Co-funded by the European Union

EQF 4-5 LYGIS
PROFESINIO MOKYMO STUDENTAMS
SKIRTI MOKYMO MODULIAI

CYBER AGENT 01.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

www.cyberagents.eu

3 darbo paketas: CyberAgent mokymo(si) išteklių kūrimas

Rezultatas 3.2: Mokymo moduliai profesinio mokymo studentams
3.2 lyderis – TIMTAL (TR)

TURINYS

LENTELIŲ SĄRAŠAS

ĮVADAS

Sparčiai kintant mokslui, technologijoms, visuomenės poreikiams bei mokymo metodams, keičiasi ir reikalavimai pačiam žmogui. Dabar iš jo tikimasi, kad jis ne tik kaups žinias, bet ir gebės jas pritaikyti praktiškai: spręsti problemas, mąstyti kritiškai, būti iniciatyvus ir ryžtingas. Taip pat svarbūs tampa geri bendravimo įgūdžiai, empatija ir noras prisidėti prie visuomenės gerovės.

Informacijos amžiaus sparta ir naujovės mokymo srityje keičia lūkesčius, keliamus kiekvienam individui. Šiandien svarbu ne tik turėti žinių, bet ir mokėti jas panaudoti sprendžiant sudėtingas problemas, kritiškai vertinti situacijas, veikti versliai, efektyviai bendrauti, suprasti kitus ir kurti pridėtinę vertę visuomenei. Šie pokyčiai skatina žmones nuolat mokytis, prisitaikyti ir tobulėti.

Šiame kontekste smarkiai keičiasi ir profesinis mokymas. Vietoj tradicinių profesijų atsiranda naujos, paremtos technologijomis ir nuolat kintančios. Kibernetinis saugumas šiuose procesuose yra ypač svarbus, nes skaitmeniniame pasaulyje jo rizikos auga visuose sektoriuose. Jis atlieka esminį vaidmenį visur: nuo asmens duomenų ar įmonės paslapčių saugojimo iki kritinių infrastruktūrų ir finansinių operacijų apsaugos.

Kibernetinio saugumo mokymas apima ne vien techninių įgūdžių lavinimą – juo siekiama ugdyti etiškus, atsakingus, teisės aktus išmanančius ir nuolat tobulėti pasirengusius specialistus. Kibernetinis saugumas yra ne tik techninis iššūkis, bet ir socialinė atsakomybė, todėl skirti jam deramą dėmesį profesiniame rengime yra būtina visos visuomenės ateičiai.

Profesinis mokymas – tai sistema, apimanti profesinio ir techninio švietimo planavimą, tyrimus, organizavimą, valdymą ir mokymą. Ši sistema veikia glaudžiai bendradarbiaujant su žemės ūkio, pramonės ir paslaugų sektoriais. Pagrindinis tikslas – parengti aukštos kvalifikacijos darbuotojus ir specialistus, kurie yra būtini kiekviename gamybos etape ir užtikrina visuomenės raidą.

Pagal profesinio mokymo programą „Cyberagent“ (4-5 EKS lygis) siekiama rengti specialistus kibernetinio saugumo sričiai. Programa sukurta atsižvelgiant į realius darbo rinkos poreikius ir atlikus išsamią analizę. Programos turiniu siekiama suteikti būsimam specialistui reikiamų žinių, įgūdžių ir nuostatų, o visas mokymo procesas yra suplanuotas taip, kad parengtų žmogų sėkmingai profesinei veiklai šioje srityje.

1. KIBERAGENTO EQF 4-5 LYGIO PROGRAMOS TIKSLAI

Pastaraisiais metais kibernetinio saugumo poreikis sparčiai išaugo ne tik visame pasaulyje, bet ir Europos Sąjungos šalyse. Kartu su technologijų plėtra tokiu pat greičiu keitėsi ir sudėtingėjo kibernetinės rizikos bei grėsmės. Šiandien jos gali sukelti daug didesnę ir platesnio masto žalą nei fizinės atakos. Kadangi tokie sektoriai kaip finansai, elektroniniai ryšiai, energetika, transportas ir aviacija savo paslaugas teikia skaitmeninėje erdvėje, nacionalinio kibernetinio saugumo užtikrinimas tapo vienu svarbiausių valstybės prioritetų. Todėl siekiama integruoti kibernetinio saugumo mokymą į formaliojo ir neformaliojo švietimo sistemas, nuolat plėtoti ir tobulinti mokymo turinį.

2. EUROPOS KVALIFIKACIJŲ SISTEMA

Europos Sąjunga sukūrė Europos kvalifikacijų sistemą (EKS) kaip tam tikrą vertimo įrankį, padedantį geriau suprasti ir palyginti skirtingų šalių nacionalines kvalifikacijas. EKS siekiama skatinti besimokančiųjų ir darbuotojų judumą tarp valstybių, remti mokymąsi visą gyvenimą ir profesinį tobulėjimą visoje Europoje.

EKS – tai 8 lygmenų sistema, apimanti visų tipų kvalifikacijas ir pagrįsta mokymosi rezultatais. Ji veikia kaip standartas, leidžiantis susieti skirtingas nacionalines kvalifikacijų sistemas. Ši sistema padidina kvalifikacijų skaidrumą, palyginamumą ir perkėlimo galimybes, todėl tampa lengviau gretinti skirtingų šalių ir institucijų suteiktas kvalifikacijas.

EKS apima visų rūšių ir visų lygmenų kvalifikacijas, o mokymosi rezultatų aprašymas aiškiai parodo, ką konkretus asmuo žino, supranta ir geba daryti. Kvalifikacijos lygmuo, kurių iš viso yra aštuoni, kyla priklausomai nuo gebėjimų sudėtingumo – nuo pirmo (žemiausio) iki aštunto (aukščiausio). Svarbiausia, kad EKS yra glaudžiai susieta su nacionalinėmis kvalifikacijų sistemomis. Dėl šios sąsajos ji veikia kaip išsamus visų Europoje esančių kvalifikacijų žemėlapis, kurį galima pasiekti per kvalifikacijų duomenų bazes.

EKS buvo sukurta 2008 metais ir atnaujinta 2017-aisiais. Po atnaujinimo išliko pagrindiniai tikslai – užtikrinti Europos kvalifikacijų skaidrumą ir tarpusavio pasitikėjimą. Valstybės narės įsipareigojo toliau tobulinti EKS, kad darbdaviai, darbuotojai ir besimokantieji galėtų lengviau suprasti ir palyginti ne tik nacionalines ar tarptautines, bet ir trečiųjų šalių kvalifikacijas.

