digitaltech
EDIH

SZOLGÁLTATÁSI KATALÓGUS

BLOKKLÁNC ÉS KIBERBIZTONSÁG

MŰEGYETEM 1782

TARTALOMJEGYZÉK

BLOCKCHAIN

KIBERBIZTONSÁG

ADATMEGOSZTÁS ÉS -KÖVETÉS BLOKKLÁNCON

Képzés tartalma:

- Adatmegosztás alapfogalmai és demonstrációja

BLOCKCHAIN

Képzés leírása:
A blokkláncok által nyújtott egyik fő előny a megbízható adatmegosztás támogatása, egyetlen, minden résztvevő által elismert megbízható “harmadik fél” vagy közvetítő nélkül. Ezzel egyidőben a digitális iker (Digital Twin) és digitális szál (Digital Thread) megközelítések egyre érettebbek, támogató szabványokkal, adatszerkezetekkel és szolgáltatásmodellel.
A kurzus során demonstráljuk, hogyan tudja a blokklánc elosztott, megbízható adattárként segíteni potenciálisan ellenérdekelt felek együttműködését. Az NIST (USA szabványügyi hivatal) vonatkozó ajánlása alapján agilis gyártást támogató adatcsere folyamatot mutatunk be a blokklánc lehetőségeinek illusztrálása céljából.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

ÜZLETI EGYÜTTMŰKÖDÉSEK „BLOKKLÁNCOSÍTÁSA”

Képzés tartalma:

- A kurzus bemutatja a már ismert legjobb gyakorlatokat, megközelítéseket és felhasználási eseteket, beleértve a „blockchain-as-a-service” szintű szolgáltatásokat bemutatását is, melyek korábbiaknál alacsonyabb gazdasági/technológiai belépési küszöb mellett is lehetővé teszik a részvételt blokklánc hálózatokban.

BLOCKCHAIN

Képzés célja:

Bár a bemutatott felhasználási esetek listáját általánosságban állítottuk össze, a résztvevői igények mentén nyitottak vagyunk további szakterületek példáinak kiértékelésére is.
A kurzus az előadás/szeminárium jellegű oktatás mellett brainstorming jellegű közös kiértékelést/ ötletelést támogató foglalkozást is magába foglal.

Képzés időtartama: 8 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

A DIGITÁLIS IDENTITÁSOK JÖVŐJE

Képzés tartalma:

- Digitális identitások alapfogalmai
- Demonstráció

BLOCKCHAIN

Képzés célja:
A képzés résztvevői ismerjék meg a digitális identitások kezelésének alapfogalmait, kiemelten az önrendelkezésű azonosítókat, melyek megoldást adnak arra, hogyan lehet több szervezet által kibocsátott dokumentumokat/igazolásokat úgy felhasználni digitális szolgáltatásokban, hogy a szervezetek közt ne legyen szükség közvetlen kommunikációra.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

ÜZLETI BLOKKLÁNC MEGOLDÁSOK HYPERLEDGER ÉPÍTŐELEMEKBŐL

Képzés tartalma:

- Blokklánc alapú elosztott főkönyvi technológiák alapfogalmai és célja
- Mintaalkalmazás, egy tipikus követelményrendszer és funkciótervezés
- Blokklánc alapplatform (Hyperledger Fabric és Hyperledger Besu)
- Fejlesztéstámogatás (inkl. Hyperledger Firefly és Web3J)
- Tesztelés, verifikáció, validáció (inkl. Hyperledger Caliper)
- Digitális identitáskezelés (Hyperledger Aries, Indy, AnonCreds)
- Integráció (inkl. Hyperledger Cacti), Telepítés (inkl. Hyperledger Cello)
- Felhő szolgáltatások, Felügyeleti támogatás

BLOCKCHAIN

Képzés célja:

Kurzusunk az építőelemek között való eligazodást és megoldástervezésben alkalmazásukat segíti, fókuszban a szervezetközi blokkláncokkal és a Hyperledger Alapítvány nyílt forráskódú és ingyenes blokklánc projektjeivel. A kurzus során egy alkalmazási példán végigvezetve bemutatjuk, hogy hogyan vezet a tervezés és megvalósítás útja az ötlettől az okosszerződés-fejlesztésen keresztül a teljes rendszer kialakításáig; tárgyaljuk a fejlesztéstámogatást, fejlesztési idejű kód- és rendszerellenőrzéseket, a digitális identitáskezelést, a telepítéstámogatást, a felhő szolgáltatásokat és az integrációs megoldásokat. Azon funkciók esetén, ahol technológiai alternatívák léteznek, megadjuk ezek rövid összehasonlítását.

