GLOC

Great Lakes Oracle Conference

Oracle Database Security Assessment Tool, Know Your Risks

MAY 15 & 16, 2019

CLEVELAND PUBLIC AUDITORIUM, CLEVELAND, OHIO

WWW.NEOOUG.ORG/GLOC

Speaker Introduction

Michael Messina

Senior Managing Consultant. Rolta AdvizeX

Working with Oracle Approximately 25 years

Background includes Performance Tuning, High Availability and Disaster Recovery

Oracle Database OCP

Oracle RAC Certified Expert

Oracle Exadata Implementation Specialist

Oracle MySQL Certified Implementation Specialist

Oracle ACE

mmessina@advizex.com

www.advizex.com

ROLTA | ADVIZEX

ROLTA | ADVIZEX

Agenda

1. Security
2. The Oracle DB Security Assessment Tool
3. Setup and Installation
4. Running the DBSAT Collector
5. Running the DBSAT Reporter
6. Analyze the Reporter Output
7. Discover
8. Analyze Discover Output
9. Questions/Discussion

Security

- Security Breaches 2018
  - Sak, Lord & Taylor -> 5 million records
  - PumpUp -> 6 million records
  - Sacramento Bea -> 19.5 million records
  - Ticketfly -> 27 million records
  - Panera -> 37 million records
  - Facebook -> 87 million records
  - MyHeritage -> 92 million records
  - Under Armour -> 150 million records
  - Exactis -> 340 million records
  - Aadhaar -> 1.1 billon records

  Source: https://blog.barkly.com/biggest-data-breaches-2018-so-far

ROLTA ADVIZEX

Security

Insider threat often more overlooked then outside threat so need to ensure focus on security includes the more likely insider threat to data breach. (ie. Separation of Duties)

Physical Security typically has had more focus then data security though that has been changing.

Data Security is getting more focus as more breaches are highlighted in Media as they happen.

Regulatory Compliance must be adhered to for Health Care and Financial information some critical business data is left unprotected leaving organization exposed to that data being stolen by competitors and organization may not even realize it.

Security

Average cost of a data breach is $7.35 million,

$225 per stolen record

Damage to victims (our customers and clients), brand (our business reputation), and business (revenue hit)

HIPAA

GDPR

SOX

The List goes On

Protect Our Organization

4 Pillars of Data Protection

- Assessment
  - Investigate your Risks, know you data and where it is
  - Discover what needs protecting so you can take action
  - Oracle Database Security Assessment Tools can help with this
- Goverance
  - Policy and procedures
- Training
  - Make sure your staff have the knowledge and training to protect data
- Response
  - Data Breaches
  - Loss of data
  - Take proper action
  - I say this means be proactive, monitor and consistently assess

Source: https://securitythinkingcap.com/four-pillars-of-data-protection-for-the-modern-enterprise/

ROLTA ADVIZEX

Protect The Data and the Database Environment

Where is the Data That needs to be protected?

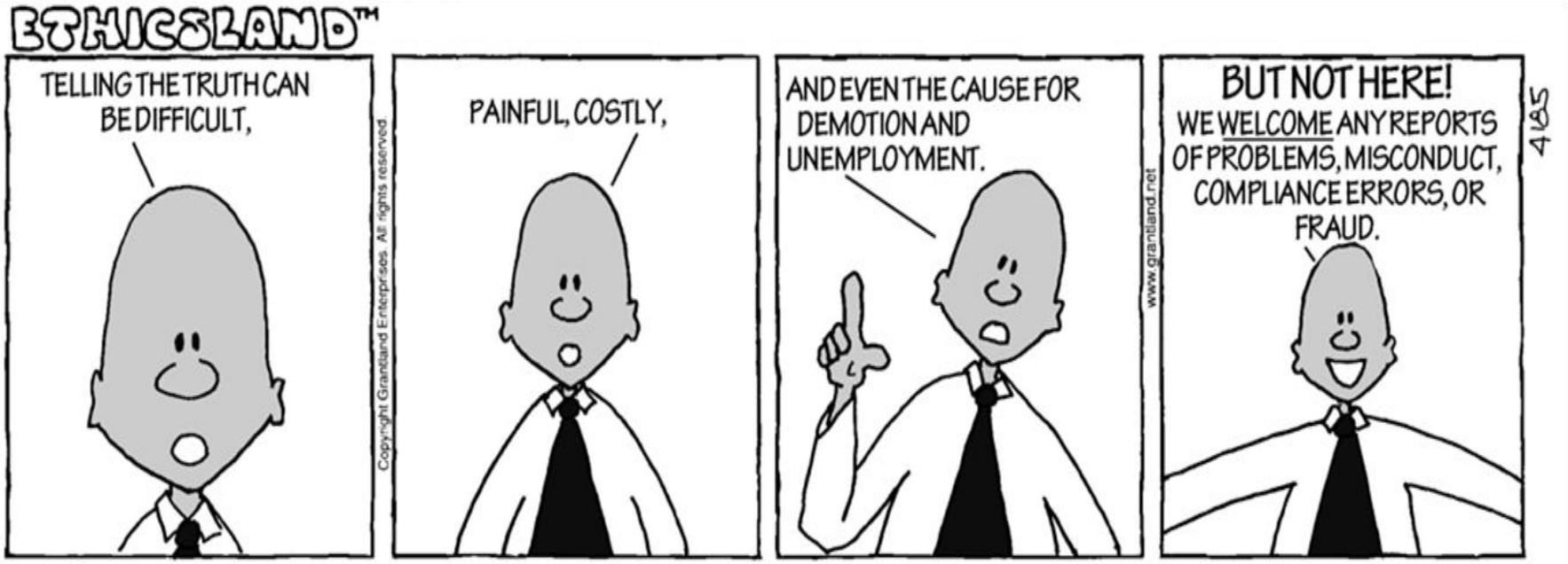
Are there current security issues in my environment?

Who has access to the Data, should they have access to the data?

Is data Encrypted that should be encrypted?

Am I following security best practices?

Knowledge is Power When it Comes to Security



Security?

What Options do we have?

What do we need to do?

What should we do?

The Oracle DB Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool is a tool provided by Oracle to assist with evaluating security best practices for your environment and helping identify security risks, best practice violations so that you can take action to better secure the environment and database.

The Oracle DB Security Assessment Tool (DBSAT)

- State of user accounts, role and privilege grants, and policies
- Fix immediate short-term risks
- Implement a comprehensive security strategy
- Identify security configuration issues for Oracle databases
- Promote and implement security best practices
- Improve the security for Oracle Databases
- Reduce exposure to risk for known security issues

The Oracle DB Security Assessment Tool (DBSAT)

Scans the database for sensitive data

Uses customizable regular expression patterns

Reports on the amount and type of sensitive data found

Get deeper insight on how much sensitive data exists

Determine where sensitive data exists

Knowing there is data to protect knowing it exists and where it is being the first step to protecting it with encryption, access control, etc.

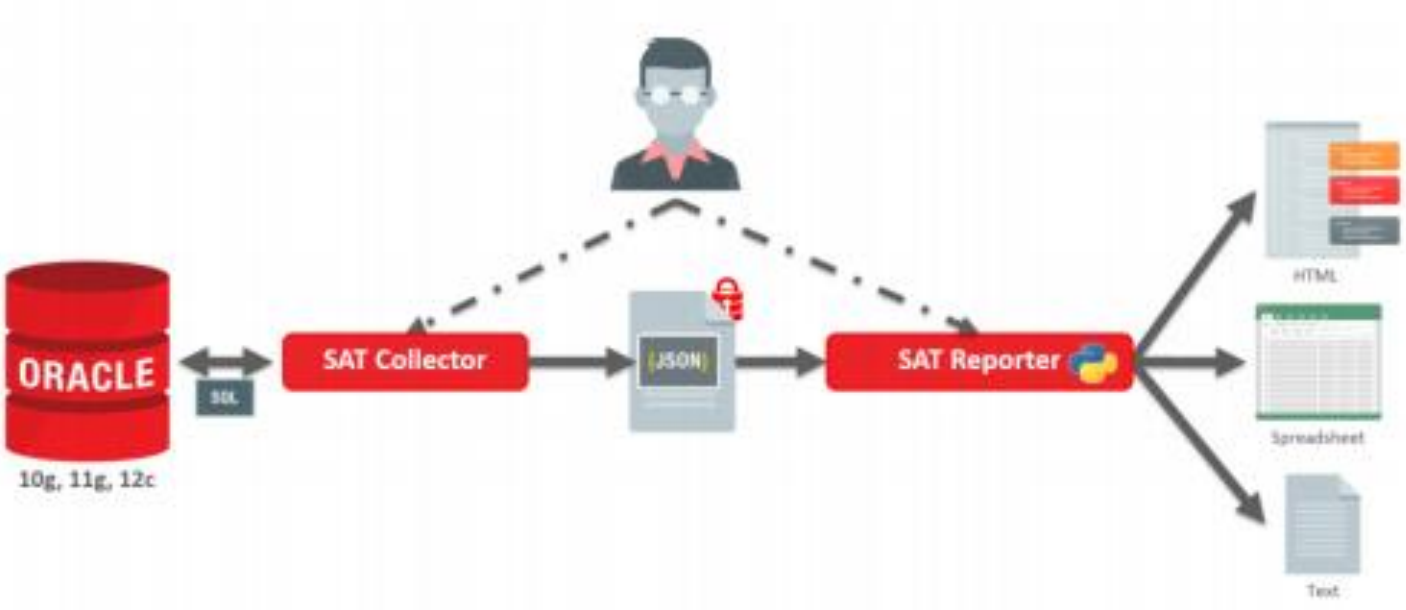
The Oracle DB Security Assessment Tool (DBSAT)

Components

- Collector
    1. Executes SQL
    2. Executes OS Command
    3. Collect Data from System
- Reporter
    1. Analyze collected data from collector
    2. Report findings and recommendations

The Oracle DB Security Assessment Tool (DBSAT)

** From Oracle Database Security and Assessment Tool Tutorial, Oracle Corporation



The Oracle DB Security Assessment Tool (DBSAT)

DBSAT will not create any objects in the database.

DBSAT only executes queries similar to the ones a normal DBA would execute under normal checks and investigations.

Setup and Installation

Database User Privileges Needed for Collector

- CREATE SESSION
- SELECT on SYS.REGISTRY$HISTORY
- Role SELECT_CATALOG_ROLE
- Role DV_SECANALYST (if Database Vault is enabled)
- Role AUDIT_VIEWER (12c only)
- Role CAPTURE_ADMIN (12c only)
- SELECT on SYS.DBA_USERS_WITH_DEFPWD (11g and 12c)
- SELECT on AUDSYS.AUD$UNIFIED (12c only)

Setup and Installation

Example of User:

- create user dbsat identified by myoraclepassord#1 ;
- grant create session to dbsat;
- grant select on sys.registry$history to dbsat;
- grant select_catalog_role to dbsat;
- grant audit_viewer to dbsat;
- grant capture_admin to dbsat;
- grant select on sys.dba_users_with_defpwd to dbsat;
- grant select on audsys.aud$unified to dbsat;

Setup and Installation

Download the Oracle Database Security Assessment Tool (DBSAT) and place download zip file on the server for installation.

http://www.oracle.com/technetwork/database/security/dbsat.html

Setup and Installation

Place the DBSAT utility on the server in a standard location and unzip.

** Note your environment may vary

cd /u01/app/oracle

mkdir dbsat

mv dbsat.zip /u01/app/oracle/dbsat

cd /u01/app/oracle/dbsat

unzip dbsat.zip

Running the DBSAT Collector

DSTAT Collector Execution

dbstat collect username/password@connect_string outputfile

Example:

cd /u01/app/oracle/dbsat

./dbsat collect dbsat/myoraclepassword#1@mydb dbstat_collect_20181031

** Collector will prompt for password to protect the .zip created will need this when running reporter process

Running the DBSAT Collector

Upon completion of dbsat collector execution the output file name provided with a .zip extension is created in the location where executed from.

Example:

cd /u01/app/oracle/dbsat

ls -l dbstat_collect_20181031.zip

Running the DBSAT Reporter

Execute the reporter process for the generated collector file from collector execution

Example:

cd /u01/app/oracle/dbsat

./dbsat report dbstat_collect_20181031

** will prompt for password used when executing collector to protect zip

Running the DBSAT Reporter

Reporter execution will create a report zip file matching the output name specified in the collector adding _report to the filename for the final zip file.

Example:

cd /u01/app/oracle/dbsat

ls -l dbstat_collect_20181031_report.zip

Examining the Reporter Output

To examine the Reporter output we unzip the reporter zip file created by the reporter execution

Example:

cd /u01/app/oracle/dbsat

unzip dbstat_collect_20181031_report.zip

Examining the Reporter Output

Files Example:

- dbstat_collect_20181031.xlsx
- dbstat_collect_20181031.html
- dbstat_collect_20181031.txt

After unzipping the .zip file created by the reporter you will have 3 files of type xlsx, html and txt. These files should be readable by the appropriate program mating their extension for example .xlsx would be MS Excel or compatible spreadsheet program that can read MS Excel Spreadsheet files, .html from any web browser and .txt from any text editor utility like notepad, notepad++, vi, etc.

Analyze the Reporter Output

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	1	0	0	0	0	0	**1**
User Accounts	4	0	0	5	1	0	**10**
Privileges and Roles	4	14	0	1	0	0	**19**
Authorization Control	0	0	2	0	0	0	**2**
Data Encryption	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	1	4	0	0	0	**5**
Auditing	4	5	1	0	2	0	**12**
Database Configuration	5	3	0	1	2	1	**12**
Network Configuration	0	0	0	1	2	0	**3**
Operating System	1	1	0	2	1	0	**5**
Total	**19**	**25**	**8**	**10**	**8**	**1**	**71**

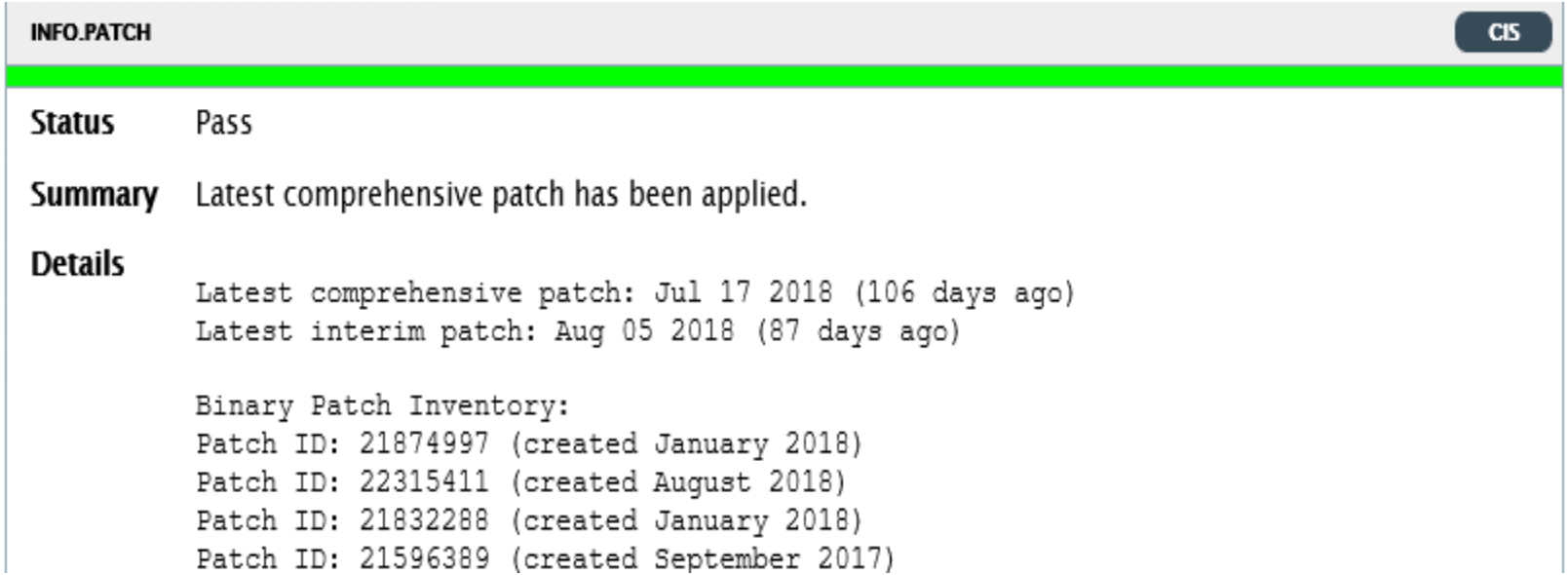
Analyze the Reporter Output

Security Features

Feature	Currently Used
AUTHORIZATION CONTROL	
Database Vault	No
Privilege Analysis	No
DATA ENCRYPTION	
Column Encryption	No
Tablespace Encryption	No
Network Encryption	Yes
FINE-GRAINED ACCESS CONTROL	
Data Redaction	No
Virtual Private Database	Yes
Real Application Security	No
Label Security	No

Analyze the Reporter Output

Patching Check



Analyze the Reporter Output

Check Users

- Check System Permissions
- Check Role Permissions

Check Roles

- Check System Permissions
- Check Object Grants

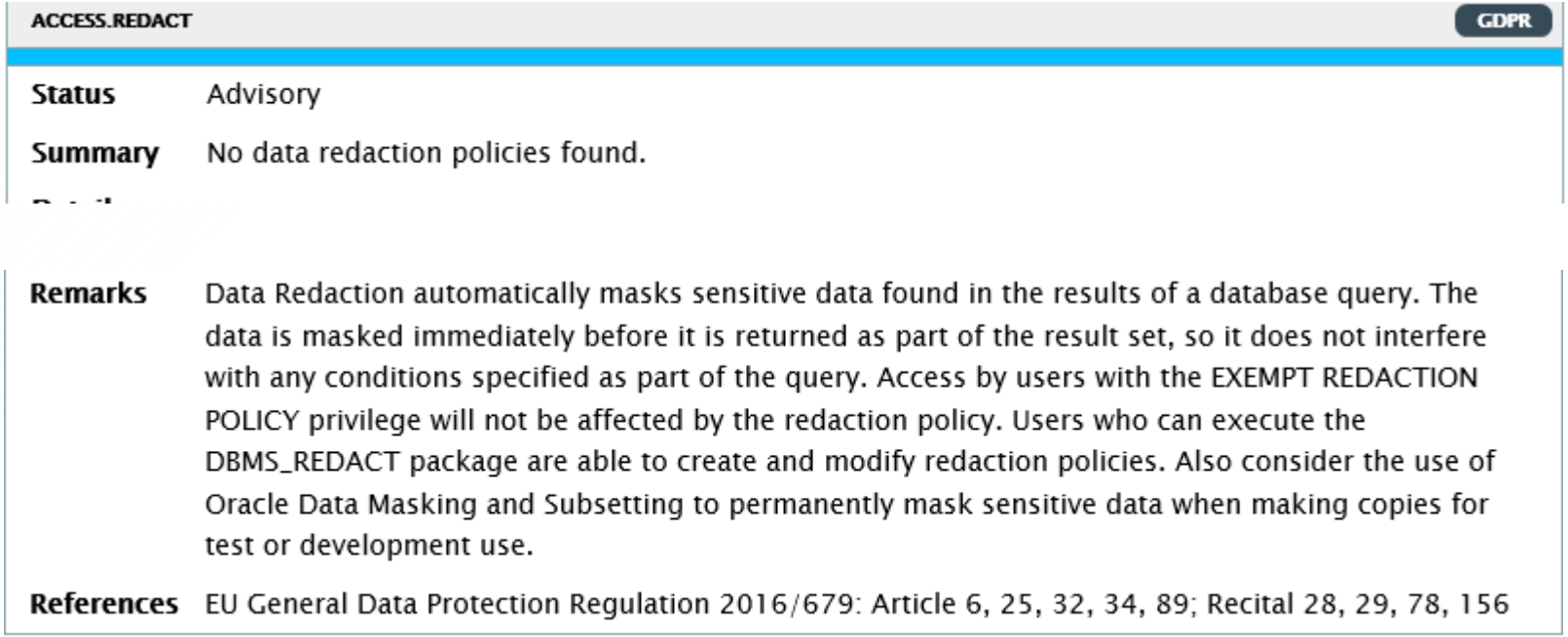
Check Profiles

- Password lifetime
- Password verify rules

Check Privileges to PUBLIC

Analyze the Reporter Output

Data Redaction



ACCESS.REDACT GDPR

Status	Advisory
Summary	No data redaction policies found.
Remarks	Data Redaction automatically masks sensitive data found in the results of a database query. The data is masked immediately before it is returned as part of the result set, so it does not interfere with any conditions specified as part of the query. Access by users with the EXEMPT REDACTION POLICY privilege will not be affected by the redaction policy. Users who can execute the DBMS_REDACT package are able to create and modify redaction policies. Also consider the use of Oracle Data Masking and Subsetting to permanently mask sensitive data when making copies for test or development use.
References	EU General Data Protection Regulation 2016/679: Article 6, 25, 32, 34, 89; Recital 28, 29, 78, 156

DBSAT Discover

Discover is a tool that will allow the table and columns to be examined for sensitive data. This is a secondary tool to the DB Security Assessment Tool, but powerful in determining if there is possible identifiable data that needs protection.

DBSAT Discover

Find the possible Sensitive Data in your Database

Discover requires Java 1.8 or above, make sure you have this installed on the server

Configure the Discover for each database

Example:

cd /u01/app/oracle/dbsat/Discover/conf

cp sample_dbsat.config <dbname>_dbsat.config

vi <dbname>_dbsat.config

DBSAT Discover

Set the parameters in the <dbname>_dbsat.config

DB_HOSTNAME = <host for database> ** Listener host

DB_PORT = 1521 ** Listener port

DB_SERVICE_NAME = <db service name> ** Service name as registered with the listener

** Then save the file

DBSAT Discover

Customize the filters that locate schemas, tables and columns that potentially have Sensitive data.

cd /u01/app/oracle/dbsat/Discover/conf

sensitive_en.ini

** Update this file for new patterns or changes to existing patterns used to locate tables and columns in schemas with potential sensitive data.

DBSAT Discover

Ready to Run the Discover

Example:

cd /u01/app/oracle/dbsat

export JAVA_HOME=/ggs/jdk

./dbsat discover -c /u01/app/oracle/dbsat/Discover/conf/avdev_dbsat.config dbsat_discover_20181101

DBSAT Discover

```
Database Security Assessment Tool version 2.0.2 (May 2018)

This tool is intended to assist in you in securing your Oracle database
system. You are solely responsible for your system and the effect and
results of the execution of this tool (including, without limitation,
any damage or data loss). Further, the output generated by this tool may
include potentially sensitive system configuration data and information
that could be used by a skilled attacker to penetrate your system. You
are solely responsible for ensuring that the output of this tool,
including any generated reports, is handled in accordance with your
company's policies.

Enter username: dbsat
Enter password:
DBSAT Discover ran successfully.
Calling /usr/bin/zip to encrypt the generated reports...

Enter password:
Verify password:
        zip warning: dbsat_discover_20181101_report.zip not found or empty
  adding: dbsat_discover_20181101_discover.html (deflated 93%)
  adding: dbsat_discover_20181101_discover.csv (deflated 90%)
Zip completed successfully
```

Extract the Discover Output

Discover execution create zip fie as formatted based on output parameter.

Example:

dbsat_discover_20181101_report.zip

unzip dbsat_discover_20181101_report.zip

Open html with browser: dbsat_discover_20181101_discover.html

Analyze the Discover Output

Data Check Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
FINANCIAL DATA – BANKING	6	18	2684
FINANCIAL DATA – PCI	125	220	100864355
HEALTH DATA	394	913	66306197
JOB DATA	64	72	1886244
PII	168	450	28276288
PII – ADDRESS	111	391	103187097
PII – IDS	100	150	26222727
PII – IT DATA	227	384	37234129
PII–LINKED	24	35	1006959
PII–LINKED – BIRTH DETAILS	63	80	2388436
TOTAL	**886***	**2713**	**308684182****

Analyze Discover Output

Schemas with Sensitive Data identified

Tables Detected within Sensitive Category: FINANCIAL DATA - PCI

Tables Detected within Sensitive Category: PII

Tables Detected within Sensitive Category: PII - ADDRESS

Tables Detected within Sensitive Category: PII - IDS

Tables Detected within Sensitive Category: PII - IT DATA

Analyze Discover Output

Tables Detected within Sensitive Category: FINANCIAL DATA - BANKING

Tables Detected within Sensitive Category: HEALTH DATA

Tables Detected within Sensitive Category: JOB DATA

Tables Detected within Sensitive Category: PII-LINKED

Tables Detected within Sensitive Category: PII-LINKED - BIRTH DETAILS

Take Action

We all Must do our part to secure our data for the benefit of our organization, but also our customers who are counting on us to protect their information. We have a responsibility.

ROLTA | ADVIZEX

THANK YOU