Kádár Sándor, üzletágvezető

2007. április 22.

SYNERGON

Incidens menedzsment heterogén környezetben

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

Az incidens menedzsment célja

SYNERGON

- Problémák:
  - Az informatikai rendszerekben a naplóesemények elosztottan keletkeznek.
  - Minden rendszert külön kell analizálni.
  - A naplóesemények kizárólagosan az adott rendszerre vonatkozóan biztosítanak információt.
  - Az elemzést csak az adott rendszer szakavatott ismerője képes értelmezni.
  - Riasztások is csak az adott rendszerre vonatkozóan definiálhatók az adott rendszer képességeinek függvényében.
  - A False Positive riasztások száma magas lehet.

Az incidens menedzsment célja

SYNERGON

Megoldások a problémákra

Probléma	Megoldás
A naplóesemények elosztottan keletkeznek.	Központosított naplógyűjtés
Külön kell analizálni.	Egységesített eszköz az elemzéshez
Naplóesemények az adott rendszerre vonatkoznak.	Minden naplóesemény egyidejű elemzése
A rendszer szakavatott ismerője képes értelmezni.	Normalizált eseménykezelés

Az incidens menedzsment célja

SYNERGON

Megoldások a problémákra

Probléma	Megoldás
Riasztások csak az adott rendszerre vonatkozóan definiálhatók.	Egységesített rendszerben komplex szabályalapú riasztások alkalmazása
Riasztások az adott rendszer képességeinek függvényében	Professzionális riasztási alkalmazás
A False Positive riasztások száma magas lehet.	Megfelelően konfigurált szabályalapú riasztások

Heterogén rendszerek kapcsolódása

SYNERGON

- A heterogén rendszerek kapcsolódásának kritikus feladata az információátadás módja. Az átadás leggyakoribb esetei:
  - Napló állomány olvasása incidens menedzsment által
  - Adatbázis olvasása incidens menedzsment által
  - Naplóüzenetek küldése incidens menedzsmentnek, mint napló szervernek
  - SNMP üzenetek küldése

Elemzések normalizációja

- Heterogén rendszerek összekapcsolásakor másik feladat a különböző rendszerek különböző üzeneteinek egységes értelmezése.
- Az összegyűjtött naplóeseményeket automatizáltan kell átfordítani az incidens menedzsmentben az egységesített megfelelőjére.
- A megfeleltetést automatizáltan is tudnia kell frissíteni az új verziók megjelenésével.
- A normalizációt a hasznos információk sérülése nélkül kell megoldani.

Korrelációs lekérdezések, szabályrendszerek

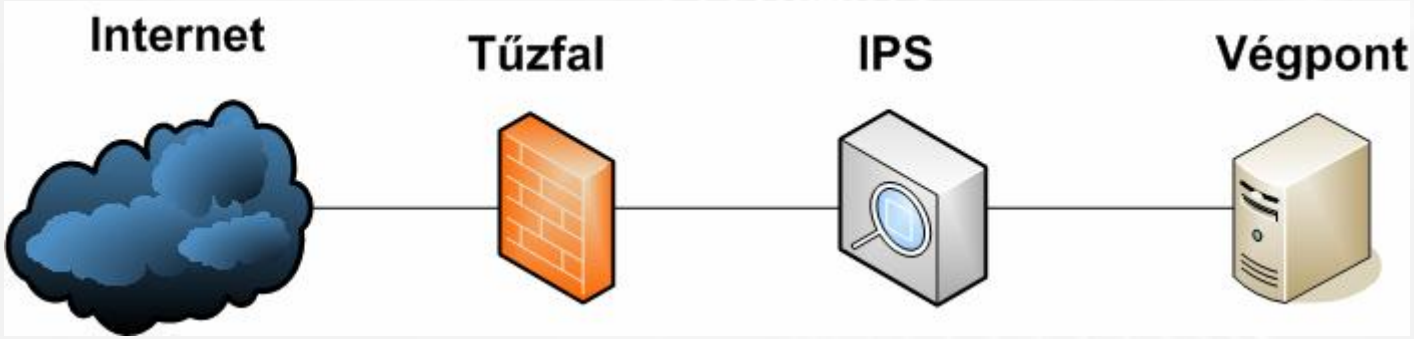
SYNERGON

- Az összegyűjtött és normalizált információkat egységesen kell kezelni.
- A rendszerekre vonatkozóan összefüggéseiben kell vizsgálni az eseményeket – egy esemény önmagában még nem feltétlenül kritikus.
- Sérülékenység vizsgálati adatokkal kiegészítve tovább finomíthatóak a riasztások, a false positive riasztások száma csökkenthető.

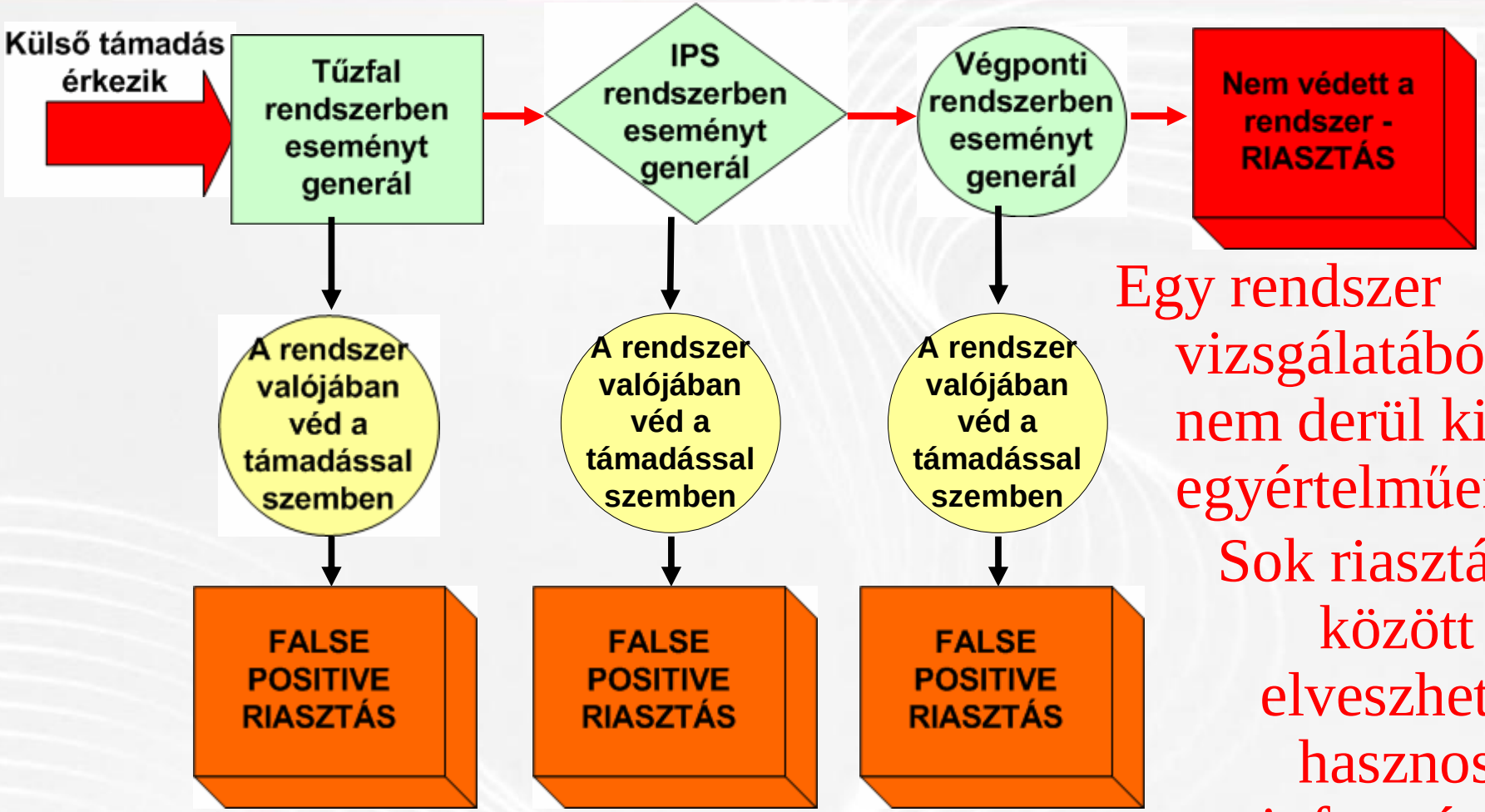
Korrelációs lekérdezések, szabályrendszerek

SYNERGON

Példa

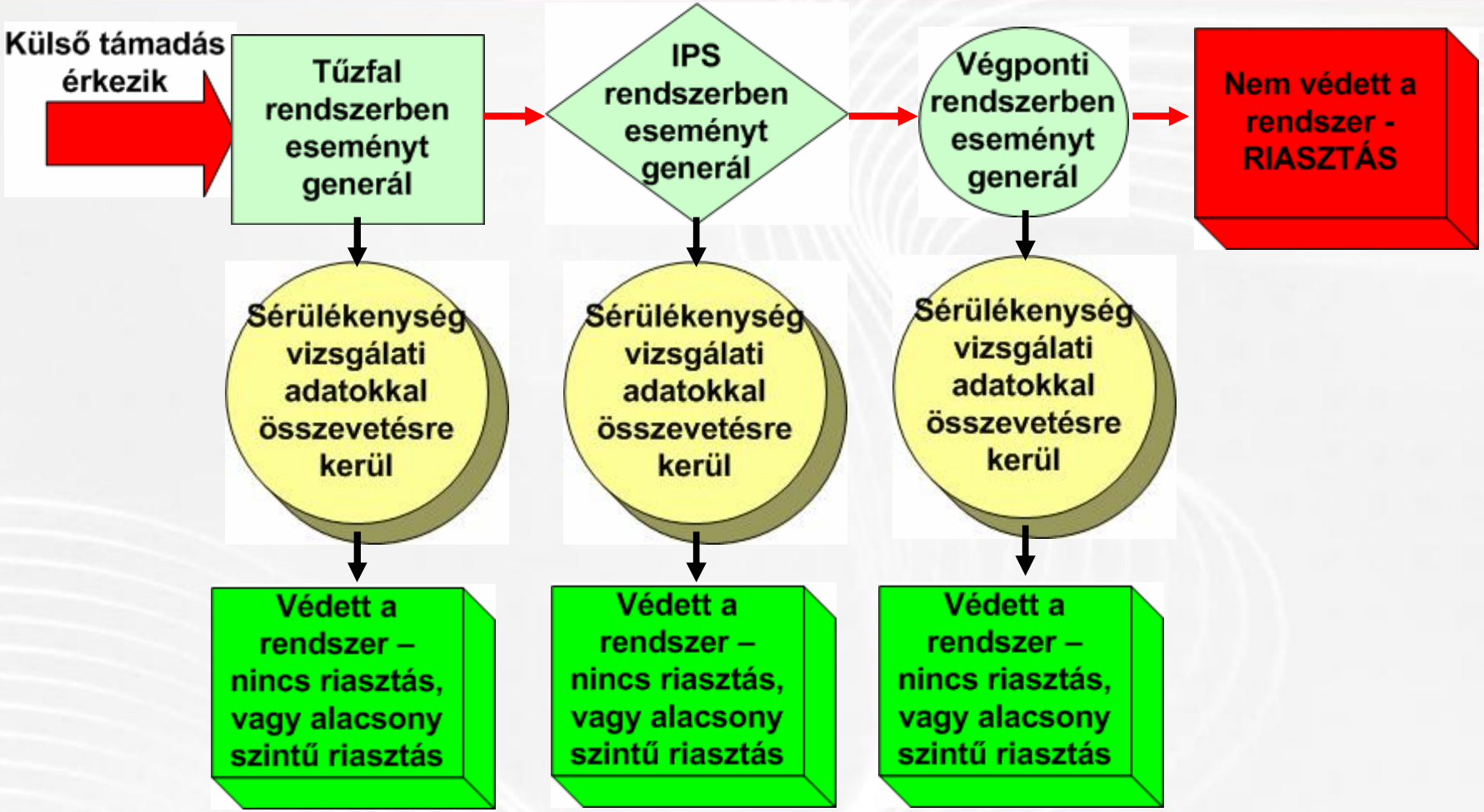


Korrelációs lekérdezések, szabályrendszerek



Egy rendszer vizsgálatából nem derül ki egyértelműen Sok riasztás között elveszhet a hasznos információ

Korrelációs lekérdezések, szabályrendszerek



Kádár Sándor, üzletágvezető

2007. április 22.

SYNERGON

Köszönöm figyelmüket!

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON