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?

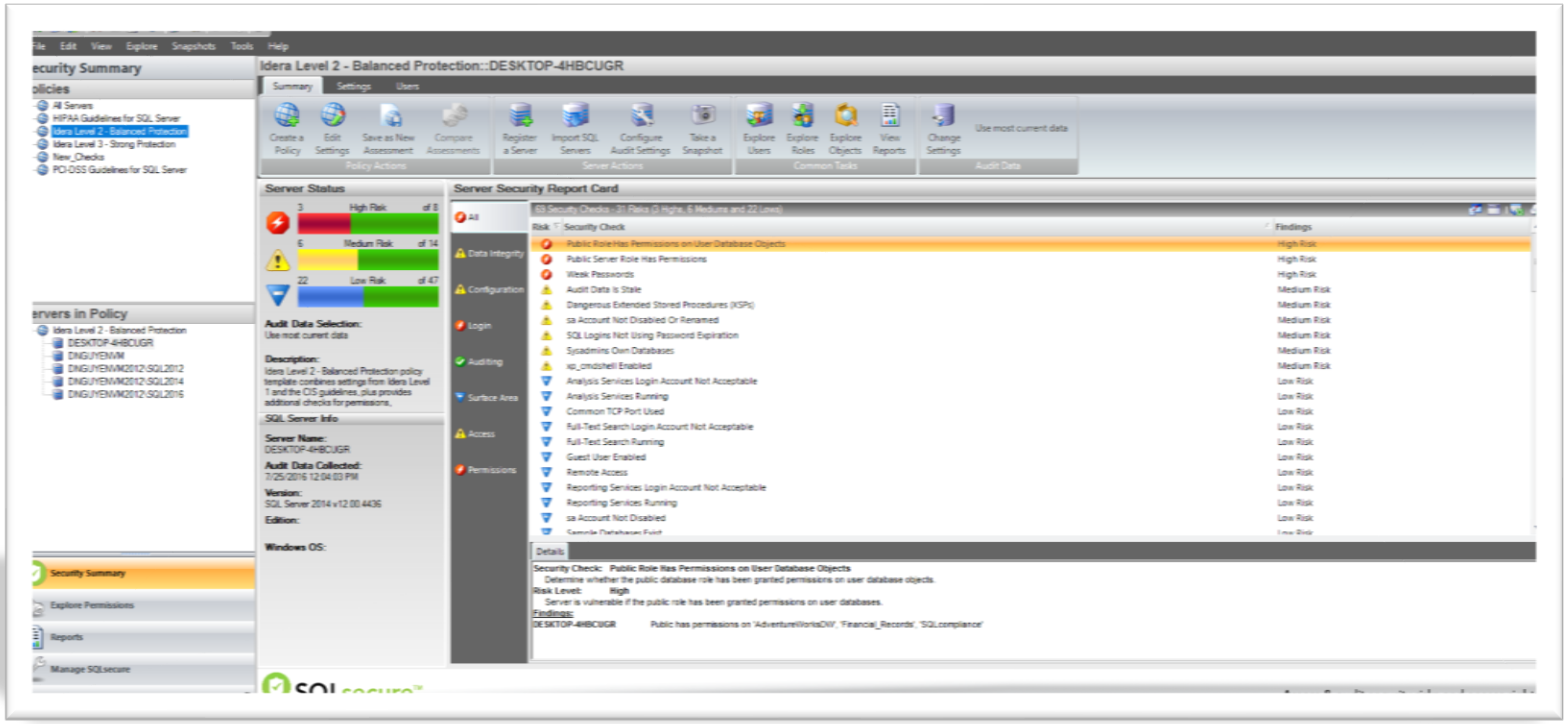
Baze podataka

- 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 :

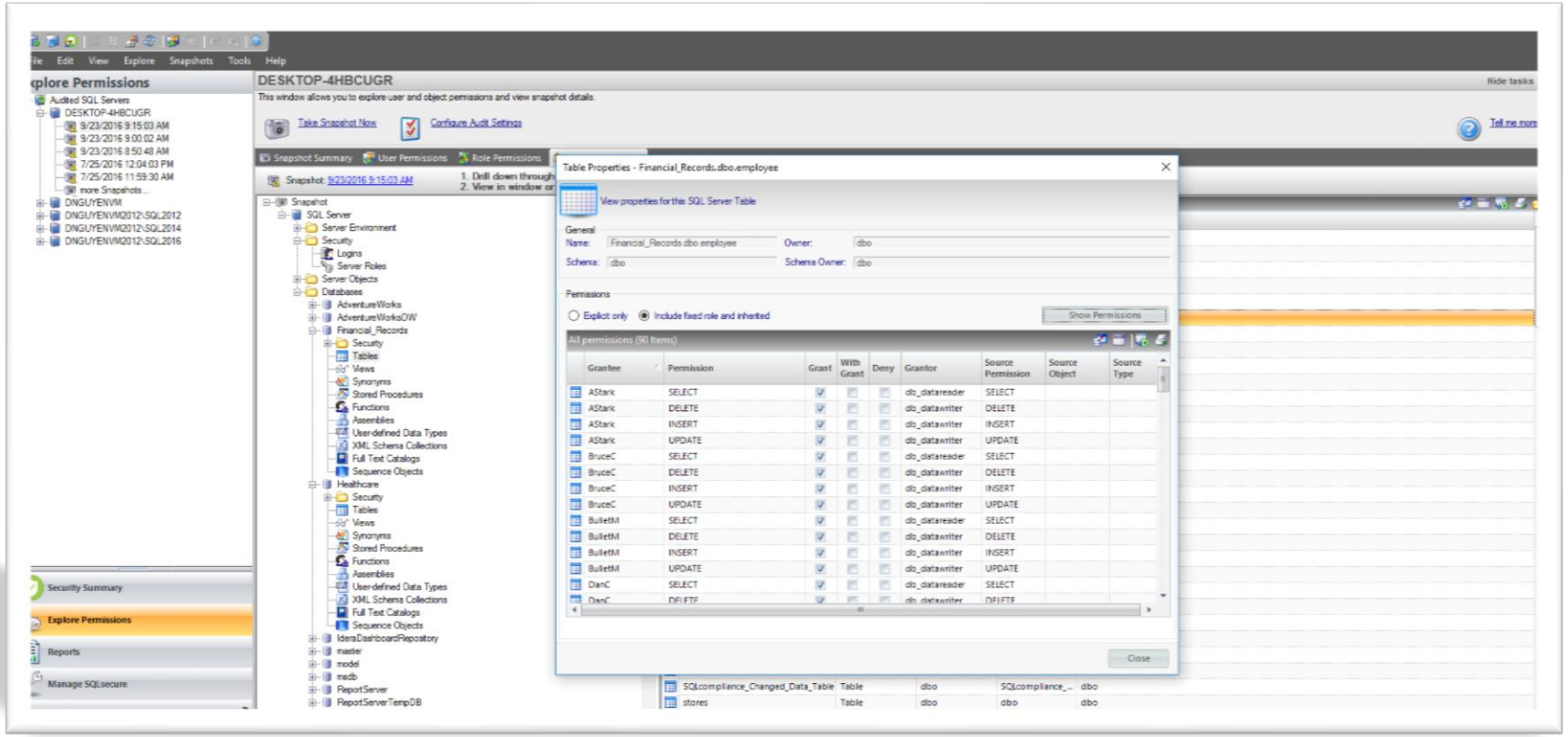
- Usporedba sigurnosnih postavki svih SQL Servera u organizaciji
- Provjera definirane razine sigurnosti 2 za zaštitu od upada.
- Identifikacija najčešćih sigurnosnih ranjivosti.
- Pravila za procjenu rizika omogućuju provjere pristupa bazama podataka, konfiguracijske provjere i provjere dozvola.
- Svaka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



Tko može pristupiti podacima?

SQL Server User Permissions :

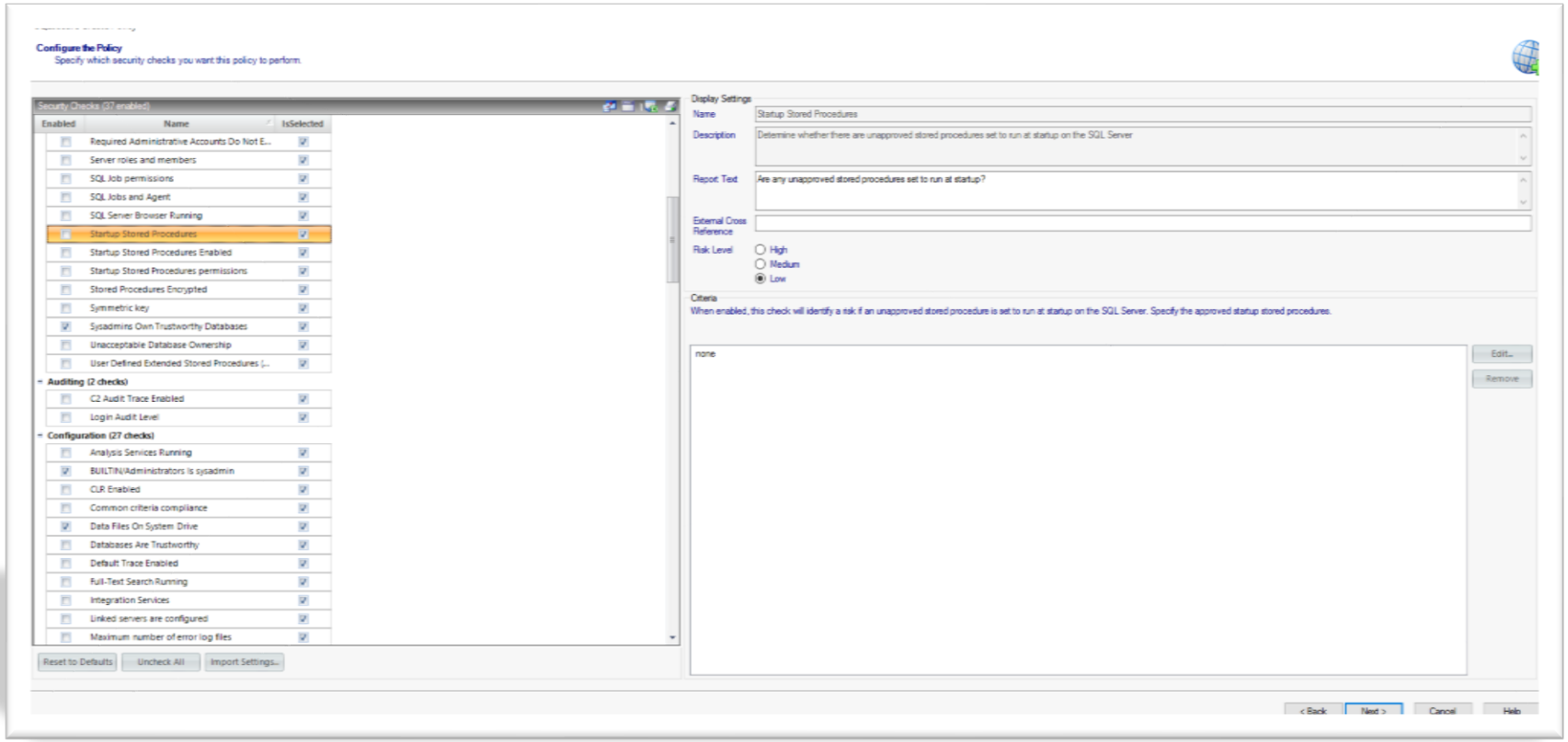
- Otkrivanje svih prava pristupa na SQL Server i Azure SQL bazama podataka.
- Pregled i analiza svih SQL Server objekata od razine servera do razine uloga.
- Pregled svih sigurnosnih svojstava i dopuštenja za sve objekte.
- Povijesni pregled audita i usporedba stanja (traženje promjena)



Kako vidjeti koja su pravila ponašanja na serveru?

SQL Server Policies :

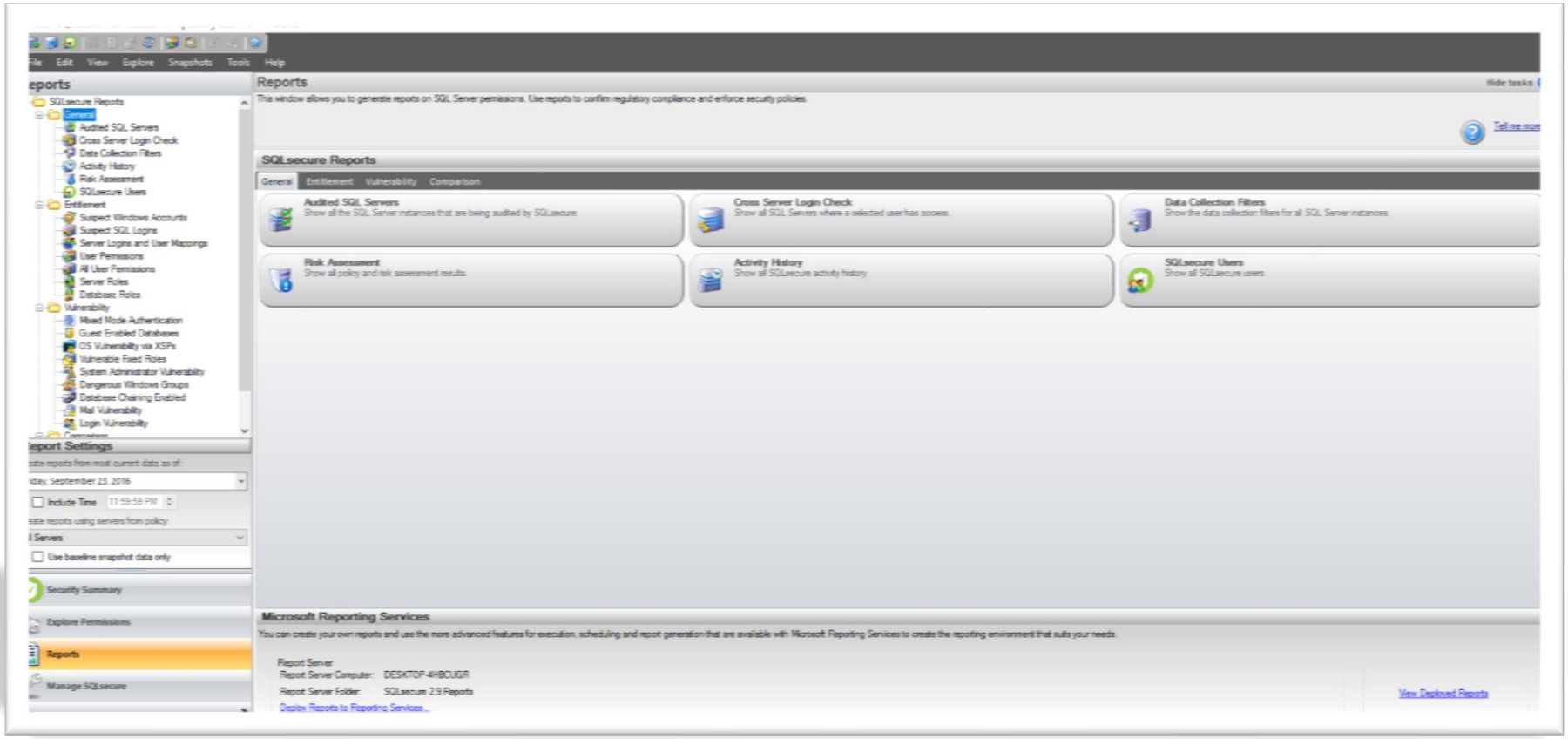
- 80+ provjera ponašanja kroz 7 kategorija
- Import predložaka pravila ponašanja na temelju preporuka autoriteta kao što su DISA SRR, CIS i SNAC, kao i IDERA definirane kategorije zaštite:Osnovna, Nalansirana i Jaka.



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

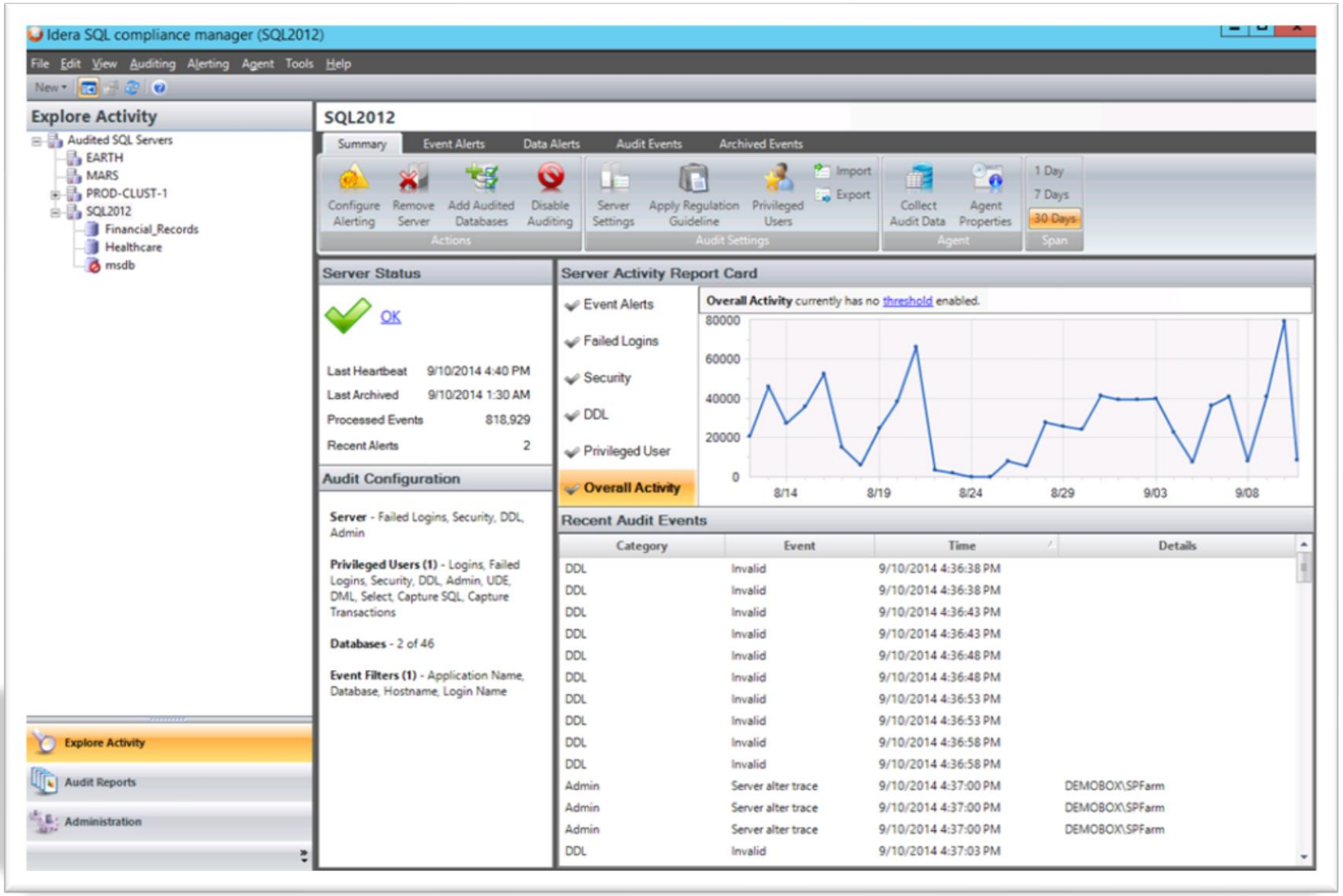
Što ako dođe do neovlaštenog pristupa i/ili gubitka podataka?

- 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 :

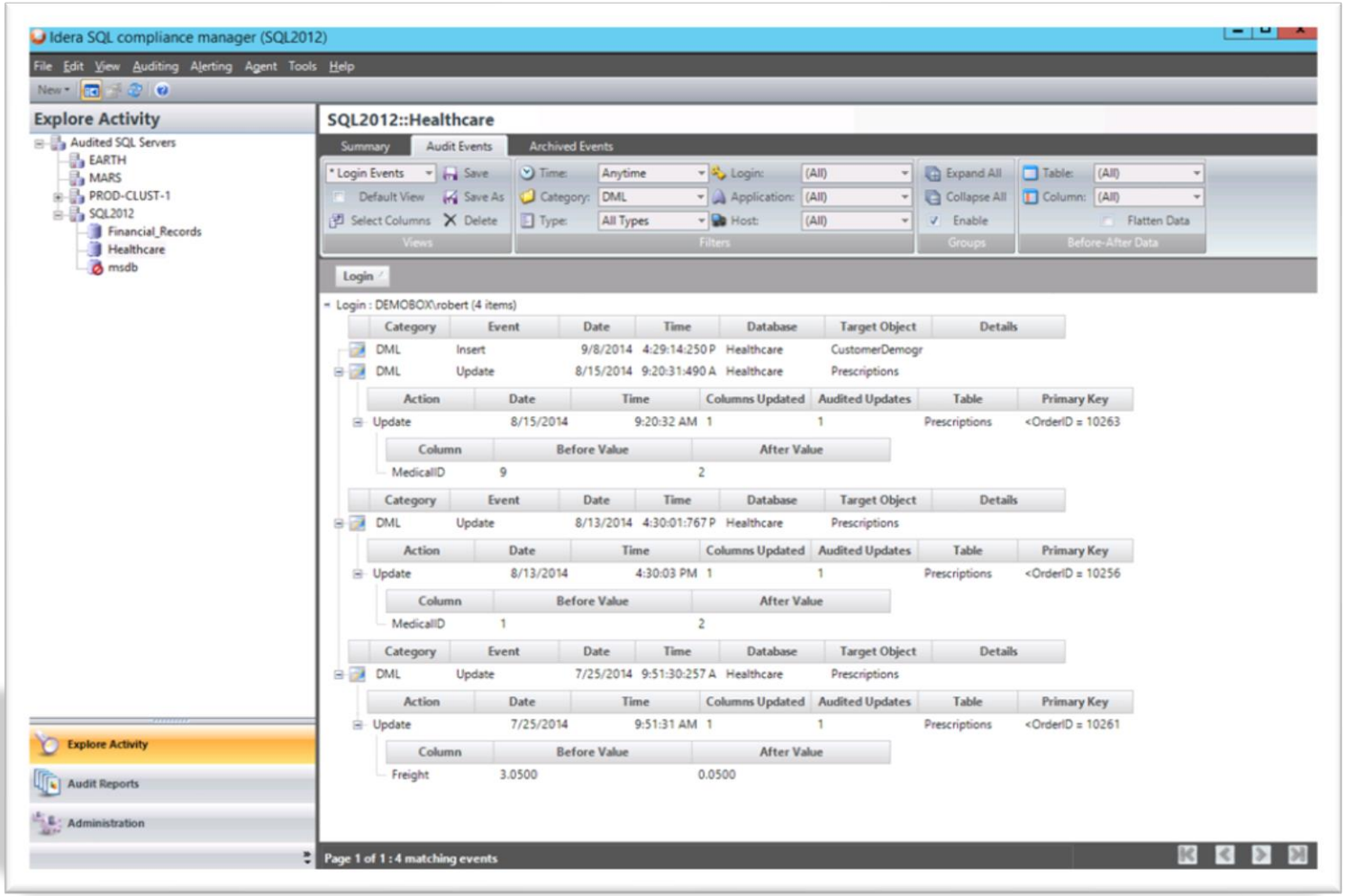
- Centralizirani audit svih SQL Server-a I baza podataka
- Praćenje svih aktivnosti korisnika I upozoravanje na promjene podataka u stvarnom vremenu
- Definiranje alarma za pristup osjetljivim podacima
- Praćenje trendova aktivnosti korisnika



Dnevnik aktivnosti za forenzičku analizu incidenta

Bilježenje aktivnosti:

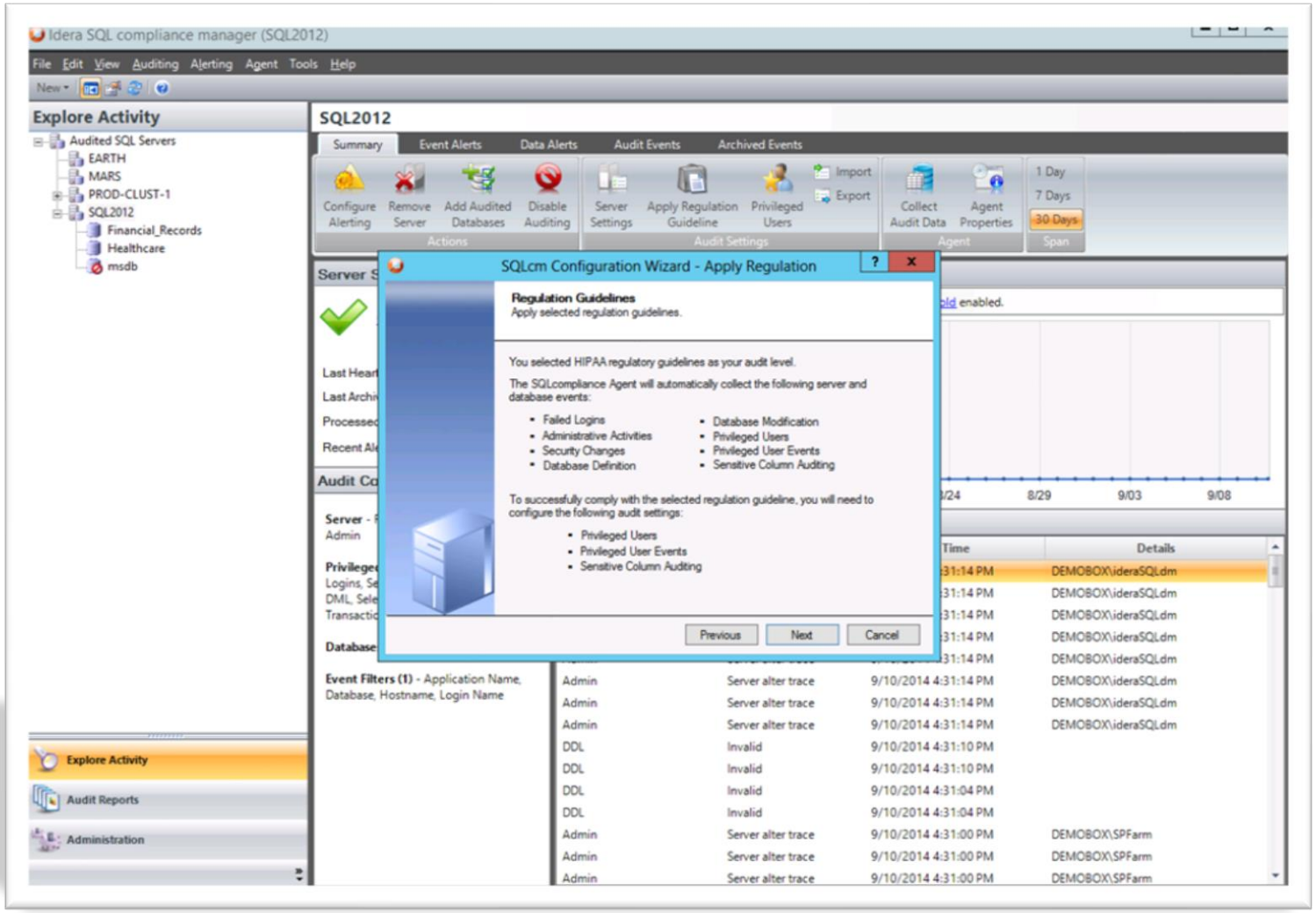
- Bilježenje svih aktivnosti korisnika
- Analiza promjena podataka
- Pregld DML-a koji je promjenio podatke, pregled vrijednosti prije I poslije promjene
- Posebna pažnja posvećena pristupu osjetljivim podacima



Regulatorni izvještaji

Predlošci standardnih izvještaja:

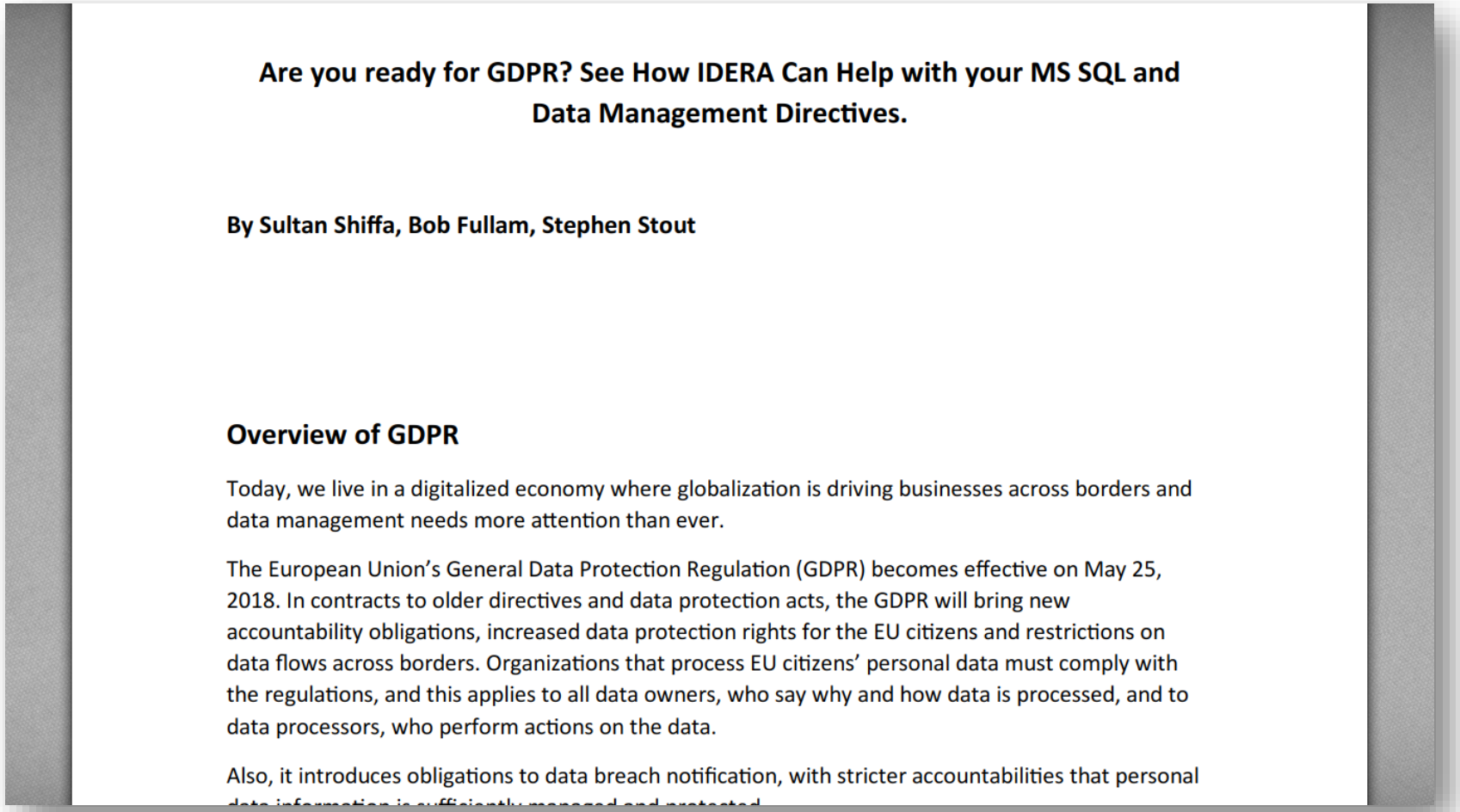
- Automatsko stvaranje izvještaja koji udovoljavaju zahtjevima HIPAA, HITECH and PCI DSS I dr. regulative
- 25 gotovih predložaka audita uz stalno proširenje



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.

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

- 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

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