Képzés megnevezése	Időtartam (óra)	Kiberbiztonsági és szoftvertechnológiai képzés – A szolgáltatás rövid leírása
BME/CrySys - Bevezetés a kiberbiztonságba	4	Ez a képzés bevezetést nyújt az alapvető kiberbiztonsági fogalmakba és áttekintést ad a főbb biztonságtechnológiai trendekről, melyek az ICT rendszerek különböző architektúrális szintjein megjelenhetnek. Az egyes bemutatott biztonsági megoldásokat potenciális támadási példák motiválják. Bevezetésre kerül a kiberbiztonsági kockázat fogalma és a kockázatot befolyásoló tényezők, és a támadói modellek, valamint a biztonsági technológiák, módszerek és eszközök ezen tényezőkkel összefüggésben kerülnek bemutatásra. Ez a tananyagegység ajánlott mindenkinek, aki a kiberbiztonság területén meg akarja tenni az első lépéseket.
BME/CrySys - Kiberbiztonság-menedzsment	4	A képzés célja a kiberbiztonsági szabályozással kapcsolatos ismeretek átadása, a kockázatkezelés fázisainak, a fenyegetések modellezésére és a kockázatok kategorizálására alkalmas módszerek bemutatása.
BME/CrySys - Anonimizációs technikák & Re-identifikációs támadások	4	A képzés célja pár elterjedt anonimizációs technika ismertetése, illetve a különböző adattípusok adatvédelmi kockázataira való figyelemfelhívás és a tudatosság fokozása a látszólag nem személyes adatok érzékenységével kapcsolatban.
BME/CrySys - Adatvédelem-menedzsment	4	A képzés célja az adatvédelmi szabályozással, kockázatokkal, a kockázatokkal szembeni védekezéssel kapcsolatos ismeretek legfontosabb ismeretek átadása, valamint a jogszerű adatkezelés, a kockázat azonosítás, kiértékelés és csökkentés példákon keresztüli bemutatása.
BME/ftsrg - Hatásanalízis informatikai rendszerek megbízhatóságának kiértékelésében	4	A ma már mindenütt jelenlevő fejlett informatika alapozza meg a fizikai környezet, ipari és gazdasági termelés és szolgáltatások intelligens vezérlését. Egyidejűleg azonban az informatikai infrastruktúra elleni sikeres támadások megsokszorozott hatást gyakorolhatnak azáltal, hogy blokkolják, megzavarják vagy éppen szétrombolják a termelő technológiát, amelyeknek eredményképpen akár az emberi életre, a környezetre vagy a gazdaságra gyakorolt jelentős veszteségek jöhetnek létre. A tanfolyam célja olyan módszer bemutatása, melynek segítségével a résztvevők képesek lesznek szisztematikus kockázatelemzést előkészíteni, követni, ill. ilyen elemzés eredményét értelmezni.
BME/ftsrg - Adatelemzés alapú rendszer- és folyamatfejlesztés	4	A digitalizációt megalapozó informatikai termékek és szolgáltatások fejlesztése során számos megfigyelés (pl. naplóbejegyzés) jön létre. Ezek szisztematikusan gyűjtve és elemezve értékes bemeneti információt szolgáltatnak a fejlesztési és üzemeltetési folyamatok, valamint a szoftver által megvalósított szolgáltatások minőségének, biztonságának, megbízhatóságának és hatékonyságának javításához. A tanfolyam fő célja az, hogy bemutassa az ilyen jellegű információk projekt- és terméknapló formájában történő szervezett gyűjtését, majd az intelligens adatelemzésének módszereit és ezek alkalmazását a fejlesztési-üzemeltetési folyamatok minőségének és hatékonyságának növelésében. A részvevők képesek lesznek megérteni és kiértékelni a fejlesztési és üzemeltetési folyamatokból származó adatokat, valamint áttekintő adatelemzést végezni ezeken.
BME/CrySys - Szoftverbiztonság	4	Ez a tananyagegység bemutatja a szoftvertervezés biztonsági kihívásait. Az életciklus modellt követve áttekintésre kerül, hogy az egyes fázisokban hogyan jelenik meg a biztonság. Ezek közül kiemelten tárgyaljuk a tervezési fázisban felmerülő kihívásokat, és azokat a tervezési irányelveket, amik jelentősen növelhetik egy szoftver biztonságát. A folyamatot magas szinten mutatjuk be, amivel célunk az, hogy átfogó képet adjunk a lehetséges módszerek helyes használatáról.
BME/CrySys - Webes alkalmazások biztonsága	4	A képzés célja, hogy a résztvevők megismerjék és megértsék a webes technológiákra épülő alkalmazásokra leselkedő leggyakoribb támadásokat, valamint a tipikus fejlesztés során felmerülő hibákat, amik veszélybe sodorhatják a készülő rendszer biztonságát. Bemutatásra kerülnek többek között olyan sérülékenységek, mint az SQL injection vagy a Cross-Site Scripting. Az elméleti áttekintés mellett gyakorlati példák és kódrészletek is segítik a training anyagának az elsajátítását. A szoftverfejlesztési hibákon túl, a résztvevők megismerhetik a böngészőkben alkalmazott biztonsági modellt, és annak lehetséges megerősítését Content Security Policy alkalmazásával.
BME/CrySys - Windows biztonsági megoldások	4	A képzés célja a Windows rendszerek otthoni és céges környezetben történő biztonságos használatával kapcsolatos ismeretek átadása.
BME/CrySys - Linux biztonsági megoldások	4	A résztvevők megismerkednek néhány, Linux alapú rendszerek elleni támadással, majd ezt követően azokkal a biztonsági funkciókkal, beállításokkal és jó gyakorlatokkal, melyek segítségével védekezhetünk ezek ellen a támadások ellen. A cél a Linux rendszerek mindennapos használatának biztonságosabbá tétele.
BME/CrySys - Virtuális magánhálózatok	4	A képzés célja, hogy a résztvevők megértsék a virtuális magánhálózatok célját és jelentőségét a hálózati védelemben. Virtuális magánhálózatok segítségével egy nem biztonságos csatornán keresztül (mint például az Internet) lehet elérni olyan belső erőforrásokat, amiket egyébként csak helyileg lehetne használni. A technológia segítségével az otthonról dolgozó munkavállalók munkáját lehet nagyban segíteni, illetve a távoli telephelyek központi integrációja is elősegíthető. A képzés során a technológia használhatóságának az alapjait mutatjuk be, kiegészítve széles körben használt megoldások bemutatásával virtualizált környezetben.
BME/CrySys - Hálózati határvédelem tűzfalakkal	4	A tananyagegység célja, hogy a résztvevők megértsék a tűzfalak célját és jelentőségét a hálózati védelemben. Tűzfalak segítségével a vállalat határain átlépő forgalmakat szűrni lehet, hogy csak a cég számára szükséges forgalmak léphessenek át a határon. A képzés folyamán a résztvevők megértik a tűzfalak működésének alapjait, mikor és miért van rájuk szükség, illetve hogy mire alkalmasak vagy éppen nem alkalmasak. Többféle tűzfal is bemutatásra kerül az erősségeikkel és gyengeségeikkel egyetemben. Pár gyakran használt megoldás segítségével javaslatokat teszünk a telepítés és konfigurálás elkezdéséhez is.

Képzés megnevezése	Időtartam (óra)	Kiberbiztonsági és szoftvertechnológiai képzés – A szolgáltatás rövid leírása
BME/CrySys - Kiberbiztonsági incidensek kezelése	4	A tananyagegység áttekintést ad a kiberbiztonsági incidenskezelés főbb kihívásairól, módszereiről, és az incidenskezelés folyamatáról. A képzés célja, hogy a résztvevők megismerjék és elsajátítsák az incidenskezelés alapjait, folyamatát, vezetés-szervezési részleteit, az incidenskezelés fontosságát, működését, eredményét; értelmezni tudják az incidenskezelés előtt, közben és a végén elkészült anyagok tartalmát a műszaki-technikai részletek teljes értelmezée nélkül; és megértsék a szakszavakat használó általános leírásokat, szerződéseket, dokumentumokat.
BME/ftsrg - Folytonos integráció és szoftverellenőrzés	4	A folytonos integráció (Continuous Integration – CI) egy modern szoftverfejlesztési módszer, aminek során a fejlesztő csapatok folyamatosan integrálják egymás munkáit a gyors visszajelzés és jó minőség érdekében. A CI folyamat olyan eszközökkel segíthető, amik a szoftver elemeinek fordítását, tesztelését és ellenőrzését tudják automatizálni. A képzés célja a CI folyamat és módszerek bemutatása, melyhez Java programozási nyelv ismerete ajánlott. A résztvevők a tanfolyam után megértik a CI szerepét és jelentőségét jobb és biztonságosabb szoftverek létrehozásában.
BME/ftsrg - Szoftvertesztelési technikák	4	A szoftvertesztelés az egyik legalapvetőbb technika, amivel egy szoftver minőségét lehet mérni, majd javítani. A képzés célja, hogy a résztvevők megismerjék és megértsék a tesztelés különböző szintjeit, a teszttervezés alapvető módszereit.
BME/ftsrg - Statikus szoftverellenőrzési technikák	4	A statikus szoftverellenőrzési technikák a szoftver kód minőségét és biztonságát vizsgálják a kód végrehajtása nélkül. A statikus szoftverellenőrzés technikák széles csoportját ölelik fel a kódolási szabályoktól kezdve a kód felülvizsgálaton át az automatizált statikus analízis eszközökig. A résztvevők megértik, hogyan lehet különböző csapatok/fejlesztők számára kódolási szabványokat adni, és hogyan javítható a kód minősége statikus elemzési módszerekkel és eszközökkel. A tanfolyam a Java nyelvet használja példának.