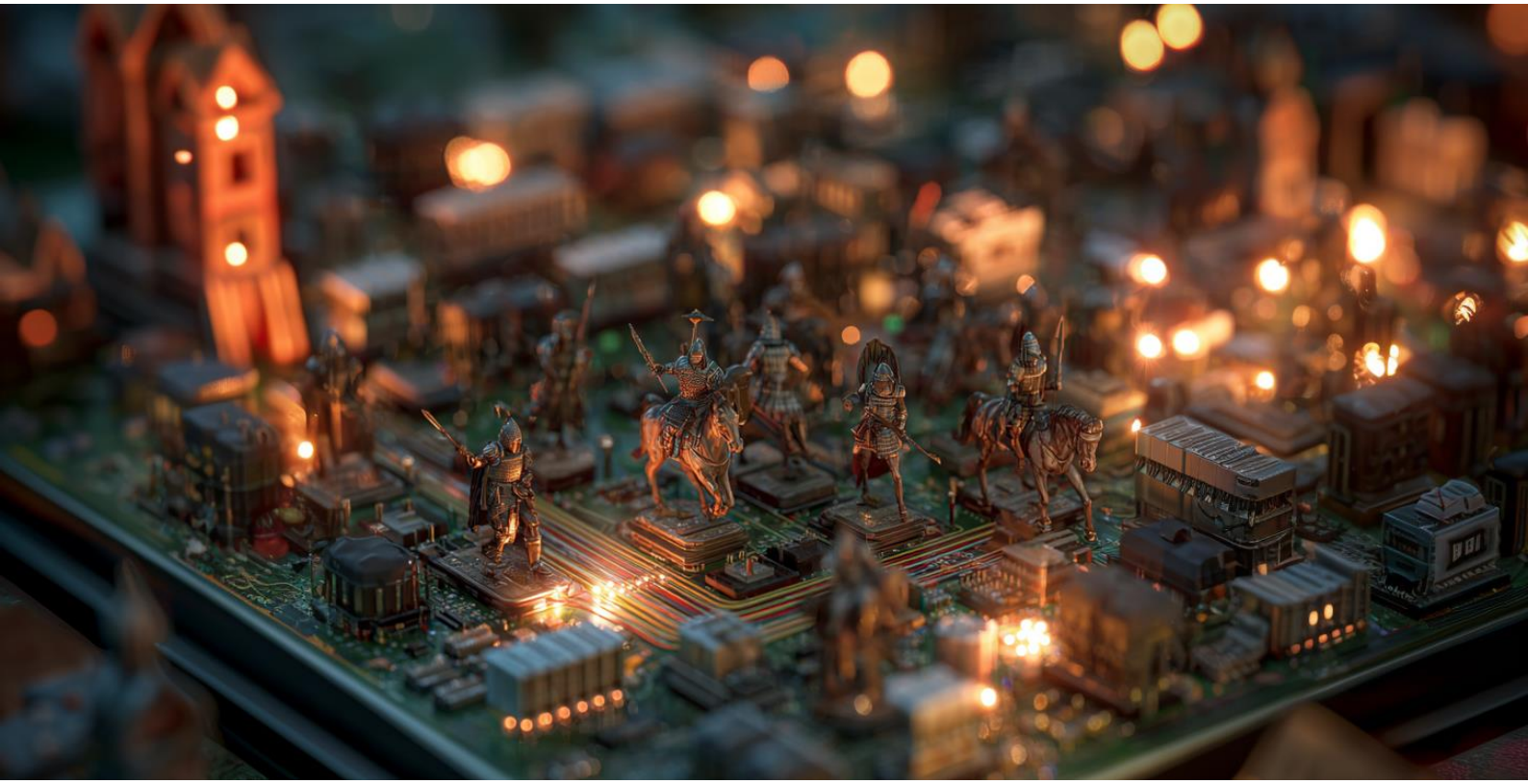
TRAINING360

CyberSecurity Connect



Kiberbiztonsági védelmi vonalak kialakítása és incidensmenedzsment

A Training360 új kiberbiztonsági blended learning képzése, október 13-tól

Kiberbiztonsági védelmi vonalak kialakítása és incidensmenedzsment képzés

Bevezetés

A 2025-ös kiberbiztonsági jelentések és előrejelzések szerint a kiberfenyegetések száma és kifinomultsága jelentősen nőtt az elmúlt időszakban. A kiberbűnözés által okozott kár összértéke ma már akkora, hogy ha ország lenne, a GDP-je a világon a harmadik lenne az Egyesült Államok és Kína után.

A mesterséges intelligencia és a nagy nyelvi modellek (LLM) egyre inkább beépülnek az adathalász valamint a social engineering támadásokba, jelentősen megnövelve a kockázatokat. Az Európai Unió NIS2 direktívának és hazai jogszabályoknak való megfelelés pedig szintén nyomást helyez a vállalatokra, szervezetekre a megfelelő szervezeti és technikai intézkedések bevezetésére, fejlesztésére.

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.

Ennek első képzése a "Kiberbiztonsági védelmi vonalak kialakítása és incidensmenedzsment" c. blended learning tanfolyam.

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
- Professzionális, modern és folyamatos támogatású távoli elérésű 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 „Kiberbiztonsági védelmi vonalak kialakítása és incidensmenedzsment” képzés célja:

- teljes és átfogó képet adjon a kiberbiztonsági védelmi vonalak és az incidens menedzsment kialakításáról és üzemeltetésről technikai és szervezeti szinten egyaránt
- megismertesse a résztvevőket, hogyan alakíthatják ki és üzemeltethetik a szervezetük, vállalatuk biztonsági védelmi vonalait, és hogyan integrálhatják ebbe az incidensmenedzsment megoldásokat
- ismertesse azokat a szervezeti intézkedéseket, jogszabályi háttereket, lépéseket, melyek az incidensek kezeléséhez szükségesek
- bemutassa a gyakorlatban a naplózó és elemző eszközök, protokollok és kapcsolódó biztonsági rendszerek működését, bevezetésének tervezését, alkalmazását és használatát
- ismertesse az üzletmenet-folytonosság és az incidensmenedzsment kapcsolatát és megfelelő BCP terv kialakítását
- ismertesse a biztonság tesztelés alapjait
- bemutassa a Red, Blue és Purple Teaming megoldások alapelveit, különböző támadási eszközöket és a naplózó rendszerek alkalmazhatóságát ezek detektálására, felderítésére

A képzés célcsoportja

A képzés a kis és közepes méretű szervezetek, vállalatok technikai megvalósításért felelős és az információvédelem menedzsment területen dolgozó munkatársak, csapatok részére egyaránt ajánlott.

- ideális lehet rendszergazdák, hálózatüzemeltetők, kezdő biztonsági szakértők, biztonság elemzők számára, akiknek feladatuk lesz a védelmi vonalak kialakítása és támogatása, és ehhez szeretnének átfogó, elméleti és gyakorlati tudást szerezni.
- A képzés javasolt IT üzemeltetési előélettel rendelkező információbiztonsági vezetők és technikai vezetők számára is, akik a technikai megvalósítási lehetőségek mellett a megfelelő szervezeti intézkedéseket is szeretnék megismerni.
- Azon IT szakértők részére, akik értékálló és eladható piaci tudást szeretnénk szerezni, karrierjüket építeni a védelmi vonalépítés és biztonsági incidensmenedzsment területén.

A képzés időtartama, felépítése

A képzés teljes óraszáma 40 óra. A képzés önálló feldolgozású, moduláris videós anyagokra, valamint vezetett és önálló gyakorlati feladatokra, illetve élő, oktató által vezetett konzultációkra (mentorálásra), valamint aszinkron, fórumos támogatásra és egyedülálló módon, mesterséges intelligencia alapú támogatásra épül. Mindez időben rugalmas formában.

- Az e-learning anyagok a képzés ideje alatt folyamatosan elérhetők, hozzáférhetők és feldolgozhatók a Training360 e-learning tárán keresztül a képzésben résztvevők számára.
- A gyakorlati feladatok interneten keresztül elérhető, előkészített virtuális infrastruktúrán végezhetők el, ahol az elérés időtartamáig (20 óra) szabadon használhatók. A gyakorlati feladatok egy része vezetett laborgyakorlat (videós demonstrációval), másik fel önálló gyakorlat írásos útmutatók segítségével.
- Heti rendszereséggel összesen 10 órányi, élő oktató által vezetett konzultációt / mentorálást, valamint a képzés ideje alatt aszinkron, chaten/fórumon történő szakmai támogatást biztosítunk a felmerülő kérdések, problémák megválaszolására, illetve a nagyobb tananyagegységek összefoglalására.
- Ehhez a képzésünkhöz az élő szakértői támogatás mellett, a hazai oktatóközpontok között elsőként, mesterséges intelligencia asszisztensi szolgáltatást is biztosítunk az elméleti anyaggal, valamint a gyakorlati feladatok elvégzéséhez kapcsolódóan. Az AIDA a Training360 tanfolyamai mellé elérhető generatív mesterséges intelligencia (LLM) megoldás, mely segíti a résztvevőket a tanulásban és eligazodni a tananyagokban. Az LMS rendszerebe és gyakorlati környezetbe integrált AI asszisztens segítségével gyorsan kaphatunk választ vagy javaslatokat, ötleteket a tanulás illetve a tananyag feldolgozása során felmerült szakmai kérdéseinkre, felvetéseinkre, vagy bizonyos gyakorlati feladatok megoldására. Mindezt 0/24-ben. A kérdéseket és válaszokat oktatóink is aszinkron módon követni tudják, és szükség esetén ellenőrzik és minősítik azokat.

A képzési anyag teljes feldolgozási ideje a konzultációkkal együtt 8 hét, ami heti 4-6 óra elfoglaltságot jelent (az e-learning anyagok és gyakorlatok a javasolt ütemezés szerint, de időben rugalmasan, szabadon feldolgozhatók; az élő konzultációs alkalmak pedig délutánonként kerülnek megtartásra (17.00-19.00 óra között). Az élő konzultációs alkalmak rögzítésre is kerülnek és visszanézhetők a képzés végét követő 1 hónapig.

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

A képzés témái

0. modul: Bevezetés. A szakértők (oktatók), a képzés felépítésének és a javasolt tanulási módszertannak, anyagainak és eszközeinek a bemutatása (élő, online forma).
1. modul: Az incidensmenedzsment alapjai. Az incidens menedzsment alapfogalmainak és alap folyamatainak ismertetése, illetve az incidens kezelést szabályozó hazai és nemzetközi előírások vázlatos ismertetése (videós e-learning forma).
2. modul: Incidens menedzsment szervezeti keretei, CSIRT-ek és SOC-ok. Incidensek kezelésének szervezeti háttere vállalati, állami és nemzetközi szinten. Hogyan épülnek fel ezek a szervezetek és csapatok, mi a szerepük, hogyan működnek és hogyan kapcsolódnak egymáshoz? (videós e-learning forma).
3. modul: Incidens menedzsment műszaki eszköztára, log források és SIEM rendszerek. A szervezetben keletkező naplók (log-ok) kezelésének architekturális kérdéseinek és teljes életciklusának az ismertetése.

   Mik azok a naplók, milyen naplók keletkeznek, hogyan keletkeznek? Hogyan kezeljük és védjük őket? Naplókezelés a gyakorlatban. Hogyan támogathatja az AI a naplózási és naplóelemzési feladatokat?(videós e-learning forma).

Élő, online konzultációs alkalom, 1 óra (1-3. modul).

4. modul: SIEM rendszerek tervezési kérdései. Egy vállalati naplókezelő infrastruktúra és azt felépítő elemek ismertetése, az egyes célok, funkciók és a felmerülő tervezési megfontolások és javaslatok bemutatása.(videós e-learning forma).
5. modul: EDR, XDR, MDR és CTI incidens menedzsment folyamata a gyakorlatban. Átfogó kép az EDR, XDR és MDR technológiák szerepéről a modern kibervédelemben, valamint azok gyakorlati alkalmazásáról az incidensmenedzsment során. Hogyan egészítik ki egymást ezek a megoldások a fenyegetések detektálása, vizsgálata és válaszlépései során, valamint hogyan használható a CTI (Cyber Threat Intelligence) az incidensek kontextusba helyezésére és priorizálására? (videós e-learning forma).
6. modul: Üzletmenet-folytonosság és Incidensmenedzsment. Üzletmenetfolytonsági terv (BCP) elkészítéséhez szükséges ismeretek és lépések vázlatos ismertetése. Milyen célokat érdemes kitűzni, milyen dokumentációkat és milyen erőforrásokat kell biztosítani egy működőképes BCP elkészítéséhez? (videós e-learning forma).

Élő, online konzultációs alkalom, 1 óra (4-6. modul).

7. modul: Naplózó protokollok és eszközök használata. A piacon használt naplózó protokollok részletes ismertetése és értékelése. Naplózó protokollok története, a jelenleg használatos szabványos és nem szabványosított protokollok, üzenet formátumok és feldolgozási lehetőségek. Naplózó infrastruktúrák kiépítésének műszaki kihívásai és megoldási lehetőségei. A gyakorlati részben a résztvevők Linux alapú log szervereketet telepítenek és kötnek össze, majd Windows eszközöket csatlakoztatnak a rendszerhez, üzenet formátumokat konvertálnak és egy-egy archiválási rendszert

telepítenek és állítanak be. (videós e-learning forma, vezetett és önálló gyakorlatokkal távoli laborkörnyezetben).

Élő, online konzultációs alkalom, 2 óra (7. modul).

8. modul: Naplózó tároló eszközök a gyakorlatban. Az előző modulban összeállított környezetbe telepítünk napló tároló appliance eszközt, mely alkalmas a beérkező üzeneteket tárolni, osztályozni és az üzeneteket értelmezni, valamit az értelmezett (parse) adatokból különböző statisztikákat készíteni és azokat különböző vizualizációs megoldásokkal ábrázolni (videós e-learning forma, vezetett és önálló gyakorlatokkal távoli laborkörnyezetben).

Élő, online konzultációs alkalom, 2 óra (8. modul).

9. modul: Naplóelemző eszközök használata a gyakorlatban. Egy naplóelemző eszköz bemutatása valamint összehasonlítása egy hagyományos naplószerver funkcióival. A résztvevők a gyakorlat során telepítik az eszközt, majd a korábban telepített rendszert illesztik a napló elemzőhöz. A későbbi gyakorlatok alkalmával különböző támadásokat is tesztelnek majd, melyek az itt telepített naplóelemzőben látszanak és kimutathatóak (vagy nem…).(videós e-learning forma, vezetett és önálló gyakorlatokkal távoli laborkörnyezetben).

Élő, online konzultációs alkalom, 2 óra (9. modul).

10. modul: Biztonsági tesztelések. A kibertámadások folyamata és módszertana, az emberi tényező kihasználásától (social engineering) az IT-alapú támadásokig. A digitális lábnyom és az OSINT jelentősége, az anonimitás előnyei és kockázatai, a Dark Web világa. Sérülékenységek típusai, OWASP Top 10 lista, a sérülékenységvizsgálat és etikus hackelés gyakorlata, a Red Team / Blue Team / Purple Team szerepei. Tesztelési módszertanok és a hazai vizsgálatok jogi-szakmai környezetének bemutatása. (videós e-learning forma, vezetett gyakorlatokkal távoli laborkörnyezetben).
11. modul: Red/Blue/Purple Teaming bemutatása a gyakorlatban. Különböző offenzív eszközök ismertetése egy előre elkészített laborkörnyezetben. Cél, hogy a résztvevők kipróbáljanak pár támadási eszközt, valamint lássák, hogy az adott támadás milyen "zajt" generál, és hogyan és mennyire detektálható különböző naplózó rendszerek segítségével.(videós e-learning forma, vezetett és önálló gyakorlatokkal távoli laborkörnyezetben).

Élő, online konzultációs alkalom, 2 óra (11. modul).

12. modul: Összefoglalás, tudásfelmérő. Az utolsó rész egy önálló ismétlési szakasz, ahol lehetőség van a teljes rögzített képzési anyagot még egyszer átnézni, feldolgozni, ismételni, illetve felmerülő kérdéseket a chatbe szakértőinknek beküldeni, melyekre egy élő adás keretében választ is adunk a teljes képzés összefoglalása mellett. A képzés egy 50 kérdésből álló online tudásfelmérő teszttel zárul, melynek kitöltésére 2 választható időpontot biztosítunk. Sikeresség (70% felett) esetén a képzés a felnőttképzési törvény alapján Tanúsítvánnyal zárul.

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 jogosultág 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 weboldalán elérhető lesz egy tudásfelmérő teszt is, amivel tesztelhető az előképzettségünk.

A képzés témái részletesen

0. modul – Bevezetés (élő, online)

A modul célja a szakértők (oktatók), a képzés felépítésének és a javasolt tanulási módszertannak, anyagainak és eszközeinek a bemutatása.

- Bemutatkozás, a képzés szakértő oktatóinak bemutatása
- A képzés aktualitása és célja
- A képzés témakörei. Miről is lesz szó?
- A képzés felépítése
    - Képzési óraszám
    - Az e-learning anyagok és javasolt feldolgozásuk
    - Gyakorlati feladatok, laborkörnyezet elérése és bemutatása (demo)
    - Konzultációs alkalmak felépítése
- A képzési anyagok elérése, hozzáférése (e-learning tár)
- Online támogatás (Teams csoportok)
- Kérdezz-felelek

1. modul – Az incidens menedzsment alapjai (videós e-learning)

A modul célja az incidens menedzsment alapfogalmainak és alap folyamatainak ismertetése, illetve az incidens kezelést szabályozó hazai és nemzetközi előírások vázlatos ismertetése.

- Bevezetés

- Fogalmak ismertetése
- Incidens típusok bemutatása
- Folyamatok ismertetése
- Incidensek osztályozása
- Incidens megoldás
- Incidenst követő (Post incident) teendők
- Traffic light protocol
- NIS2 követelmények
- Jogszabályi (Ibtv és GDPR) háttér, követelmények és kapcsolódási pontok
- Szabványszintű háttér, követelmények és kapcsolódási pontok (IEC:ISO27001, PCI DSS)

2. modul – Incidens menedzsment szervezeti keretei, CSIRT-ek és SOC-ok (videó e-learning)

A modul témája az incidensek kezelésének szervezeti háttere vállalati, állami és nemzetközi szinten. Hogyan épülnek fel ezek a szervezetek és csapatok, mi a szerepük, hogyan működnek és hogyan kapcsolódnak egymáshoz?

- CERT/CSIRT/IRT fogalma
- NIS2 irányelvek, CSIRT-ek
- Kiber TV
- Nemzetközi együttműködések
- Incidens kezelés a gyakorlatban
- Fusion centerek szerepe és működésük
- Speciális együttműködések
- Európai kiberbiztonsági stratégia átfogó ismertetése

3. modul – Incidens menedzsment műszaki eszköztára, log források és SIEM rendszerek (videó e-learning)

A modul célja a szervezetben keletkező naplók (log-ok) kezelésének architekturális kérdéseinek és teljes életciklusának az ismertetése. Mik azok a naplók, milyen naplók keletkeznek, hogyan keletkeznek? Hogyan kezeljük és védjük őket? Naplókezelés a gyakorlatban. Hogyan támogathatja az AI a naplózási és naplóelemzési feladatokat?

- Az incidens kezelés eszköztára
- Log források
- Üzemeltetési feladatok
- Napló generálás
- Napló tárolás
- Napló megsemmisítés
- Napló biztonsága
- Reagálás
- Hosszú távú megőrzés

- Tesztelés és validálás
- Szerepkörök
- SIEM rendszerek naplókezelése és használata
- Mesterséges intelligencia megoldások alkalmazása naplókezeléshez és elemzéshez

4. modul – SIEM rendszerek tervezési kérdései (videós e-learning)

A modul célja egy vállalati naplókezelő infrastruktúra és azt felépítő elemek ismertetése, az egyes célok, funkciók és a felmerülő tervezési megfontolások és javaslatok bemutatása.

- Naplók létrehozása
- Naplók továbbítása
- Naplók tárolása
- Naplók törlése
- Naplók elemzése
- Agent-ek fogalma, működése és kezelésük
- Kollektorok fogalma, működése és kezelésü
- Központi elemek
- Adatelemzési megoldások
- Korrelációk
- Dashboardok és jelentések (Riporting)
- Riasztások (Alerting)
- Hozzáférés vezerlés (Access control)
- Telepítés
- Skálázhatóság
- Mentés
- Felület
- Rendelkezésre állás
- Monitoring
- Gyakorlati kihívások

5. modul – EDR, XDR, MDR és CTI Incidens menedzsment folyamata a gyakorlatban (videós e-learning)

A modul átfogó képet ad az EDR, XDR és MDR technológiák szerepéről a modern kibervédelemben, valamint azok gyakorlati alkalmazásáról az incidensmenedzsment során. Bemutatjuk, hogyan egészítik ki egymást ezek a megoldások a fenyegetések detektálása, vizsgálata és válaszlépései során, valamint hogyan használható a CTI (Cyber Threat Intelligence) az incidensek kontextusba helyezésére és priorizálására.

- Cyber Threat Intelligence (CTI) fogalma
- A CTI szintjei
- Kinek szól a CTI?

- Kompromittációs indikátorok (IoC)
- Takitkák, technikák és eljárások (TTP)
- A MITRE ATT&CK® keretrendszer
- Threat Intelligence lehetőségek
- Hol vannak információk?
- Az információ megosztás formája
- CTI automatizálása
- Strukturált fenyegetési információleíró nyelv - Structured Threat Information Expression (STIX)
- OpenC2 – az automatizálás protokollja
- Kibermegfigyelési leíró nyelv - Cyber Observable eXpression
- Endpoint Detection and Response (EDR) rendszerek
- Extended Detection and Response (XDR) rendszerek

6. modul – Üzletmenet-folytonosság és Incidensmenedzsment (videós e-learning)

A modul célja egy üzletmenetfolytonssági terv (BCP) elkészítéséhez szükséges ismeretek és lépések vázlatos ismertetése. Milyen célokat érdemes kitűzni, milyen dokumentációkat és milyen erőforrásokat kell biztosítani egy működőképes BCP elkészítéséhez?

- Mi az üzletmenet folytonosság?
- Hogyan érhető el a cél?
- Tervezés és dokumentáció
- Célok meghatározása
- A BCP elkészítésének lépései
- Üzleti visszaállítási stratégia
- Létesítmény visszaállítási stratégia
- Emberi erőforrással történő újraindítása stratégia
- Műszaki visszaállítási stratégia
- Előfizetéses szolgáltatások
- Adatvisszaállítási stratégia
- Az ISO22301 BCM szabvány rövid bemutatása

7. modul – Naplózó protokollok és eszközök (videós e-learning és gyakorlatok)

A modul célja a jelenleg a piacon használt naplózó protokollok részletes ismertetése és értékelése, melyben részletesen bemutatjuk a naplózó protokollok történetét, a jelenleg használatos szabványos és nem szabványosított protokollokat, ismertetjük az üzenet formátumokat és feldolgozási lehetőségek. Tárgyaljuk a naplózó infrastruktúrák kiépítésének műszaki kihívásait és megoldási lehetőségeit.

A gyakorlati részben a résztvevők Linux alapú log szervereketet telepítenek és kötnek össze, majd Windows eszközöket csatlakoztatnak a rendszerhez, üzenet formátumokat konvertálnak és egy-egy archiválási rendszert telepítenek és állítanak be.

- Protokollok bemutatása és ismertetése:

    - RFC: RFC3164, RFC5424
    - Non-RFC: WINDOWS EVTX …
- Üzenet formátumok ismertetése: CLF, WELF, JSON, SOAP…
- SIEM rendszerek
- Elemzők
- Naplózó infrastruktúra felépítése, a NIST-800-92 és rev1 szabvány
- Naplózó protokollok és eszközök labor gyakorlat
    - Syslog kliens
    - Syslog relay
    - Syslog szerver telepítés és beállítás
- Napló adatok feldolgozása: szűrés, újraírás, parszolás, kiegészítés (enrichment)
- Adatfogadás és továbbítási funkciók (Relay)

8. modul – Naplózó tároló eszközök a gyakorlatban (videós e-learning és gyakorlatok)

A modul és kapcsolódó gyakorlati feladatok során az előző alkalommal összeállított környezetbe telepítünk napló tároló appliance eszközt, mely alkalmas a beérkező üzeneteket tárolni, osztályozni és az üzeneteket értelmezni, valamit az értelmezett (parse) adatokból különböző statisztikákat készíteni és azokat különböző vizualizációs megoldásokkal ábrázolni.

- Napló tároló rendszer telepítése
- Kezdeti rendszerbeállítások
    - Források beállítása: GELF és IETF syslog formátum
- Agent bekötés
- Logrelay telepítés
- Logrelay bekötés
- Beállítások
    - Üzenet szortírozás, üzenetek streamekre osztása
    - Üzenet részek feldolgozása
    - Dashboard létrehozása
    - Geo IP elemzés
    - Üzenetek ábrázolása térképen
    - Üzenetek vizualizációja diagramokkal
    - Tor exit node-ok felismerése
    - Riasztás konfigurálása

9. modul – Naplóelemző eszközök használata a gyakorlatban (videós e-learning és gyakorlatok)

A modul célja egy naplóelemző eszköz bemutatása valamint összehasonlítása egy hagyományos naplószerver funkcióival. A résztvevők a gyakorlat során telepítik az eszközt, majd a korábban telepített rendszert illesztik a napló elemzőhöz. Különböző támadásokat is tesztelnek majd, és elemzik a naplóelemzőben az eredményeket.

- A Wazuh rendszer áttekintése
    - Főbb komponensek és architektúra

    - Funkcionalitás
    - Összehasonlítás a hagyományos naplószerverrel
- Telepítés és alapkörnyezet kialakítása
    - Wazuh szerver telepítése és konfigurációja
    - Ügynök telepítése egy kliens rendszerre
    - Tesztkörnyezet felkészítése a gyakorlatokhoz
- Integráció meglévő naplógyűjtő rendszerrel
    - Korábban telepített naplószerver csatlakoztatása a Wazuh-hoz
    - Adatáramlás validálása (log forward és ingest)
- Alapvető keresési és elemzési műveletek
- Támadások és kimutatásuk

10. modul – Biztonsági tesztelések (videós e-learning és gyakorlatok)

A modul átfogó képet ad a kibertámadások folyamatáról és módszertanáról, az emberi tényező kihasználásától (social engineering) az IT-alapú támadásokig. Bemutatjuk a digitális lábnyom és az OSINT jelentőségét, az anonimitás előnyeit és kockázatait, valamint a Dark Web világát. A résztvevők megismerik a sérülékenységek típusait, az OWASP Top 10 listáját, a sérülékenységvizsgálat és etikus hackelés gyakorlatát, valamint a Red Team / Blue Team / Purple Team szerepeit. Külön blokkban tárgyaljuk a tesztelési módszertanokat és a hazai vizsgálatok jogi-szakmai környezetét.

- A kibertámadás folyamata
- Az ember sebezhetősége
- Social Engineering
- IT alapú támadások
- Digitális lábnyom
- OSINT
- Dark Web / Dark Net
- Anonimitás pro és kontra
- Sebezhetőségek típusai
- OWASP Top 10
- Sérülékenység vizsgálat
- Red Team / Blue Team / Purple Team
- Ethical hacking
- Tesztelési módszertanok
- Vizsgálatok Magyarországon

11. modul – Red / Blue / Purple Teaming (videós e-learning és gyakorlatok)

A modul célja a különböző offenzív eszközök ismertetése egy előre elkészített laborkörnyezetben. Cél, hogy a résztvevők kipróbáljanak pár támadási eszközt, valamint lássák, hogy az adott támadás milyen "zajt" generál, és hogyan és mennyire detektálható különböző naplózó rendszerek segítségével.

- Red Teaming
- Blue Teaming
- Purple Teaming
- Labor bekötése a korábban beállított naplótároló szerverhez
- Labor bekötése a korábban beállított naplóelemző szerverhez
- Windows Server jelszótörés (password hacking)
- Kerberos támadások (Rubeus)
- Sérülékenység-kiaknázás (Metasploit)
- Hitelesítő adatok gyűjtése (LaZagne)
- Jelszótörés (Hashcat)
- Hálózati jogosultság térképezése (BloodHound)
- Gyakorlati támadás-szimuláció (CTF Kali környezetben)Rubeus használata
- Tevékenységek elemzése naplótároló és elemző szerverek segítségével

12. modul – Összefoglalás (videós e-learning, gyakorlatok, élő online)

Az utolsó rész egy önálló ismétlési szakasz, ahol lehetőség van a teljes rögzített képzési anyagot még egyszer átnézni, feldolgozni, ismételni, illetve felmerülő kérdéseket a chatbe szakértőinknek beküldeni, melyekre egy élő adás keretében választ is adunk a teljes képzés összefoglalása mellett. A modult követően 2 választható időpontot biztosítunk az online tudásfelmérő kitöltésére.

A képzés tervezett ütemezése:

- Tervezett kezdés: 2025. október 13.
- Az élő konzultáció alkalmak tervezett időpontjai: október 13., október 21., 28., november 6., 13., 20., 27., december 4., 10. (ezek még csak tájékoztató jellegűek, változhatnak)
- Várható befejezés: 2025. december 12.

A képzés szakértői, oktatói

dr. Krasznay Csaba

Csaba rendszeres előadója hazai és nemzetközi konferenciáknak, valamint az egyik legtöbbet foglalkoztatott kiberbiztonsági médiaszakértő Magyarországon. A Nemzeti Közszolgálati Egyetem docense, kutatási témája a kiberbiztonság. Az egyetem Kiberbiztonsági Intézetének korábbi vezetője. A kiberbiztonsági mesterképzésért is felelős, korábban pedig az elektronikus információbiztonsági menedzser posztgraduális képzésért volt felelős.

2011-ben az „Év biztonsági szakértője” címre választották. Elnökségi tagja és az Önkéntes Kibervédelmi Egyesületnek, korábbi elnökségi tagja a Magyar E-közigazgatási Egyesületnek, az

ISACA Magyarországnak és a Magyar Elektronikus Aláírás Szövetségnek. Tagja a Magyar Hadtudományi Társaságnak és az Infokommunikációs Tudományos Egyesületnek is

Főbb releváns minősítései: CISA, CISM, CISSP, CSSLP, Certified SOC Analyst, Certified Ethical Hacker, Certified Incident Handler, ISO27001 Lead Auditor, ITILv3 szakértő.

Illés Gábor

Gábor több mint 20 éves tapasztalattal rendelkezik különböző informatikai és kiberbiztonsági pozíciókban. Mentor és vendégelőadó a Nemzeti Közszolgálati Egyetemen. Saját kiberbiztonságra fókuszáló és képzési környezetet is biztosító saját startup cégének vezetője és technikai szakértője.

A Balabitnál presales mérnökként dolgozott és a kiberbiztonság, a vállalati szintű hálózati telepítések és a technológiai védelem számtalan aspektusának bonyolult kérdéseiben fejlesztette ki tudását. Ezt követően a Balasys Kft-nél technológiai fejlesztési kutatóként és tanácsadóként.

Gábor számos penetrációs tesztelési és sebezhetőségkezelési projektben vett részt tanácsadóként és technológiai tanácsadóként. Gábor képzései, tudása az ipari kiberbiztonság, a felhőbiztonság, a DevSecOps és a hálózati biztonság témakörét is lefedik. ISO 27001 lead auditor és CISM tanúsítvánnyal rendelkezik.

Szoldán Márk

Több mint 25 éves szakmai tapasztalattal rendelkezik az informatika és üzleti tanácsadás területén, amelynek részeként több mint egy évtizede kiemelten kiberbiztonsági megoldásokkal foglalkozik, ezt a Balabitnál kezdte, nemzetközi trénerként. Dolgozott Magyarországon és külföldön a Microsoftnál, az IBM-nél, a PwC-nél, valamint szabadúszóként is, széleskörű tapasztalatot szerezve nemzetközi környezetben és változatos technológiai és iparági projektekben. Jelenleg a kiberbiztonsági megoldásokat fejlesztő One Identity termékeinek oktatását és bevezetését támogatja, világszerte ügyfeleknek tartva képzéseket, a hozzáférés-kezeléssel és a naplóelemzéssel foglalkozik kiemelten. A Magyar Mérnökakadémia tagja.

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.

Jelentkezési információk

A képzésre az első körös jelentkezési határidő: 2025. október 1.
A képzés minimálisan 30 fő jelentkezése esetén indul.
Simon Ferenc, +36 (30) 388-8264, ferenc.simon@training360.com