Képzés időtartama: 8 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

ÜZLETMENET BLOKKLÁNC FELETT

Képzés tartalma:

- Blokkláncosítás fogalmai és lépései
- Blokklánc as a service

BLOCKCHAIN

Képzés célja:

A képzés résztvevői ismerjék meg a blokklánc fölötti üzletmenet főbb jellemzőit, adott üzleti folyamatok blokkláncra vitelének feltételrendszerét és lépéseit.

Képzés időtartama: 7 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

BEVEZETÉS A KIBERBIZTONSÁGBA

Képzés tartalma:

- Alapfogalmak bevezetése
- Támadó modellek
- Sérülékenységek és ellenintézkedések
- Kockázatkezelés

KIBERBIZTONSÁG

Képzés leírása:
Ez a tananyagegység 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.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

KIBERBIZTONSÁG-MENEDZSMENT

Képzés tartalma:

- A kiberbiztonsági kockázatmenedzsment alapjai
- Fenyegetésmodellezés
- Fontosabb kiberbiztonsági szabályozások, törvények, és megfelelési követelményeik
- Fontosabb kiberbiztonsági szabványok
- Ismert kiberbiztonsági legjobb gyakorlatok

KIBERBIZTONSÁG

Képzés célja:

A képzés célja a kiberbiztonsági szabályozással kapcsolatos ismeretek átadása, a kockázatkezelés fázisainak, a fenyegetések modellezésére és a kockázatok kategorizálására alkalmas módszerek bemutatása.

A képzés sikeres elvégzésével a résztvevő:

- ismerni fogja a legfontosabb, nemzetközi és hazai, kiberbiztonsággal kapcsolatos szabályozásokat, törvényeket és szabványokat, az azoknak való megfelelés követelményeit, kihívásait és módszereit, a legjobb gyakorlatokat összefoglaló ajánlásokat, a kockázatkezelés fázisait, valamint fenyegetések modellezésére és a kockázatok kategorizálására alkalmas STRIDE módszert;
- képes lesz egy adott rendszerrel vagy szolgáltatással kapcsolatos főbb kiberbiztonsági kockázatok felismerésére és a kockázatok csökkentését célzó lépések megtételére.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

ADATVÉDELEM-MENEDZSMENT

Képzés tartalma:

- Az adatvédelem fogalma és célja, a GDPR alkalmazhatósága, a szereplők meghatározása
- A személyes, érzékeny és bizalmas adatok fogalma és azok azonosítása
- Az adatkezelés jogszerűsége
- Elszámoltathatóság, adatvédelmi hatásanalízis

KIBERBIZTONSÁG

Képzés célja:

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.
A képzés sikeres elvégzésével a résztvevő:

- ismerni fogja az Általános Adatvédelmi Rendelet (GDPR) fogalmait és a személyes adatokat feldolgozó adatkezelőkkel szemben támasztott követelményeket, a GDPR hatályát és alapelveit, az adatvédelmi kockázat- és hatáselemzés főbb lépéseit és technikai folyamatát, a kockázati események valószínűségének becslési, illetve a kockázat csökkentését célzó védekezési módszereket;
- képes lesz a kockázati események és azok attribútumainak, a lehetséges negatív hatások és az adott kockázati eseményekhez vezető fenyegetések (támadások) azonosítására

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

SZOFTVERBIZTONSÁG

Képzés tartalma:

- Az SDL folyamat általános áttekintése
- Követelmények fázis szükséges lépései
- Tervezés fázis szükséges lépései
- Implementáció fázis szükséges lépései
- Tesztelés fázis szükséges lépései

KIBERBIZTONSÁG

Képzés leírása:
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.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

WEBES RENDSZEREK BIZTONSÁGA

Képzés tartalma:

- Leggyakoribb webes sérülékenységek áttekintése
- Szerver oldali sérülékenységek
- Kliens oldali sérülékenységek

KIBERBIZTONSÁG

Képzés célja:
A tananyagegység 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.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

LINUX BIZTONSÁGI MEGOLDÁSOK

Képzés tartalma:

- Bevezető
- Általános jó gyakorlatok
- Esettanulmányok

KIBERBIZTONSÁG

Képzés célja:
A résztvevők megismerkednek a Linux alapú rendszerek elleni jellegzetes támadásokkal, majd ezt követően azokkal a biztonsági funkciókkal, beállításokkal és jó gyakorlatokkal, melyek segítségével védekezhetnek ezek ellen a támadások ellen. A cél a Linux rendszerek mindennapos használatának biztonságosabbá tétele.
A képzés sikeres elvégzésével a résztvevő:

