CyberAgent

Co-funded by the European Union

POZIOM 4 EUROPEJSKICH RAM KWALIFIKACJI

PROGRAM SZKOLENIOWY

WERSJA ROBOCZA
OPRACOWANA PRZEZ TIMTAL

CYBERAGENT 01.2025

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

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak wyłącznie poglądami i opiniami autora (autorów) i nie muszą odzwierciedlać poglądów Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie ponoszą za nie odpowiedzialności.

Pakiet roboczy 3: Tworzenie zasobów edukacyjnych dla agentów zmian w dziedzinie cyberbezpieczeństwa

Wynik 3.2: Moduły szkoleniowe dla studentów kształcenia i szkolenia zawodowego
Lider 3.2 – TIMTAL (TR)

TREŚĆ

WYKAZ TABEL

WPROWADZENIE

Szybkie zmiany w nauce i technologii, zmieniające się potrzeby jednostek i społeczeństwa, innowacje i rozwój teorii i podejść do uczenia się i nauczania mają bezpośredni wpływ na role oczekiwane od jednostek. Zmiana ta definiuje osobę, która tworzy wiedzę, potrafi ją funkcjonalnie wykorzystać w życiu, potrafi rozwiązywać problemy, myśleć krytycznie, jest przedsiębiorcza, zdeterminowana, posiada umiejętności komunikacyjne, potrafi empatię, wnosi wkład w społeczeństwo i kulturę itp.

Oszałamiające tempo zmian w erze informacji niesie ze sobą nieustannie zmieniające się potrzeby jednostek i społeczeństw. Innowacje w teoriach uczenia się i nauczania radykalnie zmieniają role oczekiwane od poszczególnych osób. Obecnie na pierwszy plan wysuwają się nie tylko wiedza, ale także umiejętności, takie jak umiejętność funkcjonalnego wykorzystania tej wiedzy w życiu, umiejętność tworzenia rozwiązań złożonych problemów, umiejętność krytycznego myślenia, umiejętność działania w duchu przedsiębiorczości, umiejętność skutecznej komunikacji, umiejętność okazywania empatii i wnoszenia wartości dodanej do społeczeństwa. Ta transformacja zachęca jednostki do ciągłego uczenia się, dostosowywania się i doskonalenia.

W tym kontekście szkolenia zawodowe również przechodzą poważną transformację. Tradycyjne zawody są zastępowane przez nowe, oparte na technologii i stale rozwijające się profesje. Cyberbezpieczeństwo ma kluczowe znaczenie w tej zmianie. Ponieważ w cyfryzującym się świecie ryzyko związane z cyberbezpieczeństwem rośnie w każdym sektorze i każdym zawodzie. Cyberbezpieczeństwo odgrywa istotną rolę w wielu obszarach, od danych osobowych po ochronę tajemnic przedsiębiorstwa, od bezpieczeństwa infrastruktury krytycznej po bezpieczeństwo transakcji finansowych.

Znaczenie szkolenia w zakresie cyberbezpieczeństwa w kształceniu zawodowym nie ogranicza się do umiejętności technicznych. Obejmuje ono również wychowywanie osób posiadających wartości etyczne, wysokie poczucie odpowiedzialności, znających przepisy prawne i otwartych na ciągłe uczenie się. Ponieważ cyberbezpieczeństwo to nie tylko problem techniczny, ale także odpowiedzialność społeczna. Dlatego też nadanie niezbędnego znaczenia szkoleniom w zakresie cyberbezpieczeństwa w kształceniu zawodowym jest kluczowym krokiem dla przyszłości zarówno poszczególnych osób, jak i całego społeczeństwa.

Kształcenie zawodowe obejmuje planowanie, badania, rozwój, organizację i skoordynowane zarządzanie, nadzór i działalność dydaktyczną wszystkich usług w zakresie kształcenia zawodowego i technicznego wraz z sektorem rolniczym, przemysłowym i usługowym w ramach integralności systemu edukacji. Celem tych działań edukacyjnych jest kształcenie ekspertów, którzy zapewnią ciągłość funkcjonowania społeczeństwa i wykwalifikowaną kadrę potrzebną na każdym etapie produkcji, oraz położenie nacisku na szkolenia zawodowe.

Program kształcenia zawodowego Cyber Agent (EQF4) ma na celu przygotowanie osób do życia w cyberprzestrzeni i opiera się na potrzebach rynku pracy oraz analizie stanowisk pracy. W ramach tego podejścia analizowane są umiejętności w zakresie cyberbezpieczeństwa, definiowany jest profil zawodowy oraz określane są zadania i procedury, które musi wykonywać personel zajmujący się cyberbezpieczeństwem. Program nauczania Cyber Agent ma na celu przekazanie wiedzy, umiejętności, postaw i zachowań, które należy posiadać, aby wykonywać odpowiednią pracę i transakcje poprzez lekcje i osiągnięcia, z drugiej strony działania edukacyjne są planowane w sposób, który przygotuje osoby do życia zawodowego zgodnie z tymi ramami.

1. CELE PROGRAMU CYBERAGENT EQF POZIOM 4

Potrzeba zapewnienia cyberbezpieczeństwa stała się dość ważna, zwłaszcza w krajach UE, a także na całym świecie, i w ostatnich latach gwałtownie wzrosła. Równolegle z rozwojem technologicznym, cyberzagrożenia i cyberryzyko również zmieniły się w tym samym tempie i stały się bardziej złożone. Ryzyko i zagrożenia cybernetyczne osiągnęły potencjał, który spowoduje znacznie bardziej kompleksowe i negatywne skutki niż ataki fizyczne. Ponieważ sektory takie jak finanse, komunikacja elektroniczna, energetyka, transport i lotnictwo świadczą usługi w bezpiecznym środowisku cyfrowym, zapewnienie krajowego bezpieczeństwa cybernetycznego stało się jednym z priorytetów naszego kraju. W tym kontekście dąży się do upowszechniania edukacji w zakresie bezpieczeństwa cybernetycznego w ramach edukacji formalnej i nieformalnej oraz do opracowywania i wzbogacania treści edukacyjnych.

2. EUROPEJSKIE RAMY KWALIFIKACJI

UE opracowała europejskie ramy kwalifikacji (EQF) jako narzędzie tłumaczeniowe, aby ułatwić zrozumienie i porównywalność kwalifikacji krajowych. EQF ma na celu wspieranie transgranicznej mobilności osób uczących się i pracowników, promowanie uczenia się przez całe życie i rozwoju zawodowego w całej Europie.

EQF to 8-poziomowe ramy oparte na efektach uczenia się dla wszystkich rodzajów kwalifikacji, które służą jako narzędzie tłumaczenia między różnymi krajowymi ramami kwalifikacji. Ramy te pomagają poprawić przejrzystość, porównywalność i przenoszalność kwalifikacji osób oraz umożliwiają porównywanie kwalifikacji z różnych krajów i instytucji.

