AGENTÚRA EURÓPSKEJ ÚNIE
PRE KYBERNETICKÚ
BEZPEČNOSŤ

ECSF

EURÓPSKY RÁMEC ZRUČNOSTI V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

SEPTEMBER 2022

O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúrou Únie, ktorá sa zameriava na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Európe. Agentúra Európskej únie pre kybernetickú bezpečnosť zriadená v roku 2004 a posilnená Aktom EÚ o kybernetickej bezpečnosti prispieva ku kybernetickej politike EÚ, zvyšuje dôveryhodnosť IKT produktov, služieb a procesov so systémami certifikácie kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy budúcnosti. Prostredníctvom výmeny poznatkov, budovania kapacít a zvyšovania informovanosti, agentúra spolupracuje so svojimi kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v prepojenú ekonomiku, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zabezpečiť digitálnu bezpečnosť európskej spoločnosti a občanov. Viac informácií o agentúre ENISA a jej práci nájdete tu: www.enisa.europa.eu.

KONTAKT

Pre kontaktovanie redaktora použite euskills@enisa.europa.eu.

POĎAKOVANIE

Tento rámec je výsledkom odborného stanoviska a dohody pracovnej skupiny ad hoc pre rámec zručností, ktorú tvoria 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 a Jan HAJNY.

Fabio DI FRANCO a Athanasios GRAMMATOPOULOS viedli túto činnosť pre agentúru ENISA.

PRÁVNE OZNÁMENIE

*Spravodajca ad-hoc pracovnej skupiny pre európsky rámec zručností v oblasti kybernetickej bezpečnosti

obsiahnutých v tejto publikácii.

Agentúra ENISA si zachováva svoje práva duševného vlastníctva v súvislosti s touto publikáciou.

UPOZORNENIE O AUTORSKÝCH PRÁVACH

ISBN: 978-92-9204-584-5 – DOI: 10.2824/859537

Obsah

1. PREHĽAD


Hlavný úradník pre bezpečnosť informácií (CISO)
Koordinátor reakcie na kybernetické incidenty
Úradník pre kybernetické právo, politiku a dodržiavanie predpisov
Špecialista na spravodajské informácie o kybernetických hrozbách
Architekt kybernetickej bezpečnosti
Audítor kybernetickej bezpečnosti
Pedagóg v oblasti kybernetickej bezpečnosti
Implementátor kybernetickej bezpečnosti
Výskumník v oblasti kybernetickej bezpečnosti
Manažér pre riziká kybernetickej bezpečnosti
01 101
Digitálny forenzný vyšetrovateľ
01010 11101 00101
Penetračný tester

2. PROFILY

2.1 HLAVNÝ ÚRADNÍK PRE BEZPEČNOSŤ INFORMÁCIÍ (CISO)

Názov profilu	Hlavný úradník pre bezpečnosť informácií (CISO)
Alternatívny názov (názvy)	Riaditeľ programu kybernetickej bezpečnosti Pracovník pre bezpečnosť informácií (ISO) Manažér informačnej bezpečnosti Vedúci informačnej bezpečnosti Bezpečnostný riaditeľ IT/IKT
Súhrnný výkaz	Riadi stratégiu kybernetickej bezpečnosti organizácie a jej vykonávanie s cieľom zabezpečiť, aby digitálne systémy, služby a aktíva boli primerane bezpečné a chránené.
Určenie	Definuje, udržiava a komunikuje víziu, stratégiu, politiky a postupy v oblasti kybernetickej bezpečnosti. Riadi vykonávanie kyberneticko-bezpečnostnej politiky v celej organizácii. Zabezpečuje výmenu informácií s externými a profesijnými orgánmi.
Výstup (výsledky)	• Stratégia kybernetickej bezpečnosti • Politika kybernetickej bezpečnosti
Hlavná úloha (hlavné úlohy)	• Definovať, vykonávať, komunikovať a udržiavať kyberneticko-bezpečnostné ciele, požiadavky, stratégie, politiky v súlade s obchodnou stratégiou na podporu organizačných cieľov • Pripraviť a predložiť kyberneticko-bezpečnostnú víziu, stratégie a politiky na schválenie vrcholovým manažmentom organizácie a zabezpečiť ich vykonávanie • Dohľad nad uplatňovaním a zlepšovaním systému riadenia informačnej bezpečnosti (ISMS) • Vzdelávať vrcholový manažment o kyberneticko-bezpečnostných rizikách, hrozbách a ich vplyve na organizáciu • Zabezpečiť, aby vrcholový manažment schvaľoval kyberneticko-bezpečnostné riziká organizácie • Vypracovať plány kybernetickej bezpečnosti • Rozvíjať vzťahy s orgánmi a komunitami súvisiacimi s kybernetickou bezpečnosťou • Nahlasovať kyberneticko-bezpečnostné incidenty, riziká, zistenia vrcholovému manažmentu • Monitorovať pokrok v oblasti kybernetickej bezpečnosti • Zabezpečenie zdrojov na vykonávanie stratégie kybernetickej bezpečnosti • Rokovanie o rozpočte na kybernetickú bezpečnosť s vrcholovým manažmentom • Zabezpečiť odolnosť organizácie voči kybernetickým incidentom • Riadenie neustáleho budovania kapacít v rámci organizácie • Preskúmanie, plánovanie a prideľovanie primeraných zdrojov kybernetickej bezpečnosti

Kľúčové zručnosti	• Posúdiť a zlepšiť postavenie organizácie v oblasti kybernetickej bezpečnosti • Analyzovať a vykonávať kyberneticko-bezpečnostné politiky, certifikácie, štandardy, metodiky a rámce • Analyzovať a dodržiavať zákony, nariadenia a právne predpisy súvisiace s kybernetickou bezpečnosťou • Vykonávať kyberneticko-bezpečnostné odporúčania a osvedčené postupy v oblasti kybernetickej bezpečnosti • Spravovať kyberneticko-bezpečnostné zdroje • Rozvíjať, presadzovať a viesť realizáciu stratégie kybernetickej bezpečnosti • Ovplyvniť kultúru kybernetickej bezpečnosti organizácie • Navrhnúť, aplikovať, monitorovať a kontrolovať systému riadenia informačnej bezpečnosti (ISMS) buď priamo, alebo prostredníctvom vedenia outsourcingu • Preskúmať a vylepšiť bezpečnostné dokumenty, správy, (SLA dohody) o úrovni poskytovaných bezpečnostných služieb a zaistiť bezpečnostné cieľov • Identifikovať a riešiť problémy súvisiace s kybernetickou bezpečnosťou • Vypracovať plán kybernetickej bezpečnosti • Komunikovať, koordinovať a spolupracovať s internými a externými zainteresovanými stranami • Predvídať požadované zmeny v stratégii informačnej bezpečnosti organizácie a formulovať nové plány • Definovať a aplikovať modely vyspelosti pre riadenie kybernetickej bezpečnosti • Predvídať hrozby, potreby a nadchádzajúce výzvy v oblasti kybernetickej bezpečnosti • Motivovať a povzbudzovať ľudí	
Kľúčové znalosti	• Politiky kybernetickej bezpečnosti • Štandardy, metodiky a rámce kybernetickej bezpečnosti • Odporúčania a osvedčené postupy v oblasti kybernetickej bezpečnosti • Zákony, nariadenia a právne predpisy súvisiace s kybernetickou bezpečnosťou • Certifikácie súvisiace s kybernetickou bezpečnosťou • Etické požiadavky na organizáciu kybernetickej bezpečnosti • Modely zrelosti kybernetickej bezpečnosti • Postupy kybernetickej bezpečnosti • Riadenie zdrojov • Postupy riadenia • Normy, metodiky a rámce riadenia rizík	
e-kompetentnosť (z e-CF)	A.7. Monitorovanie technologických trendov D.1. Rozvoj stratégie informačnej bezpečnosti E.3. Riadenie rizík E.8 Riadenie informačnej bezpečnosti E.9. Riadenie informačných systémov	Úroveň 4 Úroveň 5 Úroveň 4 Úroveň 4 Úroveň 5

2.2 KOORDINÁTOR REAKCIE NA KYBERNETICKÉ INCIDENTY

Názov profilu	Koordinátor reakcie na kybernetické incidenty
Alternatívny názov (názvy)	Spracovateľ kybernetických incidentov Expert na kybernetickú krízu Inžinier reakcie na incidenty Analytik centra bezpečnostných operácií (SOC) Kybernetický bojovník/Ochranca Analytik bezpečnostných operácií (SOC Analyst) Manažér kybernetickej bezpečnosti SIEM
Súhrnný výkaz	Monitorovať kyberneticko-bezpečnostný stav organizácie, riešiť incidenty počas kybernetických útokov a zabezpečiť nepretržitú prevádzku systémov IKT.
Určenie	Monitoruje a posudzuje stav kybernetickej bezpečnosti systémov. Analyzuje, hodnotí a zmierňuje dopad kybernetických incidentov. Identifikuje hlavné príčiny kybernetických incidentov a zlomyseľných aktérov. Podľa plánu reakcie na incidenty organizácie obnovuje funkcie systémov a procesov do prevádzkového stavu, zhromažďuje dôkazy a dokumentuje prijaté opatrenia.
Výstup (výsledky)	• Plán reakcie na incidenty • Správa o kybernetických incidentoch
Hlavná úloha (hlavné úlohy)	• Prispievať k rozvoju, udržiavaniu a hodnoteniu Plánu reakcie na incidenty • Vyvinúť, vykonávať a posúdiť postupy súvisiace s riešením incidentov • Identifikovať, analyzovať, zmierňovať a komunikovať kybernetické incidenty • Posudzovať a riadiť technické zraniteľností • Merať účinnosť odhaľovania a reakcie na kyberneticko-bezpečnostné incidenty • Vyhodnotiť odolnosť kontrol kybernetickej bezpečnosti a zmierňujúcich opatrení prijatých po incidente v súvislosti s kybernetickou bezpečnosťou alebo porušením ochrany údajov • Prijať a vyvinúť skúšobné techniky na riešenie incidentov • Stanoviť postupy analýzy výsledkov incidentov a podávania správ o incidentoch • Dokumentovať analýzu výsledkov incidentov a opatrenia na riešenie incidentov • Spolupracovať s bezpečnostnými operačnými centrami (SOC) a jednotkami pre riešenie počítačových bezpečnostných incidentov (CSIRT) • Spolupracovať s kľúčovými pracovníkmi pri hlásení bezpečnostných incidentov podľa platného právneho rámca

Kľúčové zručnosti	• Precvičiť si všetky technické, funkčné a prevádzkové aspekty riešenia a odozvy kybernetických incidentov • Zhromažďovať, analyzovať a korelovať informácie o kybernetických hrozbách pochádzajúce z viacerých zdrojov • Práca na operačných systémoch, serveroch, cloudoch a príslušných infraštruktúrach • Práca pod tlakom • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Spravovať a analyzovať protokolové súbory	
Kľúčové znalosti	• Štandardy, metodiky a rámce na zvládanie incidentov • Odporúčania a osvedčené postupy zvládanie incidentov • Nástroje na zvládanie incidentov • Komunikačné postupy na zvládanie incidentov • Bezpečnosť operačných systémov • Bezpečnosť počítačových sietí • Kybernetické hrozby • Postupy kyberneticko-bezpečnostného útoku • Zraniteľnosť počítačových systémov • Certifikácie súvisiace s kybernetickou bezpečnosťou • Zákony, nariadenia a právne predpisy súvisiace s kybernetickou bezpečnosťou • Prevádzka bezpečných operačných centier (SOC) • Operácie jednotiek reakcie na počítačové bezpečnostné incidenty (CSIRT)	
e-kompetentnosť (z e-CF)	A.7. Monitorovanie technologických trendov B.2. Integrácia komponentov B.3. Testovanie B.5. Výroba dokumentácie C.4. Riadenie problémov	Úroveň 3 Úroveň 2 Úroveň 3 Úroveň 3 Úroveň 4

2.3 ÚRADNÍK PRE KYBERNETICKÉ PRÁVO, POLITIKU A DODRŽIAVANIE PREDPISOV

Názov profilu	Úradník pre kybernetické právo, politiku a dodržiavanie predpisov
Alternatívny názov (názvy)	Úradník pre ochranu údajov (DPO) Úradník pre ochranu súkromia Konzultant pre kybernetické právo Poradca pre kybernetické právo Úradník pre správu informácií Úradník za dodržiavanie súladu s údajmi Úradník pre kybernetickú bezpečnosť Manažér súladu s IT/IKT Konzultant pre dodržiavanie predpisov riadenia rizík (GRC)
Súhrnný výkaz	Riadi dodržiavanie noriem súvisiacich s kybernetickou bezpečnosťou, právnych a regulačných rámcov na základe stratégie a právnych požiadaviek organizácie.
Určenie	Dohliada a zabezpečuje dodržiavanie právnych, regulačných rámcov a politík týkajúcich sa kybernetickej bezpečnosti a údajov v súlade so stratégiou a právnymi požiadavkami organizácie. Prispieva k činnostiam organizácie v oblasti ochrany údajov. Poskytuje právne poradenstvo pri vývoji procesov riadenia kybernetickej bezpečnosti organizácie a odporúča sanačné stratégie/riešenia na zabezpečenie súladu.
Výstup (výsledky)	• Príručka o dodržiavaní predpisov • Správa o dodržiavaní predpisov

Hlavná úloha (hlavné úlohy)	• Zabezpečiť súlad s normami, zákonmi a nariadeniami, a právnymi predpismi týkajúcimi sa ochrany osobných údajov a poskytovať právne poradenstvo a usmernenia, • Identifikovať a zdokumentovať nedostatky v dodržiavaní predpisov • Vykonávať posúdenia vplyvu na súkromie a vyvíjať, udržiavať, komunikovať a školiť o zásadách ochrany osobných údajov, postupoch • Presadzovať a obhajovať program organizácie na ochranu osobných údajov a súkromia • Zabezpečiť, aby vlastníci, držitelia, prevádzkovatelia, sprostredkovatelia, subjekty, interní alebo externí partneri a právnické osoby boli informovaní o svojich právach, povinnostiach a zodpovednostiach v oblasti ochrany údajov • Pôsobiť ako kľúčové kontaktné miesto na vybavovanie otázok a sťažností týkajúcich sa spracovania údajov • Pomoc pri navrhovaní, vykonávaní, audite a testovaní zhody s cieľom zabezpečiť súlad s kybernetickou bezpečnosťou a ochranou súkromia • Monitorovať audity a vzdelávacie činnosti súvisiace s ochranou údajov • Spolupracovať a zdieľať informácie s orgánmi a profesijnými skupinami • Prispievať k rozvoju stratégie, politiky a postupov v oblasti kybernetickej bezpečnosti organizácie • Rozvíjať a navrhovať odbornú prípravu v oblasti informovanosti zamestnancov s cieľom dosiahnuť súlad a podporiť kultúru ochrany údajov v rámci organizácie; Riadiť právne aspekty zodpovednosti v oblasti informačnej bezpečnosti a vzťahov s tretími stranami
Kľúčové zručnosti	• Komplexné pochopenie obchodnej stratégie, modelov a produktov a schopnosť zohľadniť právne, regulačné a štandardné požiadavky • Vykonávať postupy pracovného života v otázkach ochrany údajov a súkromia, ktoré sú spojené s implementáciou organizačných procesov, financií a obchodnej stratégie • Viesť vývoj vhodných politík a postupov v oblasti kybernetickej bezpečnosti a ochrany súkromia, ktoré dopĺňajú obchodné potreby a právne požiadavky; ďalej zabezpečiť jeho prijatie, porozumenie a vykonávanie a komunikovať o ňom medzi zúčastnenými stranami • Vykonávať, monitorovať a preskúmavať posúdenia vplyvu na súkromie pomocou noriem, rámcov, uznávaných metodík a nástrojov • Vysvetľovať a komunikovať témy ochrany údajov a súkromia zainteresovaným stranám a používateľom • Pochopiť, praktikovať a dodržiavať etické požiadavky a normy • Pochopiť dôsledky zmien právneho rámca na stratégiu a politiky organizácie v oblasti kybernetickej bezpečnosti a ochrany údajov • Spolupracovať s ostatnými členmi tímu a kolegami

Kľúčové znalosti	• Zákony, nariadenia a právne predpisy súvisiace s kybernetickou bezpečnosťou • Normy, metodiky a rámce kybernetickej bezpečnosti • Politiky kybernetickej bezpečnosti • Právne, regulačné a legislatívne požiadavky na dodržiavanie predpisov, odporúčania a osvedčené postupy Normy, metodiky a rámce hodnotenia vplyvu na súkromie	
e-kompetentnosť (z e-CF)	A.1. Informačné systémy a obchodná stratégia Zosúladenie D.1. Rozvoj stratégie informačnej bezpečnosti E.8 Riadenie informačnej bezpečnosti E.9. Riadenie informačných systémov	Úroveň 4 Úroveň 4 Úroveň 3 Úroveň 4

2.4 ŠPECIALISTA NA SPRAVODAJSKÉ INFORMÁCIE O KYBERNETICKÝCH HROZBÁCH

Názov profilu	Špecialista na spravodajské informácie o kybernetických hrozbách
Alternatívny názov (názvy)	Analytik kybernetického spravodajstva Modelár kybernetických hrozieb
Súhrnný výkaz	Zhromažďovať, spracovávať, analyzovať údaje a informácie s cieľom vypracovať použiteľné spravodajské správy a šíriť ich cieľovým zainteresovaným stranám.
Určenie	Riadi životný cyklus spravodajských informácií o kybernetických hrozbách vrátane zhromažďovania informácií o kybernetických hrozbách, analýzy a tvorby použiteľných spravodajských informácií a šírenia informácií zainteresovaným stranám v oblasti bezpečnosti a komunite CTI na taktickej, operačnej a strategickej úrovni. Identifikuje a monitoruje taktiku, techniky a postupy (TTP), ktoré používajú aktéri kybernetických hrozieb, a ich trendy, sleduje činnosti aktérov v oblasti hrozieb a sleduje, ako môžu nekybernetické udalosti ovplyvniť kybernetické činnosti.
Výstup (výsledky)	• Manuál pre spravodajstvo o kybernetických hrozbách • Správa o kybernetických hrozbách
Hlavná úloha (hlavné úlohy)	• Vypracovať, implementovať a riadiť stratégiu organizácie pre spravodajstvo o kybernetických hrozbách • Vypracovať plány a postupy na riadenie spravodajských informácií o hrozbách • Preložiť obchodné požiadavky do požiadaviek na spravodajstvo • Vykonávať zhromažďovanie spravodajských informácií o hrozbách, analýzu a tvorbu vykonateľných spravodajských informácií a šírenie informácií zainteresovaným stranám v oblasti bezpečnosti • Identifikovať a posúdiť aktérov kybernetických hrozieb, ktorí sa zameriavajú na organizáciu • Identifikovať, monitorovať a posudzovať taktiky, techniky a postupy (TTP), ktoré používajú aktéri kybernetických hrozieb, a to analýzou údajov, informácií a spravodajských informácií s otvoreným zdrojovým kódom a vlastníckym právom • Vypracúvať vykonateľné správy na základe údajov spravodajských informácií o hrozbách • Vypracovať a poskytovať poradenstvo v súvislosti so zmierňujúcimi plánmi na taktickej, operačnej a strategickej úrovni • Koordinovať so zainteresovanými stranami s cieľom zdieľať a využívať spravodajské informácie o relevantných kybernetických hrozbách • Využiť spravodajské údaje na podporu a pomoc pri modelovaní hrozieb, odporúčania týkajúce sa zmierňovania rizika a lovu kybernetických hrozieb • Formulovať a komunikovať inteligenciu otvorene a verejne na všetkých úrovniach • Sprostredkovať náležitú bezpečnostnú závažnosť vysvetlením vystavenia riziku a jeho dôsledkov netechnickým zainteresovaným stranám

Kľúčové zručnosti	• Spolupracovať s ostatnými členmi tímu a kolegami • Zhromažďovať, analyzovať a korelovať informácie o kybernetických hrozbách pochádzajúce z viacerých zdrojov • Identifikovať aktérov hrozieb TTP a kampane • Automatizovať postupy riadenia spravodajských informácií o hrozbách • Vykonávať technickú analýzu a podávanie správ • Identifikovať nekybernetické udalosti s dôsledkami na kybernetické činnosti • Modelové hrozby, aktéri a TTP • Komunikovať, koordinovať a spolupracovať s internými a externými zainteresovanými stranami • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Používať a aplikovať platformy a nástroje CTI	
Kľúčové znalosti	• Bezpečnosť operačných systémov • Bezpečnosť počítačových sietí • Kontroly a riešenia kybernetickej bezpečnosti • Počítačové programovanie • Spoločné využívanie noriem, metodík a rámcov kybernetických hrozieb spravodajskej služby (CTI) • Zodpovedné postupy zverejňovania informácií • Medzi-doménové a hraničné znalosti týkajúce sa kybernetickej bezpečnosti • Kybernetické hrozby • Aktéri kybernetických hrozieb • Postupy kyberneticko-bezpečnostného útoku • Pokročilé a pretrvávajúce kybernetické hrozby (APT) • Taktiky, techniky a postupy aktérov hrozieb (TTP) • Certifikácie súvisiace s kybernetickou bezpečnosťou	
e-kompetentnosť (z e-CF)	B.5. Výroba dokumentácie D.7. Dátová veda a analytika D.10. Správa informácií a znalostí E.4. Spravovanie vzťahov E.8 Riadenie informačnej bezpečnosti	Úroveň 3 Úroveň 4 Úroveň 4 Úroveň 3 Úroveň 4

2.5 ARCHITEKT KYBERNETICKEJ BEZPEČNOSTI

Názov profilu	Architekt kybernetickej bezpečnosti
Alternatívny názov (názvy)	Architekt riešení kybernetickej bezpečnosti Dizajnér kybernetickej bezpečnosti Architekt zabezpečenia dát
Súhrnný výkaz	Plánuje a navrhuje riešenia bezpečnosti už v štádiu návrhu (infraštruktúry, systémy, aktíva, softvér, hardvér a služby) a kontroly kybernetickej bezpečnosti.
Určenie	Navrhuje riešenia založené na zásadách bezpečnosti už v štádiu návrhu a súkromia už v štádiu návrhu. Vytvára a neustále zdokonaľuje architektonické modely a vyvíja vhodnú architektonickú dokumentáciu a špecifikácie. Koordinovať bezpečný vývoj, integráciu a údržbu komponentov kybernetickej bezpečnosti v súlade s normami a inými súvisiacimi požiadavkami.
Výstup (výsledky)	• Diagram architektúry kybernetickej bezpečnosti • Správa o požiadavkách na kybernetickú bezpečnosť
Hlavná úloha (hlavné úlohy)	• Navrhnúť a navrhnúť bezpečnú architektúru na implementáciu stratégie organizácie • Rozvíjať kyberneticko-bezpečnostnú architektúru organizácie s cieľom riešiť požiadavky na bezpečnosť a ochranu súkromia • Vypracovať architektonickú dokumentáciu a špecifikácie • Predložiť zainteresovaným stranám návrh bezpečnostnej architektúry na vysokej úrovni • Vytvoriť bezpečné prostredie počas vývoja životného cyklu systémov, služieb a produktov • Koordinovať vývoj, integráciu a údržbu kyberneticko-bezpečnostných komponentov zabezpečujúcich kyberneticko-bezpečnostné špecifikácie • Analyzovať a hodnotiť kybernetickú bezpečnosť architektúry organizácie • Zabezpečiť bezpečnosť architektúr riešení prostredníctvom bezpečnostných previerok a certifikácie • Spolupracovať s ostatnými tímami a kolegami • Hodnotiť vplyv kyberneticko-bezpečnostných riešení na návrh a výkonnosť architektúry organizácie • Prispôsobiť štruktúru organizácie vznikajúcim hrozbám • Posúdiť implementovanú architektúru s cieľom zachovať primeranú úroveň bezpečnosti

Kľúčové zručnosti	• Vykonávať analýzu bezpečnostných požiadaviek používateľov a podnikov • Nakresliť architektonické a funkčné špecifikácie kybernetickej bezpečnosti • Rozložiť a analyzovať systémy s cieľom vypracovať požiadavky na bezpečnosť a ochranu súkromia a identifikovať účinné riešenia • Navrhovať systémy a architektúry založené na bezpečnosti a ochrane súkromia už v štádiu návrhu a štandardne založené na zásadách kybernetickej bezpečnosti • Usmerňovať a komunikovať s realizátormi a IT/OT personálom • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Navrhnúť architektúry kybernetickej bezpečnosti založené na potrebách a rozpočte zainteresovaných strán • Vybrať vhodné špecifikácie, postupy a kontroly • Budovať odolnosť voči bodom zlyhania v celej architektúre • Koordinovať integráciu bezpečnostných riešení	
Kľúčové znalosti	• Certifikácie súvisiace s kybernetickou bezpečnosťou • Odporúčania a osvedčené postupy v oblasti kybernetickej bezpečnosti • Normy, metodiky a rámce kybernetickej bezpečnosti • Analýza požiadaviek súvisiacich s kybernetickou bezpečnosťou • Bezpečný životný cyklus rozvoja • Referenčné modely bezpečnostnej architektúry • Technológie súvisiace s kybernetickou bezpečnosťou • Kontroly a riešenia kybernetickej bezpečnosti • Riziká kybernetickej bezpečnosti • Kybernetické hrozby • Trendy v oblasti kybernetickej bezpečnosti • Právne, regulačné a legislatívne požiadavky na dodržiavanie predpisov, odporúčania a osvedčené postupy • Predchádzajúce postupy kybernetickej bezpečnosti • Technológie zvyšujúce súkromie (PET) • Štandardy, metodiky a rámce ochrany súkromia už v štádiu návrhu	
e-kompetentnosť (z e-CF)	A.5. Architektonický dizajn A.6. Dizajn aplikácie B.1. Vývoj aplikácií B.3. Testovanie B.6. Inžinierstvo systémov IKT	Úroveň 5 Úroveň 3 Úroveň 3 Úroveň 3 Úroveň 4

2.6 AUDÍTOR KYBERNETICKEJ BEZPEČNOSTI

Názov profilu	Audítor kybernetickej bezpečnosti
Alternatívny názov (názvy)	Audítor pre informačnú bezpečnosť (IT alebo právny audítor) Audítor pre kontrolu, riziká a dodržiavanie predpisov (GRC) Manažér auditu pre kybernetickú bezpečnosť Audítor postupov procesov kybernetickej bezpečnosti Audítor rizika informačnej bezpečnosti a dodržiavania predpisov Analytik pre hodnotenie údajov
Súhrnný výkaz	Vykonávať kyberneticko-bezpečnostné audity ekosystému organizácie. Zabezpečenie súladu so zákonnými, regulačnými, politickými informáciami, bezpečnostnými požiadavkami, priemyselnými normami a osvedčenými postupmi.
Určenie	Vykonáva nezávislé preskúmania s cieľom posúdiť účinnosť procesov a kontrol a celkový súlad s právnymi a regulačnými rámovými politikmi organizácie. Vyhodnocuje, testuje a overuje produkty súvisiace s kybernetickou bezpečnosťou (systémy, hardvér, softvér a služby), funkcie a politiky zabezpečujúce dodržiavanie usmernení, noriem a predpisov.
Výstup (výsledky)	• Plán auditu kybernetickej bezpečnosti • Správa o audite kybernetickej bezpečnosti
Hlavná úloha (hlavné úlohy)	• Vypracovať audítorskú politiku, postupy, štandardy a usmernenia organizácie • Stanoviť metodiky a postupy používaných pri audite systémov • Vytvoriť cieľové prostredie a riadiť audítorské činnosti • Vymedziť rozsah, ciele a kritériá na základe, ktorých sa má audit vykonávať • Vypracovať plán auditu, v ktorom sa opisujú rámce, štandardy, metodika, postupy a audítorské testy • Preskúmať ciele hodnotenia, bezpečnostných cieľov a požiadaviek na základe rizikového profilu • Súlad auditu s platnými zákonmi a nariadeniami týkajúcimi sa kybernetickej bezpečnosti • Súlad auditu s uplatniteľnými normami týkajúcimi sa kybernetickej bezpečnosti • Vykonať plán auditu a zhromaždiť dôkazy a merania • Udržiavať a chrániť integritu audítorských záznamov • Vypracúvať a komunikovať správy o posudzovaní zhody, uisťovaní, audite, certifikácii a údržbe • Monitorovať činnosti sanácie rizík

Kľúčové zručnosti	• Organizovať a pracovať systematickým a deterministickým spôsobom na základe dôkazov • Dodržiavať a praktizovať rámce, štandardy a metodiky auditu • Používanie audítorských nástrojov a techník • Analyzovať obchodné procesy, posudzovať a kontrolovať bezpečnosť softvéru alebo hardvéru, ako aj technické a organizačné kontroly • Rozložiť a analyzovať systémy na identifikáciu nedostatkov a neúčinných kontrol • Komunikovať, vysvetľovať a prispôsobovať právne a regulačné požiadavky a obchodné potreby • Zhromažďovať, vyhodnocovať, udržiavať a ochrániť informácie o audite • Auditovať bezúhonne, nestranne a nezávisle	
Kľúčové znalosti	• Kontroly a riešenia kybernetickej bezpečnosti • Právne, regulačné a legislatívne požiadavky na dodržiavanie predpisov, odporúčania a osvedčené postupy • Monitorovanie, testovanie a hodnotenie účinnosti kontrol kybernetickej bezpečnosti • Normy, metodiky a rámce posudzovania zhody • Audítorské štandardy, metodiky a rámce • Normy, metodiky a rámce kybernetickej bezpečnosti • Certifikácia súvisiaca s auditom • Certifikácie súvisiace s kybernetickou bezpečnosťou	
e-kompetentnosť (z e-CF)	B.3. Testovanie B.5. Výroba dokumentácie E.3. Riadenie rizík E.6 Riadenie kvality IKT E.8 Riadenie informačnej bezpečnosti	Úroveň 4 Úroveň 3 Úroveň 4 Úroveň 4 Úroveň 4

2.7 PEDAGÓG V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Názov profilu	Pedagóg v oblasti kybernetickej bezpečnosti
Alternatívny názov (názvy)	Špecialista na zvyšovanie povedomia o kybernetickej bezpečnosti Tréner kybernetickej bezpečnosti Fakulta kybernetickej bezpečnosti (profesor, lektor)
Súhrnný výkaz	Zlepšuje znalosti, zručnosti a kompetencie ľudí v oblasti kybernetickej bezpečnosti.
Určenie	Navrhuje, rozvíja a realizuje informačné, školiace a vzdelávacie programy v oblasti kybernetickej bezpečnosti a ochrany údajov. Využíva vhodné metódy, techniky a nástroje výučby a odbornej prípravy na komunikáciu a posilnenie kultúry, spôsobilostí, znalostí a zručností v oblasti kybernetickej bezpečnosti v oblasti ľudských zdrojov. Podporuje dôležitosť kybernetickej bezpečnosti a konsoliduje ju do organizácie.
Výstup (výsledky)	• Program na zvyšovanie povedomia o kybernetickej bezpečnosti • Výcvikový materiál v oblasti kybernetickej bezpečnosti
Hlavná úloha (hlavné úlohy)	• Vypracovať, aktualizovať a poskytovať učebné osnovy kybernetickej bezpečnosti a ochrany údajov a vzdelávacie materiály pre odbornú prípravu a informovanosť na základe obsahu, metód, nástrojov, potrieb stážistov • Organizovať, navrhovať a poskytovať činnosti, semináre, kurzy a praktické školenia zamerané na zvyšovanie informovanosti o kybernetickej bezpečnosti a ochrane údajov. • Monitorovať, vyhodnocovať a podávať správy o účinnosti odbornej prípravy • Hodnotiť a podávať správy o výkonnosti stážistov • Hľadať nových prístupov k vzdelávaniu, odbornej príprave a zvyšovaniu informovanosti • Navrhovať, vyvíjať a poskytovať simulácie kybernetickej bezpečnosti, virtuálne laboratória alebo prostredia kybernetického rozsahu • Poskytovať usmernenia k programom certifikácie kybernetickej bezpečnosti pre jednotlivcov • Neustále udržiavať a zlepšovať odborné znalosti; podporovať a posilňovať neustále zlepšovanie kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti

Kľúčové zručnosti	• Identifikovať potreby v oblasti informovanosti, odbornej prípravy a vzdelávania v oblasti kybernetickej bezpečnosti • Navrhovať, vyvíjať a poskytovať vzdelávacie programy na pokrytie potrieb kybernetickej bezpečnosti • Rozvíjať kyberneticko-bezpečnostné cvičenia vrátane simulácií využívajúcich prostredie kybernetického rozsahu • Poskytovať odbornú prípravu zameranú na kybernetickú bezpečnosť a odborné certifikácie v oblasti ochrany údajov • Využívať existujúce zdroje odbornej prípravy súvisiace s kybernetickou bezpečnosťou • Vypracovať hodnotiace programy pre činnosti v oblasti informovanosti, odbornej prípravy a vzdelávania • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Identifikácia a výber vhodných pedagogických prístupov pre určené publikum • Motivovať a povzbudzovať ľudí	
Kľúčové znalosti	• Pedagogické normy, metodiky a rámce • Rozvoj programu zvyšovania povedomia, vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti • Certifikácie súvisiace s kybernetickou bezpečnosťou • Normy, metodiky a rámce vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti • Zákony, nariadenia a právne predpisy súvisiace s kybernetickou bezpečnosťou • Odporúčania a najlepšie postupy v oblasti kybernetickej bezpečnosti • Normy, metodiky a rámce kybernetickej bezpečnosti • Kontroly a riešenia kybernetickej bezpečnosti	
e-kompetentnosť (z e-CF)	D.3. Poskytovanie vzdelávania a odbornej prípravy D.9. Personálny rozvoj E.8 Riadenie informačnej bezpečnosti	Úroveň 3 Úroveň 3 Úroveň 3

2.8 IMPLEMENTÁTOR KYBERNETICKEJ BEZPEČNOSTI

Názov profilu	Implementátor kybernetickej bezpečnosti
Alternatívny názov (názvy)	Implementátor pre informačnú bezpečnosť Expert na riešenia kybernetickej bezpečnosti Vývojár kybernetickej bezpečnosti Kyberneticko-bezpečnostný inžinier Inžinier pre vývoj, bezpečnosť a prevádzku (DevSecOps)
Súhrnný výkaz	Vyvíja, zavádza a prevádzkuje riešenia kybernetickej bezpečnosti (systémy, aktíva, softvér, kontroly a služby) v oblasti infraštruktúr a produktov.
Určenie	Poskytuje kyberneticko-bezpečnostný technický vývoj, integráciu, testovanie, implementáciu, prevádzku, údržbu, monitorovanie a podporu riešení súvisiacich s kybernetickou bezpečnosťou. Zabezpečuje dodržiavanie špecifikácií a požiadaviek na zhodu, zabezpečuje dobrý výkon a rieši technické problémy požadované v riešeniach súvisiacich s kybernetickou bezpečnosťou (systémy, aktíva, softvér, kontroly a služby), infraštruktúry a produkty organizácie.
Výstup (výsledky)	• Riešenia kybernetickej bezpečnosti
Hlavná úloha (hlavné úlohy)	• Vyvíjať, implementovať, udržiavať, modernizovať, testovať kyberneticko-bezpečnostných produktov • Poskytovať používateľom a zákazníkom podporu súvisiacu s kybernetickou bezpečnosťou • Integrovať kyberneticko-bezpečnostné riešenia a zabezpečiť ich správne fungovanie • Bezpečne konfigurovať systémy, služby a produkty • Udržiavať a aktualizovať bezpečnosť systémov, služieb a produktov • Implementovať postupy a kontroly kybernetickej bezpečnosti • Monitorovať a zabezpečovať vykonávanie zavedených kontrol kybernetickej bezpečnosti • Dokumentovať a podávať správy o bezpečnosti systémov, služieb a produktov • Úzko spolupracovať so zamestnancami IT/OT na opatreniach súvisiacich s kybernetickou bezpečnosťou • Implementovať, aplikovať a spravovať opravy produktov na technické riešenie zraniteľnosti
Kľúčové zručnosti	• Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Integrovať riešenia kybernetickej bezpečnosti do infraštruktúry organizácie • Konfigurovať riešenia podľa bezpečnostnej politiky organizácie • Posúdiť bezpečnosť a výkonnosť riešení • Vyvíjať kód, skripty a programy • Identifikovať a riešiť problémy súvisiace s kybernetickou bezpečnosťou • Spolupracovať s ostatnými členmi tímu a kolegami

Kľúčové znalosti	• Bezpečný životný cyklus rozvoja • Počítačové programovanie • Bezpečnosť operačných systémov • Bezpečnosť počítačových sietí • Kontroly a riešenia kybernetickej bezpečnosti • Útočné a obranné bezpečnostné praktiky • Odporúčania a osvedčené postupy bezpečného kódovania • Odporúčania a osvedčené postupy v oblasti kybernetickej bezpečnosti • Testovacie normy, metodiky a rámce • Testovacie postupy • Technológie súvisiace s kybernetickou bezpečnosťou	
e-kompetentnosť (z e-CF)	A.5. Dizajn architektúry A.6. Návrh aplikácie B.1. Vývoj aplikácií B.3. Testovanie B.6. Inžinierstvo systémov IKT	Úroveň 3 Úroveň 3 Úroveň 3 Úroveň 3 Úroveň 4

2.9 VÝSKUMNÍK V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Názov profilu	Výskumník v oblasti kybernetickej bezpečnosti
Alternatívny názov (názvy)	Výskumný inžinier v oblasti kybernetickej bezpečnosti Vedúci výskumu (CRO) v oblasti kybernetickej bezpečnosti Vedúci výskumný pracovník v oblasti kybernetickú bezpečnosť Pracovník pre výskum a vývoj v oblasti kybernetickej bezpečnosti Vedecký personál v oblasti kybernetickej bezpečnosti Pracovník pre výskum a inovácie/expert v oblasti kybernetickej bezpečnosti Výskumný pracovník v oblasti kybernetickej bezpečnosti
Súhrnný výkaz	Výskum v oblasti kybernetickej bezpečnosti a začlenenie výsledkov do kyberneticko-bezpečnostných riešení.
Určenie	Vykonáva zásadný/základný a aplikovaný výskum a uľahčuje inovácie v oblasti kybernetickej bezpečnosti prostredníctvom spolupráce s inými zainteresovanými stranami. Analyzuje trendy a vedecké zistenia v oblasti kybernetickej bezpečnosti.
Výstup (výsledky)	• Publikácia v oblasti kybernetickej bezpečnosti
Hlavná úloha (hlavné úlohy)	• Analyzovať a posudzovať kyberneticko-bezpečnostné technológie, riešenia, vývoj a procesy • Vykonávať výskum, inovácie a vývoj v oblastiach súvisiacich s kybernetickou bezpečnosťou • Zjaviť a vytvárať výskumné a inovačné nápady • Pokročiť v súčasnom stave v oblastiach súvisiacich s kybernetickou bezpečnosťou • Pomáhať pri vývoji inovatívnych riešení súvisiacich s kybernetickou bezpečnosťou • Vykonávať experimenty a rozvíjať dôkaz o koncepte, pilotných projektoch a prototypoch riešenia kybernetickej bezpečnosti • Vybrať a uplatňovať rámce, metódy, normy, nástroje a protokoly vrátane budovania a testovania koncepcie na podporu projektov • Prispievať k špičkovým podnikateľským nápadom, službám a riešeniam v oblasti kybernetickej bezpečnosti • Pomáhať pri budovaní kapacít súvisiacich s kybernetickou bezpečnosťou vrátane informovanosti, teoretickej odbornej prípravy, praktickej odbornej prípravy, testovania, mentorstva, dohľadu a zdieľania • Identifikovať medziodvetvové úspechy v oblasti kybernetickej bezpečnosti a uplatňovať ich v inom kontexte alebo navrhnúť inovačné prístupy a riešenia • Viesť inovačné procesy a projekty alebo sa na nich zúčastňovať vrátane projektového riadenia a rozpočtovania • Publikovať a prezentovať vedecké práce a výsledky výskumu a vývoja

Kľúčové zručnosti	• Generovať nové myšlienky a preniesť teóriu do praxe • Rozložiť a analyzovať systémy na identifikáciu nedostatkov a neúčinných kontrol • Rozložiť a analyzovať systémy s cieľom vypracovať požiadavky na bezpečnosť a ochranu súkromia a identifikovať účinné riešenia • Monitorovať nové pokroky v technológiách súvisiacich s kybernetickou bezpečnosťou • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Identifikovať a riešiť problémy súvisiace s kybernetickou bezpečnosťou • Spolupracovať s ostatnými členmi tímu a kolegami	
Kľúčové znalosti	• Výskum, vývoj a inovácie súvisiace s kybernetickou bezpečnosťou (RDI) • Normy, metodiky a rámce kybernetickej bezpečnosti • Právne, regulačné a legislatívne požiadavky týkajúce sa uvoľňovania alebo používania technológií súvisiacich s kybernetickou bezpečnosťou • Multidisciplinárny aspekt kybernetickej bezpečnosti • Zodpovedné postupy zverejňovania informácií	
e-kompetentnosť (z e-CF)	A.7. Monitorovanie technologických trendov A.9. Inovácia D.7. Dátová veda a analytika C.4. Riadenie problémov D.10. Správa informácií a znalostí	Úroveň 5 Úroveň 5 Úroveň 4 Úroveň 3 Úroveň 3

2.10 MANAŽÉR PRE RIZIKÁ KYBERNETICKEJ BEZPEČNOSTI

Názov profilu	Manažér pre riziká kybernetickej bezpečnosti
Alternatívny názov (názvy)	Analytik pre riziká kybernetickej bezpečnosti Poradca pre riziká kybernetickej bezpečnosti Posudzovateľ rizík kybernetickej bezpečnosti Analytik vplyvu kybernetickej bezpečnosti Manažér pre kybernetické riziká
Súhrnný výkaz	Riadiť riziká súvisiace s kybernetickou bezpečnosťou organizácie v súlade so stratégiou organizácie. Vyvíjať, udržiavať a komunikovať procesy a správy riadenia rizík.
Úloha	Priebežne riadi (identifikuje, analyzuje, posudzuje, odhaduje, zmierňuje) riziká súvisiace s kybernetickou bezpečnosťou infraštruktúr, systémov a služieb IKT prostredníctvom plánovania, uplatňovania, podávania správ, komunikovania analýzy rizík, hodnotenia a ošetrenia. Stanovuje stratégiu riadenia rizík pre organizáciu a zabezpečuje, aby riziká zostali pre organizáciu na prijateľnej úrovni výberom zmierňujúcich opatrení a kontrol.
Výstup (výsledky)	• Správa o hodnotení rizík kybernetickej bezpečnosti • Akčný plán na nápravu rizík kybernetickej bezpečnosti
Hlavná úloha (hlavné úlohy)	• Vypracovať stratégiu riadenia rizík kybernetickej bezpečnosti organizácie • Spravovať súpis aktív organizácie • Identifikovať a posudzovať hrozby a zraniteľné miesta systémov IKT súvisiace s kybernetickou bezpečnosťou • Identifikovať prostredia hrozieb vrátane profilov útočníkov a odhad potenciálu útokov • Posúdiť riziká kybernetickej bezpečnosti a navrhnúť najvhodnejšie možnosti zaobchádzania s rizikami vrátane bezpečnostných kontrol a zmierňovania rizika a vyhýbania sa riziku, ktoré najlepšie riešia stratégiu organizácie • Monitorovať účinnosť kontrol kybernetickej bezpečnosti a úrovne rizika • Zabezpečiť, aby všetky riziká kybernetickej bezpečnosti zostali na prijateľnej úrovni pre aktíva organizácie • Vyvinúť, udržiavať, reportovať a komunikovať kompletný cyklus riadenia rizík
Kľúčové zručnosti	• Implementovať rámce, metodiky a usmernenia pre riadenie rizík kybernetickej bezpečnosti a zabezpečiť súlad s predpismi a normami • Analyzovať a konsolidovať postupy organizácie v oblasti kvality a riadenia rizík • Umožniť vlastníkom podnikových aktív, vedúcim pracovníkom a iným zainteresovaným stranám prijímať informované rozhodnutia o riadení a zmierňovaní rizík • Vybudovať uvedomele prostredie s o riziku kybernetickej bezpečnosti • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Navrhovať a riadiť možnosti zdieľania rizika

Kľúčové znalosti	• Normy, metodiky a rámce riadenia rizík • Nástroje na riadenie rizík • Odporúčania a osvedčené postupy riadenia rizík • Kybernetické hrozby • Zraniteľnosť počítačových systémov • Kontroly a riešenia kybernetickej bezpečnosti • Riziká kybernetickej bezpečnosti • Monitorovanie, testovanie a hodnotenie účinnosti kontrol kybernetickej bezpečnosti • Certifikácie súvisiace s kybernetickou bezpečnosťou • Technológie súvisiace s kybernetickou bezpečnosťou	
e-kompetentnosť (z e-CF)	E.3. Riadenie rizík E.5. Zlepšenie procesu E.7. Riadenie obchodných zmien E.9. Riadenie informačných systémov	Úroveň 4 Úroveň 3 Úroveň 4 Úroveň 4

2.11 DIGITÁLNY FORENZNÝ VYŠETROVATEĽ

Názov profilu	Digitálny forenzný vyšetrovateľ
Alternatívny názov (názvy)	Digitálny forenzný analytik Špecialista na kybernetickú bezpečnosť a forenznú oblasť Počítačový forenzný konzultant
Súhrnný výkaz	Zabezpečiť, aby vyšetrovanie počítačovej kriminality odhalilo všetky digitálne dôkazy na preukázanie škodlivej činnosti.
Úloha	Spája artefakty s fyzickými osobami, zachytáva, obnovuje, identifikuje a uchováva údaje vrátane prejavov, vstupov, výstupov a procesov skúmaných digitálnych systémov. Poskytuje analýzu, rekonštrukciu a interpretáciu digitálnych dôkazov na základe kvalitatívneho stanoviska. Predstavuje nezaujatý kvalitatívny pohľad bez interpretácie výsledných zistení.
Výstup (výsledky)	• Výsledky digitálnej forenznej analýzy • Elektronické dôkazy
Hlavná úloha (hlavné úlohy)	• Vypracovať politiku, plány a postupy v oblasti digitálneho forenzného vyšetrovania • Identifikovať, obnoviť, extrahovať, dokumentovať a analyzovať digitálne dôkazy • Zachovať a chrániť digitálne dôkazy a sprístupniť ich oprávneným zainteresovaným stranám • Kontrolovať prostredia s cieľom zistiť dôkazy o neoprávnených a nezákonných činoch • Systematicky a deterministický dokumentovať, hlásiť a prezentovať digitálne forenzné zistenia a výsledky analýzy • Vyberať a prispôsobovať forenzné testovanie, analýzy a techniky podávania správ
Kľúčové zručnosti	• Pracovať eticky a nezávisle; neovplyvnený a nezaujatý internými alebo externými aktérmi • Zhromažďovať informácií pri zachovaní ich integrity • Identifikovať, analyzovať a korelovať udalosti kybernetickej bezpečnosti • Vysvetliť a prezentovať digitálne dôkazy jednoduchým, jednoduchým a ľahko zrozumiteľným spôsobom • Vypracúvať a komunikovať podrobné a odôvodnené správy o vyšetrovaní

Kľúčové znalosti	• Digitálne forenzné odporúčania a osvedčené postupy • Digitálne forenzné normy, metodiky a rámce • Postupy digitálnej forenznej analýzy • Testovacie postupy • Postupy, štandardy, metodiky a rámce trestného vyšetrovania • Zákony, nariadenia a právne predpisy súvisiace s kybernetickou bezpečnosťou • Nástroje na analýzu malvéru • Kybernetické hrozby • Zraniteľnosť počítačových systémov • Postupy kyberneticko-bezpečnostného útoku • Bezpečnosť operačných systémov • Bezpečnosť počítačových sietí • Certifikácie súvisiace s kybernetickou bezpečnosťou	
e-kompetentnosť (z e-CF)	A.7. Monitorovanie technologických trendov B.3. Testovanie B.5. Výroba dokumentácie E.3. Riadenie rizík	Úroveň 3 Úroveň 4 Úroveň 3 Úroveň 3

2.12 PENETRAČNÝ TESTER

Názov profilu	Penetračný tester
Alternatívny názov (názvy)	"Pentester" Etický hacker Analytik zraniteľnosti Tester kybernetickej bezpečnosti Ofenzívny expert na kybernetickú bezpečnosť Expert na obrannú kybernetickú bezpečnosť "Red Team Expert" "Red Teamer"
Súhrnný výkaz	Posúdiť účinnosť bezpečnostných kontrol, odhaliť a využívať zraniteľné miesta v oblasti kybernetickej bezpečnosti a posúdiť ich kritickosť, ak ich zneužívajú aktéri hrozieb.
Úloha	Plánuje, navrhuje, implementuje a vykonáva činnosti penetračného testovania a scenáre útoku s cieľom vyhodnotiť účinnosť nasadených alebo plánovaných bezpečnostných opatrení. Identifikuje slabé miesta alebo zlyhania technických a organizačných kontrol, ktoré majú vplyv na dôvernosť, integritu a dostupnosť produktov IKT (napr. systémy, hardvér, softvér a služby).
Výstup (výsledky)	• Správa o výsledkoch hodnotenia zraniteľnosti • Správa o penetračnom testovaní
Hlavná úloha (hlavné úlohy)	• Identifikovať, analyzovať a posúdiť technickú a organizačnú kybernetickú bezpečnosť zraniteľnosti • Identifikovať vektory útokov, odhaľovať a demonštrovať využívanie technických zraniteľností v oblasti kybernetickej bezpečnosti • Skúšať systémy a prevádzky v súlade s regulačnými normami • Vybrať a vyvinúť vhodné techniky penetračného testovania • Organizovať plány testov a postupy penetračného testovania • Stanoviť postupy analýzy výsledkov penetračného testovania a podávania správ • Dokumentovať a podávať správy o výsledkoch penetračných testov zainteresovaným stranám • Nasadiť nástroje na penetračné testovanie a testovacie programy

Kľúčové zručnosti	• Vyvíjať kódy, skripty a programy • Vykonávať sociálne inžinierstvo • Identifikovať a využívať zraniteľné miesta • Vykonávať etické hackovanie • Myslieť kreatívne a mimo rámca • Identifikovať a riešiť problémy súvisiace s kybernetickou bezpečnosťou • Komunikovať, prezentovať a podávať správy príslušným zainteresovaným stranám • Efektívne používať nástroje penetračného testovania • Vykonávať technickú analýzu a podávanie správ • Rozložiť a analyzovať systémy na identifikáciu nedostatkov a neúčinných kontrol • Preskúmať kódy a posúdiť ich bezpečnosť	
Kľúčové znalosti	• Postupy kyberneticko-bezpečnostných útokov • Zariadenia informačných technológií (IT) a prevádzkových technológií (OT) • Útočné a obranné bezpečnostné postupy • Bezpečnosť operačných systémov • Bezpečnosť počítačových sietí • Postupy penetračného testovania • Normy, metodiky a rámce penetračného testovania • Nástroje na penetračné testovanie • Počítačové programovanie • Zraniteľnosť počítačových systémov • Odporúčania a osvedčené postupy v oblasti kybernetickej bezpečnosti • Certifikácie súvisiace s kybernetickou bezpečnosťou	
e-kompetentnosť (z e-CF)	B.2. Integrácia komponentov B.3. Testovanie B.4. Nasadenie riešenia B.5. Výroba dokumentácie E.3. Riadenie rizík	Úroveň 4 Úroveň 4 Úroveň 2 Úroveň 3 Úroveň 4

3 KNIŽINCA VÝSTUPOV

V zozname výstupov sa uvádzajú niektoré orientačné a praktické príklady výsledkov/výstupov každého profilu rolí. Uvedené výstupy sú ponúkané ako príklady, pretože zoznam nie je úplný, a preto nemusia pokrývať všetky aspekty každého profilu.

Názov profilu	Výstup	Popis
Hlavný úradník pre bezpečnosť informácií (CISO)	Stratégia kybernetickej bezpečnosti	Stratégia kybernetickej bezpečnosti je akčný plán určený na zlepšenie bezpečnosti a odolnosti infraštruktúr a služieb organizácie.
Hlavný úradník pre bezpečnosť informácií (CISO)	Politika kybernetickej bezpečnosti	Pravidlá týkajúce sa zoznamu postupov s cieľom zabezpečiť kybernetickú bezpečnosť organizácie.
Koordinátor reakcie kybernetické incidenty	Plán reakcie na incidenty	Súbor zdokumentovaných postupov, v ktorých sa podrobne uvádzajú kroky, ktoré by sa mali prijať v každej fáze reakcie na incident (príprava, detekcia a analýza, zadržanie, eradikácia a obnova, aktivita po havárii).
Koordinátor reakcie kybernetické incidenty	Správa o kybernetických incidentoch	Správa obsahujúca podrobnosti o jednom alebo viacerých kybernetických incidentoch.
Úradník pre kybernetické právo, politiku a dodržiavanie predpisov	Príručka o dodržiavaní predpisov	Príručka poskytujúca dôkladné pochopenie povinností organizácie týkajúcich sa dodržiavania právnych predpisov. Môže zahŕňať vnútorné politiky alebo postupy na zabezpečenie súladu so zákonmi, inými právnymi predpismi a/alebo normami.
Úradník pre kybernetické právo, politiku a dodržiavanie predpisov	Správa o dodržiavaní predpisov	Správa, v ktorej sa uvádza súčasný stav polohy dodržiavania predpisov organizácie.
Špecialista na spravodajské informácie o kybernetických hrozbách	Príručka pre spravodajstvo o kybernetických hrozbách (alebo manuál)	Manuál predstavujúci nástroje a/alebo metodiky na zhromažďovanie a/alebo spoločné využívanie spravodajských informácií o kybernetických hrozbách.
Špecialista na spravodajské informácie o kybernetických hrozbách	Správa o kybernetických hrozbách	Správa, v ktorej sa identifikujú hlavné hrozby, hlavné trendy pozorované v súvislosti s hrozbami, aktérmi hrozieb a/alebo technikami útoku. Správa môže obsahovať aj príslušné zmierňujúce opatrenia.

Architekt kybernetickej bezpečnosti	Diagram architektúry kybernetickej bezpečnosti	Vizuálne znázornenie architektúry kybernetický-bezpečnostného systému organizácie, ktorá sa používa na ochranu aktív pred kybernetickými útokmi.
Architekt kybernetickej bezpečnosti	Správa o požiadavkách na kybernetickú bezpečnosť	Správa obsahujúca súbor požiadaviek potrebných na zabezpečenie kybernetickej bezpečnosti systému.
Audítor kybernetickej bezpečnosti	Plán auditu kybernetickej bezpečnosti	Plán, ktorý predstavuje celkovú stratégiu a postupy, ktoré bude audítor dodržiavať pri vykonávaní auditu kybernetickej bezpečnosti.
Audítor kybernetickej bezpečnosti	Správa o audite kybernetickej bezpečnosti	Správa, ktorá poskytuje dôkladné pochopenie úrovne bezpečnosti systému a posudzuje jeho silné a slabé stránky v oblasti kybernetickej bezpečnosti. Môže tiež poskytnúť nápravné opatrenia na zlepšenie celkovej kybernetickej bezpečnosti systému.
Pedagóg v oblasti kybernetickej bezpečnosti	Program na zvyšovanie povedomia o kybernetickej bezpečnosti	Program činností na zvýšenie informovanosti v otázkach súvisiacich s kybernetickou bezpečnosťou (napr. prednášky o útokoch a hrozby) pomáhať organizáciám predchádzať súvisiacim rizikám v oblasti kybernetickej bezpečnosti a zmierňovať ich.
Pedagóg v oblasti kybernetickej bezpečnosti	Výcvikový materiál v oblasti kybernetickej bezpečnosti	Materiál poskytujúci vysvetlenie koncepcií, metodík a nástrojov odbornej prípravy alebo zvyšovania úrovne zručností jednotlivcov súvisiacich s kybernetickou bezpečnosťou. Môže zahŕňať príručky pre učiteľov, súbory nástrojov pre študentov a/alebo virtuálne obrázky na podporu rúk na školeniach.
Implementátor pre kybernetickú bezpečnosť	Riešenia kybernetickej bezpečnosti	Riešenia kybernetickej bezpečnosti môžu zahŕňať nástroje a služby, ktorých cieľom je chrániť organizácie pred kybernetickými útokmi.
Výskumník v oblasti kybernetickej bezpečnosti	Publikácia v oblasti kybernetickej bezpečnosti	Akademická publikácia, v ktorej sa uvádzajú zistenia a výsledky výskumu v kontexte kybernetickej bezpečnosti. Účelom publikácie môže byť pokrok v technológii a/alebo vývoj nových inovovaných riešení.
Manažér pre riziká kybernetickej bezpečnosti	Správa o hodnotení rizík kybernetickej bezpečnosti	Správa obsahujúca výsledky identifikácie, analýzy a hodnotenia kybernetickej bezpečnosti rizík systému. Môže zahŕňať aj kontroly na zmiernenie alebo zníženie zistených rizík na prijateľnú úroveň.

Manažér pre riziká kybernetickej bezpečnosti	Akčný plán na nápravu rizík kybernetickej bezpečnosti	Akčný plán obsahujúci zoznam činností súvisiacich s vykonávaním zmierňujúcich opatrení zameraných na zníženie rizík kybernetickej bezpečnosti.
Digitálny forenzný vyšetrovateľ	Výsledky digitálnej forenznej analýzy	Výsledky analýzy digitálnych údajov, ktoré odhaľujú potenciálne dôkazy o škodlivých incidentoch a identifikujú možných aktérov hrozieb.
Digitálny forenzný vyšetrovateľ	Elektronické dôkazy	Potenciálne dôkazy odvodené z údajov obsiahnutých v akomkoľvek zariadení alebo vytvorených týmto zariadením, ktorých fungovanie závisí od softvérového programu alebo údajov uložených alebo prenášaných v počítačovom systéme alebo sieti. (napr. presný zber záznamov)
Penetračný tester	Správa o výsledkoch hodnotenia zraniteľnosti	Správa, v ktorej sa uvádza a posudzuje kritickosť zraniteľností odhalených v systéme počas (zvyčajne automatického) skenovania zraniteľnosti. V správe by sa mohli navrhnúť aj základné nápravné opatrenia.
Penetračný tester	Správa o penetračnom testovaní	Správa poskytujúca podrobnú a komplexnú analýzu zraniteľností systému identifikovaných počas bezpečnostného testovania. Správa by mohla obsahovať aj navrhované nápravné opatrenia.

O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť ENISA je agentúrou Únie, ktorá sa zameriava na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Európe. Agentúra Európskej únie pre kybernetickú bezpečnosť zriadená v roku 2004 a posilnená Aktom EÚ o kybernetickej bezpečnosti prispieva k kybernetickej politike EÚ, zvyšuje dôveryhodnosť produktov, služieb a procesov IKT so systémami certifikácie kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na budúce kybernetické výzvy. Prostredníctvom výmeny poznatkov, budovania kapacít a zvyšovania informovanosti agentúra spolupracuje so svojimi kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v prepojené hospodárstvo, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zabezpečiť digitálnu bezpečnosť európskej spoločnosti a občanov. Viac informácií o agentúre ENISA a jej práci nájdete tu: www.enisa.europa.eu.

ENISA
Agentúra Európskej únie pre kybernetickú bezpečnosť

Aténska kancelária
Agamemnon 14, Chalandri 15231, Attiki, Grécko

Kancelária v Heraklione
95 Nikolaou Plastira 700 13 Vassilika Vouton, Heraklion, Grécko

enisa.europa.eu