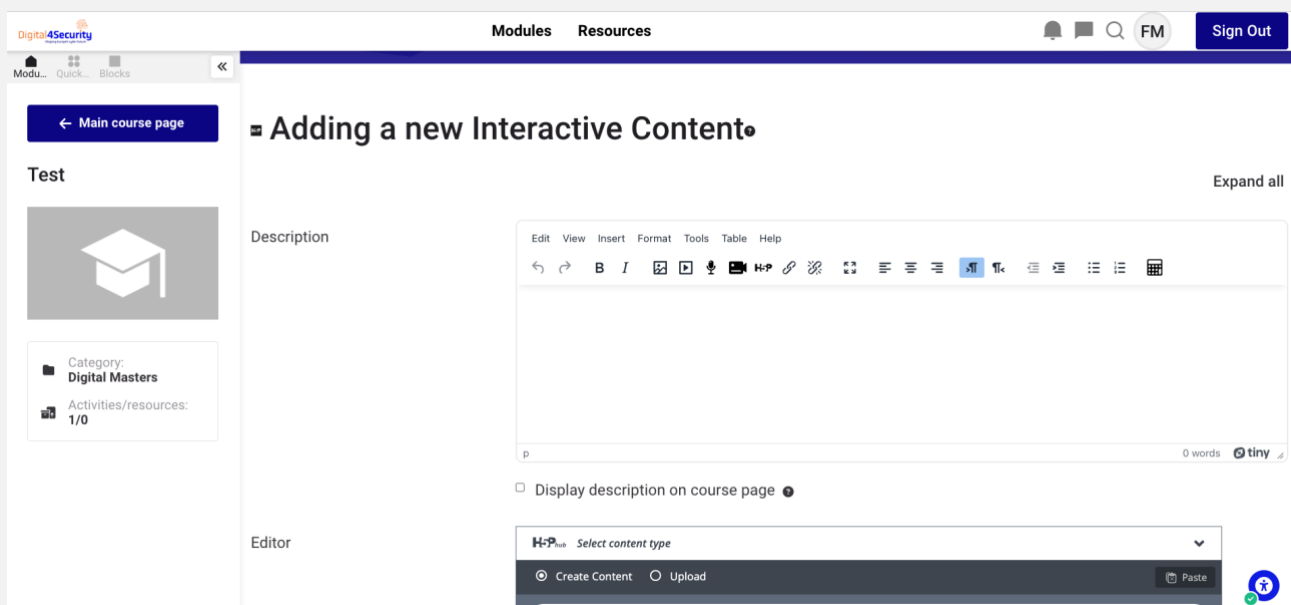


Figure: showing how an academic can add an activity or resource to Moodle



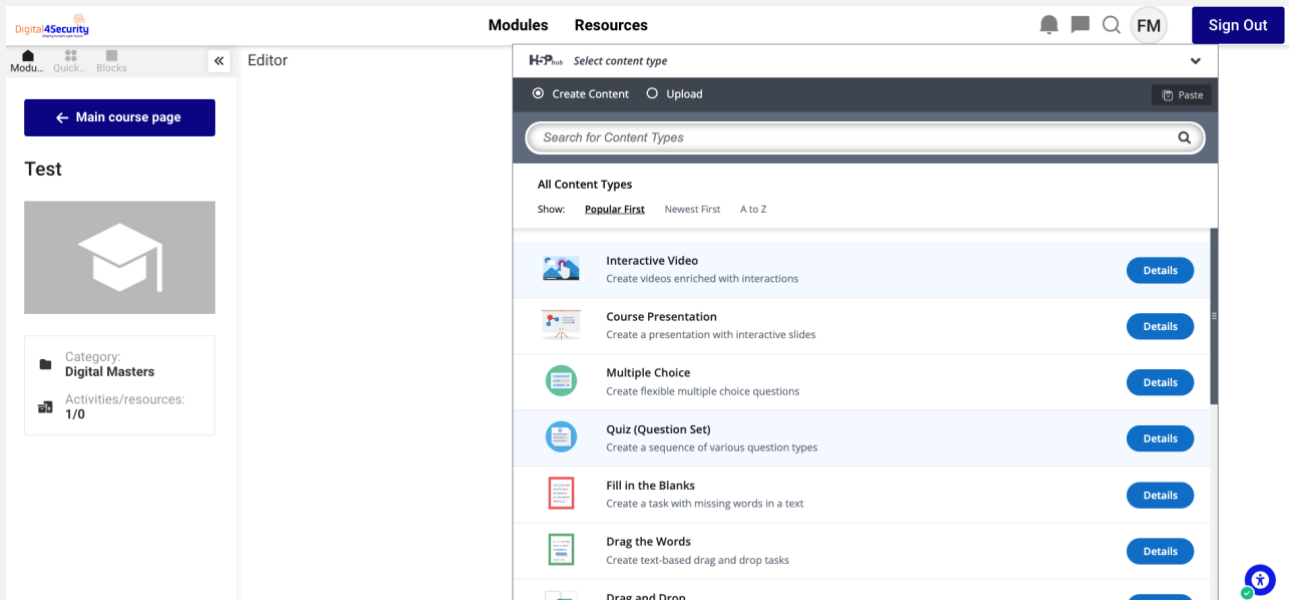


Figure: showing how an academic can add interactive content to Moodle

The Train the Trainer Programme deliverable leaders have created a comprehensive template to guide all academics on the creation content for population on Moodle.

Synchronous (real-time) learning

To facilitate synchronous learning we are integrating and using a number of third party tools, such as The Big Blue Button for delivering live lessons.

Asynchronous (self-paced) learning

Self-paced learning will be a key component of the Master's programme. To support this, we are leveraging the full capabilities of Moodle, along with additional tools outlined here. We will also investigate if we can enable access to the academic partner libraries.

Third party services

Matrix implemented a platform with the tools required to deliver an immersive platform. The academic Partners reviewed and compiled a list of requirements for delivering a more adaptive experience for all platform stakeholders, including those involved in the Train the Trainer programme.

Platform Video Tool

For real-time learning, for the pilot we've selected Big Blue Button. This platforms allow for live teacher training through video links, and come equipped with features like video sharing, whiteboards and breakout rooms to enhance the learning experience. Based on the students feedback we will evaluate if this is the best platform video tool.

Word processing software

We will investigate the best solution for giving students access to tools to create reports, assignments, and more, to ensure that all submissions are in a standardised format.

Intelliboard

Intelliboard, an analytics extension for Moodle, retrieves and analyses platform data, identifying areas for improvement and addressing any issues.

H5P interactive content

HTML5 Package (H5P) allows educators to create interactive content like videos, quizzes and presentations.

Flip (formerly Flipgrid)

Flip is a free app from Microsoft that lets educators set up secure groups for students to engage with the curriculum through short video, text and audio messages.

Miro

Miro is a third-party tool that enables users to create interactive whiteboards, which can be embedded using an HTML embed code.

Video streaming platform

Ideally we would like to use Vimeo as it is a completely ad-free video streaming service that enables customised configurations and streaming of video content to specific destinations. Users can embed videos with full control over the content that appears at the end. However initially we will utilise YouTube as we already have an account setup

www.youtube.com/@Digital4security

MOSS

MOSS integrates with Moodle to detect source code plagiarism in assignments

Proctored (timed) exams

Moodle supports basic exam proctoring through plugins. For more advanced proctoring, it integrates with solutions like Smowl, offering a comprehensive proctoring experience.

Labs

In the later phases of the digital learning platform, we will assess the need for labs and explore Moodle add-ons and CyberRanges as potential solutions. Pilot testing and review will help us to select the best option for Digital4Security students.

Full Fabric



Full Fabric

Full Fabric² is a comprehensive admissions and enrolment platform that streamlines the process of recruiting, admitting and enrolling students at scale.

Full Fabric includes the following basic blocks:

1. “Foundation” CRM system;
2. “Origin” admissions system;
3. “Core” student information system.

Full Fabric handles the entire student user experience and workflows outside of the learning content, which is managed by the Moodle LMS system.

Full Fabric covers the following aspects of the user journey:

- Eligibility process;
- Student application;
- Onboarding;
- Remarketing and reminders (GDPR-compliant);
- Online payments;

² <https://www.fullfabric.com/>

- Course enrolment;
- Student dashboard and links to LMS.

We have agreed the following Implementation plan:

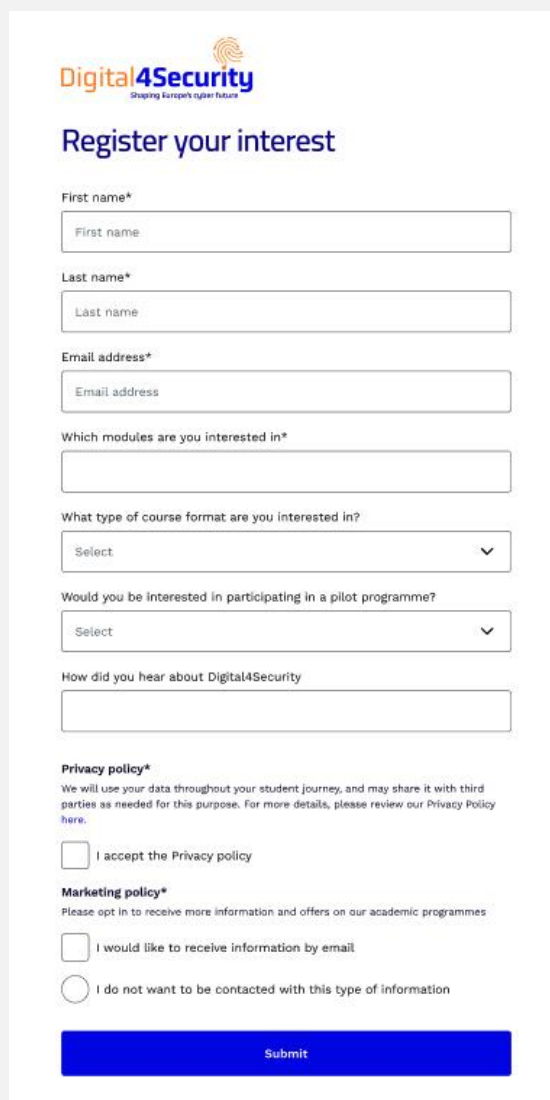
- Phase 0 - Pilot;
- Phase 1 - Application Form;
- Phase 2 - Evaluation and Acceptance/Rejection;
- Phase 3 - Enrolment.

The following tasks will be completed as part of the process:

- Weekly call for integration;
- Process mapping;
- Assets for applying branding on platform;
- Setup of subdomain, dns management, emails for administration of Full Fabric and student communication;
- Related required policies for remarketing and reminders (GDPR-compliant);
- Register your interest form fields and setup - needs to be setup as as soon as possible to start outreach;
- Integration of required forms on project website;
- All automated emails styling and content writing;
- Course setup - programme and intake;
- API integration;
- Student application form architecture and content, setup, review, consortium outreach for feedback, QA and testing;
- Offer letter content and styling;
- Payment gateway and online payment;
- Student on-boarding and access to LMS;
- Accreditation certificate content, stamps and styling, issuing process of accreditation;
- Admissions process, criteria and administration;

- Application Evaluation process, implementation and testing;
- Administration on-boarding for rollout of Masters and courses;
- Ongoing QA and review and end-to-end testing once full integration complete.

Our primary focus was getting a "Register Your Interest" form created to start capturing students interested in applying for the Masters: <https://www.digital4security.eu/register-your-interest/>



Digital4Security
Shaping Europe's cyber future

Register your interest

First name*

Last name*

Email address*

Which modules are you interested in*

What type of course format are you interested in?

Select ▼

Would you be interested in participating in a pilot programme?

Select ▼

How did you hear about Digital4Security

Privacy policy*
We will use your data throughout your student journey, and may share it with third parties as needed for this purpose. For more details, please review our Privacy Policy [here](#).

☐ I accept the Privacy policy

Marketing policy*
Please opt in to receive more information and offers on our academic programmes

☐ I would like to receive information by email

☐ I do not want to be contacted with this type of information

Submit

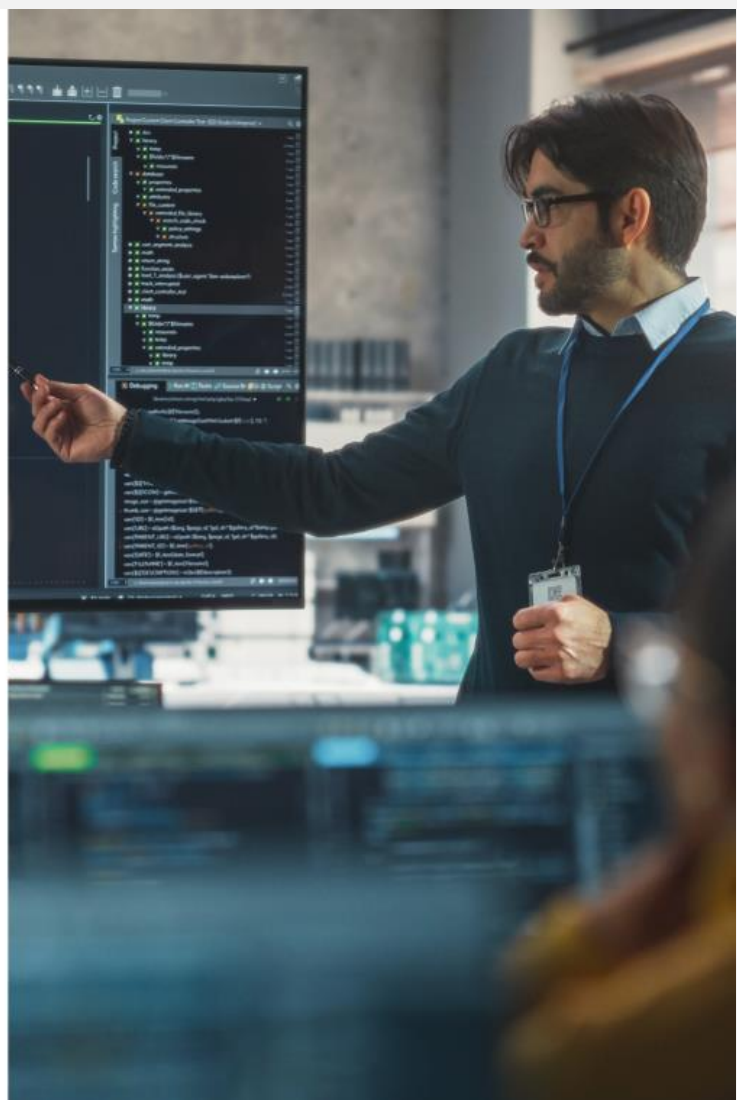


Figure: shows a UI mockup the 'Register Your Interest' form.

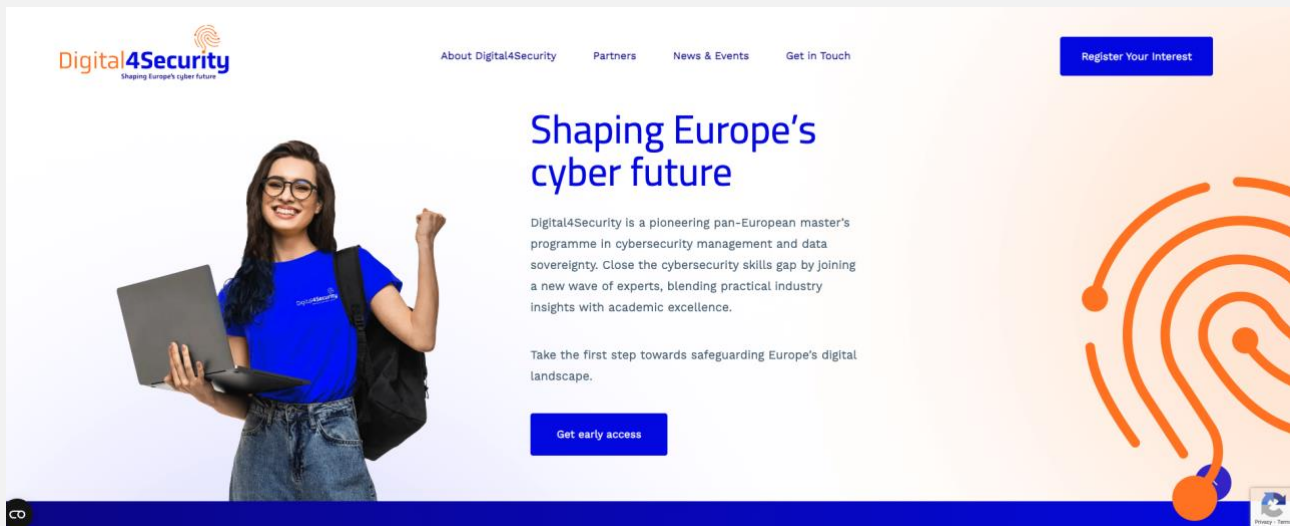


Figure: shows the registration form embedded on the project website linked to on the main navigation on all website pages via a 'Register Your Interest' CTA

Digital4Security admissions process and candidate lifecycle with FULL FABRIC

The steps below outline the planned admissions process for Digital4Security's admissions team and the candidate life cycle. This process will be adjusted as needed based on insights from pilot testing and user feedback.

Suggested prospect lifecycle in Full Fabric

Prospect state	Description
Cold	The prospect has signed up on the portal
Pass Eligibility	The prospect has submitted and passed the eligibility assessment
Fail Eligibility	The prospect has submitted and failed the eligibility assessment
Started application	The prospect has started an application

Suggested applicant lifecycle in Full Fabric

Applicant state	Description
Submitted	The applicant has submitted their application
Incomplete	The applicant has uploaded unreadable files and needs to provide them again
Rejected	Applicant has been rejected by the admissions team after initial review
Admitted	The applicant has been admitted by the admissions team after initial review
Needs Board Review	The applicant has been reviewed by the admissions team and needs to be reviewed by the Admissions Board
Board Admitted	The applicant has been admitted after the Admissions Board review
Board Rejected	The applicant has been rejected after the Admissions Board review
Acceptance Submitted	The applicant has completed their offer acceptance form
Registered	The applicant has completed the registration form where they selected the modules they will be doing as part of their programme and paid the relevant fees
STUDENT Enrolled	The profile is fully enrolled
*Withdrawn	The profile has decided to withdraw the application – this sub-state is available throughout the lifecycle

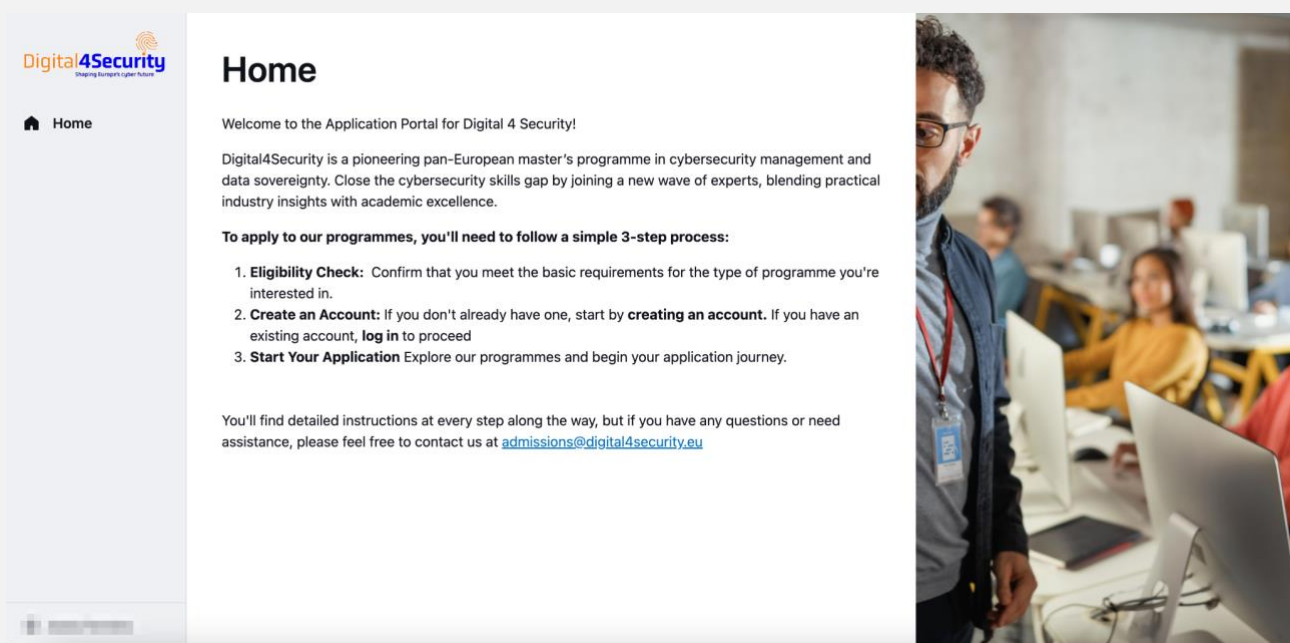
Admissions/enrolment process narrative

Step 1

The applicant visits the client website and clicks “Apply now,” or clicks the “Apply now” call to action in an email.

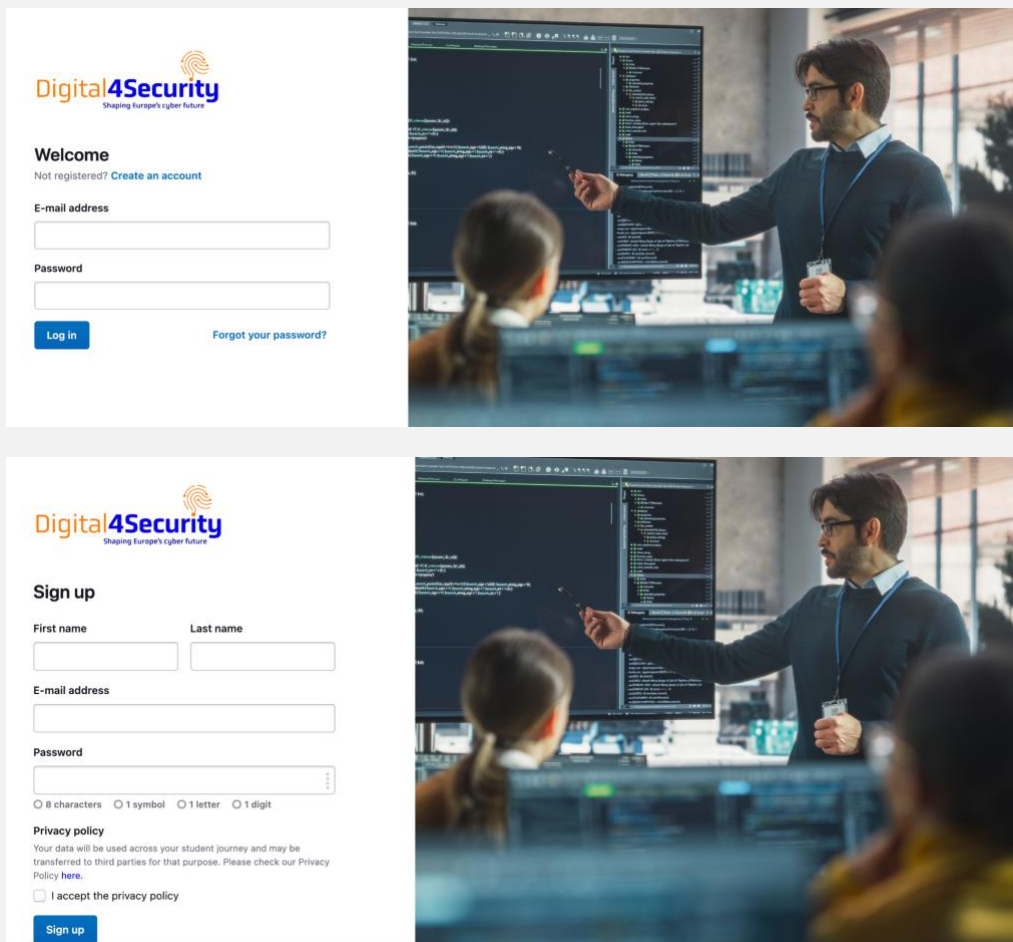
Step 2

The applicant is redirected to the Full Fabric platform’s [Home Page](#), where they receive instructions on the application process.



Step 3

Applicant [Signs Up/Logs In](#) to the portal:



Welcome
Not registered? [Create an account](#)

E-mail address

Password

[Log in](#) [Forgot your password?](#)

Sign up

First name Last name

E-mail address

Password

☐ 8 characters ☐ 1 symbol ☐ 1 letter ☐ 1 digit

Privacy policy
Your data will be used across your student journey and may be transferred to third parties for that purpose. Please check our [Privacy Policy here](#).
☐ I accept the privacy policy

[Sign up](#)

Step 4

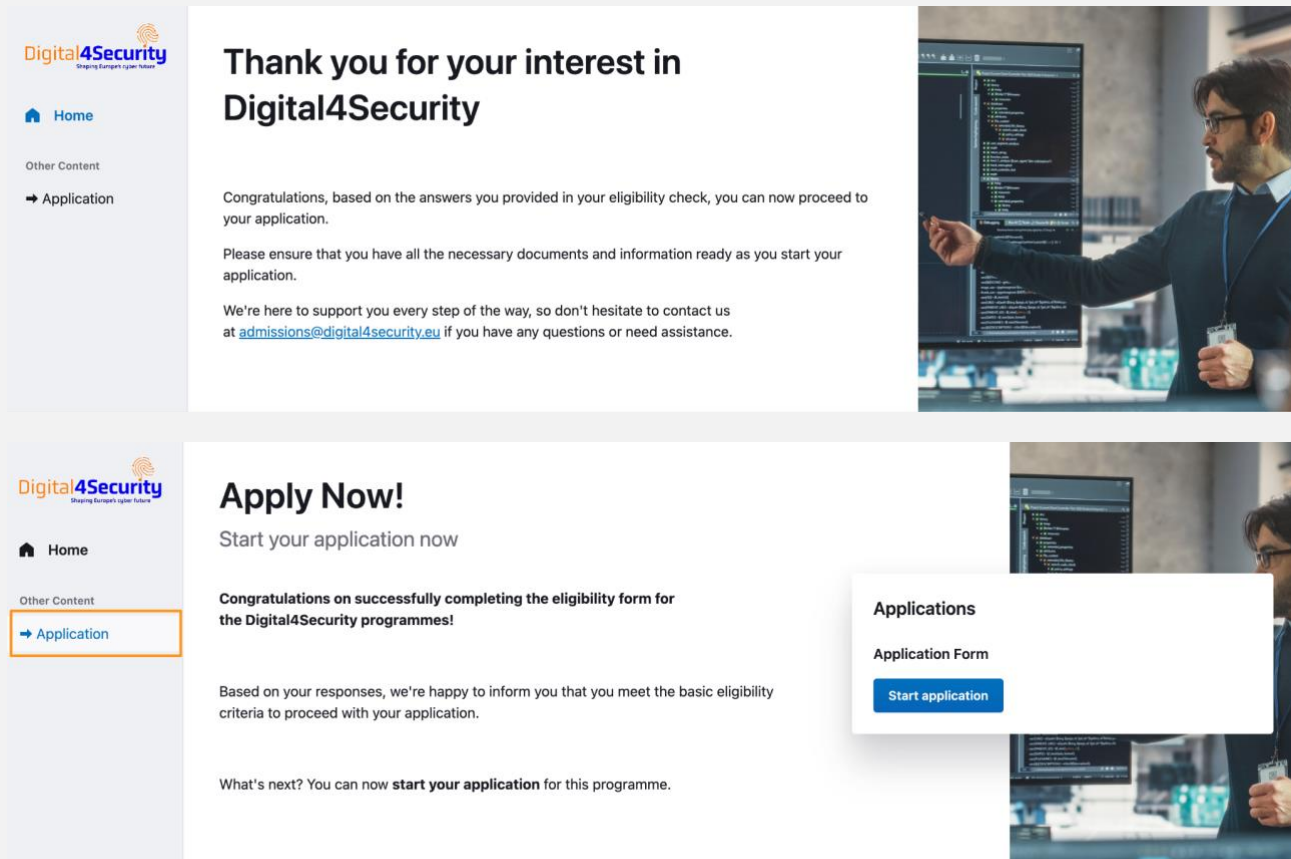
Applicant completes the Eligibility Assessment for Digital4Security's programmes (selecting the programmes they are interested in)

Result 1: Eligibility assessment — PASS

The applicant immediately receives an automated email confirming their eligibility to apply to the programme – State: Prospect_pass_ eligibility.

YES: Applicant receives an email confirming they can now apply to the programme. — Prospect_pass_eligibility

If **PASS/YES** - Applicant navigates to the relevant page to start/continue application:



The image displays two screenshots of the Digital4Security application portal. The top screenshot shows the 'Thank you for your interest in Digital4Security' page. The bottom screenshot shows the 'Apply Now!' page, which includes a 'Start application' button and a sidebar menu with 'Application' highlighted.

Thank you for your interest in Digital4Security

Congratulations, based on the answers you provided in your eligibility check, you can now proceed to your application.

Please ensure that you have all the necessary documents and information ready as you start your application.

We're here to support you every step of the way, so don't hesitate to contact us at admissions@digital4security.eu if you have any questions or need assistance.

Apply Now!

Start your application now

Congratulations on successfully completing the eligibility form for the Digital4Security programmes!

Based on your responses, we're happy to inform you that you meet the basic eligibility criteria to proceed with your application.

What's next? You can now **start your application** for this programme.

Applications

Application Form

[Start application](#)

Result 2: Eligibility Assessment - FAIL

State: Prospect_fail_eligibility – The prospect has submitted and failed the eligibility assessment.

State

Prospect::Fail eligibility ▾

- Prospect::Cold
- Prospect::Fail eligibility
- Prospect::Pass eligibility
- Prospect::Started application

- Applicant::Submitted
- Applicant::Incomplete
- Applicant::Rejected
- Applicant::Admitted
- Applicant::Needs board review
- Applicant::Board rejected
- Applicant::Board admitted
- Applicant::Acceptance submitted
- Applicant::Registered

- Student::Enrolled

NO: Applicant receives rejection email. — Prospect_fail_eligibility

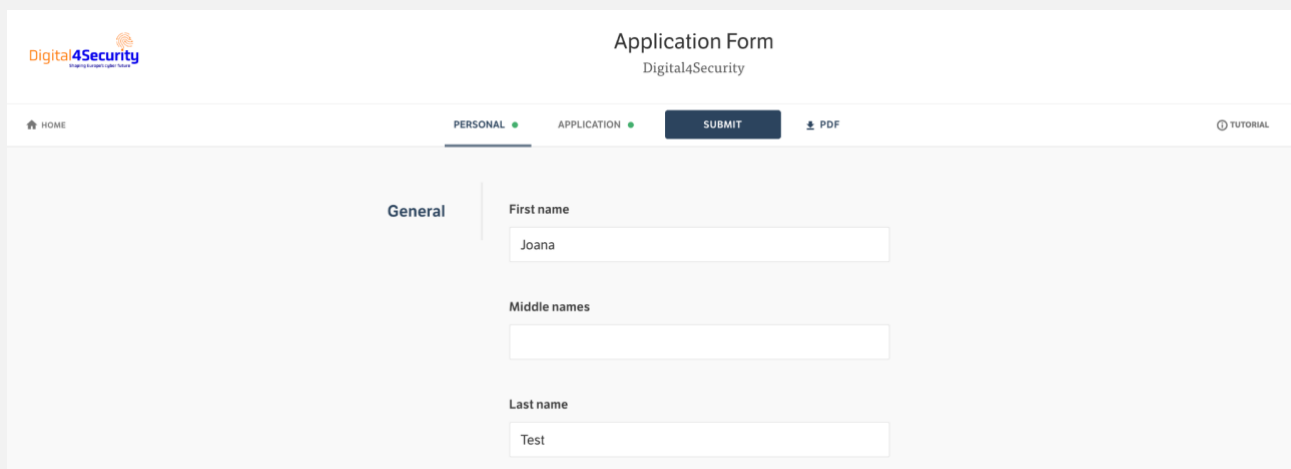
Step 5

Applicants validate their email address through a link received automatically by email.

Step 6

The applicant starts the application process and fills out all required information – State: Prospect_started_application.

Each tab of the application form includes the necessary questions and uploads for the applicant to complete their submission. The form's content is fully customisable and can be updated at any time.



The screenshot shows the 'Application Form' interface for Digital4Security. The header includes the logo and the title 'Application Form Digital4Security'. Below the header is a navigation bar with tabs: 'HOME', 'PERSONAL' (active), 'APPLICATION', 'SUBMIT', 'PDF', and 'TUTORIAL'. The main content area is titled 'General' and contains three text input fields: 'First name' (with the value 'Joana'), 'Middle names' (empty), and 'Last name' (with the value 'Test').

Step 7

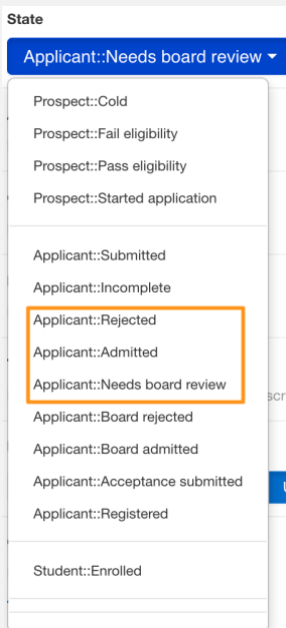
The applicant submits the application form – An automated confirmation email is sent to the applicant, and a notification is sent to the admissions team to review the application – State: Applicant_submitted.

Step 8

The admissions team reviews the submitted application forms using evaluation criteria to ensure the applicant's profile meets the programme's admission requirements.

Step 9

The admissions team moves applicants to the appropriate status based on the outcome of their review:



- State: `APPLICANT_REJECTED` – Applicant receives automatic rejection email informing of the reasons for rejection.
- State: `APPLICANT_ADMITTED` – Applicant receives automatic acceptance letter with instructions on the next steps they must take.
- State: `APPLICANT_NEEDS BOARD REVIEW` – Notification sent to board members to review application form.

Step 10

The board reviews each applicant's submission, makes a decision, records it on the evaluation form, and submits the evaluation.

Step 11

The admissions team receives a notification with the board's evaluation results and takes the necessary actions based on each applicant's decision, updating the applicant's status accordingly.

- State: `APPLICANT_BOARD_REJECTED` – Applicant is sent an automatic email informing them they have been rejected.

- State: APPLICANT_BOARD_ADMITTED - Applicant receives automatic acceptance letter with instructions on their next steps.

Applicant admitted or applicant board admitted

Step 1

Transcripts and payment plans are automatically generated for the applicant:

Transcript

This will include the list of courses they can select as part of the programme/certificate (for Master's).

Payment plan

An upfront full payment plan that the applicant must complete to enroll in the courses of the programme or micro-credentials.

- The full upfront payment plan is the default option, but it can be customised on a case-by-case basis at the discretion of the Digital4Security Consortium.

Step 2

Applicants receive an email with the attached acceptance letter, informing them of their admission and instructing them to log in, select their courses, and pay their tuition.

Step 3

The applicant logs in to the Full Fabric portal and accesses an enrolment area where they can select their courses and pay their tuition.

Step 4

Applicant starts their enrolment form

Selecting courses:

At a later stage will be implementing the process for selection of elective modules. applicants will have a form listing out the modules and electives that they need to select with on-screen guidance to support the process.

Tuition payment

Deposit fee enrolment form

APPLICATION

PAYMENT PLAN

SUBMIT

Payment plan

Please select your preferred payment plan. Please note that only the payment of deposit fee is required at this time.

Product selected:

Please select a payment plan Required

Tuition fee - Full upfront

Description	Due date	Subtotal	Total
Full upfront deposit discount	0 days from application submission	€1,000 - €500	€500
TOTAL			€500

Enter a discount code

APPLY DISCOUNT

Step 5

The applicant submits their enrolment form, and their profile status is automatically updated to Student_Enrolled. A notification is then sent to the admissions team.

Student Enrolled

Step 1

API integration is triggered to send student data and course enrolments to Moodle.

Full Fabric API Introduction

- Full Fabric uses HTTP verbs and a RESTful endpoint structure
- Rate limiting:
 - 40 per 8 seconds
 - 180 per 1 minute

- 10,000 per 1 hour
- Secure encrypted communication over internet:
 - via SSL/HTTPS
 - in JSON format
- Low data throughput requirements
 - User unit registrations and grades = 2.44 KB
 - Courses = 0.23 KB per course
 - User profile = 4.7 KB
 - Hypothetically, if 1,000 sign-ups convert to students at the same time, it will result in a data transfer of 4.7MB, taking 1Gbps line 0.038 seconds to transfer.
 - In such a case, rate limiting will be the bottleneck and the operation will be artificially rate-limited and it will take 5 minutes.
 - As new signups will take days to convert students and start the programme, this latency is negligible.

```
[  
  {  
    "Id": 0,  
    "FirstName": "string",  
    "LastName": "string",  
    "Name": "string",  
    "EmailAddress": "string",  
    "TerritoryId": 0  
  }  
]
```


Full Fabric Process Diagram

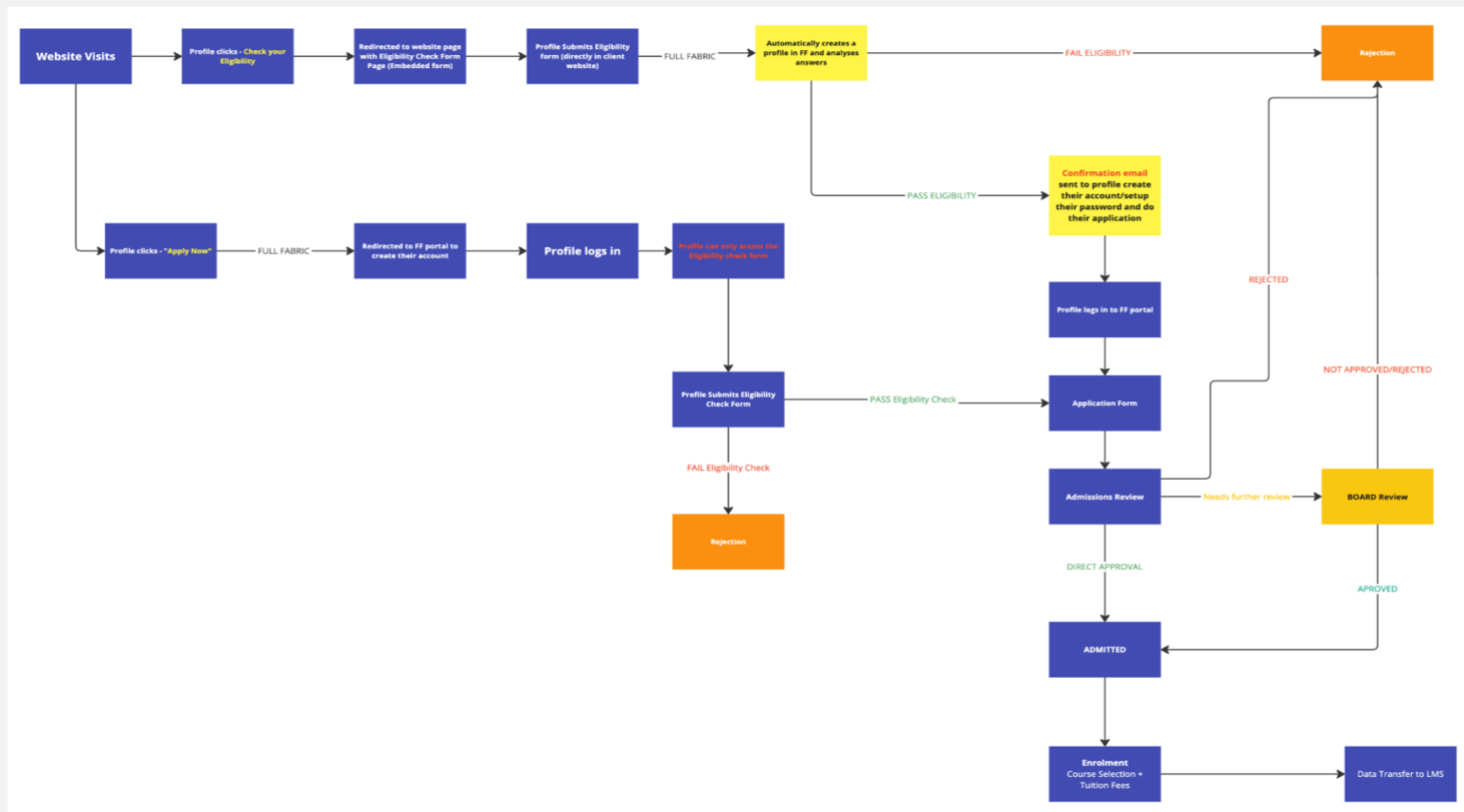


Figure: outcome of the process mapping workshop

Part 1: Sign up and eligibility check

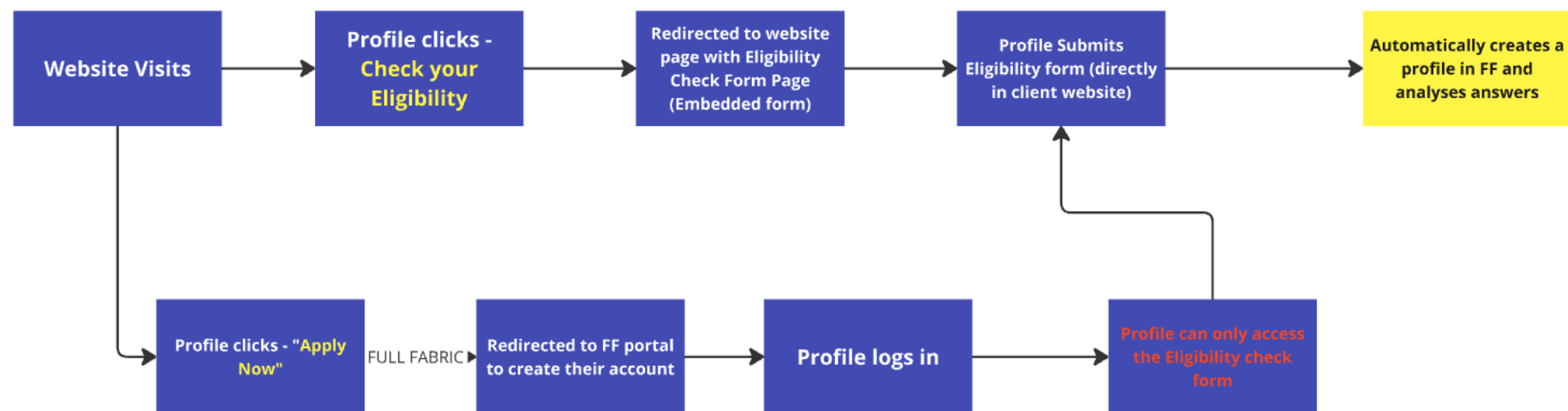


Figure: the signup and eligibility check process

Part 2: Application outcome

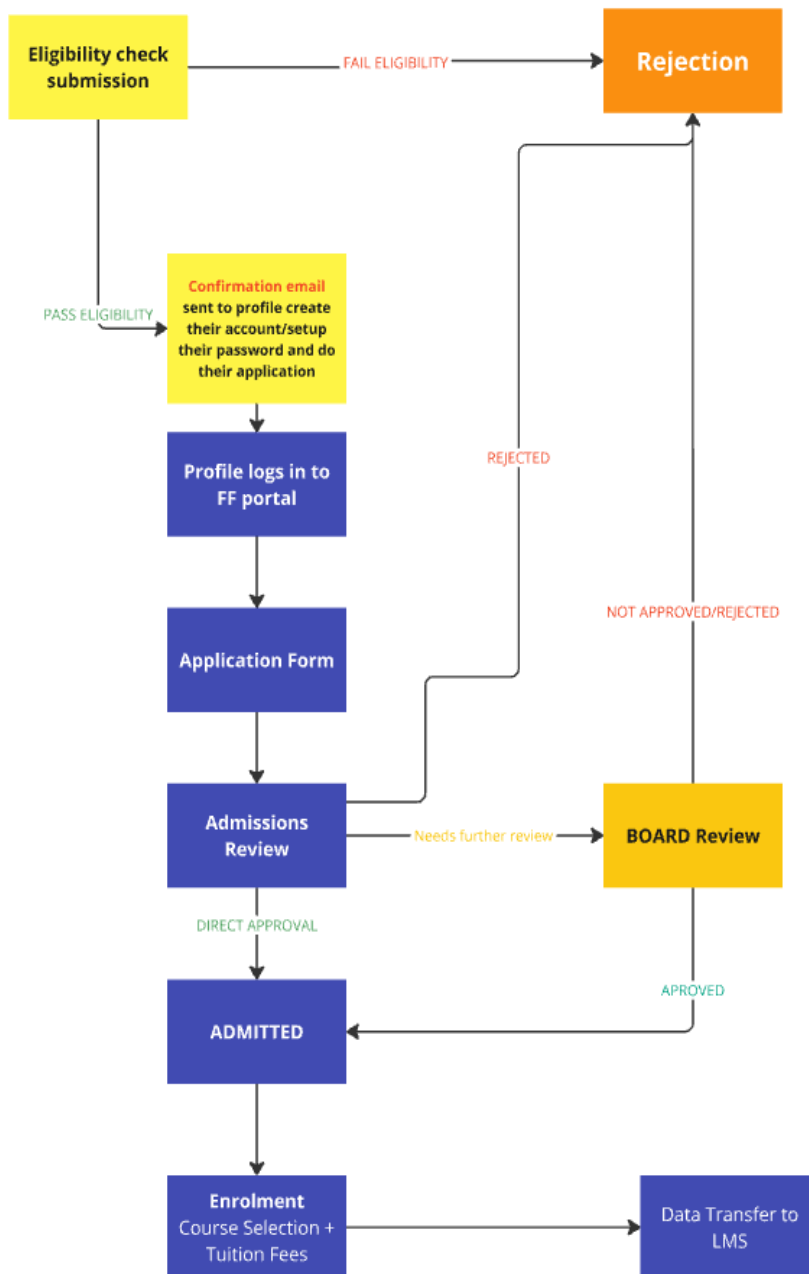
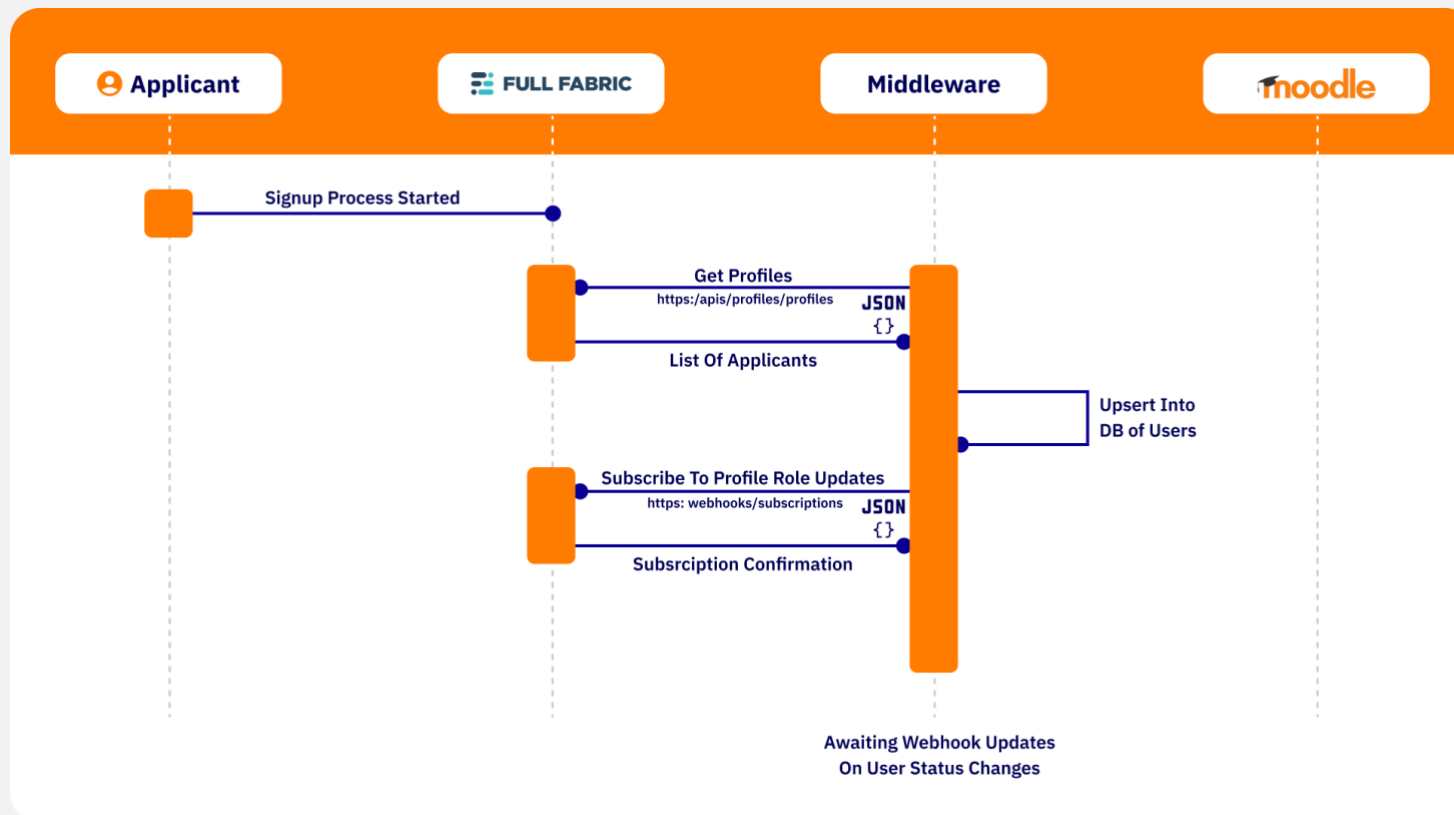


Figure: student application application process flow

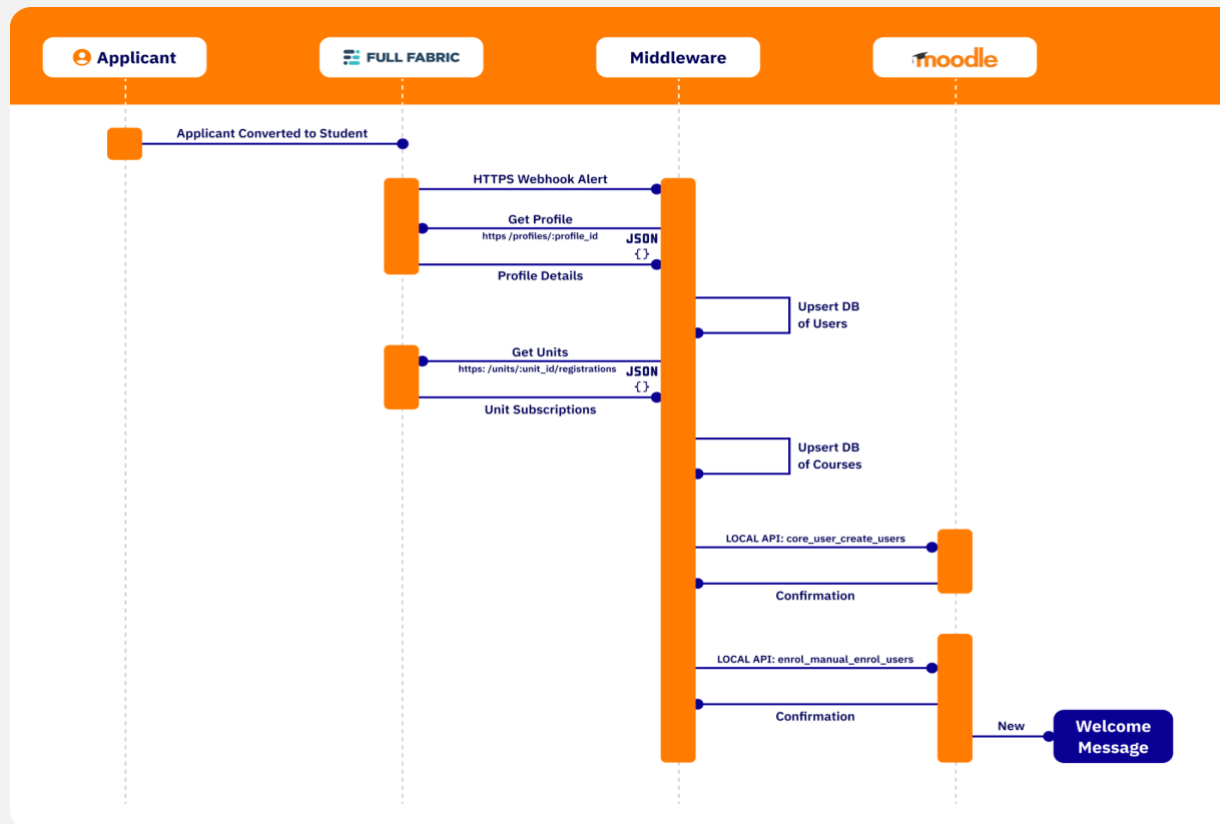
Sequence Diagram of Integration Workflow 1

Subscription to User Updates



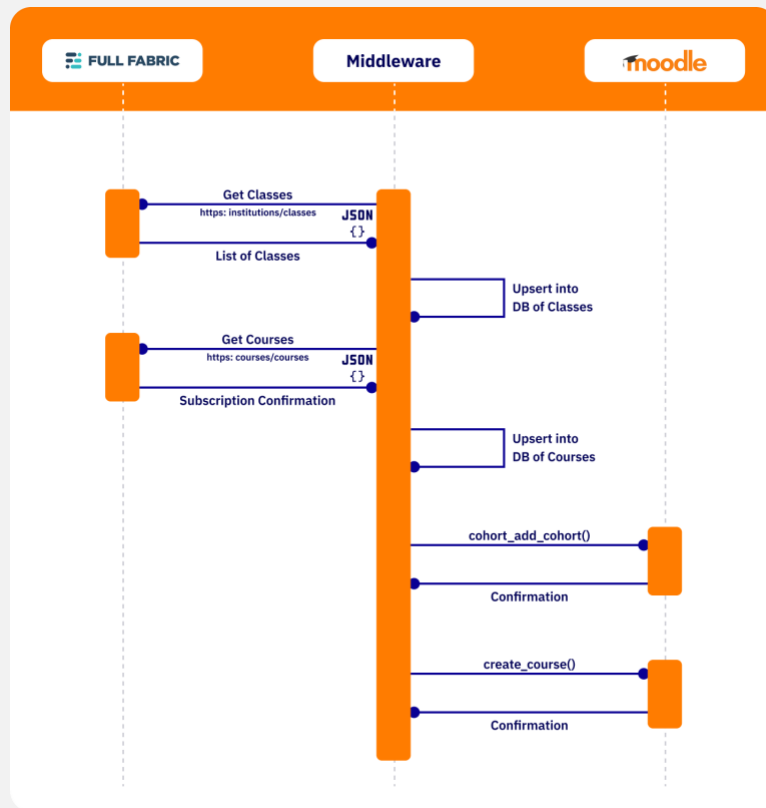
Sequence Diagram of Integration Workflow 2

User Import and Enrollment



Integration Workflow 3

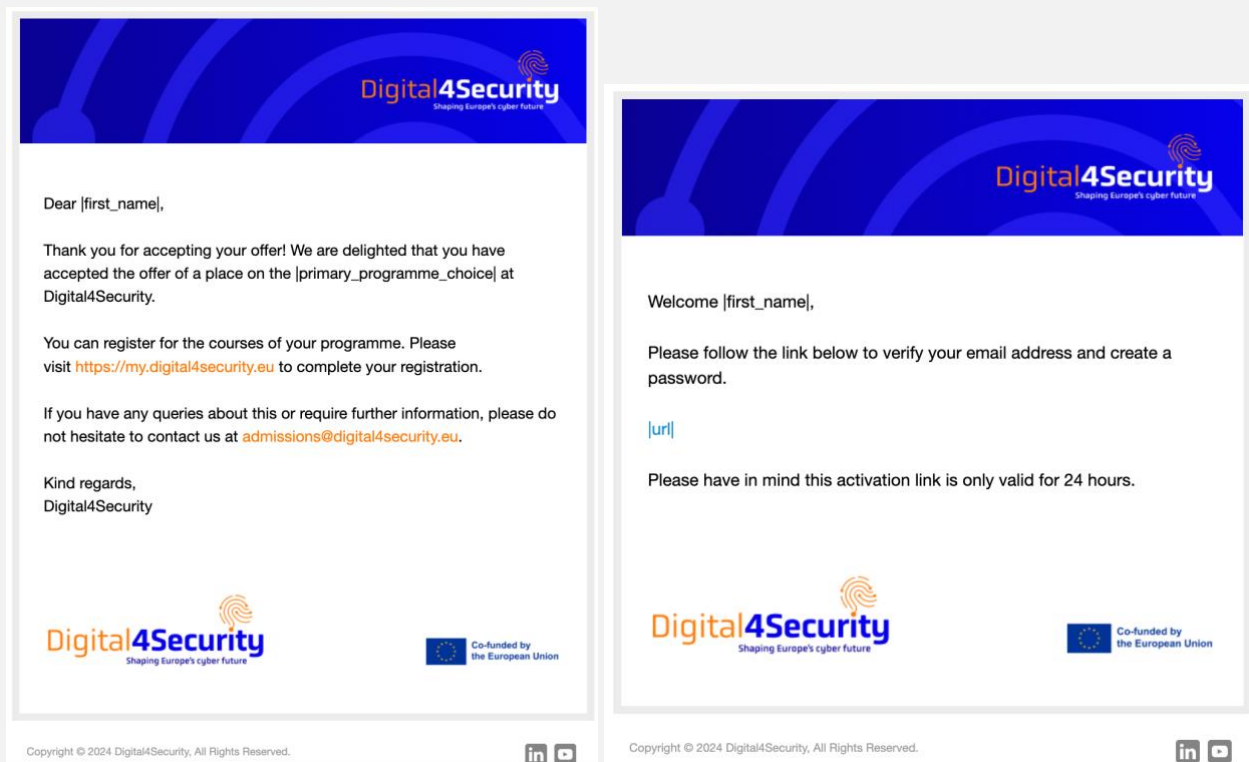
Synchronisation of Classes and Courses Sequence Diagram



Daily overnight process

Emails

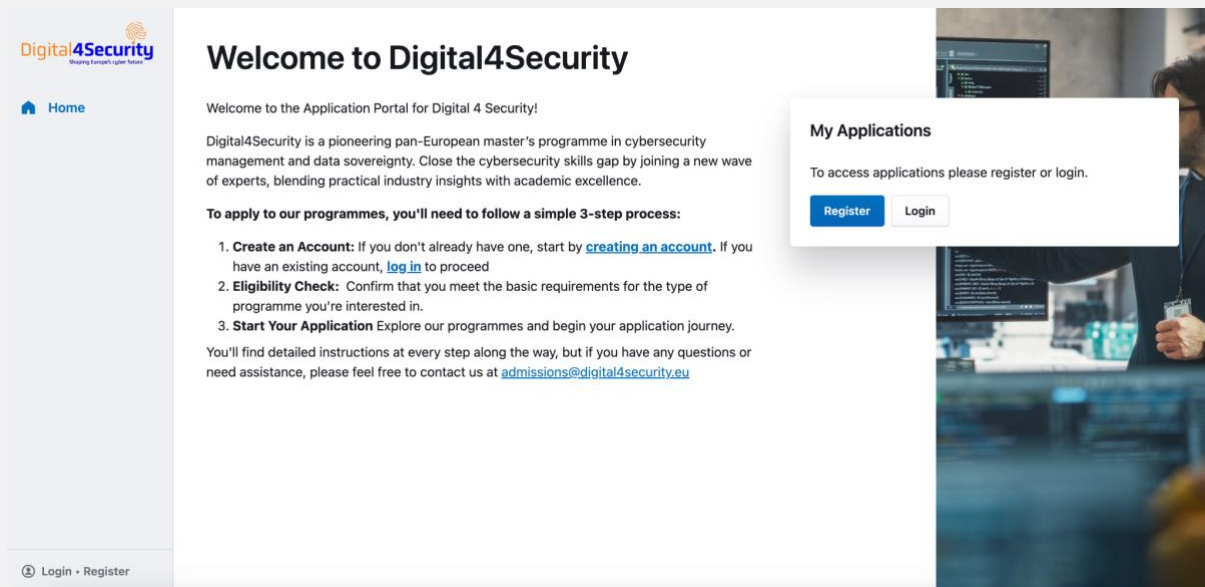
Full Fabric offers a suite of automated emails that can be configured with customisable messages that can be sent as required. We have applied the brand guidelines and the template is as follows:



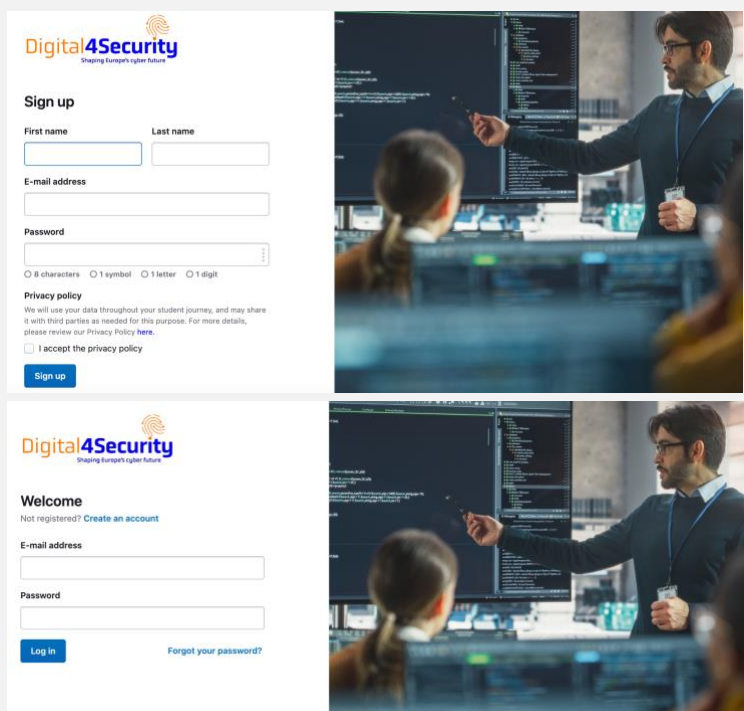
We are currently working on the student registration form for the pilot:

<https://my.digital4security.eu/templates/672107073b5d000b7e88249e/start>

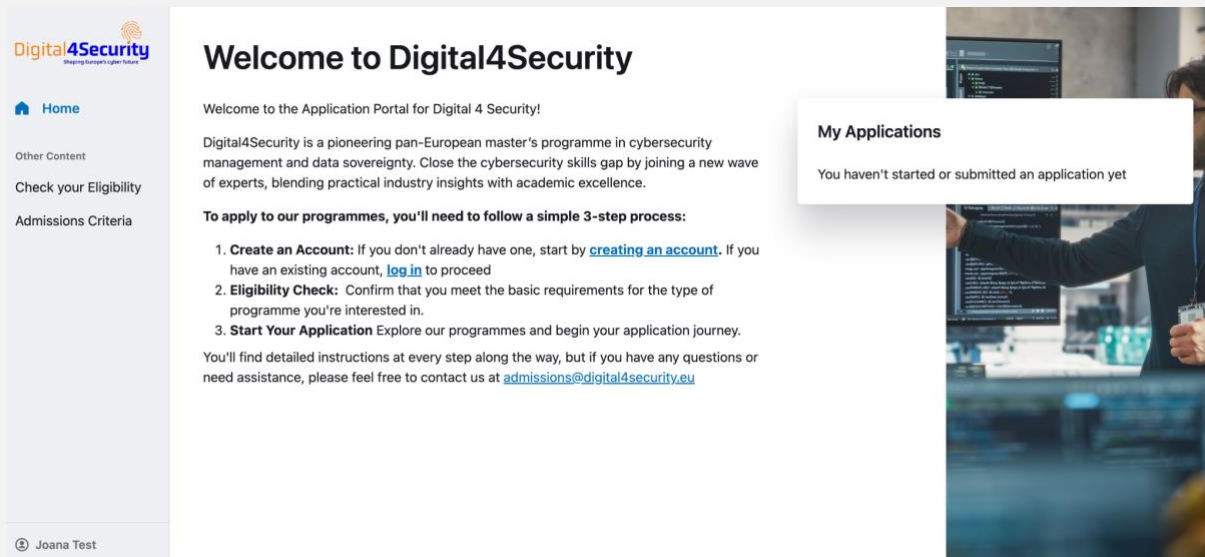
Applicant accesses the admissions' portal:



Applicant creates an account/logs in:



This is what the applicant will see once logged in:



The screenshot shows the Digital4Security application portal interface. On the left is a sidebar with the Digital4Security logo and navigation links: Home, Other Content, Check your Eligibility, and Admissions Criteria. At the bottom of the sidebar is a user profile for 'Joana Test'. The main content area is titled 'Welcome to Digital4Security' and contains a welcome message, a description of the programme, and a 3-step application process. A 'My Applications' box on the right indicates that no applications have been submitted yet. The background of the interface features a blurred image of a person working at a computer.

Welcome to Digital4Security

Welcome to the Application Portal for Digital 4 Security!

Digital4Security is a pioneering pan-European master's programme in cybersecurity management and data sovereignty. Close the cybersecurity skills gap by joining a new wave of experts, blending practical industry insights with academic excellence.

To apply to our programmes, you'll need to follow a simple 3-step process:

- 1. Create an Account:** If you don't already have one, start by [creating an account](#). If you have an existing account, [log in](#) to proceed
- 2. Eligibility Check:** Confirm that you meet the basic requirements for the type of programme you're interested in.
- 3. Start Your Application** Explore our programmes and begin your application journey.


You'll find detailed instructions at every step along the way, but if you have any questions or need assistance, please feel free to contact us at admissions@digital4security.eu

My Applications

You haven't started or submitted an application yet

Joana Test

Admissions Criteria Page:



Home

Other Content

Check your Eligibility

Admissions Criteria

Admissions Criteria

Below, you will find the requirements necessary for admission, including academic qualifications, English proficiency, and other key criteria.

1. Academic Qualifications

Applicants are expected to hold at least an [EQF Level 6](#) qualification in one of the following disciplines:


- **STEM Disciplines:** Information Management Systems, Information Technologies, Computer Science, Engineering, Physical Sciences, Mathematics.
- **Business/Legal Disciplines:** Business Information Systems, Business Administration, Accountancy, Finance, Economics, Business and Law.

Applicants with Business or Legal qualifications must also demonstrate numerical and computing proficiencies. Evidence can be provided through:

- **Work Experience:** Relevant roles showcasing these skills.
- **Formal Training:** Certifications or short courses in quantitative or computational areas.
- **Academic Modules:** Completed coursework such as ICT in Business, Statistics, Quantitative Methods, Operations Research, Informatics, Business Analysis, Risk Analytics, or Econometrics.

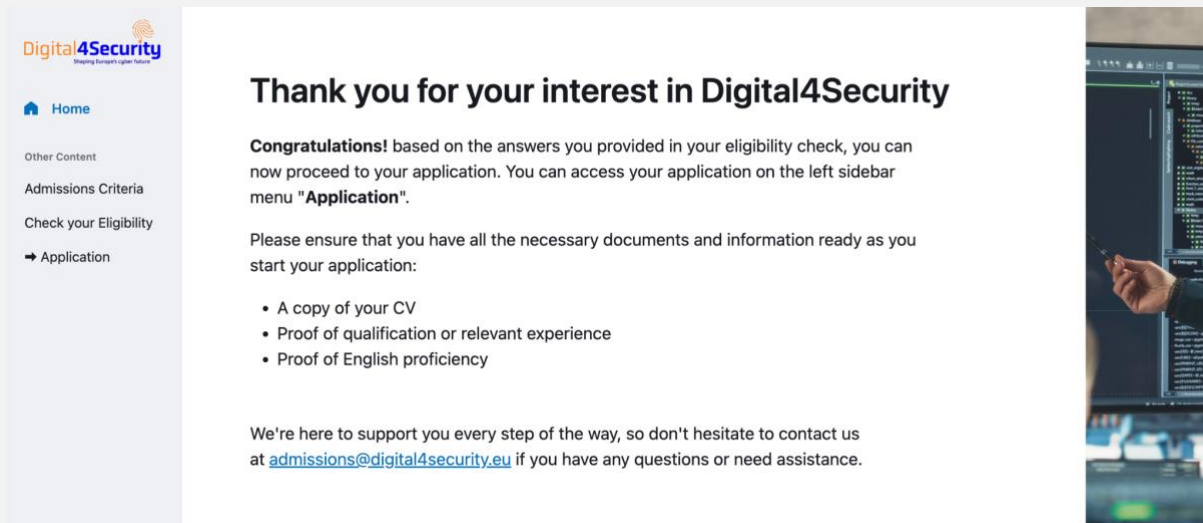
Recognition of Prior Learning (RPL) Policy

We understand that formal qualifications don't always reflect an applicant's abilities and



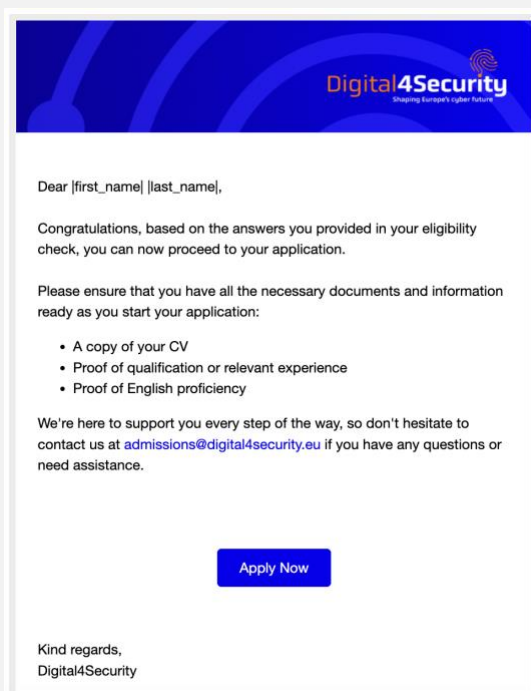
Eligibility PASS:

● Page:



The screenshot shows a web application interface. On the left is a sidebar with the Digital4Security logo and navigation links: Home, Other Content, Admissions Criteria, Check your Eligibility, and Application (highlighted with a right arrow). The main content area has the heading "Thank you for your interest in Digital4Security". Below this, it says "Congratulations! based on the answers you provided in your eligibility check, you can now proceed to your application. You can access your application on the left sidebar menu 'Application'." It then asks the user to ensure they have necessary documents ready and lists three requirements: a copy of their CV, proof of qualification or relevant experience, and proof of English proficiency. At the bottom, it offers support and provides the email admissions@digital4security.eu. On the right side of the screenshot, there is a vertical image of a person's hand pointing at a computer screen displaying code.

● Email:



The screenshot shows an email template from Digital4Security. The header features the Digital4Security logo. The body of the email is personalized with the recipient's name: "Dear [first_name] [last_name],". It congratulates the recipient and informs them they can proceed to their application. It then lists the necessary documents: a copy of their CV, proof of qualification or relevant experience, and proof of English proficiency. It also offers support and provides the email admissions@digital4security.eu. At the bottom, there is a blue "Apply Now" button and a sign-off: "Kind regards, Digital4Security".

- b. Trigger cron jobs for integration with Full Fabric
 - c. Accept Webhooks from Full Fabric
- Secondary auto-scaling server tier
- Load Balancer with SSL termination
- MySQL database
- Elastic File System for static assets
- Single sign-on (SSO) instance to facilitate user accounts and SSO

Technical Support



There are a number of partners offering technical support as it is a large platform with many integrated parts. Full Fabric will be offering support to the consortium for their entire system.

Our Hosting Partner will be offering full support for the hosting platform, servers and databases for Moodle.

Moodle support will be offered by the platform developers Matrix Internet.

GDPR



Currently it is an independent install of Moodle hosted on development cloud servers hosted within the EU. The production version will also be hosted on servers within the EU. All data and backups will be stored within the EU.

Our nominated DPO is Costin Carabas.

Sample GDPR Compliance Disclaimer (to be updated)

We are committed to protecting your privacy and ensuring compliance with the General Data Protection Regulation (GDPR). Our learning platform takes data security and privacy seriously. This GDPR Compliance Disclaimer outlines how we collect, use, and protect your personal information.

1. **Data Collection:** We collect only the data necessary to provide you with access to our platform, courses, and resources. This includes but is not limited to, your name, email address, and account information. All data is processed lawfully and transparently.
2. **Data Usage:** Your data is used strictly to enhance your learning experience, manage course progress, and provide support. We do not sell or share your information with third parties, except for the purposes of improving our services, in which case we ensure they are GDPR compliant.
3. **Data Protection:** We implement industry-standard security measures to safeguard your personal data from unauthorized access, alteration, or disclosure. Access to your data is restricted to authorized personnel only.

4. User Rights: Under GDPR, you have the right to access, rectify, or erase your data, as well as the right to restrict or object to our processing of your data. You may also request a copy of your data in a portable format. To exercise these rights, please contact us at [support@digital4security.eu].

5. Cookies and Tracking: Our platform may use cookies to personalize content, track performance, and enhance user experience. You have the option to manage cookie preferences upon visiting the site.

6. Data Retention: We retain your data only as long as necessary to fulfill the purposes outlined in this disclaimer or as required by law. Upon account termination, your data will be deleted in accordance with our data retention policy, unless a longer retention period is required or permitted by law.

Updates: We may update this disclaimer periodically to reflect changes in our practices or applicable laws. We encourage you to review this disclaimer regularly.

For more information on how we handle your personal data, please refer to our Privacy Policy. If you have any questions about this GDPR Compliance Disclaimer, please contact our Data Protection Officer at [dpo@digital4security.eu].

By using our platform, you acknowledge that you have read and understood this GDPR Compliance Disclaimer.

Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Copyright © 2023 by Digital4Security Consortium



Digital4Security

Shaping Europe's cyber future



Co-funded by
the European Union