Co-funded by the European Union

NIVEL EQF 4-5

MODULE DE FORMARE PENTRU STUDENȚII VET

CYBER AGENT 01.2025

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

Pachetul de lucru 3: Dezvoltarea resurselor de învățare CyberAgent

Rezultatul 3.2: Module de formare pentru studenții VET
Coordonator al 3.2 – TIMTAL (TR)

CONȚINUT

LISTA DE TABELE

INTRODUCERE

Schimbările rapide din domeniul științei și tehnologiei, nevoile în continuă schimbare ale indivizilor și ale societății, inovațiile și evoluțiile în teoriile și abordările de învățare și predare au afectat în mod direct rolurile așteptate de la indivizi. Această schimbare definește un individ care produce cunoștințe, le poate utiliza în mod funcțional în viață, poate rezolva probleme, gândește critic, este întreprinzător, hotărât, are abilități de comunicare, poate empatiza, contribuie la societate și cultură etc.

Viteza amețitoare adusă de era informațională aduce cu sine nevoile în continuă schimbare ale indivizilor și societăților. Inovațiile în teoriile învățării și predării schimbă radical rolurile așteptate de la indivizi. Acum, nu mai este vorba doar de a avea cunoștințe, ci și de abilități precum capacitatea de a utiliza aceste cunoștințe în mod funcțional în viață, capacitatea de a produce soluții la probleme complexe, capacitatea de a gândi critic, capacitatea de a acționa cu spirit antreprenorial, capacitatea de a comunica eficient, capacitatea de a arăta empatie și de a adăuga valoare societății. Această transformare încurajează indivizii să învețe, să se adapteze și să se perfecționeze în mod constant.

În acest context, formarea profesională suferă, de asemenea, o transformare majoră. Profesiile tradiționale sunt înlocuite de profesii noi, axate pe tehnologie și în continuă dezvoltare. Securitatea cibernetică are o importanță crucială în această schimbare. Deoarece, într-o lume în curs de digitalizare, riscurile de securitate cibernetică sunt în creștere în fiecare sector și în fiecare profesie. Securitatea cibernetică joacă un rol vital în multe domenii, de la datele personale la protecția secretelor corporative, de la securitatea infrastructurilor critice la securitatea tranzacțiilor financiare.

Importanța formării în domeniul securității cibernetice în învățământul profesional nu se limitează la competențele tehnice. Ea include și formarea de persoane care au valori etice, un înalt simț al responsabilității, sunt familiarizate cu reglementările legale și sunt deschise învățării continue. Pentru că securitatea cibernetică nu este doar o problemă tehnică, ci și o responsabilitate socială. Prin urmare, acordarea importanței necesare formării în domeniul securității cibernetice în învățământul profesional este un pas crucial pentru viitorul atât al indivizilor, cât și al societății.

Educația profesională include planificarea, cercetarea, dezvoltarea, organizarea și gestionarea coordonată, supravegherea și activitățile didactice ale tuturor serviciilor de educație profesională și tehnică, împreună cu sectoarele agriculturii, industriei și serviciilor, în cadrul integrității sistemului educațional. Scopul acestor activități educaționale este de a forma experți care să asigure continuitatea societății și personalul calificat necesar în fiecare etapă a producției, precum și de a pune accentul pe formarea profesională.

Programul de educație profesională Cyber Agent (EQF4-5) este conceput pentru a pregăti persoanele pentru viața în domeniul securității cibernetice și se bazează pe nevoile pieței muncii și pe abordarea analizei locurilor de muncă. Curriculumul Cyber Agent are ca scop furnizarea cunoștințelor, abilităților, atitudinilor și comportamentelor necesare pentru a efectua munca și tranzacțiile relevante prin lecții și realizări, în timp ce, pe de altă parte, activitățile educaționale sunt planificate într-un mod care să pregătească persoanele pentru viața profesională în conformitate cu acest cadru.

1. OBIECTIVELE PROGRAMULUI CYBERAGENT EQF NIVELUL 4-5

Nevoia de securitate cibernetică a devenit destul de importantă, în special în țările UE, precum și în întreaga lume, și a crescut rapid în ultimii ani. Odată cu evoluțiile tehnologice, riscurile și amenințările cibernetice s-au schimbat la aceeași viteză și au devenit complexe. Riscurile și amenințările cibernetice au atins un potențial care va provoca rezultate mult mai cuprinzătoare și negative decât atacurile fizice. Având în vedere că sectoare precum finanțele, comunicațiile electronice, energia, transporturile și aviația furnizează servicii într-un mediu digital securizat, asigurarea securității cibernetice naționale a devenit una dintre prioritățile principale ale țării noastre. În acest context, se urmărește diseminarea educației în domeniul securității cibernetice în cadrul educației formale și informale, precum și dezvoltarea și îmbogățirea conținutului educațional.

2. CADRUL EUROPEAN DE CALIFICARE

UE a elaborat Cadrul european al calificărilor (CEC) ca instrument de traducere pentru a facilita înțelegerea și comparabilitatea calificărilor naționale. CEC urmărește să sprijine mobilitatea transfrontalieră a cursanților și a lucrătorilor, să promoveze învățarea pe tot parcursul vieții și dezvoltarea profesională în întreaga Europă.

EQF este un cadru cu 8 niveluri, bazat pe rezultatele învățării, pentru toate tipurile de calificări, care servește ca instrument de traducere între diferite cadre naționale de calificări. Acest cadru contribuie la îmbunătățirea transparenței, comparabilității și portabilității calificărilor persoanelor și face posibilă compararea calificărilor din diferite țări și instituții.

EQF acoperă toate tipurile și toate nivelurile de calificări, iar utilizarea rezultatelor învățării clarifică ceea ce o persoană știe, înțelege și este capabilă să facă. Nivelul crește în funcție de nivelul de competență, nivelul 1 fiind cel mai scăzut și nivelul 8 cel mai ridicat. Cel mai important este faptul că EQF este strâns legat de cadrele naționale de calificări, astfel încât poate oferi o hartă cuprinzătoare a tuturor tipurilor și nivelurilor de calificări din Europa, care sunt din ce în ce mai accesibile prin intermediul bazelor de date privind calificările.

CEC a fost creat în 2008 și revizuit ulterior în 2017. Revizuirea sa a păstrat obiectivele principale de a crea transparență și încredere reciprocă în peisajul calificărilor din Europa. Statele membre s-au angajat să dezvolte în continuare CEC și să îl facă mai eficient în facilitarea înțelegerii calificărilor naționale, internaționale și din țări terțe de către angajatori, lucrători și cursanți.

Fiecare dintre cele 8 niveluri ale CEC este definit printr-un set de descriptori care indică rezultatele învățării relevante pentru calificările de la acel nivel în orice sistem de calificări. Rezultatele învățării sunt definite în termeni de:

- Cunoștințe: în contextul CEC, cunoștințele sunt descrise ca fiind teoretice și/sau factuale.
- Competențe: în contextul CEC, competențele sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive și creative) și practice (implicând dexteritate manuală și utilizarea de metode, materiale, unelte și instrumente).
- Responsabilitate și autonomie: în contextul CEC, responsabilitatea și autonomia sunt descrise ca fiind capacitatea cursantului de a aplica cunoștințele și competențele în mod autonom și cu responsabilitate.

Tabelul 1- Nivel EQF 4 - Rezultate ale învățării

Cunoștințe	Abilități	Responsabilitate și autonomie
Cunoștințe factuale și teoretice în contexte largi într-un domeniu de studiu sau învățare	Un set de abilități cognitive și practice necesare pentru a găsi soluții la probleme specifice într-un domeniu de activitate sau de învățământ.	Aplică auto-managementul în cadrul liniilor directoare ale contextelor de lucru sau de învățare care sunt în general previzibile, dar supuse schimbării; supraveghează activitatea de rutină a altora, își asumă o parte din responsabilitatea pentru evaluarea și îmbunătățirea activităților de lucru sau de învățare.

3. STUDENȚI VET ÎN DOMENIUL SECURITĂȚII CIBERNETICE (NIVEL EQF 4-5)

Angajatul în domeniul securității cibernetice (nivelul 4-5) este un profesionist calificat care lucrează în domeniul sistemelor informatice la locul de muncă, participă la studii privind activitățile preventive în domeniul securității cibernetice în cadrul proceselor de urmărire a vulnerabilităților și de sensibilizare cu privire la securitatea cibernetică, urmărește acțiunile, monitorizează funcționarea și durabilitatea sistemelor utilizate în analizele de securitate cibernetică, determină cerințele rețelelor simple, configurează rețele fizice, efectuează configurații simple legate de hardware-ul rețelei, asigură securitatea, întreținerea și îmbunătățirea rețelei, oferă asistență tehnică utilizatorilor și realizează studii de dezvoltare profesională pentru a proteja infrastructurile IT de la locul de muncă împotriva amenințărilor cibernetice în cadrul cerințelor de calitate, prin implementarea măsurilor de sănătate și siguranță la locul de muncă și de protecție a mediului.

3.1. PROGRAMUL DE FORMARE CYBER AGENT PENTRU EQF-4-5

Curriculumul VET (EQF 4-5) a fost elaborat prin adaptarea strategică a curriculumului cuprinzător al instituțiilor de învățământ superior (EQF 5-6). Procesul de adaptare a implicat concentrarea materialului pentru a se alinia la domeniul de aplicare 1 ECTS și concentrarea pe rezultatele învățării cele mai relevante pentru publicul VET și nevoile imediate ale IMM-urilor. S-a acordat prioritate subiectelor care pun accentul pe aplicarea practică și competențele fundamentale în domeniul securității cibernetice, în timp ce conceptele teoretice mai aprofundate au fost simplificate pentru a se potrivi parcursului de învățare VET.

Tabelul 2-Modulul: 1

<table>
<tr><th>Unități</th><th>Teme</th></tr>
<tr><td>Managementul proiectului</td><td>Planificarea proiectului
Definirea obiectivelor proiectului
Amenințări actuale la adresa securității cibernetice (DDoS, ransomware, malware, phishing, zero-day, atacuri IoT etc.)
Modelarea amenințărilor și analiza vulnerabilităților
Raportarea amenințărilor și incidentelor de securitate cibernetică</td></tr>
<tr><td colspan="2">Obiective de învățare:
• Cursanții vor fi capabili să definească etapele managementului de proiect și să creeze un plan de proiect de bază. (Aplicare)
• Cursanții vor articula obiective de proiect clare, măsurabile și realizabile. (Analiză)
• Cursanții vor identifica, clasifica și evalua diverse amenințări la adresa securității cibernetice. (Analiză)
• Cursanții vor dezvolta modele de amenințări și vor efectua analize de vulnerabilitate pentru scenarii specifice. (Aplicare)
• Cursanții vor pregăti rapoarte de incidente în conformitate cu protocoalele stabilite. (Aplicare)</td></tr>
<tr><td>Managementul reurselor</td><td>Instrumente și software de securitate
Utilizarea eficientă a resurselor tehnologice</td></tr>
<tr><td colspan="2">Obiective de învățare:
• Cursanții vor demonstra utilizarea eficientă a instrumentelor și software-ului de securitate cibernetică pentru detectarea și răspunsul la amenințări. (Aplicație)
• Cursanții vor optimiza resursele tehnologice pentru o securitate și eficiență sporite. (Aplicație)</td></tr>
<tr><td>Indicatori de securitate</td><td>Indicatori de securitate și tehnici de măsurare
Colectarea datelor cu SIEM
Analiza indicatorilor de securitate
Monitorizarea proiectelor și evaluarea performanței
Raportarea indicatorilor de securitate</td></tr>
<tr><td colspan="2">Obiective de învățare:
• Cursanții vor identifica și aplica metrici de securitate și tehnici de măsurare relevante. (Aplicare)
• Cursanții vor configura și utiliza instrumente SIEM pentru colectarea datelor și monitorizarea securității. (Aplicare)
• Cursanții vor interpreta și analiza metrici de securitate pentru a evalua starea de securitate. (Analiză)
• Cursanții vor monitoriza și evalua performanța proiectului utilizând metrici de securitate. (Evaluare)
• Cursanții vor compila și prezenta rapoarte bazate pe analiza metricilor de securitate. (Aplicare)</td></tr>
<tr><td>Asigurarea calității și controlul calității</td><td>Managementul calității
Standarde de calitate în domeniul securității cibernetice
Tehnici de testare și validare</td></tr>
</table>

Rezultatele învățării: • Cursanții vor implementa practici de management al calității în proiectele de securitate cibernetică. (Aplicare) • Cursanții vor identifica și aplica standardele relevante de calitate în domeniul securității cibernetice. (Aplicare) • Cursanții vor dezvolta și executa proceduri de testare și validare pentru soluții de securitate cibernetică. (Aplicare)	

Tabelul 3-Modulul: 2

Unități	**Teme**
Administrarea sistemului de operare	Sisteme de operare Relația dintre hardware și software Binarele, numărarea hexadecimală Biți și octeți Linia de comandă în sistemul de operare Comenzi Windows și Linux Client și server Windows Aplicații, procese și servicii în Windows Extensii și tipuri de fișiere Chei și valori de registru Setări panou de control Utilizatori și grupuri Structura domeniului și managerul serverului AD și GPO Interfețe Linux și kernel Procese în Linux Convenții de denumire a fișierelor și directoarelor Shell-uri Linux și sintaxa comenzilor Manipularea fișierelor și folderelor Lucrul cu comenzi de monitorizare a sistemului și pipe Gestionarea proceselor și controlul sarcinilor Gestionarea serviciilor
Obiective de învățare: • Cursanții vor compara și vor contrasta diferite sisteme de operare și arhitecturile acestora.	

• Cursanții vor explica interacțiunea dintre hardware și software într-un mediu de sistem de operare. • Cursanții vor efectua conversii binare și hexazecimale și vor înțelege reprezentarea datelor. • Cursanții vor executa comenzi fundamentale în medii Windows și Linux. • Cursanții vor gestiona aplicații, servicii și procese folosind instrumente de sistem. • Cursanții vor configura și gestiona Active Directory și GPO-uri. • Cursanții vor interacționa cu interfețele Linux și vor efectua operațiuni la nivel de kernel. • Cursanții vor gestiona servicii și procese de sistem folosind comenzi Linux.	
Administrarea sistemului de baze de date	Repozitorii și liste de surse Gestionarea unui server web Jurnale de sistem și monitorizarea jurnalelor Programarea sarcinilor în Linux Depanarea serverului și a rețelei Backup și recuperare Securizarea GRUB Firewall-uri Obiecte Active Directory și gestionarea GPO DNS și DHCP Noțiuni fundamentale PowerShell Microsoft BitLocker, AppLocker și Firewall LDAP și Kerberos NTLM Politici privind parolele și blocarea conturilor Autentificare și controlul accesului Protocolul de mesaje de control al internetului (ICMP) TCP vs UDP NetBIOS și SMB SSL și TLS Certificate Protocoale Telnet și Secure Shell (SSH) HTTP și HTTPS Protocoale ale sistemelor de poștă electronică Protocolul sistemului de nume de domeniu (DNS) FTP și RDP Încapsulare vs. decapsulare Sniffere de rețea și Wireshark TCP/UDP DHCP, DNS
Obiective de învățare: • Learners will configure repositories and manage source lists. • Learners will analyze and monitor logs for troubleshooting and security. • Learners will perform backup and recovery operations to ensure data integrity. • Learners will implement security measures including firewalls, BitLocker, and AppLocker.	
Administrarea rețelelor	Tipuri de rețele și rețele fără fir Rețele și topologii Dispozitive de identificare și acces

	Dispozitive de infrastructură și securitate Dispozitive specializate și arhitectura rețelei Rețele virtuale Adrese fizice și logice OSI și modele de rețea Încapsularea și decapsularea datelor Protocoale de rețea și numere de porturi Mijloace de transport și cabluri de rețea Tehnologii fără fir Instrumente de administrare a rețelei Cisco Packet Tracer Clasele de rețea și subrețelele Protocolul de rezolvare a adreselor (ARP) Adresarea IP statică vs. dinamică Traducerea adreselor de rețea (NAT) Comutatoare și Cisco IOS Securitatea porturilor comutatoarelor și interfețele routerelor Configurarea VLAN-urilor și DTP Rutarea între VLAN-uri Introducere în ACL-uri Depanarea rețelelor
Obiective de învățare: • Cursanții vor proiecta și gestiona rețele, înțelegând protocoalele și topologiile. • Cursanții vor configura VLAN-uri, ACL-uri și vor gestiona scheme de adresare IP. • Cursanții vor utiliza instrumente precum Wireshark și Cisco Packet Tracer pentru monitorizare și depanare.	
Administrarea cloud	Hipervizori și mașini virtuale Containere Securizarea mediilor virtuale Backup și recuperare Cloud Computing și CSP-uri Ce sunt modelele de servicii cloud Tipuri de implementare cloud Rețele virtuale Servicii de calcul AWS Amazon Elastic Compute Cloud (EC2) Instrumente de monitorizare cloud Instrumente de automatizare și orchestrare Amenințări și vulnerabilități de securitate în cloud Gestionarea identității și a accesului (IAM) Controlul accesului bazat pe roluri (RBAC) Autentificare multifactorială (MFA) Criptarea datelor în cloud Cloud privat virtual (VPC) Docker și Kubernetes
Obiective de învățare: • Cursanții vor gestiona medii virtuale folosind AWS, Docker și Kubernetes. • Cursanții vor implementa controale de securitate în cloud și gestionarea identității.	

Administrarea sistemelor ciber-fizice	Securitate și controale de acces Tipuri de autentificare TACACS+ și RADIUS Configurarea AAA Obiective de gestionare a riscurilor Criptare și decriptare Hash și tabele Rainbow Spoofing MAC și otrăvirea ARP VLAN Hopping și DHCP necorespunzător Inundație ICMP Inundație TCP și UDP Deturnarea sesiunii Spoofing DNS Apărare în profunzime (DID) și Zero Trust Zone demilitarizate (DMZ) Honeypots și întărirea rețelei Cele mai bune practici pentru o rețea sigură VPN-uri SSH și VNC Firewall-uri cu stare vs. firewall-uri fără stare Bazate pe gazdă vs. bazate pe rețea Firewall-uri hardware vs. firewall-uri software Firewall pentru aplicații web (WAF) AI în firewall-uri IDS și IPS NIDS și HIDS Snort tcpdump
Obiective de învățare: • Cursanții vor securiza rețelele folosind firewall-uri, IDS/IPS și instrumente de detectare a amenințărilor. • Cursanții vor aplica tehnici de criptare și vor gestiona protocoale de securitate.	
Consolidarea sistemului	Tehnici GenAI Generarea de coduri Gestionarea conturilor utilizatorilor și controlul accesului Detectarea anomaliilor și depanarea Rezolvarea erorilor serviciului Apache2 Gestionarea patch-urilor și actualizări Backup și recuperare automate Recuperarea fișierelor șterse cu GenAI Proceduri de securitate cibernetică Detectarea și analiza amenințărilor Răspunsul la amenințări și remedierea acestora Utilizarea AI pentru detectarea amenințărilor în timp real Validarea și testarea modelelor GenAI Configurarea și securitatea DNS Configurarea și securitatea DHCP Noțiuni fundamentale PowerShell

	Securitatea porturilor de comutare Sistemul de bază de intrare/ieșire în rețea (NetBIOS) Protocolul Server Message Block (SMB) Secure Sockets Layer (SSL) și Transport Layer Security (TLS) Certificate de securitate Protocoale pentru sisteme de poștă electronică Protocolul sistemului de nume de domeniu (DNS) Protocolul de transfer de fișiere (FTP) Protocolul desktop la distanță (RDP) Programarea sarcinilor în Linux Depanarea serverului Depanarea rețelei Backup și recuperare Securizarea GRUB Configurarea și securizarea firewall-urilor
Obiective de învățare: • Cursanții vor aplica tehnici de întărire pentru a îmbunătăți securitatea sistemului. • Cursanții vor utiliza inteligența artificială pentru detectarea amenințărilor și monitorizarea sistemului.	
Consolidarea sistemului	IR vs. SOC Evenimente și incidente Detectarea alertelor și trierea alertelor Documentare și raportare Ce sunt atacurile web? DoS și DDoS Injectare SQL și XSS Injectare de comenzi și includere de fișiere locale (LFI) Falsificare de cereri între site-uri (CSRF) Forță brută și umplere de credențiale Pass the Hash și Pass the Ticket Controlul accesului defectuos Ransomware Viruși și viermi informatici Troieni și adware Keylogger și cryptojacking Malware fără fișiere Înțelegerea răspândirii malware-ului Gestionarea IOC-urilor și a politicilor privind parolele Politici de utilizare acceptabilă (AUP) Politici BYOD (Bring Your Own Device) Politici de acces la distanță
Obiective de învățare: • Distingeți rolurile cheie și colaborarea dintre R și SOC. • Definiți diferența dintre incidentele de securitate și încălcările de securitate. • Explicați sursele alertelor de securitate și procesele de triere. • Furnizați documentație și rapoarte eficiente pentru incidentele de securitate. • Prezentați tipurile comune de atacuri web (DoS/DDoS, SQL Injection, XSS, Command Injection, LFI, CSRF).	

• Explicați atacurile de forță brută și de umplere a credențialelor și prezentați contramăsurile acestora. • Înțelegerea principiilor de bază ale atacurilor „pass the hash" și „pass the ticket". • Explicarea modului în care pot fi exploatate vulnerabilitățile controlului accesului defectuos. • Explicarea diferitelor tipuri de malware (ransomware, virus, worm, troian, adware, keylogger, cryptojacking, malware fără fișiere) și a metodelor lor de propagare. • Explicați importanța gestionării indicatorilor de informații privind amenințările (IOC). • Prezentați elementele cheie ale politicilor privind parolele puternice și ale politicilor de utilizare acceptabilă (AUP). • Evaluați impactul asupra securității al politicilor BYOD și de acces la distanță.

Tabelul 4-Modulul: 3

Unități	**Teme**
Măsurarea performanței (indicatori)	Indicatori de performanță Monitorizarea sistemului și a rețelei Monitorizarea indicatorilor de performanță Cartografierea rețelei Scanarea vulnerabilităților Analiza traficului de rețea
Obiective de învățare: • Cursanții vor defini indicatorii de performanță și vor explica importanța acestora în evaluarea performanței sistemului și a rețelei. • Cursanții vor demonstra configurarea și utilizarea instrumentelor de monitorizare pentru evaluarea continuă a performanței sistemului și a rețelei. • Cursanții vor analiza și interpreta indicatorii de performanță pentru a evalua starea sistemului și a identifica oportunitățile de optimizare. • Cursanții vor crea hărți de rețea pentru a vizualiza, monitoriza și optimiza structurile de rețea. • Cursanții vor efectua scanări de vulnerabilitate, vor identifica riscurile de securitate și vor recomanda măsuri de remediere. • Cursanții vor efectua analize ale traficului de rețea pentru a detecta și a răspunde la potențialele amenințări.	
Analiza datelor	Colectarea datelor Curățarea și preprocesarea datelor Analiza datelor Vizualizarea datelor Instrumente analitice Aplicații ale analizei datelor în domeniul securității cibernetice
Obiective de învățare: • Cursanții vor colecta date relevante din sisteme, rețele și jurnale de securitate pentru analiză. • Cursanții vor curăța și preprocesa datele brute pentru a asigura acuratețea și consecvența.	

• Cursanții vor aplica tehnici statistice și analitice pentru a extrage informații semnificative din date. • Cursanții vor crea vizualizări de date pentru a comunica în mod eficient rezultatele analizei. • Cursanții vor utiliza instrumente precum Python, R și Power BI pentru analiza cuprinzătoare a datelor. • Cursanții vor aplica tehnici de analiză a datelor pentru a detecta, analiza și atenua amenințările la adresa securității cibernetice.	
Informații de securitate	Înțelegerea informațiilor de securitate Surse de informații de securitate Metode de colectare a informațiilor privind amenințările Studii de caz privind aplicațiile informațiilor de securitate
Obiective de învățare: • Cursanții vor explica importanța informațiilor de securitate în gestionarea proactivă a amenințărilor. • Cursanții vor evalua sursele de informații de securitate, inclusiv fluxurile de amenințări, rapoartele și instrumentele open-source. • Cursanții vor descrie metode de colectare și analizare a informațiilor privind amenințările. • Cursanții vor examina cazuri reale pentru a înțelege aplicarea informațiilor de securitate în prevenirea amenințărilor cibernetice.	

Tabelul 5-Modulul: 4

Unități	**Teme**
Noțiuni fundamentale privind operațiunile de securitate	Înțelegerea operațiunilor de securitate și SOC (Centrul de operațiuni de securitate) Roluri și responsabilități în operațiunile de securitate Prezentare generală a instrumentelor și tehnologiilor de operațiuni de securitate Exemple practice și studii de caz
Obiective de învățare: • Cursanții vor explica scopul și structura unui centru de operațiuni de securitate și rolul acestuia în domeniul securității cibernetice. • Cursanții vor descrie rolurile și responsabilitățile personalului din cadrul operațiunilor de securitate, inclusiv răspunsul la incidente, identificarea amenințărilor și monitorizarea. • Cursanții vor identifica și demonstra utilizarea instrumentelor și tehnologiilor comune din cadrul operațiunilor de securitate. • Cursanții vor analiza exemple reale și studii de caz pentru a înțelege operațiunile de securitate în practică.	
Convergența securității	Înțelegerea convergenței securității Bazele securității fizice (principii de securitate fizică, protejarea bunurilor fizice, politici) Amenințări comune cu care se confruntă IMM-urile Studii de caz care evidențiază probleme de convergență
Obiective de învățare:	

• Cursanții vor defini convergența securității și vor explica importanța acesteia în integrarea măsurilor de securitate fizică și cibernetică. • Cursanții vor aplica principiile securității fizice pentru a proteja bunurile, instalațiile și personalul. • Cursanții vor identifica și evalua amenințările la adresa securității cu care se confruntă în mod frecvent întreprinderile mici și mijlocii (IMM-uri). • Cursanții vor examina studii de caz pentru a înțelege impactul provocărilor legate de convergență. • Cursanții vor analiza procesele de gestionare a informațiilor și evenimentelor de securitate.	
Gestionarea informațiilor și evenimentelor de securitate	Revizuirea principiilor de monitorizare a securității (pe baza modulului altor parteneri) Implementarea soluțiilor SIEM Configurarea jurnalelor și alertelor Revizuirea metodologiilor de detectare și informare privind amenințările (pe baza modulului altor parteneri)
Obiective de învățare: • Cursanții vor explica principiile monitorizării securității și aplicarea acestora în soluțiile SIEM. • Cursanții vor configura și opera soluții SIEM pentru detectarea și răspunsul eficient la amenințări. • Cursanții vor configura mecanisme de înregistrare și alertare în instrumentele SIEM pentru a monitoriza evenimentele de securitate. • Cursanții vor evalua informațiile privind amenințările și metodologiile de detectare pentru operațiuni de securitate eficiente.	
Practici privind operațiunile de securitate	Conformitate și reglementare Strategii de îmbunătățire continuă în operațiunile de securitate Automatizare și coordonare Indicatori și raportare
Obiective de învățare: • Cursanții vor explica importanța conformității și reglementării în operațiunile de securitate. • Cursanții vor proiecta și implementa strategii de îmbunătățire continuă pentru operațiunile de securitate. • Cursanții vor utiliza automatizarea și coordonarea pentru a spori eficiența operațiunilor de securitate. • Cursanții vor dezvolta și utiliza indicatori de securitate și tehnici de raportare pentru a comunica starea de securitate.	

Tabelul 6-Modulul: 5

Unități	**Teme**
Context organizațional	Evoluția securității cibernetice în IMM-uri Principalele amenințări și vulnerabilități actuale Impactul securității cibernetice asupra strategiei de afaceri

	Provocări specifice ale securității cibernetice în IMM-uri față de întreprinderile mari Înțelegerea implicațiilor normative ale practicilor de securitate cibernetică și modul în care acestea se aliniază structurilor de guvernanță. Provocări comune specifice IMM-urilor în materie de securitate cibernetică, cum ar fi bugetele limitate, lipsa personalului dedicat securității și metode practice de prioritizare a investițiilor în securitatea cibernetică.
Obiective de învățare: • Cursanții vor urmări evoluția practicilor de securitate cibernetică în cadrul întreprinderilor mici și mijlocii. • Cursanții vor identifica și evalua cele mai critice amenințări și vulnerabilități actuale care afectează IMM-urile. • Cursanții vor analiza modul în care securitatea cibernetică influențează strategia de afaceri și luarea deciziilor operaționale. • Cursanții vor compara provocările în materie de securitate cibernetică cu care se confruntă IMM-urile cu cele întâlnite de organizațiile mai mari. • Cursanții vor interpreta cerințele de reglementare în materie de securitate cibernetică și vor evalua modul în care acestea se integrează în guvernanța organizațională. • Cursanții vor descrie soluții practice pentru provocările comune în materie de securitate cibernetică cu care se confruntă IMM-urile, cum ar fi constrângerile bugetare și personalul limitat.	
Confidențialitate	Principiile confidențialității în domeniul securității cibernetice Protecția datelor cu caracter personal și RGPD Impactul confidențialității asupra operațiunilor IMM-urilor Instrumente și tehnici pentru protecția confidențialității
Obiective de învățare: • Cursanții vor explica principiile fundamentale ale confidențialității în contextul securității cibernetice. • Cursanții vor aplica cerințele GDPR și vor evalua impactul acestora asupra protecției datelor cu caracter personal. • Cursanții vor evalua modul în care reglementările privind confidențialitatea afectează operațiunile zilnice și modelele de afaceri ale IMM-urilor. • Cursanții vor utiliza instrumente și vor implementa tehnici pentru menținerea confidențialității și protejarea datelor sensibile.	
Legislație, etică și conformitate	Organizații, politici și standarde în domeniul securității cibernetice Legislația națională și internațională relevantă Conformitatea cu reglementările în IMM-uri Etica în domeniul securității cibernetice Consecințele juridice ale neconformității în domeniul securității cibernetice Analiza modului în care instrumentele bazate pe IA pot fi utilizate pentru a consolida guvernanța în domeniul securității cibernetice și pentru a asigura conformitatea prin monitorizare continuă și răspuns automat la amenințări.
Obiective de învățare:	

<table>
<tr><td colspan="2">
• Cursanții vor identifica organizațiile cheie din domeniul securității cibernetice și vor evalua cadrele relevante de politici și standarde.
• Cursanții vor rezuma legile cheie care afectează securitatea cibernetică la nivel național și internațional.
• Cursanții vor elabora strategii pentru a atinge și menține conformitatea cu reglementările în contextul IMM-urilor.
• Cursanții vor examina considerentele etice în luarea deciziilor și comportamentul în materie de securitate cibernetică.
• Cursanții vor evalua ramificațiile juridice ale nerespectării legilor privind securitatea cibernetică.
• Cursanții vor explora modul în care instrumentele de IA pot îmbunătăți guvernanța, automatiza monitorizarea și spori conformitatea.
</td></tr>
<tr><td>Guvernanța securității</td><td>Structura de guvernanță în domeniul securității cibernetice
Roluri și responsabilități în gestionarea securității
Modele de maturitate în domeniul securității cibernetice
Îmbunătățirea abilităților de evaluare a riscurilor și de formulare a planurilor strategice de răspuns în condiții de criză simulate (ransomware, atacuri de phishing etc.)
Comunicarea la nivel executiv și la nivelul consiliului de administrație
Strategii de comunicare în domeniul securității cibernetice
Raportarea aspectelor legate de securitate către conducerea superioară
Gestionarea crizelor și comunicarea în domeniul securității cibernetice
Stăpânirea abilităților de gestionare a crizelor și de luare a deciziilor în scenarii extrem de stresante, care implică atacuri bazate pe inteligența artificială și ransomware.</td></tr>
<tr><td colspan="2">
Obiective de învățare:
• Cursanții vor proiecta și evalua structuri de guvernanță care să sprijine gestionarea eficientă a securității cibernetice.
• Cursanții vor atribui și clarifica responsabilitățile în cadrul organizațional de securitate.
• Cursanții vor evalua maturitatea securității cibernetice folosind modele consacrate.
• Cursanții vor efectua evaluări de risc și vor dezvolta strategii de răspuns pentru scenarii precum ransomware sau phishing.
• Cursanții vor dezvolta planuri de comunicare pentru a transmite informații privind securitatea cibernetică către membrii conducerii superioare și ai consiliului de administrație.
• Cursanții vor formula strategii de comunicare eficiente pentru părțile interesate interne și externe în domeniul securității cibernetice.
• Cursanții vor genera rapoarte care informează conducerea superioară cu privire la performanța și riscurile în materie de securitate cibernetică.
• Cursanții vor exersa gestionarea și comunicarea în timpul crizelor de securitate cibernetică, inclusiv cele care implică atacuri bazate pe inteligența artificială.
</td></tr>
<tr><td>Politica managerială</td><td>Implementarea și monitorizarea politicilor</td></tr>
<tr><td colspan="2">
Obiective de învățare:
• Cursanții vor implementa politici de securitate cibernetică și vor stabili proceduri pentru monitorizarea și aplicarea continuă a acestora.
</td></tr>
</table>

Tabelul 7-Modulul: 6

Unitîți	**Teme**
Introducere în planificarea securității cibernetice: securitatea datelor, a persoanelor și a societății	Securitatea datelor - Securitatea stocării informațiilor, procesul de investigare Securitatea datelor - Tehnici de atacare a parolelor Securitatea umană - Conștientizare și înțelegere Securitatea socială - Ce sunt criminalitatea cibernetică și etica cibernetică Securitatea socială - Legislația cibernetică - Dovezi digitale, contracte digitale, convenții multinaționale (acorduri)
Obiective de învățare: • Cursanții vor implementa strategii pentru securizarea informațiilor stocate și vor sprijini procesele de investigare. • Cursanții vor identifica și analiza tehnici comune de atac asupra parolelor și vor dezvolta contramăsuri adecvate. • Cursanții vor promova conștientizarea privind securitatea cibernetică și vor încuraja înțelegerea în rândul angajaților și părților interesate. • Cursanții vor explica implicațiile sociale ale criminalității cibernetice și vor evalua considerentele etice în mediile digitale. • Cursanții vor interpreta conceptele cheie ale legislației cibernetice, inclusiv probele digitale, contractele și acordurile internaționale.	
Management operațional și tactic	Implementarea controalelor de acces Gestionarea patch-urilor și actualizările software Monitorizarea continuă a sistemului Instruirea angajaților în materie de securitate
Obiective de învățare: • Cursanții vor proiecta și implementa mecanisme eficiente de control al accesului pentru a proteja sistemele și datele. • Cursanții vor stabili proceduri pentru gestionarea la timp a patch-urilor și actualizările software pentru a reduce vulnerabilitățile. • Cursanții vor monitoriza continuu sistemele pentru a detecta și a răspunde la evenimentele de securitate. • Cursanții vor dezvolta și vor livra programe de formare în domeniul securității pentru a spori implicarea angajaților și a reduce riscul uman.	

Tabelul 8-Modulul: 7

Unități	**Teme**
Evaluarea riscurilor	Cadrul general și procesul de gestionare a riscurilor Principiile gestionării riscurilor Standarde de gestionare a riscurilor Exemple practice și studii de caz
Obiective de învățare: • Cursanții vor descrie și aplica cadrul general și procesul de gestionare a riscurilor în domeniul securității cibernetice. • Cursanții vor explica principiile de bază care stau la baza gestionării eficiente a riscurilor în domeniul securității cibernetice. • Cursanții vor identifica și interpreta standardele de gestionare a riscurilor larg acceptate. • Cursanții vor evalua scenarii de risc prin exemple reale și studii de caz.	
Identificarea riscurilor	Surse tangibile și intangibile de risc Cauze și evenimente Amenințări și oportunități Vulnerabilități și capacități Schimbări în contextul extern și intern Indicatori ai riscurilor emergente Natura și valoarea activelor și resurselor Consecințe și impactul acestora asupra obiectivelor Limitări ale cunoștințelor și fiabilității informațiilor Prejudecăți, ipoteze și convingeri ale persoanelor implicate. Exemple practice și studii de caz.
Obiective de învățare: • Cursanții vor face distincția între sursele tangibile și intangibile de risc în mediile de securitate cibernetică. • Cursanții vor identifica cauzele riscurilor și evenimentele declanșatoare. • Cursanții vor analiza amenințările la adresa securității cibernetice și vor evalua potențialele oportunități de îmbunătățire. • Cursanții vor evalua vulnerabilitățile și capacitățile organizaționale în gestionarea riscurilor. • Cursanții vor evalua modul în care schimbările contextuale influențează riscurile de securitate cibernetică. • Cursanții vor identifica indicatorii care semnalează apariția unor noi amenințări la adresa securității cibernetice. • Cursanții vor evalua valoarea activelor și importanța resurselor în raport cu riscul. • Cursanții vor estima consecințele potențiale și impactul acestora asupra obiectivelor strategice. • Cursanții vor recunoaște limitele informațiilor și cunoștințelor în procesul de identificare a riscurilor. • Cursanții vor reflecta asupra modului în care factorii umani afectează percepția și identificarea riscurilor. • Cursanții vor aplica tehnici de identificare prin scenarii din lumea reală.	
Amenințări interne	Definiția și tipurile amenințărilor interne

	Detectarea și identificarea amenințărilor interne Exemple practice și studii de caz
Obiective de învățare: • Cursanții vor defini amenințările interne și vor clasifica diferitele tipuri. • Cursanții vor dezvolta abilități pentru a detecta și a răspunde la indicatorii amenințărilor interne. • Cursanții vor analiza studii de caz ale incidentelor reale de amenințări interne.	
Modele și metodologii de măsurare și evaluare a riscurilor	Modele și metodologii cantitative și calitative de evaluare a riscurilor Probabilitatea evenimentelor și consecințele acestora Natura și amploarea consecințelor Niveluri de sensibilitate și încredere. Exemple practice și studii de caz
Obiective de învățare: • Cursanții vor compara și aplica atât modele cantitative, cât și calitative în evaluarea riscurilor de securitate cibernetică. • Cursanții vor evalua probabilitatea și potențialele consecințe ale riscurilor identificate. • Cursanții vor evalua gravitatea și amploarea consecințelor asociate riscurilor de securitate cibernetică. • Cursanții vor determina nivelurile de incertitudine și încredere în evaluarea riscurilor. • Cursanții vor implementa modele de evaluare a riscurilor în scenarii practice.	
Controlul riscurilor	Monitorizare și revizuire Înregistrare și raportare Exemple practice și studii de caz
Obiective de învățare: • Cursanții vor efectua procese regulate de monitorizare și revizuire a riscurilor. • Cursanții vor documenta și raporta în mod eficient măsurile de control al riscurilor. • Cursanții vor examina exemple din lumea reală pentru a înțelege implementarea eficientă a controlului riscurilor.	

Tabelul 9-Modulul: 8

Unități	**Teme**
Răspuns la incident	Definiția și importanța răspunsului la incident Componentele cheie ale unui plan eficient de recuperare pentru răspunsul la incident Amenințări comune la securitatea cibernetică
Obiective de învățare: • Cursanții vor defini răspunsul la incident și vor explica importanța acestuia în managementul securității cibernetice. • Cursanții vor identifica și implementa elementele cheie ale unui plan structurat de recuperare a răspunsului la incident. • Cursanții vor recunoaște și vor răspunde amenințărilor comune la securitatea cibernetică întâlnite în timpul gestionării incidentelor.	

Recuperare în caz de dezastru	Înțelegerea recuperării în caz de dezastru Roluri și responsabilități în recuperarea în caz de dezastru Etape de recuperare după dezastru
Obiective de învățare: • Cursanții vor explica principiile și obiectivele recuperării în caz de dezastru în contextul securității cibernetice. • Cursanții vor descrie rolurile și responsabilitățile membrilor echipei implicați în recuperarea în caz de dezastru. • Cursanții vor dezvolta un plan pas cu pas pentru a restabili sistemele și operațiunile după un dezastru cibernetic.	
Business continuity	Înțelegerea continuității afacerii Roluri și responsabilități în continuitatea afacerii Analiza impactului afacerii
Obiective de învățare: • Cursanții vor explica conceptul și importanța planificării continuității afacerii. • Cursanții vor identifica rolurile și responsabilitățile legate de asigurarea continuității afacerii. • Cursanții vor efectua o analiză a impactului asupra afacerii pentru a evalua funcțiile și dependențele critice.	
Conștientizarea, instruirea și educația în materie de securitate	Înțelegerea conștientizării securității Responsabilitățile angajaților în securitatea cibernetică
Obiective de învățare: • Cursanții vor explica rolul conștientizării securității în reducerea riscurilor de securitate cibernetică legate de oameni. • Cursanții vor recunoaște responsabilitățile angajaților în respectarea protocoalelor de securitate cibernetică și a celor mai bune practici.	
Practici de angajare de securitate	Definirea cerințelor rolurilor de securitate Efectuarea verificărilor antecedentelor
Obiective de învățare: • Cursanții vor defini rolurile de muncă în domeniul securității cibernetice și vor formula cerințe adecvate. • Cursanții vor aplica cele mai bune practici în efectuarea verificărilor antecedentelor pentru roluri sensibile la securitate.	
Practici de terminare a securității	Revocarea imediată a accesului Notificarea echipelor relevante Considerații legale și de conformitate
Obiective de învățare: • Cursanții vor implementa proceduri pentru revocarea promptă a accesului la rezilierea angajatului. • Cursanții vor coordona comunicarea cu departamentele relevante în timpul procesului de offboarding. • Cursanții vor examina cerințele legale și de conformitate legate de încetarea angajării în domeniul securității cibernetice.	
Securitate terță parte	Evaluarea riscului terților Implementarea contrastelor și cerințelor de securitate

	Monitorizare și audit continuă Răspunsul la incident și comunicarea
Obiective de învățare: • Cursanții vor evalua riscurile de securitate asociate cu furnizorii și partenerii terți. • Cursanții vor concepe și vor aplica clauze contractuale pentru a asigura conformitatea cu securitatea terților. • Cursanții vor stabili practici continue de monitorizare și audit pentru securitatea terților. • Cursanții se vor coordona cu terți în timpul activităților de răspuns la incident.	
Securitate în procesele de revizuire	Încorporarea securității în recenzii Evaluarea vulnerabilității și testarea de penetrare Recenzii post-incident
Obiective de învățare: • Cursanții vor integra considerentele de securitate în procesele de revizuire organizațională. • Cursanții vor efectua evaluări de vulnerabilitate și teste de penetrare ca parte a activităților de revizuire. • Cursanții vor efectua analize după incident pentru a evalua eficiența și pentru a îmbunătăți răspunsurile viitoare.	
Problemă specială privind confidențialitatea informațiilor personale ale angajaților	Limitări de colectare a datelor Stocare si control acces Respectarea reglementărilor privind confidențialitatea Partajarea datelor și terților Consimțământul și drepturile angajaților
Obiective de învățare: • Cursanții vor identifica limitele adecvate pentru colectarea datelor personale ale angajaților. • Cursanții vor aplica măsuri securizate de stocare și control al accesului pentru datele sensibile ale angajaților. • Cursanții vor asigura conformitatea cu reglementările relevante privind confidențialitatea, cum ar fi GDPR. • Cursanții vor evalua riscurile și regulile legate de partajarea datelor angajaților cu terți. • Cursanții vor înțelege drepturile angajaților și importanța obținerii consimțământului informat.	

CONCLUZII

Acest raport prezintă curriculumul adecvat nivelului de educație profesională care ar trebui luat în considerare pentru implementarea cu succes a formării CyberAgent. În urma cercetărilor efectuate încă de la începutul proiectului de identificare a nevoilor de formare, acest document descrie nevoile de participare ale studenților din învățământul profesional.

Curriculumul pregătit pentru proiectul CyberAgent EQF Level 5-6 a fost luat ca referință în timpul pregătirii programului. Din curriculum-ul acestui nivel au fost selectate subiecte potrivite pentru EQF Nivelul 4-5.

În sfârșit, pentru a ne asigura că instruirea este de cea mai bună calitate în ceea ce privește conținutul, organizarea și dezvoltarea competențelor, întrebările legate de subiecte nu au fost transferate de la EQF Nivelul 5-6.

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