Europski diplomski program iz upravljanja kibernetičkom sigurnošću i suverenitetom podataka Digital4Security

Kristina Ferara Blašković, Profil Klett
Tomislav Slaviček-Car, UNIRI

https://www.digital4security.eu

Co-funded by the European Union

Digital4Security is a pioneering pan-European Master's programme in cybersecurity management and data sovereignty.

Our mission?

To reskill and upskill graduates, professionals, managers and business leaders to become "cyber confident", equipped to protect and empower European SMEs in the face of global cyber threats.

Discover more!

SCAN HERE

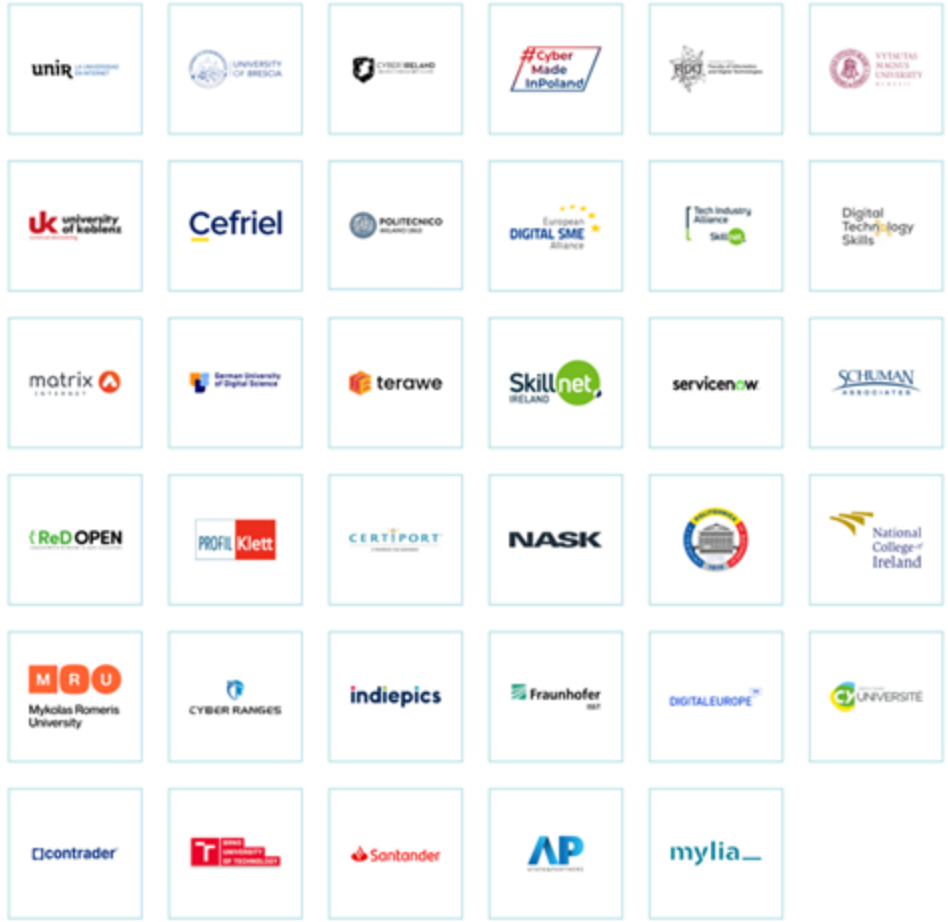
A groundbreaking European Master's

Digital4Security.eu

admin@digital4security.eu

Co-funded by the European Union

Partneri



Koordinator: POLITEHNICA B.

Akademski partneri: POLITEHNICA B., POLIMI, UNIBS, UDS, UNI KO, BUT, MTU, MRU, UNIRI, VMU, UNIR, NCI, CY CERGY PARIS

Komercijalni partneri: SA, Ataya, CEFRIEL, CMIP, Contrader, DTSL, indiepics, MATRIX, PROFIL KLETT, ServiceNow, SKILLNET, IT@CORK, ADECCO TRAINING, ADECCO GROUP, ADECCO ITALIA, DIGITAL SME, DIGITALEUROPE, NASK, TERAWE, BANCO SANTANDER, CYBER RANGES, RED OPEN S.R.L.

Pridruženi partneri: FHG, Pearson Benelux, AGORIA ASBL

Co-funded by the European Union

Europski diplomski studij za napredne digitalne vještine

Projekt **DIGITAL4Security** odgovara na hitnu potrebu za stručnjacima iz područja kibernetičke sigurnosti unutar europskih malih i srednjih poduzeća (MSP) i drugih organizacija, s ciljem zaštite industrija od kibernetičkih napada i očuvanja gospodarske prosperiteta. Glavni ciljevi programa uključuju:

- **Unapređenje i prekvalifikacija:** Poboljšati vještine diplomiranih studenata, stručnjaka i poslovnih lidera za jačanje kibernetičke sigurnosne infrastrukture.
- **Premošćivanje jaza u vještinama:** Osposobiti studente iz različitih sektora, s naglaskom na osobe koje rade sa pametnim tehnologijama i upravljanjem visokovrijednim informacijama.
- **Fleksibilni obrazovni putevi:** Pružiti prilagođene edukacijske programe koji kombiniraju tehnički i menadžerski sadržaj kako bi zadovoljili različite potrebe industrije.
- **Suradnja s industrijom:** Osigurati relevantnost prema zahtjevima tržišta kroz kontinuiranu i blisku suradnju s europskim tvrtkama i MSP-ovima u dizajnu i provedbi programa.
- **Dugoročna konkurentnost:** Doprinijeti gospodarskom rastu Europe usklađivanjem s Europskim okvirom za vještine kibernetičke sigurnosti (ECSF) i ciljevima programa DIGITAL Europe.
- **Prvenstveno online pristup:** Maksimizirati online sadržaje kako bi se omogućio fleksibilan i inkluzivan pristup vrhunskom obrazovanju iz kibernetičke sigurnosti, bez obzira na lokaciju ili osobne okolnosti.
- **Pan-europska stručnost:** Iskoristiti online suradnju kako bi studenti imali pristup vrhunskim stručnjacima iz vodećih institucija diljem Europe, pružajući raznovrsnije i suvremenije iskustvo učenja nego što to lokalna sveučilišta mogu sama ponuditi.