EQF obejmuje wszystkie rodzaje i poziomy kwalifikacji, a wykorzystanie efektów uczenia się pozwala jasno określić, co dana osoba wie, rozumie i potrafi zrobić. Poziom wzrasta wraz z poziomem biegłości, poziom 1 jest najniższy, a 8 najwyższy. Co najważniejsze, EQF jest ściśle powiązany z krajowymi ramami kwalifikacji, dzięki czemu może zapewnić kompleksowy obraz wszystkich rodzajów i poziomów kwalifikacji w Europie, które są coraz bardziej dostępne dzięki bazom danych kwalifikacji.

EQF został ustanowiony w 2008 r., a następnie zrewidowany w 2017 r. W ramach tej rewizji zachowano podstawowe cele, jakim jest zapewnienie przejrzystości i wzajemnego zaufania w zakresie kwalifikacji w Europie. Państwa członkowskie zobowiązały się do dalszego rozwoju EQF i zwiększenia jego skuteczności w ułatwianiu pracodawcom, pracownikom i osobom uczącym się zrozumienia kwalifikacji krajowych, międzynarodowych i kwalifikacji z państw trzecich.

Każdy z 8 poziomów EQF jest zdefiniowany przez zestaw deskryptorów wskazujących efekty uczenia się istotne dla kwalifikacji na danym poziomie w dowolnym systemie kwalifikacji. Efekty uczenia się są definiowane w kategoriach:

- Wiedza: w kontekście EQF wiedza jest opisywana jako teoretyczna i/lub faktograficzna.
- Umiejętności: w kontekście EQF umiejętności opisuje się jako poznawcze (obejmujące stosowanie logicznego, intuicyjnego i kreatywnego myślenia) oraz praktyczne (obejmujące zręczność manualną oraz stosowanie metod, materiałów, narzędzi i instrumentów).
- Odpowiedzialność i autonomia: w kontekście EQF odpowiedzialność i autonomia są opisane jako zdolność uczącego się do samodzielnego i odpowiedzialnego stosowania wiedzy i umiejętności.

Tabela1 – Efekty uczenia się na poziomie 4 EQF

Wiedza	***Umiejętności***	***Odpowiedzialność i autonomia***
Wiedza faktograficzna i teoretyczna w szerokim kontekście w ramach danej dziedziny studiów lub nauki	Zestaw umiejętności poznawczych i praktycznych wymaganych do opracowywania rozwiązań konkretnych problemów w dziedzinie pracy lub edukacji	Stosowanie samokontroli w ramach wytycznych dotyczących pracy lub nauki, które są ogólnie przewidywalne, ale mogą ulec zmianie; nadzorowanie rutynowej pracy innych osób, przejmowanie części odpowiedzialności za ocenę i doskonalenie działań związanych z pracą lub nauką

3. STUDENCI KSZTAŁCENIA I SZKOLENIA Z ZAKRESU CYBERBEZPIECZEŃSTWA (POZIOM 4 EQ

Pracownik ds. cyberbezpieczeństwa (poziom 4) to wykwalifikowany specjalista, który pracuje w dziedzinie systemów informatycznych w miejscu pracy, uczestniczy w badaniach dotyczących działań zapobiegawczych w zakresie cyberbezpieczeństwa w ramach procesów śledzenia podatności i podnoszenia świadomości w zakresie cyberbezpieczeństwa, monitoruje działania, monitoruje działanie i trwałość systemów wykorzystywanych w analizach cyberbezpieczeństwa, określa wymagania prostych sieci, konfiguruje sieci fizyczne, wykonuje proste konfiguracje związane ze sprzętem sieciowym, zapewnia bezpieczeństwo sieci, konserwację i ulepszenia, zapewnia wsparcie techniczne użytkownikom oraz prowadzi badania w zakresie rozwoju zawodowego w celu ochrony infrastruktury informatycznej w miejscu pracy przed cyberzagrożeniami w ramach wymagań jakościowych poprzez wdrażanie środków bezpieczeństwa i higieny pracy oraz ochrony środowiska.

3.1. PROGRAM CYBERAGENT LEARNING DLA EQF-4

Program nauczania VET (EQF 4-5) został opracowany poprzez strategiczne dostosowanie kompleksowego programu nauczania HEI (EQF 5-6). Proces adaptacji polegał na skoncentrowaniu materiału w celu dostosowania go do zakresu 1 ECTS oraz skupieniu się na efektach uczenia się najbardziej istotnych dla odbiorców kształcenia i szkolenia zawodowego oraz bezpośrednich potrzeb MŚP. Priorytetowo potraktowano tematy kładące nacisk na praktyczne zastosowanie i podstawowe umiejętności w zakresie cyberbezpieczeństwa, natomiast bardziej szczegółowe koncepcje teoretyczne zostały uproszczone, aby dostosować je do ścieżki kształcenia i szkolenia zawodowego.

Tabela2 -Moduł: 1

<table>
<tr><th>Jednostki</th><th>Tematy</th></tr>
<tr><td>Zarządzanie projektami</td><td>Planowanie projektów
Określanie celów projektu
Aktualne zagrożenia dla cyberbezpieczeństwa (ataki DDoS, oprogramowanie ransomware, złośliwe oprogramowanie, phishing, ataki typu zero-day, ataki na urządzenia IoT itp.
Modelowanie zagrożeń i analiza podatności
Zgłaszanie zagrożeń i incydentów związanych z cyberbezpieczeństwem</td></tr>
<tr><td colspan="2">Efekty uczenia się:
Uczestnicy będą potrafili zdefiniować fazy zarządzania projektem i stworzyć podstawowy plan projektu. (Zastosowanie)
Uczestnicy będą potrafili sformułować jasne, mierzalne i osiągalne cele projektu. (Analiza)
Uczestnicy będą identyfikować, klasyfikować i oceniać różne zagrożenia dla cyberbezpieczeństwa. (Analiza)
Uczestnicy opracują modele zagrożeń i przeprowadzą analizy podatności dla konkretnych scenariuszy. (Zastosowanie)
Uczestnicy przygotują raporty dotyczące incydentów zgodnie z ustalonymi protokołami. (Zastosowanie)</td></tr>
<tr><td>Zarządzanie zasobami</td><td>Narzędzia i oprogramowanie zabezpieczające
Efektywne wykorzystanie zasobów technologicznych</td></tr>
<tr><td colspan="2">Efekty kształcenia:
Uczestnicy kursu będą potrafić efektywnie korzystać z narzędzi i oprogramowania służących do wykrywania zagrożeń i reagowania na nie. (Zastosowanie)
Uczestnicy kursu zoptymalizują zasoby technologiczne w celu zwiększenia bezpieczeństwa i wydajności. (Zastosowanie)</td></tr>
<tr><td>Wskaźniki bezpieczeństwa</td><td>Wskaźniki bezpieczeństwa i techniki pomiarowe
Gromadzenie danych za pomocą SIEM
Analiza wskaźników bezpieczeństwa
Monitorowanie projektu i ocena wydajności
Raportowanie wskaźników bezpieczeństwa</td></tr>
</table>

Efekty kształcenia: • Uczestnicy szkolenia będą potrafili zidentyfikować i zastosować odpowiednie wskaźniki bezpieczeństwa oraz techniki pomiarowe. (Zastosowanie) • Uczestnicy skonfigurują i będą wykorzystywać narzędzia SIEM do gromadzenia danych i monitorowania bezpieczeństwa. (Zastosowanie) • Uczestnicy będą interpretować i analizować wskaźniki bezpieczeństwa w celu oceny stanu bezpieczeństwa. (Analiza) • Uczestnicy będą monitorować i oceniać wydajność projektu przy użyciu wskaźników bezpieczeństwa. (Ocena) • Uczestnicy będą kompilować i przedstawiać raporty oparte na analizie wskaźników bezpieczeństwa. (Zastosowanie)	
Zapewnienie jakości i kontrola jakości	Zarządzanie jakością Standardy jakości w cyberbezpieczeństwie Techniki testowania i walidacji
Efekty kształcenia: • Uczestnicy wdrożą praktyki zarządzania jakością w projektach dotyczących cyberbezpieczeństwa. (Zastosowanie) • Uczestnicy szkolenia będą identyfikować i stosować odpowiednie standardy jakości w zakresie cyberbezpieczeństwa. (Zastosowanie) • Uczestnicy opracują i wdrożą procedury testowania i walidacji rozwiązań w zakresie cyberbezpieczeństwa. (Zastosowanie)	

Tabela3 -Moduł: 2

Jednostki	**Tematy**
Administracja systemem operacyjnym	Systemy operacyjne Związki między sprzętem a oprogramowaniem Pliki binarne, liczenie szesnastkowe Bity i bajty Wiersz poleceń w systemie operacyjnym Polecenia systemu Windows i Linux Klient i serwer Windows Aplikacje, procesy i usługi w systemie Windows Rozszerzenia i typy plików Klucze i wartości rejestru Ustawienia panelu sterowania Użytkownicy i grupy Struktura domeny i menedżer serwera AD i GPO Interfejsy i jądro systemu Linux

	Procesy w systemie Linux Konwencje nazewnictwa plików i katalogów Powłoki systemu Linux i składnia poleceń Manipulowanie plikami i folderami Praca z poleceniami monitorowania systemu i potokami Zarządzanie procesami i kontrolą zadań Zarządzanie usługami
Efekty kształcenia: • Uczestnicy porównają i zestawią ze sobą różne systemy operacyjne oraz ich architektury. • Uczestnicy wyjaśnią interakcję między sprzętem a oprogramowaniem w środowisku systemu operacyjnego. • Uczestnicy będą wykonywać konwersje binarne i szesnastkowe oraz zrozumieją reprezentację danych. • Uczestnicy będą wykonywać podstawowe polecenia w środowiskach Windows i Linux. • Uczestnicy będą zarządzać aplikacjami, usługami i procesami przy użyciu narzędzi systemowych. • Uczestnicy kursu będą konfigurować i zarządzać usługą Active Directory oraz obiektami GPO. • Uczestnicy będą korzystać z interfejsów systemu Linux i wykonywać operacje na poziomie jądra. • Uczestnicy będą zarządzać usługami i procesami systemowymi za pomocą poleceń systemu Linux.	
Administracja systemami baz danych	Repozytoria i listy źródeł Zarządzanie serwerem WWW Dzienniki systemowe i monitorowanie dzienników Planowanie zadań w systemie Linux Rozwiązywanie problemów z serwerem i siecią Kopia zapasowa i odzyskiwanie Zabezpieczanie GRUB Zapory sieciowe Zarządzanie obiektami Active Directory i obiektami GPO DNS i DHCP Podstawy PowerShell Microsoft BitLocker, AppLocker i zapora sieciowa LDAP i Kerberos NTLM Zasady dotyczące haseł i blokowania Uwierzytelnianie i kontrola dostępu Protokół ICMP (Internet Control Message Protocol) TCP a UDP NetBIOS i SMB SSL i TLS Certyfikaty Protokoły Telnet i Secure Shell (SSH) HTTP i HTTPS Protokoły systemów pocztowych Protokół systemu nazw domenowych (DNS)

	FTP i RDP Kapsułkowanie a dekapitulacja Sniffery sieciowe i Wireshark TCP/UDP DHCP, DNS
Efekty kształcenia: • Uczestnicy kursu będą konfigurować repozytoria i zarządzać listami źródeł. • Uczestnicy będą analizować i monitorować logi w celu rozwiązywania problemów i zapewnienia bezpieczeństwa. • Uczestnicy będą wykonywać operacje tworzenia kopii zapasowych i odzyskiwania danych w celu zapewnienia integralności danych. • Uczestnicy wdrożą środki bezpieczeństwa, w tym zapory ogniowe, BitLocker i AppLocker.	
Administracja siecią	Typy sieci i sieci bezprzewodowe Sieci i topologie Tożsamość urządzeń i urządzenia dostępowe Infrastruktura i urządzenia zabezpieczające Urządzenia specjalistyczne i architektura sieci Sieci wirtualne Adresy fizyczne i logiczne Modele OSI i sieci Kapsułkowanie i dekapsułkowanie danych Protokoły sieciowe i numery portów Nośniki sieciowe i kable Technologie bezprzewodowe Narzędzia do administrowania siecią Cisco Packet Tracer Klasy sieciowe i podsieci Protokół rozdzielania adresów (ARP) Adresowanie statyczne a dynamiczne Translacja adresów sieciowych (NAT) Przełączniki i Cisco IOS Zabezpieczenia portów przełączników i interfejsy routerów Konfiguracja sieci VLAN i DTP Routing między sieciami VLAN Wprowadzenie do list ACL Rozwiązywanie problemów sieciowych
Efekty kształcenia: • Uczestnicy kursu będą projektować sieci i zarządzać nimi, rozumiejąc protokoły i topologie. • Uczestnicy będą konfigurować sieci VLAN, listy ACL oraz zarządzać schematami adresowania IP. • Uczestnicy będą korzystać z narzędzi takich jak Wireshark i Cisco Packet Tracer do monitorowania i rozwiązywania problemów.	
Administracja chmurą	Hypervisory i maszyny wirtualne Kontenery Zabezpieczanie środowisk wirtualnych Kopia zapasowa i odzyskiwanie

