NKI CTI platformhoz való csatlakozás követelményei

DIMOP – Digitális Megújulás Operatív Program Plusz

Felhasználói és szakmai kézikönyv intézmények számára

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Összefoglaló

A DIMOP program informatikai fejlesztéseinek éles üzembe helyezésekor elvárás, hogy a részt vevő intézmény vizsgálja meg az NBSZ NKI (Nemzeti Kiberbiztonsági Intézet) Cyber Threat Intelligence (CTI) szolgáltatásához való csatlakozás lehetőségét, mely növelheti a szervezet kiberbiztonsági felkészültségét.

Jelen dokumentum összefoglalja azokat a műszaki és szervezeti követelményeket, amelyek teljesítése szükséges az NKI Cyber Threat Intelligence (CTI) platformjához való csatlakozáshoz. A követelmények teljesítését és a megvalósítás módját a fejlesztett alkalmazás éles üzembe helyezéséhez kapcsolódó szakmai beszámolót megelőző szakmai beszámolóban (a továbbiakban: előzetes szakmai beszámoló) kell bemutatni és igazolni.

A csatlakozás szükségességének vizsgálata

A csatlakozás szükségessége a projekt megvalósulása folyamán, az információbiztonsággal kapcsolatos elvárások pontos ismeretében az NBSZ NKI bevonásával tartott vizsgálat alapján kerül meghatározásra.

- **Felelős szerv:** NBSZ NKI.
- **Feladat:** az NKI szakemberei felmérik, hogy a DIMOP-projekt által fejlesztett rendszer kockázati profilja indokolja-e a CTI-adatszolgáltatáshoz való csatlakozást.
- **Teendő az intézmény részéről:**
    - Kapcsolattartó kijelölése (technikai és adminisztratív).
    - A projekt architektúrájának és biztonsági terveinek átadása a vizsgálathoz.

Képzési előfeltétel

Amennyiben az NKI a csatlakozást szükségesnek ítéli, **legalább egy kijelölt munkatársnak** el kell végeznie egy **CTI-tematikájú képzést**, amelyről tanúsítványt kell bemutatnia.

- **Elfogadható forma:** online vagy tantermi képzés, az igazolás elektronikus formában is benyújtható, a képzés minimum időtartama 1 munkanap, a képzésen minimálisan 1 fő részvétele szükséges.
- **Ajánlás:** bármely, nemzetközileg elismert CTI alap- vagy haladó tanfolyam (például STIX/TAXII alapok, fenyegetésfelderítés bevezetés) megfelel, nem szükséges konkrét, pl. SANS FOR578 vizsga.

Adatszolgáltatási lehetőségek

Az NBSZ NKI a CTI szolgáltatása révén a csatlakozó intézmény felé:

A. Automatizált módon adatot szolgáltat
B. Az intézmény számára rendszeres időközönként összegző CTI Riportot szolgáltat
C. Az intézmény számára eseti CTI riportot vagy információt ad át.

Automatizált adatszolgáltatás

Az adatszolgáltatás minden esetben szabványos STIX2.x állományokban kerül kiküldésre a szervezetek felé, az adatok továbbítása az alábbi csatornákon történhet:

E-mail alapú kézbesítés (minimális elvárás)

Az NKI CTI platform e-mailen keresztül küldhet figyelmeztetéseket és indikátorokat a csatlakozó intézmény számára.

- **Tartalom:** STIX 2.x formátumú indikátorok (IOC-k: IP-cím, domain, hash, URL, fájljellemzők).
- **Intézményi feladat:** kézi feldolgozás és betöltés a saját biztonsági rendszerekbe (SIEM, EDR, tűzfal, DNS-szűrő stb.).
- **Követelmény:** dokumentált, auditálható folyamat a beérkező e-mailek kezelésére, felelősök és határidők megjelölésével.

Automatikus átadás

Az NKI CTI platform Trusted Automated Exchange of Intelligence Information (TAXII) protokollon keresztül küldhet figyelmeztetéseket és indikátorokat (IOC-k: IP, domain, hash, URL, fájljellemzők stb.) a csatlakozó intézmény számára.

- **Protokoll:** TAXII 2.x + STIX 2.1.
- **Működés:** pull (időzített lekérdezés) vagy push (feliratkozás/webhook).
- **Előny:** automatikus frissítés, gyors reagálás.
- **Feltétel:** TAXII-klienssel és STIX-feldolgozással rendelkező rendszer, naplózás és verziótűrés.
- **Opcionális visszacsatolás:** saját észlelések megosztása az NKI felé sztenderd formátumban.

Hálózati és biztonsági követelmények

- **Előzetes egyeztetés** az NKI-val az IP-címek, tűzfalszabályok, proxy-beállítások engedélyezéséről.
- **Eseménynaplózás** minden tranzakcióról (sikeres/hibás lekérések, időbélyegek, rekordmennyiség).
- **Adatkezelés:** TLP (Traffic Light Protocol) címkék tiszteletben tartása, személyes adatok jogszabály szerinti védelme.
- **Hozzáférés-szabályozás:** szerepkör alapú (RBAC), naplómegőrzés.

Integráció és üzemeltetés

- **Feldolgozás:** STIX 2.x fájlok validálása, normalizálása, deduplikációja, védelmi eszközökbe való terítés.
- **Méretezés:** a rendszer képes legyen nagy mennyiségű adat periódikus feldolgozására.

- **Monitoring:** automatikus egészség-ellenőrzés (health check), hibajegykezelés, teljesítménymutatók.

Rendszeres vagy eseti CTI riportok

A csatlakozott intézmény **rendszeres (időszakos) vagy eseti (alkalomszerű)** CTI összefoglaló riportokat kérhet az NBSZ NKI-tól. Ezek a riportok az aktuális fenyegetettségi környezetet, észlelt támadási trendeket, releváns incidenseket és az intézményre vonatkozó kockázatokat tartalmazzák.

A riportok elkészítéséhez az intézménynek **Attack Surface információkat** kell megosztania az NKI-val:

- **Külső IP-cím tartományok** – minden, az internet felől elérhető IP-blokk.
- **Használt FQDN nevek** – a szervezet domain- és aldomain-nevei.
- **Email címek** – különösen a kulcsfontosságú hivatalos, incidenskezelésre, bejelentésre használt postafiókok.
- **Szervezet által használt szoftverek** – főbb szerver- és kliensoldali alkalmazások, verziókkal, amennyiben ismert.

Az így összegyűjtött adatok alapján az NKI célzottan tudja vizsgálni a nyilvános felületek sebezhetőségeit, és **személyre szabott riasztásokat** vagy összefoglalókat készít.

Dokumentációs követelmények az előzetes szakmai beszámolóhoz

Kötelező tartalom

- **Architektúra és adatáramlás:**
    - Csatlakozás célja, kiberbiztonsági indoklás.
    - Logikai és hálózati rajz (adatforrások, TAXII/STIX végpontok, hitelesítés, tűzfalszabályok).
    - Adatáramlási diagram a fogadástól a védelmi eszközökig.

- **Működési leírás:**
    - Fogadás → validáció → normalizálás → deduplikáció → terítés → visszavonás.
    - Üzemeltetés, karbantartás, incidenskezelés, változáskezelés.
- **Biztonsági kontrollok:**
    - Titkosítás, hitelesítés, hozzáférés-kezelés.
    - Naplózás, eseménykorreláció, audit.
    - TLP és adatminőségi szabályok.
- **Kapcsolattartás és felelősségek:**
    - Technikai és incidenskezelési kontaktok (24/7, ha indokolt).
    - Változtatás-bejelentés, konfigurációmenedzsment.
- **Mellékletek:**
    - Magas szintű architektúra terv (HLD).
    - Konfigurációs kivonatok (TAXII végpontok, ütemezések).
    - Mintaképernyők, naplórészletek.
    - Képzési igazolások.
    - Az Attack Surface adatok összefoglalója (külső IP-tartományok, FQDN-ek, e-mail címek, használt szoftverek)

Gyakori kérdések (GYIK)

Kötelező az automatikus adatátadás?

Nem, de erősen ajánlott. Minimálisan az e-mail alapú kézbesítést és a kézi feldolgozási folyamatot kell biztosítani.

Kell adatot küldenünk vissza az NKI felé?

Nem kötelező. A sztenderd alapú (STIX/TAXII) adatszolgáltatás lehetőségét célszerű megvizsgálni, értéket növelhet.

Milyen formátumokat támogassunk?

Fogadásra javasolt a STIX 2.1 és TAXII 2.x; a kompatibilitást és a hibakezelést dokumentálni szükséges.

Mivel igazoljuk a képzést?

Hivatalos tanúsítvánnyal/igazolással, amelyet az előzetes szakmai beszámolóhoz csatolni kell.

Kapcsolat

További egyeztetéshez kérjük, jelöljék ki a technikai és üzemeltetési kapcsolattartókat (név, e-mail, telefon), és küldjék meg az NKI részére az előzetes szakmai beszámoló benyújtása előtt.

Kérdés esetén keressen minket az alábbi elérhetőségeink egyikén!

Általános kérdések esetén:
titkarsag@nki.gov.hu

Hatósági kérdések esetén:
hatosag@nki.gov.hu

Incidensbejelentéssel kapcsolatos kérdések esetén:
csirt@nki.gov.hu

Csatlakozással kapcsolatos kérdések esetén:
edt@nki.gov.hu

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET