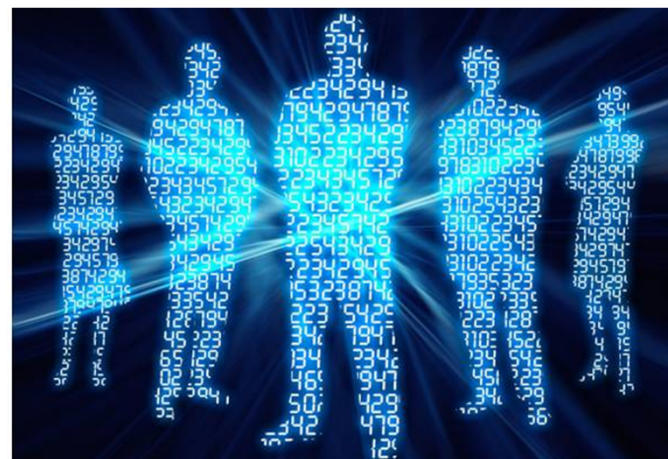


# Networkshop 2011

## Jogosultság-monitorozó rendszer kialakítása

# Jogosultságkezelés jelentősége

- Miért fontos?
  - ▣ Mindenkinek van valamilyen válasza
  - ▣ A válaszok különböző megközelítésűek lehetnek
  - ▣ Egy közös pont: **Kockázatok csökkentése**



# Jogosultságkezelés jelentősége

- Eszköz az adatvagyon védelmére
- Biztonságtudatosság
  - ▣ Kockázatok felmérése, tudatosítása, csökkentése
- Jogosultságok kézben tartása mint kockázatcsökkentés
  - ▣ Belső kényszer
  - ▣ Külső szabályozások (PSZÁF, ISO)

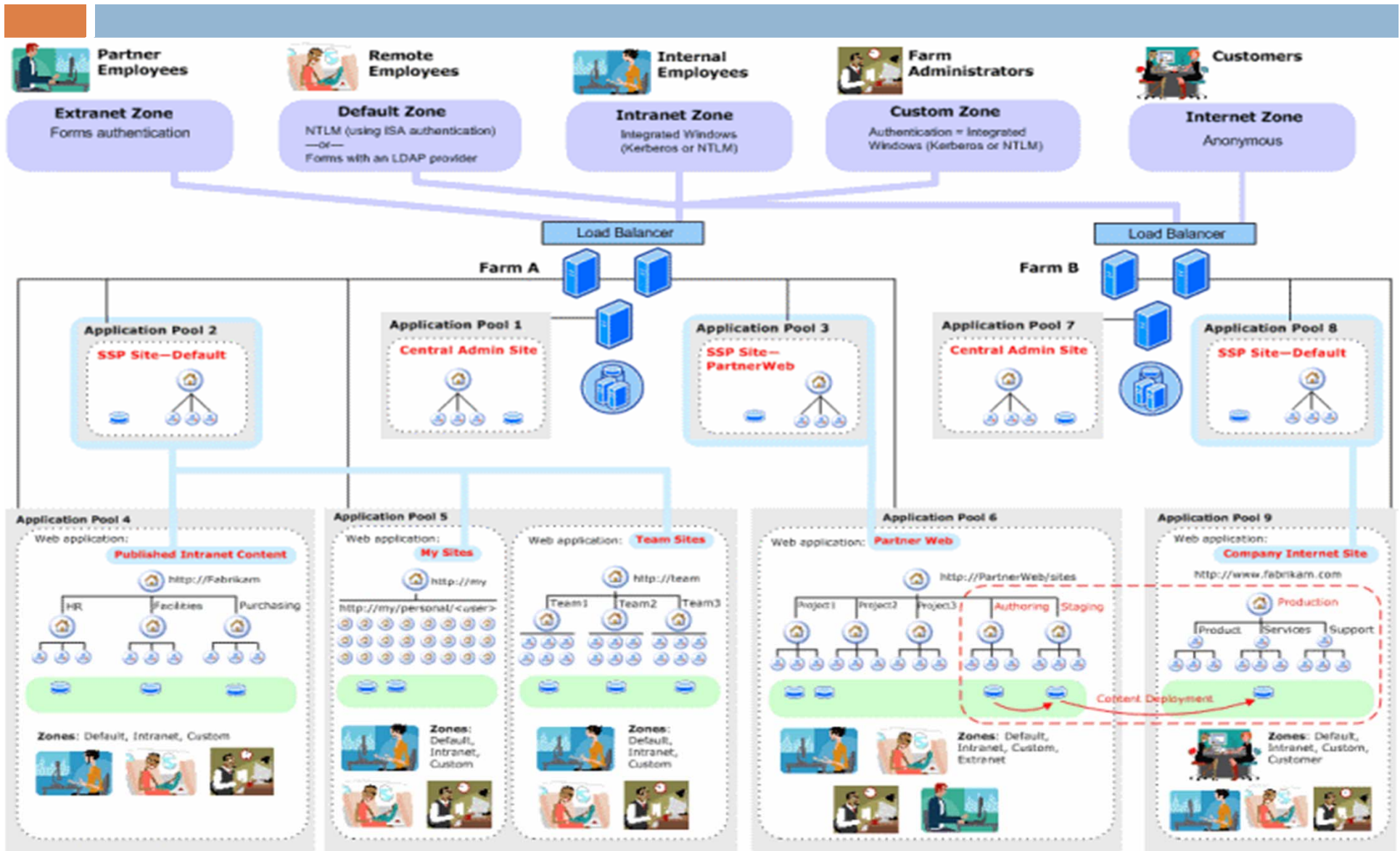


# Jogosultságkezelési kockázatok

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



# Példa jogosultsági struktúrára



# Gyakori kérdések

- Melyek azok a felhasználók, akik több jogosultsággal rendelkeznek, mint amit munkakörük megkíván?
- Egy adott felhasználó milyen fájlokhoz 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

- 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**



# 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 szemben támasztott elvárások

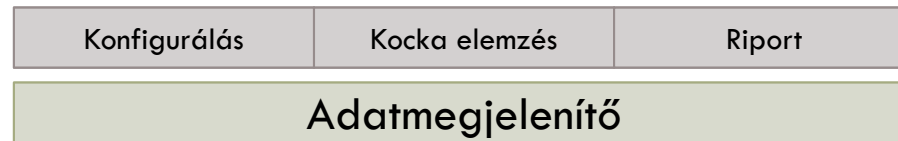
- Legyen moduláris és skálázható
- Mutassa meg az eltérést a tényleges helyzet és a vezetői szándék között
- Biztosítsa az adatok monitorozását és összetett elemzését
- Rendelkezzen fejlett riportolási képességekkel

# Elméleti felépítés

- A kialakítandó rendszer tulajdonképpen egy adattárház lesz, 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

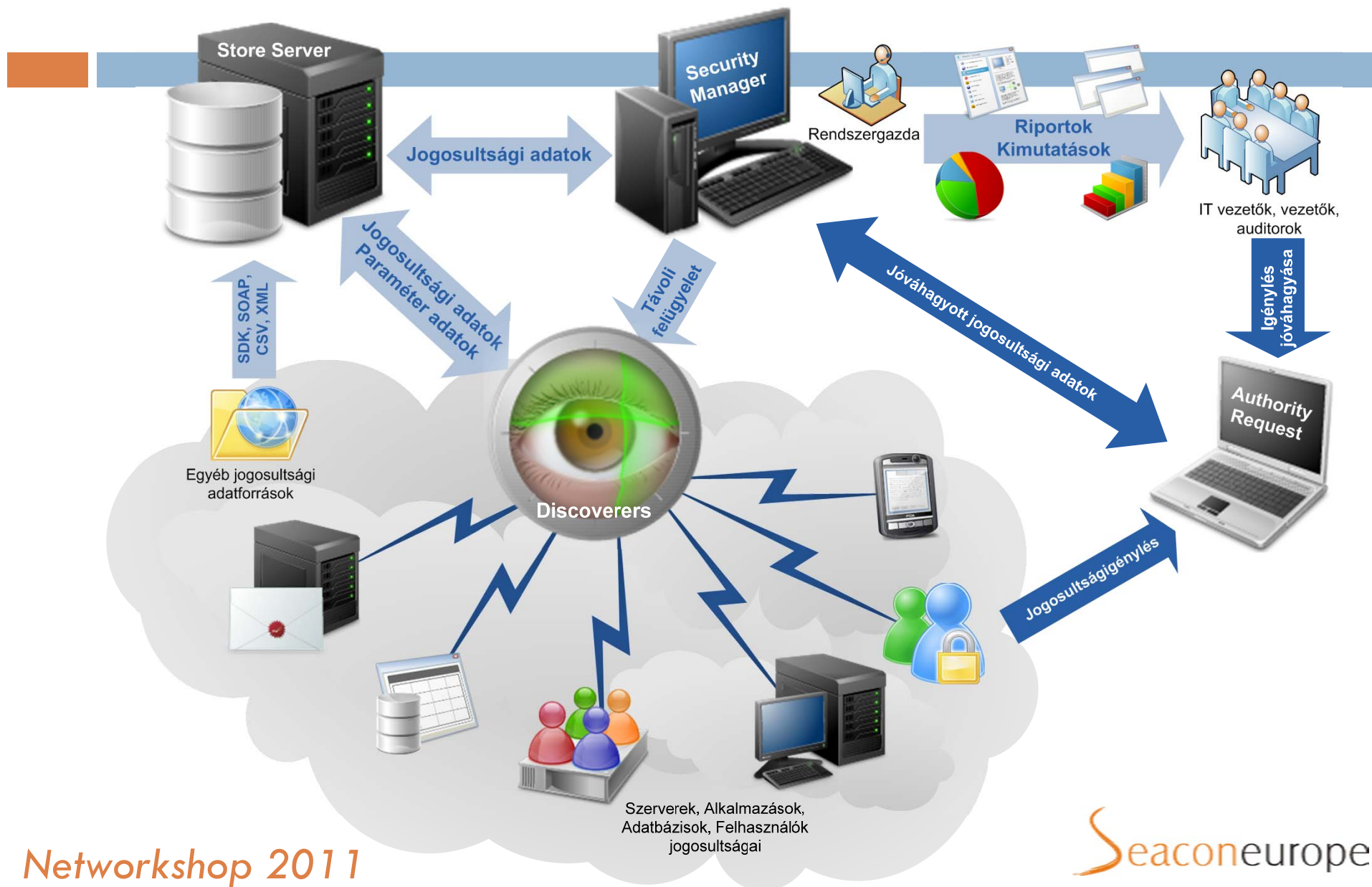


C:\Dokumentumok  
\\Seacon\Seacon

Srvportal\Sarm  
Srvportal\Helpdesk

http://intranet  
http://project

# Működési ábra



# Felhasználási példák

Reports

Beállítás riportok

- Konfigurációk gépenként.
- Forrás konfigurációk

Active Directory riportok

- Aktív domain felhasználók
- Letiltott domain felhasználók
- Domain felhasználók utolsó bejelentkezési idejük
- Lejárt domain felhasználók
- VPN felhasználói és csoportjai
- Erős jogosultságú csoportok tagjai**

Fájl és hálózat riportok

- Top 30 fájl típus méret szerint
- Top 30 fájl típus darabszám szerint
- Legrégebben módosított fájlok
- Tulajdonosok fájlainak mérete
- Tulajdonosok fájlainak száma
- Fájl és hálózat felhasználói és csoportjai

SQL adatbázis riportok

- SQL adatbázis felhasználói és csoportjai
- SQL adatbázisok objektumainak száma

Jogosultság riportok

- Jogosultsággal rendelkező felhasználók és csoportok

Letiltott domain felhasználók | Domain felhasználók utolsó bejelentkezési idejük | Lejárt domain felhasználók | VPN felhasználói és csoportjai | **Erős jogosultságú csoportok tagjai**

### Erős jogosultságú csoportok tagjai

Lista Megmutatja az erős jogosultsággal rendelkező csoportok tagjait

Nyomtatás Export

Filter

Group name

Domain Admins; ... X

Név	Teljesnév	Típus	Tag név	Tag teljesnév	Tag típus
SEACONSRV\Domain Admins	Domain Admins	Domain biztons...	SEACONSRV\Ad...	Admin - Tartomán...	Domain biztons...
SEACONSRV\Domain Admins	Domain Admins	Domain biztons...	SEACONSRV\Ad...	Administrator	Domain felhaszn...
SEACONSRV\Domain Admins	Domain Admins	Domain biztons...	SEACONSRV\csi...	Csizmadia Attila	Domain felhaszn...
SEACONSRV\Domain Admins	Domain Admins	Domain biztons...	SEACONSRV\sea...	SeaLogReader	Domain felhaszn...
SEACONSRV\Domain Admins	Domain Admins	Domain biztons...	SEACONSRV\sea...	SeaLogTest	Domain felhaszn...
SEACONSRV\Domain Admins	Domain Admins	Domain biztons...	SEACONSRV\xlo...	xlogload	Domain felhaszn...

Count = 6

# Bevezetési alapelvek

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



Köszönöm

a

figyelmet!

[csizmadia.attila@seacon.hu](mailto:csizmadia.attila@seacon.hu)  
[www.sarm.hu](http://www.sarm.hu)

Networkshop 2011

Seaconeurope