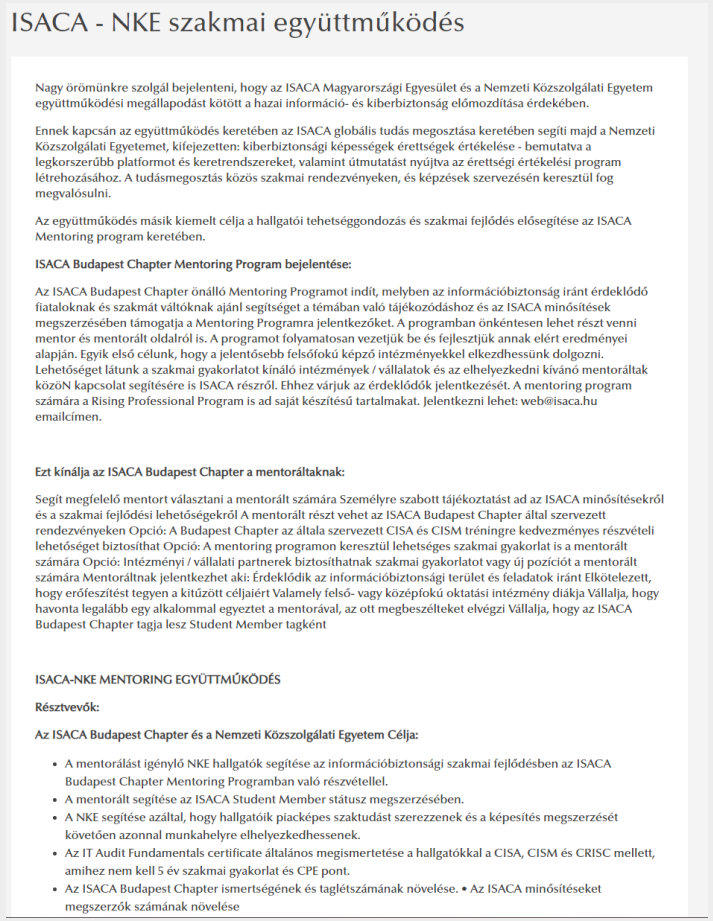
Mentorokat keresünk!



ISACA - NKE szakmai együttműködés

Nagy örömünkre szolgál bejelenteni, hogy az ISACA Magyarországi Egyesület és a Nemzeti Közszolgálati Egyetem együttműködési megállapodást kötött a hazai információ- és kiberbiztonság előmozdítása érdekében.

Ennek kapcsán az együttműködés keretében az ISACA globális tudás megosztása keretében segíti majd a Nemzeti Közszolgálati Egyetemet, kifejezetten: kiberbiztonsági képességek érettségek értékelése - bemutatva a legkorszerűbb platformot és keretrendszereket, valamint útmutatást nyújtva az érettségi értékelési program létrehozásához. A tudásmegosztás közös szakmai rendezvényeken, és képzések szervezésén keresztül fog megvalósulni.

Az együttműködés másik kiemelt célja a hallgatói tehetséggondozás és szakmai fejlődés elősegítése az ISACA Mentoring program keretében.

ISACA Budapest Chapter Mentoring Program bejelentése:

Az ISACA Budapest Chapter önálló Mentoring Programot indít, melyben az információbiztonság iránt érdeklődő fiataloknak és szakmát váltóknak ajánl segítséget a témában való tájékozódáshoz és az ISACA minősítések megszerzésében támogatja a Mentoring Programra jelentkezőket. A programban önkéntesen lehet részt venni mentor és mentorált oldalról is. A programot folyamatosan vezetjük be és fejlesztjük annak elért eredményei alapján. Egyik első célunk, hogy a jelentősebb felsőfokú képző intézményekkel elkezdhessünk dolgozni. Lehetőséget látunk a szakmai gyakorlatot kínáló intézmények / vállalatok és az elhelyezkedni kívánó mentoráltak közöN kapcsolat segítésére is ISACA részről. Ehhez várjuk az érdeklődők jelentkezését. A mentoring program számára a Rising Professional Program is ad saját készítésű tartalmakat. Jelentkezni lehet: web@isaca.hu emailcímen.

Ezt kínálja az ISACA Budapest Chapter a mentoráltaknak:

Segít megfelelő mentort választani a mentorált számára Személyre szabott tájékoztatást ad az ISACA minősítésekről és a szakmai fejlődési lehetőségekről A mentorált részt vehet az ISACA Budapest Chapter által szervezett rendezvényeken Opció: A Budapest Chapter az általa szervezett CISA és CISM tréningre kedvezményes részvételi lehetőséget biztosíthat Opció: A mentoring programon keresztül lehetséges szakmai gyakorlat is a mentorált számára Opció: Intézményi / vállalati partnerek biztosíthatnak szakmai gyakorlatot vagy új pozíciót a mentorált számára Mentoráltnak jelentkezhet aki: Érdeklődik az információbiztonsági terület és feladatok iránt Elkötelezett, hogy erőfeszítést tegyen a kitűzött céljaiért Valamely felső- vagy középfokú oktatási intézmény diákja Vállalja, hogy havonta legalább egy alkalommal egyeztet a mentorával, az ott megbeszélteket elvégzi Vállalja, hogy az ISACA Budapest Chapter tagja lesz Student Member tagként

ISACA-NKE MENTORING EGYÜTTMŰKÖDÉS

Résztvevők:

Az ISACA Budapest Chapter és a Nemzeti Közszolgálati Egyetem Célja:

- A mentorálást igénylő NKE hallgatók segítése az információbiztonsági szakmai fejlődésben az ISACA Budapest Chapter Mentoring Programban való részvétellel.
- A mentorált segítése az ISACA Student Member státusz megszerzésében.
- A NKE segítése azáltal, hogy hallgatóik piacképes szaktudást szerezzenek és a képesítés megszerzését követően azonnal munkahelyre elhelyezkedhessenek.
- Az IT Audit Fundamentals certificate általános megismertetése a hallgatókkal a CISA, CISM és CRISC mellett, amihez nem kell 5 év szakmai gyakorlat és CPE pont.
- Az ISACA Budapest Chapter ismertségének és taglétszámának növelése. • Az ISACA minősítéseket megszerzők számának növelése

1. A kurzus címe, témája, óraszáma:

Nappali: Kiberbiztonsági akkreditáció és tanúsítás, 28 óra

Levelező: Kiberbiztonsági akkreditáció és tanúsítás, 8 óra

2. Általános oktatási, képzési, nevelési célok:

Milyen oktatási célok elérésére törekszik majd a kurzus során? Mi a célja a kurzussal?

A kurzus célja az NKE kiberbiztonsági mesterképzésének kiegészítése gyakorlati ismeretekkel, melynek során a hallgatók külső mentorok segítségével mélyednek el azoknak a szabványoknak és jogszabályoknak az alkalmazásában, melyet a képzés során elméletben megismerne. További cél az Intézményfejlesztési Tervvel összhangban olyan kurzus indítása, mely közvetlenül hozzájárul a hallgatók jövőbeni elhelyezkedésének elősegítéséhez, a csoportmunkában való munka elsajátításához. A kurzus végrehajtása során kihasználjuk azokat az együttműködési megállapodásokat, melyeket a korábbi években az NKE kötött, így különösen a Nemzeti Akkreditáló Hatóság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az ISACA Magyarország bevonására, emellett megszólítjuk a Szabályozott Tevékenységek Felügyeleti Hatóságát is. Ezen szervezetek előadásokkal, mentorokkal segítik a kiberbiztonsági akkreditáció és tanúsítás gyakorlati megismerését.

Milyen képzési eredmények várhatók a kurzus végére feladatok elérésére törekszik (minimum, optimum) a kurzus végére?

Minimum: A hallgatók egy életszerű auditban való csoportos részvétellel megismerik az akkreditálás és tanúsítás gyakorlati folyamatát, valamint a releváns szabályozókat.

Optimum: A hallgatók egy életszerű auditban való csoportos részvétellel megismerik az akkreditálás és tanúsítás gyakorlati folyamatát, valamint a releváns szabályozókat, illetve képesek önállóan elkészíteni az auditálást támogató dokumentációt.

NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Az Európai Kiberbiztonsági Készség-keretrendszer bemutatása

Legárd Ildikó nyomán Dr. Krasznay Csaba

2022.

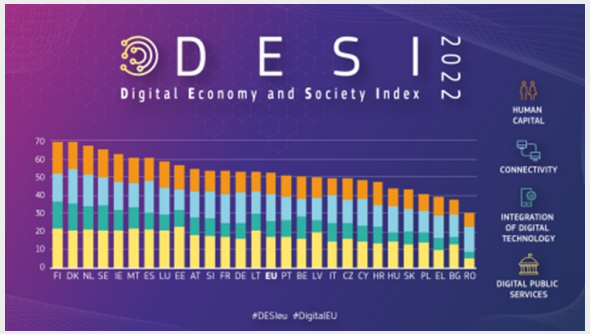
FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

ISACA®
Budapest Chapter

Kiberbiztonsági szakemberhiány



European Economic and Social Committee

Digitális Gazdasági és Társadalmi Index (DESI) 2022:

- 2021-ben 8,9 millió személy dolgozott IKT-szakemberként az Európai Unióban (teljes munkaerőpiac 4,5 %-a);
- az IKT-szakemberek aránya lassan növekszik (2020-ban az összes foglalkoztatott 4,3%-a);
- 2030-ra 20 millió foglalkoztatott IKT-szakértő elérése a cél az EU-ban;
- jelentősen javítani kell a képzési- és karrierlehetőségeken.

Az EU kiberbiztonsági stratégiája a digitális évtizedre (2021):

- figyelmeztet a kiberbiztonsági szakemberek hiányának veszélyeire
- uniós szintű kiberbiztonsági pályafutási eszközt javasol

↓

- ismeretek, készségek és képességek, amelyekre szükség van a kiberbiztonsági pálya elkezdéséhez vagy fejlesztéséhez

European Cybersecurity Skills Framework

Az Európai Kiberbiztonsági Készség-keretrendszer

A létező keretrendszerek

- összeegyeztethetetlenek lehetnek;
- nem mindig igazodnak az EU igényeihez, jogszabályaihoz;
- magas szintű komplexitással rendelkeznek;
- nem foglalkoznak a megjelölt problémával.

„Közös nyelv kialakítása”

- meg kell teremteni a kiberbiztonsági szerepek, kompetenciák, készségek és ismeretek közös nyelvét, megértését;
- elő kell segíteni a kiberbiztonsági készségek azonosítását;
- támogatni kell a kiberbiztonsághoz kapcsolódó képzési programok tervezését.

Keretrendszer

Olyan keretrendszer kialakítása a cél, amely:

- szilárd,
- könnyű a használata,
- bővíthető,
- elérhető,
- interoperábilis,
- szektorokon átívelő,
- megfelelő az EU szervezeti számára.

Az ECSF céljai, használatának fő előnyei

A kiberbiztonsággal kapcsolatos **közös terminológia és közös értelmezés** biztosítása a szakemberek számára az EU-ban.

A kiberbiztonsági munkakörökhöz kapcsolódó **kritikus készségek** meghatározása, mely biztosítja a készségek további fejlesztését is.

A kiberbiztonsági **oktatás, képzés és munkaerő-fejlesztési programok** harmonizációjának elősegítsége.

Az európai kiberbiztonsági munkaerő kapacitásépítésén keresztül hozzájárul a kibertámadásokkal szembeni jobb **ellenállóképesség** eléréséhez.

Célcsoport meghatározása

Döntéshozók

Szervezeti vezetők

Piackutatók

HR

Kiberbiztonság iránt érdeklődők (nem szakemberek)

Kiberbiztonsági szakemberek

Képzési szolgáltatók (Köz- és magánszféra)

Új szervezeti belépők

AD-HOC Munkacsoport

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Feladata, hogy **tanácsot adjon**, valamint **segítse az ENISA-t** egy **Európai Kiberbiztonsági Készség-Keretrendszer kidolgozásában**.

17
Experts

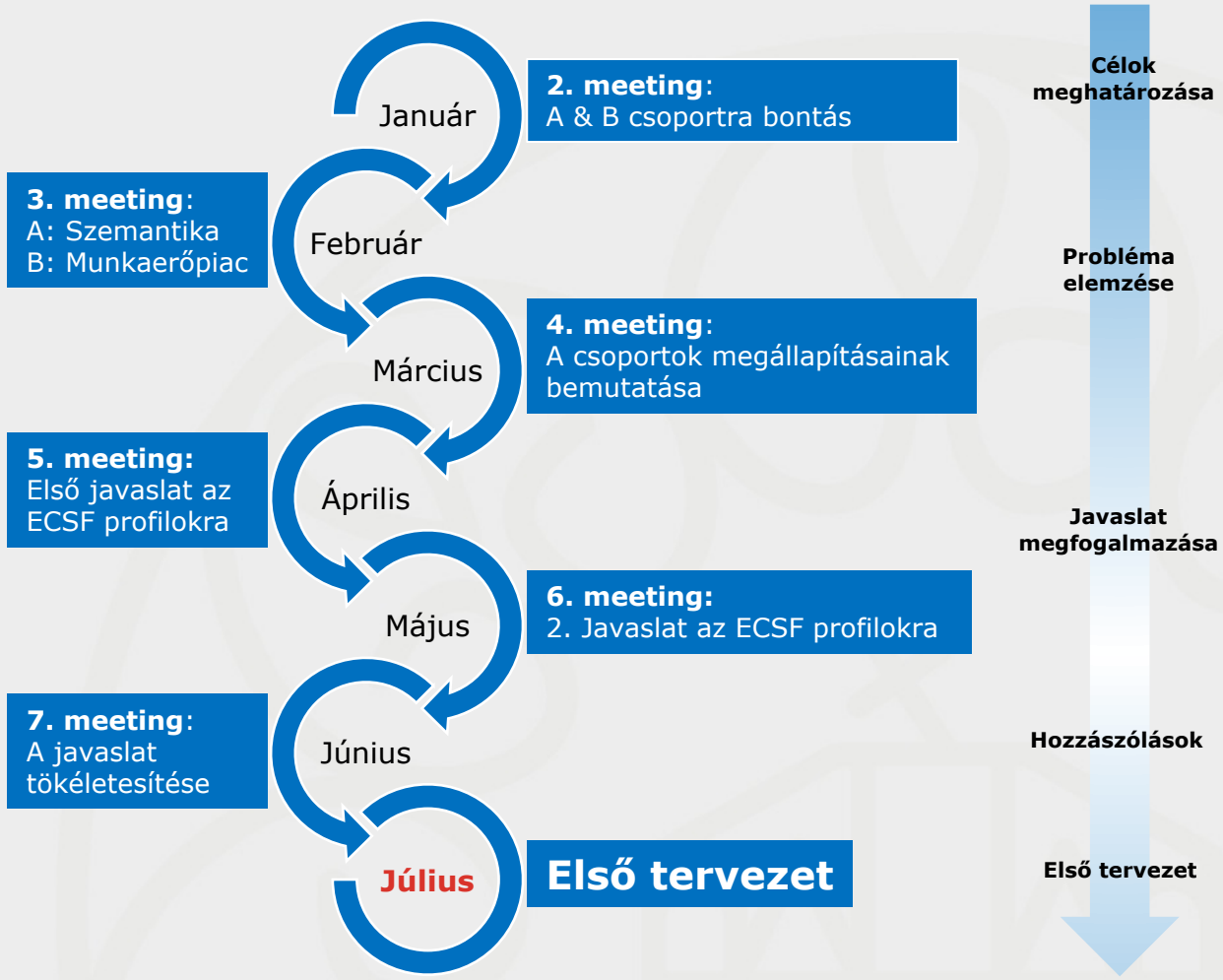
14
Countries

Dec 2020
Started

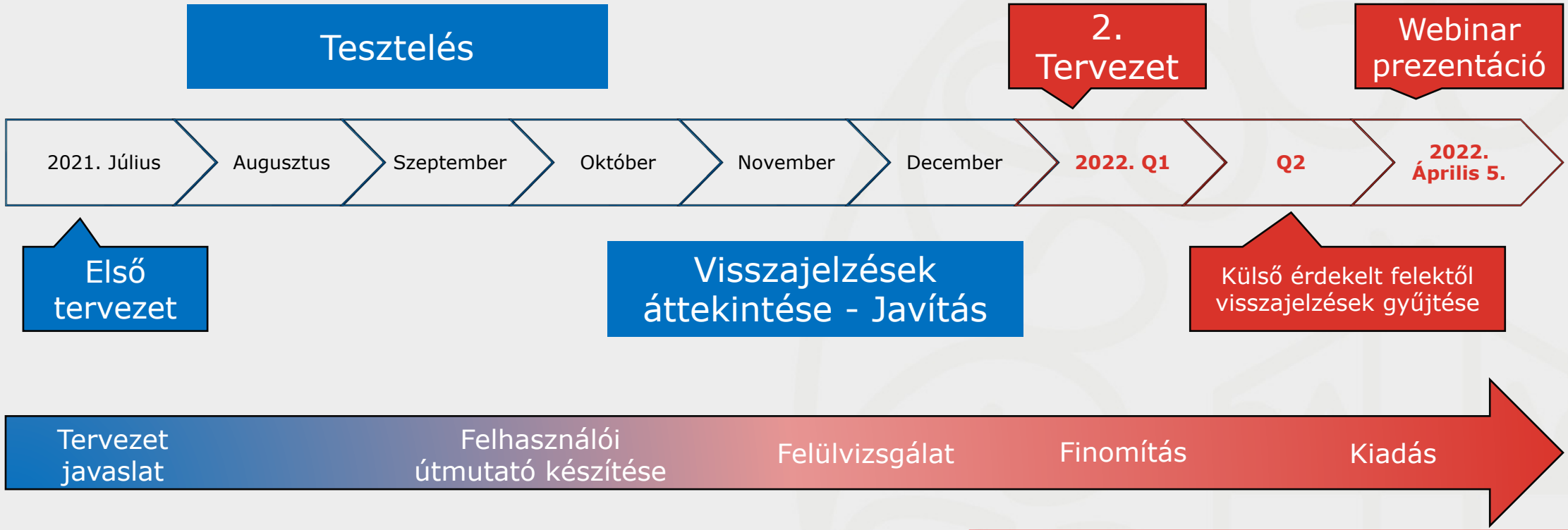
ECSF ad hoc munkacsoport tagjai, működés

First Name	Surname	Affiliation
Agata	BEKIER	Dow
Vladlena	BENSON	Cyber Security Innovation Partnership Aston University
Jutta	BREYER	Breyer publico consulting and CEN expert contracting
Sara	GARCIA	INCIBE - Spanish National Cybersecurity Institute
Markku	KORKIAKOSK	Netox Ltd
Csaba	KRASZNAY	National University of Public Service
Haralambos	MOURATIDIS	Stockholm University and University of Brighton
Christina	GEORGHIADOU	Eurobank Cyprus
Erwin	ORYE	NATO CCDCOE
Edmundas	PIESARSKAS	L3CE
Nineta	POLEMI	University of Pireaus
Paresh	RATHOD	Laurea University of Applied Sciences Finland
Antonio	SANNINO	Procter Gamble
Fred	VAN NOORD	Van Noord Consultancy
Richard	WIDH	Ancautus AB

2020. december alakuló ülés
2021



Következő lépések 2021 július-2022. szeptember



ECSF publikálása: 2022. Szeptember 19.

Probléma elemzése

A létező keretrendszerek, taxonómiák és tudományos irodalom alapján

Munkaerő-piaci trendek és igények elemzése piaci adatelemzés alapján

Tudás azonosítása strukturált megközelítéssel (a meglévő tudásosztályok alkalmazásával)

Kulcsfontosságú kiberbiztonsági készségek azonosítása a piaci igények alapján, amelyek összekapcsolhatók:

- a szakmai profilokkal, illetve
- a kompetenciákkal.

Tipikus kiberbiztonsági szakmai profilok meghatározása a piaci igények alapján:

- a profilhoz kapcsolható kulcselemek leírásával (a profil alternatív elnevezése, összefoglaló megállapítások, küldetés, tipikus feladatok, kulcskompetenciák, e-CF kompetenciák),
- a választott részletezettségi szinten azonosítva (ESCF jelenleg: 12 szint)

ECSF profilok

Forrás: User Manuel – European Cybersecurity Skills Framework (ECSF), 2022.09.19.

Profil elnevezések

1. Chief Information Security Officer (CISO)

- Cybersecurity Programme Director
- Information Security Officer (ISO)
- Information Security Manager
- Head of Information Security
- IT/ICT Security Officer

2. Cyber Incident Responder

- Cyber Incident Handler
- Cyber Crisis Expert
- Incident Response Engineer
- Security Operations Center (SOC) Analyst
- Cyber Fighter / Defender
- Security Operation Analyst (SOC Analyst)
- Cybersecurity SIEM Manager

3. Cyber Legal, Policy and Compliance Officer

- Data Protection Officer (DPO)
- Privacy Protection Officer
- Cyber Law Consultant
- Cyber Legal Advisor
- Information Governance Officer
- Data Compliance Officer
- Cybersecurity Legal Officer
- IT/ICT Compliance Manager
- Governance Risk and Compliance (GRC) Consultant

4. Cyber Threat Intelligence Specialist

- Cyber Intelligence Analyst
- Cyber Threat Modeller

5. Cybersecurity Architect

- Cybersecurity Solutions Architect
- Cybersecurity Designer
- Data Security Arcitect

6. Cybersecurity Auditor

- Information Security Auditor (IT os Legal Auditor)
- Governance Risk Compliance (GRC) Auditor
- Cybersecurity Audit Manager
- Cybersecurity Procedures and Processes Auditor
- Information Security Risk and Compliance Auditor
- Data Protection Assessment Analyst

Profil elnevezések

7. Cybersecurity Educator

- Cybersecurity Awareness Specialist
- Cybersecurity Trainer
- Faculty in Cybersecurity (Professor, Lecturer)

8. Cybersecurity Implementer

- Information Security Implementer
- Cybersecurity Solutions Expert
- Cybersecurity Developer
- Cybersecurity Engineer
- Development, Security & Operations (DevSecOps) Engineer

9. Cybersecurity Researcher

- Cybersecurity Research Engineer
- Cheif Researc Officer (CRO) in cybersecurity
- Senior Research Officer in cybersec.
- Research and Development (R&D) Officer in cybersec.
- Scientific Staff in cybersec.
- Research and Innovation Officer/Expert in cybersec.
- Research Fellow in cybersec.

10. Cybersecurity Risk Manager

- Information Security Risk Analyst
- Cybersecurity Risk Assurance Consultant
- Cybersecurity Risk Assessor
- Cybersecurity Impact Alanyst
- Cyber Risk Manager

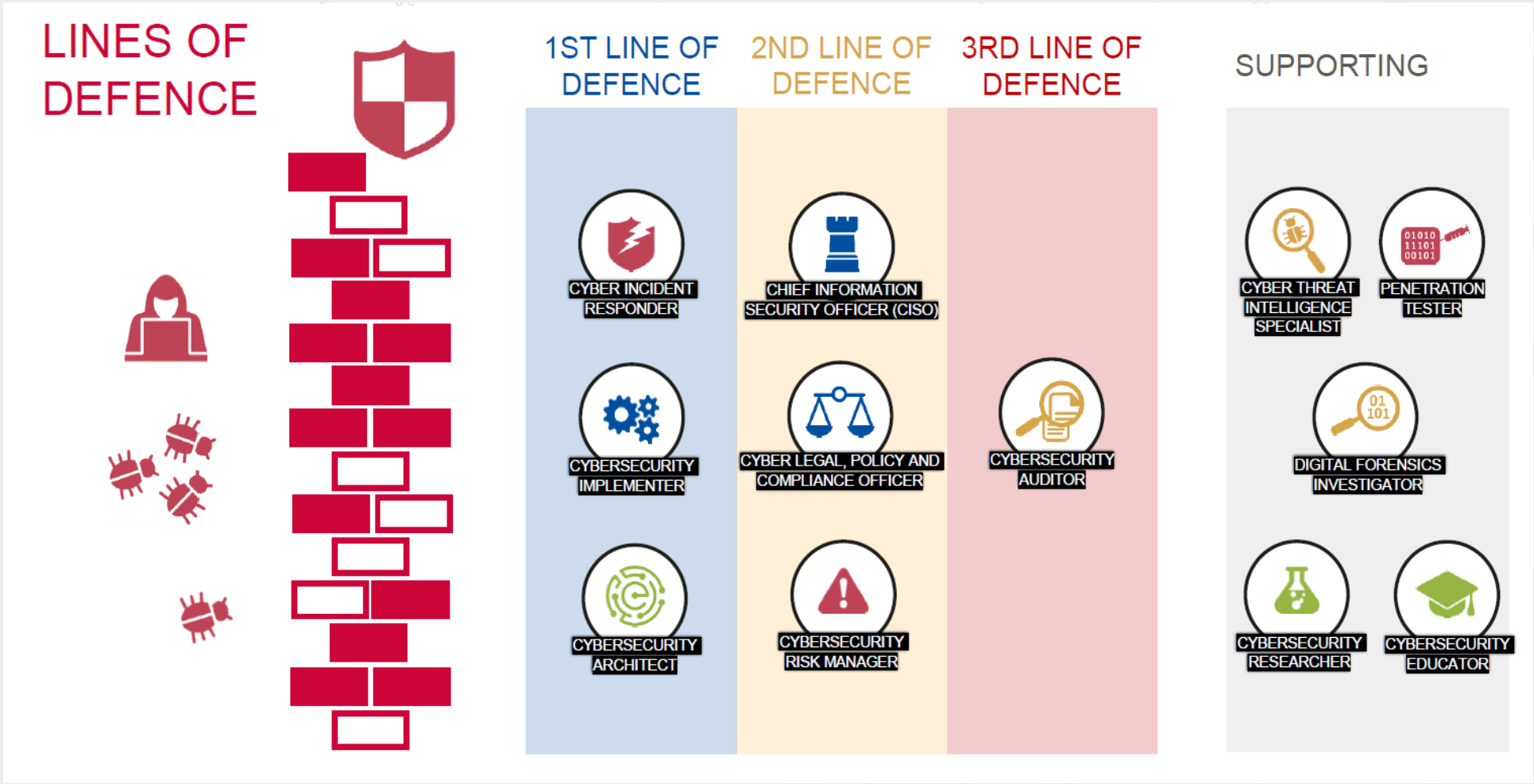
11. Digital Forensics Investigator

- Digital Forensics Analyst
- Cybersecurity & Forensic Specialist
- Computer Forensics Consultant

12. Penetration Tester

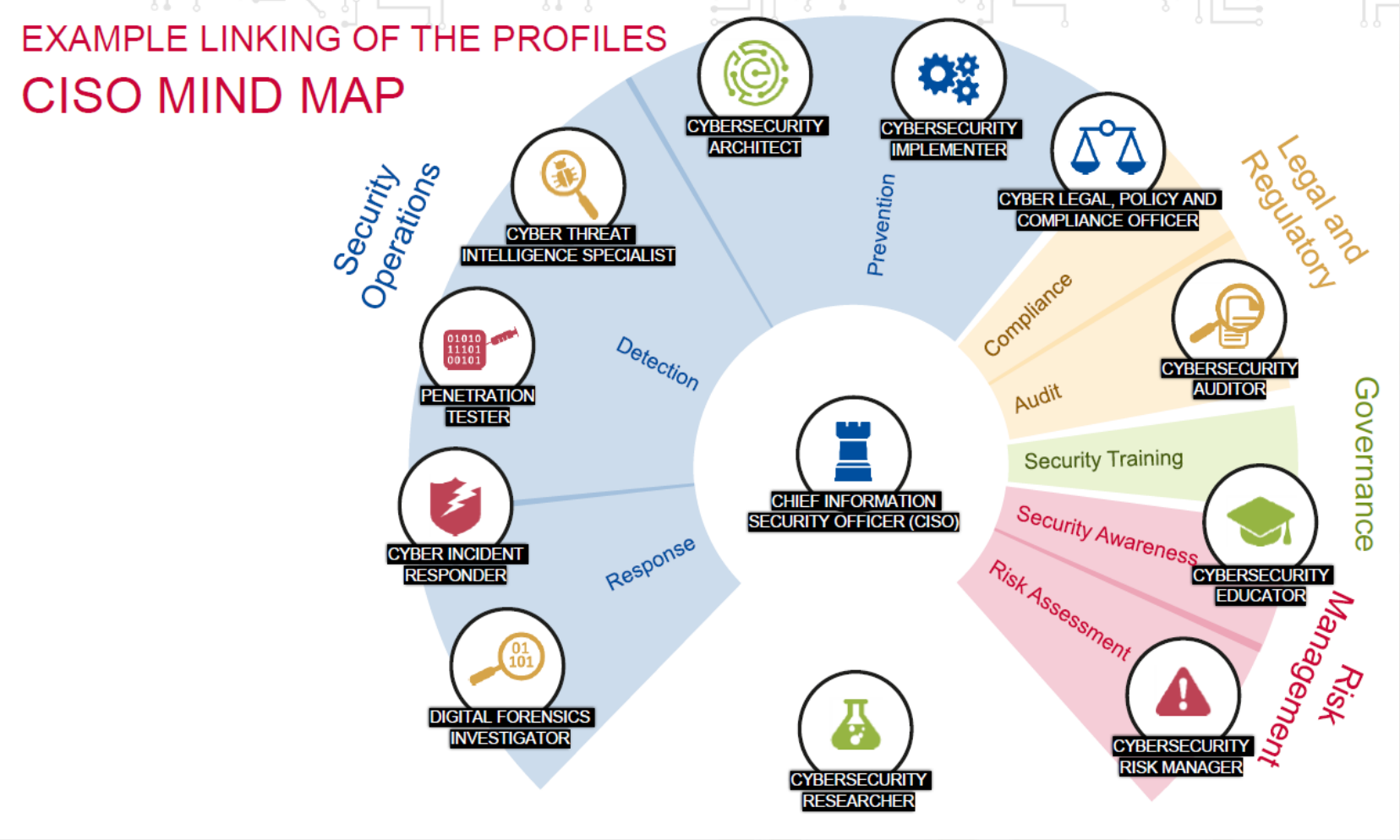
- Pentester
- Ethical Hacker
- Vulnerability Analyst
- Cybersecurity Tester
- Offensive Cybersecurity Expert
- Defensive Cybersecurity Expert
- Red Team Expert
- Red Teamer

A profilok kategorizálása



Forrás: ENISA – European Cybersecurity Skills Framework, Webinar presentation – 3. Cybersecurity Profiles, 2022.04.05.

A profilok kapcsolata



Forrás: ENISA – European Cybersecurity Skills Framework, Webinar presentation – 3. Cybersecurity Profiles, 2022.04.05.

A szakmai profilok felépítése

Profil címe	A szakmai szerepprofil neve
Alternatív elnevezés	A szakmai szerepprofil alternatív elnevezései.
Összegzés	A szerepkör fő célkitűzései.
Küldetés	A szerepkör legfőbb elemeinek bemutatása.
Eredménytermékek	A szerepkör tipikus eredményeinek listája, amely a profil relevanciáját is magyarázza egy nem szakértő számára.
Fő feladatok	A szerepkörhöz kapcsolódó fő feladatok felsorolása.
Kulcs készségek	A szerepkör munkafeladataihoz kapcsolódó és ellátásukhoz szükséges képességek felsorolása. A puha készségek (pl. kommunikáció, időgazdálkodás, együttműködési képesség) és az etika alapelvei is néhány esetben kifejezetten megjelennek a profilokban.
Kulcs ismeretek	A munkakörhöz tartozó feladatok elvégzéséhez, valamint a szerepkör betöltéséhez szükséges alapvető ismeretek listája.
E-kompetenciák	Az EN16234-1 e-kompetencia keretrendszer (e-CF) alapján kerül meghatározásra. (Közös európai keretrendszer az IKT-szakemberek számára minden ágazatban.)

A szakmai profilok felépítése

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s)	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources
Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans

enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)
SEPTEMBER 2022

	• Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people	
Key knowledge	• Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements • Cybersecurity maturity models • Cybersecurity procedures • Resource management • Management practices • Risk management standards, methodologies and frameworks	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring D.1. Information Security Strategy Development E.3. Risk Management E.8. Information Security Management E.9. IS-Governance	Level 4 Level 5 Level 4 Level 4 Level 5

Forrás: ECSF – European Cybersecurity Skills Framework, 2022.09.19.

Az ECSF használata

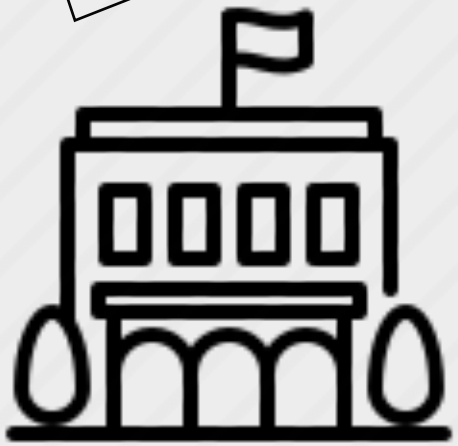
A különböző érdekelt felek igényei alapján **moduláris és rugalmas** módon alkalmazható.

A konkrét felhasználás és a **gyakorlati alkalmazás** számos tényezőtől, például a piaci perspektívától, a szervezet méretétől, az adott teljesítmény kontextusától és az általános céltól is függ.

Az ECSF által a **kiberbiztonsági szakemberek** számára meghatározott 12 szerepprofil **rugalmas eszközt és szabványos európai referenciakeret** szerinti megoldást biztosít az adott kontextusban történő testreszabott használathoz.

Az ECSF használatának előnyei

Keresünk egy információbiztonsági felelőst!



Szervezetek

Milyen készségekre van szüksége a jelöltünknek?

Információbiztonsági felelősöket képzünk!

Képzést nyújtó szervezetek

Mit kellene tartalmaznia a tananyagnak?

Információbiztonsági felelős szeretnék lenni!

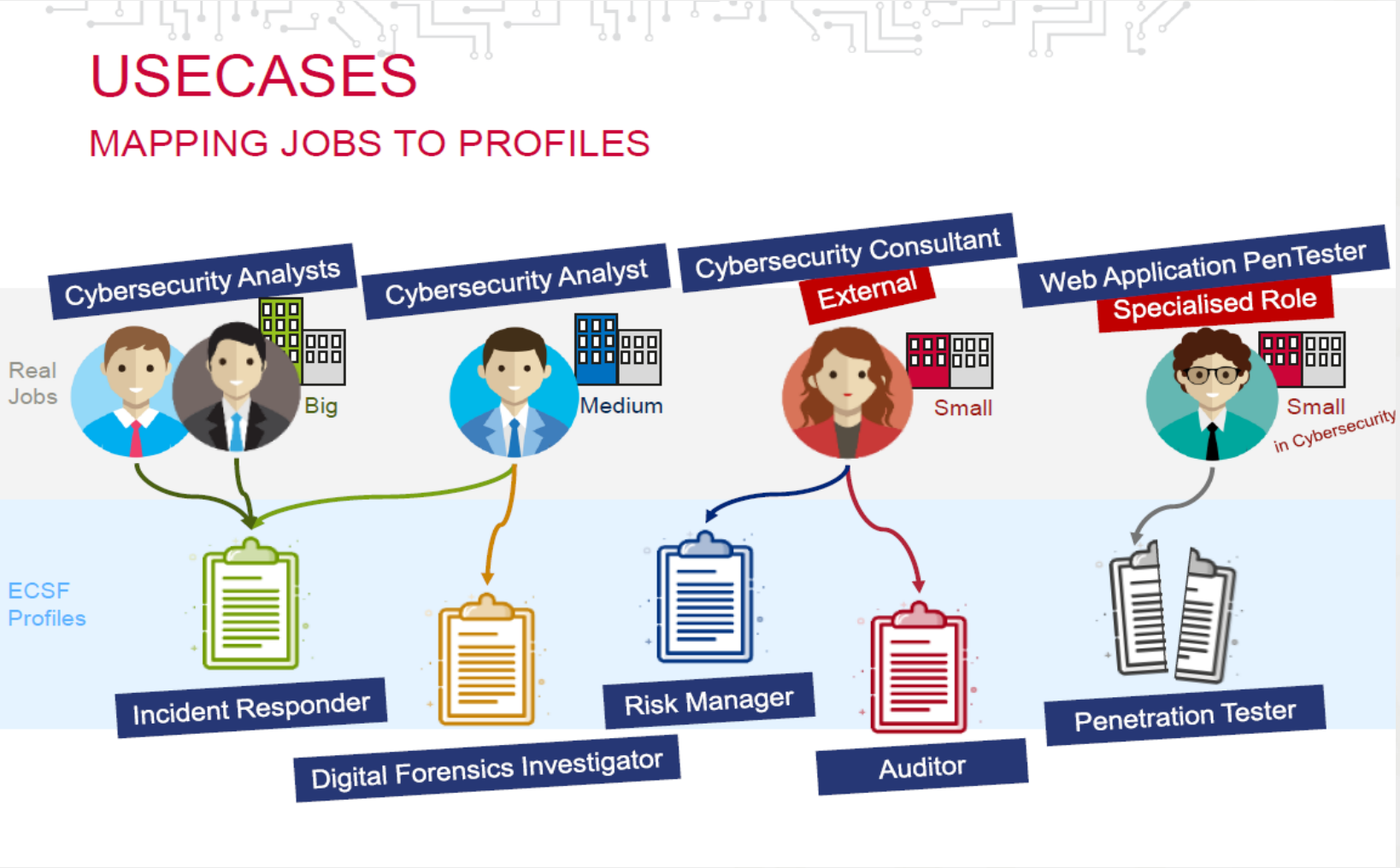
Egyének

Milyen készségekre és ismeretekre van szükségem?

Az ECSF használata

ECSF használata 1. - Szervezetek

A munkakörök profilokhoz való hozzárendelése



Forrás: ENISA – European Cybersecurity Skills Framework (ppt) VO.21, 2021.12.06.

Az ECSF-szerepek gyakorlati használata

- A szakmai szerepprofilok **NEM szakértő személyek számára** szolgálnak.
- A profilok segítenek a nem szakértő személyeknek megérteni a kiberbiztonság komplex környezetét és közös uniós nyelvet biztosít minden érdekelt fél számára.

Az **ECSF szerep profilok** nem egyediek, hanem egy **általános** szerepkör **egyszerű** leírását tartalmazzák a széleskörű használhatóság érdekében!

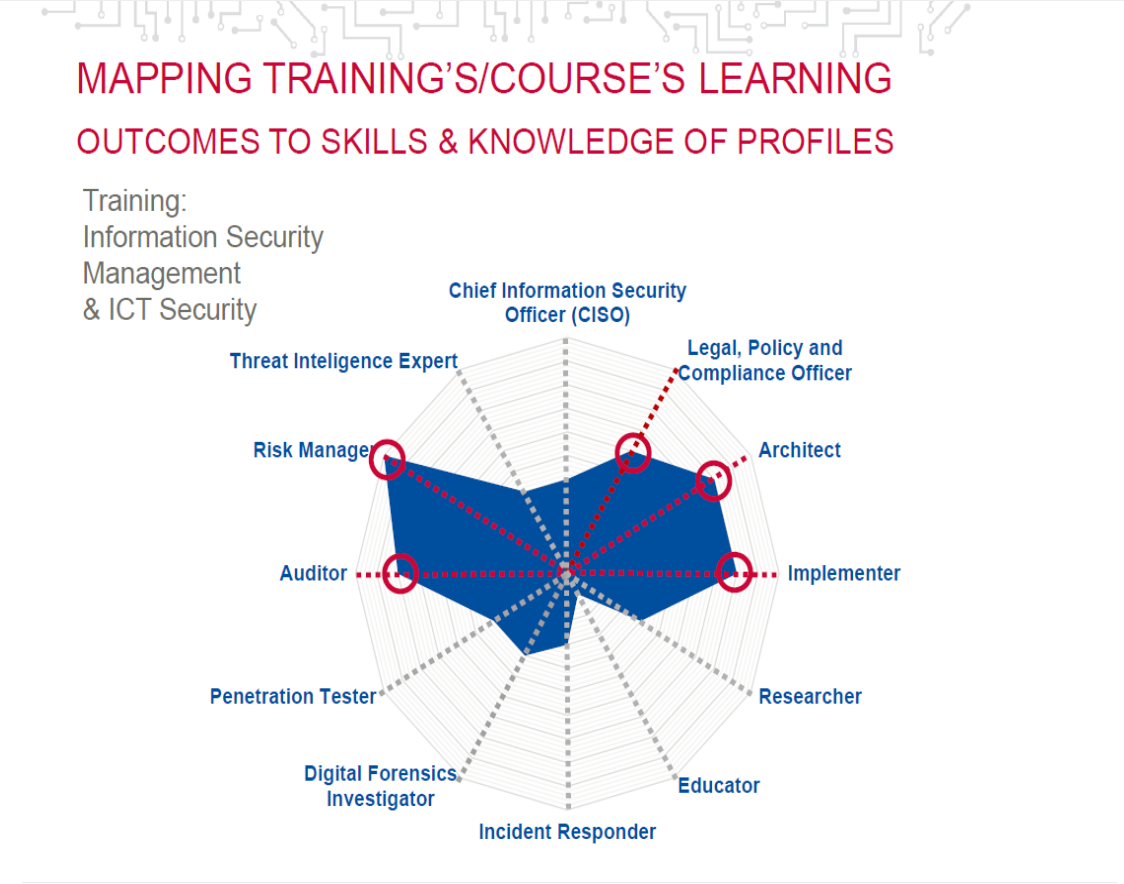
Magát a **munkakört** egy szervezeten belül **egyedi** módon határozzák meg, hozzárendelve a fizetést, a feltételeket és kikötéseket.

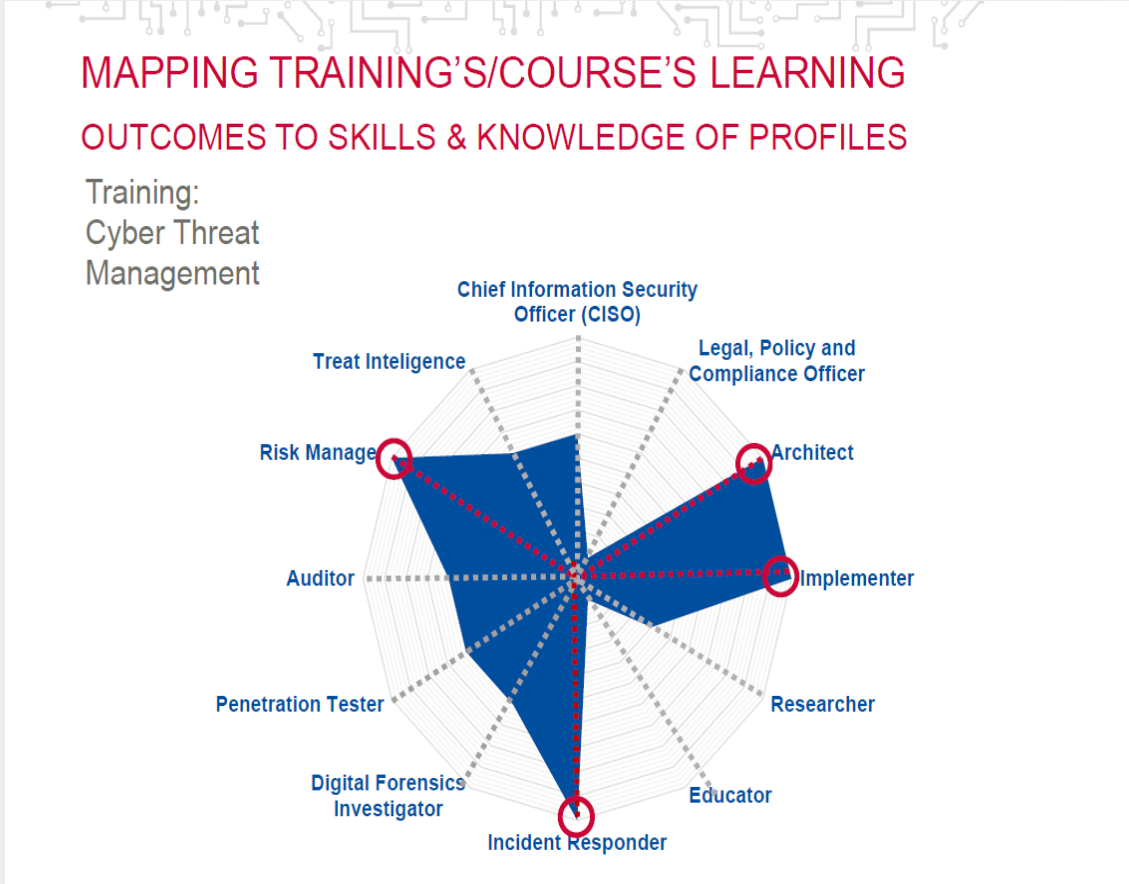
A gyakorlatban:

Egy kiberbiztonsági munka számos ECSF szerepkörből és / vagy szerepekörök részéből áll.

Az ECSF használata 2. - Képzés szolgáltatók

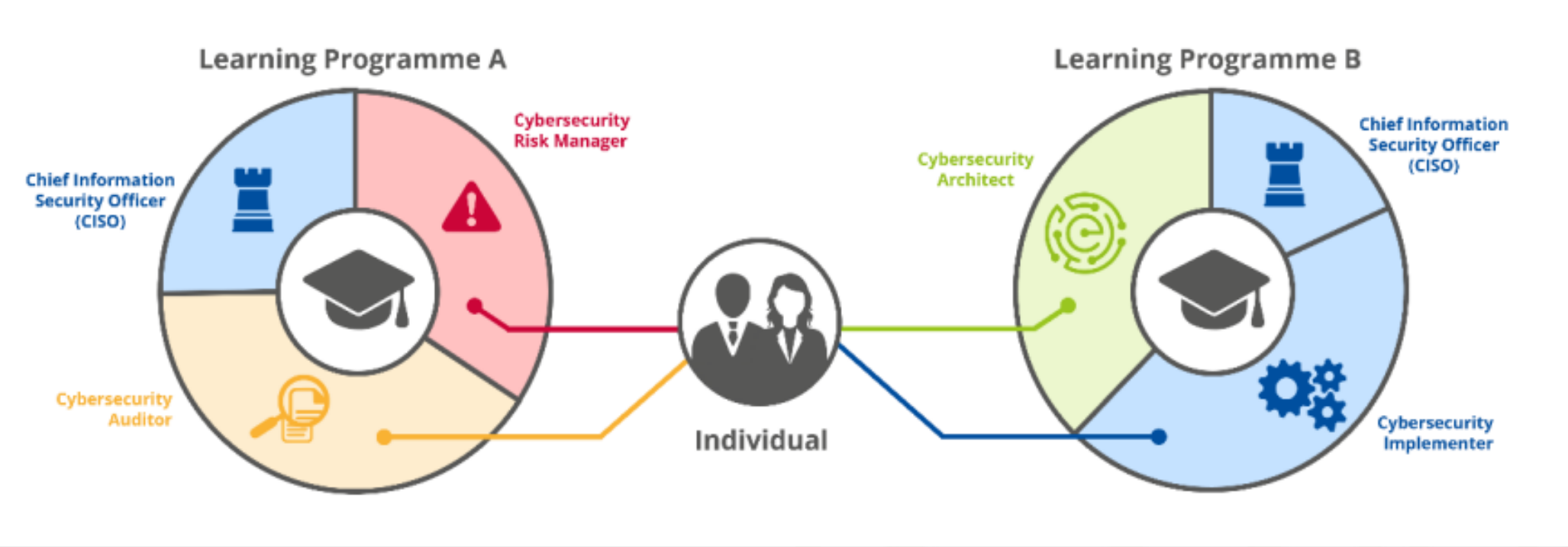
Képzések, tanfolyamok ismeretanyagainak feltérképezése - Készségek, ismeretek az ECSF profilok alapján





Forrás: ENISA –
European Cybersecurity Skills Framework (ppt)
VO.21, 2021.12.06.

ECSF használata 3. - Karriertervezés



Forrás:*Forrás: User Manuel – European Cybersecurity Skills Framework (ECSF), 2022.09.19*.

ECSF Profilok

ECSF Elérhetősége:

https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

European Cybersecurity Skills Framework Role Profiles
https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

European Cybersecurity Skills Framework (ECSF) - User Manual
https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Hazai disszemináció:

- konferenciák (ISACA – Dr. Krasznay Csaba),
- publikációk,
- magyar fordítás (2023. első félév (?)).

1. Chief Information Security Officer (CISO)

Profil Elnevezése	Információbiztonsági Vezető (CISO)
Alternatív elnevezés	Cybersecurity Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Összegzés	Irányítja egy szervezet kiberbiztonsági stratégiáját és annak végrehajtását a digitális hálózat, szolgáltatások és eszközök megfelelő biztonsága és védelme biztosítása érdekében.
Küldetés	Meghatározza, képviseli és kommunikálja a kiberbiztonsági jövőképet, stratégiát, politikát, eljárásokat, valamint irányítja annak végrehajtását a szervezeten belül. Biztosítja az információcserét a külső hatóságokkal és a szakmai testületek.
Eredménytermékek	• Kiberbiztonsági Stratégia • Kiberbiztonsági Politika
Fő feladatok	• Meghatározza, végrehajtja, kommunikálja és fenntartja a kiberbiztonsághoz kapcsolódó célokat, követelményeket, stratégiákat, politikákat beleértve az erőforrás tervezését is az üzleti stratégiával összehangolva a szervezeti célok támogatása érdekében. • Előkészíti és bemutatja a szervezet felsővezetése jóváhagyása céljából a kiberbiztonság jövőképét, stratégiáját és politikáját és biztosítja ezek megvalósítását. • Felügyeli az Információbiztonsági Irányítási Rendszer alkalmazását és fejlesztését. • Tájékoztatja a felső vezetést a kiberbiztonsági kockázatokról, fenyegetésekről és azok hatásáról a szervezetre. • Biztosítja, hogy a felső vezetés jóváhagyja a szervezet kiberbiztonsági kockázatait. • Kidolgozza a kiberbiztonsági terveket. • Kapcsolatot alakít ki a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel. • Jelentést tesz a felsővezetésnek a kiberbiztonsági incidensekről, kockázatokról és megállapításokról. • Nyomonköveti a kiberbiztonság fejlődési irányait. • Biztosítja a kiberbiztonsági stratégia végrehajtásához szükséges erőforrásokat. • Egyeztet a felső vezetéssel a kiberbiztonsággal kapcsolatos költségvetésről. • Biztosítja a szervezet ellenálló képességét a kiberbiztonsági incidensekkel szemben.
	• Irányítja a szervezeten belüli folyamatos kapacitásépítést. • Biztosítja a megfelelő kiberbiztonsági erőforrások felülvizsgálatát, tervezését és elosztását.
Kulcs készségek	• A szervezet kiberbiztonsági helyzetének értékelése és javítása • Kiberbiztonsági irányelvek, tanúsítványok, szabványok, módszertanok és keretrendszerek elemzése és végrehajtása • A kiberbiztonsággal kapcsolatos törvények, rendeletek és jogszabályok elemzése és betartása. • Kiberbiztonsági ajánlások és legjobb gyakorlatok implementálása • A kiberbiztonsági erőforrások vezetése • A kiberbiztonsági stratégia kidolgozása, támogatása és végrehajtásának irányítása. • A szervezet kiberbiztonsági kultúrájának befolyásolása. • Információbiztonsági irányítási rendszer (IBIR) kialakítása, alkalmazása, ellenőrzése és felülvizsgálata közvetlen irányítással, vagy kiszervezés révén. • A biztonsági dokumentumok, jelentések, SLA-k felülvizsgálata és javítása, valamint a biztonsági célkitűzések elérésének biztosítása. • A kiberbiztonsággal kapcsolatos problémák azonosítása és megoldása. • Kiberbiztonsági terv kidolgozása • Kommunikál, koordinál és együttműködik a belső és külső érdekelt felekkel. • A szervezet információbiztonsági stratégiájának szükséges módosításainak előrejelzése és új tervek kidolgozása. • A kiberbiztonsági irányítás érettségi modelljeinek meghatározása és alkalmazása • A kiberbiztonsági fenyegetések, igények és közelgő kihívások előrejelzése. • A munkatársak motiválása és ösztönözése

1. Chief Information Security Officer (CISO)

Kulcs ismeretek	• Kiberbiztonsági politikák • Kiberbiztonsági szabványok, módszertanok és keretrendszerek • Kiberbiztonsági ajánlások és legjobb gyakorlatok • Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok • Kiberbiztonsággal kapcsolatos tanúsítványok • Etikus kiberbiztonsági szervezeti követelmények • Kiberbiztonsági érettségi modellek • Kiberbiztonsági eljárások • Erőforrás-gazdálkodás • Irányítási gyakorlatok • Kockázatkezelési szabványok, módszertanok és keretrendszerek
E-Kompetenciák (Az E-CF alapján)	**A.7. Technology Trend Monitoring - 4. szint** Az új és újonnan megjelenő technológiák validálása az üzleti élet szakértői ismeretei segítségével, a jövőbeli megoldások elképzelése és megfogalmazása érdekében. Létrehozza az egész szervezetre kiterjedő trendfigyelési folyamatokat. **D.1. Információbiztonsági stratégia kidolgozása -5. szint** Stratégiai vezetést biztosít az információbiztonságnak a szervezet kultúrájába való beillesztése érdekében. **E.3. Kockázatkezelés - 4. szint** Vezető szerepet vállal a kockázatkezelési politika meghatározásában és annak alkalmazásban, figyelembe véve az összes lehetséges korlátozó tényezőt, beleértve a műszaki, gazdasági és politikai kérdéseket is. Feladatokat delegál. **E.8. Információbiztonsági irányítás - 4. szint** Vezeti az információs rendszerekben tárolt adatok integritásának, bizalmasságának és rendelkezésre állásának biztosítását, és megfelel az összes jogi követelménynek. **E.9. Információs rendszerek irányítása - 5. szint** Meghatározza és összehangolja az IBIR-irányítási stratégiát, beépítve azt a szervezet vállalati irányítási stratégiájába. Az IBIR-irányítási stratégiát a jogi, gazdasági, politikai, üzleti, technológiai vagy környezeti kérdésekből eredő új, jelentős események figyelembevételéhez igazítja.

2. Cyber Incident responder

Profil elnevezése	Cyber Incident responder
Alternatív elnevezés	Cyber Incident Handler Cyber Crisis Expert Incident Response Engineer Security Operations Center (SOC) Analyst Cyber Fighter /Defender Security Operation Analyst (SOC Analyst) Cybersecurity SIEM Manager
Összegzés	Nyomon követi a szervezet kiberbiztonsági állapotát, kezeli a kibertámadások során bekövetkező incidenseket, valamint biztosítja az IKT-rendszerek folyamatos működését.
Küldetés	Figyelemmel kíséri és értékeli a rendszerek kiberbiztonsági állapotát. Elemzi, értékeli és mérsékeli a kiberbiztonsági incidensek hatásait. Azonosítja a kiberincidensek kiváltó okait és a rosszindulatú szereplőket. A szervezet incidenskezelési tervének megfelelően, helyreállítja a rendszerek és folyamatok működőképes állapotát, összegyűjti a bizonyítékokat, valamint dokumentálja a megtett intézkedéseket.
Eredménytermékek	• Incidenskezelési Terv • Kiberbiztonsági Incidens Riport
Fő feladatok	• Hozzájárul az Incidenskezelési Terv fejlesztéséhez, karbantartásához és értékeléséhez. • Kidolgozza, végrehajtja és értékeli az incidensek kezelésével kapcsolatos eljárásokat. • Azonosítja, elemzi, mérsékli és kommunikálja a kiberbiztonsági incidenseket. • Értékeli és Kezeli a technikai sebezhetőségeket. • Méri a kiberbiztonsági incidensek észlelése és a válaszadás hatékonyságát. • Értékeli a kiberbiztonsági ellenőrzések és a kiberbiztonsági incidenst követően hozott enyhítő intézkedések ellenálló képességét. • Alkalmazza és fejleszti az incidenskezelési tesztelési technikákat. • Eljárásokat dolgoz ki az incidensek következményeinek elemzésére és az incidenskezelési jelentésre vonatkozó eljárásokra. • Dokumentálja az incidensek következményeinek elemzését és az incidenskezelési intézkedéseket. • Együttműködik a biztonsági műveleti központokkal (SOC) és a számítógépes biztonsági eseményelhárítási csoportokkal (CSIRT). • Együttműködik a kulcsemberekkel a biztonsági események jelentése során az alkalmazandó jogi keretnek megfelelően.

Kulcs készségek	• Gyakorolja az eseménykezelés és válaszadás során a feladatok valamennyi technikai, funkcionális és operatív aspektusát. • A kiberfenyegetésről szóló, többféle forrásból származó információk összegyűjtése, elemzése és összefüggéseinek feltárása. • Operációs rendszereken, szervereken, felhőkön és a vonatkozó infrastruktúrákon való munkavégzés. • Nyomás alatti munkavégzés • Kommunikáció, prezentáció és jelentéstétel az érintett érdekelt felek számára • Naplófájlok kezelése és elemzése
Kulcs ismeretek	• Incidenskezelési szabványok, módszertanok és keretrendszerek. • Eseménykezelési ajánlások és legjobb gyakorlatok. • Incidenskezelési eszközök • Incidenskezelési kommunikációs eljárások • Operációs rendszerek biztonsága • Számítógépes hálózatok biztonsága • Kiberfenyegetések • Kibertámadási formák • Számítógépes rendszerek sebezhetőségei • Kiberbiztonsággal kapcsolatos tanúsítványok • Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok • Biztonsági műveleti központok (SOC) működése • Számítógépes biztonsági eseményelhárítási csoportok (CSIRT) működése

2. Cyber Incident responder

E-Kompetenciák (az e-CF alapján)	**A.7. Technológiai trendfigyelés - 3. szint** Folyamatosan nyomon követi az aktuális és a trendeket meghatározó IKT technológiai fejlesztéseket, azonosítja a változásokat. Kapcsolatokat épít ki az érintettekkel. **B.2. Alkotóelemek integrálása - 2. szint** Szisztematikusan biztosítja a szoftver- és hardver-specifikációk kompatibilitását. Dokumentál minden tevékenységet a telepítés során, és rögzíti az eltéréseket és a javítási tevékenységeket is. **B.3. Tesztelés - 3. szint** Szakmai ismeretek felhasználása összetett tesztelési programok felülvizsgálata érdekében. Biztosítja a tesztek és eredmények dokumentálását, hogy az a későbbi folyamatgazdák, például a tervezők, a felhasználók vagy a karbantartók számára inputot nyújtson. Felelős a tesztelési eljárások betartásáért, beleértve a dokumentált ellenőrzési nyomvonalat is. **B.5. Dokumentumok előállítása - 3. szint** A részletesség szintjét a célcsoport igényeihez igazítja **C.4. Problémakezelés - 4. szint** Vezető szerepet tölt be és felelős a teljes problémakezelési folyamatért. Beosztja és biztosítja, hogy jól képzett emberi erőforrások, eszközök és diagnosztikai berendezések álljanak rendelkezésre a vészhelyzeti események kezelésére. Mély szakértelemmel rendelkezik a kritikus komponensek meghibásodásának előrejelzéséről és a minimális leállási idővel történő helyreállításról. Kialakítja az eszkalációs folyamatokat annak érdekében, hogy minden egyes incidenshez megfelelő erőforrásokat lehessen alkalmazni.

3. Cyber Legal, Policy and Compliance Officer

Profil Elnevezése	Cyber Legal, Policy and Compliance Officer
Alternatív Elnevezés	Data Protection Officer (DPO) Privacy Protection Officer Cyber Law Consultant Cyber Legal Advisor Information Governance Officer Data Compliance Officer Cybersecurity Legal Officer IT/ICT Compliance Manager Governance Risk Compliance (GRC) Consultant
Összegzés	Irányítja a kiberbiztonsággal kapcsolatos szabványoknak, jogi és szabályozási kereteknek való megfelelést a szervezet stratégiája és a jogi követelmények alapján.
Küldetés	Felügyeli és biztosítja a kiberbiztonsággal kapcsolatos jogi, szabályozási keretek, adatvédelemi jogszabályok és irányelvek betartását a szervezet stratégiája és a jogi követelmények alapján. Közreműködik a szervezet adatvédelemmel kapcsolatos intézkedéseinél. Jogi tanácsadást nyújt a szervezet információbiztonsági irányítási folyamatainak fejlesztéséhez, illetve a megfelelőség biztosítása érdekében az ajánlott korrekciós stratégiák/megoldások kidolgozásához.
Eredménytermékek	• Megfelelőségi kézikönyv • Megfelelési jelentés
Fő feladatok	• Biztosítja az adatvédelmi és adatbiztonsági szabványoknak, törvényeknek és rendeleteknek való megfelelést jogi tanácsadás és iránymutatás nyújtása segítségével. • Azonosítja és dokumentálja a megfelelőségi hiányosságokat. • Elvégzi az adatvédelmi hatásvizsgálatokat, kidolgozza, fenntartja, kommunikálja és oktatja az adatvédelmi irányelveket és eljárásokat. • Érvényesíti és támogatja a szervezet adatvédelmi és adatbiztonsági programját. • Biztosítja, hogy az adattulajdonosok, adatgazdák, adatkezelők, adatfeldolgozók, érintettek, belső vagy külső partnerek és szervezetek tájékoztatást kapjanak adatvédelmi jogaikról, kötelezettségeikről és felelősségeikről. • Kapcsolattartó pontként kezeli az adatkezelési eljárással kapcsolatos kérdéseket és panaszokat. • Segítséget nyújt a tervezésben, végrehajtásban, ellenőrzésben és megfelelőségi tesztelésben a kiberbiztonság és az adatvédelem megfelelőségének biztosítása érdekében.
	• Ellenőrzi az auditokat és az adatvédelemmel kapcsolatos képzési tevékenységeket. • Együttműködik és információkat oszt meg a hatóságokkal és szakmai csoportokkal. • Hozzájárul a szervezet kiberbiztonsági stratégiájának, politikájának és eljárásainak kidolgozásához. • Kidolgozza és javaslatot tesz a munkatársak tudatosságnövelő képzésére vonatkozóan a megfelelőség elérése és az adatvédelem kultúrájának szervezeten belül fejlesztése érdekében. • Kezeli az információbiztonsági felelősségi körök és a harmadik felekkel való kapcsolatok kapcsán felmerülő jogi kérdéseket.
Kulcs készségek	• Az üzleti stratégia, modellek és termékek átfogó megértése, valamint a jogi, szabályozási és szabványkövetelmények figyelembevételének képessége. • Képesség a szervezeti folyamatok, a pénzügyi és üzleti stratégia megvalósításával kapcsolatos adatvédelmi kérdések gyakorlati megvalósítására. • Az üzleti igényeket és a jogi követelményeket kiegészítő, megfelelő kiberbiztonsági és adatvédelmi irányelvek és eljárások kidolgozásának irányítása; továbbá az érintett felek közötti elfogadás, megértés, végrehajtás és kommunikáció biztosítása. • Az adatvédelmi értékelések elvégzése, nyomon követése és felülvizsgálata szabványok, keretrendszerek, elismert módszerek és eszközök felhasználásával. • Képesség az adatvédelemmel kapcsolatos témák ismertetésére és kommunikálására az érdekelt felek és a felhasználók felé. • Képes az etikai követelmények és szabványok megértésére, gyakorlására és betartására. • A jogi keretrendszer módosításainak megértése, a változások átvezetése a kiberbiztonsági és adatvédelmi stratégiába és politikákba. • Együttműködés más csapattagokkal és kollégákkal

3. Cyber Legal, Policy and Compliance Officer

Kulcs ismeretek	• Kiberbiztonsággal kapcsolatos törvények, rendeletek és jogszabályok. • Kiberbiztonsági szabványok, módszertanok és keretrendszerek. • Kiberbiztonsági politikák. • Jogi, szabályozói és jogszabályi megfelelőségi követelmények, ajánlások és legjobb gyakorlatok. • Adatvédelmi hatásvizsgálati szabványok, módszertanok és keretrendszerek.
E-Kompetenciák (Az E-CF Alapján)	**A.1. Az információs rendszerek és az üzleti stratégia összehangolása – 4. szint** Vezető szerepet vállal a hosszú távú innovatív informatikai megoldások kialakításában és végrehajtásában. **D.1. Információbiztonsági stratégia kidolgozása - 4. szint** A mély szakértelem hasznosítása, valamint a külső szabványok és legjobb gyakorlatok felhasználása. **E.8. Információbiztonsági irányítás - 3. szint** Értékeli a biztonságirányítási intézkedéseket és mutatókat, dönt ezek információbiztonsági politikának való megfelelőségéről. Vizsgálja és kezdeményezi a biztonsági előírások megsértésének orvoslását. **E.9. Információs rendszerek irányítása - 4. szint** Vezető szerepet tölt be az IS-irányítási stratégiában azáltal, hogy kommunikálja, terjeszti és ellenőrzi a vonatkozó folyamatokat a teljes IKT-infrastruktúrában.

6. Cybersecurity Auditor

Profil elnevezése	Cybersecurity Auditor
Alternatív elnevezés	Information Security Auditor (IT or Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Összegzés	A szervezet ökoszisztémájának kiberbiztonsági ellenőrzése. Megfelelőség biztosítása a jogszabályi, szabályozási, szakpolitikai információknak, biztonsági követelményeknek, ágazati szabványoknak és a legjobb gyakorlatoknak.
Küldetés	Független felülvizsgálatokat végez a folyamatok és ellenőrzések hatékonyságának értékelése és a szervezet jogi és szabályozási kereteinek való általános megfelelés megállapítása érdekében. Értékeli, teszteli és ellenőrzi a kiberbiztonsággal kapcsolatos termékeket (rendszerek, hardverek, szoftverek és szolgáltatások), funkciókat és eljárásrendeket, biztosítva ezzel az iránymutatásoknak, szabványoknak és szabályzatoknak való megfelelést.
Eredménytermékek	• Kiberbiztonsági ellenőrzési terv • Kiberbiztonsági auditjelentés
Fő feladatok	• Kidolgozza a szervezet ellenőrzési politikáját, eljárásait, szabványait és iránymutatásait. • Meghatározza a rendszerek auditálásához használt módszertanokat és gyakorlatokat. • Meghatározza a célterületet és irányítja az auditálási tevékenységeket. • Meghatározza az audit hatókörét, célkitűzéseit és az audittal szemben támasztott követelményeket. • Kidolgozza az ellenőrzési tervet, melyben megfogalmazza a keretrendszereket, szabványokat, módszertant és ellenőrzési teszteket. • Felülvizsgálja a kockázatok alapján az értékelés célját, a biztonsági célkitűzéseket és a követelményeket. • Ellenőrzi a kiberbiztonsággal kapcsolatos alkalmazandó törvényeknek és rendeleteknek való megfelelést. • Ellenőrzi a kiberbiztonsággal kapcsolatos alkalmazandó szabványoknak való megfelelést. • Végrehajtja az ellenőrzési tervet és összegyűjti a bizonyítékokat és a méréseket. • Fenntartja és védi az ellenőrzési nyilvántartások sértetlenségét.
	• Kidolgozza és kommunikálja a megfelelőségértékelési, minőségbiztosítási, ellenőrzési, tanúsítási és karbantartási jelentéseket. • Nyomon követi a kockázatjavításra irányuló tevékenységeket.
Kulcs készségek	• A munka szervezése és végzése szisztematikus és determinista módon történik a rendelkezésre álló bizonyítékok alapján. • Az ellenőrzési keretrendszereket, szabványokat és módszertanokat követése és alkalmazása. • Auditálási eszközök és technikák alkalmazása • Üzleti folyamatok elemzése, a szoftver- vagy hardverbiztonság értékelése és felülvizsgálata, technikai és szervezeti ellenőrzések. • A rendszerek elemire bontása és elemzése a gyenge pontok és a nem hatékony ellenőrzések azonosítása érdekében. • A jogi és szabályozási követelmények, valamint az üzleti igények kommunikálása, magyarázata és adaptálása. • Az auditálási információk összegyűjtése, értékelése, karbantartása és védelme. • Az ellenőrzés integránsan, pártatlanul és függetlenül történő elvégzése.
Kulcs ismeretek	• Kiberbiztonsági ellenőrzések és megoldások • Jogi, szabályozási és jogszabályi megfelelési követelmények, ajánlások és legjobb gyakorlatok • A kiberbiztonsági ellenőrzések hatékonyságának nyomon követése, tesztelése és értékelése • Megfelelőségértékelési szabványok, módszertanok és keretrendszerek • Auditálási szabványok, módszertanok és keretrendszerek • Kiberbiztonsági szabványok, módszertanok és keretrendszerek • Az auditálással kapcsolatos tanúsítás • Kiberbiztonsággal kapcsolatos tanúsítások

6. Cybersecurity Auditor

E-Kompetenciák (az e-CF alapján)	**B.3. Tesztelés – 4. szint** Széleskörű szaktudást használ ki a teljes tesztelési tevékenység folyamatának kialakítására, beleértve a belső gyakorlati szabványok kialakítását. Szakértői útmutatást és tanácsadást nyújt a tesztelési csoportnak. **B.5. Dokumentumok előállítása– 3. szint** A részletesség szintjét a célcsoport igényeihez igazítja. **E.3. Kockázatkezelés – 4. szint** Vezető szerepet vállal a kockázatkezelési politika meghatározásában és alkalmazásában, figyelembe véve az összes lehetséges nehezítő tényezőt, beleértve a műszaki, gazdasági és politikai kérdéseket is. Feladatokat delegál. **E.6. IKT minőségbiztosítás– 4. szint** Értékeli és megállapítja a minőségi követelmények teljesítésének mértékét, és irányítja a minőségpolitika végrehajtását. Gyakorlati vezetést biztosít a minőségi szabványok meghatározásához és túlteljesítéséhez.

7. Cybersecurity Educator

Profil elnevezése	Cybersecurity Educator
Alternatív elnevezés	Cybersecurity Awareness Specialist Cybersecurity Trainer Faculty in Cybersecurity (Professor, Lecturer)
Összegzés	Fejleszti a kiberbiztonsági ismereteket, készségeket és kompetenciákat.
Küldetés	Megtervezi, fejleszti és irányítja a tudatosságnövelő, képzési és oktatási programokat a kiberbiztonsággal és az adatvédelemmel kapcsolatos témákban. Megfelelő képzési és oktatási módszereket, technikákat és kommunikációs eszközöket használ a szervezet kiberbiztonsági kultúrájának, képességeinek, ismereteinek és készségeinek fejlesztésére. Kommunikálja a kiberbiztonság fontosságát, és megszilárdítja azt a szervezetben.
Eredménytermékek	• Kiberbiztonsági tudatosítási program • Kiberbiztonsági képzési tananyag
Fő feladatok	• A kiberbiztonsággal és adatvédelemmel kapcsolatos tantervek és oktatási anyagok kidolgozása, frissítése és átadása a képzés és a tudatosság növelése érdekében a tartalom, a módszer, az eszközök és a képzésben résztvevők igényei alapján. • A kiberbiztonsággal és adatvédelemmel kapcsolatos tudatosságnövelő tevékenységek, szemináriumok, tanfolyamok, gyakorlati képzések szervezése, tervezése és lebonyolítása. • A képzés hatékonyságának nyomon követése, értékelése és jelentése. • A képzésben részt vevők teljesítményének értékelése és jelentése. • Új megközelítések keresése az oktatás, képzés és tudatosságnövelés számára. • Kiberbiztonsági szimulációk, virtuális laboratóriumok vagy kibertéri környezetek tervezése, fejlesztése és megvalósítása. • Iránymutatás nyújtása a kiberbiztonsági tanúsítási programokról az egyének számára. • A szakértelem folyamatos fenntartása és fejlesztése; a kiberbiztonsági kapacitások és képességek kiépítésének ösztönzése.
Kulcs készségek	• A kiberbiztonsági tudatossággal, képzéssel és oktatással kapcsolatos igények azonosítása. • A kiberbiztonsági igények lefedésére irányuló tanulási programok tervezése, fejlesztése és megvalósítása. • Kiberbiztonsági gyakorlatok kidolgozása, beleértve a kibertér tágabb értelemben vett környezetét alkalmazó szimulációkat. • A kiberbiztonsági és adatvédelmi szakmai tanúsítványok megszerzéséhez szükséges képzés biztosítása.
	• A meglévő, kiberbiztonsággal kapcsolatos képzési források felhasználása. • Értékelési programok kidolgozása a tudatosságnövelő, képzési és oktatási tevékenységekhez. • Kommunikáció, bemutatás és jelentéstétel az érintettek számára. • A célközönségnek megfelelő pedagógiai megközelítések azonosítása és kiválasztása. • Az emberek motiválása és bátorítása.
Kulcs ismeretek	• Pedagógiai szabványok, módszertanok és keretrendszerek. • Kiberbiztonsági tudatosítás, oktatás és képzési programok fejlesztése. • Kiberbiztonsággal kapcsolatos tanúsítványok. • Kiberbiztonsági oktatási és képzési szabványok, módszertanok és keretrendszerek. • Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok. • Kiberbiztonsági ajánlások és legjobb gyakorlatok. • Kiberbiztonsági szabványok, módszertanok és keretrendszerek. • Kiberbiztonsági kontrollok és megoldások.
E-Kompetenciák (az e-CF alapján)	**D.3. Oktatási és képzési szolgáltatás - 3. szint** Kreatívan jár el a készséghiányok elemzése érdekében; konkrét követelményeket dolgoz ki és azonosítja a képzési kínálat lehetséges forrásait. Szakterületi ismeretekkel rendelkezik a képzési piacról, és visszajelzési mechanizmust hoz létre az alternatív képzési programok hozzáadott értékének értékelésére. **D.9. Humánerőforrás-fejlesztés - 3. szint** Figyelemmel kíséri és kezeli az egyének és csoportok fejlesztési igényeit. **E.8. Információbiztonsági irányítás - 3. szint** Értékeli a biztonságirányítási intézkedéseket és mutatókat, dönt ezek információbiztonsági politikának való megfelelőségéről. Vizsgálja és kezdeményezi a biztonsági előírások megsértésének orvoslását.

8. Cybersecurity Implementer

Profil elnevezése	Cybersecurity Implementer
Alternatív elnevezés	Information Security Implementer Cybersecurity Solutions Expert Cybersecurity Developer Cybersecurity Engineer Development, Security & Operations (DevSecOps) Engineer
Összegzés	Kiberbiztonsági megoldásokat (rendszerek, eszközök, szoftverek, kontrollok és szolgáltatások) fejleszt, telepít, működtet az infrastruktúrákon és az eszközökön.
Küldetés	Biztosítja a kiberbiztonsággal kapcsolatos műszaki fejlesztést, integrációt, tesztelést, a kiberbiztonsági megoldások megvalósítását, üzemeltetését, karbantartását, felügyeletét és támogatását. Biztosítja a specifikációk és a megfelelőségi követelmények betartását, a megfelelő teljesítményt, és megoldja a szükséges műszaki kérdéseket a szervezet kiberbiztonsággal kapcsolatos megoldásai (rendszerek, eszközök, szoftverek, ellenőrzések és szolgáltatások), az infrastruktúrák és az eszközök tekintetében.
Eredménytermékek	• Kiberbiztonsági megoldások
Fő feladatok	• Kiberbiztonsági termékek fejlesztése, bevezetése, karbantartása, frissítése, tesztelése. • Kiberbiztonsággal kapcsolatos támogatás nyújtása a felhasználók és az ügyfelek számára. • Kiberbiztonsági megoldások integrálása és megfelelő működésük biztosítása. • A rendszerek, szolgáltatások és termékek biztonságos konfigurálása. • A rendszerek, szolgáltatások és termékek biztonságának fenntartása és frissítése. • Kiberbiztonsági eljárások és ellenőrzések végrehajtása. • A bevezetett kiberbiztonsági kontrollok teljesítményének nyomon követése és biztosítása. • A rendszerek, szolgáltatások és termékek biztonságának dokumentálása, jelentés készítése. • Szoros együttműködés az IT/OT személyzettel a kiberbiztonsággal kapcsolatos intézkedések terén. • A technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavítások alkalmazása és irányítása.
Kulcs készségek	• Kommunikáció, bemutatás és jelentés készítése az érintett érdekelt felek számára. • Kiberbiztonsági megoldások integrálása a szervezet infrastruktúrájába.
	• Konfigurálási megoldások a szervezet biztonsági politikájának megfelelően. • A megoldások értékelése azok biztonságossága és teljesítménye alapján. • Kódok, szkriptek és programok fejlesztése. • A kiberbiztonsággal kapcsolatos problémák azonosítása és megoldása. • Együttműködés más csapattagokkal és kollégákkal.
Kulcs ismeretek	• Biztonságos fejlesztési életciklus • Számítógépes programozás • Operációs rendszerek biztonsága • Számítógépes hálózatok biztonsága • Kiberbiztonsági ellenőrzések és megoldások • Támadó és védekező biztonsági gyakorlatok • Biztonságos kódolási ajánlások és legjobb gyakorlatok • Kiberbiztonsági ajánlások és legjobb gyakorlatok • Tesztelési szabványok, módszertanok és keretrendszerek • Tesztelési eljárások • Kiberbiztonsággal kapcsolatos technológiák
E-Kompetenciák (az e-CF alapján)	**A.5. Architecture Design – 3. szint** Speciális tudást alkalmaz a releváns IKT-technológiák és specifikációk meghatározásához, amelyeket több IKT-projekt, -alkalmazás vagy infrastruktúrafejlesztés során kell alkalmazni. **A.6. Applikációtervezés – 3. szint** Elszámoltatja saját és mások tevékenységét annak biztosítása érdekében, hogy az alkalmazás megfelelően integrálódjon egy összetett környezetbe, és megfeleljen a felhasználói/ügyféligényeknek. **B.1. Applikáció fejlesztés – 3. szint** Kreatívan cselekszik az alkalmazások fejlesztése és a megfelelő technikai lehetőségek kiválasztása érdekében. Elszámol mások fejlesztési tevékenységeivel. Optimalizálja az alkalmazások fejlesztését, karbantartását és teljesítményét tervezési minták alkalmazásával és a bevált megoldások újrafelhasználásával.

8. Cybersecurity Implementer

	B.3. Tesztelés – 3. szint Szakmai ismeretek felhasználása összetett tesztelési programok felügyelete érdekében. Biztosítja a tesztek és eredmények dokumentálását annak érdekében, hogy a későbbi folyamatgazdák, például a tervezők, felhasználók vagy karbantartók számára inputot nyújtson. Felelős a tesztelési eljárások betartásáért, beleértve a dokumentált ellenőrzési nyomvonalat is. **B.6. ICT Systems Engineering – 4. szint** Kezeli a komplexitást a koherens termékfejlesztést támogató szabványos eljárások és architektúrák kidolgozásával. Meghatározza a rendszerkövetelményeket, amelyek a digitális infrastruktúra tervezését irányítják. Meghatározza, hogy mely rendszerkövetelményeket és funkciókat kell a rendszer mely elemeihez és/vagy az infrastruktúra mely rétegeihez rendelni.

10. Cybersecurity Risk Manager

Profil elnevezése	Cybersecurity Risk Manager
Alternatív elnevezés	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst Cyber Risk Manager
Összegzés	Kezeli a szervezet kiberbiztonsággal kapcsolatos kockázatait a szervezeti stratégiában megfogalmazott célokhoz igazodva. Kidolgozza, kezeli és kommunikálja a kockázatkezelési folyamatokat és jelentéseket.
Küldetés	Folyamatosan kezeli (azonosítja, elemzi, értékeli, véleményezi, mérsékeli) az IKT-infrastruktúrák, rendszerek és szolgáltatások kiberbiztonsággal kapcsolatos kockázatait a hatékony kockázatelemzés, -értékelés és -kezelés megtervezésével, alkalmazásával, jelentésével és kommunikálásával. Kockázatkezelési stratégiát dolgoz ki a szervezet számára, és biztosítja, hogy a kockázatok a szervezet számára elfogadható szinten maradjanak a kockázatcsökkentő és kontroll intézkedések kiválasztásával.
Eredménytermékek	• Kiberbiztonsági kockázatértékelési jelentés • Kiberbiztonsági kockázatok kezelésére vonatkozó cselekvési terv
Fő feladatok	• Kidolgozza a szervezet kiberbiztonsági kockázatkezelési stratégiáját. • Irányítja a szervezet eszközeinek leltározását. • Azonosítja és értékeli az IKT-rendszerek kiberbiztonsággal kapcsolatos fenyegetéseit és sebezhetőségeit. • Azonosítja a fenyegetettségi környezetet, beleértve a támadók profilját és a támadási potenciál becslését. • Értékeli a kiberbiztonsági kockázatokat és javaslatot tesz a legmegfelelőbb kockázatkezelési lehetőségekre, beleértve a biztonsági kontrollokat, valamint azokat a kockázatcsökkentő és a kockázatok elkerülését segítő intézkedéseket, amelyek a legjobban illeszkednek a szervezet stratégiájába. • Nyomon követi a kiberbiztonsági ellenőrzések hatékonyságát és a kockázati szinteket. • Biztosítja hogy valamennyi kiberbiztonsági kockázat a szervezet számára elfogadható szinten maradjon. • Kidolgozza, fenntartja, jelenti és kommunikálja a teljes kockázatkezelési ciklust.
Kulcs készségek	• Kiberbiztonsági kockázatkezelési keretrendszerek, módszertanok és iránymutatások átültetése, valamint a szabályozásoknak és szabványoknak való megfelelés biztosítása. • A szervezet minőségirányíti és kockázatkezelési gyakorlatának elemzése és megerősítése. • Képessé teszi az üzleti rendszerek tulajdonosait, a vezetőket és más érdekelt feleket arra, hogy a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozzanak. • Kiberbiztonsági kockázattudatos környezet kialakítása. • Kommunikáció, prezentálás és jelentés az érintett érdekeltek számára. • Kockázatmegosztási lehetőségek tervezése és kezelése.
Kulcs ismeretek	• Kockázatkezelési szabványok, módszertanok és keretrendszerek • Kockázatkezelési eszközök • Kockázatkezelési ajánlások és legjobb gyakorlatok • Kiberfenyegetések • Számítógépes rendszerek sebezhetőségei • Kiberbiztonsági ellenőrzések és megoldások • Kiberbiztonsági kockázatok • A kiberbiztonsági ellenőrzések hatékonyságának nyomon követése, tesztelése és értékelése • Kiberbiztonsággal kapcsolatos tanúsítványok • Kiberbiztonsággal kapcsolatos technológiák
E-Kompetenciák (az e-CF alapján)	**E.3. Kockázatkezelés - 4. szint** Vezető szerepet vállal a kockázatkezelési politika meghatározásában és annak alkalmazásban, figyelembe véve az összes lehetséges korlátozó tényezőt, beleértve a műszaki, gazdasági és politikai kérdéseket is. Feladatokat delegál. **E.5. Folyamatfejlesztés - 3. szint** Szakmai ismeretek felhasználása a meglévő IKT-folyamatok és -megoldások vizsgálatára a lehetséges innovációk értelmezése érdekében. Ésszerű érveken alapuló ajánlásokat tesz. **E.7. Üzleti változásmenedzsment - 4. szint** Vezető szerepet vállal a jelentős IKT-alapú üzleti változások megtervezésében, irányításában és végrehajtásában. **E.9. Információs rendszerek irányítása - 4. szint** Vezető szerepet tölt be az IS-irányítási stratégiában azáltal, hogy kommunikálja, terjeszti és ellenőrzi a vonatkozó folyamatokat a teljes IKT-infrastruktúrában.

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu