

Innovatív Információbiztonsági Megoldások



Seacon Access and Role Management

□ Miért fontos?

- Mindenkinnek van valamilyen válasza
- A válaszok különböző megközelítésűek lehetnek

- Egy közös pont: **Kockázatok csökkentése**



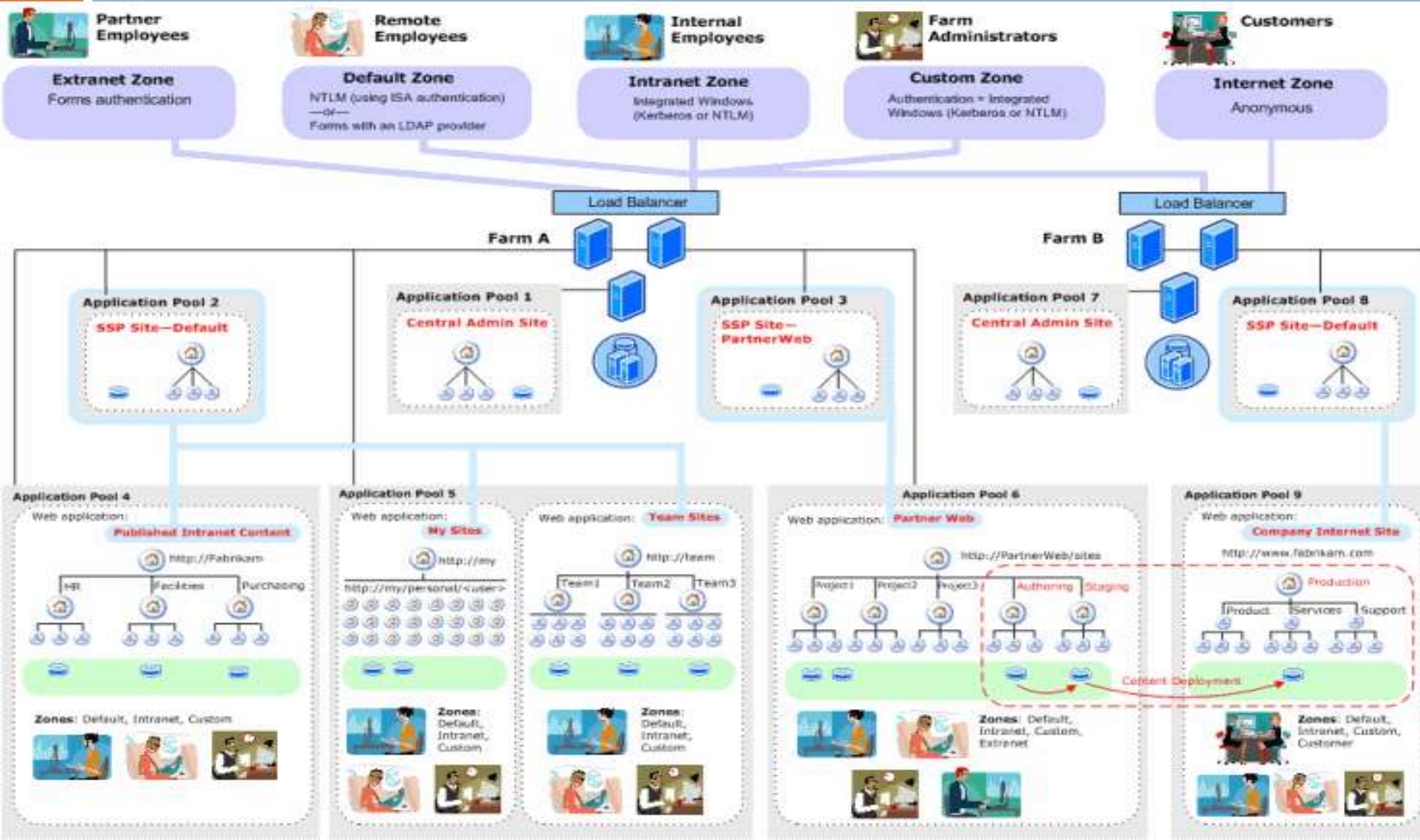
- Eszköz az adatvagyon védelmére
- Biztonságtudatosság
 - ▣ Kockázatok felmérése, tudatosítása, csökkentése
- Jogosultságok kézben tartása mint kockázatcsökkentés
 - ▣ Belső kényszer
 - ▣ Külső szabályozások (PSZÁF, ISO)



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



Példa jogosultsági struktúrára



- 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?

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



**Nincs információ
a tényleges helyzetről**

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

A tényleges jogosultsági állapot feltérképezésére nincs magyar KKV szinten megfizethető megoldás

- Kutatási-fejlesztési projekt keretén belül innovatív megoldás keresése - GOP 1.3.1 /A
 - Egységes jogosultságellenőrzés
 - Többszintű, moduláris, skálázható
 - „Felderítő robotok”
 - Begyűjtött információk adatbázisba
 - Összetett elemzések
 - Fejlett riportolás
 - Igénylési folyamat támogatása
 - Vezetői szándék és tényleges állapot

- A pályázathoz kapcsolódó know-howk
 - Bevezetési módszertan
 - Szabályzati ajánlások
 - Robotok szerepe a jogosultságok ütemezett vizsgálatára
 - Jogosultságigénylési módszertan
 - Hatékony megjelenítési formák

- 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)

Adatok felépítése

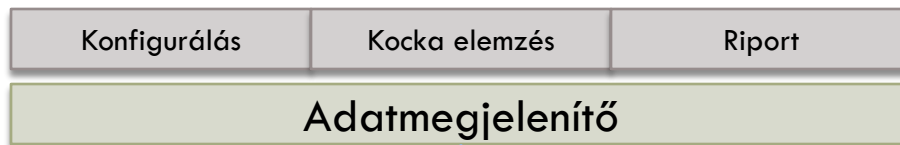


- 4 fő adatkörre épül:
(Kinek, min, milyen jogosultsága van)
 - ARO: **Felhasználók, csoportok**
 - SEACONSrv\harmat.krisztian
 - SEACONSrv\Domain Users
 - ACO: **Objektumok**
 - C:\Dokumentumok\Bemutató.pptx
 - http://project/PWA/Gop
 - ACE: **Jog**
 - Olvasás, írás, törlés, ...
 - ACL: **Jogosultság**
 - A fenti három adatkör kapcsolata

Valós felépítés



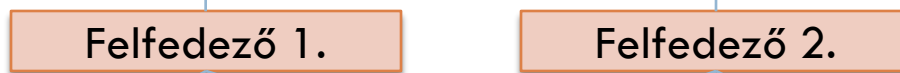
Adatmegjelenítő - elemző (Security Manager – Kocka, Riport)



Adattároló (Store Server - OLAP)



Felfedezők (Discoverer - ETL)



Adat források



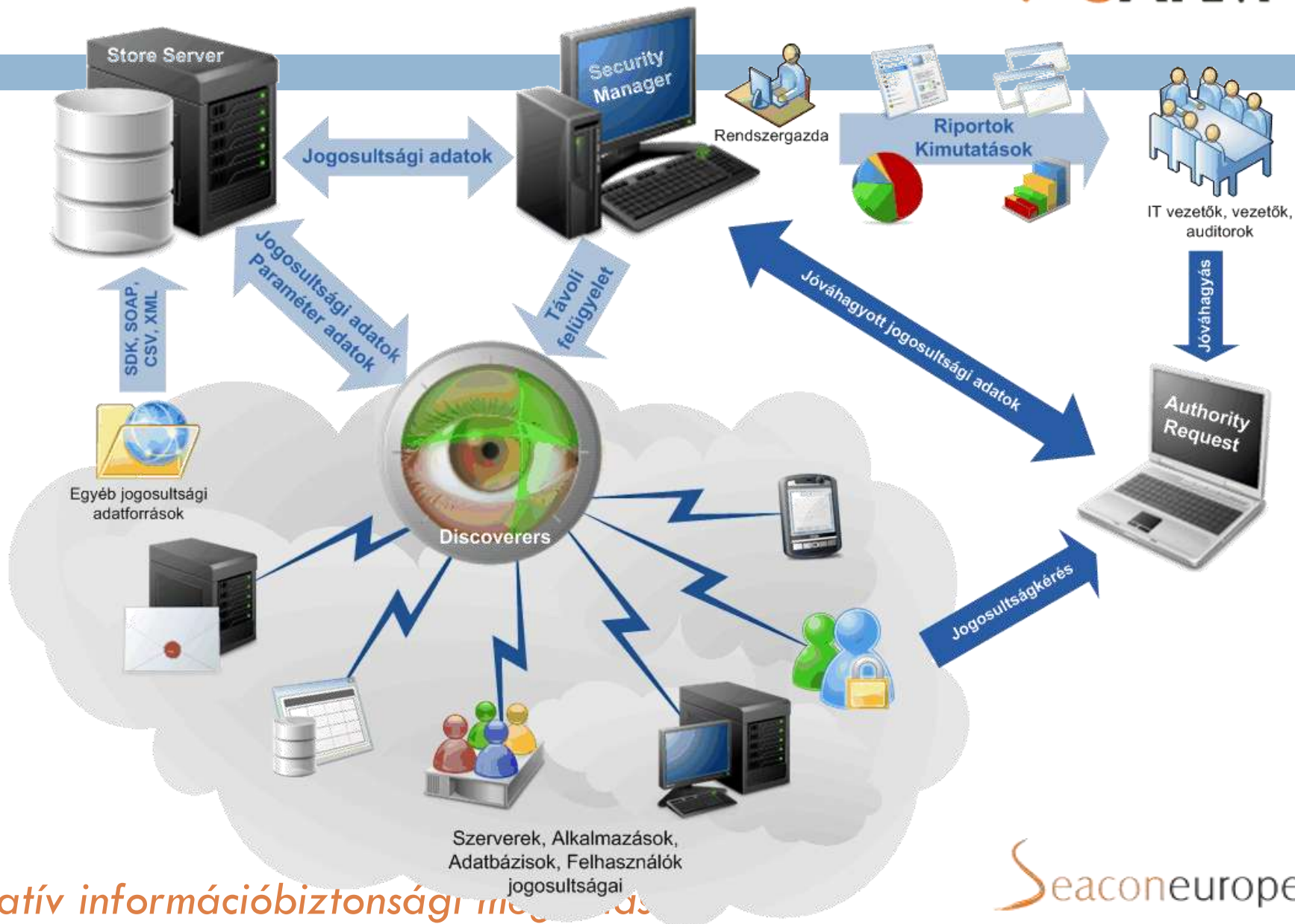
C:\Dokumentumok
\\Seacon\Seacon

Srvportal\Sarm
Srvportal\Helpdesk

http://intranet
http://project



Működési ábra



A SARM képességei



- Megfigyelt rendszerek
 - Active Directory
 - Windows File System
 - MS SQL
 - Egyedi rendszerek

- **Architektúra**
 - Discoverer – Windows Service
 - Store Server – Adatbázis szerver
 - Security Manager – Vastagkliens
 - Authority Request - Vékonykliens
- **Rendszerkövetelmények**
 - Szerver - Windows Server 2003-tól
 - Kliens - Windows Xp-től
 - Adatbázis - MS SQL 2005-től
 - .Net keretrendszer 3.5-től

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

A SARM specialitásai

- Áttekinthető, beszédes menüszerkezet
- Igényelt jogok és a valódi beállítások összevetése
- OLAP-szerű elemzés, több dimenzió mentén, a legapróbb részletekig
- Gráfos megjelenítés, lefűréssel
- Előre definiált riportok
- Egyedi rendszerek jogosultsági adatainak manuális fölvitele

A SARM előnyei

- Saját fejlesztés
- Modulonként illeszthető, skálázható és bővítésre nyitott rendszer
- Egyedi igények kielégítése
- SeaLog integráció
- Kisvállalattól, a középvállalati szinten keresztül, egészen a nagyvállalati környezetig

A SARM Központi Jogosultságkezelő Menedzsment Rendszer **jól menedzselhetővé – ellenőrizhetővé és átláthatóvá – teszi a jogosultságkezelési munkát, ezáltal radikálisan csökkenti a jogosultság kezelési kockázatokat**

Továbblépési lehetőségek

- Egyedi rendszerek beépítése
- Eddig látókörön kívül eső rendszerek implementálása
- Riportok, listák folyamatos bővítése

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

Köszönöm

a

figyelmet!

csizmadia.attila@seacon.hu