Co-funded by the European Union

Analiza potreba za vještinama

Akademske i industrijske institucije unutar konzorcija provele su opsežan pregled svih **12 ECSF profila**, fokusirajući se na znanja i vještine povezane sa svakom ulogom. Konzorcij je zajednički prioritetizirao ključna područja znanja i vještina za svaki profil kako bi identificirao najvažnije kompetencije potrebne industriji.

Kako bi se te spoznaje potvrdile i prikupile dodatne informacije, dizajnirana je i distribuirana **anketa** među partnerima konzorcija.

- distribucija se odvijala ciljano i otvoreno, kako bi se osigurao što širi odaziv iz industrije
- cilj ankete bio je potvrditi relevantnost vještina usklađenih s ECSF-om te osigurati razvoj diplomskog programa koji odgovara na aktualne i buduće potrebe radne snage

Podaci prikupljeni iz unutarnje ECSF analize i vanjske ankete konsolidirani su i analizirani.

Istovremeno je provedena detaljna revizija postojećih akademskih modula kako bi se **usporedila postojeća ponuda** s prioritetnim područjima znanja i vještina proizašlim iz unutarnjih i vanjskih analiza.

Rezultati analize portreba izravno su utjecali na dizajn obrazovnih proizvoda DIGITAL4Security, uključujući mikro-kvalifikacije (micro-credentials) i strukturu diplomskog programa.

Co-funded by the European Union

Cybersecurity Skills by Priority								
Role	ECSF Total	Total	New	Priority 5	Priority 4	Priority 3	Priority 2	Priority 1
CISO	14	22	8	7	12	3	0	0
Penetration Tester	11	21	10	3	14	4	0	0
Cyber Incident Responder	6	9	3	4	4	0	1	0
Cyber Legal Policy & Compliance Officer	8	8	0	4	3	1	0	0
Cyber Threat Intelligence Specialist	10	27	17	7	13	2	4	1
Cybersecurity Architect	10	21	11	5	15	1	0	0
Cybersecurity Auditor	7	15	8	5	8	2	0	0
Cybersecurity Educator	10	10	0	0	7	2	1	0
Cybersecurity Researcher	7	12	5	1	4	2	5	0
Digital Forensics Investigator	5	12	7	2	3	4	2	1
Cybersecurity Implementor	7	11	4	1	10	0	0	0
Cybersecurity Risk Manager	5	5	0	2	1	1	1	0

Professional Skills	Score	Transversal Skills	Score
AI	64	Communications	39
Law/Legal, Policy, Ethics	54	Leadership/Management Skills	11
Risk	46	Project Management	5
Threat Management/Analysis	43	Stakeholder Management	2
Business / Business Process	42	Analytical Skills	2
Incident Management	22	Change Management	2
Intelligence Analysis	20	Adaptability	2
Cloud	13	Problem Solving	2
Compliance	10	Decision Making	1
Forensics	9	Critical Thinking	1
Governance	7	Report Writing	1
Privacy / Data Privacy	6	Mentoring/Tutoring	1
Testing	6	Methodical Working	1
Audit	4		
Blockchain	3		
Automation	3		
Geopolitical	2		

Knowledge Areas by Priority								
Role	ECSF Total	Total	New	Priority 5	Priority 4	Priority 3	Priority 2	Priority 1
CISO	11	16	5	4	10	0	0	2
Penetration Tester	12	17	5	7	8	1	1	0
Cyber Incident Responder	15	22	7	5	11	2	0	4
Cyber Legal Policy & Compliance Officer	5	6	1	3	3	0	0	0
Cyber Threat Intelligence Specialist	13	32	19	8	3	11	2	8
Cybersecurity Architect	15	15	0	4	6	2	3	0
Cybersecurity Auditor	6	8	2	3	5	0	0	0
Cybersecurity Educator	8	14	6	1	3	2	4	4
Cybersecurity Researcher	5	8	3	3	1	1	3	0
Digital Forensics Investigator	13	22	9	3	7	1	2	9
Cybersecurity Implementor	11	18	7	7	11	0	0	0
Cybersecurity Risk Manager	10	11	1	4	3	2	0	1

6 odabranih profila

- CISO
- Cybersecurity Auditor
- Cyber Legal Policy & Compliance Officer
- Cybersecurity Risk Manager
- Cyber Threat Intelligence Specialist
- Cybersecurity Educator

