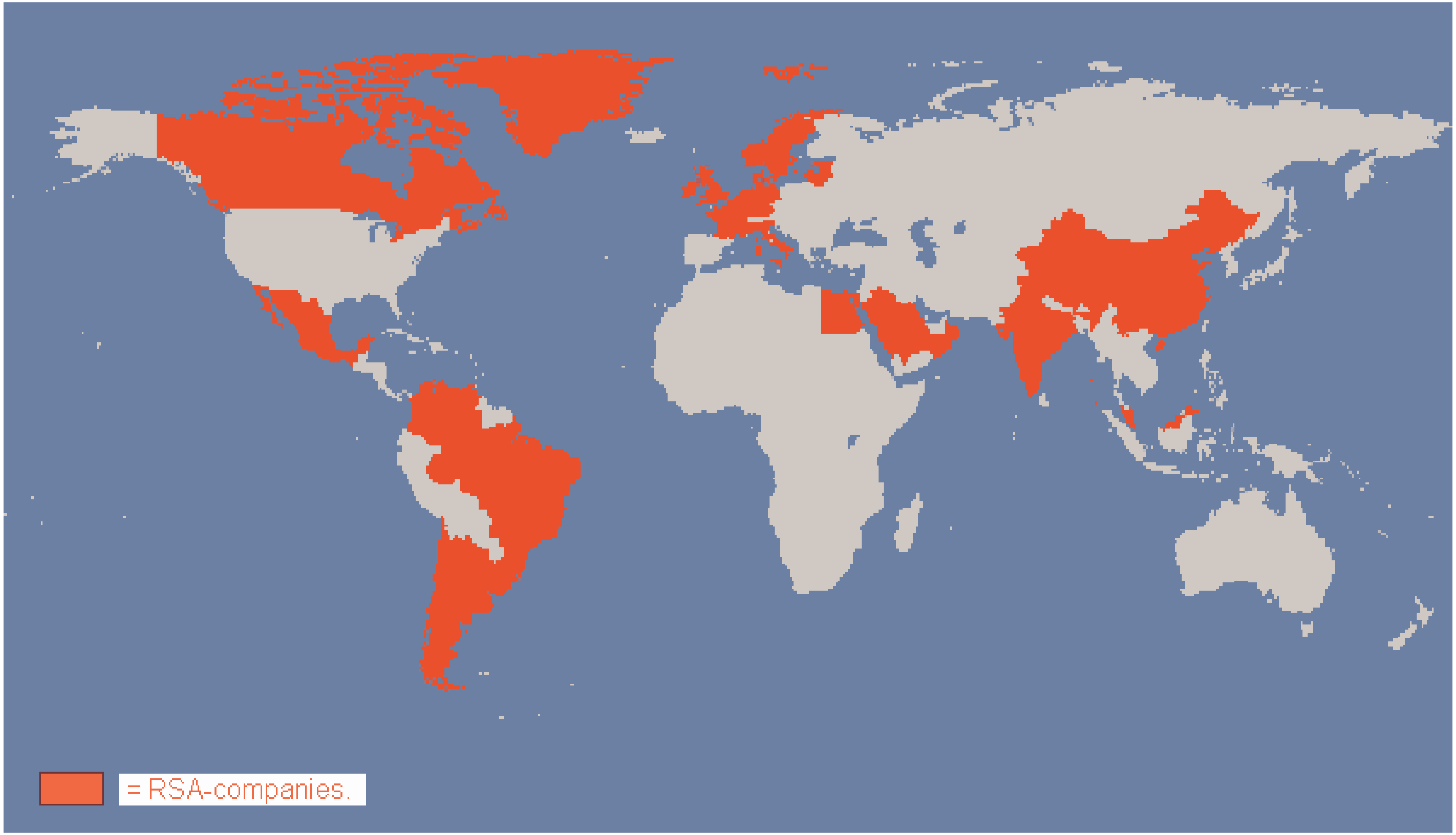
Royal & SunAlliance

How we use Consul products

Agenda

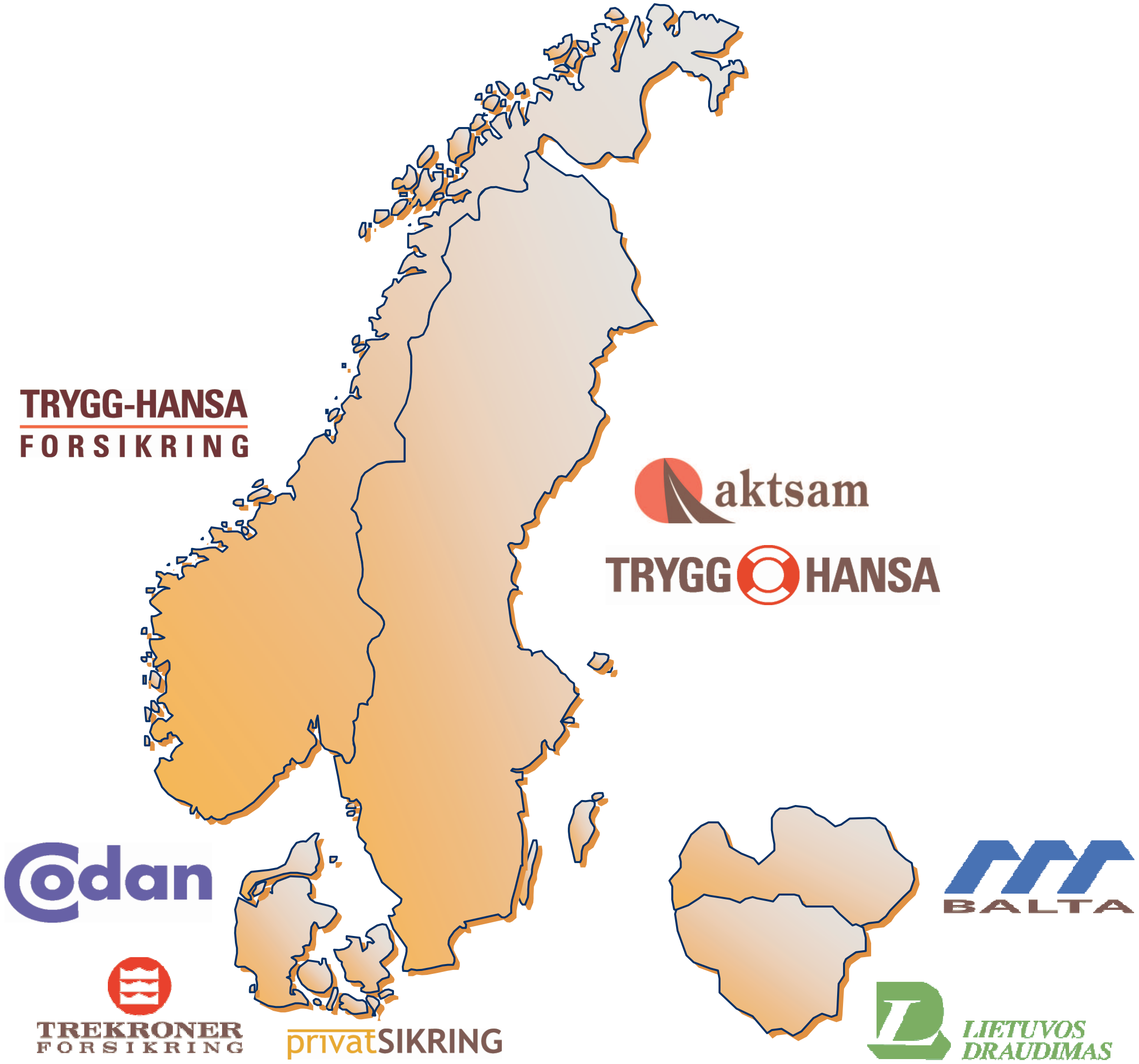
- Who are Codan & TryggHansa
- Our history with Consul - until now
- Platforms and setup
- Sarbanes Oxley demands
- Daily business
- Creating new reports
- Future

RSA - worldwide



Companies in the nordic countries

ROYAL & SUNALLIANCE



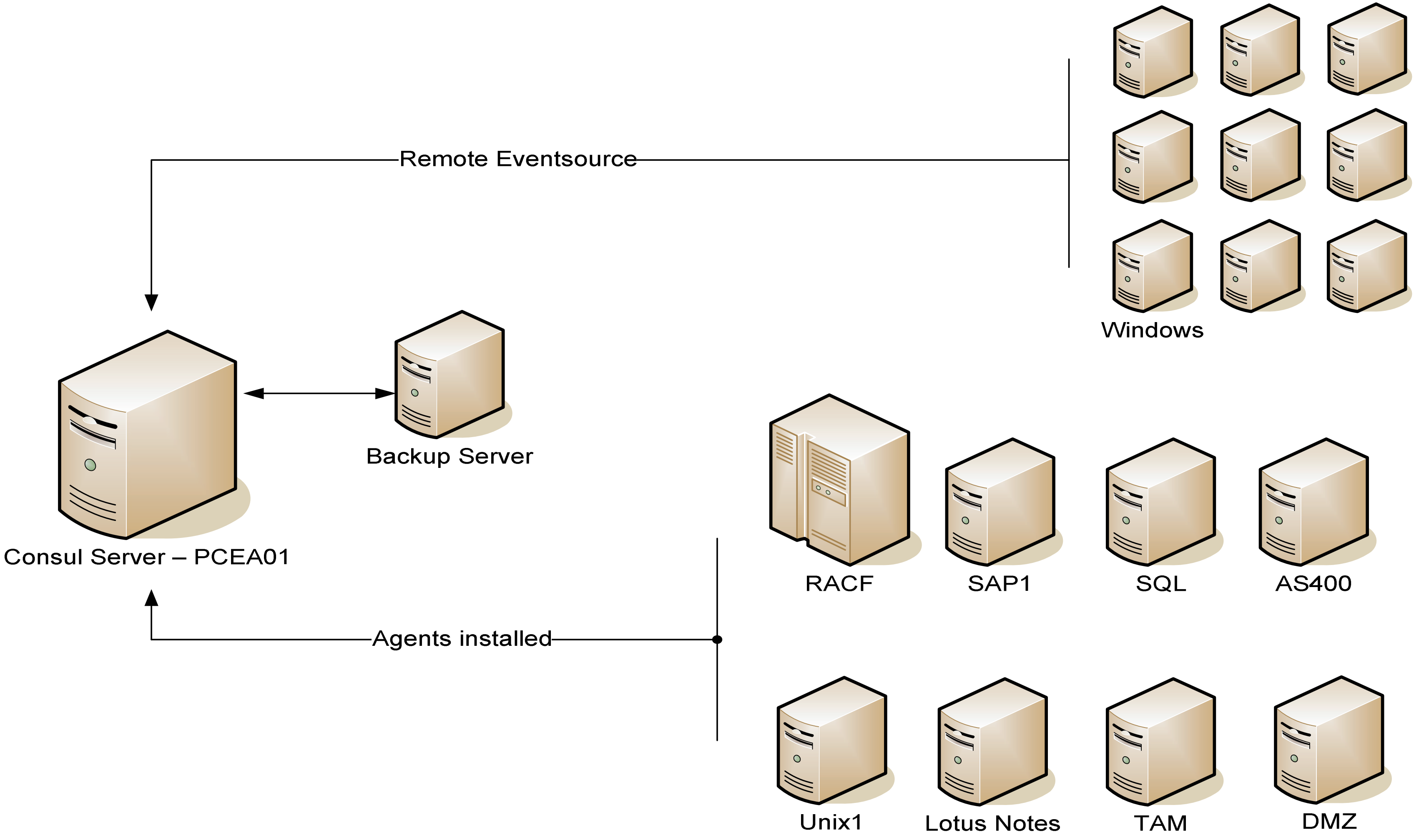
Codan & TryggHansa.

- Codan is the 3rd. largest insurancecompany in Denmark
- TryggHansa is also the 3rd. largest in Sweden
- Total of 6000 employees.

History with Consul.

- 1998 - Codan bought the first Consul product.
- 1999 - Codan started with Consul Enterprice.
- End 1999 - Starting to monitor Windows and AIX.
- During 2004 and 2005 - More platforms.
- 2005 - Sabanes Oxley Module / Sox reports.

Platforms and Setup



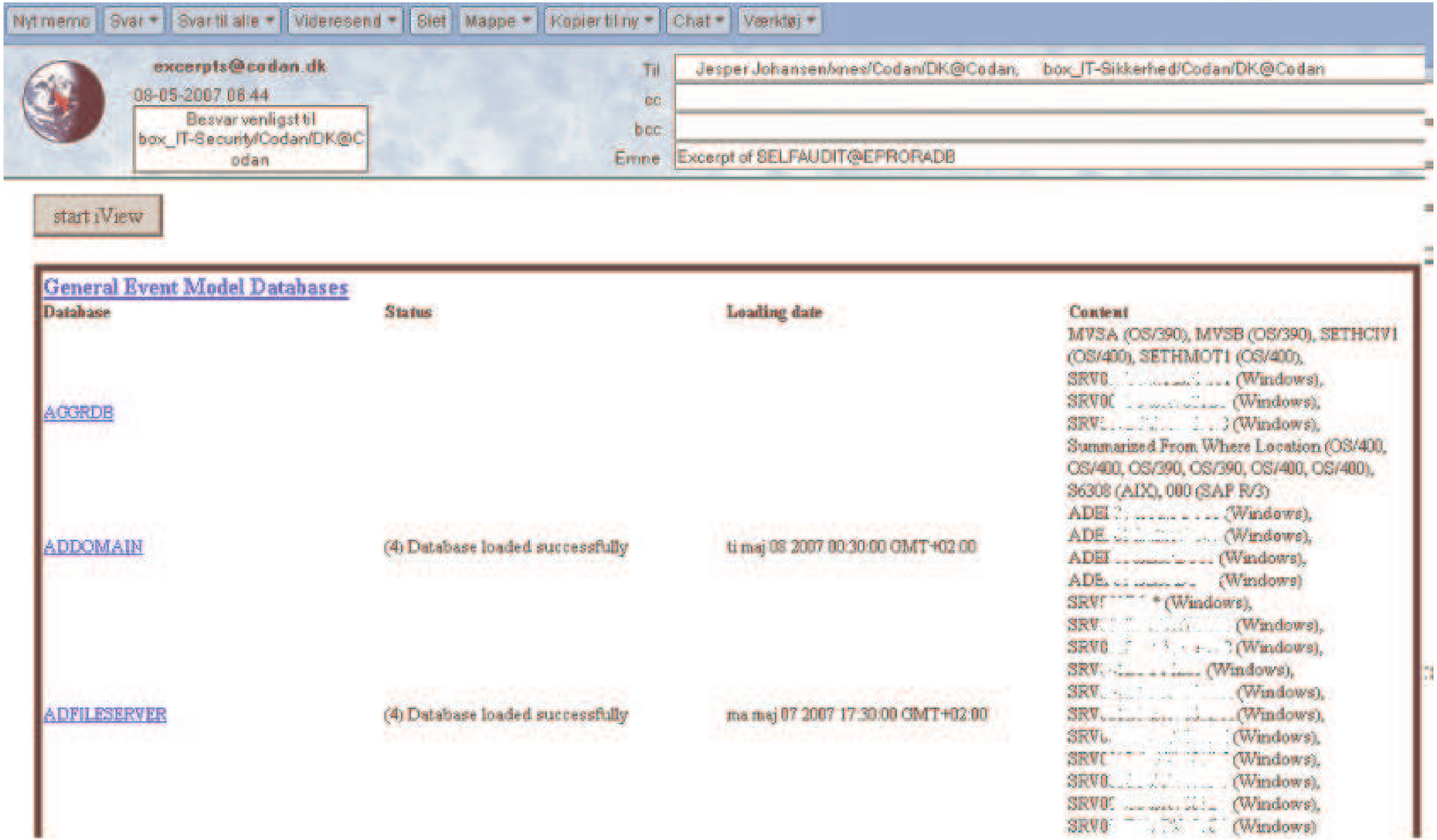
Sarbanes Oxley.

- Do you have a policy ?
- Do you use it ?
- Can you prove it ?

Daily business.

- Daily control and reports
- Policies and sensitive data
- Alerts.
- Investigation.

Mail from the server.



excerpts@codan.dk

08-05-2007 08.44

Besvar venligst til box_IT-Security/Codan/DK@Codan

Til: Jesper Johansen/xnes/Codan/DK@Codan, box_IT-Sikkerhed/Codan/DK@Codan

cc:

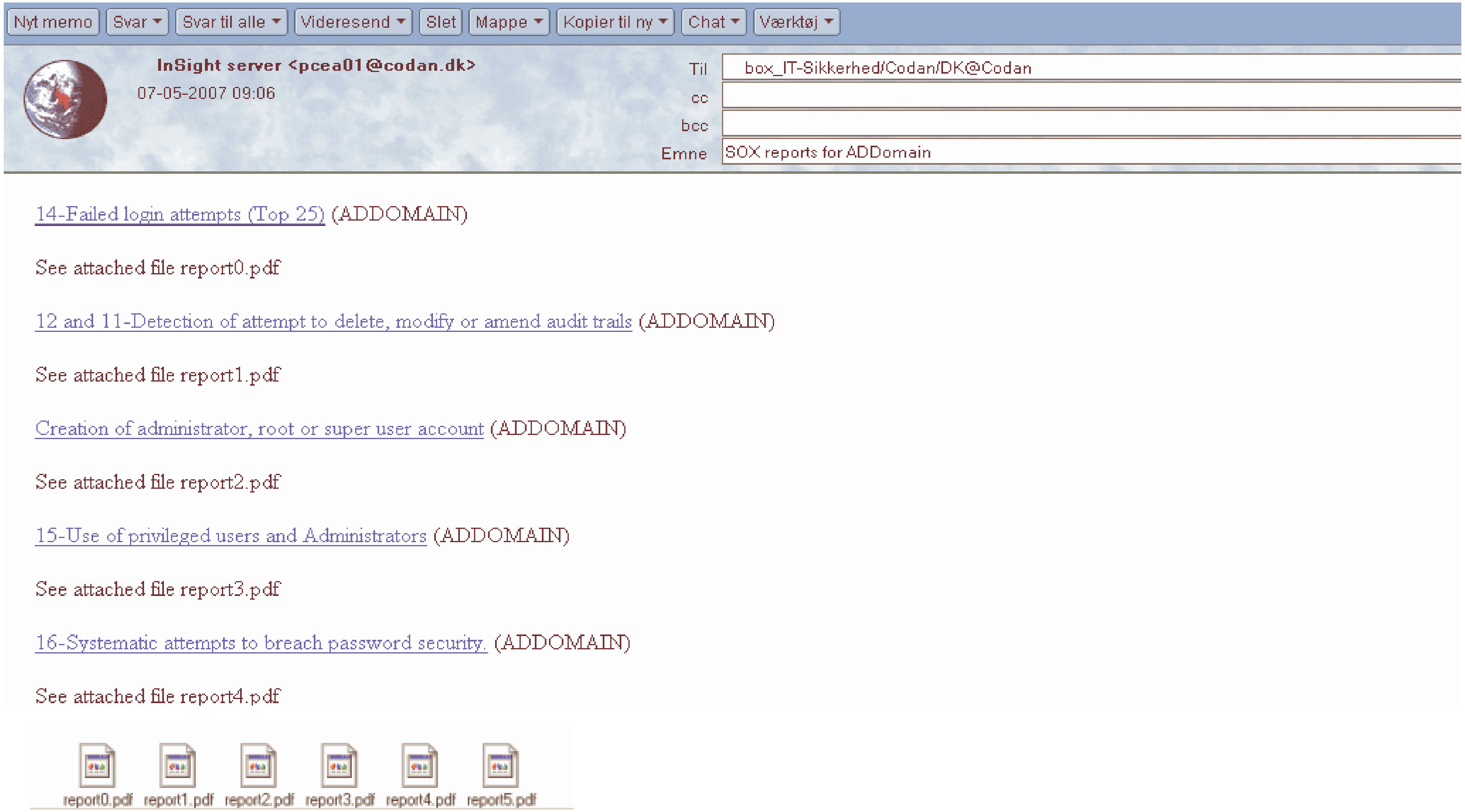
bcc:

Emne: Excerpt of SELFAUDIT@EPRORADB

General Event Model Databases

Database	Status	Loading date	Content
AGGRDB			MVSA (OS/390), MVSB (OS/390), SETHCIV1 (OS/400), SETHMOT1 (OS/400), SRV0 [redacted] (Windows), SRV0 [redacted] (Windows), SRV [redacted] (Windows), Summarized From Where Location (OS/400, OS/400, OS/390, OS/390, OS/400, OS/400), S6308 (AIX), 000 (SAP R/3)
ADDOMAIN	(4) Database loaded successfully	ti maj 08 2007 00:30:00 GMT+02:00	ADE [redacted] (Windows), ADE [redacted] (Windows), ADE [redacted] (Windows), ADE [redacted] (Windows)
ADFILESERVER	(4) Database loaded successfully	ma maj 07 2007 17:30:00 GMT+02:00	SRV [redacted] (Windows), SRV [redacted] (Windows), SRV0 [redacted] (Windows), SRV [redacted] (Windows), SRV [redacted] (Windows), SRV [redacted] (Windows), SRV [redacted] (Windows), SRV [redacted] (Windows), SRV0 [redacted] (Windows), SRV0 [redacted] (Windows), SRV0 [redacted] (Windows)

Mail - Codan Sox Reports



InSight server <pcea01@codan.dk>
07-05-2007 09:06

Til box_IT-Sikkerhed/Codan/DK@Codan
cc
bcc
Emne SOX reports for ADDomain

14-Failed login attempts (Top 25) (ADDOMAIN)

See attached file report0.pdf

12 and 11-Detection of attempt to delete, modify or amend audit trails (ADDOMAIN)

See attached file report1.pdf

Creation of administrator, root or super user account (ADDOMAIN)

See attached file report2.pdf

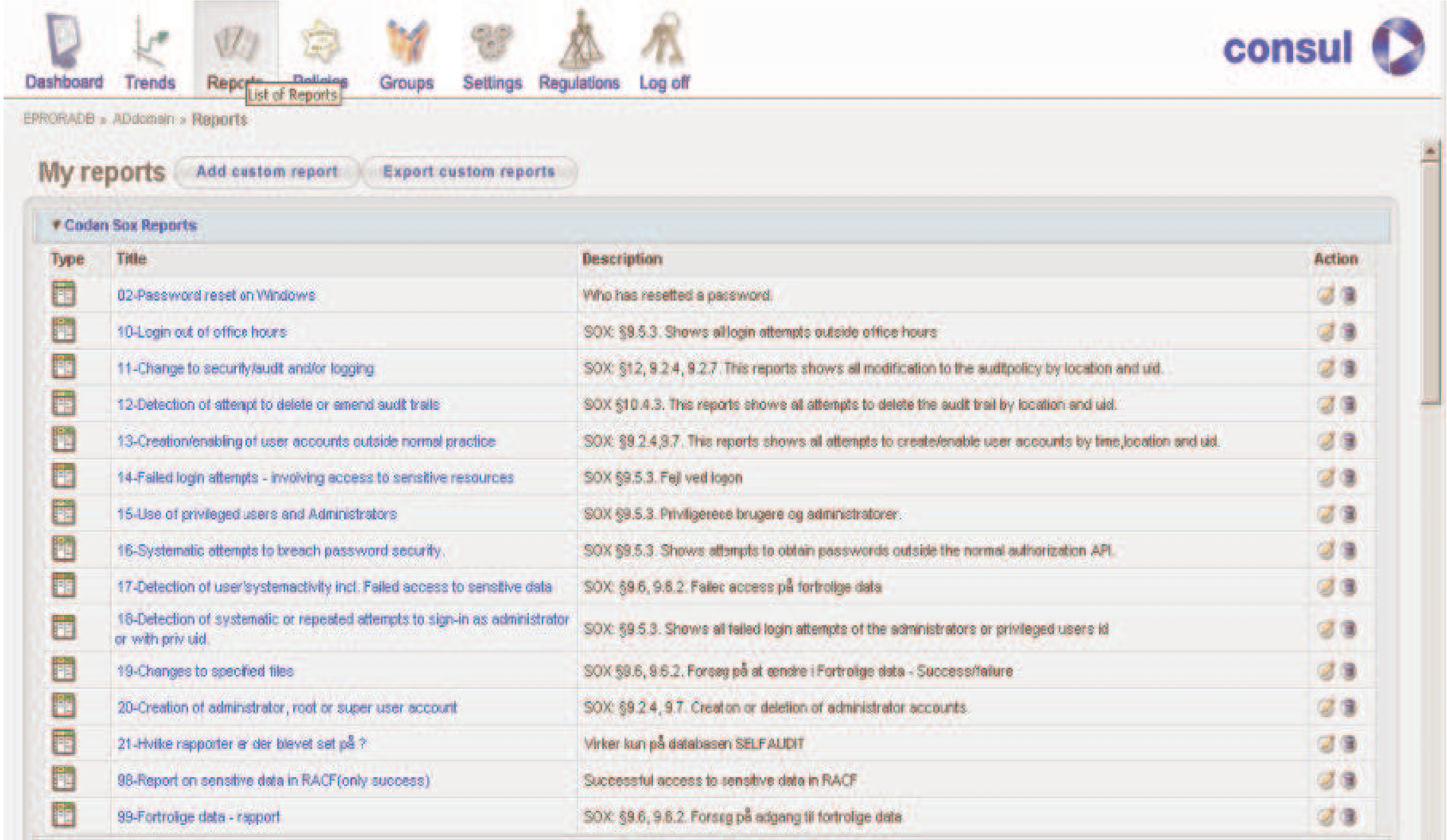
15-Use of privileged users and Administrators (ADDOMAIN)

See attached file report3.pdf

16-Systematic attempts to breach password security. (ADDOMAIN)

See attached file report4.pdf

Iview - Codan Sox Reports



EPRORADB » ADdomain » Reports

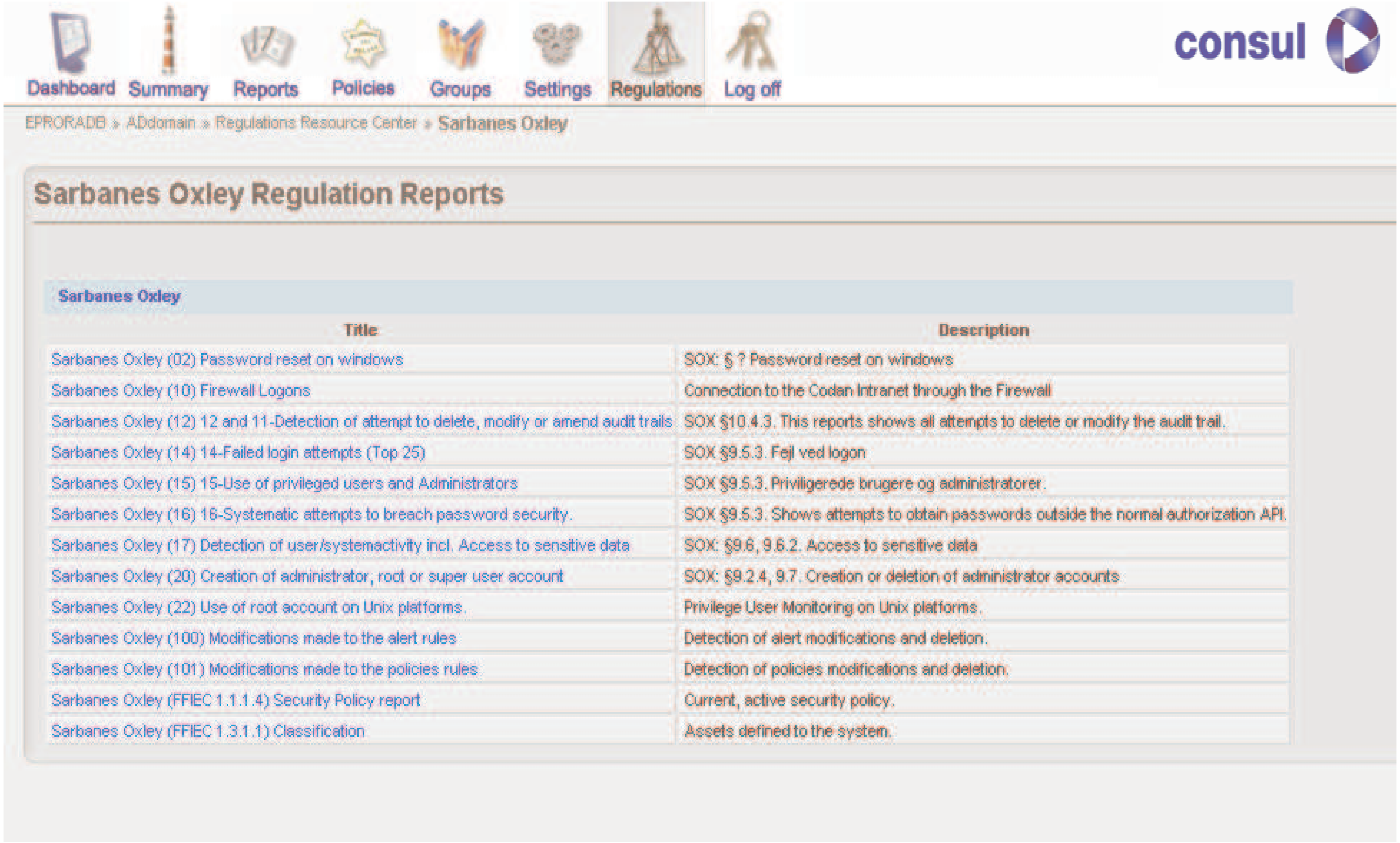
My reports

Add custom report | Export custom reports

▾ Codan Sox Reports

Type	Title	Description	Action
▦	02-Password reset on Windows	Who has resetted a password.	
▦	10-Login out of office hours	SOX: §9.5.3. Shows all login attempts outside office hours	
▦	11-Change to security/audit and/or logging	SOX: §12, 9.2.4, 9.2.7. This reports shows all modification to the auditpolicy by location and uid.	
▦	12-Detection of attempt to delete or amend audit trails	SOX §10.4.3. This reports shows all attempts to delete the audit trail by location and uid.	
▦	13-Creation/enabling of user accounts outside normal practice	SOX: §9.2.4,9.7. This reports shows all attempts to create/enable user accounts by time,location and uid.	
▦	14-Failed login attempts - involving access to sensitive resources	SOX §9.5.3. Fejl ved logon	
▦	15-Use of privileged users and Administrators	SOX §9.5.3. Priviligerede brugere og administratorer.	
▦	16-Systematic attempts to breach password security.	SOX §9.5.3. Shows attempts to obtain passwords outside the normal authorization API.	
▦	17-Detection of user'systemactivity incl. Failed access to sensitive data	SOX: §9.6, 9.6.2. Failed access på fortrolige data	
▦	18-Detection of systematic or repeated attempts to sign-in as administrator or with priv uid.	SOX: §9.5.3. Shows all failed login attempts of the administrators or privileged users id	
▦	19-Changes to specified files	SOX §9.6, 9.6.2. Forsøg på at ændre i Fortrolige data - Success/failure	
▦	20-Creation of adminstrator, root or super user account	SOX: §9.2.4, 9.7. Creation or deletion of administrator accounts	
▦	21-Hvilke rapporter er der blevet sat på ?	Virker kun på databasen SELFAUDIT	
▦	98-Report on sensitive data in RACF(only success)	Successful access to sensitive data in RACF	
▦	99-Fortrolige data - rapport	SOX: §9.6, 9.6.2. Forsøg på adgang til fortrolige data	

Iview - Codan Sox Reports



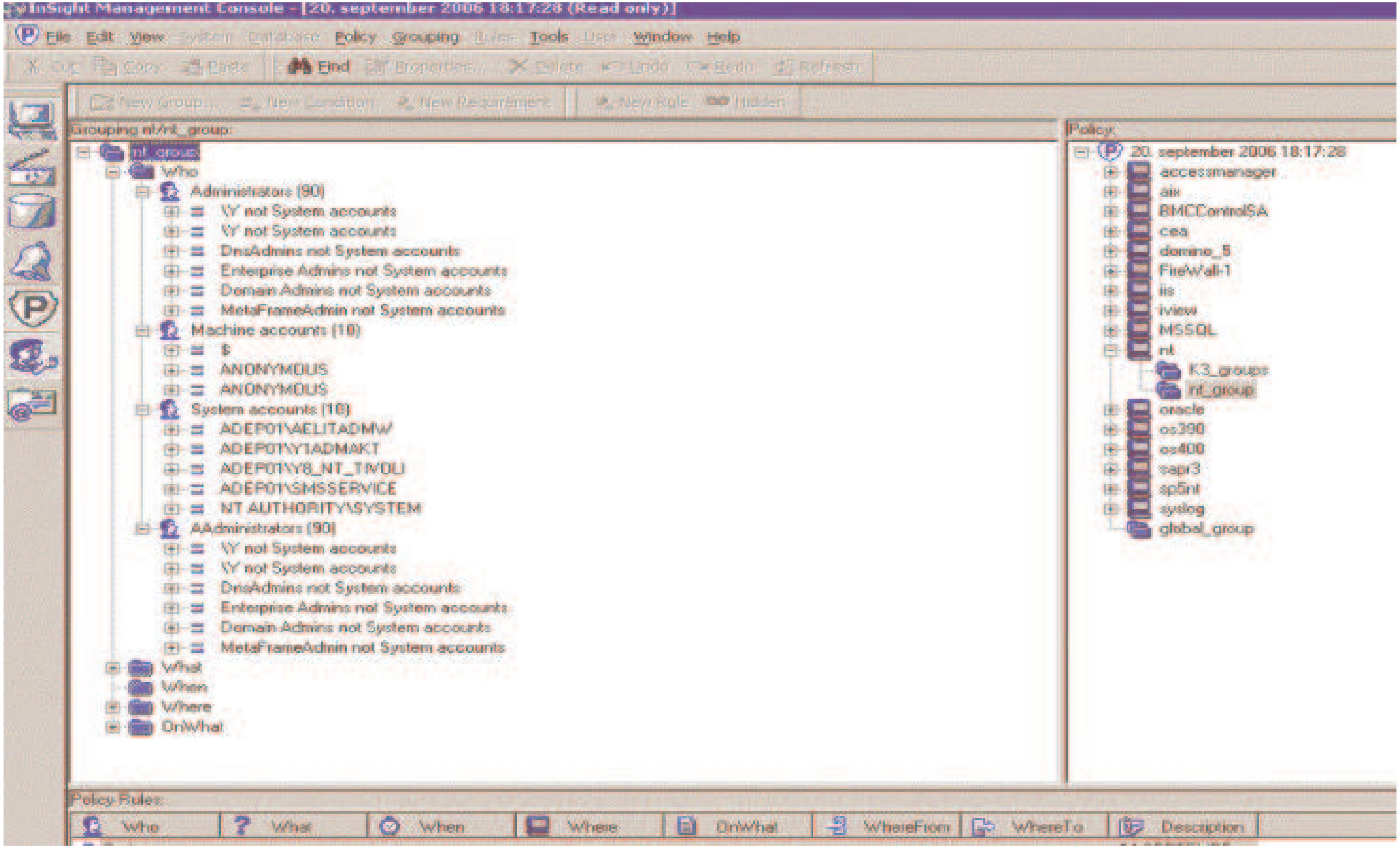
EPRORADB » ADdomain » Regulations Resource Center » Sarbanes Oxley

Sarbanes Oxley Regulation Reports

Sarbanes Oxley

Title	Description
Sarbanes Oxley (02) Password reset on windows	SOX: § ? Password reset on windows
Sarbanes Oxley (10) Firewall Logons	Connection to the Codan Intranet through the Firewall
Sarbanes Oxley (12) 12 and 11-Detection of attempt to delete, modify or amend audit trails	SOX §10.4.3. This reports shows all attempts to delete or modify the audit trail.
Sarbanes Oxley (14) 14-Failed login attempts (Top 25)	SOX §9.5.3. Fejl ved logon
Sarbanes Oxley (15) 15-Use of privileged users and Administrators	SOX §9.5.3. Priviligerede brugere og administratorer.
Sarbanes Oxley (16) 16-Systematic attempts to breach password security.	SOX §9.5.3. Shows attempts to obtain passwords outside the normal authorization API.
Sarbanes Oxley (17) Detection of user/systemactivity incl. Access to sensitive data	SOX: §9.6, 9.6.2. Access to sensitive data
Sarbanes Oxley (20) Creation of administrator, root or super user account	SOX: §9.2.4, 9.7. Creation or deletion of administrator accounts
Sarbanes Oxley (22) Use of root account on Unix platforms.	Privilege User Monitoring on Unix platforms.
Sarbanes Oxley (100) Modifications made to the alert rules	Detection of alert modifications and deletion.
Sarbanes Oxley (101) Modifications made to the policies rules	Detection of policies modifications and deletion.
Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report	Current, active security policy.
Sarbanes Oxley (FFIEC 1.3.1.1) Classification	Assets defined to the system.

Policies



Grouping nt/nt_group:

```
nt_group
  Who
    Administrators (90)
      \Y' not System accounts
      \Y' not System accounts
      DnsAdmins not System accounts
      Enterprise Admins not System accounts
      Domain Admins not System accounts
      MetaFrameAdmin not System accounts
    Machine accounts (10)
      $
      ANONYMOUS
      ANONYMOUS
    System accounts (10)
      ADEP01\AELITADMW
      ADEP01\Y1ADMAKT
      ADEP01\Y8_NT_TIVOLI
      ADEP01\SMSSERVICE
      NT AUTHORITY\SYSTEM
    AAdministrators (90)
      \Y' not System accounts
      \Y' not System accounts
      DnsAdmins not System accounts
      Enterprise Admins not System accounts
      Domain Admins not System accounts
      MetaFrameAdmin not System accounts
  What
  When
  Where
  OnWhat
```

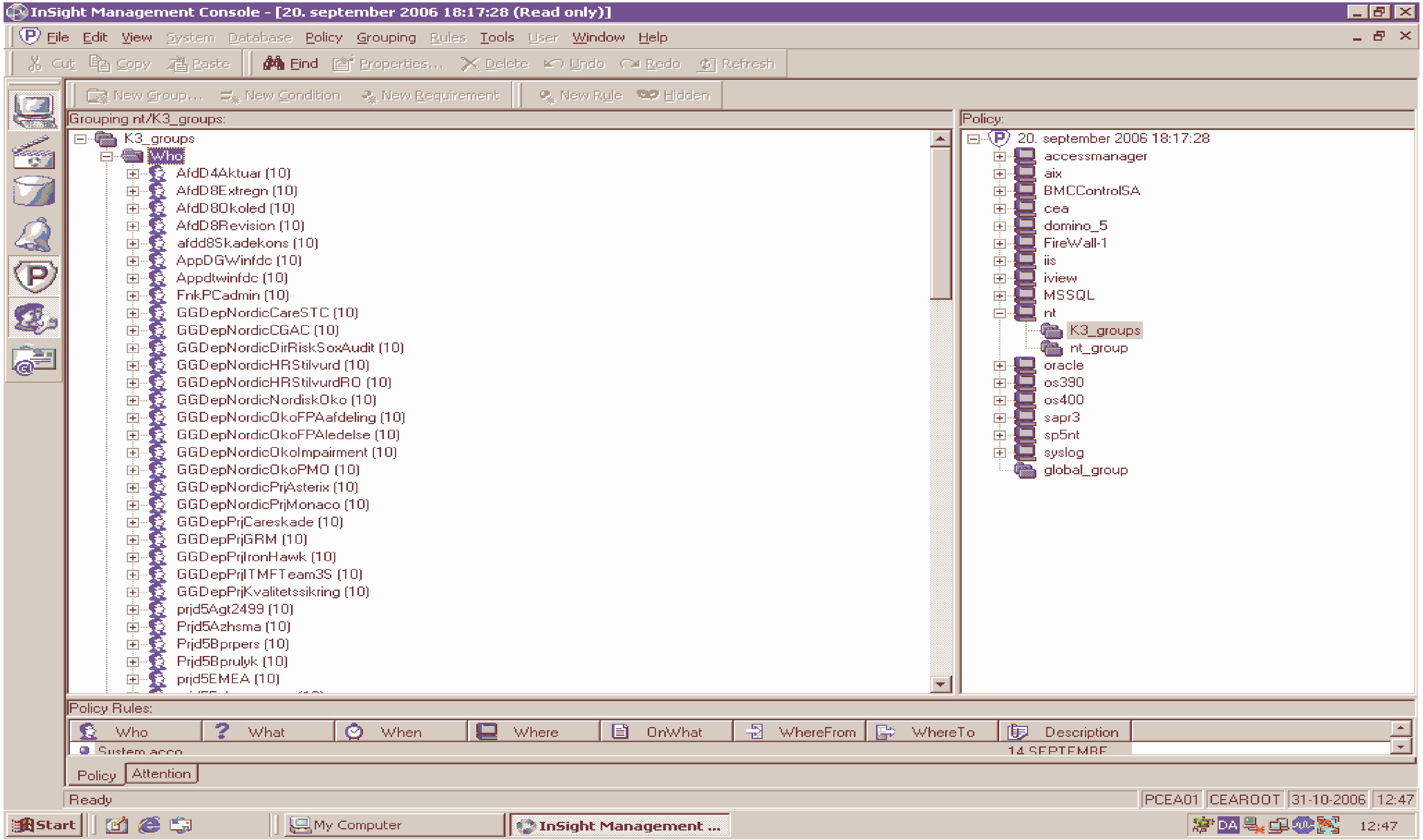
Policy:

```
20. september 2006 18:17:28
  accessmanager
  aix
  BMCControlSA
  cea
  domino_5
  FireWall-1
  iis
  iview
  MSSQL
  nt
    K3_groups
    nt_group
  oracle
  os390
  os400
  sapr3
  sp5nt
  syslog
  global_group
```

Policy Rules:

Who	What	When	Where	OnWhat	WhereFrom	WhereTo	Description

Sensitive data



InSight Management Console - [20. september 2006 18:17:28 (Read only)]
File Edit View System Database Policy Grouping Rules Tools User Window Help
Cut Copy Paste Find Properties... Delete Undo Redo Refresh
New Group... New Condition New Requirement New Rule Hidden

Grouping nt/K3_groups:

- K3_groups
  - Who
    - AfdD4Aktuar (10)
    - AfdD8Extregn (10)
    - AfdD8Okoled (10)
    - AfdD8Revision (10)
    - afdd8Skadekons (10)
    - AppDGWinfdc (10)
    - Appdtwinfdc (10)
    - FnkPCadmin (10)
    - GGDepNordicCareSTC (10)
    - GGDepNordicCGAC (10)
    - GGDepNordicDirRiskSoxAudit (10)
    - GGDepNordicHRStilvurd (10)
    - GGDepNordicHRStilvurdRO (10)
    - GGDepNordicNordiskOko (10)
    - GGDepNordicOkoFPAafdeling (10)
    - GGDepNordicOkoFPAledelse (10)
    - GGDepNordicOkoImpairment (10)
    - GGDepNordicOkoPMO (10)
    - GGDepNordicPrjAsterix (10)
    - GGDepNordicPrjMonaco (10)
    - GGDepPrjCareskade (10)
    - GGDepPrjGRM (10)
    - GGDepPrjIronHawk (10)
    - GGDepPrjITMFTeam3S (10)
    - GGDepPrjKvalitetssikring (10)
    - prjd5Agt2499 (10)
    - Prjd5Azhsma (10)
    - Prjd5Bprpers (10)
    - Prjd5Bprulyk (10)
    - prjd5EMEA (10)

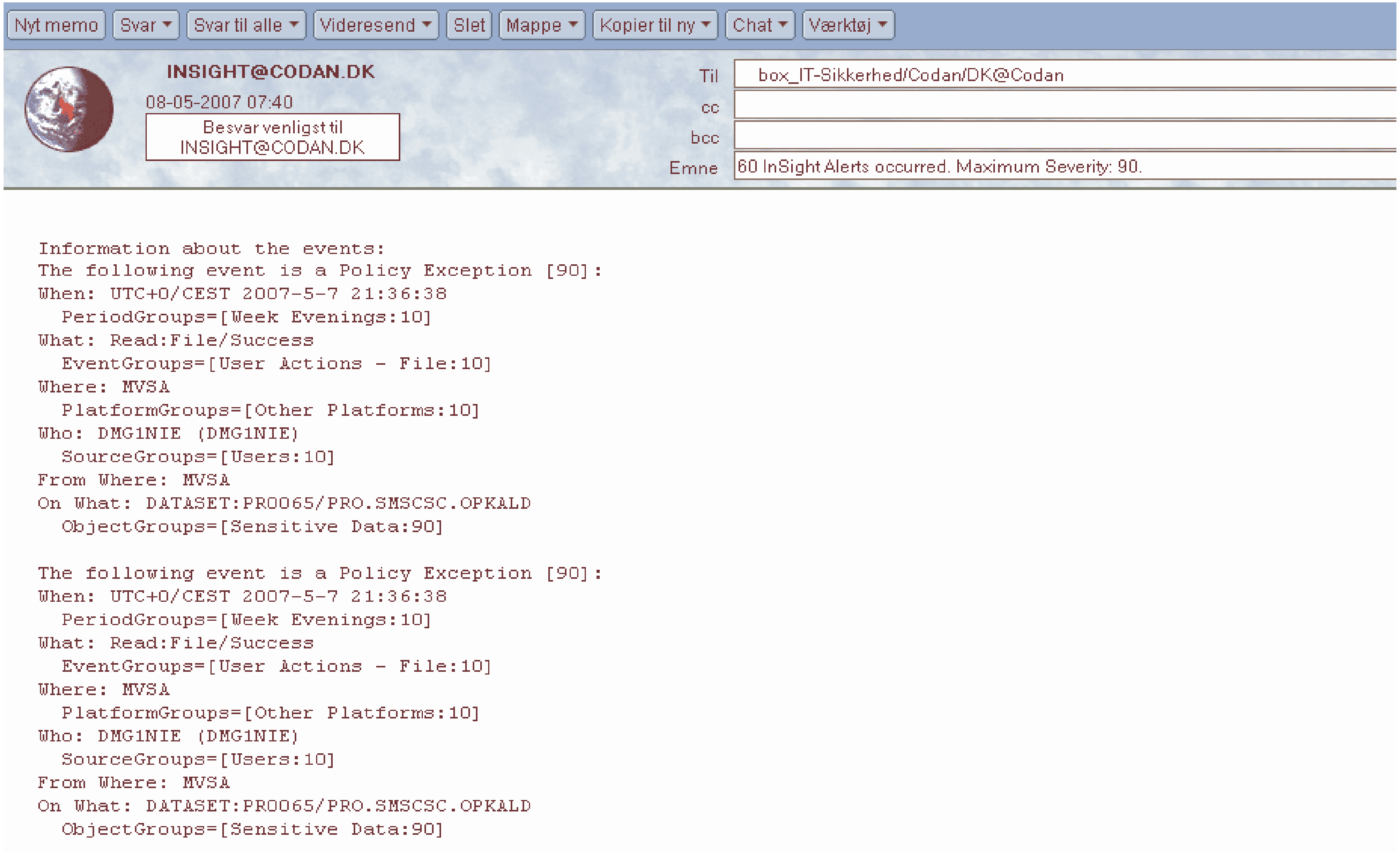
Policy:

- 20. september 2006 18:17:28
  - accessmanager
  - aix
  - BMCControlSA
  - cea
  - domino_5
  - FireWall-1
  - iis
  - iview
  - MSSQL
  - nt
    - K3_groups
    - nt_group
  - oracle
  - os390
  - os400
  - sapr3
  - sp5nt
  - syslog
  - global_group

Policy Rules:

Who	What	When	Where	OnWhat	WhereFrom	WhereTo	Description
System acco							14 SEPTEMBE

Alerts



INSIGHT@CODAN.DK

08-05-2007 07:40

Besvar venligst til INSIGHT@CODAN.DK

Til box_IT-Sikkerhed/Codan/DK@Codan

cc

bcc

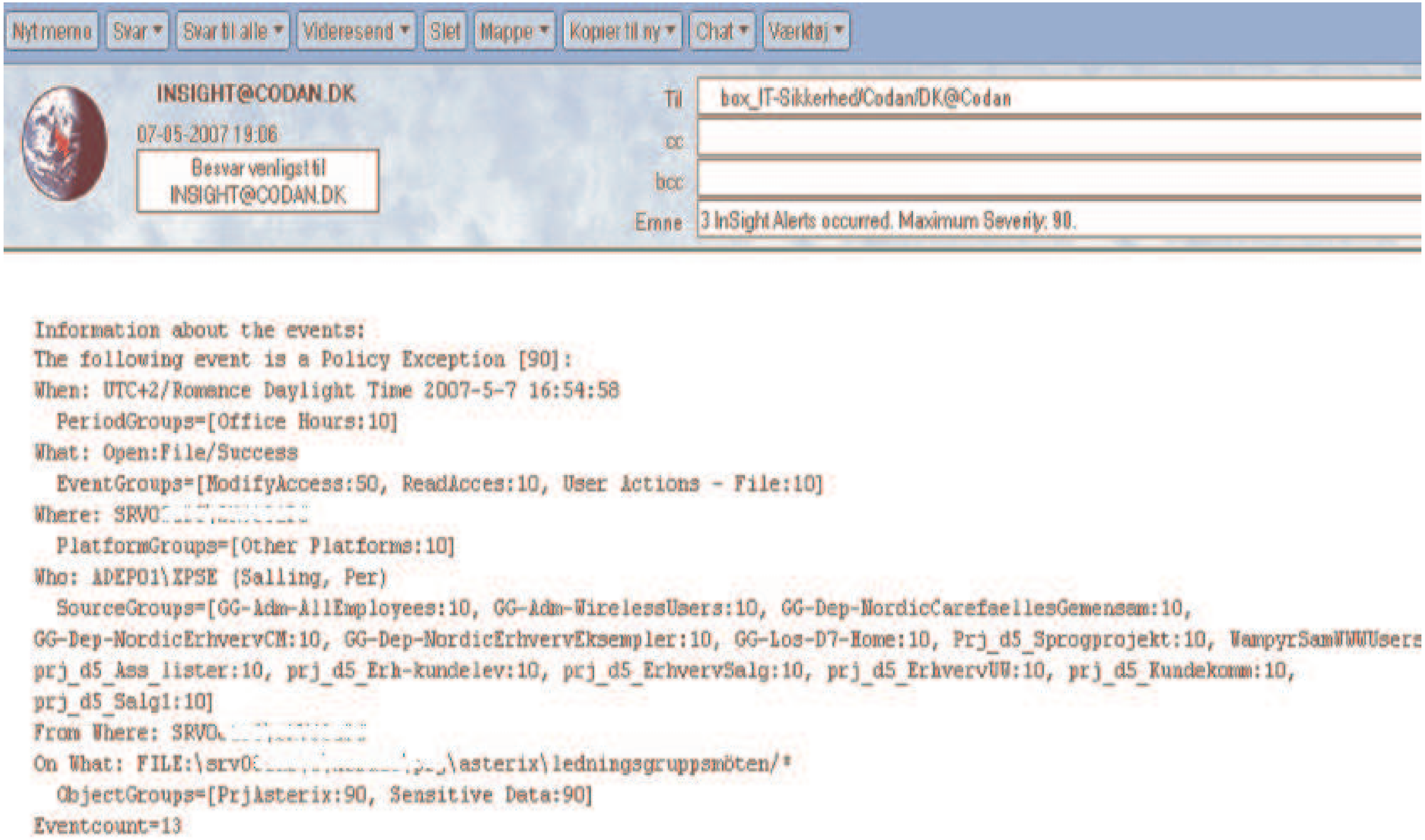
Emne 60 InSight Alerts occurred. Maximum Severity: 90.

```
Information about the events:
The following event is a Policy Exception [90]:
When: UTC+0/CEST 2007-5-7 21:36:38
  PeriodGroups=[Week Evenings:10]
What: Read:File/Success
  EventGroups=[User Actions - File:10]
Where: MVSA
  PlatformGroups=[Other Platforms:10]
Who: DMG1NIE (DMG1NIE)
  SourceGroups=[Users:10]
From Where: MVSA
On What: DATASET:PRO065/PRO.SMSCSC.OPKALD
  ObjectGroups=[Sensitive Data:90]

The following event is a Policy Exception [90]:
When: UTC+0/CEST 2007-5-7 21:36:38
  PeriodGroups=[Week Evenings:10]
What: Read:File/Success
  EventGroups=[User Actions - File:10]
Where: MVSA
  PlatformGroups=[Other Platforms:10]
Who: DMG1NIE (DMG1NIE)
  SourceGroups=[Users:10]
From Where: MVSA
On What: DATASET:PRO065/PRO.SMSCSC.OPKALD
  ObjectGroups=[Sensitive Data:90]
```

Alert

ROYAL & SUNALLIANCE



INSIGHT@CODAN.DK

07-05-2007 19:06

Besvar venligst til INSIGHT@CODAN.DK

Til: box_IT-Sikkerhed/Codan/DK@Codan

cc:

bcc:

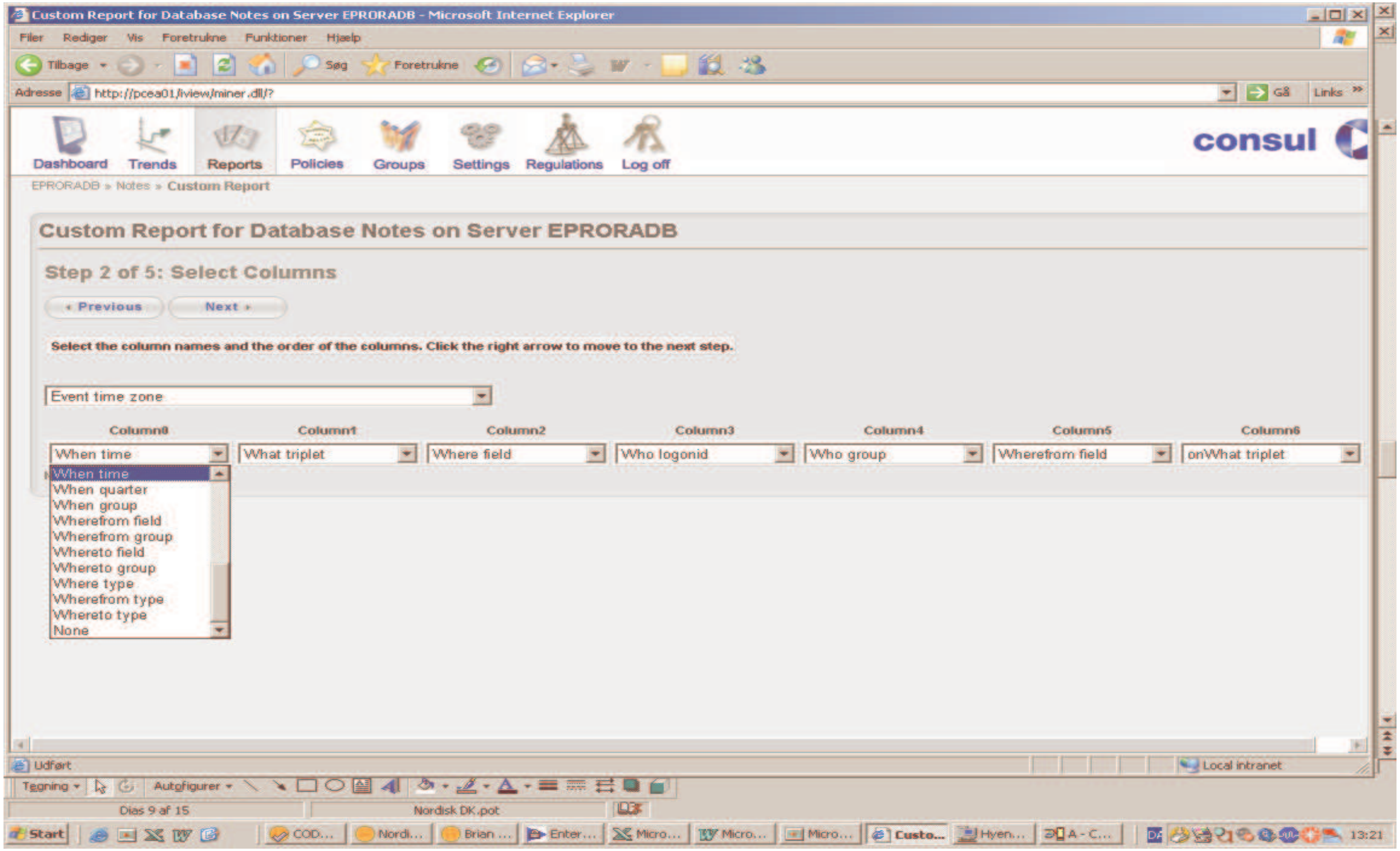
Emne: 3 InSight Alerts occured. Maximum Severity: 90.

```
Information about the events:
The following event is a Policy Exception [90]:
When: UTC+2/Romance Daylight Time 2007-5-7 16:54:58
  PeriodGroups=[Office Hours:10]
What: Open:File/Success
  EventGroups=[ModifyAccess:50, ReadAcces:10, User Actions - File:10]
Where: SRV0[redacted]
  PlatformGroups=[Other Platforms:10]
Who: ADEP01\XPSE (Salling, Per)
  SourceGroups=[GG-Adm-AllEmployees:10, GG-Adm-WirelessUsers:10, GG-Dep-NordicCarefaellesGemensam:10,
GG-Dep-NordicErhvervCM:10, GG-Dep-NordicErhvervEksempler:10, GG-Los-D7-Home:10, Prj_d5_Sprogprojekt:10, WampyrSamWWWUsers
prj_d5_Ass_lister:10, prj_d5_Erh-kundelev:10, prj_d5_ErhvervSalg:10, prj_d5_ErhvervUW:10, prj_d5_Kundekomm:10,
prj_d5_Salg1:10]
From Where: SRV0[redacted]
On What: FILE:\srv0[redacted]\asterix\ledningsgruppsmöten/*
  ObjectGroups=[PrjAsterix:90, Sensitive Data:90]
Eventcount=13
```

Investigation - on request

- What to look for ?
- Is the data online available ?
- Look at the reports - pdf-files.
- Make data available, at the server.
- Run at new load to a free database.
- Use Iview to see data - in details.

How to create new reports in Iview



Custom Report for Database Notes on Server EPRORADB - Microsoft Internet Explorer

Adresse: http://pcea01/iview/miner.dll/?

EPRORADB » Notes » Custom Report

Custom Report for Database Notes on Server EPRORADB

Step 2 of 5: Select Columns

‹ Previous | Next ›

Select the column names and the order of the columns. Click the right arrow to move to the next step.

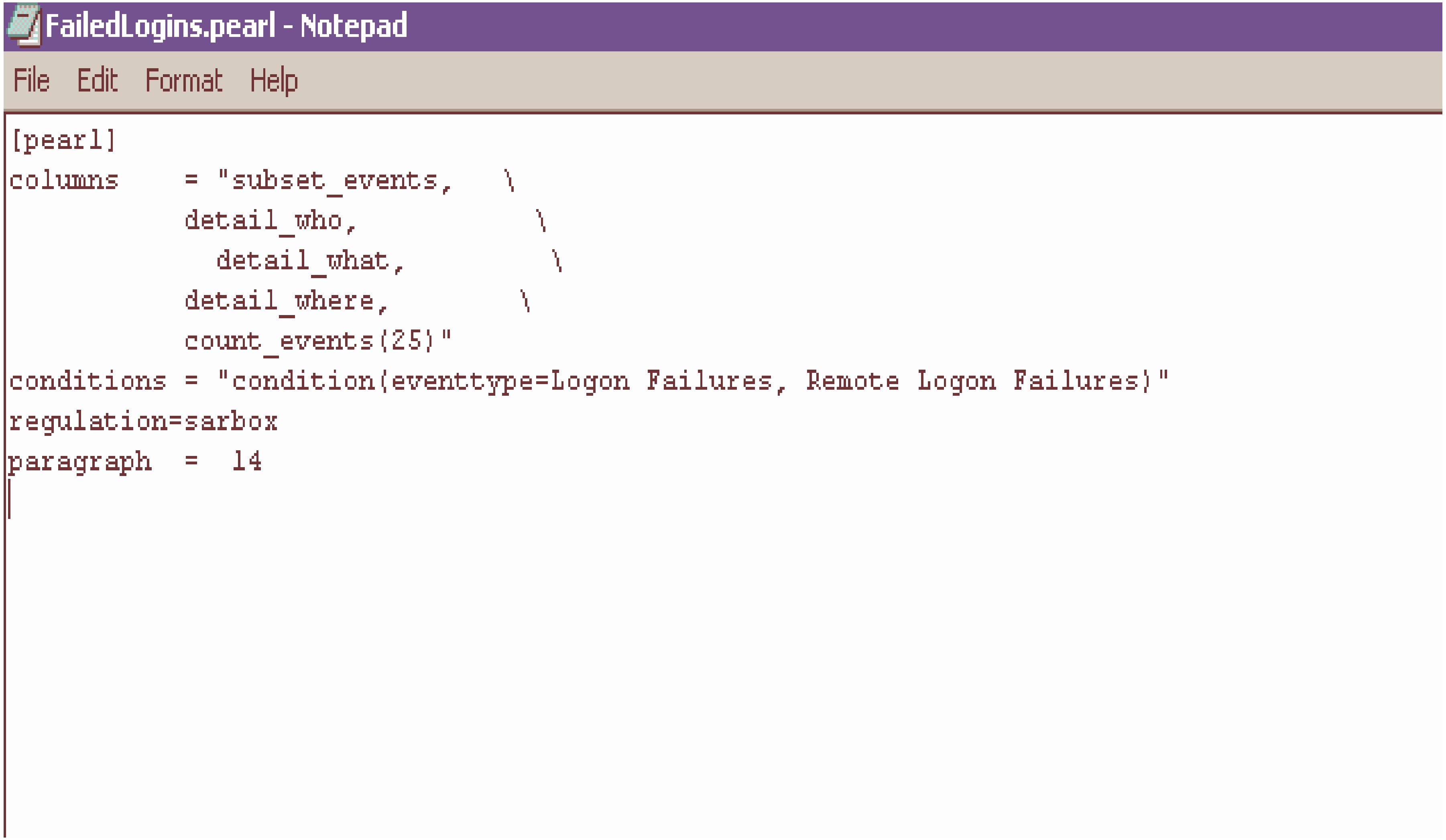
Event time zone

Column0	Column1	Column2	Column3	Column4	Column5	Column6
When time	What triplet	Where field	Who logonid	Who group	Wherefrom field	onWhat triplet

- When time
- When quarter
- When group
- Wherefrom field
- Wherefrom group
- Whereto field
- Whereto group
- Where type
- Wherefrom type
- Whereto type
- None

Udført
Local intranet
Tegning Autofigurer
Dias 9 af 15
Nordisk DK.pot
Start COD... Nordi... Brian ... Enter... Micro... Micro... Micro... Custo... Hyen... A - C...
13:21

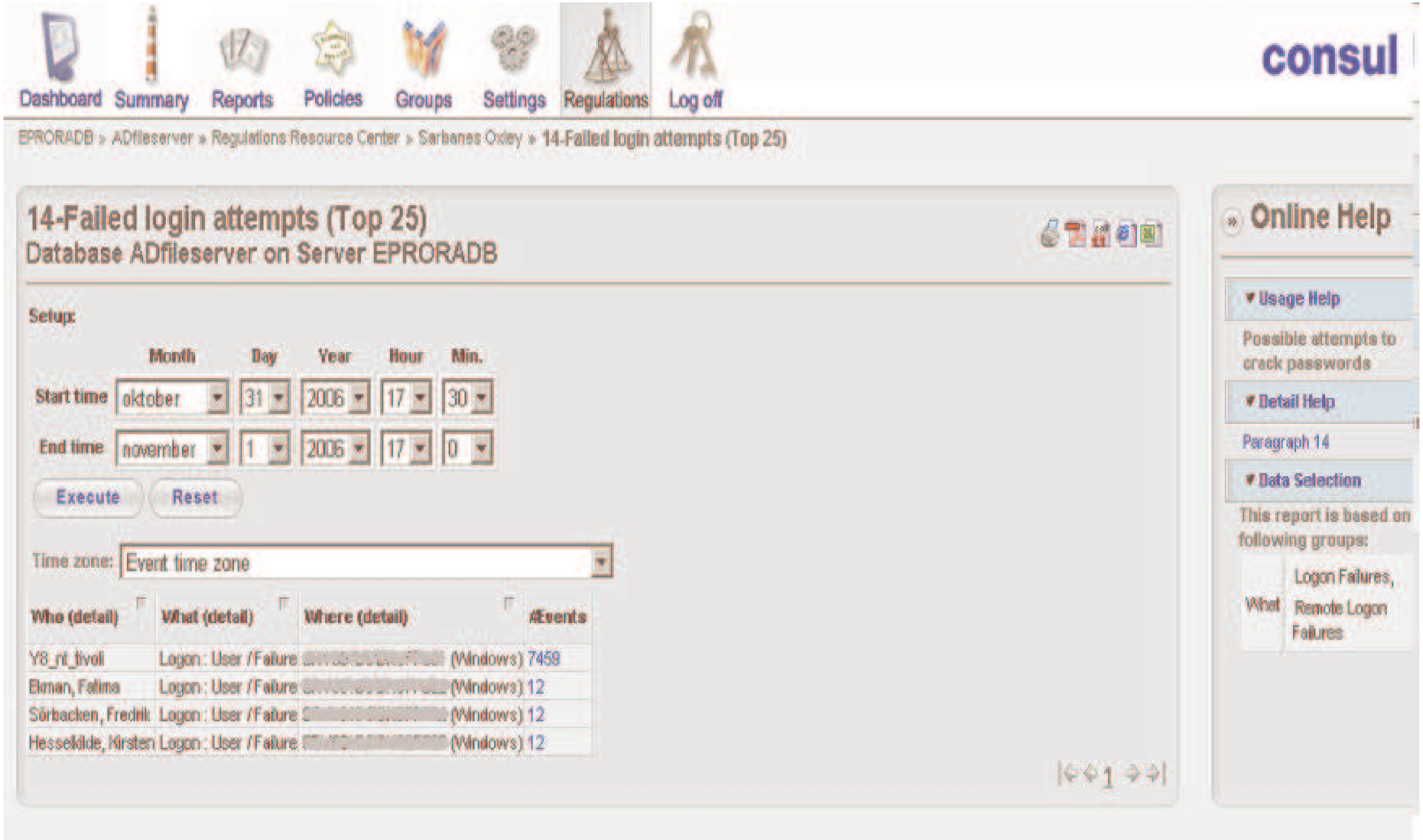
Pearl reports



```
[pearl]
columns    = "subset_events,   \
           detail_who,           \
             detail_what,          \
           detail_where,         \
           count_events(25)"
conditions = "condition(eventtype=Logon Failures, Remote Logon Failures)"
regulation=sarbox
paragraph  =  14
```

Pearl report - in Iview

ROYAL & SUNALLIANCE



EPRORADB » ADfileserver » Regulations Resource Center » Sarbanes Oxley » 14-Failed login attempts (Top 25)

14-Failed login attempts (Top 25)

Database ADfileserver on Server EPRORADB

Setup:

	Month	Day	Year	Hour	Min.
Start time	oktober	31	2006	17	30
End time	november	1	2006	17	0

Time zone: Event time zone

Who (detail)	What (detail)	Where (detail)	#Events
Y8_nt_tivoli	Logon : User / Failure	[redacted] (Windows)	7459
Ekman, Fatima	Logon : User / Failure	[redacted] (Windows)	12
Sörbacken, Fredrik	Logon : User / Failure	[redacted] (Windows)	12
Hesselkilde, Kirsten	Logon : User / Failure	[redacted] (Windows)	12

Online Help

Usage Help

Possible attempts to crack passwords

Detail Help

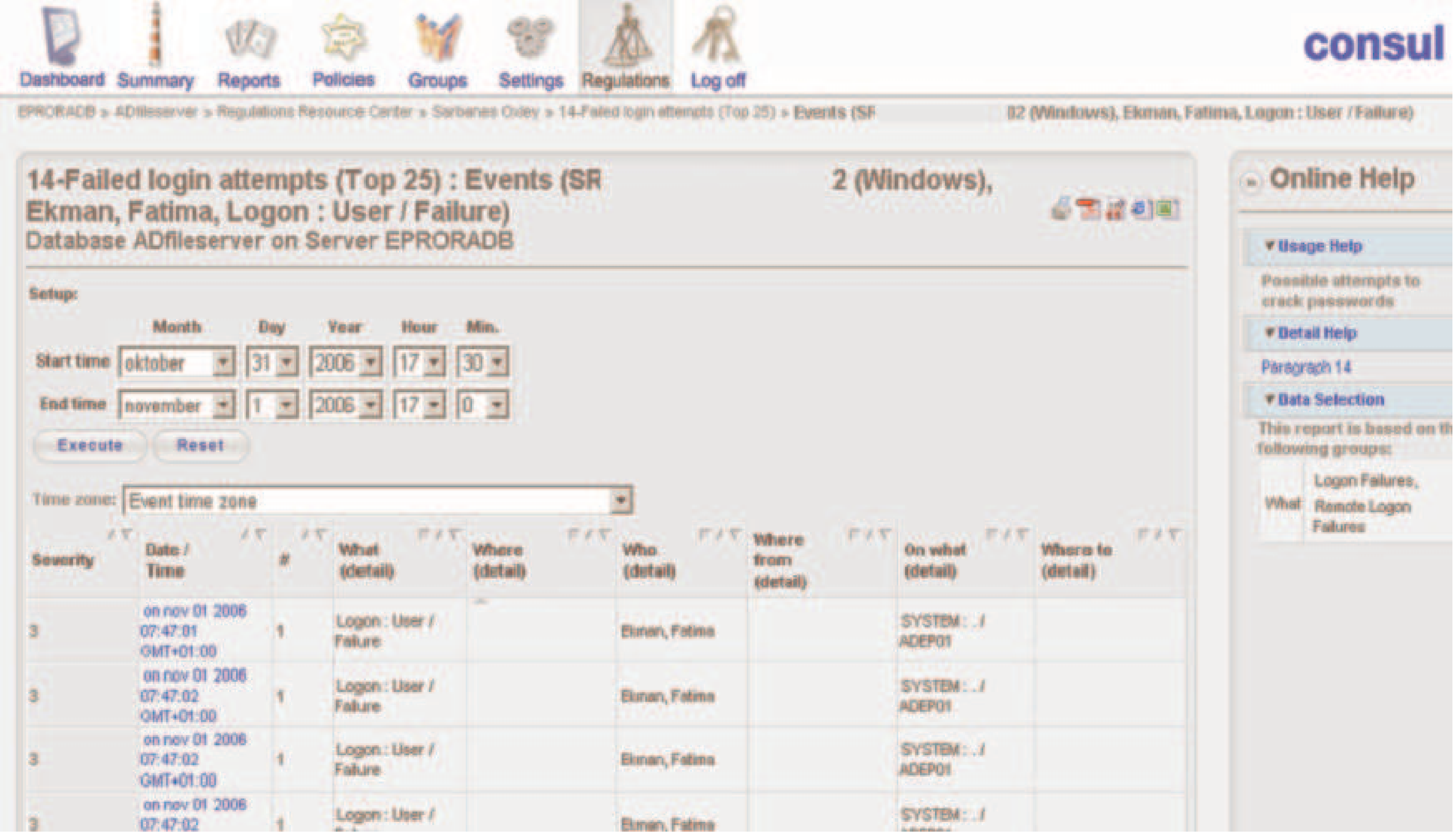
Paragraph 14

Data Selection

This report is based on following groups:

What	Logon Failures, Remote Logon Failures

Investigate - in Iview



EPRORADB » ADfileserver » Regulations Resource Center » Sarbanes Oxley » 14-Failed login attempts (Top 25) » Events (SF 02 (Windows), Ekman, Fatima, Logon : User / Failure)

14-Failed login attempts (Top 25) : Events (SR 2 (Windows), Ekman, Fatima, Logon : User / Failure)

Database ADfileserver on Server EPRORADB

Setup:

	Month	Day	Year	Hour	Min.
Start time	oktober	31	2006	17	30
End time	november	1	2006	17	0

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
3	on nov 01 2006 07:47:01 GMT+01:00	1	Logon : User / Failure		Ekman, Fatima		SYSTEM : ../ ADEP01	
3	on nov 01 2006 07:47:02 GMT+01:00	1	Logon : User / Failure		Ekman, Fatima		SYSTEM : ../ ADEP01	
3	on nov 01 2006 07:47:02 GMT+01:00	1	Logon : User / Failure		Ekman, Fatima		SYSTEM : ../ ADEP01	
3	on nov 01 2006 07:47:02	1	Logon : User /		Ekman, Fatima		SYSTEM : ../	

Online Help

Usage Help

Possible attempts to crack passwords

Detail Help

Paragraph 14

Data Selection

This report is based on th following groups:

What	Logon Failures, Remote Logon Failures

Future

- Get log-data from Balta
- Install new version of Iview