CTI Jelentés

# A SIEM rendszerek működése

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
1996
Fortes fortuna adiuvat

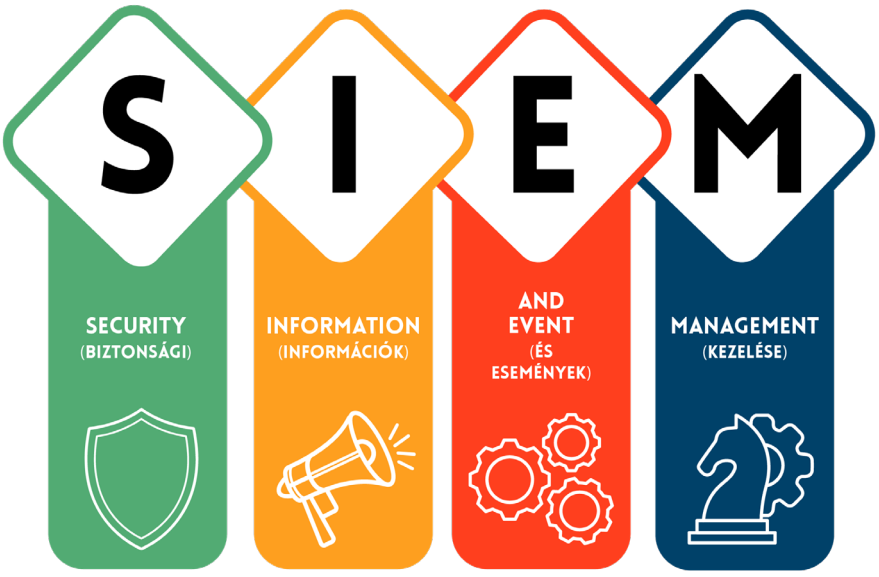
NEMZETI KIBERVÉDELMI INTÉZET

# Tartalomjegyzék

# Mi is az a SIEM?

A biztonsági információk és események kezelése (Security information and event management, röviden SIEM) olyan megoldás, amely segíti a szervezeteket a fenyegetések észlelésében és elemzésében, valamint az ezekre való reagálásban. A technológia, különböző forrásokból - például IDS/IPS - begyűjtött eseménynapló adatok és valós idejű elemzéssel azonosítja a szokatlan tevékenységeket, majd végrehajtja manuálisan vagy automatizáltan a megfelelő védelmi műveleteket.

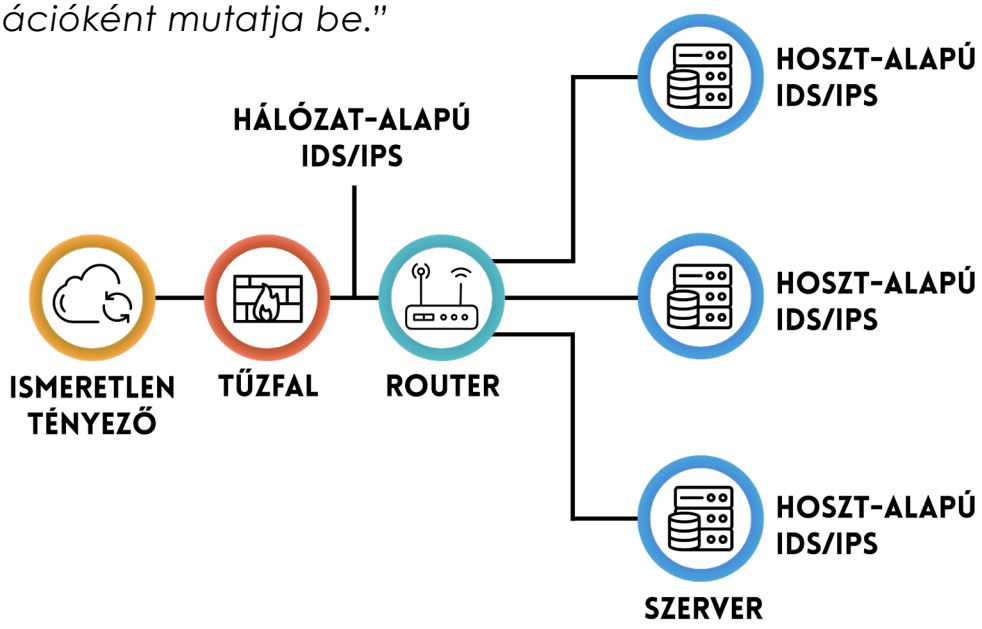
A **behatolásérzékelő rendszer (Intrusion Detection System - IDS)** olyan megoldás, amely figyeli a hálózati eseményeket és elemzi azokat a biztonsági incidensek és fenyegetések észlelése érdekében. A **behatolásmegelőző rendszer (Intrusion Prevention System - IPS)** olyan megoldás, amely a behatolásérzékelést végzi, majd egy lépéssel előrébb lép, és megakadályozza az észlelt fenyegetéseket.




1. ábra
**A "SIEM" mozaikszó jelentése**

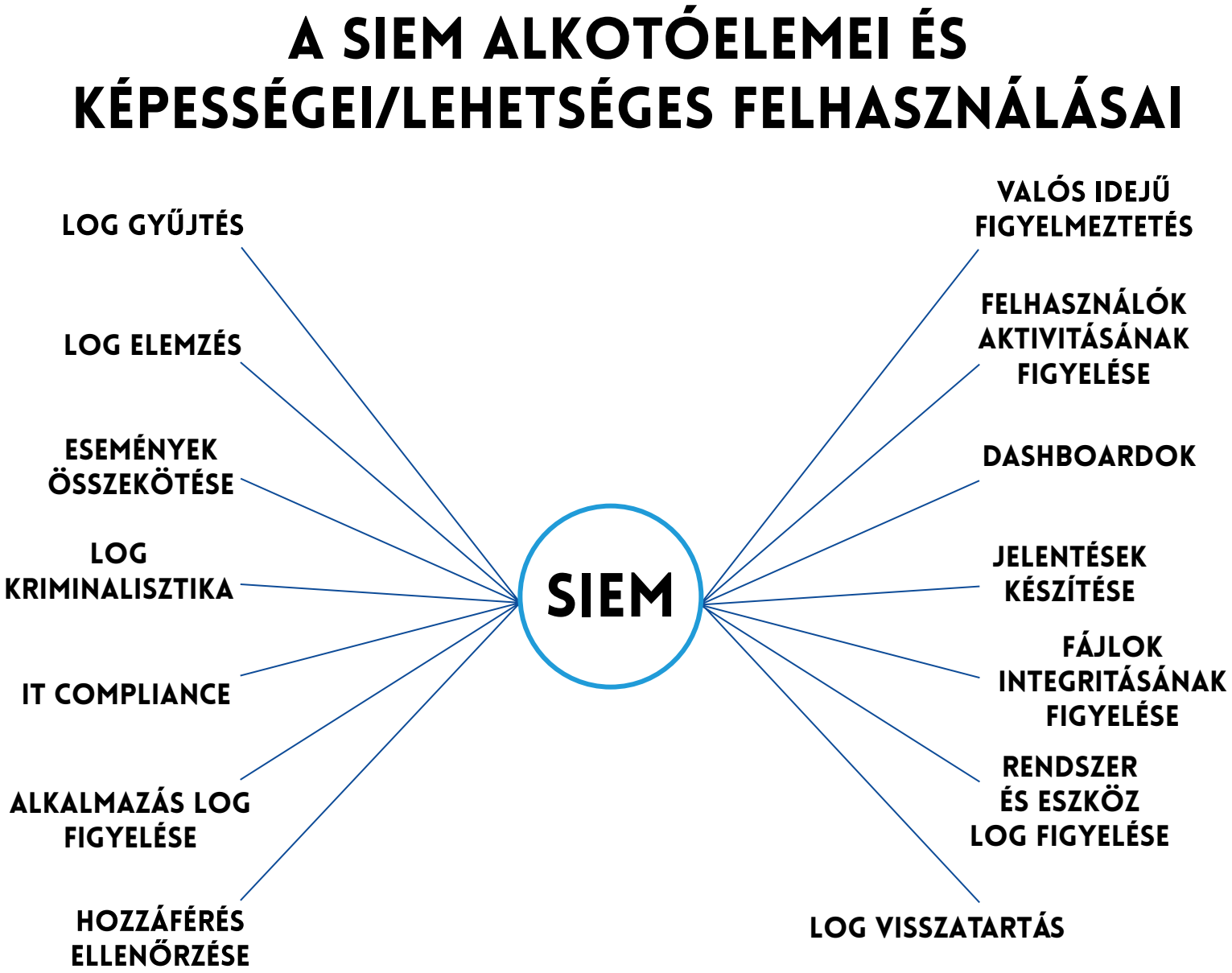
A SIEM és az IDS közötti fő különbség az, hogy a SIEM eszközök lehetővé teszik a felhasználó számára, hogy megelőző intézkedéseket tegyen a kibertámadásokkal szemben, míg az IDS csak az eseményeket észleli és jelenti.

A **National Institute of Standards and Technology (NIST)** a következő meghatározást adja a SIEM-re: *"Olyan alkalmazás, amely képes biztonsági adatok gyűjtésére az információs rendszer összetevőiből, és ezeket az adatokat egyetlen interfészen keresztül, cselekvőképes információként mutatja be."*




2. ábra
**IDS/IPS egy vállalati hálózaton**
*Forrás: spiceworks.com*

Az elmúlt évtizedben a SIEM technológia a mesterséges intelligencia segítségével intelligensebbé és gyorsabbá tette a veszélyforrások észlelését és az incidensek elhárítását. Tehát valós idejű elemzést nyújtanak az alkalmazások és a hálózati hardver által generált biztonsági riasztásokról. A gyártók a SIEM-et szoftverként, készülékként vagy menedzselt szolgáltatásként értékesítik.




3. ábra
**A SIEM rendszerek összetettsége**
*Forrás: nordcloud.com*

# Egy kis történelem

Az 1970-es évek végétől kezdve munkacsoportok alakultak, amelyek segítettek meghatározni az auditálási és felügyeleti programok irányításának kritériumait, valamint azt, hogy a rendszernaplókból mi és hogyan használható fel a bennfentes fenyegetések, az incidensekre való reagálás és a hibaelhárítás során. Ez egyúttal megteremtette a modern kiberbiztonságban ma is használt számos fogalom alapvitáját. A számítógépes biztonság ellenőrzésének és értékelésének alapja a **NIST 1977-ben kiadott 500-19-es speciális kiadványa**.

Mivel a **kockázatkezelési keretrendszereket** (**Risk Management Framework, röviden RMF**) világszerte szinte minden iparágban bevezetik, az auditálás és a monitoring az információbiztonság alapvető elemei. Az információbiztonsági személyzet, a kiberbiztonsági mérnökök és az elemzők a naplózási információkat felhasználhatják a kritikus biztonsági funkciók valós idejű végrehajtására. Ezeket az elemeket olyan irányítási modellek vezérlik, amelyek integrálják vagy használják az auditálást és a nyomon követést az említett elemző munka alapjaként. Ahogy az információbiztonság az 1990-es évek végén és a 2000-es évek felé haladva kiforrott, a rendszernaplókat központosítani kellett. Ez lehetővé teszi a feljegyzések központi elhelyezését és megtekintését, és egy adott hálózat összes gépének "idegközpontjaként" központi irányítást biztosít.

Az évszázad elején a SIEM-ek első hulláma (a ma már a Micro Focus tulajdonában lévő) **ArcSight** és a (ma az IBM tulajdonában lévő) **QRadar** volt. Ezek a korai SIEM-ek mind a naplófájlokat (nyers adatok), mind a biztonsági riasztásokat (események) egyesítették. Akkoriban arról szólt, hogy az összes használt kiberbiztonsági termékből - főként host- és hálózati alapú behatolásérzékelő eszközökből (ISS és társai), hálózati eszközökből és tűzfalakból (Check Point, Cisco és társai) - adatokat gyűjtöttek be és riasztásokat generáltak. A végpont- és vírusirtó szoftverek kicsit később következtek.

A SIEM akkoriban leginkább arra volt képes, hogy adatokat gyűjtsön, azokat összesítse, és riasztásokat küldjön a biztonsági csapatoknak. Emellett adatmegőrzésre is használták őket.

A legelterjedtebb első és második generációs SIEM-ek is nagyon egyszerű korrelációs motorokkal rendelkeztek. Képesek voltak szabályokat létrehozni, ami így működött: "*Ha X, Y és Z jelenséget látok, akkor nyissunk egy ügyet a jegyrendszerünkben, és küldjünk riasztást a biztonsági csapatnak*". Akkor még közel sem volt annyi adat, mint ma. Amit akkoriban generáltak, azt könnyen letárolták egy - általában Oracle vagy DB2 - adatbázisban. Idővel azonban az adatok mennyisége robbanásszerűen növekedni kezdett, de még mindig adatbázisokba kényszerítették. Végül a strukturált adatbázisok nem tudtak lépést tartani az IT biztonsági csapatokhoz érkező adatok mennyiségével, változatosságával és sebességével.



A **Splunkot** 2003-ban alapították, lényegében az első rugalmas és nagy teljesítményű tároló és keresőmotor a nagy adatokhoz. Bevezette az indexelést, amely bármilyen nyers adatot - a strukturáltól a strukturálatlanig - képes átkutatni, és az adatokat gyorsan kereshető eseményekké alakította át. A vállalat technológiája áttörést jelentett, mert a szervezetek számára sokkal egyszerűbbé tette a növekvő adatok bevitelét, keresését, tárolását, vizualizálását.

A Splunk architektúrája sokkal hatékonyabb volt, mint a régi gyártóké, és a vállalatnak sok éven át piaci előnye volt.

**2005**-ben Mark Nicolett és Amrit Williams, a Gartner munkatársai alkották meg a **SIEM** fogalmát. Ekkoriban terjedtek el robbanásszerűen a **nulladik napi** támadások. Ezek olyan számítógépes szoftverek sebezhetőségei, amelyek korábban ismeretlenek voltak a fejlesztők és a teszterek számára, míg a rosszindulatú szereplők felfedezték és ki is használták ezeket. Az Exabeam 2014-ben jelentette be UEBA termékünket a Splunk.conf felhasználói konferencián.

Ez idő tájt a legtöbb CISO és biztonsági csapat belefulladt az adatok tengerébe a túl sok biztonsági riasztás miatt, amelyek közül sok volt fals pozitív. Az UEBA és a riasztási triázseszközök jelentősen segítettek, de ez a probléma még ma is fennáll a hagyományos SIEM-ek esetében.

Napjainkban a hatékony SIEM-megoldások felhőalapúak, és mesterséges intelligenciát használnak a fenyegetések észlelésének, keresésének és megválaszolásának felgyorsításához. A felhő szupergyors, olcsó tárolást, azonnali keresést kínál és egyben integrál egy olyan fenyegetésérzékelő motort, amely képes elkapni a támadókat, azokat is, akik érvényes hitelesítő adatokkal törnek be.

2021. május 17-én az Egyesült Államok elnöke aláírta az **14028. számú**, **A nemzet kiberbiztonságának javításáról szóló végrehajtási rendelet**et. Ez előírja a végpontok védelmét, a naplózási követelmények további meghatározását, az ellenőrzési naplózás egységes módon történő végrehajtását, valamint a rendszer- és fiókműveletekre vonatkozó további betekintést biztosító képességek fejlesztését. Az ellenőrzési naplózást három különböző technikai területen azonosították, amelyek mindegyike az incidensekre való reagálással és azzal kapcsolatos, hogy tudjuk, mi történik egy adott rendszerben egy adott időpontban.

Ez a végrehajtási rendelet a kibertámadások növekedésére reagál, amelyek zsarolóvírusokat használnak a nemzetbiztonsággal és a nyilvánossággal kapcsolatos kritikus infrastrukturális elemek megbénítására. A meglévő információbiztonsági ellenőrzéseknek a kockázatkezelési keretrendszer részeként történő javítása megfelelő mechanizmus a megfelelés kikényszerítésére és az elnöki követelményeken alapuló finanszírozás igazolására.

# Hogyan működnek a SIEM-eszközök?

A SIEM-eszközök valós időben összegyűjtik, összesítik és elemzik a szervezet alkalmazásainak, eszközeinek, kiszolgálóinak és felhasználóinak számos adatát, hogy a biztonsági csapatok észlelhessék és blokkolhassák a támadásokat. A SIEM eszközök előre meghatározott szabályokkal segítenek a biztonsági csapatoknak a veszélyforrások azonosításában és a riasztások létrehozásában.

A SIEM rendszerek képességei eltérők, de általában ezeket az alapvető funkciókat kínálják:

- **Naplókezelés:** A rendszerek hatalmas mennyiségű adatot gyűjtenek össze egyetlen helyen, rendszerezik őket, majd megállapítják, hogy találhatók-e bennük veszélyforrásra, támadásra vagy biztonsági incidensre utaló jelek.

- **Eseménykorreláció:** Ezután az adatokat rendezve azonosítja a köztük lévő kapcsolatokat és mintázatokat annak érdekében, hogy gyorsan észlelhesse és megválaszolhassa a potenciális veszélyforrásokat.

- **Incidensek figyelése és elhárítása:** A technológia figyeli a biztonsági incidenseket a szervezet hálózatában, és riasztásokat küld, illetve auditálást végez az incidensekre vonatkozó összes tevékenységgel kapcsolatban.

A SIEM-rendszerek a számos különféle használati eset – például a gyanús felhasználói tevékenységek észlelése, a felhasználói viselkedés figyelése, a hozzáférési kísérletek korlátozása és a megfelelőségi jelentések létrehozása – révén mérsékelhetik a kibertámadásokat.

Összegezve a SIEM eszközök számos olyan előnyt biztosítanak, amelyek segíthetnek a szervezetek általános biztonsági állapotának megerősítésében, beleértve a következőket:

- Központi rálátás a potenciális fenyegetésekre
- A fenyegetések valós idejű azonosítása és elhárítása
- Speciális intelligens veszélyforrás-felderítés
- Jogszabályi megfelelés auditálása és jelentéskészítés
- Nagyobb átláthatóság a felhasználók, alkalmazások és eszközök figyelése révén


4. ábra
**Ábra az incidensek kezelésének folyamatáról**

# Egy SIEM rendszer implementálásának ajánlott eljárásai

A kisebb és nagyobb szervezetek egyaránt SIEM megoldásokat használnak a kiberbiztonsági kockázatok mérséklése, valamint a jogszabályi megfelelőségi szabványok (pl NIS2, vagy az EIR) előírásainak teljesítése érdekében. Az ajánlott lépései a következők:

- A SIEM üzembe helyezési követelményeinek meghatározása
- Tesztfuttatás
- Elegendő adat összegyűjtése
- Incidenselhárítási terv készítése
- A SIEM folyamatos továbbfejlesztése

A SIEM a szervezetek kiberbiztonsági ökoszisztémájának fontos része. Központi helyet biztosít a biztonsági csapatok számára a rengeteg vállalati adat összegyűjtéséhez, összesítéséhez és elemzéséhez, hatékonyan zökkenőmentessé téve a biztonsági munkafolyamatokat. Emellett olyan lehetőségeket is biztosít, mint amilyen például a megfelelőségi jelentések készítése, az incidenskezelés és a fenyegetésekkel kapcsolatos tevékenységeket rangsoroló irányítópultok.

# Képességek

01 · **Adatösszesítés**: A naplókezelés számos forrásból, többek között hálózatokból, , kiszolgálókból, adatbázisokból, alkalmazásokból származó adatokat aggregál, lehetővé téve a megfigyelt adatok konszolidálását, hogy elkerülhető legyen a kritikus események kihagyása.

02 · **Összefüggés**: Közös attribútumokat keres, és az eseményeket értelmes kötegekké kapcsolja össze. Ez a technológia különböző korrelációs technikák elvégzésére ad lehetőséget a különböző források integrálása érdekében, hogy az adatokból hasznos információkat lehessen kinyerni. A korreláció jellemzően a teljes SIEM-megoldás biztonsági eseménykezelési részének funkciója.

03 · **Riasztás**: A korrelált események automatikus elemzése.

04 · **Dashboardok**: Az eszközök képesek az eseményadatokat információs grafikonokká alakítani, hogy segítsenek a minták meglátásában, vagy a nem szabványos mintát alkotó tevékenységek azonosításában.

05 · **Megfelelés**: Az alkalmazások felhasználhatók a megfelelőségi adatok gyűjtésének automatizálására, a meglévő biztonsági, irányítási és ellenőrzési folyamatokhoz igazodó jelentések készítésére.

06 · **Megőrzés**: A múltbeli adatok hosszú távú tárolása az adatok időbeli korrelációjának megkönnyítése és a megfelelési követelményekhez szükséges megőrzés biztosítása érdekében. A hosszú távú naplóadatok megőrzése kritikus fontosságú a forensic vizsgálatok során, mivel nem valószínű, hogy a hálózati jogsértés felfedezése a jogsértés bekövetkezésének időpontjában történik.

07 · **Forensic elemzés**: A különböző csomópontok és időszakok naplóiban való keresés képessége meghatározott kritériumok alapján. Ez enyhíti azt, hogy a naplóinformációkat fejben kelljen összesíteni, vagy több ezer naplóban kelljen keresgélni.

# Mi a különbség a biztonsági információk kezelése (SIM) és a biztonsági események kezelése (SEM) között?

A SEM, SIM, SOAR, XDR stb. és SIEM rövidítéseket néha felváltva használják és általában a termékek eltérő funkciókészletére utalnak.

## Biztonsági információkezelés (SIM)

Az esemény- és tevékenységnapló adatok elemzés céljából való összegyűjtésének, tárolásának és megfigyelésének a folyamata. Ez egy szélesebb körű, hosszabb távú folyamat.

## Biztonsági eseménykezelő (SEM)

A biztonsági események és riasztások valós idejű megfigyelésének és elemzésének folyamata a fenyegetések kezelése, a mintázatok azonosítása és az incidensek elhárítása érdekében. A SIM-mel ellentétben ez a megoldás alaposan megvizsgálja azokat az eseményeket, amelyek valós veszélyt jelenthetnek.

## Biztonsági információ- és eseménykezelés (SIEM)

Egyesíti a SIM-et és a SEM-et, és valós idejű elemzést biztosít a hálózati hardver és alkalmazások által generált biztonsági riasztásokról.

## Managed Security Service (MSS)

Vagy másnéven **Managed Security Service Provider (MSSP)** a leggyakoribb menedzselt szolgáltatások, azaz a csatlakoztathatóság és a sávszélesség, a hálózatfelügyelet, a biztonság, a virtualizáció és a katasztrófa utáni helyreállítás körül alakulnak ki.

## Biztonság mint szolgáltatás (SECaaS)

Ezek a biztonsági szolgáltatások gyakran tartalmazzák többek között a hitelesítést, a vírusirtást, a rosszindulatú programok/kémszoftverek elleni védelmet, a behatolásérzékelést, a behatolásvizsgálatot és a biztonsági események kezelését.

A gyakorlatban sok termék ezen a területen e funkciók keverékével rendelkezik, így gyakran lesz némi átfedés - és sok kereskedelmi forgalmazó saját terminológiáját is népszerűsíti. A naplókezelés önmagában nem nyújt valós idejű betekintést a hálózati biztonságba, a SEM **önmagában nem nyújt teljes körű adatokat a mélyreható fenyegetéselemzéshez**. A SEM és a naplókezelés kombinálásával több információ áll rendelkezésre a SIEM számára a megfigyeléshez.

## SOAR

A **SOAR** a biztonsági vezénylés, automatizálás és helyreállítás rövidítése (security orchestration, automation, and response). Az elnevezés azokat a szoftvereket takarja, amelyek a fenyegetések és biztonsági rések kezelésével, a biztonsági incidensek elhárításával és a biztonsági műveletek (SecOps) automatizálásával foglalkoznak.

A SOAR az **incidenselhárítás munkafolyamatainak automatizálásával** segít a biztonsági csapatoknak a SIEM által létrehozott fenyegetések és riasztások rangsorolásában. Emellett széles körű, az összes tartományra kiterjedő automatizálás révén segít gyorsabban megtalálni és elhárítani a kritikus fenyegetéseket. Rengeteg adatból szűri ki és jeleníti meg a valós fenyegetéseket, és reagál az incidensekre.


5. ábra
**A SOAR mozaikszó jelentése**

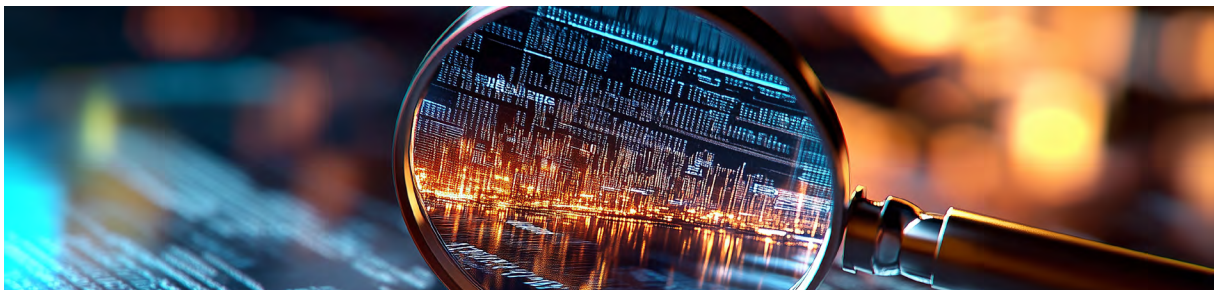
## XDR

Az **XDR**, kiterjesztett észlelés és válasz (**Extended Detection and Response**) a fenyegetések észlelésének és elhárításának javítását szolgáló teljesen új kiberbiztonsági megközelítés, amely részletes környezetfüggő adatokat biztosít bizonyos erőforrásokról. A támadásokat az adott erőforrásokkal kapcsolatos adatok ismeretében vizsgálhatja meg a platformokon és a felhőben, minden végpontra, felhasználóra, alkalmazásra, IoT-re és felhőbeli számítási feladatra vonatkozóan egységesen.

Megvédi az erőforrásokat, és megerősíti a biztonsági állapotukat a fenyegetések – például a zsarolóvírusok és az adathalászat – elleni védelem érdekében. Automatikus szervizeléssel gyorsabban reagál a fenyegetésekre. Ezek kombinációjával válik a SIEM **a szervezeten belüli biztonsági problémákkal foglalkozó központi reagáló csapat** (SOC - Security Operations Center) központi elemévé.

# Felhasználási esetek

A SIEM láthatósága és az anomáliák észlelése segíthet a nulladik napi vagy polimorf kódok felderítésében. Elsősorban az ilyen típusú, gyorsan változó rosszindulatú szoftverek elleni alacsony vírusfelismerési arányok miatt. A naplóelemzés, a napló normalizálása és kategorizálása automatikusan történhet, függetlenül a számítógép vagy a hálózati eszköz típusától, amennyiben az képes naplót küldeni.



A biztonsági események és a naplóhibák SIEM-mel történő vizualizációja segíthet a minták felismerésében.

A protokoll anomáliák, amelyek félrekonfigurálásra vagy biztonsági problémára utalhatnak, a SIEM segítségével azonosíthatók a mintafelismerés, a riasztás, az alapvonal és a műszerfalak segítségével.

A SIEM-ek képesek a rejtett, rosszindulatú kommunikáció és a titkosított csatornák felderítésére.

A SIEM-ek fel tudják fedezni a kibertámadást elkövetőket és az áldozatait is.

## Példák a korrelációs szabályokra

A SIEM rendszerek több száz és több ezer korrelációs szabállyal rendelkezhetnek. Ezek közül néhány egyszerű, néhány pedig összetettebb. Amint egy korrelációs szabály működésbe lép, a rendszer megfelelő lépéseket tehet a kibertámadás mérséklésére. Általában ez magában foglalja egy **értesítés küldését** a felhasználónak, majd esetleg a **rendszer korlátozását** vagy akár **leállítását**.

## Brute Force-érzékelés

A nyers erővel történő észlelés viszonylag egyszerű. A brute force támadás olyan hacker módszer, amely több felhasználónevet és jelszót kipróbálva tör fel jelszavakat, bejelentkezési adatokat és titkosítási kulcsokat. Ez leggyakrabban arra utal, hogy valaki folyamatosan megpróbálja kitalálni a jelszavát - akár kézzel, akár egy eszközzel. Azonban utalhat arra is, hogy URL-címeket vagy fontos fájlhelyeket próbál kitalálni a rendszerén.

Az **automatizált brute force könnyen felismerhető**, hiszen ha valaki egy perc alatt 60-szor próbálja meg beírni a jelszavát, az gyanús.

## Lehetetlen utazás

Amikor egy felhasználó bejelentkezik egy rendszerbe, általában véve az esemény időbélyegzőt hoz létre. Az időpont mellett a rendszer gyakran más hasznos információkat is rögzíthet, például a használt eszközt, a fizikai helyszínt, az IP címet, a hibás bejelentkezési kísérleteket stb. Minél több adatot gyűjtenek, annál több hasznosítható belőlük. Lehetetlen utazás esetén **a rendszer az aktuális és az utolsó bejelentkezés dátumát/idejét, valamint a rögzített távolságok közötti különbséget vizsgálja**. Ha úgy ítéli meg, hogy ez nem lehetséges, például egy percen belül több száz mérföldet utazik, akkor figyelmeztetést ad ki.

Sok alkalmazott és felhasználó használ ma már VPN-szolgáltatásokat, amelyek eltakarhatják a fizikai tartózkodási helyet. Ezt figyelembe kell venni egy ilyen szabály felállításakor.

## Túlzásba vitt fájlmásolás

Az átlagos felhasználó jellemzően nem másol vagy mozgat többször fájlokat a rendszerben. **Így a rendszeren történő túlzott mértékű fájlmásolás egy támadónak tulajdonítható,** aki kárt akar okozni a szervezetnek. Sajnos ez nem olyan egyszerű, mint azt állítani, hogy valaki illegálisan szerzett hozzáférést a hálózatához, és bizalmas információkat akar ellopni. Lehet egy alkalmazott is, aki el akarja adni a vállalati információkat, vagy egyszerűen csak az otthoni munkavégzés végett másolt át néhány fájlt.

## DDoS támadás

A DDoS (Distributed Denial of Service) támadás jelentős károkat okozhat egy vállalatnak vagy szervezetnek. Egy DDoS-támadás **nemcsak egy webhelyet tehet offline állapotba, hanem egy rendszer elérését is gyengítheti**. A megfelelő korrelációs szabályok alkalmazásával a SIEM-nek riasztást kell indítania a támadás kezdetén, hogy a vállalat megtehesse a szükséges óvintézkedéseket a létfontosságú rendszerek védelme érdekében.

## Fájlintegritás-változás

A fájlintegritás és -változtatás figyelése (FIM) a rendszerben lévő fájlok megfigyelését jelenti. A rendszerfájlokban bekövetkező **váratlan változások riasztást váltanak ki**, mivel ez egy kibertámadás valószínű jele.

## Modellek

A korrelációs szabályok mellett a SIEM-nek modelljei is lehetnek. A modellek némileg eltérnek a korrelációs szabályoktól, de ha helyesen hajtják végre, ugyanolyan hasznosak lehetnek. Az egy az egyhez **korreláció helyett a modell több lépést követel meg a riasztás kiváltásához**. Ez általában egy első szabály, majd egy szokatlan viselkedés követi. Ez lehet olyan egyszerű, mint például egy felhasználó, aki a megszokottól eltérő helyről jelentkezik be, majd nagyméretű fájlátvitelt hajt végre.

Ez rendkívül hasznos lehet, mivel egyetlen esemény nem feltétlenül jelenti a szervezet szervereinek vagy hálózatának kompromittálódását, lehet, hogy csak egy csapattag dolgozik egy kávézóból.

## Fals pozitív eredmények kezelése

Sajnos az élet minden területén **előfordulnak fals pozitív jelzések**, és ez igaz a SIEM-re is. Minden eszköz és rendszer képes ilyen eredményt produkálni. Például egy túl sok sikertelen bejelentkezési kísérlet esetén lehet, hogy csak elfelejtette az alkalmazott a jelszavát, és nem pedig valaki megpróbált betörni a rendszerbe. Fontos, hogy a kiváltott események esetében a megtett lépések indokoltak és megfelelő mértékűek legyenek, hiszen nem szeretnénk, ha az alkalmazottak órákra kizáródnának a munkakörnyezetből.

# Jogi szabályozás

A 2006 szeptemberében megjelent a **NIST SP 800-92 Guide to Computer Security Log Management** (Útmutató a számítógépes biztonsági naplók kezeléséhez), a NIST kockázatkezelési keretrendszerében használt elsődleges dokumentum arra vonatkozóan, hogy mit kell ellenőrizni. Bár nem végleges vagy kimerítő, mivel 2006 óta jelentős változások történtek a technológiában, ez az útmutató előrevetítette az iparág növekedését, mivel a dokumentum még mindig releváns. Ez a dokumentum számos, ma már jól ismert modern SIEM technológiát megelőz, ami abból is kitűnik, hogy a SIEM kifejezésre nem történik utalás. Nem ez az egyetlen útmutató az auditálásra és a felügyeletre vonatkozó szabályozási mechanizmushoz, amelyeket a decentralizált, egyedi, host alapú ellenőrzések helyett a SIEM-megoldások használatára ösztönöznek.

A **NIST SP 800-53 AU-2** eseményfigyelés alapvető biztonsági ellenőrzés a naplózási funkciók engedélyezéséhez, az információbiztosítási folyamat támogatása a rendszer egészére kiterjedő összes ellenőrzéshez. Az AU-2 eseményfigyelés az információbiztosítási és kiberbiztonsági mérnöki erőfeszítések folyamatos nyomon követésének kritikus alapjául is szolgál a hálózat egészén. A SIEM-megoldás várhatóan alapvető eszközként vagy eszközkészletként szolgál ezen erőfeszítések támogatására.

A rendszer bizalmasságára, sértetlenségére és rendelkezésre állására (CIA) gyakorolt hatásra vonatkozó rendszerkategorizálástól függően általában öt konkrét követelmény szükséges a szövetségi rendszer alapnaplózási feltételeinek teljesítéséhez (AU-2, a-e). A SIEM infrastruktúrával és működéssel kapcsolatos biztonsági ellenőrzési követelmények megértése alapvető fontosságú.

Az alábbiakban az AU-2 biztonsági ellenőrzési követelményeit ismertetjük:

**a;** Határozza meg azokat az eseménytípusokat, amelyeket a **rendszer képes naplózni az ellenőrzési funkció támogatására**;

**b;** **Koordinálja az eseménynaplózási funkciót más, az ellenőrzéssel kapcsolatos információkat igénylő szervezeti egységekkel**, hogy irányítsa és tájékoztassa a naplózandó események kiválasztási kritériumait;

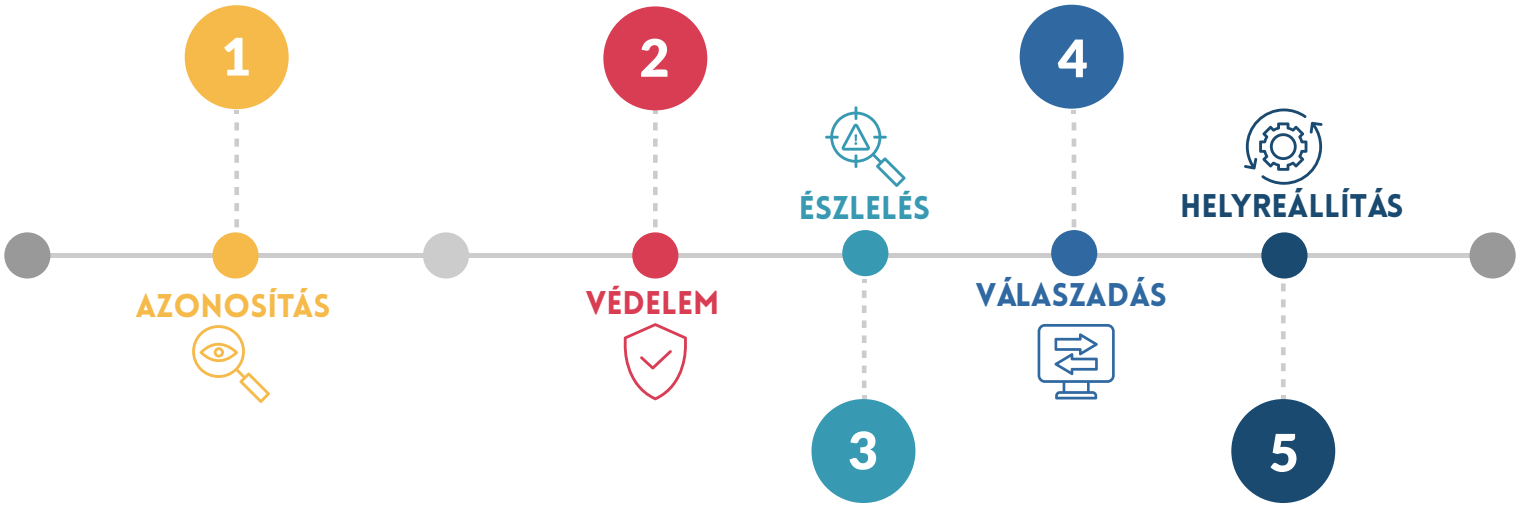
**c;** **Adja meg a következő eseménytípusokat a rendszeren belüli naplózáshoz**, valamint az egyes meghatározott eseménytípusok naplózásának gyakorisága (vagy a naplózást igénylő helyzet);

**d;** **Indoklás arról, hogy a naplózásra kiválasztott eseménytípusok miért tekinthetők megfelelőnek** az **események utólagos kivizsgálásának támogatására**; és

**e;** A naplózásra **kiválasztott eseménytípusok felülvizsgálata és frissítése.**

A rendszer eseményei közé tartozhatnak többek között a hitelesítő adatok változása, sikertelen hozzáférési kísérletek, szerepkör alap vagy attribútum változások a fiókokban, token alapú használat, hozzáférési kísérletek és sikertelenségek stb. Bár a rendszer minden egyes műveletének naplózása lehetséges, a naplók mennyisége és a biztonság szempontjából releváns, felhasználható adatok mennyisége alapján ez gyakran nem javasolt. A szervezetek az AU-2 a-tól e-ig terjedő AU-2 a-t használhatják alapként, amelyre építhetnek, miközben betartják az egyéb ellenőrzéseket, amelyek nagyobb részletességgel előírhatják az egyedi biztonsági ellenőrzési követelményeket.

A **NIST SP 800-53 SI-4 Rendszerfelügyelet** az a biztonsági ellenőrzés, amely a rendszer felügyeletét írja elő. Ez magában foglalhatja a hardvert és a szoftvert együttesen az események és anomáliák, a rosszindulatú szoftverek, a kapcsolatok és minden más olyan vonatkozó mechanizmus észlelésére, amely a támadások vagy a potenciális támadások indikátorainak észlelésére szolgál.




6. ábra
**A NIST kiberbiztonsági keretrendszer**

**a;** A **rendszer figyelése** a felderítés érdekében:

1. *Támadások és a lehetséges támadásokra utaló jelek a következő felügyeleti célkitűzésekkel összhangban; és*
2. *Jogosulatlan helyi, hálózati és távoli kapcsolatok;*

**b**; A **rendszer jogosulatlan használatának azonosítása** a következő technikák és módszerek segítségével;

**c; Belső felügyeleti képességek bevetése** vagy **felügyeleti eszközök telepítése**:

1. *Stratégiailag a rendszeren belül a szervezet által meghatározott alapvető információk összegyűjtése érdekében; és*
2. *A rendszeren belüli ad hoc helyszíneken a szervezet számára érdekes, meghatározott típusú tranzakciók nyomon*

**d;** Az észlelt **események és anomáliák elemzése**;

**e;** A **rendszerfigyelési tevékenység szintjének módosítása**, ha a szervezeti műveletekre és eszközökre, egyénekre, más szervezetekre vagy a nemzetre vonatkozó kockázat megváltozik;

**f; Jogi vélemény beszerzése** a rendszerfelügyeleti tevékenységekkel kapcsolatban.

A **NIST SP 800-53 RA-10 Threat Hunting** a NIST 800-53-hoz a legutóbbi, 5. revíziós kiadással és publikációval hozzáadott új biztonsági alapellenőrzés. A fenyegetésvadászat a hálózat proaktív védelme az összes biztonsági információ kombinálásával és a fenyegetések aktív keresésével. A művelet végrehajtásához az elemzőknek és a mérnököknek szükségük van egy információs tárra, és a SIEM-megoldást gyakran használják központként, mivel az összes rendszernaplót jellemzően erre a központi helyre küldik. A fenyegetésvadász csapat nem korlátozódik erre a megközelítésre.

A SIEM-megoldásnak azonban jelentős mennyiségű biztonsági szempontból releváns adatot kell szolgáltatnia.

**a;** **Hozzon létre és tartson fenn** kiberfenyegetettség elemző és kezelő képességet, hogy:

1. *a szervezeti rendszerekben a veszélyeztetettségre utaló jelek keresése; és*
2. *a meglévő ellenőrzéseket megkerülő fenyegetések felderítése, nyomon követése és megszakítása; és*

**b;** **alkalmazza a fenyegetésvadászat képességét.**

*A legújabb, azaz a NIST Cybersecurity Framework 2.0 (rövidítve CSF 2.0) keretrendszeréről többet is megtudhat ide kattintva.*

A NIST SP 800-53 R5 és az AU-2, SI-4 és RA-10 rövid leírása bemutatja, hogy az egyes ellenőrzések mindegyike a SIEM-en keresztül történő esemény-, riasztási és felügyeleti rendszer kritikus elemeként használatos. Ezek az ellenőrzések a NIST által biztosított egyéb technikai biztonsági ellenőrzésekkel együtt egy mélyreható védelmi rendszert alkotnak. A rendszer biztonságának biztosítását különböző kockázatértékelésekkel és folyamatos nyomon követéssel érvényesítik - gyakran a teljes kiberbiztonsági csapatban használt SIEM-termékkel kiegészítve vagy racionalizálva. Számos további technikai ellenőrzés létezik, amelyek konkrét elemeket vázolnak fel, amelyeket figyelemmel kell kísérni. Az azonosított ellenőrzések a SIEM eszköz esemény- és auditgyűjtési funkcióihoz és használatához közvetlenül kapcsolódó ellenőrzések felületes áttekintése.

# Jövőkép

Nagyobb vállalati rendszereknél közel fizikai képtelenség permanensen figyelemmel követni a logokat. A vállalat időt, energiát és humán erőforrást, ezáltal pénzt takaríthat meg egy megfelelően konfigurált SIEM rendszer segítségével. A felhő alapú rendszerek elterjedésével pedig az infrastruktúrára szánt költségeket redukálhatja. Azonban fontos menedzselni ezeket a rendszereket, hiszen csak egy jól konfigurált rendszer képes kiszűrni a támadásokat, elkülöníteni a fals pozitív találatokat. Mint mindenben ebben is egyre nagyobb segítséget nyújthat az MI.

Lefedettség 24/7! Valós időben észleli a kiberfenyegetéseket, és reagál rájuk.

A mesterséges intelligencia csökkentheti a biztonsági csapatok, az incidensek osztályozásához és az azokra való reagáláshoz szükséges idejét és erőfeszítését. Az akár órákig tartó elemzéseket elvégezheti percek alatt. Képes automatikusan rangsorolni az észlelt fenyegetéseket potenciális hatásuk és súlyosságuk alapján. Mindezt fáradhatatlanul, a hét minden napján, 0-24 óráig.

A Biztonsági szakértelem erősíthető létszámnövelés nélkül. A vállalat rendszerének bővülése esetén emberi erőforrás takarítható meg, hiszen nem feltétlen szükséges újabb operátorokat alkalmazni.

Az **AI több biztonsági funkciót egyesít**, úgymint a vírusirtást, a végpontok észlelését és reagálását (EDR), a fenyegetésvadászatot és a sebezhetőségek kezelését. Ráadásul nem kell képzésre küldeni, mivel az algoritmusokat öntanuló mechanizmussal látják el. A mesterséges intelligencia és gépi tanulási algoritmusok naponta több milliárd eseményt képesek elemezni és ezekből tanulni. Ez a folyamatos fejlődés biztosítja, hogy a végpontok továbbra is védettek maradjanak a kiberfenyegetések folyamatosan változó környezetével szemben. Az AI hatalmas mennyiségű hálózati metaadatot elemez, így a felhasználói viselkedést is. A viselkedésbeni eltérésekből a potenciális támadások finom jeleit észleli.

Míg a hagyományos vírusirtó megoldások a szignatúra alapú felismerésre támaszkodnak, a mesterséges intelligencia elemzi a fájlt, és megjósolja annak potenciális rosszindulatú viselkedését. Ez lehetővé teszi, hogy az ismert és ismeretlen fenyegetéseket - a nulladik napi támadásokat is - még **azelőtt azonosítsa és blokkolja, mielőtt azok végrehajtódnának és kárt okoznának**.

NEMZETI
KIBERVÉDELMI INTÉZET


nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast


2024