ORACLE®

October 22–25, 2018

SAN FRANCISCO, CA

#OOW18

ORACLE
OPEN
WORLD

oracle.com/openworld

ORACLE

ORACLE
OPEN
WORLD

Oracle Database Security Assessment Tool

Know Your Security Posture Before Hackers Do [TRN4107]

Pedro Lopes
DBSAT and EMEA Field Product Manager
Oracle Database Security

Riccardo D'Agostini
Data Security Design Manager
Intesa Sanpaolo Bank

ORACLE

Data – Your Most Valuable Asset

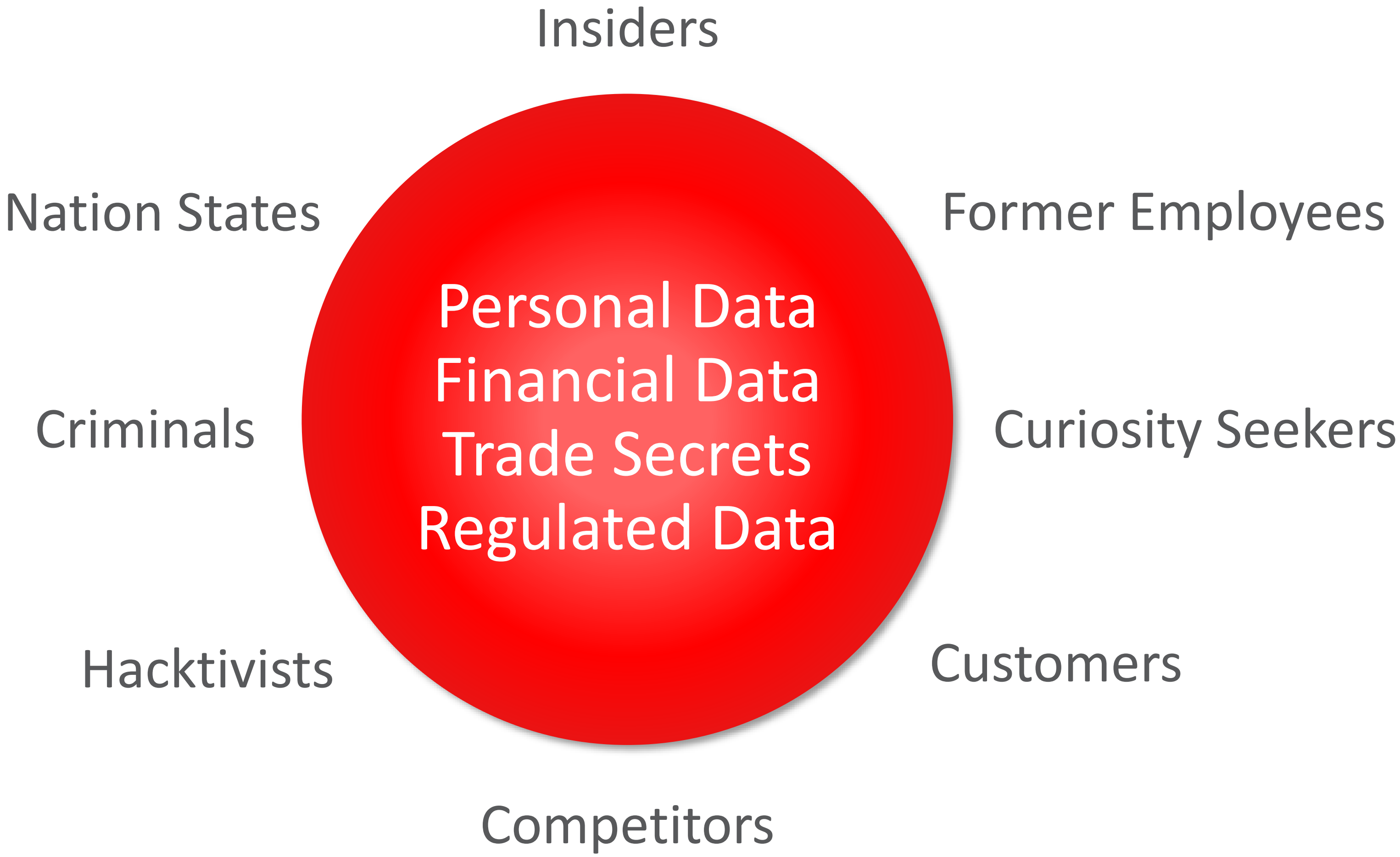
Driver’s License Number, Passport Number, Tax Payer ID, Health Insurance Numbers, ...

Credit/Debit Card Number,
Security Code, SSN, Age, Names, DOB, ...

Evolving Regulatory Landscape

- EU General Data Protection Regulation (EU GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley (SOX)
- HIPAA/HITECH
- Numerous breach notification laws

Who Wants Your Data?



Insiders

Nation States

Former Employees

Personal Data
Financial Data
Trade Secrets
Regulated Data

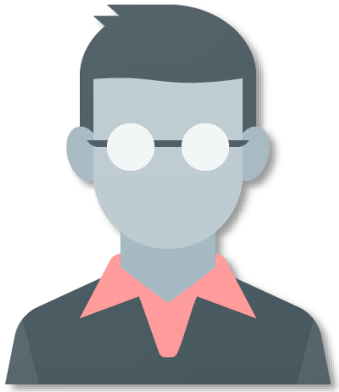
Criminals

Curiosity Seekers

Hacktivists

Customers

Competitors

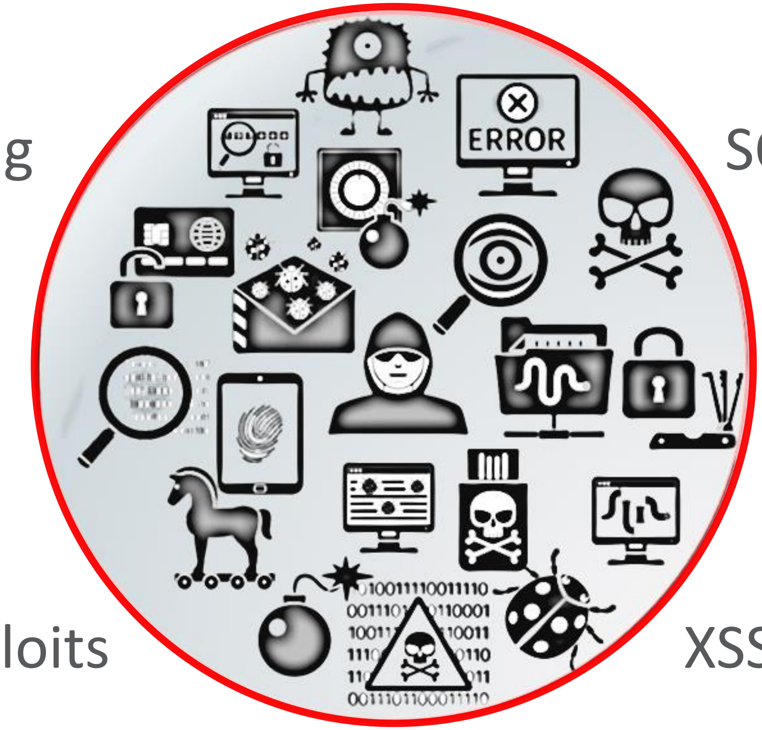


Evolving Attack Tools and Techniques

Stolen Credentials

Phishing

SQL Injection



Buffer Overflow

Privilege Escalation

App Exploits

XSS Attacks

Unpatched Systems

Think Alike

Attacker vs Owner of the Data

Insider / Outsider

Open Ports
Database SIDs
Known Users
Common Passwords
Encrypted Data
Auditing On
Privileged Users
Database Version
Known Vulnerabilities
Known Packaged Apps

Where To Start & What to look for

Where does sensitive data reside?
Who are the users and their entitlements?
What controls do I have in place?
Is my Database securely configured?

Do we have a Database Security Team? Knowledge?
Analysis time?

