ENISA-a

AGENCIJA EUROPSKE UNIJE ZA KIBERSIGURNOST

PRIRUČNIK

EUROPSKI OKVIR ZA VJEŠTINE U PODRUČJU KIBERSIGURNOSTI (ECSF)

RUJAN 2022.

O ENISA-i

Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije posvećena postizanju visoke zajedničke razine kibersigurnosti diljem Europe. Agencija Europske unije za kibersigurnost, osnovana 2004. i ojačana Aktom EU-a o kibersigurnosti, doprinosi kiberpolitici EU-a, povećava pouzdanost IKT proizvoda, usluga i procesa s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi za kiberizazove sutrašnjice. Razmjenom znanja, izgradnjom kapaciteta i podizanjem razine osviještenosti Agencija surađuje sa svojim ključnim dionicima na jačanju povjerenja u povezano gospodarstvo, jačanju otpornosti infrastrukture Unije i, u konačnici, održavanju digitalne sigurnosti europskog društva i građana. Više informacija o ENISA-i i njezinu radu možete pronaći ovdje: www.enisa.europa.eu.

KONTAKT

Za kontaktiranje autora koristite euskills@enisa.europa.eu.

SURADNICI

Ovaj okvir rezultat je stručnog mišljenja i dogovora u Ad-hoc radnoj skupini o okviru vještina koju čine 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 i Jan HAJNY.

Fabio DI FRANCO i Athanasios GRAMMATOPOULOS vodili su ovu aktivnost za ENISA-u.

PRAVNA OBAVIJEST

OBAVIJEST O AUTORSKIM PRAVIMA

* Izvjestitelj za ad hoc radnu skupinu za Europski okvir vještina u području kibersigurnosti

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

TABLICA SADRŽAJA

SAŽETAK

Nedostatak radne snage u kibernetičkoj sigurnosti i nedostatak vještina glavni su problem i za gospodarski razvoj i za nacionalnu sigurnost. Ispitivanjem problema ENISA je utvrdila potrebu Europe za sveobuhvatnim pristupom definiranju skupa uloga i vještina u području kibersigurnosti koje bi se mogle iskoristiti za smanjenje nedostatka vještina i nedostatka vještina. ENISA je radila na razvoju takvog okvira i predstavlja **Europski okvir za vještine u području kibersigurnosti (ECSF),** čiji je cilj ojačati europsku kulturu kibersigurnosti pružanjem zajedničkog europskog jezika u svim zajednicama, čime se čini ključan korak naprijed prema digitalnoj budućnosti Europe.

ECSF je praktičan alat za **potporu utvrđivanju i artikulaciji zadaća, kompetencija, vještina i znanja povezanih s** ulogama europskih stručnjaka za **kibersigurnost**. Glavna je svrha okvira **stvoriti zajedničko razumijevanje** među pojedincima, poslodavcima i pružateljima programa učenja u državama članicama EU-a, što ga čini vrijednim alatom za premošćivanje jaza između profesionalnog radnog mjesta u području kibersigurnosti i okruženja za učenje.

Okvir opisuje najvažnije zahtjeve profesionalnog radnog mjesta za kibernetičku sigurnost definiranjem skupa **od 12 tipičnih profila profesionalnih uloga u području kibersigurnosti**. Ti profili pružaju zajedničko razumijevanje glavnih misija, zadataka i vještina u području kibersigurnosti potrebnih u profesionalnom kontekstu kibersigurnosti, što ih čini savršenom referencom za profiliranje vještina i znanja potrebnih stručnjacima za kibersigurnost. Okvir je osmišljen tako da bude lako razumljiv i dovoljno sveobuhvatan da pruži odgovarajuće dubinske uvide u kibernetičku sigurnost, kao i dovoljno fleksibilan da omogući prilagodbu na temelju potreba svakog korisnika. Uključivanjem svih perspektiva dionika okvir je primjenjiv na sve vrste organizacija i podupire razvoj svih zanimanja u području kibersigurnosti.

Europski okvir za vještine u području kibersigurnosti (ECSF) namijenjen je jačanju europske kulture kibersigurnosti pružanjem zajedničkog europskog jezika u svim zajednicama, čime se čini ključan korak naprijed prema digitalnoj budućnosti Europe.

ECSF je rezultat rada ENISA-ine ad hoc radne skupine za Europski okvir vještina za kibersigurnost1 koju čine stručnjaci koji zastupaju različita stajališta. Razvijeni okvir temelji se na analizi postojećih okvira, rezultatima i nalazima istraživanja o potrebama tržišta i dogovoru među stručnjacima. Korisničke studije slučaja i indikativni primjeri, inspirirani različitim radnim mjestima i okruženjima za učenje, pokazuju praktičnu provedbu ovog okvira i podupiru ovaj rad.

Utvrđeno je da su glavne koristi korištenja ECSF-a:

- osiguravanje **zajedničke terminologije** i **zajedničkog razumijevanja** stručnjaka za kibersigurnost diljem EU-a;
- utvrđivanje **ključnih vještina** potrebnih iz perspektive radne snage u području kibersigurnosti kako bi se podržao njezin daljnji razvoj i poboljšanje;
- promicanje **usklađivanja u** programima obrazovanja**,** osposobljavanja **i** razvoja radne snage **u području kibersigurnosti**.

Ovaj korisnički priručnik ECSF-a pruža sveobuhvatan pregled glavnog područja primjene ECSF-a, okvirnih načela i mogućnosti primjene. Primarna je svrha priručnika učiniti ECSF lako dostupnim, razumljivim i upotrebljivim svim dionicima s aktivnom ulogom ili potrebom za odgovarajuće kvalificiranim stručnjacima za kibersigurnost.

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

1. UVOD

Nedostatak vještina u području kibersigurnosti jedan je od ključnih izazova koje je potrebno riješiti za kibersigurnost Europske unije. Točnije, na tržištu rada nedostaje kvalificiranog i kvalificiranog osoblja koje bi preuzelo uloge u kibersigurnosti i koje bi se moglo u dovoljnoj mjeri suočiti s rastućim kiberprijetnjama i novim izazovima u području kibersigurnosti. Jaz u vještinama kibernetičke sigurnosti ima niz temeljnih pokretača. To uključuje nedovoljnu razinu razumijevanja kompetencija i vještina potrebnih u disciplini kibersigurnosti među različitim akterima na tržištu kibersigurnosnih vještina. Tijekom godina to je postao dobro dokumentiran problem[2], koji i dalje značajno utječe na zemlje na europskoj i međunarodnoj razini.

ECSF pruža otvoreni europski alat za izgradnju zajedničkog razumijevanja profila profesionalnih uloga u području kibersigurnosti i zajedničkih mapiranja s odgovarajućim potrebnim vještinama i kompetencijama.

Kako bi se smanjio sadašnji i budući nedostatak vještina, potrebno je više stručnjaka za kibersigurnost s odgovarajućim skupovima vještina. U tu svrhu Program vještina za Europu[3], Akcijski plan za digitalno obrazovanje[4] i Pakt za vještine[5] i dalje su važni instrumenti za mobilizaciju dionika da zajedno rade na postizanju ciljeva digitalnog desetljeća[6] stvaranjem brojnijih i boljih prilika za osposobljavanje.

U tom je kontekstu ENISA u prosincu 2020. pokrenula ad hoc radnu skupinu za Europski okvir za vještine u području kibersigurnosti[7] . Okupljena je multidisciplinarna skupina stručnjaka s ciljem promicanja usklađivanja koncepata obrazovanja, osposobljavanja i razvoja radne snage u području kibersigurnosti. Razvijeni okvir (ECSF) pruža otvoreni europski alat za izgradnju zajedničkog razumijevanja profila profesionalnih uloga u području kibersigurnosti i zajedničkih mapiranja s odgovarajućim potrebnim vještinama i kompetencijama. Taj je rad temelj za udruživanje snaga u programu izgradnje kapaciteta za europsku radnu snagu u području kibersigurnosti u skladu s aktualnom potražnjom na tržištu.

1.1 CILJANA PUBLIKA

Iako su krajnji opseg sadržaja okvira ECSF-a ključni stručnjaci za kibersigurnost, poseban naglasak stavlja se i na ciljne skupine ECSF-a stručnjaka koji nisu stručnjaci za kibersigurnost kojima je potreban sveobuhvatan pogled na tu disciplinu. Taj fokus čini okvir lako razumljivim svim zainteresiranim stranama.

Krajnji opseg okvira ECSF-a su temeljni stručnjaci za kibersigurnost, dok je naglasak stavljen i na stručnjake koji nisu stručnjaci za kibersigurnost, a kojima je potreban sveobuhvatan pogled na tu disciplinu.

Ciljana publika ECSF-a su vodeći timovi organizacija, ljudski resursi i funkcije kibersigurnosti, stručnjaci za kibersigurnost, pridošlice i kiberenti, kao i pružatelji programa učenja svih vrsta u javnom i privatnom kontekstu, sektorska udruženja, istraživači tržišta i kreatori politika.

1.2 STRUKTURA PRIRUČNIKA

Korisnički priručnik strukturiran je na sljedeći način:

- U poglavlju 1. uvode se ključni izazovi koji ističu potrebu za stvaranjem okvira za vještine u području kibersigurnosti, kao i ciljnu publiku za taj rad;
- U poglavlju 2. predstavljena su načela oblikovanja ECSF-a kao i ključne prednosti njegove primjene;

[2] ENISA, 2020., Razvoj vještina u području kibersigurnosti u EU-u https://www.enisa.europa.eu/publications/the-status-of-cyber-sigurnosno-obrazovanje-u-europskoj uniji
[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/en/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 poziva WG

- U poglavlju 3. objašnjavaju se različite primjene ECSF-a s različitih gledišta.

Osim toga, dokument uključuje dva (2) priloga koji podupiru korisnički priručnik ECSF-a i njegove ciljeve:

- Prilog A povezuje ECSF s drugim standardima i okvirima EU-a.
  Cilj je ovog Priloga povezati ECSF s postojećim priznatim europskim normama i okvirima koji su relevantni za taj rad.
- U Prilogu B navedeni su slučajevi upotrebe ECSF-a.
  Cilj je ovog Priloga pružiti stvarne scenarije kako bi se prikazala praktična provedba ovog okvira.

2. RAZUMIJEVANJE ECSF-A

ECSF se sastoji od reprezentativnog skupa od **12 profila uloga stručnjaka za kibersigurnost** (prikazanih na slici 1.) koji se obično zahtijevaju i primjenjuju u organizacijama koje raspoređuju stručnjake za kibersigurnost. Svaki je profil definiran zajedničkim predloškom koji uključuje ključne kriterije (tj. titulu, alternativne nazive, sažetu izjavu, misiju, glavne zadaće, ključne vještine, ključna znanja, e-kompetencije). Sadržaj svakog kriterija prilagođen je svakoj ulozi, ali podložan je mogućoj prilagodbi kako bi se omogućila fleksibilna provedba kako bi se zadovoljile specifične situacije i zahtjevi.

Slika 1.: 12 profila uloga ECSF-a za stručnjake za kibersigurnost

ECSF uvodi reprezentativan skup od 12 profila uloga za stručnjake za kibersigurnost (koji se obično zahtijevaju i primjenjuju u organizacijama) u formatu koji je dogovoren na razini EU-a i koji se temelji na praksi i koji je namijenjen stručnom području kibersigurnosti.

12 profila uloga stručnjaka za kibersigurnost dostupno je u formatu koji je dogovoren na razini EU-a i usmjeren na praksu i koji je namijenjen stručnoj domeni kibersigurnosti. Profili su lako razumljivi i nude alternativne ulazne točke u skladu s kontekstom, perspektivom i potrebama. Putem tih profila ECSF se može koristiti kao zajednički referentni i komunikacijski alat koji se može primijeniti u različitim organizacijama i zemljama za zajedničko unutarnje i vanjsko razumijevanje.

Struktura svakog profila uloge prikazana je u tablici 1 . u nastavku.

Tablica 1.: Sastavnice svakog profila uloge ECSF-a

Naslov profila	Naziv profila profesionalne uloge
Alternativni naslov(i)	Navodi tipične alternativne naslove pod istim profilom.
Sažetak izjave	Označava glavnu svrhu profila.
Misija	Opisuje obrazloženje profila.
Rezultati	Popis tipičnih ishoda profila, koji također objašnjava relevantnost profila s nestručnog stajališta.
Glavni zadatak	Popis tipičnih zadataka koje obavlja profilirana uloga.
Ključne vještine	Popis sposobnosti potrebnih za obavljanje radnih funkcija i dužnosti uloge. Meke vještine i etika su u nekim slučajevima eksplicitne.
Ključna znanja	Popis osnovnih znanja potrebnih za obavljanje radnih funkcija i dužnosti u profiliranoj ulozi.
e-Kompetencije (EN16234-1 e-CF)	Povezivanje s EN16234-1 e-Competence Framework (e-CF) - Zajednički europski okvir za ICT stručnjake u svim sektorima.

Kako je prikazano u tablici 1., profil za svaku ulogu popunjen je skupom opisnih stavki osmišljenih kako bi se pružio pregled uloge u smislu njezina opisa, zadaća i kompetencija. Naslovi i tipični alternativni naslovi mogu se koristiti kao brza referenca za usmjeravanje korisnika ECSF-a do najprikladnijih profila uloga za njihovu primjenu.

Komponente profila uloga **mogu se izmijeniti** kako bi se bolje zadovoljile potrebe dionika, a profili **uloga** (iz ECSF-a i drugih okvira) **mogu se miješati iz** istog razloga. Više informacija o primjeni ECSF-a nalazi se u poglavlju 3.

Meke vještine (koje se nazivaju i transverzalne, prenosive ili bihevioralne vještine) sastavnice su koje su potrebne u svakom skupu profesionalnih vještina; stoga su takve vještine potrebne i stručnjacima u području kibersigurnosti. Širok raspon vještina spada u meke vještine kao što su sposobnosti komunikacije, suradnje s drugima, izvještavanja, utjecaja, kritičkog razmišljanja i upravljanja vremenom i stresom. Ključne meke vještine ugrađene su u komponentu ključnih vještina.

Na primjer, profil uloge glavnog službenika za informacijsku sigurnost (CISO) uključuje kao ključne vještine sposobnosti utjecaja, vođenja, komunikacije, suradnje i suradnje. Sve su to bitne vještine ako CISO želi ostvariti svoje misije i zadatke. Na temelju potreba dionika, profilu za CISO može se dodati više mekih vještina ili se može napraviti mapiranje s okvirom mekih vještina.

Etika je također važan međusektorski element koji utječe na sve aspekte kibersigurnosti i stoga je ključna komponenta vještina u okviru Europskog okvira vještina u području kibersigurnosti (ECSF). U kontekstu kibernetičke sigurnosti, etika se odnosi na to koje su odluke usklađene s našim vrijednostima i što je moralno prihvatljivo i za vlasnika podataka i za organizaciju. Budući da bi stručnjaci za kibernetičku sigurnost mogli dobiti povlašteni pristup različitim vrstama informacija, čak i osjetljivim informacijama, etička svijest važna je vrijednost koju bi trebali imati. Osim toga, etičko donošenje odluka važna je vještina koju bi stručnjaci za kibernetičku sigurnost trebali imati kako njihove odluke utječu na druge pojedince. Kao i u slučaju mekih vještina, ECSF je izričito analizirao je li etička strana sektora usklađena s europskim vrijednostima i etikom.

Zainteresirana strana može provesti detaljniju analizu mekih i etičkih vještina jer je okvir fleksibilan i prilagodljiv.

2.1 NAČELA OBLIKOVANJA ECSF-A

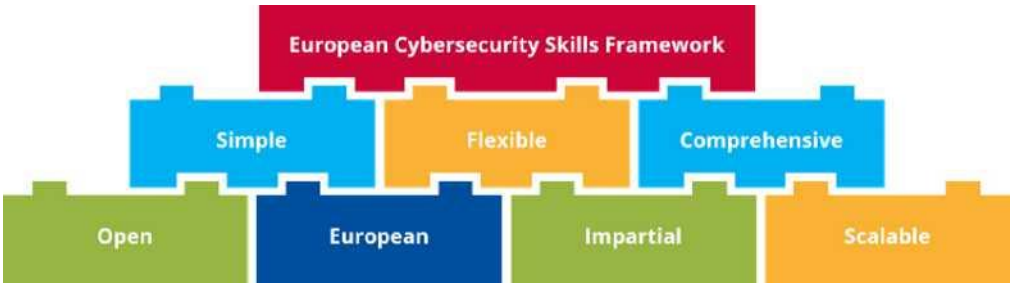
Europski okvir za vještine u području kibersigurnosti temelji se na nizu načela osmišljenih kako bi se zadovoljile potrebe dionika. To omogućuje jednostavno razumijevanje, usvajanje i primjenu okvira, a istovremeno zadržava relevantnost i učinak u kratkoročnom i dugoročnom razdoblju.

2.1.1 Jednostavan, ali sveobuhvatan

Okvir je osmišljen tako da bude prikladno općenit kako bi se osiguralo da ga šira publika može lako razumjeti i primijeniti. Istodobno, uključuje dovoljno detalja za pružanje detaljnih uvida u kibernetičku sigurnost. Ti atributi olakšavaju upotrebu okvira u širokom spektru aktivnosti i okruženja te dionicima iz različitih sredina (npr. organizacije različitih veličina, tehničko stručno znanje različitog intenziteta i poslovni sektori s različitim temeljnim djelatnostima).

ECSF se temelji na načelima osmišljenima kako bi se zadovoljile potrebe dionika, pružajući lako razumijevanje, usvajanje i primjenu uz zadržavanje relevantnosti i učinka u kratkoročnom i dugoročnom

Slika 2.: Načela oblikovanja ECSF-a



To je postignuto primjenom odgovarajuće razine detalja na sadržaj ECSF-a koji nije previše specifičan niti previše apstraktan. S 12 profila, ECSF obuhvaća širok spektar različitih radnih aktivnosti, ali zadržava format jednostavan za korištenje.

2.1.2 Fleksibilan i skalabilan

Usvajanjem modularnog pristupa i fleksibilne strukture, okvir omogućuje da se svaka komponenta može proširiti ili koristiti neovisno. Te značajke podupiru daljnje proširenje ECSF-a i/ili povezivanje s drugim okvirima kako bi se proširile njegove primjene.

Primjenom te fleksibilnosti, profili i njihove komponente, kako su definirani ECSF-om, mogu se primjenjivati po modulima, što omogućuje prilagodbu svakog modula kako bi se zadovoljile specifične potrebe. Ta fleksibilnost osigurava relevantnost okvira tijekom godina i omogućit će jednostavna ažuriranja okvira u budućnosti.

2.1.3 Otvoren i nepristran

Okvir je razvijen uz doprinos velike i raznolike radne skupine profesionalnih stručnjaka za kibersigurnost. Kako bi razvila nepristran okvir, ENISA je osnovala tu skupinu od različitih stručnjaka iz različitih sredina. Uključivanjem stručnjaka iz različitih pozadina, proces razvoja okvira slijedio je višeperspektivni pristup kojim se uklanja svaka pristranost prema određenim područjima interesa. Nadalje, kao publikacija ENISA-e, okvir je javno dostupan, dostupan i otvoren. Profili i komponente ECSF-a razvijeni su na temelju perspektive više dionika s naglaskom ne samo na stajalištu zapošljavanja u području kibersigurnosti, već i iz perspektive pružatelja programa učenja. Nadalje, istinitost okvira poboljšana je angažmanom i preispitivanjima raznih dodatnih dionika.

2.1.4 Europski

Potaknut zahtjevom da se nedostaci u vještinama u području kibersigurnosti i nedostatak radne snage diljem Europe svedu na najmanju moguću mjeru, ECSF je trebao biti usklađen s posebnim europskim zahtjevima kako bi se europskim organizacijama omogućilo jednostavno usvajanje i korištenje. Taj se smjer temeljio na usklađivanju s postojećim europskim standardima i okvirima.

ECSF se dobro povezuje s trenutačnim europskim profesionalnim okruženjem u području IKT-a kako bi se osiguralo lako prihvaćanje i široko priznavanje. ECSF na najbolji način iskorištava postojeća iskustva i strukture te pruža dosljedne veze s relevantnim profesionalnim standardima i okvirima EU-a u području IKT-a. Profili definirani okvirom osmišljeni su tako da budu usklađeni i komplementarni s europskim zakonima i propisima te da poboljšaju pristupe europskoj etici kako je utvrđeno na europskom tržištu. ECSF uzima u obzir zahtjeve za zaštitu podataka i privatnosti postavljene europskim propisima, zajedničke radne uloge koje zahtijeva europsko tržište te europske standarde i

okvire koji se koriste u ICT sektoru.

2.2 GLAVNE KORISTI ECSF-A

ECSF je jednostavan za korištenje, ali sveobuhvatan alat. Temelji se na nedavnim istraživanjima tržišta, suradnji stručnjaka za kibernetičku sigurnost i analizi šireg okruženja okvira za kibersigurnost i IKT. Time se izražavaju relevantne potrebe europskog tržišta. Sastoji se od 12 tipičnih profesionalnih uloga u kibersigurnosti, s povezanim sažetim izjavama, misijom, uočljivim ishodima (rezultatima), zadacima, kompetencijama, vještinama, znanjem i razinama stručnosti, kako je potrebno i primijenjeno u kontekstu rada u Europi, koje treba razumjeti i koristiti u cijeloj Europi.

ECSF pruža nedvosmisleno upućivanje za utvrđivanje i smanjenje trenutačnih i budućih nedostataka i nedostataka vještina u području kibersigurnosti. Općenita je, ali istodobno dovoljno detaljna da tržištu EU-a pruži jasnu taksonomiju vještina, kompetencija i zanimanja radne snage u području kibersigurnosti. Nadalje, može se lako povezati s drugim postojećim strukturama i okvirima u povezanim područjima.

ECSF pruža nedvosmisleno upućivanje za utvrđivanje i smanjenje trenutačnih i budućih nedostataka i nedostataka vještina u

Upotreba ECSF-a kao zajedničkog europskog jezika za profesionalne uloge, vještine, znanje i kompetencije u području kibersigurnosti nudi brojne prednosti, od kojih su neke navedene u nastavku.

1. Upotrebom ECSF-a osigurava se zajednička terminologija i zajedničko razumijevanje između potražnje stručnjaka u području kibersigurnosti (radno mjesto, zapošljavanje) i ponude (kvalifikacija, osposobljavanje, procjena i priznavanje) diljem EU-a.
2. ECSF podupire utvrđivanje kritičnih zahtjeva skupa vještina iz perspektive radne snage. Omogućuje pružateljima programa učenja da podrže razvoj ključnih vještina, a kreatorima politika da podrže ciljane inicijative za ublažavanje utvrđenih nedostataka u vještinama.
3. ECSF pomaže u razumijevanju profesionalnih uloga u području kibersigurnosti i potrebnih osnovnih vještina te relevantnog zakonodavstva. Konkretno, nestručnjaci i odjeli za ljudske resurse mogu bolje razumjeti zahtjeve za planiranje resursa kibernetičke sigurnosti, zapošljavanje i planiranje karijere.
4. ECSF promiče usklađivanje u obrazovanju, osposobljavanju i razvoju radne snage u području kibersigurnosti. Osim toga, upotreba zajedničkog europskog jezika u vještinama i ulogama u području kibersigurnosti izravno se odnosi na cijelo profesionalno područje IKT-a.
5. ECSF pridonosi postizanju bolje otpornosti na kibernapade i osiguravanju sigurnih IKT sustava u cijelom društvu. Njime se pruža standardna struktura i savjeti o tome kako provesti izgradnju kapaciteta europske radne snage u području kibersigurnosti.

ECSF pruža dodatne pogodnosti ovisno o vrsti dionika. Primjer glavnih dionika i ključnih povezanih glavnih koristi prikazan je u 3.

Slika 3.: Primjer glavnih korisnika ECSF-a koji izražavaju potrebu za zajedničkom definicijom upravitelja rizikom

Tablica 2.: Potencijalne primjene ECSF-a i koristi za dionike

Dionika	Prednosti korištenja ECSF-a

Organizacije	• podupire razvoj strategije i organizacijske strukture za kibersigurnost • podupire razvoj planiranja ljudskih resursa u području kibersigurnosti • pruža podršku u postupku zapošljavanja, posebno: o utvrđivanje zahtjeva za uloge u kibersigurnosti o procjenu kandidata za kibersigurnost • pruža analizu uloge i nedostatka vještina u području kibersigurnosti te posljedično predviđanje potrebe na individualnoj, timskoj ili organizacijskoj razini • definira planove razvoja i osposobljavanja na individualnoj, timskoj ili organizacijskoj razini • podupire evaluaciju uloga u području kibersigurnosti pomažući u izgradnji prilagođenih Predlošci za uloge u kibernetičkoj sigurnosti • pruža uobičajen i lako razumljiv jezik za natječaje za kibersigurnost, nabava, slobodna radna mjesta i revizije
Pružatelji programa učenja	• podupire osmišljavanje programa učenja i kurikuluma, preoblikovanje i održavanje • nudi suradnju među institucijama i mobilnost u programima učenja, npr. Međueuropski programi učenja iz više institucija • promiče ponudu programa učenja i podiže svijest • pozicioniranje ishoda učenja u stvarnom kontekstu radnog mjesta • podupiru postupci procjene i priznavanja • studentima pruža profesionalnu orijentaciju

Pojedinci	• podupire pojedince u odabiru profesionalne karijere i pozicioniranju sebe • proširuje perspektive učenja, otvara nove karijere i promiče profesionalne razvoj za potporu prekvalifikaciji i usavršavanju • pomaže u razumijevanju praktičnih zahtjeva na radnom mjestu i očekivanja od posla u više detalj • utvrđuje formalne i neformalne načine učenja • pruža podršku u izgradnji karijernih putova
Strukovna udruženja	• omogućuje konsolidaciju zajednica dionika kako bi se poduprla razmjena znanja, nova kretanja, poboljšanja i daljnja provedba u državama članicama EU-a • pruža podršku u provođenju analize tržišta i predstavljanju rezultata u Zajednički jezik • pomaže u pružanju sveobuhvatnih stručnih smjernica u sektoru kibersigurnosti
Kreatori politika i vladini dionici	• podupire zajedničko razumijevanje u području kibersigurnosti • potiče planiranje prioriteta i izgradnju kapaciteta za kibersigurnost • omogućuje mapiranje mnogih inicijativa za kibersigurnost na temelju profila ECSF-a • podupire političke inicijative koje se temelje na analizi podataka
Sve	• nudi zajednički jezik za sve dionike • ubrzava suradnju pružajući zajedničku referentnu polaznu točku • pruža zajedničku referencu za prikupljanje i predstavljanje stručnjaka za kibersigurnost povezanih s informacije i potrebe na svim razinama, na nacionalnoj, europskoj i međunarodnoj razini

3. PRIMJENE ECSF-A

12 profila uloga definiranih ECSF-om fleksibilan su alat i standardna europska referenca za prilagođenu uporabu u određenom kontekstu.

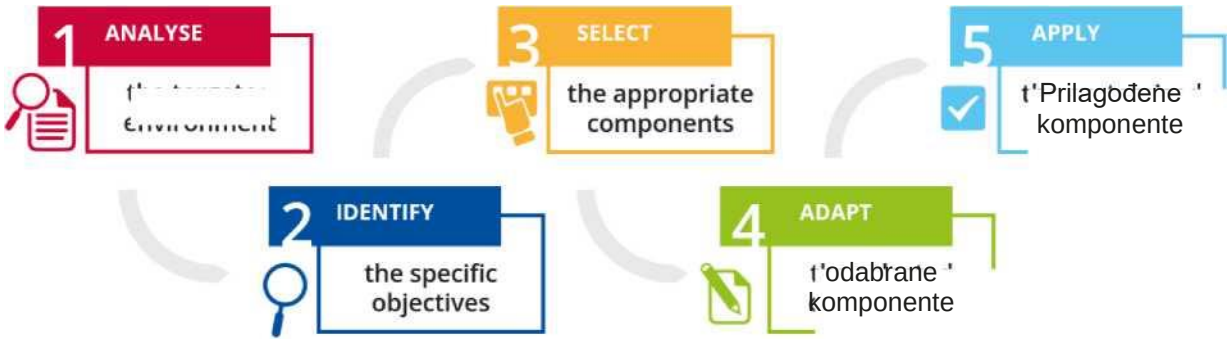
U ovom poglavlju prikazano je kako se Europski okvir vještina u području kibersigurnosti (ECSF) može primijeniti na modularan i fleksibilan način na temelju potreba različitih dionika.

Specifična primjena i praktična primjena ovise o mnogim čimbenicima kao što su tržišna perspektiva, veličina organizacije, kontekst određenog učinka i opća svrha.

12 profila uloga stručnjaka za kibersigurnost definiranih ECSF-om fleksibilan su alat i standardna europska referenca za prilagođenu upotrebu u određenom kontekstu.

Sljedeći opći vodič u pet koraka pruža osnovnu orijentaciju:

Slika 4.: Modularni vodič u pet koraka za primjenu ECSF-a



1. **Analizirajte** stanje ciljnog okruženja.
   Prikupiti i obraditi odgovarajuće potrebne informacije o stanju ciljnog okruženja (npr. organizacije) povezanom s kibersigurnošću kako bi se stvorila polazna vrijednost. Identificirajte uključene strane i cilj koji treba postići.

2. **Identificirajte** specifične ciljeve koje treba postići.
   Razmotriti status ciljnog okruženja i utvrditi sve posebne zahtjeve povezane s kibersigurnošću koje treba obuhvatiti ili bilo koji cilj koji ciljano okruženje treba postići. Ovisno o situaciji, ECSF se može koristiti kao taksonomija za utvrđivanje predmetnih ciljeva.

3. **Odaberite** odgovarajuće komponente ECSF-a.
   Pregledajte profile ECSF-a i odaberite profile koji su relevantni za određenu situaciju. Zatim odaberite komponente koje pomažu u pokrivanju potreba ili postizanju potrebnih ciljeva ciljanog okruženja.

4. Prilagodite odabrane komponente prema svojim potrebama.
   Napravite odgovarajuće promjene na odabranim komponentama kako bi bolje odgovarale određenoj situaciji i/ili ciljanom okruženju. Profili ECSF-a i/ili njihovi sastavni dijelovi mogu se

mješovite, podijeljene ili dovedene u kontekst specifičan za sektor u skladu s potrebama svake situacije.

5. **Primijenite** prilagođene komponente na ciljno okruženje.
   Poduzeti mjere s pomoću prilagođenih komponenti ECSF-a kako bi se obuhvatili ciljevi povezani sa sigurnošću koji su potrebni za poboljšanje stanja u ciljnom okruženju i postizanje organizacijskog cilja.

U tablici 3 . prikazani su neki indikativni primjeri zahtjeva ECSF-a nakon pet prethodno navedenih koraka.

Tablica 3.: Modularni pristup ECSF-a u praksi

Primjer	Korak	Opis
Primjena kibersigurnosti Stručnjaci u organizaciji	1. Analizirajte	Analizirajte trenutno stanje organizacije u vezi s kibernetičkom sigurnošću.
	2. Identificirajte	Identificirajte nedostatak osoblja za rješavanje porasta problema s kibernetičkom sigurnošću.
	3. Odaberite	Odaberite odgovarajući zadatak iz ECSF profila koji artikulira utvrđeni nedostatak ili nedostatak u određenim vještinama.
	4. Prilagodite se	Kombinirati profile ECSF-a sa zadaćama od interesa za organizaciju i strukturirati nove uloge s ažuriranim zadaćama, vještinama i znanjem kako bi se zadovoljile promjenjive organizacijske potrebe i stvorile izmijenjene uloge u području kibersigurnosti.
	5. Prijavite se	Upotrijebite novostvoreni profil za stvaranje slobodnih radnih mjesta usmjerenih na specifične potrebe organizacije.
Usavršavanje kibernetičke sigurnosti Profesionalci	1. Analizirajte	Razumjeti poslovne ciljeve i strategiju organizacije.
	2. Identificirajte	Identificirajte nedostatak stručnosti i osoblja u područjima povezanim s kibernetičkom sigurnošću.
	3. Odaberite	Upotrijebite profile ECSF-a kako biste utvrdili povezane vještine i znanja koja organizaciji nedostaju.
	4. Prilagodite se	Analizirati odabrane vještine i znanja iz ECSF-a kako bi se utvrdile potrebe stručnjaka za kibersigurnost kako bi se zadovoljile potrebe organizacije.
	5. Prijavite se	Identificirati intervencije obuke za poboljšanje kompetencija radne snage organizacije.
Donošenje vlastitih odluka o karijeri	1. Analizirajte	Odaberite karijeru koja vas zanima.
	2. Identificirajte	Utvrdite nedostatak vještina i znanja potrebnih za prelazak u sektor kibernetičke sigurnosti.
	3. Odaberite	Utvrdite profile ECSF-a koji su vam korisni iz perspektive razvoja karijere i upotrijebite povezane vještine, znanja i kompetencije kao smjernice za prekvalifikaciju i usavršavanje.

4. Prilagodite se	Poboljšati odabrane profile ECSF-a uključivanjem dodatnih vještina i znanja na temelju individualnih potreba.
5. Prijavite se	Utvrditi program osposobljavanja koji uključuje većinu vještina i razvoja znanja potrebnih za prekvalifikaciju ili usavršavanje za profil.

3.1 ZAPOŠLJAVANJE STRUČNJAKA ZA KIBERSIGURNOST – PRIMJENA ECSF-A KAO ORGANIZACIJE

ECSF pruža standardni referentni skup od 12 tipičnih uloga koje stručnjaci za kibersigurnost obavljaju iz organizacijske perspektive, a obuhvaća kibersigurnosne potrebe organizacija i kibersigurnosne procese koje je potrebno slijediti kako bi se osiguralo njihovo poslovanje, proizvodi, usluge i njihovi lanci opskrbe. **Okvir stoga pruža vrijedan vodič i plan ne samo za izgradnju, širenje i vođenje funkcija povezanih s kibersigurnošću unutar organizacije, već i za osiguravanje ispunjenja njezine misije, vizije i ciljeva povezanih s kibersigurnošću.** Stoga organizacija može koristiti ECSF kao polazište ili vodič za brz i jednostavan pristup primarnim ulogama potrebnim za upravljanje rizicima u kibersigurnosti i izgradnju pristupa kibersigurnosti. Istodobno, profili ECSF-a pružaju zajedničko razumijevanje uključenih strana u pogledu kibersigurnosnih uloga organizacije.

ECSF se može koristiti kao vodič i plan kojim se osigurava zajedničko razumijevanje uključenih strana u pogledu kibersigurnosnih uloga organizacije.

Tri indikativna primjera, koja su predstavljena kasnije u ovom poglavlju, imaju za cilj prikazati praktičnu provedbu okvira u:

I. poboljšanje praksi kibernetičke sigurnosti male tvrtke;
II. proces zapošljavanja velike tvrtke sa sve većim zahtjevima usklađenosti;
III. planiranje resursa za kibernetičku sigurnost u velikoj organizaciji.

Primjer I.: *Poboljšanje kibersigurnosnih praksi malog poduzeća* predstavlja primjenu ECSF-a za zadovoljavanje potreba malog poduzeća koje želi poboljšati svoju strukturu i praksu u području kibersigurnosti. Pokazuje kako bi se poduzeće moglo koristiti ECSF-om za potporu razvoju strategije kibersigurnosti, uključujući planiranje ljudskih resursa za kibersigurnost i planiranje nabave za kibersigurnost.

Korištenjem ECSF-a kao početne točke ili vodiča, tvrtka ne mora izmišljati ili istraživati osnovne uloge potrebne za poboljšanje svog položaja kibernetičke sigurnosti. Uloge se mogu dodijeliti različitim osobama ili se mogu spojiti kako bi ih preuzela samo jedna ili samo nekoliko osoba, ovisno o strategiji, zahtjevima, potrebama i proračunu.

Primjer pokazuje i kako ECSF može pružiti potporu organizaciji u procesu zapošljavanja utvrđivanjem uloga i odgovornosti u području kibersigurnosti koje su potrebne u malom poduzeću. U ovom primjeru navedena je i analiza nedostatka vještina u području kibersigurnosti te posljedično predviđanje potreba na organizacijskoj razini. Osim što podupire postupke zapošljavanja ljudskih resursa, ECSF pruža i zajednički jezik za nabavu usluga kibersigurnosti.

Primjer I.: Poboljšanje praksi kibersigurnosti malog poduzeća

Mala tvrtka za usluge u oblaku postala je uspješna u samo nekoliko mjeseci nakon što su osnivači, braća i sestre Alicia i Max, implementirali svoju ideju za inovativno rješenje. Alicia je bila stručni 'tehnički' genij, dok je Max bio marketinški genij. Nažalost, nijedan od njih nije imao iskustva u vođenju ili izgradnji tvrtke. Nakon godinu dana tvrtka je počela rasti pa su se preselili u vlastiti ured i zaposlili osoblje za razvoj poslovanja. Tijekom ovog

faza širenja, nitko nije razmišljao o organizaciji tvrtke. Mnoge su uloge i dužnosti podijeljene, a izazovi su rješavani na ad hoc način. Srećom, tijekom ove prijelazne faze nije se dogodio ozbiljan kibernetički incident.

Na kraju je tvrtka stekla određenu medijsku izloženost koja je postala viralna što je rezultiralo povećanim interesom novih investitora i klijenata za mali start-up. Međutim, veći klijenti i investitori zahtijevali su jamstvo i dokaz o odgovarajućim sigurnosnim mjerama i organizacijskoj strukturi prije nego što su se uključili u tvrtku. Osnivači su shvatili da će morati stvarno oblikovati stvari unutar svoje organizacije. Bili su svjesni da su ključ **uspjeha organizacije** zaposlenici i, kako bi organizacija mogla napredovati i ponuditi otporne usluge, **bilo je ključno definirati njihove uloge i odgovornosti u području kibernetičke** sigurnosti. Međutim, pitanje na koje je trebalo odgovoriti bilo je koja je organizacija potrebna te koje su uloge i kakve kompetencije potrebne organizaciji?

Financijeri **su koristili ECSF i utvrdili da je njihovoj organizaciji potrebno pet ključnih uloga** kako bi podržali svoju osnovnu kibersigurnost:

- a strateški menadžer kibernetičke sigurnosti (CISO)
- a Pravni službenik za kibersigurnost
- a Arhitekt kibernetičke sigurnosti
- a malo implementatora kibernetičke sigurnosti
- a Odgovor na kibernetičke incidente.

Tražeći interno kako bi utvrdili mogu li **njihovi zaposlenici pokriti te uloge**, otkrili su da njihova pravna službenica već upravlja usklađenošću s pravnim i regulatornim okvirima i da je u interesu **obogatiti** svoje **kompetencije u pravnim pitanjima privatnosti i kibernetičke** sigurnosti. Ljudski resursi mogli bi **poduprijeti usavršavanje upotrebom** popisa ključnih **znanja** i **vještina** stečenih **iz ECSF-a**.

ICT arhitekt organizacije imao je prethodno iskustvo u projektiranju sigurnih mreža i stoga je uz dodatnu **obuku za ažuriranje i obogaćivanje** svojih **kompetencija** mogao **pokriti i arhitektonske zahtjeve kibernetičke sigurnosti organizacije**.

Administratori sustava slijedili su mnoge najbolje prakse kibernetičke sigurnosti, ali su uglavnom radili na ad-hoc način bez strategije ili strukture. Slijedom toga, osnivači **su identificirali potrebu za zapošljavanjem strateškog menadžera za kibernetičku sigurnost.** Službenik za zapošljavanje imao je zadatak sastaviti **opis posla na temelju CISO profila ECSF-a** i navesti slobodno radno mjesto na njihovoj web stranici. Konačno, utvrđeno je da funkcije odgovora na incidente tvrtke moraju raditi 24 sata dnevno, 7 dana u tjednu kako bi se osigurao kontinuirani rad usluga.

Slika 5.: Ključne potrebne uloge utvrđene upotrebom ECSF-a i mjere koje treba poduzeti

Primjer: Pokazao sam koliko ECSF može biti koristan za sljedeće prednosti:

- Razumijevanje uloga kibernetičke sigurnosti
- utvrđivanje zahtjeva za radnom snagom
- evaluacija procesa i strukture
- prekvalifikacija i/ili usavršavanje zaposlenika
- podrška procesu zapošljavanja
- izgradnja kapaciteta za kibersigurnost
- izgradnja kibersigurne i pouzdane organizacije
- izgradnja otpornosti na kibernapade.

Slika 6.: Prednosti korištenja ECSF-a kao što je prikazano u

Primjer II: *Izrada opisa posla* pokazuje primjenu ECSF-a pri izradi opisa posla. Pokazuje kako ECSF može biti koristan iz perspektive ljudskih resursa bez potrebe za dubokim razumijevanjem profesije u području kibersigurnosti. Ovaj primjer pokazuje kako se može stvoriti slobodno radno mjesto i kako izbjeći stvaranje obmanjujućih ili zbunjujućih očekivanja te kako privući odgovarajuće kvalificirano osoblje. Također pokazuje kako kombinirati komponente profila uloge ECSF-a i kako ih prilagoditi potrebama posla organizacije.
Ovaj primjer pokazuje kako organizacija može upotrijebiti ECSF za izradu opisa uloge. Čak i bez HR znanja, moguće je definirati zadatke, vještine i znanja potrebna kandidatu za zapošljavanje poznavajući misiju uloge. Osim pružanja podrške procesu zapošljavanja, ECSF također može pomoći poduzeću u definiranju planova osposobljavanja za novozaposleno osoblje. Važno je napomenuti da ECSF ne pruža samo zajednički jezik za javnu nabavu u području kibersigurnosti, već i za potrebe revizije, posebno ako se provodi načelo odgovornosti, te je potrebna bitna i jasna podjela dužnosti.

Primjer II: Izrada opisa posla

Veliko osiguravajuće društvo proširuje svoj portfelj na osiguranje kibernetičke sigurnosti jer mnogi klijenti traže ovu uslugu. Nakon blagog internog restrukturiranja i ažuriranja inventara osoblja, tvrtka odlučuje dodati kibernetičku sigurnost u odjel usklađenosti. Slijedom toga, uprava odjela za usklađenost zaključuje da **trebaju zaposliti službenika za cyber usklađenost** koji će podržati novu misiju.

Odjel za ljudske resurse tvrtke zadužen je za **pronalaženje i zapošljavanje najprikladnijeg kandidata**. Budući da je kibernetička sigurnost novo područje za organizaciju, HR također mora **stvoriti opis uloge**. Kako bi definirao ovu novu ulogu, **HR intervjuira obrazovane** menadžere i osoblje **kako bi identificirao potrebe** i **ključne zadatke** za ovu poziciju. Te su potrebe utvrđene, a odabrani su sljedeći ključni zadaci:

- osigurati usklađenost sa standardima, zakonima i propisima o privatnosti i zaštiti podataka te pružiti pravne savjete i smjernice o njima;
- utvrditi i dokumentirati nedostatke u usklađenosti;
- izraditi plan revizije u kojem se opisuju okviri, standardi, postupci i revizijska ispitivanja;
- izvršiti plan revizije i prikupiti dokaze i mjerenja;
- razvoj i priopćavanje rezultata revizije (izvješćivanje).

Odgovorni službenik za ljudske resurse prepoznaje da je to složena uloga i da nisu dostupni predlošci za zapošljavanje koji bi odgovarali toj ulozi. Stoga **uprava mora stvoriti i odobriti** novi opis uloge i predložak.

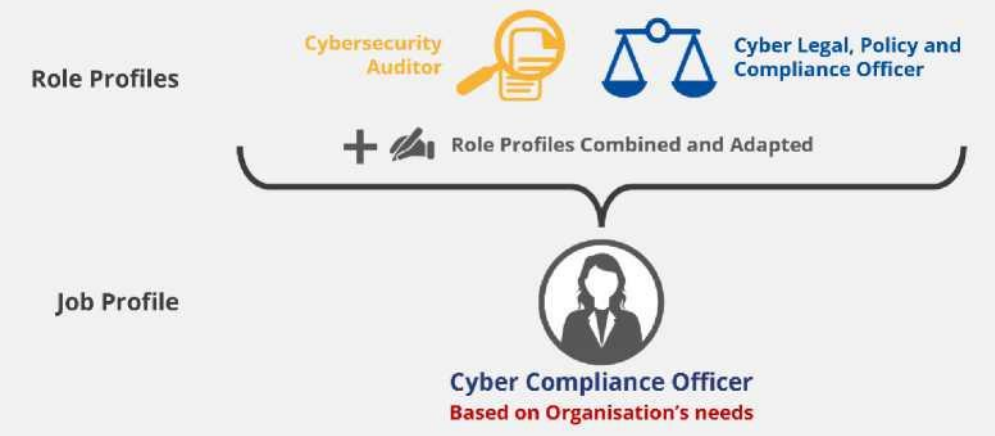
Službenik za ljudske resurse, koji sada **koristi ECSF, analizira različite uloge unutar okvira**. Navedene dužnosti uključene su u **ključne zadatke utvrđene u ulogama** Cyber Pravnog stručnjaka, Službenika za politiku i usklađenost te Revizora **za kibernetičku sigurnost**.

Za obavljanje ovih zadataka potrebne **su identificirane vještine i znanja**:

- Vještine
  - razumjeti implikacije izmjena pravnog okvira na strategiju i politike organizacije u području kibersigurnosti i zaštite podataka;
  - slijediti i prakticirati revizijske okvire, standarde i metodologije;
  - primijeniti revizijske alate i tehnike;
  - Radite kao dio tima i surađujte s kolegama.
- Znanje
  - napredno poznavanje nacionalnih, EU i međunarodnih standarda kibersigurnosti i povezanih standarda, zakonodavstva, politika i propisa o privatnosti;
  - poznavanje usklađenosti informacijske sigurnosti i regulatornih zahtjeva na međunarodnoj, nacionalnoj i EU razini;
  - osnovno razumijevanje pohrane, obrade i zaštite podataka unutar sustava, usluga i infrastruktura.

Novi **opis uloge** prilagođen potrebama poduzeća sada se može izraditi **mapiranjem i kombiniranjem** dijelova profila za ulogu **službenika za kibernetičke pravne poslove, politike i usklađenost** i dijelova profila za ulogu revizora **kibernetičke sigurnosti**. Značajno je da se mapiranjem okvira ova nova jedinstvena uloga **temelji na temeljnom sadržaju ECSF-a**. To osigurava ujednačenu i strukturiranu ulogu koja se može pratiti do njezina podrijetla.

Slika 7.: Profil radnih mjesta u području kibersigurnosti izrađen na temelju profila uloga ECSF-a



Nakon ovog mapiranja na ECSF, potreban opis uloge dostupan je i može se koristiti za izradu uloge i naknadnog opisa posla koji je HR-u potreban za dobivanje internog odobrenja i objavljivanje na web stranici tvrtke za zapošljavanje. Daljnji elementi, kao što je misija profila, mogu se koristiti kao uvodni tekst za objavu ovog slobodnog radnog mjesta.

Primjer II pokazao je koliko ECSF može biti koristan za sljedeće koristi:

- Razumijevanje uloga kibernetičke sigurnosti
- utvrđivanje zahtjeva za radnom snagom
- utvrđivanje zahtjeva za uloge
- podrška procesu zapošljavanja
- potpora izradi prilagođenog predloška za slobodno radno mjesto
- korištenje zajedničkog jezika za slobodna radna mjesta.

Slika 8.: Prednosti korištenja ECSF-a prikazane u primjeru II.

***Primjer III**.: Velika korporacija s glavnom djelatnošću izvan ICT-a mora uspostaviti odjel za kibernetičku sigurnost* demonstrira primjenu ECSF-a pri stvaranju novog odjela za kibernetičku sigurnost i pripremi strategije kibernetičke sigurnosti za korporaciju. Predlaže se i kategorizacija 12 profila u četiri (4) makropodručja za razumijevanje i komunikaciju na visokoj razini. Pokazuje kako velika organizacija može iskoristiti ECSF za potporu razvoju strategije kibersigurnosti,

uključujući planiranje ljudskih resursa i razvoj talenata u području kibersigurnosti.

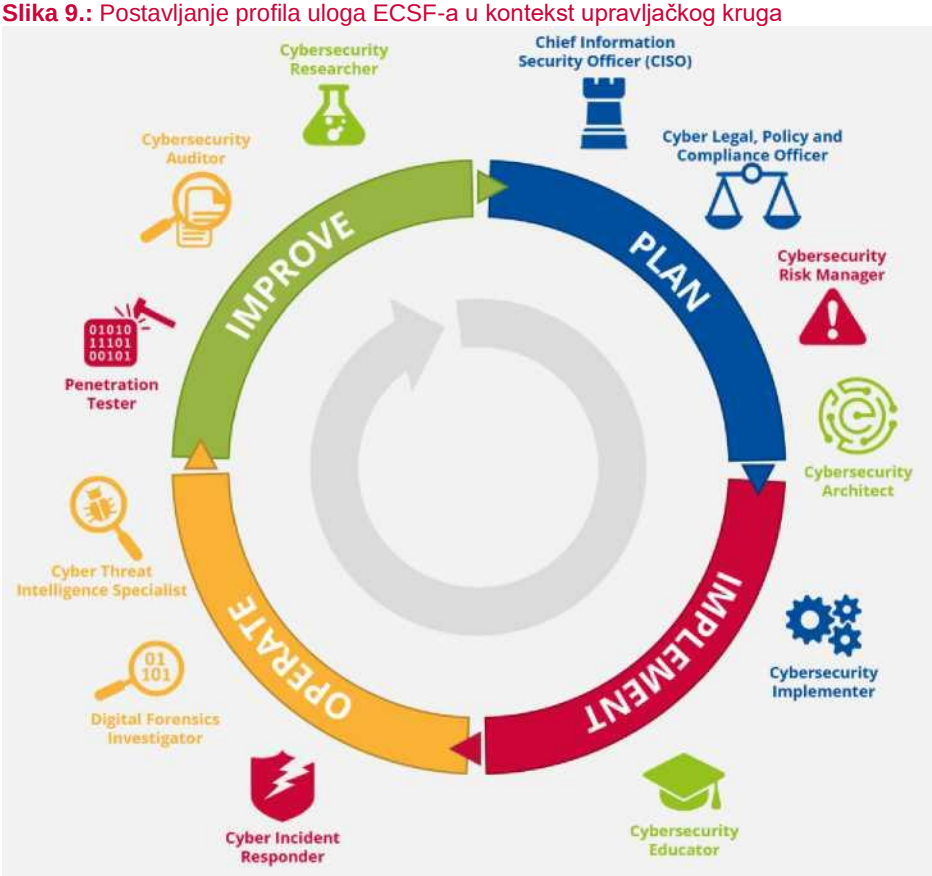
Primjer III.: Velika korporacija s glavnom djelatnošću izvan ICT-a mora osnovati odjel za kibernetičku sigurnost

Velika korporacija s osnovnom djelatnošću koja nije povezana s IKT-om ili uslugama kibersigurnosti shvatila je potrebu za zaštitom svoje vrijedne imovine od kibersigurnosnih prijetnji. Zapravo, usvojena poslovna strategija uključivala je opsežan plan digitalizacije poslovnih procesa, a ovisnost o ICT-u postajala je znatno veća za kritične poslovne operacije.

Budući da tvrtka nije imala nikakvu internu stručnost za rješavanje rizika kibernetičke sigurnosti, odbor je odlučio zaposliti glavnog službenika za sigurnosne informacije (CISO) kako bi **definirao cjelokupnu strategiju kibernetičke sigurnosti** u skladu s poslovnim ciljevima tvrtke. To bi također zahtijevalo **osnivanje odjela** za **rješavanje kibernetičkih rizika**.

CISO, koji je nedavno imenovan, **koristio je ECSF kao smjernicu i** kao čvrstu referencu **za** uloge u kibernetičkoj sigurnosti potrebne za rješavanje kibersigurnosnih rizika. Koristila ga je kao **fleksibilan alat** za pomoć u **strukturiranju odjela za kibernetičku sigurnost**. Također je prepoznala da bi, kako bi se osigurala jasna shema, bilo korisno smjestiti **uloge ECSF-a u kontekst upravljačkog kruga**, u četiri (4) makro područja: a) Plan, b) Provedba, c) Operacija i d) Poboljšanje.

Slika 9.: Postavljanje profila uloga ECSF-a u kontekst upravljačkog kruga



U makro području Plana postavljeni su prioriteti i ciljevi, razvijene strategije, politike i akcijski planovi, definirane arhitekture, dodijeljena sredstva. U ovom makro području profili CISO-a, službenika za politiku i usklađenost, voditelja rizika i arhitekta bili su prirodno pozicionirani.

Provedba mjera kibernetičke sigurnosti (Implementator) te obuka i podizanje svijesti (Edukator) dodijeljeni su makro području Implementacija.

Svakodnevne operacije bile su "najopipljivije" područje. Reagiranje na incidente (uključujući SOC timove), forenzičke aktivnosti su svakodnevne aktivnosti stručnjaka za kibernetičku sigurnost. Profil obavještajnih podataka o prijetnjama također se smatrao operativnim područjem, jer ti stručnjaci rade na operativnim podacima koristeći više izvora.

Penetracijski tester (testiranje trenutnih i novih prijetnji), istraživač (donošenje novih tehnologija i rješenja) i revizor (identificiranje nedostataka) podržavaju fazu poboljšanja.

Međutim, budući da je ECSF fleksibilan alat za prilagođenu upotrebu u određenom kontekstu, CISO **je primijenio vodič u 5 koraka kako bi prilagodio profile uloga svojim specifičnim potrebama i ciljevima**.
Analiza profila ECSF-a pomogla joj je da definira **planove resursa** potrebne za postizanje korporativnog cilja.

U makro području Plana odlučila je:

- biti zadužen za zadaće politike i usklađenosti kako bi se pojednostavila organizacijska struktura;
- angažirati arhitekta za kibersigurnost koji bi pomogao definirati cjelokupnu strategiju arhitekture za suočavanje s rizicima kibersigurnosti i osigurati sigurna rješenja za potporu digitalnoj transformaciji;

- Angažirajte upravitelja rizika kibernetičke sigurnosti koji će vam pomoći u procjeni stanja korporativnih kibernetičkih rizika i pomoći u definiranju akcijskih planova za upravljanje identificiranim rizicima.

U makro području implementacije iskoristila je **komponente vještina i znanja ECSF-a** kako bi **razumjela koje bi usavršavanje bilo potrebno** kako bi se iskoristili dostupni interni resursi ili alternativno odlučila za zapošljavanje izvana. Multinacionalna korporacija imala je postojeći tim instruktora u drugom području. Međutim, nije postojao stručni tim koji bi osmislio i proveo tečajeve podizanja svijesti o kibernetičkoj sigurnosti ili obuke. CISO **je istražio jesu li neki od trenera imali vještine i znanja navedene u ECSF-u** i interes **da se pridruže njezinom novom** timu.

U makro području Operate, CISO je razmotrio kako upravljati svakodnevnim operacijama kibernetičke sigurnosti i odlučio **uspostaviti globalne sigurnosne operativne centre s odgovorima na incidente** koji rade na različitim kontinentima kako bi pružili podršku 24/7. Štoviše, **stručnjak za obavještajne podatke o prijetnjama angažiran** je za pružanje operativnih uvida za usmjeravanje lova na prijetnje i ublažavanje rizika. CISO je zaključio da nema **potrebe angažirati digitalnog forenzičkog istražitelja** , već **angažirati specijaliziranu konzultantsku tvrtku** za sve **forenzičke potrebe**.