	Przetwarzanie w chmurze i dostawcy usług chmurowych Czym są modele usług w chmurze Rodzaje wdrożeń chmury Sieci wirtualne Usługi obliczeniowe AWS Amazon Elastic Compute Cloud (EC2) Narzędzia do monitorowania chmury Narzędzia do automatyzacji i koordynacji Zagrożenia i luki w zabezpieczeniach chmury Zarządzanie tożsamością i dostępem (IAM) Kontrola dostępu oparta na rolach (RBAC) Uwierzytelnianie wieloskładnikowe (MFA) Szyfrowanie danych w chmurze Wirtualna chmura prywatna (VPC) Docker i Kubernetes
Efekty kształcenia: • Uczestnicy będą zarządzać środowiskami wirtualnymi przy użyciu AWS, Docker i Kubernetes. • Uczestnicy wdrożą zabezpieczenia chmury i zarządzanie tożsamością.	
Administracja systemami cyberfizycznymi	Bezpieczeństwo i kontrola dostępu Rodzaje uwierzytelniania TACACS+ i RADIUS Konfiguracja AAA Cele zarządzania ryzykiem Szyfrowanie i deszyfrowanie Hashowanie i tabele tęczy Spoofing adresów MAC i zatruwanie ARP Skakanie po sieciach VLAN i nieautoryzowane DHCP Flood ICMP Flooding TCP i UDP Przejęcie sesji Spoofing DNS Obrona w głębi (DID) i Zero Trust Strefy zdemilitaryzowane (DMZ) Honeypoty i wzmocnienie sieci Najlepsze praktyki dotyczące bezpiecznej sieci VPN SSH i VNC Zapory stanowe a zapory bezstanowe Zapory oparte na hoście a zapory oparte na sieci Zapory sprzętowe a zapory programowe Zapora sieciowa aplikacji internetowych (WAF) Sztuczna inteligencja w zaporach sieciowych IDS i IPS NIDS i HIDS Snort tcpdump
Efekty kształcenia:	

<table>
<tr><td colspan="2">

- Uczestnicy kursu będą zabezpieczać sieci za pomocą zapór sieciowych, systemów IDS/IPS oraz narzędzi do wykrywania zagrożeń.
- Uczestnicy kursu będą stosować techniki szyfrowania i zarządzać protokołami bezpieczeństwa.

</td></tr>
<tr><td>Wzmacnianie systemu</td><td>Techniki GenAI
Generowanie kodu
Zarządzanie kontami użytkowników i kontrola dostępu
Wykrywanie anomalii i rozwiązywanie problemów
Rozwiązywanie błędów usługi Apache2
Zarządzanie poprawkami i aktualizacjami
Automatyczne tworzenie kopii zapasowych i odzyskiwanie danych
Odzyskiwanie usuniętych plików za pomocą GenAI
Procedury dotyczące cyberbezpieczeństwa
Wykrywanie i analiza zagrożeń
Reagowanie na zagrożenia i usuwanie skutków
Wykorzystanie sztucznej inteligencji do wykrywania zagrożeń w czasie rzeczywistym
Weryfikacja i testowanie modeli GenAI
Konfiguracja i bezpieczeństwo DNS
Konfiguracja i bezpieczeństwo DHCP
Podstawy PowerShell
Zabezpieczenia portów przełączników
Sieć Basic Input/Output System (NetBIOS)
Protokół SMB (Server Message Block)
Protokół SSL (Secure Sockets Layer) i TLS (Transport Layer Security)
Certyfikaty bezpieczeństwa
Protokoły systemów pocztowych
Protokół systemu nazw domenowych (DNS)
Protokół transferu plików (FTP)
Protokół zdalnego pulpitu (RDP)
Planowanie zadań w systemie Linux
Rozwiązywanie problemów z serwerem
Rozwiązywanie problemów z siecią
Tworzenie kopii zapasowych i odzyskiwanie danych
Zabezpieczanie GRUB
Konfiguracja i zabezpieczanie zapór sieciowych</td></tr>
<tr><td colspan="2">Efekty uczenia się:

- Uczestnicy kursu będą stosować techniki wzmacniania zabezpieczeń w celu poprawy bezpieczeństwa systemu.
- Uczestnicy wykorzystają sztuczną inteligencję do wykrywania zagrożeń i monitorowania systemu.

</td></tr>
<tr><td>Wzmacnianie systemu</td><td>IR a SOC
Zdarzenia i incydenty
Wykrywanie alertów i ich klasyfikacja
Dokumentacja i raportowanie
Czym są ataki internetowe?</td></tr>
</table>

	DoS i DDoS Wstrzyknięcie kodu SQL i XSS Wstrzyknięcie poleceń i lokalne włączenie plików (LFI) Cross-Site Request Forgery (CSRF) Brute-Force i Credential Stuffing Przekazywanie skrótu i przekazywanie biletu Uszkodzona kontrola dostępu Oprogramowanie ransomware Wirusy komputerowe i robaki Trojan i oprogramowanie reklamowe Keylogger i cryptojacking Złośliwe oprogramowanie bezplikowe Zrozumienie rozprzestrzeniania się złośliwego oprogramowania Zarządzanie wskaźnikami naruszenia bezpieczeństwa (IOC) i zasadami dotyczącymi haseł Zasady dopuszczalnego użytkowania (AUP) Zasady dotyczące korzystania z własnych urządzeń (BYOD) Zasady dotyczące zdalnego dostępu
Efekty kształcenia: • Rozróżnienie kluczowych ról i współpracy między R i SOC. • Zdefiniowanie różnicy między incydentami bezpieczeństwa a naruszeniami bezpieczeństwa. • Wyjaśnienie źródeł alertów bezpieczeństwa i procesów segregacji. • Zapewnienie skutecznej dokumentacji i raportowania incydentów bezpieczeństwa. • Przedstawienie typowych rodzajów ataków internetowych (DoS/DDoS, SQL Injection, XSS, Command Injection, LFI, CSRF). • Wyjaśnij, czym są ataki brute force i credential stuffing, oraz przedstaw sposoby przeciwdziałania im. • Zrozum podstawowe zasady ataków typu „pass the hash” i „pass the ticket”. • Wyjaśnij, w jaki sposób można wykorzystać luki w zabezpieczeniach kontroli dostępu. • Wyjaśnij różne rodzaje złośliwego oprogramowania (ransomware, wirusy, robaki, trojany, oprogramowanie reklamowe, keyloggery, cryptojacking, złośliwe oprogramowanie bezplikowe) oraz metody ich rozprzestrzeniania się. • Wyjaśnij znaczenie zarządzania wskaźnikami zagrożeń (IOC). • Przedstaw kluczowe elementy polityki silnych haseł i polityki dopuszczalnego użytkowania (AUP). • Oceń wpływ polityk BYOD i zdalnego dostępu na bezpieczeństwo.	

Tabela4 -Moduł: 3

Jednostki	**Tematy**
Pomiar wydajności (metryki)	Metryki wydajności Monitorowanie systemu i sieci

	Monitorowanie wskaźników wydajności Mapowanie sieci Skanowanie podatności Analiza ruchu sieciowego
Efekty kształcenia: • Uczestnicy zdefiniują wskaźniki wydajności i wyjaśnią ich znaczenie w ocenie wydajności systemu i sieci. • Uczestnicy pokażą, jak skonfigurować i używać narzędzi monitorujących do ciągłej oceny wydajności systemu i sieci. • Uczestnicy przeanalizują i zinterpretują wskaźniki wydajności w celu oceny stanu systemu i zidentyfikowania możliwości optymalizacji. • Uczestnicy kursu stworzą mapy sieci w celu wizualizacji, monitorowania i optymalizacji struktur sieciowych. • Uczestnicy przeprowadzą skanowanie podatności, zidentyfikują zagrożenia bezpieczeństwa i zaproponują działania naprawcze. • Uczestnicy przeprowadzą analizę ruchu sieciowego w celu wykrycia potencjalnych zagrożeń i reagowania na nie.	
Analiza danych	Gromadzenie danych Czyszczenie i wstępne przetwarzanie danych Analiza danych Wizualizacja danych Narzędzia analityczne Zastosowania analizy danych w cyberbezpieczeństwie
Efekty kształcenia: • Uczestnicy kursu będą gromadzić odpowiednie dane z systemów, sieci i dzienników bezpieczeństwa w celu ich analizy. • Uczestnicy kursu będą oczyszczać i wstępnie przetwarzać surowe dane w celu zapewnienia ich dokładności i spójności. • Uczestnicy zastosują techniki statystyczne i analityczne w celu uzyskania znaczących wniosków na podstawie danych. • Uczestnicy kursu będą tworzyć wizualizacje danych w celu skutecznego przekazywania wyników analizy. • Uczestnicy będą korzystać z narzędzi takich jak Python, R i Power BI do kompleksowej analizy danych. • Uczestnicy kursu będą stosować techniki analizy danych w celu wykrywania, analizowania i ograniczania zagrożeń dla cyberbezpieczeństwa.	
Wywiad bezpieczeństwa	Zrozumienie wywiadu bezpieczeństwa Źródła wywiadu bezpieczeństwa Metody gromadzenia informacji o zagrożeniach Studia przypadków dotyczące zastosowań wywiadu bezpieczeństwa
Efekty kształcenia: • Uczestnicy wyjaśnią znaczenie wywiadu bezpieczeństwa w proaktywnym zarządzaniu zagrożeniami. • Uczestnicy ocenią źródła informacji dotyczących bezpieczeństwa, w tym kanały informacyjne dotyczące zagrożeń, raporty i narzędzia open source. • Uczestnicy opiszą metody gromadzenia i analizowania informacji o zagrożeniach.	

• Uczestnicy przeanalizują rzeczywiste przypadki, aby zrozumieć zastosowanie wywiadu bezpieczeństwa w zapobieganiu cyberzagrożeniom.

Tabela5 -Moduł: 4

Jednostki	**Tematy**
Podstawy operacji bezpieczeństwa	Zrozumienie operacji bezpieczeństwa i SOC (centrum operacji bezpieczeństwa) Role i obowiązki w operacjach bezpieczeństwa Przegląd narzędzi i technologii związanych z operacjami bezpieczeństwa Praktyczne przykłady i studia przypadków
Efekty kształcenia: • Uczestnicy wyjaśnią cel i strukturę centrum operacji bezpieczeństwa oraz jego rolę w cyberbezpieczeństwie. • Uczestnicy opiszą role i obowiązki personelu operacji bezpieczeństwa, w tym reagowanie na incydenty, wykrywanie zagrożeń i monitorowanie. • Uczestnicy szkolenia zidentyfikują i zademonstrują wykorzystanie popularnych narzędzi i technologii służących do zapewnienia bezpieczeństwa. • Uczestnicy przeanalizują rzeczywiste przykłady i studia przypadków, aby zrozumieć praktyczne aspekty operacji bezpieczeństwa.	
Konwergencja bezpieczeństwa	Zrozumienie konwergencji bezpieczeństwa Podstawy bezpieczeństwa fizycznego (zasady bezpieczeństwa fizycznego, ochrona aktywów fizycznych, polityki) Typowe zagrożenia, przed którymi stoją małe i średnie przedsiębiorstwa Studia przypadków podkreślające kwestie konwergencji
Efekty kształcenia: • Uczestnicy zdefiniują konwergencję bezpieczeństwa i wyjaśnią jej znaczenie w integracji środków bezpieczeństwa fizycznego i cyberbezpieczeństwa. • Uczestnicy zastosują zasady bezpieczeństwa fizycznego w celu ochrony aktywów, obiektów i personelu. • Uczestnicy zidentyfikują i ocenią zagrożenia bezpieczeństwa, z którymi często borykają się małe i średnie przedsiębiorstwa (MŚP). • Uczestnicy przeanalizują studia przypadków, aby zrozumieć wpływ wyzwań związanych z konwergencją. • Uczestnicy przeanalizują procesy zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem.	
Zarządzanie informacjami i zdarzeniami związanymi z bezpieczeństwem	Przegląd zasad monitorowania bezpieczeństwa (w oparciu o moduł innych partnerów) Wdrażanie rozwiązań SIEM Konfiguracja logów i alertów Przegląd metodologii analizy zagrożeń i wykrywania (w oparciu o moduł innych partnerów)
Efekty uczenia się:	

• Uczestnicy szkolenia będą potrafili wyjaśnić zasady monitorowania bezpieczeństwa i ich zastosowanie w rozwiązaniach SIEM. • Uczestnicy skonfigurują i będą obsługiwać rozwiązania SIEM w celu skutecznego wykrywania zagrożeń i reagowania na nie. • Uczestnicy skonfigurują mechanizmy rejestrowania i alertów w narzędziach SIEM w celu monitorowania zdarzeń związanych z bezpieczeństwem. • Uczestnicy ocenią metody gromadzenia informacji o zagrożeniach i wykrywania zagrożeń pod kątem skutecznych działań związanych z bezpieczeństwem.	
Praktyki operacyjne w zakresie bezpieczeństwa	Zgodność z przepisami i regulacjami Strategie ciągłego doskonalenia w zakresie operacji bezpieczeństwa Automatyzacja i koordynacja Wskaźniki i raportowanie
Efekty kształcenia: • Uczestnicy wyjaśnią znaczenie zgodności i regulacji w działaniach związanych z bezpieczeństwem. • Uczestnicy kursu opracują i wdrożą strategie ciągłego doskonalenia działań związanych z bezpieczeństwem. • Uczestnicy wykorzystają automatyzację i koordynację w celu zwiększenia efektywności działań związanych z bezpieczeństwem. • Uczestnicy opracują i będą stosować wskaźniki bezpieczeństwa oraz techniki raportowania w celu przekazywania informacji o stanie bezpieczeństwa.	

Tabela6 -Moduł: 5

Jednostki	**Tematy**
Kontekst organizacyjny	Ewolucja cyberbezpieczeństwa w MŚP Obecne główne zagrożenia i słabe punkty Wpływ cyberbezpieczeństwa na strategię biznesową Szczególne wyzwania związane z cyberbezpieczeństwem w MŚP w porównaniu z dużymi przedsiębiorstwami Zrozumienie implikacji regulacyjnych praktyk w zakresie cyberbezpieczeństwa i ich zgodności ze strukturami zarządzania. Typowe wyzwania związane z cyberbezpieczeństwem charakterystyczne dla MŚP, takie jak ograniczone budżety, brak wyspecjalizowanego personelu ds. bezpieczeństwa oraz praktyczne metody ustalania priorytetów inwestycji w cyberbezpieczeństwo.
Efekty uczenia się: • Uczestnicy prześledzą rozwój praktyk w zakresie cyberbezpieczeństwa w małych i średnich przedsiębiorstwach. • Uczestnicy zidentyfikują i ocenią najbardziej krytyczne aktualne zagrożenia i słabe punkty mające wpływ na MŚP. • Uczestnicy przeanalizują wpływ cyberbezpieczeństwa na strategię biznesową i podejmowanie decyzji operacyjnych.	

• Uczestnicy porównają wyzwania związane z cyberbezpieczeństwem, przed którymi stoją MŚP, z wyzwaniami napotykanymi przez większe organizacje. • Uczestnicy kursu zinterpretują wymogi regulacyjne dotyczące cyberbezpieczeństwa i ocenią, w jaki sposób integrują się one z zarządzaniem organizacyjnym. • Uczestnicy kursu opiszą praktyczne rozwiązania typowych wyzwań związanych z cyberbezpieczeństwem w MŚP, takich jak ograniczenia budżetowe i ograniczona liczba pracowników.	
Prywatność	Zasady prywatności w cyberbezpieczeństwie Ochrona danych osobowych i RODO Wpływ prywatności na działalność MŚP Narzędzia i techniki ochrony prywatności
Efekty kształcenia: • Uczestnicy wyjaśnią podstawowe zasady prywatności w kontekście cyberbezpieczeństwa. • Uczestnicy zastosują wymogi RODO i ocenią ich wpływ na ochronę danych osobowych. • Uczestnicy ocenią, w jaki sposób przepisy dotyczące prywatności wpływają na codzienną działalność i modele biznesowe MŚP. • Uczestnicy będą korzystać z narzędzi i wdrażać techniki służące do zachowania prywatności i ochrony danych wrażliwych.	
Prawo, etyka i zgodność z przepisami	Organizacje, polityki i standardy dotyczące cyberbezpieczeństwa Odpowiednie przepisy krajowe i międzynarodowe Zgodność z przepisami w MŚP Etyka w cyberbezpieczeństwie Konsekwencje prawne nieprzestrzegania przepisów dotyczących cyberbezpieczeństwa Analiza sposobów wykorzystania narzędzi opartych na sztucznej inteligencji do wzmocnienia zarządzania cyberbezpieczeństwem i zapewnienia zgodności z przepisami poprzez ciągłe monitorowanie i zautomatyzowaną reakcję na zagrożenia.
Efekty uczenia się: • Uczestnicy szkolenia zidentyfikują kluczowe organizacje zajmujące się cyberbezpieczeństwem oraz ocenią odpowiednie ramy polityki i standardów. • Uczestnicy podsumują kluczowe przepisy prawne mające wpływ na cyberbezpieczeństwo na poziomie krajowym i międzynarodowym. • Uczestnicy opracują strategie mające na celu osiągnięcie i utrzymanie zgodności z przepisami w kontekście małych i średnich przedsiębiorstw. • Uczestnicy przeanalizują kwestie etyczne związane z podejmowaniem decyzji i zachowaniami w zakresie cyberbezpieczeństwa. • Uczestnicy ocenią konsekwencje prawne nieprzestrzegania przepisów dotyczących cyberbezpieczeństwa. • Uczestnicy kursu zbadają, w jaki sposób narzędzia sztucznej inteligencji mogą poprawić zarządzanie, zautomatyzować monitorowanie i zwiększyć zgodność z przepisami.	
Zarządzanie bezpieczeństwem	Struktura zarządzania cyberbezpieczeństwem Role i obowiązki w zarządzaniu bezpieczeństwem Modele dojrzałości cyberbezpieczeństwa

	Zwiększenie umiejętności przeprowadzania ocen ryzyka i formułowania strategicznych planów reagowania w symulowanych warunkach kryzysowych (oprogramowanie ransomware, ataki phishingowe itp.) Komunikacja na szczeblu kierowniczym i zarządu Strategie komunikacji w zakresie cyberbezpieczeństwa Raportowanie kwestii bezpieczeństwa kierownictwu wyższego szczebla Zarządzanie kryzysowe i komunikacja w zakresie cyberbezpieczeństwa Opanowanie umiejętności zarządzania kryzysowego i podejmowania decyzji w sytuacjach silnego stresu związanych z atakami opartymi na sztucznej inteligencji i oprogramowaniem ransomware.
Efekty kształcenia: • Uczestnicy kursu będą projektować i oceniać struktury zarządzania, które wspierają skuteczne zarządzanie cyberbezpieczeństwem. • Uczestnicy kursu przydzielą i wyjaśnią obowiązki w ramach organizacyjnych struktur bezpieczeństwa. • Uczestnicy ocenią dojrzałość cyberbezpieczeństwa przy użyciu ustalonych modeli. • Uczestnicy przeprowadzą ocenę ryzyka i opracują strategie reagowania na scenariusze takie jak oprogramowanie ransomware lub phishing. • Uczestnicy opracują plany komunikacji służące przekazywaniu informacji dotyczących cyberbezpieczeństwa kadrze kierowniczej wyższego szczebla i członkom zarządu. • Uczestnicy kursu sformułują skuteczne strategie komunikacyjne dla wewnętrznych i zewnętrznych interesariuszy zajmujących się cyberbezpieczeństwem. • Uczestnicy kursu będą tworzyć raporty informujące kierownictwo wyższego szczebla o wynikach i zagrożeniach związanych z cyberbezpieczeństwem. • Uczestnicy będą ćwiczyć zarządzanie i komunikację podczas kryzysów związanych z cyberbezpieczeństwem, w tym ataków opartych na sztucznej inteligencji.	
Polityka zarządzania	Wdrażanie i monitorowanie polityki
Efekty kształcenia: • Uczestnicy wdrożą politykę cyberbezpieczeństwa i ustalą procedury jej bieżącego monitorowania i egzekwowania.	

Tabela7 -Moduł: 6

Jednostki	**Tematy**
Wprowadzenie do planowania cyberbezpieczeństwa: bezpieczeństwo danych, ludzi i społeczeństwa	Bezpieczeństwo danych – bezpieczeństwo przechowywania informacji, proces dochodzeniowy Bezpieczeństwo danych – techniki ataków na hasła Bezpieczeństwo ludzi – świadomość i zrozumienie Bezpieczeństwo społeczne – czym jest cyberprzestępczość, cyberetyka

	Bezpieczeństwo społeczne – prawo cyberprzestrzeni – dowody cyfrowe, umowy cyfrowe, konwencje międzynarodowe (porozumienia)
Efekty kształcenia: • Uczestnicy wdrożą strategie zabezpieczania przechowywanych informacji i wspierania procesów dochodzeniowych. • Uczestnicy szkolenia będą identyfikować i analizować typowe techniki ataków na hasła oraz opracowywać odpowiednie środki zaradcze. • Uczestnicy będą promować świadomość w zakresie cyberbezpieczeństwa i wspierać zrozumienie wśród pracowników i interesariuszy. • Uczestnicy wyjaśnią społeczne konsekwencje cyberprzestępczości i ocenią kwestie etyczne w środowiskach cyfrowych. • Uczestnicy będą interpretować kluczowe pojęcia prawa cybernetycznego, w tym dowody cyfrowe, umowy i porozumienia międzynarodowe.	
Zarządzanie operacyjne i taktyczne	Wdrażanie kontroli dostępu Zarządzanie poprawkami i aktualizacjami oprogramowania Ciągłe monitorowanie systemu Szkolenia dla pracowników w zakresie świadomości bezpieczeństwa
Efekty kształcenia: • Uczestnicy kursu zaprojektują i wdrożą skuteczne mechanizmy kontroli dostępu w celu ochrony systemów i danych. • Uczestnicy ustalą procedury terminowego zarządzania poprawkami i aktualizacjami oprogramowania w celu zmniejszenia podatności na zagrożenia. • Uczestnicy będą prowadzić ciągłe monitorowanie systemów w celu wykrywania zdarzeń związanych z bezpieczeństwem i reagowania na nie. • Uczestnicy opracują i przeprowadzą szkolenia z zakresu świadomości bezpieczeństwa, aby zwiększyć zaangażowanie pracowników i zmniejszyć ryzyko związane z czynnikiem ludzkim.	

Tabela8 -Moduł: 7

Jednostki	**Tematy**
Ocena ryzyka	Ogólne ramy i proces zarządzania ryzykiem Zasady zarządzania ryzykiem Standardy zarządzania ryzykiem Praktyczne przykłady i studia przypadków
Efekty kształcenia: • Uczestnicy szkolenia będą potrafili opisać i zastosować ogólne ramy i proces zarządzania ryzykiem w zakresie cyberbezpieczeństwa. • Uczestnicy wyjaśnią podstawowe zasady skutecznego zarządzania ryzykiem w zakresie cyberbezpieczeństwa. • Uczestnicy szkolenia będą identyfikować i interpretować powszechnie przyjęte standardy zarządzania ryzykiem. • Uczestnicy ocenią scenariusze ryzyka na podstawie rzeczywistych przykładów i studiów przypadków.	
Identyfikacja ryzyka	Materialne i niematerialne źródła ryzyka Przyczyny i zdarzenia Zagrożenia i możliwości Słabe punkty i możliwości Zmiany w kontekście zewnętrznym i wewnętrznym Wskaźniki pojawiających się ryzyk Charakter i wartość aktywów i zasobów Konsekwencje i ich wpływ na cele Ograniczenia wiedzy i wiarygodności informacji Uprzedzenia, założenia i przekonania osób zaangażowanych. Praktyczne przykłady i studia przypadków.
Efekty uczenia się: • Uczestnicy nauczą się rozróżniać między namacalnymi i niematerialnymi źródłami ryzyka w środowiskach cyberbezpieczeństwa. • Uczestnicy szkolenia będą identyfikować przyczyny ryzyka i zdarzenia wywołujące ryzyko. • Uczestnicy przeanalizują zagrożenia dla cyberbezpieczeństwa i ocenią potencjalne możliwości poprawy. • Uczestnicy ocenią słabe punkty i możliwości organizacyjne w zakresie zarządzania ryzykiem. • Uczestnicy kursu będą oceniać, w jaki sposób zmiany kontekstowe wpływają na ryzyko związane z cyberbezpieczeństwem. • Uczestnicy szkolenia będą identyfikować wskaźniki sygnalizujące pojawienie się nowych zagrożeń dla cyberbezpieczeństwa. • Uczestnicy ocenią wartość aktywów i krytyczność zasobów w odniesieniu do ryzyka. • Uczestnicy kursu oszacują potencjalne konsekwencje i ich wpływ na cele strategiczne. • Uczestnicy szkolenia rozpoznają ograniczenia informacji i wiedzy w procesie identyfikacji ryzyka. • Uczestnicy zastanowią się nad tym, jak czynniki ludzkie wpływają na postrzeganie i identyfikację ryzyka.	

• Uczestnicy szkolenia zastosują techniki identyfikacji w rzeczywistych scenariuszach.	
Zagrożenia wewnętrzne	Definicja i rodzaje zagrożeń wewnętrznych Wykrywanie i identyfikowanie zagrożeń wewnętrznych Praktyczne przykłady i studia przypadków
Efekty kształcenia: • Uczestnicy zdefiniują zagrożenia wewnętrzne i sklasyfikują ich różne rodzaje. • Uczestnicy zdobędą umiejętności wykrywania i reagowania na oznaki zagrożeń wewnętrznych. • Uczestnicy przeanalizują studia przypadków rzeczywistych incydentów związanych z zagrożeniami wewnętrznymi.	
Modele i metodologie pomiaru i oceny ryzyka	Modele i metodologie ilościowej i jakościowej oceny ryzyka Prawdopodobieństwo wystąpienia zdarzeń i ich konsekwencje Charakter i skala konsekwencji Poziomy wrażliwości i pewności. Praktyczne przykłady i studia przypadków
Efekty uczenia się: • Uczestnicy porównają i zastosują modele ilościowe i jakościowe w ocenie ryzyka związanego z cyberbezpieczeństwem. • Uczestnicy ocenią prawdopodobieństwo wystąpienia zidentyfikowanych zagrożeń oraz potencjalne skutki ich wystąpienia. • Uczestnicy ocenią powagę i zakres konsekwencji związanych z ryzykiem cyberbezpieczeństwa. • Uczestnicy określą poziomy niepewności i pewności w ocenie ryzyka. • Uczestnicy wdrożą modele oceny ryzyka w praktycznych scenariuszach.	
Kontrola ryzyka	Monitorowanie i przegląd Rejestrowanie i raportowanie Praktyczne przykłady i studia przypadków
Efekty uczenia się: • Uczestnicy będą regularnie monitorować ryzyko i przeprowadzać procesy przeglądu. • Uczestnicy będą skutecznie dokumentować i raportować środki kontroli ryzyka. • Uczestnicy będą analizować rzeczywiste przykłady, aby zrozumieć skuteczne wdrażanie kontroli ryzyka.	

