

IIR – Internal Audit 2011

*Hogyan segítheti az
IT háttér a hatékony
kockázatkezelést?*

Néhány szó az ISACA-ról

2.

- Alapítás 1969-ben (az ISACA-HU 20 éves)
- Tagok kb. 95 ezer (ISACA-HU 411 tag)
- IT irányítási nyílt szabványok és ajánlások az ITGI segítségével (COBIT, ValIT, RiskIT, ITAF, BMIS, stb.)
- Szabványok integrálása (mapping on ITIL, ISO27001, ISO13335, Basel2, COSO, stb.)
- Nemzetközi minősítések (CISA, CISM, CGEIT, CRISC)
- Szakmai cikkek és kapcsolatok (www.isaca.hu)
- Nemzetközi konferenciák és előadások (www.isaca.org)

A belső ellenőrzést segítő szoftverek

3.

- Elterjedt megoldások
 - ▣ ACL, BENy, Revizor, Auto Audit
- Általában magát az audit folyamatot támogatják
- A fejlettebbek rendelkeznek adatbányászati modullal is
- Az igazán komplex megoldás folyamatos kontroll monitorozási funkciót is biztosít

Egy másfajta megközelítés

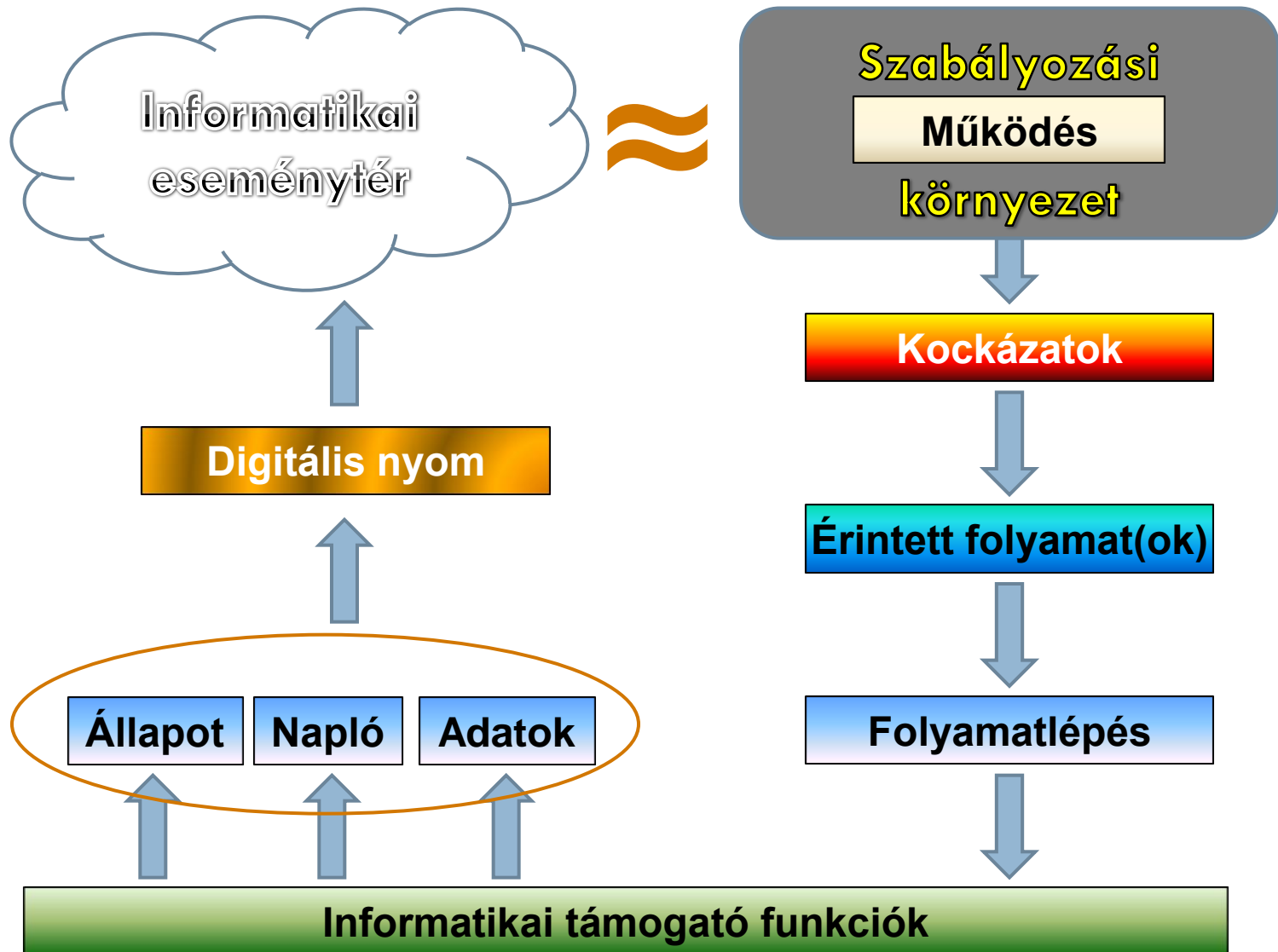
4.

- Nem a konkrét auditálási folyamat támogatása a cél, hanem a kockázatok kezelése, mérséklése

- Ennek két legfontosabb összetevője, hogy tudjuk:
 - ▣ Ki, mikor, mit csinált
 - ▣ Kinek, mihez, milyen hozzáférési jogosultsága van

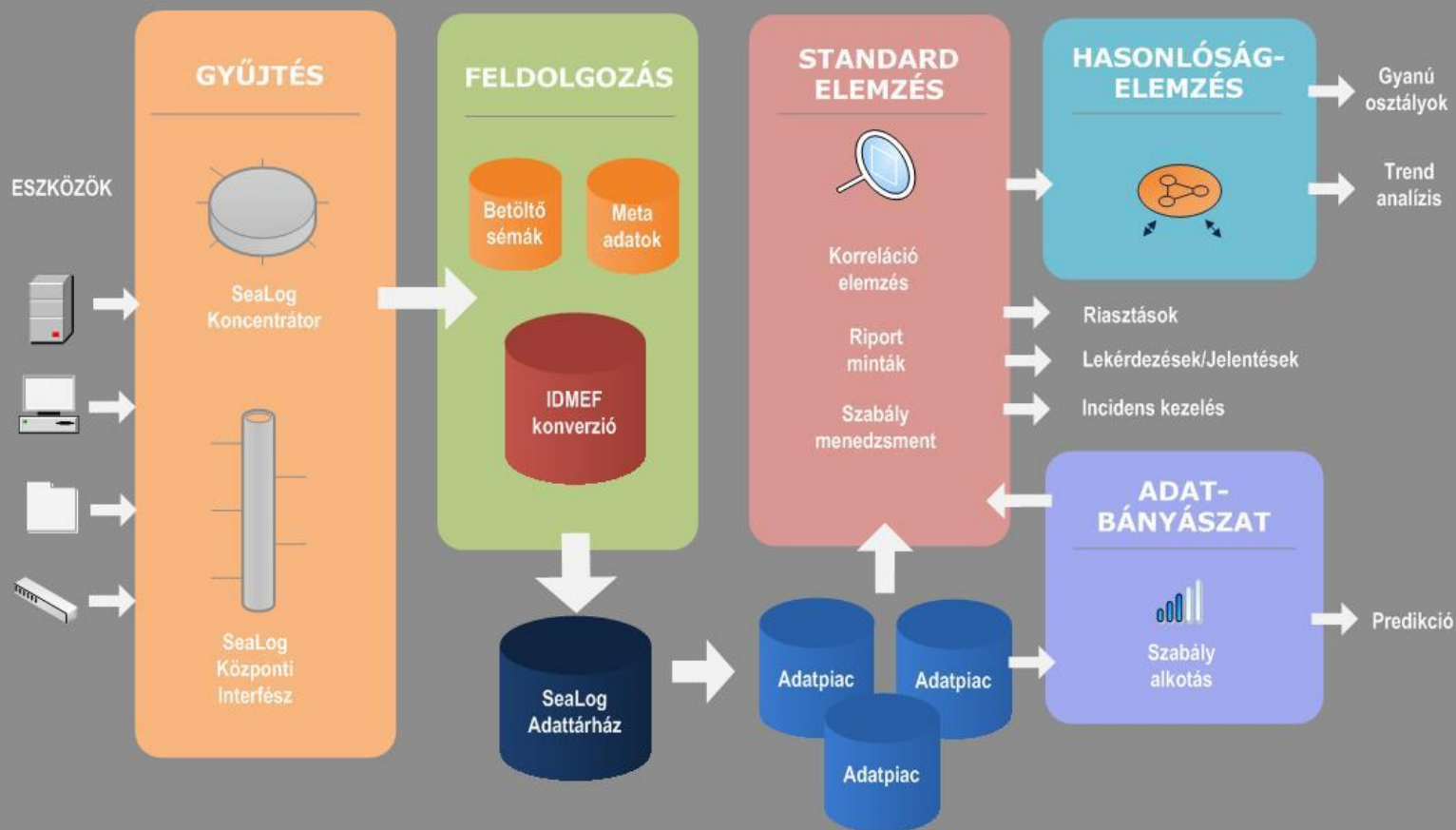
- Ma már a működési folyamatok túlnyomó része elektronikus formában zajlik, ezért a folyamatok kontrollja is informatikai módszerekkel történik

Informatikai eseménytér felépítése



Nyomelemző logikai felépítése

SeaLog Enterprise Logikai Architektúra



A digitális nyomelemző működése

7.

- Adatgyűjtés tetszőleges rendszerekből
 - ▣ Logok, naplóadatok, tranzakciós adatok, operatív adatok, helymeghatározási adatok, stb.
- Feldolgozás
 - ▣ Konzolidálás, egységesítés, dimenzionálás, adatpiac frissítés
- Felderítés/Elemzés (Operatív funkciók)
 - ▣ Szabálymenedzselés, riasztás, elemzés, biztonsági naplózás
- Mesterséges Intelligencia
 - ▣ Szabály felismerés, predikció, trendanalízis, szakértői vélemény generálás

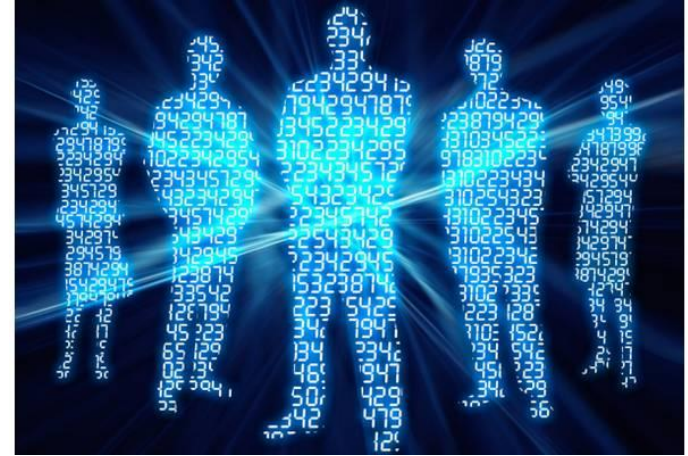
Kontrollgyengeségek felismerése I.

8.

- A digitális nyomgyűjtő rendszer elemzési moduljának segítségével a **rendellenességek kiszűrése**
- A Mesterséges Intelligencia modul adatbányászati eszköze, mint **szabályfelismerő** és **trendelemző** alkalmazás
- **Automatikus szabályalkotás, predikció** és **automatikus szakértői vélemény** generálása a hasonlóságelemzés segítségével

Kontrollgyengeségek felismerése II.

- **Jogosultságok**
kézbentartása mint
kockázatcsökkentés
 - Belső kényszer
 - Külső szabályozások
(PSZÁF, ISO)



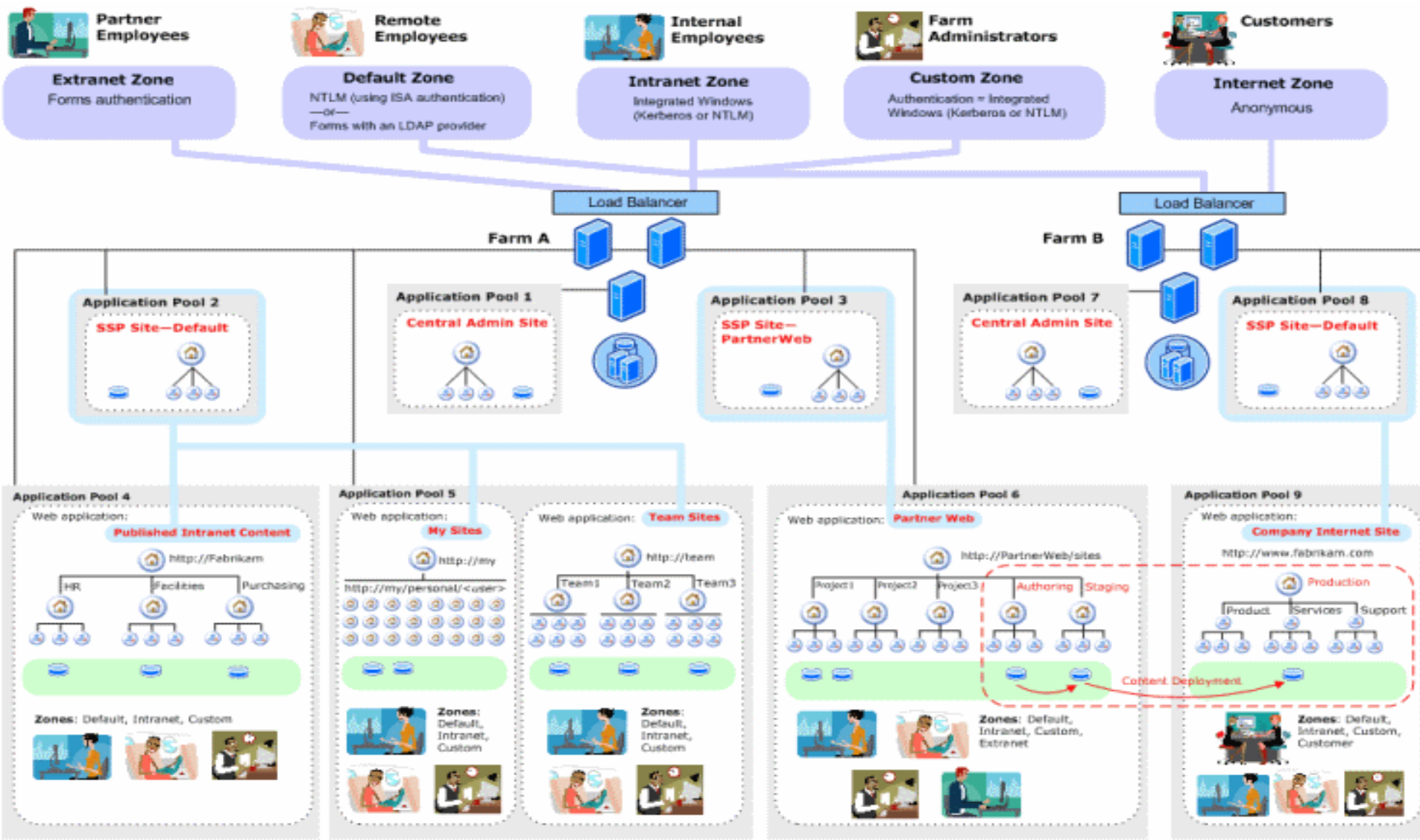
- Nagyon fontos eszköz az
adatvagyon védelmére
- Biztonságtudatosság
 - Kockázatok felmérése,
tudatosítása, csökkentése

Jogosultságkezelési kockázatok

- Alacsony minőségű jogosultságkezelés
- Plusz jogok
 - ▣ **Indokolatlan jogok kiosztása**
 - ▣ Jogok visszavonásának elmaradása
- Erős jogkörrel rendelkező felhasználók önhatalmú működése



Példa jogosultsági struktúrára



Jogosultsági kontroll gyengeségek

- Melyek azok a felhasználók, akik több jogosultsággal rendelkeznek, mint amit munkakörük megkíván?
- Egy adott felhasználó milyen fájlhoz és rendszerekhez férhet hozzá és milyen jogosultsági szinttel?
- Milyen felhasználók rendelkeznek teljes adminisztrációs jogkörrel?
- Milyen technikai felhasználók léteznek és milyen jogkörrel rendelkeznek?
- Milyen inaktív account-ok találhatóak a rendszerekben?

A fő probléma a jogosultságkezeléssel

- Manuális módszerrel áttekinthetetlen beállítások
 - ▣ Öröklődő jogosultságok miatti káosz
 - ▣ Ad-hoc beállítások
 - ▣ Csoportjogtól eltérő jogok



**Nincs információ
a tényleges helyzetről**

Ismert megoldások

- Egyedi, manuális jogosultságkezelés
- Központi jogosultságkezelés
 - ▣ Belső szabályozással (nem hatékony)
 - ▣ Teljeskörűen, elektronikusan (drága)
- **Tényleges jogok felolvasása – nem igazán elterjedt megoldás**

Újszerű megoldási javaslat

Induljunk ki a tényleges helyzetből!

- A kialakítandó rendszernek képesnek kell lennie
 - ▣ A pillanatnyi jogosultságok föltérképezésére
 - ▣ A beállított jogosultságok védett adatbázisban történő tárolására
 - ▣ Standard és adhoc jellegű riportok készítésére a belső összefüggések feltárására

A rendszerrel szembeni elvárások

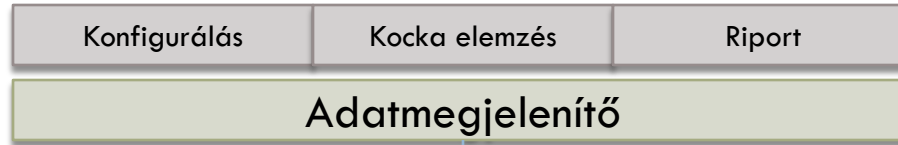
- Legyen moduláris és skálázható
- Mutassa meg az eltérést a tényleges helyzet és a vezetői szándék között
- Biztosítsa az adatok monitorozását és összetett elemzését
- Rendelkezzen fejlett riportolási képességekkel

Elméleti felépítés

- A kialakítandó rendszer tulajdonképpen egy adattárház, mivel:
 - ▣ Különböző adatokat, különböző helyről gyűjtünk össze egy adatbázisba (ETL)
 - ▣ Az adatokon transzformációkat végzünk és közös alapokra hozzuk őket (OLAP)
 - ▣ Az adatok több dimenzión keresztül is elérhetőek, megjeleníthetőek (Kocka)
 - ▣ A több dimenziós adatok egy-egy nézetéről pillanatfelvétel készíthető (Riport)

Valós felépítés

Adatmegjelenítő - elemző (Security Manager – Kocka, Riport)



Adattároló (Store Server - OLAP)



Felfedezők (Discoverer - ETL)



Adat források

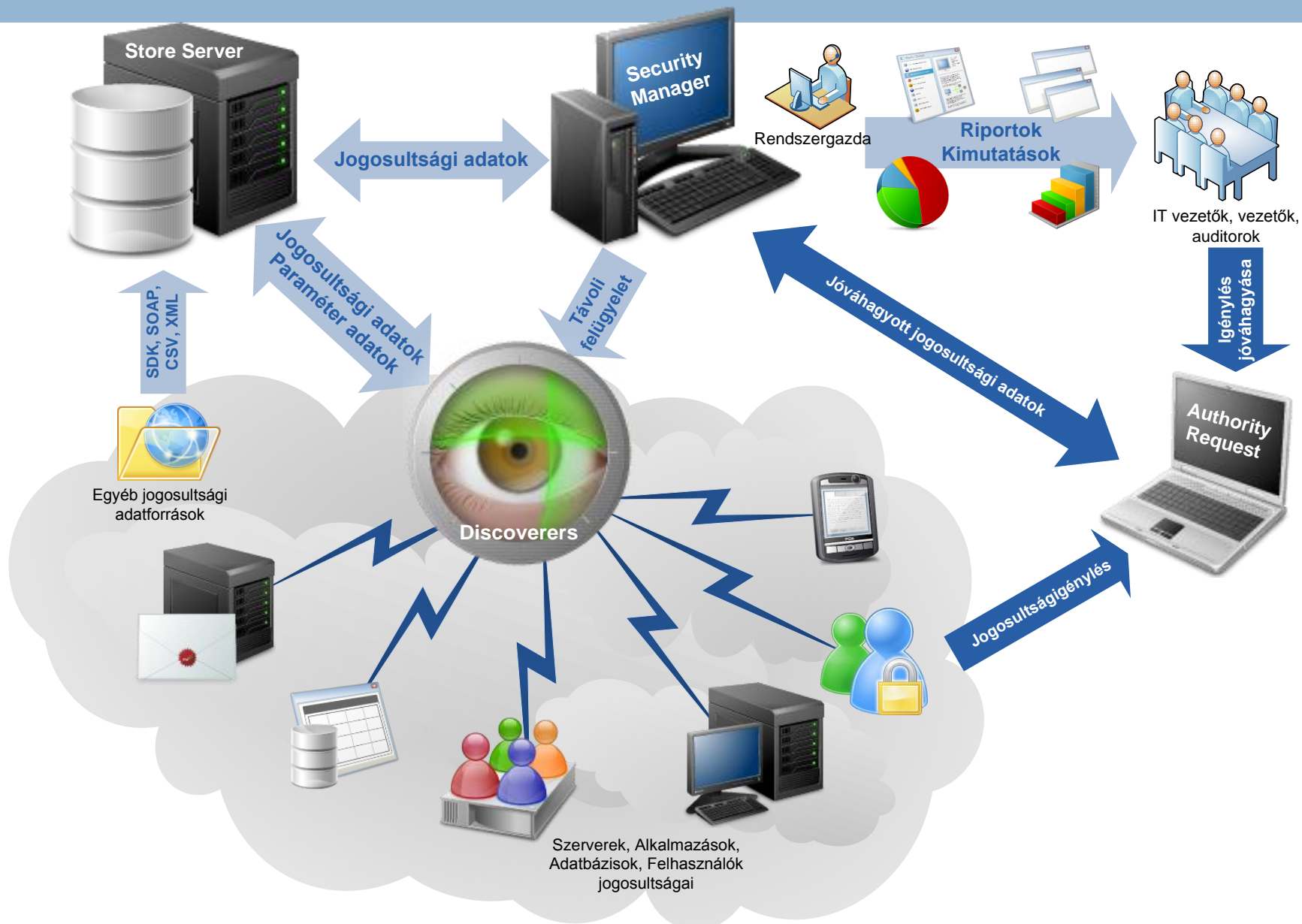


C:\Dokumentumok
\\Seacon\Seacon

Srvportal\Sarm
Srvportal\Helpdesk

http://intranet
http://project

Működési ábra



Felhasználási példák

- Rendszerüzemeltetők, rendszergazdák
 - ▣ Elemzések készítése
 - ▣ Anomáliák felderítése
 - ▣ Elvégzendő feladatok listája
- IT vezetők, vezetők
 - ▣ Előre definiált jelentések, statisztikák
- Auditorok
 - ▣ Megfelelőségi riportok

Bevezetési alapelvek

- Informatikai stratégia és IT biztonsági szabályozással összhangban
- Kockázatfelmérés alapján kritikus rendszerek mentén
- Vállalat működési folyamataiba integrált módon

Auditorok szerepe

- A fentiekhez hasonló rendszerek önmagukban nem működőképesek, a mesterséges intelligencia ellenére sem
- A megfelelő szinteken folyamatosan hozzá kell tenni azt a tudást és tapasztalatot, amit az auditorok és az egyéb szakértők az adott területeken felhalmoztak
- Ezzel együtt a hasonló képességű rendszerek jelentősen meg tudják könnyíteni mind a rendszerüzemeltetőket, mind az auditorok munkáját



Köszönöm

a

figyelmet!

csizmadia.attila@seacon.hu

www.sarm.hu

www.sealog.hu