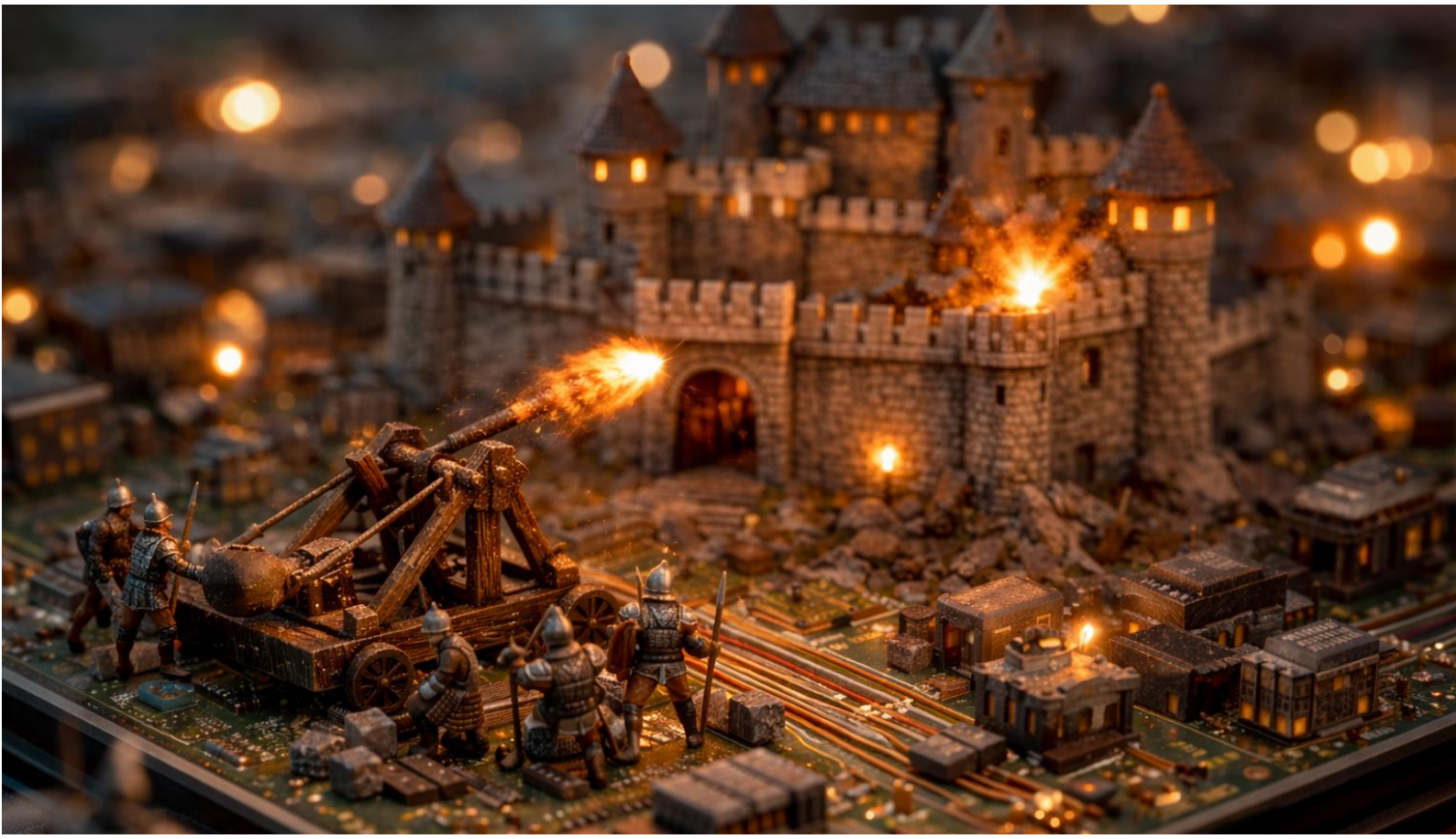
TRAINING360

CyberSecurity Connect **2**



Sérülékenységvizsgálati projektek és automatizált biztonsági vizsgálatok

A Training360 új kiberbiztonsági blended learning képzése, 2026. áprilistól

Bevezetés

A Training360 **CyberSecurity Connect** elnevezésű képzéssorozatának célja, hogy hasznos, naprakész és a gyakorlatban is jól hasznosítható technikai és menedzsment ismereteket adjon át a kiberbiztonsági területen, elősegítve ezáltal a cégek proaktív felkészülését és hatékonyabb működését. Mindezt rugalmasan és kedvező áron.

A digitalizáció felgyorsulásával a sérülékenységek száma és kihasználásuk sebessége soha nem látott mértékben nő. Az automatizált sérülékenységvizsgálat ma már nem csupán „jó, ha van", hanem alapvető eszköz a modern információbiztonságban: segít időben azonosítani a kockázatokat, csökkenteni az üzleti károkat és megfelelni a szabályozói elvárásoknak.

A Training360 újabb blended learning formájú képzése **gyakorlatorientált** módon mutatja be az automatizált eszközök használatát és az eredmények értelmezését, így a résztvevők azonnal alkalmazható tudást szereznek – legyen szó vállalati környezetről és felhasználásról, akár az egyéni szakmai tudás fejlesztéséről.

A képzés egyben felhasználható a 17/2025. (VII. 24.) EM rendelet („Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelmények-ről") 3. § és 4. § alapján az a), b), e) g) jelű területekre mint kiberbiztonsági továbbképzés.

Miért érdemes a Training360 kiberbiztonsági képzéseit választani?

- A trendek, piaci ismeretek és az aktuális jogszabályi környezet figyelembevételével, naprakész információkkal alakítottuk ki a képzési programokat és anyagainkat.
- Mind technikai, mind pedig a szervezeti (menedzsment) oldalról is körüljárjuk és ismertetjük a kiberbiztonsági témákat.
- A képzések és az anyagok fejlesztésében hazai és nemzetközi szintén is ismert és elismert, a kiberbiztonsági és információvédelem menedzsment területén több tíz éves tapasztalattal és gyakorlattal rendelkező szakértő oktatók vesznek részt.
- Modern és folyamatos támogatású távoli elérésű vagy fizikai laborkörnyezetet biztosítunk a különböző kiberbiztonsági eszközök, rendszerek és szituációk gyakorlatban történő kipróbálására.
- Időben és térben is rugalmas kialakítású tanulási módszertanok és támogatás áll a résztvevők rendelkezésére.

A képzés célja

A CyberSecurity Connect sorozatban a „Sérülékenységvizsgálati projektek és automatizált biztonsági vizsgálatok” képzés célja, hogy átfogó, gyakorlatorientált ismeret nyújtani azon szervezetek és szakembereik, valamint az IT-biztonság iránt érdeklődők számára, akik szeretnék megérteni és alkalmazni az automatizált sérülékenységvizsgálatok módszertanát és technológiai eszközeit, a projektek tervezésétől, a végrehajtáson keresztül, a célokat teljesítő zárásáig.

A tananyag elméleti oldalról széles körben tárgyalja:

- a sérülékenységek keletkezésének elvi alapvetéseit, besorolásuk nemzetközi sztenderdjeit, adatbázisaikat és a kapcsolódó keretrendszerek alkalmazását a szervezetek infrastruktúrájának tesztelése és védelme szempontjából.

- sérülékenységvizsgálati projektek felépítését, megvalósítását, az eredmények kiértékelését és prezentálását, valaminta a riportok készítését és befogadását részletesen, élő előadások és konzultációk formájában.

A tanfolyam gyakorlati oldalról:

- a támadó szemüvegén keresztül világítja meg az infrastruktúrák lehetséges hiányosságait, azok feltérképezését, a sebezhetőségek automatizált feltárásának, kihasználásának és validálásának lehetőségeit.

- Etikus hacker metodológiákat, automatizált vizsgálati módszereket és az azokra szolgáló eszközök használatát tanítja meg a résztvevőknek

- megfelelő technikai tudást biztosít, hogy a résztvevő ne csak brand-, vagy szoftverspecifikus készségeket szerezzen, hanem stabil ismeretekhez jusson a vizsgálatok során felmerülő problémák megoldásához, az eszközök által adott visszajelzések értelmezéséhez és az eredmények kiértékeléséhez.

A tudásanyag megszerzésének aktualitását és annak hosszú távú piacképességét – mind az érintett szervezetek, mind a területen munkát vállalók szempontjából – nagyban növeli, hogy míg a szervezetek hétköznapjaiban saját érdekből is, elkerülhetetlenül egyre nagyobb hangsúlyt kell kapnia a kiberbiztonság technológiai megvalósításának és tesztelésének, addig az EU NIS2 direktívájának a magyar jogrendbe történő ültetése kifejezetten előírja a kiberbiztonsági audit keretében sérülékenységvizsgálatok lefolytatását az arra kötelezett szervezeteknél.

A képzés elvégzésével…

A képzés elvégzésével a résztvevők az alábbi kompetenciákat szerezhetik meg:

- Automatizált sérülékenységvizsgálati projektek tervezése és menedzselése, a scope meghatározásától az eredmények üzleti szempontú kiértékeléséig.
- Sérülékenységek elméleti és gyakorlati megértése, nemzetközi szabványok, adatbázisok és keretrendszerek alkalmazásával.
- Technikai sérülékenységvizsgálatok végrehajtása, automatizált eszközök használatával, a találatok validálásával és értelmezésével.
- Etikus hacker szemlélet alkalmazása, támadói gondolkodásmóddal feltárt hiányosságok elemzése red és blue team környezetben is.
- Vizsgálati eredmények dokumentálása és kommunikálása, szakmailag megalapozott riportok és vezetői prezentációk készítésével.
- Eszközfüggetlen, problémamegoldó biztonsági gondolkodás, amely fejlesztési, üzemeltetési és megfelelőségi területeken is alkalmazható.

A képzés célcsoportja

A képzés a kis, közepes vagy akár nagyvállalati szervezetek technikai megvalósításért felelős és az információvédelem menedzsment területen dolgozó munkatársak, csapatok részére egyaránt ajánlott:

- Rendszergazdák, üzemeltetők, kezdő biztonsági szakértők, biztonság elemzők, akik szeretnék megérteni és alkalmazni az automatizált sérülékenységvizsgálatok módszertanát, eszközeit és megismerni azok technológiai hátterét.
- IT üzemeltetési előélettel rendelkező információbiztonsági vezetők, GRC feladatkörökben dolgozók számára a technológiai szakemberekkel történő hatékony együttműködés és munkavégzés érdekében.
- A NIS2, illetve a 2025. évi LXIX. törvény és a végrehajtási rendeletek alapján a kiberbiztonsági audit során sérülékenységvizsgálatok lefolytatására kötelezett szereplők számára (minden oldalon), hogy megismerjék az automatizált sérülékenységvizsgálati auditok felépítését és technikai hátterét.
- IT területen dolgozók, akik értékálló és eladható piaci tudást szeretnénk szerezni, és karrierjüket építeni például IT-biztonsági, etikus hacker, pentester irányba.

A képzés formája, felépítése

A tanfolyam online formában, blended learning módszertannal valósul meg. A képzés élő, online előadásokból, konzultációs alkalmakból; rögzített, önállóan feldolgozandó videós tananyagokból; tudásellenőrző tesztekből és házi feladatokból áll.

A képzés és anyagainak óraszáma: körülbelül nettó 30 óra, de a feldolgozási idő ennél több lehet a résztvevők előképzettsége, illetve a példák reprodukálására, a gyakorlati feladatok, tudásfelmérők megoldására, valamint a témák önálló feldolgozására és kiegészítésére való hajlandósága függvényében.

A képzés teljes átfutási ideje: 8 hét, ami heti 6-8 óra elfoglaltságot jelent (az élő alkalmakat is beleszámítva, melyek kb. 3 órásak). A magas élő óraszám, a konzultációknak a hallgatói aktivitás függvényében alakuló hossza, valamint a tematika komplexitása és a tanfolyam volumene miatt a meghirdetett 8 hét mellett egy további hétre opcionálisan egy tartaléknapot („esőnapot") is betervezünk.

Ütemezés: a gyakorlatok a kapcsolódó e-learning anyagokból a javasolt ütemezés szerint, de időben rugalmasan, szabadon feldolgozhatók a képzés ideje alatt; az élő képzési alkalmak pedig tervezetten szerdai napokon délutánonként kerülnek megtartásra (17.00-20.00 óra között). Az élő alkalmak rögzítésre is kerülnek és visszanézhetők a képzés végét követő 1 hónapig.

A gyakorlatok elvégzésére két lehetőség van:

a) saját környezetben: a képzés során a teljes laborkörnyezetet lépésről-lépésre alakítják ki a résztvevők és a későbbi példák elvégezhetők saját számítógépen. Ehhez min. Intel Corei5 vagy magasabb, vagy ennek megfelelő AMD teljesítményű és virtualizációt támogató CPU, min. 16GB RAM, és min. 200 GB SSD szabad tárhely, internetkapcsolat, lokális rendszergazdai jog szükséges.

b) távoli elérésű laborkörnyezet: a képzéshez igénybe vehető a Training360 interneten keresztül elérhető alapgépe, amire felépíthető majd a képzési laborkörnyezet. Ezen esetben elegendő egy kisebb teljesítményű laptop vagy PC, amin keresztül elérhető a távoli gép. Szélessávú internetkapcsolat szükséges. Ez a megoldás azok részére is megfelelő, akik pl. vállalati biztonsági beállítások miatt nem tudnak saját rendszert telepíteni.

A képzés ideje alatt aszinkron, chaten/fórumon történő szakmai támogatást biztosítunk a felmerülő kérdések, problémák megválaszolására.

Az egyes anyagok megfelelő elvégzéséhez **egy tanulási útvonalat** is adunk, illetve a képzés első, bevezetés moduljában élőben is részletesen ismertetjük a képzés felépítését, ütemezését és a hatékony tanulási stratégiát.

A képzéshez szükséges előképzettség

- Információbiztonsági alapfogalmak és alapelvek ismerete
- Hálózati és TCP/IP alapismeretek
- Alapfokú Linux üzemeltetési ismeretek valamilyen Linux disztribúcióban (fájlrendszer, működés, alapvető parancsok, fájlmenedzsment, folyamatok kezelése, csomagkezelés, felhasználó és jogosultság kezelési alapok, naplózási alapok, SSH)
- Alapfokú Windows üzemeltetési ismeretek valamilyen Windows Server rendszeren (fájlmenedzsment, hálózati és AD DS eszközök alapvető ismerete, programok menedzselése)
- Korábbi IT projektekben való részvétel előnyt jelent.
- Mivel sok esetben az információbiztonsági terminológia angol, ezért alapfokú szakmai angol nyelvismeret előnyt jelent, de nem feltétel a résztvételhez. A képzés magyar nyelven zajlik.

A képzés tervezett témái

Megjegyzés: a felsorolt témakörök, anyagok és előadások sorrendje (illetve részben az élő adások tartalmi mélysége) változhat, idomúlva a lebonyolítás menetéhez és a résztvevői előképzettségekhez és haladáshoz.

Az egyes előadásokhoz kapcsolódóan ellenőrző kérdések és önálló utánajárást igénylő feladatok is kapcsolódnak, illetve áttekintjük az előző gyakorlati feladatok megoldását. A modulok gyűjtőtémák, ezeken belül több fejezet is lehetséges.

1. téma – A sérülékenységvizsgálati projektek

A modul bemutatja, hogyan illeszkednek a sérülékenységvizsgálatok egy szervezet védelmi stratégiájába. A résztvevők megismerik a sérülékenységvizsgálati projektek felépítését és kivitelezését, a szükséges körülményeket, valamint a mérföldkövek és a szerepkörök meghatározását.

Tárgyaljuk a manuális, a rendszer- illetve alkalmazáscélzott, és az általános automatizált sérülékenységvizsgálati procedúrák, a behatolás tesztelésének és az ethical hacking munkamenetének különbségeit, és az ezekből adódó lehetőségeket, előnyöket és hátrányokat. Külön hangsúlyt kap az előkészítés, a lebonyolítás, az eredmények elfogadása vagy visszautasítása, valamint a zárás témaköre, miközben a teljes folyamatot áttekintjük.

A résztvevők megismerik a sérülékenységvizsgálati riport elkészítésének folyamatát, annak jelentőségét, tartalmának felépítését és kritikus pontjait .

A modul betekintést nyújt abba, hogyan épül fel egy sérülékenységvizsgálati projekt, hogyan zajlik és hogyan érinti a szervezet életét, miközben biztosítja, hogy átláthatóan és hatékonyan valósuljon meg. Mindez hasznos tudást nyújt akkor is amikor a végrehajtó, de akkor is, amikor a megbízó vagy befogadó oldalon vállalunk szerepet – bármely szinten – a projektekben vagy a szervezet életében.

2. téma – Sérülékenységek keletkezése, természetük, típusaik, rendszerezésük és súlyozásuk

A résztvevők megismerik a sérülékenységekhez kapcsolódó definíciókat, keletkezési okaikat és támadásuk, illetve kihasználásuk vektorait a támadó szemszögéből nézve. A témakör emellett kitér a technológiai, az ellátási láncot érintő és az emberi tényezőkből fakadó, technológiai sérülékenységek formájában megjelenő kockázatokra, valamint a hálózati, kiszolgáló és alkalmazás szintű sebezhetőségek keletkezésére.

A modul bemutatja az ismert sérülékenységek besorolását, súlyozását, a vonatkozó nemzetközi sztenderdeket és jó gyakorlatokat, a sebezhetőségeket soroló adatbázisok szerepét azok feltárásában és kezelésében. Ez a tudás elengedhetetlen a sérülékenységek és ezzel a kockázatok megértéséhez, priorizálásához, kezeléséhez. Megismerése ad lehetőséget arra is, hogy a hallgató később megértse az ismert, tipikus és ismeretlen sérülékenységek keresésére törekvő automatizált sérülékenységvizsgálatok céljait, kivitelezésüket és az azt végző eszközök működését.

A témakörben elsajátítható tudás nem csak technológiai szakembereknek és nem csak a sérülékenységvizsgálatokhoz kötődő munkakörökben, hanem az IT- és információbiztonság, illetve az infrastruktúrák üzemeltetésében és fejlesztésében bármely területén szerepet vállalók számára kötelező (kellene, hogy legyen).

3. téma – Az infrastruktúrák és a hálózati eszközök szervezéséből és működtetéséből adódó sérülékenységek

A modul tárgyalja az infrastruktúrákban és a hálózatokon előforduló alapvető sérülékenységek típusait és példákat hoz azokra. Ideértve – és mások mellett – a konfigurációs hibákat, az emberi tévedéseket, vagy az eszközök és szoftverek kezelésének hiányosságaiból fakadó problémákat, illetve ezeknek a támadó által történő kihasználásának lehetőségeit.

A témakör tárgyához szorosan kapcsolódik az emberi tényező által létrehozott sebezhetőségek témaköre a rendszerszervezés és az üzemeltetés oldaláról, illetve a jó- és rosszhiszemű felhasználói / munkavállalói magatartásból eredő, végső soron támadási vektorokká alakuló lehetséges problémák köreinek megismerése.

A résztvevők technológiai megközelítésből, prezentációkon bemutatott példákon keresztül ismerik meg a hálózati architektúrát érintő, az ellenérdekelt fél által támadási vektorokká alakítható tipikus hibákat és problémákat.

4. téma – A protokollok, eszközök és infrastruktúrák szabványosított működésében velünk élő sebezhetőségek

A modulban tárgyaljuk az informatika számos területén már ismert sebezhetőségekkel, illetve elfogadott / elfogadható kockázatokkal bíró és a keretrendszerek és a jó gyakorlatok alapján már kerülendő eljárásokat és protokollokat. Kitérünk az informatikai szabványokban rögzített hálózati protokollok működésében, azok verziózásában, kezelésében és a kompatibilitást biztosító megoldásokban rejlő problémákra és veszélyekre.

A témakörben tárgyaljuk és demózzuk a nyers erő alapú támadási vektorokat, illetve a hálózati mechanizmusok szabványosításában és az informatika korlátaiban velünk élő támadási vektorokat és azok aspektusait.

A megértés és a tesztesetek lehetőségének megismerése szándékával demózzuk a próbálgatásos, a túlterheléses, az eltereléseses és a középreállásos támadások legfontosabb metódusait. A résztvevők megértik miért állnak elő végtelen számban ezek a sebezhetőségek, miért éltek túl évtizedeket és miért lesznek velünk a következőkben is, miközben ugyanezen okokból fakadóan számolnunk kell velük az infrastruktúráink védelmének kialakításakor és tesztelésük alkalmával is.

Mindeközben a résztvevők megtanulják ezek kivitelezésének és tesztelésének automatizált módszereit és, hogy ezeknek a cseppet sem barátságos, szélsőségesen veszélyes támadási vektoroknak hol a helyük, mikor, hogyan és milyen körülmények között tesztelhetőek – vagy sem – a szervezet életében és infrastruktúrájában.

5. téma – Infrastruktúrák automatizált feltérképezése és a védelmi intézkedések kijátszásának és tesztelésének lehetőségei

A modul a szervezeti és informatikai infrastruktúrák internet és intranet oldali automatizált feltérképezésétől halad, a védelmi intézkedések tesztelésének és kijátszásának lehetőségei felé, majd megalapozza a fellelt eszközök és kiszolgálók automatizált sérülékenységvizsgálatának kivitelezését.

A hallgató megismerkedik az infrastruktúrák feltérképezésének módszereivel és eszközeivel, illetve a kapcsolódó folyamatok mögött zajló technológiai történésekkel. Mivel ennek során biztosan szembesülünk azok jelenlétével a komplex infrastruktúrákon, a témakörhöz tartozik az azt óvó védelmi intézkedések áttekintése, a védelemért felelős rendszerek alapvető természetének tárgyalása, azok funkcióinak és reakcióinak tesztelésének és kijátszásának lehetőségei. A tanuló megismeri a „hallgatózó”, a forgalmat figyelő eszközök felderítésének lehetőségeit és gátjait is.

A szekció része a fizikai hálózatok és szerverek mellett, a virtualizált hálózatok, a VM, a VPS, illetve a VPN-en keresztül az infrastruktúrába kapcsolt telephelyek néhány, a felderítés, a sérülékenységvizsgálatok és a biztonságos működése szempontjából fontos sajátosságának tárgyalása.

A résztvevő megismerkedik a kapcsolódó, alacsony szintű hálózati eljárásrendek működésével és az azok sztenderdizációjában rejlő, a publikus és zárt infrastruktúrákon történő felderítésre és sérülékenységek keresésére történő felhasználásával. A résztvevők megtanulják használni az ezeket a folyamatokat automatizáló alapvető eszközöket, miközben megismeri az infrastruktúrák és a védelmi intézkedéseik feltérképezésének, és a sérülékenységek feltárásának komplex összefüggéseit.

6. téma – Kiszolgálók és eszközök automatizált sérülékenységvizsgálata

A modul az infrastruktúra feltérképezése során fellelt kiszolgálók, felhasználói és egyéb eszközök operációs rendszereinek és élő szolgáltatásainak, azok verzióinak azonosítását, illetve ezek sérülékenységeinek automatizált keresésének technológiai hátterét és eszközeinek használatát dolgozza fel. Ezek lehetnek direkt a „szervervason" és annak operációs rendszerén futó, vagy virtualizált kiszolgálók, a munkavállalók mobil vagy asztali eszközei, IoT eszközök, de akár a hálózati eszközök adminisztrációs felületei vagy portjai mögött futó operációs rendszerek vagy szolgáltatások is. Egyszóval bármi, ami LAN / WLAN infrastruktúrát használ, akár az ilyen hálózatokra kapcsolt ipari, megfigyelő, vagy beléptető eszközök is.

A résztvevő megismeri ezek automatizált sérülékenységvizsgálatának menetét és mély tudást szerez a kivitelezésükre szolgáló eszközök működéséről, használatáról és a háttérben zajló technológiai folyamatokról. A tanfolyam során több parancssori eszközt is megtanul használni, melyeken keresztül rálátást kap arra, hogy milyen folyamatok, milyen metodológia mentén kerülnek integrálásra és automatizálásra a komplex vállalati megoldásokat nyújtó eszközök által. Ezzel hatékonyan használható, brand-független tudást szerez meg.

A témakör részét képezi néhány, összetett vállalati megoldásokat kínáló eszköz áttekintése és lehetőségeik összevetése, illetve a vizsgálati eredmények aggregálására szolgáló tool megismerése és használata. Mindeközben a tanfolyam egyik legfontosabb erőssége, hogy a hallgató olyan tudást szerez meg, amelynek birtokában erős alapokkal és megfelelő technológiai ismeretekkel fog rendelkezni, függetlenül attól, hogy mely gyártó, melyik eszközén, vagy épp milyen „színű vagy szagú" kezelőfelületen kell dolgoznia.

Tervezett élő, online előadások és konzultációk *(a sorrend és tartalom még változhat)*

1. hét

- Útmutató a platform és a tananyag használatához, a tesztek kitöltéséhez, a feladatok megoldásához – Bevezető, tematika, elvi alapvetések, tárgy- és fogalomkörök, kontextusok a tanfolyam anyagához

2. hét

- Sebezhetőségek és kockázatok keletkezése – Sérülékenységek fő típusai, osztályozása és besorolása – Támadási vektorok kialakulása – Sztenderdizálás és kapcsolódó keretrendszerek

3. hét

- A sérülékenységvizsgálati projekt: célok, felépítés, lebonyolítás, felelősségek, skálázás, hozzáadott érték – Audit szcenáriók és jó gyakorlatok

4. hét

- Az infrastruktúra védelmének alapvető eljárásai, eszközei és azok legfontosabb jellemzői, valamint tesztelésük és kijátszásuk lehetőségei

5. hét

- Az örökké velünk élő alapvető támadástípusok – Az eltereléses, középreállásos, nyers erő alapú, próbálgatásos és túlterheléses támadások – Megvalósításuk – Tesztelésük lehetőségei és korlátai

6. hét

- Protokollok és szabványok veleszületett gyengeségei – A hálózati eszközök alapértelmezett működéséből, illetve az infrastruktúrák nem megfelelő szervezéséből fakadó sebezhetőségek

7. hét

- Sérülékenységek és sebezhetőségek keresésének összetett lehetőségei és projektjei – Kapcsolódó auditeljárások az automatizált sérülékenységvizsgálatok tematikáján és lehetőségein túl

8. hét

- Sérülékenységvizsgálati riport készítése, elemei, kapcsolódó jó gyakorlatok és nemzetközi sztenderdek – Teljes és részleges riportok, azok átadása, átvétele, visszautasítása és verziózása

Rögzített és hetente megjelenő, és önállóan feldolgozandó gyakorlati videós anyagok
(a sorrend és tartalom még változhat)

1. hét

- Laborkörnyezet létrehozása – Vizsgáló gép építése és kritériumai – Alapvető hálózati folyamatok és mechanizmusok – Hálózati forgalom monitorozása Wireshark használatával

2. hét

- A hálózati kommunikáció protokolljai és működése – A belső infrastruktúrák (intranet) felderítése, annak eszközei és módszerei

3. hét

- Szervezetek és infrastruktúráik internet oldali feltérképezése – Publikus IP és DNS infrastruktúrák – OSINT – A threat hunting és a threat intelligence alapvetései

4. hét

- Infrastruktúrák és sérülékenységek felderítésének speciális és következtetés alapú módszerei – A védelem eszközeinek kijátszásának és tesztelésének módszerei és eszközei

5. hét

- Forgalom elterelése, középreállás megvalósítása, nyers erő és próbálgatás alapú, illetve túlterheléses támadások megvalósítása és tesztelése, ezek lehetőségei és korlátai a gyakorlatban

6. hét

- Operációs rendszerek és szolgáltatások azonosítása – Eszközök és kiszolgálók automatizált sérülékenységvizsgálata, annak parancssori, illetve összetett vállalati eszközei

7. hét

- Sérülékenységek validálásának metódusai, módszerei, követelményei és a technológiai validálás – Exploitálás, a támadás eszkalációja és annak következményei

A képzés tervezett ütemezése:

- Tervezett kezdés: 2026. április 22.
- Az élő elméleti adások és konzultációs alkalmak tervezett időpontjai: 2026. április 22., április 29., május 6., május 13., május 20., május 27., június 3., június 10. (tartaléknap: június 17.)
- Várható befejezés: 2026. június második hete.

A képzés szakértője, oktatója

Kiss Sándor

Sándor szakterülete a szervezetek és infrastruktúrák komplex információbiztonsága, annak átfogó vizsgálata és tesztelése. Az elmúlt 20 évben az online pénzügyi szolgáltató és szerencsejáték, illetve az autóipari, közlekedési és feldolgozóipari szektorban is tapasztalatokat szerzett. Jelenleg vállalkozó, aki hazai és nemzetközi biztonsági projektekben vállal – mindent "is" lefedő – tanácsadói szerepet. Ezzel párhuzamosan 2019 óta fejleszt szakmai anyagokat és tart képzéseket az ethical hacking, az IT infrastruktúrák és a biztonsági vizsgálatok tárgykörében. Tananyagainak kialakítása és átadása során trainer hozzáállást követ, és a területen elengedhetetlen, a gyakorlati valóságra építő, széleskörű és biztonságcentrikus világlátás átadására helyezi a hangsúlyt.

A képzés zárása

A képzés végén egy 50 kérdésből álló online tudásfelmérő tesztet kell kitölteni, melynek sikeresség esetén a képzés a felnőttképzési törvény alapján Tanúsítvánnyal zárul.

A képzés egyben felhasználható a 17/2025. (VII. 24.) EM rendelet („Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelmények-ről") 3. § és 4. § alapján az a), b), e) g) jelű területekre mint kiberbiztonsági továbbképzés

Jelentkezési információk

A képzésre az első körös jelentkezési határidő: 2026. március 27.
A képzés minimálisan 30 fő jelentkezése esetén indul.
Simon Ferenc, +36 (30) 388-8264, ferenc.simon@training360.com

Tovább információk és jelentkezés

https://www.training360.com/cybersec-connect-2

Érdekel a kiberbiztonság és információ védelem-menedzsment?

Ne hagyd ki a CyberSecurity Connect első képzését sem, ami a **Kibervédelmi vonalak kiépítéséről és az incidensmenedzsmentről** szól.

- Teljes és átfogó képet kapsz az incidens menedzsment kialakításáról és üzemeltetésről technikai és szervezeti szinten egyaránt.
- Megismerheted a fontosabb szervezeti intézkedéseket, jogszabályi háttereket, lépéseket, melyek az incidensek kezeléséhez szükségesek.
- Elméletben és gyakorlatban is megismerheted és kipróbálhatod a népszerű naplózó és elemző eszközök, és kapcsolódó biztonsági rendszerek működését és alapvető alkalmazását és használatát.
- Elsajátíthatod a biztonság tesztelés alapjait.

További információk, érdeklődés:

https://www.training360.com/cybersec-connect