

Központi **jogosultság-
menedzsment** és **biztonsági
felügyelet** megvalósítása
nagy felhasználószámú, nagy
fluktuációjú szervezeteknél

Bartos Zoltán Balázs
bartos.balazs@kfk-lnx.hu

Agenda

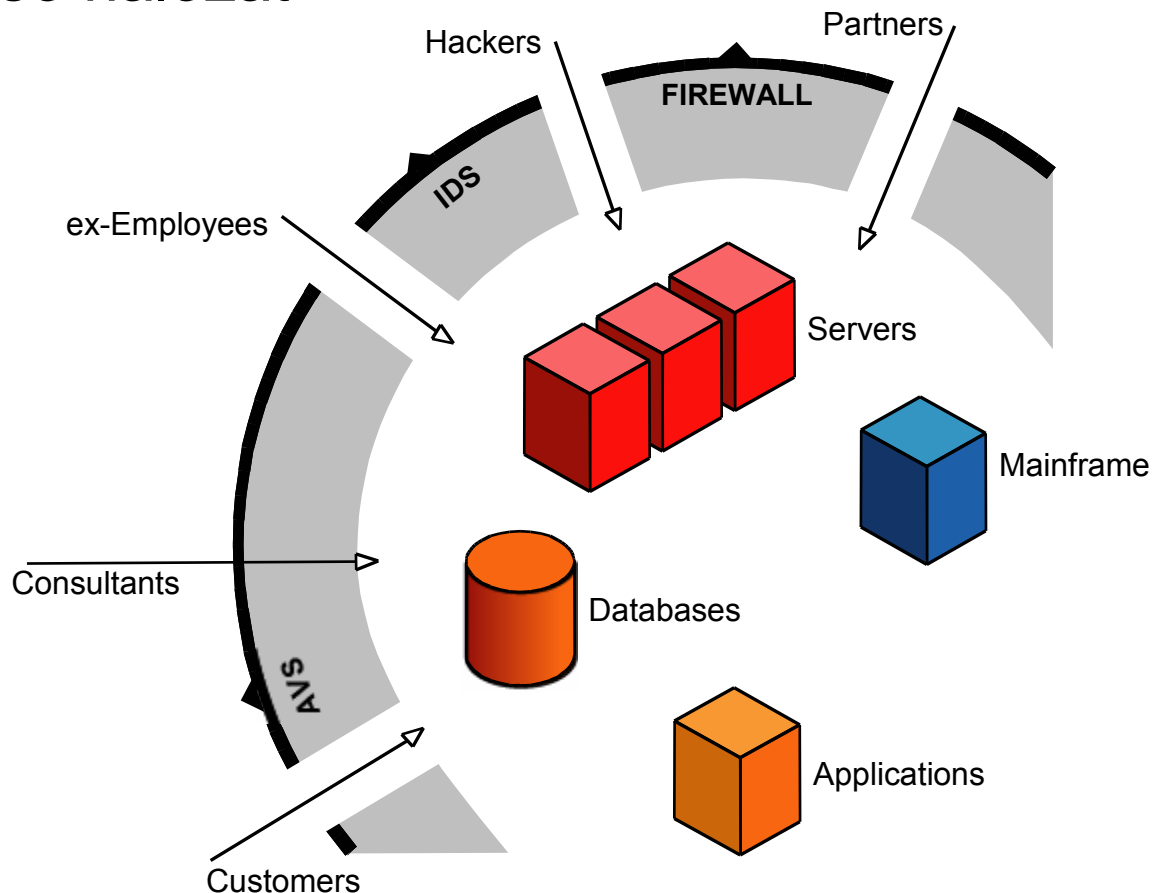
- **Miért van szükség jogosultságmenedzsmentre?**
- BMC Control-SA – egy lehetséges megvalósítás
- Control-SA/PassPort – bízzuk a felhasználóra!
- InSight for Control-SA – teljes körű biztonsági felügyelet



A hálózati perem lassan eltűnik

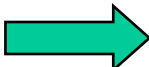
- Nincs többé zárt belső hálózat
- Extranet
- Web szolgáltatások
- Wireless
- Dial-up
- VPN

Az egész informatikai rendszert felügyeljük, vagy csak a határvonalát?



Bevezetés – az Identity Managementről

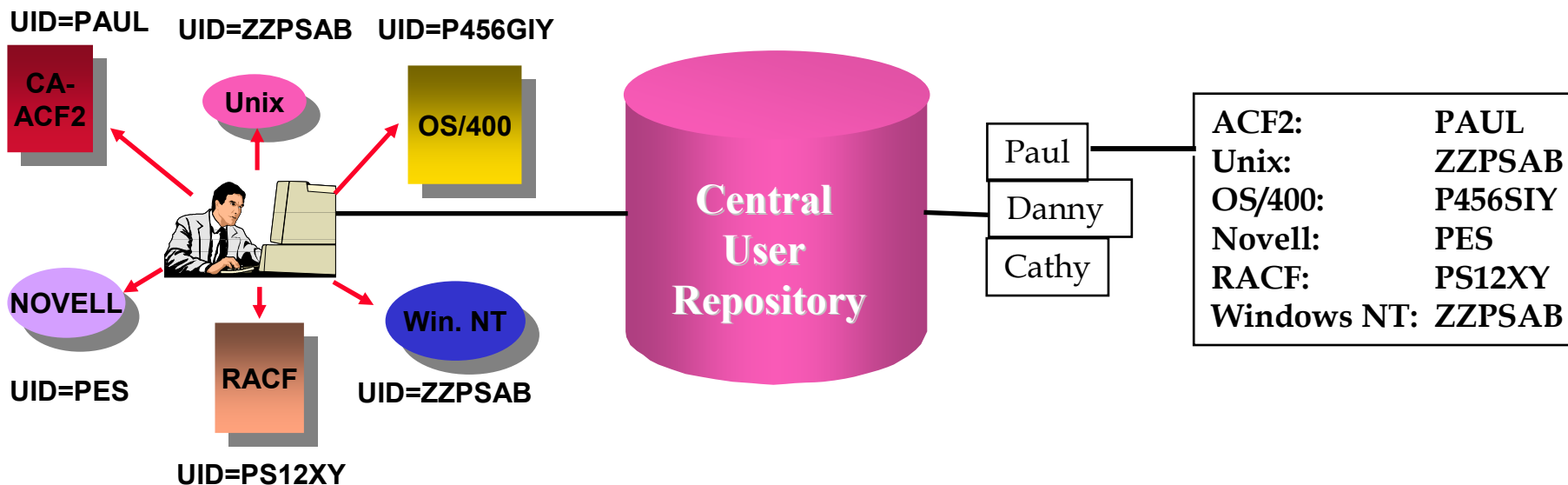
Identity Management (Jogosultság- vagy hozzáférés menedzsment)

- Felhasználói **hozzáférések** és **jogosultságok** központosított, egységes kezelése heterogén környezetben.
- Hozzáférések központi 
 - **Létrehozása**
 - **Módosítása**
 - **Megszűntetése**
- Felhasználók által önállóan elvégezhető tevékenységek bővítése (password-reset, hozzáférés igénylés).



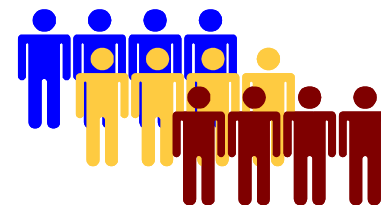
Felhasználók és jogosultságok

- Központi felhasználói adattárház:
 - Felhasználói adatok összevont megjelenítése
 - Átlátható kapcsolat az emberek és a hozzáférések között
 - Belső ellenőrzések megkönnyítése



Miért szükséges a hozzáférés-menedzsment?

- **Nagy számú** felhasználó a rendszerben.
- **Heterogén** környezet – különféle platformok, külön felügyelettel.
- Sok újonnan érkező / távozó felhasználó.
- Új felhasználói hozzáférés minél gyorsabban.



Agenda

- Miért van szükség jogosultságmenedzsmentre?
- **BMC Control-SA – egy lehetséges megvalósítás**
- Control-SA/PassPort – bízzuk a felhasználóra!
- InSight for Control-SA – teljes körű biztonsági felügyelet



A Control-SA jellemzői

- Felhasználói hozzáférések **automatizált** kialakítása.
- **Munkakörhöz** rendelt jogosultság-kiosztás.
- A biztonsági házirend **központi felügyelete**.
- Jelszavak összehangolása.
- Központi riasztás felügyelet.
- **Visszakereshető** biztonsági beállítások és módosítások.
- Fejlett **jelentéskészítés**.
- Egységes felhasználói felület.



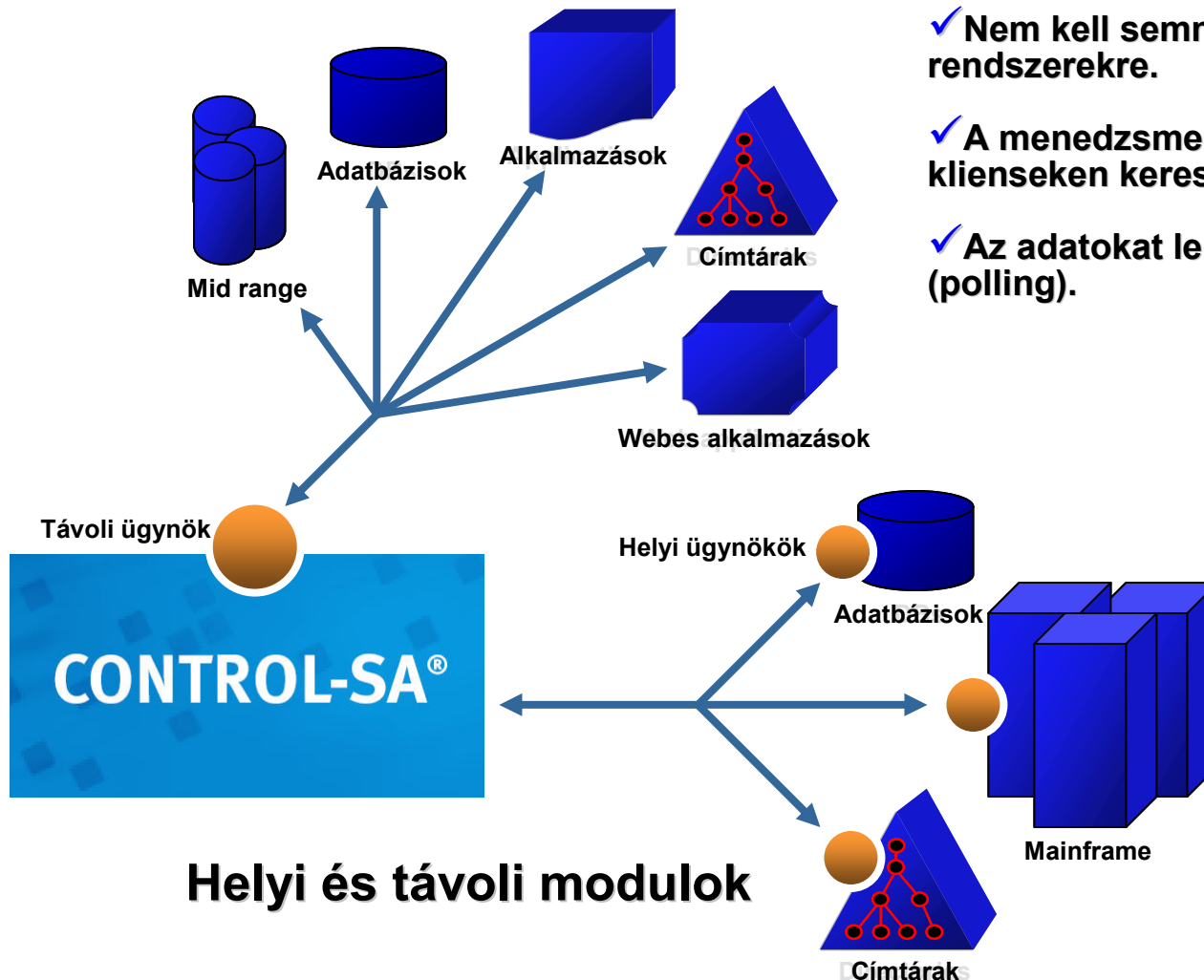
A BMC Control-SA modell

Távoli menedzsment

- ✓ Nem kell semmit telepíteni a menedzselte rendszerekre.
- ✓ A menedzsment távolról, vagy alkalmazás-klienseken keresztül történik.
- ✓ Az adatokat lekérdezés útján nyeri ki (polling).

Lokális menedzsment

- ✓ Agent szoftver telepítése a menedzselte rendszerekre.
- ✓ Az agent szoftver a központi rendszer kiterjesztése
- ✓ A változásokat azonnal észleljük.



Lokális menedzsment agent szoftver telepítésével

A megoldás előnyei:

- Valós idejű, kétirányú menedzsment – a központi és a lokális felhasználói adatbázis konzisztens .
- Riasztási lehetőség a biztonsági szabályok megsértésekor.
- Hálózatkimaradás esetén a lokális agent szoftverek továbbra is működnek, helyreállítás után adatszinkronizáció.
- Titkosított hálózati forgalom (3DES), csökkentett hálózati terhelés

Hátrányok:

- Időigényesebb az implementáció (telepítés minden rendszerre)
- A helyi agent szoftverek lefoglalják a rendszer erőforrásainak egy kis részét (tapasztalat: 1-3%)

CONTROL-SA Agent szoftverek

•Mainframe

- RACF
- CA-ACF2
- CA-Top Secret
- VM:Secure

•Network Systems

- Win NT Server
- Win 2K A.D.
- Novell/Netware
- OS/2 LAN Server
- LDAP
- Netscape / iPlanet
- Netscape NDS

•UNIX

- Sun/Solaris NCR
- IBM/AIX
- SGI/IRIX
- HP-UX Digital Unix
- NIS Tru64
- Linux

•Midrange

- AS400
- VMS
- TANDEM

CONTROL-SA Agent szoftverek

- Informix
- Oracle
- Oracle Apps.
- Sybase
- Lotus Notes
- MS-Exchange
- MS-SQL
- Oracle Applications
- SAP/R3
- PeopleSoft
- *Tivoli Access Mgr for eBusiness
- *CA-eTrust Access Cont. & SSO
- Netegrity Sitminder
- Cisco Secure
- DB2
- Entrust/PKI
- Netscape Enterprise Server
- Proxima SSO
- ACE/Server
- SeOS
- Tandem Safeguard
- * Novell GroupWise

** Tanúsított BMC MarketZone partner fejlesztése*

Távoli menedzsment

A megoldás előnyei:

- Egyszerű, gyors implementáció.
- Jó megoldást nyújthat, ha különböző korlátozások miatt nem engedélyezik egy platformra az agent szoftver telepítését.

Hátrányok:

- Adatkonzisztencia (polling) – hálózatkimaradás esetén a változások csak később jutnak érvényre.
- Hálózati terhelés megnövekedhet.
- Biztonsági kérdések – hogyan érzékeljük a szabálysértéseket?
- Gondoskodni kell a hálózati forgalom biztonságáról

Távoli menedzsment – támogatott rendszerek

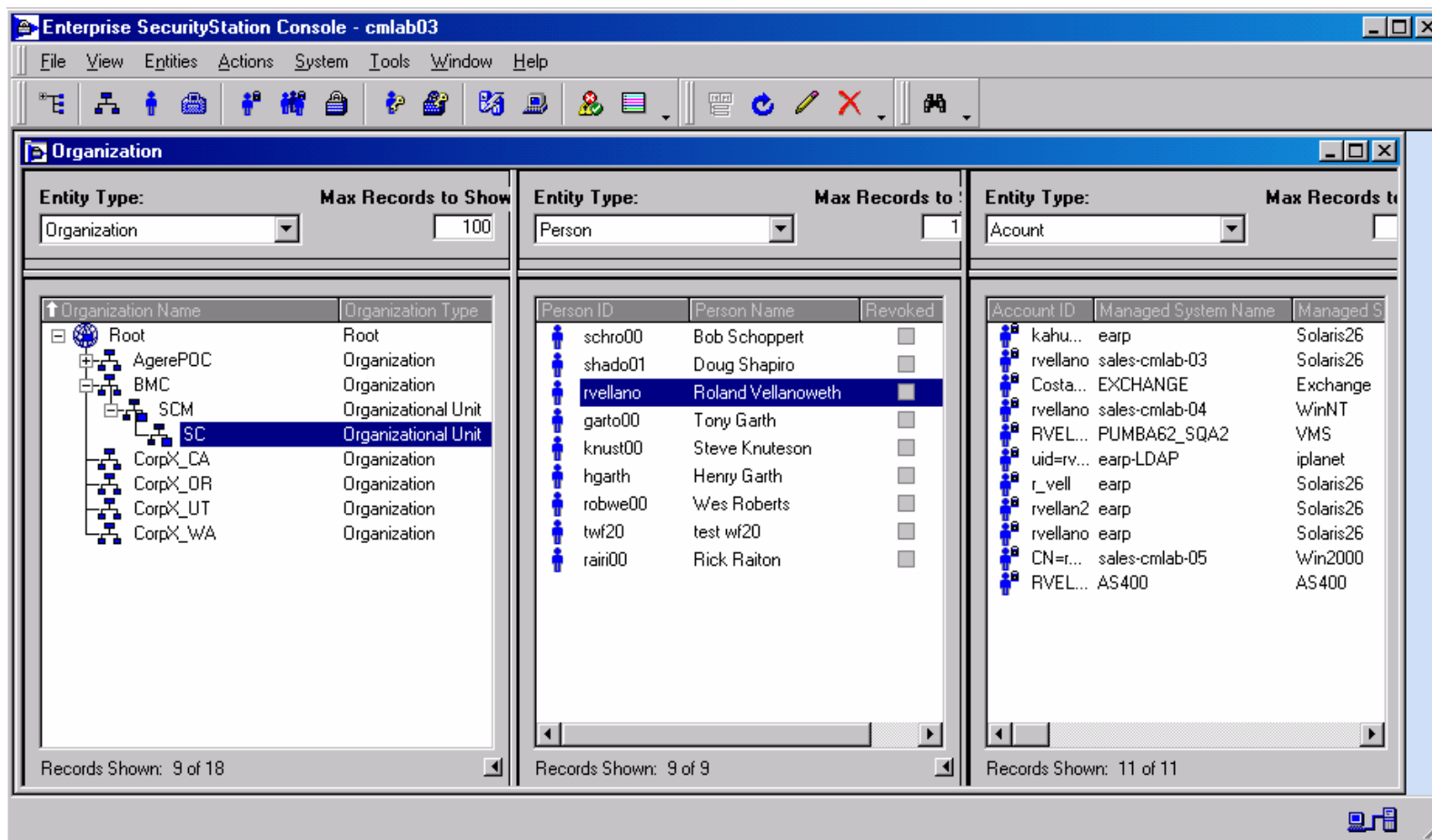
- LDAP

- Adatbázisok – Oracle, Sybase, DB2, Informix, MS-SQL – A Control-SA agentek az adatbázis kliensekkel egy gépre települnek – menedzsment az adatbázis klienseken keresztül.

- Egyéb támogatott rendszerek kliens-szerver alapokon:
 - Lotus Notes
 - SAP R/3
 - PeopleSoft
 - Exchange
 - Entrust
 - Oracle Applications
 - Netware
 - etc.
- Windows A.D.
- WinNT Server / Workstation
- Unix

CONTROL-SA Adminisztrátori nézet

- Enterprise SecurityStation Console GUI version 3.8



The screenshot displays the Enterprise SecurityStation Console GUI version 3.8. The interface is divided into three main sections:

- Organization Panel:** Shows a tree view of the organizational structure. The selected entity is 'SC' (Organizational Unit). The table below lists the visible records:

Organization Name	Organization Type
Root	Root
AgerePOC	Organization
BMC	Organization
SCM	Organizational Unit
SC	Organizational Unit
CorpX_CA	Organization
CorpX_OR	Organization
CorpX_UT	Organization
CorpX_WA	Organization

Records Shown: 9 of 18

- Person Panel:** Shows a list of person records. The selected record is 'rvellano' (Roland Vellanoweth). The table below lists the visible records:

Person ID	Person Name	Revoked
schro00	Bob Schoppert	<input type="checkbox"/>
shado01	Doug Shapiro	<input type="checkbox"/>
rvellano	Roland Vellanoweth	<input type="checkbox"/>
garto00	Tony Garth	<input type="checkbox"/>
knust00	Steve Knuteson	<input type="checkbox"/>
hgarth	Henry Garth	<input type="checkbox"/>
robwe00	Wes Roberts	<input type="checkbox"/>
twf20	test wf20	<input type="checkbox"/>
rairi00	Rick Raiton	<input type="checkbox"/>

Records Shown: 9 of 9

- Account Panel:** Shows a list of account records. The table below lists the visible records:

Account ID	Managed System Name	Managed S
kahu...	earp	Solaris26
rvellano	sales-cmlab-03	Solaris26
Costa...	EXCHANGE	Exchange
rvellano	sales-cmlab-04	WinNT
RVEL...	PUMBA62_SQA2	VMS
uid=rv...	earp-LDAP	iplanet
r_vell	earp	Solaris26
rvellan2	earp	Solaris26
rvellano	earp	Solaris26
CN=r...	sales-cmlab-05	Win2000
RVEL...	AS400	AS400

Records Shown: 11 of 11

CONTROL-SA Webes felület



Person: David Cohen

Person ID: 56965326 | Department: Marketing | Phone: #3456 | E-mail: david_C@bmc.com
Status: OK

Accounts connected to David Cohen:

#	Account ID	Account Name	System Type	Default Group	Revoked	Last Transaction	Completion Status
1	RSS User ID	Domain Users	Oracle	Public		342	✓
2	RSS User ID	Domain Users	Oracle	Public		2356	✓
3	RSS User ID	Domain Users	Oracle	Public		332568	✓
4	RSS User ID	Domain Users	Oracle	Public		52	✓
5	RSS User ID	Domain Users	Oracle	Public		3256	✓
6	RSS User ID	Domain Users	Oracle	Public		65	✓
7	cdavid	Domain Users	Oracle	Public		5689	✓
8	RSS User ID	Domain Users	Oracle	Public		5698	✓
9	RSS User ID	Domain Users	Oracle	Public		2145	✓
10	DavidC	Domain Users	Oracle	Public		222	✓

2 Accounts selected

CONTROL-SA®

- ✓ Adminisztráció böngészőn keresztül.
- ✓ Gyorsabb implementáció.
- ✓ Nem szükséges konzolt telepíteni.
- ✓ Bármelyik PC-ről elérhető.

Architektúra:

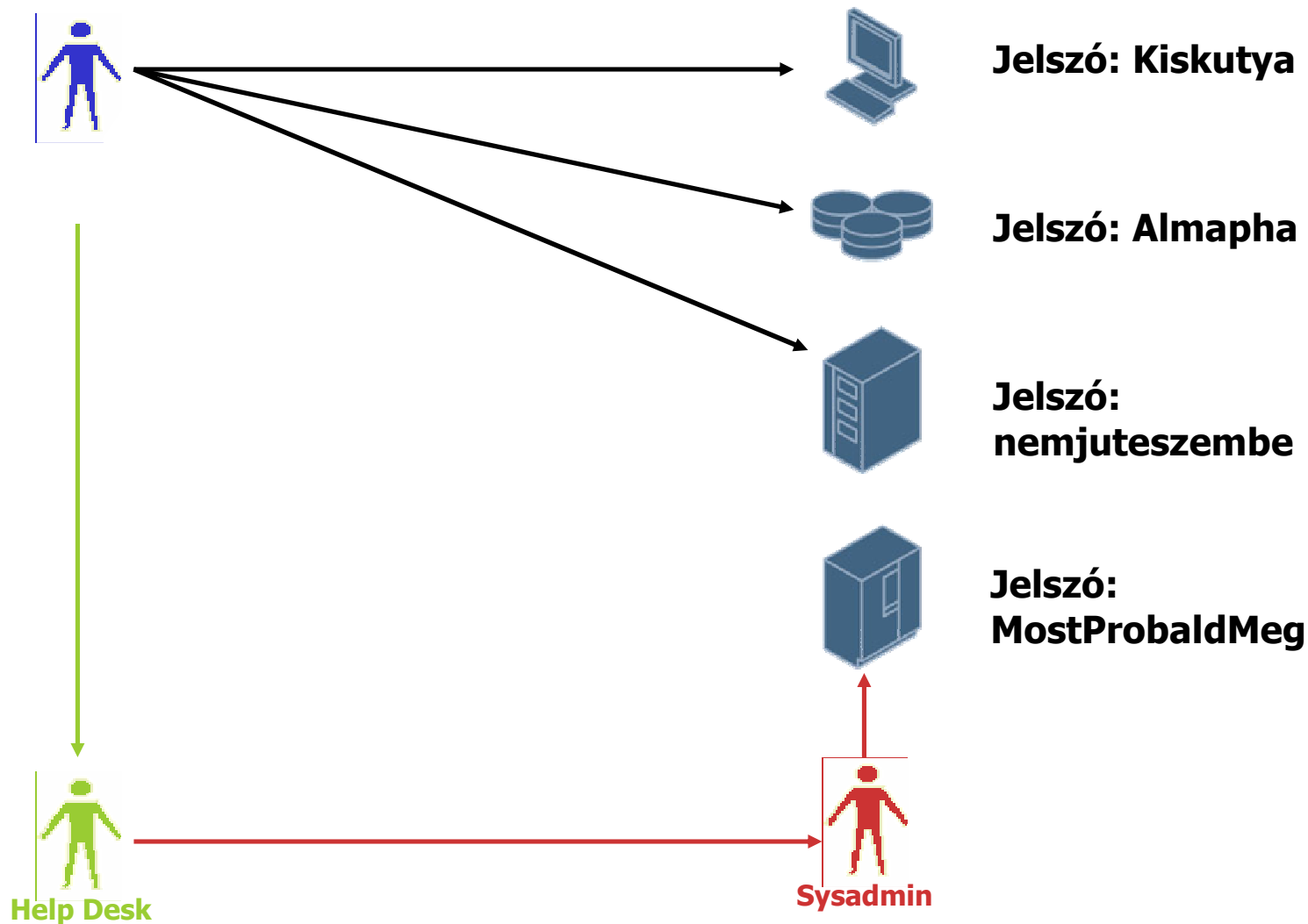
- OS: Solaris a központi szerver (ESS) alatt
- Web szerver: Tomcat
- Támogatott böngészők: IE 5.5 felett
- JAVA alapú fejlesztés

Agenda

- Miért van szükség jogosultságmenedzsmentre?
- BMC Control-SA – egy lehetséges megvalósítás
- **Control-SA/PassPort – bízzuk a felhasználóra!**
- InSight for Control-SA – teljes körű biztonsági felügyelet

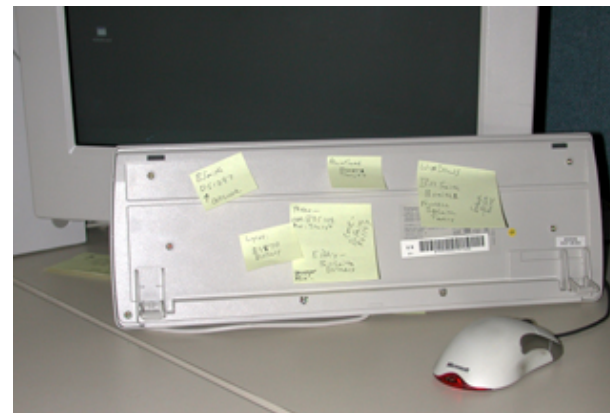


Miért van gond a jelszavakkal?



CONTROL- SA/PassPort

- Lehetővé teszi az „átlagos” felhasználó számára is:
 - Kezdeti regisztráció a PassPort rendszerbe.
 - „Jelszó reset” kezdeményezése.
 - Bejelentkezés a PassPort rendszerbe „kérdés/válasz” jellegű autentikációval.
 - Testreszabott „kérdés/válasz” információk feltöltése.



A PassPort webes felülete

BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://rvellano-com-92/PassPort/EsPassPort.dll?> Go Links

New password:

Retype new password:

2. Select the accounts on which you want to change the password:

CONTROL-SA/PassPort Account

<input type="checkbox"/> Change Password	<input type="checkbox"/> Restore Account	User Account	Revoked	Platform/Service	System	System Type
<input checked="" type="checkbox"/>	<input type="checkbox"/>	kahun01	No	Solaris	earp	Solaris26
<input checked="" type="checkbox"/>	<input type="checkbox"/>	rvellano	No	Solairs	sales-cmlab-03	Solaris26
<input type="checkbox"/>	<input type="checkbox"/>	Costa Mesa/Recipients/rvellano	No		EXCHANGE	Exchange
<input checked="" type="checkbox"/>	<input type="checkbox"/>	rvellano	No	WinNT PDC	sales-cmlab-04	WinNT
<input checked="" type="checkbox"/>	<input type="checkbox"/>	RVELLANO	No	Alpha OpenVMS	PUMBA62_SQA2	VMS
<input checked="" type="checkbox"/>	<input type="checkbox"/>	uid=rvellano,ou=Control-SA Software Consultants,ou=West Area,ou=Western Region,ou=North America,ou=BMC Software,dc=cmlab,dc=com	No	iPlanet LDAP	earp-LDAP	iplanet
<input checked="" type="checkbox"/>	<input type="checkbox"/>	r_vell	No	Solaris	earp	Solaris26
<input checked="" type="checkbox"/>	<input type="checkbox"/>	rvellan2	No	Solaris	earp	Solaris26
<input checked="" type="checkbox"/>	<input type="checkbox"/>	rvellano	No	Solaris	earp	Solaris26
<input checked="" type="checkbox"/>	<input type="checkbox"/>	CN=rvellano,CN=Users,DC=SALES-CMLAB-AD,DC=bmc,DC=com	No	WIN 200 AD Server	sales-cmlab-05	Win2000
<input checked="" type="checkbox"/>	<input type="checkbox"/>	RVELLANO	No	AS400 Demo	AS400	AS400

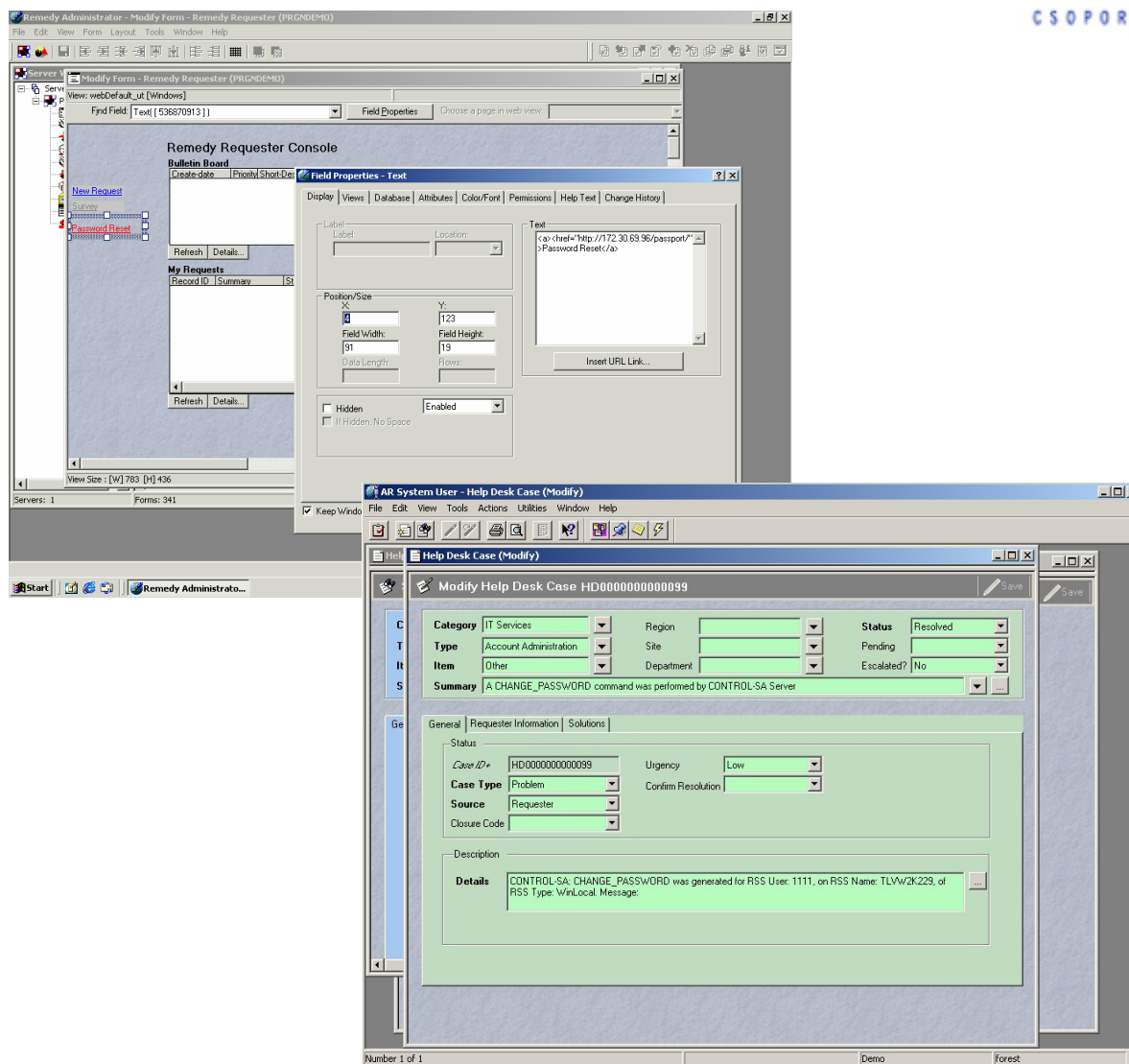
Apply Changes Cancel Hide Individual Accounts

Done Local intranet

További lehetőségek

› Remyedy Help Desk integráció

- Automatikus ticket készítés, a reset érvényességének ellenőrzésére.
- Ha nem sikerült a jelszó reset, figyelmeztető ticket készül.

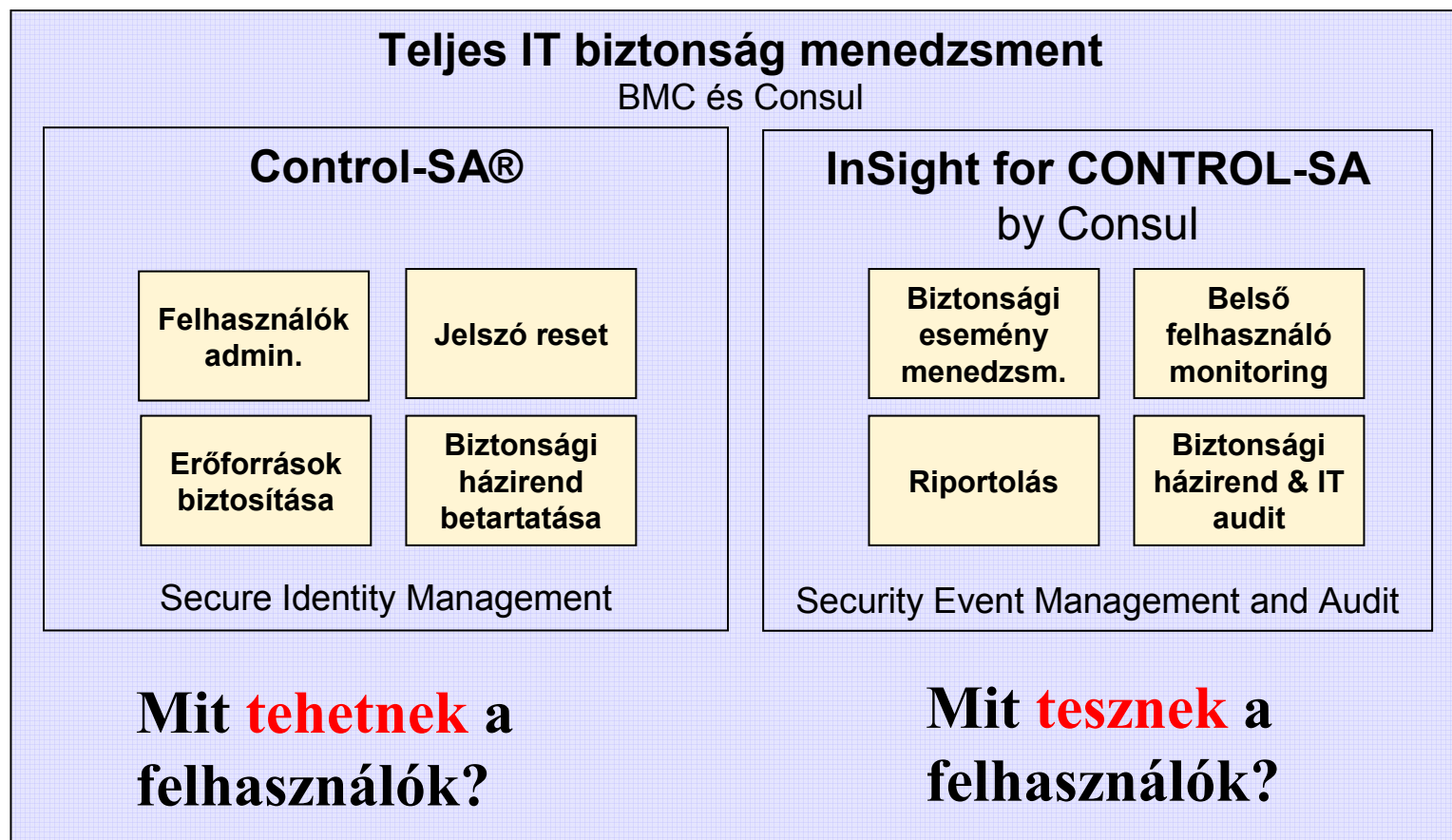


Agenda

- Miért van szükség jogosultságmenedzsmentre?
- BMC Control-SA – egy lehetséges megvalósítás
- Control-SA/PassPort – bízzuk a felhasználóra!
- **InSight for Control-SA – teljes körű biztonsági felügyelet**

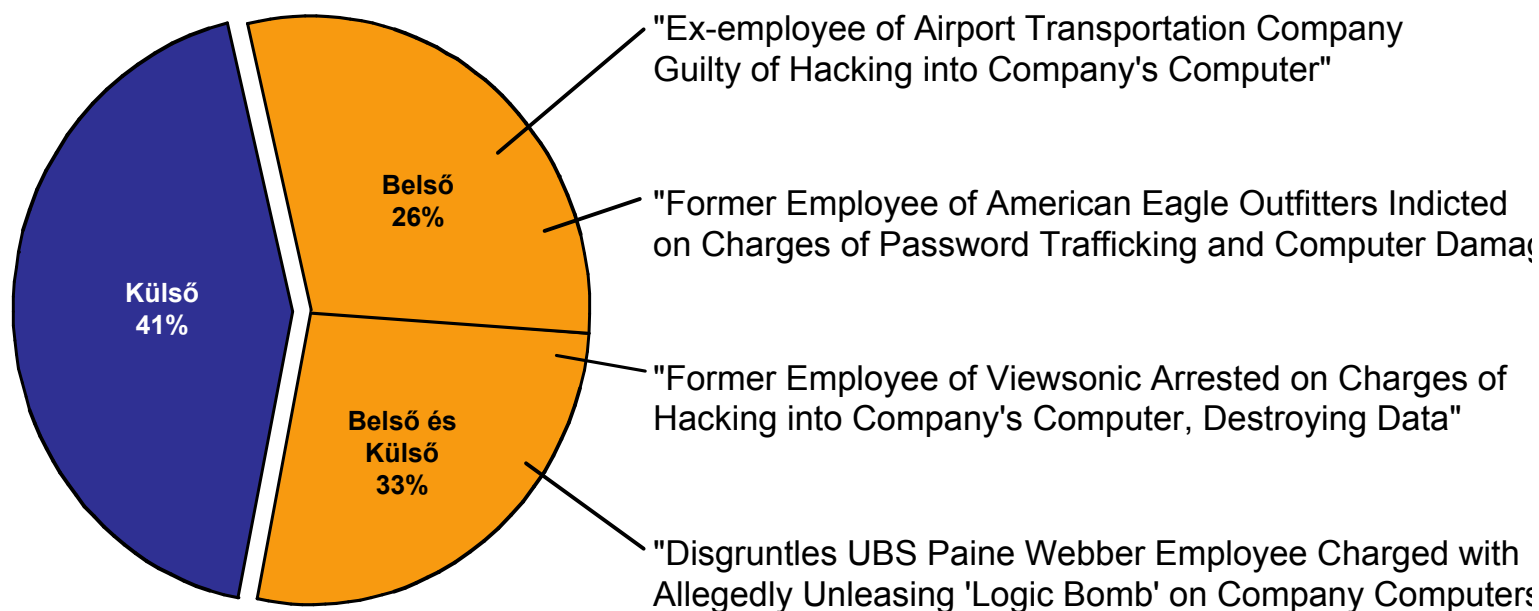


A teljes IT biztonság menedzsment



A „Megbízható Felhasználó” veszélye

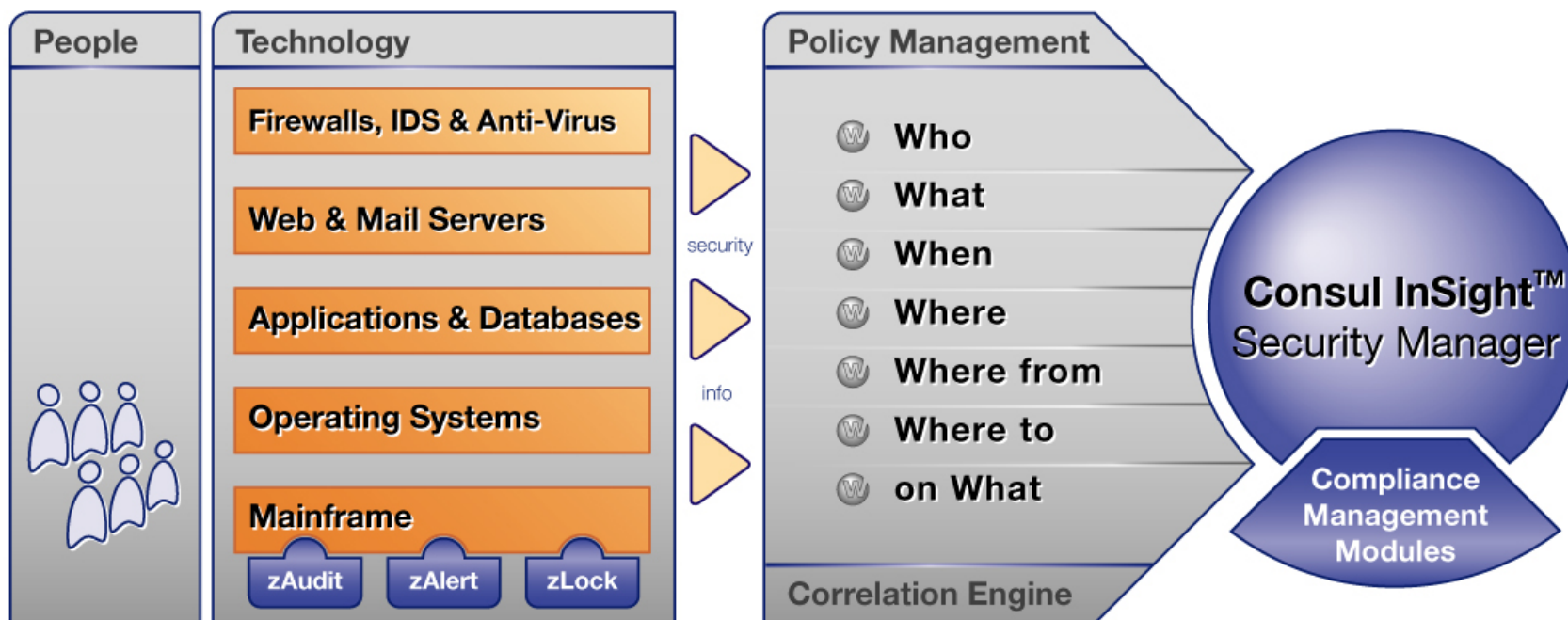
Hálózati támadások forrásai



Forrás: Global Security Survey 2003, Deloitte Touche Tohmatsu

A külső támadások problémákat okozhatnak; a belső támadások tönkreteszhetik a szervezetet.

InSight for Control-SA by Consul

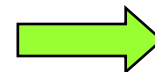
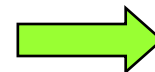
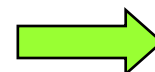
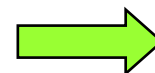
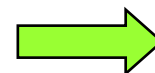
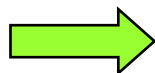


Cél: az IT üzemeltetési és a biztonsági feladatkörök és felelőségek egyértelmű szétválasztása.

Helyi feljegyzések vs. Központi adatgyűjtés

- Lokális megoldás

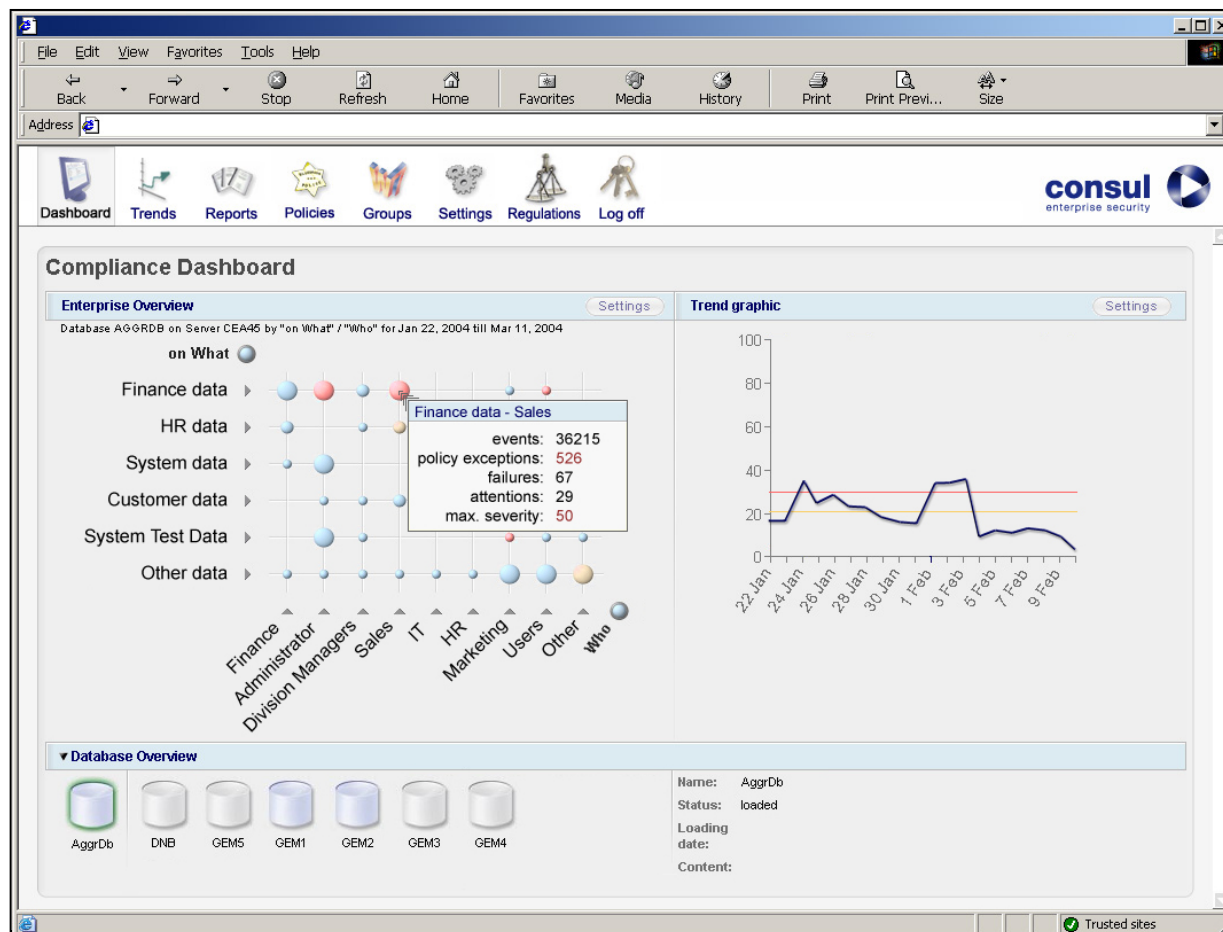
- Csak homogén környezetben
- Nagy, gyakran kezelhetetlen adattömeg
- A feljegyzések törölhetőek
- Reaktív beavatkozás
- IT üzemeltetés részéről erőforrásigény
- A felelősség homályos és nehezen bizonyítható



- Centrális megoldás:

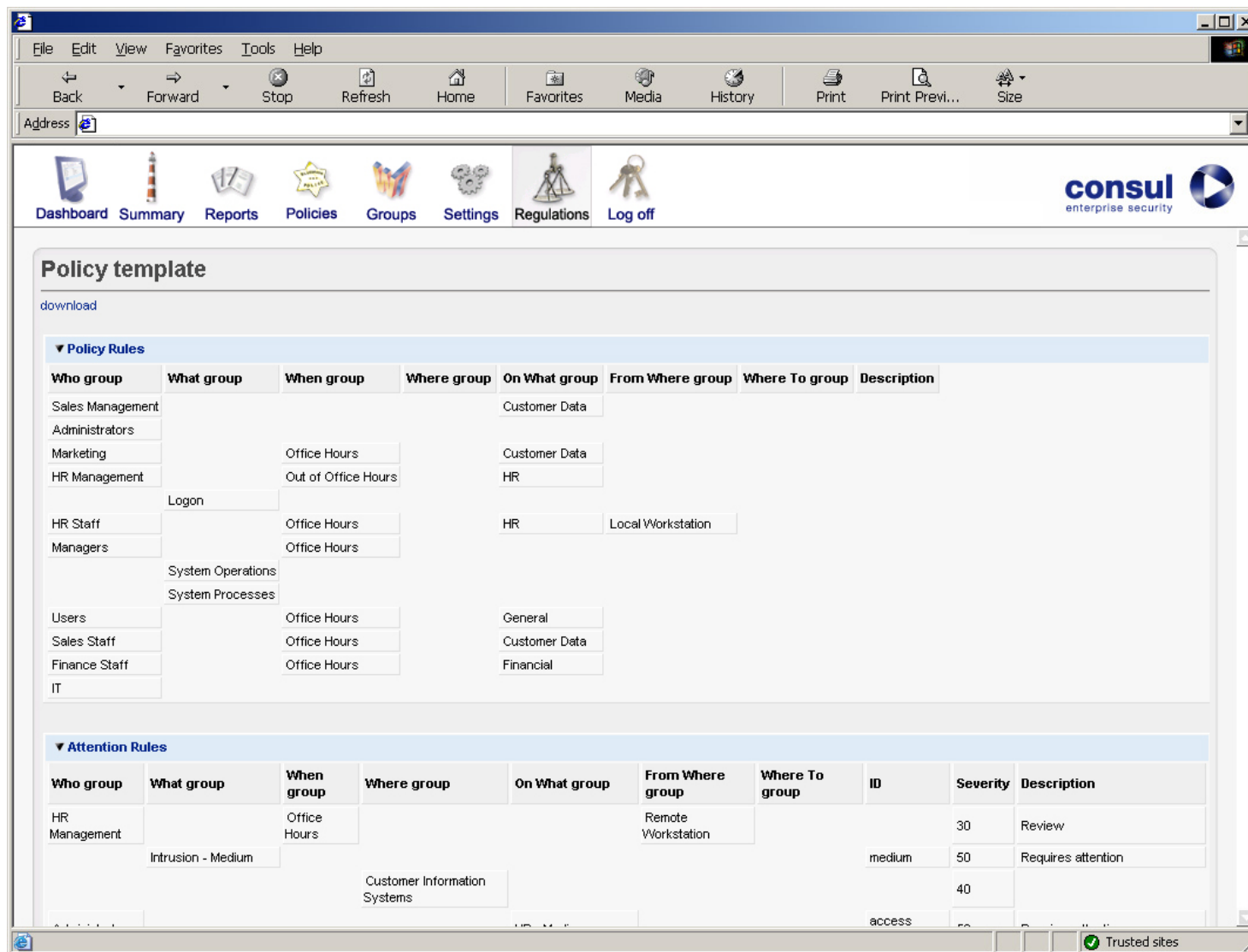
- Tetszőleges számú és típusú platformon
- Könnyen definiálható szűrési feltételek
- Központi tárolás akár évekig
- Proaktív monitorozás és beavatkozás
- Üzemeltetés és biztonság szétválasztása
- A felelősség egyértelmű és bizonyítható

Az InSight jellemzői



- A biztonsági naplóbejegyzések központi összegyűjtése, rendszerezése és kiértékelése.
- Események közötti összefüggések (Correlation Engine).
- Egyszerű, áttekinthető kezelőfelület.
- Valós idejű riasztás és közbeavatkozás (Control-SA).
- Utólagos vizsgálatok, audit, jelentéskészítés.

Biztonsági házirend definiálása



download

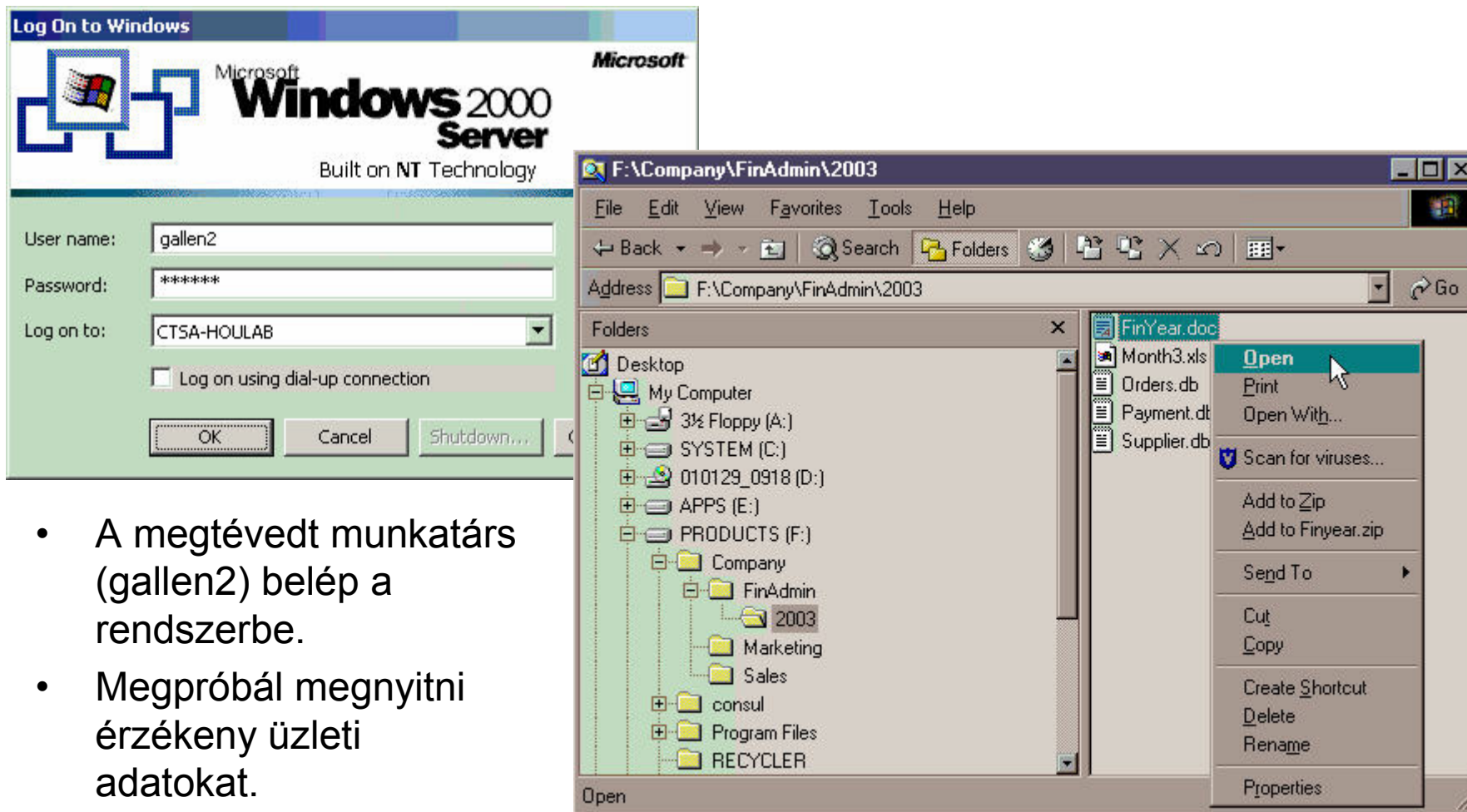
Policy Rules

Who group	What group	When group	Where group	On What group	From Where group	Where To group	Description
Sales Management				Customer Data			
Administrators							
Marketing		Office Hours		Customer Data			
HR Management		Out of Office Hours		HR			
	Logon						
HR Staff		Office Hours		HR	Local Workstation		
Managers		Office Hours					
	System Operations						
	System Processes						
Users		Office Hours		General			
Sales Staff		Office Hours		Customer Data			
Finance Staff		Office Hours		Financial			
IT							

Attention Rules

Who group	What group	When group	Where group	On What group	From Where group	Where To group	ID	Severity	Description
HR Management		Office Hours			Remote Workstation			30	Review
	Intrusion - Medium						medium	50	Requires attention
			Customer Information Systems					40	
							access		

Az InSight működés közben (1.)



The image shows two overlapping windows from a Windows 2000 Server environment. The background window is the 'Log On to Windows' dialog box, where the user 'gallen2' is logging in with a password and selecting 'CTSA-HOULAB' as the log-on location. The foreground window is a File Explorer window showing the directory 'F:\Company\FinAdmin\2003'. A context menu is open over the file 'FinYear.doc', with the 'Open' option highlighted by the mouse cursor. The directory structure in the File Explorer includes 'Desktop', 'My Computer', '3½ Floppy (A:)', 'SYSTEM (C:)', '010129_0918 (D:)', 'APPS (E:)', 'PRODUCTS (F:)', 'Company', 'FinAdmin', '2003', 'Marketing', 'Sales', 'consul', 'Program Files', and 'RECYCLER'.

- A megtévedt munkatárs (gallen2) belép a rendszerbe.
- Megpróbál megnyitni érzékeny üzleti adatokat.

Az InSight működés közben (2.)

Enterprise SecurityStation Console - hou-lab

File View Entities Actions System Tools Window Help

Enterprise User

Entity Type: Enterprise User Max Records to Show: 100

Filtering Rules:

Enterprise User ID Like [] And []

User Name Like [] And []

Ignore Capitalization

Enterprise User ID	User Name
00000000	ESS Manager
00000001	Unattended Administrator
cearoot	CeA/Actuator 4.5 account
consul	Consul
gallen	Greg Allen
imedina	Isaac Medina
jwayne	John Wayne
mtyson	Mike Tyson
rtraiton	Rick Raiton
wclark	Walter Clark

Records Shown: 10 of 10

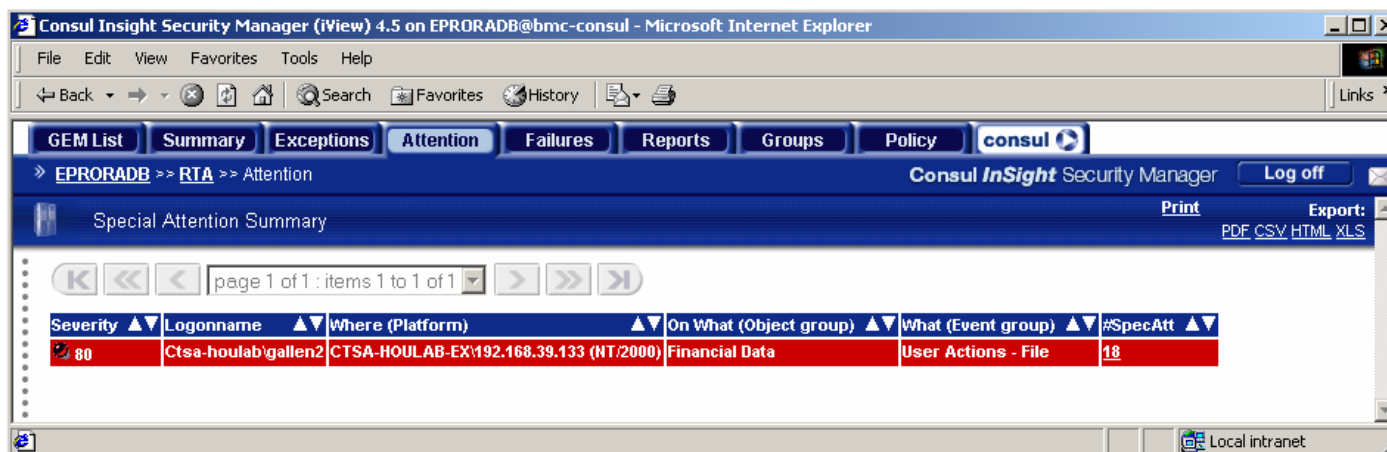
Entity Type: RSS User Max Records to Show: 100

RSS User ID	RSS Name	RSS Type
CN=Greg Allen,CN=Users,DC=CTSA-HOULAB,DC=BMC,DC=com	HOULAB-AD-Win...	Win2000
CN=gallen,CN=Users,DC=CTSA-HOULAB,DC=BMC,DC=com	HOULAB-AD-Win...	Win2000

Records Shown: 2 of 2

Az InSight működés közben (3.)

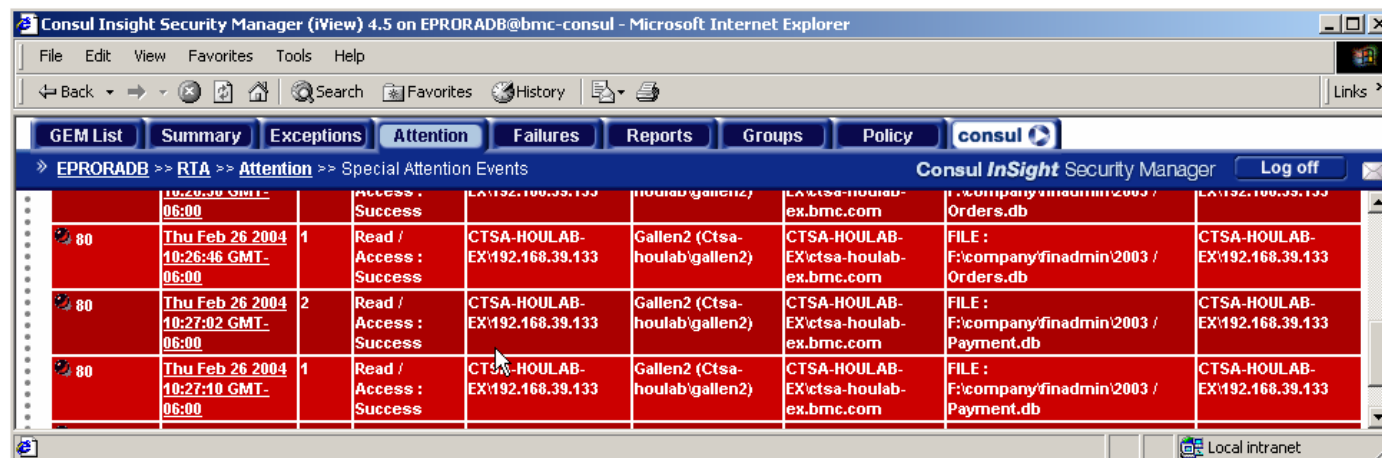
- Az InSight szerver érzékeli a szabálysértést és riasztást generál.



The screenshot shows the 'Special Attention Summary' page in the Consol InSight Security Manager. The interface includes a navigation menu with tabs like 'GEM List', 'Summary', 'Exceptions', 'Attention', 'Failures', 'Reports', 'Groups', and 'Policy'. The current view is 'Attention' for user 'EPRORADB' on the 'RTA' platform. The summary shows one item with a severity of 80, logoname 'Ctsa-houlab/gallen2', and location 'CTSA-HOULAB-EX\192.168.39.133 (NT/2000)'. The event is categorized as 'Financial Data' and 'User Actions - File'.

Severity	Logoname	Where (Platform)	On What (Object group)	What (Event group)	#SpecAtt
80	Ctsa-houlab/gallen2	CTSA-HOULAB-EX\192.168.39.133 (NT/2000)	Financial Data	User Actions - File	18

- Mivel *gallen2* munkaköre alapján számára tilos ezekhez az adatokhoz hozzáférni, ezért súlyos riasztás történik.



The screenshot shows the 'Special Attention Events' page in the Consol InSight Security Manager. It displays a list of events with details such as severity, timestamp, access status, and the specific files accessed. The events are categorized as 'Access : Success' and involve reading files like 'Orders.db' and 'Payment.db'.

Severity	Time	Access	Where (Platform)	On What (Object group)	What (Event group)	#SpecAtt
80	Thu Feb 26 2004 10:26:46 GMT-06:00	Read / Access : Success	CTSA-HOULAB-EX\192.168.39.133	Gallen2 (Ctsa-houlab/gallen2)	FILE : F:\company\finadmin\2003 / Orders.db	1
80	Thu Feb 26 2004 10:27:02 GMT-06:00	Read / Access : Success	CTSA-HOULAB-EX\192.168.39.133	Gallen2 (Ctsa-houlab/gallen2)	FILE : F:\company\finadmin\2003 / Payment.db	2
80	Thu Feb 26 2004 10:27:10 GMT-06:00	Read / Access : Success	CTSA-HOULAB-EX\192.168.39.133	Gallen2 (Ctsa-houlab/gallen2)	FILE : F:\company\finadmin\2003 / Payment.db	1

Az InSight működés közben (4.)

Az InSight megmagyarázza a riasztás konkrét okát is.

Consul InSight Security Manager (iView) 4.5 on EPRORADB@bmc-consul - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Links

GEM List Summary Exceptions Attention Failures Reports Groups Policy consul

EPRORADB >> RTA >> Explanation of Severity Consul InSight Security Manager Log off

This event is a Special Attention Event and a [Policy Exception](#). It matches an Attention Rule and does not comply with the Security Policy, because it does not match any of the Policy Rules.

The event is given the higher of the Policy Exception Severity and the Special Attention Severity.

Policy Exception Severity is determined from Group Significance.

For every event, Consul InSight Security Manager shows into which W7 groups it falls.

When you configured Consul InSight Security Manager you gave each W7 group a significance (see the numbers in brackets).

The most significant group (ObjectGroup "Financial Data" in this case) determines the Policy Exception Severity.

event:

When : Period	What : Eventtype	Where : Platform	Who : Source	WhereFrom : Origin	onWhat : Object	WhereTo : Target
Thu Feb 26 2004 14:00:00 GMT-06:00	Read : Access / Success	CTSA-HOULAB-EX192.168.39.133 (NT/2000)	Gallen2 (Ctsa-houlab@gallen2)	CTSA-HOULAB-EX\ctsa-houlab-ex.bmc.com (NT/2000)	FILE : F:\company\winadmin\2003 / Supplier.db	CTSA-HOULAB-EX192.168.39.133 (NT/2000)

groups:

When : PeriodGroup	What : EventtypeGroup	Where : PlatformGroup	Who : SourceGroup	WhereFrom : OriginGroup	onWhat : ObjectGroup	WhereTo : TargetGroup
Office Hours (10)	User Actions - File	Win2k (10)	Unauthorized_FIN (70) Unauthorized_ADMIN (70) System Admins (10)	Other Platforms (10)	Financial Data (80)	Win2k (10)

Policy Exceptions have a severity (in the range 10-99), equal to the Group Significance.

In this case, ObjectGroup "Financial Data" is the most significant W7 group, with significance 80.

Therefore, the Policy Exception Severity is 80.

Special Attention Severity is determined from Attention Rule Severity.

When you configured Consul InSight Security Manager, you defined the Attention Rules and their severity.

Attention Rules have a severity in the range 10-99.

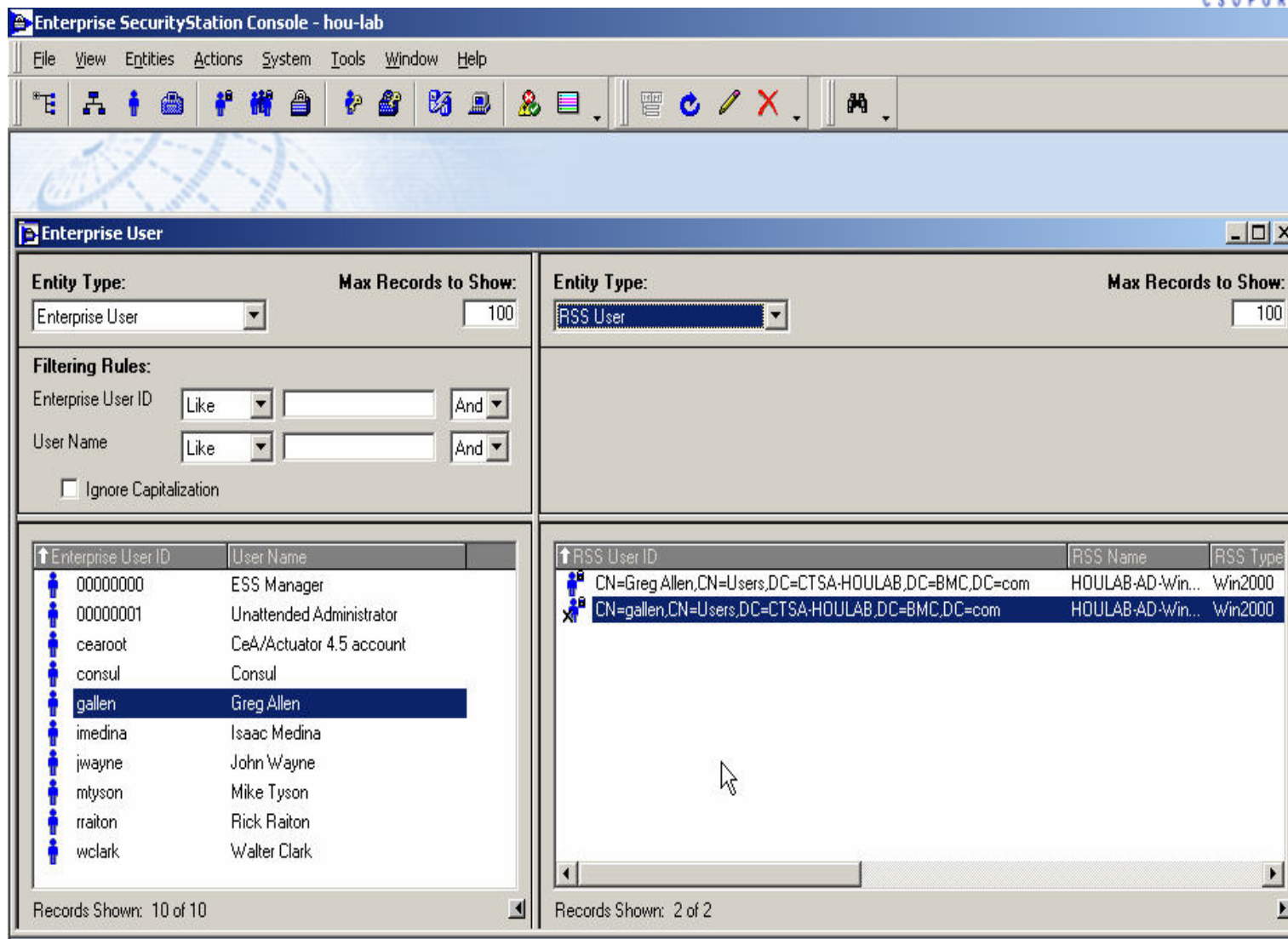
This is a Special Attention Event, because it matches the rule:

Who (Source group)	What (Event group)	When (Period group)	Where (Platform group)	On What (Object group)	fromWhere (Origin group)	WhereTo (Target group)	Description	Severity
Unauthorized_FIN	User Actions - File	_ANY_	_ANY_	Financial Data	_ANY_	_ANY_	Unauthorized access - Financial data	80

name (type) - Click here to see the Event list by Platform Local intranet

Az InSight működés közben (5.)

A Control-SA visszavonja *gallen2* felhasználói hozzáféréseit.



The screenshot shows the Enterprise SecurityStation Console interface. The main window is titled "Enterprise SecurityStation Console - hou-lab" and contains two panes for viewing user entities.

Left Pane: Enterprise User

- Entity Type: Enterprise User
- Max Records to Show: 100
- Filtering Rules:
 - Enterprise User ID: Like [] And
 - User Name: Like [] And
 - Ignore Capitalization
- Table:

Enterprise User ID	User Name
00000000	ESS Manager
00000001	Unattended Administrator
cearoot	CeA/Actuator 4.5 account
consul	Consul
gallen	Greg Allen
imedina	Isaac Medina
jwayne	John Wayne
mtyson	Mike Tyson
rtraiton	Rick Raiton
wclark	Walter Clark
- Records Shown: 10 of 10

Right Pane: RSS User

- Entity Type: RSS User
- Max Records to Show: 100
- Table:

RSS User ID	RSS Name	RSS Type
CN=Greg Allen,CN=Users,DC=CTSA-HOULAB,DC=BMC,DC=com	HOULAB-AD-Win...	Win2000
CN=gallen,CN=Users,DC=CTSA-HOULAB,DC=BMC,DC=com	HOULAB-AD-Win...	Win2000
- Records Shown: 2 of 2

A biztonsági szabályozás betartatása

BSM Identity Management

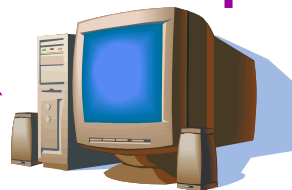
Greg Allen megpróbál hozzáférni az üzleti statisztikákhoz.



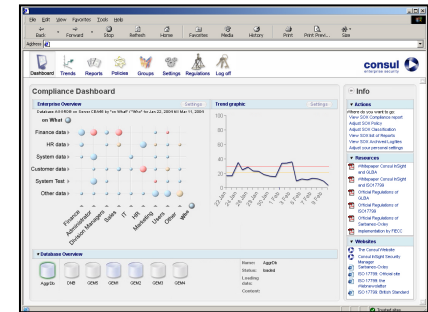
A Consul Insight érzékeli a hozzáférési kísérletet.

A Control-SA felfüggeszti Greg Allen hozzáférését.

Az integrált InSight jelzi a Control-SA felé a házirend megsértését.



CONTROL-SA



Consul InSight



CONTROL-SA Admin

Itt a vége...

**Köszönöm
a figyelmet !**