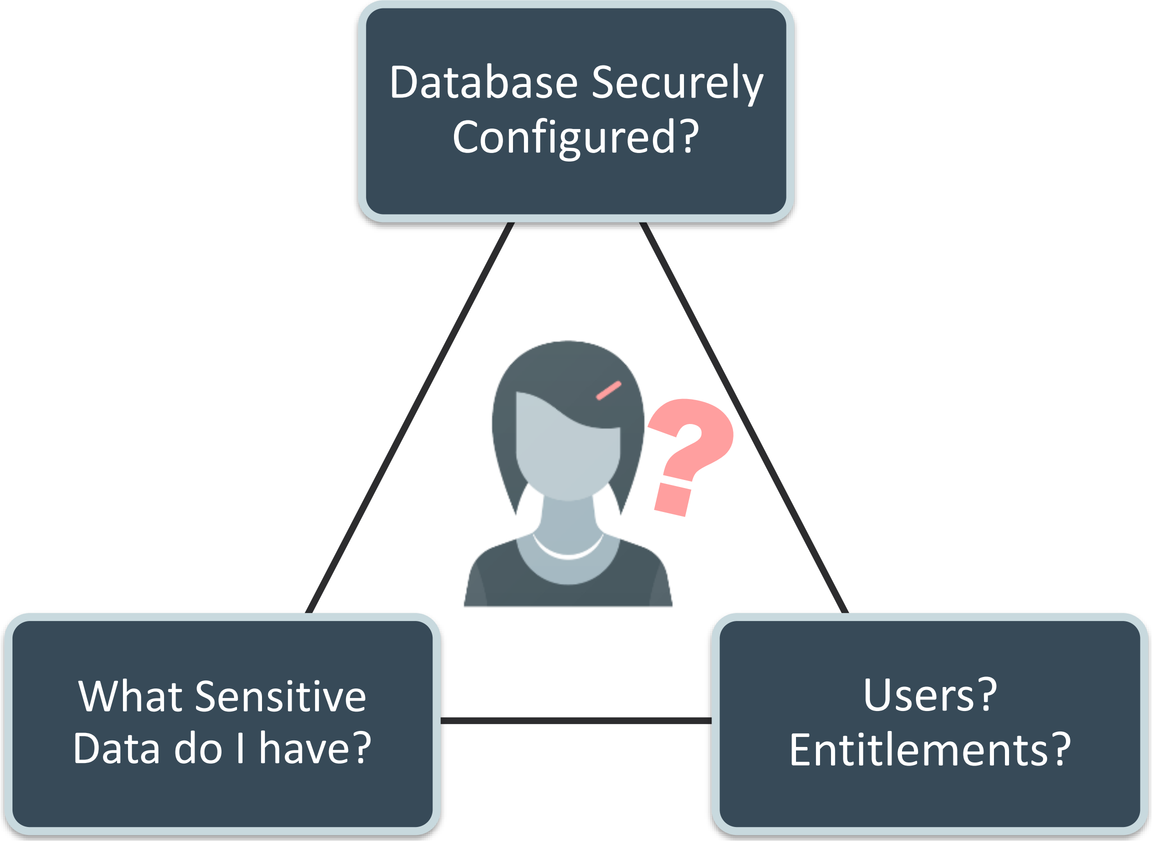
Introducing

Oracle Database Security Assessment Tool

Oracle Database Security Assessment Tool (DBSAT)

Know Your Security Posture Before Hackers Do

- Understand how (in)secure your database is
  - Report on overall security status
  - Find the users, entitlements, and risks
  - Discover sensitive data
- Actionable Assessment Reports
  - Summary and detailed information
  - Prioritized recommendations
  - Mapping to **EU GDPR** and CIS Benchmark
- Stand-alone light weight tool: Quick, Easy
- **FREE** to current Oracle customers



Database Securely Configured?

What Sensitive Data do I have?

Users? Entitlements?

What does DBSAT Check?

1. **Security Configuration**
   - Data Encryption
   - Auditing Policies
   - Fine-grained Access Control
   - Database and Listener Configuration
   - OS File permissions
   - Security Patches
2. **Users and Entitlements**
   - User Accounts, Privileges and Roles
3. **Sensitive Data**
   - Which type, where, how many

For Oracle Databases
10g and later

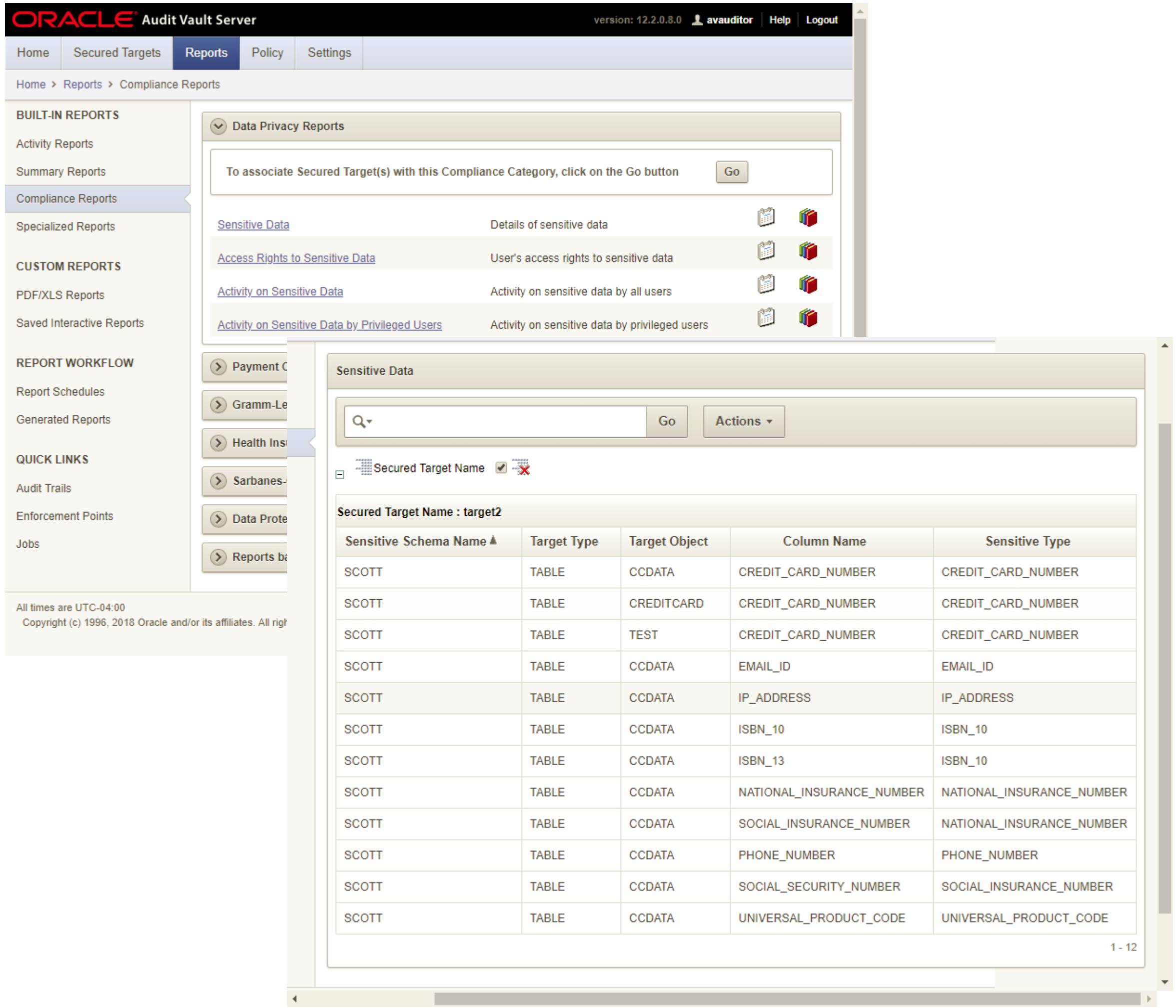
2.0.1 DBSAT New Features

- References to CIS Benchmark recommendations
- References to GDPR Articles/Recitals
- JSON output for integration with other tools
- Introduced Sensitive Data Discovery
  - English pattern file included out of the box
  - Customizable

2.0.2 DBSAT New Features

Introduced in July

- Support for Discoverer to Connect to Database servers over SSL channel
- Discover Sensitive Data in Exadata Express CS and ADW
- Discovered Sensitive Data columns can be imported into AVDF to power new Data Privacy Reports



To associate Secured Target(s) with this Compliance Category, click on the Go button

Sensitive Data	Details of sensitive data
Access Rights to Sensitive Data	User's access rights to sensitive data
Activity on Sensitive Data	Activity on sensitive data by all users
Activity on Sensitive Data by Privileged Users	Activity on sensitive data by privileged users

All times are UTC-04:00
Copyright (c) 1996, 2018 Oracle and/or its affiliates. All righ

Secured Target Name : target2

Sensitive Schema Name ▲	Target Type	Target Object	Column Name	Sensitive Type
SCOTT	TABLE	CCDATA	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	CREDITCARD	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	TEST	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	CCDATA	EMAIL_ID	EMAIL_ID
SCOTT	TABLE	CCDATA	IP_ADDRESS	IP_ADDRESS
SCOTT	TABLE	CCDATA	ISBN_10	ISBN_10
SCOTT	TABLE	CCDATA	ISBN_13	ISBN_10
SCOTT	TABLE	CCDATA	NATIONAL_INSURANCE_NUMBER	NATIONAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	SOCIAL_INSURANCE_NUMBER	NATIONAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	PHONE_NUMBER	PHONE_NUMBER
SCOTT	TABLE	CCDATA	SOCIAL_SECURITY_NUMBER	SOCIAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	UNIVERSAL_PRODUCT_CODE	UNIVERSAL_PRODUCT_CODE

1 - 12

ORACLE

NEW

Upcoming DBSAT version (2.0.3)

- STIG rules highlighting
- New findings on password file, global names, instance name RMAN backups and more
- Simplify identification of directly granted System Privileges.
  - Now marked with (**<-**)

- Now includes sensitive pattern files for German, Dutch, French , Spanish, Italian and Portuguese
- New Sensitive Types, Categories and Subcategories
- Sensitive Data Categories now grouped by Risk Level
- Report include remarks and recommended controls for different Risk Levels

ORACLE

How does it work?

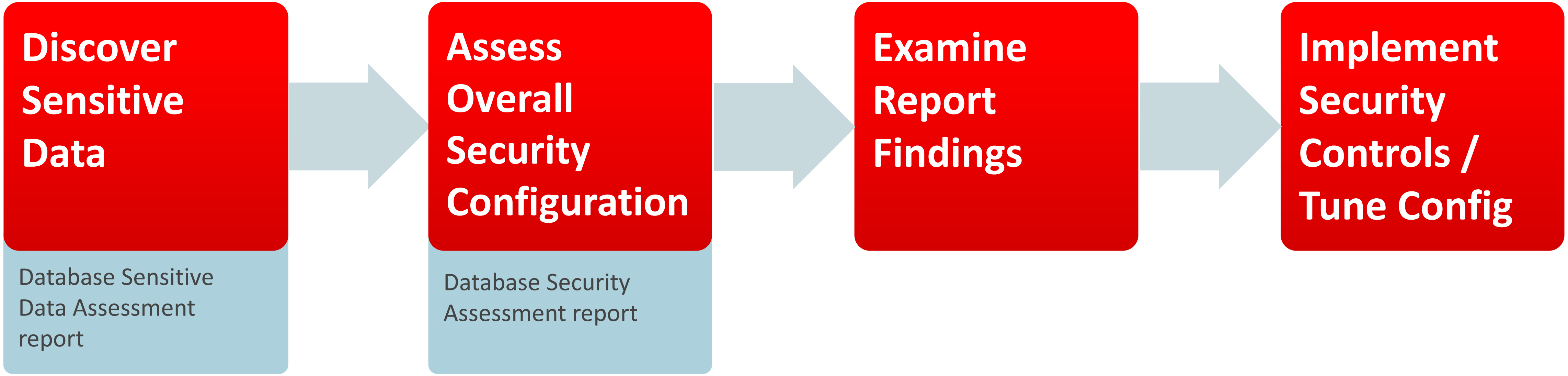
Oracle Database Security Assessment Tool

Easy as Download and count to 3!

1. Download
   https://www.oracle.com/database/technologies/security/dbsat.html
2. To get a Database **Security Assessment** report
   - Execute DBSAT Collector
   - Execute DBSAT Reporter
3. To get a Database **Sensitive Data Assessment** report
   - Execute DBSAT Discoverer

E.g. Assessment Flow Steps for Data Privacy initiative

From Discovery to Recommendations



Discover Sensitive Data

Database Sensitive Data Assessment report

Assess Overall Security Configuration

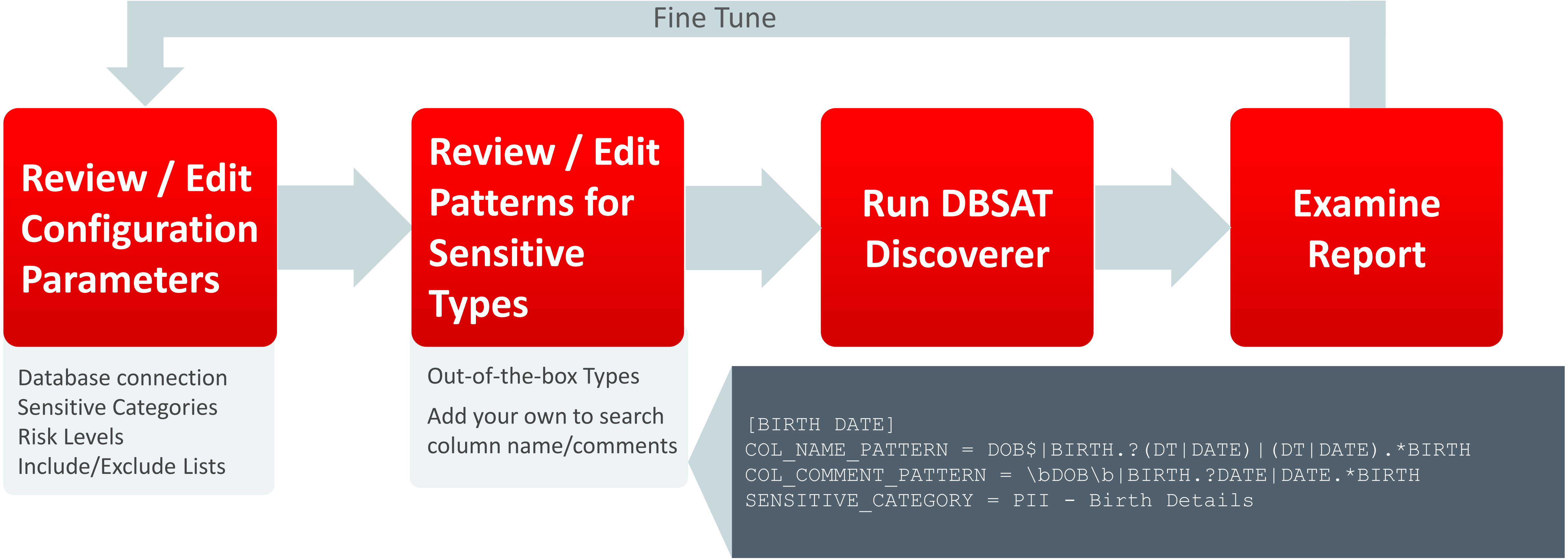
Database Security Assessment report

Examine Report Findings

Implement Security Controls / Tune Config

Discover Sensitive Data

Find What You Have, Where, How Much


Fine Tune
Review / Edit Configuration Parameters
Review / Edit Patterns for Sensitive Types
Run DBSAT Discoverer
Examine Report

Database connection
Sensitive Categories
Risk Levels
Include/Exclude Lists

Out-of-the-box Types

Add your own to search column name/comments

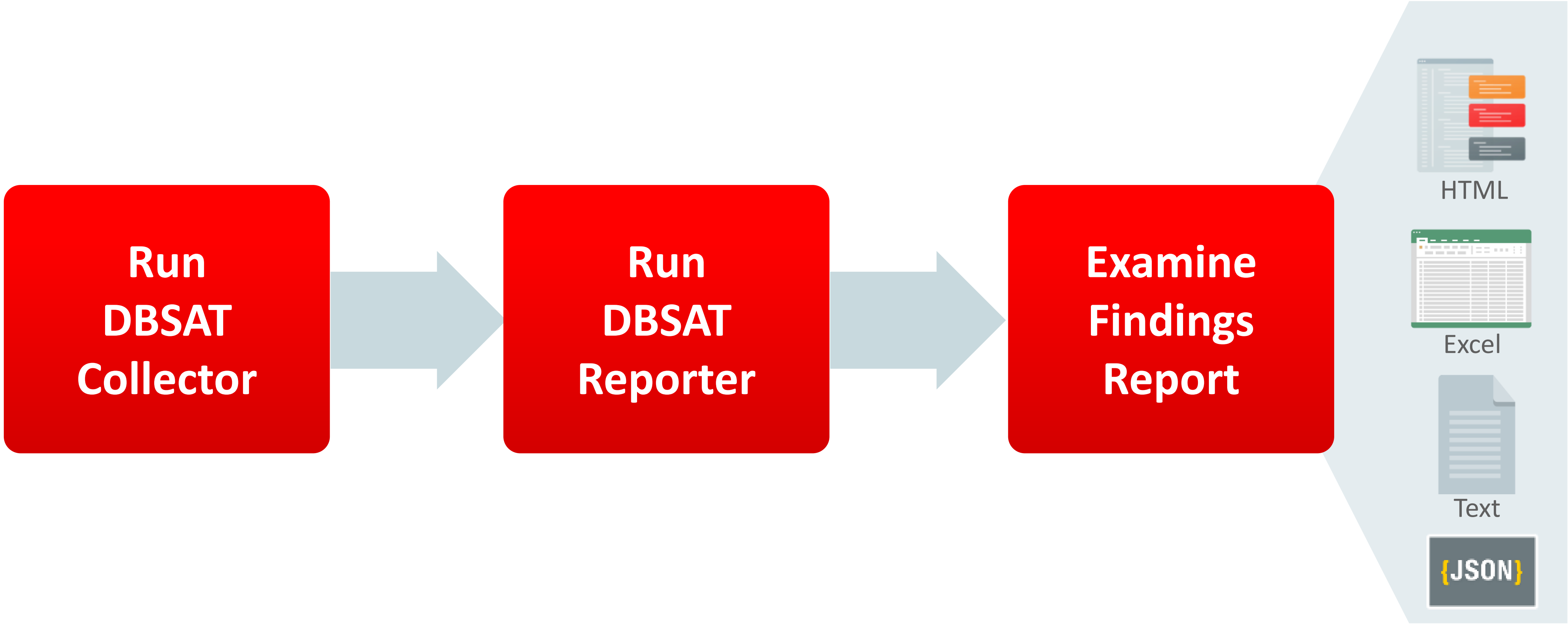
```
[BIRTH DATE]
COL_NAME_PATTERN = DOB$|BIRTH.?(DT|DATE)|(DT|DATE).*BIRTH
COL_COMMENT_PATTERN = \bDOB\b|BIRTH.?DATE|DATE.*BIRTH
SENSITIVE_CATEGORY = PII - Birth Details
```

Demonstration

DBSAT Sensitive Data Discovery Report

Database Security Assessment Report

Security Configuration Status, Users and their Entitlements



Anatomy of a Finding

Can be Evaluate, Advisory, Pass, Low Risk, Medium Risk, High Risk

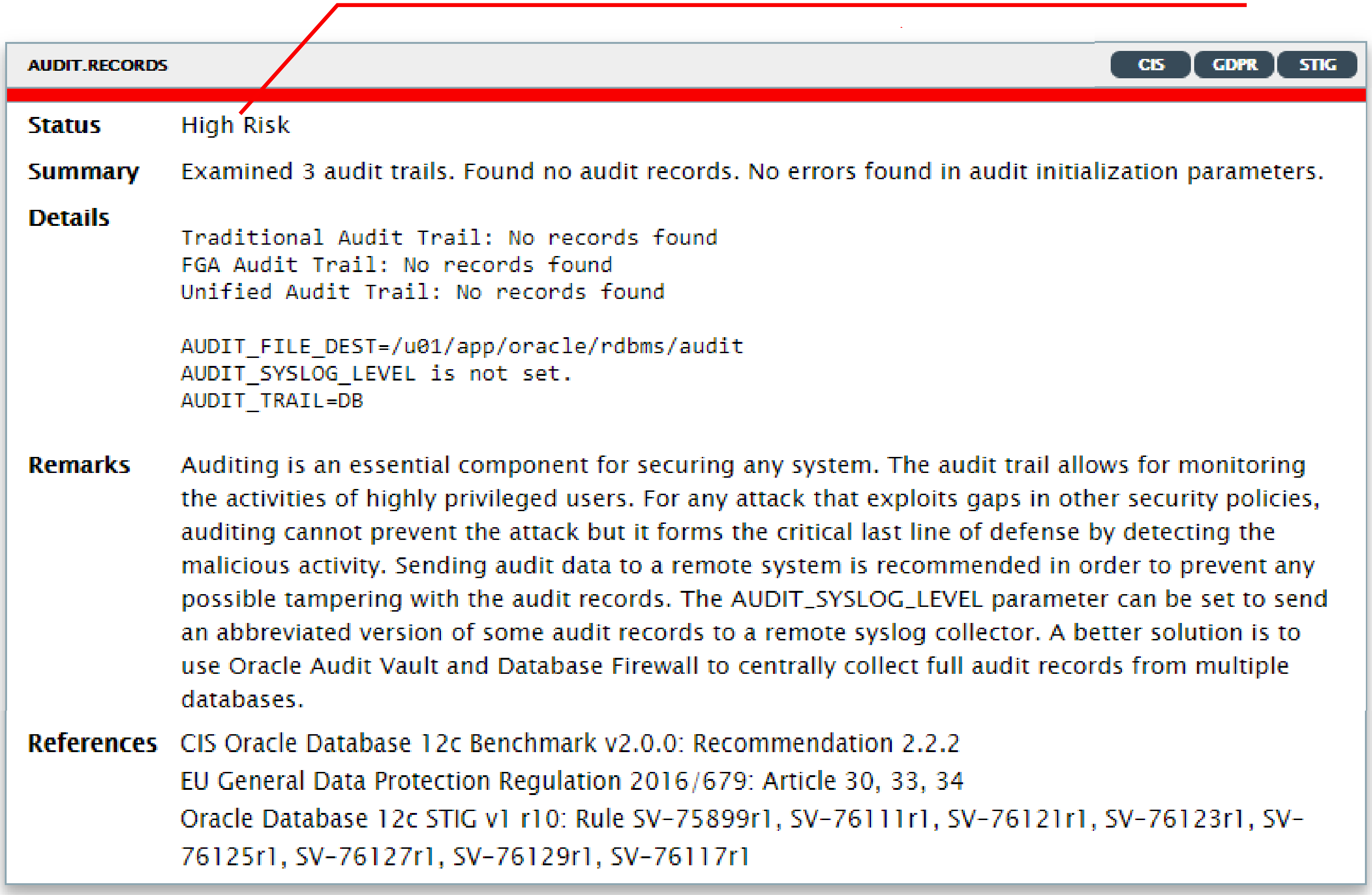
Category of the Finding

Applicability to Regulations

Details of the Finding

Rationale and Recommendations

Mapping to Regulations



Status High Risk

Summary Examined 3 audit trails. Found no audit records. No errors found in audit initialization parameters.

Details

```
Traditional Audit Trail: No records found
FGA Audit Trail: No records found
Unified Audit Trail: No records found

AUDIT_FILE_DEST=/u01/app/oracle/rdbms/audit
AUDIT_SYSLOG_LEVEL is not set.
AUDIT_TRAIL=DB
```

Remarks Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT_SYSLOG_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.

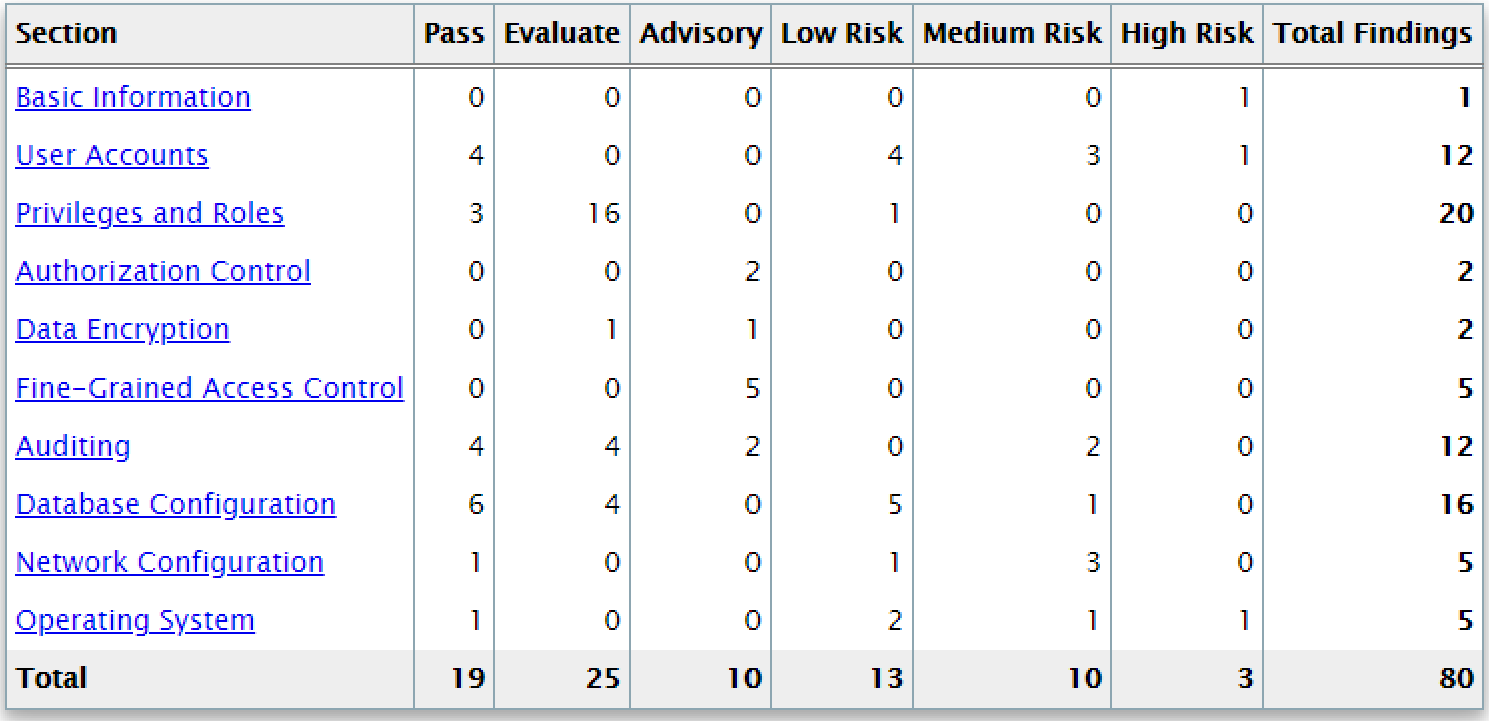
References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.2
EU General Data Protection Regulation 2016/679: Article 30, 33, 34
Oracle Database 12c STIG v1 r10: Rule SV-75899r1, SV-76111r1, SV-76121r1, SV-76123r1, SV-76125r1, SV-76127r1, SV-76129r1, SV-76117r1

Demonstration

DBSAT Security Assessment Report

Use Case: Is the Database Securely Configured?

Summary Output with Prioritized Findings

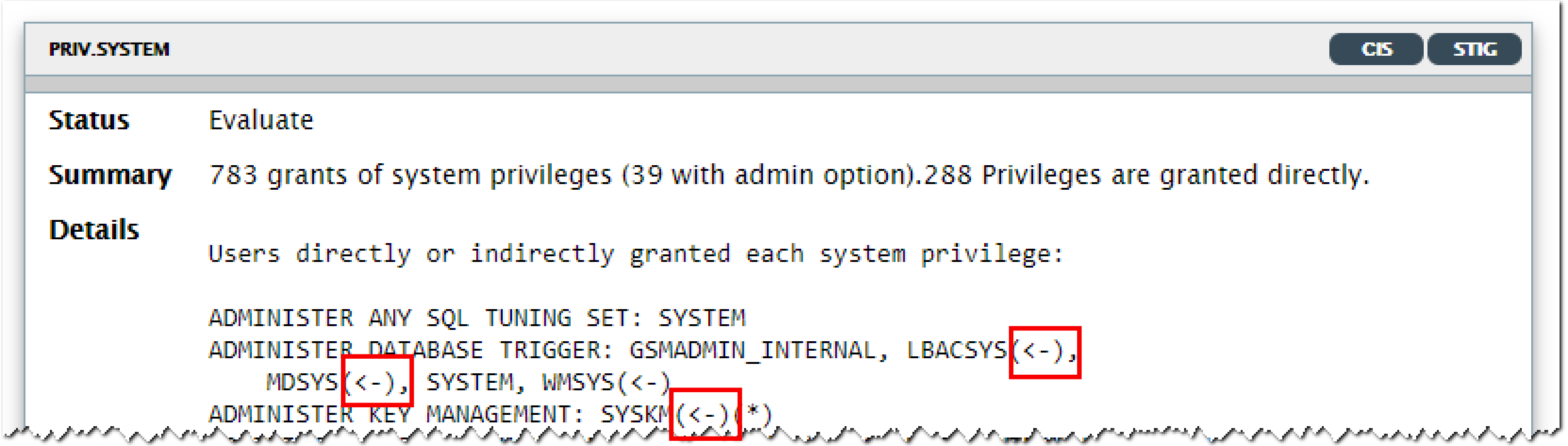


Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	**1**
User Accounts	4	0	0	4	3	1	**12**
Privileges and Roles	3	16	0	1	0	0	**20**
Authorization Control	0	0	2	0	0	0	**2**
Data Encryption	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	0	5	0	0	0	**5**
Auditing	4	4	2	0	2	0	**12**
Database Configuration	6	4	0	5	1	0	**16**
Network Configuration	1	0	0	1	3	0	**5**
Operating System	1	0	0	2	1	1	**5**
Total	**19**	**25**	**10**	**13**	**10**	**3**	**80**

NEW

Use Case: Users and Their Entitlements?

Directly Granted System Privileges



Status Evaluate

Summary 783 grants of system privileges (39 with admin option).288 Privileges are granted directly.

Details

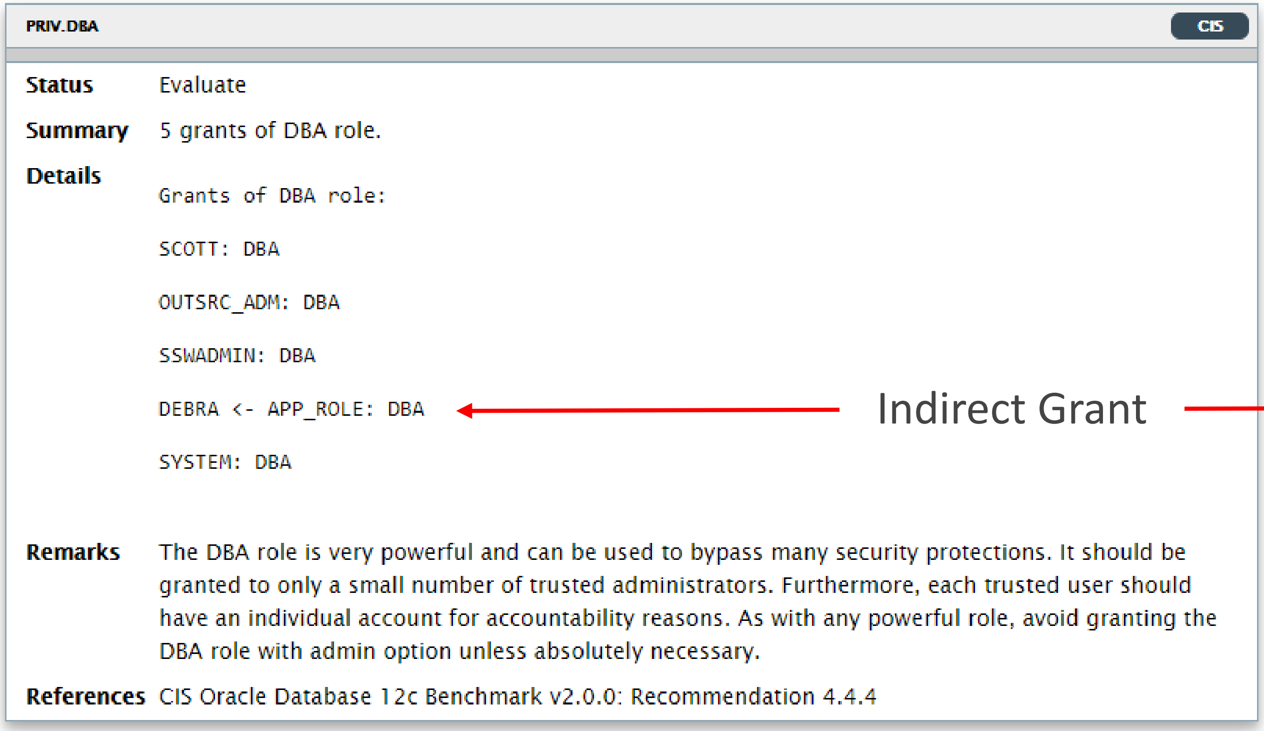
```
Users directly or indirectly granted each system privilege:

ADMINISTER ANY SQL TUNING SET: SYSTEM
ADMINISTER DATABASE TRIGGER: GSMADMIN_INTERNAL, LBACSYS(<-),
    MDSYS(<-), SYSTEM, WMSYS(<-)
ADMINISTER KEY MANAGEMENT: SYSKM(<-)(*)
```

Use Case: Users and Their Entitlements?

Users with DBA Role Granted Directly and Indirectly

DBA Role



PRIV.DBA

CIS

Status Evaluate

Summary 5 grants of DBA role.

Details

```
Grants of DBA role:

SCOTT: DBA

OUTSRC_ADM: DBA

SSWADMIN: DBA

DEBRA <- APP_ROLE: DBA

SYSTEM: DBA
```

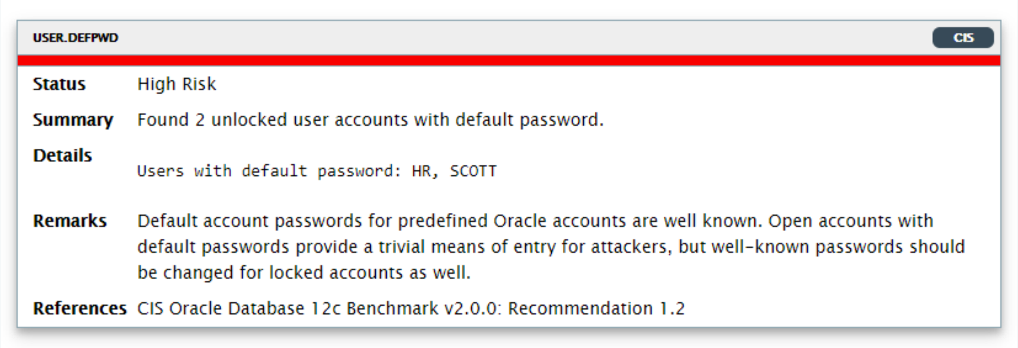
Indirect Grant

Remarks The DBA role is very powerful and can be used to bypass many security protections. It should be granted to only a small number of trusted administrators. Furthermore, each trusted user should have an individual account for accountability reasons. As with any powerful role, avoid granting the DBA role with admin option unless absolutely necessary.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 4.4.4

User DEBRA got the DBA role indirectly via the role APP_ROLE

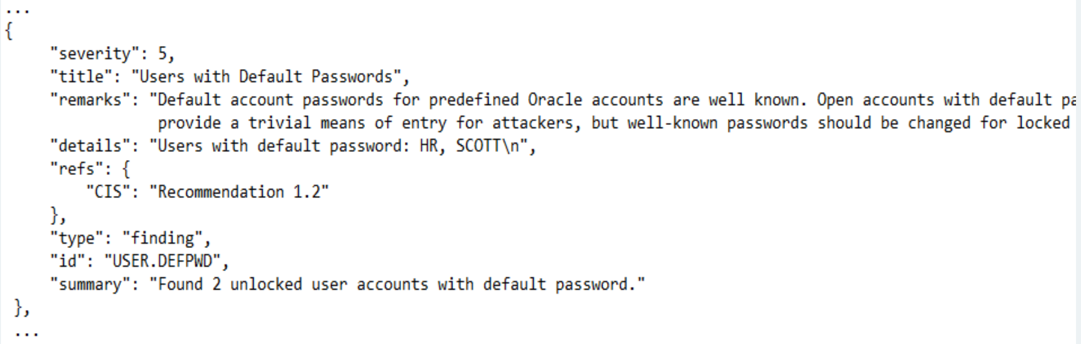
Report in Multiple Formats



USER.DEFPWD

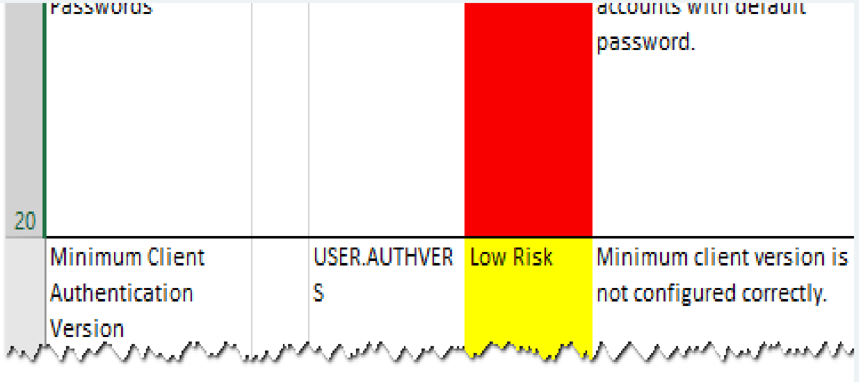
Status	High Risk
Summary	Found 2 unlocked user accounts with default password.
Details	`Users with default password: HR, SCOTT`
Remarks	Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2

HTML



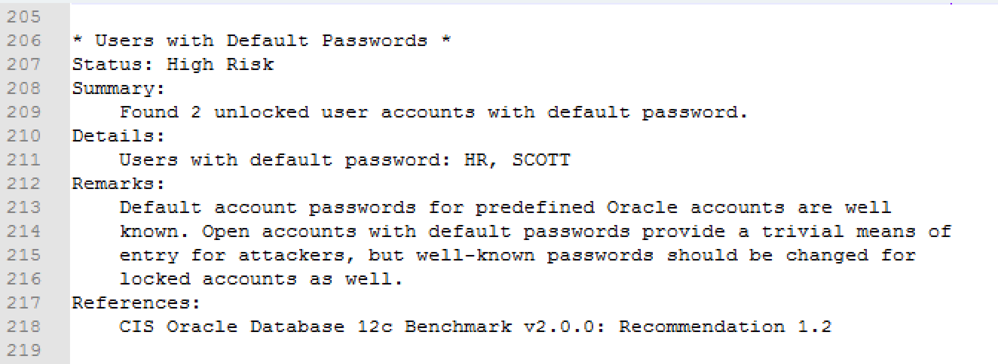
```
...
{
    "severity": 5,
    "title": "Users with Default Passwords",
    "remarks": "Default account passwords for predefined Oracle accounts are well known. Open accounts with default pa
              provide a trivial means of entry for attackers, but well-known passwords should be changed for locked
    "details": "Users with default password: HR, SCOTT\n",
    "refs": {
        "CIS": "Recommendation 1.2"
    },
    "type": "finding",
    "id": "USER.DEFPWD",
    "summary": "Found 2 unlocked user accounts with default password."
 },
 ...
```

JSON



20	Passwords				accounts with default password.
	Minimum Client Authentication Version		USER.AUTHVERS	Low Risk	Minimum client version is not configured correctly.

Spreadsheet



```

* Users with Default Passwords *
Status: High Risk
Summary:
    Found 2 unlocked user accounts with default password.
Details:
    Users with default password: HR, SCOTT
Remarks:
    Default account passwords for predefined Oracle accounts are well
    known. Open accounts with default passwords provide a trivial means of
    entry for attackers, but well-known passwords should be changed for
    locked accounts as well.
References:
    CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2

```

Text

Start Today!
Your attackers have already started!

Easy to Install and Run

- Download DBSAT 2.0.2 today from http://www.oracle.com/technetwork/database/security/dbsat.html
  - **DBSAT** 2.0.3 (STIG highlights, new rules, and new Sensitive Types) soon
  - Available to all Oracle database customers with active support contract

- Collect security config data by running ‘dbsat collect’ on the target
- Run ‘dbsat report’ on the target or elsewhere
- Run ‘dbsat discover’ on the target to generate sensitive data report
- Restrict access to the generated reports as they have sensitive data

Where To Start & What to look for

Where does sensitive data reside?
Who are the users and their entitlements?
What controls do I have in place?
Is my Database securely configured?

Do we have a Database Security Team? Knowledge?
Analysis time?

Summary

- Quickly assess the current security status of database before hackers do
- Identify sensitive data to determine risk and appropriate security controls
- Reduce risk exposure using proven best practices
- Accelerate compliance with EU GDPR and other regulations
- Support Oracle Database 10g, 11g, 12c and 18c
- Provided at no additional cost
- Quick to deploy and use

ORACLE

INTESA SANPAOLO

How to Leverage Oracle Database Security Assessment Tool on a regulatory compliace initiative (GDPR)

Riccardo D'Agostini
Data Security Design Manager
Intesa Sanpaolo Bank

Intesa Sanpaolo

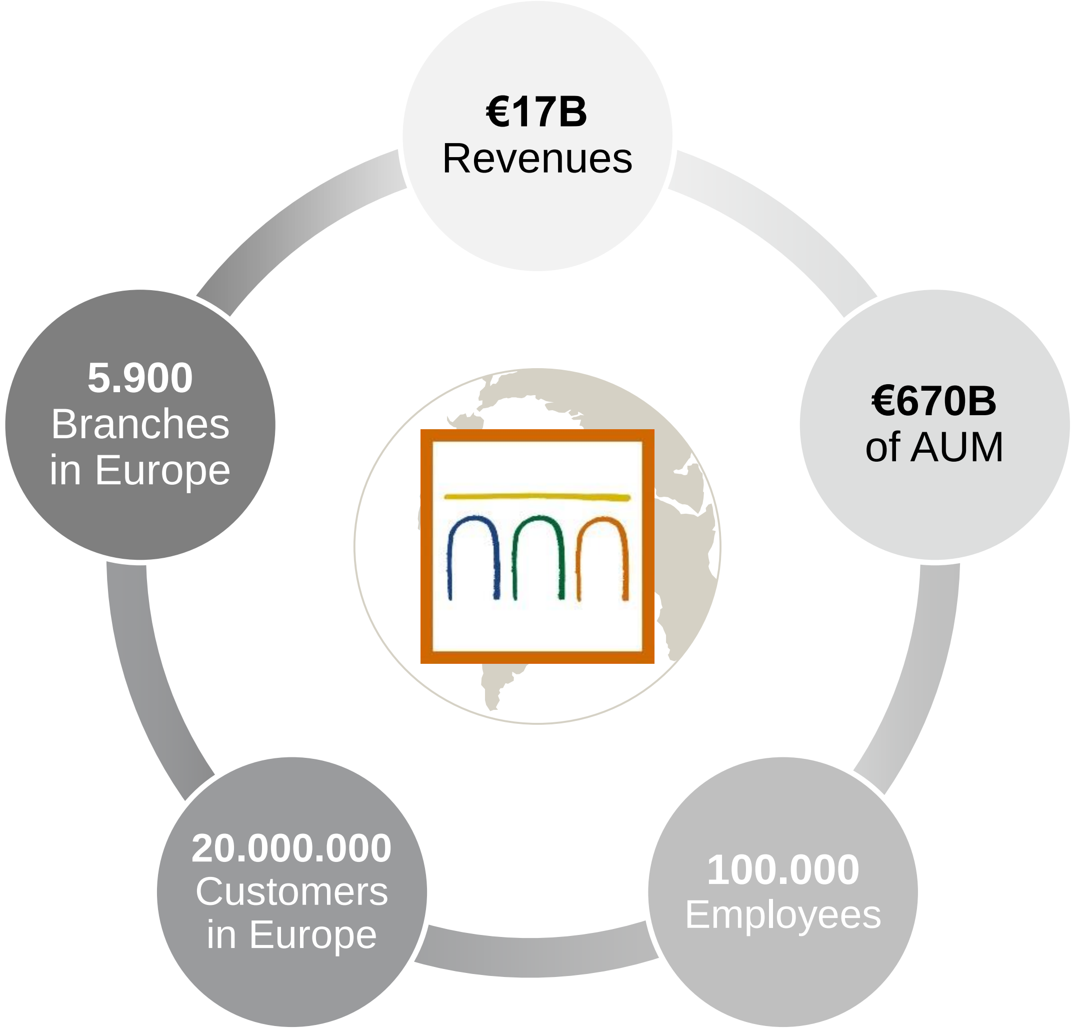
CORPORATE OVERVIEW

Intesa Sanpaolo is the major Italian Bank also operating in many Countries of Eastern Europe

CYBERSECURITY ORGANIZATION

~250 professionals

- Cyber Security Operations
- Cyber Security Governance
- Cyber Security projects delivery



€17B Revenues

€670B of AUM

100.000 Employees

20.000.000 Customers in Europe

5.900 Branches in Europe

ORACLE

Intesa Sanpaolo

CORPORATE CHALLENGES

Digitalization

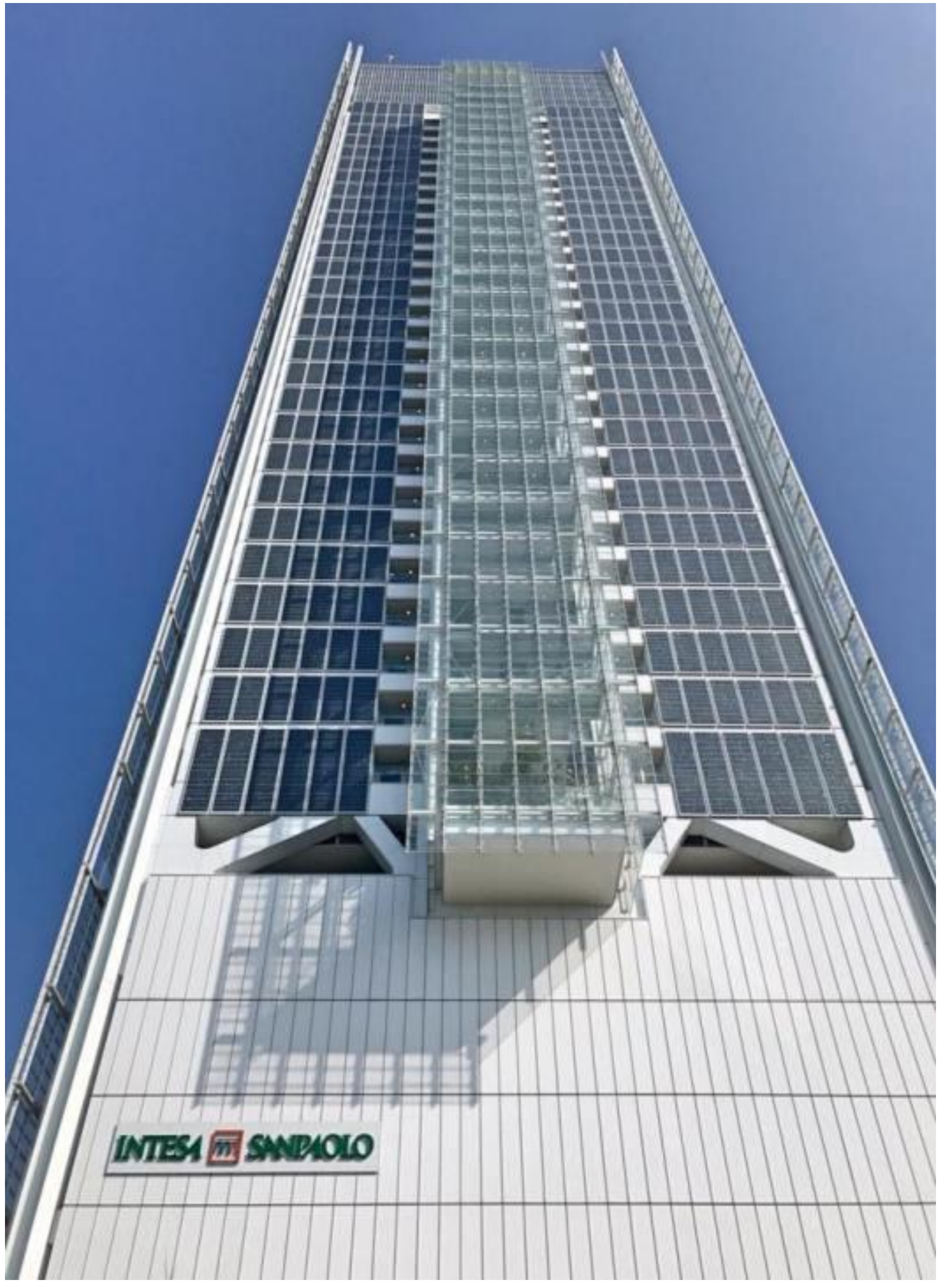
Operations transformation

Innovation

Cost reduction

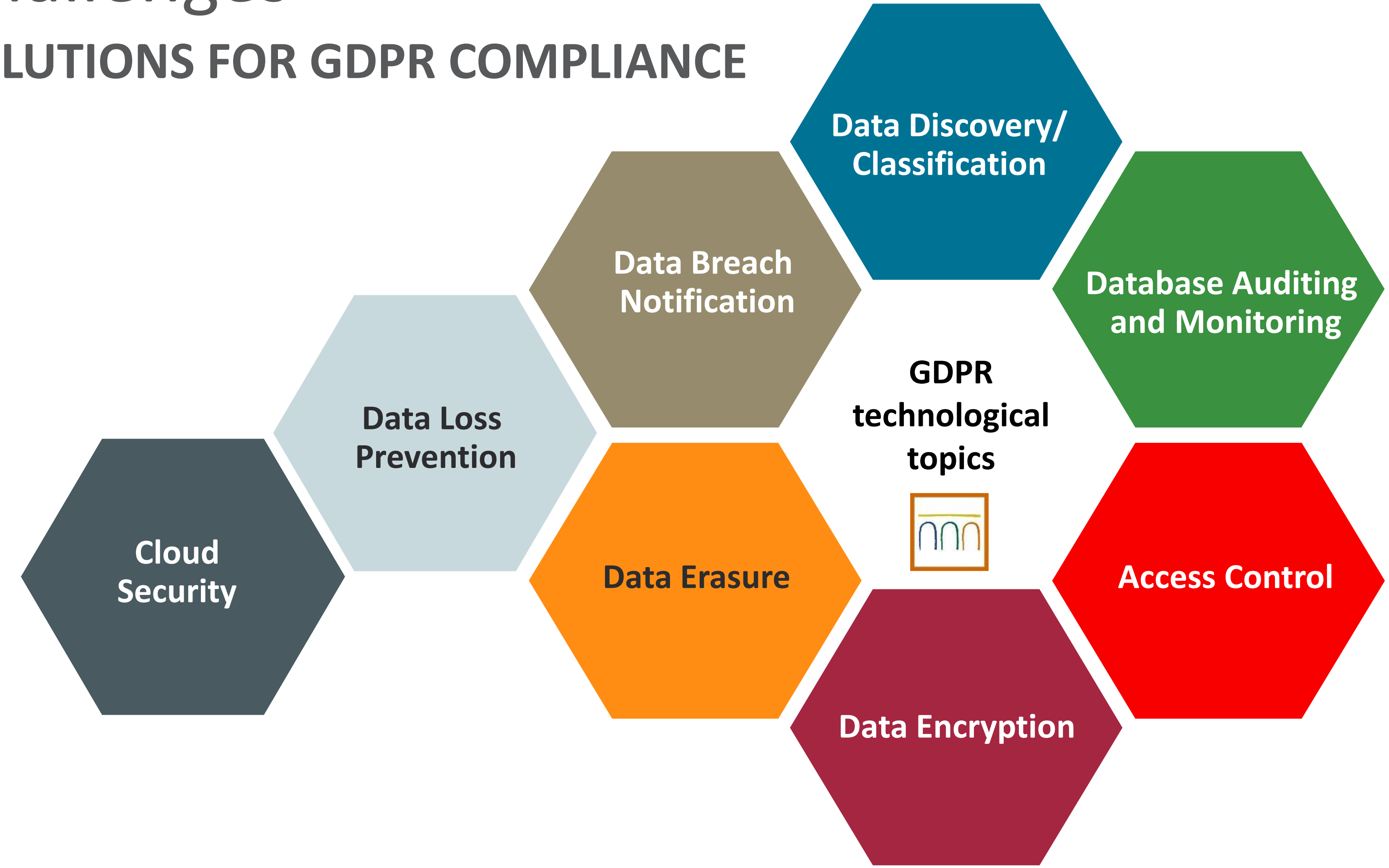
Law & Compliance

Technology



Challenges

SOLUTIONS FOR GDPR COMPLIANCE



GDPR technological topics

Data Discovery/ Classification

Database Auditing and Monitoring

Access Control

Data Encryption

Data Erasure

Data Breach Notification

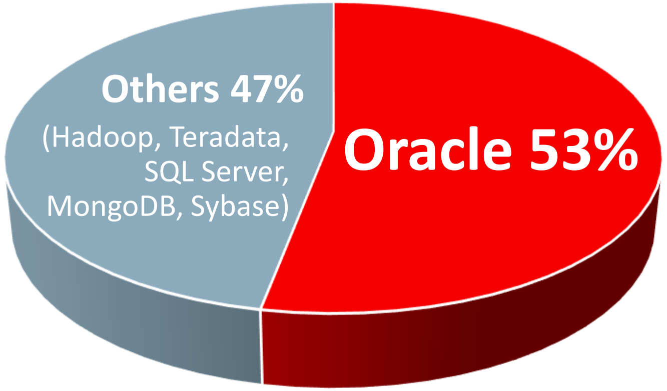
Data Loss Prevention

Cloud Security

The project

OUR TECHNOLOGICAL SCOPE

Databases containing personal data



ORACLE

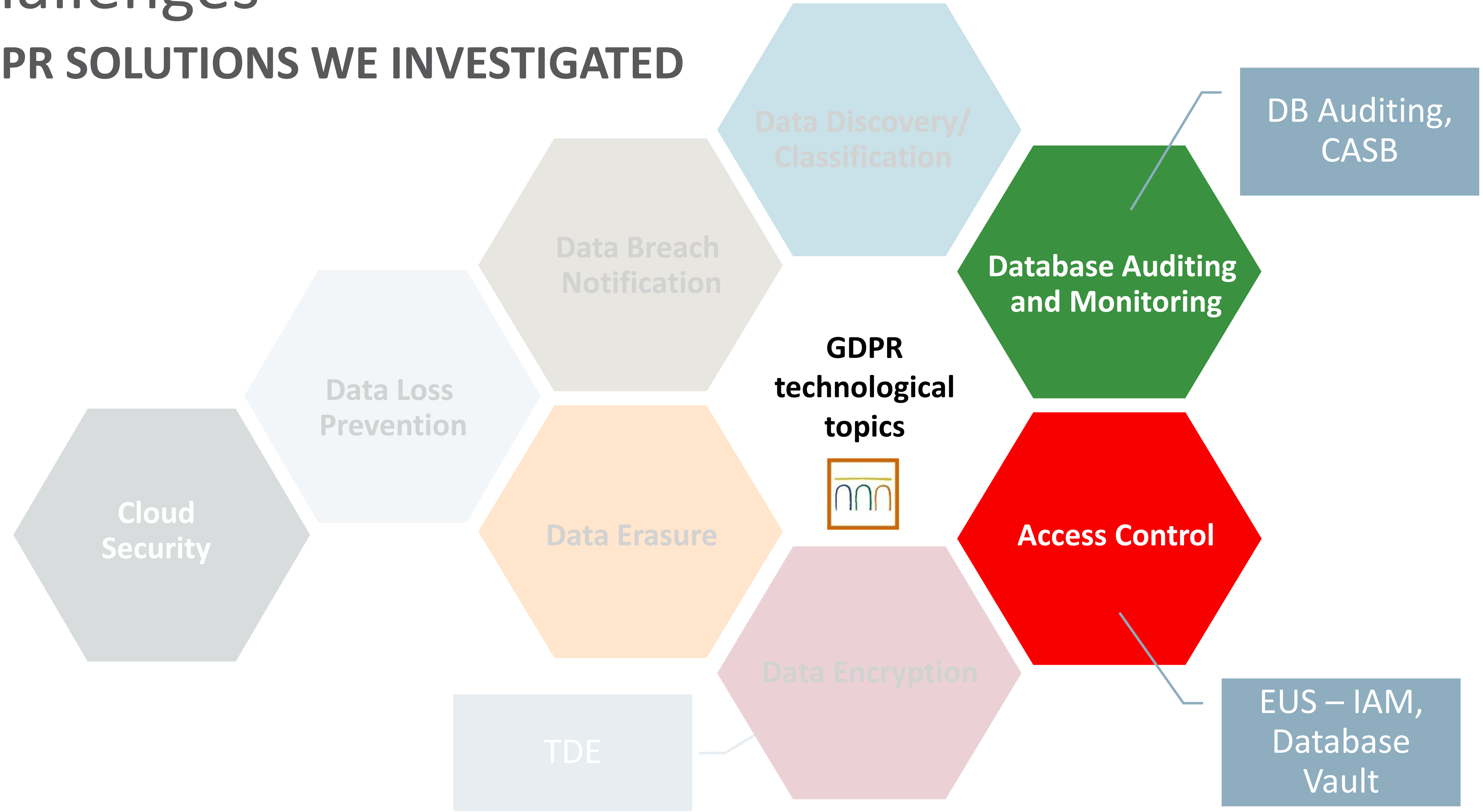
- One of the **bigger Exadata in Europe**
- **Biggest Exadata Stack** installed base **in Italy**
- More than **65 Exadata, Exalogic, Exalytics and ZDLRA boxes**

DBSAT

- **Privileged users identification**
- **Privileges and roles identification**
- **Sensitive data risk evaluation and controls**
- **Data Protection Impact Assessments (DPIA)**
- **Recommend security controls**

Challenges

GDPR SOLUTIONS WE INVESTIGATED



GDPR technological topics

Data Discovery/ Classification

Data Breach Notification

Data Loss Prevention

Cloud Security

Data Erasure

Data Encryption

TDE

Database Auditing and Monitoring

DB Auditing, CASB

Access Control

EUS – IAM, Database Vault

GDPR : lessons learned

WHAT WE HAVE LEARNED

- **It’s a long and complex program**
- **Project results depending by the collaboration** between Legal, IT and Cybersecurity team working as an integrated team
- **Security solutions** and **Data Governance tools** allow to speed-up the GDPR compliance
- **Play with the big vendor** to ensure to achieve the project plan
- **Continuous monitoring of market trends** and solutions to get the innovation advantages

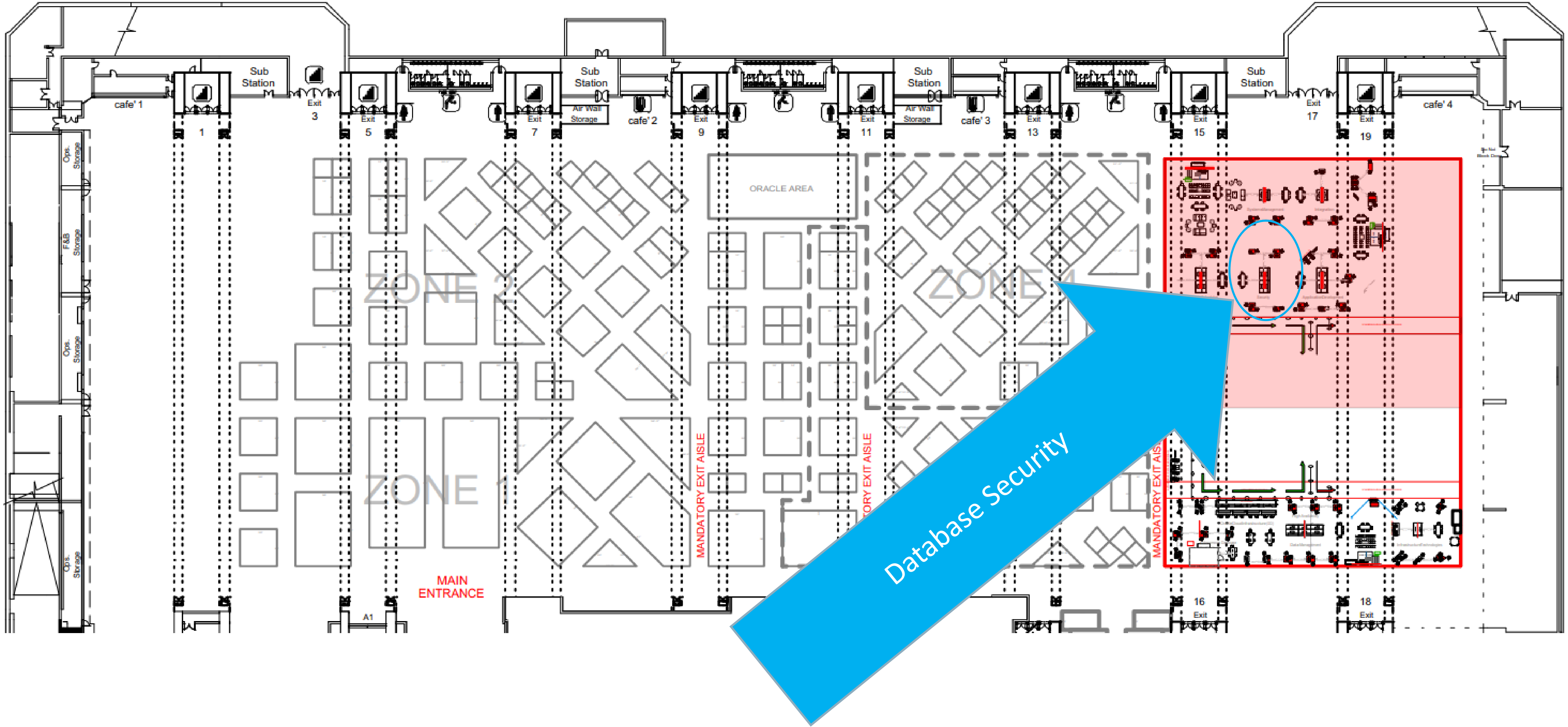
Know More

During OOW & beyond

Database Security at Oracle Open World 2018

Session	Title	Speaker	Location	Date & Time
TRN4106	Encrypt Your Crown Jewels and Manage Keys Efficiently with Oracle Key Vault	Michael Mesaros, Oracle	Moscone West - Room 3006	Wednesday 4:45 PM
TIP4104	Appdev: Building Secure Database Applications Quickly in the Cloud Era	Alan Williams, Oracle	Moscone West - Room 3006	Thursday 11:00 AM
PRO4110	Detecting and Blocking Attacks with Oracle Audit Vault and Database Firewall	Russ Lowenthal, Oracle	Moscone West - Room 3006	Thursday 12:00 PM
TIP4112	Recent Database Security Innovations You Might Not Be Using, but Should Be	Alan Williams, Oracle	Moscone West - Room 3006	Thursday 1:00 PM

Demo Grounds Moscone South



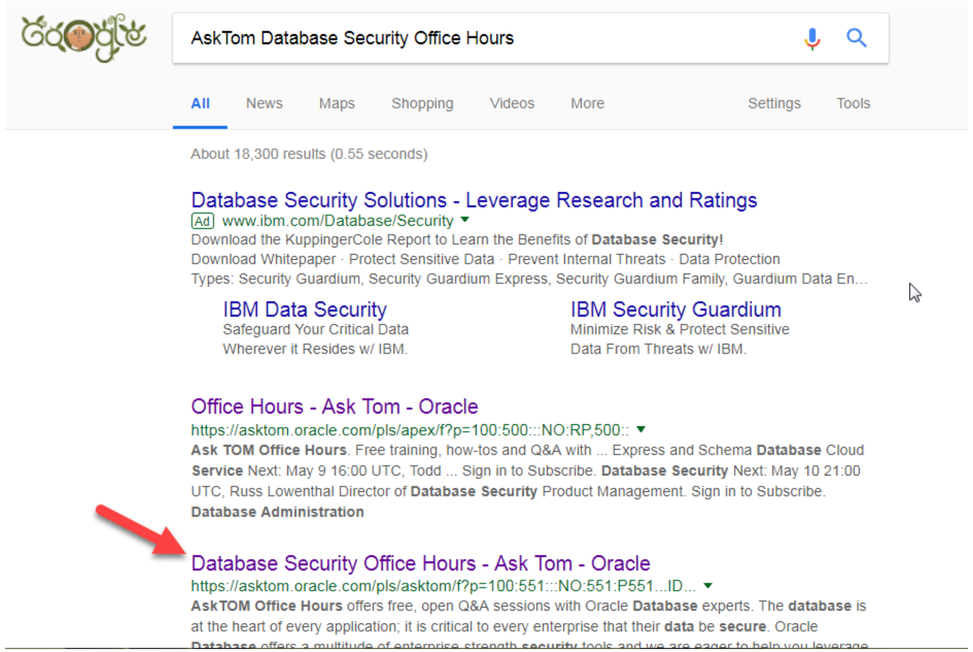
Visit Us in the Oracle Database Security Demo Grounds

Demo Booth Title	Featured Solutions
Database Security – Detect & Assess	Database Security Products/Technologies • TDE, Redaction, Database Vault, Label Security, Real Application Security, Centrally Managed Users, Data Masking and Subsetting, Key Vault, Audit Vault and Database Firewall Solutions • GDPR Services • Data Security Cloud Services
Database Security – Detect & Assess Solutions	
Database Security – Prevent & Control	
Database Security – Prevent & Control Solutions	

External: AskTOM Database Security Office Hours

- Direct line for customers into Database Security product development
- Second Thursday of every month, 09:00 and 20:00 UTC (identical sessions)
- URL: http://bit.ly/asktomdbsec
- Or, just search

  AskTom Database Security Office Hours



AskTom Database Security Office Hours

About 18,300 results (0.55 seconds)

Database Security Solutions - Leverage Research and Ratings
Ad www.ibm.com/Database/Security ▾
Download the KuppingerCole Report to Learn the Benefits of **Database Security!**
Download Whitepaper · Protect Sensitive Data · Prevent Internal Threats · Data Protection
Types: Security Guardium, Security Guardium Express, Security Guardium Family, Guardium Data En...

IBM Data Security
Safeguard Your Critical Data
Wherever it Resides w/ IBM.

IBM Security Guardium
Minimize Risk & Protect Sensitive
Data From Threats w/ IBM.

Office Hours - Ask Tom - Oracle
https://asktom.oracle.com/pls/apex/f?p=100:500:::NO:RP,500:: ▾
Ask TOM Office Hours. Free training, how-tos and Q&A with ... Express and Schema **Database** Cloud **Service** Next: May 9 16:00 UTC, Todd ... Sign in to Subscribe. **Database Security** Next: May 10 21:00 UTC, Russ Lowenthal Director of **Database Security** Product Management. Sign in to Subscribe. **Database Administration**

Database Security Office Hours - Ask Tom - Oracle
https://asktom.oracle.com/pls/asktom/f?p=100:551:::NO:551:P551...ID... ▾
AskTOM Office Hours offers free, open Q&A sessions with Oracle **Database** experts. The **database** is at the heart of every application; it is critical to every enterprise that their **data** be **secure**. Oracle **Database** offers a multitude of enterprise strength **security** tools and we are eager to help you leverage

Connect With Us

/OracleDatabase
#DBSAT

/OracleSecurity

https://blogs.oracle.com/securityinsideout/

Oracle Database Insider

/Oracle Database Security

/Oracle Cloud

http://oracle.com/database/security

http://oracle.com/technetwork/database/security

ORACLE

Q & A

Integrated Cloud

Applications & Platform Services