



JUNIOR KIBERBIZTONSÁGI SZAKEMBER KÉPZÉS
ISMERTETŐ RÉSZTVEVŐKNEK



Tartalom

Mi az a CyberCamp?	3
A CyberCamp szakmai háttere, a FORTIX Academy.....	3
Kinek szól a CyberCamp?	4
Miért érdemes elindulni a kiberbiztonság területén?	4
Mennyit kereshetsz a képzés sikeres elvégzése után?	5
Milyen munkaköröket láthatsz el?	5
Garanciát vállalunk a karrieredre!	6
Képzési információk	7
Miről fogsz tanulni a CyberCamp 5 hónapja alatt?.....	7
Hány órát kell tanulással töltened?.....	10
Milyen oktatási módszereket alkalmazunk?.....	11
Felvételi követelmények.....	11
Vizsgarendszer	11
Tandj és fizetési lehetőségek	12
Kapcsolat.....	13
Ügyfélszolgálat rendje.....	13

Mi az a CyberCamp?

Saját magad is tapasztalhatod, hogy napról napra egyre nagyobb jelentősége van az információvédelemnek. Bizonyára te is kaptál már automatikus figyelmeztetéseket, hogy fel akarják törni az e-mail fiókod, vagy küldtek neked zsaroló leveleket, melyben bizonyos összeg fizetésére kérnek. Ez nagyban is így megy, és ahhoz, hogy a cégek megfelelő módon tudják megvédeni adataikat, kiberbiztonsági szakemberek szükségesek.

A CyberCamp-et azért hoztuk létre, mert célunk, hogy szakértő, profi kiberbiztonsági szakembereket képezzünk ki. Több évtizedes tapasztalattal rendelkezünk az információbiztonság területén, és látjuk, hogy mekkora a munkaerőhiány ezen a területen.

A CyberCamp Magyarország vezető kiberbiztonsági szakember képző bootcamp-je, ahol 5 hónap alatt magabiztos tudást és gyakorlatot kapsz, és egy garantált, felfelé ívelő karrierútra lépsz!

Képzésünk segítségével elindíthatod e területen karrieredet akkor is, ha eddig teljesen más szakterületen dolgoztál, és szakirányú előképzettséged sincs.

A CyberCamp szakmai háttere, a FORTIX Academy

A FORTIX Consulting Kft. jogelődje, a Secure-IT Hungary Kft. 2011-ben alakult, 100%-os magyar tulajdonosi háttérrel.

Elsődleges célunk az volt, hogy az információbiztonság és üzletfolytonosság területén szerzett megrendelői és szolgáltatói tapasztalatokra támaszkodva minőségi és magas szakmai tanácsadást nyújtsunk az ügyfeleink számára.

Munkánk során az ügyfelek komplex biztonságát helyezük előtérbe, mivel hisszük, hogy a vállalatok sikerének egyik kulcseleme az információbiztonság és az üzletfolytonossági rendszer megfelelő, stratégiai szintű kezelése.

A tanácsadási tapasztalatokból adódó lehetőségeket kihasználva az oktatás területét 2017-től önálló szolgáltatásként működtetjük, immár saját arculattal. Tesszük mindezt abból a felismerésből adódóan, hogy a piacon elérhető hasonló témájú tréningek leginkább egy-egy követelményrendszerhez kapcsolódnak, jellemzően nem használják ki a különböző területek között fellelhető azonosságokat (hasonlóságokat) és alig nyújtanak konkrét megoldásokat, technikákat a megismertetett elvárásokhoz.

A FORTIX Academy különböző szakterületeken kínál oktatási, illetve tréning szolgáltatásokat információbiztonság, üzletfolytonosság és menedzsment témakörökben, továbbá az ezekhez kapcsolódó szakmai területeken.

Az oktatások fő jellemzői a gyakorlatorientáltság, a napi életből vett példák feldolgozása és a kiemelt szakmai színvonal. A könnyen elérhető követelmények ismertetése helyett az alkalmazható megoldásokra koncentrálnak a tréningek, oktatások eredményeként a hallgatók képessé válnak a napi működésbe könnyen beépíthető megoldások alkalmazására.

Kinek szól a CyberCamp?

Pályaváltóknak

Szabadulj meg attól a munkától, amivel elégedetlen vagy! Ez a képzés segít abban, hogy karriert válts az egyik leggyorsabban növekvő szakma felé. Nem számít, milyen a háttered, nincs szükség előképzettségre, hogy csatlakozz a CyberCamp-hez, minimális feltételünk, hogy legyen érettséged.

Diákoknak és diplomásoknak

Ha most fejezted be tanulmányaidat, de szeretnél a jövő egyik legdinamikusabban fejlődő iparágára specializálódni, akkor itt a lehetőség! Csatlakoz hozzánk egy egészen új szemlélettel felvértezett képzésre! Az első naptól kezdve el tudod kezdeni a tanulást, fejlődést és készen fogsz állni arra, hogy a munkaerőpiacra egy olyan vadonatúj készlegkészlettel lépj ki, amelyet a vállalatok széles körben keresnek szerte a világon.

Karriererősítőknak

Amennyiben már IT-val foglalkozol, de érdekel a kiberbiztonsági terület, biztos lehetsz benne, hogy megtalálsz nálunk a számításodat! A CyberCamp-et kifejezetten arra terveztük, hogy fejlesszük képességeidet, hogy kiberbiztonsági szakemberként dolgozhass junior pozícióban.

Miért érdemes elindulni a kiberbiztonság területén?

A technológia leggyorsabban fejlődő területe

Nem csak egy gyorsan növekvő területről van szó, a kiberbiztonság területén közel egy évtizede nulla százalékos a munkanélküliség. Versenyképes javadalmazással és rengeteg lehetőséggel teli jövőbiztos karrieredet egyetlen módon érheted el, mégpedig azzal, hogy elsajátítod a témát.

Munkaerő-szakadék

Ahogy a kiberfenyegetések egyre kifinomultabbak, a szervezetek állandó kihívással néznek szembe. Olyan képzett kiberbiztonsági szakembereket kell toborozniuk, akik képesek megvédeni rendszereiket a rosszindulatú szereplők fenyegetésével szemben.

Digitális jogsértések és üzleti biztonsági rések

A technológia fejlődése a gazdasági növekedés fő hajtóereje, de a kibertámadások gyakoribb előfordulásához is vezethet. Az olyan vezető trendek, mint az e-kereskedelem, a mobilfizetés, a számítási felhő, a Big Data és az analitika, az IoT, az AI, a gépi tanulás és a közösségi média, mind növelik a felhasználók és a vállalkozások kiberkockázatát.

A kiberbiztonság igényének növekedése a globális világjárvány miatt

A kiberbiztonságban erőteljes növekedést tapasztalunk a Covid-19 okozta világjárvány miatt. Munkavállalók milliói kénytelenek több időt home office-ban, online tölteni, ez óriási teret teremtett a kiberbűnözők számára. Ez azt is indukálta, hogy a vállalatoknak többet kell befektetni kiberbiztonsági szakemberekbe.

Mennyit kereshetsz a képzés sikeres elvégzése után?

Junior kiberbiztonsági munkatársként akár bruttó 450.000-650.000 Ft/hó munkabért is kaphatsz. Ez az összeg, minél tapasztaltabb leszel, annál magasabb lehet.

Milyen munkaköröket láthatsz el?

Információbiztonsági tanácsadó

Feladatok:

- IT biztonsági rendszerek bevezetése, fejlesztése
- IT biztonsági projektek projektmenedzsmentje
- IT fejlesztések információbiztonsági kontrollja
- Véleményezés, javaslattétel, figyelemmel kísérés
- Alkalmazásbiztonsági feladatok ellátása
- Mobileszközök biztonsági feladatainak ellátása, mobil védelmi eszköz üzemeltetése biztonsági incidensek kivizsgálása, kezelése
- Közreműködés a vállalat informatikai biztonsági rendszereit érintő auditokban

Információbiztonsági munkatárs

Feladatok:

- Rendszeres IT biztonsági ellenőrzések, felülvizsgálatok végzése
- Kockázati nyilvántartás vezetése, kockázatok nyomon követése
- Informatikai projektek IT biztonsági támogatása
- Az informatikai infrastruktúra információbiztonsági vonatkozásainak kiértékelése, véleményezése
- Új vagy meglévő IT rendszerekhez biztonsági ajánlások megfogalmazása

Incidenskezelő

Feladatok:

- IT biztonsági monitoring tevékenység végzése, IT biztonsági monitoring eszközök felügyelete megszakítás nélküli munkarendben
- Behatolásmegelőzés – hálózati forgalom vizsgálata és értékelése, lehetséges gyenge pontok jelzése
- Forensic – naplóesemények értelmezése, egyéb környezeti jellemzők, bizonyítékok gyűjtése és események pontos dokumentálása, szükség esetén eskalálása L2 támogatói szintre
- IT biztonsági események azonosítása, eskalálása
- Az IT biztonsági eseményekhez, incidensekhez kapcsolódó biztonsági jelentések, beszámolók készítése
- Együttműködés az IT üzemeltetés, a hálózatfelügyelet, SOC L2 illetve L3 támogató területekkel, illetve az IT Helpdesk munkatársaival
- Az informatikai környezet kialakításának szakmai elkísérése

Kiberbiztonsági üzemeltető

Feladatok:

- Kiberbiztonsági technológiák, rendszerek bevezetése, konfigurálása, üzemeltetése és felügyelete
- Hálózati és végponti védelmi eszközök felügyelete
- Felhasználói hozzáférések beállítása, felügyelete, felülvizsgálata
- Sérülékenységi vizsgálatok lefolytatása, sérülékenységek kezelése
- Szoftverek biztonsági frissítése, és ezek felügyelete
- Felhasználók biztonsági tudatosítása, támogatása

Kiberbiztonsági elemző

Feladatok:

- Biztonsági események monitorozása, gyanús események elemzése
- Reagálás az incidensekre (fogadás, validálás, besorolás, koordináció, kommunikáció stb.)
- Evidenciagyűjtés, elemzés és kiértékelés
- Utólagos incidensek kiértékelése, tanulási célból az incidensben érintett területeken a munkatársak oktatása
- Sérülékenységek elemzése, érintett rendszerek körének meghatározása, kockázatcsökkentő akciók koordinálása
- Fenyegtettségek elemzése, jelentése
- A változó támadási technikák, a kártékony kódok, programok működésének folyamatos elemzése

Garanciát vállalunk a karrieredre!

A FORTIX Academy elkötelezett abban, hogy a megfelelő szakmai minőség és színvonal mellett hallgatóink karrierjét is támogassa. Éppen ezért több megoldással készültünk, hogy minél nagyobb lehetőséged legyen rögtön a képzés sikeres elvégzését követően használni, fejleszteni a megszerzett tudásodat.

Tégy magad is a karrieredért! Válaszd ki a számodra megfelelő konstrukciót!

1. Kizárólag a képzés és/vagy a tanúsítvány érdekel.

Ebben az esetben a képzés tananyagának elsajátítására, a vizsgák letételére koncentrálhatsz. Ha csak a képzés érdekel, nem szabjuk meg, hogy hány százalékot érj el a modulzáró, valamint a képzést záró vizsgákon.

Amennyiben a tanúsítvány megszerzése is a célod, a záró vizsga eredménye minimum 60% kell legyen. A vizsgarendszerről alább olvashatsz.

2. **Garantált karriertámogatást szeretnék!**

Itt már az eredményen is nagy a hangsúly, nem csak a minimális erőbedobás számít a részedről. Amennyiben azt szeretnéd, hogy segítsünk abban, hogy a megszerzett tanúsítványoddal el tudj helyezkedni, a záróvizsgán minimum 80%-os eredményt kell elérned!

Amennyiben ez sikerül, segítségül hívunk egy partner-állásközvetítő céget, aki mindent meg fog tenni annak érdekében, hogy mielőbb megtaláld álmaid munkahelyét.

3. **Gyakornok szeretnék lenni!**

Mondhatnánk, hogy ez a hegy csúcsa, ebben a konstrukcióban ugyanis, amennyiben a záróvizsga eredményed 90% vagy afölötti, vagy a FORTIX-nál, vagy pedig valamely partnercégünknél dolgozhatsz napi 8 órában, garantáltan minimum 6 hónapig.

A gyakornoki program leteltét követően a munkáltatóval történő egyeztetés eredménye a mérvadó.

Képzési információk

A képzés formája: élő online + e-learning

A képzés időtartama: 15 hét (hétfő, kedd, szerda, csütörtök: 17:00-20:00)

A képzés nyelve:

- Az élelőszavas előadások, prezentációk nyelve magyar
- A képzési platform, tananyagok, prezentációs anyagok, kiadandó anyagok, videók, projektfeladatok, vizsgafeladatok nyelve magyar és angol.

Hiányzás:

A képzésről a megengedett hiányzás az összes óraszám 20%-a, azaz összesen 42 óra. Ezen óraszám feletti hiányzás esetén még sikeres záróvizsga elérésével sem állítható ki tanúsítvány. Így sem a garantált karriertámogatás, sem pedig a gyakornoki programban való részvétel nem lehetséges.

Miről fogsz tanulni a CyberCamp 5 hónapja alatt?

Információbiztonsági alapok

Ebben a modulban a kiberbiztonság alapjain túl egyéb nélkülözhetetlen témakörökkel – többek között a fizikai biztonsággal és a humán biztonsággal – is meg fogsz ismerkedni.

E tantárgy témái:

- A kiberbiztonság alapjai
- Fizikai biztonság
- Humánbiztonság, kockázatok, biztonsági tudatosítás és kommunikáció
- Biztonság az ellátási láncban

Rendszerbiztonság

Milyen operációs rendszert használasz? Windows? Linux? Hallottál már a virtualizációról? Ha nem, az sem baj! E tantárgy keretei között minden releváns ismeretet meg fogsz kapni.

E tantárgy témái:

- Windows alapok és biztonság
- Linux alapok és biztonság
- Végpontvédelem
- Virtualizáció

Információvédelem

A 21. században az információ fénysebességgel értékelődik fel. Szakemberként mindent meg kell tudnod tenni e vagyon védelme érdekében. Ebben segít neked ez a modul.

E tantárgy témái:

- Identitás- és hozzáféréskezelés
- Alkalmazott kriptográfia
- Adatszivárgás elleni védelem

Sérülékenység-menedzsment

Sérülékenységei már a középkori váraknak is voltak. Sajnos e gyengepontok az informatikai rendszerekben is jelen lehetnek. Nem mindegy azonban, hogy ezeket milyen gyorsan fedezzük fel és javítjuk ki. Tegyük együtt bevehetetlenné a várat!

E tantárgy témái:

- Kiberfenyegetések felderítése és modellezése
- Sérülékenységek felderítése és menedzsmentje

Etikus hacker ismeretek

Az etikus hacker-ek egyre keresettebbek és egyre fejlettebb eszköztárral rendelkeznek ahhoz, hogy meg tudják határozni egy-egy számítógépes rendszer gyengepontjait. Rajta hát, fedezd fel velünk azt az eszköztárat !

E tantárgy témái:

- Etikus hacker ismeretek
- Behatolásvizsgálat

Kommunikációs alapok

Ahhoz, hogy maximálisan teljesíts, nagyon jó kommunikációs képességekre van szükséged. Bizony, jó eséllyel nem egy kapucnis pulcsiban fogsz ülni egy sötét szobában. Fontos, hogy mindenkiel könnyedén megtaláld a hangot. Ebben segít neked ez a modul.

E tantárgy témái:

- Kollaboráció és kommunikáció, facilitálás, moderáció, interjúk, workshop-ok
- Konfliktuskezelés
- Asszertív kommunikáció
- Active listening, érzelmi intelligencia
- Prezentáció, retorika, előadás

Irányítási és menedzsment folyamatok

A különböző szabványok, a kockázatmenedzsment és az üzletfolytonosság elemeinek alapos ismerete nélkül a legjobb szakember is csak félkarú óriás.

E tantárgy témái:

- Irányítási rendszerek alapjai, szabályzatok, folyamatok (ISO27001 és ITIL alapokon)
- Kockázatmenedzsment
- Megfelelés, audit, adatvédelem
- Üzletfolytonosság, szolgáltatásfolytonosság

Hálózatbiztonság

A számítógépes hálózatok képezik az internet alapját. Működésük ismerete elengedhetetlen a szakmában. Protokollok, hálózati eszközök, infrastruktúrák... A kurzus végére már ezek a kifejezések sem lesznek ismeretlenek számodra.

E tantárgy témái:

- A számítógépes hálózatok alapjai
- Vállalati hálózatbiztonság

Naplózás, észlelés és incidenskezelés

Ahogy egy betörő is hagyhat nyomot maga után, ez a kibertér bűnözőire is igaz. Nagyon fontos a nyomok korai felismerése, értelmezése, illetve a megfelelő lépések megtétele. Képzésünkben természetesen ez sem marad ki.

E tantárgy témái:

- Naplózás és észlelés
- Incidenskezelés (SOC műveletek)
- Digitális kriminalisztika (Forensics)

Webalkalmazás-biztonság

Ma már szinte minden komolyabb alkalmazás valamilyen szerveren fut. Ebből következik, hogy a szolgáltatásokat akár a telefonodról is igénybe tudod venni. Gondolkodtál már rajta, hogy egy-egy ilyen program hány különböző típusú támadásnak van kitéve? Ha nem, itt az ideje...

E tantárgy témái:

- Kódolás
- Webalkalmazás-biztonság / Secure SDLC

Feltörekvő technológiák

5G, blockchain, önvezető autó, okosváros? Csak néhány, a manapság oly divatos technológiák közül. Kerülj képbe velük és ne csak a barátaidat kápráztasd el, hanem a leendő munkaadódat is!

E tantárgy témái:

- Biztonsági automatizálás, Devops, Devsecops
- Feltörekvő technológiák, trendek a védekezésben

Munkaszervezés

A korszerű munkamódszerek és a projektmenedzsment ma már egy külön tudomány részét képezik. Vannak olyan helyzetek, amikor egy-egy döntést pillanatok alatt kell meghoznod, mi több, e döntésnek maximálisan megalapozottnak kell lennie. A munkaszervezés – többek között – az ilyen helyzetekben segít neked.

E tantárgy témái:

- Operatív feladatok ellátása
- IT projektmenedzsment
- Agile + scrum

Hány órát kell tanulással töltened?

Munkaidőn kívüli képzésünk heti 4 napon 3 órát vesz igénybe. Hétfőn, kedden, szerdán, csütörtökön 3 kontaktórát lesz, amelyek délután 17:00-20:00 óráig kerülnek megtartásra. A pénteki napot az e-learning tananyagok elsajátítására szánjuk.

Mivel csodát sajnos mi sem tudunk tenni, fontosnak tartjuk megemlíteni, hogy mindez önálló tanulás nélkül nem elég. Javasoljuk, hogy hetente 5-10 órát szánj az ismeretek alapos feldolgozására, gyakorlására, ismétlésére.

Milyen oktatási módszereket alkalmazunk?

Képzésünk maximálisan gyakorlatorientált. Nem hiszünk sem a végtelen diasorokban, sem az indokolatlanul mély elméleti megközelítésben. Természetesen az elmélet, vagyis a módszertani alapok megismerése és az előadások nem mellőzhetők, de minden tantárgy esetén figyelünk a helyes arány megválasztására. A képzés során önállóan és csapatban is fogsz dolgozni.

Felvételi követelmények

Ahhoz, hogy felvételt nyerj a CyberCamp képzésünkre, minimum érettségivel kell rendelkezned, illetve a jelentkezési lapot ki kell töltened és felmutatnod a középfokú tanulmányaid elvégzését igazoló dokumentumot..

Vizsgarendszer

Modulzáró vizsga

Minden tantárgy elsajátítása után modulzáró vizsgán fogsz számot adni a tudásodról. Természetesen, a felkészülésben maximális segítséget nyújtanak a CyberCamp szakértő oktatói, bármi kérdésed lenne, vagy esetleg elakadnál a tananyagban.

A modulzáró vizsgán minimum 60%-os eredményt kell elérned minden tantárgyból, csak ebben az esetben mehetsz a záróvizsgára.

A modulzáró vizsga online formában lesz megtartva, jellemzően gyakorlati feladatok lesznek, kiegészítve egy-egy teszt jellegű vagy kifejtős feladattal. Amennyiben alapos indokkal nem tudsz részt venni a modulzáró vizsgán, egy előzetesen egyeztetett időpontban pótolhatod azt egy alkalommal.

Záróvizsga

A záróvizsgára bocsátás feltétele, hogy az összes tantárgy modulzáró vizsgáján minimum 60%-os eredményt érj el. Nem mehet záróvizsgára az, akinél akár csak egy tantárgy sikeres eredménye nem igazolt!

A záróvizsgára biztosítunk felkészülési időt.

A záróvizsga egy módszertani vizsgarészből és egy komplex gyakorlati feladat megoldásából áll.

Módszertani vizsgarész:

A képzés során elsajátított módszertani tudás mérése, mely tesztjellegű, illetve kifejtős feladatokból fog állni. Az módszertani vizsgarészen minimum 60%-os eredményt kell elérni, akkor lesz értékelhető.

Gyakorlati vizsgarész

A képzés során elsajátított gyakorlati tudás mérése, mely feladatmegoldás(ok)ból fog állni. A gyakorlati vizsgarészen minimum 60%-os eredményt kell elérni, akkor lesz értékelhető.

Tanúsítvány

Tanúsítvány abban az esetben állítható ki, amennyiben a záróvizsga eredménye legalább 60%-os.

A tanúsítványon a képzésen való részvétel és a sikeres vizsga tényét rögzítjük. A tanúsítvány adott munkakör betöltésére nem, de junior kiberbiztonsági feladatokat láthat el.

A képzés sikeres elvégzése után jogosult leszel a FORTIX által kiállított tanúsítványra.

Tandíj és fizetési lehetőségek

Hiszünk abban, hogy aki hajlandó keményen dolgozni karriercéljaiért, megérdemli a lehetőséget a sikerre. Ezért kínálunk különféle fizetési lehetőségeket, hogy megvalósíthasd álmaid karrierjét.

Előre fizetés egy összegben

A tandíjat fizetheted előre egy összegben önköltségen vagy munkáltatói utalással.

Fizetendő összeg: Bruttó 640.000 Ft / fő

Teljes tandíj: 503.937 Ft+ÁFA = 640.000 Ft / fő

Részletekben a képzés közben

A tandíjat havi részletekben is fizetheted a teljes képzés időtartama alatt. Ez azt jelenti, hogy a tandíj összegét 5 részre osztottuk, így minden hónapban ugyanakkora összeget kell fizetned.

Fizetendő összeg: Bruttó 132.000 Ft / hó / fő, 5 hónapon keresztül

Teljes tandíj: 519.685 Ft+ÁFA = 660.000 Ft / fő

Részletekben utólag

A tandíjat havi részletekben is fizetheted a képzés befejezése utáni hónaptól egy éven keresztül. Ez azt jelenti, hogy a tandíj összegét 12 részre osztottuk, így minden hónapban ugyanakkora összeget kell fizetned.

Fizetendő összeg: Bruttó 59.000 Ft / hó / fő, 12 hónapon keresztül

Teljes tandíj: 557.480 Ft+ÁFA = 708.000 Ft / fő

Mit tartalmaz a tandíj?

- ✓ 214 óra élő online képzést, plusz a képzéshez tartozó e-learning tananyagokat a képzés végéig
- ✓ A tanúsítvány megszerzéséhez szükséges vizsgadíjakat
- ✓ Hozzáférést a teljes képzési tananyaghoz (prezentációk, videók, feladatlapok, esettanulmányok)
- ✓ Saját névre szóló cybercamp.hu e-mail címet a kurzuson való részvétel ideje alatt
- ✓ A CyberCamp zárt Facebook csoportjához tagságot
- ✓ A gyakornoki programban fix fizetést legalább 6 hónapon keresztül a fent részletezett feltételek teljesítése esetén

Kapcsolat

Kollégánk, **Vas Eszter** oktatásszervező munkaidőben, hétfőtől péntekig 09:00 és 17:00 óra között szívesen áll rendelkezésedre bármilyen kérdés esetén a webinfo@cybercamp.hu e-mail címen.

Weboldalunk címe: www.cybercamp.hu

Ügyfélszolgálat rendje

Ügyintézési, észrevétel-, reklamációbejelentési lehetőség kedden és csütörtökön 09:00-10:00 óráig a +36 70 620 7242 telefonszámon.