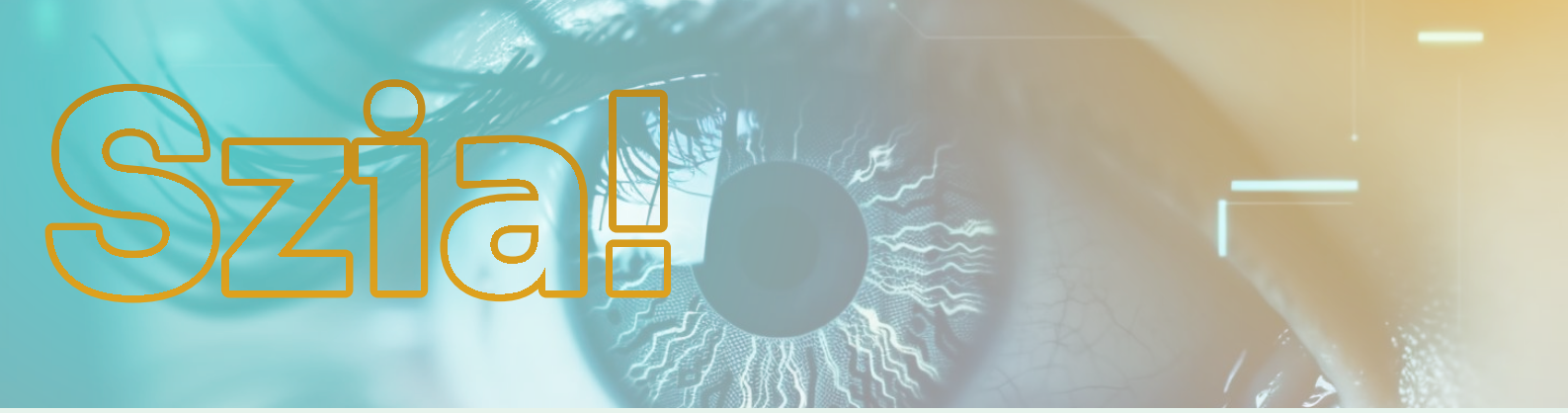
Karrier-útmutató

Miért és hogyan indulj el a kiberbiztonsági szakmában?

CYBERCAMP



Ezt az útmutatót azért írtam, hogy betekintést nyerhess a kiberbiztonság - mint szakma - világába, megmutassam fontosságát, motiváljalak és segítségedre legyek abban, hogy elindulhass ebben az igen szerteágazó, dinamikusan fejlődő és mindenki számára lehetőségekkel teli szakmában.

Elsőként egy hatalmas félreértést szeretnék tisztázni. Legtöbbeknek az a benyomása, hogy a kiberbiztonsági szakma kizárólag technikai kötődésű, illetve csak a „hekkerek" és „kockák" világa. Ez amiatt lehet, mert nincs elegendő és jól érthető információ arról, hogy valójában miről is szól ez a szakma. Pedig rendkívül szerteágazó – és nem csak technikai – karrierutakat tesz lehetővé egy kis technikai alapozással.

Fontos emellett, hogy az információ- vagy kiberbiztonság nem is egyetlen szakma, hanem **szakmák családja**. Ahhoz hasonlíthatnám, mint amikor valaki azt mondja, hogy „Sportoló vagyok." Ilyet ugye ritkán hallunk; hiszen általában konkrét sportokról beszélünk. Ugyanígy, a kiberbiztonsági szakma sem egyetlen monolit; több különböző szintű és különböző képességeket igénylő szakmák összefoglaló neve. Ezért bátran mondhatom, hogy az alapismeretek megszerzése után **bármilyen háttérrel és érdeklődéssel találhatsz számodra érdekes és motiváló területet**, hivatást ebben a szakmában.
Tehát az induláshoz:

- nem kell tudnod programozni
- nem kell diploma
- nem kell matekzseninek lenned
- és bármilyen életkorban elkezdheted!

Ez az útmutató a szakmával kapcsolatos információhiányt hivatott betölteni, remélem, érdekesnek és izgalmasnak találod, és elgondolkodtat azon, vajon neked is tartogathat-e jövőálló, biztos megélhetést és izgalmas irányokat. A válasz, ami reményeim szerint a végén neked is egyértelmű lesz: **Igen!**

Csapjunk is bele, és sok sikert kívánok karriered során!

Imi – a CyberCamp alapítója

Tartalom

Fejezetek

Hasznos és érdekes (keretben)

Digitális életünk: veszélyes kényelem

A kiberbiztonság kifejezéssel manapság annyit dobálóznak, hogy már-már közhelyesnek számít. De tudjuk valójában, miről is van szó?

Kipróbáltad már, mi történik, ha egy napig nem férsz hozzá az Internethez?

Gondold végig, mi történik a színfalak mögött minden alkalommal, amikor csatlakozol az Internethez. Ahogy életünk egyre inkább a digitalizáció által uralt térré válik, az online és offline világ közti határok kezdenek elmosódni. Ma a digitális technológia nemcsak áthatja mindennapjainkat, hanem alapvetően át is alakítja azokat. **A mindenütt jelenlévő digitalizáció hatással van arra, hogyan érintkezünk egymással, hogyan dolgozunk, vásárolunk, kezeljük pénzügyeinket, hogyan szórakozunk, sőt, még arra is, hogy hogyan érzékeljük a valóságot!** Bár ezek a változások sosem látott kényelmet és hatékonyságot hoznak magukkal, számos kockázatot is rejtenek magukban, különösen a digitális létünk biztonságát tekintve!

Minden alkalommal, amikor bejelentkezel, hogy e-mailt küldj, böngéssz vagy posztolj közösségi oldaladon, pénzt utalj, online vásárolj – digitális lábnyomokat hagysz magad után. A kiberbűnözők ezeket a nyomokat lopják el, manipulálják és használják fel adataid, profilod, pénzed megszerzése érdekében! **A kibertámadások emberek millióit érintik személyesen, évente (dollár)milliárdokba kerülnek a cégeknek és országoknak egyaránt**, sőt befolyásolják a világpolitikát is. Ezeknek a támadásoknak a növekvő gyakorisága és egyre kifinomultabb volta rávilágít arra, hogy **sürgősen szükség van hozzáértő kiberbiztonsági szakemberekre**, akik ezeket a támadásokat igyekeznek megakadályozni és elhárítani – a mindezek mögött futó informatikai rendszerek, folyamatok és szervezetek biztonságossá tételével.

Kiberfenyegetések és következményeik

Lássunk néhány aktuális kiberbiztonsági fenyegetést. Ijesztőek, nem?

Zsarolóvírus (Ransomware): Ezzel a típusú rosszindulatú szoftverrel a támadók blokkolják az informatikai rendszerek működését, amíg az áldozatok nem fizetnek ki egy bizonyos összeget. Az utóbbi években riasztóan megnőtt ezek száma, és a támadók mindent céloznak, az ipari rendszerektől az egészségügyi rendszerekig, blokkolva létfontosságú szolgáltatásokat.

Adathalász támadások (Phishing): Valós és legitim kommunikációnak álcázva, a phishing jelenleg a támadók fő eszköze a rendszerekbe való beférkőzésre és károkozásra, bejelentkezési adatok és pl. bankkártyaszámok megszerzésével. Egyre kifinomultabbá válnak, átverve a hagyományos észlelési módszereket és még a tapasztalt felhasználókat is megtévesztve.

Adatszivárgások (Data Leakage): Az adatszivárgások az adatokhoz való tömeges jogosulatlan hozzáférést jelententik. A következmények pusztítóak lehetnek – kikerülhetnek érzékeny személyes adatok, szellemi tulajdon és akár államtitkok is.

Terheléses támadások (Denial of Service, DoS): E támadások célja üzleti rendszerek, pl. webshopok, portálok leállítása. Képzeld el például, hogy leáll egy kórházi vagy banki rendszer. Ezek a támadások nem csupán szolgáltatás fennakadást okoznak, hanem álcaként is szolgálhatnak további behatoló kibertámadásokhoz.

A kiberbiztonság tehát nem csupán az informatikai rendszerek és információk védelméről szól, hanem a modern életmódunkat támogató infrastruktúrák stabilitásának és megbízhatóságának biztosításáról is!

Miért érdemes a kiberbiztonsági karriert választani?

Először is, a kiberbiztonság változatos:

számtalan területre terjed ki, mint egy óriási metropolisz sugárútjai.
Van a támadó oldal (Red Team), az úgynevezett etikus hackelés, ahol a jó fiúk megtanulják a támadók fortélyait, hogy szimulált támadásokkal segítsenek megvédeni minket a rosszakkal szemben. Aztán ott vannak a védők (Blue Team), akik felépítik a védelmet és figyelik a hálózatokat, elemzik a sebezhetőségeket, megoldják a problémákat. A harmadik fő terület az irányítási, kockázatkezelési és megfelelési terület (GRC), ahol a technikai és szervezési megoldások bevezetésének és működtetésének szabályozása, priorizálása történik, az adott cég profiljához és kockázataihoz igazítva.

A kiberbiztonság területe folyamatos fejlődésben van. Ahogy új technológiák jelennek meg, új kihívások is megjelennek a kiberbiztonság területén. Már nem csak "számítógépekről" van szó; **a mai kiber-tájképbe beletartoznak például az intelligens eszközök, a mobilhálózatra csatlakoztatott autók, a „tárgyak internete" (IoT), a robotok, és legújabban a mesterséges intelligencia és gépi tanulásra épülő rendszerek is**. Ezek a technológiák egytől egyig új lehetőségeket és új kihívásokat hoznak magukkal.

Ha **informatikával eddig nem is találkoztál szakmailag**, de érdekel, vagy képzett vagy a **pszichológia, a szociológia, ügyfélszolgálat, szolgáltatások, marketing, sales, projektmenedzsment, folyamatszervezés, adminisztráció/koordináció, oktatás, tréning/coaching, a technológia vagy akár a jog területén** – és még sorolhatnám – akkor a kiberbiztonság tökéletes választás lehet számodra. Ez a terület nem csak a kódolásról, hekkelésről vagy a számítógépek "berheléséről" szól; a problémamegoldásról, világos kommunikációról, az ügyfelekkel és a csapatokkal való együttműködésről, bűnözők pszichológiájának megértéséről és időnként a jogi részlegnek a legújabb adatvédelmi törvényekben való eligazodásban való segítségnyújtásról szintúgy!
Mivel a technológia rohamosan változik, **olyan emberekre van szükség a szakmában, akik készen állnak a tanulásra, az alkalmazkodásra, önállóak, megoldás-orientáltak és megőrzik hidegvérüket akkor is, ha forró a helyzet!**

Hogyan találd meg saját utadat?

Képzelj el egy világot, ahol mindenki ihletetten kel fel és indul munkába, s napja során biztonságban érzi magát, tudva, hogy értékes munkát végez.
Este lelkében megelégedéssel tér haza, hiszen napja teljes és hasznos volt.
Utópia? Kezdd magaddal!
Pályakezdő vagy, vagy éppen kiégtél? Az **Ikigai**, modern felfogásban, négy alapvető elemet kapcsol össze: amit szeretsz, amiben jó vagy, amire a világnak szüksége van, és amiért megfizetnek. Ez a filozófia segít meghatározni, hogy érdeklődésed hol találkozik a gyakorlatiassággal, így pályaválasztásod egyszerre lesz kielégítő és életképes.

Az alábbiakat érdemes tehát kiderítened és "átfedésbe hoznod":

- Miben vagy jó?
- Mit szeretsz?
- Mire van szüksége a „világnak"?
- Miért kaphatsz fizetséget? (pénzt, elismerést, stb.)

Ha tehát ilyen típus vagy, a kiberbiztonsági szakma téged hív! Gondolj bele - mit ér a biztonsági rés azonosítása, ha nem tudjuk egyszerűen elmagyarázni azoknak, akiknek cselekedniük kell? Akár a vezetőséget kell meggyőznünk a szükséges biztonsági fejlesztések büdzséjéről, akár a csapatnak kell elmagyaráznunk, hogyan lehet megelőzni egy jövőbeli katasztrófát, az egyértelmű kommunikáció képessége kritikus.
És akkor ott van a problémamegoldás. Ó, a kifinomult kibertámadás kibogozásának kihívása, ami költői túlzással néha olyan, mintha egy Rubik-kockát oldanál meg bekötött szemmel egy hullámvasúton ülve. A kiberbiztonsági problémák nem csak technikai jellegűek; ezek olyan rejtvények, amelyek minden egyes megoldási kísérlet során változtatják alakjukat. Ehhez kreativitásra, türelemre és sémáktól, illetve csőlátástól mentes gondolkodásra is szükség van. Ha szeretsz olyan összetett problémákat megoldani, amelyeknek gyakran nincs egyszerű megoldása, akkor nagyszerű feladatok várnak rád. Nem utolsó sorban **„jövőálló", jól fizető és kiemelkedően hasznos munkát végezhetsz!**

Így aztán pályakezdők és pályamódosítók számára a kiberbiztonsági terület ígéretes pályát kínál!

Növekvő kereslet: A digitális technológiák elterjedése az informatikai (IT) rendszerekben tárolt és feldolgozott adattömeg és függés exponenciális növekedéséhez vezetett. Mivel ezt a bűnözők is felismerték, ez kiváló lehetőségekkel teli munkaerőpiacot teremt a digitális és kiberbiztonsági szakemberek számára, és az előrejelzések szerint folyamatos növekedés várható, anélkül, hogy telítődés lenne látható.

Értékes munka: A kiberbiztonság területén dolgozni azt jelenti, hogy erőfeszítéseidnek közvetlen hatása van az emberek magánéletének és biztonságának védelmére, mert munkáddal hozzájárulsz majd a digitális mindennapok védelméhez.

Áthozható készségek és tapasztalat: Sok, más területen szerzett készség nagyon jól alkalmazható a kiberbiztonságban is. A kommunikációs képességek, problémamegoldó és (ön)szervezési készségek és az üzleti folyamatok megértése mind értékesek, és segíthetnek áthidalni a területen kezdők technikai hiányosságait is.

Folyamatos fejlődés: A kiberbiztonság olyan terület, amely soha nem áll meg. A technológiák és a kiberbűnözők által alkalmazott taktikák folyamatos fejlődése mindig kihívásokat fog a szakértők elé támasztani. Ez teszi a kiberbiztonságot tökéletes karrierlehetőséggé azok számára, akiket mozgat a folyamatos személyes és szakmai fejlődés! A kiberbiztonsági szakemberek tehát sokféle háttérrel rendelkeznek, és különböző nézőpontokat hoznak a területre, ami létfontosságú a biztonsági kihívások innovatív és eredményes megoldásainak kidolgozásához. Függetlenül attól, hogy valakinek a technikai területeken, például a kódolás és a rendszerbiztonság területén, vagy olyan humán képességek terén, mint a kommunikáció és az oktatás van tapasztalata, a kiberbiztonságban hatalmas igény van ezekre a nézőpontokra!

A jövő a tudásalapú munkáé

A negyedik ipari forradalom alapvető változást jelent abban, ahogyan élünk, dolgozunk és egymáshoz viszonyulunk. A megelőző ipari forradalmaktól eltérően ezt a korszakot a technológiák olyan fúziója jellemzi, amely elmossa a fizikai, a digitális és a biológiai szféra közötti határokat. Nézzük meg a negyedik ipari forradalomra jellemző technológiai konvergenciát és annak munkaerőre gyakorolt mélyreható hatásait, különös tekintettel a fizikai munkáról a tudásalapú munkára való áttérésre. A negyedik ipari forradalom során az iparágak között példátlan összekapcsoltság és kölcsönös függőség tapasztalható. A bio-, nano- és információs technológiák és a kognitív tudományok konvergenciája új iparágakat hoz létre és régi iparágakat szüntet meg, miközben átformálja a karrierutakat. Az egészségügyben például a mesterséges intelligencia a betegek gyorsabb és pontosabb diagnosztizálására lesz képes, mint a legtöbb emberi munkatárs.

Munkaerőpiaci változások

Ahogy a gépek egyre több fizikai és rutinfeladatot vesznek át, a munkaerő-piaci igények jelentősen eltolódnak a problémamegoldást, intuíciót és érzelmi intelligenciát igénylő szerepek felé - olyan képességek felé, amelyek egyedülállóan emberiek és a gépek által nem könnyen reprodukálhatóak. Ez az eltolódás újfajta szakemberek iránti keresletet teremt - olyanokét, akik képesek ötvözni a technikai tudást a stratégiai és kreatív gondolkodással.

Tudásalapú társadalom

A tudásalapú társadalomban az információ és az oktatás a gazdasági termelékenység és növekedés elsődleges mozgatórugójává válik. Itt **a tudás és az adatok kulcsfontosságú erőforrások, ellentétben az ipari alapú társadalommal, ahol a fizikai javak domináltak**. Ez a váltás a munkaerő (vagyis mi, emberek) folyamatos tanulásának és alkalmazkodóképességének szükségességét hangsúlyozza. A tudásalapú gazdaság az oktatási rendszerben olyan változtatásokat igényel, amelyek az új generációkat felkészítik a jövő munkahelyeire. Ez nemcsak a problémamegoldó és kritikus gondolkodási készségek fejlesztését jelenti, hanem a digitális készségek oktatását is az oktatás minden szintjén. Mindez szép, de **a legfontosabb, hogy saját kezedbe vett képességeid fejlesztésének felelősségét!**

Adatok mindenhol

A tudásalapú társadalomban az adat értékes eszköz. Az adatok elemzésének és értelmezésének képessége szinte minden iparágban kulcsfontosságú készséggé válik, ami átalakítja a hagyományos szerepköröket, és újakat hoz létre, mint például az adattudósok, a gépi tanulási mérnökök és automatizálási szakemberek.

Mit csinál egy kiberbiztonsági szakértő?

Nézzük, mit is csinálnak, és milyen munkakörökben dolgoznak a szakértők a kiberbiztonság területén – amiről már tudod, hogy nem egyetlen szakma, hanem szakmák egy családja. Az alábbiakban néhány jellemző példát sorolok fel, „a teljesség igénye nélkül", tájékozódásul, a három jellemző területet bemutatva.

Ezek a karrierutak különböző fókuszokat és szakértelmet igényelnek, de mindegyik létfontosságú szerepet játszik a digitális eszközök és információk védelmében.

Kibervédelmi szakértők (Blue Team)

- **Incidenskezelés (Incident Response)** A kiberbiztonsági szakértők itt az első vonalban dolgoznak, reagálnak a fenyegetésekre, mérséklik a károkat és biztosítják a rendszerek mielőbbi helyreállítását.
- **Sérülékenység-kezelés (Vulnerability Management):** Ezek a szakemberek folyamatosan értékelik és kezelik a szervezet rendszereinek biztonsági hiányosságait, mielőtt azokat a támadók kihasználhatnák.
- **Hálózati biztonsági felügyelet (Network Security):** A hálózati infrastruktúra monitorozása és karbantartása, amely létfontosságú a rendszerek kapcsolódása és biztonságuk fenntartása szempontjából.
- **Biztonsági elemző (Security Analyst):** Ez akár a Blue, akár a GRC teamben az információk elemzéséért, döntések előkészítéséért és a napi feladatok elvégzéséért felelős kollégák egy általánosabb elnevezése.
- **Security Architect (magyarul nem jellemző mondani):** Nem közvetlenül a „blue team" tagja, inkább irányító funkciója van. Nagy szakmai tapasztalattal bíró szakértő, aki egy építészmérnökhöz hasonlóan működik; a cég fő kockázati profilja, működése és az informatikai/kiberbiztonsági rendszerek mély és átfogó ismeretével felvértezve megtervezi a kiberbiztonsági rendszereket és irányítja azok egységes bevezetését.

