SĂ NE PROTEJĂM MAI BINE VIITORUL! CYBERSECURITY AVANSAT

CUPRINS:

Titlul proiectului

SĂ NE PROTEJĂM MAI BINE VIITORUL! CYBERSECURITY AVANSAT
Cod SMIS: 133334

Obiectivul general al proiectului

Crearea de competențe durabile și locuri de muncă în unul din domeniile prioritare identificate în SNC - **Tehnologia informației și comunicațiilor** (TIC), pentru **330 de studenți**, în **securitate cibernetică** sau în alte ocupații/meserii care necesită **competențe de securitate cibernetică**, prin intermediul dezvoltării și implementării unui **centru de securitate cibernetică**.

UNIUNEA EUROPEANA

Instrumente Structurale 2014-2020

Partenerii proiectului

1. EURO-TESTING SOFTWARE SOLUTIONS SRL

Răcuciu Silviu - Claudiu

(Manager general)

2. Universitatea Româno-Americană

Tabușcă Alexandru

(Coordonator proiect)

3. Academia Navală ”Mircea cel Bătrân”

Cdor.conf.univ.dr.ing. Toma Alecu

(Coordonator proiect)

Finanţarea proiectului

4.660.699,97 lei

1. Selecţia grupului ţintă

Procesul de selecție a grupului ţintă va fi centrat pe recrutarea studenţilor proprii (din ANMB și URA) şi ulterior poate fi extins către alte universităţi de profil cu care vor fi încheiate parteneriate. Prioritate în activitatea de recrutare ca grup ţintă o vor avea studenții ANMB/URA care îndeplinesc criteriile de încadrare în grupul țintă.

Grupul ţintă va fi compus din:

- **100 studenţi de la Universitatea Româno-Americană (P1)**
- **230 studenţi de la Academia Navală ”Mircea cel Bătrân” (P2)**

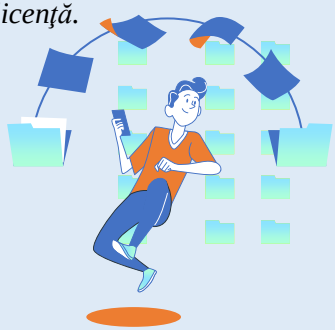
din care:

- **5% vor fi de etnie rromă (16 studenți);**
- **10% vor proveni din mediul rural (33 studenți);**
- **minim 30% vor fi femei (minim 99 femei).**

Total GŢ = 330 studenţi în practică, din care 16 de etnie rromă şi 33 din mediul rural.

a) Documente personale care se depun personal, in copie la dosar:

- *Copie după cartea de identitate;*
- *Copie certificat de naştere, certificat de căsătorie, hotărâre de divorţ (dacă este cazul);*
- *Curriculum Vitae în format Europass însoţit de copii după documentele de studii;*
- *Formular de înregistrare grup țintă (tipizat);*
- *Copie diplomă ultimele studii absolvite - bacalaureat, licenţă.*



b) Documente tipizate (vor fi completate la sediul ANMB):

- *Acord de utilizare a datelor personale (tipizat);*
- *Angajament de respectare a cerinţelor proiectului şi de disponibilitate în privinţa deschiderii unei afaceri (tipizat);*
- *Declaraţia candidatului că nu este angajat al liderului de proiect sau partenerilor acestuia (tipizat);*

- *Declarația candidatului că nu beneficiază de alte proiecte finanțate prin POCU pentru AXA 6 obiectivul 6.13 (pentru evitarea dublei finanțări).*

Documentele tipizate vor fi puse la dispoziția studenților în perioada imediat următoare, în timpul sesiunilor de informare sau pentru accesare directă de pe pagina web a proiectului: **https://adl.anmb.ro/cybersecurity-avansat**

2. Consilierea și orientarea profesională a studenților

Consilierea şi orientarea profesională a celor 330 studenţi se va aplica **individualizat şi personalizat** şi are ca obiectiv principal **creşterea gradului de motivare a acestora pentru dezvoltarea unei cariere profesionale în domeniul IT, pentru integrarea performantă pe piaţa muncii**.

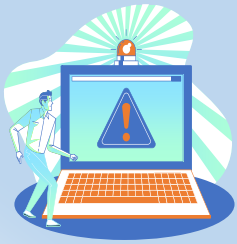
Furnizarea serviciului de consiliere şi orientare profesională pentru grupul țintă se va derula astfel:

- **etapa 1 - luna a 3-a –> luna a 6-a** (4 luni);
- **etapa 2 - luna a 12-a –> luna a 14-a** (3 luni);
- **etapa 3 - luna a 18-a –> luna a 20-a** (3 luni).

În **etapa 1** şi partial în **etapa 2** se va realiza **testarea psiho-profesională a participanţilor.**
În **etapa 2** și **etapa 3** se urmărește dezvoltarea personală şi orientarea profesională a studenţilor, după ce au efectuat deja practica, pentru a-i pregăti în tranziția către viața activă și pentru a le creşte șansa valorizării oportunităţilor de angajare.