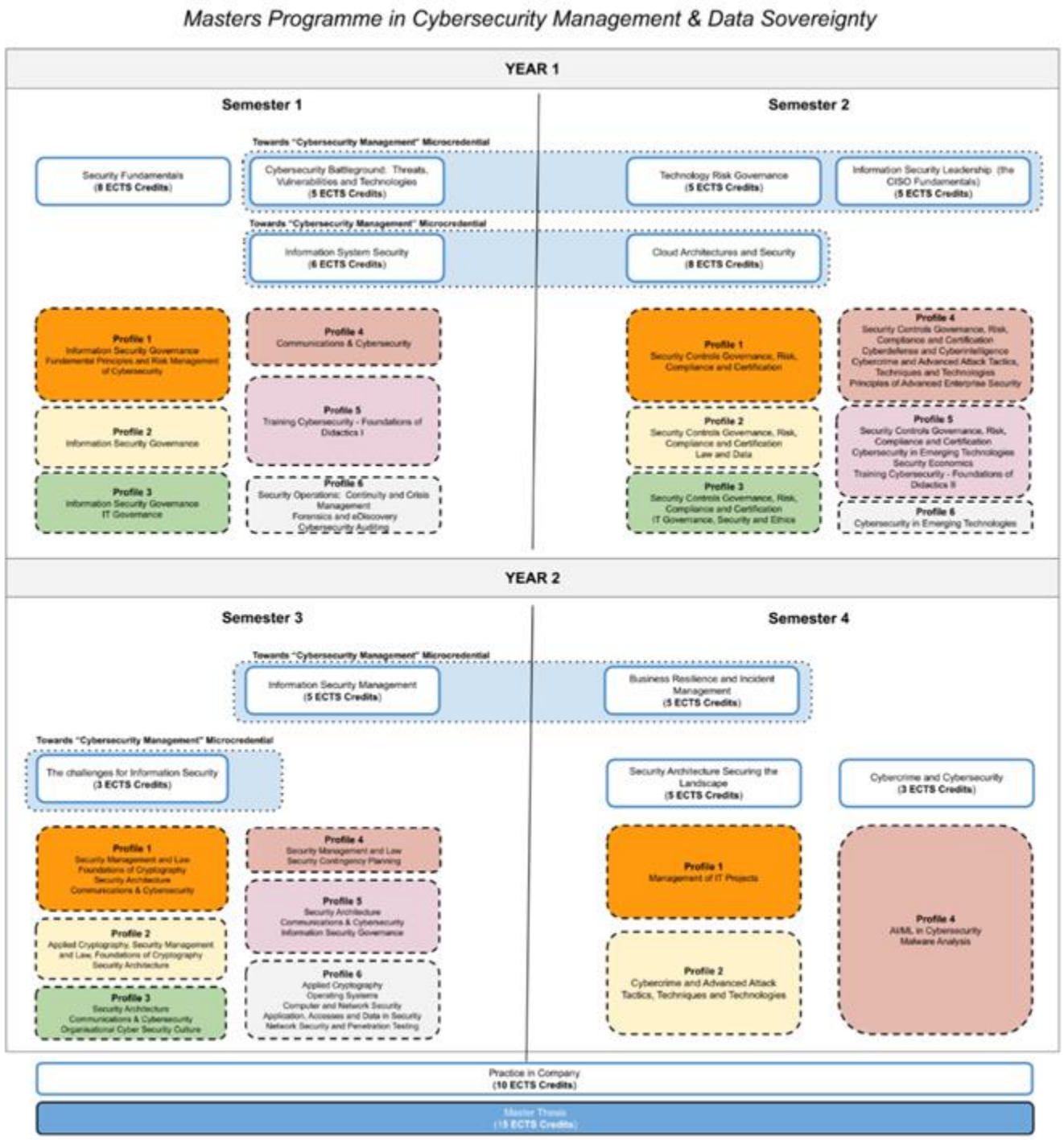
Co-funded by the European Union

I faza – Razvoj kurikuluma za online diplomski studiji od 120 ECTS-a

- 120 ECTS bodova (full-time 2 godine, part – time 3 godine)
- 24 modula – usmjeravanje prema profilima putem izbornih predmeta
- Nastavni plan i program razvili su akademski partneri uz podršku industrijskih partnera

Izazovi:

- Velik broj partnera/država - različiti propisi (nemogućnost izvođenja onlije diplomskih programa, neprihvaćanje Europskog prisutpa akreditaciji
- Trajanje D4S u skladu s prijavom projekta – u neskladu s potrebama industrije
- Akreditacija (Europski pristup akreditaciji)



Co-funded by the European Union

Faza II - prilagodba tržištu rada

Tri različita oblika izvođenja programa:

I. **online diplomski** s 60 ECTS – planirani početak veljača 2026. g
II. **hibridni diplomski** s 120 ECTS – planirani početak Listopad 2025. G (akreditacija u tijeku) – početak upisa lipanj/srpanj 2025.
III. **mikro-kvalifikacije** – planirani početak Rujan/Listopad 2025 g.

+ kratki tečajevi, industrijski certifikati....

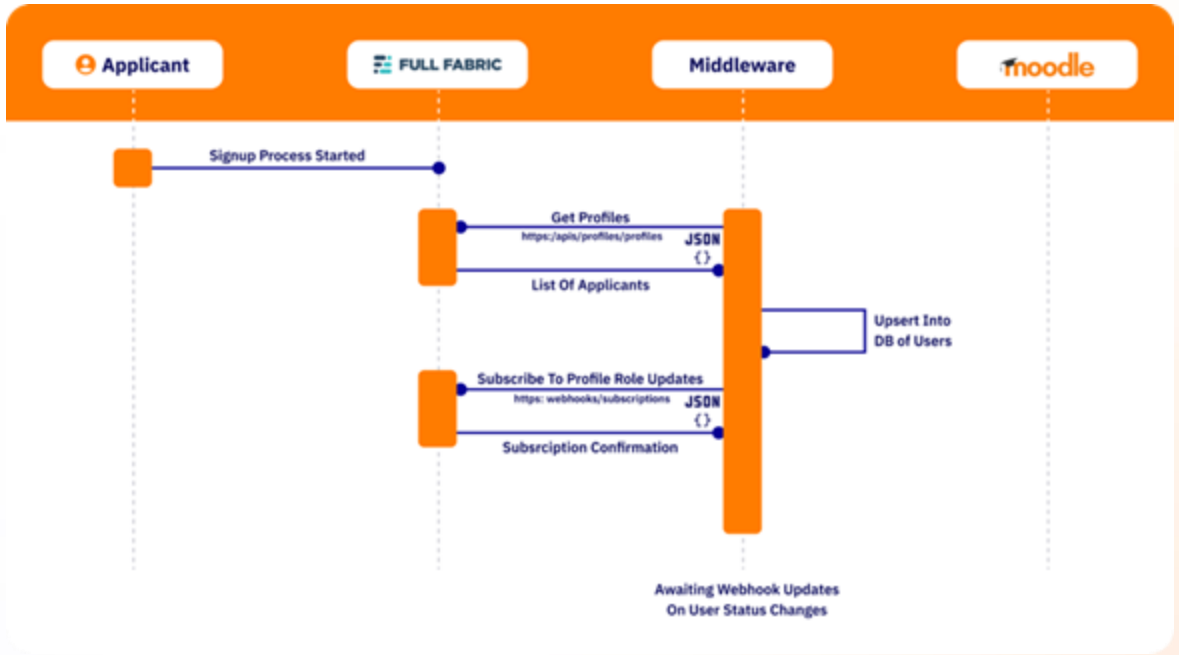
Co-funded by
the European Union

Digitalna obrazovna platforma - Moodle

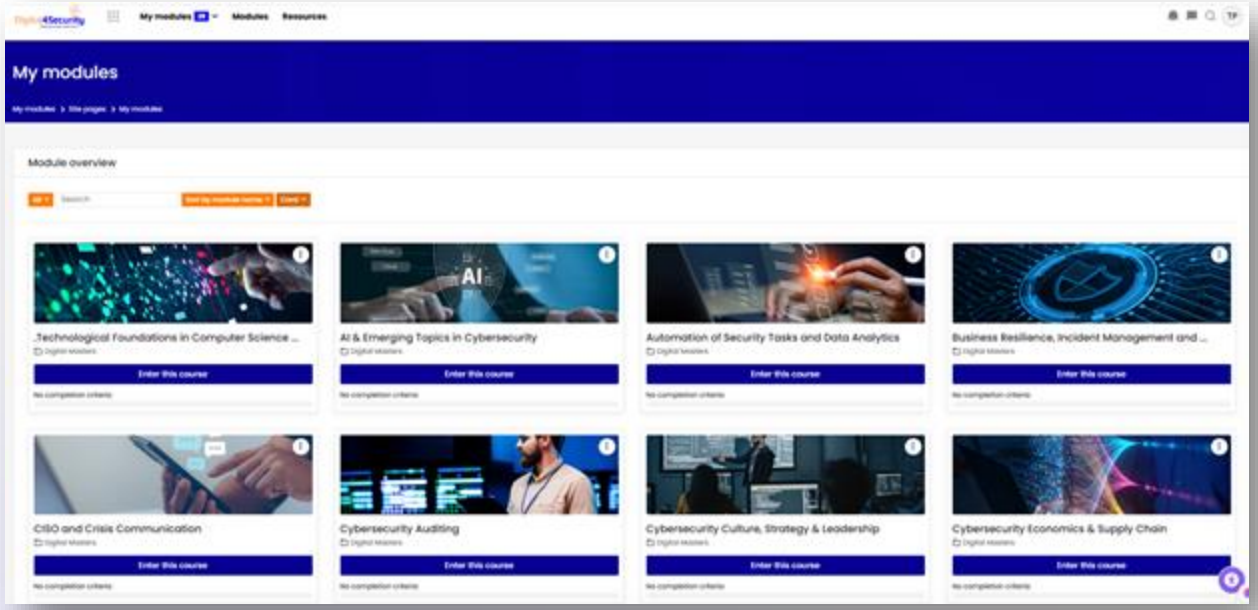
Specijalizirana i centralizirana **digitalna obrazovna platforma** uspostavljena je za potrebe online izvođenja diplomskog programa, omogućujući suradnju među visokim učilištima, pružateljima edukacija, istraživačkim institucijama i industrijskim partnerima diljem Europe.

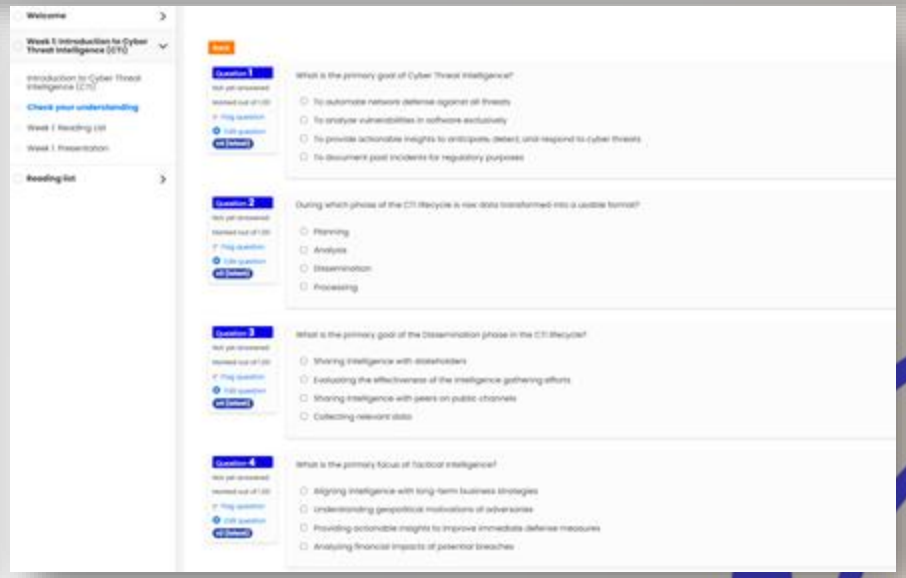
Implementiran je **Moodle** analitički sustav koji trenutno prikuplja podatke kako bi se definirali odgovarajući modeli analitike.

U okviru Moodle sustava kreiran je niz modula, usklađenih s dogovorenim okvirom koji osigurava interaktivno i pristupačno iskustvo učenja.



Co-funded by
the European Union

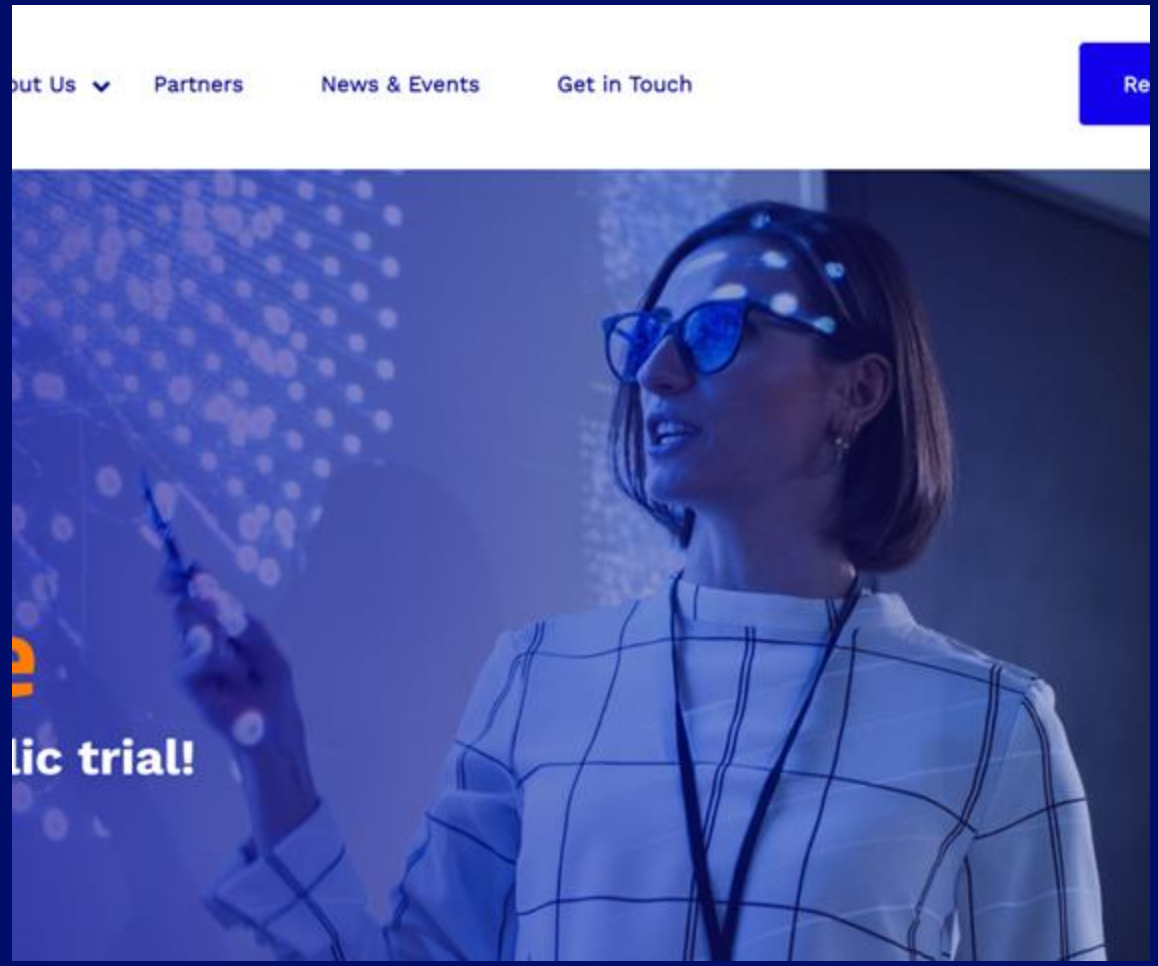




Co-funded by the European Union

Digital4Security pilotiranje

- između ožujka i travnja 2025. godine s ciljem:
  - testiranja sadržaja modula za ciljane skupine diplomskog studija
  - testiranja funkcionalnosti D4S digitalne platforme iz perspektive korisnika
- 8 sudionika u kratkom programu i 23 sudionika u dugom programu, koji je još uvijek u tijeku



Co-funded by the European Union

Vidljivost D4S

Web stranica

Društvene mreže

Publikacije i stvaranje sadržaja (Newsletteri, članci)

Događaji – organizacija raznih događaja iz područja kibernetičke sigurnosti i digitalnih vještina na europskoj razini./Uspostavljena je suradnja s donositeljima politika, predstavnicima industrije i akademskom zajednicom radi maksimiziranja vidljivosti projekta.

Suradnja s relevantnim inicijativama EU

Utjecaj i doprinos politici:

- Pruženi uvidi i preporuke usklađene s politikama EU-a o digitalnim vještinama i kibernetičkoj sigurnosti.
- Doprinos raspravama o nedostatku vještina u kibernetičkoj sigurnosti i razvoju radne snage.

Co-funded by the European Union

Digital4Security konzorcijski sastanak u Dubrovniku

- Konzorcijski sastanak održan 28.–29. travnja u Dubrovniku
- Fokus: evaluacija projekta i planiranje sljedećih koraka
- Rasprava o formatima studija i akreditaciji u EU
- Predstavljena Digital4Security platforma
- Izvješća o napretku WP1–WP6 i tehnička evaluacija

Co-funded by the European Union

Dizajn mikro-kvalifikacija za integraciju u oba magistarska programa

- Dizajnirane su složive mikro-kvalifikacije koje se integriraju u magistarski program, s početkom izvođenja u rujnu i siječnju.
- Industrijski partneri uključeni su u kreiranje sadržaja i dizajn, što je utjecalo na ažuriranja modula.
- Razvijen je „Predložak za procjenu prikladnosti i kvalitete mikro-kvalifikacija“ kako bi se osigurala usklađenost s potrebama industrije.

Co-funded by the European Union

Mikro-kvalifikacije (rujan/siječanj)

- Cybersecurity Law
- Secure data handling
- Risk Management of Cyber-Physical Systems
- Cybersecurity in Industry - Security of OT and Cyber-Physical Systems
- Law, Compliance, Governance, Policy, and Ethics
- Cybersecurity Teaching
- Cyber Range Scenario Design
- DORA Compliance and ICT Risk Management
- Operational Resilience and Supply Chain Risk under DORA
- Communication Design for Cybersecurity
- Cybersecurity Culture and Landscape
- Cybersecurity Strategy and Leadership
- CISO and Crisis Communication

Pregled modula - kolegija diplomskog studija

Co-funded by the European Union

Ataya & Partners (Belgium)

Cybersecurity Auditing

Ishodi učenja:

- Upoznavanje s revizijskim aktivnostima kao dijelom procesa osiguranja kvalitete
- Vještine za planiranje, razvoj i provođenje sveobuhvatnih zadataka revizije kibernetičke sigurnosti
- Izrada revizijskih planova prilagođenih potrebama dionika i poslovnim zahtjevima
- Razvoj godišnjih revizijskih programa temeljenih na procjeni rizika i revizijskom okviru

Co-funded by the European Union

BUT (Brno University of Technology, Czech Republic)

Cybersecurity Education & Training Delivery I

Ishodi učenja:

- Kritički vrednovati metodologije i materijale za obrazovanje iz područja kibernetičke sigurnosti
- Procijeniti potrebe za planiranje i provedbu treninga iz kibernetičke sigurnosti
- Izraditi nove nastavne materijale koji odražavaju nove trendove u području kibernetičke sigurnosti
- Koristiti suvremene tehnologije poput Cyber Ranges, Gita i GitHuba za isporuku sadržaja

Co-funded by the European Union

BUT (Brno University of Technology, Czech Republic)

Cybersecurity Law & Data Sovereignty

Ishodi učenja:

- Razumjeti i primijeniti mjere kibernetičke sigurnosti u okviru regulatornih okvira EU-a
- Procijeniti pravne okvire kibernetičke sigurnosti i instrumente međunarodne usklađenosti
- Primijeniti pravne alate za incidente kibernetičke sigurnosti i suradnju s timovima za odgovor
- Razumjeti propise o suverenitetu podataka i postupanje s elektroničkim dokazima

Co-funded by the European Union

CEFRIEL (Italy)

Cybersecurity in Industry - Security of OT and Cyber-Physical Systems

Ishodi učenja:

- Vrednovati načela i izazove sigurnosti operativne tehnologije (OT) u odnosu na informatičku sigurnost (IT)
- Kritički procijeniti prijetnje u OT okruženju i analizirati specifične taktike napada
- Ispitati studije slučaja kibernetičkih incidenata u OT okruženjima
- Razviti sveobuhvatne modele rizika i sigurnosne mjere za OT okruženja

Co-funded by the European Union

CY CERGY (CY Cergy Paris University, France)

Security Operations

Ishodi učenja:

- Razumjeti ulogu i rad Centra za sigurnosne operacije (SOC) i njegovih analitičara
- Koristiti alate za nadzor mreže radi otkrivanja i odgovora na sigurnosne incidente
- Analizirati i interpretirati sigurnosne podatke radi prepoznavanja potencijalnih prijetnji
- Primijeniti kriptografske metode za zaštitu podataka

Co-funded by the European Union

MRU (Mykolas Romeris University, Lithuania)

Cybersecurity Economics & Supply Chain

Ishodi učenja:

- Razumjeti ekonomske implikacije kibernetičke sigurnosti unutar organizacija
- Procijeniti izravne i neizravne troškove kibernetičkih incidenata pomoću studija slučaja
- Analizirati ekonomski utjecaj kibernetičkih prijetnji na financijsku stabilnost i reputaciju
- Strateški planirati ulaganja u kibernetičku sigurnost i raspodjelu proračuna

Co-funded by the European Union

MTU (Munster Technological University, Ireland)

Enterprise Architecture, Infrastructure Design and Cloud Computing

Ishodi učenja:

- Vrednovati sigurnosnu arhitekturu poduzeća i kontrole kibernetičke sigurnosti u kontekstu višeslojne obrane (Defense in Depth)
- Procijeniti komponente za zaštitu računalnih sustava poput vatrozida (Firewall), VPN-a i sustava za otkrivanje i sprječavanje upada (NIDRS)
- Procijeniti primjenjivost arhitektonskih okvira za kibernetičku sigurnost
- Ispitati temeljna načela sigurnosti u cloud-u i razlikovati ih od tradicionalne IT sigurnosti

Co-funded by the European Union

NCI (National College of Ireland, Ireland)

Business Resilience, Incident Management and Threat Response

Ishodi učenja:

- Evaluirati planove za odgovor na incidente i njihovu usklađenost s industrijskim standardima
- Kritički procijeniti aktivnosti odgovora od početne kompromitacije do oporavka
- Usporediti metode za procjenu sposobnosti organizacije za odgovor na incidente
- Vrednovati mehanizme za korištenje sposobnosti „plavog tima” i „crvenog tima” tijekom incidenata

Co-funded by the European Union

NCI (National College of Ireland, Ireland)

Digital Forensics, Chain of Custody and eDiscovery

Ishodi učenja:

- Pokazati kritičku osviještenost o zakonima i zahtjevima usklađenosti u području digitalne forenzike
- Provoditi forenzične istrage operacijskih sustava, mobilnih uređaja i mreža
- Usporediti, vrednovati i koristiti forenzične alate za analizu digitalnih uređaja
- Provoditi eDiscovery postupke na različitim platformama

Co-funded by the European Union

POLIMI (Politecnico di Milano, Italy)

Risk Management of Cyber-Physical Systems

Ishodi učenja:

- Identificirati i kategorizirati tehnološke rizike operativnih i digitalnih tehnologija
- Opisati i odrediti prioritete značajki otpornosti i rizika u socio-kibernetičko-fizičkim sustavima
- Odabrati i primijeniti odgovarajuće pristupe i metode procjene rizika
- Ispitati i procijeniti model upravljanja tehnološkim rizicima u organizaciji

Co-funded by the European Union

UDS (German University of Digital Science, Germany)

A.I. & Emerging Topics in CyberSecurity

Ishodi učenja:

- Steći temeljna znanja iz podatkovne znanosti i umjetne inteligencije relevantna za kibernetičku sigurnost
- Osmisliti i razviti rješenja temeljena na umjetnoj inteligenciji za stvarne izazove u području kibernetičke sigurnosti
- Kritički vrednovati prednosti i ograničenja primjene umjetne inteligencije u kibernetičkoj obrani
- Procijeniti etičke i regulatorne implikacije odgovorne primjene umjetne inteligencije u kibernetičkoj sigurnosti

Co-funded by the European Union

UNI KO (University of Koblenz, Germany)

Dissertation / Internship

Ishodi učenja:

- Steći znanje o istraživanjima u području specijalizacije kandidata
- Razumijevanje akademske teorije i priprema za istraživački rad
- Sposobnost odabira odgovarajućih istraživačkih metoda i tehnika
- Analizirati zahtjeve poslodavca i jasno izraziti vlastite vještine i iskustvo (stručna praksa)

Co-funded by the European Union

UNI KO (University of Koblenz, Germany)

Research Methods

Ishodi učenja:

- Poznavati različite istraživačke pristupe i metodologije u području kibernetičke sigurnosti
- Osmisliti istraživačke prijedloge primjenom relevantnih strategija za prikupljanje i testiranje podataka
- Primijeniti metode vrednovanja kvalitativnih i kvantitativnih podataka
- Provoditi odgovarajuća istraživanja uz osiguranje etičke metodologije

Co-funded by the European Union

UNIBS (University of Brescia, Italy)

Law, Compliance, Governance, Policy, and Ethics

Ishodi učenja:

- Analizirati i kritički vrednovati pravne okvire i etičke standarde u području kibernetičke sigurnosti
- Tumačiti i primijeniti zakonske zahtjeve za zaštitu informacijskih sredstava
- Izraditi i procijeniti politike koje obuhvaćaju etičke, pravne i praktične aspekte kibernetičke sigurnosti
- Integrirati i promicati etička razmatranja u donošenju odluka na razini cijele organizacije

Co-funded by the European Union

UNIR (Universidad Internacional de La Rioja, Spain)

Ethical Hacking & Penetration Testing

Ishodi učenja:

- Poznavati osnovna načela i važnost etičkog hakiranja i revizije sustava
- Analizirati i upravljati metodologijama i tehnikama koje se koriste u etičkom hakiranju
- Prepoznati alate koji se koriste za revizije u etičkom hakiranju i tumačiti njihove rezultate
- Razviti vještine za prepoznavanje ranjivosti i njihovo otklanjanje u računalnim sustavima

Co-funded by the European Union

UNIR (Universidad Internacional de La Rioja, Spain)

Malware Analysis

Ishodi učenja:

- Poznavati povijest razvoja zlonamjernog softvera, relevantne propise i ključne pojmove
- Razumjeti proces analize zlonamjernog softvera i metode njegove klasifikacije
- Prepoznati alate za analizu zlonamjernog softvera i tumačiti njihove rezultate
- Analizirati strukturu i funkcionalnost zlonamjernog softvera raščlanjivanjem koda i prepoznavanjem ponašanja

Co-funded by the European Union

UNIRI (University of Rijeka, Croatia)

Automation of Security Tasks and Data Analytics

Ishodi učenja:

- Koristiti Python za provedbu napredne automatizacije zadataka u području kibernetičke sigurnosti
- Osmisliti i implementirati automatizirane procese za otkrivanje prijetnji i prikupljanje obavještajnih podataka
- Koristiti Python za obradu, analizu i vizualizaciju podataka iz područja kibernetičke sigurnosti
- Primijeniti etičke i pravne standarde u automatizaciji zadataka vezanih uz kibernetičku sigurnost

Co-funded by the European Union

UNIRI (University of Rijeka, Croatia)

Machine and Deep Learning in Cybersecurity

Ishodi učenja:

- Usporediti prednosti i nedostatke algoritama strojnog učenja za potrebe kibernetičke sigurnosti
- Analizirati i primijeniti odgovarajuće metode strojnog učenja za otkrivanje anomalija i zlonamjernog softvera
- Analizirati i odabrati metode dubokog učenja za zadatke u području kibernetičke sigurnosti
- Osmisliti i primijeniti modele strojnog i dubokog učenja za samostalno definirane probleme iz područja kibernetičke sigurnosti

Co-funded by the European Union

UPB (University Politehnica of Bucharest, Romania)

Technological Foundations for CS & Security Controls

Ishodi učenja:

- Opisati hardversko-softverski sloj u suvremenim računalnim sustavima
- Definirati i objasniti temeljne sigurnosne pojmove
- Koristiti aplikacije za konfiguriranje, osiguravanje i otklanjanje poteškoća u radu s podacima, aplikacijama i mrežom
- Ispitati, procijeniti i revidirati sigurnosna svojstva: povjerljivost, cjelovitost, pouzdanost

Co-funded by the European Union

UPB (University Politehnica of Bucharest, Romania)

Cybersecurity Education & Training Delivery II

Ishodi učenja:

- Osmisliti praktične vježbe iz kibernetičke sigurnosti kao temelj za učenje i vrednovanje
- Opisati uobičajene obrasce napada i obrane u području kibernetičke sigurnosti
- Razviti, primijeniti i vrednovati praktične vježbe i ranjive virtualne okoline (vulnerable boxes)
- Osmisliti i postaviti okruženja za cyber range i natjecanja tipa CTF (Capture The Flag)

Co-funded by the European Union

UPB (University Politehnica of Bucharest, Romania)

Threat Intelligence

Ishodi učenja:

- Prepoznati različite vrste kibernetičkih prijetnji i primijeniti analitičke tehnike
- Prikupljati podatke o prijetnjama iz otvorenih i vlasničkih izvora
- Uključiti obavještajne podatke o prijetnjama u automatizirane procese odgovora na incidente
- Koristiti specijalizirane platforme i alate za analizu podataka o prijetnjama i dijeljenje informacija

Co-funded by the European Union

VMU (Vytautas Magnus University, Lithuania)

Cybersecurity Culture, Strategy & Leadership

Ishodi učenja:

- Razumijevanje uloge CISO-a (glavnog direktora za informacijsku sigurnost) te praksi kulture i upravljanja za postizanje ciljeva zaštite
- Steći vještine za uspješno obavljanje različitih CISO zadataka u domenama planiranja, izgradnje, provedbe i nadzora
- Sposobnost izgradnje funkcionalne CISO organizacije usklađene s poslovnim ciljevima

Co-funded by the European Union

VMU (Vytautas Magnus University, Lithuania)

CISO and Crisis Communication

Ishodi učenja:

- Upoznati se s glavnim komunikacijskim zahtjevima za vodstvo u području kibernetičke sigurnosti
- Steći vještine za uspješno planiranje, razvoj i provođenje komunikacijskih aktivnosti
- Izrada komunikacijskih planova koji uključuju dizajn, vremenski raspored, identifikaciju ciljne publike i procjenu učinka

Co-funded by the European Union

Digital4Security
Shaping Europe's cyber future

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

Posted on March 5, 2024

Digital4Security was officially launched in October 2023 as a pioneering pan-European master's programme, designed to tackle the increasing challenges of cybersecurity threats and data privacy issues across various industries. With funding from the European Union, this four-year, €20 million project has attracted the support of a Consortium of 35 partners across 14 countries. The launch event, hosted by Politecnica University of Bucharest, represented a crucial step forward in combating the escalating digital threats. This industry-led programme will equip European SMEs and companies with thorough knowledge in cybersecurity management, regulatory compliance, and technical expertise.

Zaključak

- Digital4Security je inovativni europski diplomski program koji osposobljava **stručnjake za kibernetičku sigurnost** spremne odgovoriti na stvarne potrebe industrije.
- Program nudi fleksibilne obrazovne puteve, uključujući **mikro-kvalifikacije, online, te hibridni pristup**, što omogućava brzu prilagodbu i prekvalifikaciju u dinamičnom sektoru.
- Suradnja s vodećim **akademskim i industrijskim partnerima** jamči relevantnost i kvalitetu sadržaja te povezanost sa stvarnim tržištem rada.
- Cilj je dugoročno jačanje konkurentnosti europske industrije kroz osposobljavanje visoko kvalificiranih stručnjaka.

Co-funded by the European Union

Digital4Security is a pioneering pan-European Master's programme in cybersecurity management and data sovereignty.

Our mission?

To reskill and upskill graduates, professionals, managers and business leaders to become "cyber confident", equipped to protect and empower European SMEs in the face of global cyber threats.

Discover more!

SCAN HERE

A groundbreaking European Master's

Digital4Security.eu

admin@digital4security.eu

Digital4Security
Shaping Europe's cyber future

Co-funded by the European Union

Digital4Security
Shaping Europe's cyber future

Hvala na pažnji!

Co-funded by
the European Union