

ARE YOU READY FOR GDPR?

BY BOB FULLAM AND STEPHEN STOUT

Demonstrate Compliance with IDERA SQL Security Suite

OVERVIEW

The European Union's General Data Protection Regulation (GDPR) takes effect 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. GDPR also requires evidence of compliance against these directives.

In this solution brief, we discuss the most important issues that Microsoft SQL Server database management teams need to consider to comply with the GDPR Articles and how to tackle these challenges with the IDERA SQL Security suite, which includes SQL Compliance Manager and SQL Secure.

ARTICLE 25 DATA PROTECTION BY DESIGN AND DEFAULT

Many Microsoft SQL Server environments lack control over the exposure of personal data. With SQL Compliance Manager, not only will companies be able to control accessibility but they can also see how and by whom the data is being accessed. There are several ways to specify which data is considered “sensitive” and to monitor what happens to that specific data.

Diagram 1 is the result of alerting on a Select that returns the NI Column. Please note, the NI column does not need to be explicitly selected.

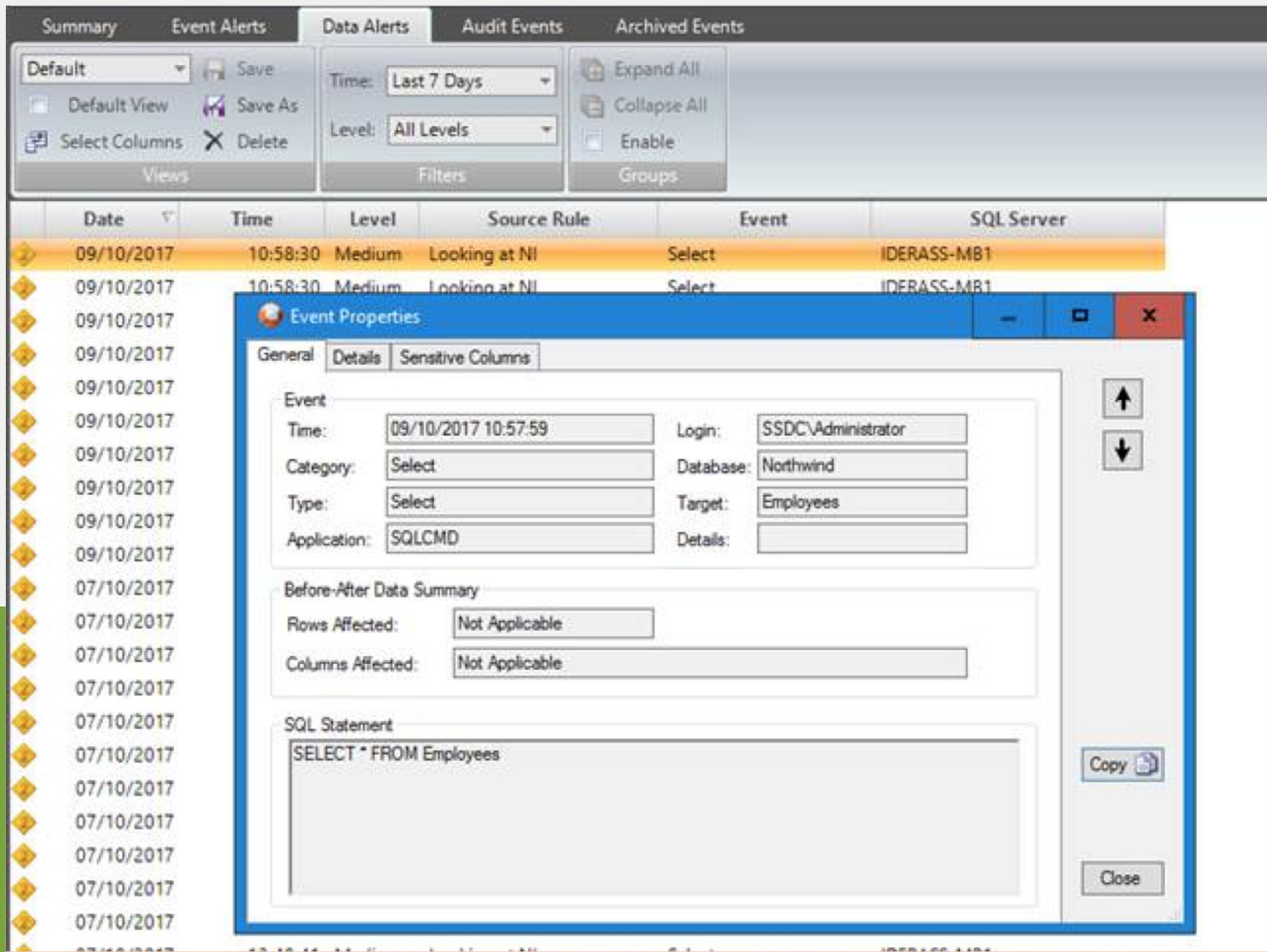


Diagram 1 Example of Event Properties for alerts in SQL Compliance Manager

ARTICLE 30 RECORDS OF PROCESSING ACTIVITIES

In order for organizations to log and monitor operations, it is imperative to keep an audit record of processing activities on personal data. With SQL Compliance Manager, database administrators can track specific changes throughout the environment, including to personal data while keeping a repository of those changes. Refer to the following diagrams for specific examples.

```
katja salary up.sql...rthwind (katja (100)) x
USE Northwind
GO
update SalaryInfo set usersalary = 150150 where userlastname = 'jones'
Go
|
```

Diagram 2 An example of making a change to data in a database table

The screenshot displays the SQL Compliance Manager interface. At the top, there are tabs for 'Summary', 'Audit Events', and 'Archived Events'. The 'Audit Events' tab is active, showing a list of events. The event details for a DML Update are expanded, showing the following information:

Category	Event Type	Date	Time	Login	Database	Target Object	Details
DML	Commit Transacti	09/10/2017	2:51:42:070 P	katja	Northwind	SalaryInfo	
DML	Update	09/10/2017	2:51:42:070 P	katja	Northwind	SalaryInfo	

The 'Update' event is further detailed in a table:

Action	Date	Time	Columns Updated	Audited Updates	Table	Primary Key
Update	09/10/2017	14:51:42	1	1	SalaryInfo	

Below this, a 'Before-After Data' summary table shows the change to the 'usersalary' column:

Column	Before Value	After Value
usersalary	140150	150150

An 'Event Properties' dialog box is open, showing the following details:

- Event Time: 09/10/2017 14:51:42
- Login: katja
- Category: DML
- Database: Northwind
- Type: Update
- Target: SalaryInfo
- Application: Microsoft SQL Server Management
- Details: (empty)

The 'Before-After Data Summary' section shows:

- Rows Affected: 1
- Columns Affected: usersalary

The 'SQL Statement' section contains the following text:

```
update SalaryInfo set usersalary = 150150 where userlastname = 'jones'
```

Diagram 3 Review the “Event” stored in SQL Compliance Manager that shows the DML change to the data

ARTICLE 30 RECORDS OF PROCESSING ACTIVITIES CONTINUED

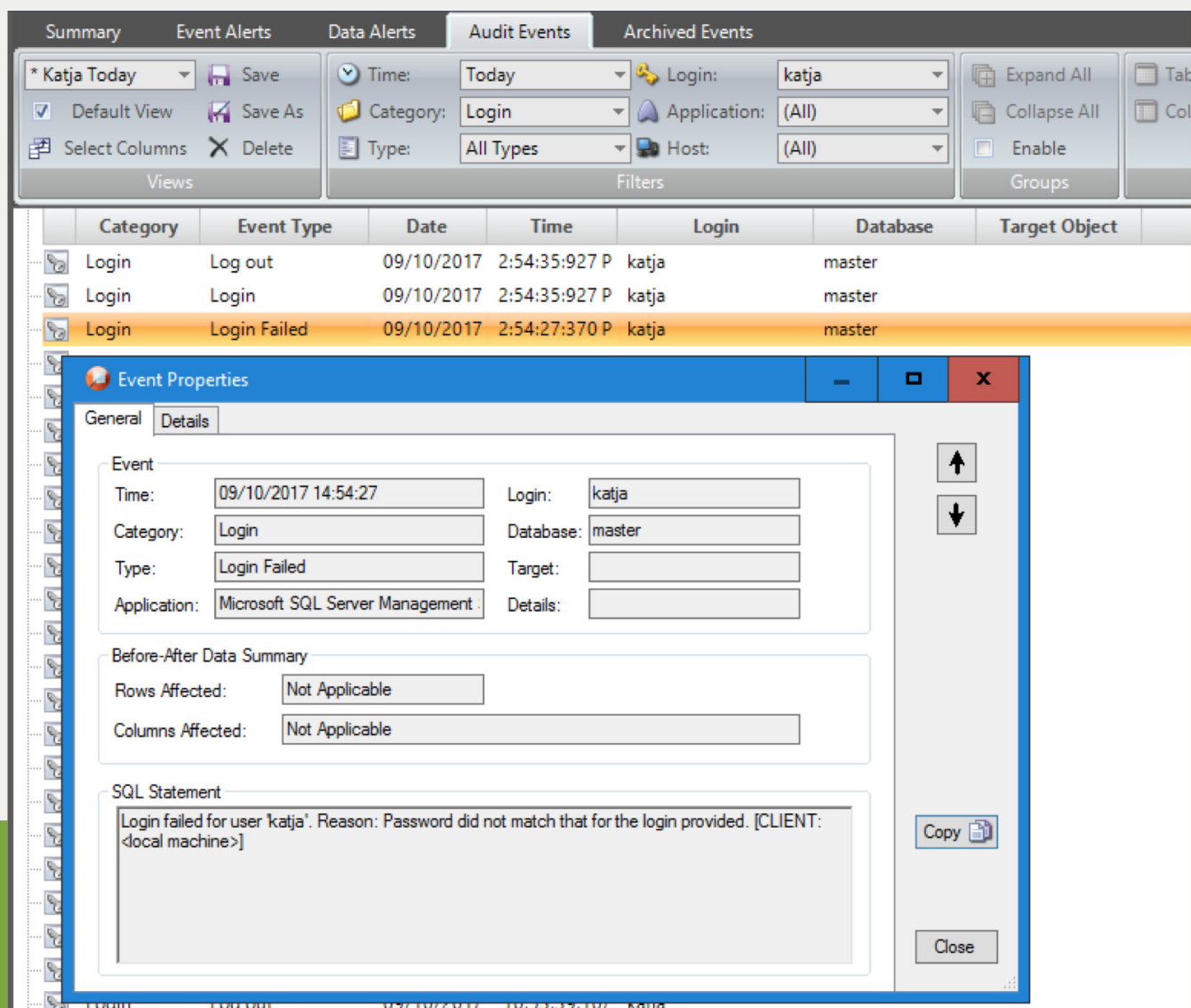


Diagram 4 SQL Compliance Manager can capture login activity, both failures and successes, as needed

ARTICLE 32 SECURITY OF PROCESSING

In order to achieve a secure environment for processing data, SQL database professionals are required to regularly test and assess the effectiveness of security measures. These security mechanisms will ensure personal data is safe throughout the system. With SQL Secure, you can schedule or “manually” take “snap shots” of the well-being of the security system, as shown in Diagram 5. From here, it is easy to compare the previous hardened “snap shot” to the current one, which will allow for quick assessment of any changes to the specific areas within your security system.

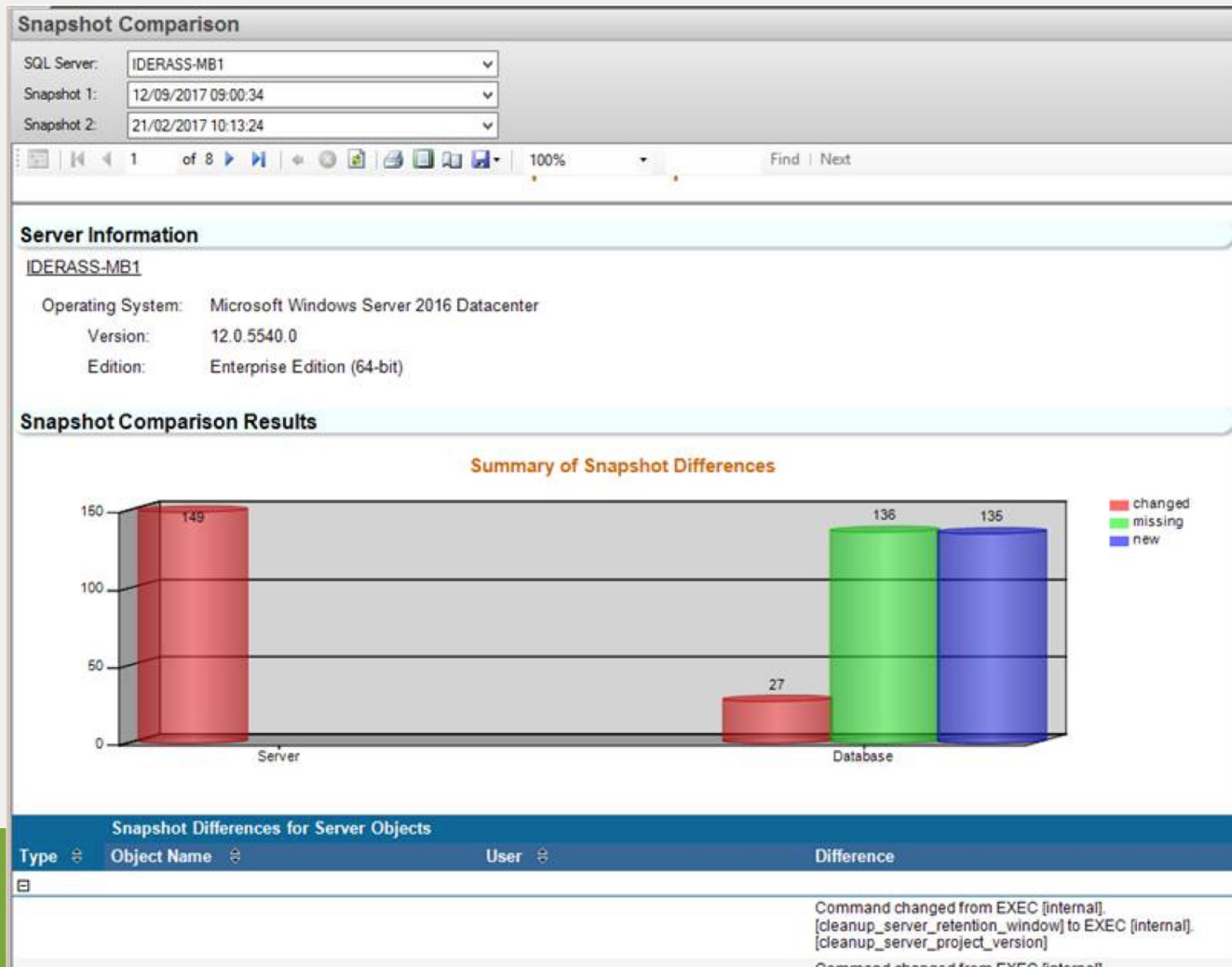


Diagram 5 A view of SQL Secure “snap shot” comparison

ARTICLE 33 NOTIFICATION OF PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

Should a breach occur, SQL Compliance Manager is configured to alert personnel when identified sensitive data is being accessed. This automatic notification can be defined based on specific properties, as shown in Diagram 6.

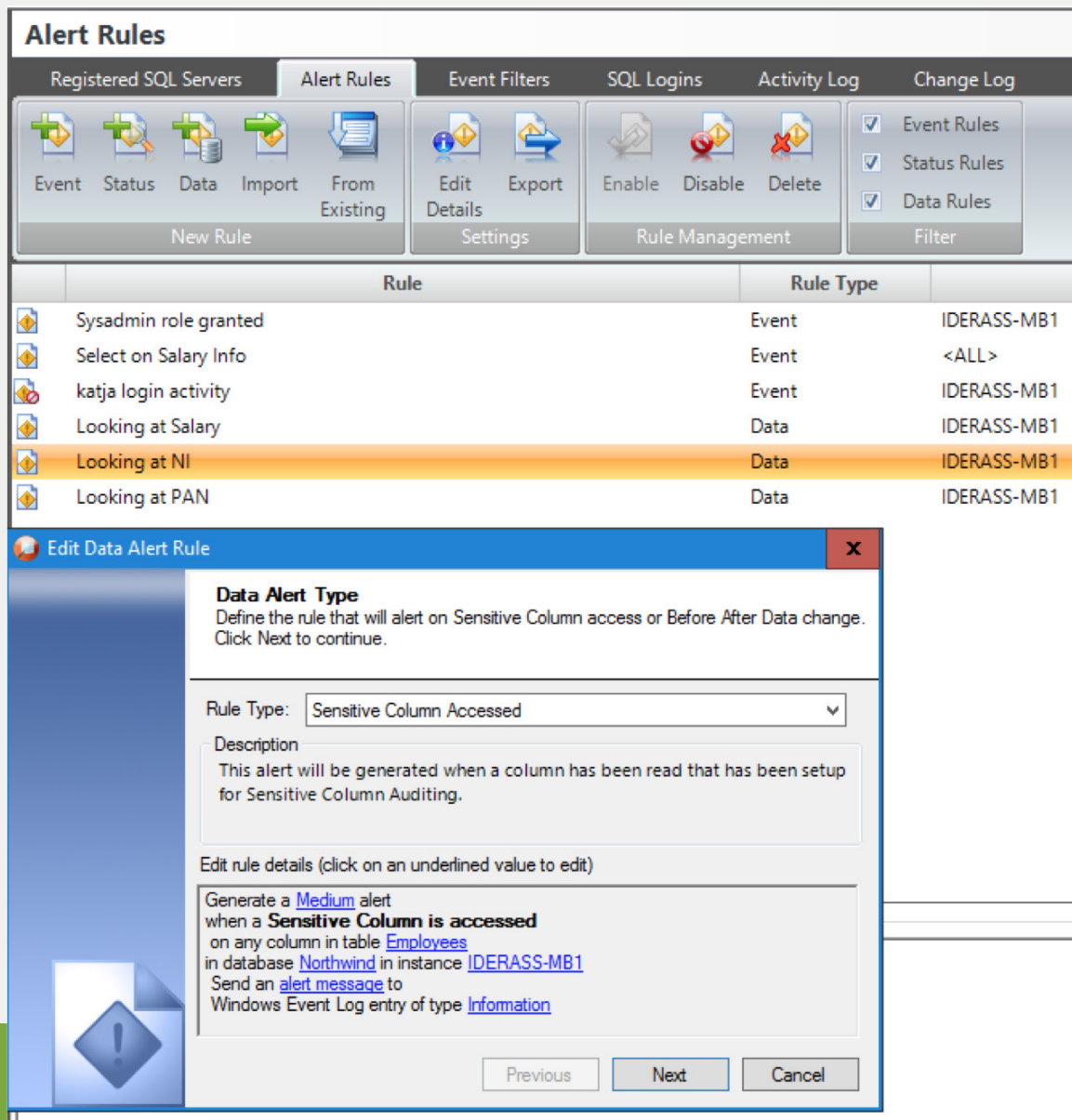


Diagram 6 Set up alert rules in SQL Compliance Manager

ARTICLE 35 DATA PROTECTION IMPACT ASSESSMENT

Throughout your environment, it is vital to manage, monitor, and document security risks and measures. With the IDERA SQL Security suite, you can apply measures to address risks and protect personal data while assisting with GDPR compliance. SQL Compliance Manager and SQL Secure both offer reporting capabilities that can provide a compliance summary for audits.

Audit Reports

- Agent History**
List all activity for SQL compliance manager Agent.
- Alert Activity - Status**
Show SQL compliance manager status alert activity.
- Application Activity Statistics**
List a summary of application activity by activity type.
- Change History (by object)**
List security changes for specified objects.
- Database Schema Change History**
List all schema changes made to specified databases.
- Integrity Check**
List all integrity check violations.
- Object Activity**
List all activity for specified objects.
- Sensitive Column Activity**
Lists every time a sensitive column was accessed.
- User Login History**
List all login activity for sp...
- Alert Activity - Data**
Show SQL compliance manager data alert activity.
- Alert Rules**
List alert rules.
- Audit Control Changes**
List all changes to SQL compliance manager audit settings.
- Change History (by user)**
List security changes performed by specified users.
- DML Activity (Before-After)**
Lists DML events for which before and after data is available.
- Login Creation History**
List all login creation activity.
- Permission Denied Activity**
Lists all activity for which permission was denied.
- Server Login Activity Summary**
Lists login statistics per server with per login details.
- Alert Activity - Events**
Show SQL compliance manager event alert activity.
- Application Activity**
List all activity by application.
- Backup and DBCC Activity**
List all backup, restore and DBCC activity.
- Daily Audit Activity Statistics**
Provides summary audit statistics per day.
- Host Activity**
List all activity for specified hosts.
- Login Deletion History**
List all login deletion activity.
- Regulation Guidelines**
Shows Regulation Guideline details for all the guidelines applied to database on this instance.
- User Activity History**
List all activity for specified users.

Diagram 7

The available SQL Compliance Manager reports

Sensitive Column Activity

Server Instance: IDERASS-MB1 Database: Northwind
 Login: * Table Name: *
 Start Date: 09/09/2017 End Date: 11/10/2017
 Show SQL: True

Run Report

SQL compliance manager™

Sensitive Column Activity
From 09/09/2017 to 11/10/2017 23:59:59

Event	Time	Login	Database	Table	Column	Application Name
Select	10/10/2017 10:08:51	SSDCAdministrator	Northwind	Employees	NI	SQLCMD
SELECT * FROM Employees						
Select	10/10/2017 10:08:51	sa	Northwind	Employees	NI	SQLCMD
SELECT * FROM Employees						
Select	10/10/2017 10:02:16	SSDCAdministrator	Northwind	Employees	NI	SQLCMD
SELECT * FROM Employees						

Diagram 8 Sample SQL Compliance Manager report, showing “Sensitive Column Activity”

ARTICLE 35 DATA PROTECTION IMPACT ASSESSMENT CONTINUED

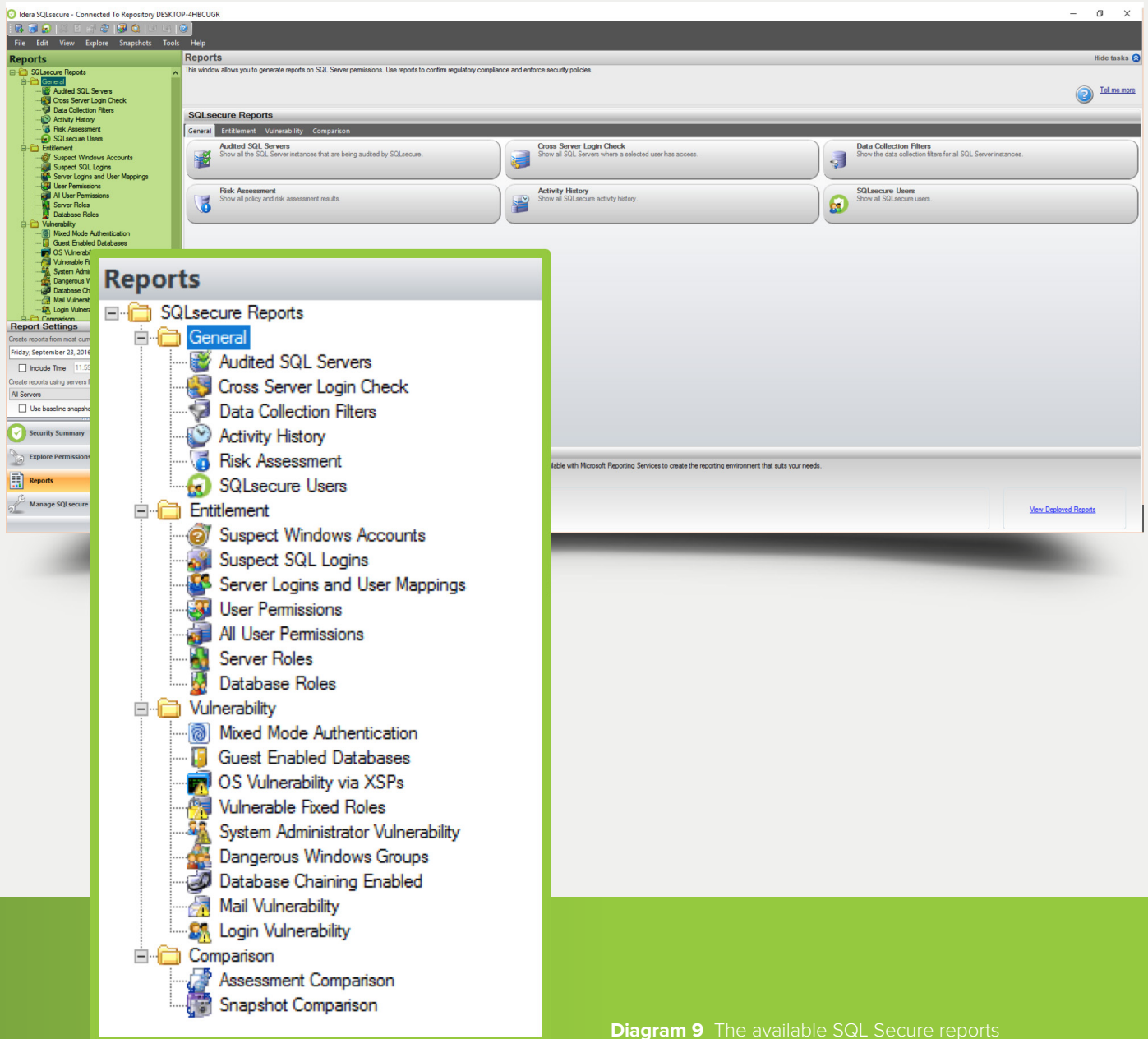


Diagram 9 The available SQL Secure reports

ARTICLE 35 DATA PROTECTION IMPACT ASSESSMENT CONTINUED

User Permissions

SQL Server: IDERASS-MB1 Level: User

Permission Type: Assigned User: katja

Login Type: Windows User or Group SQL Login

1 of 1 100% Find | Next

SQLsecure™ Assess & audit security risks and access rights

User Permissions

Most current audit data as of 02 January 2018

Login: katja Permission Type: Assigned
 Login Type: SQL Login Server: IDERASS-MB1

About: This report shows all user permissions.

SQL Server: IDERASS-MB1

Login Name	Server Access	Disabled	Roles
katja	Yes	No	sysadmin

Type	Database	Object Name	Permission	Access	Grantee	Aliased	Grantor	Owner
Aggregate Function (CLR)								
master								
		GeographyCollectionAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeographyConvexHullAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeographyEnvelopeAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeographyUnionAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeometryCollectionAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeometryConvexHullAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeometryEnvelopeAggregate	EXECUTE	Grant	public	No	dbo	sys
		GeometryUnionAggregate	EXECUTE	Grant	public	No	dbo	sys
		ORMask	EXECUTE	Grant	public	No	dbo	sys
Database								
Healthcare								
	Healthcare		CONNECT	Grant	dbo	No	dbo	katja
master								
	master		CONNECT	Grant	quest	No	dbo	sa

Diagram 10 Sample SQL Secure report, showing [named] "User Permissions"

SUMMARY

GDPR expects customer data privacy and industry compliance by design and default.

The first step to support data protection requirements would be to establish a robust data governance program and create awareness about the rules and impact of not being GDPR compliant, leveraging integrated process and data modeling tools.

Discovery is the second step to look into existing systems and processes. Whether we are working on new systems or looking into existing legacy systems, we need to store and maintain our data fields in line with the GDPR rules. The IDERA SQL Security suite helps you to focus on data breaches, personal information revisions and overall environment changes, specific to your SQL Server databases. Both products help to document and encourage discussions on how organizations are complying with GDPR legislation within the organization and external regulators in case of an audit.

IDERA understands that IT doesn't run on the network – it runs on the data and databases that power your business. That's why we design our products with the database as the nucleus of your IT universe.

Our database lifecycle management solutions allow database and IT professionals to design, monitor and manage data systems with complete confidence, whether in the cloud or on-premises.

We offer a diverse portfolio of free tools and educational resources to help you do more with less while giving you the knowledge to deliver even more than you did yesterday.

Whatever your need, IDERA has a solution.

I D E R A