06125001 számú Információbiztonsági rendszerüzemeltető megnevezésű szakképesítés megszerzésére irányuló szakmai képzéseket megalapozó programkövetelmény

1. A programkövetelmény, illetve az ennek alapján szervezhető szakmai képzés

1.1 Megnevezése: Információbiztonsági rendszerüzemeltető

1.2 Ágazat megnevezése: Informatika és távközlés

1.3 Besorolása a képzési területek egységes osztályozási rendszere (KEOR) szerinti kód alapján: 0612 Adatbázisok, hálózattervezés és adminisztráció

2. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítés

2.1 Megnevezése: Információbiztonsági rendszerüzemeltető

2.2 Szintjének besorolása

2.2.1 Az Európai Képesítési Keretrendszer (EKKR) szerint: 5

2.2.2 A Magyar Képesítési Keretrendszer (MKKR) szerint: 5

2.2.3 A Digitális Kompetencia Keretrendszer szerint: 8

3. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítés és az azzal betölthető munkakör vagy végezhető tevékenység kapcsolata, összefüggése[1]:

3.1 A szakmai képzéshez kapcsolódóan megszerezhető szakképesítéshez szükséges kompetenciákkal szakmajegyzékben szereplő szakma körébe vonható munkaterület, tevékenység vagy munkakör magasabb szinten gyakorolható, vagy a szakmai képzés szakmajegyzékben szereplő szakma képzési és kimeneti követelményeiben meg nem határozott speciális szakmai ismeretek és szakmai készségek megszerzésére irányul.

3.2 A szakmai képzéshez kapcsolódóan megszerezhető szakképesítés jogszabályban meghatározott képesítési követelmény munkakör betöltéséhez vagy tevékenység folytatásához.

A képesítési követelményt előíró jogszabály:

4. A programkövetelmény alapján szervezhető szakmai képzéshez kapcsolódóan megszerezhető szakképesítéssel ellátható legjellemzőbb munkaterület, tevékenység vagy munkakör leírása:

A megszerezhető szakképesítés birtokában el tudja látni a kis, közép vagy nagyvállalatoknál alkalmazott biztonsági rendszerek telepítési, konfigurálási, napi üzemeltetési feladatait. A

[1] A megfelelő elem kiválasztandó.

képzés során gyakorlati ismereteket szerez az informatikai infrastruktúra biztonságos működését támogató eljárásokról, alkalmazásokról. Képessé válik a jogszabályi elvárásoknak megfelelő és az iparági jó gyakorlatokon alapuló megoldásokat tervezni, kialakítani, üzemeltetni.
Tisztában van az információbiztonság alapelveivel, alapfogalmaival eljárásaival. Napi munkavégzése során biztonságtudatos gondolkodásmód jellemzi.
Munkája során jelentkező problémákat önállóan oldja meg. Az új technológiák alkalmazására nyitott, tudását folyamatosan fejleszti. Szakmai témákban hatékonyan kommunikál magyarul és angolul egyaránt.

5. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítéshez szükséges képzési tartalom szabadalmi vagy szerzői jogi oltalom alatti állása:

5.1 Szabadalmi vagy szerzői jogi oltalom alatt áll:

5.1.1 Az oltalom típusának megjelölése:

5.1.2 Nyilvántartó hatóság:

5.1.3 Azonosító vagy nyilvántartásba vételi száma:

6. A programkövetelmény alapján szervezhető szakmai képzés megkezdéséhez szükséges bemeneti feltételek:

6.1 Iskolai előképzettség[2]:

- érettségi végzettség

6.2 Szakmai előképzettség: -

6.3 Egészségügyi alkalmassági követelmény: -

6.4 Szakmai gyakorlat területe és időtartama: -

6.5 Egyéb feltételek:

A képzésben résztvevőnek az alábbi tudással és gyakorlati készségekkel kell rendelkeznie a képzés kezdetekor:

- magas szintű tudással rendelkezik a hálózati ismeretek terén
    - a forgalomirányítási alapismeretekkel rendelkezik
    - jártas a hálózati eszközök alapszintű konfigurációjában
    - ismeri a statikus forgalomirányítást
    - ismeri a VLAN-ok használatát és azok közötti forgalomirányítást
    - ismeri a IPv4-es és IPv6-os címzést
    - tisztában van a hálózatbiztonság alapfogalmaival
    - ismeri a vezeték nélküli technológiákat
    - tisztában van a dinamikus forgalomirányítás működésével
    - ismeri a statikus és dinamikus címkiosztást és a címfordítás lehetőségeit

[2] A megfelelő elem kiválasztandó.

- ismeri a VPN fogalmát, szerepét

- a hálózati operációs rendszerekkel kapcsolatban magabiztos tudással rendelkezik
  - ismeri a virtualizációt és a konténerek hálózatkezelését
  - telepítési gyakorlattal rendelkezik szolgáltatások tekintetében szerver környezetben
  - különböző szerverek üzemeltetésében jártas
  - ismeri a Linux és Windows operációs rendszerek működését

A fenti tudás és készségek ellenőrzése előzetes tudásfelméréssel történik, mely során a résztvevőnek az alábbi feladatot kell megoldania:

1. Teszt kitöltése részterületenként a meglévő tudásszintjének felmérésére.

2. Egy gyakorlati feladatot kell elkészítenie, melyben előfordulhatnak a következő témakörök:

   - Csatlakozás a hálózathoz, a kapcsoló alapkonfigurációja
   - Vezetékes és vezeték nélküli kapcsolódás helyi hálózathoz
   - Forgalomirányítási alapok, adatfolyam kezelés
   - IP címzés a gyakorlatban
   - Szerver-kliens kapcsolódás, hálózatbiztonság
   - Kapcsolás folyamata és a VLAN-ok használata
   - Statikus és dinamikus forgalomirányítás
   - A biztonságos hálózat kialakítása, forgalomszűrés
   - IP szolgáltatások a gyakorlatban
   - Operációs rendszer telepítése, frissítése
   - Szoftvercsomag hitelességének (aláírásának, annak érvényességének) ellenőrzése
   - SQL lekérdezés készítése

Az előzetes tudásmérés alól mentesül, aki a (5 0612 12 02) Informatikai rendszer- és alkalmazás-üzemeltető technikus végzettséggel rendelkezik.

7. A programkövetelmény alapján szervezhető szakmai képzés elvégzéséhez szükséges foglalkozások minimális és maximális óraszáma (Amennyiben a programkövetelmény modulszerű felépítésű, a minimális óraszám a <u>modulonként</u> meghatározott minimális, a maximális óraszám a modulonként meghatározott maximális óraszámok összege):

7.1 Minimális óraszám: 400

7.2 Maximális óraszám: 550

8. A szakmai követelmények leírása:

1. 9.1 Modulszerű felépítés esetén[3]

8.1.1 Programkövetelmény-modul neve: Általános információbiztonsági alapok

8.1.1.1 Programkövetelmény-modul sorszáma: 1.

8.1.1.2 Programkövetelmény-modul tanulási eredményeinek elsajátításához szükséges foglalkozások minimális és maximális óraszáma:

8.1.1.2.1 Minimális óraszám: 72
8.1.1.2.2 Maximális óraszám: 108

Készségek, képességek	**Ismeretek**	**Elvárt viselkedésmódok, attitűdök**	**Önállóság és felelősség mértéke**
Készség szinten használja az információbiztonság alapfogalmait. Képes az egyes információbiztonsági elvárásokat visszavezetni az alapfogalmakra.	Ismeri a biztonság általános informatikai és információbiztonsági definícióját, az információbiztonság három alappillérét.	Az egyes szituációkban képes felismerni, hogy a biztonság melyik alappillére sérül. Meg tudja határozni, hogy az adott intézkedés melyik alappillérre lesz hatással.	Felméri a tevékenységéből adódó kockázatokat, felelősséggel végzi a munkáját.
Eligazodik az információbiztonság jogszabályi környezetében, kapcsolódó szabványokban.	Ismeri az információbiztonságra vonatkozó hazai és nemzetközi jogszabályokat, szabványokat.	Képes különbséget tenni a jogszabályok és szabványok között. Figyelmet fordít rá, hogy tisztában legyen a releváns jogszabályok főbb tartalmi elemeivel.	Önállóan képes jogszabályi hivatkozásokat kezelni.
Ismeri a biztonságot támogató dokumentációk követelményeit, ezek tartalmi és formai elvárásait.	Ismeri a jogszabályok által elvárt információbiztonsági dokumentumokat,	Fontosnak tartja, hogy betartsa a dokumentációs elvárásokat napi munkavégzése során.	A rendelkezésére bocsátott sablon alapján képes azt releváns információkkal feltölteni.

[3] Legalább két modul esetén modulonként szükséges meghatározni a tanulási eredményeket! A sablont a modulok számának függvényében további táblázatokkal ki lehet egészíteni a modulra vonatkozó információk megjelenítésével.

	ezek főbb tartalmi elemeit.		
Átlátja az információbiztonság főbb területeit.	Tisztában van az információbiztonsági irányítási rendszer működésével, főbb elemeivel és ezek szerepeivel	Törekszik arra, hogy az információbiztonság minden területéről rendelkezzen átfogó ismeretekkel.	Önállóan képes az egyes területekhez kontrollokat megfogalmazni.
Elvégzi a sérülékenységvizsgálat eredményének kiértékelését.	Átfogó ismeretekkel rendelkezik a sérülékenység vizsgáló eszközök működéséről. Tisztában van a sérülékenységet feltáró manuális és automata megoldások különbségével. Ismeri a leggyakoribb sérülékenység fajtákat és az ezekre adott válaszokat.	Magabiztosan értelmezi a sérülékenység vizsgálatok eredményét.	Önállóan azonosítja az illetékességi területéhez tartozó rendszer/alkalmazás tekintetében a legsúlyosabb sérülékenységet.
Képes önállóan elvégezni egy kisebb szervezet vagy egy komplex informatikai rendszer kockázatelemzését.	Ismeri a fenyegetések, sérülékenységek leggyakoribb fajtáit, és tisztában van a kockázatkezelési eljárások típusaival. Ismeri a kockázati étvágy fogalmát és a kockázatok kezelésének módjait.	Törekszik arra, hogy egyes kockázatokra alternatív intézkedéseket is meg tudjon fogalmazni.	A lehetséges fenyegetések felmérése során képes megfelelő kockázatcsökkentő intézkedéseket javasolni.
Tisztában van a jogosultságkezelési rendszer szerepével, a kialakításkor	Ismeri a jogosultsági rendszert, a hozzáférés azonosítás szerepét. Tisztában van a jogosultságkialakítás	Igyekszik az adott felhasználási területnek leginkább megfelelő jogosultsági rendszert kialakítani	Önállóan képes az összeférhetetlen szerepkörök felismerésére. Tisztában van a helytelen

alkalmazandó alapelvekkel.	alapelveivel, az elemi jogosultságok és szerepkörök fogalmával.	a biztonsági alapelvek maximális szem előtt tartása mellett.	jogosultsági rendszerből adódó kockázatokkal.
Képes a megfelelő hitelesítő eszköz kiválasztására.	Ismeri a hitelesítés szerepét, a hitelesítő eszközök típusait, főbb jellemzőit. Tisztában van a többtényezős hitelesítés szerepével. Ismeri az elavult hitelesítési eszközök jelentette veszélyeket.	Törekszik az adott alkalmazás/szolgáltatás/rendszer számára az ideális hitelesítési mód megtalálására. Nyitott a többtényezős hitelesítés alkalmazására.	Felelősségi körébe tartozó információs rendszerben képes biztonságos jelszó házirend kialakítására.

8.1.2 Programkövetelmény-modul neve: IT üzemeltetői ismeretek

8.1.2.1 Programkövetelmény-modul sorszáma: 2.

8.1.2.2 Programkövetelmény-modul tanulási eredményeinek elsajátításához szükséges foglalkozások minimális és maximális óraszáma:

8.1.2.2.1 Minimális óraszám: 328
8.1.2.2.2 Maximális óraszám: 442

Készségek, képességek	**Ismeretek**	**Elvárt viselkedésmódok, attitűdök**	**Önállóság és felelősség mértéke**
Képes a biztonságos hálózati kapcsolatok kiépítésére, konfigurálására.	Ismeri a VPN működési módját, biztonsági beállításait.	Törekszik arra, hogy a felelősségi körébe tartozó hálózati eszközök biztonságosan legyenek konfigurálva.	Önállóan kiválasztja és konfigurálja az adott hálózati kapcsolathoz tartozó biztonsági beállításokat.
Képes az általa üzemeltetett rendszer hitelesítési eszközök biztonságos konfigurálását elvégezni. Képes	Ismeri a hitelesítő eszközök típusait, főbb jellemzőit. Tisztában van az egyes hitelesítési módokhoz tartozó	Fontosnak tartja a többfaktoros autentikáció bevezetését, törekszik annak beállítására az általa	Autonóm módon azonosítja az elavult hitelesítési megoldásokat.

ellátni egy rendszer jogosultságkezelési (beállítás, visszavonás) folyamatát.	biztonságos, illetve elavult, sérülékeny megoldásokkal. Ismeri a központi azonosítás és a helyi azonosítás előnyeit, hátrányait.	üzemeltetett rendszerekben.	Önállóan ellátja a hatáskörébe tartozó rendszerekre vonatkozó jogosultságigényekhez kapcsolódó üzemeltetési feladatokat.
Képes hatékony monitorozó rendszert kiépíteni, üzemeltetni.	Tisztában van a monitorozás szerepével. Ismeri a legelterjedtebb felügyeleti eszközöket.	Törekszik rá, hogy a releváns paramétereket monitorozza, illetve minden hatáskörébe tartozó eszközt bevonjon a monitorozásba.	Önállóan képes riasztási szinteket meghatározni.
Képes az adatbázisok biztonságos üzemeltetéséhez kapcsolódó feladatok ellátására.	Tisztában van az adatok átvitele és tárolása során alkalmazott kriptográfiai módszerekkel, ezek szerepével. Ismeri az adatbázisok mentésére, helyreállítására vonatkozó iparági jógyakorlatokat.	Tudatosan ellenőrzi a mentési eljárás megfelelő működését. Folyamatosan nyomon kíséri az adatbázis rendszer működési paramétereit.	Önállóan felméri az egyes feladatokhoz tartozó jogosultságokat és szerepköröket.
Képes az elektronikus levelezéshez kapcsolódó biztonsági beállítások elvégzésére. Digitális aláírás. Be tud állítani levelező szoftvert, hogy enkriptált levelet küldjön és fogadjon. Észreveszi, ha egy levél aláírása	Ismeri az e-mailek hitelességének ellenőrzéséhez kapcsolódó megoldásokat. Tisztában van az e-mail útján terjedő kártékony kódok jelentette fenyegetéssel.	Folyamatosan ellenőrzi, hangolja a levélszemét szűrő eszköz beállításait a hatékonyabb működés érdekében.	Önállóan képes egy gyanús e-mail fejlécadatainak elemzésére.

hiányos, vagy meghamisították.			
Képes az adott feladat elvégzéséhez szükséges távelérési megoldás kiválasztására, telepítésére, konfigurálására és használatára.	Ismeri a leggyakoribb távoli elérést lehetővé tevő alkalmazásokat. Tisztában van ezek működésével, előnyeivel, hátrányaival.	A távoli elérést lehetővé tévő távoli alkalmazást csak a szükséges ideig működteti. Azt követően letiltja vagy eltávolítja.	Felismeri, ha elavult vagy rosszul konfigurált távoli elérést biztosító alkalmazással van dolga. Önállóan javaslatot fogalmaz meg a kockázat csökkentésére.
Képes biztonságos konténerizációs környezet kialakítására és fenntartására.	Rendelkezik a szükséges ismeretekkel a konténerizációs környezet biztonságos beállításához. Ismeri a konténereknél alkalmazott sérülékenységvizsgáló eszközök működését.	Elvégzi a konténerek sérülékenységvizsgálatát és javaslatot fogalmaz meg a talált sérülékenységek javítására.	Önállóan futtatja a sérülékenységvizsgáló eszközöket. Priorizálja a feltárt sérülékenységeket.
Használja a projekt- és csoportmunka-támogató eszközöket.	Ismeri a legelterjedtebb projekt- és csoportmunka-támogató eszközöket.	Igyekszik munkatársaival hatékonyan, igazi csapatjátékosként együtt dolgozni. Törekszik a csoporton belül megkapott feladatok precíz, határidőre történő elkészítésére, társai segítésére és az elvégzett munka dokumentálására.	A projektben irányítás alatt dolgozik, a rábízott részfeladatok megvalósításáért felelősséget vállal.
Képes a hálózati szegmentáció megvalósítására, VLAN, tagged	Tisztában van a hálózati szegmentáció és a biztonsági zónák szerepével. Ismeri az	A hatáskörébe tartozó eszközök tekintetében törekszik a hálózati	Önállóan meghatározza az adott eszköz funkciója alapján az elhelyezésére ideális

VLAN, dinamikus VLAN beállítására.	ezek kialakítására, fenntartására vonatkozó alapelveket, eljárásrendeket.	szegmentáció megvalósítására.	hálózati biztonsági zónát.
Képes a felügyeleti rendszerből érkező riasztások értelmezésére, kezelésére.	Ismeri a leggyakoribb rendszer-monitorozó eszközöket, azok működését, használatát.	Folyamatosan nyomon követi a felügyeleti rendszerből érkező riasztásokat.	Javaslatot tesz a monitorozási paraméterek finomhangolására.
Képes biztonságos vezetéknélküli hálózat kialakítására, konfigurálására.	Ismeri a vezetéknélküli autentikációs szabványokat. Tisztában van a WIFI kontrollerek működésével, szerepével.	Vezetéknélküli hálózat tervezése, konfigurálása során szem előtt tartja a biztonsági beállításokat.	Önállóan felismeri a nem biztonságos vezetéknélküli hálózati beállításokat. Képes javaslatot megfogalmazni a feltárt hibák javítására.
Biztonságos kriptográfiai megoldásokat alkalmaz.	Ismeri a biztonságos és nem biztonságos kriptográfiai módszereket, algoritmusokat. Tisztában van ezek szerepével a rendszerek üzemeltetése, biztonsági funkcióinak megvalósítása tekintetében.	Kerüli a nem biztonságos kriptográfiai megoldások használatát.	Naprakészen tartja tudását a kriptográfiai megoldásokat érintő sérülékenységekkel kapcsolatban. Dokumentáció alapján képes hardening feladatokat végrehajtani.
Képes telepíteni, konfigurálni tűzfal-funkcionalitást biztosító megoldást	Tisztában van a hardver és szoftver alapú tűzfal megoldások előnyeivel, hátrányaival. Ismeri a tűfalakhoz kapcsolódó	Körültekintően határozza meg a szükséges beállításokat. Felméri az egyes konfigurációs	Önállóan elvégzi a tűzfal szabályok rendszeres felülvizsgálatát, javaslatokat fogalmaz meg a

	alapfogalmakat főbb konfigurációs beállításokat.	változtatások veszélyeit, hatásait.	szükséges változtatásokról.
Képes a hozzá eljutó igényeket megvizsgálni olyan szempontból, hogy mennyire illeszkednek a biztonsági architektúrához.	Tisztában van az egyes jelentősebb IT szervezeti szerepkörökkel, ezek főbb feladataival. Ismeri a biztonsági architektúra főbb részeit.	Törekszik arra, hogy az általa kezelt eszközök illeszkedjenek a biztonsági architektúrához.	Önállóan felismeri ha egy probléma megoldása más IT szerepkör bevonását igényli.

8.2 A szakmai képzés megszervezhető kizárólag távoktatásban: igen/nem[4]

9. A programkövetelmény alapján szervezhető szakmai képzéssel megszerezhető szakképesítés társadalmi-gazdasági hasznosíthatóságának bemutatása (munkaerő-piaci relevanciája):

A munkaerőpiacon tapasztalható jelentős IT – azon belül is különös tekintettel az információbiztonsági területen tapasztalható - szakemberhiány enyhítésében fontos szerepe van jelen képzésnek. A tanfolyam elvégzésével a résztvevők mélyreható tudásra tehetnek szert a hálózat-, szerver- és alkalmazásüzemeltetés területén. Elméleti és gyakorlati ismeretekre tesznek szert az informatikai eszközök biztonságos üzemeltetése, biztonságtámogató funkcióinak használata, illetve a biztonságot megvalósító eszközök üzemeltetése terén. Az elsajátított ismeretek révén képessé válnak a kis, közepes- vagy nagyvállalati informatikai rendszerek biztonságtudatos üzemeltetésére, a biztonsági rendszerek hatékony konfigurálására, kezelésére, ami jelentősen csökkentheti az adott szervezet kiberbiztonsági kitettségét.

10. A képesítő vizsga megszervezéséhez szükséges feltételek és a képesítő vizsga vizsgatevékenységeinek részletes leírása:

10.1 A képesítő vizsgára bocsátás feltétele:

A szakmai képzés követelményeinek igazolásáról a képző intézmény által kiállított tanúsítvány.

Egyéb feltételek:

10.2 Írásbeli vizsga

10.2.1 A vizsgatevékenység megnevezése: Általános információbiztonsági alapok

10.2.2 A vizsgatevékenység, vagy részeinek leírása:

[4] A megfelelő válasz aláhúzandó.

Az írásbeli vizsga kérdéseit a következők szerint kell összeállítani:

- Kérdések: 20 db feleletválasztós tesztkérdés
-
- A feleletválasztásos tesztkérdéseket úgy kell kialakítani, hogy egyetlen helyes válaszlehetőség legyen lehetséges.
- A teszt témaköreit és az egyes témakörökhöz tartozó kérdésszámot az alábbi táblázat tartalmazza:

Témakör	**Kérdések száma**
Információbiztonsági alapfogalmak	3
Információbiztonsági jogszabályok, szabványok	3
Információbiztonsági dokumentációk	1
Információbiztonsági irányítási rendszer elemei, főbb feladatai	2
Sérülékenység-vizsgálat fogalma, szerepe, fajtái, értelmezése	3
Kockázatelemzés, kockázatkezelés	3
Jogosultságkezelés fogalma, szerepe	2
Hitelesítés folyamata, hitelesítőeszközök használata, többtényezős hitelesítés, jelszó házirend szerepe, elemei	3
Összesen:	**20**

10.2.3 A vizsgatevékenység végrehajtására rendelkezésre álló időtartam: 30 perc

10.2.4 A vizsgatevékenység aránya a teljes képesítő vizsgán belül: 20 %

10.2.5 A vizsgatevékenység értékelésének szempontjai:

A) Az írásbeli vizsgát a következők szerint kell értékelni:

- Maximálisan elérhető pontszám/százalék: 40 pont / 100%
- 20 db tesztkérdés IT üzemeltetői ismeretekből (20*2 pont) 100%

B) Egyéb értékelési szempontok az írásbeli vizsgaértékeléssel kapcsolatban:

- A helyes válasz 2 pontot ér, a helytelen válasz 0 pontot ér.
- A rossz válasz megjelölésért pontlevonás nem jár.

10.2.6 A vizsgatevékenység akkor eredményes, ha a vizsgázó a megszerezhető összes pontszám legalább 51%-át elérte. Törtpontszámos eredmény esetén a kerekítés szabályait szükséges alkalmazni.

10.3 Projektfeladat

10.3.1 A vizsgatevékenység megnevezése: Információbiztonsági üzemeltető projektfeladat

10.3.2 A vizsgatevékenység, vagy részeinek leírása:

A) Információbiztonsági üzemeltető vizsgaremek elkészítése és bemutatása

A vizsgázóknak minimum 2, maximum 3 fős csapatot alkotva kell a vizsgát megelőzően egy komplex informatikai rendszerfejlesztési projektet megvalósítaniuk. A projekt egy valós vagy képzelt vállalat hálózatának tervezését, a hálózat egy működő prototípusának gyakorlati kivitelezését, valamint a prototípus működésének tesztelését foglalja magában konténerizálva.

Az elkészítendő projektnek az alábbi elvárásoknak kell megfelelni:

Életszerű, valódi problémára nyújt megoldást.

- A hálózati infrastruktúrának legalább 3 telephelyet vagy irodát kell lefednie.
- Legalább egy telephelyen több VLAN kialakítását foglalja magában.
- Vezeték nélküli hálózatot is tartalmaz.
- Statikus és dinamikus forgalomirányítást egyaránt megvalósít.
- Statikus és dinamikus címfordítást alkalmaz.
- WAN-összeköttetéseket is alkalmaz.
- Biztonságos távelérési megoldást tartalmaz a távmunka támogatására.
- Programozott hálózat-konfigurációt használ.
- Forgalomirányítón megvalósított biztonsági funkciókat tartalmaz.
- Határvédelmi tűzfalat alkalmaz.
- Minimum 1-1 Linux vagy Windows kiszolgálót tartalmaz, amelyek legalább az alábbi szolgáltatásokat nyújtják:
    - Címtár
    - DHCP
    - DNS
    - HTTP/HTTPS
    - Fájl- és nyomtató megosztás
    - Automatizált mentés távoli telephelyre (a hozzá kapcsolódó, legkisebb szükséges jogosultság elve alapján kialakított tűzfal szabályokkal együtt)
    - Kliens számítógépekre automatizált szoftvertelepítés és frissítés
- Elkészíti és alkalmazza a felhasznált eszközökhöz a security baseline-t
- Tartalmaz egy eljárásrendet a hiteles telepítési könyvtárba (DSL) kerülő szoftverek ellenőrzési szempontjait, feladatait, felelősségi köreit (RACI mátrix) illetően.

A vizsgaremek benyújtásának módja:

A projekt teljes anyagát elektronikus formában a vizsga előtt minimum 14 nappal kell a vizsgaközponthoz benyújtani Git vagy más hasonló projekt-/csoportmunka támogató eszközön megosztva. A benyújtott anyagnak tartalmaznia kell az alábbiakat:

- A hálózat tervezését, működésének leírását tartalmazó dokumentáció. A hálózati topológia ábrán tüntesse fel az alkalmazott hálózatbiztonsági eszközöket is.
- A hálózat tesztelésének dokumentációja
- Kiszolgálókra vonatkozó telepítési és üzemeltetési leírások
- Hardening guide/security baseline

A vizsgafeladat során a vizsgázó gyakorlati bemutatóval összekapcsolt szóbeli előadás formájában mutatja be a

- a hálózat tervezését, a tervezés során használt biztonsági alapelveket
- műszaki megvalósítását
- működésének bemutatását
- az alkalmazott kiszolgáló eszközökön megvalósított biztonsági beállításokat
- az alkalmazott projektszervezési eszközökön mutassák be a csapaton belüli munkamegosztást, az egyes csapattagok által végzett feladatokat, időráfordításokat, a projekt fázisait, az egyes fázisok közötti függőségeket.

Nem a vizsgázó szellemi terméke minden olyan – más szerzőtől átvett tartalom – amelynek forrását a vizsgázó nem jelzi egyértelműen.

A vizsgázó által bemutatott anyagot nem az ő szellemi termékének tekintjük, amennyiben az alábbi kritériumok közül legalább 2 teljesül:

- nem ismeri a bemutatásra kerülő anyag szerkezetét, felépítését
- nem tudja elmagyarázni az egyes modulok/komponensek szerepét
- a bemutatott anyagot korábban már publikálták, egészében vagy részben elérhető az interneten és nem az ő szellemi terméke

A vizsgaremek bemutatására és megvédésére maximum 20 perc áll a vizsgázók rendelkezésére, mely közben biztosítani kell, hogy minden vizsgázó egyenlő arányban vegyen részt a bemutatóban, illetve minden vizsgázónak önállóan kell bemutatnia a saját feladatrészét.

B) Egy kapott szoftver sérülékenység vizsgálatának elvégzése

A vizsgafeladat során a vizsgázónak egy számítógépes szoftver sérülékenység vizsgálatát kell elvégeznie. A vizsgálat során a vizsgázónak fel kell ismernie a sérülékenységi pontokat, meg kell neveznie a sérülékenység lehetséges következményeit, és javaslatot kell tennie a sérülékenység elhárítására.

10.3.3 A vizsgatevékenység végrehajtására rendelkezésre álló időtartam: 30 perc

Ezen belül:

A) Információbiztonsági üzemeltetői vizsgaremek vizsgarész: 20 perc
B) Egy kapott szoftver sérülékenység vizsgálatának elvégzése: 10 perc

10.3.4 A vizsgatevékenység aránya a teljes képesítő vizsgán belül: 80%

10.3.5 A vizsgatevékenység értékelésének szempontjai:

A) Információbiztonsági üzemeltetői vizsgaremek vizsgarész:

- benyújtott dokumentáció mélysége, minősége: 20 pont
- előadásmód, szakmai nyelvezet használata: 10 pont
- a hálózati kialakítás szakmai megfelelősége: 20 pont
- a kiszolgálói környezet szakmai megfelelősége: 20 pont
- alkalmazott biztonsági megoldások: 20 pont
- a bemutatott munka életszerűsége, megvalósíthatósága: 5 pont
- alkalmazott projekt támogató rendszer megfelelő használata: 5 pont.

B) Egy kapott szoftver sérülékenység vizsgálatának elvégzése:

- sérülékenységi pontok vizsgálata, a tényleges sérülékenységek felismerése, megnevezése: 5 pont
- a sérülékenységek lehetséges következményeinek ismertetése: 10 pont
- javaslat a sérülékenység elhárítására: 10 pont

10.3.6 A vizsgatevékenység akkor eredményes, ha a vizsgázó minden vizsgarésznél a megszerezhető pontszám legalább 51%-át elérte. Amennyiben a projektfeladat bemutatása közben kiderül, hogy a projektfeladat nem a vizsgázó szellemi terméke, ahhoz jelentős külső segítséget vett igénybe akkor a vizsgatevékenység kötelezően eredménytelennek tekintendő.

10.4 A vizsgatevékenységek lebonyolításához szükséges személyi feltételek:

A vizsga során 15 vizsgázónként legalább 1 rendszergazdának rendelkezésre kell állnia.

10.5 A vizsgatevékenységek lebonyolításához szükséges tárgyi feltételek:

- Számítógép / laptop
- A vizsgaremek védése során internetkapcsolat

10.6 A vizsgatevékenységek alóli felmentések speciális esetei, módja, és feltételei: -

10.7 A képesítő vizsgán használható segédeszközökre és egyéb dokumentumokra vonatkozó részletes szabályok:

- Papír és toll/ceruza használata megengedett.
- A vizsgaremek védése során a vizsgaközpont által ellenőrzött és jóváhagyott, a technikai feltételeknek megfelelő, saját számítógép használata engedélyezett.

10.8 A vizsgatevékenységek megszervezésére, azok vizsgaidőpontjaira, a vizsgaidőszakokra vonatkozó sajátos feltételek: -