Kibervédelmi tanfolyam tematika – Braining Hub

Miről szól az oktatás?

Az oktatás során a szakemberek megismerkedhetnek a leggyakoribb kibertámadási fogalmakkal, technikákkal és a detektálási, megelőzési folyamatokkal is. A tanfolyam célja, hogy elméleti és gyakorlati szinten is alkalmazható tudást biztosítson a résztvevőknek, hogy a szervezet felépítését átlássák, gyenge pontjait egyszerűbben felismerjék és időben tudjanak azonosítani és kezelni támadási próbálkozásokat. Az első modul az információbiztonsági incidenskezelés témáját járja körül, végigvezetve a jelenlévőket a bekövetkezéstől a továbblépésig vezető úton. A második modul a védelmi oldal elméletét és alapfogalmait mutatja be, a harmadik pedig annak gyakorlati részébe enged betekintést. A negyedik modul a támadói oldalra koncentrál, illetve emellett az ethical hacking és a social engineering alapfogalmait és folyamatait ismerteti. Az egyes modulok egymástól függetlenül elvégezhetők, szorosabban csak a második és a harmadik alkalom épül egymásra.

Kiknek ajánljuk a tanfolyamot?

Olyan szakembereknek ajánlunk, akik olyan vállalatnál dolgoznak, amely rendelkezik IT-biztonsági stratégiával és koncepcióval, amelyben az egyik leghatékonyabb és leggazdaságosabb védekezési módszerként szerepet kap a munkatársak képzése, biztonságtudatosságának fejlesztése. Ajánljuk a tanfolyamot azoknak is, akik – különösen a tömeges távmunka és home office idején – a műszaki jellegű védekezés mellett nagyobb szerepet kívánnak adni a humán jellegű védekezésnek, a leggyengébb láncszem megedzésének. Modulokra bontott képzésünkkel azoknak szeretnénk kedvezni, akik érdeklődnek a kibervédelem iránt, ám mégsem tudnak elköteleződni a kurzus teljes időtartamára, illetve azoknak, akik csak egy-egy nap témájáról tanulnának szívesen.

Milyen témaköröket tekintünk át?

1. **NAP**

<u>Védelmi oldal elmélet</u>

1. Alapfogalmak ismertetése
    a. Blue Team fogalma és felelősségi köre
    b. Általános fogalmak (incidens, detektálás, monitorozás, SIEM, IDS, IPS, SOC stb)
    c. Detektációs és elhárító eszközök
    d. Források (szignatúrák, szabályok, blacklist, CTI)
2. A Biztonsági Műveleti Központ (SOC) kialakítása és működése
    a. A SOC fogalma és hatásköre
    b. A SOC típusai (menedzselt, saját, társmenedzselt)

   c. A SOC feladai (monitorozás, incidenskezelés, elhatárolás, sérülékenységmanagement, kommunikáció, dokumentáció)
   d. A SOC szerepkörei (L1, L2, L3 level analyst, engineer, manager, threat hunter)
3. Az incidenskezelés alapjai
   a. Az incidens és az incidenskezelés, kockázati besorolás fogalma
   b. Az incidenskezelés folyamata
      - Detekciós
      - Triázs
      - Elhárítás
      - Károk felmérése és remediáció
      - Visszaállítás levezetése
      - Életciklus nyomonkövetése
      - Dokumentáció
      - Detektációs eszközök, módszerek finomítása
4. IT biztonsági rendszerek
   a. IT biztonsági rendszerek típusai
   b. SIEM rendszerek fogalma, működése, típusai
   c. Loggyűjtő rendszerek
   d. Hálózati behatolásvédelmi és detektációs rendszerek (IDPS)
   e. Full Packet Capture
   f. Tűzfalak
   g. Antivírus (AV)
   h. Végponti behatolásvédelmi rendszerek (HIDS, EPS)
   i. Cyber Threat Intelligence (CTI) és Threat Hunting
   j. Sérülékenységvizsgálók (VA)

2. **NAP**

<u>Védelmi oldal gyakorlat</u>

1. Naplózás
   a. Windows Event Log bevezetés
   b. Syslog bevezetés
   c. Logolás és feldolgozás lehetőségei
2. Virtualizációs rendszerek
   a. Bevezetés
   b. Virtualizációs rendszerek típusai
   c. A virtualizációs rendszerek előnyei és hátrányai
   d. Virtualizációs rendszerek – példák
   e. Logolás és hardening
3. SIEM rendszerek

   a. Bevezetés
   b. Eseményfeldolgozás
   c. Hibafeldolgozás
   d. Parsing
   e. Korreláció
   f. Riasztás
   g. Active Response
4. SIEM rendszerek hardverigénye
   a. Tárolás
   b. Elosztott környezetek
   c. Komponensek
   d. Hálózat
5. SIEM alkalmazások
   a. Gyártói eszközök
   b. Open Source eszközök

3. **NAP**

<u>Támadói oldal</u>

I. Ethical Hacking tematika

1. Alapfogalmak ismertetése
   a. Jogi szabályozás, törvényes keretek
   b. Általános, informatikai alapfogalmak
   c. Támadói fogalmak
   d. Védelmi fogalmak
   e. Team-ek bemutatása (Red, Blue, Green, stb.)
2. Támadói oldal ismertetése
   a. Rosszindulatú támadás fázisai
      - OSINT
      - Sérülékenységek keresése és validálása
      - A betörés folyamata
      - Nyomok eltüntetése
      - Folyamatos jelenlét, utógondozás
      - Megszerzett információk sorsa, használhatósága
   b. Komolyabb támadások, állami hátterű hackercsapatok bemutatása
   c. Social Engineering (külön tárgyalva a támadás fázisaitól)
   d. Eszközök, tool-ok bemutatása
   e. Red Teaming

II. Social Engineering tréning előadás tematika

1. Mi a Social Engineering?
2. A social engineering vizsgálat digitális eszközei
3. A social engineering vizsgálat humán eszközei
4. Esettanulmány
    - előkészület
    - bejuttatás folyamata
    - következmény
5. Mihez kezdhetünk a folyamat során megszerzett személyes és egyéb adatokkal?

4. NAP

<u>Információbiztonsági Incidens kezelése</u>

1. Információbiztonsági incidens bekövetkezése
2. Bejelentési kötelezettség, reagálási idő
3. Kríziskommunikáció
4. Incidenskezelési eljárásrend vagy Business Continuity Plan (Üzletmenet-folytonossági Terv)?
5. BCP: tartalmi, formai követelmények hatáskörök, eljárás.
6. DRP azaz Disaster Recovery Plan (Katasztrófa helyreállítási terv)
7. Végjáték: konzekvenciák, koczkázatelemzés felülvizsgálata, továbblépés