Értékelést megalapozó dokumentum

Jelen dokumentum részletes azonosítási adatokat tartalmaz a(z) .... (VE megnevezése) vonatkozóan, összegezve az alkalmazott követelményeket, vizsgálati módszereket és vizsgálati eredményeket.

1. Vizsgált eszköz azonosító adatai

VE megnevezése	
Modellazonosító	
Hardverkonfiguráció	
Futtatókörnyezet vagy operációs rendszer	
Firmware verzió	
Gyártó megnevezése	

2. Alkalmazott értékelési módszertan

Az értékelés az alábbi módszerek kombinációjával történt:

☐ Alkalmazhatósági vizsgálat

☐ Dokumentumalapú vizsgálat

☐ Koncepcionális vizsgálat

☐ Megvalósítási vizsgálat

☐ Sérülékenységvizsgálat

☐ Egyéb: _____

Az alkalmazott módszerek kiválasztása a vizsgálat megbízhatósági szintjével arányosan került meghatározásra.

3. Az önértékelés/megfelelőségértékelés adatai

3.1 Az értékelés céljának meghatározása

3.2 Az elvégzendő értékelési feladatok meghatározása

3.3 Az értékelés típusának meghatározása

☐ Megfelelőségi önértékelés
☐ Megfelelőségértékelő szervezet által végzett megfelelőségértékelés

3.4 Az értékelés megbízhatósági szintje

☐ Alap ☐ Jelentős ☐ Magas

3.5 Értékelési normatíva:
Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről szóló 10/2024 (VIII.8.) SZTFH rendelet.

3.6 Vizsgáló laboratórium által végzett tevékenységek

3.7 Értékelés időszaka

3.8 Értékelés eredményei

Például:

„Nem alkalmazható”: *akkor jelölhető, ha a VE vonatkozásában a követelmény nem értelmezhető, a VE fizikai kialakítása, tervezett funkciói és felhasználási területe a követelmény teljesítését nem teszi lehetővé.*

„Alkalmazható és teljesített”: *akkor jelölhető, ha a VE vonatkozásában a követelmény értelmezhető, és a VE a követelményt teljesíti*

4. Követelmények teljesítésének értékelése

4.1 Eszköz azonosítása

ESZKÖZAZONOSÍTÁS				
Eszközazonosítás				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
DEVID-1	Az IoT-eszköz modelljelölése egyértelműen felismerhető, akár az eszközön található címkén, akár egy fizikai interfészen keresztül.			
DEVID-2	Az IoT-eszköz egyedi, az eszközön található címkén vagy interfészen keresztül lekérdezhető logikai azonosítóval rendelkezik.			
DEVID-3	Távolról vezérelhető IoT-eszköz egyedi azonosítója és modelljelölése megállapítható.			
DEVID-4	Az IoT-eszköz lehetőséget biztosít egyedi fizikai azonosító hozzáadására, amelyhez az arra jogosult entitások hozzáférnek.			

Műveletvégzés				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
DEVOP-1	Az IoT-eszköz képes olyan műveletek végrehajtására, amelyek az eszköz azonosítása alapján vagy a felhasználásával előfordulhatnak.			
DEVOP-2	Az IoT-eszköz képes különbséget tenni azonosított és nem azonosított felhasználók között.			
DEVOP-3	Nem jogosult felhasználó által az egyedi logikai IoT-eszközazonosító nem megismerhető.			
DEVOP-4	Az IoT-eszköz azonosító ismeretében az aktuális szoftververzió ellenőrizhető.			
DEVOP-5	A hálózati eszközök azonosítása és kezelése céljából az eszközazonosító felhasználható az IoT-eszköz felderítésére.			

Eszközazonosítás támogatása				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
IDSUPP-1	Az IoT-eszköz képes arra, hogy más eszközök számára előzetesen azonosított entitásként hirdesse magát.			
IDSUPP-2	Más IoT-eszközök hitelességének ellenőrzése biztosított.			
IDSUPP-3	Az IoT-eszköz hálózati és távoli hálózati kapcsolat esetén az azonosított kapcsolat felépítése előtt kriptográfiai alapú, kétirányú azonosítást végez.			
IDSUPP-4	Az IoT-eszköz tanúsítványalapú azonosítást és hitelesítést támogat.			

4.2 Eszköz konfigurációja

ESZKÖZ KONFIGURÁCIÓJA				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
DEVCONF-1	A logikai hozzáférési jogosultságok beállítására, az IoT-eszköz konfigurációjára – Külső kapcsolatok, interfész-kontroll követelményeknek megfelelően – csak privilegizált felhasználókon keresztül nyílik lehetőség.			
DEVCONF-2	Csak arra jogosult felhasználók konfigurálhatják az IoT-eszköz azonosítási házirendjét és a hozzáférési korlátozási listákat a Külső kapcsolatok, interfész-kontroll követelményekkel összhangban.			
DEVCONF-3	Csak arra jogosult felhasználók konfigurálhatják az IoT-eszköz logikai és fizikai interfészeit a Külső kapcsolatok, interfész-kontroll követelményekkel összhangban.			

DEVCONF-4	Feljogosított felhasználók konfigurálhatják az IoT-eszköz szoftverbeállításait.			
DEVCONF-5	Feljogosított felhasználók az IoT-eszközt gyári állapotára visszaállíthatják.			
DEVCONF-6	Feljogosított felhasználók az IoT-eszközt valamely korábbi – a gyáritól eltérő – biztonságos állapotára visszaállíthatják.			
DEVCONF-7	Az IoT-eszköz szervizelése, javítása alatt vagy után a korábbi konfigurációs állapot biztosított.			

4.3. Adatvédelem

ADATVÉDELEM				
Kriptográfiai támogatás				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
CRYPT-1	Az IoT-eszköz megfelelő erősségű és hatékonyságú kriptográfiai algoritmust biztosít az adatok védelme érdekében.			
CRYPT-2	Az IoT-eszköz képes egyedi tanúsítványok érvényesítésére.			
CRYPT-3	Digitális aláírások ellenőrzése biztosított.			
CRYPT-4	Az IoT-eszköz képes Hash algoritmusok futtatására.			
CRYPT-5	A kriptográfiai algoritmusoknak és primitíveknek ajánlott verziókra frissíthetőek.			
CRYPT-6	Az eszköz forráskódja nem tartalmaz hard-coded kritikus biztonsági paramétereket.			

CRYPT-7	A szoftverfrissítések integritásának és hitelességének ellenőrzésére, valamint az eszközszoftverben a kapcsolódó szolgáltatásokkal folytatott kommunikáció védelmére használt kritikus biztonsági paraméterek eszközönként egyediek, és azokat olyan mechanizmussal állítják elő, amely csökkenti az automatizált támadások kockázatát.			

Kriptográfiai támogatás				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
CRYKEY-1	Az IoT-eszköz a kriptográfiai kulcsokat biztonságosan kezeli.			
CRYKEY-2	Az IoT-eszköz képes kulcspárok generálására.			
CRYKEY-3	Az IoT-eszköz a kriptográfiai kulcsokat biztonságosan tárolja.			
CRYKEY-4	Az IoT-eszköz a kriptográfiai kulcsok változtatását biztonságosan végzi.			
CRYKEY-5	Az IoT-eszköz a külső rendszerek által generált kriptográfiai kulcsokat ellenőrzi.			

Biztonságos tárolás				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
SECSTR-1	Az IoT-eszköz a jelszavakat nem tárolja – ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hash érték tárolást – és nem továbbítja.			
SECSTR-2	Biztonságos tárolás engedélyezhető az IoT-eszközön vagy annak interfészén keresztül.			
SECSTR-3	Gyári állapotban az adatok biztonságos, titkosított tárolása engedélyezett.			
SECSTR-4	A személyes adatok védelme a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelettel (általános adatvédelmi rendelet) összhangban biztosított.			

SECSTR-5	Az IoT-eszköz – ideértve az adatok elérését biztosító felhőinfrastruktúrát is – csak az üzemszerű működéséhez szükséges mennyiségű adatot tárolja.			
SECSTR-6	Az IoT-eszköz az adatokat képes lokálisan titkosítottan tárolni.			
SECSTR-7	Az IoT-eszközhöz kapcsolódó távoli rendszerelemek (pl. felhő) az adatokat titkosítottan tárolják.			
SECSTR-8	Érzékeny biztonsági paraméterek perzisztens tárolóban tárolódnak.			
SECSTR-9	A rendszer- és felhasználói adatok külön partíciókon helyezkednek el.			
SECSTR-10	Az adatok biztonságos mentése biztosított.			
SECSTR-11	Az IoT-eszközön lokálisan tárolt felhasználói adatok egyszerűen, visszaállíthatatlanul törölhetőek.			
SECSTR-12	Az IoT-eszközhöz kapcsolódó távoli rendszerelemek által tárolt felhasználói adatok egyszerűen törölhetőek.			

Biztonságos adatátvitel				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
SECDT-1	Az IoT-eszköz be- és kimeneti interfészein az adatáramlás biztonságos.			
SECDT-2	A biztonságos adatátvitel kriptográfiai algoritmusa konfigurálható.			
SECDT-3	Az IoT-eszköz rendelkezik a jogosulatlan hozzáférés és módosítás elleni védelemmel az adatkapcsolati közegben.			
SECDT-4	Az IoT-eszköz a továbbított és fogadott adatok integritását kriptográfiai megoldással ellenőrzi.			

4.4. Logikai hozzáférés az interfészekhez

LOGIKAI HOZZÁFÉRÉS AZ INTERFÉSZEKHEZ				
Azonosítás támogatása				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
AUTH-1	Az IoT-eszköz támogat authentikációs metódusokat.			
AUTH-2	Az IoT-eszköz a kapcsolatok felépítéséhez – kiemelten a távoli kapcsolatok esetén – authentikációs metódus megkövetelésére képes.			
AUTH-3	Az IoT-eszköz többfaktoros hitelesítési metódust támogat meghatározott felhasználói kör esetén.	sérülékenységvizsgálat		
AUTH-4	Ha az IoT-eszköz gyári alapértelmezett jelszavakat használ, azok eszközönként egyediek.			
AUTH-5	Az IoT-eszköz a gyári alapértelmezett jelszavak generálása során olyan generálási algoritmust alkalmaz, amely csökkenti az automata támadások kockázatát.	sérülékenységvizsgálat		

AUTH-6	A használatban lévő hitelesítési mechanizmusnak megfelelő hitelesítő azonosító megváltoztatása egyszerűen biztosított a felhasználó számára.			
AUTH-7	Az IoT-eszköz a hitelesítési folyamat során az adatokat elrejti.	sérülékenységvizsgálat		
AUTH-8	Az IoT-eszköz standardizált, egységes authentikációs metódust támogat (pl. SAML, OAuth2).	sérülékenységvizsgálat		
AUTH-9	Az IoT-eszköz távoli elérés esetén az authentikációs adatokat műveletenként ellenőrzi.	sérülékenységvizsgálat		
AUTH-10	Az IoT-eszköz a hitelesítési metódus feedbackjében található információk rejtett visszacsatolásával biztosítja, hogy a hitelesítési azonosítók illetéktelenek számára megismerhetővé, újrafelhasználhatóvá váljanak.	sérülékenységvizsgálat		

Azonosítás konfigurációja				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
IDENT-1	Az IoT-eszköz életciklusa során az authentikációs metódusok, szabályok és korlátozások beállíthatóak és változtathatóak.			
IDENT-2	Az IoT-eszköz a fiókkezelést automatizált módon támogatja.			
IDENT-3	A sikertelen azonosítási kísérletek száma konfigurálható, amely után az IoT-eszköz az adott felhasználót tiltja meghatározott, beállítható időtartam erejéig.			
IDENT-4	Az IoT-eszköz a sikertelen azonosítási kísérletek miatt tiltott felhasználói fiók visszaállítását alternatív azonosítási metódussal támogatja.			
IDENT-5	Az IoT-eszköz visszajelzést ad a legutolsó sikeres authentikáció időpontjáról.			
IDENT-6	Az IoT-eszköz az inaktív fiókok kijelentkeztetését támogatja, amelynek időtartama konfigurálható.			
IDENT-7	Az IoT-eszköz az ideiglenes felhasználói fiókokat konfigurálható módon, automatikusan tiltja.			

IDENT-8	Az IoT-eszköz a sikertelen belépési kísérleteket naplózza, amelyekről riport készíthető.			
IDENT-9	Az IoT-eszköz a sikertelen belépési kísérletek számát a következő sikeres bejelentkezés során jelzi a felhasználó számára.			
IDENT-10	Az IoT-eszköz a külső felhasználók és rendszerek authentikációját támogatja.	sérülékenységvizsgálat		
IDENT-11	A felhasználói fiókok, külső felhasználók és rendszerek hozzáférése visszavonható, amely esetében az IoT-eszköz a fennálló kapcsolatot bontja.			
IDENT-12	Az IoT-eszköz támogatja fiókok lejárati dátumának beállítását, amely lejárati dátumon túl az érintett fiók tiltásáról gondoskodik.			

Felhasználók értesítése				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
NOTIF-1	Az IoT-eszköz állapota ránézésre megállapítható státuszállapot-jelzők segítségével.			
NOTIF-2	Az IoT-eszköz kijelzőjén megjelenő információk konfigurálhatóak.			
NOTIF-3	Az IoT-eszköz képes a felhasználók számára (konfigurált módon) értesítéseket küldeni.			
NOTIF-4	Személyes adatokat tartalmazó, továbbá biztonsági értesítések teljes tartalma csak azonosítás után megismerhető, érzékeny adatok a figyelmeztető üzenetben nem jelennek meg.	sérülékenységvizsgálat		
NOTIF-5	Az IoT-eszköz által kijelzett, küldött üzenetek tartalma konfigurálható.			
NOTIF-6	Ha a figyelmeztető üzenet az IoT-eszköz kijelzőjén jelenik meg, az IoT-eszköz biztosítja, hogy az üzenet felhasználói interakcióig a kijelzőn maradjon.			

Hozzáférés-kezelés támogatása				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
ACCESS-1	Az IoT-eszköz a jogosulatlan műveleteknek ellenáll.	sérülékenységvizsgálat		
ACCESS-2	Az IoT-eszköz képes a felhatalmazott felhasználók és folyamatok (pl. csatlakozó rendszerek) azonosítására.			
ACCESS-3	Az IoT-eszköz különbséget tesz a feljogosított és nem feljogosított felhasználók között.			
ACCESS-4	Bizonyos, az üzemeltető által meghatározható funkciók azonosítás nélkül elérhetőek.			

Szerepkörtámogatás és -kezelés				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
ROLE-1	Az IoT-eszköz több típusú felhasználói fiók kezelésére képes.			
ROLE-2	Az IoT-eszköz elkülöníti legalább a következő típusú felhasználói fiókokat: személyhez kötött fiókok (általános és privilegizált), osztott privilegizált fiókok.			
ROLE-3	Az IoT-eszköz támogatja a felhasználói fiókok hozzáadását.			
ROLE-4	A felhasználói fiókokhoz szerepkörök rendelhetőek.			
ROLE-5	A felhasználói fiókok egyedi azonosítóval vannak ellátva.			
ROLE-6	Az IoT-eszköz szerepköralapú logikai hozzáférés-vezérlést végez.			
ROLE-7	Adminisztrátor felhasználó által a szerepkörökkel elérhető funkciók, folyamatok konfigurálhatóak.			
ROLE-8	A szerepkörök standardizált, egységes authorizációs metódusokkal kompatibilisek, a			

	megfeleltetés konfigurálható (pl. LDAPS).			
ROLE-9	Adminisztrátor felhasználó által új szerepkör konfigurálható.			
ROLE-10	Alapértelmezetten a szerepkörök a legkisebb jogosultság elve mentén kerülnek kialakításra.			
ROLE-11	Az audit naplókhoz és biztonsági beállításokhoz való hozzáférés-kezelés konfigurációja támogatott.			
ROLE-12	Az IoT-eszköz az egyes felhasználótípusokhoz korlátozó feltételek megadására biztosít lehetőséget (pl. időalapú korlátozás, IP-korlát).	sérülékenységvizsgálat		
ROLE-13	A szerepkörökhöz rendelt feljogosítók ellenőrzése a privilegizált funkciók és folyamatok elérésére irányuló felhasználói interakció esetén megtörténik.			
ROLE-14	Az egyes felhasználói fiókok esetén használt authentikációs metódusok konfigurálhatóak.			

ROLE-15	Osztott fiókok esetén konfigurálható fiókonként az egyidejű bejelentkezés engedélyezése (gyári állapotban tiltott).			
ROLE-16	Az IoT-eszköz képes előre beállított korlátozások érvényesítésére az eszköz használata során.			

Külső kapcsolatok, interfész-kontroll				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
INTCTRL-1	Az IoT-eszköz külső, 3rd party rendszerekkel való kapcsolatát biztonságos metódussal biztosítja.			
INTCTRL-2	Az IoT-eszköz komponenseinek használata korlátozható (portok, funkciók, be- és kimeneti eszközök).	sérülékenységvizsgálat		
INTCTRL-3	Azok a fizikai vagy logikai interfészek, amelyek nem szükségesek az IoT-eszköz működéséhez, tilthatóak.	sérülékenységvizsgálat		
INTCTRL-4	Gyári alapértelmezett állapotban csak a telepítéshez, beüzemeléshez minimálisan szükséges logikai és fizikai interfészek engedélyezettek.	sérülékenységvizsgálat		
INTCTRL-5	Gyári alapértelmezett állapotban az IoT-eszköz védelmet biztosít a biztonsági információk azonosítás nélküli kinyerése ellen.	sérülékenységvizsgálat		
INTCTRL-6	A fizikai interfészeket a hardver szükségtelen kockázatnak nem teszi ki.			

INTCTRL-7	Az IoT-eszköz szolgáltatásainak használata korlátozható.			
INTCTRL-8	A menedzsment felület elérésének külső hozzáférése tiltható.	sérülékenységvizsgálat		
INTCTRL-9	Az IoT-eszköz logikai interfészeinek elérése szabályozható.	sérülékenységvizsgálat		
INTCTRL-10	Az IoT-eszköz vezeték nélküli kapcsolatot támogat, amelynek biztonságos és engedélyezett authentikációs protokollja konfigurálható.	sérülékenységvizsgálat		
INTCTRL-11	Ha az IoT-eszköz rendelkezik debug interfésszel, az szoftveresen tiltott.	sérülékenységvizsgálat		

4.5 Szoftverfrissítés

SZOFTVERFRISSÍTÉS				
Frissítési képességek				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
UPD-1	Az IoT-eszköz szoftvere biztonságosan frissíthető a szoftver által biztosított módon vagy interfészen keresztül.			
UPD-2	A szoftverfrissítés azonosított, arra feljogosítással rendelkező felhasználói fiókkal végezhető el, biztonságos és konfigurálható mechanizmussal támogatva.			
UPD-3	Az IoT-eszköz szoftverének aktuális verziója lekérdezhető.			
UPD-4	Feljogosított fiókok a szoftvert korábbi szoftververzióra visszaállíthatják.	sérülékenységvizsgálat		
UPD-5	A szoftverfrissítések hiteles forrásból származnak, és ennek a feltételnek a teljesülését az IoT-eszköz ellenőrzi.	sérülékenységvizsgálat		

UPD-6	A szoftverfrissítések nem okozzák az IoT-eszköz kiberbiztonsági felkészültségének csökkenését, és ennek a követelménynek az ellenőrzésére az IoT-eszköz beépített metódussal rendelkezik.			

Frissítések kezelése alkalmazástámogatás által				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
UPDCTRL-1	Az IoT-eszköz a frissítések hitelességét és integritását ellenőrzi.			
UPDCTRL-2	Az IoT-eszköz automatikus frissítése kikapcsolható.			
UPDCTRL-3	Manuális és automatikus frissítési metódus támogatott.			
UPDCTRL-4	A frissítési metódus megválasztható.			
UPDCTRL-5	A szoftver állítható időközönként ellenőrzi új frissítés rendelkezésre állását.			
UPDCTRL-6	Újonnan megjelenő szoftververziókról az IoT-eszköz értesítést küld, amely funkció kikapcsolható.			
UPDCTRL-7	Újonnan megjelenő szoftververziókról az IoT-eszköz értesítést küld, az értesítendők köre konfigurálható.			
UPDCTRL-8	Az IoT-eszköz tájékoztatja a felhasználót arról, ha a frissítés az IoT-eszköz alapvető működésére kockázatot jelent.			

4.6. Eseménykezelés támogatása

ESEMÉNYKEZELÉS TÁMOGATÁSA				
Naplózás				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
LOG-1	Az IoT-eszköz képes események naplózására.			
LOG-2	Az IoT-eszköz külső naplózó rendszer kapcsolatot támogat.			
LOG-3	A naplóbejegyzések minimális tartalma a következő: az IoT-eszköz egyedi azonosítója, időjelzés, esemény forrása, esemény típusa, esemény besorolása, felhasználóazonosító vagy folyamatazonosító, esemény leírása.			
LOG-4	Az IoT-eszköz képes a hálózati kommunikáció naplózására.			
LOG-5	Az IoT-eszköz képes az eszközkonfiguráció változásainak naplózására.			
LOG-6	Az IoT-eszköz képes a sikeres és sikertelen hozzáférési kísérletek naplózására.			

LOG-7	Az IoT-eszköz képes a saját és szenzorai állapotának naplózására.			
LOG-8	A naplózható események listája alapján a naplózandó események konfigurálhatóak.			
LOG-9	Az IoT-eszköz állapota interfészen lekérdezhető.			
LOG-10	Az események maximális megőrzési ideje, a tárolt naplóesemények száma, illetve a naplóállomány maximális mérete beállítható.			
LOG-11	Az IoT-eszközön a megőrzési kritériumokon túli naplóállomány maradéktalan törlése biztosított.			

Időjelzés kezelése				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
TIMESTP-1	Az IoT-eszköz által naplózott események időjelzése legalább másodperc pontosságú.			
TIMESTP-2	Az IoT-eszköz NTP hálózati protokollt támogat.			
TIMESTP-3	Megbízható időforrás konfigurálható.			
TIMESTP-4	Az IoT-eszköz szabványos, UTC-re visszavezethető időjelzést használ.			

Eseménykezelés támogatása				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
INC-1	Az IoT-eszköz figyelmeztetést küld a biztonsági eseménynek tekintendő, konfigurált eseményekről.			
INC-2	Az IoT-eszköz figyelmeztetést küld a biztonsági eseménynek tekintendő, konfigurált eseményekről a kapcsolódó információs rendszerek felé.			
INC-3	A figyelmeztetés módja konfigurálható.			
INC-4	Az IoT-eszköz alternatív naplózási megoldást támogat az elsődleges naplózási mechanizmus kiesése esetére.			

4.7. Eszközbiztonság

ESZKÖZBIZTONSÁG				
Biztonságos kommunikáció				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
SECCOM-1	Más eszközökkel való kapcsolat kezdeményezése és lezárása biztonságosan történik.			
SECCOM-2	Az IoT-eszköz forgalomirányítási szabályok érvényesítésére képes.	sérülékenységvizsgálat		
SECCOM-3	Az IoT-eszköz a kommunikáció során standardizált protokollokat használ.			
SECCOM-4	Az IoT-eszköz IP-címe beállítható.			
SECCOM-5	Az IoT-eszköz interfészeinek portjai konfigurálhatóak.			
SECCOM-6	Az IoT-eszköz DNS-támogatással rendelkezik.			

Erőforrások biztonságos használata				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
RESRC-1	Az IoT-eszköz erőforrások megosztott használatára képes.			
RESRC-2	Az IoT-eszköz képes memóriaterületeket folyamatokhoz rendelni.			
RESRC-3	Az egyes folyamatok más folyamathoz rendelt memóriaterületet nem érnek el.	sérülékenységvizsgálat		
RESRC-4	A memóriaterület csak kernelen keresztül hozzáférhető.	sérülékenységvizsgálat		
RESRC-5	A memória hardveralapú hozzáférés-vezérléssel védett.	sérülékenységvizsgálat		
RESRC-6	A lemezhasználathoz kvóták rendelhetőek.			
RESRC-7	Hálózati kapcsolat elvesztése esetén korlátozott működés biztosított.			
RESRC-8	Az IoT-eszköz tömörített adattárolást támogat.			

Integritásvédelem				
Követelményazonosító	**Követelmény rövid leírása**	**Vizsgálati módszer**	**Eredmény**	**Indokolás/ Megjegyzés**
INT-1	Az IoT-eszköz egyedi, nem hiteles forrásból származó kód futtatása elleni védelemmel rendelkezik.	sérülékenységvizsgálat		
INT-2	Az IoT-eszköz rendelkezik a nem kívánt hardver- és szoftvermódosítás észlelési képességgel.	sérülékenységvizsgálat		
INT-3	Az IoT-eszköz az alapkonfiguráció biztonsági megfelelőségét ellenőrző funkcióval rendelkezik.	sérülékenységvizsgálat		
INT-4	Az IoT-eszköz integritás-ellenőrző funkcióval rendelkezik.	sérülékenységvizsgálat		
INT-5	Az IoT-eszköz a szoftverét biztonságos rendszerindítási mechanizmusok segítségével ellenőrzi.	sérülékenységvizsgálat		

INT-6	Ha az IoT-eszköz a szoftver jogosulatlan módosítását észleli, figyelmezteti a felhasználót, illetve a rendszergazdát a problémára, és nem csatlakozik a riasztási funkció végrehajtásához szükségesnél szélesebb hálózatokhoz.	sérülékenységvizsgálat		
INT-7	Az IoT-eszköz a rendszer fejlesztési életciklusa során manipuláció észlelésére képes.			
INT-8	A futtató környezet read-only adathordozón tárolódik.			

(A táblázat a 2. melléklet valamennyi releváns követelményére kitöltendő.)

5. **Vizsgálati eredmények összegzése**
6. **Sérülékenységi vizsgálat módszerének és eredményeinek ismertetése**
7. **Eltérések**
8. **Következtetés és javaslat**
9. **Rövidítések és szakkifejezések**

Készítette:

Kelt: