kancellar.hu
AZ INFORMATIKAI BIZTONSÁG SZAKÉRTŐJE

Hiteles, elosztott log kezelés

nagyvállalati környezetben
Log4ensics-szel

Duna Tower, 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704tel, f: +36 1 2704fax, e: info@kancellar.hu, w: kancellar.hu

WE HAVE A STRATEGIC PLAN.

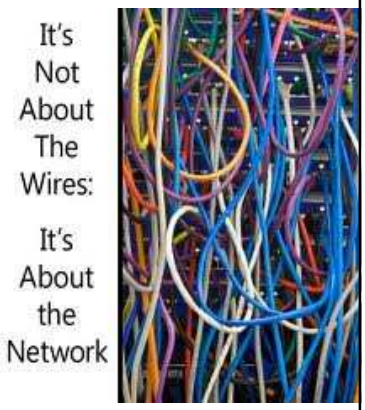
Duna Tower, 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704tel, f: +36 1 2704fax, e: info@kancellar.hu, w: kancellar.hu

IT'S CALLED DOING THINGS.

Herb Kelleher

Mi az igény?

Törvényi kötelezettség, külföldi-belföldi



Technológiai igény
Mi történik a rendszereinkben?

Mik az összefüggések, tendenciák?

1 Házon belül fejlesztett megoldások

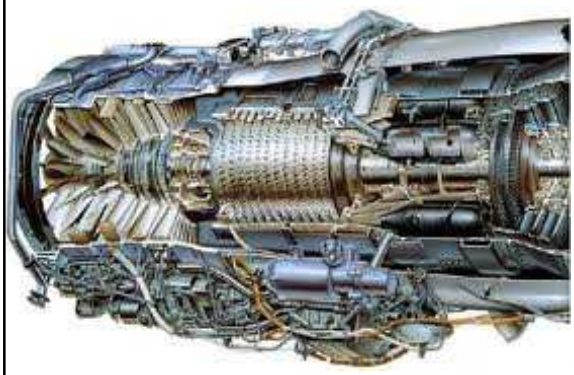
…néha kényelmetlenek

…nehezen újrafelhasználható megoldások

2 Nagyvállalati termékek

…nagyon sokat adnak,

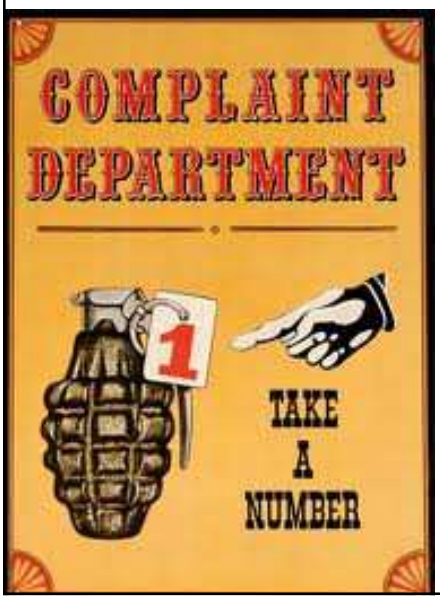
…ebből kifolyólag nagyon bonyolultak



…hosszú a betanulási idő

…nagy az erőforrásigényük

Elhangzott kifogások...



...nem elég intuitív

...kikapcsoltam az XY rendszer naplózását, mert túl sok volt

...nem telepítem az agentet, túl nagy a memóriaigénye

...túl bonyolult megírni az elemzőt

...nem biztonságos

Mit építettünk mindezek alapján?

Intuitív
Előszűrés
Elosztott működés
Törvényi megfelelőség
Egyszerű elemző nyelv
Könnyű integrálhatóság
Kis erőforrás igényű agent
Speciális adatforrások kezelése
Végponttól-végpontig biztonság

Agent

Mezőkre bontás - syslog, eventlog

Normalizálás - hiányos, hibás mezők, kódlapok

További elemzés - *.message további mezőkre bontása, pl.: ip, port, username, stb.

Lokális korreláció – riasztás, már az agentről

Hibatűrés (lokális, biztonságos pufferelés) – „a naplózás ne álljon le”

Hitelesség – időpecsételés, HMAC

Szerver oldal

Minden komponens könnyen menedzselhető

- Agentek, tanúsítványok, adatforrások
- A központ és az agent ugyanazon képességekkel rendelkezik

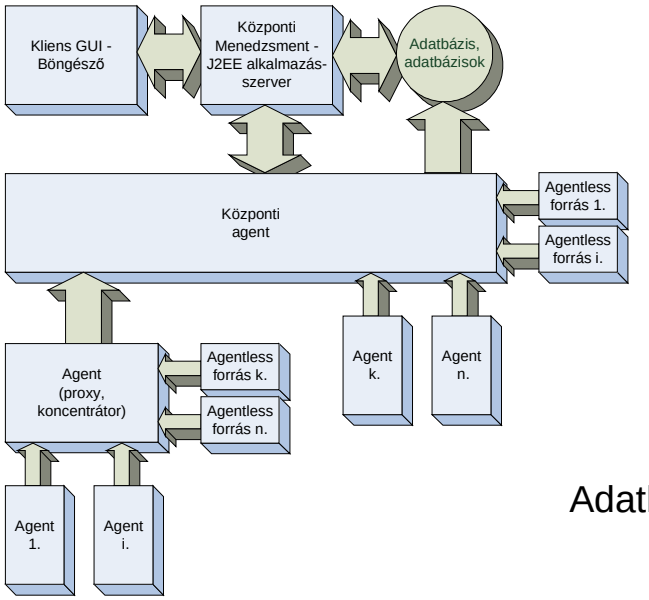
Tehermentesített központi elemzés és korreláció

Elemző szabályok létrehozása és tesztelése egyszerű és gyors

Hatékony keresés és drill-down

Több regionális központ is szervezhető pl. fa struktúrába

A log4ensics rendszer architektúrája



Adatkapcsolatok

Teljesítmény

Az agent memóriagénye néhány 10MB
Az agent csak a konfigurált modulokat tölti be
Masszív többszálú architektúra

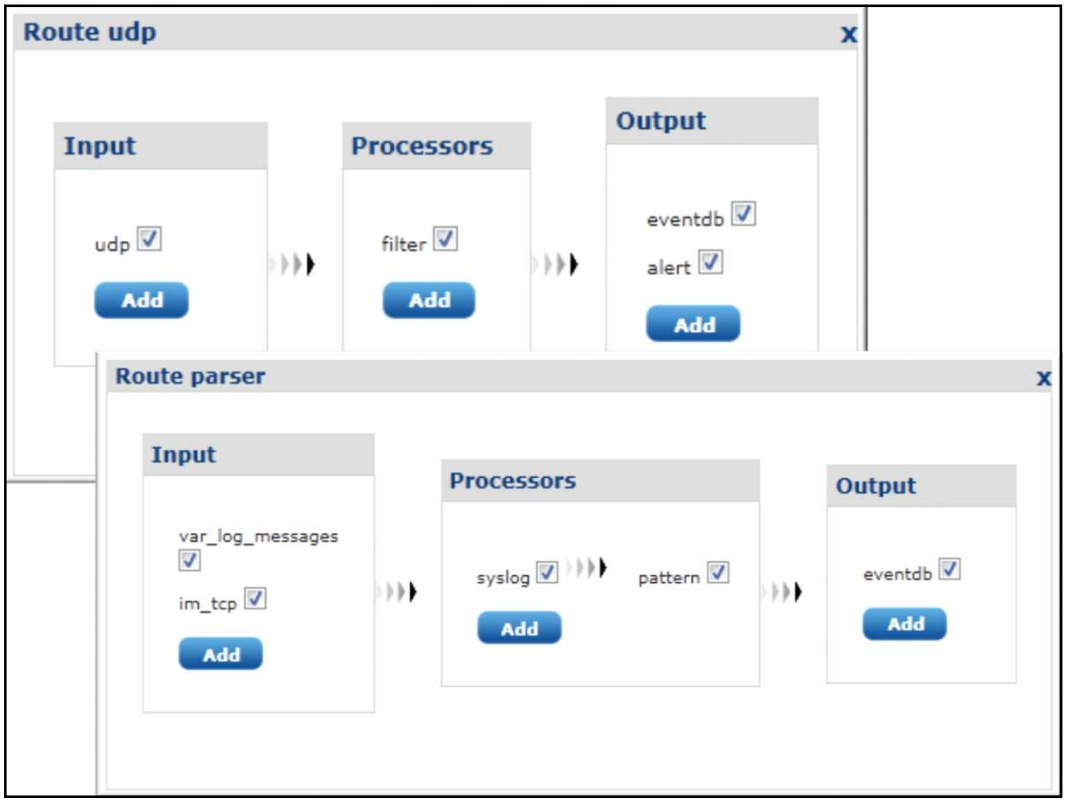
RAW: **108000 EPS**
1200 minta illesztése
minden bejövő logsorra: **32000 EPS**

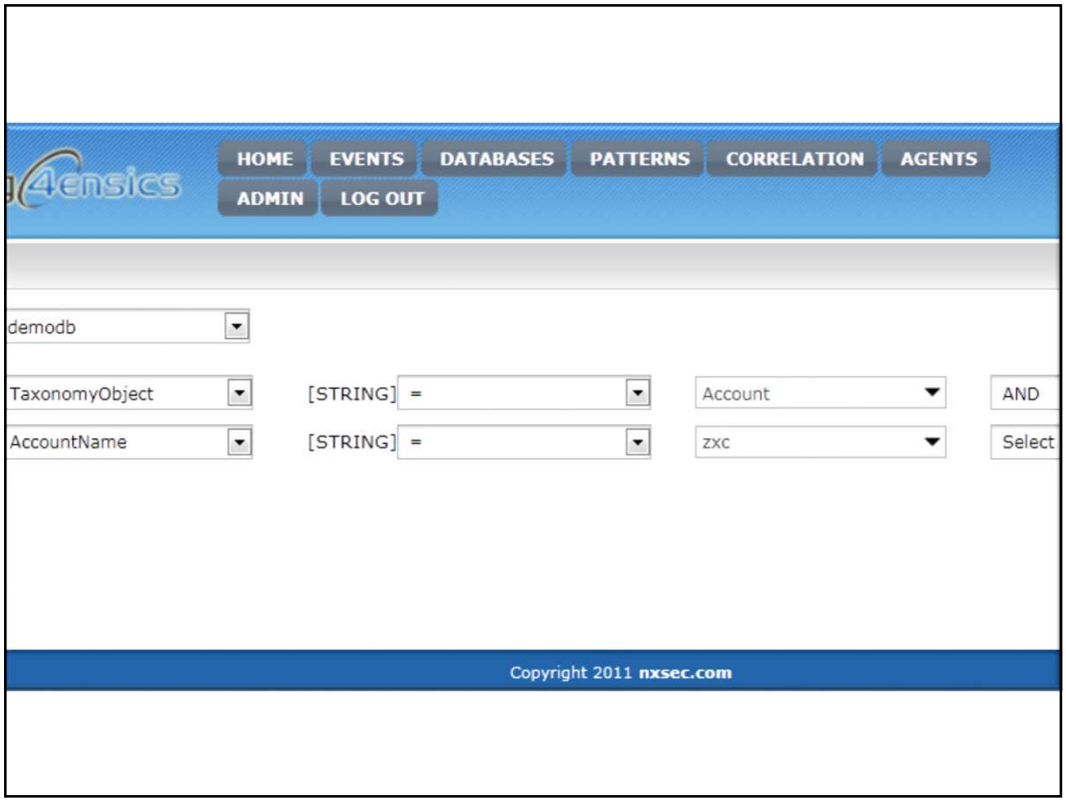
PKI

Név	Típus	Aktiválás	Lejárat	Állapot	Privát kulcs
l4e-ca	CA	2011-01-19 18:03:09	2012-01-14 18:03:09	VALID	IGEN
win-sbs	CERT	2011-05-17 12:12:54	2014-05-31 00:00:00	VALID	IGEN
central-collector	CERT	2011-05-03 17:48:20	2012-05-31 00:00:00	VALID	IGEN
agent-manager	CERT	2011-05-03 17:45:51	2012-05-31 00:00:00	VALID	IGEN

log4ensics
HOME
EVENTS
DATABASES
AGENTS
ADMIN
LOG OUT
Info
Configure
Global
Modules
Routes
Config
*Agent name:
central-agent
*Agent connection type:
Connect to agent manag
*Address:
172.17.39.5
*Port:
4041
*CA:
log4ensics0
*Certificate:
central-agent
*Log level:
INFO
Log to file:

log4ensics
HOME
EVENTS
DATABASES
AGENTS
ADMIN
LOG OUT
Welcome, Log4ensics Administrator !
Info
Configure
Global
Modules
Routes
Config
Route main
Input
SSL_input
Add
Processors
Add
Output
eventdb
Add


Route udp
Input
udp
Add
Processors
filter
Add
Output
eventdb
alert
Add
Route parser
Input
var_log_messages
im_tcp
Add
Processors
syslog
pattern
Add
Output
eventdb
Add


HOME
EVENTS
DATABASES
PATTERNS
CORRELATION
AGENTS
ADMIN
LOG OUT
demodb
TaxonomyObject
[STRING]
=
Account
AND
AccountName
[STRING]
=
zxc
Select
Copyright 2011 nxsec.com

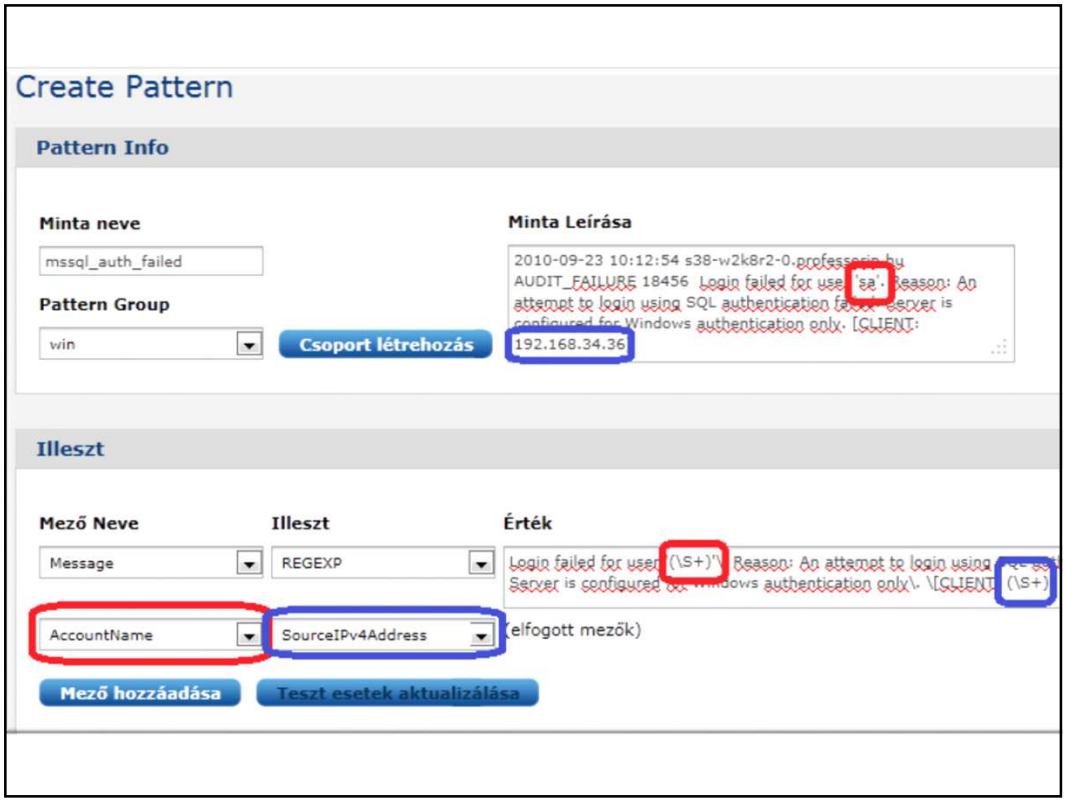
Search:

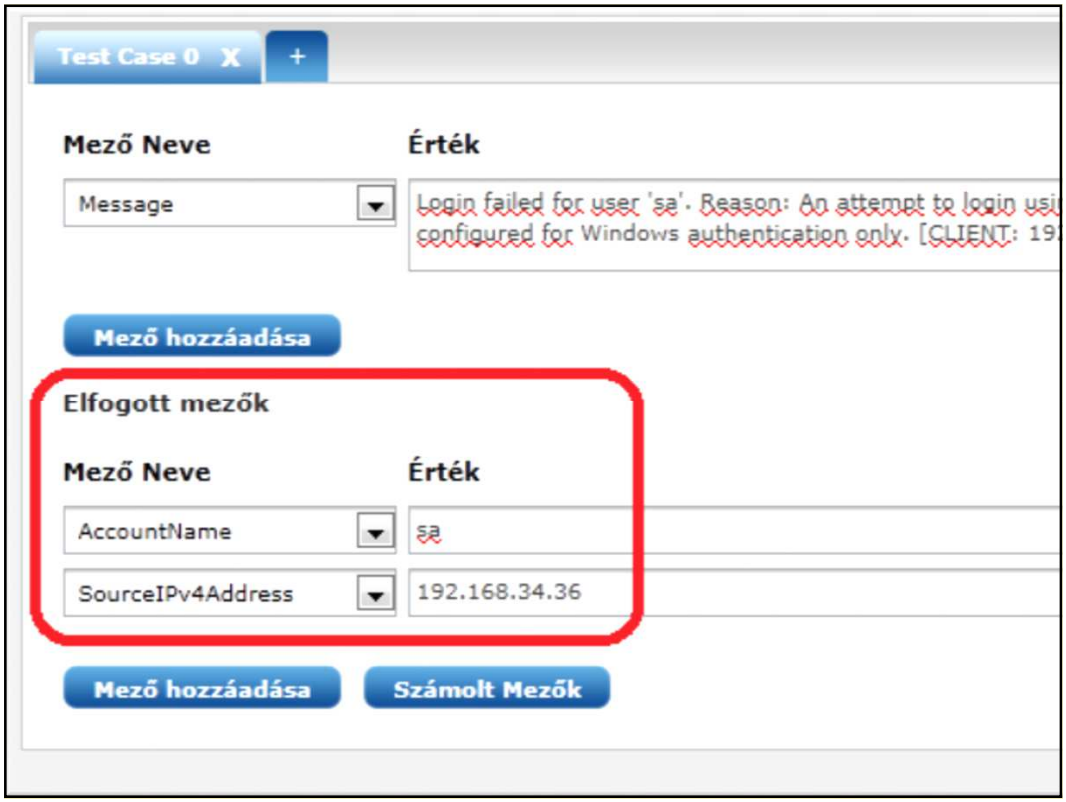
Field value

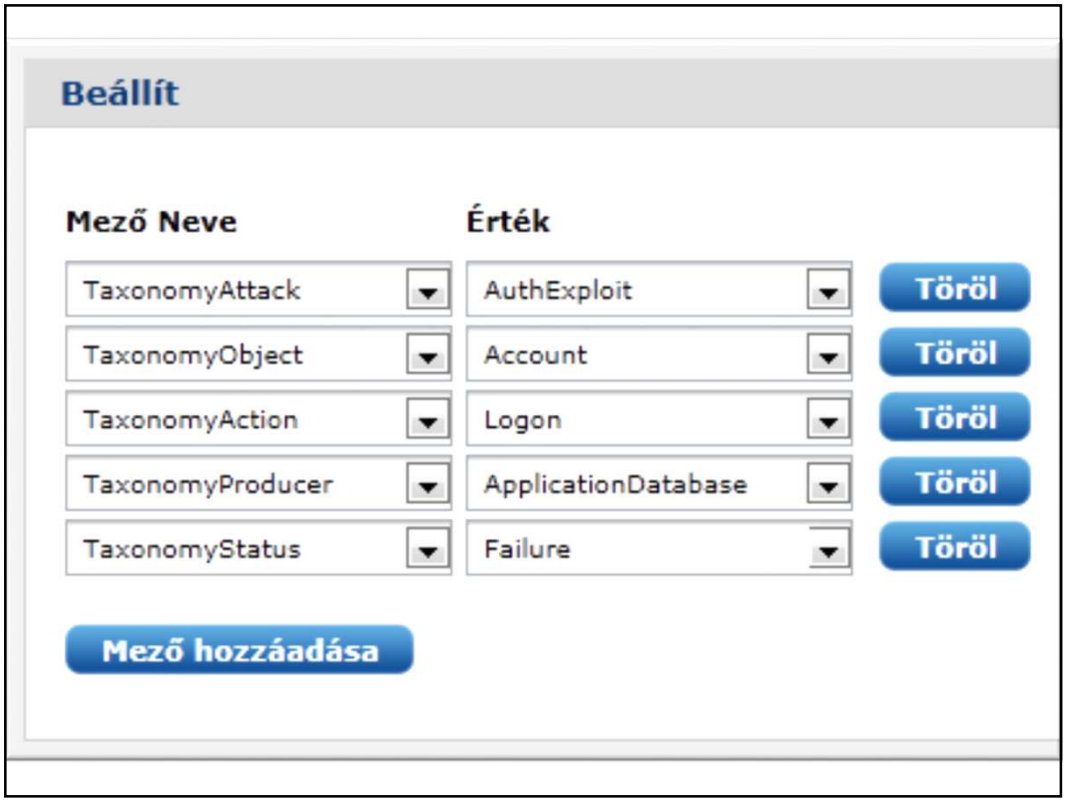
```
2010-08-27 15:03:48 s38-w2k8r2-0.professorip.hu AUDIT_SUCCESS 4624  An
account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           S38-W2K8R2-0$
        Account Domain:         WORKGROUP
        Logon ID:               0x3e7

Logon Type:                     10

New Logon:
        Security ID:
S-1-5-21-1094972579-1599888189-[illegible]3292-1006
        Account Name:           zxc
        Account Domain:         [illegible]-W2K8R2-0
        Logon ID:               0x87af25
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
```

		- Key length indicates the length of the generate This will be 0 if no session key was requested.
☐	AccountName	zxc
☐	Category	Logon
☐	CategoryNumber	12544
☐	EventID	4624
☐	EventReceivedTime	2011-05-15 22:13:21.0
☐	EventTime	2010-08-27 15:03:48.0
☐	EventType	AUDIT_SUCCESS
☐	FileName	Security
☐	Hostname	s38-w2k8r2-0.professorip.hu
☐	Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: S38-W2K8R2-0$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 10 New Logon: Security ID: S-1-5-21-1094972579-1599888189-[illegible]3292-1006 Account Name: zxc Account Domain: [illegible]-W2K8R2-0 Logon ID: 0x87af25

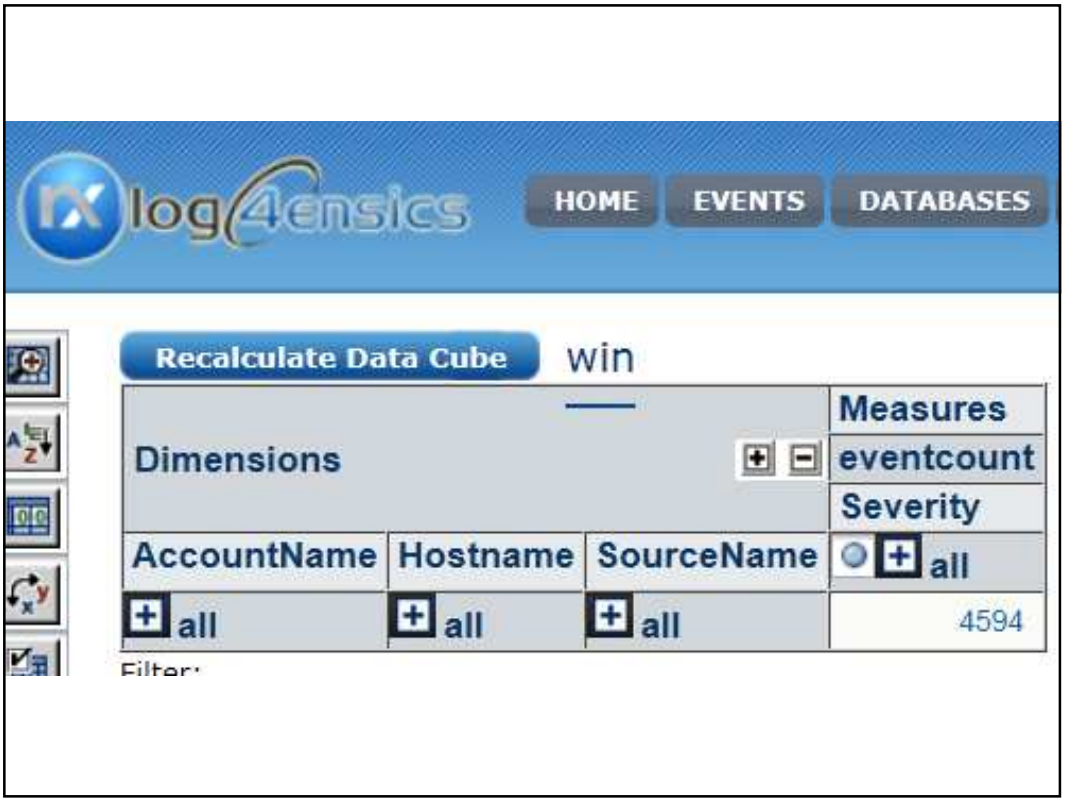
Logon	
4	
18456	
2011-05-15 22:13:12.0	
2010-09-23 10:12:54.0	
AUDIT_FAILURE	
Application	
s38-w2k8r2-0.professorip.hu	
Login failed for user 'sa'. Reason: An attempt to login using SQL authentication failed. Server is configured for Windows authentication only. [CLIENT: 192.168.34.36]	
4711	
ERROR	
4	
MSSQL$SQLEXPRESS	




Test Case 0 X
+
Mező Neve
Érték
Message
Login failed for user 'sa'. Reason: An attempt to login usi
configured for Windows authentication only. [CLIENT: 19
Mező hozzáadása
Elfogott mezők
Mező Neve
Érték
AccountName
sa
SourceIPv4Address
192.168.34.36
Mező hozzáadása
Számolt Mezők


Beállít
Mező Neve
Érték
TaxonomyAttack
AuthExploit
Töröl
TaxonomyObject
Account
Töröl
TaxonomyAction
Logon
Töröl
TaxonomyProducer
ApplicationDatabase
Töröl
TaxonomyStatus
Failure
Töröl
Mező hozzáadása

		NTLM protocols. - Key length i This will be 0 if no s
☐	NTDomain	NT AUTHORITY
☐	PatternName	winlogon
☐	RecordNumber	38
☐	Severity	INFO
☐	SeverityValue	2
☐	SourceName	Microsoft-Windows-Secu
☐	TaxonomyAction	Logon
☐	TaxonomyObject	Account
☐	TaxonomyProducer	OS
☐	TaxonomyStatus	Success



log4ensics HOME EVENTS DATABASES PATTERNS CORRELATI

Recalculate Data Cube win

Dimensions				Measures: eventcount, Severity: all
AccountName	AccountName	Hostname	SourceName	
all		all	all	4594
all	Administrator	all	all	1120
	cyg_server	all	all	158
	LOCAL SERVICE	all	all	292
	NETWORK SERVICE	all	all	86
	SYSTEM	all	all	2927
	zxc	all	all	11

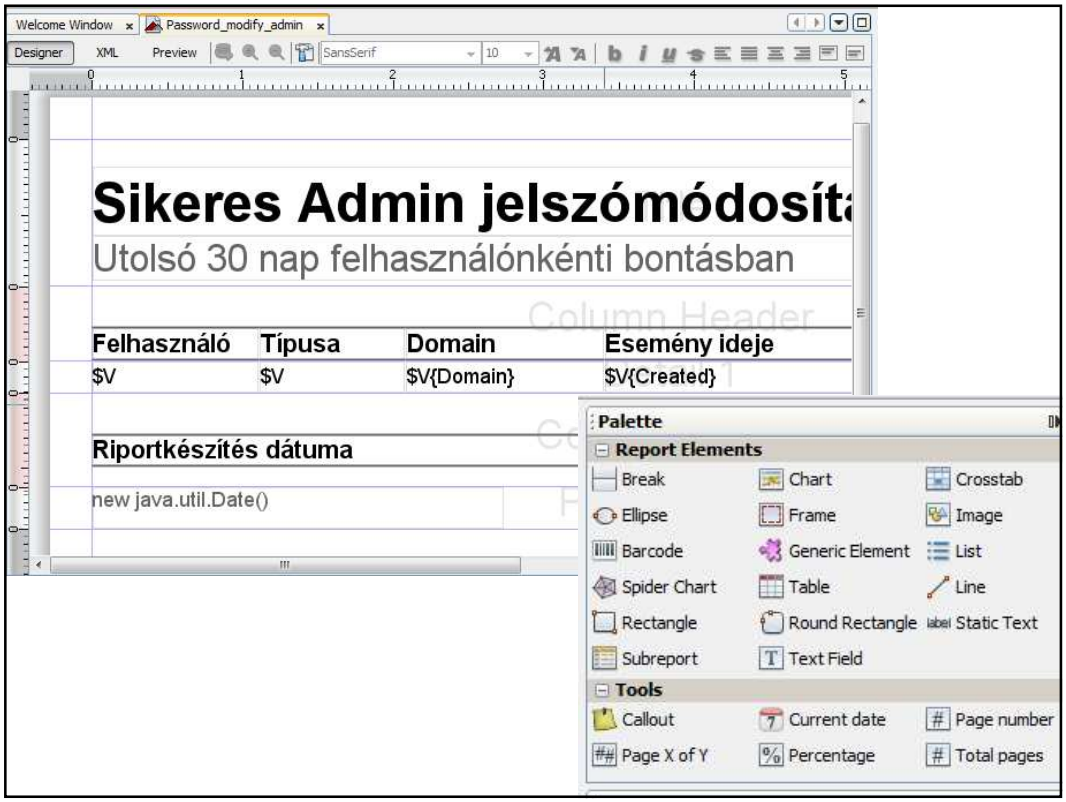
Filter:

KEZDŐLAP ESEMÉNYEK ADATBÁZISOK MINTÁK KORRELÁCIÓ ÜGYNÖKÖK ADMINISZTRÁCIÓ KILÉP

Üdvözöljük, Log4ensics Administrator !

late Data Cube win

ók					Mértékek: eventcount, Severity: all			
tName	AccountName	Hostname	Hostname	SourceName		ERROR	INFO	WARNING
		all		all	4594	65	4257	272
	Administrator	all		all	1120	9	1099	12
	cyg_server	all		all	158	46	112	
	LOCAL SERVICE	all		all	292		230	62
		all	37L4247D25-07	all	4		4	
			S38-W2K8R2-0	all				
			s38-w2k8r2-0.professorip.hu	all	139		80	59
			WIN-OUNNPISDHIG	all	149		146	3
	NETWORK SERVICE	all		all	86			86
	SYSTEM	all		all	2927	10	2805	112
	zxc	all		all	11		11	



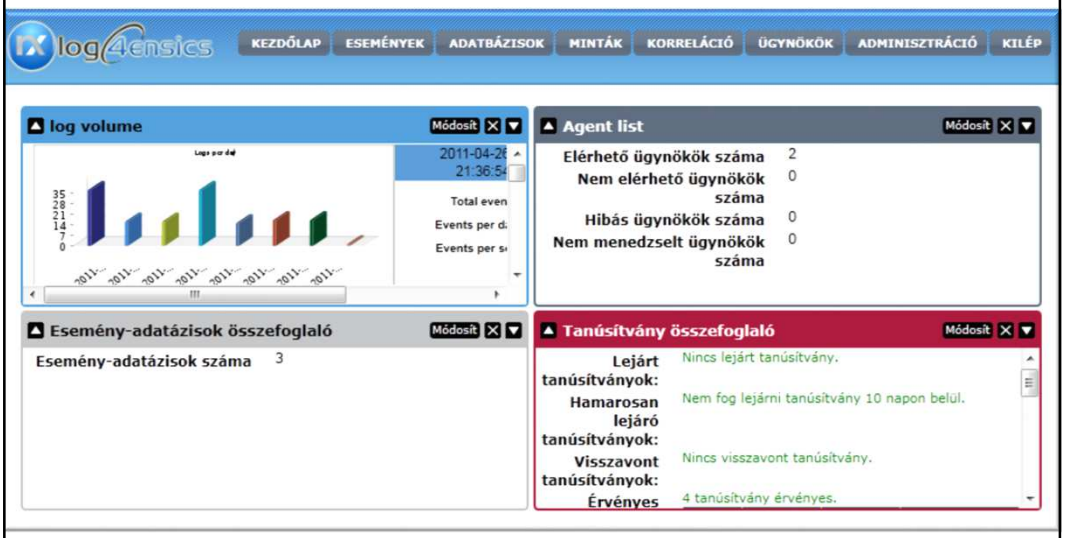
Riport

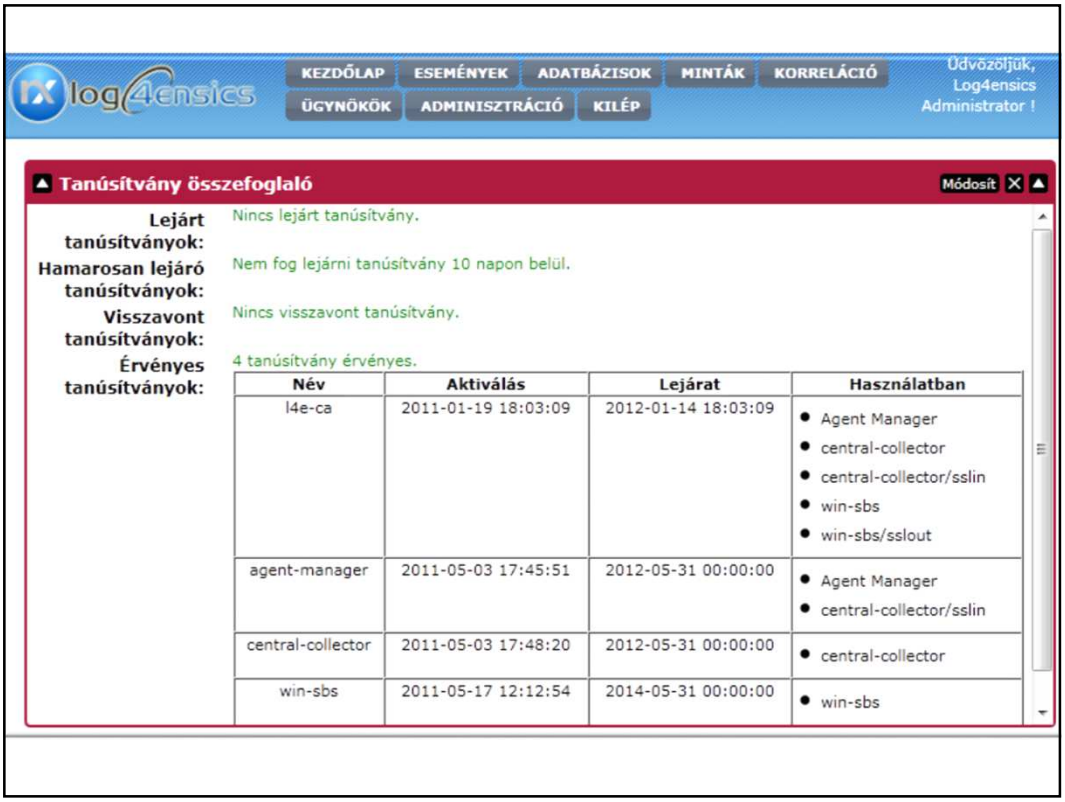
TOP10 bejelentkezés

Utolsó 30 nap felhasználónkénti bontásban

Darabszám	Felhasználó	Domain
975	SYSTEM	NT AUTHORITY
312	Administrator	S38-W2K8R2-0
95	zxc	S38-W2K8R2-0
38	Administrator	WIN-OUNNPISDHIG
28	cyg_server	WIN-OUNNPISDHIG
22	cyg_server	S38-W2K8R2-0
2	gberkes	S38-W2K8R2-0

Dashboard


log4ensics
KEZDŐLAP
ESEMÉNYEK
ADATBÁZISOK
MINTÁK
KORRELÁCIÓ
ÜGYNÖKÖK
ADMINISZTRÁCIÓ
KILÉP
log volume
Módosít
Total even
Events per d
Events per s
Agent list
Módosít
Elérhető ügynökök száma 2
Nem elérhető ügynökök száma 0
Hibás ügynökök száma 0
Nem menedzselt ügynökök száma 0
Esemény-adatázisok összefoglaló
Módosít
Esemény-adatázisok száma 3
Tanúsítvány összefoglaló
Módosít
Lejárt tanúsítványok: Nincs lejárt tanúsítvány.
Hamarosan lejáró tanúsítványok: Nem fog lejárni tanúsítvány 10 napon belül.
Visszavont tanúsítványok: Nincs visszavont tanúsítvány.
Érvényes 4 tanúsítvány érvényes.


log4ensics
KEZDŐLAP
ESEMÉNYEK
ADATBÁZISOK
MINTÁK
KORRELÁCIÓ
ÜGYNÖKÖK
ADMINISZTRÁCIÓ
KILÉP
Üdvözöljük, Log4ensics Administrator !
Tanúsítvány összefoglaló
Módosít
Lejárt tanúsítványok: Nincs lejárt tanúsítvány.
Hamarosan lejáró tanúsítványok: Nem fog lejárni tanúsítvány 10 napon belül.
Visszavont tanúsítványok: Nincs visszavont tanúsítvány.
Érvényes tanúsítványok: 4 tanúsítvány érvényes.
Név | Aktiválás | Lejárat | Használatban
l4e-ca | 2011-01-19 18:03:09 | 2012-01-14 18:03:09 | Agent Manager, central-collector, central-collector/sslin, win-sbs, win-sbs/sslout
agent-manager | 2011-05-03 17:45:51 | 2012-05-31 00:00:00 | Agent Manager, central-collector/sslin
central-collector | 2011-05-03 17:48:20 | 2012-05-31 00:00:00 | central-collector
win-sbs | 2011-05-17 12:12:54 | 2014-05-31 00:00:00 | win-sbs

Összefoglalás – a log4ensics hasznos, ha..

Még nincs implementált megoldás

Van, de nem elégséges megoldás

- Egyedi alkalmazások logjait nem tudják kezelni
- Van központi gyűjtés de nincs elemzés

Van központi elemzés

- de szükség lenne előszűrésre,
- könnyűsúlyú agentekre ,
- és hiteles tárolásra is.

kancellar.hu
AZ INFORMATIKAI BIZTONSÁG SZAKÉRTŐJE

Köszönöm szépen!

berkes.gabor@kancellar.hu

Duna Tower, 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704tel, f: +36 1 2704fax, e: info@kancellar.hu, w: kancellar.hu

Duna Tower, 1138 Budapest, Népfürdő u. 22.
t: +36 1 2704tel, f: +36 1 2704fax, e: info@kancellar.hu, w: kancellar.hu