Bendrai finansuoja Europos Sąjunga

CYBARVERSE

Kibernetinis saugumas profesiniame rengime pasitelkiant įtraukiąsias technologijas *CybARverse*

Gerosios patirties gairės

Dokumentą parengė:

projekto partneriai SCP, LIA, CCS, EOS ir Tech.mt.

2024 m. spalis

Bendrai finansuoja Europos Sąjunga

PROJEKTO SANTRAUKA

„CybARverse“ - tai programos „Erasmus+“ bendrai finansuojamas projektas, kuriuo siekiama padėti IT bei kitų dalykų mokytojams ir dėstytojams tobulinti skaitmeninius įgūdžius naudojant įtraukiančias technologijas. Šiame projekte pagrindinis dėmesys skiriamas tikslinės grupės mokymui, kaip atpažinti kibernetines atakas ir tinkamai į jas reaguoti. Projektas padeda gerinti supratimą apie kibernetinį saugumą, įgyvendinti Skaitmeninio švietimo veiksmų planą (5 ir 7 veiksmai) bei nacionalines darbotvarkes ir prisideda prie skaitmeninio, ekologiškesnio ir įtraukesnio mokymo ir mokymosi.

Projekto Nr. 2022-1-LT01-KA220-VET-000089116

Tikslai

- Skatinti profesinio mokymo mokytojų ir dėstytojų profesinius, asmeninius ir skaitmeninius įgūdžius kibernetinio saugumo srityje.
- Į profesinio mokymo kibernetinio saugumo mokymą įtraukti modernias ir įtraukiančias technologijas.
- Sistemingai kelti mokytojų ir dėstytojų kvalifikaciją, kad jie įgytų kibernetinio saugumo žinių ir raštingumo.
- Užtikrinti projekto rezultatų tvarumą.

Projektą įgyvendina:

Šis projektas finansuojamas remiant Europos Komisijai. Šis leidinys atspindi tik autoriaus požiūrį, todėl Europos Komisija, jos institucijos ir Švietimo mainų paramos fondas negali būti laikomi atsakingi už šios medžiagos turinį ir bet kokį pateikiamos informacijos naudojimą.

TURINYS

1. ĮVADAS

1.1. Projektas ir jo tikslai

Pagal programą „Erasmus+“ įgyvendintas projektas „CybARverse“ skirtas skaitmeninio raštingumo ir kibernetinio saugumo įgūdžiams gerinti, pasitelkiant įtraukiančias technologijas profesinio mokymo sistemoje. Projektu, kuriam vadovauja asociacija „Langas į ateitį“ Lietuvoje ir kuris vykdomas bendradarbiaujant su „S.C.P. Serv Limited“ ir Kipro kompiuterininkų draugija Kipre, „Tech.mt“ Maltoje ir „Fundatia EOS - Educating for an Open Society“ Rumunijoje, siekiama pašalinti esamas skaitmeninių įgūdžių spragas, į profesinio mokymo programas įtraukiant naujausias papildytosios (AR) ir virtualiosios realybės (VR) technologijas. Toks metodas ne tik praturtina mokymosi patirtį, bet ir pasiūlo pedagogams ir instruktoriams būtinų priemonių, padedančių perteikti esminius kibernetinio saugumo įgūdžius, taip didinant švietimo aplinkos atsparumą kibernetinėms grėsmėms.

1.1.1. Pagrindiniai projekto uždaviniai

Projekto „CybARverse“ struktūra apima keturis pagrindinius uždavinius, kurių kiekvienas skirtas visapusiškam ir tvariam poveikiui kibernetinio saugumo švietimo srityje stiprinti.

1. **Profesinių, asmeninių ir skaitmeninių kompetencijų tobulinimas**.

- **Profesinis tobulėjimas:** suteikti pedagogams ir instruktoriams naujausių kibernetinio saugumo žinių ir patirties, kad jie galėtų veiksmingai reaguoti į kylančias kibernetines grėsmes ir jas įveikti.
- **Asmeninis tobulėjimas**: ugdyti esminius įgūdžius, tokius kaip kritinis mąstymas, problemų sprendimas ir sprendimų priėmimas, pasitelkiant interaktyvią ir scenarijais pagrįstą mokymosi patirtį.
- **Skaitmeninė kompetencija**: tobulinti profesinio mokymo specialistų skaitmeninius gebėjimus, ypatingą dėmesį skiriant išmaniajam AR ir VR technologijų naudojimui, siekiant modeliuoti kibernetinio saugumo iššūkius ir į juos reaguoti.

2. **Šiuolaikinių ir įtraukiančių technologijų integravimas.**

- AR ir VR panaudojimas kuriant dinamišką, įtraukiančią mokymo aplinką, kurioje imituojami realūs kibernetinio saugumo scenarijai ir kuri suteikia patirtinę mokymosi patirtį, pranokstančią tradicinius mokymo metodus.

3. **Struktūrizuota profesinė kvalifikacija.**

   - Nuosekli daugiapakopė mokymo programa, kuri sistemingai didintų kibernetinio saugumo informuotumą ir kompetenciją, pradedant fundamentaliomis žiniomis ir baigiant pažangiomis veikimo kompetencijomis.

4. **Tvarus švietimo poveikis.**

   - Tvarus švietimo modelis, apimantis nuolatinį profesinį tobulėjimą ir mokymo medžiagos atnaujinimą, užtikrinantis, kad mokymo programa atitiktų sparčią kibernetinio saugumo grėsmių ir technologijų raidą. Taip pat stiprinama patirties bendruomenė, palaikanti nuolatinį mokymąsi ir dalijimąsi gerąja patirtimi tarp kibernetinio saugumo mokytojų.

Laikantis šių uždavinių, „CybARverse“ projektu siekiama sukurti patikimą mokymo sistemą, kuri ne tik atitiktų dabartinius poreikius, bet ir prisitaikytų prie būsimų kibernetinio saugumo mokymo srities poreikių.

1.2. Metodinės rekomendacijos ir jų vaidmuo

Laikantis išsamaus požiūrio į kibernetinio saugumo švietimo gerinimą profesinio mokymo sistemoje, įgyvendinant projektą „CybARverse“ parengtas svarbus dokumentas „Metodinės rekomendacijos“. Šis dokumentas atlieka pagrindinį vaidmenį profesinio rengimo ir mokymo pedagogams nurodant veiksmingus būdus, kaip integruoti pažangias skaitmenines ir įtraukiančias technologijas mokymo procese.

1.3. Metodinių rekomendacijų tikslas ir poveikis

Metodinės rekomendacijos pateikia pedagogams ir mokytojams išsamią informaciją apie papildytosios ir virtualiosios realybės (AR) ir virtualiosios realybės (VR) technologijų pedagogiškai pagrįstą taikymą. Šios rekomendacijos yra labai svarbios siekiant pagrindinių „CybARverse“ projekto tikslų.

1. **Skaitmeninių įgūdžių tobulinimas.** Šiose rekomendacijose išsamiai aprašomas AR ir VR taikymas švietimo įstaigose, todėl pedagogai įgyja įgūdžių, kaip veiksmingai įtraukti šias technologijas į mokymo programas ir taip pagerinti besimokančiųjų skaitmeninius gebėjimus.

2. **Struktūrizuoti mokymosi keliai.** Šiose rekomendacijose pateikiami struktūruoti įtraukiančiųjų technologijų naudojimo principai, užtikrinantys, kad mokymas būtų sistemingas ir išsamus. Tai padeda formuoti aukštos kvalifikacijos profesinio mokymo mokytojų, išmanančių kibernetinį saugumą ir skaitmeninį raštingumą, gretas.

3. **Įtraukios švietimo veiklos skatinimas.** Taikydami rekomendacijose siūlomus naujoviškus mokymo metodus, pedagogai gali sukurti patrauklesnę ir interaktyvesnę mokymosi patirtį. Tai ne tik pagerintų ugdymo kokybę, bet ir padarytų mokymąsi patrauklesnį ir efektyvesnį mokiniams.

4. **Švietimo veiklos tvarumas.** Rekomendacijose raginama nuolat atnaujinti ir pritaikyti mokymo strategijas, kad jos neatsiliktų nuo technologinės pažangos. Toks požiūris užtikrina, kad ugdymo turinys išliktų aktualus, o projekto nauda būtų ilgalaikė.

Nors metodinės rekomendacijos yra savarankiškas „CybARverse“ projekto rezultatas, jos papildo platesnius „Gerosios patirties gairėse“ išdėstytus tikslus, nes jose praktiškai pritaikomos aptartos teorinės sistemos. Pedagogams, kurie naudosis „Gerosios patirties gairėmis“, metodinės rekomendacijos bus neįkainojamas šaltinis, padėsiantis veiksmingai įgyvendinti siūlomą metodiką.

Metodinės rekomendacijos nėra tik instrukcijų rinkinys; tai permainų priemonė, įgalinanti pedagogus išnaudoti šiuolaikinių technologijų potencialą kibernetinio saugumo švietimui. Išsamiai aprašydamos veiksmingą AR ir VR naudojimą, šios rekomendacijos padeda sumažinti atotrūkį tarp tradicinių mokymo metodų ir skaitmeninio amžiaus reikalavimų.

Šios rekomendacijos parodo projekto „CybARverse“ įsipareigojimą siekti holistinės švietimo strategijos, kuri yra ir perspektyvi, ir pagrįsta praktiniu taikymu. Šiame aprašyme pabrėžiamas abiejų dokumentų tarpusavio ryšys ir jų bendras poveikis ugdymo praktikos tobulinimui.

Metodinių rekomendacijų dokumentą rasite čia: https://www.cybarverse.eu/teacher-center/.

1.4. Mokymosi lygių apžvalga

Projektas „CybARverse“ siūlo tris nuoseklius mokymo lygius, pritaikytus skirtingiems dalyvių skaitmeninių technologijų ir kibernetinio saugumo išmanymo bei patirties lygiams.

1. **Pradmenų lygis.** Šiame pradiniame lygyje supažindinama su pagrindinėmis skaitmeninio raštingumo ir kibernetinio saugumo sąvokomis, orientuojantis į tuos mokytojus ir dėstytojus, kurie yra skaitmeninės srities naujokai. Tai padeda pagrindus sudėtingesniam mokymuisi.
2. **Pagrindų lygis.** Šiame lygyje plėtojamos bazinės žinios, nagrinėjant sudėtingesnius kibernetinio saugumo procesus ir skaitmeninę veiklą. Dalyviai naudojasi interaktyviais AR ir VR scenarijais, kuriuose imituojamos realios kibernetinės grėsmės, o tai gerina jų analitinius ir problemų sprendimo įgūdžius.

3. **Pažengusiųjų lygis.** Šis sudėtingiausias lygis yra skirtas dalyviams, kurie gerai išmano skaitmenines priemones ir kibernetinį saugumą. Jame daugiausia dėmesio skiriama tokioms specializuotoms sritims kaip grėsmių analizė, pažangūs programavimo būdai ir strateginis kibernetinio saugumo priemonių įgyvendinimas švietimo įstaigose.

1.5. Trumpas kurso turinio ir sandaros aprašymas

Projekto „CybARverse“ mokymo sistema kruopščiai sudaryta taip, kad būtų galima įgyti visapusiškos edukacinės patirties, kuri būtų įtraukianti ir informatyvi. Kursų turinys sukurtas siekiant ugdyti skaitmeninį raštingumą ir gebėjimus praktiškai naudotis kibernetinio saugumo priemonėmis, papildytas inovatyviomis AR ir VR technologijomis.

- Kurso turinys. Mokymo programa apjungia teorines žinias ir praktinius kibernetinio saugumo įgūdžius, taip pat išsamiai supažindina su AR ir VR technologijomis ir jų taikymu švietimo įstaigose. Kiekvienas modulis yra sukurtas taip, kad remtųsi ankstesniuoju moduliu, todėl sulig kiekvienu moduliu gilinamos žinios ir didinamas įgūdžių lygis.

- Kurso sandara. Kursas sudarytas iš modulių, todėl kiekvienas kibernetinio saugumo ir skaitmeninio raštingumo aspektas nagrinėjamas kryptingai. Jame integruoti interaktyvūs elementai, pavyzdžiui, VR ir AR modeliavimas, dirbtuvės ir tiesioginiai internetiniai seminarai, kuriuos rengia šios srities ekspertai. Po kiekvieno modulio atliekamas išsamus vertinimas, siekiant užtikrinti, kad dalyviai suprastų medžiagą ir būtų pasirengę tolesniems lygiams.

- Interaktyvūs komponentai. Naudojant AR ir VR technologijas, kurse kuriami realistiški scenarijai, pagal kuriuos dalyviai gali pritaikyti kibernetinio saugumo įgūdžius virtualioje, tačiau tikroviškoje aplinkoje. Šis metodas ne tik padeda sustiprinti mokymąsi, bet ir paruošia juos veiksmingai spręsti panašius iššūkius realioje aplinkoje.

Projektas „CybARverse“ numato ne tik pagrindinę mokymo programą, bet ir nuolatinio profesinio tobulėjimo komponentus, kad mokytojai ir instruktoriai galėtų neatsilikti nuo naujausių kibernetinio saugumo tendencijų bei technologinės pažangos. Šis nuolatinis mokymosi procesas užtikrina, kad mokymo metodikos išliktų aktualios ir veiksmingos, taip dar labiau sustiprinant bendrą kibernetinio saugumo būklę atitinkamoje švietimo aplinkoje.

Integruojant šias pažangias technologines priemones su ekspertų parengtu mokymo turiniu, „CybARverse“ gerosios patirties gairėse siekiama suteikti profesinio mokymo mokytojams ir instruktoriams reikiamų įgūdžių, kad jie galėtų veiksmingai mokyti kibernetinio saugumo, taip

prisidedant prie saugesnės skaitmeninės ateities kūrimo. Puoselėdama nuolatinio mokymosi ir prisitaikymo ekosistemą, „CybARverse“ užtikrina, kad jos naudos gavėjai būtų gerai pasirengę vadovauti ir diegti naujoves nuolat besikeičiančioje skaitmeninėje aplinkoje, o tai galiausiai padidintų jų švietimo poveikį ir efektyvumą.

2. MOKYMOSI VALDYMO SISTEMA (MVS)

Kurso turinys pateikiamas „LearnPress“ mokymosi valdymo sistemoje (MVS). Tai viena iš plačiausiai naudojamų internetiniams kursams skirtų MVS, suteikianti galimybę kurti kurso turinį iš pamokų ir testų, turinti lengvai naudojamą sąsają besimokantiesiems vartotojams.

2.1. Kurso sandara

Kursas sukurtas taip, kad jo struktūra būtų modulinė, leidžianti tikslingai nagrinėti kiekvieną kibernetinio saugumo ir skaitmeninio raštingumo aspektą. Jame integruoti interaktyvūs elementai, pavyzdžiui, VR ir AR modeliavimo priemonės, seminarai ir tiesioginiai internetiniai seminarai, kuriuos rengtų šios srities ekspertai. Po kiekvieno modulio atliekamas nuodugnus žinių vertinimas, kad būtų patikrintas dalyvių supratimas ir pasirengimas vėlesniems lygiams.

Kursą sudaro 17 mokymosi modulių, suskirstytų į tris skirtingus lygius, todėl besimokantieji gali pasirinkti jiems labiausiai tinkamus.

Pradmenų lygyje nagrinėjamos šešios pradedantiesiems svarbiausios kibernetinio saugumo temos, mokymosi apimtis – 6 valandos:

- įvadas į kenkėjiškas programas,
- socialinė inžinerija,
- viliojimas,
- socialinės žiniasklaidos grėsmės,
- duomenų išviliojimas,
- daiktų interneto atakos.

Pagrindų lygio kurse nagrinėjamos šešios sudėtingesnės kibernetinio saugumo grėsmės, mokymosi apimtis - 8 valandos:

- išpirkos reikalaujanti programinė įranga,
- šakninė kenkėjiška programinė įranga,
- apgaulinga IP taktika,
- kriptovaliutinė vagystė,
- kryžminiai svetainės scenarijai,
- SQL injekcijos.

Pažengusiųjų lygyje nagrinėjamos 5 sudėtingos kibernetinio saugumo grėsmės, mokymosi apimtis - 10 valandų:

- tarpininko atakos,
- daiktų interneto pažeidžiamumai,
- nulinės dienos spragų išnaudojimas,
- DoS atakos,
- DDoS atakos.

Kiekvieno modulio struktūra yra panaši.

1. Teoriniai skaitiniai, kuriuose aprašoma pati grėsmė, požymiai, leidžiantys atpažinti grėsmę, ir grėsmės valdymo ar prevencijos priemonės. Teorinė medžiaga pateikiama struktūruotai ir kartu išsamiai, kad besimokantysis galėtų geriau suprasti grėsmę.
2. Keletas atvejo studijų, padedančių geriau suprasti aprašytos grėsmės aktualumą šiuolaikiniame internetiniame pasaulyje.
3. Interaktyvūs komponentai – vaizdo įrašai, AR, VR, „WebVR“ technologijos objektai, padedantys sukurti tikroviškus scenarijus, pagal kuriuos besimokantieji gali taikyti kibernetinio saugumo įgūdžius virtualioje, tačiau gyvenimiškoje aplinkoje.
4. Kiekviename modulyje pateikiami pamokų planai, kad būtų galima modeliuoti ir perprasti šias grėsmes, taip pat suteikti besimokantiesiems papildomų žinių.
5. Kiekvieno lygio kursas baigiamas testu, kuriuo įvertinamos profesinio mokymo mokytojų įgytos žinios ir kompetencija. Norint gauti kurso pažymėjimą, būtina išlaikyti testą.

2.2. Veiksmingos mokymosi internetu strategijos

Projekto metu sukurtą kursą galima naudoti savarankiškam individualiam mokymuisi arba profesinio mokymo įstaiga gali organizuoti internetinius ar mišrius kursus visai grupei.

Besimokantieji turėtų gauti dėstytojo pagalbą tiek dalyko, tiek LMS ir išteklių naudojimo klausimais.

2.2.1. Instruktoriams ir pedagogams

Organizuojant mokymus pagal šio internetinio kurso medžiagą, reikėtų atsižvelgti į šiuos dalykus.

1. **Kurso išdėstymas ir sandara**

   - **Aiškūs tikslai.** Nustatykite aiškius kiekvieno modulio mokymosi tikslus ir rezultatus. Tai padės studentams suprasti, ko jie turėtų išmokti ir pasiekti.

- **Modulinis turinys.** Kurso turinys suskirstomas į lengvai valdomus modulius arba skyrius. Kiekvienas modulis turėtų apimti konkrečią kibernetinio saugumo temą ar įgūdžius.
- **Interaktyvieji elementai**. kiekviename modulyje pateikiami interaktyvūs elementai, pavyzdžiui, testai, demonstravimas, modeliavimas, atvejo analizė ir VR bei AR praktiniai darbai. Ši veikla padeda įtvirtinti mokymąsi ir sudominti mokinius.
- **Įvairialypės terpės ištekliai.** Pasitelkite įvairialypės terpės išteklius, taip pat ir esančius kurse ar internetinius vaizdo įrašus, kad galėtumėte prisitaikyti prie įvairių mokymosi stilių.

2. **Įsitraukimas ir bendradarbiavimas**

- **Diskusijų forumai.** Sukurkite diskusijų forumus (pvz., socialiniame tinkle), kuriuose mokiniai galėtų užduoti klausimus, dalytis įžvalgomis ir bendradarbiauti. Skatinkite aktyviai dalyvauti pateikdami mąstymą skatinančius klausimus.
- **Tiesioginės pamokos.** Suplanuokite reguliarias tiesiogines pamokas (internetinius seminarus arba virtualias pamokas), kad būtų galima bendrauti realiuoju laiku ir gauti atsiliepimus. Šiose pamokose pasitelkite klausimus ir atsakymus, diskusijas, į jas pakvieskite tos pramonės srities ekspertus.
- **Grįžtamojo ryšio priemonės**. Stebėkite besimokančiųjų pažangą ir laiku pateikite konstruktyvius atsiliepimus.

3. **Vertinimas**

- **Formuojamieji ir apibendrinamieji vertinimai**. Kiekvieno kurso baigiamasis testas yra kaip apibendrinamasis vertinimas, tačiau dėstytojas gali naudoti savo trumpas užduotis, kad galėtų įvertinti studentų supratimą viso kurso metu. Tai leidžia prireikus laiku įsikišti į mokymosi procesą.

4. **Techninė parama ir ištekliai**

- **Techninė pagalba.** Suteikite aiškius nurodymus ir pagalbą naudojantis internetine mokymosi sistema ir priemonėmis. Pasiūlykite mokomąsias instrukcijas ir atsakymus į dažniausiai užduodamus klausimus, kad padėtumėte mokiniams naudotis technologijomis.

- **Išteklių prieinamumas.** Užtikrinkite, kad visa kurso medžiaga būtų prieinama neįgaliems studentams. Naudokite prieinamus formatus ir prireikus pateikite alternatyvius išteklius.

5. **Veiklų internete ir neprisijungus integravimas**

- **Sklandus perėjimas.** Užtikrinkite sklandų perėjimą tarp veiklų internete ir neprisijungus. Suderinkite internetinius modulius su asmeniniais užsiėmimais, taip sustiprindami mokymąsi.

- **Mišrios užduotys.** Sukurkite užduotis, kurias atliekant reikia ir atlikti internetinius tyrimus, ir atlikti veiklas neprisijungus. Tai padeda mokiniams integruoti žinias iš įvairių šaltinių.

2.2.2. Dalyviams

1. **Laiko valdymas**

- **Sudarykite tvarkaraštį.** Sukurkite studijų tvarkaraštį, kuriame būtų numatytas laikas, skirtas tiesioginėms pamokoms, užduotims atlikti ir kurso medžiagai peržiūrėti. Laikykitės šio tvarkaraščio, kad nenukryptumėte nuo plano.

- **Nustatykite užduočių prioritetus.** Nustatykite užduočių prioritetus pagal terminus ir svarbą. Siekdami efektyviai valdyti darbo krūvį, naudokitės tokiomis priemonėmis kaip darbų sąrašai ir kalendoriai.

2. **Aktyvus dalyvavimas**

- **Dalyvaukite diskusijose.** Dalyvaukite diskusijų forumuose ir tiesioginėse transliacijose. Dalinkitės savo įžvalgomis, užduokite klausimus ir bendradarbiaukite su kolegomis.

- **Prašykite informacijos.** Nedvejodami kreipkitės į dėstytojus ir kolegas. Naudokitės jų atsiliepimais, kad pagerintumėte savo supratimą ir rezultatus.

3. **Savimotyvacija ir drausmė**

- **Nustatykite tikslus.** Nustatykite konkrečius, pasiekiamus tikslus kiekvienai mokymosi sesijai. Tai padeda išlaikyti dėmesį ir motyvaciją.

- **Laikykitės drausmės.** Būkite drausmingi ir mokymosi metu kuo mažiau blaškykite dėmesį. Sukurkite palankią mokymosi aplinką, kurioje nebūtų trukdžių.

4. **Naudokitės ištekliais**

   - **Įvairialypės terpės panaudojimas.** Pasinaudokite kurso metu pateiktais multimedijos ištekliais. Žiūrėkite vaizdo įrašus ir vaizdines priemones, kad geriau įsisavintumėte žinias.
   - **Įgykite praktinių įgūdžių.** Pasinaudokite VR/AR modeliavimu ir pritaikykite teorines žinias praktiniuose scenarijuose. Tai ypač svarbu kibernetinio saugumo mokymuose.

2.3. Prieinamumo ir įtraukties aspektai atsižvelgiant į besimokančiųjų įvairovę

Norint užtikrinti, kad visi besimokantieji, nepriklausomai nuo jų gebėjimų ar padėties, galėtų visapusiškai dalyvauti mokymosi procese ir gauti naudos iš jo, būtina kurti prieinamą ir įtraukią mokymosi medžiagą ir interneto svetaines. Nors projekte siūloma jau parengta mokymosi medžiaga, ją reikės atnaujinti, ji gali būti lokalizuota kitose šalyse ir bus naudojama pedagogų įvairiems, pavyzdžiui, mišriems mokymosi kursams rengti.

2.3.1. Prieinamumas - svarbiausieji aspektai

Pateikiame keletą svarbiausių aspektų, susijusių su kursų kūrimu ir taikymu.

1. Universalus mokymosi modelis

Universalusis mokymosi modelis (UMM) - tai švietimo sistema, kuria siekiama sukurti visiems besimokantiesiems pritaikytą mokymosi aplinką. UMM principai yra šie.

- **Įvairūs pateikimo būdai.** Informacija pateikiama įvairiais formatais, pavyzdžiui, tekstu, vaizdo įrašais, garso įrašais ir interaktyviais elementais, kad būtų atsižvelgta į skirtingus mokymosi poreikius.
- **Įvairios raiškos priemonės.** Suteikite besimokantiesiems galimybę parodyti savo žinias įvairiais būdais, pavyzdžiui, raštu, pateiktimis ar projektais.
- **Kelios įsitraukimo priemonės.** Motyvaciją ir įsitraukimą skatinkite siūlydami įvairią veiklą ir užduotis, atitinkančias besimokančiųjų interesus ir poreikius.

2. Prieinamumas

Prieinamumo užtikrinimas reiškia, kad mokymosi medžiaga turi būti prieinama visiems, įskaitant neįgaliuosius. Pagrindiniai aspektai yra šie.

- **Alternatyvus vaizdinio ir garsinio turinio tekstas**. Pateikite tekstinius paveikslėlių aprašymus ir vaizdo įrašų antraštes, kad visas turinys būtų prieinamas.

- **Tinkamas spalvų kontrastas**. Naudokite lengvai įskaitomus ir suprantamus spalvų derinius, ypač regos sutrikimų turintiems asmenims.
- **Suderinamumas su ekrano skaitytuvais**. Užtikrinkite, kad svetainės ir dokumentai būtų suderinami su ekrano skaitytuvais, kurie padėtų regos negalią turintiems besimokantiesiems.
- **Navigacija naudojant klaviatūrą**. Užtikrinkite, kad svetainėje būtų galima lengvai naršyti naudojantis tik klaviatūra, o tai labai svarbu judėjimo negalią turintiems asmenims.

Praktiškai svetainės ir mokomosios medžiagos dizainas grindžiamas pagrindinėmis WCAG 2.0 gairėmis. Toliau pateikiame svarbias, bet lengvai įgyvendinamas rekomendacijas.

- Užtikrinkite, kad tekstas būtų **lengvai įskaitomas**, taikant pakankamą kontrastą tarp teksto ir fono. Fono reikėtų vengti, jei jis nėra būtinas.
- Naudokite **didesnius šriftus** ir leiskite vartotojams prireikus keisti šrifto dydį. Naudokite aiškų ir paprastą šriftą, pavyzdžiui, „Arial“ arba „Verdana“. Venkite kursyvo ir pabraukimų, kurie gali apsunkinti skaitymą.
- **Antraštėms taikomi stiliai** apibrėžia teksto struktūrą, todėl jie turėtų būti nuosekliai naudojami nuo aukščiausio iki žemesnio lygio; jie nėra dekoratyviniai elementai tekstui paryškinti.
- Niekada nepateikite tekstų (pavyzdžiui, pavadinimų, meniu, prierašų) kaip paveikslėlių. Tokios informacijos negali perskaityti ekrano skaitytuvai ir daugeliu atvejų negalima keisti jų dydžio.
- **Pridedami dokumentai**. Įsitikinkite, kad pridedami dokumentai yra suderinami su ekrano skaitytuvais. PDF dokumentus galima pritaikyti naudojant internetinę priemonę https://pave-pdf.org/index.html?lang=en.
- **Vaizdinė medžiaga**. Prie visų paveikslėlių (išskyrus dekoratyvinius elementus) pridėkite alternatyvųjį tekstą, kad ekrano skaitytuvai galėtų apibūdinti paveikslėlį. Naudokite aiškias ir suprantamas iliustracijas ir diagramas.
- **Vaizdo ir garso medžiaga**. Prie visų vaizdo įrašų pridėkite subtitrus. Pateikite garso įrašų stenogramas.

- **Navigacija ir struktūra**. Užtikrinkite, kad svetainėje būtų lengva naršyti naudojant klaviatūrą. Naudokite aiškią ir logišką svetainės struktūrą su nuosekliais meniu ir nuorodomis.

Atviros medžiagos prieinamumą internete galite patikrinti naudodamiesi internetine priemone https://www.accessibilitychecker.org/.

3. Kalba ir vaizdavimas

Įtraukios kalbos ir vaizdinių vartojimas padeda visiems besimokantiesiems jaustis vertinamiems ir įtrauktiems.

- Lengvai suprantama. Vartokite trumpus sakinius ir pastraipas. Svarbiausią informaciją pateikite pradžioje. Naudokite sąrašus ir papunkčius, kad informaciją būtų lengviau suprasti.
- Įtraukioji kalba. Venkite lyčių šališkumo ir stereotipų. Vartokite neutralią ir įtraukią kalbą, kuria vienodai paisoma visų asmenų.
- Vaizdų įvairovė. Naudokite vaizdus, atspindinčius skirtingas kultūras, gebėjimus ir kilmę, kad atspindėtumėte besimokančios bendruomenės įvairovę.

4. Technologijų prieinamumas

Užtikrinkite, kad visi besimokantieji turėtų prieigą prie reikiamų technologijų.

- **Galimybė naudotis technologijomis**. Užtikrinkite besimokantiesiems prieigą prie reikiamų priemonių ir patikimo interneto ryšio. Kadangi besimokantieji retai turi asmeninę prieigą prie VR ir AR įrangos, jiems reikia pasiūlyti sutartą laiką, kada jie galėtų ja naudotis profesinio mokymo įstaigoje ir gauti reikiamą techninę pagalbą.
- **Tarptautiniai apribojimai.** Atsižvelkite į tarptautinius technologijų naudojimo ypatumus ir užtikrinkite, kad medžiaga būtų prieinama visiems besimokantiesiems, nepriklausomai nuo jų buvimo vietos.

5. Laiko galimybės

Atsižvelkite į ribotą besimokančiųjų laiką.

- **Lankstus grafikas.** Siūlykite lanksčius terminus ir galimybę peržiūrėti medžiagą bet kuriuo metu, kad būtų galima prisitaikyti prie skirtingų dienotvarkių.

2.3.2. Rekomendacijos

Papildyta ir virtualioji realybė (AR ir VR) gali būti ypač naudingos mokymui, tačiau svarbu užtikrinti, kad šios technologijos būtų saugios žmonėms su negalia. Pateikiame keletą rekomendacijų.

1. **Fizinė sauga**
    - Užtikrinkite, kad vartotojai turėtų pakankamai erdvės judėti ir būtų apsaugoti nuo kliūčių.
    - Paaiškinkite, kaip saugiai naudotis įranga, ir prižiūrėkite vartotojus, kad būtų išvengta galimų sužeidimų.
2. **Emocinė sauga**
    - Naudokite paprastą ir mažiau stimuliuojančią VR aplinką, kad išvengtumėte pernelyg didelės sensorinės perkrovos, kuri gali sukelti stresą ar nerimą.
    - Venkite ryškių šviesų ir greitai judančių vaizdų.
    - Nuolat stebėkite mokinių fizinę ir emocinę savijautą jiems naudojant VR technologijas. Ilgalaikis VR naudojimas gali sukelti trumpalaikių kognityvinių sutrikimų, pavyzdžiui, dėmesio sutrikimų, atminties problemų ir sunkumų orientuotis realioje aplinkoje.
    - Leiskite mokiniams bet kada pasitraukti iš užsiėmimo, jei jie jaučiasi nepatogiai arba patiria diskomfortą.

Laikantis šių rekomendacijų, galima sukurti prieinamą ir įtraukią mokymosi aplinką, kurioje visi besimokantieji galėtų sėkmingai mokytis ir išnaudoti visas savo galimybes.

3. MOKYMOSI MODULIAI

3.1. Atvejų tyrimų įtraukimas

Atvejų analizės įtraukimas į „CybARverse“ mokymosi modulius profesinio mokymo mokytojams yra galinga kibernetinio saugumo koncepcijų mokymo priemonė. Atvejų tyrimai naudojami kaip praktiniai, realaus pasaulio pavyzdžiai, leidžiantys instruktoriams neapsiriboti teoriniu mokymu ir įtraukti besimokančiuosius į realių kibernetinio saugumo problemų sprendimą. Šie kruopščiai parengti scenarijai leidžia iš pirmų lūpų suprasti, kaip kyla kibernetinės grėsmės ir kokių veiksmų reikia imtis joms pažaboti, todėl jie yra esminė mokymo programos dalis instruktoriams, siekiantiems suteikti mokiniams praktinių įgūdžių.

Internetinėje „CybARverse“ mokymosi valdymo sistemoje (MVS) https://www.cybarverse.eu/courses/ pateikiama nemažai išsamių pamokų planų, kurių kiekvienas parengtas pagal konkrečius atvejų tyrimus, apimančius įvairių tipų kibernetinio saugumo incidentus. Šie 45 min. trukmės pamokų planai sukurti taip, kad būtų lankstūs ir juos būtų galima pritaikyti skirtingiems mokymo stiliams ir kompetencijos lygiams. Instruktoriai gali naudotis šiais ištekliais naudodamiesi MVS, todėl jie gali lengvai integruoti atvejų analizes į esamas mokymo programas. Kiekviename pamokos plane nurodyti tikslai, mokymosi rezultatai ir žingsnis po žingsnio pateikiamos atvejo tyrimo gairės, užtikrinančios, kad instruktoriai galėtų veiksmingai organizuoti diskusijas, palengvinti problemų sprendimo veiklą ir įvertinti besimokančiųjų supratimą.

Atvejo analizės yra parengtos taip, kad jose būtų nagrinėjamos įvairios kibernetinio saugumo temos, pavyzdžiui, kenkėjiškos programos, sukčiavimo atakos, išpirkos reikalaujančių programų incidentai ir socialinės inžinerijos taktikos. Kiekvieno scenarijaus pamokų planuose pateikiama pagrindinė informacija ir svarbiausi kibernetinio saugumo pavyzdžiai, padedantys besimokantiesiems atlikti atvejo tyrimą. Tokia struktūra padeda dėstytojams pabrėžti kritinį mąstymą ir sprendimų priėmimą, nes besimokantieji tiria, kaip ir kodėl įvyksta saugumo pažeidimai ir ką galima padaryti, kad jų būtų išvengta. Be to, į pamokų planus įtraukti užsiėmimai, skirti grupinėms diskusijoms ir kolektyviniam problemų sprendimui, kurių metu instruktoriai gali padėti besimokantiesiems ugdyti ir technines žinias, ir netechnologinius įgūdžius, būtinus norint sėkmingai dirbti kibernetinio saugumo srityje.

MVS taip pat suteikia mokytojams galimybę stebėti besimokančiųjų pažangą atliekant vertinimus, susietus su kiekvienu atvejo tyrimu. Testai ar praktinės užduotys padeda instruktoriams įvertinti, kaip besimokantieji supranta medžiagą, ir nustatyti sritis, kurias reikia tobulinti. MVS analizės priemonės padeda suprasti, kaip mokiniai atlieka užduotis, todėl instruktoriai gali pritaikyti savo mokymą, kad jis geriau atitiktų mokinių poreikius.

Profesinio rengimo ir mokymo instruktoriams atvejo analizės įtraukimas reiškia ne tik kibernetinio saugumo sąvokų mokymą - tai galimybė besimokantiesiems pritaikyti šias sąvokas pagal realius scenarijus. Naudodamiesi „CybARverse LMS“ turimais pamokų planais ir ištekliais, instruktoriai gali pasiūlyti patrauklią ir paveikią mokymosi patirtį, kuri parengtų mokinius šiuolaikinio kibernetinio saugumo iššūkiams.

Atvejo analizės išteklių lankstumas ir prieinamumas užtikrina, kad instruktoriai gali lengvai juos integruoti į savo mokymą, o MVS suteikia priemones, reikalingas besimokančiųjų pažangai stebėti, diskusijoms skatinti ir užtikrinti veiksmingą mokymą. Reikėtų pabrėžti, kad MVS yra parengta 5 kalbomis (anglų, graikų, lietuvių, maltiečių ir rumunų).

3.2. Realūs praktinio mokymosi scenarijai

Profesinio mokymo instruktoriams labai svarbu kibernetinio saugumo mokymuose taikyti tikroviškus scenarijus, kad besimokantieji įgytų praktinės patirties. „CybARverse“ mokymosi moduliuose pristatomi realūs kibernetiniai incidentai, todėl besimokantieji gali pritaikyti teorines žinias realioje, kontroliuojamoje aplinkoje. Šis taikomojo mokymosi metodas sumažina atotrūkį tarp pamokų klasėje ir nuolat kylančių iššūkių, su kuriais susiduria kibernetinio saugumo specialistai, todėl tai yra esminis mokymo proceso elementas.

Projekto „CybARverse“ internetinėje mokymosi valdymo sistemoje (MVS) pateikiami tikroviški scenarijų pavyzdžiai, kuriuos instruktoriai gali lengvai įtraukti į savo pamokas. Kiekvienas scenarijus kruopščiai parengtas taip, kad atspindėtų dabartines kibernetinio saugumo grėsmes, tokias kaip socialinė inžinerija, apgaulinga IP taktika, SQL injekcijos ir nulinės dienos atakos. Prie šių scenarijų pridedami išsamūs pamokų planai, kuriuose nurodomi tikslai, laipsniškos instrukcijos ir laukiami rezultatai, todėl instruktoriai gali sklandžiai įtraukti juos į savo mokymo procesą.

Kiekvienas tikroviškas scenarijus sukurtas taip, kad jį būtų galima pritaikyti skirtingiems įgūdžių lygiams, todėl jis tinka profesinio rengimo ir mokymo instruktoriams, dirbantiems su besimokančiaisiais skirtingais kibernetinio saugumo mokymo etapais. Pradedančiųjų scenarijuose gali būti pateikiamos paprastos užduotys, pavyzdžiui, nustatyti įprastus bandymus sukčiauti arba aptikti pagrindines kenkėjiškas programas. Pažengusiems mokiniams scenarijai gali tapti vis sudėtingesni, reikalaujantys valdyti sudėtingus atakų veiksnius, pavyzdžiui, sudėtingas nuolatines grėsmes arba daugelio veiksnių atakas, kai labai svarbu greitai priimti sprendimus ir taikyti pažangius kibernetinio saugumo metodus.

Dėstytojai gali naudoti šiuos realaus pasaulio scenarijus siekdami skatinti aktyvų dalyvavimą ir įsitraukimą. Besimokantieji skatinami bendradarbiauti su kolegomis sprendžiant modeliuojamus kibernetinius incidentus, taip atkartojant komandinį darbą, kurio

reikalaujama profesionalioje kibernetinio saugumo aplinkoje. Šios bendradarbiavimo pratybos gerina bendravimo įgūdžius ir skatina geriau suprasti, kaip kibernetinio saugumo specialistai turi dirbti kartu, kad sumažintų kibernetines grėsmes ir užkirstų joms kelią realiuoju laiku.

Tikroviškų scenarijų įtraukimas į „CybARverse“ mokymosi modulius padeda profesinio rengimo ir mokymo instruktoriams veiksmingai įgyti taikomosios mokymosi patirties. Struktūrizuotas, scenarijais paremtas metodas, kurį galima taikyti pasitelkiant MVS, užtikrina, kad besimokantieji ne tik susipažintų su teorinėmis kibernetinio saugumo koncepcijomis, bet ir su praktinėmis gynybos nuo kibernetinių grėsmių realijomis. Naudodamiesi šiomis priemonėmis, instruktoriai gali puoselėti gilesnę, interaktyvesnę mokymosi patirtį, kuri suteikia besimokantiesiems įgūdžių, reikalingų orientuotis nuolat besikeičiančioje kibernetinio saugumo srityje.

3.3. Vaizdo įrašų taikymas įtraukiąjame mokyme

Vaizdo įrašų taikymas yra veiksmingas būdas kurti įtraukiančią ir įtraukiančią mokymosi patirtį projekto „CybARverse“ kibernetinio saugumo mokymo programoje. Vaizdo įrašai yra veiksminga priemonė sudėtingoms kibernetinio saugumo sąvokoms iliustruoti, demonstruoti jų pritaikymą realiame pasaulyje ir palaikyti aktyvų besimokančiųjų dalyvavimą visame mokymo procese. Įtraukdami trumpus vaizdo įrašus į pamokas, instruktoriai gali pagilinti ir pagerinti mokymo kokybę, pateikdami besimokantiesiems vizualinių ir garsinių pavyzdžių, kuriuos jie lengviau supranta ir įsimena.

„CybARverse“ mokymosi valdymo sistemoje (MVS) siūlomi devyni trumpi vaizdo įrašai, kuriuos instruktoriai gali nesunkiai įtraukti į savo kursus. Vaizdo įrašai, pateikiami „CybARverse" „YouTube“ kanale (https://www.youtube.com/@CybARverseproject), apima šias temas: socialinė inžinerija, kenkėjiškos programos, duomenų išviliojimas, socialinės žiniasklaidos grėsmės bei viliojimas pradmenų lygio kursui, išpirkos reikalaujančios programos, apgaulinga IP taktika ir kryžminiai svetainių scenarijai (XSS) pagrindų lygio kursui, taip užtikrinant, kad profesinio mokymo instruktoriai turėtų prieigą prie aukštos kokybės medžiagos, tinkamos įvairių įgūdžių lygių besimokantiesiems. Vaizdo įrašai sukurti taip, kad papildytų teorines pamokas ir taikomąją mokymosi veiklą, todėl jie yra universali priemonė, padedanti geriau suprasti ir įtraukti mokinius.

Šis vaizdinis mokymosi metodas padeda atskleisti sudėtingas sąvokas, todėl jos tampa prieinamesnės besimokantiesiems, ypač tiems, kurie gali susidurti su sunkumais skaitydami vien tik tekstinę medžiagą. Mokymų vadovai gali naudoti šiuos vaizdo įrašus pradėdami

diskusijas, skatindami besimokančiuosius analizuoti priimtus sprendimus ir siūlyti jų alternatyvas.

Vaizdo įrašai taip pat yra vertinga priemonė mokymosi patirčiai pajvairinti, pritaikyta skirtingiems mokymosi stiliams. Besimokantiems naudinga pamatyti, kaip viskas veikia arba klausytis įgarsinimo bei ekspertų paaiškinimų. Mokymų vadovai gali pasinaudoti šia lankstumo galimybe, kad sukurtų įtraukesnę mokymosi aplinką didesnei besimokančiųjų įvairovei. MVS taip pat siūlo palengvintos prieigos galimybes, pavyzdžiui, subtitrus ir transkripcijas, todėl vaizdo įrašų turinys tampa prieinamas klausos negalią turintiems besimokantiesiems arba tiems, kurie mėgsta skaityti žiūrėdami.

3.4. Įtraukiančių technologijų (VR ir AR) integravimas

Įtraukiančių technologijų, ypač virtualios realybės (VR) ir papildytosios realybės (AR) įtraukimas į „CybARverse“ mokymosi modulius parodo naujovišką požiūrį į kibernetinio saugumo mokymą profesinio mokymo instruktoriams ir jų mokiniams. Šios technologijos sukuria itin interaktyvią ir įtraukiančią mokymosi aplinką, leidžiančią besimokantiesiems tiesiogiai išgyventi sudėtingus kibernetinio saugumo scenarijus. Pasitelkę VR ir AR, instruktoriai gali geriau praktiškai išmėginti kibernetinio saugumo sampratas, todėl mokymo patirtis tampa ir veiksmingesnė, ir įsimintinesnė.

Vienas iš pagrindinių VR ir AR technologijų privalumų yra jų gebėjimas įtraukti besimokančiuosius į tikroviškus scenarijus. Pavyzdžiui, VR modulis gali imituoti įmonės aplinką, kurioje besimokantieji turi atpažinti ir reaguoti į apgaulės ataką arba išpirkos reikalaujančios programinės įrangos incidentą. Aktyviai dalyvaudami tokiuose imitaciniuose modeliuose besimokantieji gali pritaikyti teorines žinias praktinėse situacijose, taip pagerindami savo problemų sprendimo įgūdžius ir gebėjimą priimti sprendimus. Ši įtraukianti patirtis leidžia besimokantiesiems suprasti kibernetinio saugumo iššūkių aktualumą ir sudėtingumą, stiprina pasirengimo ir pasitikėjimo savo jėgomis jausmą.

VR programėlė pateikiama projekto svetainėje (https://www.cybarverse.eu/courses/), ji apima šiuos aštuonis mokymo modulius: kenkėjiška programinė įranga, daiktų interneto atakos, šakninė kenkėjiška programinė įranga ir išpirkos reikalaujanti programinė įranga (pradedantiesiems), SQL injekcijos ir kryžminiai svetainių scenarijai (XSS) (pagrindų lygio) ir Dos bei DDos atakos (pažengusiems).

„YouTube“ kanale https://www.youtube.com/@CybARverseproject rasite 3 vaizdo įrašus iš AR ir VR programėlės: kaip naudotis vairalazdėmis, kenkėjiškos programos ir DDoS.

Įtraukiančių technologijų kaip VR ir AR integravimas į „CybARverse“ mokymosi modulius siūlo profesinio mokymo instruktoriams aktyvų būdą pagerinti kibernetinio saugumo mokymą.

Suteikdami besimokantiesiems praktinę, interaktyvią patirtį, imituojančią realaus pasaulio iššūkius, instruktoriai gali ugdyti gilesnį supratimą, kritinį mąstymą ir sustiprinti kibernetinio saugumo įgūdžius. Naudodamiesi mokymosi aplinkoje esančiais ištekliais, instruktoriai gali nesunkiai įtraukti šias technologijas į savo pamokas, tokiu būdu užtikrindami, kad besimokantieji gerai pasirengtų orientuotis sudėtingoje kibernetinio saugumo aplinkoje. Daugiau informacijos pateikiama kitame skyriuje.

4. VR IR AR TECHNOLOGIJŲ SĄRANKA IR DIEGIMAS

4.1. Tinkami akiniai

Tinkami VR akiniai yra „Meta Quest 2“ ir „Meta Quest 3“.

4.2. „Meta“ paskyros sukūrimas

Norėdami naudoti „Meta Quest“ akinius, turite turėti „Meta“ (anksčiau „Facebook“) paskyrą. Atsižvelgdami į savo poreikius, galite susikurti asmeninę „Facebook“ paskyrą arba bendrąją paskyrą (skirtą verslui ar organizacijai).

4.3. Asmeninės „Facebook“ paskyros kūrimo žingsniai

1. **Apsilankykite „Facebook“**. Eikite į „Facebook“ svetainę arba atsisiųskite „Facebook“ programėlę.
2. **Užsiregistruokite.** Paspauskite „Sukurti naują paskyrą“.
3. **Įveskite asmeninius duomenis.** Įveskite savo vardą ir pavardę, mobiliojo telefono numerį arba e. pašto adresą, slaptažodį, gimimo datą ir lytį. Būtina įvesti tik privalomus duomenis.
4. **Patvirtinkite.** Į jūsų e. paštą arba telefoną „Facebook“ atsiųs patvirtinimo kodą. Įveskite kodą patvirtinimui.
5. **Nusistatykite paskyrą.** Pridėkite savo anketos ir viršelio nuotraukas bei papildykite anketą papildoma informacija (nebūtina).
6. **Pridėkite draugų**, prisijunkite prie grupių ir sekite puslapius (nebūtina).

4.4. Programėlės „Meta Quest“ nustatymas telefone

Programėlė „Meta Quest“ yra būtina VR aplinkai valdyti. Štai kaip ją nustatyti.

1. **Atsisiųskite** (https://play.google.com/store/search?q=oculus&c=apps&hl=en) ir paleiskite „Meta Quest“ programėlę telefone.
2. **Prisijunkite** prie savo „Meta“ paskyros (asmeninės arba verslo).
3. **Susiekite** „Meta Quest“ ausines vadovaudamiesi ekrane rodomais nurodymais.
4. **Naudokitės** programėle nustatymams keisti, turiniui atsisiųsti ir įrenginiui valdyti.

4.5. Reikalinga įranga

- **Mobilusis įrenginys.** Pasirūpinkite išmaniuoju telefonu, kad galėtumėte naudotis „Meta Quest“ programėle ir sąrankos procesu.
- **Kompiuteris.** Kompiuteris, kuris bus naudojamas ryšiui su akiniais ir APK programai įkelti.

- **„Oculus Quest“ akiniai.** „Oculus“ įrenginys, į kurį norite įdiegti programą.
- **USB duomenų kabelis** (iš USB-A į USB-C): Juo „Oculus“ ausinės bus prijungtos prie kompiuterio, kad galėtumėte perkelti APK.

4.5.1. Programinė įranga

- **„Meta Quest“ programa**. Norint valdyti „Oculus“ akinius, į mobilųjį įrenginį reikia įdiegti „Meta Quest“ programėlę. Ši programėlė padės atlikti pradinę sąranką ir tvarkyti kūrėjų leidimus.
- Programėlės „Meta Quest“ atsisiuntimas ir diegimas: https://www.meta.com/quest/setup/.
- **„SideQuest“.** Atsisiųskite ir įdiekite „SideQuest“ savo kompiuteryje. Su „SideQuest“ galėsite įkelti APK (tokias „Android“ programėles) į savo „Oculus Quest“ įrenginį.
- „SideQuest“ sąrankos vadovas: https://sidequestvr.com/setup-howto.
- **APK failas.** Programos, kurią norite įkelti, APK failas turi būti atsisiųstas ir išpakuotas kompiuteryje.

4.5.2. Leidimai

- „Meta Developer“ organizacija. Kad ausinėse įjungtumėte kūrėjo režimą, turite sukurti „Meta“ kūrėjų organizaciją, užsiregistruodami „Meta“ kūrėjų valdymo skydelyje. Jūsų organizacija turės būti patvirtinta.
- „Meta Developer Dashboard“: https://developer.oculus.com/manage/organizations/
- „Oculus" akinių administratoriaus teisės. Kad galėtumėte valdyti „Oculus“ įrenginio leidimus, turite būti jo administratorius. Daugiau apie tai sužinokite „Meta“ kūrėjo režimo vadove.
- „Meta Quest“ kūrėjų režimo nustatymas: https://developer.oculus.com/documentation/quest/latest/concepts/mobile-device-setup/.
- Narystė kūrėjų organizacijoje. „Oculus“ ausinių administratorius turi būti anksčiau sukurtos ‚Meta‘ kūrėjų organizacijos narys. Įsitikinkite, kad pridėjote administratorių kaip narį kūrėjų valdymo skydelyje pasinaudodami pirmiau pateikta nuoroda.
- „Oculus“ akinių PIN kodas. Nustatykite „Oculus“ įrenginio PIN kodą vadovaudamiesi instrukcijomis, pateiktomis „Meta“ pagalbos puslapyje.
- „Meta Oculus Headset“ ausinių PIN nustatymas: https://support.meta.com/279555412449097/?locale=en_US.
- Mobiliojo įrenginio prieigos kodas. Patikrinkite, ar turite savo mobiliojo įrenginio prieigos kodą.

4.6. „Meta Quest“ akinių sąranka

„Meta Quest“ akinių nustatymas.

- Prieš naudodami akinius pirmą kartą, įkraukite juos.
- Sureguliuokite galvos dirželį, kad patogiai priglustų.
- Įjunkite prietaisą įjungimo mygtuku.
- Vadovaukitės sąrankos instrukcijomis: Užsidėkite akinius ir vadovaukitės ekrane rodomais nurodymais.
- Prisijunkite prie „Wi-Fi“: pasirinkite savo tinklą ir įveskite slaptažodį, kai bus paprašyta.
- Nustatykite apsaugos ribą. Nustatykite saugią žaidimų zoną, kad naudojant akinius būtų išvengta nelaimingų atsitikimų.

4.7. Rankų sekimas ir gestų naudojimas programoje „Meta Quest"

„Meta Quest“ galima valdyti rankų judesiais, todėl galėsite sąveikauti su VR aplinka be valdiklių. Norėdami naudotis šia funkcija, akinių nustatymuose įjunkite rankų sekimą.

- Išmokite ir praktikuokite gestus: Pradėkite nuo pagrindinių gestų, pavyzdžiui, suspaudimo, suėmimo ir rodymo, kad galėtumėte sąveikauti su VR programomis.
- Išbandykite rankų sekimui skirtose programose, kad galėtumėte patogiai bendrauti be valdiklio.
- Kaip naudotis gestais: https://www.youtube.com/watch?v=Ll5ywZZFM0A.

5. BANDOMIEJI MOKYMAI

„CybARverse“ kursas buvo bandomas keturiose šalyse - Lietuvoje, Kipre, Maltoje ir Rumunijoje, kur dalyvavo IT ir ne IT pedagogai, įskaitant mokytojus, kuratorius ir dėstytojus. Šie pedagogai pateikė vertingų atsiliepimų vykdydami išsamų vertinimo procesą, kurio metu buvo patikrintas kurso veiksmingumas.

Buvo atliktos trys atskiros apklausos: viena skirta kursų dalyviams, kita - ekspertams, vertinusiems atskiras pamokas, o trečia - ekspertams, vertinusiems įvairius kurso elementus, pavyzdžiui, navigaciją, aiškumą, dizainą, įsitraukimą ir įtraukiančių technologijų naudojimą. Kiekvienoje apklausoje buvo komentarų ir pasiūlymų skiltis, skirta kokybinėms įžvalgoms surinkti, taip dar labiau praplečiant grįžtamąjį ryšį.

Iš viso vertinime dalyvavo 70 dalyvių, kurie pateikė įvairias nuomones apie stipriąsias kurso puses ir tobulintinas sritis. Ekspertai pateikė išsamius kiekvieno iš 17 kibernetinių atakų scenarijaus pamokų vertinimus - gautas 71 atsakymas. Šie atsiliepimai labai svarbūs tobulinant kursą, kad jis geriau atitiktų būsimų besimokančiųjų poreikius.

Be to, 14 ekspertų iš dalyvaujančių šalių pateikė savo nuomonę kitoje apklausoje, kurioje daugiausia dėmesio skirta įvairiems kurso aspektams. Jų išsamūs atsiliepimai, įskaitant kokybines įžvalgas, pateiktas komentarų skiltyse, padės nuolat tobulinti „CybARverse“ kursą, užtikrinant, kad jis taptų veiksmingesnis ir labiau atitiktų būsimų dalyvių poreikius.

5.1. Pradinių bandymų rezultatai

1. Kurso struktūra ir suprantamumas

Internetinio kibernetinio saugumo kurso struktūra sulaukė itin teigiamų atsiliepimų - 79 proc. ekspertų jo suprantamumą įvertino puikiai. Tai rodo, kad kurso turinys pateikiamas aiškiai ir prieinamai, efektyviai supaprastinant sudėtingas kibernetinio saugumo sąvokas besimokantiesiems. Aukštas įvertinimas atspindi mokymo struktūros pranašumus, kuri užtikrina, kad paaiškinimai būtų glausti ir paremti aukštos kokybės medžiaga, taip prisidedant prie geros bendros mokymosi patirties.

2. Gramatika ir sintaksė

Gramatika ir sintaksė buvo labai gerai įvertintos - 80 proc. dalyvių jas įvertino puikiai. Šie teigiami atsiliepimai pabrėžia aiškios ir profesionalios kalbos svarbą išlaikant švietimo turinio vientisumą ir veiksmingumą. Tinkama gramatika ir sintaksė ne tik apsaugo nuo klaidinančių

veiksnių, bet ir padeda besimokantiesiems sutelkti dėmesį į medžiagą, taigi padeda geriau ją suprasti.

3. Turinio aktualumas

Dar viena stiprioji pusė - kursų turinio atitikimas dabartiniams kibernetinio saugumo iššūkiams. 70 proc. respondentų šį dalyką įvertino puikiai, o dar 27 proc. – labai gerai. Tai rodo, kad kurso medžiaga gerai atitinka realius kibernetinio saugumo srities poreikius, todėl besimokantieji gauna aktualių ir pritaikomų žinių.

4. Pritaikymas prie mokymosi stilių ir kompetencijos lygių

Atsiliepimai apie kurso elementų pritaikomumą įvairiems mokymosi stiliams ir patirties lygiams buvo nevienareikšmiai. Nors nemaža dalis ekspertų teigiamai įvertino įtraukų ir įvairiapusį kurso požiūrį, kai kurie manė, kad jis nepakankamai atitinka jų konkrečius poreikius. Tai rodo, kad kursą reikia toliau tobulinti, kad jis būtų geriau pritaikytas visam besimokančiųjų spektrui.

5. Testų veiksmingumas

Dauguma ekspertų pripažino internetinių testų veiksmingumą, tačiau taip pat nurodė tobulintinas sritis. Nors dauguma buvo patenkinti testams skiriamu laiku, kai kurie manė, kad šis laikas buvo per ilgas, o testų turinys galėtų būti išsamesnis ir įvairesnis, kad būtų galima geriau įvertinti įvairius dalyvių žinių lygius.

6. Bendras sudėtingumo lygis

Bendrą kurso sudėtingumo lygį puikiai įvertino 9 proc. ekspertų, o tai reiškia, kad nors kursas buvo gerai pritaikytas vieniems, kitiems jis galėjo būti nepakankamai sudėtingas. Toks nevienareikšmis vertinimas rodo, kad reikia veiksmingiau subalansuoti sudėtingumo lygį.

7. VR ir AR patirties gerinimas

Atsiliepimai parodė, kad reikia daugiau AR ir VR elementų sąveikos ir aktyvumo. Dalyviai taip pat atkreipė dėmesį į iššūkius, su kuriais susidurta diegiant programą „Oculus“ įrenginiuose, pabrėždami aiškių, žingsnis po žingsnio instrukcijų svarbą.

Bandomojo mokymo rezultatai pabrėžia stipriąsias kurso puses, ypač jo struktūrą, turinio aktualumą ir aiškumą. Tačiau, toliau tobulinant kursą, labai svarbu atsižvelgti į pastabas, susijusias su pritaikomumu, testų efektyvumu ir VR bei AR sąveika. Įgyvendinus šią gerąją

patirtį, kursas bus geriau pritaikytas įvairiems besimokančiųjų poreikiams, padidins jų mokymosi patirtį ir sėkmę kibernetinio saugumo srityje.

5.2. Patobulinimai, įgyvendinti po bandomojo mokymo

5.2.1. Mokymosi valdymo sistemos (MVS) patobulinimai

Siekiant pagerinti naudotojų patirtį ir kursų organizavimą, buvo atlikti atitinkami MVS patobulinimai.

- **Turinio prieinamumas ir patogumas:** svetainės kursų turinys dabar yra labiau prieinamas ir patogus naudoti, jame įdiegtos geresnės pritaikymo priemonės, pvz., disleksijos pagalba, teksto didinimas, ryškus kontrastas, įskaitomi šriftai, paryškinti pavadinimai ir nuorodos ir kt., kad naudotojai galėtų pritaikyti sąsają savo poreikiams. Be to, dirbtiniu intelektu pagrįsta programa nuolat optimizuoja pasiekiamumą, pritaikydama svetainės HTML ekrano skaitytuvams ir klaviatūros funkcijoms, kad padėtų naudotojams, turintiems regos ir judėjimo sutrikimų.
- **Geresnis mobiliojo meniu rodymas:** mobiliųjų įrenginių meniu buvo pertvarkytas taip, kad būtų užtikrinta sklandi navigacija įvairiuose įrenginiuose, o tai pagerino prieinamumą naudotojams, kurie mieliau mokosi mobiliosiose programose.
- **Atvejų analizės susietos** su PDF dokumentais. Siekiant užtikrinti patikimą prieigą prie išteklių, atvejo analizės susietos su atsisiunčiamais PDF dokumentais, o ne su išorinėmis svetainėmis, taip užtikrinant nuoseklesnę mokymosi aplinką ir sumažinant neveikiančių nuorodų riziką.
- **Registracijos patvirtinimas**: siekiant supaprastinti naudotojų registraciją ir užtikrinti, kad prieigą prie kurso gautų tik autorizuoti dalyviai, įdiegtos patobulintos patikros procedūros.
- Patikslinti **lygių aprašymai**: kiekvieno lygio kursų aprašymai dabar yra skirtingi, todėl besimokantieji aiškiau supranta turinį ir tikslus kiekviename kurso etape.
- **Vartotojo anketos** pritaikymas: norint supaprastinti sąsają ir sutelkti dėmesį į svarbiausią su kursu susijusią informaciją, buvo patobulintos naudotojų anketos - pašalintos nereikalingos funkcijos, pavyzdžiui, pageidavimų sąrašai ir užsakymai.

5.2.2. Testų ir turinio optimizavimas

Siekiant geriau įvertinti besimokančiųjų supratimą ir įsitraukimą, buvo atlikti keli testų bei vertinimo pakeitimai.

- Pakoreguotas laikas: nustatytas standartinis 20 minučių testų laikas, kad besimokantieji turėtų pakankamai laiko apgalvotai atsakyti į klausimus, tačiau kartu tektų paskubėti.
- Įvairūs klausimų tipai: klausimai buvo pajvairinti, įtraukiant įvairius formatus, pavyzdžiui, klausimų su keliais atsakymų variantais ir tiesos ir netiesos, kad būtų galima tiksliau įvertinti įvairius besimokančiųjų žinių ir supratimo aspektus.
- Nustatytas 60 proc. išlaikymo balas, taip užtikrinant pusiausvyrą tarp reikalavimų ir tikslo užtikrinti besimokančiųjų sėkmę ir pasitikėjimą savimi.

5.2.3. VR ir AR programėlės patobulinimai

Siekiant sukurti labiau įtraukiančią ir interaktyvią mokymosi aplinką, buvo atlikti keli VR bei AR programėlės atnaujinimai.

- Patobulintas interaktyvusis personažas. Integruotos papildomos animacijos, todėl mokymosi patirtis tapo dinamiškesnė ir patrauklesnė.
- Pridėtas įgarsintas tekstas: įgarsintas pasakojimas, papildantis vaizdinius elementus, gerinantis bendrą supratimą.
- Modulio užbaigimo rodikliai: įtraukti vizualiniai rodikliai, pagal kuriuos galima stebėti modulio užbaigimą, kad besimokantieji aiškiai matytų pažangą ir pasiekimus.
- Atnaujintas scenarijaus fonas: atrinktų scenarijų fonas buvo atnaujintas, kad besimokantiesiems būtų sukurta labiau įtraukianti ir kontekstą atitinkanti aplinka.
- Muzikos pritaikymas: pridėtos įvairios foninės muzikos parinktys, taip pat galimybė išjungti garsą, kad besimokantieji galėtų pritaikyti savo mokymosi aplinką.
- Įvadinis vaizdo įrašas: VR programėlėje buvo pridėtas mokomasis filmukas, kuris supažindino naudotojus su programėlės funkcijomis ir padėjo jiems įgyti patirties.
- Logotipai ir atsakomybės apribojimai: skiltyje „Apie mus“ buvo įtraukti logotipai ir atsakomybės apribojimai, taip padidinant skaidrumą ir pateikiant svarbiausią informaciją apie kursą ir jo kūrėjus.
- Peržiūrėtos ir iš dalies pakeistos programėlių valdymo priemonės. Vartotojo valdikliai buvo kruopščiai peržiūrėti ir pakoreguoti, siekiant užtikrinti intuityvią sąveiką su VR bei AR aplinka ir pagerinti bendrą naudojimo patogumą.

- „WebVR“ scenarijai: įtraukti žiniatinklio VR scenarijai nulinės dienos spragų išnaudojimo, tarpininko atakų, kriptovaliutinės vagystės temoms, todėl įtraukianti patirtis tapo prieinama įvairiose platformose.

Šie patobulinimai buvo strategiškai įgyvendinti siekiant užtikrinti, kad kibernetinio saugumo internetinis kursas būtų ne tik patrauklus ir interaktyvus, bet ir veiksmingas suteikiant besimokantiesiems praktinių įgūdžių, reikalingų siekiant tobulėti šioje srityje. Naudojant įtraukiančias technologijas ir tobulinant tiek MVS, tiek turinio pateikimą, kursu siekiama suteikti visapusišką ir paveikią mokymosi patirtį. Be to, šie pakeitimai ne tik padidins naudotojų pasitenkinimą, bet ir užtikrins, kad kursas veiksmingai patenkintų visų dalyvių mokymosi poreikius.

5.3. Įgyta patirtis

Surengus bandomąjį kibernetinio saugumo kurso mokymą taikant įtraukiančias technologijas, buvo gauta keletas svarbių įžvalgų, išryškinančių šio naujoviško metodo veiksmingumą ir dalyvių įsitraukimą.

1. Didesnis įsitraukimas ir įsiminimas

- **Aukštas įsitraukimo lygis:** palyginti su tradiciniais mokymo metodais, dalyviai buvo gerokai labiau susidomėję. Įtraukiančios technologijos, pavyzdžiui, virtualioji realybė (VR) arba papildytoji realybė (AR), kartu su vaizdo įrašais suteikė praktinės patirties, todėl sudėtingos kibernetinio saugumo sąvokos tapo prieinamesnės ir suprantamesnės.
- **Geresnis įgūdžių išlaikymas:** interaktyvus kurso pobūdis padėjo geriau įsiminti informaciją. Dalyviai galėjo aktyviai taikyti tai, ko išmoko realiuoju laiku vykstančių modeliavimų metu, o tai sustiprino pagrindinių kibernetinio saugumo principų supratimą ir įsiminimą.

2. Teigiami atsiliepimai apie interaktyvumą

- **Palankiai įvertintas interaktyvumas:** ypač gerai buvo įvertinti interaktyvūs kurso elementai. Dalyviai teigiamai įvertino galimybę bendrauti su virtualia aplinka, kuri tiksliai atkartoja realaus pasaulio scenarijus. Dėl tokio interaktyvumo kursas ne tik tapo patrauklesnis, bet ir suteikė galimybę mokytis praktiškai, iš patirties, o tai, dalyvių nuomone, buvo neįkainojama.
- **Pritaikymas realiame pasaulyje:** dalyviai teigė, kad vaizdo įrašai ir atvejo analizės padėjo sumažinti atotrūkį tarp teorinių žinių ir praktinio taikymo. Dalyvaudami

interaktyviuose modeliavimo procesuose jie jautėsi geriau pasirengę valdyti realias kibernetinio saugumo grėsmes.

3. Didesnis pasitikėjimas įgūdžiais

- **Pasitikėjimo savimi stiprinimas:** įtraukianti technologija padėjo dalyviams sustiprinti pasitikėjimą savo kibernetinio saugumo įgūdžiais. Galimybė praktikuotis kontroliuojamoje, nerizikingoje aplinkoje leido jiems daryti klaidas, mokytis iš jų ir tobulinti įgūdžius nebijant realių pasekmių.

4. Vartotojo patirtis ir prieiga

- **Naudojimo paprastumas:** nors daugumai dalyvių įtraukianti technologija atrodė intuityvi ir paprasta naudoti, tačiau tiems, kurie mažiau susipažinę su VR ar AR, teko susidurti su tam tikrais pradiniais mokymosi sunkumais. Tačiau po trumpo prisitaikymo laikotarpio dauguma dalyvių teigė, kad patirtis buvo sklandi ir maloni.
- **Prieiga ir įranga:** kai kurie dalyviai pažymėjo, kad jie neturi reikiamos įrangos (pvz., VR akinių) ir tai gali būti kliūtis. Tačiau, kai įranga buvo suteikta, ji labai pagerino mokymosi patirtį.
- **Pritaikymo priemonės:** prieinamumo kliūtis pašalino patobulintos priemonės, padedančios užtikrinti ryškų kontrastą, skaitymo orientyrai, įskaitomi šriftai ir tarpai tarp eilučių bei paryškinti pavadinimai ir nuorodos, taip užtikrinant įtraukią patirtį visiems naudotojams, įskaitant asmenis, sergančius disleksija.

5. Tobulintinos sritys

- **Techninės problemos:** keletas dalyvių susidūrė su nedidelėmis techninėmis problemomis, pvz., trikdžiais ar sunkumais naršant virtualioje aplinkoje. Nors šios problemos nebuvo plačiai paplitusios, tačiau jos rodo, kad prieš pradedant plačiau diegti virtualią virtualią erdvę reikia užtikrinti patikimą techninę pagalbą ir atlikti išsamius bandymus.
- **Įvairi mokymosi eiga:** nors dauguma dalyvių gerai prisitaikė prie įtraukiančios technologijos, kai kuriems prireikė papildomos pagalbos. Pritaikius mokymą įvairiems technologinio išprusimo lygiams, būtų galima padidinti bendrą veiksmingumą.

6. Bendras pasitenkinimas

- **Aukštas pasitenkinimo lygis:** apskritai dalyviai buvo labai patenkinti įtraukiančiais kibernetinio saugumo mokymais ir vaizdo įrašais. Jie teigiamai įvertino novatorišką požiūrį ir patrauklią, interaktyvią aplinką.

- **Rekomendacija dėl platesnio naudojimo:** daugelis dalyvių išreiškė norą, kad daugiau mokymo programų būtų taikomos įtraukiančios technologijos, nurodydami geresnę mokymosi patirtį ir tokių metodų galimybes sukelti perversmą kibernetinio saugumo ir kitose mokymo srityse.

6. IŠVADOS

6.1. Kibernetinio saugumo kursų rengimo gerosios patirties santrauka

Veiksmingas kibernetinio saugumo kursų organizavimas „CybARverse“ sistemoje, kurioje naudojama įtraukianti technologija, pagrįstas keletu pagrindinių gerosios patirties pavyzdžių.

1. **Interaktyvi mokymosi aplinka.** Naudokite įtraukiančias VR ir AR simuliacijas, kad būtų sukurti tikroviški praktiniai scenarijai, kuriuose besimokantieji galėtų lavinti kibernetinio saugumo įgūdžius valdomoje ir įtraukiančioje aplinkoje.
2. **Turinio pritaikymas.** Pritaikykite kurso turinį, kad jis atitiktų skirtingus besimokančiųjų kompetencijos lygius. Pritaikykite esminę medžiagą pradmenų, pagrindų ir pažengusiųjų lygiams, taip užtikrindami, kad mokymai būtų naudingi visiems vartotojams.
3. **Vertinimas.** Kiekvieno kurso pabaigoje atliekami testai parodo dalyvių pažangą ir įtvirtina mokymosi rezultatus.
4. **Technologijų prieinamumas.** Užtikrinkite, kad reikalingos įtraukiančios technologijos būtų lengvai prieinamos ir patogios naudoti. Kurso pradžioje pasiūlykite pagalbą besimokantiesiems, kurie gali būti menkiau susipažinę su VR / AR priemonėmis.
5. **Saugumo ir privatumo aspektai.** Užtikrinkite, kad įtraukiančiųjų technologijų sistema atitiktų aukščiausius saugumo standartus, kad būtų apsaugoti vartotojų duomenys ir išlaikytas mokymo aplinkos vientisumas.

6.2. Šių gairių paskirtis ir poveikis

Šių gairių tikslas - pateikti pedagogams, instruktoriams ir mokymų rengėjams išsamią sistemą, kaip rengti veiksmingus ir įdomius kibernetinio saugumo kursus naudojant „CybARverse“ platformą. Laikydamiesi šiame vadove aprašytos gerosios praktikos, instruktoriai gali sukurti įtraukiančią mokymosi patirtį, kuri ne tik padės geriau suprasti sudėtingas kibernetinio saugumo koncepcijas, bet ir gerokai pagerins besimokančiųjų praktinius įgūdžius.

Šio vadovo poveikis neapsiriboja vien tik atskirais mokymais. Taikydamos šią praktiką organizacijos gali užtikrinti, kad jų kibernetinio saugumo komandos būtų geriau pasirengusios kovoti su realiomis grėsmėmis, o tai leistų sukurti saugesnę skaitmeninę aplinką. Be to, šis vadovas padeda standartizuoti įtraukiančiomis technologijomis grindžiamų mokymų vykdymą, skatinant nuoseklumą ir kokybę įvairiose mokymosi aplinkose.

6.3. Baigiamosios mintys ir tolesni nuolatinio tobulinimo žingsniai

Kadangi toliau sparčiai keičiasi technologinis kraštovaizdis, būtina šį vadovą laikyti gyvu dokumentu. Kibernetinio saugumo sritis yra dinamiška, joje nuolat atsiranda naujų grėsmių ir technologijų. Todėl labai svarbu nuolat tobulėti ir prisitaikyti.

Tolesni žingsniai.

1. **Reguliarus atnaujinimas.** Periodiškai peržiūrėti ir atnaujinti vadovą, kad jame atsispindėtų naujausi kibernetinio saugumo ir įtraukiančio mokymosi technologijų pokyčiai. Atsižvelgti į instruktorių ir besimokančiųjų atsiliepimus, kad būtų galima patobulinti gerąją patirtį.
2. **Bendradarbiavimas su bendruomene.** Skatinti dėstytojų, kibernetinio saugumo specialistų ir technologų bendradarbiavimą, kad būtų galima dalytis įžvalgomis, patirtimi ir naujovėmis. Kuriant bendruomenę, susijusią su įtraukiančiu kibernetinio saugumo mokymu, galima kurti naujus metodus ir priemones.
3. **Plečiamumas ir pritaikymas.** Išnagrinėti būdus, kaip pritaikyti įtraukiančio mokymo metodą įvairiose organizacijose ir pritaikyti jį konkretiems pramonės poreikiams. Tai padės padaryti „CybARverse“ sistemą universalesnę ir plačiau pritaikomą.

Apibendrinant galima teigti, kad taikydami šią geriausią praktiką ir įsipareigodami nuolat tobulėti, galime užtikrinti, kad kibernetinio saugumo mokymas „CybARverse“ ne tik išliktų veiksmingas, bet ir pirmautų novatoriškų, įtraukiančių mokymosi patirčių srityje. Toks požiūris suteiks kibernetinio saugumo specialistams žinių ir įgūdžių, reikalingų apsaugoti mūsų skaitmeninį pasaulį vis sudėtingesnėje grėsmių aplinkoje.