EUROPEAN UNION AGENCY
FOR CYBERSECURITY

BRUGERMANUAL

EUROPÆISKE CYBERSIKKERHEDSFÆRDIGHEDER
RAMME (ECSF)

SEPTEMBER 2022

OM ENISA

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, er EU's agentur dedikeret til at opnå et højt fælles niveau af cybersikkerhed i hele Europa. Etableret i 2004 og styrket af EU's cybersikkerhedslov, bidrager Den Europæiske Unions Agentur for Cybersikkerhed til EU's cyberpolitik, øger troværdigheden af IKT-produkter, -tjenester og -processer med cybersikkerhedscertificeringsordninger, samarbejder med medlemsstater og EU-organer og hjælper Europa med at forberede til morgendagens cyberudfordringer. Gennem videndeling, kapacitetsopbygning og bevidstgørelse arbejder agenturet sammen med sine nøgleinteressenter for at styrke tilliden til den forbundne økonomi, for at øge modstandskraften i Unionens infrastruktur og i sidste ende holde Europas samfund og borgere digitalt sikre. Mere information om ENISA og dets arbejde kan findes her: www.enisa.europa.eu.

KONTAKT

For at kontakte forfatterne, brug venligst euskills@enisa.europa.eu.

ANKENDELSER

Denne ramme er resultatet af ekspertudtalelsen og enigheden i Ad-Hoc-arbejdsgruppen om kompetencerammen sammensat af Agata BEKIER, Vladlena BENSON, Jutta BREYER*, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta POLEMI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN og Jan HAJNY.

Fabio DI FRANCO og Athanasios GRAMMATOPOULOS ledede denne aktivitet for ENISA.

JURIDISK MEDDELELSE

Denne publikation repræsenterer ENISA's synspunkter og fortolkninger, medmindre andet er angivet. Den godkender ikke en lovgivningsmæssig forpligtelse for ENISA eller ENISA-organer i henhold til forordning (EU) nr. 2019/881.

ENISA har ret til at ændre, opdatere eller fjerne publikationen eller noget af dens indhold. Den er kun beregnet til informationsformål, og den skal være tilgængelig gratis. Alle henvisninger til det eller dets brug som helhed eller delvist skal indeholde ENISA som kilde.

Tredjepartskilder citeres efter behov. ENISA er ikke ansvarlig eller ansvarlig for indholdet af de eksterne kilder, herunder eksterne websteder, der henvises til i denne publikation.

Hverken ENISA eller nogen person, der handler på dets vegne, er ansvarlig for den brug, der måtte blive gjort af informationen i denne publikation.

ENISA bevarer sine intellektuelle ejendomsrettigheder i forhold til denne publikation.

OPHAVSRET MEDDELELSE

* Ordfører for Ad-Hoc Working Group on the European Cybersecurity Skills Framework

ISBN: 978-92-9204-583-8 – DOI: 10.2824/95989

INDHOLDSFORTEGNELSE

RESUMÉ

Manglen på arbejdsstyrke inden for cybersikkerhed og kvalifikationskløft er en stor bekymring for både økonomisk udvikling og national sikkerhed. Ved at se nærmere på problemet identificerede ENISA Europas behov for en omfattende tilgang til at definere et sæt cybersikkerhedsroller og -kompetencer, som kunne udnyttes til at reducere manglen og kvalifikationskløften. ENISA har arbejdet på udviklingen af en sådan ramme og præsenterer **European Cybersecurity Skills Framework (ECSF),** som har til formål at styrke den europæiske cybersikkerhedskultur ved at levere et fælles europæisk sprog på tværs af fællesskaber og tage et væsentligt skridt fremad mod Europas digitale fremtid.

ECSF giver et praktisk værktøj til at **støtte identifikation og artikulation af opgaver, kompetencer, færdigheder og viden, der er forbundet med** rollerne for europæiske **cybersikkerhedsprofessionelle.** Hovedformålet med rammerne er at **skabe en fælles forståelse** mellem enkeltpersoner, arbejdsgivere og udbydere af læringsprogrammer på tværs af EU's medlemsstater, hvilket gør det til et værdifuldt værktøj til at bygge bro mellem den professionelle cybersikkerhedsarbejdsplads og læringsmiljøer.

Rammen beskriver de vigtigste krav til en professionel cybersikkerhedsarbejdsplads ved at definere et **sæt af 12 typiske cybersikkerhedsprofessionelle rolleprofiler.** Disse profiler giver en fælles forståelse af de vigtigste cybersikkerhedsmissioner, opgaver og færdigheder, der er nødvendige i en professionel cybersikkerhedskontekst, hvilket gør det til den perfekte reference til profilering af færdigheder og viden, som cybersikkerhedsprofessionelle har brug for. Rammen blev designet til at være let forståelig og omfattende nok til at give passende dybdegående cybersikkerhedsindsigt samt fleksibel nok til at tillade tilpasning baseret på hver brugers behov. Ved at inkorporere alle interessentperspektiver er rammen anvendelig for alle typer organisationer og understøtter udviklingen af alle cybersikkerhedsprofessioner.

ECSF er resultatet af arbejde udført af ENISA's ad-hoc arbejdsgruppe om den europæiske ramme for cybersikkerhedsfærdigheder1 dannet af eksperter, der repræsenterer forskellige synspunkter. Den udviklede ramme er baseret på en analyse af eksisterende rammer, resultater og resultater fra forskning om markedsbehov og enighed mellem eksperter. Brugercasestudier og vejledende eksempler, inspireret af forskellige arbejdspladser og læringsmiljøer, demonstrerer den praktiske implementering af denne ramme og understøtter dette arbejde.

De vigtigste fordele ved at bruge ECSF viste sig at være:

- at sikre en **fælles terminologi** og **fælles forståelse** vedrørende cybersikkerhed fagfolk i hele EU;
- identifikation af de **kritiske færdigheder, der** kræves ud fra et cybersikkerhedsperspektiv arbejdsstyrke til at støtte dens videre udvikling og forbedring;
- at fremme **harmonisering** inden for cybersikkerhedsuddannelse , **træning** og **arbejdsstyrke udviklingsprogrammer .**

Denne ECSF-brugermanual giver et omfattende overblik over ECSF's vigtigste anvendelsesområde, rammeprincipper og anvendelsesmuligheder. Det primære formål med manualen er at gøre ECSF let tilgængelig for, forståelig for og anvendelig af alle interessenter med en aktiv rolle eller behov for passende kvalificerede cybersikkerhedsprofessionelle.

Den europæiske Cybersikkerhed Færdigheder Ramme (ECSF) har til formål at styrke europæisk cybersikkerhedskultur ve almindelige Europæisk sprog på tværs af samfund, der tager et væsentligt skridt fremad mod Europas digitale fremtid.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

1. INTRODUKTION

Manglen på cybersikkerhedsfærdigheder er en af de vigtigste udfordringer, der skal løses for et cybersikkert EU. Mere specifikt er der mangel på kvalificeret og kvalificeret personale på arbejdsmarkedet til at påtage sig roller inden for cybersikkerhed, og som i tilstrækkelig grad kan adressere de udviklende cybertrusler og de nye cybersikkerhedsudfordringer. Kløften i cybersikkerhedsfærdigheder har en række underliggende drivere. Disse omfatter et utilstrækkeligt niveau af forståelse af de kompetencer og færdigheder, der er nødvendige i cybersikkerhedsdisciplinen mellem forskellige aktører på markedet for cybersikkerhedsfærdigheder. I årenes løb er dette blevet et veldokumenteret problem[2] , som fortsat påvirker lande i væsentlig grad på europæisk og internationalt plan.

For at reducere den nuværende og den fremtidige kvalifikationskløft og mangel, er der behov for flere cybersikkerhedsprofessionelle med passende kvalifikationssæt. Til dette formål, den europæiske dagsorden for færdigheder[3] , handlingsplanen for digital uddannelse[4] og færdighedspagten[5] er fortsat vigtige redskaber for mobilisering af interessenter til at arbejde sammen mod målene for det digitale årti[6] ved at skabe flere og bedre muligheder for uddannelse.

I denne sammenhæng lancerede ENISA en ad hoc-arbejdsgruppe om den europæiske cybersikkerhedsfærdighedsramme[7] i december 2020. En tværfaglig gruppe af eksperter blev samlet med det formål at fremme harmonisering af cybersikkerhedsuddannelse, -træning og arbejdsstyrkeudviklingskoncepter. Den udviklede ramme (ECSF) giver et åbent europæisk værktøj til at opbygge en fælles forståelse af de professionelle cybersikkerhedsrolleprofiler og fælles kortlægninger med de nødvendige færdigheder og kompetencer. Dette arbejde danner grundlag for at forene kræfterne i et kapacitetsopbygningsprogram for den europæiske cybersikkerhedsarbejdsstyrke i overensstemmelse med den løbende markedsefterspørgsel.

ECSF giver et åbent europæisk værktøj til at bygge en almindelige forståelse af

cybersikkerhedsfaglige ro almindelige kortlægninger med passende færdigheder og nødvendige kompetencer.

1.1 MÅL PUBLIKUM

Mens det ultimative omfang af indholdet af ECSF-rammen er cybersikkerhedsprofessionelle, lægges der også særlig vægt på ECSF-målgrupperne af ikke-cybersikkerhedseksperter, som har brug for et omfattende overblik over disciplinen. Dette fokus gør rammen let at forstå for alle berørte interessenter.

Målgruppen for ECSF er organisationers ledelsesteams, menneskelige ressourcer (HR) og cybersikkerhedsfunktioner, cybersikkerhedsprofessionelle, nytilkomne og cyberentusiaster samt udbydere af læringsprogrammer af alle typer i den offentlige og private kontekst, brancheforeninger, marked forskere og politiske beslutningstagere.

Det ultimative omfanget af ECSF-ramme er cybersikkerhed kerne fagfolk, mens der også lægges vægt på ikke-

cybersikkerhedseksperter, der samlet overblik over disciplin.

1.2 MANUALENS STRUKTUR

Brugermanualen er opbygget som følger:

- Kapitel 1 introducerer de centrale udfordringer, der fremhæver behovet for at skabe rammer for cybersikkerhedsfærdigheder såvel som målgruppen for dette arbejde;
- Kapitel 2 præsenterer ECSF-designprincipperne samt de vigtigste fordele ved at bruge det;

[2] ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196
[4] https://education.ec.europa.eu/focus-topics/digital-education/action-plan
[5] https://ec.europa.eu/commission/presscorner/detail/da/qanda_20_1197
[6] https://digital-strategy.ec.europa.eu/en/node/157
[7] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

- Kapitel 3 forklarer de forskellige anvendelser af ECSF fra forskellige synspunkter.

Derudover indeholder dokumentet to (2) bilag, der understøtter ECSF-brugermanualen og dens mål:

- Bilag A forbinder ECSF med andre EU-standarder og -rammer.

  Formålet med dette bilag er at forbinde ECSF med eksisterende anerkendte europæiske standarder og rammer, der er relevante for dette arbejde.
- Bilag B viser Use Cases af ECSF.

  Formålet med dette bilag er at tilvejebringe virkelige case-scenarier for at vise den praktiske implementering af denne ramme.

2. FORSTÅELSE AF ECSF

ECSF består af et repræsentativt sæt af **12 rolleprofiler for cybersikkerhedsprofessionelle** (præsenteret i figur 1), som typisk kræves og anvendes i organisationer, der implementerer cybersikkerhedsprofessionelle. Hver profil er defineret af en fælles skabelon, der inkorporerer nøglekriterier (dvs. titel, alternative titler, resuméerklæring, mission, hovedopgaver, nøglefærdigheder, nøgleviden, e-kompetencer). Indholdet af hvert kriterium er skræddersyet til hver rolle, men er underlagt mulig tilpasning for at muliggøre en fleksibel implementering for at imødekomme specifikke situationer og krav.

Figur 1: ECSF's 12 rolleprofiler for cybersikkerhedsprofessionelle

ECSF introducerer et repræsentativt sæt af 12 rolleprofiler for

cybersikkerhedsprofess

De 12 rolleprofiler for cybersikkerhedsprofessionelle leveres i et EU-aftalt, praksisdrevet format dedikeret til det professionelle cybersikkerhedsdomæne. Profilerne er letforståelige og tilbyder alternative indgange alt efter kontekst, perspektiv og behov.
Gennem disse profiler kan ECSF bruges som et fælles reference- og kommunikationsværktøj, der kan anvendes på tværs af forskellige organisationer og lande til en fælles gensidig intern og ekstern forståelse.

Strukturen af hver rolleprofil er skitseret i tabel 1 nedenfor.

Tabel 1: Komponenterne i hver ECSF-rolleprofil

Profil titel	Navnet på den professionelle rolleprofil
Alternative titler	Viser typiske alternative titler under samme profil.
Sammenfattende erklæring	Angiver hovedformålet med profilen.
Mission	Beskriver begrundelsen for profilen.
Leverance(r)	En liste over typiske resultater af profilen, der også forklarer profilens relevans fra et ikke-ekspert synspunkt.
Hovedopgave(r)	En liste over typiske opgaver udført af den profilerede rolle.
Nøglekompetencer)	En liste over nødvendige evner til at udføre rollens arbejdsfunktioner og pligter. Bløde færdigheder og etik udtrykkes i nogle tilfælde.
Nøgleviden	En liste over den væsentlige viden, der kræves for at udføre arbejdsfunktionerne og pligterne i den profilerede rolle.
e-kompetencer (EN16234-1 e-CF)	Tilslutning til EN16234-1 e-Competence Framework (e-CF) - En fælles europæisk ramme for IKT-professionelle i alle sektorer.

Som vist i tabel 1 er profilen for hver rolle udfyldt af et sæt beskrivende elementer designet til at give et øjebliksbillede af rollen med hensyn til dens beskrivelse, opgaver og kompetencer.
Titler og typiske alternative titler kan bruges som en hurtig reference til at guide ECSF-brugere til de mest passende rolleprofiler til deres ansøgning.

Komponenter i rolleprofilerne **kan ændres,** så de bedre dækker interessenternes behov, og **rolleprofiler** (fra ECSF og andre rammer) **kan blandes sammen** af samme årsag. Yderligere oplysninger om anvendelse af ECSF findes i kapitel 3.

Bløde færdigheder (også kaldet tværgående, overførbare eller adfærdsmæssige færdigheder) er komponenter, der er nødvendige i ethvert professionelt færdighedssæt; derfor er sådanne færdigheder også nødvendige for fagfolk inden for cybersikkerhedsdomænet. En bred vifte af færdigheder falder ind under bløde færdigheder såsom evnerne til at kommunikere, samarbejde med andre, rapportere, påvirke, tænke kritisk og håndtere tid og stress. Bløde nøglefærdigheder er inkorporeret i nøglefærdighedskomponenten.

Eksempelvis omfatter rolleprofilen for en Chief Information Security Officer (CISO) som nøglefærdigheder evnerne til at påvirke, lede, kommunikere, samarbejde og samarbejde. Alle disse er essentielle færdigheder, hvis en CISO skal nå sine missioner og opgaver. Baseret på en interessents behov, kan der tilføjes flere bløde færdigheder til profilen for en CISO, eller der kan laves en kortlægning med en ramme for bløde færdigheder.

Etik er også et vigtigt tværgående element, som påvirker alle aspekter af cybersikkerhed og er derfor en væsentlig færdighedskomponent inden for den europæiske cybersikkerhedsfærdighedsramme (ECSF). I forbindelse med cybersikkerhed handler etik om, hvilke beslutninger der er i overensstemmelse med vores værdier, og hvad der er moralsk acceptabelt for både dataejeren og organisationen. Da cybersikkerhedsprofessionelle kunne få privilegeret adgang til forskellige typer information, selv følsomme oplysninger, er etisk bevidsthed en vigtig værdi, de bør have. Bortset fra det er etisk beslutningstagning en vigtig færdighed, som cybersikkerhedsprofessionelle bør have

deres beslutninger påvirker andre individer. Som i tilfældet med bløde færdigheder analyserede ECSF eksplicit, om den etiske side af sektoren er i overensstemmelse med europæiske værdier og etik.

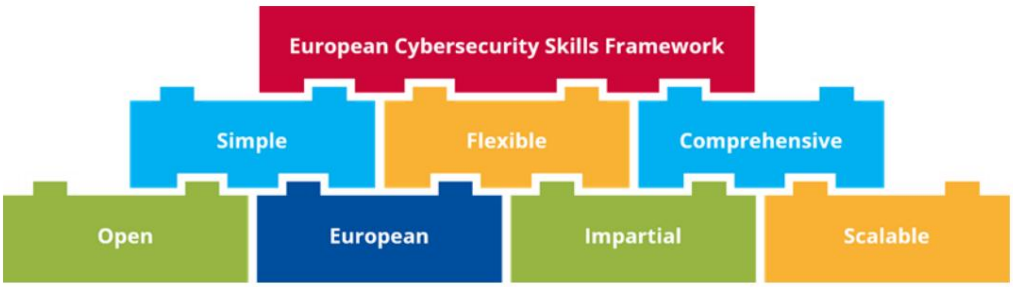
En mere detaljeret analyse af de bløde og etiske færdigheder kan foretages af den interesserede part, da rammerne er fleksible og tilpasningsdygtige.

2.1 ECSF'S DESIGNPRINCIPPER

European Cybersecurity Skills Framework er baseret på en række principper designet til at dække interessenternes behov. Dette giver nem forståelse, vedtagelse og anvendelse af rammen, samtidig med at relevans og effekt bevares på kort og længere sigt.