- ismerni fogja a Linux alapú rendszerekkel kapcsolatos jellegzetes támadási módszereket, valamint a támadások elleni védekezés biztonsági funkcióit, beállításait és az alkalmazott jó gyakorlatokat;
- képes lesz az üzemeltetett Linux alapú rendszerrel kapcsolatos biztonsági kockázatok felimerésére és az alkalmazható védekezési módszerek kiválasztására.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

VIRTUÁLIS MAGÁNHÁLÓZATOK

Képzés tartalma:

- VPN-ek célja és feladata
- VPN-ek alapelemei
- VPN esettanulmányok

KIBERBIZTONSÁG

Képzés célja:
A tananyagegység 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.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

HÁLÓZATI HATÁRVÉDELEM TŰZFALAKKAL

Képzés tartalma:

- Tűzfalak célja és feladata
- Tűzfalak fajtái
- Tűzfal esettanulmányok

KIBERBIZTONSÁG

Képzés célja:
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 időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

KIBERBIZTONSÁGI INCIDENSEK KEZELÉSE

Képzés tartalma:

- Bevezetés az incidenskezelésbe
- Incidensre való felkészülés
- A kontextus meghatározása
- Kezdeti incidens válasz
- Csapat követelmények
- Esettanulmányok

KIBERBIZTONSÁG

Képzés célja:
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.

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

ANONIMIZÁCIÓS TECHNIKÁK ÉS RE-IDENTIFIKÁCIÓS TÁMADÁSOK

Képzés tartalma:

- Relációs adatok
- Aggregált adatok
- K-anonimitás
- Differenciális adatvédelem

KIBERBIZTONSÁG

Képzés célja:
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.
A képzés sikeres elvégzésével a résztvevő:

- megismeri a legelterjedtebb anonimizálási technikákat;
- elsajátít egy adatvédelmet szem előtt tartó gondolkodásmódot,
- képes lesz nem triviális adatvédelmi fenyegetések felismerésére és azok kockázatának becslésére

Képzés időtartama: 4 óra

Képzés formája: online

Szervező: BME/CrySys

ADATELEMZÉS ALAPÚ RENDSZER- ÉS FOLYAMATFEJLESZTÉS

Képzés tartalma:

- Fejlesztési/üzemeltetési folyamatok adatainak áttekintése
- Adatelemzési módszerek alkalmazása

KIBERBIZTONSÁG

Képzés leírása:
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.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

FOLYTONOS INTEGRÁCIÓ ÉS SZOFTVERELLENŐRZÉS

Képzés tartalma:

- A folytonos integráció alapfogalmai és jó gyakorlatai
- Biztonsági és funkcionális tesztelő/analízis eszközök bemutatása és integrálási lehetőségei a szoftverfejlesztésbe.
- GitHub Actions eszköz használatán keresztül bemutatott példák.

KIBERBIZTONSÁG

Képzés leírása:
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 tananyagegység 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.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

HATÁSANALÍZIS INFORMATIKAI RENDSZEREK MEGBÍZHATÓSÁGÁNAK KIÉRTÉKELÉSÉBEN

Képzés tartalma:

- Informatikai infrastruktúra elleni támadások lehetséges hatásai
- Modellezési módszert bemutatása hatáselemzéshez
- Szisztematikus kockázatelemzés előkészítése: begyűjtendő kulcsinformációk körének meghatározása
- Esettanulmány bemutatása.

KIBERBIZTONSÁG

Képzés leírása:
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.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

STATIKUS SZOFTVERELLENŐRZÉSI TECHNIKÁK

Képzés tartalma:

- Szoftverminőség mérése
- Szoftverminőség javításának módszerei

KIBERBIZTONSÁG

Képzés célja:
A statikus szoftverellenőrzési technikák a szoftver kód minőségét és biztonságát vizsgálják a kód végrehajtása nélkül. A statikus szoftverellenőrzés technikák széles csoportját öleli 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 tananyagegység a Java nyelvet használja példának.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

SZOFTVERTESZTELÉSI TECHNIKÁK

Képzés tartalma:

- Szoftvertesztelés alapjai
- Teszttervezési módszerek

KIBERBIZTONSÁG

A képzés célja:
A szoftvertesztelés az egyik legalapvetőbb technika, amivel egy szoftver minőségét lehet mérni, majd javítani. A tananyagegység célja , hogy a résztvevők megismerjék és megértsék a tesztelés különböző szintjeit, a teszttervezés alapvető módszereit.

Képzés időtartama: 4 óra

Képzés formája: hibrid

Szervező: BME/ftsrg

ELÉRHETŐSÉGEK, JELENTKEZÉS

Elérhetőségeink:

https://dtedih.bme.hu/

https://digitaltechedih.hu/

dtedih@vik.bme.hu

Jelentkezés képzésekre:

BME képzések