Tabela9 -Moduł: 8

Jednostki	**Tematy**
Reagowanie na incydenty	Definicja i znaczenie reagowania na incydenty Kluczowe elementy skutecznego planu reagowania na incydenty Typowe zagrożenia dla cyberbezpieczeństwa
Efekty kształcenia: • Uczestnicy zdefiniują reagowanie na incydenty i wyjaśnią jego znaczenie w zarządzaniu cyberbezpieczeństwem. • Uczestnicy zidentyfikują i wdrożą kluczowe elementy ustrukturyzowanego planu reagowania na incydenty i przywracania sprawności.	

• Uczestnicy rozpoznają typowe zagrożenia dla cyberbezpieczeństwa występujące podczas obsługi incydentów i nauczą się na nie reagować.	
Odzyskiwanie danych po awarii	Zrozumienie odzyskiwania danych po awarii Role i obowiązki w odzyskiwaniu po awarii Kroki przywracania sprawności po awarii
Efekty kształcenia: • Uczestnicy szkolenia wyjaśnią zasady i cele odzyskiwania danych po awarii w kontekście cyberbezpieczeństwa. • Uczestnicy opiszą role i obowiązki członków zespołu zaangażowanych w odzyskiwanie danych po awarii. • Uczestnicy opracują szczegółowy plan przywrócenia systemów i operacji po cyberkatastrofie.	
Ciągłość działania	Zrozumienie ciągłości działania Role i obowiązki w zakresie ciągłości działania Analiza wpływu na działalność
Efekty kształcenia: • Uczestnicy wyjaśnią koncepcję i znaczenie planowania ciągłości działania. • Uczestnicy określą role i obowiązki związane z zapewnieniem ciągłości działania. • Uczestnicy przeprowadzą analizę wpływu na działalność w celu oceny krytycznych funkcji i zależności.	
Świadomość bezpieczeństwa, szkolenia i edukacja	Zrozumienie świadomości bezpieczeństwa Obowiązki pracowników w zakresie cyberbezpieczeństwa
Efekty uczenia się: • Uczestnicy wyjaśnią rolę świadomości bezpieczeństwa w ograniczaniu ryzyka związanego z cyberbezpieczeństwem wynikającego z czynnika ludzkiego. • Uczestnicy szkolenia poznają obowiązki pracowników w zakresie przestrzegania protokołów i najlepszych praktyk dotyczących cyberbezpieczeństwa.	
Praktyki zatrudniania w zakresie bezpieczeństwa	Określanie wymagań dotyczących ról związanych z bezpieczeństwem Przeprowadzanie kompleksowej weryfikacji kandydatów
Efekty uczenia się: • Uczestnicy szkolenia zdefiniują role związane z cyberbezpieczeństwem i sformułują odpowiednie wymagania. • Uczestnicy zastosują najlepsze praktyki w zakresie przeprowadzania weryfikacji przeszłości kandydatów ubiegających się o stanowiska związane z bezpieczeństwem.	
Praktyki dotyczące zakończenia zatrudnienia w obszarze bezpieczeństwa	Natychmiastowe cofnięcie dostępu Powiadomienie odpowiednich zespołów Kwestie prawne i zgodność z przepisami
Efekty uczenia się: • Uczestnicy szkolenia wdrożą procedury natychmiastowego cofania dostępu po zakończeniu zatrudnienia pracownika. • Uczestnicy będą koordynować komunikację z odpowiednimi działami podczas procesu odejścia pracownika.	

• Uczestnicy szkolenia zapoznają się z wymogami prawnymi i zgodnością z przepisami dotyczącymi zakończenia zatrudnienia w obszarze cyberbezpieczeństwa.	
Bezpieczeństwo stron trzecich	Ocena ryzyka związanego z podmiotami zewnętrznymi Wdrażanie kontrastów i wymagań bezpieczeństwa Bieżące monitorowanie i audyt Reagowanie na incydenty i komunikacja
Efekty uczenia się: • Uczestnicy ocenią ryzyko związane z bezpieczeństwem związane z zewnętrznymi dostawcami i partnerami. • Uczestnicy kursu będą projektować i stosować klauzule umowne w celu zapewnienia zgodności z wymogami bezpieczeństwa stron trzecich. • Uczestnicy szkolenia ustanowią praktyki ciągłego monitorowania i audytu bezpieczeństwa stron trzecich. • Uczestnicy będą koordynować działania z podmiotami zewnętrznymi podczas reagowania na incydenty.	
Bezpieczeństwo w procesach przeglądu	Włączanie bezpieczeństwa do przeglądów Ocena podatności i testy penetracyjne Przeglądy po incydentach
Efekty uczenia się: • Uczestnicy szkolenia będą uwzględniać kwestie bezpieczeństwa w procesach przeglądu organizacyjnego. • Uczestnicy przeprowadzą ocenę podatności i testy penetracyjne w ramach działań przeglądowych. • Uczestnicy będą przeprowadzać przeglądy po incydentach w celu oceny skuteczności i poprawy przyszłych reakcji.	
Kwestia szczególna dotycząca prywatności danych osobowych pracowników	Ograniczenia dotyczące gromadzenia danych Przechowywanie i kontrola dostępu Zgodność z przepisami dotyczącymi prywatności Udostępnianie danych i strony trzecie Zgoda i prawa pracowników
Efekty kształcenia: • Uczestnicy szkolenia nauczą się określać odpowiednie granice gromadzenia danych osobowych pracowników. • Uczestnicy zastosują środki bezpiecznego przechowywania i kontroli dostępu do wrażliwych danych pracowników. • Uczestnicy zapewnią zgodność z odpowiednimi przepisami dotyczącymi prywatności, takimi jak RODO. • Uczestnicy ocenią ryzyko i zasady dotyczące udostępniania danych pracowników stronom trzecim. • Uczestnicy zrozumieją prawa pracowników i znaczenie uzyskania świadomej zgody.	

WNIOSKI

Niniejszy raport przedstawia program nauczania odpowiedni dla poziomu kształcenia zawodowego, który należy wziąć pod uwagę w celu pomyślnego wdrożenia szkolenia CyberAgent. W oparciu o badania przeprowadzone od początku projektu w celu określenia potrzeb szkoleniowych, niniejszy dokument opisuje potrzeby uczniów szkół zawodowych w zakresie ich udziału w szkoleniu.

Podczas przygotowywania programu za punkt odniesienia przyjęto program nauczania przygotowany dla projektu CyberAgent na poziomie 6 EQF. Z programu nauczania na tym poziomie wybrano tematy odpowiednie dla poziomu 4 EQF, a te, które nie były odpowiednie, zostały usunięte.

Wreszcie, aby zapewnić najwyższą jakość szkolenia pod względem treści, organizacji i rozwoju umiejętności, pytania związane z tematami, które nie zostały przeniesione z poziomu 6 EQF, nie zostaną uwzględnione w fazie oceny i ewaluacji.

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