U makro području Poboljšaj, CISO je odlučio angažirati vanjskog pružatelja **usluga za penetracijsko testiranje** s ciljem testiranja otpornosti korporativne infrastrukture i aplikacija. CISO je također procijenio kapacitet tima za unutarnju reviziju i odlučio angažirati **revizora kibernetičke sigurnosti** za reviziju politika povezanih sa sigurnošću. CISO nije osjećao potrebu zaposliti istraživača kibernetičke sigurnosti jer su istraživanja kibernetičke sigurnosti bila izvan djelokruga njezine organizacije.

Ukratko, u primjeru III . istaknuto je koliko ECSF može biti koristan za sljedeće koristi:

- Razumijevanje uloga kibernetičke sigurnosti
- pomoć u stvaranju organizacijske strukture
- utvrđivanje zahtjeva za uloge u kibersigurnosti
- pomoć u planiranju ljudskih resursa
- usavršavanje zaposlenika
- potpora procjeni kandidata
- Korištenje uobičajene terminologijeza suradnju.

Slika 10.: Prednosti upotrebe ECSF-a prikazane u primjeru III.

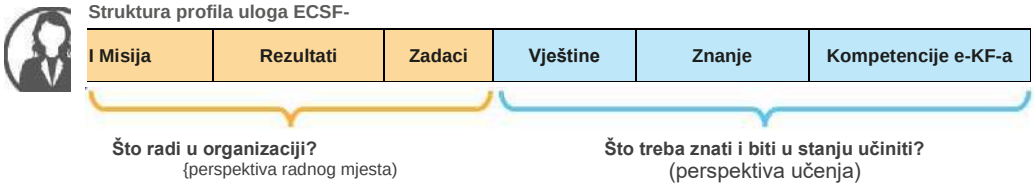
3.2 STJECANJE VJEŠTINA STRUČNJAKA ZA KIBERSIGURNOST – PRIMIJENITE ECSF KAO PRUŽATELJ OBRAZOVANJA

ECSF nudi zajednički jezik i vokabular za razvoj profesionalnih vještina u području kibersigurnosti pružateljima programa učenja i obrazovnih ustanova svih vrsta, kao što su visoko obrazovanje, strukovno obrazovanje i osposobljavanje ili bilo koji drugi obrazovni program ili osposobljavanje povezani s kibersigurnošću. Definirani profili uloga pružaju pristup usmjeren na kibersigurnost na radnom mjestu i ugrađen u Europu kako bi se postojeći zahtjevi za stručnu praksu povezali s kurikulumima i programima učenja povezanima s kibersigurnošću.

ECSF definira tipične zahtjeve profila s dva temeljna gledišta.

- Čemu služi ova uloga u organizaciji?
  Bavi se perspektivom radnog mjesta (odjeljci profila o misiji, rezultatima i zadacima)
- Što ova uloga treba znati i moći učiniti?
  Bavite se perspektivom učenja (profilni odjeljci o vještinama, znanju i kompetencijama e-KF-a)

Slika 11.: Odjeljci o profilima uloga ECSF-a povezani s radnim mjestom i perspektivama učenja



ECSF pozicionira ishode učenja u stvarnom kontekstu na radnom mjestu. Konkretno, opisi uloga u profilima ECSF-a omogućuju pružateljima programa učenja da preispitaju svoje kurikulume na strukturiran i sustavan način, među ostalim sa stajališta stručnjaka.

ECSF nudi zajednički jezik i vokabular za razvoj profesionalnih vještina u području kibersigurnosti pružateljima programa učenja i obrazovnim ustanovama svih vrsta.

Kako je prikazano u Prilogu B.2., ECSF bi mogao doprinijeti nekoliko aktivnosti koje se poduzimaju u akademskim ustanovama.

- ECSF može poslužiti za razvoj ili ažuriranje ishoda učenja tečajeva i njegovo usklađivanje s potrebama tržišta rada. Vještine, znanja i kompetencije unutar profila uloge mogu se koristiti za usmjeravanje faze osmišljavanja kurikuluma i potporu uspostavljanju željenih ishoda učenja. Na primjer, kada se analiziraju obrazovne potrebe određenog posla u području kibersigurnosti, usklađeni profil ECSF-a pruža solidnu polaznu točku za razumijevanje povezanih obrazovnih zahtjeva.
- ECSF bi mogao poslužiti kao alat za suradnju za stvaranje zajedničkih akademskih programa i omogućavanje mobilnosti studenata.
- ECSF bi mogao poslužiti kao osnova za definiranje okvira za kurikulum kibersigurnosti koji bi pomogao sveučilištima da mapiraju glavni fokus svojeg programa kibersigurnosti i priopće ga studentima.

Kako je prikazano u Prilogu B.1., ECSF rješava neke od izazova utvrđenih u europskom okruženju stručnih kvalifikacija u području kibersigurnosti. Posebno:

- ECSF podupire međudomensku i međuindustrijsku terminologiju povezanu s vještinama u području kibersigurnosti;
- ECSF bi mogao poduprijeti razvoj integrirane platforme za vještine kako bi se pružile ažurirane informacije o tržištu rada, kompetencijama, tečajevima osposobljavanja, programima certificiranja i planu za karijeru.

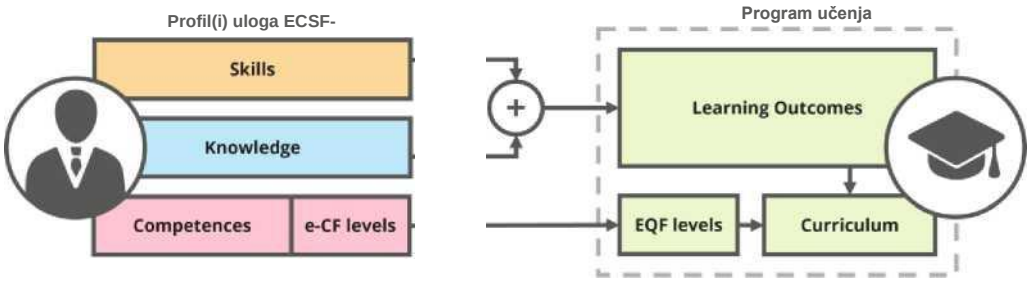
Slika 12.: Prednosti korištenja ECSF-a kao pružatelja učenja

ECSF se može koristiti kao komunikacijski alat između poslodavaca i nastavnika.

U kontekstu razvoja kvalifikacija u području kibersigurnosti i izrade kurikuluma, profili uloga ECSF-a služe kao komunikacijski alat između poslodavaca i nastavnika kako bi se poboljšao postupak savjetovanja i ishodi suradnje. Poslodavac može brzo definirati potrebne aktivnosti ili zadatke i raditi unatrag kako bi utvrdio kompetencije, vještine i znanja koja bi nastavnici trebali uključiti u kurikulume. Ovaj pristup značajno ubrzava oblikovanje kurikuluma dogovorenih između poslodavaca, vlada i nastavnika.

Na slici 13. prikazano je kako se dijelovi profila uloga ECSF-a posvećeni kompetencijama, znanju i vještinama mogu upotrijebiti za definiranje ishoda učenja, utvrđivanje odgovarajućih razina programa učenja i izradu kurikuluma za zanimanja u području kibersigurnosti. Budući da su znanja i vještine, kao i sav sadržaj opisa uloga, navedeni kao vodeći primjeri za fleksibilnu prilagodbu kontekstu, mogu se koristiti i drugi izvori.[8]

Slika 13.: Profili ECSF-a kojima se vodi stručno učenje u području



Povezivanje razina učenja (EQF) i razina stručnosti na radnom mjestu (e-KF)

Europski kvalifikacijski okvir (EQF) zajednički je europski referentni okvir za kvalifikacije. Svrha je europskog kvalifikacijskog okvira usporediti kvalifikacije i ishode učenja koji nastaju u različitim zemljama i nacionalnim obrazovnim sustavima. Europski kvalifikacijski okvir temelji se na

Preporuka o Europskom kvalifikacijskom okviru za cjeloživotno učenje koju su Europski parlament

[8] Odjeljci ECSF-a o vještinama, znanju i kompetencijama nisu ni iscrpni ni restriktivni, što korisniku omogućuje da ih obogati uključivanjem i vanjskih resursa, npr. Korpus znanja o kibernetičkoj sigurnosti (CyBOK) https://www.cybok.org/, JRC Klasifikacija https://joint-research-centre.ec.europa.eu/publications/unified-conceptual-okvir-zadataka-vještina i kompetencija hr

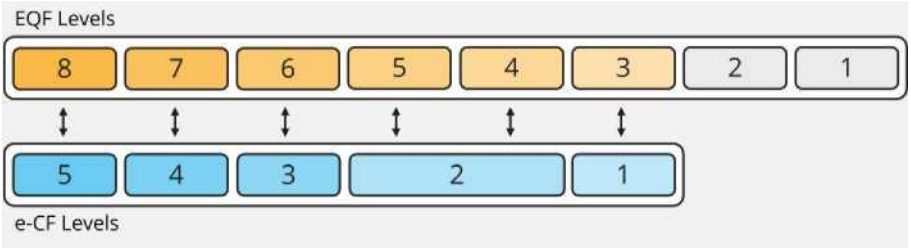
i Vijeće donijeli 23. travnja 20089.

Europskim kvalifikacijskim okvirom definira se osam (8) razina obrazovnog postignuća s deskriptorima koji razlikuju svaku razinu. Kriterij za svaku razinu temelji se na procjeni znanja, vještina, odgovornosti i autonomije.

Europski **okvir e-kompetencija (e-KF),** norma EN 16234-1, koju koristi ECSF, zajednički je europski okvir za stručne kompetencije, znanja i vještine u području [9]IKT-a. Odnosi se na kompetencije prema potrebi i primjenjuju se na radnom mjestu. Dimenzija 3 e-CF-a definira razine kompetencija koje proizlaze iz stručnosti na radnom mjestu. Postoji pet (5) definiranih razina e-kompetencija od e-1 do e-5 koje se odnose na razine učenja od 3 do 8 Europskog kvalifikacijskog okvira (razine 1 i 2 EQF-a nisu relevantne u ovom kontekstu).

U nastavku je prikazan odnos između razina e-CF e-1 do e-5 s razinama 3. – 8. europskog kvalifikacijskog okvira:

Slika 14.: Odnos između razina EQF-a i e-CF-a



Zahvaljujući ovom sustavno razvijenom odnosu, moguće je povezati razine znanja e-CF-a s razinama učenja EQF-a. Odnos, zbog različite prirode svakog okvira, nije potpuno ekvivalentan. Međutim, može se primijeniti kako bi se povećala transparentnost i **osigurao zajednički jezik između zahtjeva za profesionalne kompetencije na radnom mjestu i povezanih kvalifikacija obrazovnih** [10]ustanova. Stoga se razine kompetencija e-CF-a uključene u profile uloga ECSF-a mogu koristiti kao opći vodič za potrebne razine obrazovanja.

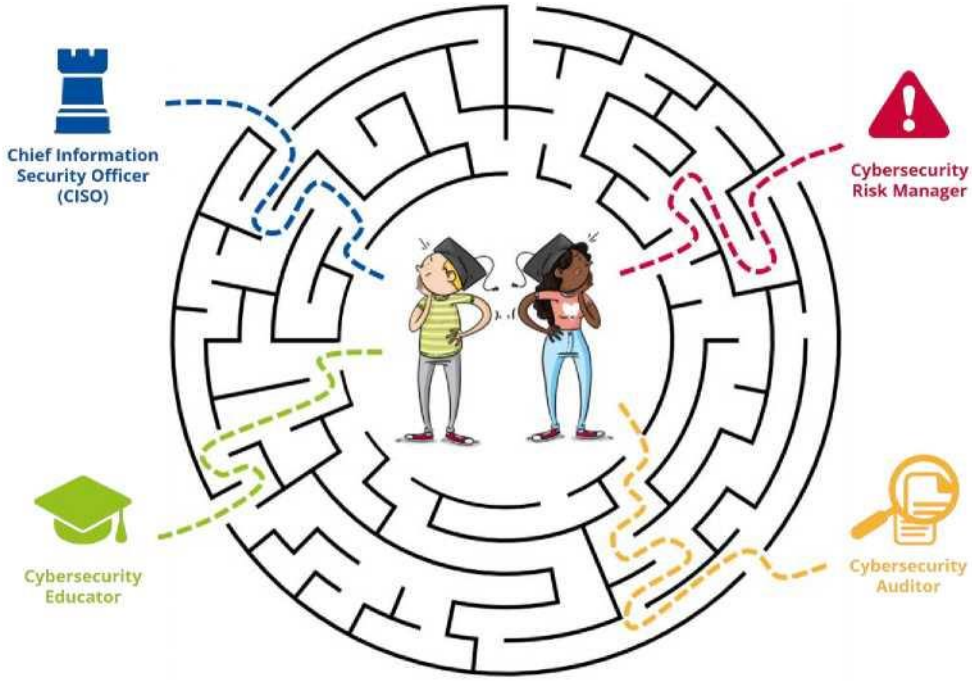
[9] EN16234-1:2019: Okvir e-kompetencija (e-KF) - zajednički europski okvir za stručnjake u području IKT-a u svim sektorima
[10] Za dodatne praktične smjernice vidjeti: CEN/TS 17699:2022 Smjernice za razvoj stručnih kurikuluma IKT-a u skladu s područjem primjene EN16234-1 (e-KF)

3.3 DONOŠENJE VLASTITIH ODLUKA O KARIJERI – PRIMIJENITI ECSF KAO POJEDINAČNI STRUČNJAK

Zajednički jezik definiran ECSF-om može se koristiti za uklanjanje zabune između profesionalnih radnih mjesta u području kibersigurnosti i obrazovnih programa za kibersigurnost. Pružanjem zajedničkog jezika i jasnog opisa profesionalnih radnih uloga u području kibersigurnosti, zadaća za koje se očekuje da će ih obavljati te potrebnih vještina, kompetencija i znanja, ECSF može izgraditi zajedničko razumijevanje i pružiti jasnoću potrebnu za privlačenje novih pojedinaca u područje kibersigurnosti ili pomoć u planiranju njihove karijere.

Stručnjaci koji već rade na pozicijama povezanima s kibersigurnošću mogu koristiti ECSF kao

Slika 15.: Upotreba ECSF-a za definiranje karijernih putova



vodič za napredovanje u svom području. Mapiranjem svojih vještina i znanja u profile uloga ECSF-a koji ih zanimaju, pojedinci mogu identificirati sve vještine ili znanja koja im nedostaju za razvoj, savladavanje ili učenje kako bi bili spremni pokriti buduće zahtjeve za posao ili moguće prijelaze s jedne uloge u području kibersigurnosti dok napreduju u svojoj profesionalnoj karijeri. To pomaže u dijalogu između zaposlenika i poslodavaca pri planiranju kontinuirane edukacije u području kibernetičke sigurnosti. Budući da ECSF navodi i formalne i neformalne načine učenja, pomaže i novim sudionicima koji nisu svjesni odakle početi. Dodavanje prethodnog znanja i kompetencija često je lakši put od početka potpuno iznova. Prilog B.6 bavi se ovom temom i pruža dublje uvide i primjere u "pojedinačnom donošenju odluka o karijeri" s pomoću ECSF-a.

ECSF može izgraditi zajedničko razumijevanje i pružiti jasnoću potrebnu za privlačenje novih pojedinaca u područje kibersigurnosti ili im pomoći u planiranju njihove

Koristeći ECSF kao osnovu, pojedinac može identificirati potrebne kompetencije i vještine za prelazak iz jedne uloge u drugu ili za utvrđivanje trenutnih potreba za osposobljavanjem.

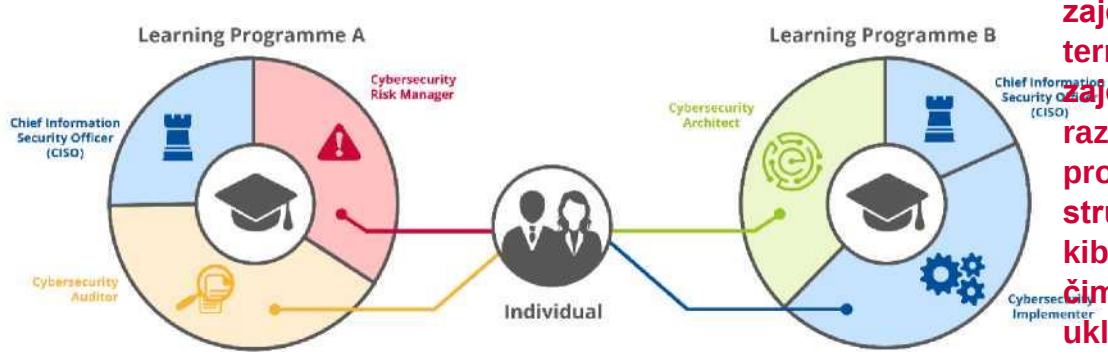
Zajednički jezik definiran ECSF-om može biti koristan za pojedince koji traže poslove u području kibersigurnosti. ECSF može pomoći u filtriranju otvorenih radnih mjesta i razumijevanju opisa radnog mjesta, a također može olakšati ukupnu mobilnost radnog mjesta u području kibersigurnosti mapiranjem vještina, znanja i kompetencija pojedinca u ECSF-u.

Kibernetička sigurnost dobra je prilika za karijeru čak i za pojedince koji su trenutno specijalizirani za druga područja, stoga je prekvalifikacija ljudi i njihovo premještanje u područje kibernetičke sigurnosti dobar način da se zadovolje potrebe tržišta za radnom snagom i smanje praznine radne snage u tom području. Budući da je kibernetička sigurnost multidisciplinarna tema, takva bi promjena karijere mogla biti brža za pojedince s pozadinom bliskom jednom od glavnih aspekata tog područja[11]:

- **tehničke** – povezane s tehnologijom, konkretnim tehnološkim pristupima i rješenjima koja se mogu koristiti u borbi protiv kibernetičkog kriminala i kiberterorizma;
- **ljudske** – povezane s ljudskim čimbenicima, aspektima ponašanja, pitanjima privatnosti, kao i podizanjem svijesti i znanja društva o prijetnjama kibernetičkog kriminala i terorizma;
- **organizacijski** - vezani uz procese, postupke i politike unutar organizacija, kao i suradnju (javno-privatnu, javno-javnu) između organizacija;
- **regulatorni** - u vezi s odredbama zakona, standardizacije i forenzike.

Imajući jasno razumijevanje glavnih profila uloga u području kibersigurnosti u tom području i zajednički jezik za kibersigurnost u širem rasponu sektora, kako je predviđeno ECSF-om, pojedinci koji žele promijeniti karijeru u području kibersigurnosti mogu koristiti ECSF kao polazište za utvrđivanje posebnih kompetencija, vještina i znanja koje trebaju steći za tranziciju.

Slika 16.: Upotreba ECSF-a za analizu i usporedbu programa učenja o kibersigurnosti



Bez obzira na to radi li pojedinac u području kibersigurnosti (želi proširiti svoje znanje), trenutačno je zaposlen u drugom području (želi promijeniti karijeru) ili traži akademsko obrazovanje (u budućnosti želi raditi u području kibersigurnosti), ECSF može pomoći u razumijevanju glavnih profila uloga u području kibersigurnosti (davanjem opisa i analizom u zadatke, vještine, znanja i kompetencije) te pomoć u analizi i usporedbi dostupnih programa učenja (mapiranje ishoda učenja s potrebnim vještinama i znanjem o preferiranim profilima kibersigurnosti).

ECSF stvara zajedničku terminologiju i zajedničko razumijevanje profila uloga stručnjaka za kibersigurnost, čime se može ukloniti terminološka zbrka i nedostatak razumijevanja

3.4 IZGRADNJA ZAJEDNICA U PODRUČJU KIBERSIGURNOSTI – PRIMJENA ECSF-A KAO STRUKOVNOG UDRUŽENJA

ECSF stvara zajedničku terminologiju i zajedničko razumijevanje profila uloga stručnjaka za kibersigurnost. Stoga ga strukovna udruženja mogu upotrebljavati kao standard kako bi osigurala da se njihov rad može upotrebljavati i primjenjivati u cijelom EU-u, čime se uklanjaju terminološke zabune i nerazumijevanje.

Strukovne organizacije mogu koristiti okvir za provođenje analiza tržišta s pomoću profila uloga ECSF-a i predstavljanje rezultata na zajedničkom jeziku. Na primjer, očekuje se da će ECSF biti od pomoći u isticanju profila koji nedostaju na tržištu, radnih mjesta u području kibersigurnosti koja

[11] https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity

su vrlo traženi, kao i zakonodavni aspekti nekih profesionalnih profila poslova. Nadalje, upotrebom ECSF-a kao zajedničke terminologije strukovna udruženja mogu raditi na profesionalnom usmjeravanju u sektoru kibersigurnosti, kako je prikazano u Prilogu B.5.

Upotreba ECSF-a omogućuje i konsolidaciju zajednice dionika kako bi se poduprla nova kretanja, poboljšanja i daljnja provedba u državama članicama EU-a. Takav okvir za suradnju omogućuje ljudsku interakciju koja rezultira koristima kao što su razmjena znanja, utvrđivanje trendova na razini EU-a, aktivnosti uzajamnog učenja, primjena multidisciplinarnih pristupa i osnaživanje za prilagodbu ECSF-a posebnim zahtjevima.

Općenito, profesionalna udruženja za kibersigurnost mogu koristiti ECSF kao alat za temeljenje svojih aktivnosti na osiguravanju njihove primjenjivosti u cijelom EU-u u cilju postizanja boljeg pooštravanja protiv kibernapada u cijelom EU-u kao društvu.

3.5 STRATEŠKO OSNAŽIVANJE SEKTORA – PRIMJENA ECSF-A KAO OBLIKOVATELJA POLITIKA

S ECSF-om, ključna profesionalna zajednica osigurava jasnu vidljivost jer korištenje okvira stvara zajedničko razumijevanje onoga što stručnjaci za kibernetičku sigurnost rade. Stoga ECSF pruža alat za analizu i razmjenu ključnih zbirki podataka i statističkih podataka povezanih s radnom snagom u području kibersigurnosti u zajedničkoj i razumljivoj terminologiji na razini EU-a. Takvi su podaci važni za tvorce politika jer stječu bolji uvid u stanje radne snage u području kibersigurnosti diljem EU-a, što im omogućuje da razumiju i procijene buduće potrebe stručnjaka za kibersigurnost u pogledu količine i kvalitete. Takav strateški doprinos pomaže u ažuriranju i održavanju samog ECSF-a kako bi njegova relevantnost u budućnosti ostala valjana. Nadalje, definiranjem zajedničke terminologije ECSF omogućuje prekograničnu suradnju među tvorcima politika razmjenom podataka i informacija.

S obzirom na strukturirani pristup vrlo raznolikom tržišnom okruženju, profili uloga ECSF-a vrijedan su alat za potporu oblikovateljima politika, istraživačima tržišta i drugim dionicima koji imaju utjecaj i ulogu u strateškom osnaživanju sektora.

S obzirom na strukturirani pristup vrlo raznolikom tržišnom okruženju, profili uloga ECSF-a vrijedan su alat za potporu oblikovateljima politika, istraživačima tržišta i drugim dionicima koji imaju utjecaj i ulogu u strateškom osnaživanju sektora. Profili ECSF-a mogu biti korisni za studije podataka o ponudi i potražnji koje se provode na nacionalnoj, europskoj i međunarodnoj razini. Profili sadržavaju zajedničku, dogovorenu definiciju kako bi se olakšalo prikupljanje pouzdanih i usporedivih podataka na tržištu rada u području kibersigurnosti, uključujući ponudu i potražnju za različitim vrstama stručnjaka za kibersigurnost i povezane zahtjeve za određene vještine.

Postupci donošenja politika koji se odnose na kibersigurnost mogu imati koristi od prikupljanja podataka u trenutku donošenja odluka, npr. odredbe o financiranju, prioriteti ulaganja i razdoblja intervencije. Osim temeljnih aktivnosti svakog profila, aktivnosti koje provode mogu doprinijeti stvaranju i prikupljanju relevantnih skupova podataka koji mogu poduprijeti odluke o politikama. Prilog B.3 pokazuje kako fragmentirane informacije predstavljaju izazov pri donošenju odluka i mjere koje INCIBE poduzima u rješavanju tog izazova uz potporu ECSF-a. Uključivanjem ECSF-a kao homogenog okvira za definiranje kibersigurnosnih profila države članice EU-a dobivaju dragocjenu potporu u postizanju svojih ciljeva povećanja talenata u području kibersigurnosti i usklađivanja s ostalim zemljama na europskoj razini.

4. POJMOVI I DEFINICIJE

Termin	Definicija	Izvor
kibersigurnost	Sve aktivnosti potrebne za zaštitu mrežnih i informacijskih sustava, korisnika takvih sustava i drugih osoba pogođenih kiberprijetnjama.	Mandat ENISA-e (Uredba (EU) 2019/881)
kibernetička prijetnja	Sve potencijalne okolnosti, događaje ili radnje koje bi mogle oštetiti, poremetiti ili na drugi način negativno utjecati na mrežne i informacijske sustave, korisnike takvih sustava i druge osobe.	Mandat ENISA-e (Uredba (EU) 2019/881)
Informacijska i komunikacijska tehnologija	ICT je kratica za informacijsku i komunikacijsku tehnologiju. Koristi se u mnogim različitim kontekstima, a s tehničkog stajališta IKT se odnosi na digitalna računala i internetske (komunikacijske) sustave, uključujući softver, hardver i mreže. S gospodarskog i političkog stajališta, IKT se odnosi na međusektor poduzeća, uključujući proizvođače, dobavljače proizvoda ili pružatelje usluga koji se odnose na područje IKT-a.	EN16234-1:2019 Okvir e-kompetencija (e-KF)
nadležnost	Dokazana sposobnost primjene znanja, vještina i stavova za postizanje vidljivih rezultata. Primjeri su B.1. Razvoj aplikacija i E.3. Upravljanje rizicima.	EN16234-1:2019 Okvir e-kompetencija (e-KF)
vještina	Sposobnost obavljanja upravljačkih ili tehničkih aktivnosti i zadataka na kognitivnoj ili praktičnoj razini; znati kako to učiniti.	EN16234-1:2019 Okvir e-kompetencija (e-KF)
meke vještine	Interaktivne vještine koje se koriste za uspješnu interakciju sa situacijama na radnom mjestu; može se odnositi na kvalitetu rada, društvenu interakciju ili emocije. (koje se nazivaju i transverzalne, prenosive ili bihevioralne vještine)	EN16234-1:2019 Okvir e-kompetencija (e-KF)
znanje	Skup činjenica koje se primjenjuju u području rada ili studija; znati što učiniti.	EN16234-1:2019 Okvir e-kompetencija (e-KF)
stav	Prikaz ljudskog elementa e-kompetencije; Odražava kako osoba integrira znanja i vještine i primjenjuje ih na odgovarajući način u kontekstu.	EN16234-1:2019 Okvir e-kompetencija (e-KF)
Ishod učenja	Izjava o tome što osoba zna, razumije i može učiniti po završetku procesa učenja	Europski kvalifikacijski okvir (EQF)
Profil uloge	Nacrt ili opći dokument koji pokazuje odnos između određenih aktivnosti ili zadataka u ulozi i pojedinačnih vještina, kompetencija i znanja potrebnih za njihovo poduzimanje. Za razliku od određenog posla, uloga proizlazi iz	Kreativno vodstvo - Upravljanje talentima CWA ICT profili

	organizacijska potreba da nešto učini. Dodijeljeni zaposlenici mogu ispuniti organizacijske zahtjeve izvršavanjem svih ili dijela zadataka potrebnih za osiguranje njihove uloge.	
profil posla	Kontekstualno specifičan i detaljan opis onoga što zaposlenik radi kako bi osigurao da nositelj posla nema sumnje u svoje zadatke, dužnosti, odgovornosti, a često i one kojima odgovara. Obično sadržava precizne informacije o potrebnim kompetencijama, vještinama i znanju te praktične informacije o zdravlju i sigurnosti te naknadama.	ICT profili CWA
razina stručnosti	Jasan pokazatelj stupnja majstorstva koji omogućuje stručnjaku da ispuni zahtjeve u obavljanju kompetencije. EN 16234-1 (e-CF) uključuje razine stručnosti od e-1 do e-5. e-CF karakterizira razine stručnosti kombinirajući razine utjecaja unutar zajednice, složenost konteksta i autonomiju.	EN16234-1:2019 Okvir e-kompetencija (e-KF)
razina učenja	Označava ocjenu i može biti predstavljena formalnom kvalifikacijom. Razine učenja općenito proizlaze iz obrazovnog sustava ili ukazuju na ocjenjivanje u taksonomiji intelektualnih ponašanja ili ponašanja u učenju (kao što su pamćenje, primjena, tumačenje) i imaju odnos s razinama znanja, ali ih treba razlikovati od njih.	EN16234-1:2019 Okvir e-kompetencija (e-KF)

5. REFERENCE

Mandat ENISA-e, Uredba (EU) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

Europski profili profesionalnih uloga u području IKT-a, CWA 16458
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=1799176DA0D15C74D91B71423CAD4A9A3

EN 16234-1:2019 Okvir e-kompetencija (e-CF), Zajednički europski okvir za stručnjake u području IKT-a u svim sektorima

CEN/TS 17699:2022 Smjernice za izradu stručnih kurikuluma IKT-a u skladu s EN 16234-1 (e-CF)

CEN/TS 17834:2022 Europski okvir profesionalne etike za struku IKT-a (EU ICT etika)

Europski kvalifikacijski okvir (EQF)

ESCO Europska višejezična klasifikacija vještina, kompetencija i zanimanja, http://www.ec.europa.eu/esco

IFIP etički kodeks

Životni ciklus odgovora na incidente NIST-a

Nacionalna inicijativa za obrazovanje o kibernetičkoj sigurnosti (NICE) Nacionalnog instituta za standarde i tehnologiju u
SAD-a

Nacionalne strategije kibernetičke sigurnosti (NCSS), https://www.enisa.europa.eu/topics/national-cyber-security-strategije/nacionalne-strategije-kibernetičke sigurnosti-smjernice-alati

Tijelo znanja o kibernetičkoj sigurnosti (CyBOK) Nacionalnog programa za kibernetičku sigurnost Ujedinjenog Kraljevstva i Sveučilišta u Bristolu https://www.cybok.org

JRC, Taksonomija i glosar za kibersigurnost Europske komisije,
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Program vještina za Europu, https://ec.europa.eu/commission/presscorner/detail/en/ip 20 1196

Akcijski plan za digitalno obrazovanje https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education-akcijski_plan

Pakt za vještine, https://ec.europa.eu/commission/presscorner/detail/en/qanda 20 1197

predvodnik u digitalnom desetljeću, https://ec.europa.eu/commission/presscorner/detail/en/qanda 20 1197

ENISA, Forenzička analiza, Analiza web-poslužitelja, Priručnik, Dokument za nastavnike, 2016.,
https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-Resources /EX3 Forenzička analiza III-Priručnik

Vijeće Europe, Elektronički dokazi u građanskim i upravnim postupcima, Smjernice i obrazloženja Memorandum, 2019,https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

A PRILOG: POVEZIVANJE ECSF-A S DRUGE NORME EU-A I OKVIRA

ECSF je okvir za potporu profesionalnom području kibersigurnosti u EU-u. Povezivanje postojećih priznatih europskih struktura od važnosti za profesionalno područje kibersigurnosti EU-a bilo je ključno načelo osmišljavanja ECSF-a (vidjeti odjeljak 2.1.)

U sljedećim odlomcima daje se kratak pregled glavnih standarda i okvira s kojima se ECSF povezuje.

A.1 EN16234-1 E-CF ZAJEDNIČKI EUROPSKI REFERENTNI OKVIR ZA STRUČNJAKE U PODRUČJU IKT-A U SVIM SEKTORIMA

Europska norma (EN) 16234-1 Europski okvir e-kompetencija (e-KF) pruža referencu na 41 kompetenciju koja se primjenjuje na radnom mjestu informacijske i komunikacijske tehnologije (IKT) koristeći standardni europski jezik za kompetencije, vještine, znanje i razine znanja koje se mogu razumjeti u cijeloj Europi. Glavni je cilj ove norme osigurati zajednički europski jezik za kompetencije, vještine, znanje i razine znanja i stručnosti povezane s IKT-om na radnom mjestu kako to zahtijevaju i primjenjuju organizacije i stručnjaci. Na taj način svi dionici u sektoru, uključujući javni i privatni sektor i pojedince, imaju pristup zajedničkoj referenci.

Standard je uspostavljen kao alat za potporu međusobnom razumijevanju i osiguravanje transparentnosti jezika kroz artikulaciju kompetencija koje zahtijevaju i primjenjuju ICT stručnjaci. Ovaj standard je strukturiran u više dimenzija. Dimenzije odražavaju područja planiranja poslovanja i ljudskih resursa te uključuju smjernice za posao i radnu stručnost. Osim toga, ovaj standard dodaje transverzalnu komponentu koja pruža osnovne generičke ICT deskriptore za uspješnu primjenu kompetencija e-CF-a u kontekstu radnog mjesta.

Tablica 4: Pregled EN16234-1 (e-CF). Izvor: CEN 2019.

Dimenzija 1 5 područja e-KF	**Dimenzija 2** Utvrđena je 41 e-kompetencija	**Dimenzija 3** 5 Pružatelj e-kompetencija			Razine	
		E-1	E-2	e<3	E-4	E-5
A. Plan	A.1. Usklađivanje informacijskih sustava i poslovne strategije					
	A.2. Upravljanje razinom usluge					
	A.3. Izrada poslovnog plana					
	A.4. Planiranje proizvoda/usluge					
	A.5. Dizajn arhitekture					
	A.6. Dizajn aplikacije					
	A.7. Praćenje tehnoloških trendova					
	A.8. Upravljanje održivošću					

	A.9. Inovacije
	A.10. Korisničko iskustvo
B. Izgradnja	B.1. Razvoj aplikacija
	B.2. Integracija komponenata
	B.3. Ispitivanje
	B.4. Uvođenje rješenja
	B.5. Izrada dokumentacije
	B.6. Inženjerstvo IKT sustava
C. Trčanje	C.1. Korisnička podrška
	C.2. Podrška za promjenu
	C.3. Pružanje usluga
	C.4. Upravljanje problemima
	C.5. Upravljanje sustavima
E. Omogući	D.1. Razvoj strategije informacijske sigurnosti
	D.2. Razvoj strategije kvalitete IKT-a
	D.3. Obrazovanje i osposobljavanje
	D.4. Kupnja
	D.5. Razvoj prodaje
	D.6. Digitalni marketing
	D.7. Znanost o podacima i analitika
	D.8. Upravljanje ugovorima
	D.9. Razvoj osoblja
	D.10. Upravljanje informacijama i znanjem
	D.11. Utvrđivanje potreba
E. Upravljanje	E.1. Predviđanje razvoja
	E.2. Upravljanje projektima i portfeljem
	E.3. Upravljanje rizicima
	E.4. Upravljanje odnosima
	E.5. Poboljšanje procesa
	E.6. Upravljanje kvalitetom IKT-a
	E.7. Upravljanje poslovnim promjenama
	E.8. Upravljanje informacijskom sigurnošću
	E.9. Upravljanje informacijskim sustavima

ENISA

E-KF pruža dosljedne veze u kontekstu kvalifikacija IKT-a i drugih okvira relevantnih za sektor (posebno EQF, DigComp, europski profili profesionalnih uloga u području IKT-a, bihevioralne vještine, ESCO, EQANIE, SFIA, temeljni korpus znanja za struku u području IKT-a, ISO i drugi standardi industrije IKT-a).

Za svaku ulogu u području kibersigurnosti odabran je skup primjenjivih kompetencija za e-KF na razini aplikacije kao ugrađeni element opisa profila za ulogu stručnjaka za kibersigurnost.

A.2. EUROPSKI PROFESIONALNI PROFILI ULOGA U IKT-U

CWA 16458 Europski ICT profesionalni profili uloga pruža generički skup tipičnih uloga koje obavljaju ICT stručnjaci u bilo kojoj organizaciji, pokrivajući cijeli ICT poslovni proces. Ukupno trideset profila pruža dobro polazište i inspiraciju za stvaranje kontekstno specifičnijih i fleksibilnijih profila na temelju organizacijskih uloga, pojedinačnih opisa poslova ili specijalizacija poddomena iz različitih konteksta. Primjenom kompetencija za e-KF na izradu profila IKT-a, europski profili profesionalnih uloga u području IKT-a također pružaju alat i ulaznu točku za primjenu e-KF-a pojedincima i organizacijama koji žele raditi s e-KF-om.

Europski profili profesionalnih uloga u području IKT-a opisani su u dosljednom formatu koji uključuje sljedeće elemente: sažetu izjavu, izjavu o misiji, rezultate, glavne zadaće, e-kompetencije i područja ključnih pokazatelja uspješnosti (KPI[13]).

Donošenjem najprikladnijih elemenata europske dogovorene i praktične sheme opisa profila IKT-a profili ECSF-a postaju usporedivi i pružaju jedinstven, lako dostupan i sveobuhvatan pregled zahtjeva za europske stručnjake u području kibersigurnosti.

Ti detaljni profili visokog sadržaja imaju labave veze s generičkim ulogama uključenima u cjelokupni skup europskih profesionalnih profila u području IKT-a. Iz perspektive korisnika ECSF-a, povjerenje u održivost strukture može se uspostaviti njezinom povezanošću s europskim ICT profilima, ali uz usmjerenu primjenu na zajednicu kibersigurnosti.

A.3. EUROPSKI KVALIFIKACIJSKI OKVIR

EU je razvio **Europski kvalifikacijski okvir (EQF)** kao alat za prevođenje kako bi nacionalne kvalifikacije učinili razumljivijima i usporedivijima. Europskim kvalifikacijskim okvirom nastoji se poduprijeti prekogranična mobilnost učenika i radnika te promicati cjeloživotno učenje i profesionalni razvoj diljem Europe.

Europski kvalifikacijski okvir je na 8 razina koji se temelji na ishodima učenja[14] za sve vrste kvalifikacija. Služi kao alat za prevođenje između različitih okvira nacionalnih kvalifikacija. Taj okvir pomaže u poboljšanju transparentnosti, usporedivosti i prenosivosti kvalifikacija ljudi te omogućuje usporedbu kvalifikacija iz različitih zemalja i institucija.

Europskim kvalifikacijskim okvirom obuhvaćene su sve vrste i sve razine kvalifikacija, a upotrebom ishoda učenja jasno je što osoba zna, razumije i što je sposobna učiniti. Razina se povećava ovisno o razini učenja, pri čemu je razina 1 najniža, a 8 najviša razina. Ono što je najvažnije, europski kvalifikacijski okvir usko je povezan s nacionalnim kvalifikacijskim okvirima[15], pa pruža sveobuhvatnu kartu svih vrsta i razina kvalifikacija u Europi, koje su sve dostupnije putem baza podataka o kvalifikacijama. Europski kvalifikacijski okvir uspostavljen je 2008., a kasnije je revidiran 2017[16].

Profili ECSF-a sadržavaju kompetencije e-KF i dodjele na razini e-KF-a, što osigurava dosljednu vezu s razinama EQF-a (vidjeti odjeljak 3.2.). Ovaj orijentacijski odnos pruža most u razumijevanju između pružanja programa učenja i zahtjeva na radnom mjestu.

A.4 ESCO – EUROPSKA KLASIFIKACIJA VJEŠTINA, KOMPETENCIJA I ZANIMANJA

ESCO je višejezična klasifikacija europskih vještina, kompetencija, kvalifikacija i zanimanja. Ključna je svrha ESCO-a osigurati rječnik u kojem se opisuju, identificiraju i klasificiraju profesionalna zanimanja i vještine relevantne za tržište rada, obrazovanje i osposobljavanje EU-a te sustavno prikazuju odnosi između tih zanimanja i vještina. ESCO-om upravlja Europska komisija, koja je odgovorna za ažuriranje klasifikacije. Resursom ESCO-a podupiru se dvije ključne strategije EU-a u tom području, Europa 2020. i Program vještina za Europu[17].

[13] CWA 16458 Europski profili profesionalnih uloga u području IKT-a
[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=HR
[17] https://ec.europa.eu/social/main.jsp?catId=1326&langId=en

Cilj ESCO-a je opisati sva zanimanja na europskom tržištu rada, pa tako i kibernetičku sigurnost. Stoga je korisno uspostaviti orijentacijsko mapiranje između profila uloga ECSF-a i nekih profila ESCO-a.

U tablici 5. navedeno je nekoliko zanimanja ESCO-a povezanih s kibersigurnošću zajedno s indikativnim mapiranjem profila uloga ECSF-a. Budući da odnos između njih nije uvijek jedan-na-jedan, definirani su sljedeći odnosi kako bi se objasnile odgovarajuće veze:

- **je -** Ovo zanimanje ESCO-a može se mapirati u odgovarajući profil uloge ECSF-a jer oba opisuju istu ulogu u kibernetičkoj sigurnosti.
- **može uključivati** - Ovo zanimanje ESCO-a može uključivati, ovisno o kontekstu, navedeni profil uloge ECSF-a. (Ovo je indikativno mapiranje.)
- **mogu biti uključeni** - Neki aspekti ovog ESCO zanimanja mogu opisati navedene dijelove profila uloge ECSF-a. (Ovo je indikativno mapiranje.)

Tablica 5.: Odnosi profila ESCO-a i profila ECSF-a

ESCO oznaka	ESCO zanimanje	Odnos	Profil uloge ECSF-a
2149.2.8	Istraživački inženjer	može uključivati	Istraživač kibernetičke sigurnosti
2310.1	Predavač visokog obrazovanja	može uključivati	Edukator za kibernetičku sigurnost
2356	Trener informacijske tehnologije	može uključivati	Edukator za kibernetičku sigurnost
2511.18	IT revizor	može uključivati	Revizor kibernetičke sigurnosti
2519.2	Voditelj ICT revizora	može uključivati	Revizor kibernetičke sigurnosti
2529.1	Glavni službenik za ICT	je	Glavni službenik za informacijsku sigurnost
2529.2	Stručnjak za digitalnu forenziku	je	Istražitelj digitalne forenzike
2529.3	Inženjer sigurnosti ugrađenih sustava	mogu biti uključeni	Implementator kibernetičke sigurnosti
2529.4	Etički haker	je	Ispitivač penetracije
2529.6	Administrator ICT sigurnosti	mogu biti uključeni	Implementator kibernetičke sigurnosti
2529.7	Inženjer ICT sigurnosti	mogu biti uključeni	Arhitekt kibernetičke sigurnosti
2529.7	Inženjer ICT sigurnosti	mogu biti uključeni	Implementator kibernetičke sigurnosti
2619.4	Službenik za zaštitu podataka	je	Službenik za kibernetičko pravo, politiku i

Važna napomena: Odnos između zanimanja ESCO-a i profila uloge ECSF-a ne predstavlja ekvivalentnost; on nudi najprikladniju aproksimaciju koju bi čitatelji mogli htjeti istražiti.

B PRILOG: SLUČAJEVI UPOTREBE

Slučaj upotrebe pokazuje zašto i kako organizacija koristi ECSF, naglašavajući raznolikost pristupa i prednosti. Ovaj je prilog zbirka predmeta koji su bili javno dostupni 20. srpnja 2022.

Sljedeći slučajevi upotrebe samo su ilustrativni primjeri. Informacije i sadržaj uključeni u te slučajeve ne bi se trebali smatrati izjavom ENISA-e o odobrenju ili potvrđivanju. Korištenje ovih primjera treba promatrati kao inspirativne slučajeve, a ne kao uvjetovanje polaznih vrijednosti ili referentnih referenci.

8.1 SLUČAJ UPOTREBE IZ PROJEKTA CONCORDIA H2020

Ovaj odjeljak uključuje dijelove iz slučaja upotrebe koji je napisao projekt CONCORDIA H2020[18].

Ususret integriranoj platformi za vještine u području kibersigurnosti koja se temelji na europskom okviru za vještine u području kibersigurnosti

Teško je razumjeti veliku sliku treninga

Potrebe za zaštitom od prijetnji informacijama i operacijama, održavanjem kibernetičke sigurnosti organizacije i povećanjem otpornosti na takve prijetnje još uvijek hitno osjećaju sve zainteresirane strane. Ključna komponenta za ispunjavanje ovih potreba je postojanje cyber - kompetentnih stručnjaka. A kompetencija u vezi s kibernetičkom sigurnošću nije potrebna samo predanim stručnjacima (vanjskim ili unutarnjim u organizaciji), već i svim članovima osoblja organizacije, čak i ako nisu izravno uključeni u procese i aktivnosti kibernetičke sigurnosti.

Kada je riječ o stručnjacima za kibernetičku sigurnost, razne publikacije još uvijek izvještavaju o nedostatku vještina u području kibernetičke sigurnosti, ističući da se 3 glavne kompetencije koje nedostaju ili nisu dovoljno pokrivene od postojećih stručnjaka razlikuju od godine do godine[19]. S druge strane, razne europske i međunarodne organizacije nude znatan broj tečajeva i osposobljavanja povezanih s kibersigurnošću. Jednostavnim pretraživanjem na internetu otkrit će se mnogi tečajevi koji se odnose na područje kibernetičke sigurnosti, a da se ne pruži jasna slika o ponuđenim kompetencijama ili kako bi se one mogle povezati s određenom ulogom. Da bi se dodala ova zbrka, postoje tečajevi za koje se čini da se bave jednom specifičnom ulogom (npr. CISO), imaju slične nazive, ali imaju drugačiji kurikulum.

Stoga u nekoliko slučajeva pružene informacije zbunjuju polaznika o tome što i kako bi trebao percipirati koncepte kibersigurnosti, kao i kako ih koristiti za pokrivanje svojih profesionalnih potreba. Osim toga, tečajevi za stručnjake promoviraju se na različitim platformama i teško ih je usporediti s obzirom na pokrivene kompetencije i profil uloga koje se obrađuju. To pojedincu otežava izgradnju jasnog puta u karijeri i prepoznavanje prilika za razvoj.

CONCORDIA karta tečajeva za stručnjake za kibernetičku sigurnost

U pokušaju rješavanja ovih izazova, izradili smo CONCORDIA kartu tečajeva i treninga za stručnjake za kibernetičku sigurnost[20]. Karta prikazuje strukturirane informacije o postojećoj europskoj ponudi kratkih tečajeva/osposobljavanja i pruža različite filtre kako bi se ponudom lakše uskladila posebna potreba za razvojem vještina. [...]

Tečajevi se mogu razvrstati na temelju razine kibernetičke sigurnosti (uređaj, mreža, softver/sustav,

[18] https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-european-okvir_vještina kibernetičke sigurnosti/
[19] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-istraživanje-pokazuje-poteškoće-zadržavanja-u-godinama
[20] https://www.concordia-h2020.eu/map-courses-cyber-professionals/

podaci/aplikacija, usmjerenost na korisnika) ili relevantnosti za industrijski sektor (npr. telekomunikacije, financije, prometna e-mobilnost, e-zdravstvo ili obrana), ali i prema formatu (licem u lice, online, kombinirano) i vremenu tečaja/osposobljavanja.

Nedostaje ključni sastojak - rješenje koje omogućuje ECSF

Iako na karti CONCORDIA nudimo veliko mnoštvo filtara kako bismo korisnicima pomogli da lakše prepoznaju tečaj(e) koji ih zanimaju, bazi podataka nedostaje ključni sastojak - poveznice na profile uloga kojima se svaki od tečajeva bavi kroz obrađena znanja i vještine. Europski okvir kompetencija za stručnjake u području IKT-a dostupan u trenutku izrade karte definira 30 profila uloga i 40 povezanih kompetencija, ali ih je teško povezati sa specifičnostima područja kibersigurnosti.

To je bio izazov obrazovnog ekosustava za kibernetičku sigurnost koji smo označili već prije dvije godine i zabilježili u CONCORDIA Roadmap for Education[21] pod naslovom C5: Heterogenost terminologije vezane uz kompetencije. Nedostatak međudomenske i međusektorske dogovorene terminologije povezane s vještinama kibersigurnosti potrebnima za određenu ulogu otežava poduzećima popunjavanje otvorenih radnih mjesta. Teško im je uskladiti kriterije za zapošljavanje sa studijima i kvalifikacijama navedenima u životopisima kandidata zbog upotrebe nestandardne terminologije. Pojedinci, pak, ne mogu lako identificirati vještine koje trebaju posjedovati ili razviti kako bi zadovoljili potražnju na tržištu. I, konačno, pružatelji tečajeva imaju poteškoća u osmišljavanju nastavnih planova i programa koji odgovaraju potrebama tržišta.

Kao dio CONCORDIA plana, obvezali smo se na jednu platformu koja će ugostiti sve postojeće programe povezane s kibernetičkom sigurnošću (sveučilišna razina i doktorski programi, kratki tečajevi i treninzi za profesionalce). [...]

Platforma bi trebala razmotriti prikupljanje sadržaja upotrebom kategorija koje se temelje na standardnoj terminologiji (uključujući poseban okvir vještina). Kategorije bi se dalje koristile kao filtri za različite upite baze podataka tečajeva. Čini se da je 12 profila uloga definiranih u trenutačnoj verziji Europskog okvira za vještine u području kibersigurnosti (ECSF) prirodno rješenje.

Korist za dionike

Usvajanje standardnog leksikona kao što je onaj koji je predložio ESCF, uključujući profile uloga u kibersigurnosti, pomoći će poduzećima da identificiraju prave talente za radna mjesta, kao i pružateljima obrazovnih usluga da bolje oblikuju svoj kurikulum kako bi odgovarao potrebama radne snage u području kibersigurnosti. Primjenom iste terminologije i upotrebom okvira vještina na razini EU-a na opise poslova, opis tečaja i profil uloga pomoglo bi pojedincima da odaberu prave obrazovne module za potporu svojoj karijeri i bolje filtriraju otvorena radna mjesta u skladu s njihovim kompetencijama i razinom stručnosti. Naposljetku, kreatori politika mogli bi prikupljati strukturiranije podatke na državnoj/regionalnoj razini kao potporu budućem razvoju politika i imati čvrstu osnovu u koordinaciji s vanjskim zemljama u cilju rješavanja globalnih izazova kibernetičke sigurnosti.

Ususret integriranoj platformi za vještine

Nadovezujući se na bazu podataka CONCORDIA s tečajevima i osposobljavanjem za stručnjake za kibersigurnost, projekt REWIRE[22] pokušava poduzeti daljnje korake prema integraciji relevantnog sadržaja povezanog s vještinama u području kibersigurnosti. Platforma REWIRE CyberABILITY, koja je trenutačno u fazi dizajna, pružit će ažurirane informacije o tržištu rada, kompetencijama, tečajevima osposobljavanja, programima certificiranja i planu karijere.

8.2 SLUČAJ UPOTREBE IZ PROJEKTA SPARTA H2020

Ovaj odjeljak uključuje dijelove iz slučaja upotrebe koji je napisao projekt SPARTA H2020[23].

Unaprjeđenje visokog obrazovanja korištenjem ECSF-a i SPARTA Curriculumricula Designera

[21] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf
[22] https://rewireproject.eu/
[23] https://sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula%20Designer.pdf

Uvod

Ovaj slučaj upotrebe daje preporuke o tome kako se ECSF može koristiti za oblikovanje obrazovnih programa koji su povezani s kibersigurnošću. Budući da ECSF manifestira strukturu profila na visokoj razini sa stajališta praktičara, uključujući glavne zadatke, relevantna znanja i vještine, to može pružiti fokusiraniji pristup za izgradnju specijaliziranih i sveobuhvatnih studijskih programa, prilagođenih specifičnim profilima, umjesto pokrivanja kibernetičke sigurnosti općenito.

Izazov

Obrazovne ustanove sastavljaju svoje kurikulume uzimajući u obzir cijeli put - počevši od temeljnih tečajeva koji su potrebni za učenje učenika kao osnova za sljedeći skup naknadnih tečajeva, koji su često specifični za kibernetičku sigurnost. Međutim, odabir tečajeva koji će biti uključeni u nastavne planove i programe kibernetičke sigurnosti ovisi o instituciji.

Svaka obrazovna ustanova ima svoje specifično okruženje (određeno npr. infrastrukturom, opremom, stručnošću nastavnika, sastavom postojećih programa itd.) i ne postoji univerzalni način na koji bi kurikulum trebao biti konstruiran.

Pružatelji obrazovanja razlikuju se u tome na koju bi se konkretnu poddomenu kibernetičke sigurnosti željeli usredotočiti. Neki pružatelji usluga su vrlo tehnički, usredotočujući se na, npr. informatiku, neki više društveno orijentirani, usredotočujući se na pravne i društvene aspekte. Stoga je interoperabilnost između rezultirajućih studijskih programa i zajedničkog jezika trenutno značajan izazov.

Neki akademski programi ne izgrađuju vještine i kompetencije koje pripremaju studente za specifične radne uloge dostupne na tržištu rada. To predstavlja izazov za studente koji ne razumiju koje su mogućnosti zanimanja na kraju studija.

Rješenje koje omogućuje ECSF

ECSF može doprinijeti sljedećim aktivnostima kojima se rješavaju prethodno navedeni izazovi:

- Evaluacija: Opis profila omogućuje institucijama da preispitaju svoje kurikulume na strukturiran i sustavan način, razumijevajući stajalište stručnjaka. To omogućuje razumijevanje za koji profil institucija uglavnom cilja na svoje diplomante.

- Poboljšanje: Može se učiniti na temelju evaluacije. To je posebno važno s obzirom na skup znanja/vještina koje se pripisuju određenom profilu.
- Fokus: Obrazovanje koje pružaju sveučilišta može se razlikovati u načinu na koji se bave temeljnim kompetencijama. Neki bi mogli biti više usredotočeni na određene tehnološke tečajeve, neki na pravo, drugi na forenziku itd. Imajući ECSF s kojim mogu raditi, mogu mapirati svoje temeljne kompetencije na različita područja tečajeva, važna za definirane profile. To omogućuje instituciji da razvije učinkovitije ciljane programe oko glavnih kompetencija.
- Suradnja: ECSF pružateljima obrazovanja daje zajednički jezik i vokabular za opisivanje njihovih kolegija, stvaranje zajedničkih programa i omogućavanje mobilnosti studenata.

Pri primjeni ECSF-a na obrazovanje o kibernetičkoj sigurnosti preporučuje se sljedeći pristup:

- Tečajevi u nastavnim planovima i programima mogu se klasificirati kao pripadnici kategorija Temeljna ili Kibernetička sigurnost. Temeljni tečajevi su oni koji možda nisu izravno povezani s ECSF-om, ali služe kao preduvjet za kasnije studije. Na primjer, temeljna kriptologija preduvjet je za kriptoanalizu ili naprednu kriptologiju; Teorija brojeva neophodna je za većinu srednjih i naprednih računalnih tečajeva.
- Nakon što se identificiraju temeljni tečajevi, mogu se predložiti tečajevi kibernetičke sigurnosti kako bi se odgovorilo na zahtjeve radnih uloga kojima studenti teže. Povezivanje se ostvaruje na temelju sadržaja pojedinih kolegija, koji se mogu povezati s profilima i na kraju s radnim ulogama. Konkretni koraci, [...], su:
    a. Za određenu radnu ulogu 1 pružatelji obrazovnih usluga pronalaze relevantne profile (profil 1 i profil 12 u našem primjeru). Ovo mapiranje, označeno smeđim strelicama, trebali bi odrediti oglašivači posla/poslodavci.
    b. Pružatelji obrazovnih usluga identificiraju potrebna znanja i vještine za odabrane profile. Ti su zahtjevi definirani ECSF-om, označeni plavim strelicama.

c. Pružatelji obrazovnih usluga osmišljavaju nove ili ponovno upotrebljavaju postojeće tečajeve (u našem primjeru tečajeva 1,2, 3, 4) koji se bave znanjem i vještinama navedenim u gornjem koraku. Ovo mapiranje između tečajeva i njihovog sadržaja moraju napraviti administratori tečaja.
d. Imajući sve potrebne tečajeve (i sve preduvjete za njih, opće tečajeve koji nisu kibernetička sigurnost, druge tečajeve za proširenje opsega studenata itd.), jezgra kurikuluma je spremna.

• Naravno, ECSF se može primijeniti i na potpuno suprotan način: prvo sastavljanje kurikuluma iz pojedinačnih kolegija, analiza pruženih znanja i vještina, korištenje ECSF-a za utvrđivanje profila i, konačno, pronalaženje radnih uloga koje su podržane kurikulumom. Ovo mapiranje otkriva koja su točna znanja i vještine već prisutne u nastavnim planovima i programima ili, s druge strane, što nedostaje i što treba naglasiti ili dodati kolegijima. Na taj način ECSF pomaže u strukturiranju kurikuluma kako bi se bolje uklopili u očekivane profile i radne uloge.

Rezultat / dodana vrijednost tvrtke SPARTA

Projekt SPARTA koristio je okvir vještina kibernetičke sigurnosti za stvaranje besplatnog alata pod nazivom Cybersecurity Curricula Designer. To je jednostavna web aplikacija koja pomaže pružateljima obrazovnih usluga u stvaranju novih studijskih programa o kibernetičkoj sigurnosti i/ili analizi postojećih studijskih programa prema njihovom sadržaju i njegovom odrazu zahtjeva za poslovima kibernetičke sigurnosti.

Alat [...] omogućuje administratorima studijskih programa da sastave svoj studijski program povlačenjem i ispuštanjem predmeta iz lijevog u srednji dio. Tečajevi, od kojih Administratori razvijaju studijske programe, mogu biti unaprijed definirani ili prilagođeni. Prilikom sastavljanja studijskog programa, statistički podaci o njegovom sadržaju prikazani su u desnom odjeljku. Osim ostalih podataka, pružaju se informacije o tome koje kompetencije i radne uloge podržava program. Korištenjem alata lako je saznati koji sadržaj nedostaje u studijskom programu i koje su konkretne radne uloge najprikladnije za diplomante programa. U ovom slučaju, okvir za vještine kibersigurnosti jezgra je aplikacija koja omogućuje povezivanje vještina i znanja s radnim ulogama. [...]

8.3 SLUČAJ UPOTREBE IZ INCIBEA

Ovaj odjeljak uključuje dijelove iz slučaja upotrebe koji je napisao INCIBE.[24]

Slučaj upotrebe iz INCIBE-a

Uvod

Učinkovitost u zaštiti zemlje uvelike ovisi o sposobnostima njezinih ljudi, a procjenjuje se da bi do 2022. godine Španjolska mogla dostići radnu snagu u području kibernetičke sigurnosti od blizu 122.284 radnika s nedostatkom talenata koji se procjenjuje na 24.119. Posljedično, jedan od glavnih prioriteta današnje administracije je suočavanje s izazovom prepoznavanja, privlačenja, razvoja i zadržavanja talenata u različitim područjima kibernetičke sigurnosti.

Dokaz ove predanosti je razvoj Nacionalne strategije kibernetičke sigurnosti španjolske vlade za 2019[25]., koja naglašava potrebu ne samo za obrambenim i zaštitnim položajem za tvrtke i građane, već i za podrškom jačanju kibernetičke industrije, prepoznajući ključnu ulogu koju kibernetička sigurnost igra u trenutnom okruženju transformacije i neizvjesnosti te priliku koju nudi za povećanje konkurentnosti Španjolske. U skladu s ciljem 4. strategije, u 5. akcijskom smjeru naglašava se važnost jačanja španjolske industrije kibersigurnosti, uz stvaranje i zadržavanje talenata za jačanje digitalne autonomije.

S druge strane, Planom za digitalnu Španjolsku 2025[26] . nastoje se ojačati poluge koje će olakšati povratak na put gospodarskog rasta, a jedna je od njegovih strateških osi jačanje kapaciteta Španjolske za kibersigurnost kako bi se ublažili rizici i povećalo povjerenje u put prema digitalnom i održivom gospodarstvu.

U svojoj strateškoj osi 4, koja je monografski posvećena kibersigurnosti, uključuje mjere koje čine tri glavna smjera djelovanja INCIBE-a u nadolazećim godinama: povećanje kapaciteta građana i poduzeća u području kibersigurnosti; jačanje španjolskog ekosustava kibersigurnosti oko svoje industrije, istraživanja, razvoja i inovacija te talenata za kibersigurnost; i konsolidaciju Španjolske kao međunarodnog čvorišta u sektoru. Spain Digital 2025 već prepoznaje ključnu ulogu talenata za kibernetičku sigurnost kao pokretačke snage sektora.

[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 España Digital 2025.aspx

Ove nacionalne inicijative generiraju prikladan scenarij koji favorizira istraživanje, inovacije i uključuje najrelevantnije agente lanca vrijednosti, kao što su obrazovne institucije i organizacije, kako bi vidjeli korist od upravljanja znanjem, sposobnostima i tehnološkim iskustvima koja odgovaraju na velike izazove s kojima se zemlja suočava u pogledu kibernetičke sigurnosti.

Sa svoje strane, španjolski Nacionalni institut za kibernetičku sigurnost (INCIBE), tvrtka pod Ministarstvom gospodarstva i digitalne transformacije, putem državnog tajnika za digitalizaciju i umjetnu inteligenciju; a referentni subjekt za razvoj kibersigurnosti i digitalnog povjerenja građana i poduzeća te španjolske akademske i istraživačke mreže (RedIRIS) ima misiju poboljšanja kibersigurnosti i digitalnog povjerenja građana, maloljetnika i privatnih poduzeća u Španjolskoj.

Osim toga, njegova misija uključuje zaštitu i obranu ovih skupina, promicanje španjolske industrije i istraživanja, razvoja i inovacija u kibernetičkoj sigurnosti, kao i identifikaciju, stvaranje i privlačenje talenata u sektor kibernetičke sigurnosti.

Talent za kibernetičku sigurnost stoga je kamen temeljac djelovanja INCIBE-a. Bez talenta nemoguće je razviti snažnu industriju ili rješenja s visokom dodanom vrijednošću koja su potrebna za sudjelovanje na visoko konkurentnom tržištu kao što je kibersigurnost.

Međutim, dosad dostupne informacije o stanju talenata u sektoru kibersigurnosti u Španjolskoj bile su raznolike i rascjepkane, a dolazile su iz različitih izvora, što je otežalo duboko razumijevanje okruženja potrebnog za usmjeravanje djelovanja. [...]

Zbog toga, s ciljem pružanja jasne vizije talenata za kibernetičku sigurnost u Španjolskoj, INCIBE u ožujku 2022. objavljuje rezultate analize i dijagnoze talenata za kibernetičku sigurnost na nacionalnoj razini, čiji je proces proveden kroz rigorozne analitičke premise, globalni pristup radu te participativne i uključive procese koji su uzeli u obzir glavne aktere ekosustava kibersigurnosti. [...]

Izazov

Preporuke proizašle iz ovog projekta analize polazište su za osiguravanje robusne i profitabilne industrije kibernetičke sigurnosti koju karakterizira stavljanje talenta ljudi u središte inicijativa. U tom smislu, cijeli lanac vrijednosti kibernetičke sigurnosti može vidjeti ovu studiju kao priliku za daljnje povezivanje i bolje razumijevanje talenata za kibernetičku sigurnost u Španjolskoj.

Stoga je potrebno strukturirati i implementirati učinkovite prakse koje utječu na upravljanje ovom specifičnom vrstom talenata u organizacijama. Važnost kibernetičke sigurnosti za opstanak organizacija zahtijeva potrebu za rješavanjem problema identificiranja ove vrste specifičnih talenata u kibernetičkoj sigurnosti, evolucijom procesa zapošljavanja i ukrcavanja, kao i usvajanjem radnji koje doprinose poboljšanju upravljanja i ublažavanju odljeva talenata.

Iz tog razloga, promicanje nacionalnih politika, koordiniranih od strane uprave koje se usredotočuju na jačanje i promicanje inicijativa kako bi kibernetička sigurnost postala strateški prioritet u organizacijama, kao i strukturiranje i strukturiranje itinerara obuke za obavljanje kibernetičke sigurnosti kao profesionalne djelatnosti prioriteti su na kojima će se uspostaviti i organizacije i tvrtke za zapošljavanje u svojim akcijama za identifikaciju, privlačenje, zapošljavanje i upravljanje talentima za kibersigurnost.

Na taj se način utvrđuje niz preporuka koje bi ova vrsta agenata (javna uprava, tvrtke za zapošljavanje i druge organizacije) mogla implementirati kako bi povećala talente za kibernetičku sigurnost u Španjolskoj i koje postavljaju polazište za rješavanje izazova koji su pred nama u tom pogledu. [...]

Rješenje koje omogućuje ECSF

Postoji nekoliko čimbenika (politički, gospodarski, društveni, tehnološki, pravni itd.) koji mogu utjecati na industriju kibernetičke sigurnosti, a posljedično i na nedostatak talenata, jaz i općenito neusklađenost između ponude i potražnje.

Jedan od tih relevantnih čimbenika u Europskoj uniji je nedostatak standardizacije definicije uloga i vještina kibernetičke sigurnosti povezanih s tim ulogama.

Osigurati osnovu za kontinuiranu komunikaciju između različitih dionika (vlade, industrije, akademske zajednice, kreatora politika i građana).

Ova vrsta alata služi kao osnova za kompetentniju i potpuniju radnu snagu koja razumije isti jezik kao i drugi stručnjaci na europskoj razini. [...]

Rezultat / dodana vrijednost

Stoga su, u predstavljenom kontekstu, na nacionalnoj razini pokrenute dvije inicijative koje će dati vrijednost ECSF-u koji je razvila ENISA-a i koje će biti vrlo korisne. [...]

Obje inicijative, međusobno koordinirane, uključivat će ECSF kao homogen okvir za definiranje profila kibersigurnosti, što će Španjolskoj omogućiti da ostvari svoje ciljeve u pogledu talenata i uskladi se s ostalim zemljama na europskoj razini. [...]

8.4 SLUČAJ UPOTREBE IZ EUROPSKE KIBERNETIČKE SIGURNOSTI ORGANIZACIJA (ECSO)

Ovaj odjeljak uključuje dijelove slučaja upotrebe koji je napisala Europska organizacija za kibernetičku sigurnost (ECSO).[27]

Prema usklađenom obrazovnom pristupu s Europskim okvirom za vještine u području kibersigurnosti (ECSF)

Nakon što je od 2016. radio na obrazovanju, osposobljavanju i vještinama u svojoj WG5, ECSO je iz prve ruke vidio izazove koje predstavljaju fragmentacija i raspršeni pristupi koji danas postoje u kibernetičkoj sigurnosti. U ovom postu na blogu ECSO se osvrće na postojeće europske pristupe obrazovanju i usavršavanju te se usredotočuje na ENISA-in Europski okvir za vještine u području kibersigurnosti (ECSF).

Obrazovanje nije samo nacionalni prerogativ. Također je neodvojivo povezan sa suradnjom između nacionalnih subjekata, šire zajednice za kibersigurnost i europskih tijela. Imajući to na umu, suradnja je ključna pri osmišljavanju paneuropskih pristupa usklađivanju obrazovnih kurikuluma o kibersigurnosti i rješavanju problema vještina ili, konkretnije, nedostatka radne snage. Postoji dovoljno prilika da se iskoristi suradnički duh europske zajednice za kibersigurnost kako bi se pronašla praktična rješenja i inicijative koje mogu imati učinak "na terenu", a ENISA-in Europski okvir za vještine u području kibersigurnosti (ECSF) može imati veliku ulogu u tom pogledu.

Obrazovanje o kibernetičkoj sigurnosti: perspektiva ECSO-a

Iz perspektive Europske organizacije za kibersigurnost (ECSO), kao predstavničkog tijela europskog javno-privatnog ekosustava i zajednice u području kibersigurnosti, potencijal

vrijednost ECSF-a nije zanemariva kada je riječ o povezivanju postojećih napora, pružanju temeljnih elemenata za europsku radnu snagu u području kibersigurnosti te uspostavi zajedničkog okvira i taksonomije za primjenu profila i vještina. Stručnjaci za kibersigurnost, pružatelji obrazovanja i osposobljavanja, tvorci politika i stručnjaci za zapošljavanje mogu imati koristi od šire provedbe ECSF-a.

Izazov

Očito je da postoji sve veća potreba za kvalificiranom radnom snagom za kibernetičku sigurnost. Razne studije diljem svijeta iz industrije i akademske zajednice potvrđuju da je potražnja za radnom snagom za kibernetičkom sigurnosnošću vrlo velika i da je teško zaposliti kompetentne stručnjake. U izdanju godišnje studije radne snage u području kibersigurnosti iz 2021. koju je objavio član ECSO-a (ISC)[228] navodi se da je manjak stručnjaka za kibersigurnost na globalnoj razini 2,72 milijuna, što je, iako se smanjilo s 3,12 milijuna godinu ranije, još uvijek

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

značajan broj. Iako te studije pružaju osnovu za procjenu globalne situacije, stvarnost je da je vrlo teško kvantificirati opseg nedostatka talenata u području kibersigurnosti u Europi. Znamo da će potražnja za stručnjacima neizbježno porasti zbog rasta tržišta kibernetičke sigurnosti i regulatornog okruženja, ostavljajući hitnu prazninu koju treba popuniti s više (i različitih vrsta) stručnjaka. [...]

Ali nije stvar samo u brojkama. Kroz nedavnu studiju ECSO-a o praksama i trendovima zapošljavanja ljudskih resursa, ECSO je također primijetio povećanje vremena koje je organizacijama u prosjeku potrebno da popune svoja radna mjesta u području kibernetičke sigurnosti. Mnoge organizacije navode da proces zapošljavanja može potrajati i do šest mjeseci, što je sporije nego u domenama znanja, dok druge navode da imaju poteškoća s popunjavanjem svojih radnih mjesta u području kibernetičke sigurnosti. To jasno ukazuje na to da postoji neusklađenost između ponude i potražnje (tj. jaz između akademske zajednice i zahtjeva industrije) i čimbenika poticanja/privlačenja (tj. prikladnost i procjena kandidata, privlačnost za radna mjesta i beneficije). Međutim, glavni problem za poslodavce ostaje opći nedostatak stručnjaka za kibernetičku sigurnost u cijelom svijetu, dok potražnja stalno raste. Nekoliko organizacija također naglašava složenost zapošljavanja stručnjaka za domenu koju ne savladavaju. Istraživanje ECSO-a također je pokazalo da, kao rastući trend, nekoliko kandidata, unatoč nedostatku značajnih vještina u području kibersigurnosti, i dalje obogaćuje svoj životopis konceptima i ključnim riječima u području kibersigurnosti.

Ovi izazovi jasno naglašavaju potrebu za zajedničkim jezikom za potporu naporima zapošljavanja i važnost razmatranja multidisciplinarne prirode kibersigurnosti koja je toliko jedinstvena za to područje u odnosu na tradicionalnija IT/ICT zanimanja. Dok postojeći okviri kao što su NICE, CyBoK i eCF pružaju korisne smjernice za razvoj vještina, nedostaje europski okvir koji pruža sveobuhvatnu taksonomiju profila i karijerne putove svojstvene kibersigurnosti. Objavljivanje ECSF-a stoga je vrlo pravodobno i ključno za potporu europskoj zajednici za kibersigurnost u privlačenju, stjecanju vještina i prekvalifikaciji stručnjaka.

Postoji rješenje

ECSO će primjenjivati ECSF na više načina kako bi potaknuo njegovu primjenu i iskoristio njegov potencijal za usklađivanje obrazovanja i vještina u području kibersigurnosti diljem Europe.

ECSO će:

- Mapirati svoj minimalni referentni kurikulum ECSF-u, dajući dizajnerima tečajeva i praktičarima uvid iz prve ruke kako najbolje definirati svoje kurikulume prema namjenskim karijernim putevima. To će pomoći osigurati da sveučilišni tečajevi na odgovarajući način odražavaju stvarnost potreba tržišta rada u području kibersigurnosti, a istovremeno će omogućiti kontinuirano ažuriranje kurikuluma.

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

- Koristite ECSF i priručnik za povezanu upotrebu za podršku ljudskim resursima/zapošljavanju u sastavljanju oglasa za posao i organizaciji postupaka procjene/evaluacije praktičnih vještina. Provest ćemo i naknadnu anketu o ljudskim resursima koristeći profile poslova ECSF-a kako bismo razumjeli koje su uloge najpotrebnije organizacijama i postupno izgradili kvantitativno razumijevanje europskog
- tržišta rada u području kibersigurnosti.
  Koristite ECSF kao osnovnu taksonomiju za dvije namjenske platforme koje su predvidjeli Women4Cyber Foundation i ECSO [...]

Rezultat i dodana vrijednost

Dodana vrijednost ECSF-a za europsku zajednicu za kibersigurnost jest u prvom redu imati zajednički okvir i taksonomiju na kojima će se raditi. To će dovesti do boljeg razumijevanja potreba za vještinama i praktične stvarnosti različitih profila radnih mjesta, čime će se poboljšati radna snaga u području kibersigurnosti, ne samo učinkovitijim mjerama zapošljavanja i zadržavanja, već i olakšavanjem ulaska ili ponovnog ulaska većeg broja žena i drugih nedovoljno zastupljenih skupina (tj. neuroraznolikih) u to područje. ECSF će isticanjem tehničkih i netehničkih aspekata različitih profila pridonijeti uklanjanju zablude da je kibersigurnost samo tehnička tema, a istovremeno se radi o ljudima i procesima. U tom će pogledu naglašavanje važnosti mekih (prenosivih) vještina u tom području znatno pridonijeti privlačenju većeg broja žena u profesiju u području kibersigurnosti. ECSF će smanjiti i rascjepkanost pristupa uvođenjem smjernica odozgo prema dolje o tome kako kategorizirati višedimenzionalnu prirodu kibersigurnosne struke. Profili koje predlaže ECSF dovoljno su široki da mogu poduprijeti brojne uloge koje profesija nudi, a istovremeno su segmentirani na način koji ga čini razumljivim i primjenjivim za praktičare, stručnjake iz industrije, kreatore politika, stručnjake za zapošljavanje i tražitelje posla.

U ECSO-u smo uvjereni da će ECSF pružiti značajnu vrijednost našem radu i podržati širu zajednicu konkretnim alatom za usklađivanje napora i premošćivanje jaza između potražnje i ponude stručnjaka.

8.5 SLUČAJ UPOTREBE IZ ISC2

Ovaj odjeljak uključuje dijelove iz slučaja upotrebe koji je napisao (ISC)[229].

Upotreba (ISC)^2 CISSP CBK za potporu Europskom okviru za vještine u području kibersigurnosti / stručnim zajednicama za kibersigurnost

Uvod

(ISC)^2 CISSP CBK - ponekad jednostavno nazvan "Tijelo znanja" - odnosi se na stručno razvijenu zbirku onoga što kompetentni stručnjak za kibernetičku sigurnost mora identificirati i posjedovati, uključujući znanje, vještine, sposobnosti, tehnike i prakse da bi bio uspješan. (ISC)2 CBK zbirka je tema relevantnih za stručnjake za kibernetičku sigurnost diljem svijeta. Njome se uspostavlja zajednički okvir pojmova i načela informacijske sigurnosti koji stručnjacima za kibersigurnost i IT/IKT diljem svijeta omogućuje raspravu, raspravu i rješavanje pitanja koja se odnose na profesiju uz zajedničko razumijevanje, taksonomiju i leksikon. (ISC)2 djelomično je uspostavljen radi objedinjavanja, standardizacije i održavanja (ISC)2 CBK-a za stručnjake u području kibersigurnosti diljem svijeta. (ISC)2 CBK predstavlja gotov resurs za sadašnje i buduće stručnjake za kibersigurnost za usvajanje u okviru ECSF-a.

29 https://www.isc2.Org/-/media/9644E0ED44954F7CAF895D45620213EA.ashx

Kao što je ENISA opisala u svojem nedavno objavljenom izvješću "Rješavanje nedostatka i nedostatka vještina u području kibersigurnosti u EU-u kroz visoko obrazovanje", globalni nedostatak vještina u području kibersigurnosti i nedostatak dovoljne i kvalificirane radne snage zabrinutost je koja znatno utječe na sposobnost država članica EU-a da zaštite javnost od sve većih prijetnji koje proizlaze iz sve veće upotrebe tehnologije u društvu. Unatoč obavljenom radu, kibernapadi i prijetnja kibernapada i dalje predstavljaju značajan rizik za javnu sigurnost. Europske organizacije bore se s odgovarajućim osobljem svojih timova za kibernetičku sigurnost. Posljedice koje se mogu spriječiti - pogrešno konfigurirani sustavi, žurna implementacija, nepotpun odgovor na incidente, odgođeno krpanje, neadekvatno upravljanje rizicima - čine mnoge europske organizacije primamljivim metama za aktere prijetnji diljem svijeta.

Rješenje koje je omogućio ECSF (kako su se suočavali s izazovima)

Kako bi se odgovorilo na izazove koje predstavlja nedostatak vještina i nedostatak radne snage, (ISC)[2] predlaže rješenje usmjereno na pomoć stručnjacima za kibersigurnost da identificiraju i mapiraju potrebna znanja, vještine, sposobnosti, tehnike i prakse u profile utvrđene u Europskom okviru vještina kibersigurnosti (ECSF). (ISC)2 CISSP CBK mapira nekoliko područja vještina i znanja u sljedećim ECSF profilima:

- 2.1 Glavni službenik za informacijsku sigurnost (CISO)
- 2.2 Odgovor na kibernetičke incidente
- 2.3 Cyber pravno, politika i usklađenostSlužbenik
- 2.4 Stručnjak za obavještajne podatke o kibernetičkim prijetnjama
- 2.5 Arhitekt kibernetičke sigurnosti
- 2.6 Revizor kibernetičke sigurnosti

Koristeći koncepte obuhvaćene CBK-om, stručnjaci koji trenutno rade u gore navedenim profilima ili oni koji žele raditi u tim profilima mogu koristiti ključne vještine i područja znanja iz ECSF profila u kombinaciji s (ISC)2 CBK kako bi utvrdili kako CBK ispunjava znanja i vještine potrebne za radno mjesto i gdje će možda trebati nadopuniti svoje obrazovanje/osposobljavanje iz drugih izvora. To će omogućiti kandidatima da izgrade obrazovni put/obuku kako bi postigli svoje ciljeve.

Sljedeća tablica daje primjer kako (ISC)2 CISSP CBK može koristiti sadašnji ili ambiciozni CISO za identificiranje ključnih vještina i područja znanja iz ECSF CISO profila koje imaju ili trebaju izgraditi. [...]

Rezultat / dodana vrijednost

Predviđena korist (ISC)2 CISSP CBK mapiranja ECSF-a jest u tome što će se njime stvoriti karijerno usmjeravanje i profesionalni obrazovni putovi kako bi se sadašnjim i budućim stručnjacima za kibersigurnost pomoglo da identificiraju i steknu potrebna stručna znanja, vještine i sposobnosti kako bi brže dobili i popunili otvorene profile, kako je utvrđeno u ECSF-u, čime bi se ublažio globalni nedostatak vještina u području kibersigurnosti i smanjio jaz kvalificirane radne snage.

B.6 SLUČAJ UPOTREBE IZ ISACA

Ovaj odjeljak uključuje dijelove iz slučaja upotrebe koji je napisao ISACA.[30]

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

Individualno donošenje odluka o karijeri: profesionalne kvalifikacije Europski okvir vještina u području kibersigurnosti

Uvod

Sabine je radila kao analitičarka SOC-a nekoliko godina nakon stjecanja sveučilišne diplome i zanimalo ju je kako najbolje unaprijediti svoju karijeru. Razgovarala je sa svojim mentorom, koji joj je savjetovao da je ISACA bila izvrsna odskočna daska za njegovu karijeru i potaknuo je da razmotri članstvo i eventualnu certifikaciju. Mora se shvatiti da ulazak u kibernetičku sigurnost daje mogućnost rada sa svime, od ljudi i psihologije preko prava, politike i upravljanja, sve do najniže (ili najviše) razine tehničke razine. Izazov je pronaći početnu točku, a zatim identificirati koje specifične kompetencije možete naučiti, a zatim savladati kako biste proširili ili čak prešli između uloga kibernetičke sigurnosti. ESCF navodi nekoliko uloga s njihovim kompetencijama potrebnima za rad u okviru te specifične uloge. Primijetite da te kompetencije nisu sve što je potrebno za određenu ulogu, već minimum. Koristeći ovo, Sabine može identificirati jaz u kompetencijama ako netko želi promijeniti ulogu ili prijeći u drugo područje unutar kibernetičke sigurnosti.

Izazov

Kao nova profesionalka u području visoke potražnje i kao žena u kibernetičkoj sigurnosti, Sabine je tražila pomoć u nekoliko različitih područja:

- Karijerno usmjeravanje i resursi - uključujući vjerodajnice - koji će joj pomoći u napredovanju u karijeri
- Mreža kolega i lidera u industriji koji će joj pomoći u snalaženju u profesionalnim izazovima
- Pomoć u razvoju mekih vještina koje će joj pomoći da postane dobro zaokružen budući vođa
- Uvidi u prevladavanje izazova i iskorištavanje prilika kao žena u kibersigurnost
- Informacije koje će joj pomoći da dobro obavlja svoj trenutni posao i da se pripremi za buduće izazove na višim pozicijama

Svaki pojedinac može koristiti ESCF da vidi koje su uloge potrebne za rješavanje gotovo bilo koje vrste izazova ili zadataka unutar domene kibernetičke sigurnosti. Također, korištenjem ESCF-a kao osnove pojedinac može utvrditi koje su kompetencije potrebne za prelazak iz jedne uloge u drugu. To će koristiti dijalogu između zaposlenika i poslodavaca pri planiranju kontinuirane edukacije u području kibernetičke sigurnosti. To će također koristiti pojedincu koji želi ući u kibernetičku sigurnost, ali nije siguran odakle početi. Za većinu pojedinaca dodavanje prethodnog znanja i kompetencija lakše je nego učenje nečeg potpuno novog.

S misijom da postane C-suite stručnjak za kibernetičku sigurnost u ovom izazovnom području, Sabine je istražila pregled odgovornosti CISO-a:

Profil 1 CISO misija	Definira, održava i komunicira viziju, strategiju, politike i postupke kibernetičke sigurnosti te upravlja implementacijom u cijeloj organizaciji. Upravlja aktivnostima povezanim s kibernetičkom sigurnošću u cijeloj organizaciji. Upravlja vezama/vezama s vanjskim tijelima i strukovnim tijelima.

Sabineina ambicija je identificirati nedostatke u svojim vještinama kako bi napredovala u karijeri s odgovarajuće usklađenim vjerodajnicama na sljedeću razinu.

ECSF rješenje

Sabine je istraživala ECSF PROFIL 1 i identificirala nedostatke u svom znanju:

Ključna znanja	7 Poznavanje standarda, okvira, politika, propisa, zakonodavstva, certifikata i najboljih praksi kibernetičke sigurnosti i privatnosti Razumijevanje etičkih zahtjeva organizacije za kibernetičku sigurnost 7 Poznavanje sigurnosnih kontrola Poznavanje modela zrelosti kibernetičke sigurnosti 7 Poznavanje taktika, tehnika i postupaka kibernetičke sigurnosti Poznavanje upravljanja resursima Poznavanje praksi upravljanja Poznavanje okvira za upravljanje rizicima

Sabine je odlučila poslušati savjet svog mentora i prisustvovati lokalnom sastanku ISACA-e kako bi vidjela je li to pravi izbor. Odmah je bila impresionirana prilikama koje je pružao. Ogranak ju je srdačno dočekao, upoznavši je s nekoliko ključnih ljudi u ogranku – ljudima koji su radili na točno onoj vrsti uloga koje je Sabine tražila i koji bi bili izvrsni mentori ili sponzori.

Predsjedavajuća za certifikaciju ogranka obavijestila je Sabine da bi joj certifikat Certified Information Security Manager (CISM) odlično odgovarao jer pokazuje dobro zaokruženo znanje o informacijskoj sigurnosti, kao i snažne menadžerske vještine. Certifikat je za one s pet ili više godina iskustva, pa je Sabine odlučila napraviti 18-mjesečni plan za studiranje i stjecanje certifikata.

Te se večeri pridružila ISACA-i kao članica i u potpunosti iskoristila resurse koje je udruga nudila na globalnoj i lokalnoj razini. Pridružila se online zajednicama udruge, počela pohađati webinare i sastanke lokalnih ogranaka koji se nude putem SheLeadsTech, programa koji nudi ISACA-ina zaklada One in Tech. I prisustvovala je gotovo svakom sastanku koji je mjesni ogranak ponudio.

Samo šest mjeseci nakon što je postala član, kolega član ogranka obratio joj se u vezi s poslom analitičara informacijske sigurnosti u njihovoj organizaciji.

Rezultat

Sabine je sada članica ISACA-e već sedam godina. Stekla je CISM certifikat i ubrzo je unaprijeđena u voditeljicu informacijske sigurnosti. Sada je direktorica informacijske sigurnosti, s jasnim putem do uloge CISO-a.

Osim pronalaženja vjerodajnica i poslova putem ISACA-e, Sabine je također pronašla nekoliko resursa koji su joj pomogli da doda vrijednost svojoj organizaciji. Prije nego što je GDPR stupio na snagu, Sabine je uspjela iskoristiti GDPR Resource Hub koji nudi ISACA kako bi joj pomogao da temeljito razumije situaciju i nauči koji su najkritičniji koraci koje treba poduzeti u njezinoj trenutnoj ulozi.

Interes i iskustvo koje je stekla u privatnosti kao rezultat tog projekta omogućili su joj da se kvalificira za ISACA-inu vjerodajnicu Certified Data Privacy Solutions Engineer (CDPSE) kroz svoj program ranog usvajanja.

Izlagala je na ISACA konferencijama na razini ogranaka i na nacionalnoj razini - usavršavajući svoje komunikacijske vještine - a prošle je godine preuzela poziciju u odboru ogranka. Kao redateljica, ona

imala je priliku zaposliti se na nekoliko pozicija, a većina njezinih zaposlenika došla je iz ISACA ogranka - baš kao što je pronašla svoje prvo promaknuće prije šest godina. Uvidjevši vrijednost CISM certifikata u vlastitoj karijeri, počela je nuditi pripremu za CISM certifikaciju svom timu kroz ISACA-inu ponudu obuke za poduzeća.

Sabinino najnovije područje fokusa dok se priprema za svoju ulogu CISO-a je osiguravanje novih tehnologija. S obzirom na povećani regulatorni fokus na umjetnu inteligenciju u Europi, prvo je usmjerila svoje napore na to područje, nedavno dobivši certifikat o osnovama umjetne inteligencije od ISACA-e.

Sedam godina nakon što je prošla kroz vrata svog prvog sastanka ISACA-inog ogranka, Sabine je proširila svoju mrežu za stotine profesionalaca na lokalnoj razini i tisućama diljem svijeta. Ona je

samouvjerena vođa i govornica, a sada je mentorica nekolicini drugih koji su nekoć bili na njezinoj poziciji. Među njezinim savjetima njezinim mentorima je da uvijek uče - i da je ISACA, kao globalna zajednica za učenje, izvrstan resurs.

Sabine je iznijela korake koje treba poduzeti kako bi dobila C-suite i planira obnašati ulogu CISO-a u roku od pet godina. Uvjerena je da će njezina ISACA mreža i vjerodajnice biti značajna prednost dok slijedi svoje ciljeve.

Karijeru:

- SOC analitičar
- Informacijska sigurnostAnalitičar
- Informacijska sigurnostUpravitelj
- Direktor informacijske sigurnosti.

B.7 SLUČAJ UPOTREBE IZ SANS/GIAC

Ovaj odjeljak uključuje dijelove iz slučaja upotrebe koji su napisali SANS institut i GIAC (Global Information Assurance Certification)[31].

Zašto su okviri i certifikati radne snage važni u kibernetičkoj sigurnosti

Direktiva o mrežama i informacijama (NIS) II ažuriranje je postojećeg mandata Europske unije. To će pomoći u poticanju zajedničkog jezika kibersigurnosti u širem rasponu gospodarskih sektora i zahtijevat će razmjenu informacija među državama članicama i međusektorima. Direktive poput ove imaju sve veću važnost u uspostavljanju zaštitnih ograda za kibernetičke aktivnosti. Kako bi zaštitila vrijednost dioničara, Komisija za sigurnost i burzu (SEC) razmatra kibernetičko izvješće za tvrtke kojima se javno trguje koje zahtijeva izvješćivanje o tome kako će njihovi sigurnosni timovi upravljati rizicima, incidentima i kibernetičkom stručnošću upravnog odbora. Izvješće o ublažavanju sigurnosnog rizika povezat će se sa skupovima vještina radnih uloga.

Okviri pomažu u artikulaciji ovih radnih uloga. Većina otvorenih radnih mjesta donedavno bili su generički popisi koji su tražili stručnjake za kibernetičku sigurnost bez dobro definiranih zadataka, vještina ili znanja o tome što je potrebno za zaštitu imovine organizacije. Okviri radne snage kao što je ECSF Europski okvir za vještine kibernetičke sigurnosti (ECSF) počinju standardizirati talente potrebne za pozicije kao što su odgovornik na kibernetičke incidente, istražitelj digitalne forenzike i glavni službenik za informacijsku sigurnost. Standardizacija omogućuje organizacijama da identificiraju pravo

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

talent za suočavanje s budućim prijetnjama. To je u skladu s drugim profesijama. Na primjer, liječnici imaju specijalizirana područja kao što su radiolozi, pedijatri i neurokirurzi koji imaju stručnost potrebnu u svom području za pružanje odgovarajućeg liječenja.

Certifikacija igra važnu ulogu u pripremi ljudi za određene radne uloge. Certifikacija potvrđuje pojedinca korištenjem najboljih praksi i smjernica za obrazovno i psihološko testiranje kao što su međunarodni standardi ISO/IEC 17024. Primjer certifikata koji se smatra globalnim standardom je ovlašteni javni računovođa (CPA). Radno iskustvo može nekoga učiniti stručnjakom, ali CPA je cijenjena osnova certificiranog stručnjaka i čak može biti uvjet za usklađenost na određenim projektima ili revizijama.

Neki primjeri u kojima su okviri radne snage pomogli unaprijediti industriju kibernetičke sigurnosti uključuju:

- Velike tehnološke i financijske tvrtke često imaju više sigurnosnih timova koji standardiziraju svoje radne uloge i zahtjeve kroz okvir za brzo repozicioniranje i rotiranje radnika na temelju misije.
- Organizacije mogu mapirati iskustvo i certifikaciju svoje radne snage kako bi brzo uskladile vještine osoblja sa zahtjevima projekta. Ovo je posebno važno za konzultantske tvrtke, tehnološke tvrtke i izvođače.
- Okviri pružaju zajednički jezik u radnoj snazi u industrijama kao što su tehnologija, financije, zdravstvo, maloprodaja i komunalne usluge, omogućujući timovima da rade zajedno na zaštiti kibernetičkih i fizičkih sigurnosnih prijetnji.
- Okviri pružaju predložak akademskim institucijama da premoste jaz između svoje obrazovne ponude i trenutnih vještina kibernetičke sigurnosti potrebnih u svim industrijama, pripremajući svoje studente za posao.

SANS i GIAC razumiju važnost okvira i uskladili su tečajeve i certifikate s tim okvirima. Okviri su predložak za organizacije da standardiziraju zahtjeve za posao iako će svaka organizacija i misija trebati neke prilagodbe povezane s njihovom specifičnom misijom. Pomogli smo u osmišljavanju i implementaciji programa razvoja radne snage koristeći okvire kao predložak za tvrtke s popisa Fortune 500, vladine agencije i organizacije svih veličina.

TP-09-22-509-HR-N

O ENISA-i

Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije posvećena postizanju visoke zajedničke razine kibersigurnosti diljem Europe. Agencija Europske unije za kibersigurnost, osnovana 2004. i ojačana Aktom EU-a o kibersigurnosti, doprinosi kiberpolitici EU-a, povećava pouzdanost IKT proizvoda, usluga i procesa s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi za kiberizazove sutrašnjice. Razmjenom znanja, izgradnjom kapaciteta i podizanjem razine osviještenosti Agencija surađuje sa svojim ključnim dionicima na jačanju povjerenja u povezano gospodarstvo, jačanju otpornosti infrastrukture Unije i, u konačnici, održavanju digitalne sigurnosti europskog društva i građana. Više informacija o ENISA-i i njezinu radu možete pronaći ovdje: www.enisa.europa.eu.

ENISA
Agencija Europske unije za kibersigurnost

Ured u Ateni
Agamemnonos 14, Chalandri 15231, Attiki, Grčka

Ured u Heraklionu
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grčka

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

[9]. Europski kvalifikacijski okvir za cjeloživotno učenje