UNIUNEA EUROPEANA

Instrumente Structurale 2014-2020



a) Consilierea individuală:

Problematica abordată în cadrul ședințelor de consiliere cuprind:

- informarea asupra procesului de consiliere și a beneficiilor posibile;
- identificarea nevoilor individuale de consiliere;
- consilierea privind posibilitățile de promovare personală;
- identificarea și clarificarea intereselor, abilităților și valorilor profesionale;
- identificarea eventualelor blocaje legate de încrederea în sine și motivație;
- dezvoltarea motivației pentru succes.

b) Consilierea de grup se va desfășura în ședințe cu durata de aproximativ 3 ore. Grupul poate fi format din **maxim 10 membri**.

Pentru tematica ședintelor de consiliere de grup se vor folosi următoarele tehnici:

- informarea asupra procesului de consiliere și asupra beneficiilor posibile;
- adaptarea la schimbarea **stilului de viață** presupus de începerea unei activități profesionale (integrare pe piața muncii) și **asumarea riscurilor calculate**;

- modalități de **prezentare la un interviu** în vederea angajării;
- **leadership, comunicare și negociere;**
- **gândirea pozitivă și orientarea spre soluții;**
- modalități de promovare personală: **CV-ul și scrisoarea de intenție**;
- autocunoaștere și dezvoltare personală: dezvoltarea **motivațiilor pentru succes, a stimei de sine și încrederii de sine**;
- managementul stresului;
- **gestionarea emoțiilor, empatia**;
- **autoafirmarea** și comportamentul **proactiv**.

3. Organizarea şi desfăşurarea practicii

a) Crearea unui centru de practică

Centru de securitate cibernetică inovativ:

Centrul va fi pus la dispoziţie pentru practica grupului țintă, dar și pentru studenţii universităţilor

cu care sunt încheiate acorduri de parteneriat în acest scop, inclusiv pe perioada sustenabilităţii proiectului, facilitând practica studenţilor şi familiarizarea cu produse performante care le cresc considerabil şansele de angajare pe piaţa securităţii cibernetice.
Mediul de practică planificat a fi dezvoltat cuprinde următoarele secțiuni majore:

➢ **Defensive:**

- *endpoint protection – Crowdstrike Falcon*
- *firewall – openSense (open-source)*
- *intrusion detection system (IDS) – Suricata (open-source)*
- *network monitoring – Zeek (open-source)*
- *threat hunting (Varianta 1 cu Splunk, Varianta 2 cu ELK)*
- *vulnerability management - Nexpose*

➢ **Ofensive:** *Metasploit + Gophish + Cobalt Strike*

➢ **Test network:** *Azure Active Directory Hybrid Lab.*

Pentru facilitarea practicii studenților vor fi folosite echipamentele și infrastructura Solicitantului, iar la fiecare din P1 și P2 se vor achiziţiona și pune la dispoziția studenților participanți **câte 50 desktopuri (2 laboratoare implementate la fiecare universitate)**.

➢ la P1 (URA) vor fi achiziționate suplimentar **două servere specializate dedicate testelor complexe în domeniul securității cibernetice**, bazate pe testarea ofensivă și defensivă legată de metode de acces biometric și eventuale metode de ocolire

neautorizată a acestora. **Ele vor fi accesibile în regim de lucru la distanță de către toți studenții implicați în practica din proiect.**

- la P2 (ANMB) vor fi achiziționate suplimentar **un laptop de deservire a sălilor de practică și o imprimantă multifuncțională**.

URA/P1 va achiziționa **licențe de Corel Photoshop, Corel Illustrator**, software vitale pentru orice profesionist în domeniul marketing, promovare sau vânzări, precum și **licențe AdobeCS**, esențiale pentru **video, design, fotografie si web, cu aplicații pentru orice, de la compoziția imaginilor și editarea fotografiilor până la designul site-urilor web, pictura digitală, 3D și realitatea augmentată, sigle, postere, reclame, ambalaje etc.**

b) Desfășurarea practicii:

Pentru studenţii Universității Româno-Americane/P1 sau ai Academiei Navale/P2 care îndeplinesc condiţiile de a fi în GŢ şi provin atât din facultatea cu profil TIC, sau după caz, din alte specializări (într-un număr redus) practica va fi derulată pe **2 paliere distincte**:

Scenariul 1 (Studenţi din facultăţi cu alt profil decât TIC – URA/P1)

- **Etapa 1** (o săptămână) - va urmări consolidarea informaţiei şi familiarizarea cu conceptele, informaţiile şi procesele care vizează planificarea, managementul, marketingul, contractarea clienților, managmentul lor, managementul resurselor umane, gestiune financiară, etc. şi va avea loc în

laboratoarele din sediul P1, cu exemple practice şi prezentarea modulelor şi aplicaţiilor utilizate la solicitant şi la alţi parteneri de practică identificaţi prin parteneriate, care pot sprijini, eficientiza şi automatiza toate aceste procese.

➢ **Etapa 2** (2 săptămâni) – se va executa la parteneri, pe componentele specifice şi utilizând în practică şi elementele învăţate în ceea ce priveşte utilizarea CorelGraphicSuite şi AdobeCS în cadrul firmei.

➢ **Etapa 3** – un proiect concret, aplicabil în cadrul firmei, cu utilizarea deprinderilor nou învăţate şi exersate.

Scenariul 2 (Studenţi din facultăţi cu profil TIC – URA/P1, ANMB/P2)

➢ **Etapa 1** (1 săptămână) - noţiuni teoretice: bazele securităţii unei reţele enterprise, dispozitive avansate de securitate, atacuri comune, tipuri de malware, instrumente de securitate, răspunsul la incidente, securitate ofensivă.

➢ **Etapa 2** (2 săptămâni) - cu acces remote la facilităţile centrului, presupune următoarea tematică:

- prezentare arhitectură reţea;
- studiu generare şi colectare loguri;
- studiu platforme threat hunting;
- studiu instrumente securitate ofensivă.

➢ **Etapa 3** - exerciţii pe baza unor scenarii similare celor identificate în practică:

- analiză breşă de securitate în urma rulării unui exploit;
- analiză breşă de securitate în urma unei campanii de phishing;
- analiză breşă de securitate în urma unei campanii red teaming.

Scenariul 3 (Studenţi din facultăţi de profil ingineresc, conex domeniului TIC – ANMB/P2)

➢ **Etapa 1** Prezentare noţiuni teoretice

Scopul acestui modul este de a introduce cursanţilor noţiuni teoretice cu privire la componentele unei reţele enterprise, topologii şi metode de securizare cât şi prezentarea dispozitivelor avansate de securizare precum IDS/IPS (intrusion detection system/ intrusion prevention system), decriptoare SSL şi honeypots-uri, pentru înţelegerea mediului de test implementat.

➢ **Etapa 2** Exploatare laborator

În acest modul fiecare cursant va avea acces la câte un endpoint din cadrul mediului de test şi vor câstiga experienţa practică în utilizarea celor două platforme de threat hunting implementate. Practicanții vor putea urmări modul de procesare al logurilor, rolul fiecărei componente din cadrul platformelor şi interacţiunea cu interfeţele pentru analişti. Cursanţii vor fi integraţi în procesul de management al vulnerabilităţilor, prin lansarea de scanări, analiza rapoartelor şi validarea vulnerabilităţilor.

➢ **Etapa 3** Exerciţii pe baza unor scenarii similare celor identificate în practică

O dată familiarizaţi cu mediul de test şi cu tool-urile din componenţa acestuia, cursanţii vor face parte, ca analişti de securitate cibernetică, din trei scenarii similare celor identificate în practică şi cu ajutorul unor playbook-uri specifice procesului de incident response, vor rezolva, lucrând în echipe, alertele asignate.

4. Evaluarea cursanților - testarea și certificarea studenților cei mai performanți în stagiile de practică

Pentru testarea cunoştinţelor asimilate pe durata cursului, participanţii vor susţine un **examen teoretic**, compus din întrebări grilă din primele două module şi un **examen practic** pe baza unui scenariu realizat în modulul trei.

Toţi elevii şi studenţii vor realiza un "**Raport de practică**".

Cursanţii care au obţinut primele **50 cele mai bune punctaje la testare** vor fi sprijiniți pentru susținerea **examenului pentru certificarea CompTIA Security+** (**certificare recunoscută la nivel internațional**, care validează abilităţile de bază necesare pentru a îndeplini funcţii de securitate de bază) pentru a facilitate continuarea unei cariere în domeniul securității IT.

La terminarea practicii toți studenţii vor primi un "**Atestat de practică**" de la partenerul de practică, din care să rezulte perioada efectuării

practicii şi calitatea activităţii desfăşurate, pentru a contribui în mod direct la creşterea angajabilităţii acestor studenţi.

5. Facilitarea angajării pe piaţa de cybersecurity sau stimularea continuării studiilor în domeniu

După finalizarea stagiului de practică, studenţii absolvenţi de practică vor fi sprijiniţi în vederea **angajării pe piaţa de cybersecurity** sau pentru **continuarea studiilor în domeniu sau participarea la alte forme de formare**. De asemenea, se include posibilitatea pentru 50 studenţi selectaţi de a susţine testele pentru certificarea CompTIA Security+ şi sprijinul pentru începerea antreprenoriatului (**înfiinţarea de microîntreprinderi proprii**) pentru un număr estimat de 40 absolvenţi de practică.

Vor fi asigurate **servicii de orientare profesională** şi activităţi care să faciliteze **ocuparea unor locuri de muncă** alternative sau **deschiderea unor afaceri în domeniul IT**, pentru un număr estimat de aproximativ **150 persoane** din cei **264 absolvenţi de practică atestaţi**, pentru a asigura atingerea indicatorilor finali propuşi în proiect.

Date de contact:

email: pocu.cyber@anmb.ro (corespondenţă grup ţintă)
website: www.anmb.ro/practica-cybersecurity
facebook: facebook.com/practica-cybersecurity/
ghişeu virtual consiliere:
http://adl.anmb.ro/cybersecurity-avansat
telefon: 0241/626200/interior 0135
adresa corespondenţă: **Academia Navală ”Mircea cel Bătrân”, strada Fulgerului nr.1, Constanţa, România**