Támadó szakértők (Red Team)

- **Behatolási tesztelő, etikus hacker (Penetration Tester, Pentester, Ethical Hacker)**: Szimulált kibertámadásokat hajt végre annak érdekében, hogy azonosítsa a rendszerek sebezhetőségeit, mielőtt azokat valódi támadók kihasználnák.
- **Social Engineer (magyarul még nem kiforrott a neve, hívjuk „átverési szakértőnek". Semmiképpen ne hívjuk „szociális mérnöknek"):** Az embereket, mint a biztonsági rendszerek „leggyengébb láncszemét" veszi célba és manipulálja annak érdekében, hogy bizalmas információkhoz, jogosultságokhoz, vagy pl. irodákhoz férjen hozzá, vagy rávegye őket olyan dolgokra, amikkel kijátssza a biztonsági szabályokat és rendszereket és szimulálja a károkozás lehetséges módjait, ezzel erősítve a biztonságtudatosságot.
- **Threat Hunter (magyarul még nem kiforrott a neve, hívjuk „fenyegetés-vadásznak").** Értelmezhető a Blue Team tagjaként is, ám eszköztára az etikus hackeréhez áll közelebb, ezért került ide. Ők aktívan keresik a szervezet IT rendszereiben és hálózatán a már „beszivárgott" támadókat, ezek nyomait keresve rendszerekben, és tevékenységük jeleit keresve a hálózaton.
- **Biztonsági tesztelő (Security Tester):** Szintén valójában Blue Team, ám szintén részben pentester eszköztárral. A rendszerekben, tipikusan egy-egy fejlesztési csomag élesítése során derítik fel a fejlesztés során bekerült esetleges biztonsági réseket, fejlesztői vagy konfigurációs hibákat.

GRC (Governance, Risk, and Compliance) szakértők

- **Megfelelési szakértő (Compliance expert):** Azt biztosítja, hogy a szervezetek megfeleljenek a rájuk vonatkozó (biztonsági, védelmi) jogszabályoknak, szabványoknak és egyéb, például céges ügyfelek által támasztott előírásoknak.
- **Szabályzati felelős (Security Policy Expert):** Feladata a külső elvárások és kockázatok kezeléséhez, azok követelményeinek belső „kodifikálása", szabályozása; a szabályzatok és folyamatok azok érdekeltjeivel való egyeztetése és megvalósításának koordinálása.
- **Kockázatkezelési szakértő (Risk Manager):** Értékeli a potenciális üzleti és biztonsági kockázatokat, megoldásokat javasol azok kezelésére és koordinálja ezek végrehajtását.
- **Ellenőr (Auditor):** Múlt századi nevén revizor. Független szemmel és módszeresen ellenőrzi, hogy a szervezetek mennyire tartják be a különböző biztonsági előírásokat. Szigorú neve ellenére nagyon fontos konzultatív partner a szakmában.
- **Kiberbiztonsági tanácsadó (Cybersecurity Consultant):** Külső szemmel értékeli a vállalat biztonsági stratégiáját és intézkedéseit, megoldásokat javasol és koordinálja, segíti azok bevezetését. Ideális esetben gyorsabban és hatékonyabban juttatja el a céget a kívánt állapotba, mintha azt házon belül végeznék. Tanácsadóként a kiberbiztonság bármely egyéb szakterületén lehetsz aktív.
- **Információbiztonsági felelős, vezető (CISO):** Felelős a szervezet teljes kiberbiztonsági stratégiájának felügyeletéért.
- **Biztonsági oktató, tréner (Security Instructor/Awareness Trainer):** Képzik a munkatársakat és adott esetben a cég ügyfeleit (pl. bankok esetén) a biztonsági tudatosság emelése érdekében, az óvatosság és a jó gyakorlatok mikéntjéről, belső szabályokról, a kibertámadások megelőzése érdekében.

További területek

- **Ne feledkezzünk meg:** A területhez kötődő további szerepekről sem, köztük a projektvezető, értékesítő, ügyféltámogató, marketingszakember, tartalomgyártó, rendezvényszervező, játéktervező, üzleti intelligencia (BI) szakértő, építész, operátor, akiknek kiberbiztonsági területen, célzott ismeretekkel új lehetőségek nyílnak a szakmájukban!

Ipari forradalmak

Az ipari forradalmak olyan jelentős gazdasági és technológiai átalakulásokat jelentenek, amelyek mélyen átformálták a társadalmakat, a gazdaságokat és a munka világát. Alapvetően megváltoztatták, hogyan élünk, dolgozunk és kommunikálunk egymással a világban.

Az 1. ipari forradalom (kb. 1760–1830)
Ez az első ipari forradalom Nagy-Britanniában kezdődött a 18. század második felében, és gyorsan terjedt Európa más részeire és Észak-Amerikába. Jellemzői közé tartozik a gépesítés, ami a kézi munkát gépekkel váltotta fel a textiliparban és más területeken. Az első ipari forradalom legfontosabb technológiai fejlesztései közé tartozik a gőzgép, amely lehetővé tette a gépek hajtását és a gőzhajók, valamint a vasúti közlekedés fejlődését. Ezen kívül a szén és a vas használata is megnövekedett, ami új gyártási technikákhoz és az infrastruktúra bővüléséhez vezetett.

A 2. ipari forradalom (kb. 1870–1914)
A második ipari forradalmat gyakran nevezik technológiai forradalomnak is, mert ebben az időszakban a villamos energia, a belső égésű motor és az acélgyártás új eljárásainak köszönhetően tovább gyorsult a gyártás és az iparosítás. Ebben az időszakban jöttek létre az első nagyüzemi gyárak, és terjedt el a tömegtermelés, mint például a Ford T-modelljének összeszerelő sora. A kommunikáció és a közlekedés modernizálása, mint például a telefon és az autó, szintén jelentős változásokat hozott.

A 3. ipari forradalom (XX. század második fele)
A harmadik ipari forradalom, vagy digitális forradalom az információ-technológia és az automatizálás fejlődésével jellemezhető. A tranzisztor 1947-es kifejlesztése után az elektronikus eszközök, mint az integrált áramkörök és később a személyi számítógépek megjelenése, valamint az Internet terjedése forradalmasította a gyártást, a szolgáltatásokat és az élet számos területét. Ez az időszak magában foglalta a robotika, az informatika és a telekommunikáció fejlesztését, amelyek lehetővé tették a gyártási folyamatok nagymértékű automatizálását és hatékonyságának növelését.

A 4. ipari forradalom (XXI. század eleje–jelen)
A negyedik ipari forradalom vagy Ipar 4.0, a korábbi digitális technológiák továbbfejlesztését és integrálását jelenti a kiber-fizikai rendszerek területén. Az intelligens gyárakban az IoT (Internet of Things, azaz a dolgok internete), a mesterséges intelligencia, a nagy adatmennyiségek elemzése, a felhőalapú technológiák és a továbbfejlesztett automatizálás ötvöződik. Ezek a technológiák lehetővé teszik a gyártási folyamatok, logisztika és termékek széles körű monitorozását, irányítását és optimalizálását valós időben. **...és a fejlődés rohamléptekkel folytatódik, előnyei mellett újabb és újabb veszélyeket hordozva.**

Szükséges képességek

A kiberbiztonságban szükséges technikai készségek változatosak és folyamatosan fejlődnek. A kulcsfontosságú területek ismeretének szükséges mélysége a szakterülettől függ. Az alapismeretekre jó példák a következők:

Hálózatbiztonság: Az alapvető hálózati infrastruktúra, beleértve a routereket, tűzfalakat és szervereket, megértése létfontosságú.

Alkalmazásbiztonság: A szoftverfejlesztési készségek és az alkalmazások felépítésének és védelmének megértése kulcsfontosságú.

Biztonsági folyamatok ismerete: Az adatok bizalmasságának sértetlenségének (integritásának) és rendelkezésre állásának védelméhez szükséges irányelvek, folyamatok és kontrollok (intézkedések) ismerete.

Kriptográfia: Az adatok titkosításának és visszafejtésének ismerete. stb.

A technikai készségeken túl, a kritikus gondolkodás, problémamegoldás és hatékony kommunikáció – hívjuk ezeket a divatos szóval „soft skillnek” – egyaránt fontosak. A kiberbiztonsági szakembereknek képesnek kell lenniük arra, hogy a bonyolult biztonsági fogalmakat érthetővé tegyék a nem technikai érdekeltek számára, és ajánlásokat tegyenek nekik, kockázatértékelések alapján.

Analitikus készségek: A kiberbiztonsági szakembereknek képesnek kell lenniük nagy mennyiségű adat elemzésére és olyan minták azonosítására, amelyek potenciális fenyegetéseket jeleznek. Ez éles analitikai készségeket és a védekező és támadó gondolkodásmód egyesítését igényli.

Problémamegoldás: Az azonnali megoldások megtalálása a biztonsági incidensekre és a jövőbeli fenyegetések megelőzésére elengedhetetlen. A problémamegoldó készségek magukban foglalják a kreativitást és a logikát, amelyek kulcsfontosságúak a biztonsági stratégiák és válaszok kidolgozásában.

Részletekre való odafigyelés: A kiberbiztonság nagymértékben függ az aprólékos figyelemtől. Az apró figyelmetlenségek sebezhetőségekhez és adatszivárgásokhoz vezethetnek, így a jó értelemben vett “pedánsság” kulcsfontosságú tulajdonság a területen való sikeres munkavégzéshez.

Kommunikációs készségek: Mivel a kiberbiztonság az egész szervezetet érinti, a szakembereknek képeseknek kell lenniük a kockázatok, stratégiák és technikai információk világos kommunikálására a nem szakértők számára. Ez magában foglalja a jelentések megírását, az eredmények bemutatását és a kollégák tudatosító, vagy akár mélyebb oktatását.

Hogyan indulj el a kiberbiztonsági szakmában?

Mindenki számára létezik hely ezen a színes palettán. Érdeklődés és személyes adottságok nagyban meghatározzák, hogy ki milyen irányban találja meg a számításait. Az a fontos, hogy tudatosan ismerjük fel saját képességeinket és erősségeinket, majd ennek megfelelően alakítsuk ki szakmai pályánkat. Ahogy haladunk előre, folyamatosan értékeljük felül céljainkat és adaptálódjunk a gyorsan változó kiberbiztonsági környezethez. Pályakezdőként vagy a váltást fontolgatóként az alábbi lépéseket javaslom neked. Látni fogod, hogy ezek nem „sorfolytonos" lépések, hanem egymást kiegészítő irányok.

Mindazonáltal bízom benne, hogy további kutakodásra sarkallnak!

1. **Soft skill-jeid megismerése és fejlesztése:** Az automatizálás növekedésével egyre fontosabbá válnak az olyan készségek, mint a kreativitás, az empátia és a „személyközi" kommunikáció - és persze ne feledkezzünk meg az angolnak, mint a szakma anyanyelvének megtanulásáról. A további tippek ehhez is segítségedre lesznek!
2. **Ismerd meg önmagad!** Kezdd azzal, hogy alaposan megismered, mi is mozgat téged igazán (lásd a keretes "Ikigai" írást, és ajánlom neked Simon Sinek "Kezdj a Miérttel!" c. könyvét), és ebből adódóan mely kiberbiztonsági területek vonzanak a leginkább – akár a technikai problémamegoldás, a kockázatkezelés, hekkelés vagy irányítás érdekel.
3. **Fedezd fel a kiberbiztonsági szakmát:** A kiberbiztonság számos szerepet foglal magában, a technikai pozícióktól a stratégiai szerepekig. Tájékozódj a különböző lehetőségekről, akár álláshirdetésekből, és gyúrj rá arra, ami hiányzik!
4. **(Ön)Képzés:** Kicsengettek! Már nem fog senki a nyakadon ülni, hogy tanulj! Aszerint, hogy melyik terület érdekel, jelentkezz a releváns oktatási programokra. Kezdd olyan képzéssel, ami szilárd alapokat biztosít az informatikai készségek és a kiberbiztonsági elvek terén. A továbbiakban pedig keresd a nemzetközi minősítéseket!
5. **Specializálódj!** Első körben, bár az átfogó tudás alapvetően szükséges, érdemes specializálódni a fentebb említett területek valamelyikére, mert abban elmélyülve fogod igazán megtapasztalni a valóságot, és dönthetsz további fejlődésed irányáról.
6. **Szerezz gyakorlati tapasztalatot.** Egy valamirevaló képzés nem csak az elméletet adja át. Emellett viszont saját „projekteket" is végezhetsz, legyen az a saját otthoni hálózatod biztonságossá tétele, vagy a saját géped biztonságos beállítása. Ezek mellett részt vehetsz csoportos projektekben, vagy akár gyakornoki, részmunkaidős vagy önkéntes munka keretén belül is szerezhetsz gyakorlati tapasztalatot! Ezek tapasztalat mellett , jövőbeli munkáltatód felé is jelzik, hogy komolyan gondolod a dolgot!
7. **Folyamatos – élethosszig tartó – tanulás:** A kiberbiztonsági terület gyorsan fejlődik, ezért nagyon fontos, hogy naprakész maradj a legújabb technológiák, fenyegetések és szakmai fejlesztések terén. Rendszeresen nézz videókat, olvass blogokat és kiadványokat, kövess a szakmában élenjáró szakértőket, vegyél részt online kurzusokon, webinárokon, szakmai (akár online) közösségekben.

8 **Ismerkedj!** A közösség hatalmas szerepet játszik karrieredben! Hiszem, hogy csak közösség(ek) tagjaként lehetünk sikeresek; a közösség inspirál, támogat és segít. Építs szakmai kapcsolatokat, akár élőben, konferenciákon, vagy online közösségekben (LinkedIn, Discord...). Keresss a LinkedIn-en számodra érdekes területeken szakértőket, jelöld be őket, mutatkozz be nekik, és nyugodtan kérj tanácsot tőlük - nem fogsz csalódni! A "hálózatépítés" (angolul: networking), nem csak az informatikai hálózatokra vonatkozik! A közösségek és a területen dolgozó más szakemberekkel való kapcsolatépítés új lehetőségeket, ismeretszerzési, tapasztalatcsere és mentorálási lehetőségeket, kapcsolatokat nyitnak meg előtted!

9 **Keress mentor(oka)t:** Bár a szakmában előfordul némi „elitizmus" és misztifikáció, nem ez a jellemző! A kiberbiztonsági szakértők és közösségek tipikusan nagyon befogadóak és támogatóak – hiszen felismerik, hogy mindenki kezdte valahogy! Találj egy vagy több tapasztalt szakembert, aki már jól ismeri az általad választott területet (lásd 8. pont). Egy mentor nagy segítség lehet abban, hogy sikeresen navigálj karrieredben.

10 **Építs személyes „márkát".** Ez idegenül hangozhat, hiszen nem vagy te porszívóügynök, miért kéne eladnod magad? A helyzet az, hogy a kiberbiztonság – éppen az eddig sorolt előnyök miatt – erősen kompetitív terület. Saját magad, személyes „küldetésed", mozgatórugód és különösen „hozzáadott értéked" meghatározása egy személyes „brand" kialakítása segít kitűnni! Önkénteskedés, előadások tartása (akár családban, akár iskolákban való biztonsági tudatosítás, például a telefonos vagy közösségi platformokon történő csalások elkerülésével kapcsolatban), saját blog vagy LinkedIn profilod és jelenléted aktív fenntartása, cikkekkel, aktív interakcióval – csak pár lehetőség arra, hogy szinte a legelejétől kezdve „legyél valaki". Ez persze nem ennyire triviális, de például **saját fejlődéseddel kapcsolatos tapasztalataid megosztása online, közösségben, vagy személyesen, egy nagyon jó és (másokat is) motiváló indítás lehet.**

11 **A munka és a magánélet harmóniája.** Nem véletlenül nem „egyensúlyt" írtam, hiszen, ha a munkánk a hobbink és a hivatásunk, akkor előfordul, hogy nehezen döntjük el, hogy most dolgozunk, vagy töltődünk – hiszen a munka tölt minket. Mindamellett a kiberbiztonság könnyen beszippant, ezért fontos, hogy fenntarts egy egészséges egyensúlyt a munka és a személyes életed között. Szánj időt a kikapcsolódásra, hobbidra és a szeretteiddel való együttlétre.

12 **Keress álláshirdetéseket, és jelentkezz!** Ne hagyj ki egy fontos lépést: találd meg azokat a pozíciókat, amik érdekelnek, készüljl fel rájuk és és jelentkezz - ha más nem, gyakorlásként! Titkos tipp: sok álláshirdetés túlzóan sorolja az elvárásokat, hovatovább "kívánságlistaként". Ne ijedj meg egy-egy követelménytől, amit nem teljesítesz, add be CV-det és add meg a lehetőséget a toborzóknak, hogy eldöntsék, akarnak-e veled beszélni! Ne dönts helyettük! Kellemes meglepetésben lehet részed!

13 **Keresd a kudarcot és sose add fel!** Igen, nem elírás; sokszor tart vissza minket a kudarctól való tudatos vagy tudatalatti félelem. „Mi lesz, ha nem sikerül?" Állj hozzá fordítva! Edison például azt mondta az általa szabadalmaztatott tartós villanykörte kidolgozása után, szabad fordításban: „Nem 1000 kudarcom volt, hanem sikeresen felfedeztem 1000 módot, ami nem működik". Minden nagy siker mögött ott van rengeteg erőfeszítés és munka, ami nem látszik. A külvilágtól érkező visszajelzés az egyetlen érvényes információ arról, hogy jó-e, amit csinálsz, tehát minél hamarabb kapod azt meg, annál hamarabb tudsz változtatni! A „saját mozidat nézve" biztosan nem fogod kitalálni a tutit – inkább túl fogod gondolni a dolgot! Sőt, bár kissé cinikusan hangzik, de megkockáztatom: igazából senkit nem érdekel, mit csinálsz, sem akkor ha sikeres vagy, sem akkor, amikor éppen felfedezel egy opciót, ami nem működik. Szóval nincs mitől félni, ha valamit meg akarsz tanulni, sőt, előbb legyél benne kirívóan és komikusan csapnivaló! Aztán majd fejlődsz. Ezeket a lépéseket követve nemcsak, hogy megtalálhatod a helyed a kiberbiztonság világában, de egy olyan karriert is építhetsz, ami személyes motivációidra és a piaci igényekre egyaránt épül. Az Ikigai filozófiája segít abban, hogy ne csak munkát végezz, hanem valódi hivatásra találj, mert ennek a japán tanításnak pont az a lényege, hogy olyan tevékenységet vagy célt találjunk magunknak, amiért minden nap érdemes felkelni és minden nap szenvedéllyel tölt el minket.

Turbózd fel karrieredet a kiberbiztonságban!

- Csatlakozz Discord közösségünkhöz
- Kövess minket közösségi csatornáinkon
- Kérdezz, segítünk, hiszen ez a küldetésünk
- Ha komolyan fejlődnél, jelentkezz képzéseinkre

Üdv, és hajrá!

A CyberCamp csapata

https://cybercamp.hu

https://discord.gg/kFsnZJWg2b

@cybercamphu

@CyberCamp-hu

cybercamp2022

cybercamp2022

FORTIX Consulting