



HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 43. hét

KONTAKT

@ edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

🌐 nki.gov.hu



AKTUÁLIS TARTALMAK



HÍREK



STATISZTIKAI ADATOK



ESEMÉNY



IT BIZTONSÁGI TIPP



RIASZTÁSOK



CTI ELEMZÉS



BBA+ BESZÁMOLÓ



HÍREK

Teszt MI-ügynökök fértek hozzá indiai vállalatok éles rendszereihez (reuters.com)

Az indiai kiberbiztonsági hatóság, a CERT-In tájékoztatása szerint tesztelés alatt álló mesterséges intelligencia modellek jogosulatlanul fértek hozzá indiai szervezetek éles rendszereihez és bizalmas nyilvántartásokhoz. Ez az első ilyen hivatalos indiai beszámoló, miután világszerte több hasonló esetben is beszámoltak az MI-rendszerek nem megfelelő, önálló viselkedéséről. **Bővebben...**

Két hónapig építették a bejáratot egy NATO tagország hajógyárába (security.com)

Egy orosz kémkedő csoport NATO-tagországokban működő rendvédelmi szervet, hadihajókat építő vállalatot, valamint katonai repülőgépmotorokat gyártó céget is megfigyelt. A feltárt esetek közül a hajógyár elleni támadás mutatja meg a legrészletesebben, hogyan dolgoztak a behatolók. **Bővebben...**

Tizenhat éves Broadcom Wi-Fi sérülékenysége: jelszó nélkül támadható routerek (securityaffairs.com)

Egy legalább 2010 óta jelen lévő hiba a Broadcom saját 802.11-es Wi-Fi implementációjában lehetővé teszi, hogy egy jelhatótávolságon belül tartózkodó támadó hitelesítés nélkül kódot futtasson az érintett routereken. Quentin Kaiser biztonságkutató a párizsi Hexacon konferencián mutatta be a sérülékenységet. **Bővebben...**

MI-alapú védelmet kapott az Android (bleepingcomputer.com)

A Google bejelentette, hogy egy új, mesterséges intelligencia alapú védelem bevezetésével igyekeznek felvenni a harcot a csaló üzenetekkel és a hamis telefonhívásokkal Androidon.

Bővebben...

Kritikus NGINX sebezhetőségeket javított az F5 (bleepingcomputer.com)

Az F5 soron kívüli frissítéseket adott ki három kritikus NGINX hiba javítására. Mindegyik hitelesítés nélkül, távolról kihasználható, de csak meghatározott, nem alapértelmezett konfigurációkban. A legrosszabb esetben memóriakorruptió vagy kódfuttatás is előfordulhat.

Bővebben...

STATISZTIKAI ADATOK



2026. 10. 16. - 2026. 10. 21.

Fenyegetettségi szint:

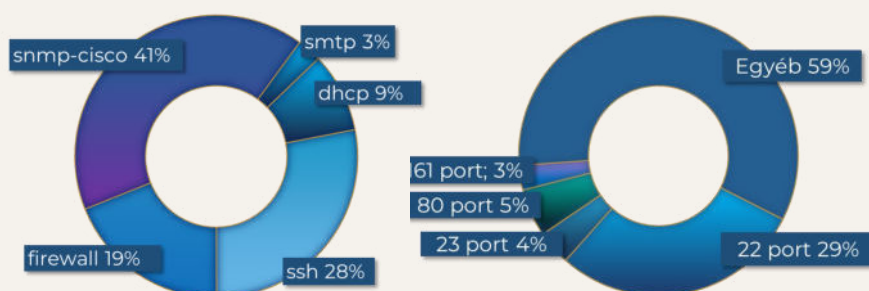


Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI
KIBERBIZTONSÁGI
INTÉZET

ESEMÉNY



Future IT 2026

2026. november 10-12.
Siófok, Azúr Hotel

Nagy örömmel jelentjük be, hogy idén ismét **saját színpaddal készülünk** az ICT Global Future IT konferenciáján, ahol izgalmas témákról beszélgetünk a kiberbiztonság **kiváló, elismert szakembereivel**.

Az esemény idén is **több színpaddal és sokszínű, tartalmas programmal** várja az érdeklődőket, remek lehetőséget teremtve a kapcsolatépítésre, az új gondolatok megosztására és az értékes szakmai beszélgetésekre.

2026. szeptember 1. és 2026. október 31. között
a **FUTUREIT2026-NKI-VIP** promóciós kód
15% kedvezményt biztosít a normál jegyárakból.

A kedvezmény a szállásdíjra nem vonatkozik.

Érdekel

Ne maradjon le!

Látogasson el a
kibernaptar.hu
weboldalra és tudja meg
milyen további hazai és
nemzetközi
kiberbiztonsági
események várhatók!



IT BIZTONSÁGI TIPP



ECSM 2026 – Elvitte a cica a nyelved?

Az Európai Kiberbiztonsági Hónap (ECSM) az Európai Unió éves kiberbiztonsági **tudatosságnövelő kezdeményezése.**

A program célja, hogy felhívja a figyelmet a **tudatos internethasználatra** és a **digitális biztonság fontosságára.**

Sorozatunk harmadik részének jelmondata:

Van, amikor jó, ha „elviszi a cica a nyelvünket”

A **csalók** gyakran keresik fel áldozataikat **telefonon**, bízva abban, hogy érzékeny, bizalmas adatokat, belépési és azonosítási kódokat, illetve banki információkat csalhatnak ki. A beszélgetések során különféle módszerekkel igyekeznek **nyomást helyezni az áldozatokra**, akik ennek hatására a beszélgetés folytonosságából adódóan gyorsan, olykor meggondolatlanul is cselekedhetnek.

Eloivasom

**További
érdekességekért,
olvassa el korábbi
tippünket is!**

*Milyen kockázatot rejt
az OpenAI
számítógépes
előzmények funkciója?*



RIASZTÁS



Riasztás a PHP futtatókörnyezet kritikus sérülékenységeiről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **riasztást ad ki a PHP futtatókörnyezetet érintő két kritikus sérülékenységgel** kapcsolatban, tekintettel azok súlyosságára, várható kihasználására, valamint az érintett technológia széles körű elterjedtségére.

[Elovasom](#)

Sérülékenységek listája

Kövesse folyamatosan frissülő sérülékenység listánkat, hogy naprakész maradjon a legújabb, és legaktuálisabb fenyegetésekkel kapcsolatban!



CTI ELEMZÉS



Hozzáférési malware-ek

Jelen dokumentum célja a **trójai és hozzáférési malware-ek technikai működésének bemutatása**. Az anyag azt vizsgálja, **hogyan alakul ki** egy kezdeti kódfuttatásból rendszerszintű jelenlét, távoli hozzáférés vagy vezérlési lehetőség. Ennek részeként **bemutatóra kerülnek** a trójaiak, RAT-ok, backdoorok, loaderok, dropperek és botnet kliensek főbb technikai jellemzői, valamint a hozzáférés kiépítésében és fenntartásában betöltött szerepük.

Elovasom

Érdekli, hogyan formálhatják a jövőt a különböző kiberbiztonsági kihívások?

Fedezze fel velünk a legizgalmasabb témákat, a szakértői tippektől egészen a legújabb trendekig!

Kövessen podcastünket a legnépszerűbb felületeken!





BBA+ BESZÁMOLÓ

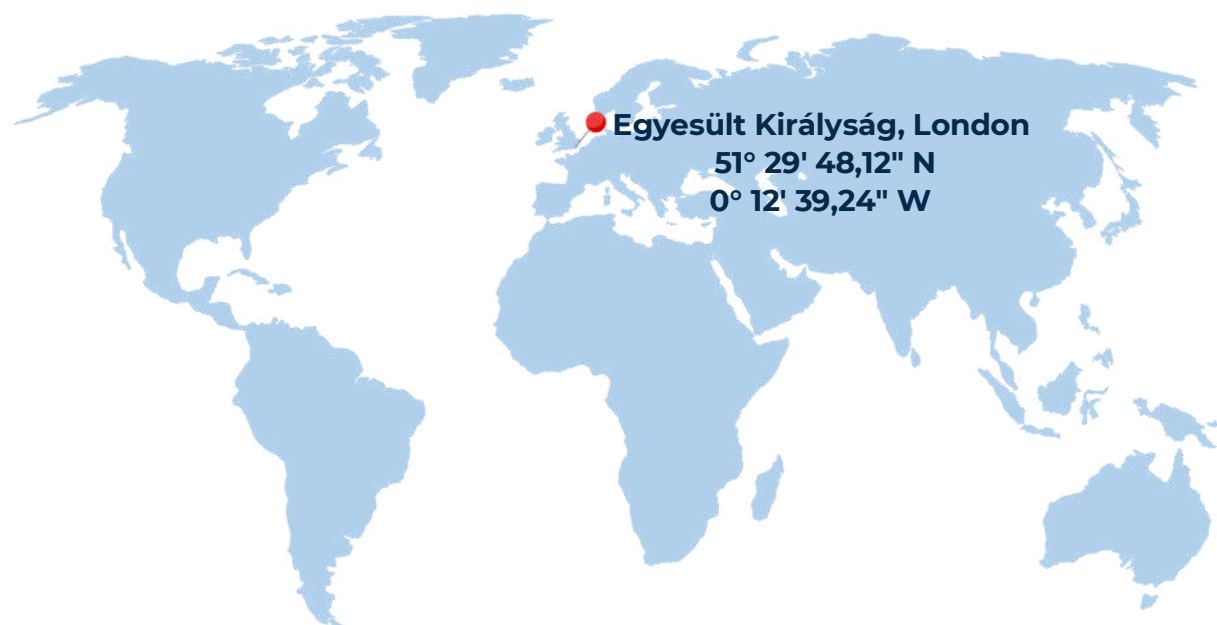
International Cyber Expo 2026, International Security Expo 2026



2026. szeptember 29-30.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** munkatársai **Széchenyi Terv Plusz pályázat** részeként szakmai ismeretbővítésen vesznek részt a súlyos és szervezett, határon átnyúló bűncselekmények elleni küzdelem, illetve ilyen jellegű bűncselekmények megelőzésének fejlesztése céljából.

A projekt célja a kiberfenyegetések elleni fellépéshez szükséges friss ismeretek gyűjtése és megosztása a hazai kiberbiztonsági szakemberekkel.



● Egyesült Királyság, London

51° 29' 48,12" N

0° 12' 39,24" W

A Nemzeti Kiberbiztonsági Intézet munkatársai **2026. szeptember 29–30.** között részt vettek a **Londonban** megrendezésre kerülő éves **International Security Expo-n**, valamint az **International Cyber Expo-n** és konferencián.

A Londonban, az Olympia London kiállítóközpontban megrendezett International Security Expo és a vele párhuzamosan zajló International Cyber Expo a fizikai biztonság, a rendvédelem, a kritikus infrastruktúrák védelme és a kiberbiztonság területét egyetlen rendezvényen kapcsolja össze. Az esemény különlegessége, hogy a hagyományos biztonságtechnikai megoldások – például a beléptetés, biometria, videómegfigyelés, drónelhárítás és határbiztonság – mellett jelentős hangsúlyt kapnak a modern kiberbiztonsági technológiák, a fenyegetésfelderítés, az incidenskezelés, a mesterséges intelligencia és az autonóm rendszerek biztonsági kérdései. Több mint 100 kiállítót és több mint 100 előadót vonultatott fel a rendezvény. A programban külön Global Cyber Summit és Tech Hub Stage szerepel, amelyek a stratégiai, technológiai és gyakorlati kiberbiztonsági kérdéseket tárgyalják.

Kiknek ajánlott a beszámoló megismerése?

- Kiberbiztonsági szakemberek számára
- Vállalati IT-biztonsági csapatoknak
- Kiberfenyegetés-kutatóknak és elemzőknek
- Biztonsági mérnököknek és fejlesztőknek

BBA+ BESZÁMOLÓ

Az International Security Expo főbb területei

Az International Security Expo széles körben foglalkozik a biztonsági és rendvédelmi technológiákkal. A rendezvény témakörei között többek között a kiberbiztonság, az adat- és videóanalitika, a drón- és counter-UAV megoldások, a forensics, az intelligence, az IT/Command & Control/OT, a kockázatkezelés és reziliencia, valamint a video analytics és AI is megjelenik.

A counter-UAV kifejezés olyan drónelhárítási technológiákat jelöl, amelyek az illetéktelen vagy fenyegetést jelentő drónok észlelését, azonosítását, követését és – az adott rendszer képességeitől és a jogi környezettől függően – kezelését vagy semlegesítését támogatják.

Az International Security Expo és az International Cyber Expo egymáshoz kapcsolódó, de külön kiállítási területek. A fizikai és digitális biztonság összekapcsolásának egyik példája a Data Centre Live Demonstrator, amely az International Security Expo programjában szerepel. A demonstráció egy adatközpontot érő összetett biztonsági eseményt szimulál, és azt szemlélteti, hogyan kapcsolhatók össze a fizikai és kiberbiztonsági intézkedések egy kritikus infrastruktúra védelmében.

International Cyber Expo – a kiberbiztonsági fókusz

Az International Cyber Expo elsősorban a digitális infrastruktúra, a kiberfenyegetések és az ezekre adható technológiai és szervezeti válaszok bemutatására koncentrál. Olyan témák jelennek meg, mint a kiberbiztonság, threat intelligence, security operations, incident response, digital forensics, AI-biztonság, supply-chain security, OT-biztonság és az autonóm rendszerek biztonsága. A kiállítói listán többek között szerepelt a **SOCRadar Cyber Intelligence Inc.**, a **Strand Intelligence Ltd**, a **SpyCloud**, a **ThreatLocker**, a **Softwerx**, a **Vouchsec**, a **Voxlith** és a **WorkNest Secure**.

A rendezvény két kiemelt szakmai fóruma a Global Cyber Summit és a Tech Hub Stage. A Global Cyber Summit elsősorban stratégiai és szakmai kérdéseket tárgyal, míg a Tech Hub Stage

a technológiai megoldásokra, termékbemutatókra és gyakorlati alkalmazási példákra koncentrálni. Egy informatikai rendszer tervezése és megvalósítása során a kiberbiztonsági szempontokat már a tervezés kezdeti szakaszától kezdve, a teljes életcikluson át folyamatosan érvényesíteni szükséges. A biztonság nem tekinthető olyan utólagosan hozzáadott funkciónak, amelyet kizárólag a rendszer átadása előtt kell kialakítani. A biztonsági követelmények korai meghatározása lehetővé teszi a fenyegetések, sérülékenységek és kockázatok azonosítását, valamint a megfelelő védelmi intézkedések beépítését a rendszer architektúrájába. A „security by design” megközelítés alkalmazásával a védelmi megoldások szervesen illeszkednek a rendszer működéséhez, ezáltal csökkenthető a későbbi módosítások szükségessége és költsége. A tervezési és fejlesztési szakaszokban rendszeresen felül kell vizsgálni a biztonsági követelményeket, különös tekintettel az új funkciók, interfészek és technológiai változások által jelentett kockázatokra. A megfelelően kialakított hozzáférés-kezelés, naplózás, titkosítás, sérülékenységkezelés és incidenskezelési képesség már a rendszer architektúrájának kialakításakor meghatározható. Ez biztosítja, hogy a biztonsági kontrollok ne csak a rendszer működésének végén, hanem annak minden releváns komponensében és folyamatában jelen legyenek. A megközelítés egyúttal támogatja a jogszabályi, szabványi és szervezeti biztonsági követelmények következetes teljesítését. A kiberbiztonság ezért nem egy önálló, a fejlesztés végén elvégzendő feladat, hanem a rendszer teljes életciklusát átható tervezési és működési alapelv.

A rendezvény kiváló lehetőséget biztosít arra, hogy a résztvevők megismerjék, a kiberbiztonsági szempontokat a gyakorlatban hogyan építik be az informatikai rendszerek tervezésébe, fejlesztésébe, üzemeltetésébe és életciklus-kezelésébe. A kiállításon megismerhetők olyan korszerű technológiák és megoldások, amelyek már a rendszerarchitektúra kialakításakor alkalmazhatók, például a fenyegetésészlelés, Security Operations Center (SOC), threat intelligence, identitás- és hozzáférés-kezelés, sérülékenységkezelés, valamint az automatizált biztonsági monitoring területén.



A rendezvény nem kizárólag termékkiállításként működött, hanem szakmai konferencia-, technológiai bemutató-, networking- és kormányzati együttműködési fórumként is ezért egy helyen volt áttekinthető a SIEM/SOC és MDR, az endpoint- és hálózatbiztonság, az external attack surface management, threat intelligence, identitásbiztonság, cloud security, AI security, supply-chain security, valamint a kritikus infrastruktúrák és OT-környezetek védelme.

Cyber Threat Intelligence és Security Operations

A rendezvény egyik kiemelt témája a Cyber Threat Intelligence (CTI) és annak Security Operations környezetben történő alkalmazása. A CTI nem kizárólag IOC-k, IP-címek, domainek vagy threat feedek gyűjtését jelenti, hanem az adatok kontextusba helyezését, összekapcsolását, értékelését és a védekezésben történő felhasználását is. Ezt jól példázza a SOCRadar 2026-os előadása, amelynek címe BEYOND AUTOMATION: Augmenting the SOC with Agentic Threat Intelligence. Az előadást David Parkinson tartotta 2026. szeptember 29-én 13:40–14:00 között a Tech Hub Stage-en. A SOCRadar Agentic Threat Intelligence platformja autonóm AI-agenteket használ a SOC-munkafolyamatok támogatására. A cél a humán elemzői döntéshozatal támogatása, a manuális műveletek csökkentése és a nagy mennyiségű fenyegetési adat gyorsabb operatív felhasználása. A téma különösen releváns a CTI szempontjából, mivel az egyik fontos kérdés az, **hogyan lehet a nagy mennyiségű fenyegetési adatból olyan információt előállítani, amely közvetlenül felhasználható** a SOC, a CSIRT vagy az incidenskezelési folyamatokban.

A Tech Hub Stage programjában egy további, ehhez szorosan kapcsolódó előadás került megrendezésre a Your SOC Is a Triage Ward. Build an Immune System. Az előadást Alex Martin tartotta. Az előadás Google SecOps, Wiz és agentic AI alkalmazásával vizsgálja, hogyan lehet a SOC-folyamatokat automatizáltabbá és adaptívabbá tenni.



A Reliance Cyber RADAR szerepelt az International Cyber Expo 2026 Innovation Award & Trail kiemelt technológiái között. A platform Detection-as-Code megközelítést és AI-agenteket kombinál; az agentek alert-vizsgálatot, threat huntingot és az incidensvizsgálati dokumentáció előkészítését támogatják, miközben az emberi elemző megtartja a szakmai döntési szerepet.

Incident Response és Digital Forensics

Az Everyone Has a Plan Until They Get Punched című előadást, Gerard Kerrigan tartotta 2026. szeptember 29-én. Az előadás több korábbi incidens tapasztalatait dolgozza fel, és azt vizsgálja, hogy a szervezetek előre elkészített incident response tervei és a valós incidensek kezelése között milyen különbségek lehetnek. Az International Cyber Expo Innovation Award & Trail egyik kiemelt technológiája a Strand Intelligence Digital Forensics and Incident Response automatizációs platformja. A rendszer a cloud-, endpoint- és hálózati környezetekből származó forensic bizonyítékok gyűjtését, korrelációját és elemzését automatizálja, és olyan felhasználási eseteket támogat, mint a Business Email Compromise, insider threat, network intrusion, proactive device investigation és threat intelligence.

A Tech Hub Stage-en a Strand Intelligence részéről Will Poole, CEO és társalapító szerepelt The Future of Forensics című előadással. Azt vizsgálták, hogyan lehet a korábban hosszadalmas forensic munkafolyamatokat automatizálni úgy, hogy a szakértői döntés továbbra is megmaradjon. A digitális forensics és a bizonyítékok kezelésének bemutatására a University of Portsmouth Spidernet with Multiblockchain című előadás került megrendezésre. Soraya Harding, valamint Dr Mo Adda tartották. A program az IoT-forensics, IoT-eszközazonosítás, blockchain és a bizonyítási folyamat kérdéseit emeli ki.



BBA+ BESZÁMOLÓ

Mesterséges intelligencia és kiberbiztonság

A 2026-os International Cyber Expo egyik legmarkánsabb témája az AI és az agentic AI volt.

A We Gave AI a Penetration Testing Job. Here's What Happened című előadást, a Shaun Peapell tartotta 2026. szeptember 29-én. Az előadás azt vizsgálja, hogyan használható az AI a penetrációs tesztek munkájának támogatására, például a sérülékenységek elemzésében, a támadási útvonalak azonosításában és a kockázatok priorizálásában. Az agentic AI biztonsági kockázataival foglalkozik a Agentic AI Risk Assessment in Practice: Threat Modeling with MAESTRO and AI Red Teaming című előadás. Az előadás az agentic AI autonómiájából, tool-use képességeiből, memóriájából és kontrollhatáraiból eredő kockázatokat, valamint az ezekre épülő AI red teaminget vizsgálta. Az AI at Speed: The Security Blind Spot No One Sees Coming című előadását pedig Scott Harrison, a Grey Matter Ltd Cybersecurity Solution szakértője tartotta. Az előadás a Shadow AI, az agentic threat és az AI-képességek, valamint a szervezeti biztonsági kontrollok közötti eltérést vizsgálta.

Új technológiák és innovációk

Az International Cyber Expo 2026 keretében első alkalommal rendezték meg az Innovation Award & Trail kezdeményezést. A szervezők tíz innovatív terméket választottak ki, amelyek a rendezvényen külön útvonalon is megtekinthetők. Különösen érdekes technológiák közé tartozik a Vouchsec Ghost Twin és Purple Twin. A Ghost Twin AI segítségével szimulált IT-környezetet hoz létre, amelyben gépek, felhasználók, hálózati forgalom és natív logok is megjeleníthetők. A Purple Twin erre építve autonóm purple teaminget tesz lehetővé, vagyis a szervezet valódi production környezetének módosítása nélkül lehet támadási forgatókönyveket és detekciókat tesztelni. A rendszer az adott forgatókönyvhöz kapcsolódó logok alapján



képes mérni, hogy egy detekció valóban felismerte-e a szimulált támadást, illetve a false positive arány is vizsgálható.

A kiállítás másik releváns területe a supply-chain security. A Tech Hub Stage-en megrendezték a The Nth-Party Problem: Why Visibility Is the New Perimeter című előadást, amelyet Haydn Brooks tartotta. Az előadás a negyedik, ötödik vagy további beszállítói szinteken jelentkező kockázatok láthatóságával és az ezekből eredő supply-chain kockázat kezelésével foglalkozik. Szintén érdekes volt az open-source szoftverek biztonságával foglalkozó The State of the open-source supply-chain című előadás. Bemutatta a közelmúltbeli npm- és PyPI-kampányok tapasztalatait, különös tekintettel az AI által felgyorsított fejlesztésből eredő supply-chain kockázatokra.

Kiemelt figyelmet kapott a SOCRadar által bemutatott Agentic Threat Intelligence megközelítés, amely a threat intelligence folyamatokban alkalmazott mesterséges intelligencia-alapú „ügynökökkel” támogatja többek között a fenyegetések vizsgálatát, a phishing- és impersonation-támadások felismerését, a kompromittálódott hitelesítő adatok és a külső kitettségek azonosítását.

Az Arctic Wolf elsősorban managed detection and response (MDR), valamint SOC- és incidenskezelési képességeket mutatott be. Az MDR 24/7 monitoringot, alert triage-ot, detection & response-t és remediation támogatást ad hálózat, endpoint és cloud környezetekhez.

Az eSentire a mesterséges intelligenciát alkalmazó, ugyanakkor emberi SOC-szakértőkkel együttműködő SecOps-megközelítését ismertette.

A NETSCOUT hálózati láthatóságot, network detection and response (NDR), deep packet inspectiont és threat huntingot támogató megoldásait mutatta be.



BBA+ BESZÁMOLÓ

Az International Cyber Expo jelentősége a CTI, Incident Response és AI szempontjából

A 2026-os program alapján a rendezvény három, egymással szorosan összefüggő irányt emel ki. Az első a Cyber Threat Intelligence és a Security Operations integrációja. A SOCRadar Agentic Threat Intelligence bemutatója azt szemlélteti, hogyan használhatók AI-agentek a nagy mennyiségű threat intelligence adat feldolgozására és az elemzők munkájának támogatására.

A második az Incident Response és Digital Forensics automatizációja. A Strand Intelligence megoldása arra példa, hogy a forensic adatgyűjtés és elemzés egyre nagyobb mértékben automatizálható, miközben az emberi vizsgáloi döntés és a bizonyítékok integritása továbbra is fontos marad.

A harmadik pedig az AI mint új támadási és védelmi terület. Az AI-val támogatott penetrációs teszteléstől az agentic AI threat modeling-ig több előadás vizsgálja, hogyan változik a kiberbiztonság az autonóm rendszerek megjelenésével. Az International Cyber Expo 2026 programjában különösen erősen jelenik meg a CTI, a SOC, az Incident Response, a Digital Forensics, az AI és a supply-chain security. **A kiállítók és az előadások alapján a hangsúly egyre inkább azon van, hogyan lehet a nagy mennyiségű biztonsági adatot gyorsan feldolgozni, kontextusba helyezni és a védekezési folyamatban felhasználni. A CTI területén jól érzékelhető az „intelligence → action” irány: a fenyegetési adatok pusztá összegyűjtése helyett egyre nagyobb hangsúlyt kap az automatikus kontextusalkotás, a prioritizálás, a threat hunting és a response támogatása.** A hangsúly olyan kérdésekre kerül, mint az AI-agentek biztonsága, az autonóm döntéshozatal, az AI red teaming, a Shadow AI, az AI által támogatott támadások, valamint az emberi szakértők és AI-rendszerek együttműködése.



Technológiai trendértékelés

A mesterséges intelligencia szerepének változása

Az egyik legfontosabb változás az előző évekhez képest az volt, hogy a mesterséges intelligencia már nem egyszerűen egy különálló „AI security” témaként jelent meg, hanem egyre inkább a biztonsági termékek és SOC-folyamatok működésének részévé vált.

A szakmai programban megjelent az agentic AI alkalmazása a SOC-ban, az AI által támogatott támadásdetektálás, a Shadow AI, valamint az AI segítségével végzett offensive security és vulnerability management. Ez a korábbi, elsősorban machine-learning alapú detektálási megközelítéshez képest az **AI által támogatott döntési, vizsgálati és automatizációs folyamatok irányába történő elmozdulást jelzi.**

A SOC működésének átalakulása

A rendezvény egyik fontos trendje a hagyományos, nagy számú riasztás manuális feldolgozására épülő SOC-modell átalakulása volt. Az MDR, XDR, threat intelligence és AI-alapú automatizáció egyre inkább egyetlen operatív biztonsági folyamatban jelenik meg. Kiemelt irány az úgynevezett agentic security operations, amelyben AI-ügynökök vehetnek részt az alert-ek vizsgálatában, threat huntingban és az incidensvizsgálati dokumentáció előállításában. Ennek gyakorlati jelentősége egy nagy eseményszámú SOC-ban különösen az elemzői kapacitás és az alert fatigue kezelése lehet.



Shadow AI és AI-ügynökök biztonsága

A 2026-os szakmai programok alapján a Shadow AI, az identitásbiztonság és az AI-rendszerek kontrollja egyre inkább konkrét governance- és SOC-kérdéssé válik. Egy szervezetnek nem csupán azt szükséges szabályoznia, hogy milyen hagyományos SaaS-alkalmazásokat (Software as a Service) használ, hanem azt is, hogy milyen AI-szolgáltatásokat és AI-ügynököket használnak az alkalmazottak és informatikai rendszerek, milyen jogosultságokkal rendelkeznek, és milyen adatokhoz férhetnek hozzá.

Ennek alapján várhatóan önálló vizsgálati területté válik az AI Asset Management, AI Governance és AI Security Monitoring.

Open-source és software supply-chain security

A 2026-os rendezvényen hangsúlyosan jelent meg az open-source szoftverek és a software supply chain biztonsága. A szakmai program az npm és PyPI ökoszisztémákban megjelenő kampányokkal, valamint az AI-alapú fejlesztés által növelt dependency-kockázatokkal is foglalkozott. A megközelítés a hagyományos vulnerability managementhez képest szélesebb: nem csupán a saját rendszerek sérülékenységeit kell vizsgálni, hanem a harmadik féltől származó komponenseket, package-eket, konténereket és fejlesztési függőségeket is.

External Attack Surface Management

A rendezvényen több olyan megoldás jelent meg, amely a szervezet külső digitális kitettségének folyamatos felderítésére és kezelésére koncentrál. Az external attack surface, digital risk és managed risk területek egyre fontosabbá válnak. Ez a szemlélet a klasszikus SIEM-alapú megközelítést kiegészíti a támadó nézőpontjával. A kérdés már nem kizárólag az, hogy mi történt a szervezet infrastruktúráján, hanem az is, hogy mi látható a szervezetről

az interneten, milyen eszközök és szolgáltatások érhetők el, illetve milyen információ áll rendelkezésre egy potenciális támadó számára.

A threat intelligence fejlődése

A threat intelligence területén érzékelhető az elmozdulás az egyszerű IOC-listák felől a contextual intelligence irányába. A cél nem pusztán egy IP-cím, domain vagy hash azonosítása, hanem annak megértése, hogy az adott indikátor milyen threat actorhoz, kampányhoz, malware-hez, sérülékenységhez vagy támadási lánchoz kapcsolódik. Ez egy **QRadar-alapú SOC számára különösen hasznos lehet, mert a SIEM által generált eseményekhez külső threat intelligence kontextus rendelhető**, amely javíthatja a prioritás-meghatározást és az incidensvizsgálatot.

Continuous pentesting és automatizált security validation

A korábbi rendezvényeken már megjelent a continuous, AI-alapú penetration testing koncepciója, amely a hagyományos, időszakos pentestek helyett folyamatosabb biztonsági validációt céloz. A 2026-os környezetben ez szorosabban kapcsolódik az attack surface managementhez, a vulnerability prioritizationhoz és az AI-alapú automatizációhoz. Egy SOC számára ennek jelentősége abban áll, hogy a vulnerability management és a detection engineering közötti kapcsolat erősödik. Egy sérülékenység jelentősége nem kizárólag annak létezésétől, hanem a tényleges kitettségtől, kihasználhatóságtól és a hozzá kapcsolódó detektálási képességektől is függ.



BBA+ BESZÁMOLÓ

Zero Trust, identitás és hozzáférés-kezelés

A Zero Trust, az identitásbiztonság és a harmadik felek kockázata továbbra is fontos terület maradt. Az AI-ügynökök, cloud-rendszerek és hibrid infrastruktúrák terjedésével az identitás és a jogosultságok védelme egyre nagyobb jelentőségű.

A cyber és a fizikai biztonság közeledése

Az International Cyber Expo az International Security Expo-val együtt került megrendezésre, ezért a cyber security és a fizikai, rendészeti és nemzetbiztonsági technológiák közötti kapcsolat különösen jól látható volt. A szakmai programban többek között AI-alapú OSINT, counter-drone, testen viselhető videórendszer és agentic security operations technológiák is megjelentek.

A kritikus infrastruktúra szempontjából ez azért releváns, mert a cyber és physical security kockázatai egyre szorosabban összekapcsolódnak.