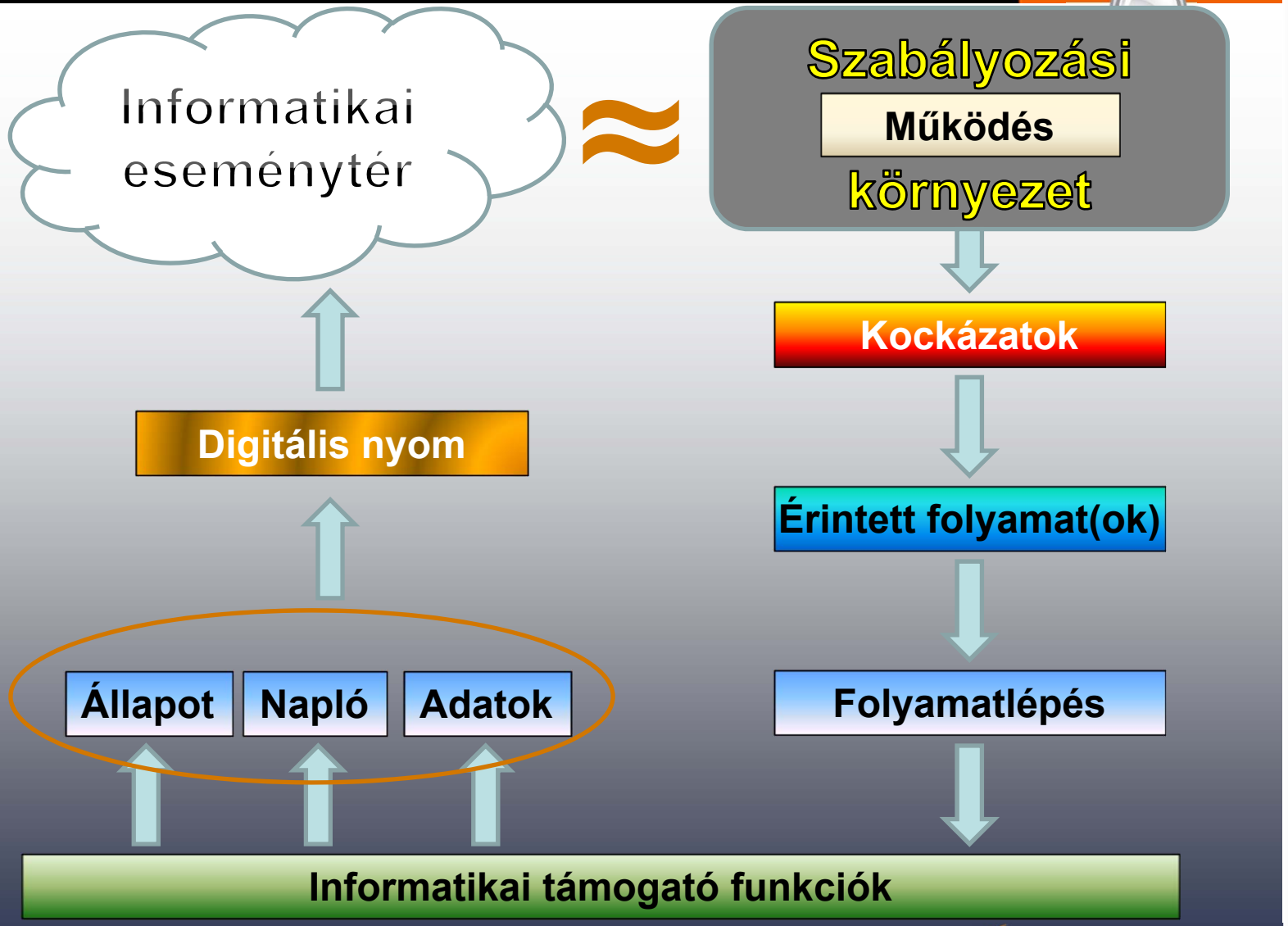
NETWORKSHOP - 2011 április 27-29.

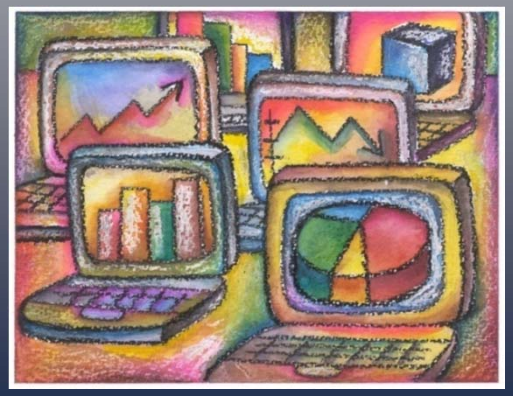
Digitális nyom elemzés az informatikai eseménytérben

Seaconeurope


Informatikai eseménytér
≈
Szabályozási
Működés
környezet
Kockázatok
Érintett folyamat(ok)
Folyamatlépés
Digitális nyom
Állapot
Napló
Adatok
Informatikai támogató funkciók

Irányelv

A vállalat működése során a - kockázatkezelés szempontjából - ***kritikus folyamatok*** mentén keletkező ***digitális nyomok****at* újra feldolgozva megvizsgáljuk, milyen események, tranzakciók történtek, és kiszűrjük belőlük az ***anomáliák***at.



Seaconeurope

Digitális nyomok

- Eszköznapló
- Rendszernapló
- Alkalmazásnapló
- Biztonsági napló
- és minden ami üzletileg fontos adat:
  - operatív rendszerek adatai
  - beléptető adatok
  - jogosultsági adatok
  - helyszín/pozíció adatok…

Jelentősége

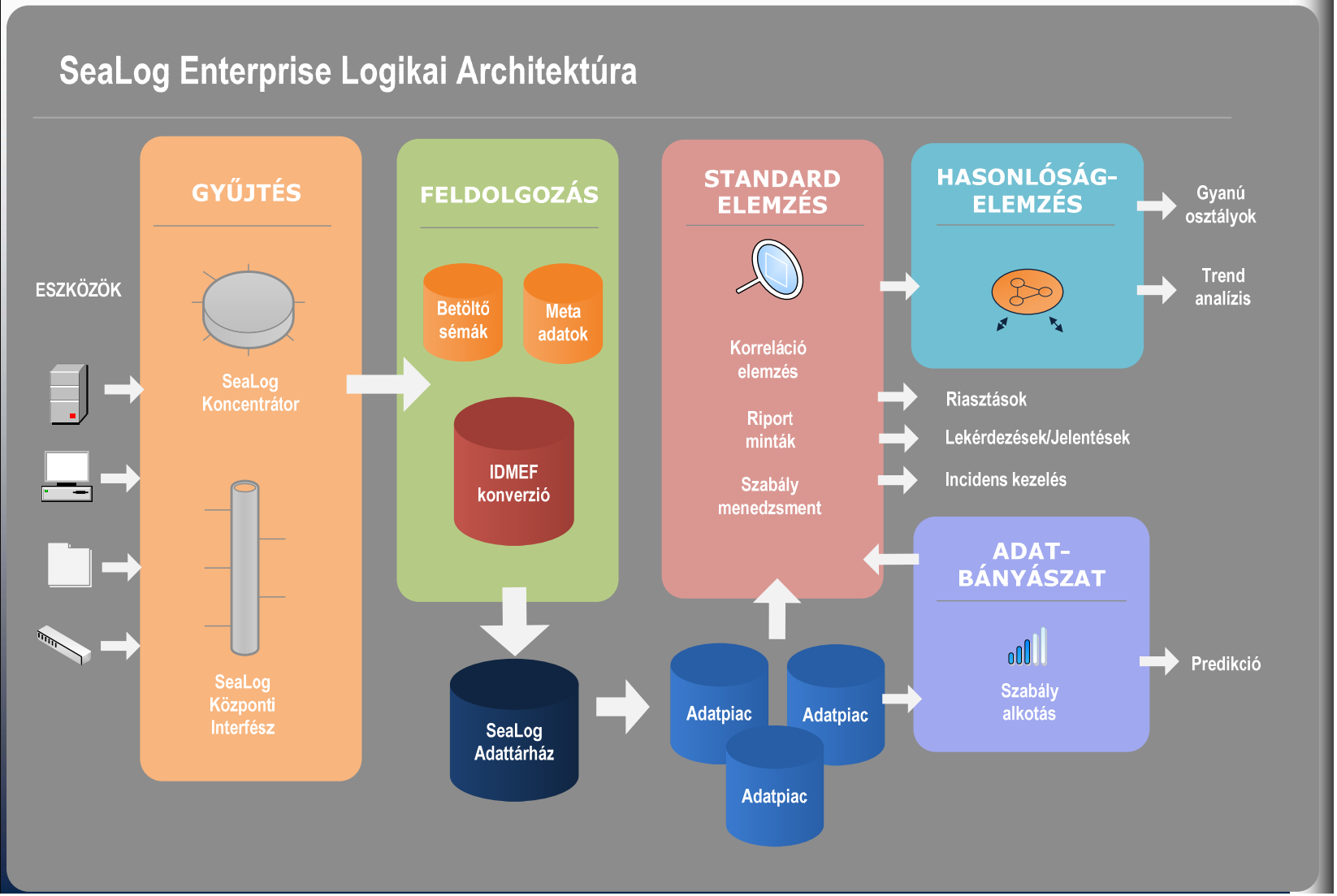
Nyomon lehet követni:

- ki/mi, mikor, mit csinált
- milyen adatokat manipulált
- milyen működési környezetben

Ellenőrizni lehet:

A lezajló események megfeleltek-e az előírásoknak <> Riasztás!

Nyomelemző logikai felépítése



Nyomelemző sajátosságai

- Időben elhúzódó folyamatok összetett vizsgálata
- Különböző digitális nyomok összekapcsolása
- A rejtett összefüggések elemzése
- Automatikus szabály felismerés, előrejelzés
- Specifikus adatpiacok
- Adattárházi technológiák alkalmazása

Szerepkörök

- Szakmai rendszergazda: a törzsadatok, eseményminták és felhasználók karbantartásáért felelős munkatárs.
- Felhasználó: szerepkörének megfelelően különböző rendszerek, területek naplóadatainak elemzésére jogosult felhasználó.
- Szakértő: speciális eszközeinek segítségével ad-hoc elemzések végrehajtása, összefüggések felismerésével új eseményminták kidolgozása.
- Rendszerüzemeltető: a betöltések felügyeletéért, illetve a rendszer működéséért felelős informatikus.
- Biztonsági menedzser: a rendszer felhasználói műveletei ellenőrző biztonsági munkatárs (ki/mikor/mit).

Felhasználási lehetőségek

- Üzleti célú
  - csalásfelderítés, belső kontroll megszegése, HR kockázatkezelés, ellenőrizhetőség
- Műszaki célú
  - rendelkezésre állás, meghibásodás, teljesítmény, kihasználtság
- IT célú
  - üzemeltetés támogatás, rendszerfelügyelet, IT biztonság, SLA
- És még …
  - összetett, második körös adatelemzés, pl: kötelező jelentések rendszere

Bevezetés feltételei

A digitális nyomoknak:

- léteznie kell abban a mélységben és tartalomban, amely a figyelés szempontjából elvárt
- vezetődnie kell abban a frekvenciában, megbízhatósággal és következetességgel, amely a figyelés szempontjából elvárt
- hozzáférhetőnek kell lennie: direkt, vagy közvetett módon importálható formátumú és tartalmú legyen

Bevezetés lépései

Keretrendszer - nem projekt, hanem program keretében!

- Projekt1 (vertikális implementáció)
  - Nyomelemző keretrendszer technológiai implementálása
  - Kommunikációs csatornák kialakítása (rendszerek, üzenetküldő szerverek, koncentrátorok között)
  - Testre szabás (interfészek készítése, adatkonvertáló eljárások kialakítása, esemény figyelési logika kidolgozása)
  - Próbaüzem/döntés a bevezetésről/éles indulás
  - Javaslat: max. 3-5 rendszer első lépésben!
- Projekt 2…n (horizontális kiterjesztés)
  - Előkészített (!) rendszerek folyamatos bekötése

Köszönöm a figyelmet!