Tanácsadás megnevezése	Minimum egység	Kiberbiztonsági és szoftvertechnológiai tanácsadás – A szolgáltatás rövid leírása
Biztonsággal kapcsolatos orientáció	fél munkanap	A szolgáltatás célja az érdeklődő kliensek segítése a számukra releváns biztonsági kockázatok azonosításában és a DigitalTech EDIH azon kapcsolódó tanácsadás szolgáltatásainak kiválasztásában, melyek a kliens számára hasznosak lehetnek az azonosított kockázatok kezelésének tekintetében.
Kockázat-menedzsment támogatása	fél munkanap	A szolgáltatás célja a kliens segítése a kockázat alapú szemlélet megértésében és elsajátításában a biztonság és az adatvédelem területén, valamint a biztonsági és az adatvédelmi kockázatok kezelésére alkalmazható módszerek és eszközök azonosításában és használatában, beleértve a kockázatbecsléssel és a kockázatok elhárításával kapcsolatos módszereket és eszközöket.
Biztonsági/technológiai érettségi szint felmérése	fél munkanap	A szolgáltatás célja a kliens segítése abban, hogy felmérje és megértse a saját biztonsági/technológiai érettségi szintjét. Az érettségi szint felmérése a klienssel folytatott irányított beszélgetésben vagy egy érettségi szint felmérését szolgáló formalizált kérdőív kitöltésén keresztül történik. A szolgáltatás részeként a kliens visszacsatolást kap arról is, hogy milyen módon növelheti biztonsági/technológiai érettségi szintjét, illetve milyen DigitalTech EDIH tanácsadás szolgáltatások igénybevétele segítheti ebben.
Biztonsági/technológiai érettségi szint fejlesztése	fél munkanap	A szolgáltatás célja a kliens segítése biztonsági/technológiai érettségi szintjének növelésében. Ez magában foglalhatja egyedi, a kliens részére testre szabott tudásanyag kidolgozását és átadását, illetve komplexebb esetben, segítség nyújtását egy biztonsági/technológiai érettségi szint növelését célzó szisztematikus program kialakításában és végrehajtásában, beleértve a célok és a mérhető teljesítménymutatók meghatározását, a megfelelő módszerek, eszközök azonosítását, a releváns folyamatok megtervezését, és a program költségeinek becslését.
Szabályozásoknak való megfelelés támogatása	fél munkanap	A szolgáltatás célja a kliensek segítése abban, hogy azonosítsák a számukra releváns biztonsági vagy adatvédelmi törvényeket és szabályozásokat, és az alkalmazható biztonsági vagy adatvédelmi szabványokat és legjobb gyakorlatokat. Azon kliensek számára, akiknek jogszabályi megfelelőségi kötelezettségeknek vagy általánosan elfogadott iparági követelményeknek kell eleget tenniük, segítünk azonosítani a megfelelőség biztosítására használható módszereket, eszközöket, és folyamatokat.
Biztonsági követelmények azonosításával kapcsolatos tanácsadás	fél munkanap	A szolgáltatás keretében konzultációs jellegű támogatást nyújtunk számítógépes rendszerek, digitális termékek, vagy szolgáltatások biztonságos működéséhez szükséges elvárások meghatározásával kapcsolatban. Ezek a követelmények a tervezés kiindulópontját és az implementáció alapját jelentik. A szükséges biztonsági követelmények meghatározása érdekében segítünk a rendszerrel/termékkel/szolgáltatással kapcsolatos releváns fenyegetések és a lehetséges támadási forgatókönyvek azonosításában, valamint az ebből fakadó biztonsági követelmények megértésében.
Biztonsági megoldásokkal kapcsolatos tervezés, modellezés támogatása	fél munkanap	A szolgáltatás célja, hogy segítséget nyújtson azoknak az ügyfeleknek, akik már rendelkeznek termékeikre, szolgáltatásaikra vagy számítógépes rendszereikre vonatkozó biztonsági specifikációval. A megadott specifikációk alapján a szolgáltatás biztonsági architektúra tervezésével kapcsolatos kérdésekben nyújt segítséget, beleértve a követelmények kielégítésére használható mechanizmusok azonosításának, ezek egy rendszerbe integrálásának, és az így kialakított architektúra analízisének támogatását.
Szoftverbiztonsággal kapcsolatos tanácsadás	fél munkanap	A digitális átalakulás következtében sok vállalkozást/szervezetet érint a szoftverfejlesztés, de sokan még mindig nem tudták a biztonságot integrálni a szoftverfejlesztési életciklus (SDLC) modelljükbe. Ennek a szolgáltatásnak az a célja, hogy segítsünk az ügyfeleknek azonosítani a fejlesztési folyamataik biztonsági hiányosságait és kiküszöbölni azokat, pl. biztonságos programozási módszertanok alkalmazásával. Rávilágítunk továbbá a statikus szoftverelemzés jelentőségére, segítünk kiválasztani az ügyfél igényeinek leginkább megfelelő szoftverbiztonsági elemzési módszereket és eszközöket, tanácsot adunk ezek használatában, az elemzések eredményeinek értelmezésében, és az azonosított hibák javításában.
Rendszerintegráció támogatása	fél munkanap	A modern IT rendszerek egyre több belső és külső szolgáltatást használnak céljaik elérése érdekében. Emiatt egy rendszer biztonságra ma már jelentősen függ az általa használt és integrált szolgáltatások biztonságától. Ezen szolgáltatások integrálásának kérdését figyelembe kell venni egy fejlesztési folyamat vagy bármilyen biztonsági analízis során. Ez a tanácsadás szolgáltatás segít azonosítani, hogy a kliens által használt üzleti és technológiai környezetben milyen jellegű szolgáltatási függőségek kritikusak, valamint milyen minőségi tulajdonságokat fontos definiálni és folyamatosan mérni ezen szolgáltatásokhoz. Ezek után a konzultációs során átnézzük a jelenlegi szolgáltatásintegrálási, naplózási és mérési gyakorlatokat, és javaslunk olyan további jó gyakorlatokat, amik relevánsak lehetne a kliens számára.
Informatikai rendszerek biztonságos üzemeltetésével, üzemeltetési adatok elemzésével kapcsolatos tanácsadás	fél munkanap	A szolgáltatás célja a kliensek segítése IT infrastruktúrájuk biztonságos üzemeltetésében, ideértve (de nem kizárólag erre limitálva) Windows és Linux szerverek és munkaállomások, lokális hálózatok, és alapvető szolgáltatások (pl. Active Directory, virtuális magánhálózatok, és DHCP) működtetését. Ezen kívül, támogatást nyújtunk biztonsági incidensek hatásos kezelésével kapcsolatban, elsősorban a megelőzésre fókuszálva, azaz például a szükséges műszaki előkészületi lépésekkel és egy incidenskezelő csapat felállításával kapcsolatban, de érintve az incidens elemzés fázisban használható módszereket és eszközöket is. Fontos kihangsúlyozni, hogy nem nyújtunk incidenskezelés szolgáltatást (pl. nem állítunk vissza adatokat egy zsarolóvírus támadás után), csupán tanácsot adunk azzal kapcsolatban, hogy hogyan lehet hatásosan felkészülni egy biztonsági incidensre (pl. zsarolóvírus támadásra).Továbbá, az informatikai rendszerek és szolgáltatások üzemeltetése és karbantartása során számos olyan adat keletkezik, amelyek részletes elemzése alapvető hozzájárulást jelenthet a fejlesztési és karbantartási folyamat hatékonyságának, valamint a termék és szolgáltatás minőségének és biztonságának javításához. Pl. egy ilyen adatelemzés képes feltárni a hatékonyság és a szolgáltatásminőség szempontjából kritikus szűk keresztmetszeteket és hibaforrásokat. Ebben a szolgáltatásban támogatást adunk az üzemeltetési adatok gyűjtésével, tárolásával és feldolgozásával kapcsolatos folyamatok kialakításában, valamint adatok vizualizációjával kapcsolatban.

Tanácsadás megnevezése	Minimum egység	Kiberbiztonsági és szoftvertechnológiai tanácsadás – A szolgáltatás rövid leírása
Informatikai rendszerek tesztelésével és helyesség-bizonyításával kapcsolatos tanácsadás	fél munkanap	A szolgáltatás célja az ügyfelek támogatása informatikai rendszerek vagy szolgáltatások szisztematikus tesztelésében, esetleg komplexebb, formalizált helyesség-bizonyítási módszerek alkalmazásában. A tesztelés és a különböző kód átvilágítási technikák a szoftveralapú rendszerek minőségének mérésére és javítására szolgáló általános módszerek. A kritikus alkalmazási területeken (pl. autóipari, orvosi, pénzügyi vagy energetikai rendszerek) azonban néha további bizalmi szintre van szükség. A formális verifikációs technikák olyan precíz matematikai algoritmusokon alapuló technikák, amelyek segítségével bizonyítani lehet egy rendszer valamilyen fontos tulajdonságát, vagy példákat lehet mutatni arra, hogy a rendszer hogyan hibásodhat meg. Ezek a technikák előzetes munkabefektetést igényelnek a rendszer modellezéséhez és elemzéséhez, de később olyan problémákra is fényt deríthetnek, amelyeket a hagyományos módszerekkel különösen nehéz feltárni.
Projekt-tervek felülvizsgálata, projekt-folyamatok hatékonyságának elemzése	fél munkanap	A biztonságossági szempontokból kritikus folyamatok esetén már idáig is szabványok hívták elő a fejlesztési-, ellenőrzési és üzemeltetési folyamatok felépítését és végrehajtását. Ez a termék- és szolgáltatáskör az Európai Parlamenthez beterjesztett "A digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről" törvényjavaslat alapján a közeljövőben várhatóan jelentősen kibővül lefedve lényegében a teljes IT bázisú spektrumot. A várható új törvény alapvető feladatává teszi az ilyen termékek és szolgáltatások nyújtóinak a biztonság folyamatos garantálását, ideértve annak karbantartását is. A felhasználó oldalán ugyanakkor ezen biztonsági szolgáltatások fogadására és a felhasználói rendszer működtetésébe integrálására fel kell készülni. A konzultáció mind az IT alapú termékek és szolgáltatások nyújtóinak, mind pedig felhasználóinak segítséget kínál a fejlesztési-, ellenőrzési és üzemeltetési feladatok megfelelő kialakításában.
Robusztus és megbízható munkafolyamat automatizálás	fél munkanap	A szolgáltatás keretében folyamatalapú rendszereket és szolgáltatásokat készítünk fel az esetlegesen előforduló hibák kezelésére és hatásuk csökkentésére, valamint támogatjuk folyamat alapú rendszerek működésének automatizálását.
Egyéb biztonsági tanácsadás	fél munkanap	Ezen szolgáltatás keretében igyekszünk támogatni ügyfeleinket minden olyan biztonsággal kapcsolatos problémakörben, melyhez rendelkezünk szakértővel. Ez magában foglalja többek között a beágyazott rendszerek (pl. járművek, ipari vezérlőrendszerek, IoT rendszerek) biztonságával kapcsolatos kérdéseket, a kriptográfiai megoldások (beleértve a poszt-kvantum kriptográfiai algoritmusok) helyes alkalmazásával kapcsolatos kérdéseket, a gépi tanulásra épülő rendszerek/szolgáltatások biztonsági kérdéseit, a személyes adatok védelmével kapcsolatos kérdéseket, és a blokklánc technológiák alkalmazását biztonsági feladatokban.
Test-before-invest tanácsadás	fél munkanap	Ezt a szolgáltatást olyan ügyfelek részére nyújtjuk, melyek új biztonsági megoldást szeretnének bevezetni rendszerükbe vagy szolgáltatásukba, és ennek megvalósítására több biztonsági technológiát is lehetségesnek tartanak és figyelembe kívánnak venni. Elvégezzük ezen biztonsági technológiák részletes elemzését, azonosítva előnyeiket és hátrányaikat, és összehasonlítjuk őket egymással. Ez az összehasonlító elemzés segíti az ügyfelet a megfelelő technológia kiválasztásában. Egy másik szinten ebben a szolgáltatásban olyan ügyfeleknek is tudunk segíteni, akik már felmérték a termékükkel, szolgáltatásukkal vagy informatikai rendszerükkel kapcsolatos biztonsági elvárásokat, rendelkeznek az elvárásoknak és biztonsági alapelveknek megfelelő tervvel, és kiválasztották a megvalósításhoz használni kívánt technológiát, de szükségesnek tartják egy ún. proof-of-concept megvalósítását és elemzését mielőtt komolyabb implementációba kezdenek. Egy proof-of-concept modellen a teljesség igénye nélkül lehet vizsgálni egy rendszer vagy szolgáltatás működését, és ez alapján eldönthető, hogy érdemes-e befektetni a valódi rendszer vagy szolgáltatás fejlesztésébe. Végül ebbe a szolgáltatásba tartozik az is amikor az ügyfél szeretné elvégezni egy már kifejlesztett komponens korai biztonsági tesztelését valamilyen valóshoz közeli működési környezetben. Ebben az esetben, segítünk kialakítani a megfelelő tesztkörnyezetet, definiálni a szükséges teszteseteket, és támogatjuk a tesztek végrehajtását és az eredmények értékelését. Ilyen módon az ügyfél megbizonyosodhat arról, hogy az új komponens integrálása a meglevő rendszerébe nem hordoz jelentős biztonsági kockázatokat. Egy másik szinten ebben a szolgáltatásban olyan ügyfeleknek is tudunk segíteni, akik már felmérték a termékükkel, szolgáltatásukkal vagy informatikai rendszerükkel kapcsolatos biztonsági elvárásokat, rendelkeznek az elvárásoknak és biztonsági alapelveknek megfelelő tervvel, és kiválasztották a megvalósításhoz használni kívánt technológiát, de szükségesnek tartják egy ún. proof-of-concept megvalósítását és elemzését mielőtt komolyabb implementációba kezdenek. Egy proof-of-concept modellen a teljesség igénye nélkül lehet vizsgálni egy rendszer vagy szolgáltatás működését, és ez alapján eldönthető, hogy érdemes-e befektetni a valódi rendszer vagy szolgáltatás fejlesztésébe. Végül ebbe a szolgáltatásba tartozik az is amikor az ügyfél szeretné elvégezni egy már kifejlesztett komponens korai biztonsági tesztelését valamilyen valóshoz közeli működési környezetben. Ebben az esetben, segítünk kialakítani a megfelelő tesztkörnyezetet, definiálni a szükséges teszteseteket, és támogatjuk a tesztek végrehajtását és az eredmények értékelését. Ilyen módon az ügyfél megbizonyosodhat arról, hogy az új komponens integrálása a meglevő rendszerébe nem hordoz jelentős biztonsági kockázatokat.