Kiekvienas iš 8 EKS lygmenų yra apibrėžiamas pagal tam tikrus reikalavimus (deskriptorius), kurie nusako to lygio kvalifikacijai būtinus mokymosi rezultatus. Mokymosi rezultatai skirstomi į tris pagrindines sritis:

- Žinios: EKS kontekste žinios apibūdinamos kaip teorinės ir (arba) faktinės.
- Gebėjimai: EKS kontekste gebėjimai skirstomi į kognityvinius (loginis, intuityvus ir kūrybinis mąstymas) ir praktinius (įgudimas naudotis metodais, medžiagomis, įrankiais ir prietaisais).
- Atsakomybė ir savarankiškumas: EKS kontekste tai apibūdinama kaip asmens gebėjimas savarankiškai ir atsakingai taikyti įgytas žinias bei įgūdžius.

1 lentelė – EQF 4 lygio mokymosi rezultatai

Žinios	***Gebėjimai***	***Atsakomybė ir savarankiškumas***
Faktinės ir teorinės žinios plačiame studijų ar mokymosi srities kontekste.	Kognityvinių ir praktinių įgūdžių rinkinys, reikalingas sprendimams konkrečioms problemoms darbo ar švietimo srityje rasti.	Taikyti savarankišką mokymąsi pagal darbo ar mokymosi konteksto gaires, kurios paprastai yra prognozuojamos, bet gali keistis; prižiūrėti kitų kasdienį darbą, prisiimti tam tikrą atsakomybę už darbo ar mokymosi veiklos vertinimą ir tobulinimą.

3. KIBERNETINIO SAUGUMO PROFESINIO MOKYMO STUDENTAI (EQF 4-5 LYGIS)

Kibernetinio saugumo specialistas (4-5 EKS lygis) – tai kvalifikuotas darbuotojas, dirbantis informacinių sistemų srityje.

Pagrindinės jo atsakomybės:

- Prevencinė veikla. Jis dalyvauja prevencinėje veikloje – stebi sistemų pažeidžiamumus, prisideda prie darbuotojų kibernetinio sąmoningumo didinimo ir kontroliuoja prevencinių veiksmų įgyvendinimą.
- Sistemų stebėsena. Specialistas stebi kibernetinio saugumo analizėms naudojamų sistemų veikimą ir stabilumą.
- Tinklų valdymas. Jis nustato nesudėtingų tinklų reikalavimus, įrengia fizinius tinklus, atlieka bazinį tinklo įrangos konfigūravimą, užtikrina tinklo saugumą, priežiūrą ir tobulinimą.
- Pagalba ir tobulėjimas. Teikia techninę pagalbą vartotojams ir nuolat tobulina savo profesines žinias.

Pagrindinis šio specialisto tikslas – apsaugoti įmonės IT infrastruktūrą nuo kibernetinių grėsmių. Visas užduotis jis atlieka laikydamasis kokybės reikalavimų, darbuotojų saugos ir sveikatos bei aplinkos apsaugos standartų.

3.1. CYBERAGENT LEARNING PROGRAMA EQF-4-5

Profesinio mokymo programa (EQF 4-5) buvo parengta strategiškai pritaikant išsamią aukštojo mokslo institucijų programą (EQF 5-6). Adaptavimo metu vieno modulio medžiaga buvo atrinkta taip, kad atitiktų 1 ECTS apimtį, o didžiausias dėmesys skirtas mokymosi rezultatams, kurie yra aktualiausi profesinio mokymo studentams ir atliepia neatidėliotinus smulkaus ir vidutinio verslo (SVV) poreikius. Prioritetas teiktas temoms, pabrėžiančioms praktinį pritaikymą ir pamatinius kibernetinio saugumo įgūdžius, o sudėtingesnės teorinės koncepcijos buvo supaprastintos, kad tiktų profesinio mokymo programai.

2 lentelė – 1 modulis

Skyriai	**Temos**
Projektų valdymas	Projekto planavimas Projekto tikslų nustatymas Dabartinės kibernetinio saugumo grėsmės (DDoS, išpirkos reikalaujanti programinė įranga, kenkėjiška programinė įranga, sukčiavimas elektroniniu paštu, „zero-day“ atakos, IoT atakos ir kt.) Grėsmių modeliavimas ir pažeidžiamumo analizė Kibernetinio saugumo grėsmių ir incidentų pranešimai
Mokymosi rezultatai • Besimokantieji gebės apibrėžti projektų valdymo etapus ir sudaryti pagrindinį projekto planą. • Besimokantieji gebės suformuluoti aiškius, išmatuojamus ir pasiekiamus projekto tikslus. • Besimokantieji gebės identifikuoti, klasifikuoti ir įvertinti įvairias kibernetinio saugumo grėsmes. • Besimokantieji gebės kurti grėsmių modelius ir atlikti konkrečių scenarijų pažeidžiamumo analizę. • Besimokantieji gebės rengti incidentų ataskaitas laikantis nustatytų protokolų.	
Išteklių valdymas	Saugumo įrankiai ir programinė įranga Veiksmingas technologinių išteklių naudojimas
Mokymosi rezultatai • Besimokantieji gebės efektyviai naudoti kibernetinio saugumo įrankius ir programinę įrangą grėsmėms aptikti ir į jas reaguoti. (Taikymas) • Besimokantieji gebės optimizuoti technologinius išteklius siekdami didesnio saugumo ir efektyvumo. (Taikymas)	
Saugumo rodikliai	Saugumo metrikos ir matavimo metodai Duomenų rinkimas naudojant SIEM Saugumo metrikų analizė Projekto stebėsena ir veiklos vertinimas Veiksmų peržiūra ir projekto pritaikymas
Mokymosi rezultatai • Besimokantieji gebės parinkti ir taikyti tinkamą saugumo metriką ir matavimo metodus. • Besimokantieji gebės konfigūruoti ir naudoti SIEM įrankius duomenims rinkti ir saugumui stebėti. • Besimokantieji gebės interpretuoti ir analizuoti saugumo metriką, kad įvertintų saugumo būklę. • Besimokantieji gebės stebėti ir vertinti projekto rezultatus naudodami saugumo metriką. • Besimokantieji gebės rengti ir pristatyti ataskaitas, pagrįstas saugumo metrikos analize.	
Kokybės užtikrinimas ir kokybės kontrolė	Kokybės valdymas Kibernetinio saugumo kokybės standartai Testavimo ir patvirtinimo metodai

Mokinių pasiekimai: • Besimokantieji gebės taikyti kokybės valdymo praktikas kibernetinio saugumo projektuose. • Besimokantieji gebės parinkti ir taikyti aktualius kibernetinio saugumo kokybės standartus. • Besimokantieji gebės kurti ir vykdyti kibernetinio saugumo sprendimų testavimo ir patvirtinimo procedūras.

3 lentelė – 2 modulis

Skyriai	**Temos**
Operacinės sistemos administravimas	Operacinės sistemos Techninė ir programinė įranga Dvejetainė ir šešioliktainė skaičiavimo sistema Bitai ir baitai Komandų eilutė operacinėje sistemoje „Windows“ ir „Linux“ komandos „Windows“ klientas ir serveris Programos, procesai ir paslaugos sistemoje „Windows“ Failų plėtiniai ir tipai Registro raktai ir tipai Valdymo skydelio nustatymai Naudotojai ir grupės Domeno struktūra ir serverio tvarkyklė AD ir GPO Linux sąsajos ir branduolys Procesai Linux sistemoje Failų ir katalogų pavadinimų suteikimo tvarka Linux Shells ir komandų sintaksė Failų ir aplankų tvarkymas Darbas su Pipe & System stebėjimo komandomis Procesų valdymas ir užduočių kontrolė Paslaugų valdymas
Mokymosi rezultatai: • Besimokantieji gebės palyginti skirtingas operacines sistemas ir jų architektūras. • Besimokantieji gebės paaiškinti techninės ir programinės įrangos sąveiką operacinės sistemos aplinkoje. • Besimokantieji gebės atlikti dvejetainius ir šešioliktainius skaičiavimus bei suprasti duomenų vaizdavimą. • Besimokantieji gebės vykdyti pagrindines komandas Windows ir Linux aplinkose. • Besimokantieji gebės valdyti programas, paslaugas ir procesus naudodami sistemos įrankius. • Besimokantieji gebės konfigūruoti ir valdyti „Active Directory“ bei grupės strategijos objektus (GPO). • Besimokantieji gebės dirbti su Linux sąsajomis ir atlikti branduolio lygio operacijas.	

<table>
<tr><td colspan="2">

- Besimokantieji gebės valdyti paslaugas ir sistemos procesus naudodami Linux komandas.

</td></tr>
<tr><td>Duomenų bazių sistemų administravimas</td><td>Sistemos žurnalai ir žurnalų stebėjimas
Užduočių planavimas Linux sistemoje
Serverių ir tinklo gedimų šalinimas
Atsarginės kopijos ir atkūrimas
GRUB apsauga
Ugniasienės
Active Directory objektų ir GPO valdymas
DNS ir DHCP
PowerShell pagrindai
Microsoft BitLocker, AppLocker ir ugniasienė
LDAP ir Kerberos
NTLM
Slaptažodžių ir blokavimo politikos
Autentiškumo patvirtinimas ir prieigos kontrolė
Interneto kontrolės pranešimų protokolas (ICMP)
TCP ir UDP
NetBIOS ir SMB
SSL ir TLS
Sertifikatai
Telnet ir Secure Shell (SSH) protokolai
HTTP ir HTTPS
Pašto sistemų protokolai
Domenų vardų sistemos protokolas (DNS)
FTP ir RDP
Inkapsuliacija ir dekapseliacija
Tinklo snifferiai ir Wireshark
TCP/UDP
DHCP, DNS</td></tr>
<tr><td colspan="2">Mokymosi rezultatai:

- Besimokantieji gebės konfigūruoti paketų saugyklas ir tvarkyti šaltinių sąrašus.
- Besimokantieji gebės analizuoti ir stebėti sistemos žurnalus ieškodami trikčių ir saugumo pažeidimų.
- Besimokantieji gebės atlikti atsarginių kopijų kūrimo ir atkūrimo operacijas, kad užtikrintų duomenų vientisumą.
- Besimokantieji gebės diegti saugumo priemones, tokias kaip ugniasienės, „BitLocker“ ir „AppLocker“.

</td></tr>
<tr><td>Tinklo administravimas</td><td>Tinklų tipai ir belaidžiai tinklai
Tinklai ir topologijos
Įrenginio tapatybė ir prieigos įrenginiai
Infrastruktūra ir saugumo įrenginiai
Specializuoti įrenginiai ir tinklo architektūra
Virtualūs tinklai
Fiziniai ir loginiai adresai
OSI ir tinklo modeliai
Duomenų įkapsulavimas ir dekapsulavimas
Tinklo protokolai ir prievadų numeriai</td></tr>
</table>

	Tinklo laikmenos ir kabeliai Belaidės technologijos Tinklo administravimo įrankiai Cisco Packet Tracer Tinklo klasės ir potinkliai Adresų nustatymo protokolas (ARP) Statinis ir dinaminis IP adresavimas Tinklo adresų vertimas (NAT) Komutatoriai ir Cisco IOS Komutatorių prievadų saugumas ir maršrutizatorių sąsajos VLAN ir DTP konfigūravimas Maršrutizavimas tarp VLAN Įvadas į ACL Tinklo gedimų šalinimas
Mokymosi rezultatai: • Besimokantieji gebės kurti ir valdyti tinklus, suprasdami protokolus ir topologijas. • Besimokantieji gebės konfigūruoti VLAN, ACL ir valdyti IP adresavimo schemas. • Besimokantieji gebės naudoti įrankius, tokius kaip „Wireshark“ ir „Cisco Packet Tracer“, tinklo stebėsenai ir trikčių šalinimui.	
Debesų administravimas	Hipervizoriai ir virtualios mašinos Konteineriai Virtualių aplinkų saugumo užtikrinimas Atsarginės kopijos ir atkūrimas Debesų kompiuterija ir CSP Kas yra debesų paslaugų modeliai Debesų diegimo tipai Virtualūs tinklai AWS skaičiavimo paslaugos „Amazon Elastic Compute Cloud“ (EC2) Debesų stebėjimo įrankiai Automatizavimo ir koordinavimo įrankiai Debesų saugumo grėsmės ir pažeidžiamumai Tapatybės ir prieigos valdymas (IAM) Prieigos kontrolė pagal vaidmenis (RBAC) Daugialypė autentifikacija (MFA) Debesų duomenų šifravimas Virtualus privatusis debesų kompiuteris (VPC) Docker ir Kubernetes
Mokymosi rezultatai: • Besimokantieji gebės valdyti virtualias aplinkas naudodami AWS, „Docker“ ir „Kubernetes“. • Besimokantieji gebės diegti debesijos saugumo kontrolės priemones ir valdyti tapatybes.	
Kiberfizinės sistemos administravimas	Saugumo ir prieigos kontrolė Autentiškumo patvirtinimo tipai TACACS+ ir RADIUS AAA konfigūracija Rizikos valdymo tikslai

	Šifravimas ir dešifravimas Hash ir Rainbow lentelės MAC „Spoofing“ & ARP „Poisoning“ VLAN „Hopping“ & „Rogue“ DHCP ICMP „Flood” TCP ir UDP „Flood” Sesijos perėmimas DNS suklastojimas „Defense in Depth (DID) & Zero Trust“ Demilitarizuotos zonos (DMZ) Honeypots ir tinklo stiprinimas Geriausia praktika saugiam tinklui VPN SSH ir VNC „Stateful“ ir „Stateless“ ugniasienės „Host-Based“ vs. „Network-Based“ Aparatinės ir programinės ugniasienės Tinklo programų ugniasienės (WAF) AI ugniasienėse IDS ir IPS NIDS ir HIDS Snort tcpdump
Mokymosi rezultatai: • Besimokantieji gebės apsaugoti tinklus naudodami ugniasienes, IDS/IPS ir grėsmių aptikimo įrankius. • Besimokantieji gebės taikyti šifravimo metodus ir valdyti saugumo protokolus.	
Sistemos stiprinimas	GenAI technikos Kodo generavimas Vartotojų paskyrų valdymas ir prieigos kontrolė Anomalijų aptikimas ir trikčių šalinimas Apache2 paslaugos klaidų sprendimas Pataisų valdymas ir atnaujinimai Automatinis atsarginių kopijų kūrimas ir atkūrimas IT turto valdymas ir inventorizacija Ištrintų failų atkūrimas naudojant GenAI Kibernetinio saugumo procedūros Grėsmių aptikimas ir analizė Reagavimas į grėsmes ir jų šalinimas AI panaudojimas realaus laiko grėsmių aptikimui GenAI modelių patvirtinimas ir testavimas Valdymo ir reguliavimo sistemos DNS konfigūracija ir saugumas DHCP konfigūracija ir saugumas PowerShell pagrindai Komutatoriaus prievado saugumas Tinklo pagrindinė įvesties/išvesties sistema (NetBIOS) Serverio pranešimų blokavimo protokolas (SMB)

	Saugių lizdų sluoksnis (SSL) ir transporto sluoksnio saugumas (TLS) Saugumo sertifikatai Pašto sistemų protokolai Domenų vardų sistemos protokolas (DNS) Failų perdavimo protokolas (FTP) Nuotolinio darbalaukio protokolas (RDP) Užduočių planavimas Linux Serverio gedimų šalinimas Tinklo gedimų šalinimas Atsarginės kopijos ir atkūrimas GRUB apsauga Ugniasienių nustatymas ir apsauga
Mokymosi rezultatai: • Besimokantieji gebės taikyti sistemų stiprinimo metodus, siekdami pagerinti saugumą. • Besimokantieji gebės pasitelkti DI grėsmių aptikimui ir sistemų stebėsenai.	
Sistemos stiprinimas	IR ir SOC Įvykiai ir incidentai Įspėjimų aptikimas ir įspėjimų rūšiavimas Dokumentacija ir ataskaitos Kas yra internetinės atakos? DoS ir DDoS SQL įterpimas ir XSS „Command Injection & Local File Inclusion“ (LFI) „Cross-Site Request Forgery“ (CSRF) „Brute-Force“ ir „Credential Stuffing“ „Pass the Hash & Pass the Ticket“ LDAP žvalgyba Sugadinta prieigos kontrolė Išpirkos reikalaujantis virusas Kompiuteriniai virusai ir kirminai Trojos arklys ir reklamos programinė įranga Keylogger ir kriptovaliutų kasyba „Fileless Malware“ Kenkėjiškų programų plitimo supratimas Statinė ir dinaminė kenkėjiškų programų analizė Saugi kenkėjiškų programų analizė Hibridinė analizė, kenkėjiškų programų tyrimas Statinės ir dinaminės kenkėjiškų programų analizės atlikimas IOC ir slaptažodžių politikos valdymas „Acceptable Use Policies“ (AUP) „Bring Your Own Device“ (BYOD) politika Nuotolinės prieigos politika
Mokymosi rezultatai: • Atskirti pagrindinius reagavimo į incidentus (IR) komandos ir saugumo operacijų centro (SOC) vaidmenis bei bendradarbiavimą. • Apibrėžti skirtumą tarp saugumo incidentų ir pažeidimų. • Paaiškinti saugumo perspėjimų šaltinius ir jų skirstymo procesus. • Parengti efektyvią saugumo incidentų dokumentaciją ir ataskaitas. • Apibūdinti dažniausius žiniatinklio atakų tipus (DoS/DDoS, SQL injekcijos, XSS, komandų injekcijos, LFI, CSRF).	

• Paaiškinti „brute-force“ ir pavogtų prisijungimo duomenų bandymo atakas bei jų prevencijos priemones. • Suprasti „pass the hash“ ir „pass the ticket“ atakų pagrindinius principus. • Paaiškinti, kaip gali būti išnaudojami prieigos kontrolės pažeidžiamumai. • Paaiškinti skirtingus kenkėjiškų programų tipus („Ransomware“, virusai, kirminai, Trojos arkliai, reklaminės programos, „Keylogger“, „Cryptojacking“, befailės programos) ir jų plitimo būdus. • Paaiškinti kompromitacijos indikatorių (IOC) valdymo svarbą. • Apibūdinti pagrindinius stiprių slaptažodžių ir priimtino naudojimo taisyklių (AUP) elementus. • Įvertinti BYOD ir nuotolinės prieigos taisyklių poveikį saugumui.

4 lentelė – 3 modulis

Skyriai	**Temos**
Veiklos rodikliai (metrika)	Veiklos rodikliai Sistemos ir tinklo stebėjimas Veiklos rodiklių stebėjimas Tinklo žemėlapiai Pažeidžiamumo skenavimas Tinklo srauto analizė
Mokymosi rezultatai: • Besimokantieji gebės apibrėžti veiklos rodiklius ir paaiškins jų svarbą vertinant sistemos ir tinklo veiklą. • Besimokantieji gebės įdiegti ir naudoti stebėsenos įrankius nuolatiniam sistemų ir tinklo našumo vertinimui. • Besimokantieji gebės analizuoti ir interpretuoti našumo metriką, kad įvertintų sistemos būklę ir nustatytų optimizavimo galimybes. • Besimokantieji gebės kurti tinklo žemėlapius, kad galėtų vizualizuoti, stebėti ir optimizuoti tinklo struktūras. • Besimokantieji gebės atlikti pažeidžiamumų skenavimą, nustatyti saugumo rizikas ir rekomenduoti šalinimo veiksmus. • Besimokantieji gebės atlikti tinklo srauto analizę, kad aptiktų potencialias grėsmes ir į jas reaguotų.	
Duomenų analizė	Duomenų rinkimas Duomenų valymas ir pirminis apdorojimas Duomenų analizė Duomenų vizualizavimas Analitinės priemonės Duomenų analizės taikymas kibernetiniame saugume
Mokymosi rezultatai • Besimokantieji gebės rinkti analizei reikalingus duomenis iš sistemų, tinklų ir saugumo žurnalų.	

• Besimokantieji gebės valyti ir apdoroti neapdorotus duomenis, kad užtikrintų jų tikslumą ir nuoseklumą. • Besimokantieji gebės taikyti statistinius ir analitinius metodus, kad iš duomenų išgautų prasmingas įžvalgas. • Besimokantieji gebės kurti duomenų vizualizacijas, kad efektyviai perteiktų analizės rezultatus. • Besimokantieji gebės naudoti įrankius, tokius kaip „Python“, „R“ ir „Power BI“, išsamiai duomenų analizei atlikti. • Besimokantieji gebės taikyti duomenų analitikos metodus kibernetinio saugumo grėsmėms aptikti, analizuoti ir mažinti.	
Saugumo žvalgyba	Saugumo žvalgybos supratimas Saugumo žvalgybos šaltiniai Grėsmių žvalgybos rinkimo metodai Saugumo žvalgybos taikymo atvejų analizė
Mokymosi rezultatai • Besimokantieji gebės paaiškinti saugumo žvalgybos svarbą proaktyviam grėsmių valdymui. • Besimokantieji gebės įvertinti saugumo žvalgybos šaltinius, įskaitant grėsmių duomenų srautus, ataskaitas ir atvirojo kodo įrankius. • Besimokantieji gebės apibūdinti grėsmių žvalgybos duomenų rinkimo ir analizės metodus. • Besimokantieji gebės nagrinėti realius pavyzdžius, kad suprastų, kaip saugumo žvalgyba taikoma užkertant kelią kibernetinėms grėsmėms.	

5 lentelė – 4 modulis

Skyriai	**Temos**
Saugumo operacijų pagrindai	Saugumo operacijų ir SOC (saugumo operacijų centro) supratimas Saugumo operacijų vaidmenys ir atsakomybė Saugumo operacijų įrankių ir technologijų apžvalga Praktiniai pavyzdžiai ir atvejų analizė
Mokymosi rezultatai • Besimokantieji gebės paaiškinti saugumo operacijų centro (SOC) tikslą, struktūrą ir jo vaidmenį kibernetiniame saugume. • Besimokantieji gebės apibūdinti saugumo operacijų personalo vaidmenis ir atsakomybes, įskaitant reagavimą į incidentus, grėsmių paiešką ir stebėseną. • Besimokantieji gebės atpažinti ir pademonstruoti, kaip naudotis įprastais saugumo operacijų įrankiais ir technologijomis. • Besimokantieji gebės analizuoti realius pavyzdžius ir atvejų studijas, kad suprastų, kaip saugumo operacijos vykdomos praktiškai.	
Saugumo konvergencija	Saugumo konvergencijos supratimas Fizinio saugumo pagrindai (fizinio saugumo principai, fizinio turto apsauga, politika) Dažniausiai MVĮ kylančios grėsmės Atvejų analizė, kurioje pabrėžiamos konvergencijos problemos

Mokymosi rezultatai • Besimokantieji gebės apibrėžti saugumo konvergenciją ir paaiškinti jos svarbą integruojant fizinio ir kibernetinio saugumo priemones. • Besimokantieji gebės taikyti fizinio saugumo principus, siekdami apsaugoti turtą, patalpas ir personalą. • Besimokantieji gebės nustatyti ir įvertinti saugumo grėsmes, su kuriomis dažniausiai susiduria smulkios ir vidutinės įmonės (SVV). • Besimokantieji gebės nagrinėti atvejų studijas, kad suprastų konvergencijos iššūkių poveikį. • Besimokantieji gebės apžvelgti saugumo informacijos ir įvykių valdymo procesus.	
Saugumo informacijos ir įvykių valdymas	Saugumo stebėjimo principų peržiūra (remiantis kitų partnerių moduliu) SIEM sprendimų įgyvendinimas Žurnalų ir įspėjimų nustatymas Grėsmių žvalgybos ir aptikimo metodikų peržiūra (remiantis kitų partnerių moduliu)
Mokymosi rezultatai: • Besimokantieji gebės paaiškinti saugumo stebėsenos principus ir jų taikymą SIEM sprendimuose. • Besimokantieji gebės konfigūruoti ir valdyti SIEM sprendimus, siekdami efektyviai aptikti grėsmes ir į jas reaguoti. • Besimokantieji gebės nustatyti registravimo ir perspėjimo mechanizmus SIEM įrankiuose, kad galėtų stebėti saugumo įvykius. • Besimokantieji gebės įvertinti grėsmių žvalgybos ir aptikimo metodikas, reikalingas efektyvioms saugumo operacijoms.	
Saugumo operacijų praktika	Atitiktis ir reguliavimas Nuolatinio tobulinimo strategijos saugumo operacijose Automatizavimas ir koordinavimas Metrikos ir ataskaitos
Mokymosi rezultatai: • Besimokantieji gebės paaiškinti atitikties ir reguliavimo svarbą saugumo operacijose. • Besimokantieji gebės kurti ir įgyvendinti nuolatinio tobulinimo strategijas saugumo operacijoms. • Besimokantieji gebės pasitelkti automatizavimą ir orkestravimą, kad padidintų saugumo operacijų efektyvumą. • Besimokantieji gebės kurti ir naudoti saugumo metriką bei ataskaitų rengimo metodus, kad informuotų apie saugumo būklę.	

6 lentelė – 5 modulis

Skyriai	**Temos**
Organizacijos kontekstas	Kibernetinio saugumo raida smulkiame ir vidutiniame versle (SVV) Dabartinės pagrindinės grėsmės ir pažeidžiamumas Kibernetinio saugumo poveikis verslo strategijai

	Konkretūs kibernetinio saugumo iššūkiai smulkiame ir vidutiniame versle (SVV) , palyginti su didžiosiomis įmonėmis Suprasti kibernetinio saugumo praktikos reguliavimo pasekmes ir kaip jos dera su valdymo struktūromis. Bendros SVV būdingos kibernetinio saugumo problemos, pvz., ribotas biudžetas, specializuoto saugumo personalo trūkumas ir praktiniai metodai, kaip nustatyti kibernetinio saugumo investicijų prioritetus.
Mokymosi rezultatai • Besimokantieji gebės atsekti kibernetinio saugumo praktikų raidą smulkiose ir vidutinėse įmonėse. • Besimokantieji gebės nustatyti ir įvertinti svarbiausias dabartines grėsmes ir pažeidžiamumus, darančius poveikį SVV. • Besimokantieji gebės analizuoti, kaip kibernetinis saugumas veikia verslo strategiją ir veiklos sprendimų priėmimą. • Besimokantieji gebės palyginti kibernetinio saugumo iššūkius, su kuriais susiduria SVV, su iššūkiais, kylančiais didesnėms organizacijoms. • Besimokantieji gebės interpretuoti teisinius kibernetinio saugumo reikalavimus ir įvertinti, kaip juos integruoti į organizacijos valdymą. • Besimokantieji gebės apibūdinti praktinius sprendimus dažniausiems SVV kibernetinio saugumo iššūkiams, tokiems kaip biudžeto ir personalo trūkumas.	
Privatumas	Privatumo principai kibernetiniame saugume Asmens duomenų apsauga ir BDAR Privatumo poveikis MVĮ veiklai Privatumo apsaugos priemonės ir metodai
Mokymosi rezultatai • Besimokantieji gebės paaiškinti pagrindinius privatumo principus kibernetinio saugumo kontekste. • Besimokantieji gebės taikyti BDAR reikalavimus ir įvertinti jų poveikį asmens duomenų apsaugai. • Besimokantieji gebės įvertinti, kaip privatumo reglamentai veikia SVV kasdienę veiklą ir verslo modelius. • Besimokantieji gebės naudoti įrankius ir taikyti metodus privatumui palaikyti ir jautriems duomenims apsaugoti.	
Teisės aktai, etika ir atitiktis	Kibernetinio saugumo organizacijos, politika ir standartai Atitinkami nacionaliniai ir tarptautiniai teisės aktai Reglamentų laikymasis SVV Etika kibernetiniame saugume Teisinės pasekmės dėl atitikties reikalavimams nesilaikymo kibernetiniame saugume Analizė, kaip AI pagrįsti įrankiai gali būti naudojami siekiant sustiprinti kibernetinio saugumo valdymą ir užtikrinti atitiktį nuolat stebint ir automatizuotai reaguojant į grėsmes.
Mokymosi rezultatai • Besimokantieji gebės nustatyti pagrindines kibernetinio saugumo organizacijas ir įvertinti susijusias taisyklių bei standartų sistemas.	

<table>
<tr><td colspan="2">

- Besimokantieji gebės apibendrinti pagrindinius nacionalinio ir tarptautinio lygmens teisės aktus, darančius poveikį kibernetiniam saugumui.
- Besimokantieji gebės kurti strategijas, skirtas pasiekti ir palaikyti teisinio reguliavimo atitiktį SVV aplinkoje.
- Besimokantieji gebės nagrinėti etinius aspektus priimant sprendimus ir veikiant kibernetinio saugumo srityje.
- Besimokantieji gebės įvertinti teisines pasekmes, kylančias dėl kibernetinio saugumo įstatymų nesilaikymo.
- Besimokantieji gebės ištirti, kaip DI įrankiai gali pagerinti valdymą, automatizuoti stebėseną ir sustiprinti atitiktį.

</td></tr>
<tr><td>Saugumo valdymas</td><td>Kibernetinio saugumo valdymo struktūra
Saugumo valdymo vaidmenys ir atsakomybė
Kibernetinio saugumo brandos modeliai
Gebėjimų atlikti rizikos vertinimus ir formuluoti strateginius reagavimo planus imituojamomis krizinėmis sąlygomis (išpirkos reikalaujantis virusas, sukčiavimo atakos ir kt.) stiprinimas
Komunikacija vykdomojo ir valdybos lygiu
Kibernetinio saugumo komunikacijos strategijos
Saugumo ataskaitos aukščiausiajai vadovybei
Krizių valdymas ir komunikacija kibernetinio saugumo srityje
Įsisavinti krizių valdymo ir sprendimų priėmimo įgūdžius didelio streso scenarijuose, susijusiuose su AI valdomomis atakomis ir išpirkos reikalaujančiais virusais.</td></tr>
<tr><td colspan="2">Mokymosi rezultatai

- Besimokantieji gebės kurti ir vertinti valdysenos struktūras, kurios palaiko efektyvų kibernetinio saugumo valdymą.
- Besimokantieji gebės priskirti ir aiškiai apibrėžti atsakomybes organizacijos saugumo sistemose.
- Besimokantieji gebės įvertinti kibernetinio saugumo brandą naudojant nusistovėjusius modelius.
- Besimokantieji gebės atlikti rizikos vertinimus ir kurti atsako strategijas scenarijams, tokiems kaip išpirkos reikalaujančių programų ar „phishing“ atakos.
- Besimokantieji gebės parengti komunikacijos planus, skirtus kibernetinio saugumo įžvalgoms perteikti aukšto lygio vadovams ir valdybos nariams.
- Besimokantieji gebės formuluoti efektyvias komunikacijos strategijas, skirtas vidinėms ir išorinėms kibernetinio saugumo suinteresuotosioms šalims.
- Besimokantieji gebės rengti ataskaitas, kurios informuoja aukščiausio lygio vadovybę apie kibernetinio saugumo veiksmingumą ir rizikas.
- Besimokantieji gebės praktikuotis valdyti krizes ir komunikuoti jų metu, įskaitant krizes, susijusias su DI valdomomis atakomis.

</td></tr>
<tr><td>Valdymo politika</td><td>Politikos įgyvendinimas ir stebėsena</td></tr>
<tr><td colspan="2">Mokymosi rezultatai

- Besimokantieji gebės įgyvendinti kibernetinio saugumo taisykles ir nustatyti jų nuolatinės stebėsenos bei vykdymo užtikrinimo procedūras.</td></tr>
</table>

7 lentelė – 6 modulis

Skyriai	**Temos**
Įvadas į kibernetinio saugumo planavimą: duomenų, žmonių ir visuomenės saugumas	Duomenų saugumas – informacijos saugojimo saugumas, tyrimo procesas Duomenų saugumas – slaptažodžių atakos metodai Žmogaus saugumas – sąmoningumas ir supratimas Visuomenės saugumas – kas yra kibernetiniai nusikaltimai, kibernetinė etika Visuomenės saugumas – kibernetiniai įstatymai – skaitmeniniai įrodymai, skaitmeniniai kontraktai, tarptautinės konvencijos (susitarimai)
Mokymosi rezultatai • Besimokantieji gebės įgyvendinti strategijas, skirtas saugoti informaciją ir palaikyti tyrimo procesus. • Besimokantieji gebės nustatyti ir analizuoti dažniausiai pasitaikančius slaptažodžių atakų metodus bei parengti atitinkamas apsaugos priemones. • Besimokantieji gebės didinti kibernetinio saugumo sąmoningumą ir skatinti darbuotojų bei suinteresuotųjų šalių supratimą. • Besimokantieji gebės paaiškinti visuomenines kibernetinių nusikaltimų pasekmes ir įvertinti etinius aspektus skaitmeninėje aplinkoje. • Besimokantieji gebės interpretuoti pagrindines kibernetinės teisės sąvokas, įskaitant skaitmeninius įrodymus, sutartis ir tarptautinius susitarimus.	
Operacinis ir taktinis valdymas	Prieigos kontrolės įgyvendinimas Pataisų valdymas ir programinės įrangos atnaujinimai Nuolatinis sistemos stebėjimas Darbuotojų saugumo sąmoningumo mokymas
Mokymosi rezultatai: • Besimokantieji gebės kurti ir diegti efektyvius prieigos kontrolės mechanizmus, skirtus sistemoms ir duomenims apsaugoti. • Besimokantieji gebės nustatyti savalaikio pataisymų valdymo ir programinės įrangos atnaujinimo procedūras, siekdami sumažinti pažeidžiamumus. • Besimokantieji gebės vykdyti nuolatinę sistemų stebėseną, kad aptiktų saugumo įvykius ir į juos reaguotų. • Besimokantieji gebės kurti ir vesti saugumo sąmoningumo mokymų programas, skirtas didinti darbuotojų įsitraukimą ir mažinti žmogiškąją riziką.	

8 lentelė – 7 modulis

Skyriai	**Temos**
Rizikos vertinimas	Bendrasis rizikos valdymo modelis ir procesas Rizikos valdymo principai Rizikos valdymo standartai Praktiniai pavyzdžiai ir atvejų analizė
Mokymosi rezultatai: • Besimokantieji gebės apibūdinti ir taikyti bendrąją rizikos valdymo sistemą bei procesą kibernetiniame saugume. • Besimokantieji gebės paaiškinti pagrindinius principus, kuriais grindžiamas efektyvus kibernetinio saugumo rizikos valdymas. • Besimokantieji gebės nustatyti ir interpretuoti plačiai pripažintus rizikos valdymo standartus. • Besimokantieji gebės įvertinti rizikos scenarijus nagrinėdami realius pavyzdžius ir atvejų studijas.	
Rizikos identifikavimas	Apčiuopiami ir neapčiuopiami rizikos šaltiniai Priežastys ir įvykiai Grėsmės ir galimybės Pažeidžiamumas ir galimybės Išorės ir vidaus konteksto pokyčiai Kylančių rizikų rodikliai Turto ir išteklių pobūdis ir vertė Pasekmės ir jų poveikis tikslams Žinių ribotumas ir informacijos patikimumas Dalyvių šališkumas, prielaidos ir įsitikinimai. Praktiniai pavyzdžiai ir atvejų analizė.
Mokymosi rezultatai: • Besimokantieji gebės atskirti materialius ir nematerialius rizikos šaltinius kibernetinio saugumo aplinkoje. • Besimokantieji gebės nustatyti rizikos priežastis ir ją sukeliančius įvykius. • Besimokantieji gebės analizuoti kibernetinio saugumo grėsmes ir įvertinti galimybes tobulėjimui. • Besimokantieji gebės įvertinti pažeidžiamumus ir organizacijos gebėjimus valdyti riziką. • Besimokantieji gebės įvertinti, kaip aplinkos pokyčiai veikia kibernetinio saugumo rizikas. • Besimokantieji gebės atpažinti indikatorius, signalizuojančius apie naujų kibernetinio saugumo grėsmių atsiradimą. • Besimokantieji gebės įvertinti turto vertę ir išteklių svarbą rizikos atžvilgiu. • Besimokantieji gebės numatyti galimas pasekmes ir jų poveikį strateginiams tikslams. • Besimokantieji gebės pripažinti informacijos ir žinių ribotumą rizikos identifikavimo procese. • Besimokantieji gebės įvertinti, kaip žmogiškieji veiksniai veikia rizikos suvokimą ir identifikavimą. • Besimokantieji gebės taikyti identifikavimo metodus analizuodami realius scenarijus.	
Vidaus grėsmės	Vidinių grėsmių apibrėžimas ir tipai

	Vidinių grėsmių aptikimas ir identifikavimas Praktiniai pavyzdžiai ir atvejų analizė
Mokymosi rezultatai: • Besimokantieji gebės apibrėžti vidines grėsmes ir klasifikuoti įvairius jų tipus. • Besimokantieji gebės ugdyti įgūdžius, reikalingus aptikti vidinių grėsmių indikatorius ir į juos reaguoti. • Besimokantieji gebės analizuoti realių vidinių grėsmių incidentų atvejų studijas.	
Rizikos matavimo ir vertinimo modeliai bei metodikos	Kiekybiniai ir kokybiniai rizikos vertinimo modeliai ir metodikos Įvykių ir pasekmių tikimybė Pasekmių pobūdis ir mastas Jautrumo ir pasitikėjimo lygiai. Praktiniai pavyzdžiai ir atvejų analizė
Mokymosi rezultatai: • Besimokantieji gebės palyginti ir taikyti tiek kiekybinius, tiek kokybinius modelius atlikdami kibernetinio saugumo rizikos vertinimą. • Besimokantieji gebės įvertinti nustatytų rizikų tikimybę ir galimus rezultatus. • Besimokantieji gebės įvertinti su kibernetinio saugumo rizikomis susijusių pasekmių sunkumą ir mastą. • Besimokantieji gebės nustatyti neapibrėžtumo ir patikimumo lygius atliekant rizikos vertinimą. • Besimokantieji gebės taikyti rizikos vertinimo modelius praktiniuose scenarijuose.	
Rizikos kontrolė	Stebėjimas ir peržiūra Įrašymas ir ataskaitų teikimas Praktiniai pavyzdžiai ir atvejų analizė
Mokymosi rezultatai • Besimokantieji gebės reguliariai vykdyti rizikos stebėsenos ir peržiūros procesus. • Besimokantieji gebės efektyviai dokumentuoti rizikos kontrolės priemones ir teikti apie jas ataskaitas. • Besimokantieji gebės nagrinėti realius pavyzdžius, kad suprastų efektyvų rizikos kontrolės priemonių įgyvendinimą.	

9 lentelė – 8 modulis

Skyriai	**Temos**
Reagavimas į incidentus	Incidentų reagavimo apibrėžimas ir svarba Veiksmingo incidentų reagavimo atkūrimo plano pagrindiniai komponentai Dažniausiai pasitaikančios kibernetinio saugumo grėsmės
Mokymosi rezultatai • Besimokantieji gebės apibrėžti reagavimą į incidentus ir paaiškinti jo reikšmę kibernetinio saugumo valdyme. • Besimokantieji gebės nustatyti ir įgyvendinti pagrindinius struktūrizuoto reagavimo į incidentus atkūrimo plano elementus. • Besimokantieji gebės atpažinti dažniausias kibernetinio saugumo grėsmes, su kuriomis susiduriama tvarkant incidentus, ir į jas reaguoti.	

Atkūrimas po nelaimių	Supratimas apie atkūrimą po nelaimės Vaidmenys ir atsakomybė atkuriant veiklą po nelaimės Atkūrimo veiksmai po nelaimės
Mokymosi rezultatai • Besimokantieji gebės paaiškinti atkūrimo po avarijų principus ir tikslus kibernetinio saugumo kontekste. • Besimokantieji gebės apibūdinti komandos narių, dalyvaujančių atkuriant po avarijų, vaidmenis ir atsakomybes. • Besimokantieji gebės parengti žingsnis po žingsnio planą, kaip atkurti sistemas ir veiklą po kibernetinės nelaimės.	
Verslo tęstinumas	Verslo tęstinumo supratimas Vaidmenys ir atsakomybė užtikrinant verslo tęstinumą Verslo poveikio analizė
Mokymosi rezultatai: • Besimokantieji gebės paaiškinti veiklos tęstinumo planavimo koncepciją ir svarbą. • Besimokantieji gebės nustatyti vaidmenis ir atsakomybes, susijusias su veiklos tęstinumo užtikrinimu. • Besimokantieji gebės atlikti poveikio verslui analizę, siekdami įvertinti kritines funkcijas ir priklausomybes.	
Saugumo sąmoningumas, mokymas ir švietimas	Saugumo sąmoningumo supratimas Darbuotojų atsakomybė kibernetinio saugumo srityje
Mokymosi rezultatai • Besimokantieji gebės paaiškinti saugumo sąmoningumo vaidmenį mažinant su žmogiškuoju faktoriumi susijusias kibernetinio saugumo rizikas. • Besimokantieji gebės atpažinti darbuotojų atsakomybes laikantis kibernetinio saugumo protokolų ir gerosios praktikos.	
Saugumo įdarbinimo praktika	Saugumo pareigų reikalavimų apibrėžimas Išsamios praeities patikros
Mokymosi rezultatai • Besimokantieji gebės apibrėžti kibernetinio saugumo darbo vaidmenis ir suformuluoti atitinkamus reikalavimus. • Besimokantieji gebės taikyti gerosios praktikos pavyzdžius atliekant biografijos patikrinimus pozicijoms, susijusioms su saugumu.	
Saugumo nutraukimo praktika	Nedelsiant atšaukti prieigą Pranešimas atitinkamoms komandoms Teisiniai ir atitikties reikalavimams aspektai
Mokymosi rezultatai • Besimokantieji gebės įgyvendinti procedūras, skirtas skubiai panaikinti prieigą nutraukus darbo santykius su darbuotoju. • Besimokantieji gebės koordinuoti komunikaciją su atitinkamais skyriais atleidimo iš darbo proceso metu. • Besimokantieji gebės nagrinėti teisinius ir atitikties reikalavimus, susijusius su darbo santykių nutraukimu kibernetinio saugumo srityje.	
Trečiųjų šalių saugumas	Trečiųjų šalių rizikos vertinimas Kontrastų ir saugumo reikalavimų įgyvendinimas Nuolatinis stebėjimas ir auditas

	Reagavimas į incidentus ir komunikacija
Mokymosi rezultatai: • Besimokantieji gebės įvertinti saugumo rizikas, susijusias su trečiųjų šalių tiekėjais ir partneriais. • Besimokantieji gebės parengti ir taikyti sutartines sąlygas, siekdami užtikrinti trečiųjų šalių atitiktį saugumo reikalavimams. • Besimokantieji gebės nustatyti nuolatinės trečiųjų šalių saugumo stebėsenos ir audito praktikas. • Besimokantieji gebės koordinuoti veiksmus su trečiosiomis šalimis reaguojant į incidentus.	
Saugumas peržiūros procesuose	Saugumo įtraukimas į peržiūras Pažeidžiamumo vertinimas ir įsiskverbimo testavimas Peržiūros po incidentų
Mokymosi rezultatai: • Besimokantieji gebės integruoti saugumo aspektus į organizacijos peržiūros procesus. • Besimokantieji gebės atlikti pažeidžiamumo vertinimus ir įsiskverbimo testavimą kaip peržiūros veiklų dalį. • Besimokantieji gebės atlikti peržiūras po incidentų, siekdami įvertinti efektyvumą ir pagerinti būsimus atsakus.	
Darbuotojų duomenų saugumas	Duomenų rinkimo apribojimai Saugojimas ir prieigos kontrolė Privatumo taisyklių laikymasis Duomenų dalijimasis ir trečiosios šalys Darbuotojų sutikimas ir teisės
Mokymosi rezultatai: • Besimokantieji gebės nustatyti tinkamas ribas renkant darbuotojų asmens duomenis. • Besimokantieji gebės taikyti saugaus saugojimo ir prieigos kontrolės priemones jautriems darbuotojų duomenims. • Besimokantieji gebės užtikrinti atitiktį susijusiems privatumo reglamentams, tokiems kaip BDAR. • Besimokantieji gebės įvertinti rizikas ir taisykles, susijusias su dalijimusi darbuotojų duomenimis su trečiosiomis šalimis. • Besimokantieji gebės suprasti darbuotojų teises ir informuoto sutikimo gavimo svarbą.	

IŠVADA

Šioje ataskaitoje pateikiama profesinio mokymo lygį atitinkanti mokymo programa, parengta siekiant sėkmingai įgyvendinti CyberAgent mokymus. Remiantis nuo projekto pradžios atliktu mokymosi poreikių tyrimu, šiame dokumente apibrėžiamos profesinio mokymo studentams reikalingos kompetencijos.

Rengiant šią programą buvo remtasi CyberAgent projektui sukurta 5-6 EKS lygio mokymo programa. Iš jos buvo atrinktos temos, tinkamos 4-5 EKS lygiui.

Galiausiai, siekiant užtikrinti aukščiausią mokymų turinio, organizavimo ir įgūdžių ugdymo kokybę, į galutinį vertinimą nebus įtraukti klausimai iš tų 5-6 EKS lygio programos temų.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau