CyberAgent

Co-funded by the European Union

STRUCTURA PARCURSULUI DE ÎNVĂȚARE A AGENȚILOR DE SCHIMBARE ÎN DOMENIUL SECURITĂȚII CIBERNETICE PENTRU IMM-URI

CYBER AGENT 06.2024

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.

Pachet de lucru 2: Abordarea CyberAgent și proiectarea structurii

Livrabil 2.3: Structura parcursului de învățare a agenților de schimbare în domeniul securității cibernetice pentru IMM-uri

Leader-ul Pachetului de lucru 2 – Olemisen Balanssia ry
Leader-ul livrabilului 2.3 –Universitatea Vilnius

CUPRINS

ABREVIERI

CBL – Model de învățare bazat pe provocări

CL – Model de învățare prin cooperare

EC – Comisia Europeană

ECTS – Sistemul european de transfer și acumulare de credite

EQF – Cadrul european al calificărilor

GICL – Model de învățare colaborativă prin investigație ghidată

HEI – Instituții de învățământ superior

PBL – Model de învățare bazat pe proiecte

POGIL – Model de învățare prin cercetare orientată pe proces

SME – Întreprinderi mici și mijlocii

VET – Instituții de învățământ profesional

LISTA FIGURILOR

LISTA TABELELOR

INTRODUCERE

Scopul general al acestui raport este de a dezvolta și descrie noi căi de învățare profesională pentru îmbunătățirea competențelor de securitate cibernetică în rândul angajaților IMM-urilor europene (întreprinderi Mici și Mijlocii).

Pe baza constatărilor din cartografierea nevoilor de formare pentru agenții de schimbare a securității cibernetice pentru IMM-uri, au fost identificate analize ale resurselor externe a rezultatelor învățării în ceea ce privește abilitățile și competențele. În urma analizei rezultatelor învățării identificate, acest raport oferă îndrumări cu privire la două tipuri de curriculum de formare de la EQF (Cadrul European al Calificărilor) nivel 4 la 6 pentru a acoperi gama de abilități și cunoștințe necesare pentru grupurile țintă ale proiectului, angajații IMM-urilor și studenți, și să adapteze rezultatele formării la diferitele medii și profiluri ale cursanților.

- Nivelul EQF 4-5 va fi implementat pentru angajații IMM-urilor care nu au studii superioare, precum și studii VET (Educație și Formare Profesională). Acest nivel va oferi abilitățile și cunoștințele de bază în domeniul securității cibernetice cu o specializare mininmă în unele module.
- Nivelul EQF 5-6, care se va adresa angajaților IMM-urilor care au, de asemenea, o pregătire adecvată și studenților (Instituții de Învățământ Superior). La acel nivel se vor desfășura activități de instruire mai avansate și mai complexe.

S-a decis actualizarea nivelurilor EQF la 4-6 nu numai pentru a acoperi o gamă largă de rezultate ale învățării, așa cum s-a menționat anterior, ci și pentru a permite o poartă de acces către programele de formare, ca o cale de perfecționare pentru studenții VET și angajații de la nivelul 4 pentru a atinge nivelul 6.

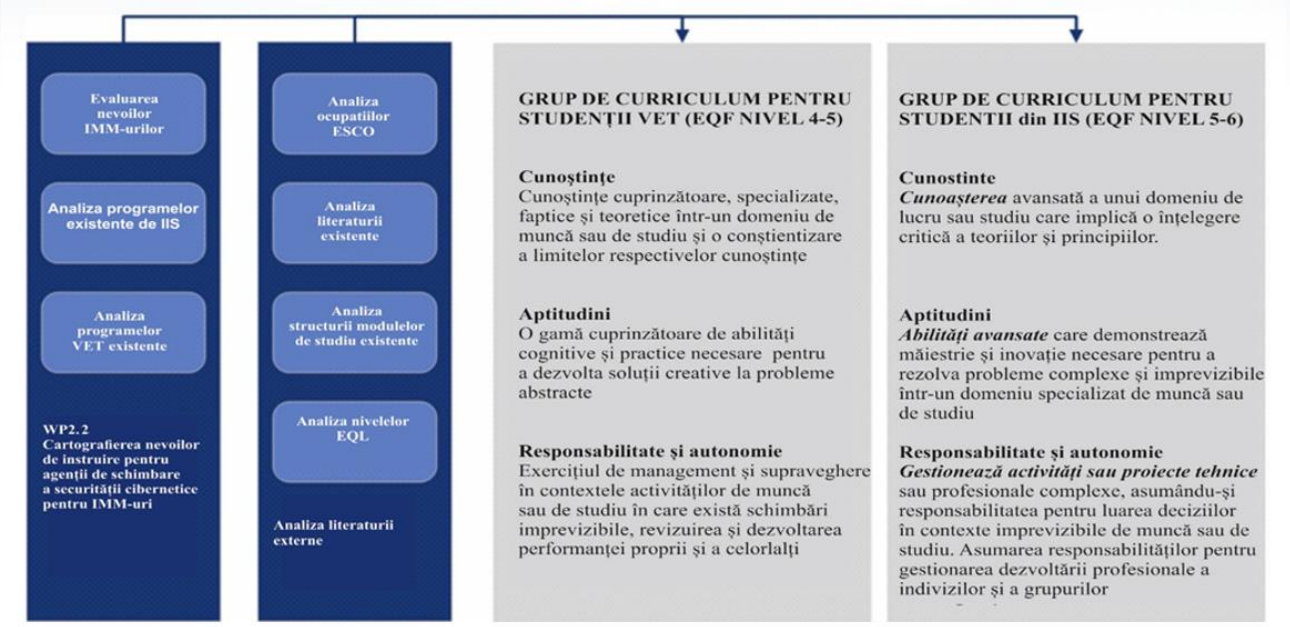

Figura* 1. *O diagramă ilustrativă, care aderă la orientările CE, prezintă cele opt niveluri EQF, oferind o reprezentare vizuală a cadrului educațional.

Curriculumul abordează rezultatele învățării și necesitatea de a forma angajații IMM-urilor pentru a se perfecționa în vederea ocupării rolului de agenți de schimbare a securității cibernetice pentru IMM-uri și pentru a educa studenții pentru a ocupa acest rol după terminarea cursului. Fiecare curriculum cuprinde opt module care acoperă patru subteme:

- Abilități tehnice - Cunoștințe actualizate despre amenințările la adresa securității cibernetice și problemele juridice conexe - Cunoștințe practice despre cum să faci față amenințărilor la securitatea cibernetică.
- Abilități analitice - Gândire critică - Capacitate de a analiza și înțelege amenințările locale, cum se întâmplă acestea, persoanele expuse riscului etc.
- Managementul riscurilor - Învață să ofere și să descrie locurile de muncă pentru IMM-uri cu rutine de securitate cibernetică – Crează propriul manual pentru IMM-uri la locul de muncă pentru securitatea cibernetică și cum să îl urmărească.
- Abilități organizaționale - Cum să implementați noi rutine și moduri de lucru în securitatea cibernetică la locurile de muncă; Efectuarea asistenței liderilor în securitatea cibernetică.

În plus, o parte centrală a creării căilor de învățare pentru îmbunătățirea competențelor de securitate cibernetică în rândul IMM-urilor europene este modul în care vor fi implementate micro-acreditările. Acestea trebuie să se refere la rezultatele învățării (cunoștințe, abilități și competențe), conținutul cursului, formare (cunoștințe, abilități și competențe), elemente de joc, durata și numărul de credite conform ECTS (Sistemul european de transfer și acumulare de credite). Pentru a se potrivi scopului, acestea trebuie să fie realizate prin stabilirea de parteneriate între instituțiile de învățământ superior cu furnizorii de VET și întreprinderi private din sectorul securității cibernetice.

Micro-secțiunile oferă cursanților mai multă libertate de a alege module sau părți ale modulelor și de a decide ce nivel de certificat au nevoie: certificate de participare sau certificate de finalizare a cursului cu test de certificare, adică dovada că respectivul curs a fost finalizat cu însușirea unei anumite competențe. Certificatele de finalizare a cursului se eliberează după promovarea testului final cu un punctaj de cel puțin 75%, iar certificatele de participare se eliberează pentru participarea la învățare față în față, blended learning sau online pe teme/module specifice. Această practică nu numai că poate crește aplicabilitatea și eficacitatea instruirii, dar stimulează și motivația pentru învățare, oferind o perspectivă valorică clară pentru cariera și dezvoltarea ulterioară a participanților.

În concluzie, acest raport prezintă ghiduri detaliate pentru dezvoltarea modulelor CyberAgent, inclusiv schița de conținut a modalităților de studiu și de dezvoltare a carierei, metodologiile de instruire și evaluare și foaia de parcurs pentru construirea curriculumului.

[1] https://europa.eu/europass/en/description-eight-eqf-levels

1. PARCURS DE ÎNVĂȚARE

Un parcurs de învățare este o călătorie întreagă pe care participantul o parcurge din momentul în care își dă seama că trebuie să își îmbunătățească abilitățile, să înceapă și să finalizeze formarea, până în momentul în care termină de învățat și începe să aplice cunoștințele primite. Există 3 etape într-un parcurs de învățare:

- Preînvățare,

- Învățare,

- Post-învățare.

Etapa de preînvățare este ilustrată în figura de mai jos.

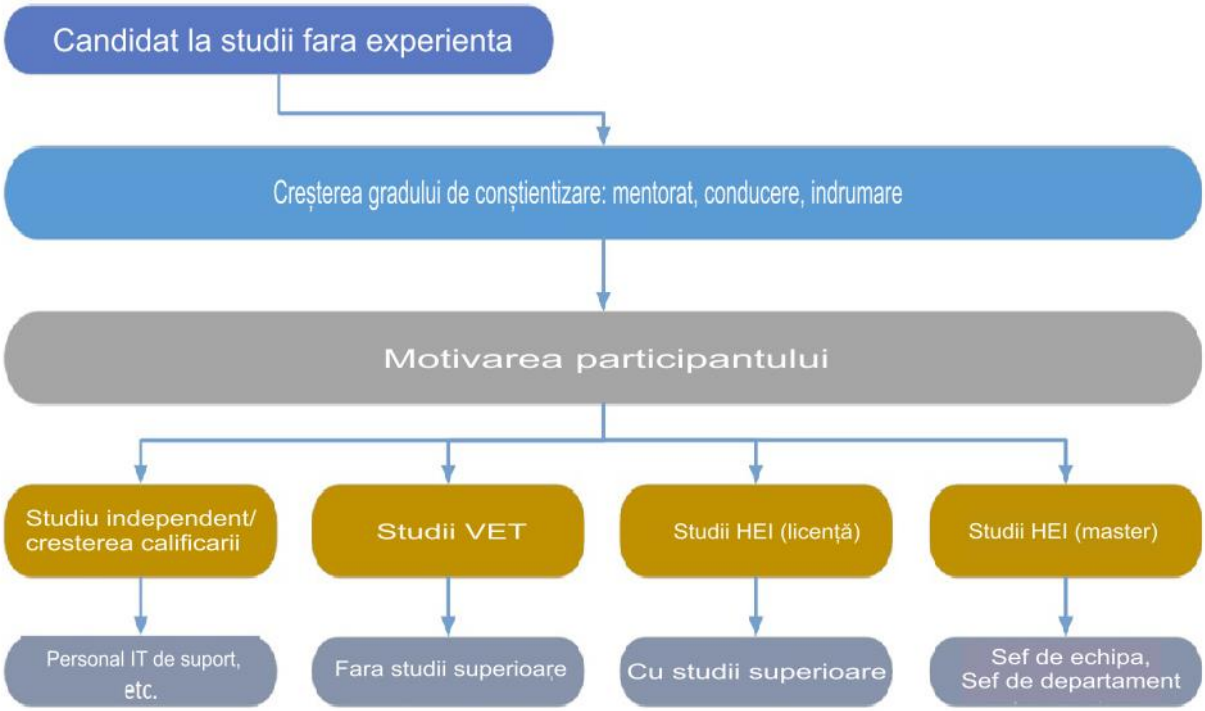

Figura* 2. *Calea de învățare înainte de începerea studiilor

În contextul IMM-urilor, această cale de învățare/studiu poate fi urmată. În figură, participantul fie decide să se antreneze, fie este influențat de o campanie de conștientizare și obține o înțelegere a beneficiilor formării, oportunităților și carierelor care pot fi dobândite după formare.

De asemenea, a fost propusă calea de învățare ca modul tipic prin structura OLE (Mediu de învățare online). După o analiză a literaturii de specialitate și a mai multor proiecte care aplică principiul micro-acreditărilor ,[2,3,4] se propune ca fiecare modul CyberAgent să aibă 1-5 ECTS (fiecare ECTS are 25-30 de ore de volum de muncă), să înceapă cu o introducere și apoi să fie împărțit în teme, care reprezintă subteme.

La final, se dă un test de autoevaluare format din mai multe întrebări. Materialele de instruire ale modulului ar trebui să acopere studiul a 6-8 teme, în fiecare dintre acestea fiind 4-6 subteme. Cursul se poate încheia cu un test de cunoștințe, care nu este obligatoriu. Acest lucru oferă angajaților IMM-urilor și studenților instituțiilor de formare posibilitatea de a dobândi și de a demonstra competențele învățate într-un anumit modul sau o parte a formării.

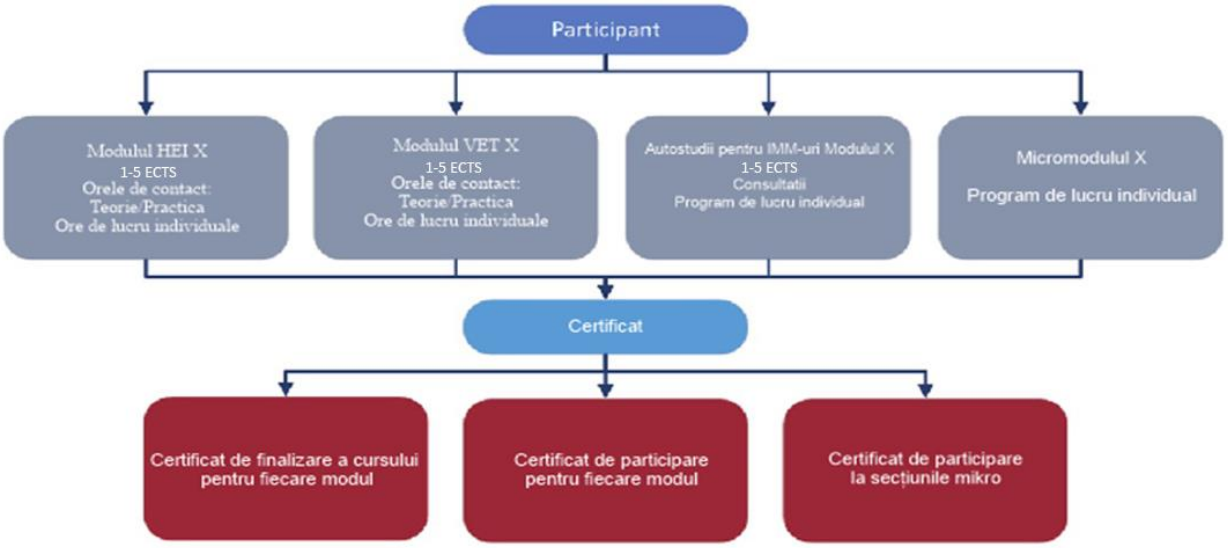

Figura 3. Structura studiilor

Micro-acreditările sunt integrate în procesul de învățare prin următoarele activități cheie:

- Dezvoltarea modulelor de formare: fiecare modul trebuie să fie formulat cu atenție ținând cont de cunoștințele și abilitățile specifice cerute în sectorul IMM-urilor, cu obiective clare, rezultate ale învățării, metode de predare și învățare, durata cursului.
- Sarcini și proiecte practice: cursanții îndeplinesc sarcini practice și dezvoltă proiecte care sunt evaluate și oferă dovezi clare ale abilităților dobândite.
- Strategia de evaluare a cunoștințelor și criteriile de evaluare clar descrise: la sfârșitul fiecărui modul, se organizează o evaluare a cunoștințelor pentru a determina dacă participantul a atins rezultatele învățării și dacă este eligibil pentru un certificat care să dovedească acest lucru.

Întrucât grupul țintă al proiectului este reprezentat de angajații IMM-urilor, studenți din învățământul superior si VET, sunt disponibile patru tipuri de studii, în funcție de posibilitățile și nevoile cursanților:

- Studii pentru învățământul superior: 8 module, fiecare 1-5 credite ECTS, unde sunt ore față în față (teorie și practică) și ore individuale de lucru;
- studii VET: 8 module, fiecare 1-5 credite ECTS, unde sunt ore față în față (teorie și practică) și ore individuale de lucru;

- Autostudii (pentru IMM-uri): 8 module, fiecare câte 1-5 credite ECTS, unde există consultații (dacă este necesar) și ore individuale de lucru;
- Micro-module: oră individuală de lucru în funcție de numărul de teme alese.

Figura 4. Structura studiilor pentru învățământul superior

Figura 5. Structura studiilor pentru VET

Figura 6. Structura studiilor pentru autostudii

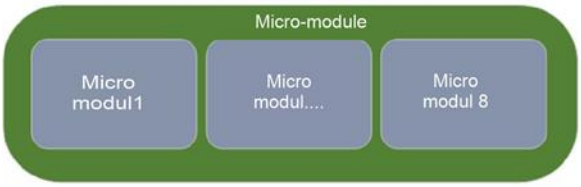

Figura 7. Structura studiilor Micro-modul

Studenții din învățământul superior și VET vor putea studia câte un modul de 1-5 credite fiecare. IMM-urile vor putea parcurgă câte un modul la un moment dat, sau putem oferi microsecțiuni ca parte a cursului.

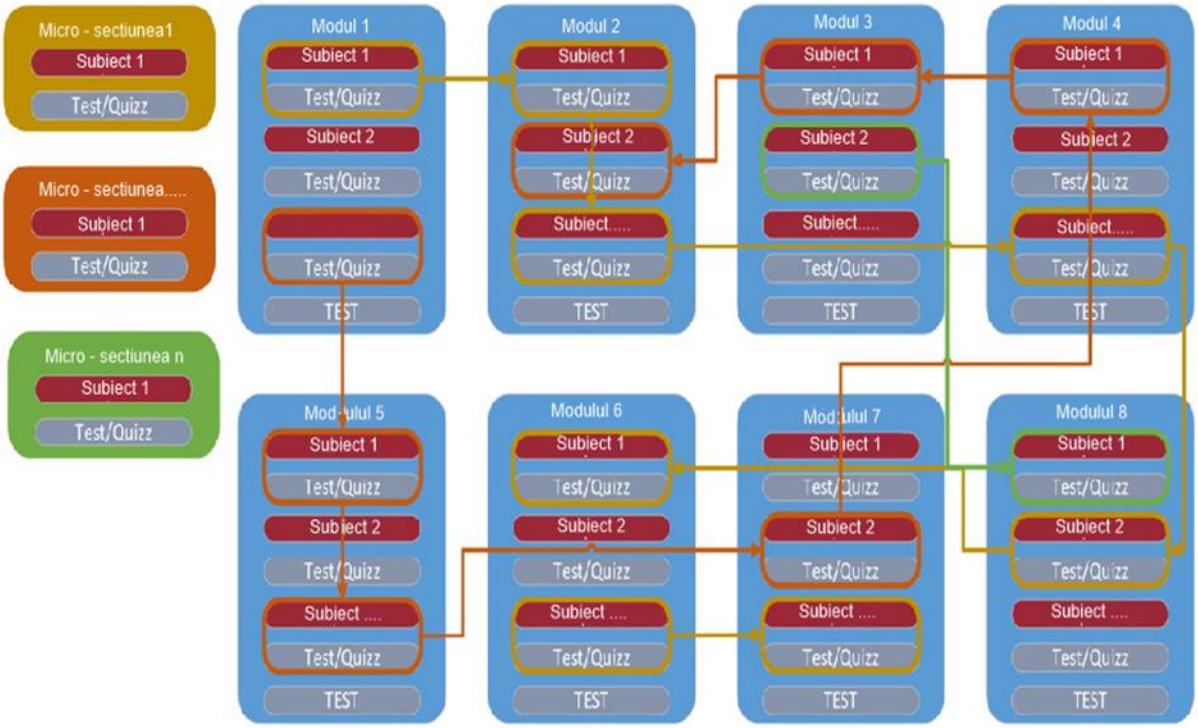

Figura 8. Legăturile căilor de învățare

În toate cele trei categorii (învățământ superior, VET, IMM-uri), cursanții studiază 8 module. În cazul Micro-modulelor, cursantul poate alege modulele dorite.

Micromodulele sunt experiențe de învățare scurte sau lungi, evaluate în mod transparent. Ele sunt parcurse de participant împreună cu provocarea sau separat. Fiecare micro-modul este evaluat cu o măsură diferită a volumului de muncă de învățare (cum ar fi ECTS) și se termină cu evaluarea. Finalizarea cu succes a evaluării micro-modulelor recompensează cursanții cu micro-acreditări.

Se propune ca fiecare modul din programul pentru învățământul superior să poată fi modularizat într-un micro-modul, fiecare prezentând sarcini specializate și un plan detaliat de implementare. Rezultatele testelor pot fi evaluate prin insigne, care sunt bazate pe imagini și care pot fi citite universal de computere. Aceste imagini încorporează metadate care detaliază competențele asociate cu fiecare insignă și informații despre participantul care o deține.

Micro-acreditare înseamnă înregistrarea rezultatelor învățării pe care un participant le-a dobândit în urma unui volum mic de învățare. Aceste rezultate ale învățării vor fi fost evaluate pe baza unor criterii transparente și clar definite. Experiențele de învățare care conduc la micro-acreditări sunt concepute pentru a oferi participantului cunoștințe, abilități și competențe specifice care răspund nevoilor societale, personale, culturale sau ale pieței muncii.[5,6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: Concept of FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[6] Council Recommendation of 16 June 2022 on a European Approach to Micro-Credentials for Lifelong Learning and Employability." Official Journal of the European Union, vol. 2022/C, 16 June 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN

2. PARCURS DE CARIERĂ

Calea post-învățare ar putea fi numită parcurs de carieră. La începutul proiectului a fost realizată analiza de cercetare a ocupațiilor ESCO (descrisă în raport: D2.2 - Raportul de cartografiere a nevoilor de pregătire a agenților de schimbare a securității cibernetice pentru IMM-uri). Analiza efectuată în trei faze a avut ca scop investigarea diferitelor ocupații de securitate cibernetică enumerate în cadrul ESCO. În prima fază, ocupațiile legate de securitatea cibernetică au fost identificate și documentate de pe portalul ESCO (**https://esco.ec.europa.eu/en/classification/occupation_main#overlayspin**), evidențiind abilitățile, competențele și cunoștințele lor respective. Aceste ocupații au inclus roluri precum ofițer șef de securitate TIC, expert în criminalistică digitală, inginer de securitate a sistemelor încorporate, hacker etic, manager de reziliență TIC, administrator de securitate TIC, inginer de securitate TIC, manager de securitate TIC și inginer de cunoștințe. Fiecare ocupație a fost definită de responsabilitățile sale specifice și zonele de interes din domeniul securității cibernetice, variind de la funcțiile de securitate corporativă până la criminalistica digitală, hacking etic și planificarea rezilienței.

În a doua fază, a fost completat un tabel pentru fiecare ocupație ESCO revizuită, detaliind titlul și responsabilitățile de bază. Acestea au inclus sarcini precum planificarea și implementarea măsurilor de securitate, efectuarea evaluărilor vulnerabilității, dezvoltarea modelelor de reziliență și recuperare în caz de dezastru și integrarea cunoștințelor în sistemele informatice.

În plus, a treia fază a implicat cartografierea ocupațiilor ESCO cu rezultatele învățării asociate, clasificarea lor în cunoștințe, abilități și competențe. Acest proces a facilitat o înțelegere cuprinzătoare a cerințelor educaționale și a competențelor așteptate pentru fiecare rol de securitate cibernetică, asigurând alinierea la standardele din industrie și cele mai bune practici. Prin aceste faze, analiza a oferit perspective valoroase pentru cercetarea ulterioară.

Figura* 9. *Ocupațiile ESCO definite în raportul anterior

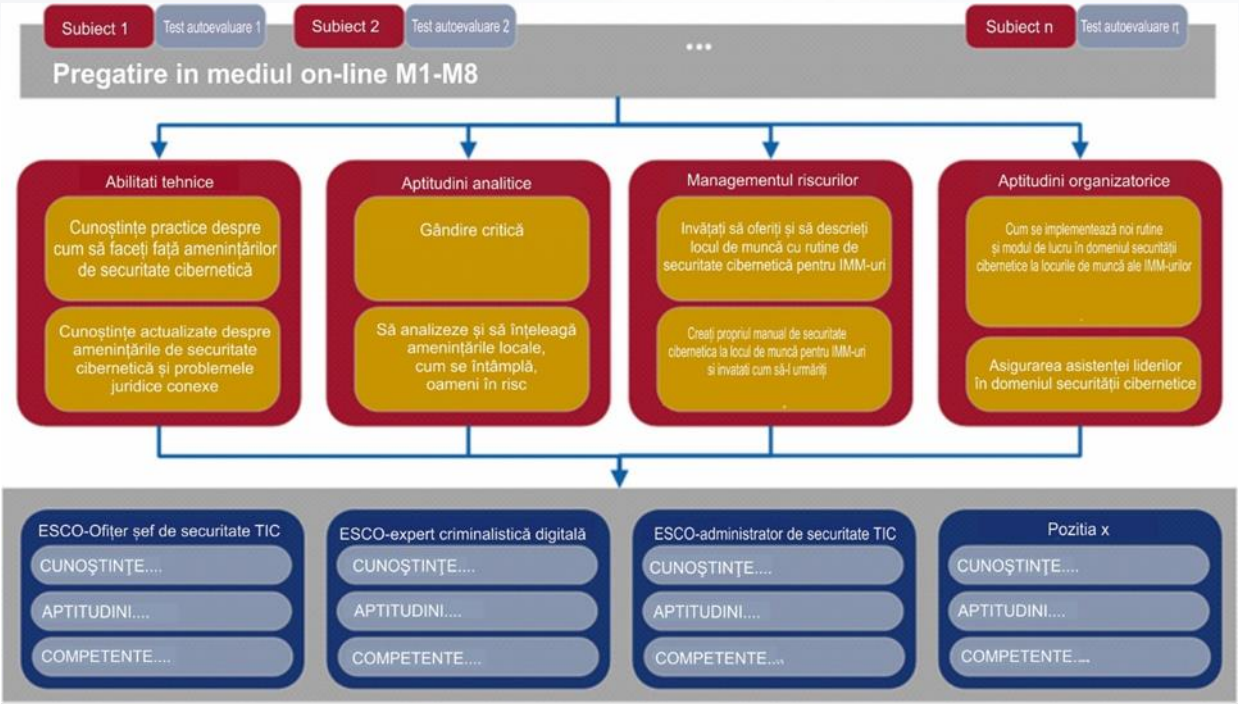

Figura* 10. *Posibile căi post-învățare

Figura 10 ilustrează potențialele parcursuri de carieră care pot fi urmate după finalizarea studiilor prin intermediul OLE (mediu de învățare online) (învățământ superior, VET, IMM) și dobândirea de competențe, în conformitate cu ocupațiile ESCO.

Cu o înțelegere mai clară a oportunităților de carieră, studenții și cursanții VET care aprofundează securitatea cibernetică vor dobândi o înțelegere mai clară a opțiunilor de carieră și vor putea alege un alt domeniu de studiu sau să lucreze în companii în poziții specifice, în timp ce studenții IT și alți studenți vor putea alege modulele CyberAgent ca module de studiu individuale, îmbunătățindu-și astfel competențele în domeniul de studiu, cum ar fi abilitățile organizaționale și de gestionare a riscurilor etc.

Personalul IMM-urilor va avea oportunitatea de a-și perfecționa competențele la locul de muncă. Pe baza traseului de carieră care a fost dezvoltat și cu oportunități clare de carieră, alți angajați ai IMM-urilor se vor putea recalifica în domeniul securității cibernetice.

O implicare sporită atât a studenților, cât și a personalului IMM-urilor este planificată prin integrarea schemelor de mentorat, organizarea de evenimente de diseminare, ateliere (proiectul include 6 ateliere comune organizate de toți partenerii, precum și campanii de diseminare organizate de fiecare partener), invitarea reprezentanților mediului de afaceri și ai securității cibernetice, cooperarea cu partenerii sociali și rețeaua CyberAgent, oferirea de stagii studenților etc. În plus, inițiativele noastre privind diversitatea, inclusiv programele de sensibilizare și sprijin direcționate, urmăresc să susțină participarea femeilor, încurajând o forță de muncă incluzivă în domeniul securității cibernetice.

Prin cartografierea completă a ocupațiilor ESCO prin modulele noastre de formare CyberAgent, participanții pot trece fără probleme de la mediile de învățare la roluri cu impact în securitatea cibernetică. Pentru a urmări evoluția carierei stagiarilor CyberAgent, este planificată organizarea de sondaje pre-formare, post-formare și de 3 luni post-training pentru a afla cum contribuie abilitățile lor la securitatea cibernetică a organizațiilor în care lucrează. Sondajele vor fi integrate în platforma de formare și vor fi oferite în mod automat cursanților înainte de începerea cursului, la sfârșitul cursului pentru a măsura progresul și pentru a evalua cursul și calitatea instruirii. Un al treilea sondaj va fi folosit pentru a afla dacă au existat schimbări în cariera participanților.

3. METODE DE PREDARE

Analiza metodelor pedagogice ale programului de studii Sisteme informaționale și securitate cibernetică al Universității din Vilnius (VU), programele de studii Timtal și Moisil Buzău și literatura externă ne permite să recomandăm mai multe combinații inovatoare de metode de predare. Aceste combinații ar putea fi incluse în modulele de studiu, ținând cont de structura fiecărui modul.

Tabelul* 1. *Metode de predare recomandate

Categoria	Informații detaliate
Prelegere și instruire directă	- Prelegeri teoretice: concepte și teorii fundamentale. - Speakeri invitați ((specialiști certificați în: Profesionist certificat în domeniul securității sistemelor informatice (CISSP), Auditor certificat în sisteme informatice (CISA), Manager certificat în securitatea informațiilor (CISM), CompTIA Security+, Hacker etic certificat(CEH), Certificarea GIAC Security Essentials (GSEC), Practician certificat în domeniul securității sistemelor (SSCP), Practician avansat în domeniul securității CompTIA (CASP+), GIAC Gestionar de incidente certificat (GCIH), Profesionist certificat de securitate ofensivă (OSCP).
Învățare practică	- Sarcini practice/Laboratoare: experimente practice și exerciții practice. - Activități practice: aplicații din lumea reală și sarcini interactive. - Analiza video tehnică: analiza conținutului video pentru învățarea abilităților tehnice. - Medii simulate: o Mașini găzduite pentru mediul cloud. o Lansați atacuri pe o mașină țintă. o Mașină pentru planificarea și efectuarea atacurilor – o cutie de atac.
Evaluare	- **Chestionare, jocuri**, ceea ce trebuie și ce nu trebuie să faci: evaluări interactive și captivante.

Categoria	Informații detaliate
	- Teste de autoevaluare: Pentru autoevaluarea cursanților la sfârșitul temelor.
Autostudii	- **Învățare autonomă**: această metodă susține căi de învățare personalizate și poate fi îmbunătățită cu resurse digitale și conținut modular pe care elevii le pot accesa după cum este necesar.
Învățare colaborativă și învățarea reciprocă	- **Învățare colaborativă**, lucru în echipă: proiecte de grup și sarcini de colaborare. - **Predare și învățare reciprocă**: cursanții predau și învață unii de la alții. - **Mentorat de grup și/sau mentorat individual**: îndrumări oferite de persoane mai experimentate.
Învățare îmbunătățită de tehnologie	- **Utilizarea platformei de învățare privind securitatea cibernetică gamificată**: implicarea cursanților prin elemente asemănătoare jocurilor în platformele de învățare. - **Competiții "Capture the flag"**: evenimente competitive pentru a îmbunătăți abilitățile de securitate cibernetică. - **Competiții**: competițiile testează abilitățile și cunoștințele elevilor într-un cadru practic, aplicat și oferă o măsură a competențelor lor într-un format competitiv.
Implicarea comunității și a publicului	- **Evenimente educaționale**: evenimente speciale precum Luna securității cibernetice. - **Prezentări publice**: seminarii, conferințe și webinarii. - **Rețele sociale**: utilizarea rețelelor sociale și a rețelelor pentru învățare și implicare. - **Ziua Campusului**: implică de obicei evenimente captivante, bazate pe campus, care pot include ateliere de lucru, prelegeri și oportunități de creare de rețele

Categoria	Informații detaliate
Modele inovatoare de învățare	- **Modelul Instrucțional BSCS 5E (5E-uri)** – cele 5E-uri se concentrează pe următoarele faze care constau în: Angajare, Explorare, Explicație, Elaborare, Evaluare. - **Modelul de învățare bazat pe provocări (CBL)** – o implementare timpurie a CBL oferă un cadru care constă din șase faze: descrieți provocarea, generarea și brainstormingul de idei, revizuirea perspectivelor multiple care pun întrebări și sprijină, cercetare și revizuire pentru cele mai bune soluții, testare ipoteză, împărtășiți constatările și concluziile. - **Modelul de Învățare Cooperativă (CL)** – similar modelelor 5E și CBL, Învățarea Cooperativă promovează învățarea activă în grupuri mici, iar elevii primesc o recompensă în funcție de performanța lor, care poate include o notă, o recompensă tangibilă precum un certificat sau o bursă sau o aprobare de la un profesor. - **Modelul de învățare bazat pe proiecte (PBL)** – Învățarea bazată pe proiecte și Învățarea bazată pe probleme folosesc aceeași abreviere pentru PBL și sunt ambele axate pe îmbunătățirea rezolvării problemelor, gândirii critice, munca în echipă, comunicarea și abilitățile creative; cu toate acestea, ele constau în diferite faze, cercetare independentă și de grup, dezvoltare și prezentare, analiza și evaluarea procesului. - **Modelul de învățare prin anchetă ghidată orientat pe proces (POGIL)** – această abordare ghidează elevii prin explorarea unui concept; urmată de invenție de concept în care elevii sintetizează și explică conceptul; şi închide ciclul de învăţare cu aplicarea conceptului teoretic. - **Modelul de învățare colaborativă cu anchetă ghidată (GICL)** – aceasta este o nouă abordare bazată în mare parte pe modelul POGIL.

Pentru a se asigura că diferitele strategii de formare oferite au cel mai bun impact posibil, fiecare abordare va fi selectată și aliniată cu obiectivele specifice de învățare ale modulelor de securitate

cibernetică în dezvoltarea unei programe cuprinzătoare de module și a materialelor de instruire. Metode suplimentare pot fi, de asemenea, alese de către lectorii/mentorii care vor oferi formarea CyberAgent. În timpul fazei de dezvoltare a materialelor de instruire, instruirea va fi oferită instructorilor cursurilor pilot pentru a-i informa cu privire la obiectivele, procesul și responsabilitățile instruirii și pentru a-i pregăti pentru a preda eficient curriculum-ul CyberAgent. Procesul de formare pilot include, de asemenea, colectarea de feedback de la cursanți și formatori pentru a monitoriza eficacitatea metodelor de formare utilizate și pentru a face ajustări acolo unde este necesar.

Modulele vor fi susținute în diferite formate de predare:

- **la distanță**,

- **prin învățare sincron** (sprijin deplin al profesorului),

- și **prin învățarea asincron** (sprijinul profesorului atunci când este necesar), învățare combinată și autoînvățare.

Întrucât sunt avute în vedere diferite moduri de furnizare a instruirii, metodele de instruire sunt prezentate în această etapă ca linii directoare.

4. STRUCTURA MODULELOR

Analiza structurii modulelor programului de studii VU Cyber security, analiza structurii modulelor proiectelor internaționale (CyberPhish (**https://cyberphish.eu/**), FuseIT (**https://www.knf.vu.lt/en/fuseit**), dComFra (**https://dcomfra.vdu.lt/**)) și analiza structurii modulelor platformelor comerciale, precum Udemy și Coursera (**https://www.coursera.org/**), a condus la crearea unei structuri tipice de module care ar putea fi aplicată atât la modulele de IFP, cât și de IFP.

