

Opasnost od gubitka podataka - upravljanje incidentima

Privatnost 2017

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?



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.

The screenshot displays the 'Server Security Report Card' for a SQL Server instance named 'DESKTOP-4HBCUGR'. The interface is divided into several sections:

- Summary:** Shows the overall security status with a 'High Risk' indicator (red circle with '2').
- Server Status:** A bar chart showing risk levels: 2 High Risk, 6 Medium Risk, and 22 Low Risk.
- Server Security Report Card:** A list of security checks. The top finding is 'Public Role Has Permissions on User Database Objects', which is highlighted in orange and marked as 'High Risk'. Other findings include 'Public Server Role Has Permissions' (High Risk), 'Weak Passwords' (High Risk), and 'Audit Data is Stale' (Medium Risk).
- SQL Server Info:** Provides details about the server, including the name 'DESKTOP-4HBCUGR', the version 'SQL Server 2014 v12.00.4436', and the edition.

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)

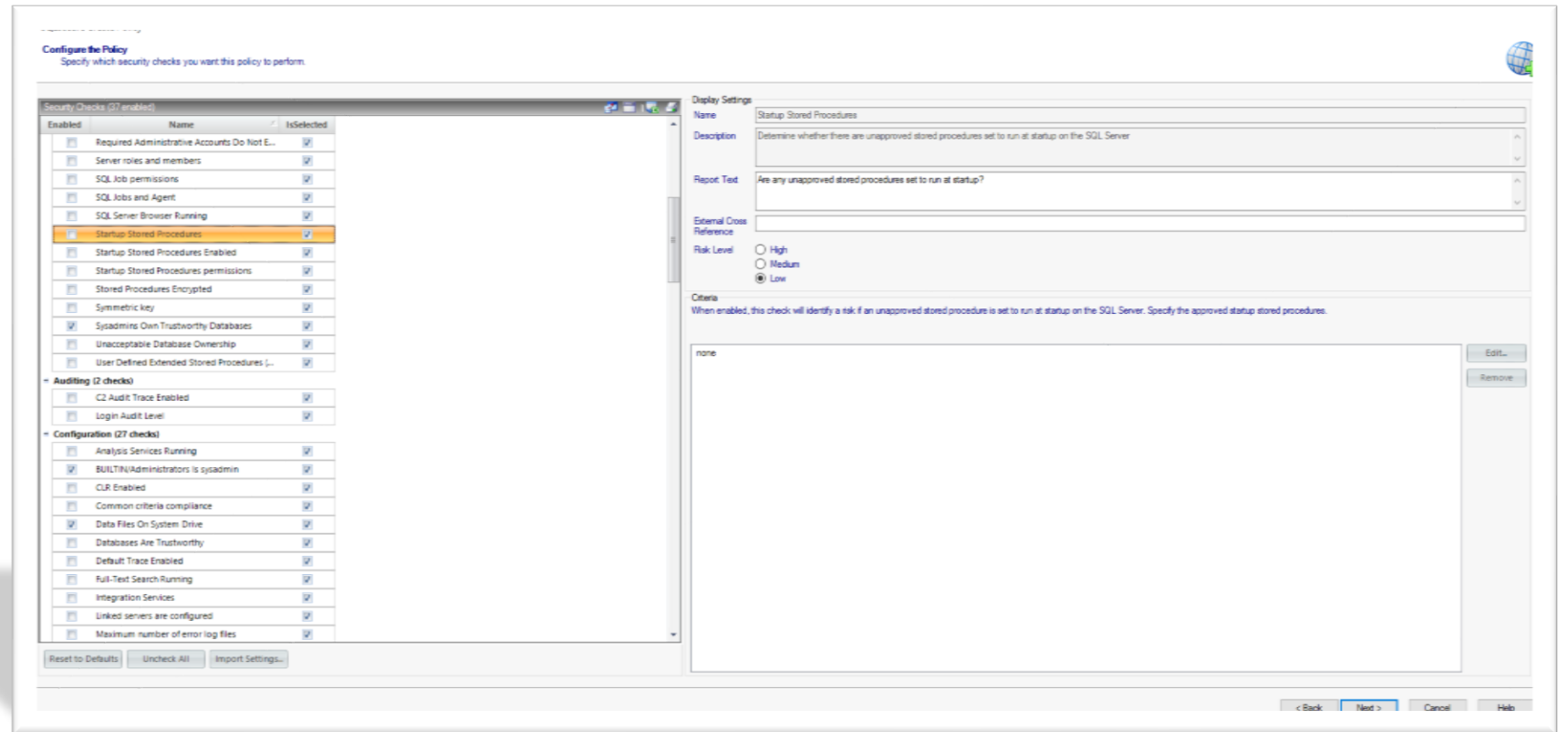
The screenshot displays the SQL Server Enterprise Manager interface. The left pane shows the 'Explore Permissions' tree view, highlighting the 'Financial_Records' database. The main pane shows the 'Table Properties - Financial_Records.dbo.employee' dialog box, which is open to the 'Permissions' tab. This tab shows a list of permissions granted to various users, including 'AStarK', 'BruceC', 'BulletM', and 'DanC'. The permissions include SELECT, DELETE, INSERT, and UPDATE. The 'Grant' column is checked for all listed users, and the 'Deny' column is unchecked. The 'Source Permission' column shows the source of the permissions, such as 'db_datareader' and 'db_datawriter'.

Grantee	Permission	Grant	With Grant	Deny	Grantor	Source Permission	Source Object	Source Type
AStarK	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
AStarK	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		
AStarK	INSERT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	INSERT		
AStarK	UPDATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	UPDATE		
BruceC	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
BruceC	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		
BruceC	INSERT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	INSERT		
BruceC	UPDATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	UPDATE		
BulletM	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
BulletM	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		
BulletM	INSERT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	INSERT		
BulletM	UPDATE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	UPDATE		
DanC	SELECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datareader	SELECT		
DanC	DELETE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	db_datawriter	DELETE		

Kako vidjeti koja su pravila ponašanja na serveru?

SQL Server Policies :

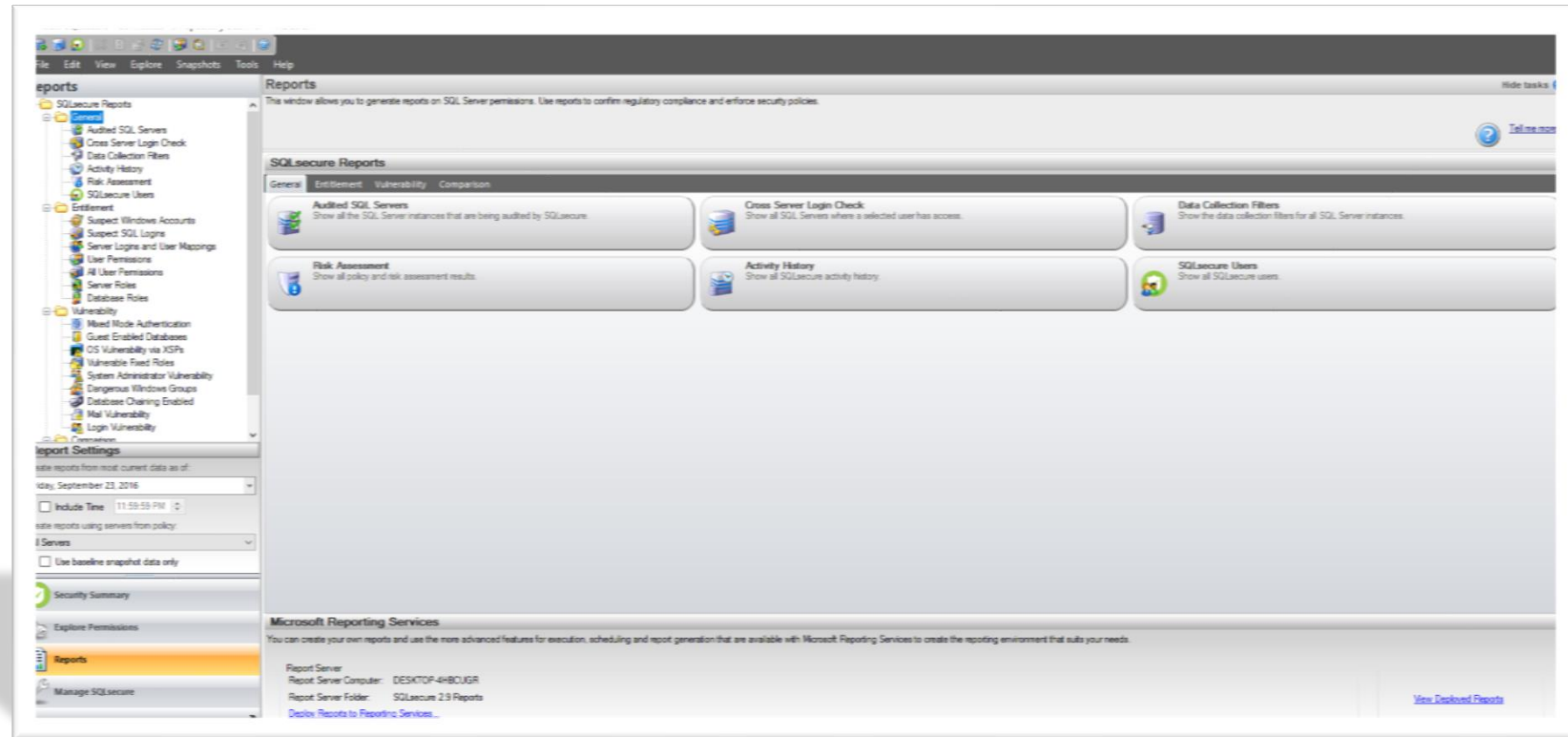
- 80+ provjera ponašanja kroz 7 kategorija
- Import predložaka pravila ponašanja na temelju preporuka autoriteta kao što su DISA SRR, CIS i SNAC, kao i IDERA definirane kategorije zaštite: Osnovna, Nalansirana i Jaka.



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.



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?

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

The screenshot displays the Idera SQL compliance manager (SQL2012) interface. The main window is titled "Idera SQL compliance manager (SQL2012)" and features a menu bar with options like File, Edit, View, Auditing, Alerting, Agent, Tools, and Help. The interface is divided into several sections:

- Explore Activity:** A tree view on the left showing a hierarchy of audited SQL Servers, including EARTH, MARS, PROD-CLUST-1, SQL2012, Financial_Records, Healthcare, and msdb.
- SQL2012 Summary:** A central panel with tabs for Summary, Event Alerts, Data Alerts, Audit Events, and Archived Events. It includes a toolbar with icons for actions like Configure Alerting, Remove Server, Add Audited Databases, Disable Auditing, Server Settings, Apply Regulation Guideline, Privileged Users, Import, Export, Collect Audit Data, Agent Properties, and Span (set to 30 Days).
- Server Status:** A section showing a green checkmark and "OK" status. It lists: Last Heartbeat (9/10/2014 4:40 PM), Last Archived (9/10/2014 1:30 AM), Processed Events (818,929), and Recent Alerts (2).
- Server Activity Report Card:** A section with a line graph showing "Overall Activity" over time. The graph indicates that "Overall Activity currently has no threshold enabled." The y-axis ranges from 0 to 80,000, and the x-axis shows dates from 8/14 to 9/08.
- Audit Configuration:** A section detailing the audit setup for the server, including "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", and "Event Filters (1) - Application Name, Database, Hostname, Login Name".
- Recent Audit Events:** A table listing recent events with columns for Category, Event, Time, and Details. The events include multiple "Invalid" DDL operations and "Server alter trace" operations performed by "Admin" users on "DEMOBOX\SPFarm".



Dnevnik aktivnosti za forenzičku analizu incidenta

Bilježenje aktivnosti:

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

The screenshot displays the Idera SQL compliance manager interface for SQL2012. The main window shows the 'Explore Activity' pane on the left, listing audited SQL servers: EARTH, MARS, PROD-CLUST-1, SQL2012, Financial_Records, and Healthcare (msdb). The main pane is titled 'SQL2012::Healthcare' and shows 'Audit Events' for 'Login' and 'DML' operations. The 'Login' event shows a user 'DEMOSBOX\robert' logging in. The 'DML' events show updates to the 'Prescriptions' table, with columns updated and audited updates recorded. The interface includes filters for Time, Login, Category, Application, Host, and Table/Column, and options for Expand All, Collapse All, and Flatten Data.

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			
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			
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

Predložci standardnih izvještaja:

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

The screenshot displays the Idera SQL compliance manager (SQL2012) interface. A dialog box titled "SQLcm Configuration Wizard - Apply Regulation" is open, showing "Regulation Guidelines" for HIPAA. The guidelines include:

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

The dialog also indicates that the SQLCompliance Agent will automatically collect the following server and database events:

- Privileged Users
- Privileged User Events
- Sensitive Column Auditing

The background interface shows a tree view of audited SQL servers (EARTH, MARS, PROD-CLUST-1, SQL2012) and a table of audit events. The table has columns for Time and Details, with entries for "Server alter trace" and "Invalid" events.

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 contrast 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.

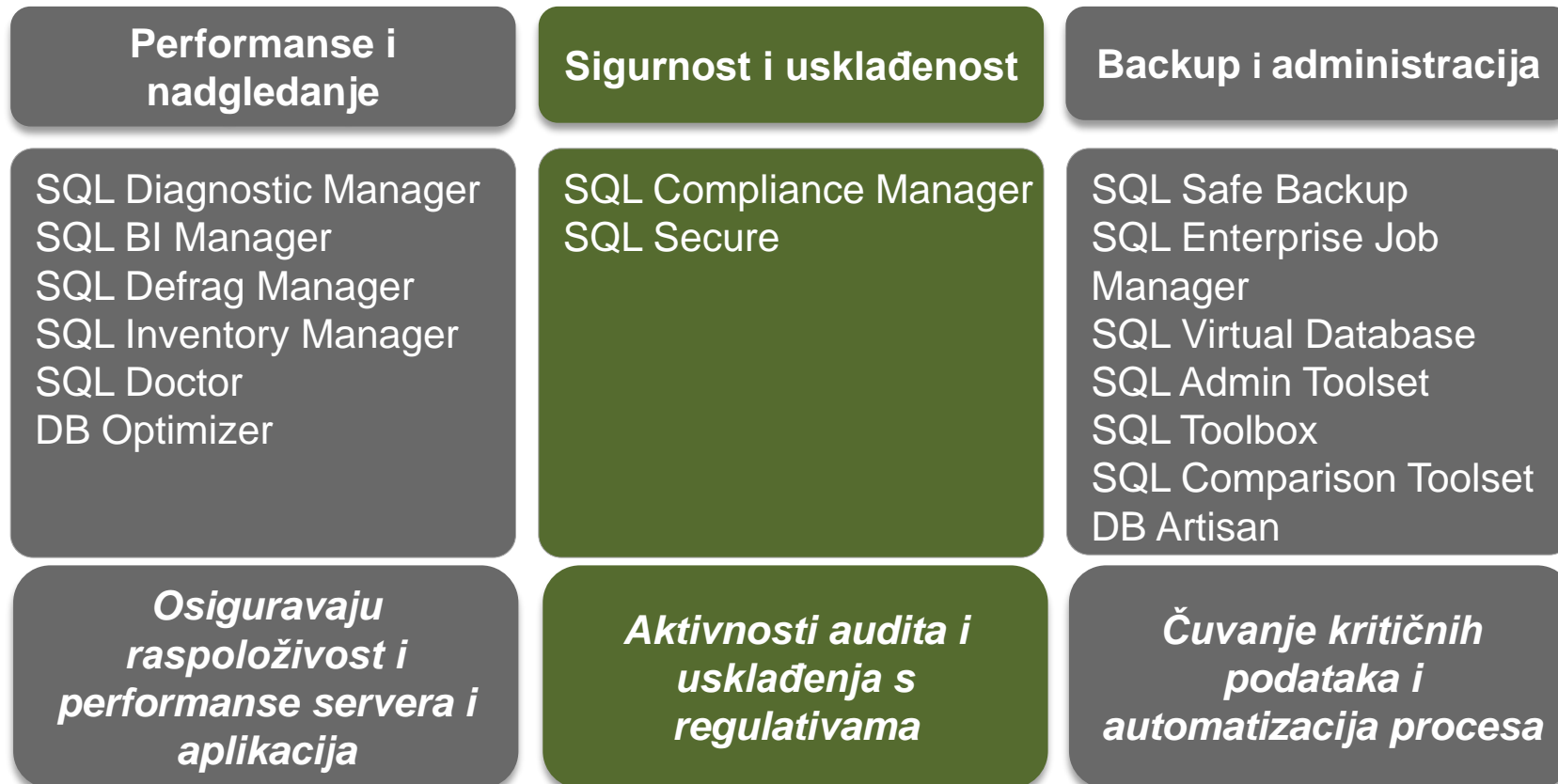
SQL Compliance Manager

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



IDERA alati za upravljanje bazama podataka

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



www.idera.com
idera@konto.hr