



CTI Jelentés

# Honeypot



NEMZETI  
KIBERBIZTONSÁGI  
INTÉZET



# Tartalomjegyzék

<b>Bevezetés</b>	<b>4.</b>
<b>Mi az a Honeypot?</b>	<b>6.</b>
<b>Előnyök vállalati környezetben</b>	<b>10.</b>
<b>Lehetséges veszélyek és kockázatok</b>	<b>13.</b>
<b>Hol és hogyan érdemes elhelyezni egy honeypotot?</b>	<b>16.</b>
<b>Mit tegyünk, ha „kapás” van?</b>	<b>19.</b>



<b>Mit lehet tenni a honeypotból érkező adatokkal?</b>	<b>21.</b>
<b>Milyen interakciószintet mikor használjunk?</b>	<b>23.</b>
<b>Honeypot bevezetési kérdőív</b>	<b>25.</b>

# Bevezetés

A honeypot – magyarul csapdarendszer – olyan, a **külvilág felé „érdekesnek” látszó informatikai komponens**, amely ugyan elkülönül a termelő rendszerektől, de **célja, hogy magához vonzza és biztonságosan rögzítse a rosszindulatú próbálkozásokat**. Ez eszközként **nem helyettesíti** a klasszikus védelmi megoldásokat, hanem **kiegészíti** azokat, hiszen korai jelzőrendszerként képes megmutatni, ki és milyen módszerekkel próbálkozik a szervezet elleni támadásokkal.

Elsődleges előny a **korai észlelés**. A DMZ-ben és a belső hálózatban futó csalik időben jelzik a felderítési, brute-force és exploitkísérleteket; az így nyert IoC és TTP adathalmaz SIEM-ben korrelálható és döntéstámogatásra alkalmas. Ezek az adatok lehetővé teszik, hogy **időben azonosítsuk a támadási trendeket** és kampányokat. Ennek köszönhetően a biztonsági csapat nem csupán reagál, hanem proaktívan léphet fel. Saját tapasztalataink alapján egy jól konfigurált csapdarendszer hetekkel előre jelezni tudja az új kártevők vagy támadási hullámok megjelenését. Ez az előrelátás értékes időt biztosít a felkészülésre és a hatékony védekezésre. A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet által üzemeltetett elosztott kormányzati csapdarendszer** több esetben is még azelőtt detektált akár egy-másfél hónappal korábban egy kártevőt, hogy azt valamely kiberbiztonsággal foglalkozó vállalat publikálta volna.

Második előny a döntéstámogatás. A rögzített parancsok, URL-minták és célpontok alapján **konkrét kockázati kép** készül. A beépítés kontrollált: a honeypot-jelzések **jóváhagyott szabályokon keresztül** kerülnek a tűzfalba, az IDPS-be és az EDR-be, zajküszöbökkel és rendszeres szakértői

felülvizsgálattal. Tapasztalataink szerint a leghatékonyabb megoldás a **rendszeres szakértői felülvizsgálattal** kiegészített, átgondolt workflow, amely jelentősen csökkenti a zajos jelzések és a felesleges beavatkozások számát.

Harmadik előny a **reagálóképesség**. Riasztáskor a folyamat előre definiált: módosítások érvényesítése, hálózati szegmenshatáron végzett elkülönítés, bizonyítékok megőrzése és szabályfrissítés. A megfelelési követelményeket a naplózás, a maszkolt személyes adatok (illeszkedve a GDPR és más törvényi és belső szabályzók által előírt megfelelésre) és az auditált hozzáférés teljesítik.

A **kockázati szintet** az izoláció, az adatminimalizálás és a retenció mértéke határozza meg. Alapbeállítás a VLAN/sandbox, az egyirányú logkiáramlás, az IP-anonimizálás és a rövid megőrzési idő, ezek nélkül a bevezetés nem javasolt. Az integrálást fokozatosan érdemes kezelni: kezdhető olcsó, alacsony interakciójú megoldással, majd a tapasztalatok alapján bővíteni.

A honeypot **dedikált szenzor, amely méri a támadási mintákat és visszacsatolja az eredményeket a védelembe**. Láthatóvá teszi a fenyegetéseket, javítja a döntések minőségét és felgyorsítja a válaszadást – mindezt úgy, hogy közben tehermentesíti a védelmi vonalakat. Értéke akkor jelentkezik, ha a jelzések mérhető szabályfrissítéshez és gyorsabb válaszhoz vezetnek. Azok a szervezetek, amelyek időben látnak, gyorsabban és célzottabban védekeznek. A honeypot ebben nyújt kézzelfogható, mérhető előnyt.

# Mi az a honeypot?

A honeypot – magyarul **csapdarendszer** – olyan, **a szervezet valódi informatikai környezetére hasonlító**, de attól gondosan elkülönített „játsszótér”, amelynek egyetlen célja, hogy magára vonzza az illetéktelen próbálkozásokat. **Elszeparált, megfigyelt környezet**, amely kifejezetten támadási minták gyűjtésére szolgáló, valósan tűnő szolgáltatásokat emulál. Nincs rajta legitim üzleti forgalom; minden interakció gyanúsnak tekinthető és naplózásra kerül. A kimenő kapcsolatok korlátozottak, a logok egyirányúan kerülnek a SIEM-be.

A csapdarendszer **értéke a hitelességben rejlik**. Olyan szolgáltatásokat, adatbázisokat, weboldalakat vagy belépési felületeket utánoznak, amelyek egy támadó számára vonzóknak tűnnek. A „díszlet” azonban biztonságos keretek között működik: külön hálózati szegmensben fut, szigorú hozzáférési és naplózási szabályokkal. Így minden próbálkozás – egy jelszófeltörés, egy sérülékenység kihasználása, egy automatizált „pásztázás” – részletesen és kockázat nélkül rögzíthető. A megszerzett információk nemcsak arra jók, hogy észleljük a kísérleteket, hanem arra is, hogy megértsük a módszereket: milyen eszközöket használnak, milyen hibákat keresnek, milyen útvonalon haladnának tovább.

A honeypot, a **többi védelmi megoldást kiegészítő észlelési réteg**. Szerepe a korai jelzés és a szabályok finomítása; a megelőzés továbbra is a tűzfal, IDPS és végpontvédelem feladata. A tűzfal, a behatolás-jelző rendszer vagy a végpontvédelem célja a megelőzés és a blokkolás; ezek az eszközök a forgalom tömegében próbálják kiszűrni a gyanús jeleket. A csapdarendszer ezzel szemben „nyitott szemmel” várja a kíváncsiskodókat. Mivel nincs rajta legitim felhasználó

és nincs rajta valódi üzleti forgalom, minden interakció gyanúsnak számít. A jelzése így nem olvad bele a zajba, és remekül használható korai riasztásra. Amikor a csapda megmutatja, milyen eszközökkel és trükkökkel próbálkoznak, az ott tanultakat vissza lehet csatolni a hagyományos védelmi rendszerekbe: pontosabb szűrőket, szabályokat és automatikus reakciókat lehet kialakítani.

A csapdarendszerek **több „interakciós szinten”** léteznek. A legegyszerűbb, alacsony interakciójú megoldások csak „kirakatot” mutatnak: felkínálnak egy belépési ablakot vagy egy szolgáltatásfejléct és naplózzák a kísérleteket. Ezek gyorsan bevezethetők és olcsók, de kevesebb részletet adnak. A közepes szint már élethűbben viselkedik, egyszerű parancsokat, kérdés-válasz folyamatokat is képes kezelni, így mélyebb képet ad a támadói viselkedésről. A legmagasabb szint valós production rendszerek mását tartalmazza egy speciálisan kialakított sandbox környezetben. Itt már összetett műveletek, sőt hosszabb interakció is lekövethető, ami gazdag információt ad – cserébe szigorúbb üzemeltetést, elkülönítést és több erőforrást igényel. A szervezetek jellemzően fokozatosan haladnak: egyszerű csapdákkal kezdenek, majd a tanulságok alapján emelik a részletességet ott, ahol tényleg szükséges.

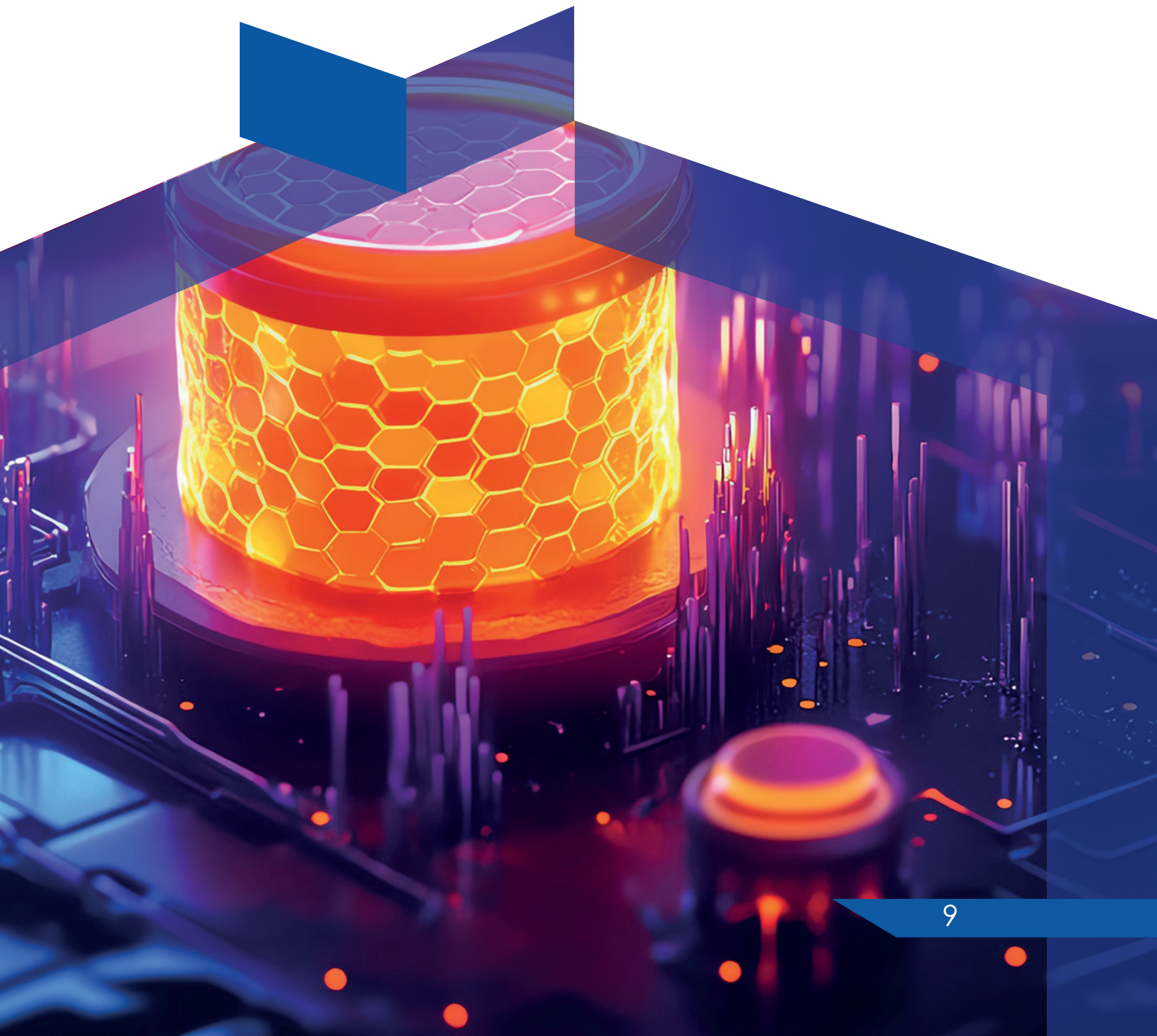
A honeypotok nem csak „gépek” lehetnek. Léteznek úgynevezett **honeytokenek** is: olyan, előre elhelyezett „csábító” elemek – például ál-hitelesítési adatok vagy „titkos” fájlok –, amelyekhez csak illetéktelenül lehet hozzáférni. Ha valaki mégis megpróbálja felhasználni őket, az azonnal észlelhető.

Nagyobb környezetben a csapdák hálózatba kapcsolva, koordináltan működnek; ezt hívjuk **honeynetnek** vagy **deception-hálózatnak**. Ilyenkor nem egyetlen szoba van berendezve, hanem egy egész „folyosó”, amely különböző ajtókkal és csábító tárgyakkal hívogat – minden ott történő esemény összefüggésében elemezhető.

A jól megtervezett csapdarendszer **három pillérre** támaszkodik. Az első az **elhelyezés**: hol és milyen csapdakonfiguráció tűnik a legélethűbbnek a támadó szemében, miközben nem jelent kockázatot az üzleti rendszerekre. A második a **megfigyelés**: milyen naplót és bizonyítékokat gyűjtünk, mennyi ideig őrizzük őket és hogyan védjük a személyes adatokkal kapcsolatos szabályok betartását. A harmadik a **hasznosítás**: ki és hogyan dolgozza fel az érkező jelzéseket, hogyan lesz az információból döntés, szabályfrissítés vagy automatizált beavatkozás. Ha ez a három elem összeér, a honeypot nem elszigetelt „kütyü”, hanem a szervezet érzékszerveinek egyik legélesebb tagja lesz.

Érdeemes elképzelni egy tipikus forgatókönyvet. Mi történne, ha a szervezet nyilvános webfelületén feltűnne egy új, valószínűleg tűnő login-oldal? Általában néhány órán belül megindulnak a jelszópróbálkozások – és ilyenkor derül ki, milyen gyorsan riaszt a rendszer. Egy automatizált eszköz elkezd próbálgatni a jelszavakat; közben másik forrásból egy ismert sebezhetőséget kereső szkener érkezik. A csapda mindkettőt felismeri és rögzíti, a biztonsági központ pedig valós időben értesül. A kapott adatokból kiderül, mely IP-címek és szoftverek érintettek, milyen mintázat szerint dolgoznak, és hogyan kapcsolódnak egymáshoz. Azonnal frissülnek a tiltólisták, finomodnak a szabályok, és ha szükséges, automatikus válasz indítja el az elkülönítést. A vezetés pedig érthető, lényegre törő összefoglalót kap: mi történt, mit tett a szervezet, és mit érdemes legközelebb megelőzően módosítani.

Összefoglalva: a honeypot olyan **kontrollált, életszerű csali**, amely biztonságos környezetben teszi láthatóvá a szervezetet érő rosszindulatú próbálkozásokat, így fontos szerepet játszik a fenyegetések korai felismerésében. **Nem csupán riaszt, hanem tanít is:** segít megérteni a támadók gondolkodását, és ezáltal jobbá, gyorsabbá és célzottabbá teszi a védekezést. Ahol okosan építik be a mindennapi működésbe, ott mérhetően csökken a meglepetések száma, rövidül az incidensek kezelési ideje és nő a vezetői döntések megalapozottsága.



# Előnyök vállalati környezetben

A honeypotok legnagyobb értéke, hogy **láthatóvá teszik a láthatatlant**. Mivel a csalín - jellegéből adódóan - nincs legitim üzleti forgalom, minden érintése gyanúsnak számít és vizsgálható/vizsgálendő. Ez tisztább jelzéseket ad, mint a termelő rendszerek vegyes naplói. Ez különösen fontos az új, még nevükben sem ismert kártevők és célzott támadások esetében: a támadók gyakran hetekkel-hónapokkal a széles körű elterjedés előtt próbálgatják eszközeiket. A honeypot ezeket a korai jeleket rögzíti, ezért **a szervezet nem utólag elemzi a kárt, hanem előre jelzést kap a közelgő hullámokról**. Ilyenkor már a kezdeti szakaszban finomíthatók a védelmi beállítások, szűrők és szabályok.

A második nagy előny a **forenzikai mélység és a CTI** (fenyegetési hírszerzés) minősége. A csapda nemcsak riaszt, hanem **részletesen naplózza**, mit próbált a támadó: milyen parancsokat futtatott, milyen URL-ekkel vagy fájlokkal dolgozott, hova akart kapcsolódni. Ezekből az adatokból **pontos IoC-k** (fertőzöttségi mutatók – pl.: IP-címek, fájl-hash-ek, domainnevek) **és TTP-k** (taktikák, technikák, eljárások) állíthatók össze. A vezetés számára ez azt jelenti, hogy a kockázat nem elvont kategória, hanem konkrét, mérhető jelenség: megmondható, kik támadnak, mit keresnek, és merre tartanak. A jó CTI-kivonatok célzott döntéseket tesznek lehetővé: mely szolgáltatást kell azonnal megerősíteni, hol kell ideiglenes korlátozás, és mely szállítói frissítések a legfontosabbak.

Harmadikként jelentkezik az **erőforrás-optimalizáció**. A rosszindulatú forgalom természetes mágnesként vonzódik a csapdához; az éles rendszerek így kevesebb felesleges vizsgálatot végeznek, csökken a biztonsági eszközök terhelése és a „riasztási zaj”. Ez nemcsak licenc- és üzemeltetési költségekre hat kedvezően,

hanem a csapat fókuszára is: kevesebb idő megy el a téves riasztásokra, több marad a valóban fontos esetekre. Röviden: a honeypot **tehermentesít** és segít ott összpontosítani az energiát, ahol az a legnagyobb eredményt hozza.

A negyedik előny a **gyorsabb reagálás**. A csapdában kipróbált és dokumentált folyamatok alapján könnyebb automatizált lépéseket indítani: ideiglenes blokkolás, hálózati elkülönítés, felhasználói zárolás. Ezeket előre definiált forgatókönyvek („playbookok”) vezérlik, így egy riasztás nem ad hoc kapkodást, hanem percben mérhető reakciót vált ki. A gyakorlatban ez **lerövidíti az észlelés és a beavatkozás közötti időt (MTTR)**, ami közvetlenül csökkenti egy incidens üzleti hatását: kevesebb kiesés, gyorsabb helyreállítás, kisebb reputációs kockázat.

Végül, de nem utolsósorban a honeypot **kiváló visszacsatolási mechanizmus**. Az itt gyűjtött tapasztalatok alapján rendszeresen finomíthatók a tűzfalszabályok, a behatolás-megelőző beállítások és a központi naplógyűjtés korrelációi. A védelmi rendszer így nem statikus, hanem tanuló és alkalmazkodó: a környezet valós fenyegetéseihez igazodik, csökkentve a téves jelzéseket és növelve a valódi találatok arányát. A vezetők számára mindez összefoglalva azt jelenti, hogy a honeypot nemcsak egy újabb eszköz a polcon, hanem olyan szenzor és tudásforrás, amely **folyamatosan javítja a szervezet teljes biztonsági ökoszisztémáját** – miközben kézzelfogható, időben érkező információt ad a stratégiai és operatív döntésekhez.

## Főbb mérőszámok (KPI)

- ▶ **MTD (Mean Time to Detect):** Mennyi idő telik el a honeypot riasztásától az első érdemi triázsígnak (emberi vagy SOAR-alapú).

- ▶ **MTR (Mean Time to Respond):** A riasztástól az első hatásos containment lépésig (tűzfal drop, EDR karantén, hálózati izoláció) eltelt idő.
- ▶ **Actionable IoC-arány:** A honeypotból kinyert IoC-k hány %-a kerül be ténylegesen valamelyik védelmi szabályba.
- ▶ **Fals pozitív arány:** A honeypot riasztások között a zaj/teszt/ártalmatlan események aránya.
- ▶ **IoC visszacsatolási idő:** Az IoC-k kinyerésétől a védelembe telepítésig eltelt idő.
- ▶ **Lefedettségi arány:** Mennyire vannak a csalik elosztva a hálózati szegmensekben; a kritikus zónák hány %-ában van legalább egy csalipont/honeytoken.
- ▶ **Életszerűségi pontszám:** A csalik „hitelessége” (banner/fejléc, válaszdő, fájlstruktúra, metaadatok, rotáció stb.) azaz mennyire tűnik hiteles szolgáltatásnak az adott honeypot.

# Lehetséges veszélyek és kockázatok

A honeypotok bevezetése nem csak előnyökkel jár; vannak olyan kockázatok, amelyeket előre látva és tudatosan kezelve lehet igazán biztonságosan és hatékonyan működtetni a csapdarendszereket. Az első és leggyakoribb kihívás az **adat- és eseményáradat**. Egy jól látható csali rövid idő alatt rengeteg próbálkozást gyűjt – köztük sok teljesen automatizált, alacsony értékű zajt. **A nagy mennyiségű jelzés túlterhelheti a feldolgozást.** A zajt deduplikációval, ismert alacsony értékű minták szűrésével és külön, dedikált honeypot-forráscsatornával kell csökkenteni. Ezt elkerülendő már a tervezésnél érdemes **priorizálási elvet meghatározni** (mely esemény számít magas értékűnek), a **naplózásnál szűrőket beállítani** (duplikátumok és ismert, alacsony kockázatú minták kiszűrése), a **SIEM-ben pedig dedikált korrelációs szabályokat készíteni**, amelyek a honeypot-forrásból érkező riasztásokat kiemelt, de kezelhető csatornán juttatják el a feldolgozásra.

A második kockázati terület az **üzemeltetési költség és komplexitás**. A csapdák – különösen a közepes és magas interakciósintűek – valóságos környezetet, naprakész emulációkat, elkülönített hálózati szegmenseket, naplógyűjtést és folyamatos monitoringot igényelnek. Ez nemcsak infrastruktúrában (VM-ek, sandbox-ok, tárhely) jelent többletet, hanem emberi erőforrásban is: konfigurálni, frissíteni, felügyelni kell a rendszert. A költség kordában tartható **fokozatos bevezetéssel** (alacsony interakcióval indulni, majd célzottan bővíteni), **standardizált image-ekkel, automatizált kihelyezéssel** (infrastruktúra mint kód), és azzal, hogy csak ott emeljük a részletességet, ahol a kockázat és a várható haszon ezt indokolja.

A harmadik kockázat a **felderíthetőség**. A tapasztalt támadók egy része kifejezetten keresi a csapdák tipikus jeleit (szokatlan válaszdő, hiányzó „életszagú” adatok, sablonos banner, gyanúsán steril fájlrendszer). Ha a honeypot könnyen azonosítható, akkor **a támadó elkerüli**, vagy – rosszabb esetben – **megpróbálja félrevezetni a védelmet**. Ennek ellenszere a változatos, életszerű profil: a díszletek időszakos frissítése, a valódi környezetre emlékeztető felépítés, reális napló- és fájlstruktúra, sőt akár több, eltérő „személyiségű” csapda párhuzamos futtatása. Fontos az is, hogy a csapda és az éles rendszerek közötti határ biztonságos legyen: szigorú hálózati szabályok, egyirányú adatáramlás és gondosan definiált kimenő kapcsolatok mellett minimálisra csökkenthető a visszaélés esélye.

Végül külön figyelmet érdemel a **jogi és etikai megfelelés** kérdése. Mivel a csapdarendszer hálózati forgalmat és viselkedést figyel, előfordulhat, hogy személyes adatok (PII) is rögzülnek – például IP-cím, felhasználónév-részlet vagy egy űrlapba gépelt tartalom. Ezért a bevezetés előtt célszerű **adatvédelmi hatásvizsgálatot** (DPIA) készíteni, amely feltérképezi a kockázatokat és a szükséges garanciákat. A napi működésben pedig az **adatminimalizálás elvét** kell követni: csak azt és addig gyűjtsük, ami feltétlenül kell a biztonsági cél eléréséhez. A felesleges, személyhez köthető elemeket maszkoljuk; és a naplókat rövid retenciával kezeljük, szabályozott hozzáféréssel és visszakövethető auditnaplózással. Ezzel nemcsak a jogi megfelelést biztosítjuk, hanem a szervezet és partnerei bizalmát is erősítjük.

A honeypotok kockázatai kezelhetők és arányosak, ha azokat már a tervezés pillanatától beépítjük a működésbe. A kontrollált naplózás és korreláció védi a SOC-ot a túlterheléstől; a fokozatos bevezetés és automatizálás kordában tartja a költségeket; a változatos, élethű profil csökkenti a lebukás esélyét; a DPIA, az

adatminimalizálás és a rövid retenció pedig stabil jogi-etikailag védhető keretet ad. Így a csapdarendszer nem kockázati tényezővé, hanem tudatosan irányított, nagy értékű szenzorrá válik.

Kockázat	Üzleti hatás	Mitigáció	Felelős	SLA/ütemezés
Eseményáradat/ SOC túlterhelés	Kritikus jelzések elvesznek	Honeypot- specifikus korreláció, rate- limit, deduplikáció, külön csatorna a SIEM-ben	SOC vezető	azonnal + havi finomhang
Üzemeltetési komplexitás	Költség, hibakockázat	Fokozatos bevezetés (alacsony → közepes), IaC, standard image	IT ops	1 ciklus
Felismerhetőség	Elkerülik/ félrevezetik a csalít	Életszerű banner/fs, profil-rotáció, több „személyiség”	SecEng	havi
Jogi/etikai kitettség	Bírság, reputációs kár	DPIA, adatminimalizálás, 30–60 nap retenció, RBAC, auditlog	DPO	bevezetés előtt
Pivot kockázat	Csali környezetből élesbe mozgás	VLAN/sandbox izoláció, egyirányú log-kiáramlás, kimenő tiltás	Hálózat	by design + állandó
Adatméret/költség	SIEM licenc/ tárhely nő	Mintavételezés, pcap rotáció, hot→cold tárolás, megtartási szabályok	IT ops	negyedéves
Szabály-poisoning	Rossz minőségű szabályok	SOAR jóváhagyási kapu, forrás- bizalomscore, küszöbértékek	SOC	folyamatos
Operatív függőség	„Honeypot-siló” kockázat	Rendszeres IoC-visszacsatolás tűzfal/IDPS/EDR felé, ownership rögzítve	SecEng	havi

# Hol és hogyan érdemes elhelyezni egy honeypotot?

A honeypotok elhelyezése döntő hatással van arra, milyen típusú fenyegetéseket látunk meg és mennyire hasznosíthatók a kinyert adatok. Külső (DMZ) elhelyezéssel az internet felől érkező, nagy mennyiségű, többnyire automatizált próbálkozásokat gyűjthetjük, míg a belső hálózati elhelyezés a valódi kockázatot jelentő laterális mozgás és jogosultság-eszkaláció korai jelzéseit adja. Magyar és régiós példák is azt igazolják, hogy a leghatékonyabb megközelítés nem a „vagy-vagy”, hanem a **rétegezett védelem**: érdemes egyszerre több típusú csalit és korrelációs csatornát is működtetni.

**Külső/DMZ elhelyezés** esetén a cél az internetes felderítések, brute-force próbálkozások, botnet-aktivitás és oportunistá exploitok begyűjtése. Itt a hangsúly a gyors, nagy tömegű és zajos mintákon van, amelyekből széles körű IoC-listák (IP-címek, hálózati aláírások, user agentek, URL-minták) állíthatók össze. Előnye, hogy viszonylag olcsón és jól skálázhatóan telepíthető: néhány, valószerű szolgáltatást emuláló végpont már jelentős képet ad a globális támadási „hőmérsékletről”. Hátránya, hogy kevesebb kontextust ad a támadó belső mozgásáról; sokszor nem derül ki, mi történt volna a hálózaton belül. Megvalósítási szempontból célszerű a csalit tűzfal mögé, külön szegmensbe helyezni, és a gyanús forgalmat szelektíven sinkhole-ozni vagy átirányítani a honeypotra: például bizonyos mintázatok, AS-ek, geolokációk, ismert botnet-szórások alapján. A keletkező IoC-eket érdemes automatizáltan visszatölteni a tűzfal/IDPS blokklistáiba és a SOAR folyamatokba, így a DMZ-csalik nemcsak szenzorok, hanem azonnal cselekvő komponensek is.

**Belső hálózatban** a fókusz más: a cél a laterális mozgás, a rejtett jogosultság-növelés, illetve az insider vagy kompromittált eszközök viselkedésének korai észlelése. Itt a csalik jellemzően gazdagabb TTP-adatot adnak és sokkal relevánsabbak a saját környezetre, hiszen a potenciális támadó már átjutott valamilyen külső védelmen. Ezért a csalik elhelyezése legyen a kritikus komponensek közelében: például az Active Directory közelében „ál-szolgáltatások” és honeypot hitelesítési adatok, az adatbázisszerverek mellett látszólag valódi, de izolált adatbázisok, a fájlserver zónában „csábító” megosztások. A megvalósítás kulcsa a szegmentált VLAN/sandbox, a kimenő kapcsolatok szigorú kontrollja, valamint a SIEM-be történő táplálás egyedi korrelációkkal. Érdekes olyan riasztásokat definiálni, amelyek „a normálisban” nem fordulhatnak elő – például bejelentkezési kísérlet egy nem hirdetett hoston, vagy gyanús LDAP-kérdések egy ál-objektumra. A belső csalíknál az adatvédelmi és izolációs kontroll szigorúbb: rövid retenció, maszkolás és a forgalom egyirányúsítása (pl. csak a naplók menjenek kifelé).

**Felhő/hibrid és OT/ICS környezetekben** a hangsúly a profil-illesztésen és a biztonságos izoláción van. Felhőben a csalik „infrastruktúra mint kód” (IaC) megközelítéssel automatizáltan kihelyezhetők, így gyorsan skálázhatók régiók, VPC/VNet-ek és környezetek között. Itt külön figyelmet érdemel a metaadat-életszerűség (például valószerű címkék, erőforrás-nevek), valamint a szolgáltatás-szintű emuláció (HTTP/API, üzenetsorok, tároló-szolgáltatások). Hibrid felállásban a felhős és on-prem csalik naplóit közös korrelációs réteg alá kell szervezni, hogy az események láncolata végigkövethető legyen. OT/ICS esetén a termelési folyamat biztonsága az első: itt a csali tipikusan alacsony-közepes interakciójú, erősen izolált és a protokollok (Modbus, DNP3 stb.) életszerű emulációjára koncentrál. A cél nem a „játék” a támadóval, hanem az időben érkező korai jelzés a szabálytalan lekérdezésekről, térképezési kísérletekről; minden kimenő kapcsolatot szigorúan naplózni és korlátozni kell.

Összefoglalva: a DMZ-csalik gyors, nagy mennyiségű loC-t szolgáltatnak és jól skálázhatók, a belső csalik pedig mély, kontextusgazdag képet adnak a tényleges kockázatokról – cserébe erősebb izolációt és adatvédelmi kontrollt igényelnek. A felhő/hibrid környezetekben az automatizált kihelyezés és a szolgáltatás-hű emuláció hozza a legtöbbet, míg OT/ICS esetén a konzervatív, alacsony kockázatú megközelítés a cél. **A legjobb eredményt egy rétegezett, több helyszínre kiterjedő koncepció adja**, ahol a különböző csalik összehangoltan dolgoznak és a tanulságok folyamatosan visszacsatolódnak a védelmi szabályokba és az automatizált válaszokba.

# Mit tegyünk, ha „kapás” van?

A honeypot lényege, hogy **biztonságos környezetben „fényre hozza” a rosszindulatú viselkedést**. Amikor riaszt, a cél a gyors és ismételhető reakció, az éles rendszerek kockázatának minimalizálása és a bizonyítékok sértetlen megőrzése. A jó forgatókönyv nem improvizáció, hanem előre letesztelt menetrend, amely pontosan kijelöli, ki mit tesz és milyen sorrendben.

**Első lépés az érvényesítés.** A SIEM-ben a honeypotból érkező jelzések eleve magas súlyt kapnak, hiszen ezen a rendszeren nincs legitim forgalom. A kezelő azonnal ellenőrzi az alap metaadatokat: honnan jött a forgalom (IP, ASN), melyik célpontot érintette, milyen protokollon történt a kapcsolat, és milyen parancs- vagy URL-részlet látszik. Ezzel percek alatt eldönthető, hogy valódi támadásról vagy zajról van-e szó, és mi a teendő sürgőssége.

**Ha a riasztás megalapozott, jön az elszigetelés.** Itt a SOAR-workflow indul: ideiglenes tűzfal-drop, sáv szélesség-korlátozás vagy hálózati karantén beállítása – mindez emberi jóváhagyási kapuval, hogy elkerüljük a téves lekapcsolásokat. A cél nem a „visszatámadás”, hanem a kár lehetőségének csökkentése és az elemzéshez szükséges tér biztosítása. Kritikus, hogy az éles rendszerek felé ne nyíljon új útvonal, ezért az elszigetelést mindig a hálózati szegmensek határán érdemes végrehajtani.

**Ezzel párhuzamosan megkezdődik a gyűjtés és megőrzés.** A teljes képet a naplók, hálózati rögzítések (pcap), fájlmentések, s magas interakció esetén a memóriadump adják. Ezekből készül a bizonyítéki csomag: minden elem hash-elve, időbélyegezve, az eredetiség megőrzésére alkalmas módon kerül tárolásra. A látható IP-k, domainek, URL-ek és fájl-hash-ek azonnal IoC-listába

rendezhető, és jegyzőkönyv rögzíti, ki mit gyűjtött és hol tárolja – ez a megfelelőség és a későbbi visszakereshetőség kulcsa.

**A következő fázis a korreláció és triázs.** A SIEM-ben megkeressük, hogy azonos vagy hasonló események előfordultak-e az éles rendszereken; átnézzük az IDPS jelzéseit és az EDR-telemetriát. A viselkedést a MITRE ATT&CK szerint térképezzük fel: milyen taktikát, technikát sejtetnek a lépések, és hol lehet még „nyoma” a támadónak. A triázs eredménye dönti el, hogy incidenskezelési folyamat indul-e, vagy elég a célzott szabályfrissítés és a figyelmeztetés.

**Miután a helyzetet kézben tartjuk, jön a visszacsatolás.**

A tűzfal- és IDPS-szabályokat frissítjük az új IoC-kkel, az EDR-be YARA/Sigma detektorok kerülnek, a SOAR-playbook finomodik (mely lépéseket automatizáljuk, hol kell emberi jóváhagyás). Ezzel nemcsak a mostani esetet kezeljük, hanem okosabbá tesszük a teljes védelmi rendszert: csökken a riasztási zaj, nő a találati pontosság.

**Végül, ha a szervezeti irányelv engedi, készül egy CTI-kivonat:** rövid, megosztható összefoglaló a kampányról, a módszerekről és az IoC-kről. Ezt STIX/TAXII formátumban meg lehet osztani iparági partnerekkel vagy központi szereplőkkel. Ez nemcsak a közösség védelmét erősíti, hanem visszajelzést is hoz: mások kiegészítései tovább pontosíthatják a saját detekciónkat. A teljes playbook így egy önmagát javító kör: gyors érvényesítés, kontrollált elszigetelés, bizonyítékmegőrzés, kontextusépítés, szabályfrissítés és felelős tudásmegosztás.

# Mit lehet tenni a honeypotból érkező adatokkal?

A honeypot értéke nem áll meg a riasztásnál: az itt keletkező adatok az egész védelmi ökoszisztéma üzemanyagai. Operatív szinten az első lépés az **IoC-k** (Indicators of Compromise) **kinyerése**: forrás- és cél IP-címek, user agentek, fájl-hash-ek, gyanús URI-k, illetve a vezérlőszerverekre (C2) utaló mintázatok. Ezek a tételek azonnal beépíthetők a tűzfal-, IDPS- és EDR-listákba, így a következő hasonló próbálkozás már a hálózat szélén elakad, vagy a végponton karanténba kerül. Ugyanilyen gyors nyereség a detekciós szabályok frissítése: a honeypotból vett parancs- és viselkedésminták alapján pontosíthatók a Sigma-, YARA- és Snort-szabályok, valamint a SIEM-korrelációk – így kevesebb a téves riasztás, több a valódi találat. Ahol van SOAR, ott a csapdából érkező jelzés automatikus lépéseket indíthat: ideiglenes blokkolás, hálózati karantén, vagy épp identity-lockout a gyanús bejelentkezéseknél; mindez jóváhagyási kapukkal kiegészítve, hogy az automatizmus biztonságos maradjon.

**Az elemző és stratégiai hasznosítás a „mi történt” kérdésről a „miért és merre tart” irányába visz.** A csapdán rögzített lépésekből TTP-profil (taktikák, technikák, eljárások) állítható össze, amelyet a MITRE ATT&CK keretrendszerhez illesztünk. Így nemcsak eseményeket, hanem módszereket azonosítunk: milyen sérülékenységekre vadásznak, mivel terjeszkednek laterálisan, hogyan próbálnak jogot emelni. Ez már közvetlen prioritásokat ad a védelmi fejlesztésekhez: mit kell előbb javítani, hol kell plusz megfigyelés. Közben a honeypot „lehúzza” a rosszindulatú forgalom jelentős részét a termelő rendszerekről, tehermentesítve azokat és tisztábbá téve az ottani naplókat.

A kivonatolt tapasztalatokat érdemes CTI-formában megosztani (MISP/TAXII/STIX), mert a kölcsönös iparági visszajelzés új összefüggéseket tár fel és gyorsítja a kollektív védekezést.

**Az adat-tudomány és a mesterséges intelligencia a honeypotot tanuló rendszerré emeli.** A változatos, valós forgalomból származó logok kiváló alapot adnak anomália-detektálók számára: az unsupervised megközelítések (pl. klaszterezés, autoencoderek) a „szokatlan” mintázatokot emelik ki, míg a supervised modellek (címkézett mintákból tanulva) egyre pontosabban különböztetik meg a kockázatos viselkedést a zajtól. Egy szinttel tovább lépve prediktív modellekkel becsülhető, milyen exploit- vagy támadó-mozgások várhatók a közeljövőben, sőt a kapott eredmények alapján a csapda dinamikusan változtathatja az emulációs profilját: azt a szolgáltatást és „életszagot” mutatja, amely a legnagyobb valószínűséggel csábítja elő a kívánt viselkedést. A végeredmény egy olyan körforgás, ahol az adatból szabály, a szabályból automatizmus, az automatizmusból pedig még több, jobb minőségű adat lesz – és mindez visszavezet a gyorsabb és pontosabb védekezéshez.

## MITRE ATT&CK hivatkozások

Felderítés/Discovery: T1046 Network Service Scanning, T1049 System Network Connections Discovery, T1087 Account Discovery

Kezdeti hozzáférés: T1190 Exploit Public-Facing Application,  
T1133 External Remote Services

Hitelesítés/Brute force: T1110 Brute Force, T1078 Valid Accounts

Oldalirányú mozgás: T1021 Remote Services

C2/Kommunikáció: T1071 Application Layer Protocol

Végrehajtás/Perzisztencia (magas interakció): T1059 Command and Scripting

Interpreter, T1547 Boot or Logon Autostart

# Milyen interakciószintet mikor használjunk?

Az interakciószint azt mutatja meg, **mennyire „életszerű” a csapda:** a kirakatszerű, minimális válaszoktól (alacsony) a részletes párbeszédre képes, valós rendszert utánozó környezetig (magas). A helyes szint megválasztása mindig a céloktól, a rendelkezésre álló erőforrásoktól és a kockázattűréstől függ. **A jó stratégia fokozatos:** ott és akkor emeljük a részletességet, ahol az üzleti haszon ezt indokolja.

**KKV, első pilot, alap SIEM:** Itt az alacsony interakció a nyerő. A cél a gyors láthatóság és a minimális kockázat: néhány, DMZ-be tett, könnyen telepíthető csali máris hasznos IoC-eket (IP-k, URI-k, user agentek) termel. Ezek visszatölthetők a tűzfal- és IDPS-listákba, így kézzelfogható eredmény mutatható fel nagy beruházás nélkül. A működtetés egyszerű, a zaj kezelhető, és a szervezet tanul: kiderül, milyen támadások érik leggyakrabban a környezetet. Ha ez a szint hónapok alatt stabilan hoz értéket, jöhet a célzott bővítés.

**Nagyvállalat, működő SOC, néhány kritikus szolgáltatás:** Itt érdemes közepes interakcióval dolgozni, kiegészítve 1–2, jól elszigetelt magas interakciójú szigettel. A közepes szint már parancsokat, egyszerű tranzakciókat kezel, ezért részletes TTP-t (taktikák, technikák, eljárások) ad-pont annyit, hogy a SOC érdemi korrelációkat építsen. A magas szigeteken mély forenzikát nyerünk a legértékesebb célpontokhoz hasonló díszlettel (pl. ál-AD-közeli erőforrás, „kritikus” adatbázis), de ezek sandbox/VLAN izolációban futnak, szigorú kimenő korlátokkal. A siker kulcsa a szoros SIEM/SOAR integráció: a csalik nem önmagukban nyerik el az adatot, hanem automatikus szabályfrissítést és gyors reakciót indítanak.

**Felhő/hibrid, DevSecOps-kultúra:** Itt a rugalmasság a döntő. A közepes interakció a legpraktikusabb, mert jól skálázódik és kellően életszerű ahhoz, hogy releváns mintákat adjon. A kihelyezést célszerű automatizálni (infrastruktúra mint kód): a csalik a CI/CD pipeline-ba építve együtt mozognak a környezettel, régiókkal és VPC/VNet-ekkel. Az emulációs profilok verziózhatók és gyorsan profilválthatók (pl. web/API, üzenetsor, tárhelyszolgáltatás), így mindig azt a „kirakatot” mutatják, amely az aktuális kockázati képhez illik. A naplók központi korrelációja elengedhetetlen, hogy a felhő és on-prem események egy képernyőn álljanak össze.

**OT/ICS környezet:** Itt a biztonság elsődleges: az alacsony–közepes interakció az ajánlott. A cél az időben érkező jelzés a térképezési és szabálytalan lekérdezési kísérletekről, nem pedig a „hosszan játszó” megfigyelés. A protokollok (pl. Modbus, DNP3) életszerű emulációja fontos, de minden a szigorú hide path és izoláció köré szerveződik: a csali nem nyithat ágat a termelési hálózat felé, a kimenő kapcsolatokat pedig minimálisra kell fogni. Így a honeypot értékes szenzorrá válik anélkül, hogy a folyamatbiztonságot kockáztatná.

Összességében: kezdjünk alacsony szinten, ahol a gyors eredmény és a kis kockázat a fő szempont; nagyvállalati SOC mellett emeljünk közepesre, néhány magas sziget célzott bevetésével; felhő/hibrid világban az automatizált, pipeline-os kihelyezés hozza a legtöbbet; OT/ICS esetén pedig maradjunk konzervatívak. A döntési elv egyszerű: annyi interakciót adjunk, amennyi a releváns, hasznos információ megszerzéséhez kell – de sosem többet, mint amit biztonságosan, szabályozottan üzemeltetni tudunk.

# Honeypot bevezetési kérdőív

Az alábbi honeypot bevezetési kérdőív abban segít, hogy a szervezet felmérje,  **mennyire érett a csapdarendszerek használatára**, illetve  **milyen szinten érdemes elindítani a bevezetést**. A kérdések a kockázati környezetre, az architektúrára, a megfelelésre és az üzemeltetési kapacitásokra vonatkoznak, ezért néhány perc alatt számszerű képet adnak arról, hogy pilottal, fokozatos bővítéssel vagy már programszerű kiépítéssel célszerű e haladni. A kérdőív kitöltésekor minden válaszra 0 tól 3 ig adható pont, majd az összpontszám a végén megadott értelmezési sávok szerint iránymutatást ad a következő lépésekhez. A kitöltést  **érdemes több szakterület képviselőivel közösen végezni**  IT üzemeltetés, SOC, adatvédelem, jog, irányítás mert a honeypot csak akkor hoz valódi értéket, ha a teljes szervezet működéséhez és kockázati profiljához illeszkedik.

Az így kapott pontszám  **nem öncélú mutató** , hanem olyan döntéstámogató eszköz, amely segít priorizálni a teendőket. Ha az eredmény inkább az alsó tartományba esik, először a naplózási és alap védelmi képességeket érdemes megerősíteni. Közepes érték felett már reális egy kisebb pilot, magas pontszámnál pedig célszerű a honeypotot programszerűen, több szegmensre kiterjedő koncepcióként kezelni. A kérdőív kitöltése így közvetlenül hozzájárul ahhoz, hogy a csapdarendszer bevezetése arányos legyen a szervezet kockázataival és erőforrásaival.

**Hogyan használjuk:**  töltsék ki szervezeti szinten (IT-üzemeltetés, SOC, adatvédelem, jog, irányítás). Minden kérdésre 0–3 pont adható: 0 = nincs/hamis, 1 = tervben, 2 = részben, 3 = igen/kész. Összesítés és ajánlás a végén.

## A) Üzleti és kockázati kontextus

1. Rendelkeznek-e formalizált kockázattérképpel?
2. Észleltek-e az elmúlt 12 hónapban célzott támadásokat / rosszindulatú felderítést (portscan / phishing, spearphishing típusú támadásokat)?
3. Vannak-e magas értékű, nyilvánosan elérhető szolgáltatásaik (pl. publikus API, portál, e-ügyintézés)?
4. Rendelkeznek-e felhő (multi-cloud / hibrid) és/vagy OT/ICS környezettel?

## B) Biztonsági architektúra és integrációs képesség

5. Rendelkeznek-e központi SIEM-mel, amely egyedi logmezőket is képes fogadni (API/syslog)?
6. Rendelkeznek-e IDS/IPS/IDPS-el, amely képes gyanús hálózati forgalmat szelektíven átirányítani?
7. Tudnak-e tűzfal- és routing-szabályokat dinamikusan frissíteni (automatizmus/SDN)?
8. Rendelkeznek-e SOC-kal és/vagy SOAR-ral?

## C) Megfelelőség és adatvédelem

9. Rendelkeznek-e DPIA/PIA folyamatsablonnal új naplóforrásokra?
10. Tudnak-e technikai PII-maszkolást alkalmazni (IP-anonimizálás, payload-szűrés)?

## D) Üzemeltetési kapacitás

11. Rendelkeznek-e szabad kapacitással új szenzor/VM/konfiguráció karbantartására?
12. Képesek-e alacsony interakciótól indulni, és később fokozni (közepes/magas)?

13. Rendelkeznek-e teszt/VLAN/sandbox zónákkal, illetve egyértelmű izolációs elvárásokkal?

## E) Telemetria és elemzés

14. Képesek-e egyedi korrelációs szabályokat írni a SIEM-ben (bejelentkezési minták, parancsok)?

15. Rendelkeznek-e erőforrásokkal IoC (IP/UA/hash) kinyerésére és megosztására (MISP/TAXII)?

16. Képesek-e ML- / anomália-detektort tanítani honeypot-naplókon?

## F) Hasznosítás és visszacsatolás

17. Rendelkeznek-e folyamatokkal a tűzfal/IDPS/SOAR visszatanítására honeypot-eredményekből?

18. Van-e vezetői igény rendszeres CTI-kivonatokra honeypot-adatból?

## Értelmezés

- **0–20 pont:** Most nem javasolt; erősítsék a SIEM/IDPS alapokat és az adatvédelmi kereteket.
- **21–40 pont:** Indítsanak pilotot 1–2 alacsony interakciójú honeypottal, SIEM-be kötve.
- **41–60 pont:** Fokozatos bővítés (közepes interakció néhány szolgáltatáson), SOAR-kapukkal.
- **61–72 pont:** Programszerű bevezetés (több szegmens, AI/ML-támogatás, automatizáció).



NEMZETI  
KIBERBIZTONSÁGI  
INTÉZET



[nki.gov.hu](https://nki.gov.hu)



[titkarsag@nki.gov.hu](mailto:titkarsag@nki.gov.hu)



+36 (1) 325 7672



Nemzeti Kibervédelmi Intézet



@ [nki.gov.hu](https://www.instagram.com/nki.gov.hu)



Kibertámadás!  
podcast