A·16 Zibersegurtasun-erronka, guardia digital bihurtu nahi duzu?

Kurtsoa/Maila
3. DBH
4. DBH

Datak
2027 Otsaila - Maiatza

Ikaskuntza-arloak
Lanbide-orientazioa
Teknologia

Jarduera formatua
Enpresa-tailerra

Hizkuntza
Gaztelania

Irismen geografikoa
Araba, Bizkaia, Gipuzkoa

Jarduera ematen duen erakundea
Mikeldi Ikasketa Zentroa

Makina birtualeko software baten bidez, ikasleei beren instalazioetan tailer teknologiko batera joateko aukera ematen zaie.

Zentroak erronka bat proposatuko die, ekipo informatikoetan jasandako zibererasoari aurre egin eta geldiarazteko eta gailu horien saio-hasierako pasahitzak betetzeko.

STEM Deskribatzaileak

STEM 1 | STEM 4 | STEM 6

Baliabideak

Baliabide materialak
Mikeldi Ikasketa Zentroak eskura jartzen ditu beharrezko ekipamendu informatikoa eta softwarea duten ikasgelak.

Baliabide ekonomikoak
Enpresara joan-etorriak

Informazio gehiago
mikeldi.com

A·16 Zibersegurtasun-erronka, guardia digital bihurtu nahi duzu?

GARAPENA

Jarduera gauzatze fasea

Mikeldi Ikasketa Zentroak jarduera honi hasiera emango dio, 2 ordu eta erdian konpondu beharko duten erronka bat plazaratuz, lanbide heziketako zentroko aditu baten laguntzarekin.

Segurtasun aktiboko eta pasiboko jarraibideak lantzeko, makina birtualeko software baten bidez zibereraso bat simulatuko dute jarduera egiten den gelako ekipo informatikoetan, eta, gainera, ordenagailu horien saio-hasierako pasahitzak hackeatuko dituzte.

Ariketa horretan, ikasleek aukera izango dute arazoari benetako konponbidea nola eman jakiteko, gida gisa jasoko dituzten azalpenei esker. Halaber, bigarren zatian, baliabide digitaletan ohikoenak diren mehatxuak detektatzeko eta prebenitzeko mekanismo eta tresna espezifikoak ezagutuko dituzte.

Tailerra amaitzeko, lanbide-orientazioaren ikuspegitik eta genero-ikuspegia oso kontuan hartuta, zentroak ordu erdiko aurkezpena egingo du bertan eskaintzen diren ikasketei buruz, eta arreta berezia jarriko du bokazio zientifiko-teknologikoetan, mota horretako profesionalen eskaeran eta horrelako zikloetan emakumeen presentzia sustatzeko beharrean.

Ikasgelan integrazio fasea

Teknologien erabilera segurua eta arduratsua ikasgelan lantzen jarraitzeko, jarduera hori ikasgelako programazioan integratuko da, teknologiaren eta tutoretza saioen bidez.

Ikasleek tailerrean ikasitako edukiei buruz hausnartu beharko dute, eta beren datuak digitalki babesteko kontuan hartu beharreko jardunbide egokiei buruzko infografia bateratua sortu.

A·16 Zibersegurtasun-erronka, guardia digital bihurtu nahi duzu?

CURRICULUMAREKIN LOTURA

Jardueran lantzen diren curriculum-ikaskuntzak:

Teknologia

- **Segurtasun aktiboa:** sistema informatikoetan kalteak prebenitzen eta saihesten saiatzen diren neurriak (nola hobetu ordenagailurako sarbidea pasahitz seguruen eta baliabide erabilgarrien bidez, nola erabili eta jardun Keepass-ekin datu-base bat, nola zifratu Windowsen partizio bat DiskCryptor kode irekiko doako programa bat erabiliz, ekipoaren bolumen batean gordetako datuen konfidentzialtasuna babesteko, etab.).
- **Segurtasun pasiboa:** datuen segurtasun-kopiak, jatorrizkoa ez den beste leku batean, hondamendia gertatuz gero (suteak, uholdeak, lapurretak, etab.) datuak berreskuratzeko. Uranium Backup doako softwarea erabiliko dugu (kopia osoak, inkrementalak eta diferentzialak).
- **Nola babestu ohiko gailuak**, aldian behin pasahitzak, sistema eragileak eta antibirusa (eguneratzeak, online antibirusa doan) konfiguratuz eta eguneratuz. Doako software bat erabiliko dugu, hala nola CCleaner, sistema eragilea optimizatuta izan dadin, azkarrago funtziona dezan.
- **Dauden software-motak eta lizentziak.** Erabiltzen den softwarea doakoa izango da (freeware lizentzia) edo Shareware lizentzia denbora mugatukoa (Windowsen kasua).
- **Segurtasuna eta pribatutasuna:** erabilera arrunteko gailuei arriskuak, mehatxuak eta erasoak saihesteko prebentzio- eta zuzentze-neurriak. Malwarebytes programa erabiliko da doako bertsioan, software maltzurrez kutsatuta ote gauden jakiteko, eta Windowseko suebakian sartu eta irteteko erregelaren bat izango dugu, erasoak saihesteko. Adibide gisa, proba bat egingo dugu Keylogger programa batekin, erabiltzaile baten pultsazioak atzemateko jakin gabe eta hori nola prebenitu jakiteko.