ECSF er baseret på principper designet til at dække over interessenternes behov, der giver nem forståelse, adoption og anvendelse, samtidig med at relevans og effekt bevares på kort og længere

Figur 2: ECSF's designprincipper



2.1.1 Enkel, men omfattende

Rammen er designet til at være passende generel for at sikre, at den let kan forstås og anvendes af et bredere publikum. Samtidig indeholder den tilstrækkelige detaljer til at give dybdegående cybersikkerhedsindsigt. Disse egenskaber letter brugen af rammerne på tværs af et bredt spektrum af aktiviteter og miljøer og af interessenter fra en række forskellige baggrunde (f.eks. organisationer af forskellig størrelse, teknisk ekspertise af forskellig intensitet og forretningssektorer med forskellige kerneaktiviteter).

Dette er opnået ved at anvende det passende detaljeringsniveau på indholdet af ECSF, som ikke er for specifikt eller for abstrakt. Med 12 profiler dækker ECSF et bredt spektrum af forskellige arbejdsaktiviteter, men opretholder et brugervenligt format.

2.1.2 Fleksibel og skalerbar

Ved at anvende en modulær tilgang og en fleksibel struktur gør rammen det muligt for hver komponent at blive udvidet eller brugt uafhængigt. Disse karakteristika understøtter yderligere udvidelse af ECSF og/eller kobling til andre rammer for at udvide dens anvendelser.

Ved at anvende denne fleksibilitet kan profilerne og deres komponenter, som defineret af ECSF, anvendes på et modul-for-modul-basis, så hver enkelt kan tilpasses til at opfylde specifikke behov. Denne fleksibilitet sikrer rammeverkets relevans gennem årene og vil også tillade simple opdateringer af rammeværket i fremtiden.

2.1.3 Åben og upartisk

Rammen er udviklet med input fra en stor og mangfoldig arbejdsgruppe af professionelle cybersikkerhedseksperter. For at udvikle en upartisk ramme oprettede ENISA denne gruppe fra en række eksperter med forskellig baggrund. Ved at involvere eksperter med forskellig baggrund fulgte udviklingsprocessen af rammen en multi-perspektiv tilgang, der eliminerede enhver skævhed over for specifikke interesseområder. Som ENISA-publikation er rammen desuden offentligt tilgængelig, tilgængelig og åben.

ECSF-profilerne og -komponenterne er udviklet ud fra et multi-stakeholder-perspektiv med fokus ikke kun på synspunktet om beskæftigelse inden for cybersikkerhed, men også fra udbydere af læringsprogrammers perspektiv. Ydermere er rigtigheden af rammerne blevet styrket af engagement og anmeldelser fra en række yderligere interessenter.

2.1.4 Europæisk

Drevet af kravet om at minimere huller i cybersikkerhedsfærdigheder og mangel i arbejdsstyrken i hele Europa, skulle ECSF være i overensstemmelse med specifikke europæiske krav for at muliggøre nem vedtagelse og brug af europæiske organisationer. Denne retning blev informeret ved at overholde eksisterende europæiske standarder og rammer.

ECSF forbinder sig godt med det nuværende europæiske IKT-professionelle landskab for at sikre nem anvendelse og bred anerkendelse. ECSF drager det bedste udbytte af eksisterende erfaringer og strukturer og giver konsekvente forbindelser til relevante EU-IKT-faglige standarder og -rammer. De profiler, der er defineret af rammen, er designet til at være kompatible og komplementære til europæiske love og regler og til at forbedre tilgange til europæisk etik, som identificeret på det europæiske marked. ECSF tager hensyn til kravene til beskyttelse af data og privatlivets fred fastsat af europæiske regler, fælles jobroller, som det europæiske marked anmoder om, og europæiske standarder og rammer, der anvendes i ikt-sektoren.

2.2 DE VIGTIGSTE FORDELE LEVERET AF ECSF

ECSF er et let at bruge, men alligevel omfattende værktøj. Den er baseret på nyere markedsundersøgelser, samarbejdet mellem cybersikkerhedseksperter og en analyse af det bredere cybersikkerheds- og IKT-rammerlandskab. Det udtrykker således de relevante behov på det europæiske marked. Den består af 12 typiske professionelle roller inden for cybersikkerhed, med en relateret sammenfattende erklæring, mission, observerbare resultater (leverancer), opgaver, kompetencer, færdigheder, viden og færdighedsniveauer, som krævet og anvendt i forbindelse med arbejde i Europa. forstået og brugt i hele Europa.

ECSF giver en utvetydig reference til at identificere og reducere nuværende og fremtidige cybersikkerhedskompetencemangler og huller. Det er generisk, men samtidig tilstrækkeligt granulært til at give EU-markedet en klar taksonomi af færdigheder, kompetencer og erhverv i cybersikkerhedsarbejdsstyrken. Desuden kan den let forbindes med andre eksisterende strukturer og rammer på tilknyttede områder.

ECSF giver en utvetydig reference til at identificere og reducere nuværende og fremtidige cybersikkerhedskompet

Brugen af ECSF som et fælles europæisk sprog til professionelle cybersikkerhedsroller, færdigheder, viden og kompetencer giver mange fordele, hvoraf nogle er anført nedenfor.

1. Brug af ECSF sikrer en fælles terminologi og fælles forståelse mellem cybersikkerhedsfaglig efterspørgsel (arbejdsplads, rekruttering) og udbud (kvalifikation, uddannelse, vurdering og anerkendelse) i hele EU.
2. ECSF støtter identifikation af kritiske kvalifikationskrav fra arbejdsstyrkens perspektiv. Det gør det muligt for udbydere af læringsprogrammer at støtte udviklingen af kritiske færdigheder og politiske beslutningstagere til at støtte målrettede initiativer for at afbøde identificerede huller i færdigheder.
3. ECSF hjælper med at forstå professionelle cybersikkerhedsroller og de nødvendige væsentlige færdigheder og relevant lovgivning. Især ikke-eksperter og HR-afdelinger er i stand til bedre at forstå kravene til cybersikkerhedsressourceplanlægning, rekruttering og karriereplanlægning.

4. ECSF fremmer harmonisering inden for cybersikkerhedsuddannelse, træning og udvikling af arbejdsstyrken. Derudover er brugen af et fælles europæisk sprog i cybersikkerhedsfærdigheder og -roller direkte relateret til hele det professionelle IKT-domæne.

5. ECSF bidrager til at opnå bedre modstandsdygtighed over for cyberangreb og til at sikre sikre ikt-systemer på tværs af samfundet. Det giver en standardstruktur og giver råd om, hvordan man håndhæver kapacitetsopbygning i den europæiske cybersikkerhedsarbejdsstyrke.

ECSF giver yderligere fordele baseret på typen af interessenter. Et eksempel på de vigtigste interessenter og de vigtigste tilknyttede hovedfordele er vist i 3.

Figur 3: Et eksempel på de vigtigste ECSF-modtagere, der udtrykker behovet for en fælles risiko Manager definition

En detaljeret liste over potentielle anvendelser og fordele ved at bruge ECSF baseret på interessenter er vist i tabel 2.

Tabel 2: ECSF's potentielle anvendelser og fordele for interessenter

Interessent	Fordele ved at bruge ECSF
Organisationer	• understøtter udviklingen af en cybersikkerhedsstrategi og organisationsstruktur • støtter udviklingen af cybersikkerheds menneskelige ressourceplanlægning • yder støtte i rekrutteringsprocessen, især: o identifikation af cybersikkerhedsrollekrav o vurdering af cybersikkerhedskandidater • giver analyse af cybersikkerhedsrolle og kvalifikationskløft og deraf følgende prognose af behov på individ-, team- eller organisationsniveau • definerer udviklings- og træningsplaner på individ-, team- eller organisationsniveau • understøtter evalueringen af cybersikkerhedsroller ved at hjælpe med at opbygge tilpassede skabeloner til cybersikkerhedsroller • giver et fælles og letforståeligt sprog til cybersikkerhedsudbud, indkøb, stillingsopslag og revision
Udbydere af læringsprogrammer	• understøtter design af læringsprogrammer og læseplaner, re-design og vedligeholdelse • tilbyder samarbejde på tværs af institutioner og mobilitet i læringsprogrammer, fx tværeuropæiske læringsprogrammer fra flere institutioner • fremmer tilbud om læringsprogrammer og øger bevidstheden • positionerer læringsresultater i en reel arbejdspladssammenhæng • understøtter vurderings- og anerkendelsesprocesser • giver karriereorientering til studerende

Enkeltpersoner	• støtter enkeltpersoner i at træffe professionelle karrierevalg og positionering dem selv • udvider læringsperspektiver, åbner nye karriereveje og fremmer professionelle udvikling til at understøtte omskoling og opkvalificering • hjælper med at forstå praktiske krav på arbejdspladsen og jobforventninger i mere detalje • identificerer formelle og ikke-formelle læringsveje • yder støtte til at bygge karriereveje
Professionel foreninger	• muliggør konsolidering af interessentsamfund for at understøtte videndeling, nye udviklinger, forbedringer og yderligere implementering i EU's medlemslande • yder støtte til at udføre markedsanalyser og præsentere resultaterne i et fælles sprog • hjælper med at give omfattende professionel vejledning i cybersikkerhedssektoren
Politikere og statslige interessenter	• understøtter en fælles forståelse inden for cybersikkerhedsområdet • stimulerer prioriteringsplanlægning og kapacitetsopbygning af cybersikkerhed • muliggør en kortlægning af mange cybersikkerhedsinitiativer baseret på ECSF-profilerne • understøtter politiske initiativer baseret på dataanalysen
Alle	• tilbyder et fælles sprog for alle interessenter • accelererer samarbejdet ved at give et fælles reference udgangspunkt • giver en fælles reference til at indsamle og præsentere cybersikkerhedsfaglig relaterede oplysninger og behov på alle niveauer, på nationalt, europæisk og internationalt niveau

3. ANVENDELSE AF ECSF

Dette kapitel demonstrerer, hvordan den europæiske cybersikkerhedsfærdighedsramme (ECSF) kan anvendes på en modulær og fleksibel måde baseret på behovene hos forskellige interessenter.

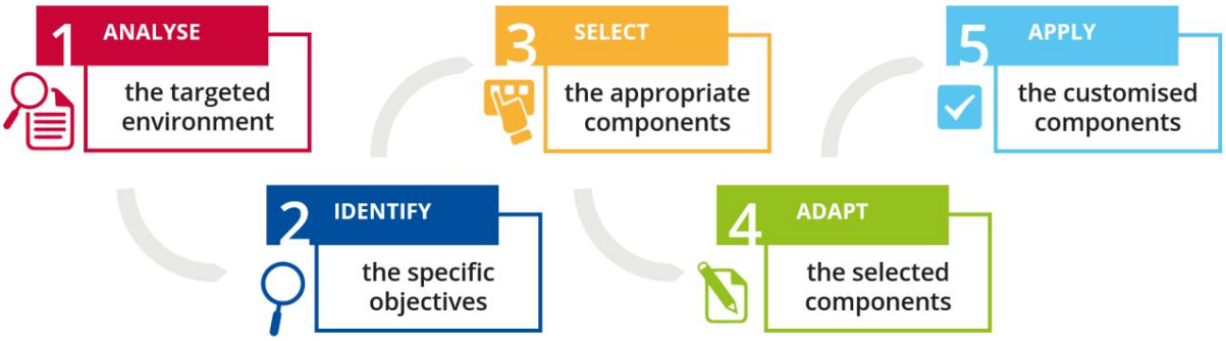
Specifik brug og praktisk anvendelse afhænger af mange faktorer såsom markedsperspektivet, organisationens størrelse, konteksten for en bestemt præstation og det overordnede formål.

De 12 rolleprofiler for cybersikkerhedsprofessionelle defineret af ECSF er et fleksibelt værktøj og en standardeuropæisk reference til skræddersyet brug i en bestemt kontekst.

Følgende generelle fem-trins guide giver grundlæggende orientering:

Rollen 12 profiler defineret af ECSF er et fleksibelt værktøj og en standard Europæisk reference for tilpasset brug i en bestemt sammenhæng.

Figur 4: En modulær vejledning i fem trin til anvendelse af ECSF



1. **Analyser** situationen i målmiljøet.
   Indsaml og bearbejd de nødvendige oplysninger om den cybersikkerhedsrelaterede tilstand i målmiljøet (f.eks. en organisation) for at skabe en baseline. Identificer de involverede parter og det mål, der skal nås.

2. **Identificer** specifikke mål, der skal nås.
   Se på status for målmiljøet og identificer eventuelle specifikke cybersikkerhedsrelaterede krav, der skal dækkes, eller ethvert mål, der skal nås af det målrettede miljø. Afhængigt af situationen kan det være muligt at bruge ECSF som en taksonomi til at identificere de pågældende mål.

3. **Vælg** de relevante komponenter i ECSF.
   Gennemgå ECSF-profilerne og vælg profiler, der er relevante for en bestemt situation.
   Vælg derefter de komponenter, der hjælper med at dække behovene eller opnå de påkrævede mål for det målrettede miljø.

4. **Tilpas** de valgte komponenter efter dine behov.
   Foretag passende ændringer på udvalgte komponenter for bedre at passe til en bestemt situation og/eller målrettet miljø. ECSF-profilerne og/eller deres komponenter kan være

blandet, opdelt eller bragt ind i en sektorspecifik kontekst i henhold til behovene i hver enkelt situation.

5. **Anvend** de tilpassede komponenter til målmiljøet.
Tag handling ved hjælp af de skræddersyede ECSF-komponenter til at dække sikkerhedsrelaterede mål, der er nødvendige for at forbedre situationen i målmiljøet og for at nå det organisatoriske mål.

Tabel 3 viser nogle vejledende eksempler på ECSF-ansøgningerne efter de fem trin, der er præsenteret ovenfor.

Tabel 3: ECSF's modulære tilgang i praksis

Eksempel	Trin	Beskrivelse
Ansættelse af cybersikkerhedsprofessionelle i en organisation	1. Analyse	Analyser den aktuelle cybersikkerhedsrelaterede tilstand i organisationen.
	2. Identificer	Identificer manglen på personale til at håndtere stigningen i cybersikkerhedsproblemer.
	3. Vælg	Vælg den relevante opgave fra en ECSF-profil, der udtrykker en identificeret mangel på eller mangel på specifikke færdigheder.
	4. Tilpas	Kombiner ECSF-profilerne med opgaver af interesse for organisationen og strukturer nye roller med de opdaterede opgaver, færdigheder og viden for at imødekomme de skiftende organisatoriske behov og skabe ændrede cybersikkerhedsroller.
	5. Ansøg	Brug den nyoprettede profil til at skabe ledige stillinger målrettet organisationens specifikke behov.
Dygtige cybersikkerhedsprofessionelle	1. Analyser	Forstå organisationens forretningsmål og strategi.
	2. Identificer	Identificer enhver mangel på ekspertise og personale inden for cybersikkerhedsrelaterede områder.
	3. Vælg	Brug ECSF-profilen(erne) til at identificere de tilknyttede færdigheder og viden, som organisationen mangler.
	4. Tilpas	Analyser udvalgte færdigheder og viden fra ECSF for at identificere uddannelsesbehovene for en cybersikkerhedsprofessionel for at imødekomme organisationens behov.
	5. Ansøg	Identificer træningsinterventioner for at øge kompetencen hos organisationens arbejdsstyrke.
At træffe egne karrierevalg	1. Analyser	Vælg en karrierevej, du er interesseret i.
	2. Identificer	Identificer din mangel på færdigheder og den viden, der kræves for at bevæge dig ind i cybersikkerhedssektoren.
	3. Vælg	Identificer den eller de ECSF-profiler, som du finder nyttige ud fra et karriereudviklingsperspektiv, og brug de tilknyttede færdigheder, viden og kompetencer som retningslinjer for omskoling og opkvalificering.

	4. Tilpas	Forbedre de udvalgte ECSF-profiler ved at inkludere yderligere færdigheder og viden baseret på individuelle behov.
	5. Ansøg	Identificer et træningsprogram, der inkorporerer størstedelen af de færdigheder og vidensudvikling, der kræves for at omkvalificere eller opkvalificere profilen.

3.1 ANSÆTTELSE AF CYBERSECURITY PROFESSIONELLE – ANVEND DEN ECSF SOM ORGANISATION

ECSF giver et standardreferencesæt af 12 typiske roller, der udføres af cybersikkerhedsprofessionelle fra et organisatorisk perspektiv, og dækker organisationernes cybersikkerhedsbehov og de cybersikkerhedsprocesser, der skal følges for at sikre deres forretning, produkter, tjenester og deres forsyningskæder . **Rammen giver således en værdifuld vejledning og køreplan, ikke kun for at opbygge, udvide og drive cybersikkerhedsrelaterede funktioner i en organisation, men også til at sikre, at dens cybersikkerhedsrelaterede mission, vision og mål opfyldes.** En organisation kan således bruge ECSF som udgangspunkt eller guide til hurtigt og nemt at få adgang til de primære roller, der er nødvendige for at styre deres cybersikkerhedsrisici og opbygge deres cybersikkerhedstilgang. Samtidig giver ECSF-profilerne en fælles forståelse blandt de involverede parter vedrørende en organisations cybersikkerhedsroller.

ECSF kan bruges som vejledning og køreplan, der giver en almindelige forståelse blandt de involverede parter vedrørende en organisations cybersikkerhedsroller.

Tre vejledende eksempler, som præsenteres senere i dette kapitel, har til formål at vise den praktiske implementering af rammen i:

I. forbedring af en lille virksomheds cybersikkerhedspraksis;
II. rekrutteringsproces for en stor virksomhed med stigende overholdelseskrav;
III. planlægning af cybersikkerhedsressourcer i en stor organisation.

Eksempel I: *Forbedring af cybersikkerhedspraksis i en lille virksomhed* præsenterer anvendelsen af ECSF til at imødekomme behovene hos en lille virksomhed, der søger at forbedre sin cybersikkerhedsstruktur og -praksis. Det viser, hvordan en virksomhed kan bruge ECSF til at støtte udviklingen af en cybersikkerhedsstrategi, herunder planlægning af menneskelige ressourcer til cybersikkerhed og planlægning af indkøb af cybersikkerhed.

Ved at bruge ECSF som udgangspunkt eller som vejledning behøver virksomheden ikke at opfinde eller undersøge grundlæggende roller, der er nødvendige for at forbedre sin cybersikkerhedsposition. Rollerne kan tildeles forskellige personer eller kan slås sammen til at blive varetaget af kun én eller kun få personer afhængig af strategi, krav, behov og budget.

Eksemplet viser også, hvordan ECSF kan støtte organisationen i rekrutteringsprocessen ved at identificere de cybersikkerhedsroller og -ansvar, som er nødvendige i en lille virksomhed. I dette eksempel er der også givet en cybersikkerhedsrolle og kvalifikationsgab-analyse og deraf følgende prognose af behov på organisationsniveau. Ud over at støtte de menneskelige ressourceprocesser i forbindelse med rekruttering giver ECSF også et fælles sprog til indkøb af cybersikkerhedstjenester.

Eksempel I: Forbedring af cybersikkerhedspraksis i en lille virksomhed

En lille cloud-tjenestevirksomhed fik succes på få måneder efter, at grundlæggerne, søskende Alicia og Max, implementerede deres idé til en innovativ løsning. Alicia var eksperten 'techie' geni, mens Max var et marketing geni. Desværre havde ingen af dem nogen erfaring med at drive eller bygge en virksomhed. Efter et år begyndte virksomheden at tage fart, og de flyttede ind på deres eget kontor og ansatte personale til at vækste virksomheden. I løbet af dette

ekspansionsfasen overvejede ingen at organisere virksomheden. Mange roller og pligter blev delt, og udfordringer blev håndteret ad hoc. Heldigvis skete der ingen alvorlig cybersikkerhedshændelse i denne overgangsfase.

Til sidst fik virksomheden en vis medieeksponering, som gik viralt, hvilket resulterede i øget interesse fra nye investorer og kunder for den lille start-up. Større kunder og investorer krævede dog sikkerhed og bevis for passende sikkerhedsforanstaltninger og en organisationsstruktur, før de blev involveret i virksomheden. Grundlæggerne indså, at de virkelig ville være nødt til at forme tingene i deres organisation. De var klar over, at nøglen til **organisationens succes** var medarbejderne, og for at gøre det muligt for organisationen at blomstre og tilbyde robuste tjenester, **var det afgørende at definere deres cybersikkerhedsroller og -ansvar.**
Spørgsmålet, der skulle besvares, var dog, hvilket organisationssetup der var behov for, og hvilke roller og hvilke slags kompetencer havde organisationen brug for?

Finansieringsmidler **brugte ECSF og identificerede, at deres organisation krævede fem nøgleroller** for at understøtte deres cybersikkerhedsbaseline:

- en strategisk cybersikkerhedschef (CISO)
- en cybersikkerhedsjurist
- en cybersikkerhedsarkitekt
- nogle få cybersikkerhedsimplementere
- en cyberhændelsesbehandler.

Ved internt at **finde ud af ,** om deres **medarbejdere** var **i stand til at dække disse roller,** fandt de ud af, at deres juridiske medarbejder allerede styrede overholdelse af juridiske og regulatoriske rammer, og at hun havde en interesse i **at berige** sine **kompetencer inden for juridiske spørgsmål om privatliv og cybersikkerhed .** Human Resources ville være i stand **til at understøtte opkvalificering ved at bruge** en liste over nøgleviden **og** -færdigheder **opnået** fra **ECSF.**

Organisationens IKT-arkitekt havde tidligere erfaring med design af sikre netværk, og derfor kunne han med yderligere **træning for at opdatere og berige** sin **kompetence** også **dække organisationens arkitektoniske cybersikkerhedskrav.**

Systemadministratorerne fulgte mange bedste praksisser for cybersikkerhed, men arbejdede for det meste ad hoc uden en strategi eller struktur. Grundlæggerne **identificerede derfor et behov for at rekruttere en Strategic Cybersecurity Manager.** Rekrutteringsmedarbejderen fik til opgave **at udarbejde en jobbeskrivelse baseret på ECSF's CISO-profil** og med at anføre den ledige stilling på deres hjemmeside.

Endelig blev det fastslået, at virksomhedens hændelsesberedskabsfunktioner skulle fungere 24/7 for at sikre den kontinuerlige drift af tjenester.

Figur 5: De nødvendige nøgleroller som identificeret ved hjælp af ECSF og de foranstaltninger, der skal træffes

Eksempel I viste, hvor nyttig ECSF kan være til følgende fordele:

- forståelse af cybersikkerhedsroller
- identifikation af krav til arbejdsstyrken
- evaluere processer og struktur
- omskoling og/eller opkvalificering af medarbejdere
- understøtte rekrutteringsprocessen
- opbygning af cybersikkerhedskapacitet
- opbygning af en cybersikker og betroet organisation
- opbygning af modstandskraft mod cyberangreb.

Figur 6: Fordele ved at bruge ECSF som vist i eksempel I

Eksempel II: *Udarbejdelse af en jobbeskrivelse* demonstrerer anvendelsen af ECSF, når der oprettes en jobbeskrivelse. Det viser, hvordan ECSF kan være gavnligt set i forhold til menneskelige ressourcer uden behov for at have en dyb forståelse af cybersikkerhedsfaget. Dette eksempel viser, hvordan en ledig stilling kan oprettes, og hvordan man undgår skabelsen af vildledende eller forvirrende forventninger, og hvordan man tiltrækker passende kvalificeret personale. Det viser også, hvordan man kombinerer komponenterne i en ECSF-rolleprofil, og hvordan man tilpasser dem i overensstemmelse med en organisations jobbehov.

Dette eksempel viser, hvordan en organisation kan bruge ECSF til at skabe en beskrivelse af en rolle. Selv uden en HR-baggrund er det muligt at definere de opgaver, færdigheder og viden, der kræves af en kandidat til rekruttering ved at kende rollens mission. Udover at yde støtte til rekrutteringsprocessen, kan ECSF også hjælpe virksomheden med at definere uddannelsesplaner for nyansat personale. Det er bemærkelsesværdigt, at ECSF ikke kun giver et fælles sprog for indkøb af cybersikkerhed, men også til revisionsformål, især hvor princippet om ansvarlighed er ved at blive implementeret, og der kræves en væsentlig og klar adskillelse af opgaver.

Eksempel II: Udarbejdelse af en jobbeskrivelse

Et stort forsikringsselskab udvider sin portefølje til cybersikkerhedsforsikring, da mange kunder søger denne service. Efter en mindre intern omstrukturering og opdatering af personaleopgørelsen beslutter virksomheden at tilføje cybersikkerhed til compliance-afdelingen.
Følgelig konkluderer compliance-afdelingens ledelse, at **de skal rekruttere en Cyber Compliance Officer** til at understøtte den nye mission.

Virksomhedens HR-afdeling har til opgave at **finde og rekruttere den bedst egnede kandidat.** Da cybersikkerhed er et nyt område for organisationen, skal HR også **lave en rollebeskrivelse.** For at definere denne nye rolle, **interviewer HR** kyndige **ledere og medarbejdere** for at **identificere** behovene og **nøgleopgaverne for** denne stilling. Disse behov identificeres, og de udvalgte nøgleopgaver er som følger:

- sikre overholdelse af og give juridisk rådgivning og vejledning om databeskyttelse og databeskyttelsesstandarder, love og regler;
- identificere og dokumentere mangler i overholdelse;
- udvikle en revisionsplan, der beskriver rammer, standarder, procedurer og revision tests;
- udføre revisionsplanen og indsamle beviser og målinger;
- udvikle og formidle revisionsresultater (rapportering).

Den ansvarlige HR-medarbejder erkender, at dette er en kompleks rolle, og at der ikke findes nogen rekrutteringsskabeloner, der passer til denne rolle. Derfor **skal en ny rollebeskrivelse og skabelon oprettes** og godkendes af ledelsen.

HR-officeren, der nu **bruger ECSF, analyserer forskellige roller inden for rammerne.** De specificerede opgaver er inkluderet i **de nøgleopgaver, der er identificeret i rollerne** som **Cyber Legal, Policy & Compliance Officer** og **Cybersecurity Auditor.**

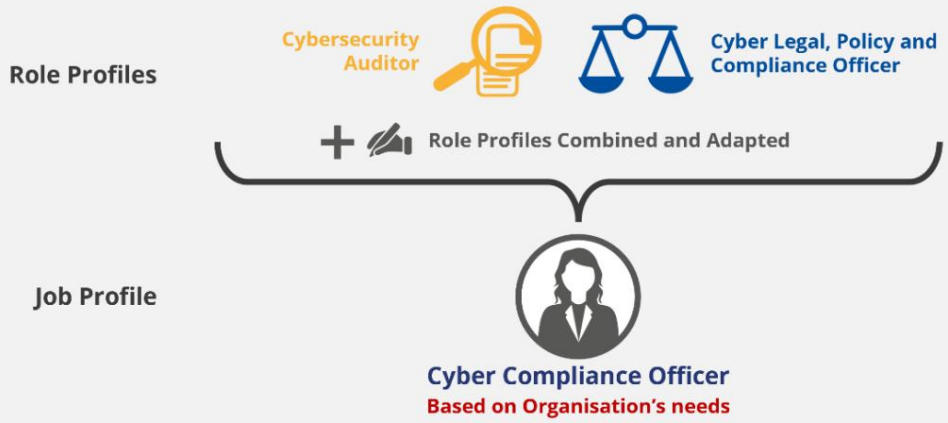
For at udføre disse opgaver er de identificerede **færdigheder og den nødvendige viden** som følger:

- Færdigheder
  - o forstå konsekvenserne af ændringer af den juridiske ramme for organisationens strategi og politikker for cybersikkerhed og databeskyttelse;
  - o følge og praktisere revisionsrammer, standarder og metoder;
  - o anvende revisionsværktøjer og -teknikker;
  - o arbejde som en del af et team og samarbejde med kollegaer.
- Viden
  - o avanceret viden om national, EU og international cybersikkerhed og relaterede privatlivsstandarder, lovgivning, politikker og regler;
  - o kendskab til overholdelse af informationssikkerhed og lovkrav på det internationale, nationale og EU-niveau;

o grundlæggende forståelse af datalagring, behandling og beskyttelse inden for systemer, tjenester og infrastrukturer.

En **ny rollebeskrivelse** skræddersyet til virksomhedernes behov kan nu skabes ved **at kortlægge og kombinere** dele af profilen for rollen som **Cyber Legal, Policy & Compliance Officer** og dele af profilen for rollen som **Cybersecurity Auditor.** Det er bemærkelsesværdigt, at ved at kortlægge rammerne er denne nye unikke rolle **baseret på ECSF's kerneindhold.** Dette giver en ensartet og struktureret rolle, der kan spores tilbage til dens oprindelse.

Figur 7: Cybersikkerhedsjobprofil oprettet baseret på ECSF-rolleprofilerne



Efter denne kortlægning til ECSF er den påkrævede rollebeskrivelse tilgængelig og kan bruges til at udarbejde den rolle og efterfølgende jobbeskrivelse, som HR har brug for for at opnå intern godkendelse og offentliggøre på virksomhedens rekrutteringswebsted. Yderligere elementer, såsom profilmission, kan bruges som indledende tekst til offentliggørelsen af denne stilling.

Eksempel II viste, hvor nyttig ECSF kan være til følgende fordele:

- forståelse af cybersikkerhedsroller
- identifikation af krav til arbejdsstyrken
- identifikation af rollekrav
- understøtte rekrutteringsprocessen
- understøtte opbygningen af en skræddersyet stillingsskabelon
- at bruge et fælles sprog til ledige stillinger.

Figur 8: Fordele ved at bruge ECSF præsenteret i eksempel II

Eksempel III: *En stor virksomhed med hovedforretning uden for IKT skal oprette en cybersikkerhedsafdeling* demonstrerer anvendelsen af ECSF, når den opretter en ny cybersikkerhedsafdeling og udarbejder en cybersikkerhedsstrategi for virksomheden. Den foreslår også en kategorisering af de 12 profiler i fire (4) makroområder for forståelse og kommunikation på højt niveau. Det viser, hvordan en stor organisation kan bruge ECSF til at støtte udviklingen af en cybersikkerhedsstrategi, herunder menneskelig ressourceplanlægning og talentudvikling inden for cybersikkerhed.

Eksempel III: En stor virksomhed med hovedforretning uden for IKT skal oprette en cybersikkerhedsafdeling

En stor virksomhed med en kerneforretning, der ikke er relateret til IKT eller cybersikkerhedstjenester, indså behovet for at beskytte sine værdifulde aktiver mod cybersikkerhedstrusler. Faktisk indeholdt den vedtagne forretningsstrategi en massiv plan for digitalisering af forretningsprocesser, og afhængigheden af IKT blev markant større for kritiske forretningsdrift.

Da virksomheden ikke havde nogen intern ekspertise til at håndtere cybersikkerhedsrisici, besluttede bestyrelsen at ansætte en Chief Security Information Officer (CISO) til at **definere den overordnede cybersikkerhed** strategi i overensstemmelse med virksomhedens forretningsmål. Dette ville også kræve, **at der oprettes en afdeling** til **håndtering af cybersikkerhedsrisici.**

CISO, der er nyudnævnt, **brugte ECSF som en rettesnor** og **som en** solid **reference** for de **cybersikkerhedsroller, der er nødvendige** for at håndtere sine cybersikkerhedsrisici. Hun brugte det som et **fleksibelt værktøj** til at hjælpe med **at strukturere en cybersikkerhedsafdeling.** Hun erkendte også, at for at give et klart skema ville det være nyttigt at placere **ECSF-rollerne i sammenhæng med en ledelsescirkel** under fire (4) makroområder: a) Plan, b) Implementer, c) Drift og d) Forbedre.

Figur 9: Placering af ECSF-rolleprofilerne i sammenhæng med en ledelsescirkel

På makroområdet Plan blev der fastsat prioriteter og mål, udviklet strategier, politikker og handlingsplaner, defineret arkitekturer, tildelt ressourcer. På dette makroområde var profilerne for CISO, Policy and Compliance Officer, Risk Manager og Arkitekter placeret naturligt.

Implementering af cybersikkerhedsforanstaltninger (Implementer) og uddannelse og bevidstgørelse (Educator) blev allokeret til Implement-makroområdet.

Den daglige drift var det mest 'håndgribelige' område. Som reaktion på hændelser (herunder SOC-hold) er retsmedicinske aktiviteter daglige aktiviteter for cybersikkerhedsspecialister.
Trusselsefterretningsprofilen blev også set som et operationsområde, da disse fagfolk arbejder på operationelle data ved hjælp af flere kilder.

Penetrationstester (testning for nuværende og nye trusler), Researcher (bringer nye teknologier og løsninger) og Auditor (identificering af huller) understøtter forbedringsfasen.

Men da ECSF er et fleksibelt værktøj til skræddersyet brug i en bestemt kontekst, **anvendte CISO 5-trins guiden til at tilpasse rolleprofilerne til hendes specifikke behov og mål.**
Analysen af ECSF-profilerne hjalp hende med **at definere de ressourceplaner ,** der var nødvendige for at nå virksomhedens mål.

På makroområdet Plan besluttede hun at:

- være ansvarlig for politik- og complianceopgaver for at strømline organisationsstrukturen;
- ansætte en cybersikkerhedsarkitekt, der vil hjælpe med at definere den overordnede arkitekturstrategi for at håndtere cybersikkerhedsrisici og sikre sikre-by-design-løsninger til at understøtte den digitale transformation;

- ansætte en cybersikkerhedsrisikomanager, som vil hjælpe med at vurdere virksomhedens cybersikkerhedsrisikoposition og hjælpe med at definere handlingsplaner for at håndtere de identificerede risici.

På makroområdet Implementering **udnyttede hun ECSF-færdigheds- og videnkomponenterne** til **at forstå, hvilken opkvalificering der kræves** for at udnytte de interne ressourcer, der er til rådighed, eller alternativt beslutte at ansætte eksternt. Det multinationale selskab havde et eksisterende hold af instruktører inden for et andet felt. Der var dog ikke noget specialistteam til at designe og gennemføre cybersikkerhedsbevidsthed eller træningskurser. CISO **undersøgte, om nogle af underviserne havde de færdigheder og den viden, som er anført i ECSF,** og om interessen **for at slutte sig til hendes nye hold.**

I Operate-makroområdet så CISO på, hvordan man administrerer de daglige cybersikkerhedsoperationer og besluttede at **oprette globale sikkerhedsoperationscentre med hændelsespersonale,** der arbejder på forskellige kontinenter for at yde support døgnet rundt. Desuden **blev en trusselsefterretningsspecialist ansat** til at give operationel indsigt til at guide jagten på trusler og mindske risikoen. CISO konkluderede, at der **ikke var behov for at ansætte en digital retsmedicinsk efterforsker ,** men snarere **at engagere et specialiseret konsulentfirma** til eventuelle **retsmedicinske behov.**

I Forbedre makroområdet besluttede CISO at ansætte en **ekstern tjenesteudbyder til penetrationstestning** med det formål at teste modstandsdygtigheden af virksomhedens infrastruktur og applikationer. CISO vurderede også det interne revisionsteams kapacitet og besluttede at **ansætte en cybersikkerhedsrevisor** til at revidere sikkerhedsrelaterede politikker. CISO følte ikke behov for at ansætte en cybersikkerhedsforsker, da cybersikkerhedsforskning lå uden for hendes organisations rammer.

For at opsummere fremhævede eksempel III, hvor nyttig ECSF kan være til følgende fordele:

- forståelse af cybersikkerhedsroller
- medvirke til at skabe en organisationsstruktur
- at identificere kravene til cybersikkerhedsroller
- hjælpe med planlægning af menneskelige ressourcer
- opkvalificering af medarbejdere
- understøtte bedømmelsen af kandidater
- bruge fælles terminologi til samarbejde.

Figur 10: Fordele ved at bruge ECSF vist i eksempel III

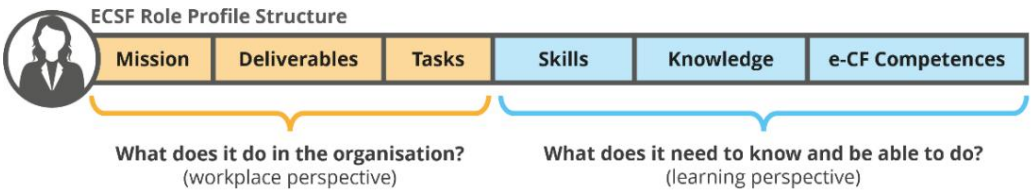
3.2 UDDANNELSE AF CYBERSIKKERHED PROFESSIONELLE – ANVEND ECSF SOM UDBYDER AF LÆRING

ECSF tilbyder et fælles sprog og ordforråd til udvikling af professionelle cybersikkerhedsfærdigheder til udbydere af læringsprogrammer og læringsinstitutioner af alle typer, såsom videregående uddannelse (HE), Vocational Education and Training (VET) eller enhver anden cybersikkerhedsrelateret uddannelsesprogram eller træning. De definerede rolleprofiler giver en cybersikkerhedsarbejdspladsdrevet, europæisk indlejret tilgang til at forbinde nuværende krav til professionel praksis med cybersikkerhedsrelaterede læseplaner og læringsprogrammer.

ECSF definerer de typiske krav til en profil ud fra to grundlæggende synspunkter.

- Hvad gør denne rolle i organisationen?
  Omhandler arbejdspladsens perspektiv (profilafsnit om mission, leverancer og opgaver)
- Hvad skal denne rolle vide og kunne?
  Håndter læringsperspektivet (profilafsnit om færdigheder, viden og e-CF-kompetencer)

Figur 11: ECSF's rolleprofilsektioner knyttet til arbejdspladsen og læringsperspektiverne



ECSF placerer læringsresultater i en reel kontekst på arbejdspladsen. Navnlig giver beskrivelser i ECSF-profiler af roller udbydere af læringsprogrammer mulighed for at gennemgå deres læseplaner på en struktureret og systematisk måde, herunder fra praktikernes synspunkt.

Som illustreret i bilag B.2 kan ECSF bidrage til adskillige aktiviteter, der gennemføres i akademiske institutioner.

- ECSF kan tjene til at udvikle eller opdatere læringsresultatet af kurser og tilpasse det til arbejdsmarkedets behov. Færdighederne, viden og kompetencer inden for en rolleprofil kan bruges til at guide udformningen af læseplaner og understøtte etableringen af ønskede læringsresultater. For eksempel, når man analyserer uddannelsesbehovene for et specifikt cybersikkerhedsjob, giver en tilpasset ECSF-profil et solidt udgangspunkt for at forstå tilknyttede uddannelseskrav.
- ECSF kan tjene som et samarbejdsværktøj til oprettelse af fælles akademiske programmer og til at tillade studerendes mobilitet.
- ECSF kan tjene som grundlag for definitionen af en ramme for et cybersikkerhedspensum, som vil hjælpe universiteter med at kortlægge hovedfokus for deres cybersikkerhedsprogram og kommunikere det til de studerende.

ECSF tilbyder almindelige sprog og ordforråd til udvikling af professionelle

cybersikkerhedsfærdigheder t

Som illustreret i bilag B.1 adresserer ECSF nogle af de udfordringer, der er identificeret i det europæiske landskab for professionelle cybersikkerhedskvalifikationer. I særdeleshed:

- ECSF understøtter en terminologi, der er aftalt på tværs af domæner og på tværs af industrien i relation til cybersikkerhedsfærdigheder;
- ECSF kan støtte udviklingen af en integreret platform for færdigheder til at levere ajourførte oplysninger om arbejdsmarkedet, kompetencer, uddannelseskurser, certificeringsordninger og en karriereplan.

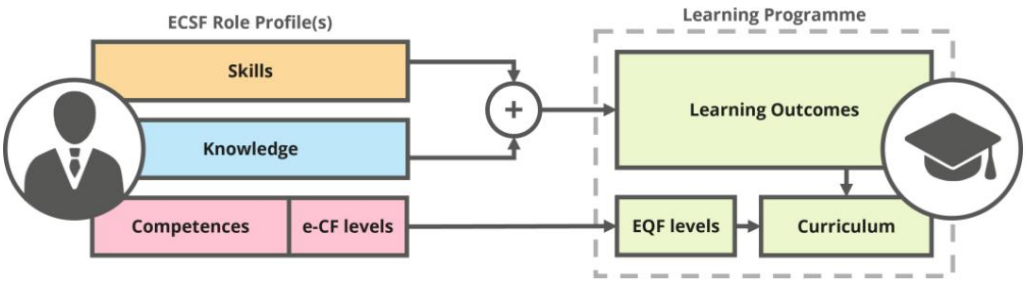
Figur 12: Fordele ved at bruge ECSF som udbyder af læring

ECSF kan være bruges som en meddelelse værktøj imellem arbejdsgivere og pædagoger.

I forbindelse med udviklingen af cybersikkerhedskvalifikationer og læseplansdesign fungerer ECSF-rolleprofilerne som et kommunikationsværktøj mellem arbejdsgivere og undervisere for at forbedre høringsprocessen og samarbejdsresultater. Arbejdsgiveren kan hurtigt definere de nødvendige aktiviteter eller opgaver og arbejde baglæns for at identificere de kompetencer, færdigheder og viden, som undervisere bør inkludere i læseplaner. Denne tilgang fremskynder betydeligt udformningen af læseplaner, der er aftalt mellem arbejdsgivere, regeringer og undervisere.

Figur 13 illustrerer, hvordan sektionerne af ECSF-rolleprofilerne, der er dedikeret til kompetencer, viden og færdigheder, kan bruges til at definere læringsresultater, identificere de passende niveauer af læringsprogrammer og skabe læseplaner for cybersikkerhedsbeskæftigelser. Da viden og færdigheder, ligesom alt indhold i rollebeskrivelser, er givet som vejledende eksempler for fleksibel tilpasning til konteksten, kan andre kilder også anvendes[8] .

Figur 13: ECSF-profiler, der vejleder professionel læring inden for cybersikkerhed



Forbindelse af læringsniveauer (EQF) og arbejdspladsfærdighedsniveauer (e-CF)

Den europæiske referenceramme for kvalifikationer (EQF) er en fælles europæisk referenceramme for kvalifikationer. Formålet med EQF er at sammenligne kvalifikationer og læringsresultater, der opstår i forskellige lande og nationale uddannelsessystemer. EQF er baseret på

[8] Sektionerne for færdigheder, viden og kompetencer i ECSF er hverken udtømmende eller begrænsende, hvilket giver brugeren mulighed for at berige dem ved også at inkludere eksterne ressourcer, f.eks. Cyber Security Body Of Knowledge (CyBOK) https://www.cybok.org/, FFC-klassifikation https://joint-research-centre.ec.europa.eu/publications/unified-conceptual-framework-tasks-skills-and-competences_en

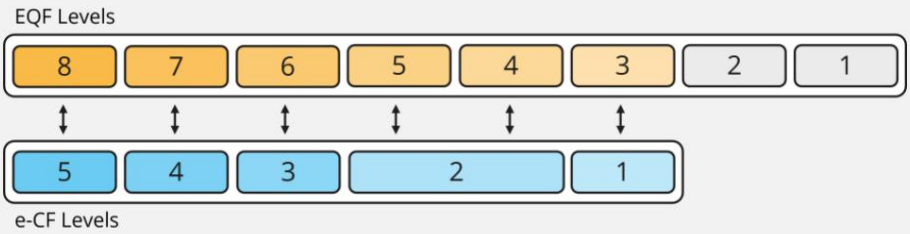
Henstilling om den europæiske kvalifikationsramme for livslang læring vedtaget af Europa-Parlamentet og Rådet den 23. april 20089 .

EQF definerer otte (8) uddannelsesniveauer med deskriptorer, der adskiller hvert niveau. Kriteriet for hvert niveau er baseret på vurdering af viden, færdigheder, ansvar og autonomi.

Den **europæiske e-kompetenceramme (e-CF),** standard EN 16234-1, der anvendes af ECSF, er en fælles europæisk ramme for IKT-faglige kompetencer, viden og færdigheder10. Det vedrører kompetencer efter behov og anvendt på arbejdspladsen. Dimension 3 af e-CF definerer kompetenceniveauer, der stammer fra arbejdspladsens færdigheder. Der er fem (5) definerede e-kompetenceniveauer e-1 til e-5 relateret til EQF-læringsniveauerne 3 til 8 (EQF-niveau 1 og 2 er ikke relevante i denne sammenhæng).

Forholdet mellem e-CF niveauerne e-1 til e-5 med EQF niveauerne 3 – 8 er illustreret nedenfor:

Figur 14: Forholdet mellem EQF og e-CF niveauer



På grund af dette systematisk udviklede forhold er det muligt at relatere e-CF-færdighedsniveauerne til EQF-læringsniveauerne. Forholdet er på grund af den forskellige karakter af hver ramme ikke af fuld ækvivalens. Den kan dog anvendes for at øge gennemsigtigheden og **skabe et fælles sprog mellem krav til faglige kompetencer på arbejdspladsen og relaterede kvalificationer fra uddannelsesinstitutioner11.** Således kan e-CF-kompetenceniveauerne, der er indarbejdet i ECSF-rolleprofilerne, derfor bruges som en generel vejledning til påkrævede uddannelsesniveauer.

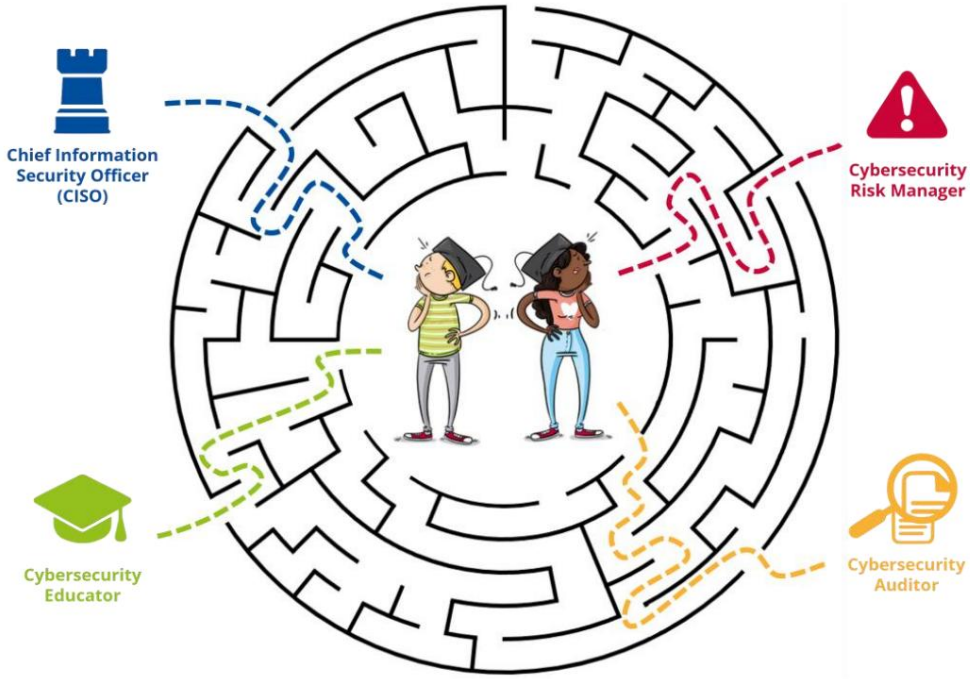
[9] European Qualifications Framework for livslang læring
[10] EN16234-1:2019: e-Competence Framework (e-CF) – en fælles europæisk ramme for IKT-professionelle i alle sektorer

[11] For yderligere praktisk vejledning se: CEN/TS 17699:2022 Retningslinjer for udvikling af IKT-professionelle læseplaner i henhold til omfanget af EN16234-1 (e-CF)

3.3 AT TAGE EGNE KARRIEREVALG – ANVEND ECSF SOM EN INDIVIDUELT PROFESSIONEL

Det fælles sprog, der er defineret af ECSF, kan bruges til at fjerne enhver forvirring mellem professionelle cybersikkerhedsjobroller og cybersikkerhedsuddannelsesprogrammer. Ved at give et fælles sprog og en klar beskrivelse af de professionelle jobroller inden for cybersikkerhed, de opgaver, der forventes at blive udført af dem, samt de færdigheder, de kompetencer og den nødvendige viden, kan ECSF opbygge en fælles forståelse og skabe klarhed påkrævet for at tiltrække nye personer til cybersikkerhedsområdet eller hjælpe dem med at planlægge deres karriereveje.

Figur 15: Brug af ECSF til at definere individets karriereveje



ECSF kan bygge en fælles forståelse og give den klarhed, der kræves for at tiltrække nye enkeltpersoner ind cybersikkerhedsområdet eller assist dem i planlægningen af deres karriere stier.

Fagfolk, der allerede arbejder i cybersikkerhedsrelaterede stillinger, kan bruge ECSF som en guide til at komme videre inden for deres felt. Ved at kortlægge deres færdigheder og viden til ECSF rolleprofiler af interesse, kan enkeltpersoner identificere eventuelle manglende færdigheder eller viden, som de har brug for at udvikle, mestre eller lære, så de er klar til at dække fremtidige jobkrav eller mulige overgange mellem cybersikkerhedsroller, mens de udvikler deres professionel karriere. Dette hjælper dialogen mellem medarbejdere og arbejdsgivere ved planlægning af efteruddannelse inden for cybersikkerhed. Da ECSF angiver både formelle og ikke-formelle læringsveje, hjælper den også nytilkomne, som ikke er klar over, hvor de skal starte. At tilføje til tidligere viden og kompetencer er ofte en lettere vej end at starte helt forfra. Bilag B.6 omhandler dette emne og giver dybere indsigt og eksempler i "individuel karrierebeslutningstagning" ved hjælp af ECSF.

Ved at bruge ECSF som udgangspunkt kan en person identificere de nødvendige kompetencer og færdigheder for at flytte fra en rolle til en anden eller identificere aktuelle uddannelsesbehov.

Det fælles sprog, der er defineret af ECSF, kan være nyttigt for personer, der leder efter job inden for cybersikkerhed. ECSF kan hjælpe med at filtrere jobåbninger og med at forstå jobbeskrivelsen, samtidig med at det også kan gøre jobbets overordnede mobilitet inden for cybersikkerhed lettere ved at kortlægge individets færdigheder, viden og kompetencer til ECSF.

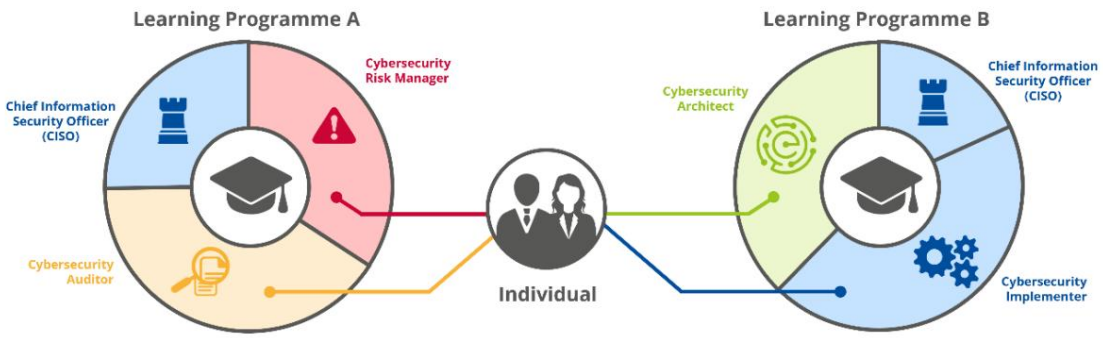
Cybersikkerhed er en god karrieremulighed, selv for personer, der i øjeblikket er specialiseret i andre områder, og derfor er omskoling af folk og flytning af dem til cybersikkerhedsområdet en god måde at tilfredsstille markedets arbejdsstyrkes behov og reducere arbejdsstyrkens kløfter på området. Da cybersikkerhed er et tværfagligt emne, kunne et sådant karriereskift være hurtigere for personer med en baggrund tæt på et af hovedaspekterne af feltet12:

- **teknisk** – relateret til teknologi, konkrete teknologiske tilgange og løsninger der kan bruges til at bekæmpe cyberkriminalitet og cyberterrorisme;
- **menneskelig** – relateret til menneskelige faktorer, adfærdsmæssige aspekter, privatlivsspørgsmål, samt øge bevidstheden om og viden om samfundet med hensyn til cyberkriminalitet og terrortrusler;

- **organisatorisk** – relateret til processer, procedurer og politikker i organisationer, samt samarbejde (offentlig-privat, offentlig-offentlig) mellem organisationer;
- **regulatorisk** – relateret til lovens bestemmelser, standardisering og retsmedicin.

Ved at have en klar forståelse af hovedprofilerne for cybersikkerhedsroller på området og et fælles cybersikkerhedssprog på tværs af en bredere vifte af sektorer som leveret af ECSF, kan enkeltpersoner, der søger at skifte karriere mod cybersikkerhed bruge ECSF som udgangspunkt for at identificere specifikke kompetencer færdigheder og viden, som de skal tilegne sig for overgangen.

Figur 16: Brug af ECSF til at analysere og sammenligne cybersikkerhedslæringsprogrammer



Uanset om personen allerede arbejder med cybersikkerhed (søger at udvide deres viden), i øjeblikket er ansat i et andet felt (søger at skifte karriere) eller søger en akademisk uddannelse (ønsker at arbejde med cybersikkerhed i fremtiden), kan ECSF hjælpe med forståelse af hovedprofilerne af cybersikkerhedsroller (ved at give en beskrivelse og analysere dem i opgaver, færdigheder, viden og kompetencer) samt hjælp til analyse og sammenligning af tilgængelige læringsprogrammer (kortlægning af læringsresultaterne til de nødvendige færdigheder og viden om foretrukne cybersikkerhedsprofiler).

ECSF skaber en almindelige terminologi og delt forståelse af cybersikkerhedsprofessionell eliminere forvirring i terminologi og enhver mangel på forståelse

3.4 OPBYGNING AF CYBERSIKKERHEDSFÆLLESSKABER – ANVEND ECSF SOM EN PROFESSIONEL FORENING

ECSF skaber en fælles terminologi og en fælles forståelse af cybersikkerhedsprofessionelles rolleprofiler. Det kan således bruges af faglige sammenslutninger som en standard for at sikre, at deres arbejde kan bruges og anvendes på tværs af EU, hvilket eliminerer forvirring i terminologi og enhver mangel på forståelse.

Professionelle organisationer kan bruge rammerne til at udføre markedsanalyser ved hjælp af ECSF-rolleprofilerne og præsentere resultaterne i et fælles sprog. For eksempel forventes ECSF at være behjælpelig med at fremhæve de profiler, der mangler på markedet, cybersikkerhedsjob, der

Ved at bruge ECSF, kan man sikre, at en

[12] https://www.enisa.europa.eu/publications/analysis-of-the-european-rd-priorities-in-cybersecurity

er i høj efterspørgsel, og de lovgivningsmæssige aspekter af nogle professionelle jobprofiler. Desuden kan faglige sammenslutninger ved at bruge ECSF som en fælles terminologi arbejde hen imod professionel vejledning i cybersikkerhedssektoren som præsenteret i bilag B.5.

Brugen af ECSF gør det også muligt at konsolidere et fællesskab af interessenter for at støtte nye udviklinger, forbedringer og yderligere implementering i EU's medlemsstater. En sådan ramme for samarbejde muliggør menneskelig interaktion som resulterer i fordele som f.eks
videndeling, identifikation af tendenser i EU-skala, peer-læringsaktiviteter, anvendelse af tværfaglige tilgange og bemyndigelse til at tilpasse og tilpasse ECSF til specifikke krav.

Samlet set kan ECSF bruges af professionelle cybersikkerhedsforeninger som et værktøj til at basere deres aktiviteter på at sikre deres EU-dækkende anvendelighed med det formål at opnå en bedre hærdning mod cyberangreb i hele EU som samfund.

3.5 STRATEGISK BETYDNING AF SEKTOREN – ANVEND ECSF SOM POLITIKMAGER

Med ECSF sikrer et afgørende professionelt fællesskab klar synlighed, da brugen af rammerne skaber en fælles forståelse af, hvad cybersikkerhedsspecialister gør. Derfor giver ECSF et værktøj til at analysere og dele kritiske data- og statistikker i forbindelse med cybersikkerhedsarbejdsstyrke i en fælles og forståelig terminologi for hele EU. Sådanne data er vigtige for politiske beslutningstagere, da de opnår bedre indsigt i cybersikkerhedsarbejdsstyrkens tilstand i hele EU og dermed sætter dem i stand til at forstå og estimere cybersikkerhedsspecialisternes fremtidige behov for kvantitet og kvalitet. Sådanne strategiske input hjælper med at opdatere og vedligeholde selve ECSF, så dens relevans i fremtiden forbliver gyldig. Ved at definere en fælles terminologi giver ECSF desuden mulighed for grænseoverskridende samarbejde mellem politiske beslutningstagere gennem data- og informationsdeling.

Med en struktureret tilgang til et meget forskelligartet markedsmiljø udgør ECSF's rolleprofiler et værdifuldt værktøj til støtte fra politiske beslutningstagere, markedsinspektører og

Med en struktureret tilgang til et meget forskelligartet markedsmiljø udgør ECSF's rolleprofiler et værdifuldt værktøj til støtte fra politiske beslutningstagere, markedsinspektører og andre interessenter med indflydelse og rolle til at styrke sektoren strategisk. ECSF-profilerne kan være nyttige til dataundersøgelser om udbud og efterspørgsel, der udføres på nationalt, europæisk og internationalt plan. Profilerne giver en fælles, aftalt definition for at lette indsamlingen af pålidelige og sammenlignelige data på arbejdsmarkedet for cybersikkerhed, herunder udbud og efterspørgsel efter forskellige typer cybersikkerhedsprofessionelle og relaterede krav til særlige færdigheder.

Politikudformende processer, der adresserer cybersikkerhed, kan drage fordel af dataindsamling på tidspunktet for beslutningstagning, f.eks. finansieringsbestemmelser, investeringsprioriteter og interventionsperioder. Udover kerneaktiviteterne for hver profil kan de aktiviteter, de udfører, bidrage til at generere og indsamle relevante datasæt, der kan understøtte politiske beslutninger. Bilag B.3 viser, hvordan fragmenteret information udgør en udfordring, når der skal træffes beslutninger, og de handlinger INCIBE tager for at løse denne udfordring med støtte fra ECSF. Ved at indarbejde ECSF som en homogen ramme for definitionen af cybersikkerhedsprofiler får EU-medlemsstaterne værdifuld støtte til at nå deres mål om at øge cybersikkerhedstalenter og blive på linje med resten af landene på europæisk niveau.

4. VILKÅR OG DEFINITIONER

Semester	Definition	Kilde
cybersikkerhed	Enhver aktivitet, der er nødvendig for at beskytte netværks- og informationssystemer, brugerne af sådanne systemer og andre personer, der er berørt af cybertrusler.	ENISA mandat (Forordning (EU) 2019/881)
cybertrussel	Enhver potentiel omstændighed, begivenhed eller handling, der kan beskadige, forstyrre eller på anden måde have en negativ indvirkning på netværks- og informationssystemer, brugerne af sådanne systemer og andre personer.	ENISA mandat (Forordning (EU) 2019/881)
Information og Meddelelse Teknologi	IKT står for informations- og kommunikationsteknologi. Det bruges i mange forskellige sammenhænge og fra et teknisk synspunkt relaterer IKT sig til digitale computere og internet (kommunikations)systemer, herunder software, hardware og netværk. Fra et økonomisk og politisk synspunkt relaterer IKT sig til en tværsektor af virksomheder, herunder producenter, produktleverandører eller tjenesteudbydere, der relaterer sig til IKT-området.	EN16234-1:2019 e-kompetenceramme (e-CF)
kompetence	Den demonstrerede evne til at anvende viden, færdigheder og holdninger til at opnå observerbare resultater. Eksempler er B.1. Applikationsudvikling og E.3. Risikostyring.	EN16234-1:2019 e-kompetenceramme (e-CF)
evne	Evnen til at udføre ledelsesmæssige eller tekniske aktiviteter og opgaver på et kognitivt eller praktisk niveau; ved, hvordan man gør det.	EN16234-1:2019 e-kompetenceramme (e-CF)
bløde værdier	Interaktive færdigheder, der bruges til at engagere sig med succes med situationer på arbejdspladsen; kan referere til arbejdskvalitet, social interaktion eller følelser. (også kaldet tværgående, overførbare eller adfærdsmæssige færdigheder)	EN16234-1:2019 e-kompetenceramme (e-CF)
viden	Sammenfatning af fakta, der skal anvendes inden for et arbejds- eller studieområde; ved hvad man skal gøre.	EN16234-1:2019 e-kompetenceramme (e-CF)
holdning	Repræsentation af det menneskelige element i en e-kompetence; den reflekterer over, hvordan en person integrerer viden og færdigheder og anvender dem hensigtsmæssigt i kontekst.	EN16234-1:2019 e-kompetenceramme (e-CF)
læringsudbytte Udtalelse af, hvad en person ved, forstår og kan udføre efter afslutning af en læringsproces		europæiske kvalifikationer Ramme (EQF)
rolle profil	En oversigt eller et generelt dokument, der viser sammenhængen mellem specifikke aktiviteter eller opgaver i en rolle og de individuelle færdigheder, kompetencer og viden, der kræves for at udføre dem. I modsætning til et bestemt job stammer en rolle fra en	Kreativt lederskab – Talent Management CWA IKT-profiler

	organisatorisk behov for at gøre noget. Tildelte medarbejdere kan opfylde organisatoriske krav ved at udføre alle eller dele af de opgaver, der er nødvendige for at sikre deres rolle.	
jobprofil	En kontekstspecifik og detaljeret beskrivelse af, hvad en medarbejder gør for at sikre, at jobindehaveren ikke er i tvivl om deres opgaver, pligter, ansvar og ofte dem, de refererer til. Den indeholder normalt præcise oplysninger om de nødvendige kompetencer, færdigheder og viden samt praktiske oplysninger om sundhed og sikkerhed og aflønning.	IKT-profiler CWA
færdighedsniveau	En klar indikation af graden af beherskelse, der tillader en professionel til at opfylde krav i udførelsen af en kompetence. EN 16234-1 (e-CF) inkorporerer færdighedsniveauerne e-1 til og med e-5. e-CF karakteriserer færdighedsniveauer ved at kombinere niveauer af indflydelse inden for et fællesskab, kontekstkompleksitet og autonomi.	EN16234-1:2019 e-kompetenceramme (e-CF)
læringsniveau	Angiver en karaktergivning og kan være repræsenteret ved en formel kvalifikation. Læringsniveauer stammer generelt fra et uddannelsessystem eller angiver en karaktergivning i en taksonomi af intellektuel eller læringsadfærd (såsom at huske, anvende, fortolke) og har et forhold til færdighedsniveauer, men skal adskilles fra disse.	EN16234-1:2019 e-kompetenceramme (e-CF)

5. REFERENCER

ENISA-mandat, forordning (EU) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

Europæiske IKT-professionelle rolleprofiler, CWA 16458
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=17991
76DA0D15C74D91B71423CAD4A9A3

EN 16234-1:2019 e-Competence Framework (e-CF), En fælles europæisk ramme for IKT-professionelle i alle sektorer

CEN/TS 17699:2022 Retningslinjer for udvikling af IKT-professionelle læseplaner som omfattet af EN 16234-1 (e-CF)

CEN/TS 17834:2022 European Professional Ethics Framework for the ICT Profession (EU ICT Ethics)

European Qualifications Framework (EQF)

ESCO Den europæiske flersprogede klassifikation af færdigheder, kompetencer og erhverv, http://
www.ec.europa.eu/esco

IFIP etiske regler

NIST Incident Response Lifecycle

National Initiative for Cybersecurity Education (NICE) af National Institute of Standards and Technology i USA

Nationale cybersikkerhedsstrategier (NCSS'er), https://www.enisa.europa.eu/topics/national-cyber-
security- strategies/national-cyber-security-strategies-guidelines-tools

Cybersecurity Body of Knowledge (CyBOK) af UK National Cyber Security Program og University of Bristol, https://www.cybok.org

JRC, taksonomi og ordliste for cybersikkerhed af Europa-Kommissionen, https://
publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Den europæiske dagsorden for færdigheder, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196

Handlingsplan for digital uddannelse, https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education- action-plan

Pagt for færdigheder, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

Leading the Digital Decade, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

ENISA, retsmedicinsk analyse, webserveranalyse, håndbog, dokument for lærere, 2016, https://
www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-
resources/exe3_forensic_analysis_iii-håndbog

Europarådet, Electronic Evidence in Civil and Administrative Proceedings, Guidelines and Explanatory Memorandum, 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

ET BILAG: TILSLUTNING AF ECSF TIL ANDRE EU-STANDARDER OG RAMMER

ECSF er en ramme til støtte for det professionelle cybersikkerhedsdomæne i EU.
At forbinde eksisterende anerkendte europæiske strukturer af relevans til EU's professionelle cybersikkerhedsdomæne var et vigtigt ECSF-designprincip (se afsnit 2.1)

De følgende afsnit giver et kort overblik over de vigtigste standarder og rammer, som ECSF er knyttet til.

A.1 EN16234-1 E-CF EN FÆLLES EUROPÆISK REFERENCE RAMMER FOR IKT-PROFESSIONELLE I ALLE SEKTORER

Den europæiske norm (EN) 16234-1 European e-Competence Framework (e-CF) giver en reference til 41 kompetencer, som anvendes på informations- og kommunikationsteknologi (IKT) arbejdspladser ved hjælp af et europæisk standardsprog for kompetencer, færdigheder, viden og færdigheder niveauer, der kan forstås i hele Europa. Det primære formål med denne standard er at levere et fælles europæisk sprog for IKT-arbejdspladsrelaterede kompetencer, færdigheder, viden og færdighedsniveauer, som kræves og anvendes af organisationer og fagfolk. På denne måde har alle sektorinteressenter, herunder den offentlige og private sektor og enkeltpersoner, adgang til en fælles reference.

Standarden blev etableret som et værktøj til at understøtte gensidig forståelse og give gennemsigtighed i sproget gennem artikulation af kompetencer, der kræves og implementeres af ikt-professionelle. Denne standard er struktureret på tværs af flere dimensioner. Dimensionerne afspejler områder inden for forretnings- og menneskelig planlægning og inkorporerer retningslinjer for job- og arbejdsfærdigheder. Derudover tilføjer denne standard en tværgående komponent, som giver grundlæggende generiske IKT-deskriptorer til vellykket anvendelse af e-CF-kompetencer i sammenhæng med en arbejdsplads.

Tabel 4: EN16234-1 (e-CF) oversigt. Kilde: CEN 2019

Dimension 1 5 e-CF områder	**Dimension 2** 41 e-kompetencer identificeret	**Dimension 3** 5 e-kompetenceniveauer				
		e-1	e-2	e-3	e-4	e-5
En plan	A.1. Informationssystemer og forretningsstrategitilpasning					
	A.2. Service Level Management					
	A.3. Udvikling af forretningsplan					
	A.4. Produkt-/serviceplanlægning					
	A.5. Arkitektur design					
	A.6. Applikationsdesign					
	A.7. Overvågning af teknologitendenser					
	A.8. Bæredygtighedsledelse					

	A.9. Innovation					
	A.10. Brugeroplevelse					
B. Byg	B.1. Applikationsudvikling B.2.					
	Komponentintegration B.3.					
	Test B.4.					
	Løsningsimplementering					
	B.5. Dokumentationsproduktion					
	B.6. IKT-systemteknik C.1.					
C. Løb	Brugersupport C.2.					
	Skift support C.3.					
	Servicelevering C.4.					
	Problemhåndtering C.5.					
	Systemstyring D.1. Udvikling					
E. Aktiver	af informationssikkerhedsstrategi D.2. Udvikling af					
	IKT-kvalitetsstrategi D.3. Uddannelses- og					
	erhvervsuddannelsesbestemmelser D.4.					
	Indkøb af D.5.					
	Salgsudvikling D.6. Digital					
	markedsføring D.7.					
	Datavidenskab og analyse D.8.					
	Kontraktstyring D.9.					
	Personaleudvikling D.10.					
	Informations- og vidensstyring					
	D.11. Behov for identifikation					
E. Administrer	E.1. Forecast Udvikling E.2.					
	Projekt- og porteføljestyring E.3.					
	Risikostyring E.4.					
	Relationsledelse E.5.					
	Procesforbedring E.6. IKT-					
	kvalitetsstyring E.7. Business					
	Change Management E.8.					
	Informationssikkerhedsstyring E.9.					
	Informationssystemstyring					

e-CF giver konsekvente links i forbindelse med IKT-kvalifikationer og andre rammer af relevans for sektoren (især EQF, DigComp, europæiske IKT-professionelle rolleprofiler, adfærdsmæssige færdigheder, ESCO, EQANIE, SFIA, Fundamental Body of Knowledge for ICT Profession, ISO og andre ICT-industristandarder).

For hver cybersikkerhedsrolle blev et sæt anvendelige e-CF-kompetencer udvalgt på ansøgningsniveau som et indarbejdet element i profilbeskrivelsen for rollen som cybersikkerhedsprofessionel.

A.2 EUROPÆISKE IKT-PROFESSIONELLE ROLLEPROFILER

CWA 16458 europæiske IKT-professionelle rolleprofiler giver et generisk sæt af typiske roller, som udføres af IKT-professionelle i enhver organisation, og dækker hele IKT-forretningsprocessen.
I alt 30 profiler giver et godt udgangspunkt og inspiration til at skabe mere kontekstspecifikke og fleksible profiler baseret på organisatoriske roller, individuelle jobbeskrivelser eller subdomænespecialiseringer fra forskellige sammenhænge. Ved at anvende e-CF-kompetencer til opbygning af IKT-profiler, giver de europæiske IKT-professionelle rolleprofiler også et værktøj og indgangspunkt for e-CF-ansøgning til enkeltpersoner og organisationer, der ønsker at arbejde med e-CF.

De europæiske IKT-professionelle rolleprofiler er beskrevet ved at bruge et ensartet format, der inkorporerer følgende elementer: en sammenfattende erklæring, en mission statement, leverancer, hovedopgaver, e-kompetencer og områder med nøglepræstationsindikatorer (KPI)13 .

Ved at vedtage de bedst egnede elementer i den europæiske aftalte og praksisdrevne IKT-profilbeskrivelsesordning bliver ECSF-profilerne sammenlignelige og giver et unikt, let tilgængeligt og omfattende overblik over kravene til europæiske cybersikkerhedsprofessionelle.

Disse detaljerede profiler med højt indhold har løse links til de generiske roller, der er inkorporeret i det overordnede europæiske ikt-professionelle profilsæt. Fra ECSF-brugerperspektivet kan der etableres tillid til strukturens bæredygtighed gennem dens tilknytning til europæiske ikt-profiler, men med fokuseret anvendelse til cybersikkerhedssamfundet.

A.3 EUROPÆISK KVALIFIKATIONSRAMME

EU udviklede den **europæiske referenceramme for kvalifikationer (EQF)** som et oversættelsesværktøj for at gøre nationale kvalifikationer lettere at forstå og mere sammenlignelige. EQF søger at støtte grænseoverskridende mobilitet for lærende og arbejdstagere og at fremme livslang læring og faglig udvikling i hele Europa.

EQF er en læringsudbyttebaseret ramme på 8 niveauer14 for alle typer kvalifikationer. Den fungerer som et oversættelsesværktøj mellem de forskellige rammer for nationale kvalifikationer. Denne ramme hjælper med at forbedre gennemsigtigheden, sammenligneligheden og overførbarheden af folks kvalifikationer og gør det muligt at sammenligne kvalifikationer fra forskellige lande og institutioner.

EQF dækker alle typer og alle niveauer af kvalifikationer, og brugen af læringsresultater gør det klart, hvad en person ved, forstår og er i stand til at gøre. Niveauet stiger i henhold til læringsniveauet, med niveau 1 det laveste og 8 det højeste niveau. Vigtigst af alt er EQF tæt knyttet til nationale kvalifikationsrammer15, så den giver et omfattende kort over alle typer og niveauer af kvalifikationer i Europa, som i stigende grad er tilgængelige gennem kvalifikationsdatabaser. EQF blev oprettet i 2008 og senere revideret i 201716 .

ECSF-profilerne indeholder e-CF-kompetencer og e-CF-niveauopgaver, som giver en konsekvent forbindelse med EQF-niveauer (se afsnit 3.2). Dette orienterende forhold giver en bro i forståelsen mellem udbuddet af læringsprogrammer og arbejdspladsens krav.

A.4 ESCO - EUROPÆISK KLASSIFIKATION AF FERDIGHEDER, KOMPETENCER OG ERHVERV

ESCO er den flersprogede klassifikation af europæiske færdigheder, kompetencer, kvalifikationer og erhverv. Hovedformålet med ESCO er at levere en ordbog, der beskriver, identificerer og klassificerer faglige erhverv og færdigheder, der er relevante for EU's arbejdsmarked, uddannelse og uddannelse og systematisk viser sammenhængen mellem disse erhverv og færdigheder. ESCO administreres af Europa-Kommissionen, som er ansvarlig for at opdatere klassifikationen. ESCO-ressourcen understøtter to af EU's nøglestrategier på området, Europa 2020 og Skills Agenda for Europe17 .

13 CWA 16458 Europæiske IKT-professionelle rolleprofiler
14 https://europa.eu/europass/en/description-eight-eqf-levels
15 https://europa.eu/europass/en/national-qualifications-frameworks-nqfs
16 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=DA
17 https://ec.europa.eu/social/main.jsp?catId=1326&langId=da

Målet med ESCO er at beskrive alle erhverv på det europæiske arbejdsmarked, og dermed også cybersikkerhed. Det er derfor nyttigt at etablere en orienterende kortlægning mellem ECSF-rolleprofilerne og nogle af ESCO-profilerne.

I tabel 5 er flere cybersikkerhedsrelaterede ESCO-erhverv opført sammen med en vejledende kortlægning til ECSF-rolleprofiler. Da forholdet mellem dem ikke altid er en-til-en, blev følgende relationer defineret for at forklare de tilsvarende forbindelser:

- **er** – Denne ESCO-beskæftigelse kan tilknyttes den tilsvarende ECSF-rolleprofil som begge beskriver den samme cybersikkerhedsrolle.
- **kan omfatte** – Denne ESCO-beskæftigelse kan, baseret på konteksten, omfatte ECSF rolleprofil angivet. (Dette er en vejledende kortlægning.)
- **kan være inkluderet** – Nogle aspekter af denne ESCO-beskæftigelse kan beskrive dele af den anførte ECSF-rolleprofil. (Dette er en vejledende kortlægning.)

Tabel 5: Relationer mellem ESCO-profilerne og ECSF-profilerne

ESCO-kode ESCO Beskæftigelse		Forholdet kan	ECSF rolleprofil
2149.2.8	Forskningsingeniør 2310.1	omfatte kan	Cybersikkerhedsforsker
Videregående lektor	Informationsteknologi-træner	omfatte kan	Underviser i cybersikkerhed
2356		omfatte	Underviser i cybersikkerhed
2511,18	IT revisor	kan omfatte	Cybersikkerhedsrevisor
2519,2	IKT-revisorchef	kan omfatte er	Cybersikkerhedsrevisor
2529,1	IKT-sikkerhedschef		Chief Information Security Officer (CISO)
2529,2	Digital retsmedicinsk ekspert	er	Digital retsmedicinsk efterforsker
2529,3	Indlejret systemsikkerhedsingeniør	kan være inkluderet	Cybersikkerhedsimplementer
2529,4	Etisk hacker	er	Penetration tester
2529,6	IKT-sikkerhedsadministrator	kan være inkluderet	Cybersikkerhedsimplementer
2529,7	IKT sikkerhedsingeniør	kan være inkluderet	Cybersikkerhedsarkitekt
2529,7	IKT sikkerhedsingeniør	kan være inkluderet	Cybersikkerhedsimplementer
2619,4	Databeskyttelsesansvarlig	er	Cyberjuridisk, politik- og complianceansvarlig

Vigtig bemærkning: Forholdet mellem ESCO-besættelsen og ECSF-rolleprofilen repræsenterer ikke en ækvivalens; det giver den bedste tilnærmelse, som læserne måske ønsker at undersøge.

B BILAG:
BRUG CASES

En use case viser, hvorfor og hvordan en organisation bruger ECSF, og understreger de mange forskellige tilgange og fordele. Dette bilag er en samling af sager, der var offentligt tilgængelige den 20. juli 2022.

De følgende use cases er blot illustrative eksempler. Oplysningerne og indholdet inkluderet i disse sager bør ikke betragtes som en påtegning eller valideringserklæring fra

ENISA. Brugen af disse eksempler skal ses som inspirerende cases snarere end som konditionerende baselines eller benchmarking-referencer.

B.1 USE CASE FRA CONCORDIA H2020 PROJEKT

Dette afsnit inkluderer dele fra use casen skrevet af CONCORDIA H2020 project18 .

På vej mod en integreret platform for færdigheder inden for cyber bygget på den europæiske cybersikkerhed Kompetenceramme

Svært at forstå træningens store billede

Behovet for at beskytte sig selv mod trusler mod information og operationer, for at opretholde en organisations cybersikkerhedsposition og øge modstandskraften mod sådanne trusler, mærkes stadig af alle interesserede parter. En kernekomponent til at opfylde disse behov er eksistensen af cyber-kompetente fagfolk. Og kompetence vedrørende cybersikkerhed er ikke kun nødvendig for de dedikerede fagfolk (eksterne eller interne i en organisation), men også for alle medarbejdere i en organisation, selvom de ikke er direkte involveret i cybersikkerhedsprocesser og -aktiviteter.

Når det kommer til cybersikkerhedsprofessionelle, rapporterer forskellige publikationer stadig om et cybersikkerhedskompetencegab, der markerer, at de 3 bedste kompetencer, der mangler eller ikke er dækket nok af de eksisterende fagfolk, varierer fra år til år19. På den anden side tilbydes en betydelig mængde cybersikkerhedsrelaterede kurser og træninger af forskellige europæiske og internationale organisationer. En simpel søgning på internettet vil afsløre mange kurser, der relaterer sig til cybersikkerhedsdomænet, uden at give et klart billede af de udbudte kompetencer, eller hvordan de kan relatere til en bestemt rolle. For at føje til denne forvirring er der uddannelseskurser, der tilsyneladende henvender sig til én specifik rolle (f.eks. CISO), har lignende titler, men har forskellige læseplaner.

Derfor forvirrer de givne oplysninger i flere tilfælde praktikanten med hensyn til, hvad og hvordan de skal opfatte cybersikkerhedsbegreber, samt hvordan de skal bruges til at dække deres professionelle behov. Desuden promoveres kurserne for professionelle på en række forskellige platforme, og de er svære at sammenligne med hensyn til de dækkede kompetencer og rolleprofilen. Dette gør det vanskeligt for en person at opbygge en klar karrierevej og identificere udviklingsmuligheder.

[18] https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-european-cybersecurity-skills-framework/

[19] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-forskning-viser-retention-vanskeligheder-i-år

CONCORDIA-kortet over kurser for cybersikkerhedsprofessionelle

I et forsøg på at løse disse udfordringer har vi bygget CONCORDIA-kortet over kurser og træninger for cybersikkerhedsprofessionelle20. Kortet viser struktureret information om eksisterende europæiske tilbud for korte kurser/uddannelser og giver forskellige filtre, der hjælper med at matche det specifikke behov for kompetenceudvikling lettere med tilbuddet. [...]

Man kan vælge at sortere kurserne ud fra det adresserede cybersikkerhedsniveau (Device-, Network-, Software/ System, Data/ Application-, User-Centric), eller efter relevansen for en industrisektor (f.eks. Telecom, Financial, Transport e) -mobilitet, e-Health eller Defence), men også på formatet (face-to-face, online, blended), og tidspunktet for kurset/træningen.

Mangler en nøgleingrediens – Løsning aktiveret af ECSF

Selvom vi på CONCORDIA-kortet tilbyder et stort væld af filtre for at hjælpe brugerne med lettere at identificere de(t) kurser, der er af interesse, mangler databasen en nøgleingrediens – links til rolleprofiler, som hvert af kurserne adresserer gennem viden og færdigheder dækket. Den e-CF European Competence Framework for IKT-professionelle, der er tilgængelig på tidspunktet for opbygningen af kortet, definerer 30 rolleprofiler og 40 tilknyttede kompetencer, men de er svære at forbinde med de særlige forhold i cybersikkerhedsdomænet.

Dette var en udfordring for det cybersikkerhedsuddannelsesøkosystem, vi markerede allerede for to år siden og fangede i CONCORDIA Roadmap for Education21 under overskriften C5: Heterogenitet af kompetencerelateret terminologi. Denne mangel på en aftalt terminologi på tværs af domæner og på tværs af brancher relateret til de cybersikkerhedsfærdigheder, der er nødvendige for en specifik rolle, gør det vanskeligt for virksomheder at besætte ledige stillinger. De har svært ved at matche rekrutteringskriterierne med de studier og de kvalifikationer, der er anført i ansøgernes CV'er på grund af brugen af ikke-standard terminologi. Individer kan til gengæld ikke let identificere de færdigheder, de skal have eller udvikle for at matche markedets efterspørgsel. Og endelig har kursusudbydere svært ved at designe læseplaner, der svarer til markedets behov.

Som en del af CONCORDIA-køreplanen lovede vi én enkelt platform, der hoster alle de eksisterende cybersikkerhedsrelaterede programmer (universitetsniveau og ph.d.-programmer, korte kurser og træninger for professionelle). [...]

Platformen bør overveje at indsamle indholdet ved at bruge kategorier baseret på en standardterminologi (specifik kompetenceramme inkluderet). Kategorierne vil yderligere blive brugt som filtre til forskellige forespørgsler i kursusdatabasen. De 12 rolleprofiler, der er defineret i den nuværende version af European Cybersecurity Skills Framework (ECSF), ser ud til at være en naturlig løsning.

Fordelen for interessenterne

Vedtagelsen af et standardleksikon som det foreslåede af ESCF, herunder cybersikkerhedsrolleprofiler, vil hjælpe virksomheder med at identificere det rigtige talent til jobbet samt uddannelsesudbydere til bedre at forme deres læseplaner, så de matcher cyberarbejdsstyrkens behov. Ved at anvende den samme terminologi og bruge en EU-dækkende kompetenceramme til jobbeskrivelser, vil kursusbeskrivelse og rolleprofil hjælpe enkeltpersoner med at vælge de rigtige uddannelsesmoduler til at understøtte deres karrierevej og bedre filtrere jobåbningerne i overensstemmelse med deres kompetence og ekspertiseniveau. Endelig vil de politiske beslutningstagere være i stand til at indsamle mere strukturerede data på lande-/regionalt niveau til støtte for fremtidig politikudvikling og have et solidt grundlag, når de koordinerer med eksterne lande for at løse globale cybersikkerhedsudfordringer.

[20] https://www.concordia-h2020.eu/map-courses-cyber-professionals/
[21] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

På vej mod en integreret platform for færdigheder

Med udgangspunkt i CONCORDIA-databasen over kurser og uddannelser for cybersikkerhedsprofessionelle forsøger REWIRE-projektet22 at tage yderligere skridt hen imod at integrere det relevante indhold, der relaterer til cybersikkerhedsfærdigheder. REWIRE CyberABILITY platformen – i øjeblikket i designfase – vil give opdateret information om arbejdsmarkedet, kompetencer, uddannelseskurser, certificeringsordninger og en karriereplan.

B.2 USE CASE FRA SPARTA H2020 PROJEKT

Dette afsnit inkluderer dele fra use casen skrevet af SPARTA H2020 project23 .

Forbedring af videregående uddannelse ved hjælp af ECSF og SPARTA Curricula Designer

Introduktion

Denne use case giver anbefalinger til, hvordan ECSF kan bruges til at forme uddannelsesprogrammer, der er forbundet med cybersikkerhed. Da ECSF manifesterer strukturen af profiler på højt niveau fra praktikeres synspunkt, herunder hovedopgaver, relevant viden og færdigheder, kan dette give en mere fokuseret tilgang til opbygning af specialiserede og omfattende studieprogrammer, skræddersyet til specifikke profiler, i stedet for at dække cybersikkerhed i generel.

Udfordring

Uddannelsesinstitutionerne sammensætter deres læseplaner under hensyntagen til den fulde vej – startende med de grundlæggende kurser, der kræves for, at den studerende kan lære som grundlag for det næste sæt af opfølgende kurser, som ofte er cybersikkerhedsspecifikke. Udvælgelsen af kurser, der skal indgå i læseplanerne for cybersikkerhed, er dog op til institutionen.

Hver uddannelsesinstitution har sit eget specifikke miljø (bestemt af f.eks. infrastruktur, udstyr, læreres ekspertise, sammensætning af eksisterende uddannelser osv.), og der er ingen universel måde, hvordan læseplanen skal opbygges.

Uddannelsesudbydere er forskellige i, hvilket konkret underdomæne af cybersikkerhed de gerne vil fokusere på. Nogle udbydere er meget tekniske, med fokus på f.eks. datalogi, nogle mere socialt orienterede, med fokus på juridiske og samfundsmæssige aspekter. Derfor er interoperabiliteten mellem de resulterende uddannelser og et fælles sprog i øjeblikket en væsentlig udfordring.

Nogle akademiske uddannelser opbygger ikke færdigheder og kompetencer, der forbereder eleverne til specifikke arbejdsroller, der er tilgængelige på arbejdsmarkedet. Dette udgør en udfordring for studerende, som ikke forstår, hvad der er erhvervsmuligheder ved afslutningen af deres studier.

Løsning aktiveret af ECSF

ECSF kan bidrage til følgende aktiviteter, der adresserer udfordringerne ovenfor:

- Evaluering: Beskrivelse af profiler giver institutioner mulighed for at gennemgå deres læseplaner i en struktureret og systematisk måde, forstå praktikernes synspunkt. Dette gør det muligt at forstå, hvilken profil institution hovedsageligt retter sig mod deres kandidater.

22 https://rewireproject.eu/
23 https://sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula__%20Designer.pdf

- Forbedring: Kan udføres på baggrund af evalueringsøvelsen. Dette er især vigtigt i betragtning af det sæt af viden/færdigheder, der tilskrives en specifik profil.
- Fokus: Uddannelser, der tilbydes af universiteter, kan variere i måden, hvorpå de adresserer kerne kompetencer. Nogle kan være mere fokuserede på specifikke teknologiske kurser, nogle på jura, andre på retsmedicin osv. Med en ECSF at arbejde med, kan de kortlægge deres kernekompetencer på forskellige kursusområder, vigtige for definerede profiler. Dette sætter institutionen i stand til at udvikle mere effektive målrettede programmer i hus omkring hovedkompetencerne.

- Samarbejde: ECSF giver uddannelsesudbyderne det fælles sprog og ordforråd til at beskrive deres kurser, skabe fælles programmer og tillade mobilitet for studerende.

Når du anvender ECSF til undervisning i cybersikkerhed, anbefales følgende tilgang:

- Kurser i læseplaner kan klassificeres som tilhørende enten Fundamental eller Cyber Sikkerhedskategorier. Grundlæggende kurser er dem, der måske ikke er direkte knyttet til ECSF, men som fungerer som en forudsætning for senere studier. For eksempel er fundamental kryptologi forudsætningen for kryptoanalyse eller avanceret kryptologi; Talteori er nødvendig for de fleste mellemliggende og avancerede computerrelaterede kurser.
- Når de grundlæggende kurser er identificeret, kan Cybersikkerhedskurserne være foreslået for at imødekomme krav til arbejdsroller, som de studerende sigter mod. Sammenkædning opnås ud fra indholdet af de enkelte kurser, som kan knyttes til profilerne og endelig til arbejdsroller. De konkrete trin, [...], er:
  - en. For en specifik Arbejdsrolle 1 finder uddannelsesudbydere de relevante Profiler (Profil 1 og Profil 12 i vores eksempel). Denne kortlægning, markeret med brune pile, bør specificeres af jobannoncørerne/arbejdsgiverne.
  - b. Uddannelsesudbydere identificerer den nødvendige viden og færdigheder til udvalgte profiler. Disse krav er defineret af ECSF, markeret med blåt pile.
  - c. Uddannelsesudbydere designer nye eller genbruger eksisterende kurser (i vores eksempel kurser 1, 2, 3, 4), der omhandler den viden og de færdigheder, der er identificeret i trin ovenfor. Denne kortlægning mellem kurser og deres indhold skal udføres af kursusadministratorer.
  - d. At have alle nødvendige kurser (og alle forudsætninger for dem, generelle ikke-cybersikkerhedskurser, andre kurser til at udvide omfanget af studerende osv.), er kernen i læseplanen klar.
- Naturligvis kan ECSF også anvendes på den stik modsatte måde: først sammensætte læseplanen ud fra individuelle kurser, analysere den viden og de tilvejebragte færdigheder, bruge ECSF til at identificere profiler og endelig finde de arbejdsroller, der understøttes af læseplan. Denne kortlægning afslører, hvilken præcis viden og færdigheder, der allerede er til stede i læseplanerne, eller på den anden side, hvad der mangler og bør understreges eller tilføjes til kurserne. På denne måde hjælper ECSF med at strukturere læseplanerne, så de passer bedre til de forventede profiler og jobroller.

Resultat / merværdi af SPARTA

SPARTA-projektet brugte en cybersikkerhedsfærdighedsramme til at skabe et gratis værktøj kaldet Cybersecurity Curricula Designer. Det er en simpel webapplikation, der hjælper uddannelsesudbydere med at oprette nye uddannelser om cybersikkerhed og/eller med at analysere eksisterende uddannelser i henhold til deres indhold og dets afspejling af cybersikkerhedsjobkrav.

Værktøjet [...] giver studieprogramadministratorer mulighed for at sammensætte deres studieprogram ved at trække og slippe kurser fra venstre afsnit til midterste afsnit. Kurser, hvorfra

administratorer udvikler uddannelserne, kan enten være foruddefinerede eller tilpassede. Mens du sammensætter studieprogrammet, vises de statistiske data om dets indhold i højre afsnit. Udover andre data gives oplysninger om hvilke kompetencer og arbejdsroller, der understøttes af programmet. Ved at bruge værktøjet er det nemt at finde ud af, hvilket indhold der mangler på uddannelsen, og hvilke konkrete arbejdsroller der passer bedst til uddannelsens dimittender. I dette tilfælde er kvalifikationsrammen for cybersikkerhed kernen i applikationerne, som gør det muligt at forbinde færdigheder og viden med jobroller. [...]

B.3 USE CASE FRA INCIBE

Dette afsnit indeholder dele fra use casen skrevet af INCIBE24 .

Use case fra INCIBE

Introduktion

Effektiviteten i at beskytte et land afhænger i vid udstrækning af dets befolknings evner, og skøn i denne henseende er, at Spanien i 2022 kan nå en cybersikkerhedsarbejdsstyrke på tæt på 122.284 arbejdere med en talentforskel anslået til 24.119. En af topprioriteterne for administrationen i dag er derfor at imødegå udfordringen med at identificere, tiltrække, udvikle og fastholde talent inden for de forskellige områder af cybersikkerhed.

Et bevis på denne forpligtelse er udviklingen af den spanske regerings 2019 nationale cybersikkerhedsstrategi25, som understreger behovet for ikke kun at have en forsvars- og beskyttelsesposition for virksomheder og borgere, men også for at støtte et boost af cyberindustrien, idet man anerkender den nøglerolle, som cybersikkerhed spiller i det nuværende miljø med transformation og usikkerhed og den mulighed, det giver for at øge Spaniens konkurrenceevne. I overensstemmelse med mål 4 i strategien fremhæver handlingslinje 5 vigtigheden af at booste den spanske cybersikkerhedsindustri, ud over generering og fastholdelse af talent for at styrke digital autonomi.

På den anden side søger Digital Spain 2025 Plan26 at forstærke de løftestænger, der vil lette en tilbagevenden til den økonomiske vækst vej, og en af dens strategiske akser er at styrke Spaniens cybersikkerhedskapacitet for at mindske risici og øge tilliden til vejen mod en digital og bæredygtig økonomi.

I sin strategiske akse 4, der er dedikeret monografisk til cybersikkerhed, inkorporerer den de tiltag, der udgør INCIBEs tre hovedlinjer for de kommende år: at øge borgernes og virksomhedernes cybersikkerhedskapacitet; at booste det spanske cybersikkerhedsøkosystem omkring dets industri, F&U&I og cybersikkerhedstalent; og konsolidering af Spanien som et internationalt knudepunkt i sektoren. Spain Digital 2025 anerkender allerede cybersikkerhedstalentets nøglerolle som en drivkraft for sektoren.

Disse nationale initiativer genererer et passende scenarie, der favoriserer forskning, innovation og involverer de mest relevante aktører i værdikæden, såsom uddannelsesinstitutioner og organisationer, så de ser fordelen ved at forvalte den viden, kapacitet og teknologiske erfaringer, der reagerer på store udfordringer, som landet har i forhold til cybersikkerhed.

[24] http://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills
[25] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
[26] https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

På sin side, det spanske nationale cybersikkerhedsinstitut (INCIBE), en virksomhed under ministeriet for økonomiske anliggender og digital transformation, gennem statssekretæren for digitalisering og kunstig intelligens; og referenceenheden for udvikling af cybersikkerhed og digital tillid blandt borgere og virksomheder, og af det spanske akademiske og forskningsnetværk (RedIRIS), har til opgave at forbedre cybersikkerhed og digital tillid hos borgere, mindreårige og private virksomheder i Spanien.

Derudover omfatter dens mission beskyttelse og forsvar af disse grupper, fremme af spansk industri og F&U&I inden for cybersikkerhed, samt identifikation, generering og tiltrækning af talent til cybersikkerhedssektoren.

Cybersikkerhedstalent er derfor en hjørnesten i INCIBEs handlinger. Uden talent er det umuligt at udvikle en stærk industri eller de høje værdiskabende løsninger, der er nødvendige for at deltage i et stærkt konkurrencepræget marked som f.eks. cybersikkerhed.

Imidlertid var de tilgængelige oplysninger indtil videre om talentets tilstand i cybersikkerhedssektoren i Spanien varierede og fragmenterede, og de kom fra forskellige kilder, hvilket hindrede den dybe forståelse af miljøet, der var nødvendig for at kanalisere handlinger. [...]

Derfor offentliggør INCIBE i marts 2022 resultaterne af en analyse og diagnose af cybersikkerhedstalenter på nationalt niveau, hvis proces er blevet udført gennem strenge analytiske præmisser, globalt med henblik på at tilbyde en klar vision om cybersikkerhedstalenter i Spanien. arbejdstilgang og deltagende og inkluderende processer, der har taget højde for hovedaktørerne i cybersikkerhedsøkosystemet. [...]

Udfordring

Anbefalingerne fra dette analyseprojekt er udgangspunktet for at sikre en robust og profitabel cybersikkerhedsbranche, der er kendetegnet ved at sætte menneskers talent i centrum af initiativer. I denne forstand kan hele cybersikkerhedsværdikæden se denne undersøgelse som en mulighed for yderligere at forbinde med og bedre forstå cybersikkerhedstalentet i Spanien.

Det er derfor nødvendigt at strukturere og implementere effektiv praksis, der påvirker ledelsen af denne specifikke type talent i organisationer. Betydningen af cybersikkerhed for organisationers overlevelse kræver behovet for at løse problemet med at identificere denne type specifikke talenter inden for cybersikkerhed, udviklingen af rekrutterings- og ombordstigningsprocessen samt vedtagelsen af handlinger, der bidrager til at forbedre ledelsen og afbøde talent dræne.

Af denne grund prioriteres fremme af nationale politikker, koordineret fra administrationen, der fokuserer på at styrke og fremme initiativer til at gøre cybersikkerhed til en strategisk prioritet i organisationer, samt strukturering og strukturering af en uddannelsesplan for udførelsen af cybersikkerhed som en professionel aktivitet. som både organisationer og rekrutteringsvirksomheder vil etablere i deres handlinger for identifikation, tiltrækning, rekruttering og ledelse af cybersikkerhedstalenter.

På denne måde etableres et sæt anbefalinger, som denne type agenter (offentlig administration, rekrutteringsvirksomheder og andre organisationer) kunne implementere for at øge cybersikkerhedstalenter i Spanien, og som sætter udgangspunktet for at løse de udfordringer, der ligger forude i denne henseende. [...]

Løsning aktiveret af ECSF

Der er adskillige faktorer (politiske, økonomiske, sociale, teknologiske, juridiske osv.), der kan påvirke cybersikkerhedsindustrien, og som følge heraf manglen på talent, huller og generelt et misforhold mellem udbud og efterspørgsel.

En af disse relevante faktorer i Den Europæiske Union er manglen på standardisering af definitionen af cybersikkerhedsroller og færdigheder forbundet med disse roller.

Skabe grundlag for kontinuerlig kommunikation mellem forskellige interessenter (regering, industri, akademia, politiske beslutningstagere og borgere).

Denne type værktøj tjener som grundlag for en mere kompetent og komplet arbejdsstyrke, der forstår det samme sprog som andre fagfolk i Europa. [...]

Resultat / merværdi

Derfor er der i den præsenterede kontekst blevet lanceret to initiativer på nationalt plan, som vil give værdi til ECSF udviklet af ENISA, og som vil være meget nyttige. [...]

Begge initiativer, koordineret med hinanden, vil inkorporere ECSF som en homogen ramme for definitionen af cybersikkerhedsprofiler, som vil gøre det muligt for Spanien at nå sine talentmål og være på linje med resten af landene på europæisk plan. [...]

B.4 USE CASE FRA DEN EUROPÆISKE CYBERSIKKERHEDSORGANISATION (ECSO)

Dette afsnit indeholder dele fra use casen skrevet af den europæiske cybersikkerhedsorganisation (ECSO)27 .

Mod en harmoniseret uddannelsestilgang med European Cybersecurity Skills Ramme (ECSF)

Efter at have arbejdet med uddannelse, træning og færdigheder i sin WG5 siden 2016, har ECSO selv set de udfordringer, som den fragmentering og spredte tilgange, der findes inden for cybersikkerhed i dag, udgør. I dette blogindlæg reflekterer ECSO over de eksisterende europæiske tilgange til uddannelse og opkvalificering og fokuserer på ENISA's European Cybersecurity Skills Framework (ECSF).

Uddannelse er ikke kun et nationalt prærogativ. Det er også i sagens natur forbundet med samarbejde mellem nationale enheder, det bredere cybersikkerhedssamfund og europæiske organer. Med dette i tankerne er samarbejde nøglen, når man kommer med paneuropæiske tilgange til at harmonisere cybersikkerhedsuddannelsespensum og tackle kvalifikationerne eller mere konkret arbejdsstyrkekløften. Der er rig mulighed for at udnytte samarbejdsånden i det europæiske cybersikkerhedsfællesskab til at levere praktiske løsninger og initiativer, der kan have en indvirkning "på stedet", og ENISA's European Cybersecurity Skills Framework (ECSF) kan spille en stor rolle i denne henseende.

Cybersikkerhedsuddannelse: et ECSO-perspektiv

Set fra den europæiske cybersikkerhedsorganisation (ECSO), som repræsentativt organ for det europæiske offentlig-private økosystem og fællesskab af cybersikkerhed, er det potentielle

[27] https://www.ecs-org.eu/newsroom/consolidated-educational-and-recruiting-scheme-the-glue-to-fix-todays-scattered-approach

værdien af ECSF er ikke ubetydelig, når det kommer til at forbinde eksisterende indsatser, tilvejebringe grundlæggende elementer for en europæisk cybersikkerhedsarbejdsstyrke og levere en fælles ramme og taksonomi for anvendelse af profiler og færdigheder. Både fagfolk inden for cybersikkerhed, uddannelses- og træningsudbydere, politiske beslutningstagere og rekrutteringsprofessionelle kan vinde ved den bredere implementering af ECSF.

Udfordringen

Det er tydeligt, at der er et stigende behov for en dygtig cybersikkerhedsarbejdsstyrke. Forskellige undersøgelser over hele kloden fra industrien og den akademiske verden bekræfter, at efterspørgslen på cybersikkerhedsarbejdsstyrken er meget høj, og at det er svært at ansætte kompetente fagfolk. 2021-udgaven af den årlige Cybersecurity Workforce Study udgivet af ECSO-medlem (ISC)²28 angiver, at manglen på cybersikkerhedsprofessionelle er 2,72 millioner globalt, hvilket, selvom det er faldet fra 3,12 millioner året før, stadig er et betydeligt antal. Selvom disse undersøgelser giver et grundlag for at vurdere den globale situation, er virkeligheden, at det er meget vanskeligt at kvantificere omfanget af cybersikkerhedstalentmanglen i Europa. Vi ved, at efterspørgslen efter eksperter uundgåeligt vil stige på grund af væksten i cybersikkerhedsmarkedet og det regulatoriske landskab, hvilket efterlader et presserende hul at udfylde med flere (og forskellige slags) eksperter. [...]

Men det er ikke kun et spørgsmål om tal. Gennem en nylig ECSO-undersøgelse om HR-rekrutteringspraksis og -tendenser har ECSO også observeret en stigning i den tid, det i gennemsnit tager for organisationer at besætte deres cybersikkerhedsstillinger. Mange organisationer angiver, at det kan tage op til seks måneder for rekrutteringsprocessen, hvilket er langsommere end på ordrevidendomæner, mens andre angiver, at de har svært ved at besætte deres cybersikkerhedsstillinger helt.
Dette indikerer tydeligt, at der er et misforhold mellem udbud og efterspørgsel (dvs. kløft mellem akademiske og industrikrav) og push/pull-faktorer (dvs. kandidatens egnethed og vurdering, tiltrækning til job og fordele). Hovedproblemet for arbejdsgivere er dog fortsat den generelle mangel på cybersikkerhedsspecialister på verdensplan, mens efterspørgslen konstant vokser. Flere organisationer fremhæver også kompleksiteten i at ansætte eksperter til et domæne, som de ikke behersker. ECSO's undersøgelse viste også, at flere kandidater, som en voksende tendens, stadig beriger deres CV med cybersikkerhedskoncepter og -nøgleord, på trods af at de mangler betydelige cybersikkerhedsfærdigheder.

Disse udfordringer fremhæver klart behovet for et fælles sprog til at understøtte rekrutteringsindsatsen og vigtigheden af at overveje den tværfaglige karakter af cybersikkerhed, der er så unik for feltet kontra de mere traditionelle IT/IKT-erhverv. Mens eksisterende rammer som NICE, CyBoK og eCF giver nyttige retningslinjer for kompetenceudvikling, har en europæisk ramme, der giver en overordnet profiltaksonomi og karriereforløb, der er iboende for cybersikkerhed, manglet. Frigivelsen af ECSF er derfor meget rettidig og grundlæggende for

støtte det europæiske cybersikkerhedssamfund med at tiltrække, kvalificere og omkvalificere eksperter.

Der er en løsning

ECSO vil anvende ECSF på en række måder for at øge dens udbredelse og udnytte dets potentiale til at harmonisere uddannelse og færdigheder i cybersikkerhed i hele Europa.

ECSO vil:

- Kortlægge dets minimumsreferencepensum til ECSF, og give kursusdesignere og praktikere et førstehåndsindblik i, hvordan de bedst kan definere deres læseplaner hen imod dedikerede karriereforløb. Dette vil bidrage til at sikre, at universitetskurser i tilstrækkelig grad afspejler realiteterne i behovene på cybersikkerhedsarbejdsmarkedet, samtidig med at det giver mulighed for en løbende opdatering af læseplanen.

[28] https://www.isc2.org/Research/Workforce-Study

• Brug ECSF og tilhørende brugsmanual til at støtte HR/rekruttering i udarbejdelsen af jobannoncer og tilrettelæggelse af praktiske færdighedsvurderings-/evalueringsprocedurer. Vi vil også gennemføre en opfølgende HR-undersøgelse ved hjælp af ECSF-jobprofilerne for at forstå, hvilke roller der er mest behov for af organisationer og gradvist opbygge en kvantitativ forståelse af det europæiske cybersikkerhedsarbejdsmarked.

• Brug ECSF som basistaksonomi for to dedikerede platforme, som er forudset af Women4Cyber Foundation og ECSO [...]

Resultat og merværdi

Merværdien af ECSF for det europæiske cybersikkerhedssamfund er først og fremmest at have en fælles ramme og taksonomi at arbejde ud fra. Dette vil føre til en bedre forståelse af kvalifikationsbehovene og de praktiske realiteter af forskellige jobprofiler, hvilket vil forbedre cybersikkerhedsarbejdsstyrken, ikke kun gennem mere effektive rekrutterings- og fastholdelsesforanstaltninger, men også gennem at lette ind- eller genindtræden for flere kvinder og andre underrepræsenterede grupper (dvs. neurodiverset) i feltet. ECSF vil, ved at fremhæve de tekniske og ikke-tekniske aspekter af forskellige profiler, bidrage til at fjerne den misforståelse, at cybersikkerhed kun er et teknisk emne, når det så meget handler om mennesker og processer. I denne henseende vil det at understrege betydningen af bløde (overførbare) færdigheder på området bidrage væsentligt til at tiltrække flere kvinder til cybersikkerhedsfaget. ECSF vil også reducere fragmenteringen af tilgange ved at indføre top-down-retningslinjer for, hvordan man kan kategorisere cybersikkerhedsprofessionens mangefacetterede karakter. Profilerne foreslået af ECSF er tilstrækkelig brede til at kunne understøtte de mange roller, som professionen har at tilbyde, samtidig med at de er segmenteret på en måde, der gør det forståeligt og anvendeligt for både praktikere, brancheeksperter, politiske beslutningstagere, rekrutteringsspecialister og jobsøgende .

Hos ECSO er vi overbeviste om, at ECSF vil give betydelig værdi til vores arbejde og støtte det bredere samfund med et konkret værktøj til at harmonisere indsatsen og bygge bro mellem efterspørgsel og udbud af eksperter.

B.5 USE CASE FRA ISC2

Dette afsnit indeholder dele fra use casen skrevet af (ISC)²29 .

Brug af (ISC)² CISSP CBK til at understøtte European Cybersecurity Skills Framework / Cybersikkerhedsfaglige fællesskaber

Introduktion

(ISC)² CISSP CBK - nogle gange blot kaldet "Body of Knowledge" - refererer til et peer-udviklet kompendium af, hvad en kompetent cybersikkerhedsprofessionel skal identificere og besidde, herunder viden, færdigheder, evner, teknikker og praksis for at få succes. (ISC)² CBK er en samling af emner, der er relevante for cybersikkerhedsprofessionelle over hele verden. Den etablerer en fælles ramme for informationssikkerhedsvilkår og -principper, som gør det muligt for cybersikkerheds- og IT/IKT-professionelle verden over at diskutere, debattere og løse sager vedrørende professionen med en fælles forståelse, taksonomi og leksikon. (ISC)² blev til dels etableret for at samle, standardisere og vedligeholde (ISC)² CBK for cybersikkerhedsprofessionelle over hele verden. (ISC)2 CBK præsenterer en færdiglavet ressource for nuværende og håbefulde cybersikkerhedsprofessionelle at adoptere inden for ECSF-rammen.

[29] https://www.isc2.org/-/media/9644E0ED44954F7CAE895D45620213EA.ashx

Udfordring

Som ENISA beskriver i deres nyligt udgivne rapport "Adressing The EU Cybersecurity Skills Shortage And Gap Through Higher Education", er mangel på global cybersikkerhedskompetence og mangel på tilstrækkelig og kvalificeret arbejdsstyrke bekymringer, der har en væsentlig indvirkning på EU-medlemsstaternes evne til at beskytte offentligheden. fra stigende trusler fra den stadigt stigende brug af teknologi i samfundet. På trods af det arbejde, der er blevet udført, er cyberangreb og truslen om cyberangreb fortsat en betydelig risiko for den offentlige sikkerhed. Europæiske organisationer kæmper for at bemande deres cybersikkerhedshold tilstrækkeligt. De forebyggelige konsekvenser – forkert konfigurerede systemer, hastede implementeringer, ufuldstændig hændelsesrespons, forsinket patching, utilstrækkelig risikostyring – gør mange europæiske organisationer lokkende mål for trusselsaktører rundt om i verden.

Løsning muliggjort af ECSF (hvordan udfordringerne blev mødt)

For at imødekomme udfordringerne som følge af kvalifikationskløften og mangel på arbejdskraft foreslår (ISC)² en løsning, der er fokuseret på at hjælpe cybersikkerhedsprofessionelle med at identificere og kortlægge nødvendig viden, færdigheder, evner, teknikker og praksis til profiler identificeret i European Cybersecurity Skills Framework (ECSF) . (ISC)2 CISSP CBK kortlægger flere færdigheder og vidensområder i følgende ECSF-profiler:

- 2.1 Chief Information Security Officer (CISO)
- 2.2 Cyber Incident Responder
- 2.3 Cyberjuridisk, politik- og overholdelsesansvarlig
- 2.4 Cyberthreat Intelligence Specialist
- 2.5 Cybersikkerhedsarkitekt
- 2.6 Cybersikkerhedsrevisor

Ved at bruge de begreber, der er dækket af CBK, kan fagfolk, der i øjeblikket arbejder i de ovennævnte profiler eller dem, der stræber efter at arbejde i disse profiler, bruge nøglekompetencerne og videnområderne fra ECSF-profilerne kombineret med (ISC)2 CBK til at bestemme hvordan CBK opfylder den viden og de færdigheder, der kræves til stillingen, og hvor de kan have behov for at supplere deres uddannelse/træning fra andre kilder. Dette vil gøre det muligt for kandidater at opbygge en uddannelses-/træningsvej for at nå deres mål.

Følgende tabel giver et eksempel på, hvordan (ISC)2 CISSP CBK kan bruges af en nuværende eller aspirerende CISO til at identificere de nøglefærdigheder og videnområder fra ECSF CISO-profilen, som de har eller skal opbygge. [...]

Resultat / Merværdi

Den tilsigtede fordel ved (ISC)² CISSP CBK-kortlægningen til ECSF er, at den vil skabe karrierevejledning og professionelle uddannelsesveje for at hjælpe nuværende og håbefulde cybersikkerhedsprofessionelle med at identificere og opnå nødvendig faglig viden, færdigheder og evner for hurtigere at opnå og udfylde åbne profiler, som identificeret i ECSF, og derved mindske mangel på kvalifikationer inden for cybersikkerhed og mindske kløften i kvalificeret arbejdsstyrke.

B.6 USE CASE FRA ISACA

Dette afsnit inkluderer dele fra use casen skrevet af ISACA30 .

[30] https://www.isaca.org/training-and-events/careers-home/career-pathway/european-cybersecurity-skills-framework-and-isaca-legitimationsoplysninger

Individuel karrierebeslutningstagning: Professionelle legitimationsoplysninger Europæisk cybersikkerhed Kompetenceramme

Introduktion

Sabine arbejdede som SOC-analytiker et par år efter at have opnået sin universitetsgrad og var interesseret i at lære, hvordan hun bedst kunne fremme sin karriere. Hun talte med sin mentor, som fortalte hende, at ISACA havde været et godt startskud for hans karriere og opfordrede hende til at undersøge medlemskab og eventuel certificering. Man må indse, at det at gå ind i Cybersikkerhed giver mulighed for at arbejde med alt, fra mennesker og psykologi via juridiske, politiske og styrende, ned til det laveste (eller højeste) tekniske niveau. Udfordringen er at finde et udgangspunkt og derefter identificere, hvilke specifikke kompetencer man kan lære og derefter mestre for at udvide eller ligefrem overgang mellem cybersikkerhedsroller. ESCF specificerer flere roller med deres kompetencer, der er nødvendige for at arbejde inden for den specifikke rolle. Bemærk, at disse kompetencer ikke er alt, der er nødvendigt for en specifik rolle, men det absolutte minimum. Ved at bruge dette kan Sabine identificere kompetencegabet, hvis man ønsker at skifte rolle eller flytte ind i et andet område inden for Cybersikkerhed.

Udfordring

Som ny professionel i et efterspurgt felt og som kvinde i cybersikkerhed søgte Sabine hjælp på et par forskellige områder:

- Karrierevejledning og ressourcer – inklusive legitimationsoplysninger – for at hjælpe med at fremme hendes karriere
- Et netværk af jævnaldrende og brancheledere til at hjælpe hende med at navigere i professionelle udfordringer
- Assistance til at udvikle bløde færdigheder for at hjælpe hende til at blive en velafrundet fremtidig leder
- Indsigt i at overvinde udfordringer og udnytte muligheder som kvinde i cybersikkerhed
- Information til at hjælpe hende med at udføre sit nuværende job godt og hjælpe hende med at forberede sig på fremtidige udfordringer i roller på højere niveau

Enhver person kan bruge ESCF til at se, hvilke roller der er nødvendige for at håndtere næsten enhver form for udfordring eller opgave inden for cybersikkerhedsdomænet. Ved at bruge ESCF som udgangspunkt kan en person også identificere, hvilke kompetencer der er nødvendige for at flytte fra en rolle til en anden.
Dette vil gavne dialogen mellem medarbejdere og arbejdsgivere ved planlægning af efteruddannelsen inden for cybersikkerhedsområdet. Dette vil også gavne en person, der ønsker at indgå i cybersikkerhed, men er usikker på, hvor de skal starte. For de fleste er det nemmere at tilføje tidligere viden og kompetencer end at lære noget helt nyt.

Med missionen om at blive en C-suite cybersikkerhedsprofessionel inden for dette udfordrende felt Sabine undersøgte omridset af CISO's ansvar:

Profil 1 CISO Mission	Definerer, vedligeholder og kommunikerer cybersikkerhedsvisionen, strategien, politikker og procedurer og styrer implementeringen på tværs af organisationen. Styrer cybersikkerhedsrelaterede aktiviteter på tværs af organisationen. Varetager forbindelser/forbindelser med eksterne myndigheder og faglige instanser.

Sabines ambition er at identificere hullerne i hendes færdigheder for at komme videre med sin karriere med passende afstemte legitimationsoplysninger til det næste niveau.

ECSF-løsning

Sabine undersøgte ECSF PROFIL 1 og identificerede huller i hendes viden:

Nøgleviden	ÿ Viden om cybersikkerhed og privatlivsstandarder, rammer, politikker, forordninger, lovgivning, certificeringer og bedste praksis Forståelse af etiske krav til cybersikkerhedsorganisationer ÿ Kendskab til sikkerhedskontrol Kendskab til modenhedsmodeller for cybersikkerhed ÿ Viden om cybersikkerhedstaktikker, teknikker og procedurer Kendskab til ressourcestyring Kendskab til ledelsespraksis Kendskab til rammer for risikostyring

Sabine besluttede at tage sin mentors råd og deltage i et lokalt ISACA-afdelingsmøde for at se, om det var det rigtige. Hun var straks imponeret over de muligheder, det gav. Kapitlet bød hende varmt velkommen og introducerede hende for flere nøglepersoner i kapitlet – mennesker, der arbejdede i præcis den type roller, Sabine søgte, og som ville være fremragende mentorer eller sponsorer.

Kapitlets certificeringsformand informerede Sabine om, at certificeringen Certified Information Security Manager (CISM) ville passe rigtig godt til hende, da den demonstrerer en omfattende viden om informationssikkerhed samt stærke ledelsesevner. Certificeringen er for dem med fem eller flere års erfaring, så Sabine besluttede at lave en 18-måneders plan for at studere og opnå certificeringen.

Hun sluttede sig til ISACA som medlem den aften og udnyttede fuldt ud de ressourcer, som foreningen tilbød på både globalt og lokalt plan. Hun sluttede sig til foreningens online-fællesskaber, begyndte at deltage i webinarer og lokale afdelingsmøder tilbudt gennem SheLeadsTech, et program, der tilbydes af ISACAs One in Tech Foundation. Og hun deltog i næsten alle møder, som den lokale afdeling tilbød.

Blot seks måneder inde i hendes medlemskab henvendte en kollega til hende hende om et job som informationssikkerhedsanalytiker i deres organisation.

Resultat

Sabine har nu været medlem af ISACA i syv år. Hun opnåede sin CISM-certificering og blev snart forfremmet til informationssikkerhedschef. Hun er nu direktør for informationssikkerhed, med en klar vej til en CISO-rolle.

Ud over at finde legitimationsoplysninger og job gennem ISACA, fandt Sabine også adskillige ressourcer, der hjalp hende med at tilføje værdi til sin organisation. Før GDPR trådte i kraft, var Sabine i stand til at udnytte GDPR Resource Hub, der tilbydes af ISACA, til at hjælpe hende med at forstå situationen grundigt og lære, hvad de mest kritiske skridt at tage i hendes nuværende rolle.

Interessen og erfaringen, hun fik i privatlivets fred som et resultat af dette projekt, gjorde det muligt for hende at kvalificere sig til ISACA's Certified Data Privacy Solutions Engineer (CDPSE) legitimation gennem dets tidlige adopter-program.

Hun har præsenteret på ISACA-konferencer på afdelings- og nationalt niveau – for at finpudse sine kommunikationsevner – og hun påtog sig en afdelingsbestyrelsespost sidste år. Som direktør har hun

har haft mulighed for at ansætte nogle få stillinger, og de fleste af hendes ansættelser er kommet fra ISACA-afdelingen – ligesom hun fandt sin første forfremmelse for seks år siden. Efter at have set værdien af CISM-certificeringen i sin egen karriere, er hun begyndt at tilbyde CISM-certificeringsforberedelser til sit team gennem ISACAs virksomhedstræningstilbud.

Sabines nyeste fokusområde, når hun forbereder sig til sin CISO-rolle, er at sikre nye teknologier. I betragtning af det øgede lovgivningsmæssige fokus på kunstig intelligens i Europa, har hun først rettet sin indsats på dette område, og hun har for nylig opnået et Artificial Intelligence Fundamentals-certifikat fra ISACA.

Syv år efter at have gået gennem dørene til sit første ISACA-kapittelmøde, har Sabine udvidet sit netværk med hundredvis af fagfolk lokalt og tusindvis globalt. Hun er en

selvsikker leder og foredragsholder, og hun er nu mentor for flere andre, der engang var i hendes stilling. Blandt hendes råd til sine mentees er altid at lære – og at ISACA, som et globalt læringsfællesskab, er en stor ressource.

Sabine har skitseret, hvilke skridt der skal tages for at få C-suiten og planlægger at varetage en CISO-rolle inden for fem år. Hun er overbevist om, at hendes ISACA-netværk og legitimationsoplysninger vil være en væsentlig fordel, når hun forfølger sine mål.

Karrierevej:

- SOC-analytiker
- Informationssikkerhedsanalytiker
- Informationssikkerhedschef
- Direktør for informationssikkerhed.

B.7 USE CASE FRA SANS/GIAC

Dette afsnit inkluderer dele fra use casen skrevet af SANS institute og GIAC (Global Information Assurance Certification)31 .

Hvorfor Workforce Frameworks og certificeringer er vigtige i cybersikkerhed

Netværks- og informationsdirektivet (NIS) II er en opdatering af det eksisterende mandat for Den Europæiske Union. Dette vil bidrage til at fremme et fælles cybersikkerhedssprog på tværs af en bredere vifte af sektorer af økonomien og vil kræve deling af information mellem medlemslande og tværsektorer. Direktiver som dette har stigende betydning for etablering af autoværn til cyberaktiviteter. For at beskytte aktionærværdien overvejer Security and Exchange Commission (SEC) en cyberrapport for børsnoterede virksomheder, der kræver rapportering om, hvordan deres sikkerhedsteam vil håndtere risici, hændelser og cybereksperti sen i bestyrelsen. Sikkerhedsrisikoreduktionsrapporten vil binde tilbage til jobrollers færdighedssæt.

Rammer er med til at formulere disse jobroller. De fleste jobåbninger var indtil for nylig generiske annoncer, der søgte cybersikkerhedsprofessionelle uden veldefinerede opgaver, færdigheder eller viden om, hvad der er nødvendigt for at beskytte organisationens aktiver. Arbejdsstyrkens rammer såsom ECSF European Cybersecurity Skills Framework (ECSF) begynder at standardisere det talent, der er nødvendigt for stillinger som Cyber Incident Responder, Digital Forensics Investigator og Chief Information Security Officer. Standardisering gør det muligt for organisationer at identificere retten

[31] https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

talent til at håndtere fremtidige trusler. Dette er i tråd med andre erhverv. For eksempel har læger specialiserede områder som radiologer, børnelæger og hjernekirurger, der har den nødvendige ekspertise inden for deres område for at give ordentlig behandling.

Certificering spiller en vigtig rolle i at gøre folk klar til specifikke jobroller. Certificering validerer individet ved at bruge bedste praksis og retningslinjer for uddannelsesmæssige og psykologiske tests såsom ISO/IEC 17024 internationale standarder. Et eksempel på en certificering, der betragtes som den globale standard, er en Certified Public Accountant (CPA). Erhvervserfaring kan gøre nogen til en ekspert, men CPA er den velrespekterede baseline for en certificeret professionel og kan endda være et krav for overholdelse af specifikke projekter eller

revisioner.

Nogle eksempler, hvor arbejdsstyrkens rammer har hjulpet med at fremme cybersikkerhedsindustrien, omfatter:

- Store teknologi- og finansvirksomheder har ofte flere sikkerhedsteams, der standardiserer deres arbejdsroller og krav gennem rammerne for hurtigt at omplacere og rotere medarbejdere baseret på missionen.
- Organisationer kan kortlægge deres arbejdsstyrkes erfaring og certificering for hurtigt at matche medarbejdernes færdigheder med projektkrav. Dette er især vigtigt for konsulentfirmaer, teknologivirksomheder og entreprenører.
- Rammer giver et fælles sprog i arbejdsstyrken på tværs af brancher som f.eks teknologi, finans, sundhedspleje, detailhandel og forsyningsselskaber, hvilket giver teams mulighed for at arbejde sammen for at beskytte cyber- og fysiske sikkerhedstrusler.
- Rammer giver en skabelon for akademiske institutioner til at bygge bro mellem deres uddannelsestilbud og de nuværende cybersikkerhedsfærdigheder, der er nødvendige på tværs af brancher, og forbereder deres studerende til job.

SANS og GIAC forstår vigtigheden af rammer og har tilpasset kurser og certificeringer til disse rammer. Rammer er en skabelon for organisationer til at standardisere jobkrav, selvom enhver organisation og mission har brug for en vis tilpasning knyttet til deres specifikke mission. Vi har hjulpet med at designe og implementere arbejdsstyrkeudviklingsprogrammer ved hjælp af rammer som skabelon for Fortune 500-virksomheder, offentlige myndigheder og organisationer af alle størrelser.

OM ENISA

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, er EU's agentur dedikeret til at opnå et højt fælles niveau af cybersikkerhed i hele Europa. Etableret i 2004 og styrket af EU's cybersikkerhedslov, bidrager Den Europæiske Unions Agentur for Cybersikkerhed til EU's cyberpolitik, øger troværdigheden af IKT-produkter, -tjenester og -processer med cybersikkerhedscertificeringsordninger, samarbejder med medlemsstater og EU-organer og hjælper Europa med at forberede til morgendagens cyberudfordringer. Gennem videndeling, kapacitetsopbygning og bevidstgørelse arbejder agenturet sammen med sine nøgleinteressenter for at styrke tilliden til den forbundne økonomi, for at øge modstandskraften i Unionens infrastruktur og i sidste ende holde Europas samfund og borgere digitalt sikre. Mere information om ENISA og dets arbejde kan findes her: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-583-8
DOI: 10.2824/95989