Scopul principal este dezvoltarea a 8 module, în care 8 module ar fi pentru studenții IIS (nivelul EQF 5-6), pentru elevii VET și IMM-uri (nivelul EQF 4-5) și micro-module pentru toate tipurile de studenți.

Figura* 11. *Structura Modulului

* Se recomandă ca fiecare subtemă să fie urmată de întrebări de autotest (auto-reflecție). Cu toate acestea, în etapa de dezvoltare a modulului, poate fi aleasă o metodă sau opțiune de evaluare diferită, în funcție de tipul de studiu ales, de ex. studenților li se pot oferi exerciții practice, simulări etc., în timp ce întrebările de autotest sunt oferite cursanților independenți.

** Un test de evaluare a cunoștințelor este opțional. Dacă cursantul dorește să obțină un certificat de absolvire a cursului pentru a verifica cunoștințele dobândite, acest test este obligatoriu. Cu toate acestea, cursantul are opțiunea de a obține un certificat de finalizare a cursului pentru a dovedi că a urmat cursul, caz în care acest test este opțional.

Pentru a se asigura că fiecare modul de formare este direct legat de aplicabilitatea practică, descrierea fiecărui modul va oferi exemple clare despre modul în care teoria este aplicată în practică. Aceasta include nu numai scenarii detaliate pentru aplicabilitatea modulelor, ci și sarcini specifice pe care studenții le vor întreprinde pentru a consolida cunoștințele teoretice în situații reale de securitate cibernetică.

Fiecare modul ar trebui să ofere abilități tehnice, abilități analitice, abilități de gestionare a riscurilor, abilități organizaționale cu proporții diferite. Testul de autoevaluare este oferit pentru a testa cunoștințele cursanților la sfârșitul oricărei părți a modulului (subiect). Acest lucru permite nu numai evaluarea sau evaluarea cunoștințelor dobândite, dar și progresul cursantului este înregistrat și participantul colectează puncte și insigne, ceea ce îi permite participantului să fie mai implicat în procesul de învățare.

Conform formalităților ECTS, fiecare ECTS este de 25-30 de ore de lucru. În conformitate cu aceasta, fiecare modul ar putea fi egal cu 5 ECTS. Orele de lucru ar putea fi distribuite astfel:

Tabel 2. Ore de lucru

	Număr de module	**Total ECTS**	**Ore la la distanță pentru abilități teoretice**	**Orele la distanță pentru abilități practice**	**Ore de lucru individual**	**Total ore de lucru**
Module pentru studenții IIS (nivelul EQF 5-6)	8	8-40	20%	20%	60%	200-1200
Module pentru elevii VET (EQF nivel 4-5)	8	8-40	15%	25%	60%	200-1200
Autostudii (învățare mixtă)	8	8-40	10%		90%	200-1080
Autostudii (online)	8	8-40				200-1200
Micro-module	1-8	1-40				24-1200

Tabel 3. Volumul de lucru al modulelor recomandat

Modul	**ECTS**	**Total ore**	**Ore față în față**	**Ore față în față (teorie)**	**Ore față în față (practică)**	**Ore lucru individual**
IIS Titlu modul	1-5	25-150	40%	20%	20%	60%
VET Titlu modul	1-5	25-150	40%	15%	25%	60%
Autostudii (învățare mixtă)	1-5	25-150	10%			90%
Autostudii (online)	1-5	25-150				100%
Micro-secțiuni						10%-100%

Fiecare modul ar trebui să aibă propria sa descriere. După analiza VU, Timtal și a altor programe folosind micro-acreditări, este propusă o structură tipică de modul pentru fiecare modul Cyber-Agent (un exemplu de structură tipică de modul este dat în Anexa 1).

Tabel 4. Structura tipică pentru modulele CyberAgent

Categorie	**Informații detaliate**
Identificarea modulului (informații de bază despre modul)	-Titlul modulului -Codul modulului -Lector -Instituția sau departamentul în care se livrează modulul -Model de livrare -Limba -Cerințe preliminare
Durata modulului și volumul de lucru (angajamentul de timp clar definit și schița structurii)	-Durata totala (număr de ECTS) -Volumul de lucru al studenților în ore -Orele de lucru față în față -Program de lucru individual
Obiectivele educaționale și rezultatele învățării (detalii despre ceea ce urmărește modulul să realizeze și ce vor învăța cursanții)	- Scopul și rezultatele modulului - Rezultatele învățării o Abilități tehnice o Abilitati analitice o Abilități de risc o Abilitati de organizare
Metode de predare și învățare	-Metode de predare și învățare
Evaluare (explicație despre cum vor fi evaluați elevii)	-Metode de evaluare -Sarcini (laboratoare, proiecte, prezentări, rapoarte etc.) -Strategia de evaluare, criteriile de evaluare
Facilitati resursele	-Echipamente, software și tehnologie
Conținutul cursului	-Teme și subteme ale modulelor

Resurse	-Lista surselor -Surse suplimentare

Fiecare ECTS reprezintă 25-30 de ore (ore față în față sau online + studiu individual).

Modulul ar trebui să aibă cel puțin o ierarhie pe două niveluri:

- **Primul nivel al ierarhiei** – teme. La acest nivel, elementele principale ale modulului ar putea fi introducerea, testul inițial, testul final și elementul de bază – tema.
- **Al doilea nivel al ierarhiei** – subteme, principalele elemente educative ale modulului.

Fiecare modul de la primul nivel al ierarhiei ar trebui să includă:

- **INTRODUCERE** în modul (descriere textuală, introducere video): relevanța și beneficiile modulului, scopurile de bază și rezultatele modulului, software-ul și hardware-ul necesar, cerințele pentru participanți.
- **TEME** – temele principale ale cursului, material teoretic și metode de predare teoretică.
- **SUBTEMA** – subtema fiecărei teme, analiză practică, analitică și sarcini, metode de predare practice și analitice. Temele și subtemele pot include informații textuale, videoclipuri, clipuri audio, prezentări, link-uri către lecturi suplimentare.
- **MODULUL Test introductiv** (dacă este necesar). Testul introductiv la nivelurile intermediare și avansate ar trebui să confirme că solicitantul și-a însușit suficiente cunoștințe și abilități la nivelurile anterioare.
- **MODULUL Teste de confirmare**. Testul de recunoaștere ar trebui să ofere verificarea obiectivă a abilităților unui student și să demonstreze competența acestuia la cerințele modulului.
- **GHID pentru mentori/profesori**. Acest document ar trebui să conțină recomandări metodologice pentru mentori/profesori cu privire la utilizarea elementelor educaționale modulare.

Fiecare TEMA de la al doilea nivel al ierarhiei ar trebui să includă:

- **INTRODUCERE** în obiectivele și rezultatele temei, cuprins scurt.

- **SUBTEME**: toate elementele educaționale necesare pentru a sprijini cursantul să stăpânească abilitățile relevante.
- **Testul TEMĂ**: scurte recomandări pentru mentori/profesori cu privire la implementarea și aplicarea modulului. Fiecare SUBTEMĂ trebuie să fie compusă din elemente educaționale, al căror conținut corespunde sarcinilor din descrierea modulului. Fiecare subtemă poate (ar trebui) să includă un TEST de subtemă, care confirmă că studentul a însușit abilitățile relevante la un nivel suficient de înalt.

Materialele de instruire ale modulului ar trebui să susțină studiul a 6-8 teme, în fiecare dintre acestea fiind 4-6 subteme și, cel puțin, un test tematic. Așadar, modulul ar trebui să conțină (aproximativ) 30-40 de elemente educaționale (metode descrise în secțiunea Metode de predare) și 6-8 teste și un modul test de confirmare finală.

5. CURRICULUM ȘI PROGRAM DE FORMARE CYBERAGENT

Foaia de parcurs pentru construirea curriculumului

Curriculum-ul CyberAgent și Programul de formare urmează Ghidurile curriculare pentru programele postliceale în domeniul securității cibernetice, dezvoltate de grupul de lucru comun al ACM, IEEE, AIS SIGSEC și IFIP (2017)[8] (denumit în continuare – **Ghiduri**). Mai precis, întrucât obiectivul general al proiectului CyberAgent este de a crește competențele interne de securitate cibernetică ale IMM-urilor europene, curriculum-ul urmează cadrul domeniului de cunoștințe privind securitatea organizațională, conform recomandărilor din prezentele Ghiduri.

Acestea fiind spuse, primul pas în construirea curriculum-ului este cartografierea subtemelor și modulelor predefinite în proiectul CyberAgent cu unitățile de cunoștințe și subiectele cheie, recomandate și descrise de Ghid (pag. 59-70). Cartografierea se bazează pe corelația logică dintre acești doi piloni, așa cum a fost discutată și agreată de partenerii proiectului.

Al doilea pas este atribuirea unor rezultate specifice ale învățării, identificate și descrise din T2.2 „Cartografiarea nevoilor de instruire pentru agenții de schimbare a securității cibernetice pentru IMM-uri" cu unitatea de cunoștințe și temele cheie, cartografiate mai sus. Trebuie remarcat aici că diferitele ocupații legate de securitatea cibernetică pot avea o varietate de cunoștințe, abilități și competențe diferite, așa cum sunt prezentate în mod elocvent în livrabilul T2.2 menționat mai sus. Cu toate acestea, propunerea prezentată mai jos reflectă setul așteptat de cunoștințe, abilități și competențe CyberAgent, care pot fi adaptate la nevoile specifice ale anumitor ocupații sau grupuri de cursanți.

Acestea fiind spuse, rezultatele acestui exercițiu de construire a curriculumului sunt prezentate în Tabelul 5 de mai jos.

[8] The Joint Task Force on Cybersecurity Education. (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: A Report in the Computing Curricula Series. Association for Computing Machinery, 31 December 2017. Available at: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf [Accessed 3 March 2024]

Tabel **5.** *Foaia de parcurs pentru construirea curriculumului*

Subteme și Module	Unitatea de cunoștințe și teme cheie	Rezultatele învăţării pentru IIS	Rezultatele învăţării pentru VET
Abilități tehnice			
- Cunoștințe actualizate despre amenințările de securitate cibernetică și problemele juridice conexe	**Managementul programului de securitate** - Management de proiect - Managementul resurselor - Măsuri de Securitate - Asigurarea calității ăi controlul calității	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate despre principiile avansate de securitate cibernetică, inclusiv amenințările cibernetice sofisticate și vectorii de atac, legislația națională și internațională de securitate cibernetică, standardele și cerințele de conformitate relevante pentru industria lor. **Abilități**: Cursanții vor fi calificați să conceapă și să implementeze strategii avansate de evaluare și management al riscurilor pentru a atenua riscurile identificate, folosind metodologii și instrumente avansate. **Competențe**: Cursanții vor fi competenți să conducă și să gestioneze proiecte și echipe de securitate cibernetică care implementează politici și cadre strategice de securitate cibernetică aliniate cu obiectivele și obligațiile de conformitate ale organizației.	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice despre cele mai recente amenințări la adresa securității cibernetice, inclusiv atacuri de tip phishing, ransomware și DDoS, și cum să le gestioneze prin gestionarea eficientă a proiectelor și a resurselor și implementarea măsurilor de asigurare și control al calității. **Abilități**: Cursanții vor fi calificați să utilizeze instrumente și software pentru protecție împotriva amenințărilor cibernetice în evoluție și să aplice practici de securitate robuste în managementul proiectelor și al resurselor pentru a îmbunătăți valorile generale de securitate și controlul calității în cadrul organizațiilor lor. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea potențialelor amenințări de securitate, în comunicarea eficientă a problemelor de securitate cibernetică și în raportarea cu acuratețe a

			amenințărilor și încălcărilor prin canalele adecvate din cadrul organizației lor.
- Cunoștințe practice despre cum să faceți față amenințărilor la securitatea cibernetică	**Administrarea sistemelor** - Administrarea sistemului de operare - Administrarea sistemului bazei de date - Administrarea rețelei - Administrare cloud - Administrarea sistemului ciber-fizic - Întărirea sistemului - Disponibilitate	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate în administrarea sistemelor de operare, baze de date, rețele, cloud și ciber-fizice și alte domenii, permițându-le să întărească în mod eficient sistemele și să asigure disponibilitatea în timp ce aplică cele mai recente mecanisme de apărare a securității cibernetice. **Abilități**: Cursanții vor fi calificați să utilizeze metodologii și instrumente avansate pentru a proiecta și implementa arhitecturi de sisteme securizate, inclusiv sisteme de operare, baze de date, rețele și infrastructuri cloud **Competențe**: Cursanții vor fi competenți să dezvolte și să implementeze cadre strategice de securitate cibernetică pentru administrarea sistemului, să conducă proiecte și echipe pentru a îmbunătăți consolidarea și disponibilitatea sistemului și să ia decizii etice în menținerea unor practici solide de securitate cibernetică în diferite domenii administrative.	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice despre cum să administreze și să securizeze sistemele de operare, bazele de date, rețelele, cloud-urile și sistemele ciber-fizice împotriva amenințărilor cibernetice comune, cum ar fi phishing, ransomware și atacuri DDoS, implementând în același timp politici eficiente de gestionare a riscurilor. **Abilități**: Cursanții vor fi calificați să identifice riscurile și vulnerabilitățile potențiale de securitate cibernetică pe diferite platforme de sistem, folosind instrumente și software specializate pentru a îmbunătăți consolidarea și disponibilitatea sistemului și implementarea practicilor de bază de securitate cibernetică, cum ar fi crearea de parole sigure, navigarea în siguranță și gestionarea în siguranță a informațiilor sensibile. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea amenințărilor de securitate în cadrul administrării sistemului, comunicând eficient problemele de securitate cibernetică și raportând prompt orice amenințări și

			încălcări către canalele organizaționale corespunzătoare.
Abilități analitice			
-Gândire critică	**Instrumente analitice** - Măsurători de performanță (metrici) - Analiza datelor - Informații de securitate	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate despre legislația națională și internațională de securitate cibernetică, standardele și cerințele de conformitate și altele relevante pentru industria lor specifică. **Abilități**: Cursanții vor fi calificați să utilizeze măsurătorile, analiza datelor și inteligența de securitate pentru a proiecta și implementa strategii eficiente de gestionare a riscurilor. **Competențe**: Cursanții vor fi competenți în utilizarea instrumentelor analitice pentru a dezvolta politici strategice de securitate cibernetică cu o gândire critică și pentru a lua decizii în practicile de securitate cibernetică aliniate cu obiectivele organizaționale și obligațiile de conformitate.	**Cunoștințe**: cursanții vor dobândi cunoștințe practice despre cum să aplice măsurătorile performanței, analiza datelor și informațiile de securitate pentru a proteja activele organizaționale. **Abilități**: Cursanții vor fi calificați în utilizarea instrumentelor analitice pentru a identifica potențialele riscuri și vulnerabilități de securitate cibernetică, să aplice informații bazate pe date pentru a consolida practicile de securitate cibernetică și să utilizeze metrici de performanță pentru a evalua și îmbunătăți securitatea parolelor, a navigării, a e-mailului și a gestionării datelor. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea potențialelor amenințări de securitate folosind instrumente analitice, raportând cu acuratețe amenințările și încălcările la canalele adecvate din cadrul organizației lor.
- Analizați și înțelegeți amenințările locale, cum	**Operațiuni de securitate**	**Cunoștințe**: cursanții vor dobândi cunoștințe avansate despre	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice despre amenințările

se întâmplă acestea, persoanele aflate în risc etc.	- Convergența securității - Centre de operațiuni globale de securitate (GSOC)	amenințările cibernetice locale, folosind informații de la centrele de operațiuni de securitate globale și tendințele actuale în strategiile de apărare a securității cibernetice. **Abilități**: Cursanții vor fi calificați să utilizeze metodologii și instrumente avansate în cadrul centrelor de operațiuni globale de securitate pentru a concepe strategii eficiente de gestionare a riscurilor și pentru a dezvolta planuri pentru a atenua eficient amenințările locale de securitate cibernetică. **Competențe**: Cursanții vor fi competenți în dezvoltarea și implementarea politicilor strategice de securitate cibernetică care abordează amenințările locale prin utilizarea centrelor de operațiuni globale de securitate.	cibernetice locale și originile acestora, vor evalua modul în care aceste amenințări afectează activele organizaționale. **Abilități**: Cursanții vor fi pricepuți să identifice riscurile și vulnerabilitățile locale de securitate cibernetică, folosind instrumente și software, cum ar fi crearea de parole sigure, navigarea în siguranță și gestionarea securizată a datelor, adaptate mediilor lor specifice. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea amenințărilor locale de securitate folosind informații de la centrele de operațiuni de securitate globale, comunicând eficient problemele de securitate cibernetică și raportând cu acuratețe amenințările și încălcările către canalele adecvate din cadrul organizației lor.
Managementul riscului			
-Învățați să oferiți și să descrieți locul de muncă pentru IMM-uri cu rutine de securitate cibernetică	**Managementul riscurilor** - Identificarea riscului - Evaluarea și analiza riscurilor - Amenințări interne	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate despre procesele de gestionare a riscurilor, inclusiv identificarea, evaluarea și controlul riscurilor, permițându-le să stabilească și să descrie rutine eficiente de	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice în procesele de identificare, evaluare și control al riscurilor și strategii de gestionare a riscurilor pentru a proteja în mod eficient locurile de muncă ale IMM-urilor.

	- Modele și metodologii de măsurare și evaluare a riscurilor - Controlul riscurilor	securitate cibernetică, adaptate nevoilor specifice ale locurilor de muncă ale IMM-urilor, în conformitate cu standardele naționale și internaționale. **Abilități**: Cursanții vor fi calificați să aplice metodologii și instrumente avansate pentru a efectua evaluări cuprinzătoare ale riscurilor, pentru a concepe și implementa strategii eficiente de gestionare a riscurilor și pentru a dezvolta rutine robuste de securitate cibernetică, special adaptate la locurile de muncă ale IMM-urilor. **Competențe**: Cursanții vor fi competenți în dezvoltarea și implementarea politicilor strategice de securitate cibernetică pentru locurile de muncă ale IMM-urilor.	**Abilități**: Cursanții vor fi calificați în identificarea și analiza potențialelor riscuri de securitate cibernetică în mediile IMM-urilor, folosind instrumente și software adecvate pentru atenuarea amenințărilor și promovarea și implementarea practicilor esențiale de securitate cibernetică, inclusiv crearea de parole sigure, navigarea securizată și gestionarea în siguranță a datelor sensibile. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea amenințărilor de securitate la locurile de muncă ale IMM-urilor, comunicând eficient problemele și procedurile de securitate cibernetică și raportând cu acuratețe amenințările și încălcările relevante către canalele organizaționale adecvate.
-Creați propriul manual pentru IMM-uri la locul de muncă pentru securitatea cibernetică și cum să îl urmăriți	**Continuitatea afacerii, recuperarea în caz de dezastru și managementul incidentelor și securitatea personalului** - Răspuns la incident - Recuperare în caz de dezastru - Continuitatea afacerii	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate despre cum să creeze și să implementeze un manual cuprinzător de securitate cibernetică la locul de muncă pentru IMM-uri, care încorporează principii avansate de securitate cibernetică, cele mai recente mecanisme de apărare și aderarea la legislația și standardele naționale și internaționale în managementul	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice despre cum să creeze un manual cuprinzător de securitate cibernetică la locul de muncă pentru IMM-uri, care încorporează strategii de răspuns la incident, recuperare în caz de dezastru, continuitatea afacerii și securitatea personalului, protejând activele organizaționale și datele sensibile.

	- Conștientizarea, instruirea și educația în materie de securitate - Practici de angajare de securitate - Practici de terminare a securității - Securitate terță parte - Securitate în procesele de revizuire - Problemă specială privind confidențialitatea informațiilor personale ale angajaților	incidentelor, continuitatea afacerii și securitatea personalului. **Abilități**: Cursanții vor fi calificați să creeze și să mențină un manual de securitate cibernetică la locul de muncă pentru IMM-uri, folosind metodologii avansate pentru a evalua riscurile, a concepe strategii eficiente de gestionare a riscurilor și de răspuns la incident și a dezvolta planuri complete de continuitate a afacerii, adaptate nevoilor organizației lor. **Competențe**: Cursanții vor fi competenți în dezvoltarea și implementarea unui manual de securitate cibernetică pentru IMM-uri, conducând proiecte și echipe de securitate în mod eficient, asigurând alinierea la obiectivele organizaționale și obligațiile de conformitate.	**Abilități**: Cursanții vor fi capabili să identifice potențialele riscuri de securitate cibernetică, să utilizeze instrumente și software pentru a se proteja împotriva amenințărilor și să aplice cele mai bune practici în domeniul securității cibernetice pentru a dezvolta și menține un manual pentru IMM-uri care să abordeze crearea de parole sigure, navigarea, securitatea e-mailurilor și protecția datelor. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea amenințărilor de securitate, în comunicarea eficientă a politicilor și practicilor de securitate cibernetică și în raportarea sistematică a incidentelor de securitate în cadrul IMM-urilor lor, așa cum este subliniat în manualul lor personalizat de securitate cibernetică.
Abilități organizatorice			
- Cum se implementează noi rutine și mod de lucru în domeniul securității cibernetice la locurile de muncă ale IMM-urilor	**Politică și guvernare de securitate** - Contextul organizatoric - Confidențialitate - Legi, etică și conformitate - - Guvernarea securității	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate despre cum să implementeze noi rutine și fluxuri de lucru de securitate cibernetică în locurile de muncă ale IMM-urilor, încorporând principiile, tendințele actuale de securitate cibernetică și	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice despre cum să integreze noi rutine și practici de securitate cibernetică în locurile de muncă ale IMM-urilor, în conformitate cu legislația, standardele, strategiile și politicile de securitate cibernetică pentru

	- Comunicare la nivel de executiv și consiliu - Politica managerială	respectarea legislației naționale și internaționale relevante pentru industria lor. **Abilități**: Cursanții vor fi calificați în utilizarea metodologiilor avansate pentru a efectua evaluări ale riscurilor, pentru a proiecta și a implementa noi rutine de securitate cibernetică și pentru a pregăti strategii de răspuns, asigurând guvernanța și conformitatea eficiente la locurile de muncă ale IMM-urilor. **Competențe**: Cursanții vor fi competenți în dezvoltarea și implementarea politicilor strategice de securitate cibernetică, conducând inițiative pentru a stabili noi rutine și fluxuri de lucru la locurile de muncă ale IMM-urilor și luând decizii etice care se aliniază cu obiectivele organizaționale și cerințele de conformitate.	securitatea informațiilor, managementul riscurilor și protecția datelor. **Abilități**: Cursanții vor fi calificați în aplicarea instrumentelor și software-ului de securitate cibernetică pentru a implementa noi rutine de securitate, pentru a identifica și a atenua riscurile și pentru a promova practici esențiale de securitate cibernetică, cum ar fi crearea de parole sigure, navigarea și manipularea datelor în cadrul de guvernanță al locurilor de muncă ale IMM-urilor. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea potențialelor amenințări de securitate, în comunicarea eficientă a modificărilor și politicilor de securitate cibernetică și în raportarea cu acuratețe a incidentelor de securitate din cadrul IMM-urilor, conform cerințelor de guvernanță și conformitate.
- **Efectuarea asistenței liderilor în domeniul securității cibernetice.**	**Planificarea securtății cibernetice** - Planificarea strategică - Managementul operațional și tactic	**Cunoștințe**: Cursanții vor dobândi cunoștințe avansate despre cum să integreze principiile avansate de securitate cibernetică și tendințele actuale în planificarea strategică și managementul operațional. **Abilități**: Cursanții vor fi calificați în planificarea strategică și	**Cunoștințe**: Cursanții vor dobândi cunoștințe practice despre cum să integreze planificarea strategică și managementul operațional în securitatea cibernetică pentru a proteja activele organizaționale, a respecta legislația și standardele relevante și vor implementa strategii eficiente de securitate a

		managementul operațional, permițându-le să proiecteze și să implementeze eficient strategii de securitate cibernetică care abordează riscurile emergente și asigură răspunsuri tactice robuste. **Competențe**: Cursanții vor fi competenți în dezvoltarea și implementarea cadrelor strategice de securitate cibernetică, conducerea și gestionarea inițiativelor de securitate cibernetică.	informațiilor și politici de gestionare a riscurilor. **Abilități**: Cursanții vor fi calificați în identificarea riscurilor de securitate cibernetică, folosind instrumente de planificare strategică și management operațional pentru a se proteja împotriva amenințărilor și promovarea implementării practicilor fundamentale de securitate cibernetică în rolurile lor de sprijin de conducere. **Competențe**: Cursanții vor fi competenți în evaluarea și atenuarea amenințărilor de securitate, în comunicarea eficientă a strategiilor și problemelor de securitate cibernetică și în raportarea fiabilă a incidentelor și vulnerabilităților către canalele adecvate din cadrul organizațiilor lor.

6. STRATEGIA DE EVALUARE A CURSULUI

Evaluarea cunoștințelor este o parte integrantă a procesului de învățare și promovează o învățare mai profundă. Acest capitol descrie abordarea evaluării cursurilor care este necesară pentru a se asigura că toți participanții la cursurile CyberAgent obțin rezultatele și competențele de învățare necesare. Procesul de evaluare în cadrul cursului este împărțit în două părți principale: teste de autoevaluare și de evaluare a cunoștințelor, care sunt adaptate atât studenților din învățământul superior (IIS), cât și elevilor din învățământul pentru formarea profesională (VET), ținând cont de nevoile și obiectivele de învățare ale acestora.

Deoarece temele modulelor ar putea fi aceleași atât pentru învățământul superior, cât și pentru VET, unele dintre întrebări pot fi potrivite pentru ambele situații. Astfel, la conceperea întrebărilor, va fi posibil să se precizeze dacă întrebarea este destinată numai VET sau învățământul superior sau pentru ambele. Acest mod de marcare va fi folosit doar la proiectarea întrebărilor, deoarece va facilita proiectarea întrebărilor. Odată ce întrebările au fost importate în platformă, bazele de date vor fi diferite pentru VET și IIS.

Figura* 12. *Baze de date de autoevaluare și evaluare a cunoștințelor

1. **Teste de autoevaluare**: După finalizarea fiecărei teme din cadrul cursului, studenții vor susține teste de autoevaluare. Aceste evaluări sunt concepute pentru a oferi feedback imediat, ajutându-i pe studenți să-și evalueze înțelegerea materialului recent acoperit. Această etapă încurajează auto-reflecția și ajută la consolidarea obiectivelor de învățare ale fiecărei teme. În plus, le permite cursanților să identifice domeniile în care ar putea avea nevoie de studii suplimentare sau clarificări, promovând o abordare proactivă a călătoriei lor de învățare.

Prin utilizarea testelor de autoevaluare, participanții la curs au putut identifica nivelul inițial de cunoștințe și ar putea verifica progresul după fiecare subiect de instruire.

Se recomandă un test de autoevaluare cu 3-5 întrebări, cu un amestec de întrebări adevărat/fals, potrivire și/sau cu răspunsuri multiple. O altă temă ar trebui deblocată numai după ce s-a răspuns correct la toate întrebările. Nu ar trebui să existe limite de timp sau restricții privind încercările. Încercarea ar trebui să selecteze aleatoriu întrebări din baza de date corespunzătoare.

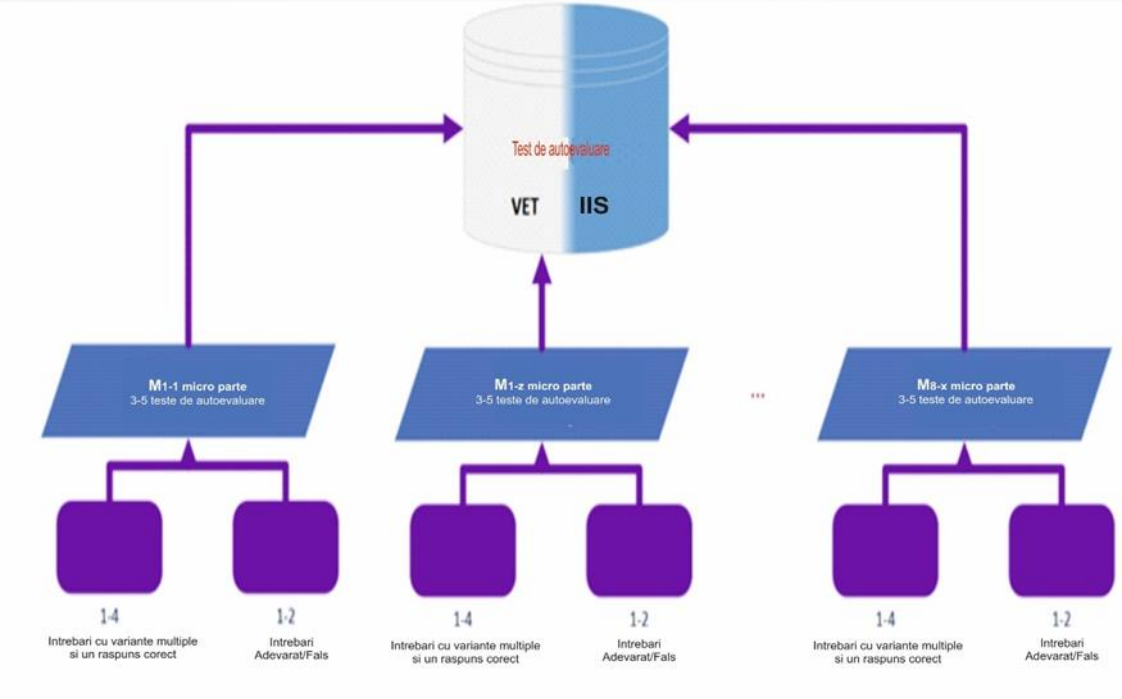

Figura* 13. *Structura bazei de date de autoevaluare

2. **Test de evaluare a cunoștințelor***: La finalizarea tuturor temelor din curs, studenții vor fi obligați să susțină un test final pentru a obține certificatul de finalizare a cursului. Această evaluare cuprinzătoare evaluează înțelegerea generală și stăpânirea conținutului cursului. Testul final evaluează reținerea de către studenți a materialului și identifică cât de bine își pot aplica cunoștințele într-un context mai larg.

* Pe parcursul elaborării curriculumului și materialelor, vor fi luate în considerare și alte metodologii de evaluare a finalizării cursului și evaluarea cunoștințelor, cum ar fi studii de caz, exerciții practice și rapoarte de reflecție, care vor permite o evaluare mai cuprinzătoare a participanților. abilități de gândire analitică și critică. Această abordare va fi, de asemenea, disponibilă lectorilor pentru studenții din IIS și VET în cadrul predării cursurilor.

Prin utilizarea testului de evaluare a cunoștințelor, participanții la curs pot identifica nivelul lor final de cunoștințe și, dacă au promovat, pot primi o insignă de finalizare a cursului (certificat).

Se recomandă un test de evaluare a cunoștințelor cu 36 de întrebări, cu o combinație de întrebări adevărat/fals, potrivire și cu răspunsuri multiple. Ar trebui să existe o limită de timp de 45 de minute și să fie permisă o singură încercare. Testul ar trebui să fie administrat prin selectarea aleatorie a întrebărilor dintr-o bază de date.

În plus, evaluarea ar trebui să ia în considerare și prevenirea înșelăciunii și, prin urmare, ar trebui dezvoltate aproximativ patru seturi de întrebări. Unele dintre întrebările testului de cunoștințe atât pentru VET, cât și pentru IIS se pot suprapune, așa că vom avea trei atribute în momentul dezvoltării: VET, învățământ superior, sau VET și învățământ superior.

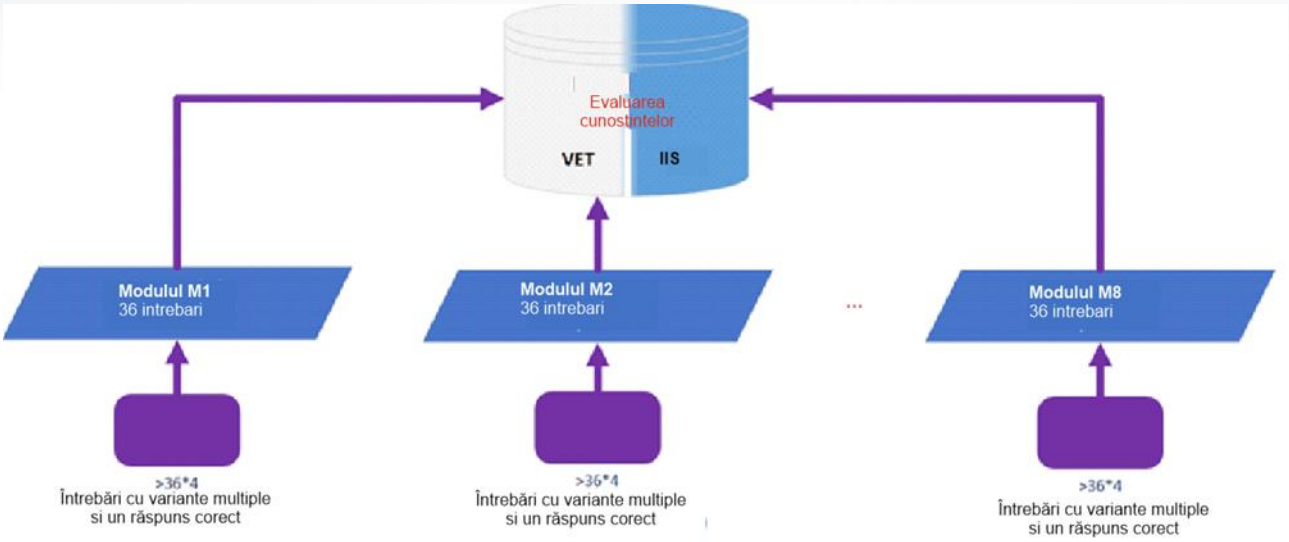

Figura* 14. *Structura bazei de date de evaluare a cunoștințelor

Această strategie de evaluare în două etape nu numai că sprijină învățarea eficientă, oferind mai multe bucle de feedback, ci și împuternicește cursanții să își asume un rol activ în formarea lor.

Testele de autoevaluare și testele de evaluare a cunoștințelor vor fi elaborate în urma programului de studii a cursurilor și pe baza rezultatelor și recomandărilor elaborate în cadrul acestui proiect.

COMPONENȚA BAZEI DE DATE CU ÎNTREBĂRI

Pentru a asigura o bază de întrebări suficient de mare și echilibrată, se vor crea cel puțin 5 întrebări de tip "adevărat/fals sau de asociere" și 5 întrebări cu alegere multiplă pentru fiecare subiect din cursul VET sau IIS.

Presupunând că vor exista cel puțin 10 subiecte în fiecare curs, baza generală pentru fiecare curs VET sau IIS ar trebui să conțină cel puțin 10-20% de întrebări de tip "adevărat/false" sau de asociere și 90-80% de întrebări cu alegere multiplă. Aceasta este o orientare generală, dar profesorul va avea posibilitatea de a alege structura întrebărilor în funcție de tematica cursului.

Luând în considerare diferențele dintre obiectivele și rezultatele învățării VET / HE, compoziția generală a bazei de date a întrebărilor pentru un singur curs ar trebui să conțină așa cum se arată în tabelul de mai jos.

Tabelul 6. Tipuri de întrebări

	Întrebări de tip "Adevărat/fals" sau de asociere	Întrebări cu alegere multiplă
Partea generală a cursului	20%	80%
Partea specifică VET a cursului	20%	80%

Partea de curs specifică instituțiilor de învățământ superior	20%	80%
Total pentru un curs VET și IIS:	20%	80%

GHID PENTRU CONSTRUIREA ÎNTREBĂRILOR

Întrebările pentru testele de autoevaluare și de evaluare a cunoștințelor trebuie să fie pregătite în limba engleză și apoi localizate în limbile partenerilor.

Atunci când se elaborează întrebări de test atât pentru autoevaluare, cât și pentru evaluarea cunoștințelor în cadrul cursului, este esențial să se asigure că întrebările sunt clare, concise și accesibile tuturor candidaților, indiferent de pregătirea acestora. Această abordare asigură faptul că evaluările reflectă cu acuratețe înțelegerea de către cursanți a conținutului cursului și capacitatea lor de a îndeplini competențele și obiectivele declarate, prezentate în programele de studiu ale cursului.

Orientări generale pentru construirea întrebărilor:

La elaborarea întrebărilor de test se vor aplica linii directoare clare: întrebările trebuie să fie ușor de înțeles și să aibă o legătură directă cu obiectivele de învățare ale cursului, fără a utiliza terminologie complexă sau formulări confuze. De asemenea, vor fi evitate întrebările specifice din punct de vedere cultural sau confuze, pentru a asigura corectitudinea și accesibilitatea pentru toți participanții la curs. Mai jos sunt oferite mai multe îndrumări privind conceperea întrebărilor.

Claritate și simplitate: întrebările trebuie să fie clare, evitându-se utilizarea unui limbaj complex sau a unui jargon care ar putea deruta sau induce în eroare candidații. Scopul este de a evalua cunoștințele și înțelegerea subiectului de către candidați, nu capacitatea lor de a descifra întrebări complicate.

Directitudine și relevanță: fiecare întrebare ar trebui să aibă o legătură directă cu competențele și obiectivele cheie ale programelor de studii. Ar trebui evitat conținutul irelevant sau tangențial pentru a menține accentul pe evaluarea rezultatelor învățării vizate.

Sensibilitate culturală și de fond: asigurați-vă că întrebările nu presupun cunoștințe sau experiențe culturale specifice, ceea ce le face accesibile și corecte pentru candidații din medii diverse.

Fără întrebări înșelătoare: intenția fiecărei întrebări trebuie să fie clară, fără nicio încercare de a induce în eroare sau de a păcăli candidații. Întrebările concepute pentru a-i prinde pe candidați sau pentru a le testa capacitatea de a detecta trucurile nu evaluează în mod eficient înțelegerea subiectului.

Prezentare clară și concisă: întrebările trebuie formulate într-un mod care să nu lase loc de interpretări, asigurându-se că toți candidații înțeleg întrebarea în același mod. Asigurați-vă că întrebările sunt concise, evitând lungimile inutile care ar putea ascunde punctul principal.

Formularea pozitivă: evitați să folosiți formulări negative în întrebări (de exemplu, "Care dintre următoarele NU este..."). Formularea negativă poate duce la confuzii și interpretări greșite, în special în condiții de examen. În schimb, formulați toate întrebările în mod pozitiv pentru a promova claritatea**.**

Orientări specifice pentru construirea întrebărilor:

Întrebări cu alegere multiplă: asigurați-vă că toate opțiunile sunt plauzibile și relevante pentru întrebare. Răspunsul corect ar trebui să fie indiscutabil corect, în timp ce variantele de distragere a atenției ar trebui să fie în mod clar incorecte pentru cineva care înțelege materialul.

Întrebări de tip Adevărat/Fals: prezentați afirmații clare, bazate pe fapte, care au legătură directă cu conținutul cursului, asigurându-vă că nu există nicio ambiguitate cu privire la valoarea lor de adevăr.

Întrebări de potrivire: asigurați-vă că ambele liste (de exemplu, termenii de pe o parte și definițiile de pe cealaltă) sunt clar legate între ele și că există o bază directă pentru a face fiecare potrivire. Evitați listele inegale în care numărul de elemente nu se aliniază, cu excepția cazului în care se precizează în mod explicit că unele elemente nu vor fi folosite sau pot fi folosite de mai multe ori.

Formarea pilot va analiza informațiile privind metodologiile de evaluare a cunoștințelor și procesul de evaluare prin colectarea de feedback atât de la cursanți, cât și de la formatori. Acest lucru va permite să se evalueze caracterul adecvat al metodelor de evaluare a cunoștințelor și, dacă este necesar, să se completeze sau să se îmbunătățească abordarea evaluării.

GAMIFICARE

Această secțiune prezintă descrierea elementelor de gamificare implementate în cursurile CyberAgent. Gamificarea este procesul de încorporare a principiilor de gamificare în activitățile tradiționale de învățare pentru a crește motivația și implicarea participanților. Aceste elemente au fost selectate pe baza celor mai recente cercetări în domeniul tehnologiei educaționale, care arată că gamificarea poate îmbunătăți semnificativ performanțele de învățare, poate crește motivația studenților de a învăța și poate spori implicarea acestora în procesul de învățare.

Elementele de gamificare care vor fi integrate în cursuri includ insigne, puncte, ranguri și porecle colorate care reflectă experiența și realizările participanților.

- Se vor acorda insigne pentru:

- Finalizarea modulului.

- Pentru promovarea unui test, pe baza procentului de promovare. De exemplu, un participant va primi o insignă de bronz pentru un punctaj minim de trecere la testul final, o insignă de argint pentru un punctaj minim de trecere de 75%, o insignă de aur pentru un punctaj de trecere de 76%-90% și o insignă de platină pentru un punctaj de trecere de 90%-100%. În acest caz, un participant poate avea 8 insigne de acest tip.

- Completarea subiectului.

- Conectarea la sistem în fiecare zi, timp de zece zile.

- O insignă de activitate specială pentru fiecare subiect va fi, de asemenea, acordată de către mentorul/instructorul cursului.

- Puncte și scoruti calculate pe baza punctajelor la testul de autoevaluare + punctajul la testul final cu multiplicator.

Participanții la cursul CyberAgent nu își vor putea vedea progresul individual, dar vor putea concura cu alți participanți în grupuri sau echipe (pe baza celui mai mare număr de puncte obținute, dar și pe baza celor mai multe insigne). Acest lucru încurajează nu doar competiția individuală, ci și cooperarea în echipă, ceea ce este important pentru dezvoltarea abilităților de cooperare.

Fiecare participant își va vedea porecla atunci când se conectează la curs, care va fi codificată în culori în funcție de evoluția cursului și de experiența acumulată (cursuri finalizate/înregistrate).

Acest lucru îi va ajuta pe participanții la curs să se implice mai bine în procesul de formare. Participanții la curs pot repeta același test de mai multe ori pentru a-și îmbunătăți punctajul (se acordă puncte pentru cel mai mare număr de teste de autoevaluare efectuate corect).

Un algoritm special va calcula scorul fiecărui participant ținând cont de timpul de răspuns, de numărul de repetări ale testului și de alți parametri, reducând astfel la minimum posibilitatea de a trișa.

Toate regulile de gamificare vor fi descrise și comunicate în mod clar participanților, astfel încât fiecare să poată înțelege cu ușurință cum pot fi atinse diferitele niveluri de gamificare și cum sunt calculate.

7. PROCESUL DE ÎNVĂȚARE/PREDARE A AGENȚILOR CIBERNETICI

Această secțiune sintetizează informațiile din toate capitolele acestui document și descrie în detaliu procesul de învățare/predare, începând cu înscrierea la un curs CyberAgent pe platforma de învățare și terminând cu finalizarea cursului sau cu eliberarea unui certificat.

Cursurile CyberAgent sunt concepute pentru a se adresa unei game variate de cursanți, inclusiv studenților din instituțiile de învățământ superior (HEI), studenților din învățământul profesional și de formare profesională (VET), precum și angajaților din IMM-uri. Ne propunem să oferim fiecărui participant posibilitatea de a alege modalitatea de învățare care i se potrivește cel mai bine, ținând cont de circumstanțele personale și de politicile organizaționale ale instituției de formare.

În ciuda metodei de învățare/formare aleasă, participanții se înregistrează pe platforma CyberAgent și utilizează platforma în timpul formării.

Înregistrare

Potențialii participanți interesați să se înscrie la cursul CyberAgent trebuie să completeze un formular de înregistrare, selectând modulele dorite și metoda de învățare preferată. Este furnizată o diagramă conceptuală pentru a ghida participanții pe parcursul parcursului de învățare, de la primul până la al optulea modul CyberAgent.

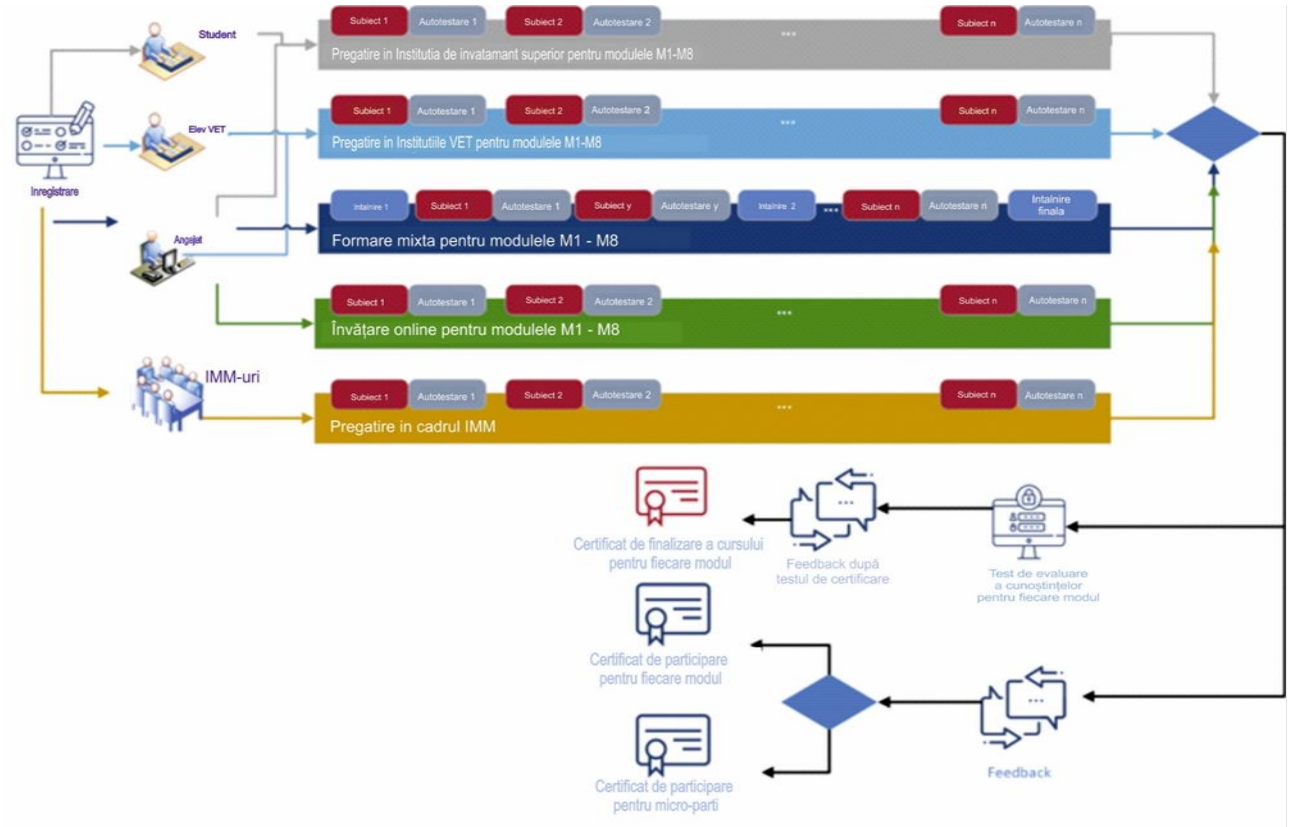

Figura* 15. *Calea de învățare/predare CyberAgent

Confidențialitatea informațiilor despre participanți va fi asigurată în timpul procesului de înregistrare, în special în ceea ce privește cerințele GDPR. În timpul înregistrării, participanții vor avea posibilitatea de a se familiariza cu regulile platformei de formare, cu regulile de confidențialitate și de protecție a datelor.

Datele de înregistrare ale participanților sunt accesibile doar persoanelor desemnate din cadrul organizației partenerilor, în conformitate cu politicile interne ale organizației. În timpul sesiunilor pilot de formare, datele participanților de la partenerii de proiect pot fi accesibile coordonatorului CyberAgent, iar ceilalți parteneri nu au voie să vadă datele participanților celorlalți. La finalizarea proiectului, coordonatorul poate accesa datele anonime ale celorlalți parteneri doar pentru monitorizarea rezultatelor proiectului, așa cum se specifică în cererea de proiect, timp de până la 5 ani după încheierea proiectului.

Oferim opțiuni de formare personalizate pentru a răspunde nevoilor diverselor noastre grupuri țintă. Studenții din învățământul superior și din învățământul profesional și tehnic se pot implica în formare prin intermediul sesiunilor de contact cu universitățile. Angajații IMM-urilor pot alege metoda de învățare care se potrivește cel mai bine nevoilor lor: învățare mixtă, doar online sau, mai rar, se pot alătura cursurilor HEI sau VET.

De asemenea, formarea poate fi oferită și companiilor mai mari, cu mai mulți angajați. În astfel de cazuri, metoda de formare va fi personalizată pentru a răspunde nevoilor specifice, încorporând în același timp cursurile din modulul CyberAgent.

După ce se înregistrează pe platformă, participanții își selectează metoda de învățare și își încep studiile. După finalizarea unui modul sau a unei părți a unui modul, aceștia se pot califica pentru un certificat de participare sau un certificat de finalizare a cursului, acesta din urmă fiind eliberat dacă participantul trece testul de modul cu un punctaj de cel puțin 75%.

În cele din urmă, participanților li se cere să completeze un formular de feedback înainte de a primi orice certificat. Acest feedback este esențial pentru îmbunătățirea continuă a ofertelor noastre de formare și pentru asigurarea satisfacției participanților.

Modalitati de învățare/formare

Angajații au la dispoziție mai multe opțiuni pentru a se implica în conținutul cursului:

- În cazul în care instituțiile de învățământ superior sau de formare profesională le permit angajaților să participe în calitate de participanți invitați, aceștia pot participa la cursuri alături de studenții înscriși. Astfel de sesiuni cu participanți externi pot fi organizate de 1-2 ori pe an, pe baza programului de cursuri publicat.

- Angajații pot opta pentru o abordare de formare mixtă, în care sesiunile de formare se desfășoară la date specifice, cu o durată recomandată de 2-4 luni. Se recomandă grupuri de cel puțin 10 participanți, cu un maxim de 30 de participanți pe grup. Formarea mixtă include atât

consultări față în față, cât și online, la începutul, în timpul și la sfârșitul cursului, pentru a facilita feedback-ul direct și pregătirea pentru evaluarea finală.

- Angajații pot alege modalitatea de învățare online pentru o învățare în ritm propriu, fără o durată stabilită pentru finalizarea cursului.

- Mai multe detalii despre modulele CyberAgent sunt furnizate în secțiunea 1. Calea de studiu.

Implicarea studenților

Studenții înscriși în programul de studii în domeniul securității cibernetice pot întâmpina diferite trasee în funcție de reglementările instituției lor academice. Aceștia pot fi obligați să parcurgă unele sau toate modulele CyberAgent sau, în funcție de politicile interne ale universității, studenții care îndeplinesc criteriile pot alege să studieze unul sau mai multe module CyberAgent. Studenții HEI sau VET se implică în mod obișnuit în subiecte prin intermediul instruirii tradiționale în clasă, așa cum este oferită de instituția lor, sau pot opta pentru metode de studiu individual pentru a se pregăti pentru testul final de evaluare a cunoștințelor.

Implicarea IMM-urilor

În organizațiile în care se consideră necesară formarea în domeniul securității cibernetice, un reprezentant al companiei poate înscrie organizația pentru sesiuni de formare internă. În astfel de cazuri, în urma unui acord separat cu universitatea și/sau instructorii, metoda de formare, programul și eliberarea certificatelor pot fi adaptate la nevoile specifice ale organizației, pe baza modulelor existente.

Colectarea de feedback

La finalizarea modulului, participanții sunt rugați să completeze un formular de feedback anonim accesibil online. Datele de feedback sunt accesibile doar personalului autorizat din cadrul organizației partenerului, măsuri de confidențialitate similare fiind aplicate în timpul sesiunilor de formare pilot și al utilizării datelor post-proiect.

Feedback-ul va fi colectat în principal de la participanții la curs, dar va fi colectat și feedback-ul din partea mentorilor/formatorilor. Feedback-ul colectat va evalua nivelul de satisfacție organizațional al participanților, aspecte legate de organizarea cursului, procesul de învățare, utilizarea în practică a competențelor dobândite, conținutul cursului, strategiile de evaluare, includerea elementelor de gamificare, domeniile de îmbunătățire etc.

Rezultatele feedback-ului vor fi analizate periodic și prezentate echipei de management al proiectului pentru a reacționa rapid și a îmbunătăți strategiile de formare în funcție de nevoile reale și de schimbările de pe piață.

Numai după completarea acestui formular, participanții sunt eligibili pentru a obține un certificat de participare sau pentru a obține certificatul de absolvire a cursului sau certificatul de participare.

Certificat de absolvire a cursului

Finalizarea cu succes a testului de evaluare are ca rezultat generarea unui certificat de absolvire a cursului pentru participant. Există un test final pentru fiecare modul.

Certificat de participare

Participanții care optează să nu susțină testul de evaluare a cunoștințelor pot primi un certificat de participare. Această recunoaștere poate fi emisă la finalizarea unui singur modul sau a mai multor microparți din cadrul cursului.

CONCLUZII ȘI SINTEZĂ

Acest raport a dezvoltat cu succes trasee de învățare structurate pentru agenții de schimbare în domeniul securității cibernetice din IMM-uri, adaptate pentru a răspunde nevoilor specifice la diferite niveluri educaționale și profesionale, de la învățământul superior la formarea profesională și la formarea directă a angajaților IMM-urilor. Curriculumul conceput, care cuprinde opt module cuprinzătoare, integrează competențe tehnice, analitice, organizaționale și de gestionare a riscurilor, care sunt esențiale pentru abilitarea eficientă a viitorilor profesioniști în domeniul securității cibernetice.

Abordarea structurată a traseelor de învățare asigură un parcurs educațional cuprinzător pentru angajații IMM-urilor. Prin intermediul etapelor de Preînvățare, Învățare și Post-învățare, aceasta sprijină retenția cunoștințelor și aplicarea practică. Micromodulele oferă flexibilitate și adaptabilitate la nevoile individuale, îmbunătățind învățarea cu micro-credințe care oferă calificări recunoscute. Această aliniere la standardele industriei contribuie semnificativ la fortificarea capacităților de securitate cibernetică în cadrul IMM-urilor, pregătind angajații pentru a face față provocărilor actuale și progreselor viitoare. Următoarea analiză Carrier Pathway a cartografiat progresia rolurilor în domeniul securității cibernetice, așa cum sunt definite de cadrul ESCO, facilitând o abordare educațională orientată care pregătește indivizii pentru o integrare eficientă în forța de muncă în domeniul securității cibernetice, îmbunătățind în cele din urmă perspectivele de carieră și dezvoltarea lor profesională.

Diversitatea explorată a abordărilor pedagogice din cadrul programului de studii în domeniul securității cibernetice ar trebui să permită un mediu de învățare dinamic și flexibil care să se adapteze la diferite stiluri și nevoi de învățare. Încorporarea diverselor metode de predare, inclusiv cursuri teoretice, laboratoare practice, gamificare și proiecte de colaborare, asigură faptul că studenții nu sunt doar destinatari ai cunoștințelor, ci și participanți activi în procesul de învățare. Această strategie cuprinzătoare ar trebui să sporească implicarea, înțelegerea și să îi pregătească mai bine pe studenți pentru provocările din lumea reală a securității cibernetice. Adaptabilitatea metodelor de predare la cerințele specifice fiecărui modul ar trebui să personalizeze și mai mult experiența de învățare, asigurând că rezultatele educaționale sunt maximizate pentru fiecare student.

Prin cartografierea sistematică a subdomeniilor și modulelor proiectului CyberAgent la unitățile de cunoaștere recunoscute la nivel internațional, planul de învățământ nu numai că îndeplinește, ci și anticipează cerințele dinamice ale domeniului securității cibernetice. Această abordare metodică asigură că fiecare rezultat al învățării este legat în mod strategic de competențele din lumea reală, care sunt esențiale pentru gestionarea eficientă a amenințărilor la adresa securității cibernetice. Adaptabilitatea programului de studii îi permite să servească diferitelor roluri profesionale din cadrul industriei, pregătind cursanții nu doar pentru provocări imediate, ci și pentru dezvoltarea pe termen lung a carierei în domeniul securității cibernetice.

Strategia de evaluare a cursurilor descrisă oferă un cadru pentru evaluarea competenței și a progresului studenților din programele de securitate cibernetică. Abordarea în două etape, care combină testele de autoevaluare și testele de evaluare a cunoștințelor cuprinzătoare, permite studenților să se implice activ în materie, să își evalueze în mod continuu înțelegerea și să își ajusteze strategiile de învățare în consecință. Prin conceperea evaluării pentru a se adapta atât instituțiilor de învățământ superior, cât și studenților din învățământul profesional și tehnic, cu întrebări adaptate, strategia asigură relevanța și adecvarea pentru fiecare nivel educațional, îmbunătățind experiența de învățare. Această metodă permite o măsurare clară a gradului de stăpânire și a pregătirii studenților de a-și aplica cunoștințele în mod practic. În plus, introducerea elementelor de gamificare, cum ar fi insignele și sistemele de punctaj, nu numai că îi motivează pe studenți, dar încurajează și un mediu de învățare competitiv, dar colaborativ.

În cele din urmă, procesul de învățare și predare CyberAgent oferă un cadru educațional cuprinzător și adaptabil, potrivit pentru o gamă diversă de cursanți din instituțiile de învățământ superior, instituțiile de formare profesională și IMM-uri. Acest sistem permite diverse metode participative, inclusiv învățarea față în față, mixtă și online, asigurând flexibilitate în ceea ce privește modul în care este oferită și accesată formarea în domeniul securității cibernetice. Înscrierea pe platforma CyberAgent inițiază un parcurs în care participanții selectează modulele și metodele de învățare preferate, care culminează cu eliberarea de certificate după finalizarea și evaluarea cu succes. Această structură nu numai că sprijină traiectoriile de învățare personalizate, dar se aliniază și la standardele riguroase de confidențialitate esențiale pentru menținerea confidențialității participanților pe tot parcursul procesului de formare.

Recomandările și orientările furnizate în acest document vor fi utilizate în faza următoare pentru a dezvolta programe de formare cuprinzătoare CyberAgent, materiale de formare, teste și evaluări ale cunoștințelor, exerciții practice și alte conținuturi de formare, care vor fi integrate în platforma de formare CyberAgent.

ANEXA 1. DESCRIEREA MODULULUI

DESCRIEREA MODULULUI

Titlul modulului	Codul modulului
...	

Profesor(i)	Instituția sau departamentul în care este livrat modulul
...	...

Mod de livrare	Limbă
Față în față, online, mixte, consultații	*Engleză, ...*

Cerințe prealabile
...

Număr de credite ECTS alocate	Volumul de lucru al elevului	Ore de lucru față în față	Ore de lucru individial
5	...	...	...

Obiectivul și rezultatele modulului		
...		
Rezultatele învățării modulului	**Metode de învățare și predare**	**Metode de evaluare**
Competențe tehnice		
Competențe analitice		
Competențe de risc		
Competențe de organizare		

Facilitarea resurselor (echipamente, software, tehnologie)
...

Conținutul modulului: defalcarea subiectelor	**Ore față în față**					**Ore de lucru individual și sarcini**	
	Cursuri (IIS/VET)	Consultații(IMMur)	Practică(IIS/VET)	Teste	**Toate activitățile față în față**	**Muncă individială**	**Sarcini**
1							
...							
n							
Total							

Strategia de evaluare	**Procentul ponderal comparativ**	**Criterii de evaluare**
Autotestare I		...
...		...
Autotestare n		...
Test de evaluare a cunoștințelor		...
Certificare IIS/VET -> Autotest I + ...+ Autotest n + Test de evaluare a cunoștințelor		
Certificare pentru IMM-uri/autoevaluare -> Test de autoevaluare I + ...+ Test de autoevaluare n + Test de evaluare a cunoștințelor		
Micromodule, micro-secțiuni -> Test de autoevaluare I (opțional), Test de autoevaluare n (opțional)		

Material de studiu (Nume, Prenume. (Anul, luna, ziua). Titlul articolului. Titlul revistei/jurnalului/jurnalului, numărul volumului (numărul numărului), numărul paginilor întregului articol, editorul, URL).
Lectură obligatorie
...
Lectură recomandată
...

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau