MEGHÍVÓ

VAN KIHEZ FORDULNI A NIS2 AUDIT FELKÉSZÜLÉSBEN

INTERAKTÍV, A RÉSZT VEVŐ CÉGEK IGÉNYEIRE SZABOTT WORKSHOP!

. Az MKIK és az SZTFH együttműködésével megvalósuló projekt a hazai vállalkozásokat segíti a kiberbiztonsági auditra történő felkészülésben.

A workshopon 5-7 cég vesz részt és testreszabottan, a résztvevőket érintő témákkal foglalkozunk.

Tegye fel a kérdéseit írásban előzetesen vagy a helyszínen, akár névtelenül is!

Igény esetén megvizsgáljuk a cég felkészültségét és segítünk megoldani a problémákat.

A helyben meg nem oldható problémákra, utólagos írásos választ adunk. A válaszadásban és a válaszok utólagos validálásában szükség esetén az SZTFH és az auditorok is részt vesznek.

Helyszín: **BKIK székház 301. terem (1016 Budapest, Krisztina krt. 99.)**

Időpont: **2025 november 13. (csütörtök) 09:30 óra**

A rendezvény ingyenes, de regisztrációhoz kötött. Regisztráció és előzetes kérdésfeltétel a https://nis2.mkik.hu oldalon lehetséges.

Program

09:30-10:00 – Regisztráció

10:00: 12:00 – Szakmai workshop I. rész

12:00: 12:30 – Ebéd

12:30: 14:00 – Szakmai workshop II. rész

A Workshop tartalma

A szakértők bemutatják a sikeres audit felkészüléshez szükséges lépéseket (speciálisan a részt vevő cégek jellemzőire szabva) és válaszolnak a felmerülő kérdésekre is. Lehetőség van a feltett kérdések eszkalálására az SZTFH-nak, vagy kiberbiztonsági auditoroknak. Időben feltett kérdés esetén ez még a workshop előtt megtörténik. Helyszínen feltett, helyben meg nem válaszolható, vagy a hatósággal validálandó kérdés esetén utólagos írásos választ kap a kérdés feltevője. Lehetőség van átfogó írásbeli iránymutatás igénylésére is. Az iránymutatásokat az SZTFH validálja, ezáltal 100%-os biztonsággal az elvárt jó gyakorlatot tükrözik.

A szakmai rész tematikája

- Mire számíthatunk egy kiberbiztonsági audit során? Az audit módszertana és gyakorlati tanácsok a felkészüléshez
- Mire számíthatunk egy kiberbiztonsági audit során? Az audit módszertana és gyakorlati tanácsok a felkészüléshez
- Az gyártó cégek NIS2 érintettsége

  - Az érintettséget megalapozó tényezők, felügyeleti hatóságok, jogszabályi környezet
- Mit tekintsünk EIR-nek az gyártó cégeknél, jellemző EIR-ek?
- JELLEMZŐ KOCKÁZATOK, KIHÍVÁSOK
  - Hosszú életciklus, örökölt (Legacy) rendszerek és elavult szoftverek
  - A folyamatos üzemeltetés elsődlegessége
  - Hiányos hálózati láthatóság és szegmentáció
  - Az incidensek észlelésének és kezelésének a nehézségei
  - Beszállítói lánc (OT specifikus) kockázatai
  - Eltérő kockázatkezelési szemlélet
- NEM ALKALMAZHATÓ 7/2024 ELŐÍRÁSOK IPARI KÖRNYEZETBEN ESETÉBEN
  - A 7/2024 MK rendelet azon előírásai, amelyek nem vagy nehezen alkalmazhatóak ipari környezetben
  - Hogyan kezeljük ezeket az eltéréseket?
- INCIDENSKEZELÉS
- ESETTANULMÁNYOK, Hogyan feleljünk meg a követelményeknek? A felkészülés legfontosabb területeinek bemutatása, a résztvevő cégek igényeire és sajátosságaira szabva. Területek:
  - Programmenedzsment
  - Hozzáférés-felügyelet
  - Tudatosság és képzés
  - Naplózás és elszámoltathatóság
  - Értékelés, engedélyezés és monitorozás
  - Konfigurációkezelés
  - Készenléti tervezés
  - Azonosítás és hitelesítés
  - Biztonsági események kezelése
  - Karbantartás
  - Adathordozók védelme
  - Fizikai és környezeti védelem
  - Tervezés
  - Személyi biztonság
  - Kockázatkezelés
  - Rendszer- és szolgáltatásbeszerzés
  - Rendszer- és kommunikációvédelem
  - Rendszer- és információsértetlenség
  - Ellátási lánc kockázatkezelése

A résztvevő cégek kérdéseit az aktuális területek kapcsán tárgyaljuk.

A tudásközpontban rendelkezésre álló kompetencia:

- IBF, DPO, audit felkészítési és auditori tapasztalat
- A 2024. évi LXIX. törvény (11. § (13) bekezdése, az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas személy
- Adatvédelmi szakjogász
- Biztonságszervezési menedzser
- Információbiztonsági szakmérnök
- ISO 20000 szolgáltatásmenedzsment auditor

- ISO 27035 incidens menedzser
- ISO 27001 információbiztonság irányítási rendszer vezető auditor
- ISO 42001 vezető auditor
- Minősített információs rendszerauditor (ISACA – CISA)
- Minősített információs rendszer menedzser (ISACA – CISM)
- Minősített etikus hacker (EC-Council – CEH)
- Minősített titkosítási szakértő (EC-Council – ECES)
- Mesterséges intelligencia és technológiai szakjogász
- Offensive Security Certified Professional (Offensive Security)

Rendelkezünk továbbá kompetenciával OT információbiztonság területén is