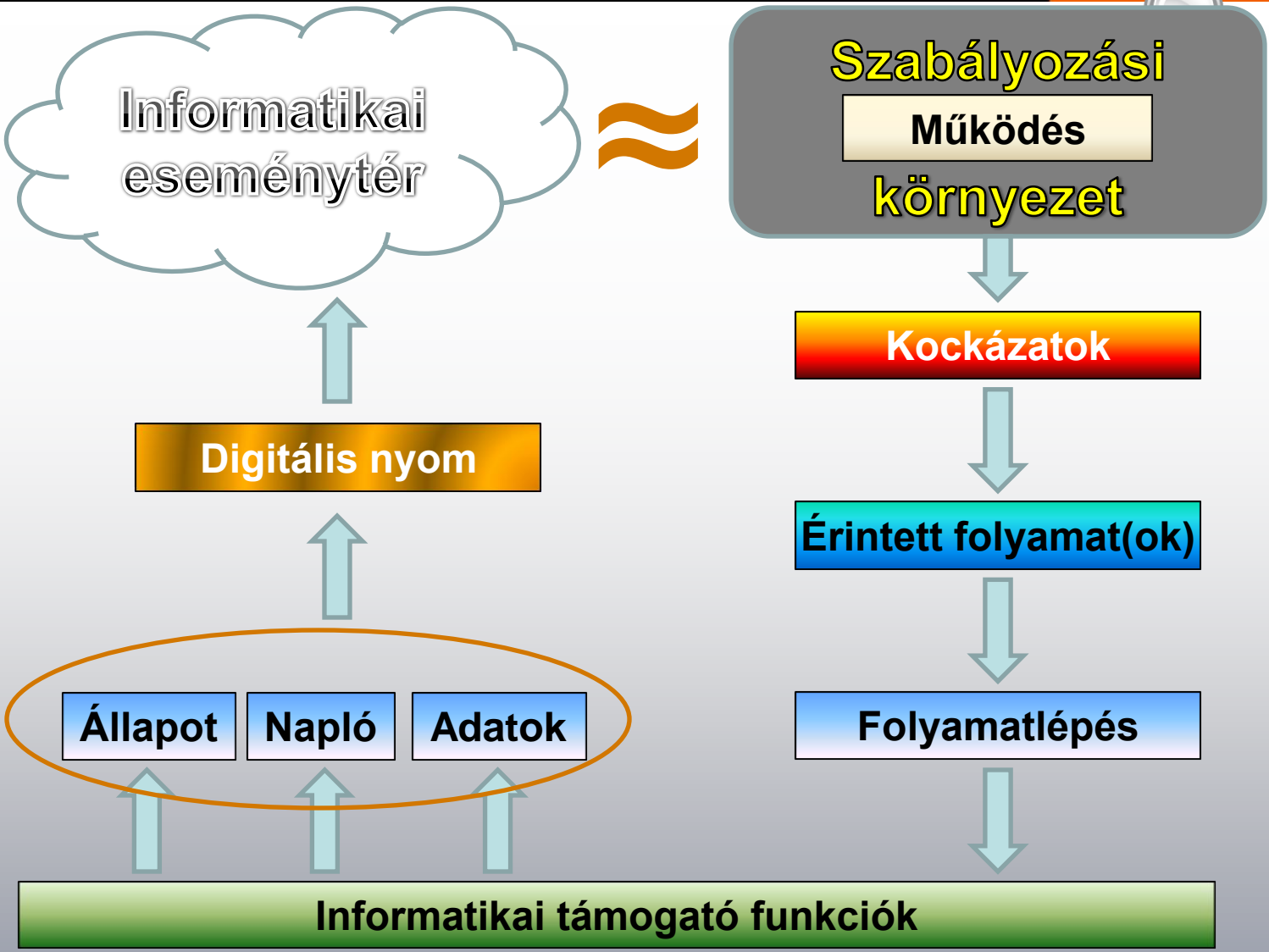




Audit és monitoring támogatás az informatikai eseménytérben







Irányelv

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





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:

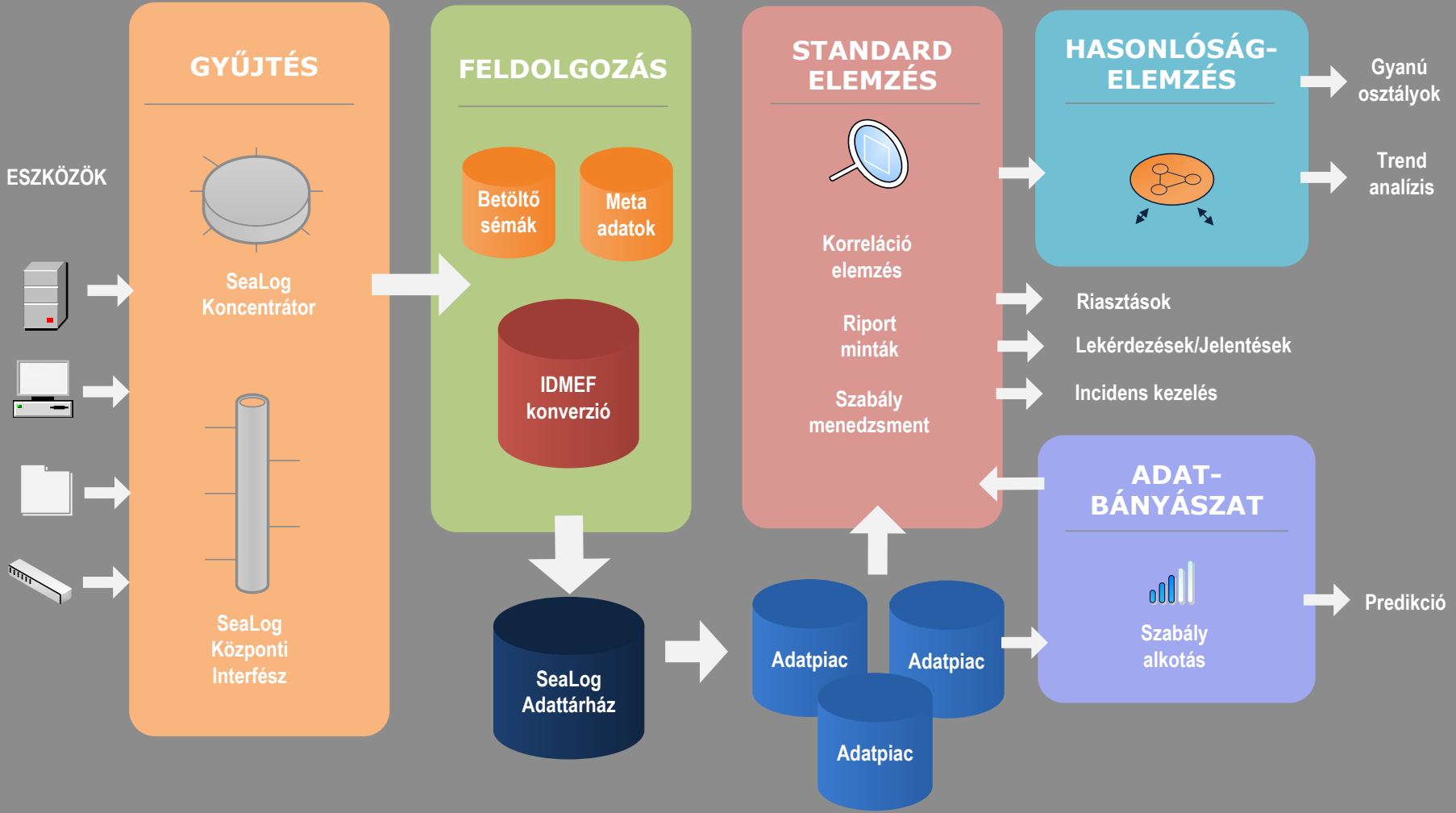
- ki/mi, mikor, mit csinált
- milyen adatokat manipulált
- milyen működési környezetben



Ellenőrizni lehet:

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

SeaLog Enterprise Logikai Architektúra





SeaLog rendszer sajátosságai

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



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



Köszönöm
a
figyelmet!