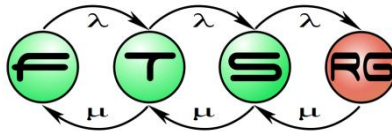


Szabályalapú rendszerek, eseményfeldolgozás

Gönczy László

gonczy@mit.bme.hu

Bergmann Gábor és az OptXware Kft. anyagainak felhasználásával



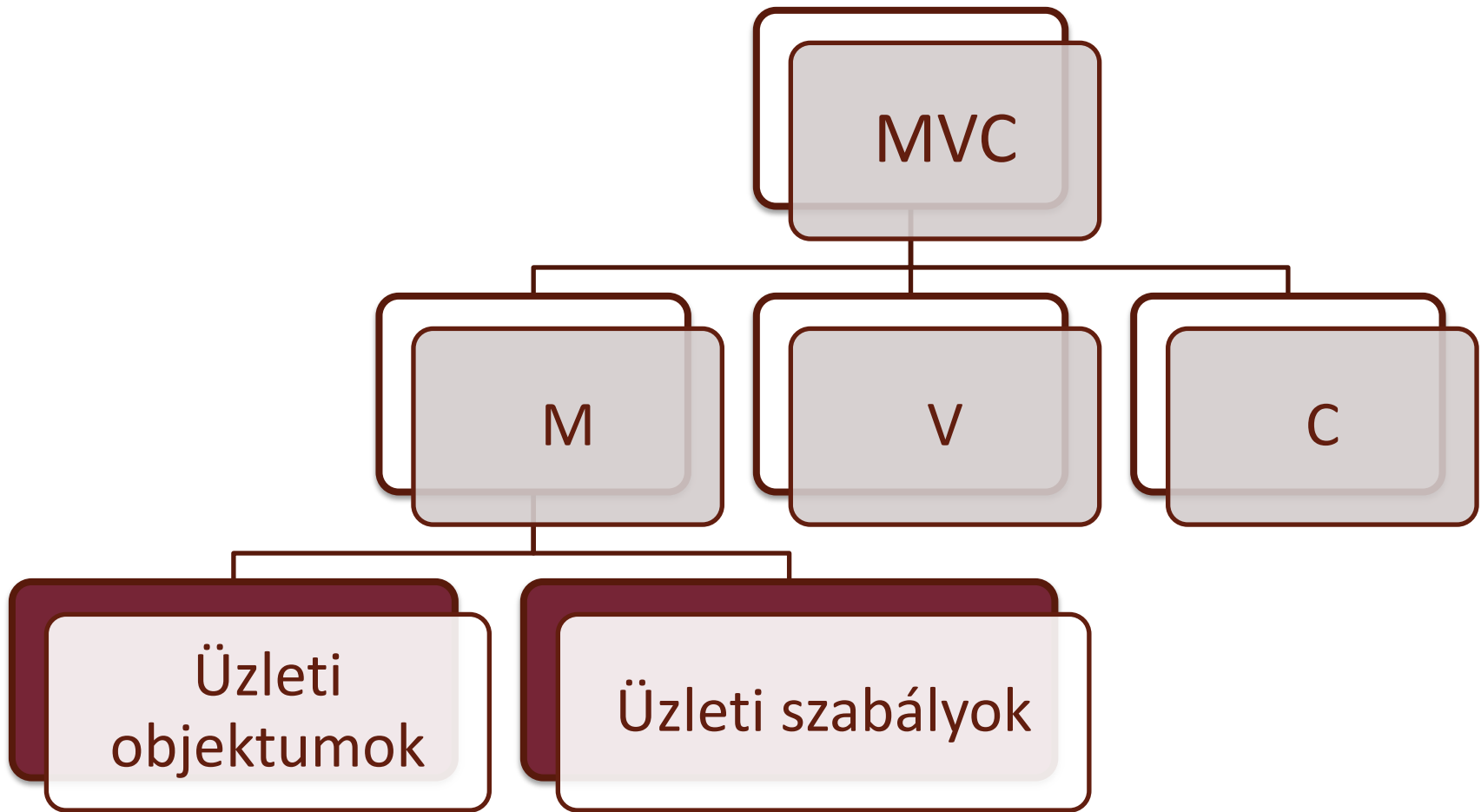
Tartalom

- Szabályalapú logika
- DROOLS
- Szabályalapú megközelítés felhasználása: CEP
- Esettanulmány: CoMiFin

Szabályalapú üzleti logika

Business Rule Systems

- Szabály alapú üzleti logika



Üzleti szabályok

- **Üzleti logika** „kiszervezésére” végrehajtható modell
- **Üzleti objektumokat** figyelhet, manipulálhat
- **Felépítése:** ha-akkor
 - „ha az ügyfél 30 év alatti, emeljük 35%-al az ajánlatot”
 - „ha az ügyfél egyenlege 500Ft alá csökkent, értesítsük”
 - „ha más ügyfél korábban bejelentkezett már azonos lakcímre, nem adunk kedvezményt”
 - „ha a hallgatónak legalább húsz lezárt féléve van, nem szerzett aláírást diplomatervezésből és nem kapott köztársasági elnöki engedélyt, akkor megszüntetendő a jogviszonya, feltéve hogy ötéves képzésre jár és az ezt előíró jogszabály hatályba lépése óta kezdte tanulmányait”

Szabály alapú üzleti logika előnyei

- Dedikált szabálytár
 - Üzleti logika könnyebben módosítható
 - Pont ez **változhat** leggyakrabban: új rendeletek, stb.
- **Redundancia elkerülése**
 - Ugyanaz az üzleti logika sok modulban megjelenhet
- Jó esetben az **üzleti döntéshozók** is tudják olvasni
 - Sőt, akár írni is: természetes nyelvi verbalizáció
- Hatékony végrehajtás
- Cserélhető körülötte az architektúra
- „Externalizáció”, karbantarthatóság
- Eszköztámogatás

Felhasználási területek - példák

- Biztosítók, bankok
 - Kalkulációk kiemelése
 - Szabályok következetes kikényszerítése
 - Ügyek elbírálásának támogatása
- E-Kormányzat
 - Regisztráció kiértékelése
 - Adó, járulékszámítás
- Logisztika
 - Szállítmányozási döntések támogatása

BRMS – szolgáltatások

■ Szabálytár

- Kereshető, automatizáltan módosítható
- Verziózás

■ Végrehajtó könyvtár, végrehajtó szerver, SOA

■ Tool support

- IDE, webes felület
- Template lehetőség
- Magasabb granularitású szabályok
- Tesztelési támogatás, gyors próba
- Üzleti szótár építése meglévő adatokból

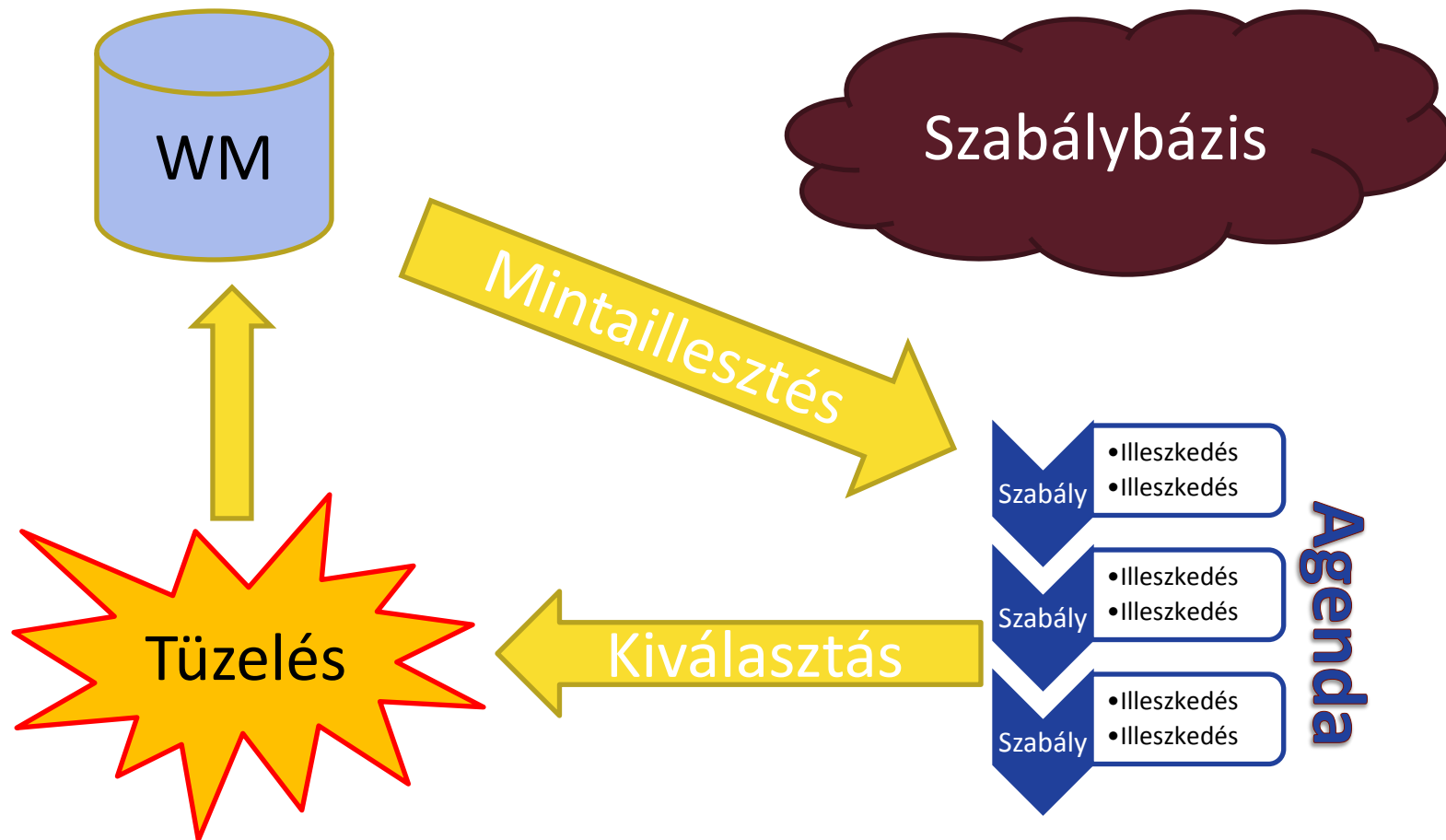
Szabály alapú rendszerek

- Adottak tények
 - „**Ténybázis**” / munkamemória
 - Változatos felépítés
- Adottak szabályok, amelyekkel új tényeket lehet kapni
 - „**Szabálybázis**”
 - Felépítés: ha-akkor
- Végül egy következtető mechanizmus

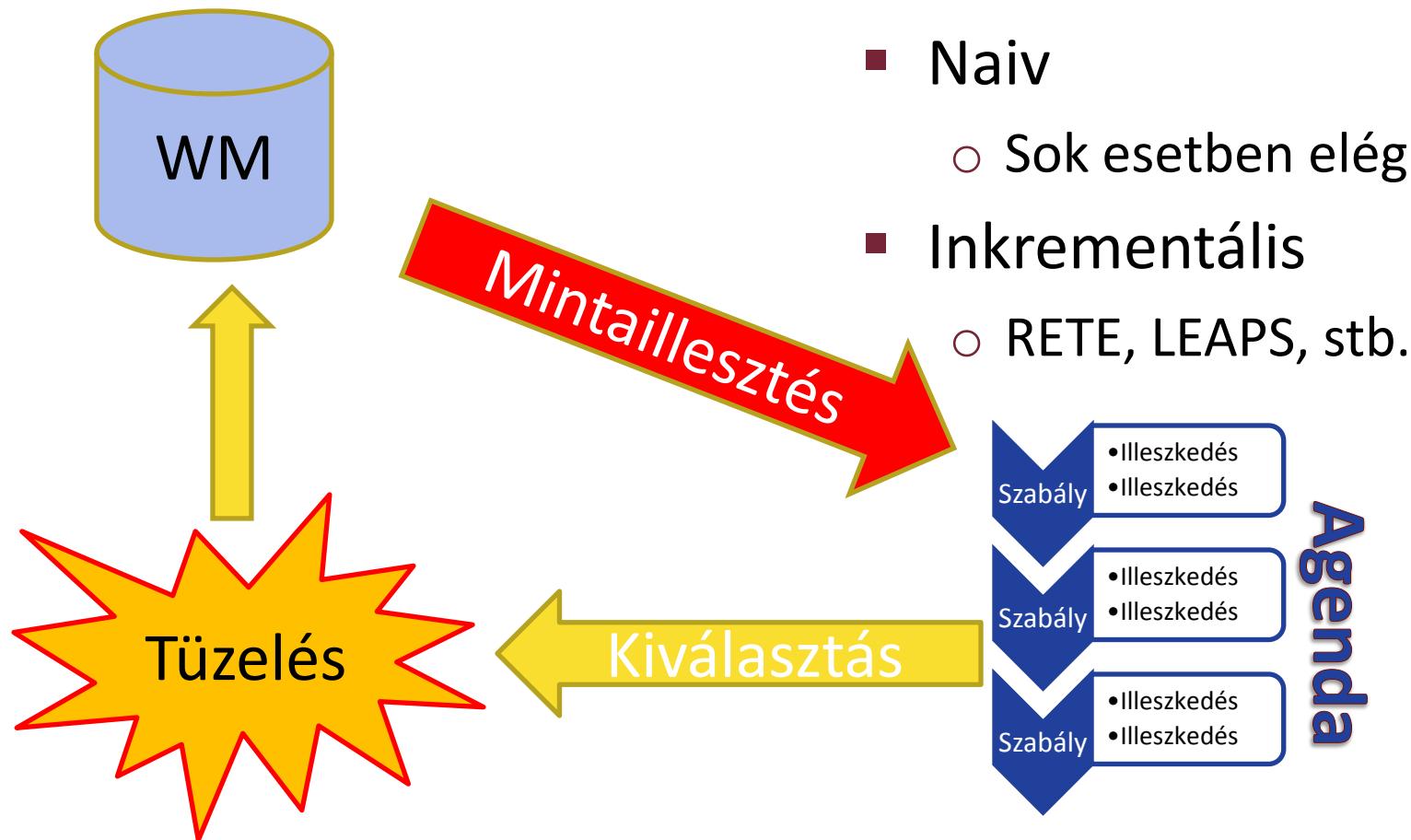
Következtetés

- **Előre** láncoló (induktív/produkciós, adatvezérelt)
 - A tényekből újabb tényeket képez
 - Analógia: generatív nyelvtan
 - Ilyenek például a üzleti szabályrendszerek
- **Hátra** láncoló (deduktív, igényvezérelt)
 - Egy cél-állítást próbál visszavezetni alaptényekre
 - Analógia: parser
 - Ilyen például a *Prolog* és számos szakértői rendszer

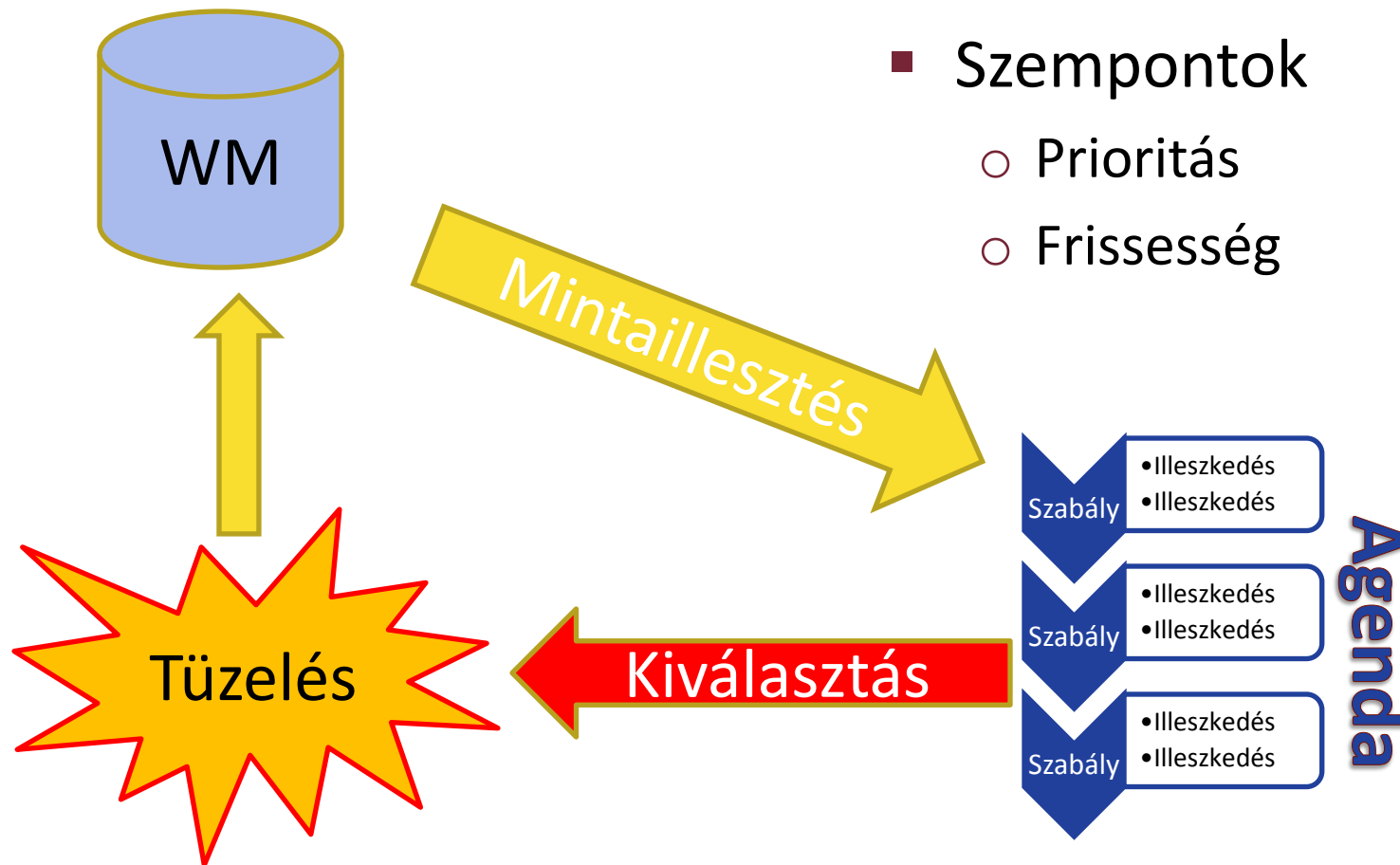
Egyszerű előre láncoló rendszer



Egyszerű előre láncoló rendszer

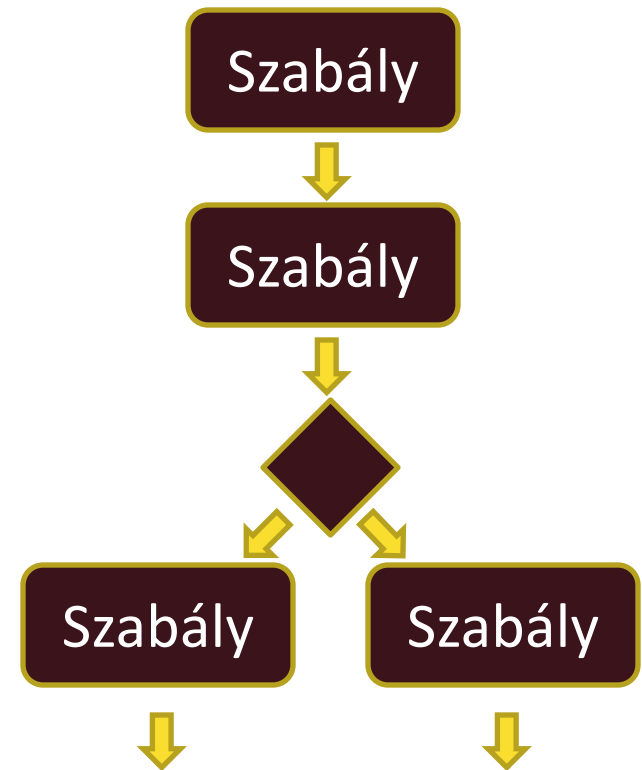


Egyszerű előre láncoló rendszer



Előre láncoló rendszer vezérlése

- Leállítás
 - STOP szabály után
 - Ha nincs több tüzelhető szabály
- Komplex rendszer: vezérlési folyamat
 - Pl. UML Activity Diagram
 - Kiválthatja a bemutatott ciklust
- Eseményvezéreltség is elképzelhető
 - „Alvó” szabályok
 - Külön utasítás nélkül



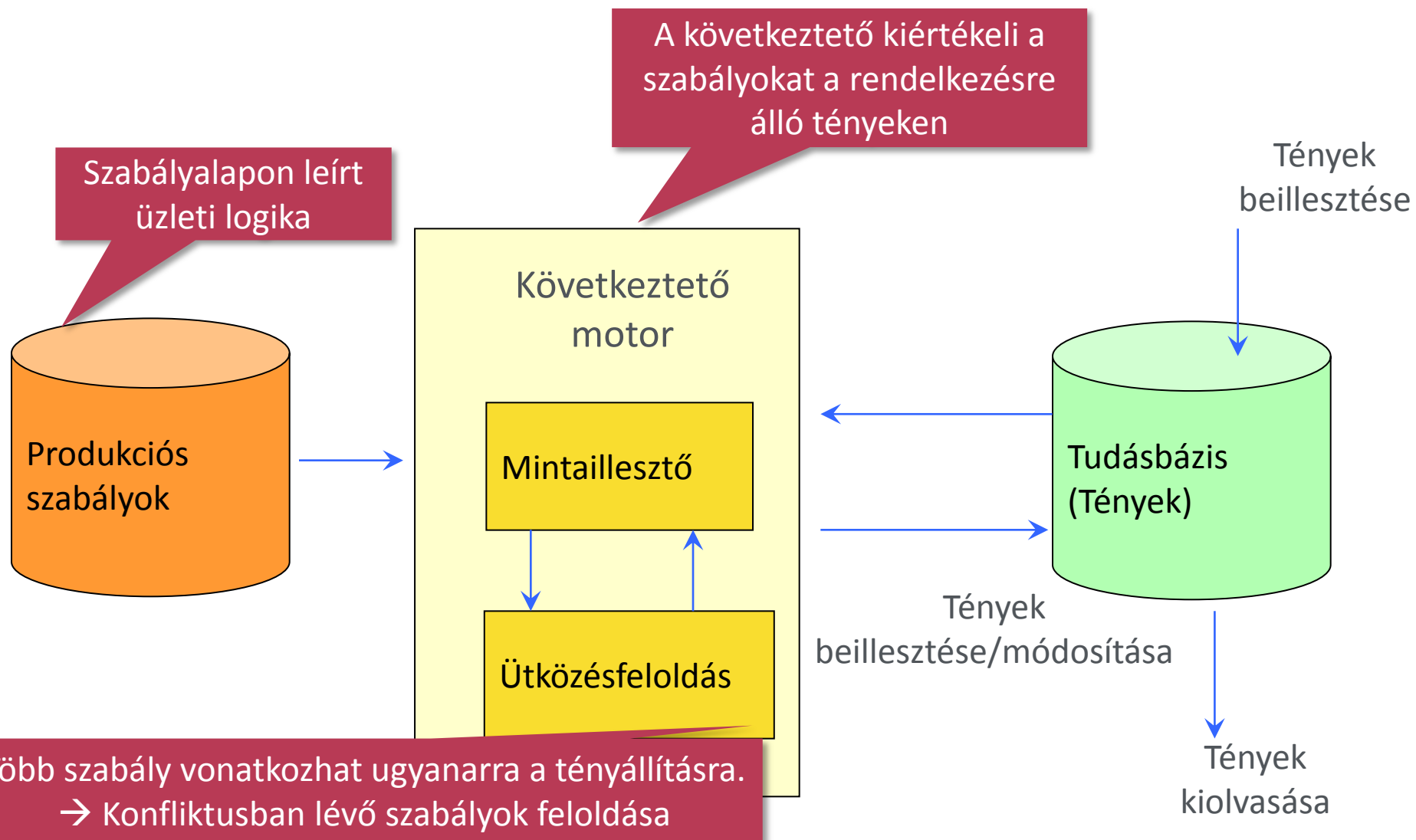
BRMS

- BRMS = **Business Rule Management System**
- Számos termék
 - *G2, JBoss Rules, IBM ILOG (J)Rules, Blaze Advisor, MS BRE, TIBCO iProcess,*

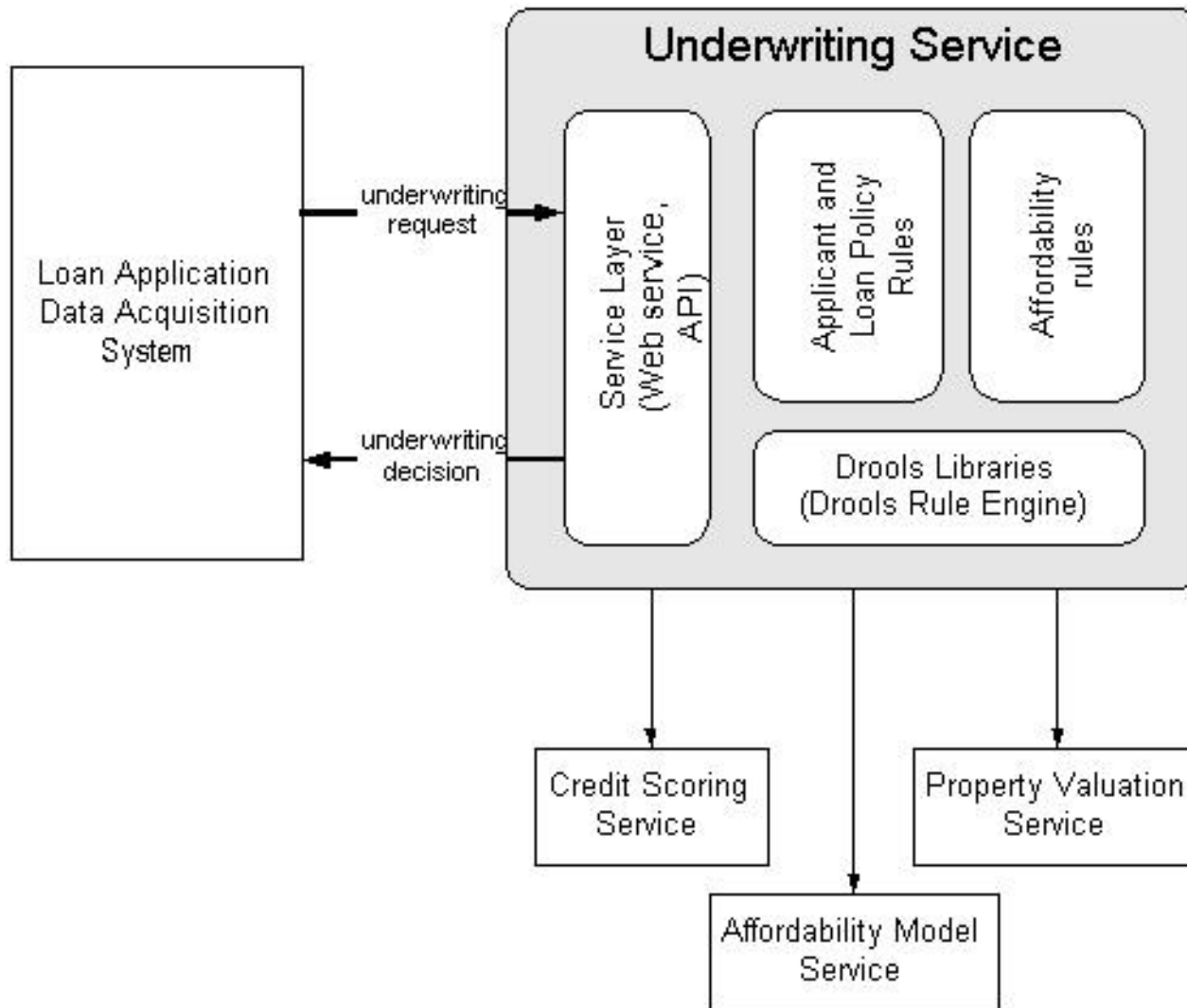
Microsoft®



BRMS működés



Példa alkalmazás



<http://onjava.com/onjava/2007/01/17/building-enterprise-services-with-drools-rule-engine.html>

Drools Expert

- Szabály szerkesztő + végrehajtó környezet
 - Eclipse alapú szerkesztés
 - Java engine, beágyazható
- Szabályok bevitele
 - Kódolás (Java, mvel)
 - Döntési táblából (Excel)
 - „Természetes nyelvű” szövegből
 - Egyszerű GUI-n (Guvnor)
 - Domain Specific Language: ~ template nyelv
- Szabály felépítése
 - Deklaratív feltétel (Left Hand Side)
 - Akció (Right Hand Side)

Összetett szabályok

rule "We have an honest Politician"

salience 10

when

exists(Politician(honest == true))

then

insertLogical(new Hope());

end

rule "Hope Lives"

salience 10

when

exists(Hope())

then

System.out.println("Hurrah!!!
Democracy Lives");

end

rule "Hope is Dead"

when

not(Hope())

then

System.out.println("We are all
Doomed!!! Democracy is Dead");

end

rule "Corrupt the Honest"

when

politician : Politician(honest == true)

exists(Hope())

then

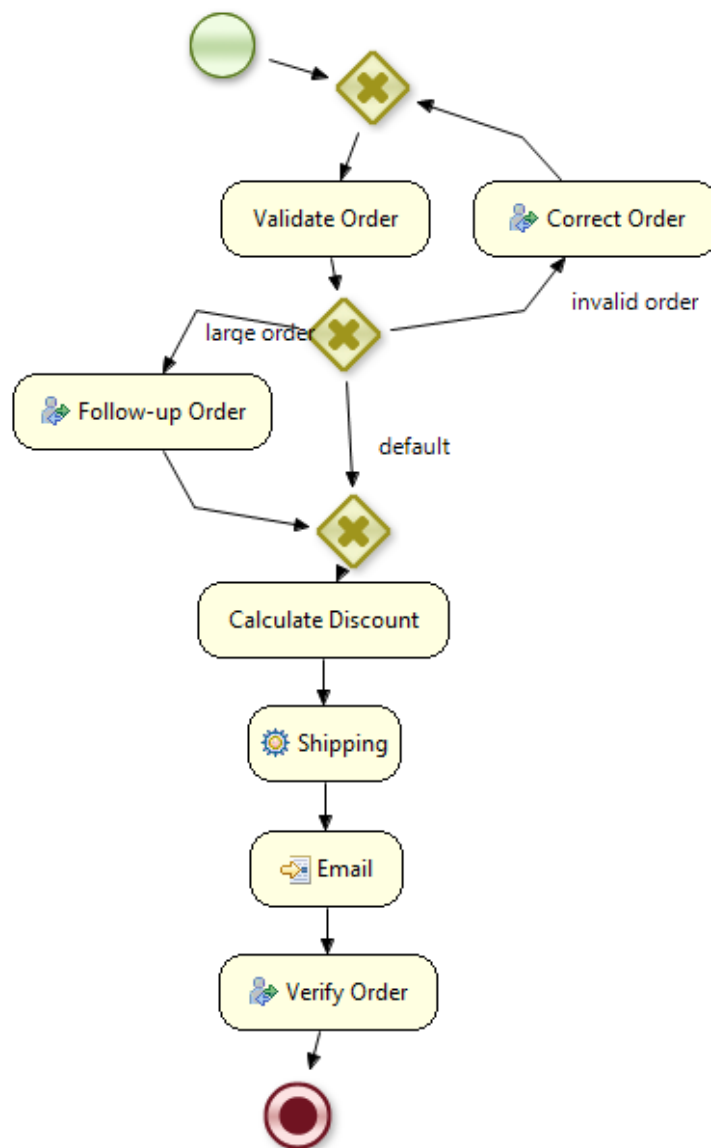
System.out.println("I'm an evil
corporation and I have corrupted " +
politician.getName());
modify(politician) {
 setHonest(false)
}

end

Drools Flow

- Szabályok vezérlése
 - Prioritás használatával
 - „Implicit módon” – megfelelő elő és utófeltételek, állapotváltozó
 - Explicit módon: egy tipikus használati módnak megfelelően
- Szabályok közti sorrendezés
 - RuleFlow vagy BPMN nyelven
 - Nem explicit vezérlés
- Nyelvi elemek
 - Szabály (csoportra) hivatkozó akció (ruleflow-group)
 - Emberi lépés
 - Automatizált lépések (script, email, ...)
- Testreszabhatóság
 - Szakterület specifikus lépések

Flow példa



Szabályalapú megközelítés alkalmazása

Complex Event Processing
Stream Processing

CEP alapelvek

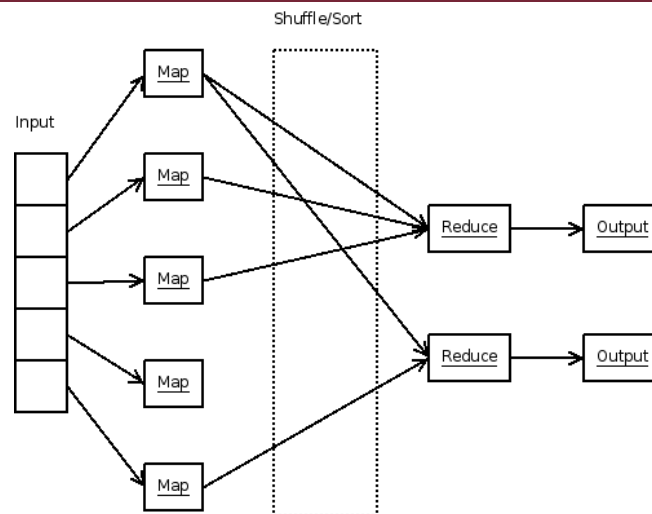
- „Komplex esemény”
 - Több elemi esemény összekapcsolása
- Tulajdonságok
 - Időzítések figyelembevétele (pl. csúszóablak)
 - Aszinkron működés
 - Oksági kapcsolatok, hierarchikus események
 - Korreláció
- SQL-szerű query nyelvek
 - Pl. EPL: Event Processing Language
 - Feldolgozási folyamatba láncolható lépések
- Elosztott adatforrások
 - Adatbázisok, beérkező kérések, megfigyelt események, stb.
- Skálázhatóság
 - Cloud környezet

CEP alkalmazási területek

- Üzleti alkalmazások
 - Tőzsde, befektetések
 - „Treasury”
 - Kockázatkieértékelés
 - Hitelek árazása
 - Szállítmánykövetés
- „Business Activity Monitoring”
- Online visszaélések felderítése/megelőzése
 - Gyanús tranzakciók ellenőrzése
 - Fogadási adatok elemzése (pl. UEFA)
- Nagy IT rendszerek üzemeltetése
 - Komplex támadások felderítése
 - Metrika kiértékelés
- Biztonságtechnika
 - Pl. dDOS ellen
- <http://www.complexevents.com/>

Map/Reduce algoritmus

- Map lépés
 - adat felosztása
- Reduce lépés
 - adat feldolgozása
- Példa
 - szöveg felosztása szavakra, szavak számának megállapítása
- Számos programnyelven
- Apache implementáció
 - Elosztott megoldás
 - Hadoop (+ Hadoop Distributed File System)
 - Ütemezés : Job Tracker, Task Tracker



CEP eszközök

- Esper
- Drools Fusion
- IBM InfoSphereStreams (System S)
- OpenESB - Intelligent Event Processor
- Apache Hadoop + ráépülő projektek
- Döntési szempontok
 - Eseményfeldolgozási logika
 - Áteresztőképeség
 - Elvárt válaszidő („low latency”)

Esettanulmány: CoMiFin

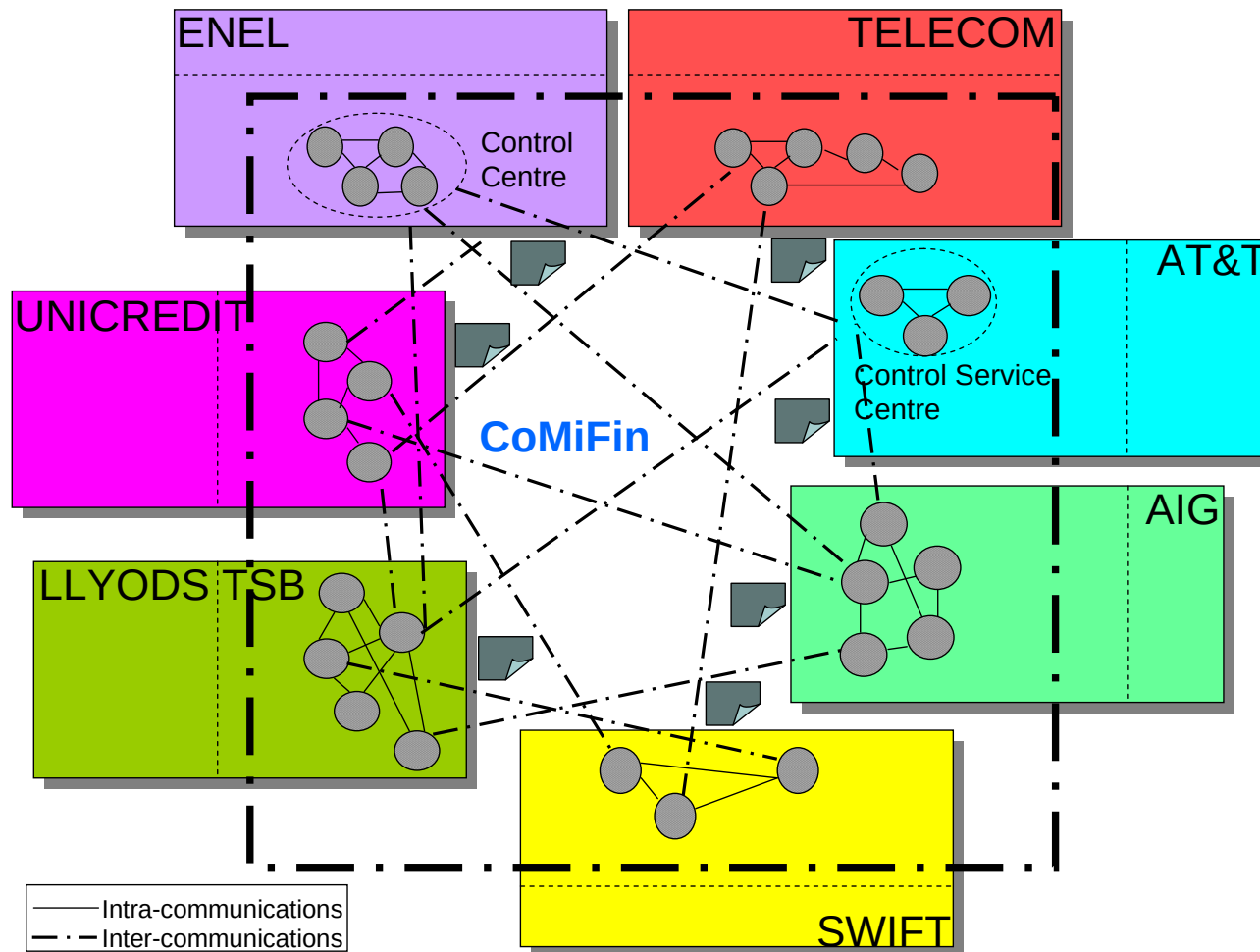
Szolgáltatásalapú rendszerek, modellvezérelt fejlesztés,
komplex eseményfeldolgozás,...

Esettanulmány: CoMiFin

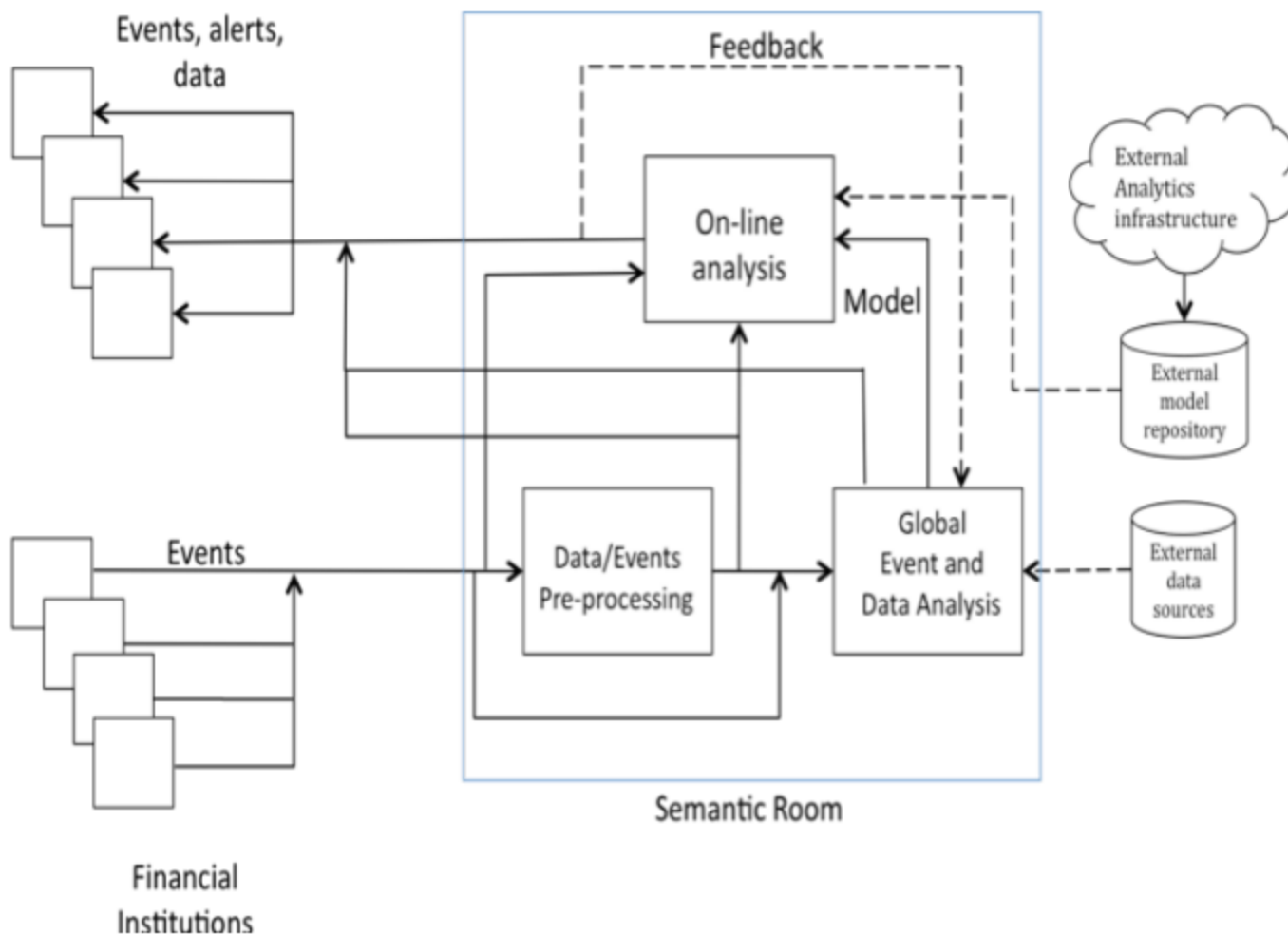
- „Communication Middleware for Financial Infrastructures”
- Motiváció
 - Banki rendszerek egyre erősebben függenek külső szolgáltatóktól
 - Támadások egyre kifinomultabbak
 - Kritikus infrastruktúrák (pl. mobilhálózat, áramellátás, Internet) elleni komplex támadások kivédése
 - Hagyományos kommunikáció lassú (példa: 8 nap egy eset lezárása)
- Cél
 - Scheme to set up and manage a secure environment (software, hardware, monitoring tools, etc.) for information exchange and analysis
- Tanszéki spin-off (OptXware) vezette a demonstrátor fejlesztését



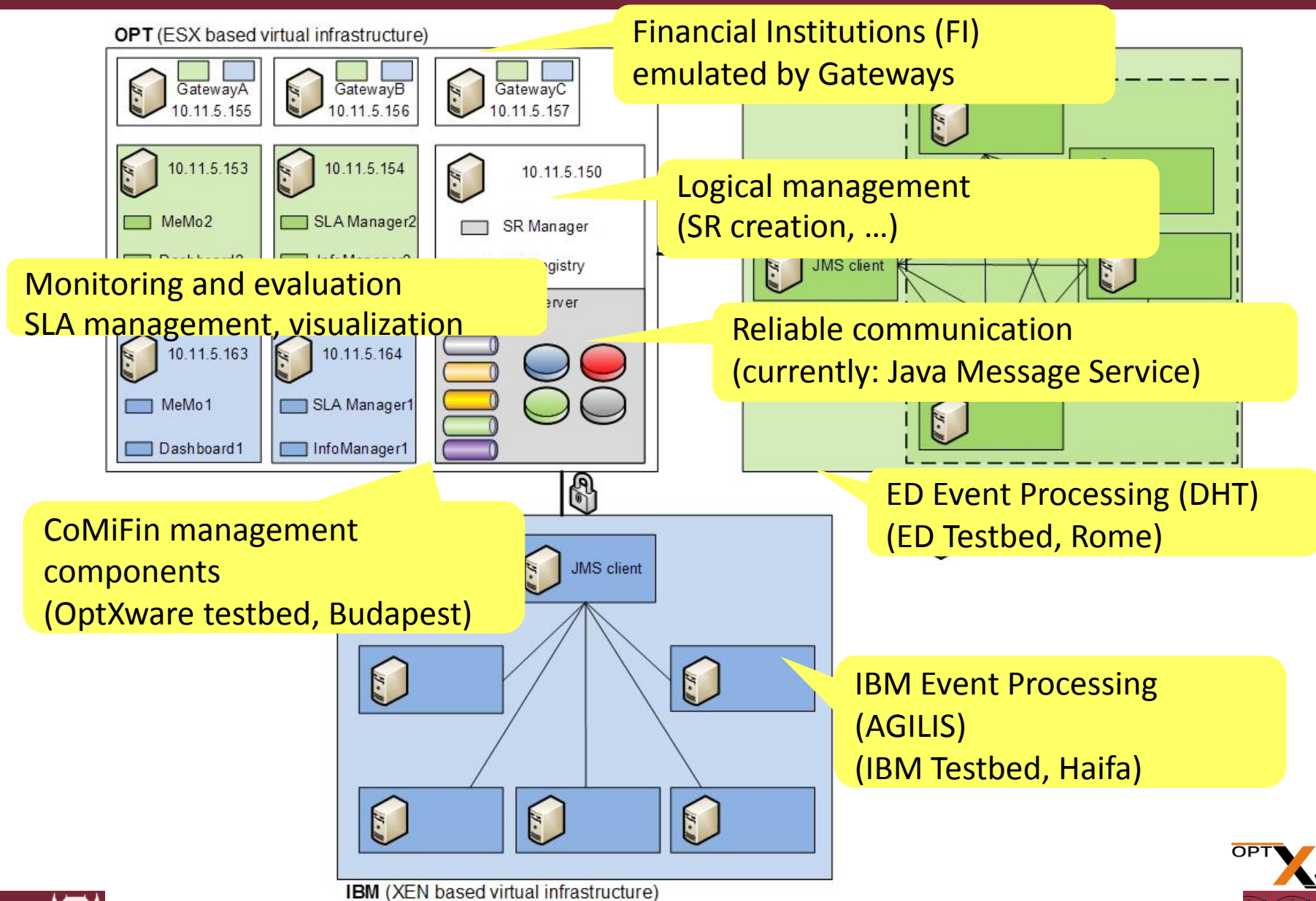
Logikai architektúra



Online adatfeldolgozás (CEP)



Architektúra



Eredmények megjelenítése

JBoss Portal 2.7.2-GA - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://10.11.5.153:8080/portal/auth/portal/Dashboard/6_AlertList

Most Visited Getting Started Latest Headlines

Popup blocker detected

JBoss Portal 2.7.2-GA

Alert details (time, source, target, etc.)

Logged in as: sr_manager

Dashboard | Copy to my dashboard | Logout

Home 5_SR_Manager_Page 6_AlertList

AlertList

Date	Origin	Participating FIs	Type	Description	Affected Services	Suspicious FIs	Priority
2010-07-01 10:07:43.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service15	1X.16X.XX.X89	-0.1799294
2010-07-01 10:07:43.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service15	13X.X5X.XX.X5	-0.181737
2010-07-01 10:07:37.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service12	6X.8X.X0X.X	-0.1778012
2010-07-01 10:07:37.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service4	17X.XX.X3X.X29	-0.1718082
2010-07-01 10:07:32.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service8	20X.XX.X4X.X5	-0.1802342
2010-07-01 10:07:31.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service8	21X.XX.XX.X79	-0.175243
2010-07-01 10:07:27.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service11	19X.X1X.X0X.X05	-0.183489
2010-07-01 10:07:27.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service11	10X.X2X.X1X.X02	-0.1774248
2010-07-01 10:07:26.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service10	6X.13X.X2X.X73	-0.1799292
2010-07-01 10:07:26.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service10	6X.13X.X2X.X73	-0.182237
2010-07-01 10:07:09.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service10	6X.13X.X2X.X73	-0.18592
2010-07-01 10:07:08.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service11	19X.X1X.X0X.X05	-0.1923068
2010-07-01 10:07:08.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service10	6X.13X.X2X.X73	-0.1886134
2010-07-01 10:07:08.0	DHT Analytics	Bank of Noldor	ALERTMitM	Statistical anomaly detected	Service10	9X.16X.X5X.X24	-0.1909274
2010-07-01 10:07:06.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service8	19X.XX.XX.X79	-0.1778006
2010-07-01 10:07:05.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service14	8X.20X.X4X.X6	-0.1798036
2010-07-01 10:07:05.0	DHT Analytics	Bank of Vanyar	ALERTMitM	Statistical anomaly detected	Service14	8X.20X.X4X.X6	-0.1798036

Service effected

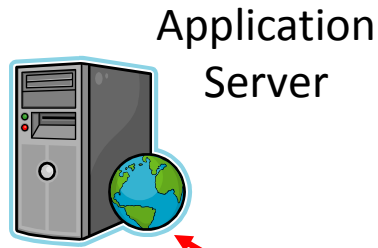
Score on the alert

Done

Session Hijack detektálás

- Session hijack: felhasználó forgalmának figyelésével beleavatkozni a munkamenetbe
- Környezet: egyszerű e-Banking alkalmazás
 - Felhasználók kezelése
 - Tranzakciók indítása
- Alkalmazás specifikus információ monitorozása
 - Kliens IP címe
 - Session azonosító
- „Hibainjektálás”

Session Hijacking



Ordinary Client

Bad Guy

Main Page

Welcome **Ordinary Client!**

Your IP address at login time was: 127.0.0.1, your current IP is: 10.11.1.248

Your session ID is: 82B02592FCD04883F13B1C29272642AA

You can choose one of the following actions

Transfer Money

Your previous transfer of 2000 to 12345 has been accepted.

Amount:

IBAN:

Transfer

Empty fields

Logout

Please [click](#) to logout.

Main Page

Welcome **Bad Guy!**

Your IP address at login time was: 10.11.1.248, your current IP is: 10.11.1.248

Your session ID is: A3ED6B154F6F303B808B056AF6923CBC

You can choose one of the following actions

Transfer Money

Amount:

IBAN:

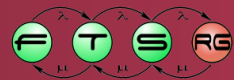
Transfer

Empty fields

Logout

Please [click](#) to logout.

OPTXWARE



Session hijack detektálás

- Az IP és a session ID Drools alapú ellenőrzésével

WARNING: possible session hijack:

```
{  
  currentAddress=127.0.0.1,  
  remoteAddress=127.0.0.1,  
  sessionId=21...B6  
}
```

and the possible attacker with the same session:

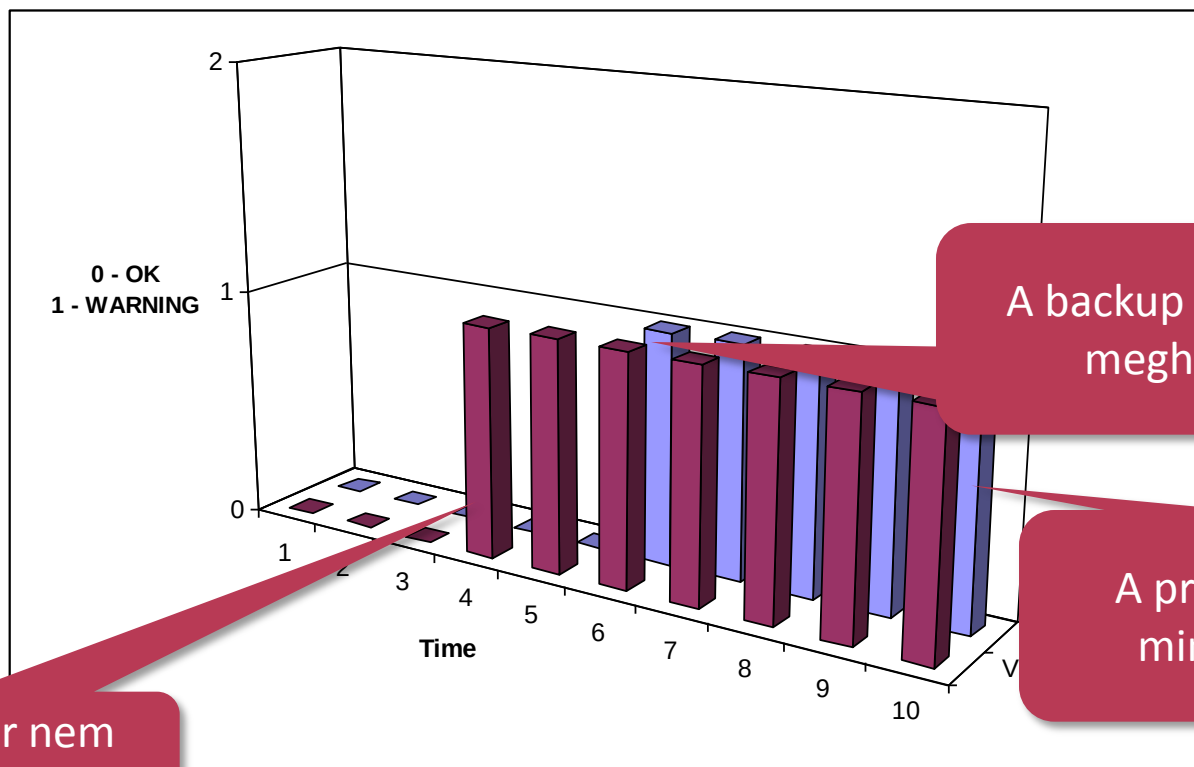
```
{  
  currentAddress=10.11.1.154,  
  remoteAddress=127.0.0.1,  
  sessionId=21...B6  
}
```

Demonstrations

- Demo 2: Készedelmes backup felderítése
 - Több alkalmazásból érkező információ
 - Komplex esemény
 - Vonatkozó előírások:
 - e.g. COBIT PO-4 “Define the IT Processes, Organization and Relationships”
 - COBIT PO-9 “Manage IT Human Resources”

Késedelmes mentés detektálása

- Monitorozott szolgáltatások
 - Backup (storage alrendszer, adatbázis, stb.)
 - Az adminisztrátor bejelentkezése
- Időzítés szimulációs alapon



Adminisztrátor nem
aktív

A backup valamiért
meghiúsult

A probléma még
mindig fennáll

Drools alapú detektálás

```
[root@p2 NagiosDrools5]# sh runSimulator.sh "2009-10-10 10:10:10" 0.01
Press enter to start simulation
```

```
Press enter to stop simulation
```

```
Next sleep time is 1800
```

```
Next sleep time is 1200
```

```
Next sleep time is 1800
```

```
Next sleep time is 1200
```

```
Next sleep time is 1800
```

```
Next sleep time is 1200
```

```
Next sleep time is 1800
```

```
Next sleep time is 1200
```

```
Next sleep time is 1800
```

```
Next sleep time is 1200
```

```
Next sleep time is 1800
```

```
Next sleep time is 3000
```

```
Insertion of events finished
```

```
[root@p2 NagiosDrools5]#
```

```
INFO: Feeder has been started
```

```
Press enter to exit
```

```
insert new (later than 09.10.10 10:10:10.000) service checks (1)
```

```
insert new (later than 09.10.10 10:13:10.000) service checks (1)
```

```
## There is an administrator missing ServiceCheck(3): 10:15:10.000 (1)
```

```
insert new (later than 09.10.10 10:15:10.000) service checks (1)
```



Message from Drools and Nagios



There could be a missing backup which is not known by the administrator

```
## There is an administrator missing ServiceCheck(7): 10:25:10.000 (1)
```

```
insert new (later than 09.10.10 10:25:10.000) service checks (1)
```

```
## There could be a missing backup which is not known by the administrator
```

```
## Missing backup: ServiceCheck(8): 10:28:10.000 (1)
```

```
insert new (later than 09.10.10 10:28:10.000) service checks (1)
```

```
## There is an administrator missing ServiceCheck(9): 10:30:10.000 (1)
```

```
insert new (later than 09.10.10 10:30:10.000) service checks (1)
```

