EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ECSF

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

EUROPOS KIBERNETINIO SAUGUMO ĮGŪDŽIŲ SISTEMA

2022 M. RUGSĖJIS

APIE ENISA

Europos Sąjungos kibernetinio saugumo agentūra ENISA yra Sąjungos agentūra, kurios tikslas - užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įsteigta 2004 m. ir įtvirtinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų patikimumą naudodama kibernetinio saugumo sertifikavimo sistemas, bendradarbiauja su valstybėmis narėmis bei ES įstaigomis ir padeda Europai pasirengti ateities kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra bendradarbiauja su pagrindinėmis suinteresuotosiomis šalimis, kad sustiprintų pasitikėjimą susietąja ekonomika, padidintų Sąjungos infrastruktūros atsparumą ir galiausiai užtikrintų Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos apie ENISA ir jos veiklą rasite čia:: www.enisa.europa.eu.

KONTAKTAI

Norėdami susisiekti su redaktoriumi, rašykite euskills@enisa.europa.eu.

PADĖKOS

Ši sistema yra parengta remiantis specialiosios darbo grupės įgūdžių sistemai rengti ekspertų 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 ir Jan HAJNY nuomone ir susitarimu.

* Specialiosios darbo grupės Europos kibernetinio saugumo įgūdžių sistemai rengti pranešėjai

TEISINĖ INFORMACIJA

Jei nenurodyta kitaip, šiame leidinyje pateikiama ENISA nuomonė ir interpretacija. Jame nėra įtvirtintos ENISA ar ENISA įstaigų reguliavimo prievolės pagal Reglamentą (ES) Nr. 2019/881.

ENISA turi teisę keisti, atnaujinti arba pašalinti šį leidinį ar bet kurią jo dalį. Jis skirtas tik informavimo tikslais ir turi būti prieinamas nemokamai. Visose nuorodose į jį ar jo naudojimą kaip visumą ar dalį turi būti nurodytas ENISA kaip šaltinis.

Prireikus cituojami trečiųjų šalių šaltiniai. ENISA neatsako ir neprisiima atsakomybės už išorinių šaltinių, įskaitant išorines interneto svetaines, į kurias pateikiamos nuorodos šiame leidinyje, turinį.

Nei ENISA, nei joks jos vardu veikiantis asmuo neatsako už tai, kaip gali būti panaudota šiame leidinyje pateikta informacija.

ENISA išlaiko savo intelektinės nuosavybės teises, susijusias su šiuo leidiniu.

AUTORIŲ TEISIŲ INFORMACIJA

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

TURINYS

1. APŽVALGA

Vyriausiasis informacijos saugumo specialistas

Reagavimo į kibernetinius incidentus specialistas

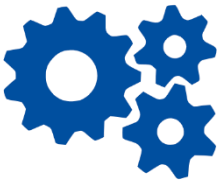
Kibernetinės teisės, politikos ir atitikties specialistas

Kibernetinių grėsmių žvalgybos specialistas

Kibernetinio saugumo architektas

Kibernetinio saugumo auditorius

Kibernetinio saugumo mokytojas



Kibernetinio saugumo diegimo specialistas

Kibernetinio saugumo tyrėjas

Kibernetinio saugumo rizikos vadovas

Skaitmeninės kriminalistikos tyrėjas

Įsiskverbimo testuotojas

2. PROFILIAI

2.1 VYRIAUSIASIS INFORMACIJOS SAUGUMO SPECIALISTAS

Profilio pavadinimas	Vyriausiasis informacijos saugumo specialistas
Kiti pavadinimai	Kibernetinio saugumo programos vadovas Informacijos saugumo pareigūnas (ISO) Informacijos saugumo vadybininkas Informacijos saugumo skyriaus vadovas IT/IRT saugumo specialistas
Santrauka	Vadovauja organizacijos kibernetinio saugumo strategijai ir jos įgyvendinimui, užtikrindamas, kad skaitmeninės sistemos, paslaugos ir turtas būtų tinkamai apsaugoti.
Pareigos	Nustato kibernetinio saugumo viziją, strategiją, taisykles ir procedūras, jas palaiko ir apie jas informuoja. Valdo kibernetinio saugumo taisyklių įgyvendinimą visoje organizacijoje. Užtikrina keitimąsi informacija su išorės institucijomis ir profesinėmis įstaigomis.
Rezultatai	• Kibernetinio saugumo strategija. • Kibernetinio saugumo taisyklės.
Pagrindinės užduotys	• Apibrėžti, įgyvendinti, komunikuoti ir prižiūrėti kibernetinio saugumo tikslus, reikalavimus, strategijas ir taisykles, suderintas su verslo strategija, kad būtų paremti organizacijos tikslai. • Rengti ir pristatyti kibernetinio saugumo viziją, strategijas ir taisykles tvirtinti organizacijos vadovybei ir užtikrinti jų vykdymą. • Prižiūrėti informacijos saugumo valdymo sistemos (ISMS) taikymą ir tobulinimą. • Edukuoti vadovybę apie kibernetinio saugumo riziką, grėsmes ir jų poveikį organizacijai. • Užtikrinti, kad vadovybė pritartų organizacijos kibernetinio saugumo rizikoms • Rengti kibernetinio saugumo planus. • Plėtoti ryšius su kibernetinio saugumo srityje veikiančiomis institucijomis ir bendruomenėmis. • Pranešti vadovybei apie kibernetinio saugumo incidentus, rizikas ir įžvalgas; • Stebėti pažangą kibernetinio saugumo srityje. • Užtikrinti išteklius kibernetinio saugumo strategijai įgyvendinti. • Derėtis su vyresniąja vadovybe dėl kibernetinio saugumo biudžeto. • Užtikrinti organizacijos atsparumą kibernetiniams incidentams. • Valdyti nuolatinį organizacijos gebėjimų stiprinimą. • Peržiūrėti, planuoti ir skirti tinkamus kibernetinio saugumo išteklius.

Pagrindiniai įgūdžiai	• Įvertinti ir sustiprinti organizacijos kibernetinio saugumo būklę. • analizuoti ir įgyvendinti kibernetinio saugumo politiką, sertifikatus, standartus, metodikas ir sistemas. • Analizuoti su kibernetiniu saugumu susijusius įstatymus, reglamentus bei teisės aktus ir jų laikytis. • Įgyvendinti kibernetinio saugumo rekomendacijas ir geriausią patirtį. • valdyti kibernetinio saugumo išteklius. • Kurti kibernetinio saugumo strategiją, ją stiprinti ir vadovauti jos įgyvendinimui. • daryti įtaką organizacijos kibernetinio saugumo kultūrai. • kurti, taikyti, stebėti ir peržiūrėti informacijos saugumo valdymo sistemą (ISMS) tiesiogiai arba vadovaujant jos užsakomiesiems darbams. • Peržiūrėti ir tobulinti saugumo dokumentus, ataskaitas, SLA ir užtikrinti saugumo tikslų įgyvendinimą. • Aptikti ir spręsti su kibernetiniu saugumu susijusias problemas. • Sudaryti kibernetinio saugumo planą. • Bendrauti, koordinuoti ir bendradarbiauti su vidaus ir išorės suinteresuotosiomis šalimis. • Numatyti reikiamus organizacijos informacijos saugumo strategijos pokyčius ir parengti naujus planus. • Apibrėžti ir taikyti kibernetinio saugumo valdymo modelius. • Numatyti kibernetinio saugumo grėsmes, poreikius ir būsimus iššūkius. • Motyvuoti ir skatinti žmones.	
Pagrindinės žinios	• Kibernetinio saugumo taisyklės. • Kibernetinio saugumo standartai, metodikos ir sistemos. • Kibernetinio saugumo rekomendacijos ir geroji patirtis. • Su kibernetiniu saugumu susiję įstatymai, reglamentai ir teisės aktai. • Su kibernetiniu saugumu susiję sertifikatai. • Etiniai kibernetinio saugumo organizavimo reikalavimai. • Kibernetinio saugumo pažangos modeliai. • Kibernetinio saugumo procedūros. • Išteklių valdymas. • Valdymo praktiniai metodai. • Rizikos valdymo standartai, metodai ir sistemos.	
E. gebėjimai (pagal e-CF)	A.7. Technologijų tendencijų stebėsena D.1. Informacijos saugumo strategijos rengimas E.3. Rizikos valdymas E.8. Informacijos saugumo valdymas E.9. IS valdymas	4 lygis 5 lygis 4 lygis 4 lygis 5 lygis

2.2 REAGAVIMO Į KIBERNETINIUS INCIDENTUS SPECIALISTAS

Profilio pavadinimas	Reagavimo į kibernetinius incidentus specialistas
Kiti pavadinimai	Kibernetinių incidentų tvarkytojas Kibernetinių krizių ekspertas Reagavimo į incidentus inžinierius Saugumo operacijų centro (SOC) analitikas Kibernetinis kovotojas (gynėjas) Saugumo operacijų analitikas (SOC analitikas) Kibernetinio saugumo SIEM vadovas
Santrauka	Stebi organizacijos kibernetinio saugumo būklę, sprendžia incidentus kibernetinių atakų metu ir užtikrina nepertraukiamą IRT sistemų veikimą.
Pareigos	Stebi ir vertina sistemų kibernetinio saugumo būklę. Analizuoja, vertina ir mažina kibernetinio saugumo incidentų poveikį. Nustato kibernetinių incidentų pagrindines priežastis ir piktavalius veikėjus. Pagal organizacijos reagavimo į incidentus planą atkuria sistemų ir procesų funkcionalumą iki darbinės būklės, renka įrodymus ir dokumentuoja atliktus veiksmus.
Rezultatai	• Reagavimo į incidentus planas. • Kibernetinio incidento ataskaita.
Pagrindinės užduotys	• Prisidėti prie reagavimo į incidentus plano kūrimo, priežiūros ir vertinimo. • Rengti, įgyvendinti ir vertinti su incidentų nagrinėjimu susijusias procedūras. • Nustatyti, analizuoti, slopinti kibernetinio saugumo incidentus ir apie juos pranešti. • Vertinti ir valdyti techninius pažeidžiamumus. • Vertinti kibernetinio saugumo incidentų aptikimo ir reagavimo į juos veiksmingumą. • Įvertinti kibernetinio saugumo kontrolės priemonių atsparumą ir padarinių mažinimo veiksmus, kurių buvo imtasi po kibernetinio ar duomenų saugumo pažeidimo incidento. • Pritaikyti ir plėtoti incidentų valdymo testavimo metodus. • Nustatyti incidentų rezultatų analizės ir incidentų tvarkymo ataskaitų teikimo procedūras. • Dokumentuoti incidentų rezultatų analizę ir incidentų valdymo veiksmus. • Bendradarbiauti su saugių operacijų centrais (SOC) ir kompiuterių saugumo incidentų reagavimo grupėmis (CSIRT). • Bendradarbiauti su pagrindiniu personalu pranešant apie saugumo incidentus pagal galiojančią teisinę sistemą.
Pagrindiniai įgūdžiai	• Praktiškai taikyti visus techninius, funkcinius ir operacinius kibernetinio saugumo incidentų tvarkymo ir reagavimo į juos aspektus. • Rinkti, analizuoti ir sieti iš įvairių šaltinių gaunamą informaciją apie kibernetines grėsmes. • Dirbti su operacinėmis sistemomis, serveriais, debesimis ir atitinkamomis infrastruktūromis. • Dirbti esant spaudimui. • Bendrauti, pristatyti ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims. • Tvarkyti ir analizuoti žurnalų failus.

Pagrindinės žinios	• Incidentų tvarkymo standartai, metodikos ir sistemos. • Incidentų tvarkymo rekomendacijos ir geroji patirtis. • Incidentų tvarkymo priemonės. • Incidentų valdymo komunikacijos procedūros. • Operacinių sistemų saugumas. • Kompiuterių tinklų saugumas. • Kibernetinės grėsmės. • Kibernetinio saugumo atakų procedūros. • Kompiuterių sistemų pažeidžiamumas. • Su kibernetiniu saugumu susiję sertifikatai. • Su kibernetiniu saugumu susiję įstatymai, reglamentai ir teisės aktai. • Saugių operacijų centrų (SOC) veikimas. • Kompiuterių saugumo incidentų reagavimo grupių (CSIRT) veikla.	
E. gebėjimai (pagal e-CF)	A.7. Technologijų tendencijų stebėsena B.2. Komponentų integravimas B.3. Testavimas B.5. Dokumentų rengimas C.4. Problemų valdymas	3 lygis 2 lygis 3 lygis 3 lygis 4 lygis

2.3 KIBERNETINĖS TEISĖS, POLITIKOS IR ATITIKTIES SPECIALISTAS

Profilio pavadinimas	Kibernetinės teisės, politikos ir atitikties specialistas
Kiti pavadinimai	Duomenų apsaugos pareigūnas (DPO) Privatumo apsaugos pareigūnas Kibernetinės teisės konsultantas Kibernetinės teisės patarėjas Informacijos valdymo pareigūnas Duomenų atitikties pareigūnas Kibernetinio saugumo teisininkas IT/IRT atitikties užtikrinimo vadybininkas Valdymo rizikos atitikties (GRC) konsultantas
Santrauka	Vadovauja su kibernetiniu saugumu susijusių standartų, teisinių ir reguliavimo sistemų laikymuisi, remdamasis organizacijos strategija ir teisiniais reikalavimais.
Pareigos	Prižiūrėti ir užtikrinti, kad būtų laikomasi su kibernetiniu saugumu ir duomenimis susijusių teisinių, reguliavimo sistemų ir taisyklių, atsižvelgiant į organizacijos strategiją ir teisinius reikalavimus. Prisidėti prie organizacijos veiksmų, susijusių su duomenų apsauga. Teikti teisines konsultacijas rengiant organizacijos kibernetinio saugumo valdymo procesus ir rekomenduojamas trūkumų šalinimo strategijas bei sprendimus, kad būtų užtikrinta atitiktis.
Rezultatai	• Atitikties vadovas. • Atitikties ataskaita.
Pagrindinės užduotys	• Užtikrinti, kad būtų laikomasi duomenų privatumo ir duomenų apsaugos standartų, įstatymų ir reglamentų, teikti teisines konsultacijas ir rekomendacijas. • Aptikti ir dokumentuoti atitikties spragas. • Atlikti poveikio privatumui vertinimą ir kurti, palaikyti, informuoti ir mokyti apie privatumo politiką, procedūras. • Įgyvendinti ir propaguoti organizacijos duomenų privatumo ir apsaugos programą. • Užtikrinti, kad duomenų savininkai, turėtojai, valdytojai, tvarkytojai, subjektai, vidaus ar išorės partneriai ir vienetai būtų informuoti apie jų teises, pareigas ir atsakomybę duomenų apsaugos srityje. • Atlikti pagrindinio kontaktinio asmens, atsakančio į užklausas ir skundus dėl duomenų tvarkymo, funkcijas. • Padėti rengti, įgyvendinti, atlikti auditą ir atitikties bandymus, kad būtų užtikrintas kibernetinio saugumo ir privatumo reikalavimų laikymasis. • Stebėti audito ir su duomenų apsauga susijusių mokymų veiklą. • Bendradarbiauti su valdžios institucijomis bei profesinėmis grupėmis ir dalytis su jomis informacija. • Prisidėti prie organizacijos kibernetinio saugumo strategijos, taisyklių ir procedūrų kūrimo. • Rengti ir siūlyti darbuotojų informuotumo didinimo mokymus, kad organizacijoje būtų užtikrinta atitiktis reikalavimams ir puoselėjama duomenų apsaugos kultūra. • Tvarkyti teisinius informacijos saugumo atsakomybės ir santykių su trečiosiomis šalimis aspektus.

Pagrindiniai įgūdžiai	• Visapusiškas verslo strategijos, modelių ir produktų išmanymas bei gebėjimas atsižvelgti į teisinius, reguliavimo ir standartų reikalavimus. • Praktiškai spręsti duomenų apsaugos ir privatumo klausimus, susijusius su organizacinių procesų, finansų ir verslo strategijos įgyvendinimu. • Vadovauti tinkamos kibernetinio saugumo ir privatumo taisyklių ir procedūrų, papildančių verslo poreikius ir teisinius reikalavimus, kūrimui; toliau užtikrinti, kad jos būtų priimtos, suprastos ir įgyvendintos, ir informuoti apie tai dalyvaujančias šalis. • Atlikti, stebėti ir peržiūrėti poveikio privatumui vertinimus, taikant standartus, sistemas, pripažintas metodikas ir priemones. • Aiškinti ir informuoti suinteresuotąsias šalis ir vartotojus duomenų apsaugos ir privatumo temomis. • Suprasti, praktiškai taikyti ir laikytis etikos reikalavimų bei standartų. • Suprasti teisinės sistemos pokyčių poveikį organizacijos kibernetinio saugumo ir duomenų apsaugos strategijai ir nuostatoms. • Bendradarbiauti su kitais komandos nariais ir kolegomis.	
Pagrindinės žinios	• Su kibernetiniu saugumu susiję įstatymai, reglamentai ir teisės aktai. • Kibernetinio saugumo standartai, metodikos ir sistemos. • Kibernetinio saugumo taisyklės. • Teisiniai, reguliavimo ir teisės aktų laikymosi reikalavimai, rekomendacijos ir geroji patirtis. • Poveikio privatumui vertinimo standartai, metodikos ir sistemos.	
E. gebėjimai (pagal e-CF)	A.1. Informacinių sistemų ir verslo strategijos derinimas D.1. Informacijos saugumo strategijos rengimas E.8. Informacijos saugumo valdymas E.9. IS valdymas	4 lygis 4 lygis 3 lygis 4 lygis

2.4 KIBERNETINIŲ GRĖSMIŲ ŽVALGYBOS SPECIALISTAS

Profilio pavadinimas	Kibernetinių grėsmių žvalgybos specialistas
Kiti pavadinimai	Kibernetinės informacijos analitikas Kibernetinių grėsmių modeliuotojas
Santrauka	Renka, apdoroja, analizuoja duomenis ir informaciją, kad parengtų veiksmingas žvalgybos ataskaitas ir išplatintų jas tikslinėms suinteresuotosioms šalims.
Pareigos	Valdo kibernetinių grėsmių žvalgybos ciklą, įskaitant informacijos apie kibernetines grėsmes rinkimą, analizę ir veiksmingos analizės rengimą bei platinimą saugumo suinteresuotosioms šalims ir CTI bendruomenei taktiniu, operatyviniu ir strateginiu lygmenimis. Nustato ir stebi kibernetinių grėsmių sukėlėjų naudojamas taktikas, technikas ir procedūras (TTP) bei jų tendencijas, seka grėsmių sukėlėjų veiklą ir stebi, kaip ne kibernetiniai įvykiai gali daryti įtaką su kibernetinėmis grėsmėmis susijusiems veiksmams.
Rezultatai	• Kibernetinių grėsmių žvalgybos vadovas. • Kibernetinių grėsmių ataskaita.
Pagrindinės užduotys	• Parengti, įgyvendinti ir valdyti organizacijos kibernetinių grėsmių žvalgybos strategiją. • Parengti grėsmių žvalgybos valdymo planus ir procedūras. • Verslo reikalavimus paversti žvalgybos reikalavimais. • Įgyvendinti informacijos apie grėsmes rinkimą, analizę, rengti naudingą žvalgybos informaciją ir ją skleisti saugumu suinteresuotosioms šalims. • Nustatyti ir įvertinti kibernetinių grėsmių sukėlėjus, nukreiptus prieš organizaciją. • Nustatyti, stebėti ir vertinti kibernetinių grėsmių subjektų naudojamas taktikas, technikas ir procedūras (TTP), analizuojant atviruosius ir nuosavybinius duomenis, informaciją ir analitinius duomenis. • Rengti veiksmingas ataskaitas, pagrįstas grėsmių žvalgybos duomenimis. • Rengti taktinio, operatyvinio ir strateginio lygmens grėsmių mažinimo planus ir dėl jų konsultuoti. • Koordinuoti veiksmus su suinteresuotosiomis šalimis, kad būtų dalijamasi informacija apie atitinkamas kibernetines grėsmes. • Pasitelkti žvalgybos duomenis grėsmėms modeliuoti, rekomendacijoms dėl rizikos mažinimo teikti ir kibernetinėms grėsmėms aptikti. • Atvirai ir viešai informuoti apie žvalgybinę informaciją visais lygmenimis. • Perteikti deramą saugumo svarbą, paaiškinant rizikos poveikį ir jos pasekmes suinteresuotiesiems asmenims, kurie nėra techninės srities specialistai.
Pagrindiniai įgūdžiai	• Bendradarbiauti su kitais komandos nariais ir kolegomis. • Rinkti, analizuoti ir susieti iš įvairių šaltinių gaunamą informaciją apie kibernetines grėsmes. • Identifikuoti grėsmių sukėlėjų veikimo būdus (TTP) ir akcijas. • Automatizuoti grėsmių žvalgybos informacijos valdymo procedūras. • Atlikti techninę analizę ir teikti ataskaitas. • Identifikuoti nekibernetinius įvykius, turinčius įtakos kibernetinei veiklai. • Modeliuoti grėsmes, jų vykdytojus ir veikimo būdus. • Bendrauti, koordinuoti ir bendradarbiauti su vidaus ir išorės suinteresuotosiomis šalimis. • Bendrauti, informuoti ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims. • Naudoti ir taikyti kibernetinio bendradarbiavimo platformas ir priemones.

Pagrindinės žinios	• Operacinių sistemų saugumas. • Kompiuterių tinklų saugumas. • Kibernetinio saugumo kontrolė ir sprendimai. • Kompiuterių programavimas. • Kibernetinių grėsmių žvalgybos (CTI) dalinimosi standartai, metodikos ir sistemos. • Atsakingo informacijos atskleidimo procedūros. • Su kibernetiniu saugumu susijusios tarpdalykinės ir paribio sričių žinios. • Kibernetinės grėsmės. • Kibernetinių grėsmių sukėlėjai. • Kibernetinio saugumo atakų procedūros. • Išplėstinės ir nuolatinės kibernetinės grėsmės (APT). • Grėsmių sukėlėjų taktikos, technikos ir procedūros (TTP). • Su kibernetiniu saugumu susiję sertifikatai.	
E. gebėjimai (pagal e-CF)	B.5. Dokumentų rengimas D.7. Duomenų mokslas ir analizė D.10. Informacijos ir žinių valdymas E.4. Santykių valdymas E.8. Informacijos saugumo valdymas	3 lygis 4 lygis 4 lygis 3 lygis 4 lygis

2.5 KIBERNETINIO SAUGUMO ARCHITEKTAS

Profilio pavadinimas	Kibernetinio saugumo architektas
Kiti pavadinimai	Kibernetinio saugumo sprendimų architektas Kibernetinio saugumo dizaineris Duomenų saugumo architektas
Santrauka	Planuoja ir projektuoja saugumo sprendimus (infrastruktūros, sistemų, turto, programinės įrangos, techninės įrangos ir paslaugų) bei kibernetinio saugumo kontrolės priemones.
Pareigos	Projektuoti sprendimus, pagrįstus projektinio saugumo ir privatumo užtikrinimo principais. Kurti ir nuolat tobulinti architektūros modelius, rengti atitinkamus architektūros dokumentus ir specifikacijas. Koordinuoti saugų kibernetinio saugumo komponentų kūrimą, integravimą ir priežiūrą pagal standartus ir kitus susijusius reikalavimus.
Rezultatai	• Kibernetinio saugumo architektūros schema. • Kibernetinio saugumo reikalavimų ataskaita.
Pagrindinės užduotys	• Parengti ir pasiūlyti saugią architektūrą organizacijos strategijai įgyvendinti. • Parengti organizacijos kibernetinio saugumo architektūrą, kuri užtikrintų saugumo ir privatumo reikalavimus. • Rengti architektūros dokumentus ir specifikacijas. • Suinteresuotosioms šalims pristatyti aukšto lygio saugumo architektūros projektą. • Užtikrinti saugią aplinką sistemų, paslaugų ir produktų kūrimo ciklo metu. • Koordinuoti kibernetinio saugumo komponentų kūrimą, integravimą ir priežiūrą, kad būtų laikomasi kibernetinio saugumo specifikacijų. • Analizuoti ir vertinti organizacijos architektūros kibernetinį saugumą. • Užtikrinti sprendimų architektūros saugumą atliekant saugumo patikrinimus ir sertifikavimą. • Bendradarbiauti su kitomis komandomis ir kolegomis. • Vertinti kibernetinio saugumo sprendimų poveikį organizacijos architektūros sandarai ir efektyvumui. • Pritaikyti organizacijos architektūrą atsižvelgiant į kylančias grėsmes. • Įvertinti įgyvendintą architektūrą, kad būtų išlaikytas tinkamas saugumo lygis.
Pagrindiniai įgūdžiai	• Atlikti vartotojų ir verslo saugumo reikalavimų analizę. • Rengti kibernetinio saugumo architektūrines ir funkcines specifikacijas. • Išskaidyti ir analizuoti sistemas, kad būtų parengti saugumo ir privatumo reikalavimai ir nustatyti veiksmingi sprendimai. • Projektuoti sistemas ir architektūras, remiantis saugumo ir privatumo užtikrinimo projektuojant ir numatytaisiais kibernetinio saugumo principais. • Vadovauti ir bendrauti su vykdytojais ir IT bei kitų sričių darbuotojais. • Bendrauti, supažindinti ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims. • Siūlyti kibernetinio saugumo architektūras, atsižvelgiant į suinteresuotųjų šalių poreikius ir biudžetą. • Parinkti tinkamas specifikacijas, procedūras ir kontrolės priemones. • Užtikrinti architektūros atsparumą gedimų židiniams. • Koordinuoti saugumo sprendimų integravimą.

Pagrindinės žinios	• Su kibernetiniu saugumu susiję sertifikatai. • Kibernetinio saugumo rekomendacijos ir geroji patirtis. • Kibernetinio saugumo standartai, metodikos ir sistemos. • Su kibernetiniu saugumu susijusių reikalavimų analizė. • Saugus plėtros gyvavimo ciklas. • Saugumo architektūros etaloniniai modeliai. • Su kibernetiniu saugumu susijusios technologijos. • Kibernetinio saugumo kontrolės priemonės ir sprendimai. • Kibernetinio saugumo rizika. • Kibernetinės grėsmės. • Kibernetinio saugumo tendencijos. • Teisiniai, reguliavimo ir teisės aktų laikymosi reikalavimai, rekomendacijos ir geroji patirtis. • Anksčiau taikytos kibernetinio saugumo procedūros • Privatumo stiprinimo technologijos (PET). • Privatumo užtikrinimo projektuojant standartai, metodikos ir sistemos.	
E. gebėjimai (pagal e-CF)	A.5. Architektūros projektavimas A.6. Taikomosios programos kūrimas B.1. Programos kūrimas B.3. Testavimas B.6. IRT sistemų inžinerija	5 lygis 3 lygis 3 lygis 3 lygis 4 lygis

2.6 KIBERNETINIO SAUGUMO AUDITORIUS

Profilio pavadinimas	Kibernetinio saugumo auditorius
Kiti pavadinimai	Informacijos saugumo auditorius (IT arba teisės auditorius) Valdymo rizikos atitikties (GRC) auditorius Kibernetinio saugumo audito vadovas Kibernetinio saugumo procedūrų ir procesų auditorius Informacijos saugumo rizikos ir atitikties auditorius Duomenų apsaugos vertinimo analitikas
Santrauka	Atlieka organizacijos ekosistemos kibernetinio saugumo auditą. Užtikrina atitiktį teisės aktų, reguliavimo, politikos informacijos, saugumo reikalavimų, pramonės standartų ir geriausios patirties reikalavimams.
Pareigos	Atlieka nepriklausomus patikrinimus, kad įvertintų procesų ir kontrolės priemonių veiksmingumą bei bendrą organizacijos teisinės ir reguliavimo sistemos nuostatų laikymąsi. Vertina, testuoja ir tikrina su kibernetiniu saugumu susijusius produktus (sistemas, techninę ir programinę įrangą bei paslaugas), funkcijas ir taisykles, užtikrindamas jų atitiktį gairėms, standartams ir nuostatoms.
Rezultatai	• Kibernetinio saugumo audito planas. • Kibernetinio saugumo audito ataskaita.
Pagrindinės užduotys	• Rengti organizacijos audito nuostatas, procedūras, standartus ir gaires. • Parengti sistemų audito metodikas ir praktiką. • Sukurti tikslinę aplinką ir valdyti audito veiklą. • Apibrėžti audito apimtį, tikslus ir kriterijus, pagal kuriuos bus atliekamas auditas. • Parengti audito planą, kuriame būtų aprašytos sistemos, standartai, metodika, procedūros ir audito testai. • Remiantis rizikos profiliu, patikrinti vertinimo objektą, saugumo tikslus ir reikalavimus. • Atlikti su kibernetiniu saugumu susijusių taikomų įstatymų ir kitų teisės aktų laikymosi auditą. • Atlikti su kibernetiniu saugumu susijusių taikomų standartų laikymosi auditą. • Vykdyti audito planą ir rinkti įrodymus bei vertinimus. • Prižiūrėti ir saugoti audito įrašų vientisumą. • Rengti ir teikti atitikties vertinimo, užtikrinimo, audito, sertifikavimo ir priežiūros ataskaitas. • Stebėti rizikos mažinimo veiksmus.
Pagrindiniai įgūdžiai	• Sistemingai ir planingai veikti ir dirbti remiantis įrodymais. • Vadovautis audito sistemomis, standartais ir metodikomis ir praktiškai jas taikyti. • Taikyti audito priemones ir metodus. • Analizuoti verslo procesus, vertinti ir peržiūrėti programinės ar techninės įrangos saugumą, taip pat technines ir organizacines kontrolės priemones. • Suskirstyti ir analizuoti sistemas, siekiant nustatyti trūkumus ir neveiksmingas kontrolės priemones. • Bendrauti, paaiškinti ir priderinti teisinius ir reguliavimo reikalavimus bei verslo poreikius. • Rinkti, vertinti, prižiūrėti ir saugoti audito informaciją. • Atlikti sąžiningą, nešališką ir nepriklausomą auditą.

Pagrindinės žinios	• Kibernetinio saugumo kontrolės priemonės ir sprendimai. • Teisiniai, reguliavimo ir teisės aktų laikymosi reikalavimai, rekomendacijos ir geroji patirtis. • Kibernetinio saugumo kontrolės priemonių veiksmingumo stebėjimas, testavimas ir vertinimas. • Atitikties vertinimo standartai, metodikos ir sistemos. • Audito standartai, metodikos ir sistemos. • Kibernetinio saugumo standartai, metodikos ir sistemos. • Su auditu susijęs sertifikavimas. • Su kibernetiniu saugumu susijęs sertifikavimas.	
E. gebėjimai (pagal e-CF)	B.3. Testavimas B.5. Dokumentų rengimas E.3. Rizikos valdymas E.6 IRT kokybės valdymas E.8. Informacijos saugumo valdymas	4 lygis 3 lygis 4 lygis 4 lygis 4 lygis

2.7 KIBERNETINIO SAUGUMO MOKYTOJAS

Profilio pavadinimas	Kibernetinio saugumo mokytojas
Kiti pavadinimai	Kibernetinio saugumo informuotumo specialistas Kibernetinio saugumo instruktorius Kibernetinio saugumo dėstytojas (profesorius, lektorius)
Santrauka	Tobulina asmenų kibernetinio saugumo žinias, įgūdžius ir kompetencijas.
Pareigos	Kurti, rengti ir vykdyti informuotumo didinimo, mokymo ir švietimo programas kibernetinio saugumo ir duomenų apsaugos temomis. Taikyti tinkamus mokymo ir mokymo metodus, būdus ir priemones, skirtas žmogiškųjų išteklių kibernetinio saugumo kultūrai, gebėjimams, žinioms ir įgūdžiams perteikti ir tobulinti. Populiarinti kibernetinio saugumo svarbą ir įtvirtinti jį organizacijoje.
Rezultatai	• Kibernetinio saugumo informuotumo programa. • Kibernetinio saugumo mokymo medžiaga.
Pagrindinės užduotys	• Kurti, atnaujinti ir teikti kibernetinio saugumo ir duomenų apsaugos mokymo programas ir mokomąją medžiagą, skirtą mokymams ir sąmoningumui ugdyti, vadovaujantis turiniu, metodais, priemonėmis ir mokinių poreikiais. • Organizuoti, rengti ir vykdyti kibernetinio saugumo ir duomenų apsaugos informuotumo didinimo veiklą, seminarus, kursus, praktinius mokymus. • Stebėti, vertinti ir teikti ataskaitas apie mokymo veiksmingumą. • Vertinti ir teikti ataskaitas apie mokymų dalyvių veiklos rezultatus. • Ieškoti naujų švietimo, mokymo ir informuotumo didinimo metodų. • Projektuoti, kurti ir vykdyti kibernetinio saugumo modeliavimo programas, virtualias laboratorijas ar kibernetinių bandymų aplinkas. • Teikti rekomendacijas dėl kibernetinio saugumo sertifikavimo programų asmenims • Nuolat prižiūrėti ir tobulinti kompetenciją; skatinti ir suteikti galimybę nuolat tobulinti kibernetinio saugumo gebėjimus ir kurti naujus įgūdžius.
Pagrindiniai įgūdžiai	• Nustatyti kibernetinio saugumo informuotumo, mokymo ir švietimo poreikius. • Kurti, tobulinti ir vykdyti mokymosi programas, skirtas kibernetinio saugumo poreikiams patenkinti. • Rengti kibernetinio saugumo pratybas, įskaitant modeliavimą kibernetinių bandymų aplinkoje. • Rengti mokymus, skirtus kibernetinio saugumo ir duomenų apsaugos specialistų sertifikatams gauti. • Naudoti esamus su kibernetiniu saugumu susijusius mokymo išteklius. • Rengti informuotumo didinimo, mokymo ir švietimo veiklos vertinimo programas. • Bendrauti, teikti informaciją ir ataskaitas atitinkamoms suinteresuotosioms šalims. • Apibrėžti ir parinkti pedagoginius metodus, tinkamus tikslinei auditorijai. • Motyvuoti ir skatinti žmones.

Pagrindinės žinios	• Pedagoginiai standartai, metodikos ir sistemos. • Kibernetinio saugumo informuotumo, švietimo ir mokymo programų rengimas. • Su kibernetiniu saugumu susiję sertifikatai. • Kibernetinio saugumo švietimo ir mokymo standartai, metodikos ir sistemos. • Su kibernetiniu saugumu susiję įstatymai, reglamentai ir teisės aktai. • Kibernetinio saugumo rekomendacijos ir geroji patirtis. • Kibernetinio saugumo standartai, metodikos ir sistemos. • Kibernetinio saugumo kontrolės priemonės ir sprendimai.	
E. gebėjimai (pagal e-CF)	D.3. Švietimo ir mokymo teikimas D.9. Personalo ugdymas E.8. Informacijos saugumo valdymas	3 lygis 3 lygis 3 lygis

2.8 KIBERNETINIO SAUGUMO DIEGIMO SPECIALISTAS

Profilio pavadinimas	Kibernetinio saugumo diegimo specialistas
Kiti pavadinimai	Informacijos saugumo diegimo specialistas Kibernetinio saugumo sprendimų ekspertas Kibernetinio saugumo plėtros specialistas Kibernetinio saugumo inžinierius Plėtros, saugumo ir operacijų (*DevSecOps*) inžinierius
Santrauka	Kurti, diegti ir eksploatuoti kibernetinio saugumo sprendimus (sistemas, išteklius, programinę įrangą, kontrolės priemones ir paslaugas) infrastruktūroje ir produktų srityse.
Pareigos	Užtikrina su kibernetiniu saugumu susijusį techninį kibernetinio saugumo sprendimų kūrimą, integravimą, testavimą, įgyvendinimą, eksploatavimą, priežiūrą, stebėseną ir palaikymą. Rūpinasi, kad būtų laikomasi specifikacijų ir atitikties reikalavimų, užtikrina tinkamą veikimą ir sprendžia technines problemas, susijusias su organizacijos kibernetinio saugumo sprendimais (sistemomis, ištekliais, programine įranga, kontrole ir paslaugomis), infrastruktūra ir produktais.
Rezultatai	• Kibernetinio saugumo sprendimai
Pagrindinės užduotys	• Kibernetinio saugumo produktų kūrimas, diegimas, priežiūra, atnaujinimas, testavimas. • Teikti su kibernetiniu saugumu susijusią pagalbą vartotojams ir klientams. • Įdiegti kibernetinio saugumo sprendimus ir užtikrinti patikimą jų veikimą. • Saugiai konfigūruoti sistemas, paslaugas ir produktus. • Prižiūrėti ir atnaujinti sistemų, paslaugų ir produktų saugumą. • Įgyvendinti kibernetinio saugumo procedūras ir kontrolės priemones. • Stebėti ir užtikrinti įdiegtų kibernetinio saugumo kontrolės priemonių veikimą. • Dokumentuoti ir teikti ataskaitas apie sistemų, paslaugų ir produktų saugumą. • Glaudžiai bendradarbiauti su IT ir operacinių technologijų darbuotojais vykdant su kibernetiniu saugumu susijusius veiksmus. • Diegti, taikyti ir tvarkyti produktų pataisas, kad būtų pašalinti techniniai pažeidžiamumai.
Pagrindiniai įgūdžiai	• Bendrauti, pateikti informaciją ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims. • Integruoti kibernetinio saugumo sprendimus į organizacijos infrastruktūrą. • Konfigūruoti sprendimus pagal organizacijos saugumo nuostatus. • Vertinti sprendimų saugumą ir veikimą. • Kurti programinį kodą, scenarijus ir programas. • Nustatyti ir spręsti su kibernetiniu saugumu susijusias problemas. • Bendradarbiauti su kitais komandos nariais ir kolegomis.
Pagrindinės žinios	• Saugus kūrimo ciklas. • Kompiuterių programavimas. • Operacinių sistemų saugumas. • Kompiuterių tinklų saugumas. • Kibernetinio saugumo kontrolės priemonės ir sprendimai. • Puolamoji ir gynybinė saugumo praktika. • Saugaus programavimo rekomendacijos ir geriausios praktikos pavyzdžiai. • Kibernetinio saugumo rekomendacijos ir geroji patirtis. • Testavimo standartai, metodikos ir sistemos. • Testavimo procedūros. • Su kibernetiniu saugumu susijusios technologijos.

E. gebėjimai (pagal e-CF)	A.5. Architektūros projektavimas A.6. Taikomosios programos projektavimas B.1. Taikomosios programos kūrimas B.3. Testavimas B.6. IRT sistemų inžinerija	3 lygis 3 lygis 3 lygis 3 lygis 4 lygis

2.9 KIBERNETINIO SAUGUMO TYRĖJAS

Profilio pavadinimas	Kibernetinio saugumo tyrėjas
Kiti pavadinimai	Kibernetinio saugumo tyrimų inžinierius Kibernetinio saugumo vyriausiasis tyrimų specialistas Kibernetinio saugumo vyresnysis tyrimų specialistas Kibernetinio saugumo tyrimų ir plėtros specialistas Kibernetinio saugumo srities mokslo darbuotojas Kibernetinio saugumo tyrimų ir inovacijų specialistas ar ekspertas Kibernetinio saugumo mokslinis bendradarbis
Santrauka	Atlieka kibernetinio saugumo srities tyrimus ir jų rezultatus pritaiko kibernetinio saugumo sprendimuose.
Pareigos	Vykdyti fundamentinius (pagrindinius) ir taikomuosius tyrimus bei skatinti inovacijas kibernetinio saugumo srityje bendradarbiaujant su kitomis suinteresuotosiomis šalimis. Analizuoti kibernetinio saugumo srities tendencijas ir mokslinius pasiekimus.
Rezultatai	• Publikacijos kibernetinio saugumo srityje
Pagrindinės užduotys	• Analizuoti ir vertinti kibernetinio saugumo technologijas, sprendimus, pokyčius ir procesus. • Atlikti mokslinius tyrimus, inovacijas ir plėtrą su kibernetiniu saugumu susijusiomis temomis. • Kelti ir plėtoti tyrimų ir inovacijų idėjas. • Plėtoti naujausius pasiekimus kibernetinio saugumo temomis. • Padėti kurti naujoviškus su kibernetiniu saugumu susijusius sprendimus. • Atlikti eksperimentus ir tikrinti kibernetinio saugumo sprendimų koncepcijas, kurti bandomuosius projektus ir prototipus. • Parinkti ir taikyti sistemas, metodus, standartus, priemones ir protokolus, įskaitant koncepcijos sukūrimą ir išbandymą, siekiant užtikrinti projektų palaikymą. • Prisidėti prie pažangiausių kibernetinio saugumo verslo idėjų, paslaugų ir sprendimų kūrimo. • Padėti ugdyti su kibernetiniu saugumu susijusius gebėjimus, įskaitant informuotumą, teorinį mokymą, praktinį mokymą, testavimą, mentorystę, priežiūrą ir dalijimąsi informacija. • Identifikuoti tarpsektorinius kibernetinio saugumo pasiekimus ir pritaikyti juos kitame kontekste arba siūlyti novatoriškus metodus ir sprendimus. • Vadovauti inovacijų procesams ir projektams arba juose dalyvauti, įskaitant projektų valdymą ir biudžeto sudarymą. • Skelbti ir pristatyti mokslinius darbus, mokslinių tyrimų ir plėtros rezultatus.
Pagrindiniai įgūdžiai	• Kelti naujas idėjas ir pritaikyti teoriją praktikoje. • Suskirstyti ir analizuoti sistemas, siekiant nustatyti trūkumus ir neveiksmingas kontrolės priemones. • Skaidyti ir analizuoti sistemas, siekiant nustatyti saugumo ir privatumo reikalavimus ir rasti veiksmingus sprendimus. • Stebėti naujus su kibernetiniu saugumu susijusių technologijų pasiekimus. • Bendrauti, pristatyti ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims. • Atpažinti ir spręsti su kibernetiniu saugumu susijusias problemas. • Bendradarbiauti su kitais komandos nariais ir kolegomis.

Pagrindinės žinios	• Su kibernetiniu saugumu susiję moksliniai tyrimai, plėtra ir inovacijos. • Kibernetinio saugumo standartai, metodikos ir sistemos. • Teisiniai, reguliavimo ir teisiniai reikalavimai, taikomi su kibernetiniu saugumu. susijusių technologijų diegimui ar naudojimui. • Daugiadalykis kibernetinio saugumo požiūris. • Atsakingo informacijos atskleidimo procedūros.	
E. gebėjimai (pagal e-CF)	A.7. Technologijų tendencijų stebėsena A.9. Naujovių diegimas D.7. Duomenų mokslas ir analizė C.4. Problemų valdymas D.10. Informacijos ir žinių valdymas	5 lygis 5 lygis 4 lygis 3 lygis 3 lygis

2.10 KIBERNETINIO SAUGUMO RIZIKOS VADOVAS

Profilio pavadinimas	Kibernetinio saugumo rizikos vadovas
Kiti pavadinimai	Informacijos saugumo rizikos analitikas Kibernetinio saugumo rizikos užtikrinimo konsultantas Kibernetinio saugumo rizikos vertintojas Kibernetinio saugumo poveikio analitikas Kibernetinės rizikos vadovas
Santrauka	Valdo su kibernetiniu saugumu susijusią organizacijos riziką, atsižvelgiant į organizacijos strategiją. Rengia, prižiūri ir informuoja apie rizikos valdymo procesus ir ataskaitas.
Pareigos	Nepertraukiamai valdo (nustato, analizuoja, vertina, įvertina, mažina) su kibernetiniu saugumu susijusią IRT infrastruktūrų, sistemų ir paslaugų riziką, planuodamas, taikydamas, pranešdamas ir informuodamas apie rizikos analizę, vertinimą ir gydymą. Nustato organizacijos rizikos valdymo strategiją ir užtikrina, kad rizika išliktų organizacijai priimtino lygio, parinkdamas rizikos mažinimo veiksmus ir kontrolės priemones.
Rezultatai	• Kibernetinio saugumo rizikos vertinimo ataskaita. • Kibernetinio saugumo rizikos šalinimo veiksmų planas.
Pagrindinės užduotys	• Parengti organizacijos kibernetinio saugumo rizikos valdymo strategiją • Valdyti organizacijos tinklo išteklių apskaitą • Nustatyti ir įvertinti su kibernetiniu saugumu susijusias grėsmes ir IRT sistemų pažeidžiamumą • Nustatyti grėsmių aplinką, įskaitant užpuolikų profilius ir atakų potencialo įvertinimą • Įvertinti kibernetinio saugumo riziką ir pasiūlyti tinkamiausias rizikos valdymo galimybes, įskaitant saugumo kontrolės priemones ir rizikos mažinimą bei išvengimą, kurios geriausiai atitiktų organizacijos strategiją • Stebėti kibernetinio saugumo kontrolės priemonių veiksmingumą ir rizikos lygius • Užtikrinti, kad visa kibernetinio saugumo rizika ir toliau būtų priimtino lygio organizacijos išteklių atžvilgiu. • Sukurti, prižiūrėti, teikti ataskaitas ir informuoti apie visą rizikos valdymo ciklą
Pagrindiniai įgūdžiai	• Diegti kibernetinio saugumo rizikos valdymo sistemas, metodikas ir rekomendacijas bei užtikrinti atitiktį reglamentams ir standartams. • Analizuoti ir apjungti organizacijos kokybės ir rizikos valdymo patirtis. • Sudaryti sąlygas verslo išteklių savininkams, vadovams ir kitiems suinteresuotiesiems subjektams priimti su rizika susijusius sprendimus, kad būtų galima ją tinkamai valdyti ir sumažinti. • Kurti kibernetinio saugumo riziką suvokiančią aplinką. • Bendrauti, pristatyti ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims • Siūlyti ir valdyti rizikos pasidalijimo galimybes.

Pagrindinės žinios	• Rizikos valdymo standartai, metodikos ir sistemos. • Rizikos valdymo priemonės. • Rizikos valdymo rekomendacijos ir geriausia patirtis. • Kibernetinės grėsmės. • Kompiuterių sistemų pažeidžiamumas. • Kibernetinio saugumo kontrolės priemonės ir sprendimai. • Kibernetinio saugumo rizika. • Kibernetinio saugumo kontrolės priemonių veiksmingumo stebėjimas, testavimas ir vertinimas. • Su kibernetiniu saugumu susiję sertifikatai. • Su kibernetiniu saugumu susijusios technologijos.	
E. gebėjimai (pagal e-CF)	E.3. Rizikos valdymas E.5. Procesų tobulinimas E.7. Verslo pokyčių valdymas E.9. IS valdymas	4 lygis 3 lygis 4 lygis 4 lygis

2.11 SKAITMENINĖS KRIMINALISTIKOS TYRĖJAS

Profilio pavadinimas	Skaitmeninės kriminalistikos tyrėjas	
Kiti pavadinimai	Skaitmeninės kriminalistikos analitikas Kibernetinio saugumo ir teismo ekspertizės specialistas Kompiuterinės kriminalistikos konsultantas	
Santrauka	Užtikrina, kad kibernetinių nusikaltimų tyrimo metu būtų atskleisti visi skaitmeniniai įrodymai, patvirtinantys kenkėjišką veiklą.	
Pareigos	Susieja radinius su fiziniais asmenimis, fiksuoja, atkuria, identifikuoja ir išsaugo duomenis, įskaitant tiriamų skaitmeninių sistemų būsenas, įvestis, išvestis ir procesus. Remdamasis kokybiniais duomenimis, atlieka skaitmeninių įrodymų analizę, rekonstrukciją ir interpretaciją. Pateikia nešališką kokybinį vertinimą, neinterpretuodamas gautų išvadų.	
Rezultatai	• Skaitmeninės kriminalistikos analizės rezultatai. • Elektroniniai įrodymai.	
Pagrindinės užduotys	• Skaitmeninės kriminalistikos tyrimų nuostatų, planų ir procedūrų kūrimas. • Nustatyti, atkurti, išgauti, dokumentuoti ir analizuoti skaitmeninius įrodymus. • Išsaugoti ir apsaugoti skaitmeninius įrodymus ir suteikti galimybę jais naudotis įgaliotoms suinteresuotosioms šalims. • Tikrinti aplinką ieškant neleistinų ir neteisėtų veiksmų įrodymų. • Sistemingai ir planingai dokumentuoti, pranešti ir pateikti skaitmeninės kriminalistinės analizės išvadas ir rezultatus. • Parinkti ir pritaikyti kriminalistikos testavimo, analizės ir ataskaitų rengimo metodus.	
Pagrindiniai įgūdžiai	• Dirbti etiškai ir nepriklausomai; nedaryti įtakos ir nebūti šališkam vidaus ar išorės veikėjams. • Rinkti informaciją išsaugant jos vientisumą. • Nustatyti, analizuoti ir susieti kibernetinio saugumo įvykius. • Paaiškinti ir pateikti skaitmeninius įrodymus paprastai, aiškiai ir suprantamai. • Rengti ir perduoti išsamias ir pagrįstas tyrimo ataskaitas.	
Pagrindinės žinios	• Skaitmeninės kriminalistikos rekomendacijos ir geroji patirtis. • Skaitmeninės kriminalistikos standartai, metodikos ir sistemos. • Skaitmeninės kriminalistikos analizės procedūros. • Testavimo procedūros. • Kriminalinės žvalgybos procedūros, standartai, metodikos ir sistemos. • Su kibernetiniu saugumu susiję įstatymai, reglamentai ir teisės aktai. • Kenkėjiškų programų analizės priemonės. • Kibernetinės grėsmės. • Kompiuterių sistemų pažeidžiamumas. • Kibernetinio saugumo atakų procedūros. • Operacinių sistemų saugumas. • Kompiuterių tinklų saugumas. • Su kibernetiniu saugumu susiję sertifikatai.	
E. gebėjimai (pagal e-CF)	A.7. Technologijų tendencijų stebėsena B.3. Testavimas B.5. Dokumentų rengimas E.3. Rizikos valdymas	3 lygis 4 lygis 3 lygis 3 lygis

2.12 ĮSISKVERBIMO TESTUOTOJAS

Profilio pavadinimas	Įsiskverbimo testuotojas
Kiti pavadinimai	„Pentester“ Etinis programišius Pažeidžiamumų analitikas Kibernetinio saugumo testuotojas Kibernetinio saugumo ekspertas Gynybinio kibernetinio saugumo ekspertas „Raudonosios komandos“ ekspertas „Raudonosios komandos“ narys
Santrauka	Vertina saugumo kontrolės priemonių veiksmingumą, atskleidžia ir pritaiko kibernetinio saugumo spragas, įvertindami jų kritinę reikšmę, jei jomis pasinaudotų grėsmių sukėlėjai.
Pareigos	Planuoti, projektuoti, įgyvendinti ir vykdyti įsiskverbimo testavimo veiklą ir atakų scenarijus, kad būtų įvertintas įdiegtų ar planuojamų saugumo priemonių veiksmingumas. Nustato techninių ir organizacinių kontrolės priemonių pažeidžiamumą ar trūkumus, kurie turi įtakos IRT produktų (pvz., sistemų, techninės ir programinės įrangos bei paslaugų) slapumui, vientisumui ir prieinamumui.
Rezultatai	• Pažeidžiamumo vertinimo rezultatų ataskaita. • Įsilaužimo bandymų ataskaita.
Pagrindinės užduotys	• Nustatyti, analizuoti ir vertinti technines ir organizacines kibernetinio saugumo spragas. • Nustatyti atakų vektorius, atskleisti ir pademonstruoti techninių kibernetinio saugumo spragų panaudojimą • Testuoti sistemų ir operacijų atitiktį reglamentuojantiems standartams. • Parinkti ir sukurti tinkamus įsiskverbimo testavimo metodus. • Organizuoti įsiskverbimo testavimo planus ir procedūras. • Nustatyti įsiskverbimo testavimo rezultatų analizės ir ataskaitų teikimo procedūras. • Dokumentuoti įsiskverbimo testavimo rezultatus ir pranešti apie juos suinteresuotosioms šalims. • Diegti įsiskverbimo testavimo priemones ir testavimo programas.
Pagrindiniai įgūdžiai	• Kurti programinį kodą, scenarijus ir programas. • Taikyti socialinę inžineriją. • Nustatyti ir išnaudoti pažeidžiamumus. • Atlikti etišką įsilaužimą. • Kūrybiškai ir nestandartiškai mąstyti. • Aptikti ir spręsti su kibernetiniu saugumu susijusias problemas. • Bendrauti, pateikti informaciją ir teikti ataskaitas atitinkamoms suinteresuotosioms šalims. • Veiksmingai naudoti įsiskverbimo testavimo priemones. • Atlikti techninę analizę ir teikti ataskaitas. • Išskaidyti ir analizuoti sistemas, siekiant nustatyti trūkumus ir neveiksmingas kontrolės priemones. • Peržiūrėti programų kodus, įvertinti jų saugumą.

Pagrindinės žinios	• Kibernetinio saugumo atakų procedūros. • Informacinių technologijų (IT) ir operacinių technologijų (OT) įrenginiai. • Puolamojo ir gynybinio saugumo procedūros. • Operacinių sistemų saugumas. • Kompiuterių tinklų saugumas. • Įsiskverbimo testavimo procedūros. • Įsiskverbimo testavimo standartai, metodikos ir sistemos. • Įsiskverbimo testavimo priemonės. • Kompiuterių programavimas. • Kompiuterių sistemų pažeidžiamumai. • Kibernetinio saugumo rekomendacijos ir geroji patirtis. • Su kibernetiniu saugumu susiję sertifikatai.	
E. gebėjimai (pagal e-CF)	B.2. Komponentų integracija B.3. Testavimas B.4. Sprendimų diegimas B.5. Dokumentų rengimas E.3. Rizikos valdymas	4 lygis 4 lygis 2 lygis 3 lygis 4 lygis

3. REZULTATŲ BIBLIOTEKA

Rezultatų sąraše pateikiami kai kurie orientaciniai ir praktiniai kiekvieno vaidmens profilio rezultatų pavyzdžiai. Išvardyti rezultatai pateikiami kaip pavyzdžiai, nes sąrašas nėra baigtinis, todėl neapima visų kiekvieno profilio aspektų.

Profilio pavadinimas	Rezultatas	Aprašymas
Vyriausiasis informacijos saugumo specialistas	Kibernetinio saugumo strategija	Kibernetinio saugumo strategija - tai veiksmų planas, skirtas organizacijos infrastruktūrų ir paslaugų saugumui ir atsparumui didinti.
Vyriausiasis informacijos saugumo specialistas	Kibernetinio saugumo taisyklės	Nuostatos, kuriose išvardijamos taisyklės, skirtos organizacijos kibernetiniam saugumui užtikrinti.
Reagavimo į kibernetinius incidentus specialistas	Reagavimo į incidentus planas	Dokumentuotų procedūrų rinkinys, kuriame išsamiai aprašyti veiksmai, kurių reikėtų imtis kiekviename reagavimo į incidentą etape (pasiruošimas, aptikimas ir analizė, suvaldymas, panaikinimas ir atkūrimas, veiksmai po incidento).
Reagavimo į kibernetinius incidentus specialistas	Kibernetinių incidentų ataskaita	Ataskaita, kurioje pateikiama išsami informacija apie vieną ar daugiau kibernetinių incidentų.
Kibernetinės teisės, politikos ir atitikties specialistas	Atitikties vadovas	Vadovas, kuriame išsamiai supažindinama su organizacijos įsipareigojimais laikytis teisės aktų reikalavimų. Jame gali būti pateikiamos vidaus taisyklės ar procedūros, skirtos užtikrinti įstatymų, kitų teisės aktų ir (arba) standartų laikymąsi.
Kibernetinės teisės, politikos ir atitikties specialistas	Atitikties ataskaita	Ataskaita, kurioje pateikiama dabartinė organizacijos atitikties reikalavimų laikymosi būklė.
Kibernetinių grėsmių žvalgybos specialistas	Kibernetinių grėsmių žvalgybos vadovas (arba žinynas)	Vadovas, kuriame pateikiamos kibernetinių grėsmių žvalgybos informacijos rinkimo, dalijimosi ja priemonės bei metodikos.
Kibernetinių grėsmių žvalgybos specialistas	Kibernetinių grėsmių ataskaita	Ataskaita, kurioje nurodomos pagrindinės grėsmės, svarbiausios pastebėtos su grėsmėmis susijusios tendencijos, grėsmių dalyviai bei atakų metodai. Ataskaitoje taip pat gali būti pateikiamos atitinkamos grėsmių mažinimo priemonės.
Kibernetinio saugumo architektas	Kibernetinio saugumo architektūros schema	Organizacijos kibernetinio saugumo sistemos architektūros, naudojamos turtui apsaugoti nuo kibernetinių išpuolių, grafinė schema.
Kibernetinio saugumo architektas	Kibernetinio saugumo reikalavimų ataskaita	Ataskaita, kurioje išvardijamas reikalavimų, reikalingų sistemos kibernetiniam saugumui užtikrinti, rinkinys.
Kibernetinio saugumo auditorius	Kibernetinio saugumo audito planas	Planas, kuriame pateikiama bendra strategija ir procedūros, auditoriaus atliekamos kibernetinio saugumo audito metu.

Kibernetinio saugumo auditorius	Kibernetinio saugumo audito ataskaita	Ataskaita, kurioje pateikiamas išsamios žinios apie sistemos saugumo lygį, įvertinamos kibernetinio saugumo stipriosios ir silpnosios pusės. Joje taip pat gali būti pateikti taisomieji veiksmai, kuriais siekiama pagerinti bendrą sistemos kibernetinį saugumą.
Kibernetinio saugumo mokytojas	Kibernetinio saugumo informuotumo didinimo programa	Veiksmų programa, skirta didinti informuotumą kibernetinio saugumo temomis (pvz., paskaitos apie atakas ir grėsmes), padedanti organizacijoms užkirsti kelią susijusioms kibernetinio saugumo grėsmėms ir jas minimizuoti.
Kibernetinio saugumo mokytojas	Kibernetinio saugumo mokymo medžiaga	Medžiaga, paaiškinanti su kibernetiniu saugumu susijusias sąvokas, metodus ir priemones, skirta mokymui ar kvalifikacijos kėlimui. Tai gali būti vadovėliai mokytojams, priemonių rinkiniai studentams ir (arba) virtualūs pavyzdžiai, padedantys rengti praktinius mokymus.
Kibernetinio saugumo diegimo specialistas	Kibernetinio saugumo sprendimai	Kibernetinio saugumo sprendimai gali apimti priemones ir paslaugas, kuriomis siekiama apsaugoti organizacijas nuo kibernetinių atakų.
Kibernetinio saugumo tyrėjas	Publikacijos kibernetinio saugumo srityje	Akademinė publikacija, kurioje skelbiamos kibernetinio saugumo kontekste atliktų tyrimų išvados ir rezultatai. Leidinio paskirtis gali būti technologijų plėtra ir (arba) naujų inovatyvių sprendimų kūrimas.
Kibernetinio saugumo rizikos vadovas	Kibernetinio saugumo rizikos vertinimo ataskaita	Ataskaita, kurioje pateikiami sistemos kibernetinio saugumo rizikos nustatymo, analizės ir vertinimo rezultatai. Joje taip pat gali būti pateiktos kontrolės priemonės, skirtos nustatytai rizikai sušvelninti arba sumažinti iki priimtino lygio.
Kibernetinio saugumo rizikos vadovas	Kibernetinio saugumo rizikos pašalinimo veiksmų planas	Veiksmų planas, kuriame išvardijama veikla, susijusi su poveikio mažinimo priemonių, kuriomis siekiama sumažinti kibernetinio saugumo riziką, įgyvendinimu.
Skaitmeninės kriminalistikos tyrėjas	Skaitmeninės teismo ekspertizės analizės rezultatai	Skaitmeninių duomenų analizės rezultatai, atskleidžiantys galimus kenkėjiškų incidentų įrodymus ir identifikuojantys galimus grėsmių sukėlėjus.
Skaitmeninės kriminalistikos tyrėjas	Elektroniniai įrodymai	Galimi įrodymai, gauti remiantis duomenimis, esančiais arba sukurtais bet kokio įrenginio, kurio veikimas priklauso nuo programinės įrangos programos arba duomenų, saugomų kompiuterių sistemoje ar tinkle arba perduodamų jais, duomenimis (pvz., tikslūs registracijos žurnalų duomenys).
Įsiskverbimo testuotojas	Pažeidžiamumo vertinimo rezultatų ataskaita	Ataskaita, kurioje išvardyti ir įvertinti skenavimo metu (paprastai automatinio) aptikti sistemos pažeidžiamumai. Ataskaitoje taip pat gali būti siūlomi pagrindiniai pažeidžiamumų ištaisymo veiksmai.
Įsiskverbimo testuotojas	Įsilaužimo bandymų ataskaita	Ataskaita, kurioje pateikiama išsami ir visapusiška sistemos pažeidžiamumų, nustatytų atliekant saugumo testavimą, analizė. Ataskaitoje taip pat gali būti siūlomi trūkumų ištaisymo veiksmai.

APIE ENISA

Europos Sąjungos kibernetinio saugumo agentūra ENISA yra Sąjungos agentūra, kurios tikslas - užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įsteigta 2004 m. ir įtvirtinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų patikimumą naudodama kibernetinio saugumo sertifikavimo sistemas, bendradarbiauja su valstybėmis narėmis bei ES įstaigomis ir padeda Europai pasirengti ateities kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra bendradarbiauja su pagrindinėmis suinteresuotosiomis šalimis, kad sustiprintų pasitikėjimą susietąja ekonomika, padidintų Sąjungos infrastruktūros atsparumą ir galiausiai užtikrintų Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos apie ENISA ir jos veiklą rasite čia: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

en sa europa eu

Originalus leidinys
SBN: 978-92-9204-584-5
DOI: 10.2824/859537