Opasnost od gubitka podataka - upravljanje incidentima

Microsoft IT Pro Community Varaždin, veljača 2018.

Mladen Kuzminski, KONTO d.o.o. Požega, Varaždin

Mladen Kuzminski, mag.inf.

- 20 godina iskustva u projektiranju informacijskih sustava
- Voditelj predstavništva Embarcadero / IDERA za Adriatik - Balkan
- IRCA Lead auditor za ISO 27001
- Autor 10 stručnih knjiga i udžbenika
- https://www.linkedin.com/in/mladen/

KONTO d.o.o. Požega, Varaždin

- Osnovano 1993. Razvoj poslovnih aplikacija.
- ISO 9001, ISO 27001, aAa bonitet
- Distributer Embarcadero / IDERA za Adriatik - Balkan
- www.konto.hr

Gdje se nalaze osobni podaci u našoj organizaciji

i koji su to podaci?

Kako ih štitimo

i kako to dokazujemo?

Baze podataka

- Sadrže većinu današnjih podataka
- Koje su potencijalne slabosti naše baze?
- Tko može pristupiti podacima?
- Da li legalni korisnici koriste slabe i nesigurne lozinke?
- Kako vidjeti koja su pravila ponašanja na serveru?
- Kako uraditi sigurnosni audit baze podataka i dobiti gotov izvještaj koji ima smisla?
- Da li sve to trebamo sami ručno uraditi ili postoje alati koji nam mogu pomoći?

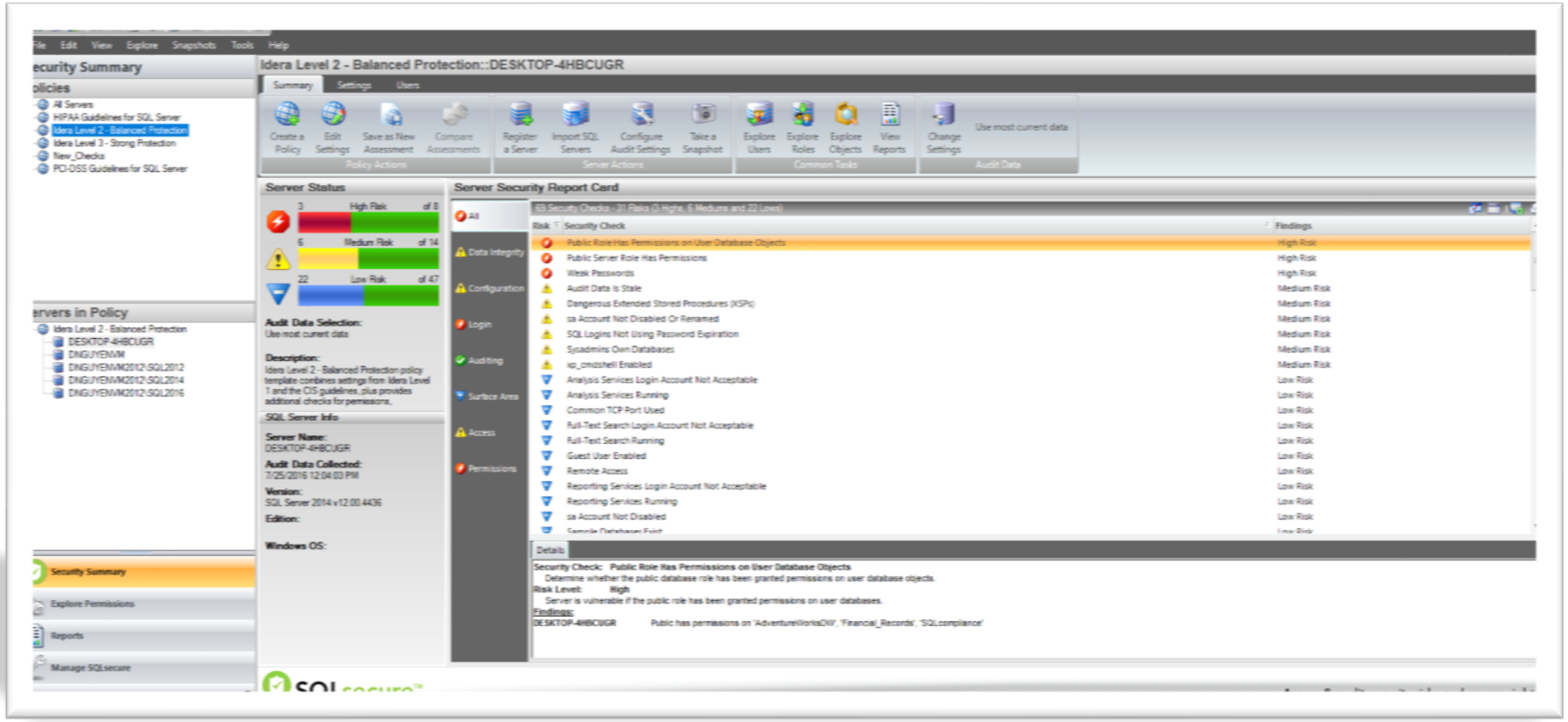
SQL Secure

Audit MS SQL baze podataka

Koje su potencijalne slabosti naše baze?

Security Report Card :

- Usporedba sigurnosnih postavki svih SQL Servera u organizaciji
- Provjera definirane razine sigurnosti 2 za zaštitu od upada.
- Identifikacija najčešćih sigurnosnih ranjivosti.
- Pravila za procjenu rizika omogućuju provjere pristupa bazama podataka, konfiguracijske provjere i provjere dozvola.
- Svaka sigurnosna provjera kategorizirana je: visoki rizik, srednji rizik ili nizak rizik.



Audit Data Selection:
Use most current data

Description:
Idera Level 2 - Balanced Protection policy template combines settings from Idera Level 1 and the CIS guidelines, plus provides additional checks for permissions.

SQL Server Info

Server Name:
DESKTOP-4HBCUGR

Audit Data Collected:
7/25/2016 12:04:03 PM

Version:
SQL Server 2014 v12.00.4436

Edition:

Windows OS:

63 Security Checks - 31 Risks (3 Highs, 6 Mediums and 22 Lows)

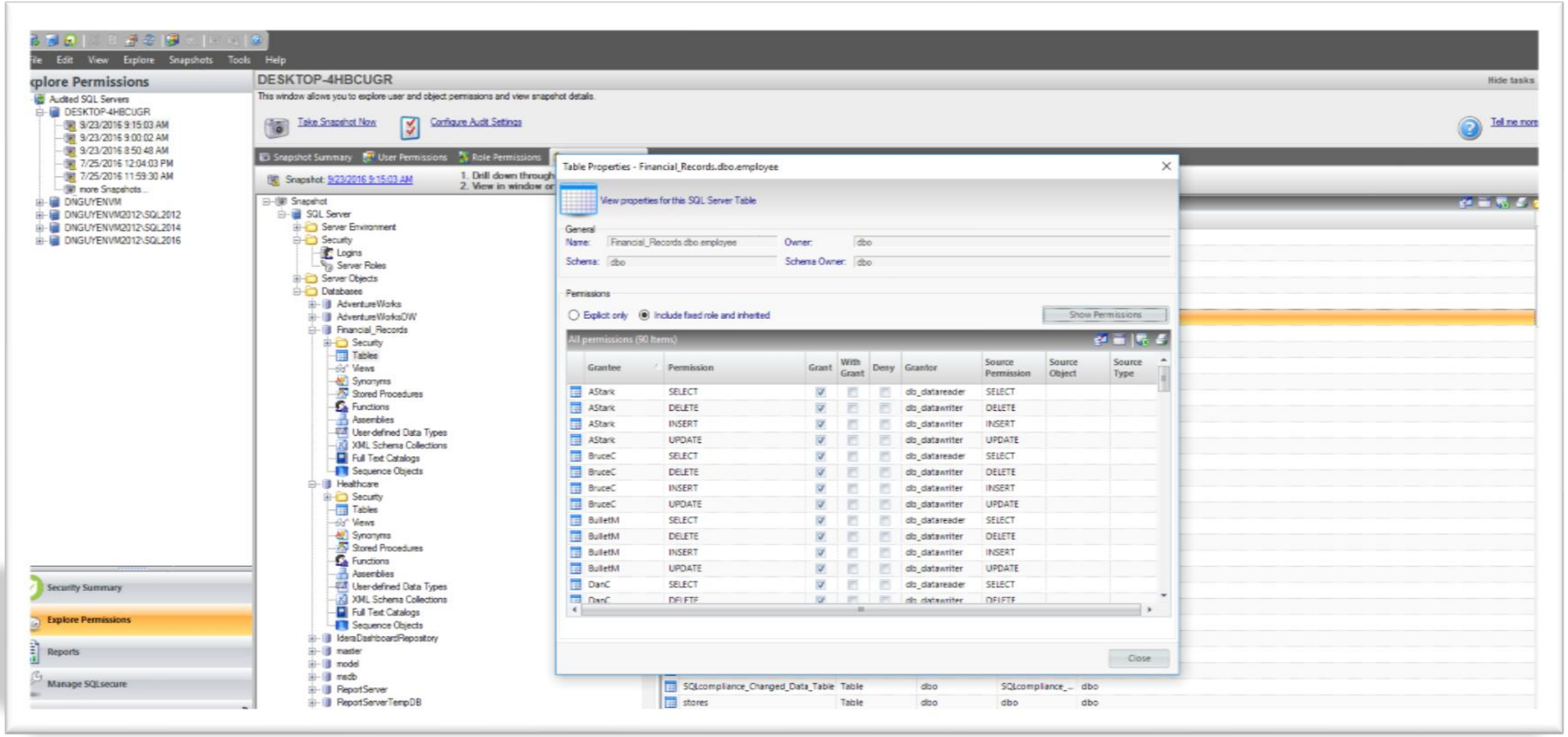
Risk	Security Check	Findings
●	Public Role Has Permissions on User Database Objects	High Risk
●	Public Server Role Has Permissions	High Risk
●	Weak Passwords	High Risk
⚠	Audit Data Is Stale	Medium Risk
⚠	Dangerous Extended Stored Procedures (XSPs)	Medium Risk
⚠	sa Account Not Disabled Or Renamed	Medium Risk
⚠	SQL Logins Not Using Password Expiration	Medium Risk
⚠	Sysadmins Own Databases	Medium Risk
⚠	xp_cmdshell Enabled	Medium Risk
▼	Analysis Services Login Account Not Acceptable	Low Risk
▼	Analysis Services Running	Low Risk
▼	Common TCP Port Used	Low Risk
▼	Full-Text Search Login Account Not Acceptable	Low Risk
▼	Full-Text Search Running	Low Risk
▼	Guest User Enabled	Low Risk
▼	Remote Access	Low Risk
▼	Reporting Services Login Account Not Acceptable	Low Risk
▼	Reporting Services Running	Low Risk
▼	sa Account Not Disabled	Low Risk
▼	Sample Databases Exist	Low Risk

Security Check: **Public Role Has Permissions on User Database Objects**
Determine whether the public database role has been granted permissions on user database objects.
Risk Level: **High**
Server is vulnerable if the public role has been granted permissions on user databases.
Findings:
DESKTOP-4HBCUGR Public has permissions on 'AdventureWorksDW', 'Financial_Records', 'SQLcompliance'

Tko može pristupiti podacima?

SQL Server User Permissions :

- Otkrivanje svih prava pristupa na SQL Server i Azure SQL bazama podataka.
- Pregled i analiza svih SQL Server objekata od razine servera do razine uloga.
- Pregled svih sigurnosnih svojstava i dopuštenja za sve objekte.
- Povijesni pregled audita i usporedba stanja (traženje promjena)



DESKTOP-4HBCUGR

This window allows you to explore user and object permissions and view snapshot details.

Snapshot: 9/23/2016 9:15:03 AM

1. Drill down through
2. View in window or

Table Properties - Financial_Records.dbo.employee

View properties for this SQL Server Table

General

Name: Financial_Records.dbo.employee Owner: dbo

Schema: dbo Schema Owner: dbo

Permissions

○ Explicit only ● Include fixed role and inherited

All permissions (90 items)

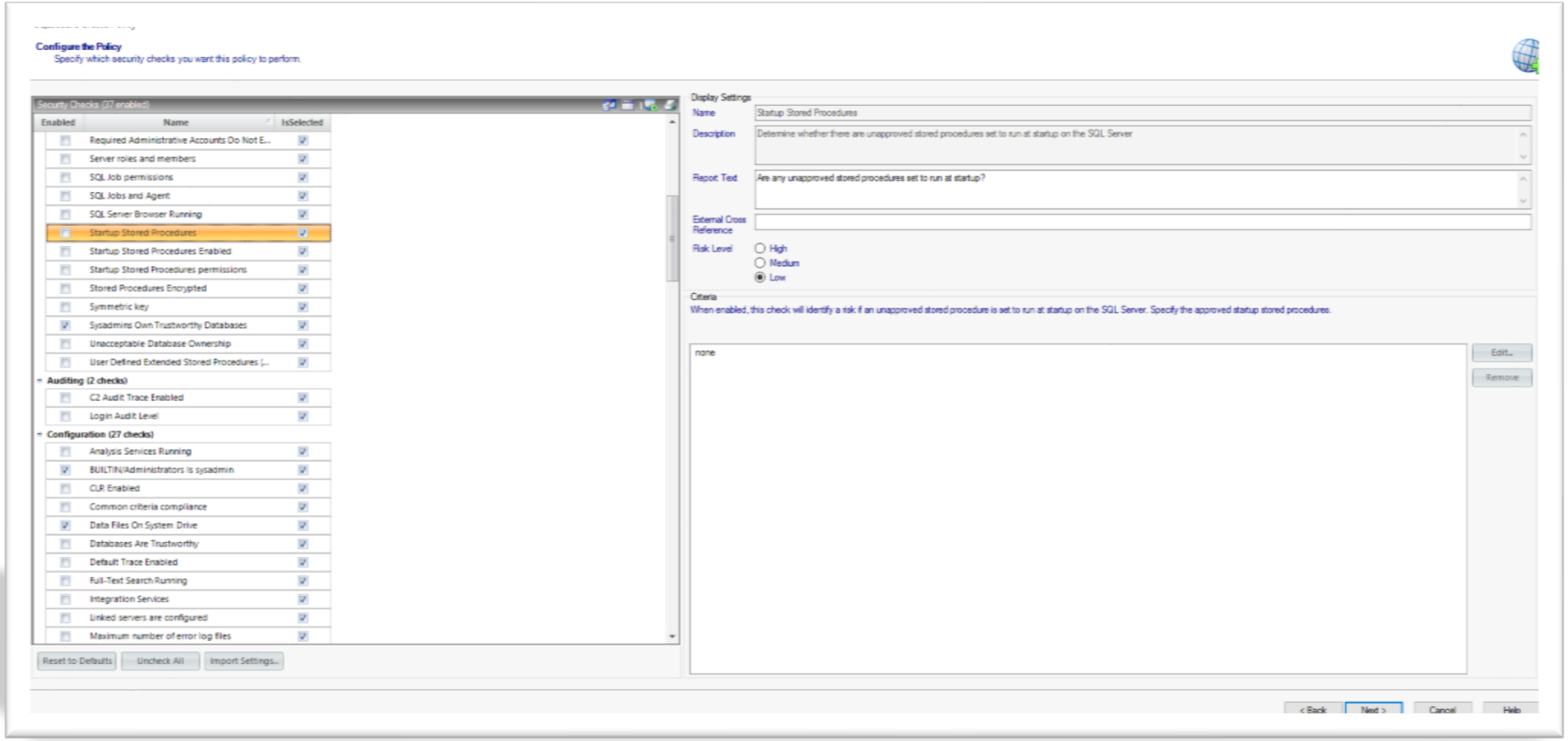
Grantee	Permission	Grant	With Grant	Deny	Grantor	Source Permission	Source Object	Source Type
AStark	SELECT	☑	□	□	db_datareader	SELECT		
AStark	DELETE	☑	□	□	db_datawriter	DELETE		
AStark	INSERT	☑	□	□	db_datawriter	INSERT		
AStark	UPDATE	☑	□	□	db_datawriter	UPDATE		
BruceC	SELECT	☑	□	□	db_datareader	SELECT		
BruceC	DELETE	☑	□	□	db_datawriter	DELETE		
BruceC	INSERT	☑	□	□	db_datawriter	INSERT		
BruceC	UPDATE	☑	□	□	db_datawriter	UPDATE		
BulletM	SELECT	☑	□	□	db_datareader	SELECT		
BulletM	DELETE	☑	□	□	db_datawriter	DELETE		
BulletM	INSERT	☑	□	□	db_datawriter	INSERT		
BulletM	UPDATE	☑	□	□	db_datawriter	UPDATE		
DanC	SELECT	☑	□	□	db_datareader	SELECT		
DanC	DELETE	☑	□	□	db_datawriter	DELETE		

SQLcompliance_Changed_Data_Table	Table	dbo	SQLcompliance_...	dbo
stores	Table	dbo	dbo	dbo

Kako vidjeti koja su pravila ponašanja na serveru?

SQL Server Policies :

- 80+ provjera ponašanja kroz 7 kategorija
- Import predložaka pravila ponašanja na temelju preporuka autoriteta kao što su DISA SRR, CIS i SNAC, kao i IDERA definirane kategorije zaštite: Osnovna, Balansirana i Jaka.



Configure the Policy
Specify which security checks you want this policy to perform.

Security Checks (37 enabled)

Enabled	Name	IsSelected
□	Required Administrative Accounts Do Not E...	☑
□	Server roles and members	☑
□	SQL Job permissions	☑
□	SQL Jobs and Agent	☑
□	SQL Server Browser Running	☑
□	Startup Stored Procedures	☑
□	Startup Stored Procedures Enabled	☑
□	Startup Stored Procedures permissions	☑
□	Stored Procedures Encrypted	☑
□	Symmetric key	☑
☑	Sysadmins Own Trustworthy Databases	☑
□	Unacceptable Database Ownership	☑
□	User Defined Extended Stored Procedures (...	☑
- Auditing (2 checks)		
□	C2 Audit Trace Enabled	☑
□	Login Audit Level	☑
- Configuration (27 checks)		
□	Analysis Services Running	☑
☑	BUILTIN/Administrators Is sysadmin	☑
□	CLR Enabled	☑
□	Common criteria compliance	☑
☑	Data Files On System Drive	☑
□	Databases Are Trustworthy	☑
□	Default Trace Enabled	☑
□	Full-Text Search Running	☑
□	Integration Services	☑
□	Linked servers are configured	☑
□	Maximum number of error log files	☑

Display Settings

Name: Startup Stored Procedures

Description: Determine whether there are unapproved stored procedures set to run at startup on the SQL Server

Report Text: Are any unapproved stored procedures set to run at startup?

External Cross Reference:

Risk Level: ○ High ○ Medium ● Low

Criteria

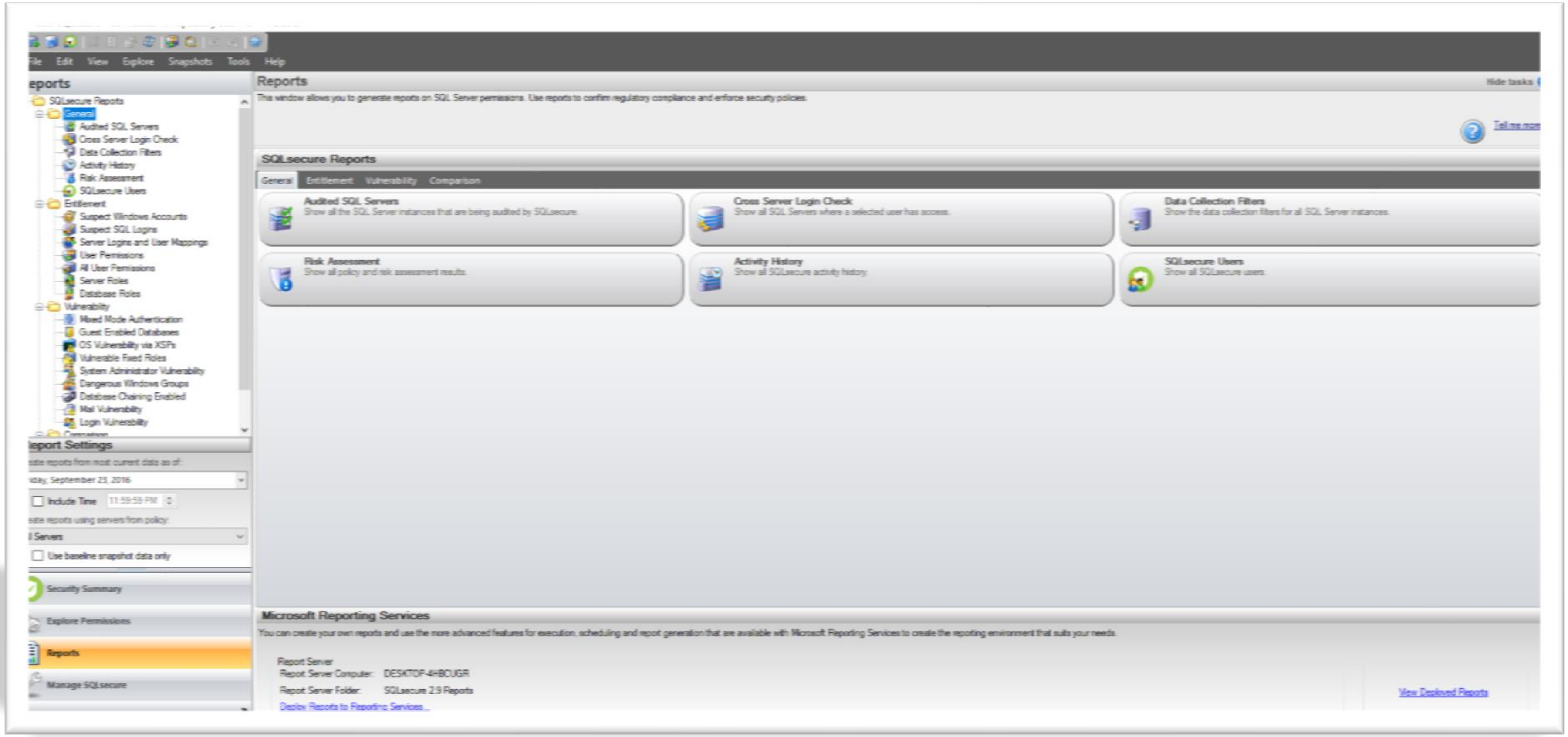
When enabled, this check will identify a risk if an unapproved stored procedure is set to run at startup on the SQL Server. Specify the approved startup stored procedures.

none

Kako uraditi sigurnosni audit baze podataka i dobiti gotov izvještaj koji ima smisla?

SQL Secure Reporting:

- Brzi i pregledni izvještaji. Prijave na više servera, svi serveri na koje je pristupio određeni korisnik, slabosti servera, prava pristupa, uloge na bazama podataka i dr.
- Vremenska usporedba izvještaja i usporedba s predefiniranim modelom.



Reports

This window allows you to generate reports on SQL Server permissions. Use reports to confirm regulatory compliance and enforce security policies.

SQLsecure Reports

Audited SQL Servers
Show all the SQL Server instances that are being audited by SQLsecure.

Cross Server Login Check
Show all SQL Servers where a selected user has access.

Data Collection Filters
Show the data collection filters for all SQL Server instances.

Risk Assessment
Show all policy and risk assessment results.

Activity History
Show all SQLsecure activity history.

SQLsecure Users
Show all SQLsecure users.

eport Settings

ate reports from most current data as of:
iday, September 23, 2016
□ Include Time 11:59:59 PM
ate reports using servers from policy:
l Servers
□ Use baseline snapshot data only

Microsoft Reporting Services

You can create your own reports and use the more advanced features for execution, scheduling and report generation that are available with Microsoft Reporting Services to create the reporting environment that suits your needs.

Report Server
Report Server Computer: DESKTOP-4HBCUGR
Report Server Folder: SQLsecure 2.9 Reports

Data Protection by Design and Default

GDPR Article 25

Security of Processing

GDPR Article 32

Data Protection Impact Assessment

GDPR Article 35

Što ako dođe do neovlaštenog pristupa i/ili gubitka podataka?

- Tko je radio s podacima i kojim točno podacima?
- Da li postoji dnevnik aktivnosti za forenzičku analizu incidenta?
- Da li postoji mogućnost 24/7 praćenja svih aktivnosti nad bazama podataka?

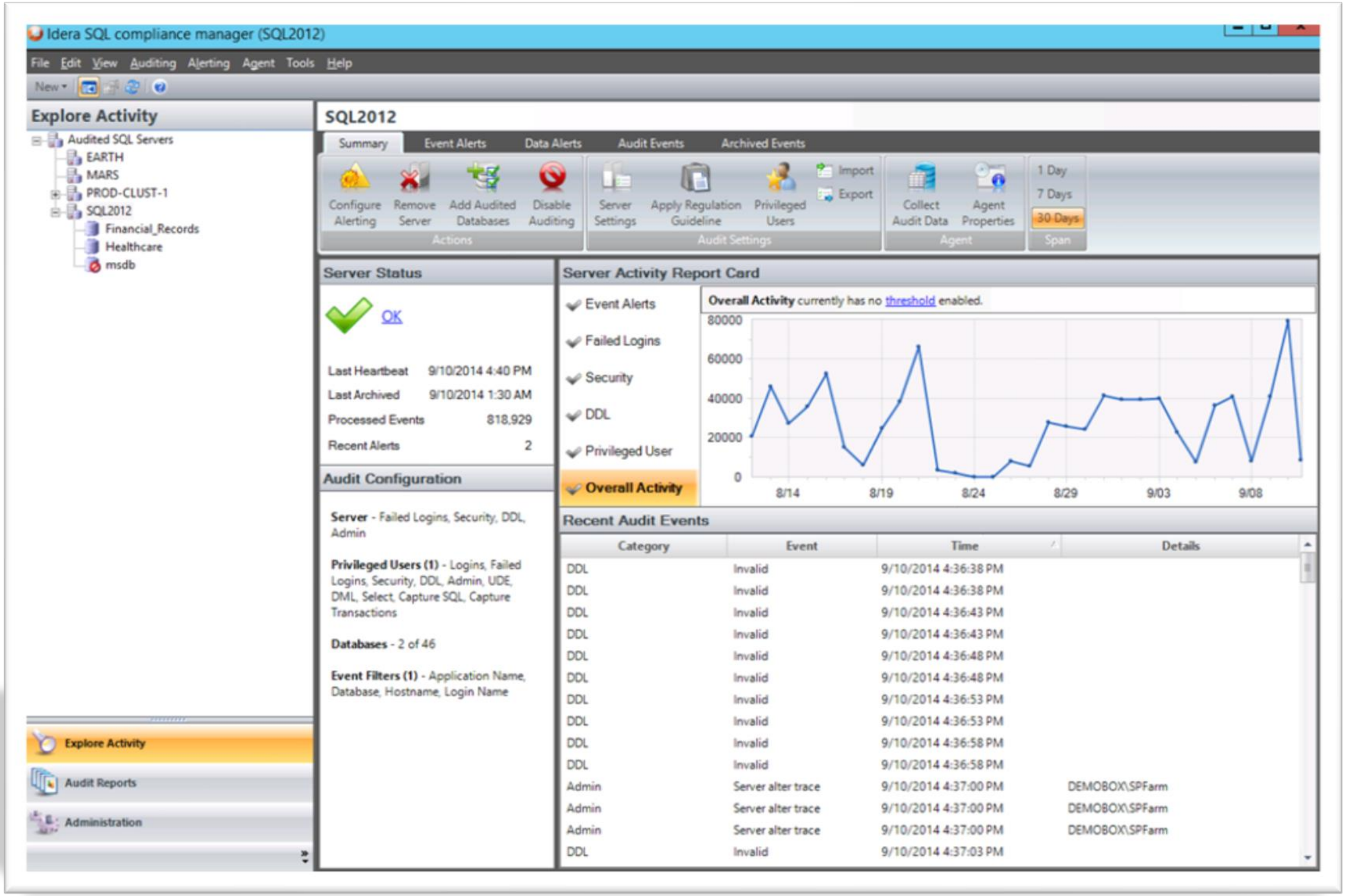
SQL Compliance Manager

Praćenje aktivnosti nad MS SQL bazom podataka sa sigurnosnog aspekta

Tko je radio s podacima i kojim točno podacima?

Audit SQL Server-a :

- Centralizirani audit svih SQL Server-a I baza podataka
- Praćenje svih aktivnosti korisnika I upozoravanje na promjene podataka u stvarnom vremenu
- Definiranje alarma za pristup osjetljivim podacima
- Praćenje trendova aktivnosti korisnika



Server Status

OK

Last Heartbeat 9/10/2014 4:40 PM
Last Archived 9/10/2014 1:30 AM
Processed Events 818,929
Recent Alerts 2

Audit Configuration

Server - Failed Logins, Security, DDL, Admin

Privileged Users (1) - Logins, Failed Logins, Security, DDL, Admin, UDE, DML, Select, Capture SQL, Capture Transactions

Databases - 2 of 46

Event Filters (1) - Application Name, Database, Hostname, Login Name

Overall Activity currently has no threshold enabled.

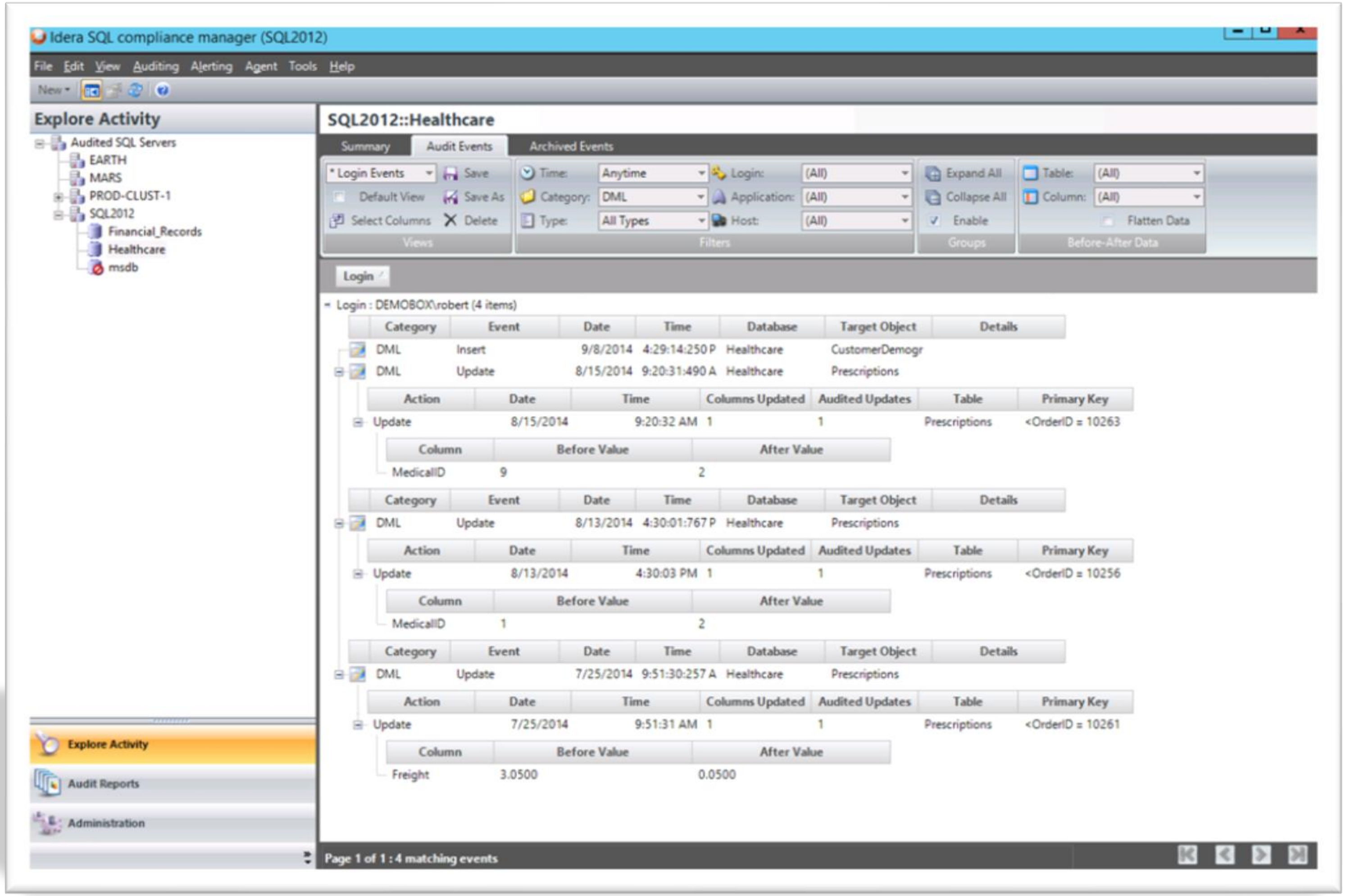
Recent Audit Events

Category	Event	Time	Details
DDL	Invalid	9/10/2014 4:36:38 PM	
DDL	Invalid	9/10/2014 4:36:38 PM	
DDL	Invalid	9/10/2014 4:36:43 PM	
DDL	Invalid	9/10/2014 4:36:43 PM	
DDL	Invalid	9/10/2014 4:36:48 PM	
DDL	Invalid	9/10/2014 4:36:48 PM	
DDL	Invalid	9/10/2014 4:36:53 PM	
DDL	Invalid	9/10/2014 4:36:53 PM	
DDL	Invalid	9/10/2014 4:36:58 PM	
DDL	Invalid	9/10/2014 4:36:58 PM	
Admin	Server alter trace	9/10/2014 4:37:00 PM	DEMOBOX\SPFarm
Admin	Server alter trace	9/10/2014 4:37:00 PM	DEMOBOX\SPFarm
Admin	Server alter trace	9/10/2014 4:37:00 PM	DEMOBOX\SPFarm
DDL	Invalid	9/10/2014 4:37:03 PM	

Dnevnik aktivnosti za forenzičku analizu incidenta

Bilježenje aktivnosti:

- Bilježenje svih aktivnosti korisnika
- Analiza promjena podataka
- Pregled DML-a koji je promijenio podatke, pregled vrijednosti prije i poslije promjene
- Posebna pažnja posvećena pristupu osjetljivim podacima



Login Events

Time: Anytime

Category: DML

Type: All Types

Login: (All)

Application: (All)

Host: (All)

Table: (All)

Column: (All)

Login : DEMOBOX\robert (4 items)

Category	Event	Date	Time	Database	Target Object	Details
DML	Insert	9/8/2014	4:29:14:250 P	Healthcare	CustomerDemogr	
DML	Update	8/15/2014	9:20:31:490 A	Healthcare	Prescriptions	

Action	Date	Time	Columns Updated	Audited Updates	Table	Primary Key
Update	8/15/2014	9:20:32 AM	1	1	Prescriptions	<OrderID = 10263

Column	Before Value	After Value
MedicalID	9	2

Category	Event	Date	Time	Database	Target Object	Details
DML	Update	8/13/2014	4:30:01:767 P	Healthcare	Prescriptions	

Action	Date	Time	Columns Updated	Audited Updates	Table	Primary Key
Update	8/13/2014	4:30:03 PM	1	1	Prescriptions	<OrderID = 10256

Column	Before Value	After Value
MedicalID	1	2

Category	Event	Date	Time	Database	Target Object	Details
DML	Update	7/25/2014	9:51:30:257 A	Healthcare	Prescriptions	

Action	Date	Time	Columns Updated	Audited Updates	Table	Primary Key
Update	7/25/2014	9:51:31 AM	1	1	Prescriptions	<OrderID = 10261

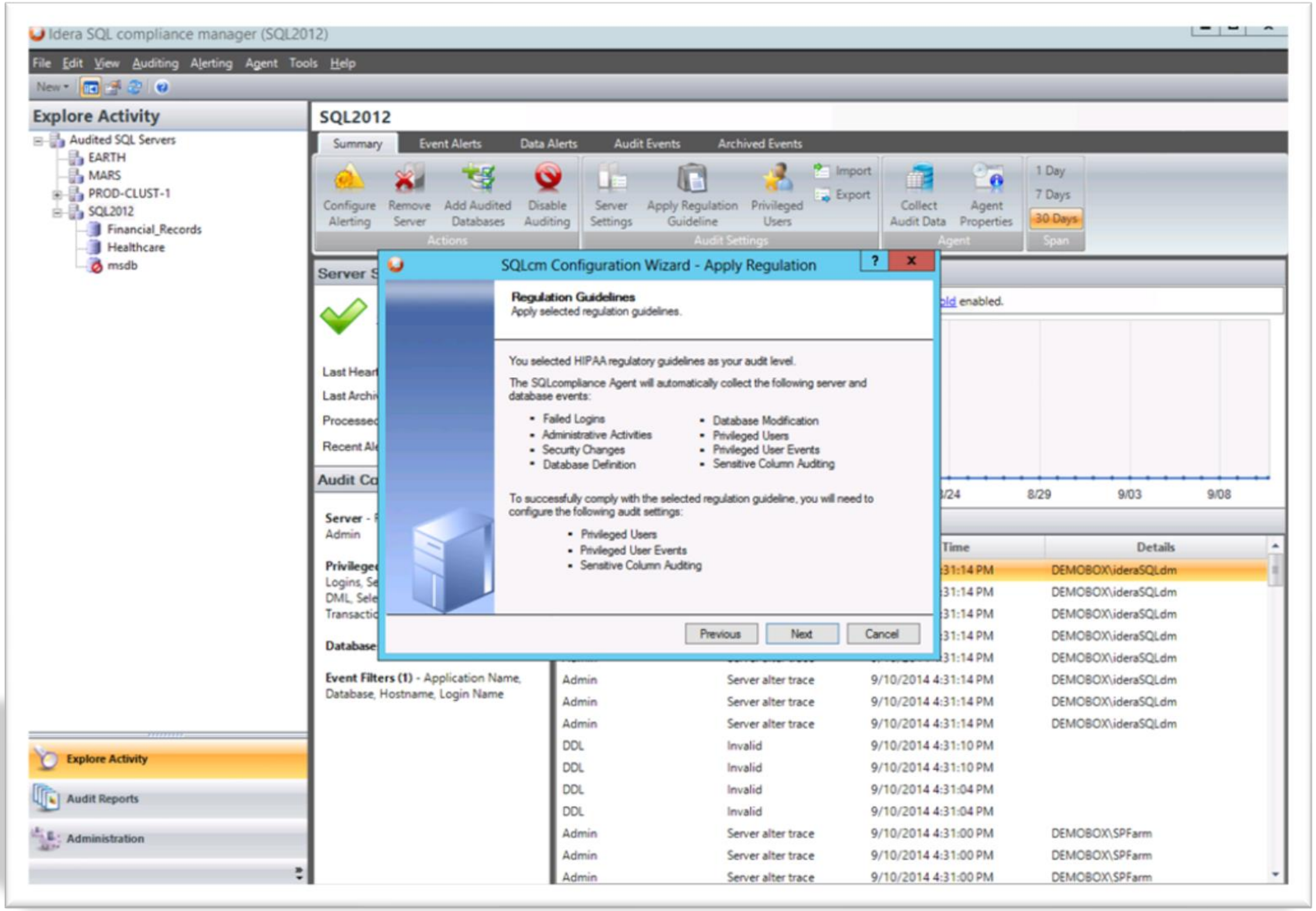
Column	Before Value	After Value
Freight	3.0500	0.0500

Page 1 of 1 : 4 matching events

Regulatorni izvještaji

Predlošci standardnih izvještaja:

- Automatsko stvaranje izvještaja koji udovoljavaju zahtjevima HIPAA, HITECH and PCI DSS I dr. regulative
- 25 gotovih predložaka audita uz stalno proširenje



SQLcm Configuration Wizard - Apply Regulation

Regulation Guidelines
Apply selected regulation guidelines.

You selected HIPAA regulatory guidelines as your audit level.

The SQLcompliance Agent will automatically collect the following server and database events:

- Failed Logins
- Administrative Activities
- Security Changes
- Database Definition
- Database Modification
- Privileged Users
- Privileged User Events
- Sensitive Column Auditing

To successfully comply with the selected regulation guideline, you will need to configure the following audit settings:

- Privileged Users
- Privileged User Events
- Sensitive Column Auditing

Previous | Next | Cancel

		Time	Details
		:31:14 PM	DEMOBOX\ideraSQLdm
		:31:14 PM	DEMOBOX\ideraSQLdm
		:31:14 PM	DEMOBOX\ideraSQLdm
		:31:14 PM	DEMOBOX\ideraSQLdm
		:31:14 PM	DEMOBOX\ideraSQLdm
Admin	Server alter trace	9/10/2014 4:31:14 PM	DEMOBOX\ideraSQLdm
Admin	Server alter trace	9/10/2014 4:31:14 PM	DEMOBOX\ideraSQLdm
Admin	Server alter trace	9/10/2014 4:31:14 PM	DEMOBOX\ideraSQLdm
DDL	Invalid	9/10/2014 4:31:10 PM	
DDL	Invalid	9/10/2014 4:31:10 PM	
DDL	Invalid	9/10/2014 4:31:04 PM	
DDL	Invalid	9/10/2014 4:31:04 PM	
Admin	Server alter trace	9/10/2014 4:31:00 PM	DEMOBOX\SPFarm
Admin	Server alter trace	9/10/2014 4:31:00 PM	DEMOBOX\SPFarm
Admin	Server alter trace	9/10/2014 4:31:00 PM	DEMOBOX\SPFarm

Notification of Personal Data Breach to the Supervisory Authority

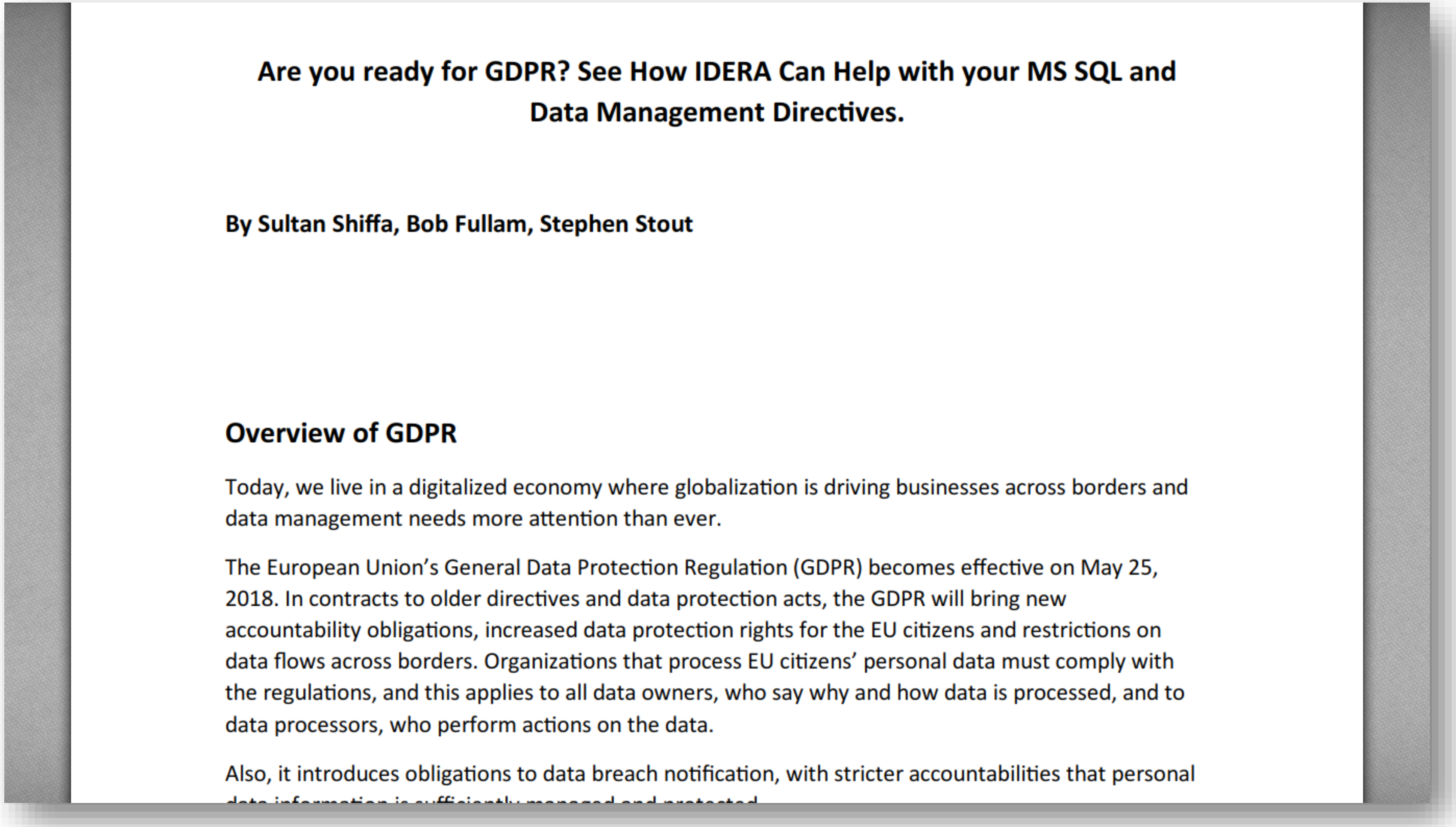
GDPR Article 33

Records of Processing Activities

GDPR Article 30

Data Protection Impact Assessment

GDPR Article 35



Are you ready for GDPR? See How IDERA Can Help with your MS SQL and Data Management Directives.

By Sultan Shiffa, Bob Fullam, Stephen Stout

Overview of GDPR

Today, we live in a digitalized economy where globalization is driving businesses across borders and data management needs more attention than ever.

The European Union's General Data Protection Regulation (GDPR) becomes effective on May 25, 2018. In contracts to older directives and data protection acts, the GDPR will bring new accountability obligations, increased data protection rights for the EU citizens and restrictions on data flows across borders. Organizations that process EU citizens' personal data must comply with the regulations, and this applies to all data owners, who say why and how data is processed, and to data processors, who perform actions on the data.

Also, it introduces obligations to data breach notification, with stricter accountabilities that personal data information is sufficiently managed and protected.

Are you ready for GDPR? See How IDERA Can Help with your MS SQL and Data Management Directives.

- Stručni dokument koji objašnjava kako razumjeti i dokumentirati kretanje I upravljanje podacima u organizaciji.
- Daje preporuke za provjeru usklađenosti s GDPR regulativom.
- Dostupan na zahtjev slanjem maila na mladen@konto.hr

SQL Secure

Dostupan na www.idera.com   Prvih 14 dana besplatna upotreba.

SQL Compliance Manager

Dostupan na www.idera.com   Prvih 14 dana besplatna upotreba.

IDERA alati za upravljanje bazama podataka

Bogat portfelj alata za nadgledanje, praćenje, optimizaciju i sigurnost MS SQL, Oracle i ostalih vodećih servera

Performanse i nadgledanje	**Sigurnost i usklađenost**	**Backup i administracija**
SQL Diagnostic Manager SQL BI Manager SQL Defrag Manager SQL Inventory Manager SQL Doctor DB Optimizer	SQL Compliance Manager SQL Secure	SQL Safe Backup SQL Enterprise Job Manager SQL Virtual Database SQL Admin Toolset SQL Toolbox SQL Comparison Toolset DB Artisan
Osiguravaju raspoloživost i performanse servera i aplikacija	***Aktivnosti audita i usklađenja s regulativama***	***Čuvanje kritičnih podataka i automatizacija procesa***

www.idera.com
idera@konto.hr