Big-data alapú fejlett analitikai fraud és cyber esemény felderítő-megoldás, avagy új generációs SIEM

Új generációs információbiztonság – alulról építkezve

Nagy Ádám – IT ISO + Főosztályvezető, Információbiztonsági kockázatkezelés (Information Risk Management-IRM)

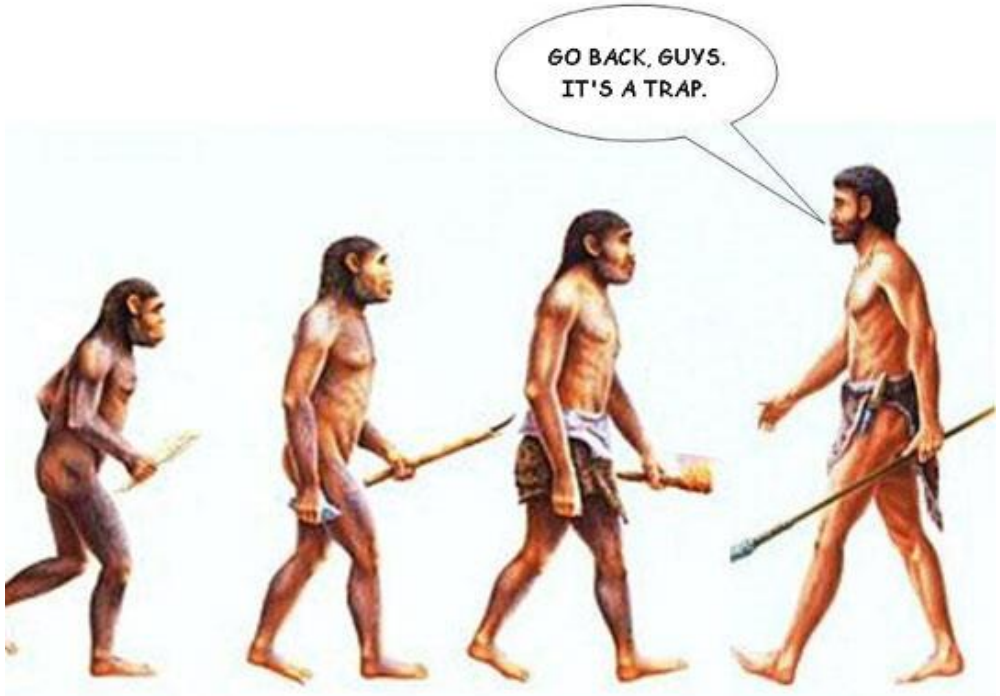
K&H Group

Miért van szükség az IT biztonsági monitorozásra?

- Kockázatokat csökkentése – számos (a legtöbb) esetben csak a detektív kontrollok működnek
- Csalás, visszaélés és cyber-támadás detektálás és megelőzés támogatása
- Konfigurációs hibák felfedezése
- Incidenskezelés
- Törvényi megfelelés

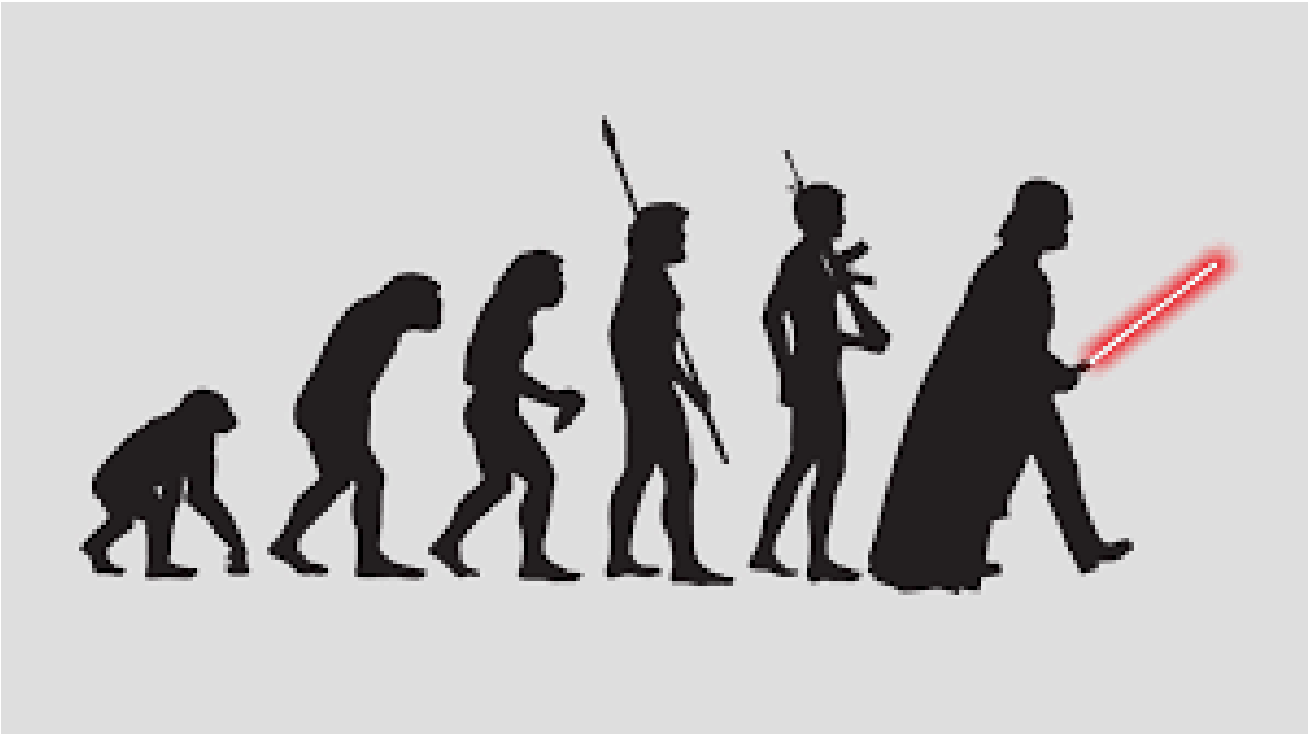
A monitorozás evolúciója

A monitorozás evolúciója



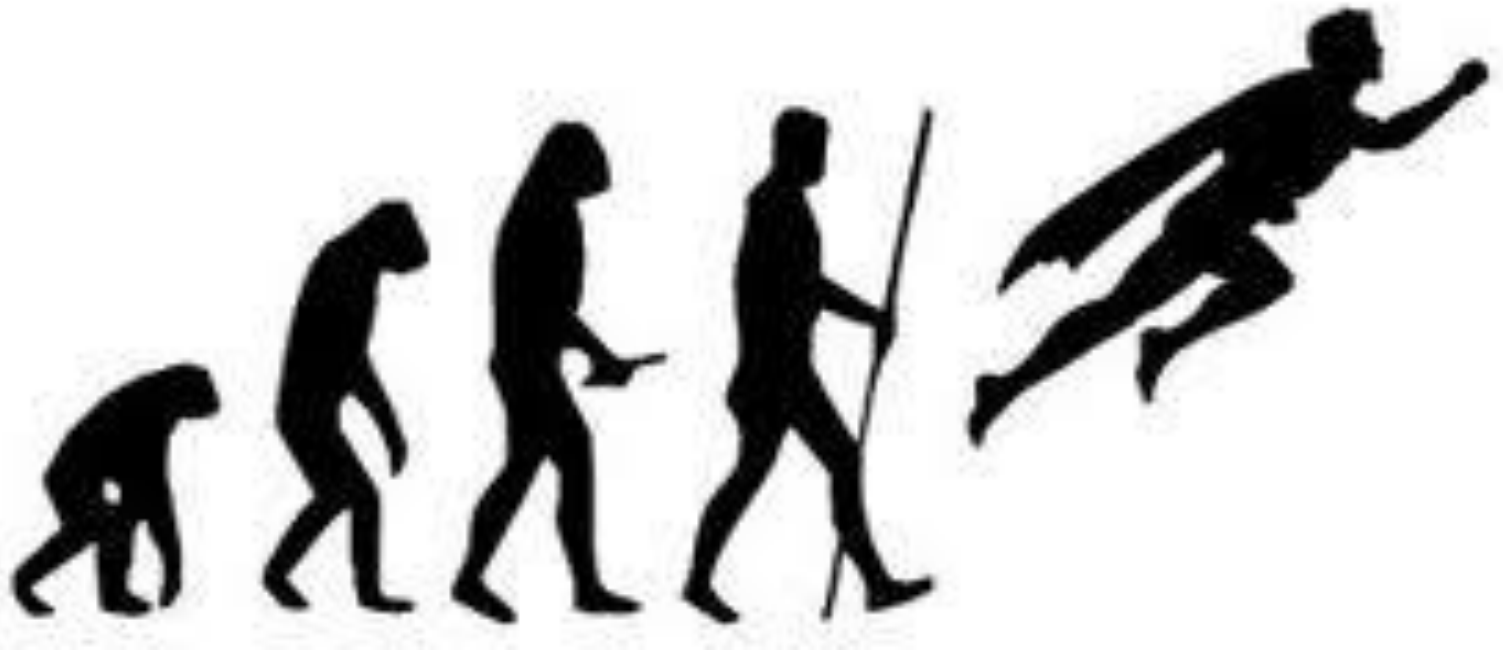
- A hagyományos Security Information and Event Management (**SIEM**) rendszerek nem fejlődtek a folyamatosan átalakuló IT biztonsági kihívásoknak megfelelően.
- Az IT napló-központú SIEM rendszerek csak a megelőző kontrollok által azonosított eseményeket képesek riportolni – vagy még azt sem.
- Nehézkes fals pozitív eseménykezelés, minden klasszikus SIEM egyik legnagyobb gondja
- Az iparági statisztikák szerint a sikeres támadások több, mint 90% -a felderítetlen maradt a napló-alapú észleléskor, hatékony korrelációs motor ide, vagy oda.

A monitorozás evolúciója



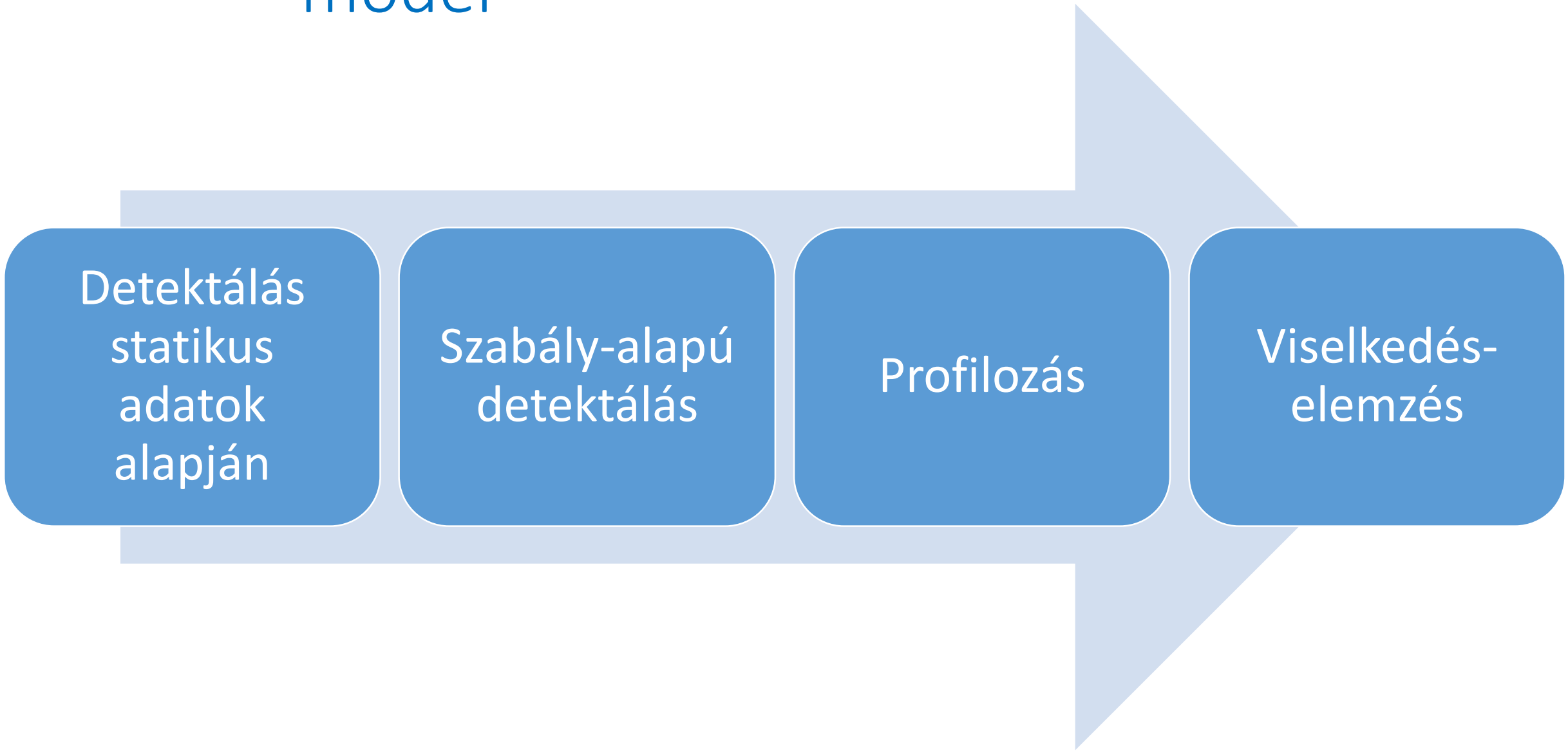
- **Új jogszabályi követelmények és iparági szabványok**
- Jogtalan felhasználás megakadályozása
- Érzékeny adatok ne mérgezzék meg a gyűjtött adatainkat és megvalósuljon a célhoz kötöttség
- Hozzáférés védelem a biztonságos adatgyűjtéshez

A monitorozás evolúciója



- Nagyfokú testreszabhatóság
- Könnyű skálázhatóság és stabilitás
- Olyan technológia, ami képes nagy strukturálatlan adattömeg **hatékony** kezelésére

Információbiztonsági monitoring érettségi model



Keresés – az igazi kihívás

Az információ-visszakeresés megfelelő működése megköveteli, hogy elkezdjük gondolkodni azon, hogy mit keresünk és hogyan fogjuk megtalálni a lekérdezési mechanizmus segítségével.

Pár ismert, klasszikus döntési pont, mielőtt megkezdjük az összegyűjtött eseménynapló-mezők keresését:

- A kisbetű-nagybetű érzékenység számít? A "DoD" ugyanaz, mint a "dod"?
- Milyen jelzőket indexel? Nyilván szeretné indexelni a „papa„ szót. És valószínűleg indexelni szeretné a „papa123" –t is. És szeretnénk indexelni az „123”, „12.3”, „192.168.1.1” szavakat is.
- Hogyan kezeljük olyan dolgokat, mint a kötőjel a szavak között?
- Ha a lekérdezési nyelvünk támogatja az kifejezések keresését?
- Milyen nyelveket fogunk támogatni? Ami angolul működik, az a magyar nyelvű ékezetes szövegen sikertelen lehet.

Alap technológiák

FTS: A teljes szöveg alapú (full-text) keresést alkalmazó rendszerek jobbak a nagy mennyiségű strukturálatlan szöveget tartalmazó szavak vagy szavak kombinációinak keresésére. Ezek széleskörű szöveges keresési lehetőségeket biztosítanak és kifinomult relevancia rangsoroló eszközöket kínálnak az eredmények rendezéséhez.

RDBMS: a strukturált adatok tárolása és manipulálása - adott típusú mezők nyilvántartása (szöveg, egész szám, pénznem stb.). Többféle rekordtípus rugalmas keresését támogatják a mezők meghatározott értékeire, valamint erős eszköz az egyedi rekordok gyors és biztonságos felülírásához.

Alap technológiák

A **KAP-probléma** azt állítja, hogy egy elosztott számítógépes rendszer számára egyszerre nem lehet mindhárom alábbi garanciát biztosítani:
- **Konzisztencia** (minden csomópont ugyanazokat az adatokat látja egyszerre)
- **Elérhetőség** (garancia arra, hogy minden kérelemre válasz érkezik arról, hogy sikeres vagy sikertelen)
- **Particionálási tűrés** (a rendszer továbbra is működik a hálózati hibák miatti tetszőleges particionálás ellenére)

Megoldás: **több adatcsomópont** helyi redundáns tárolókkal

Adatcsomópont klaszterek - az összes elsődleges és replika shard-ot elosztják egymás között (a felosztott indexeket shard-oknak nevezzük). A shard-okra osztás fontos:
- Ez lehetővé teszi vízszintes megosztást és méretezését
- Lehetővé teszi a műveletek szétosztását és párhuzamosítását (potenciálisan több csomóponton), ezáltal növelve a teljesítményt / áteresztőképességet

A replikáció két fő okból fontos:
- Magas rendelkezésre állás abban az esetben, ha a shard-ok / csomópontok nem működnek. Emiatt fontos megjegyezni, hogy egy replika shard-ot soha nem osztanak ki ugyanazon a csomóponton, mint az eredeti / elsődleges shard, ahonnan másolták.
- Lehetővé teszi, hogy kiszámításra kerüljön a keresési mennyiséget / átbocsátási mennyiséget, mivel a keresések párhuzamosan végrehajthatók az összes másolaton.

IRM
We enable you to be safe

Miért nincs igazán jó dobozos megoldás?

Mit mond a piac?

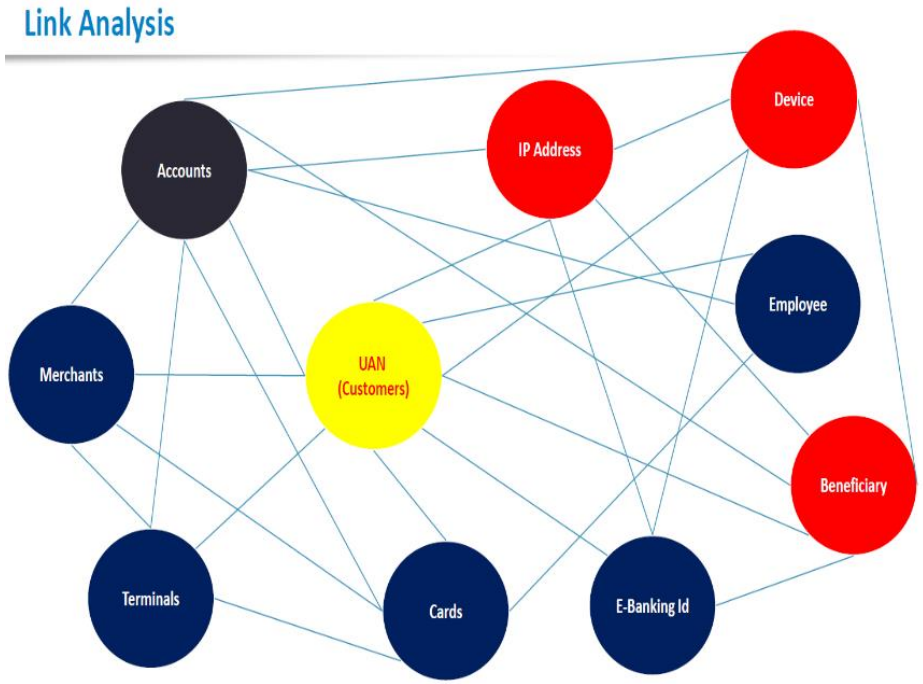
- A nagy gyártók megoldásai alacsonyabb költséggel történő alternatívájaként, egyedi helyi megoldások használata van előtérben az elemzések alapján.

- Több, specializált feladatokra használt alkalmazás közös alkalmazása hatékonyabb eredményre vezet strukturálatlan nagy adattömeg kezelésekor.

- A helyi erőforrások és kompetencia nélkül azonban ez nehezen megoldható feladat.

Holisztikus megközelítés

- Csatorna-független integrált monitorozás
- Minden csatorna a közös információhalmazt használhatja
- Felhasználói szinten, egyénileg is testre szabható felület események, naplók, megoldások, jelentések és egyéb információk megjelenítésére
- Könnyen kezelhető vizualizáció, szabadon használható diagramkészítés dinamikus tartalommal.



Indikátorok

Viselkedés elemzés

- korlátlan profilképzési képességek a viselkedés felderítéséhez
- a profilozandó objektumok szükség szerint meghatározhatók, valamint jellemző tulajdonságaik (pl: ügyfelek, ügyletek, alkalmazottak, rogue hálózatok)
- a jellemző tulajdonságok kiválaszthatók
- A tulajdonság értékek kiszámíthatók és rendszeresen frissíthetők testre szabható algoritmusokkal vagy manuális, statikus értékekkel (pl. tranzakciós határértékek / küszöbértékek, gyakran használt gépek)
- A profillal kapcsolatos értékek felhasználhatók a pontozási/súlyozási szabályokban a korreláció pontosságának fokozása érdekében

A monitorozás evolúciója

„Application Security Monitoring” - **Valós idejű biztonsági információgyűjtés, elemzés, adatdúsítás, gyorskeresés**.

IRM
We enable you to be safe