ORACLE

Oracle Database Security Assessment Tool

Learn how secure your databases are with DBSAT

Pedro Lopes
Product Manager
Database Security, Oracle
June 30, 2021

Security Zones of Control for Oracle Databases

Assess

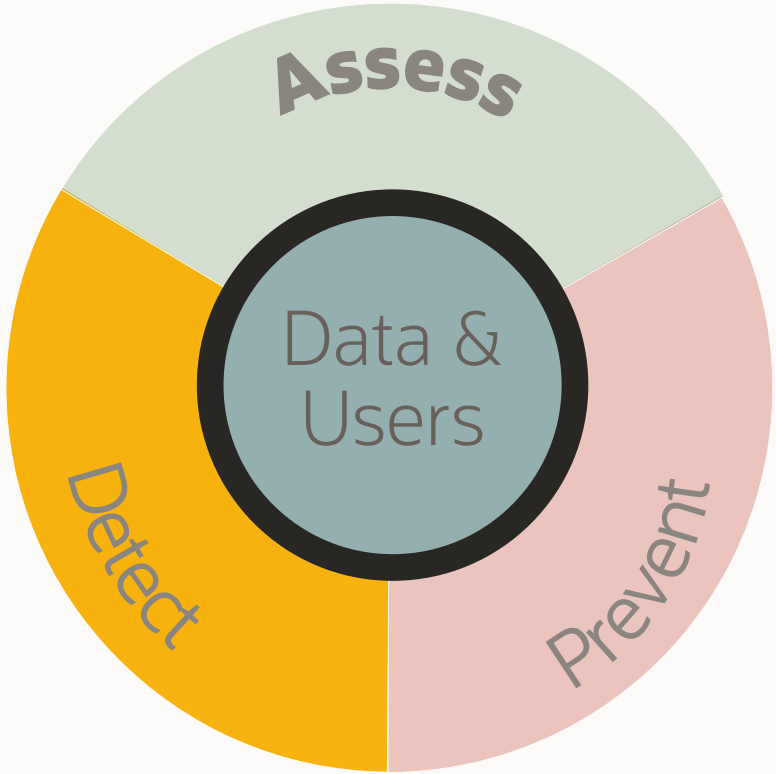
Security-Assessment (DBSAT)
Data Discovery
Privilege Analysis

Detect

Unified Auditing
Audit Vault
Database Firewall

Prevent

Encryption & Key Vault
Data Masking, Data Redaction
Database Vault



Data

Label Security
Real Application Security
Virtual Private Database
Crypto Toolkit

Users

Password, PKI, Kerberos, Radius
Proxy Users, Password Profiles
Oracle & Active Directory

Data is today's capital

"The world's most valuable resource is no longer oil, but data"

Data drives everything

- Analytics and automation
- Advertising and marketing budgets
- Personalization and improved experience
- Business analytics and decisions
- Government policies and plans

PII Data
Financial Data
Trade Secrets
Competitive Data
Employment Data
Healthcare Data
IT Security Data
Transaction Data
Browsing Data…

Overall, data helps improve products and services, provide better user experience, and support and grow businesses

Data can be a liability

The scary side of data economy

Data breaches are exploding worldwide

- Large data breaches always involve Databases

Data losses can be catastrophic for businesses, impacting

- Finances due to compensations, penalties, legal, PR, recovery cost
- Brand reputation, customer trust, intellectual property, competitiveness
- Overall business and revenue

Fast evolving, stringent regulatory landscape

- Across industries and regions
- Laws that aim to protect data and citizen privacy

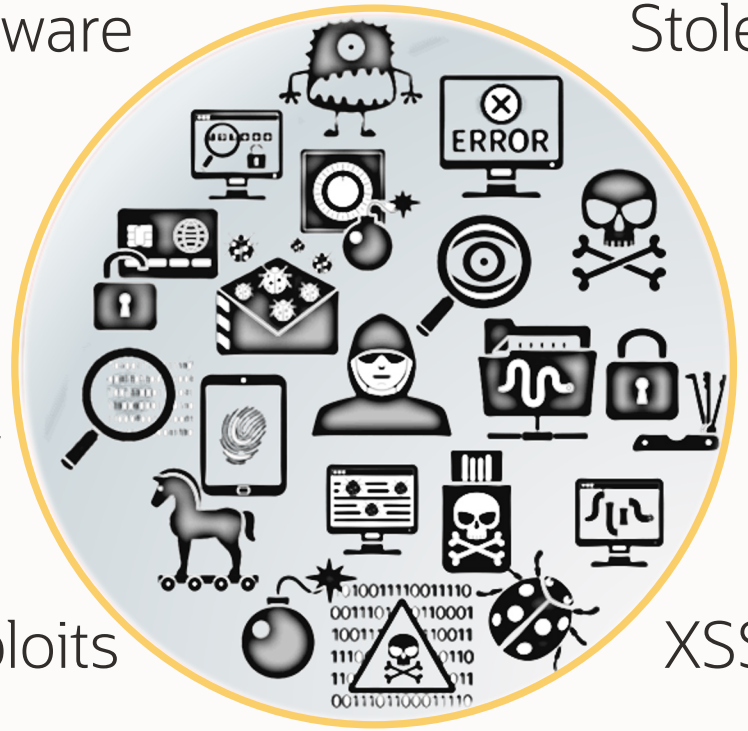
Evolving attack tools and techniques

Ransomware

Stolen Credentials

Phishing

SQL Injection



Buffer Overflow

Privilege Escalation

App Exploits

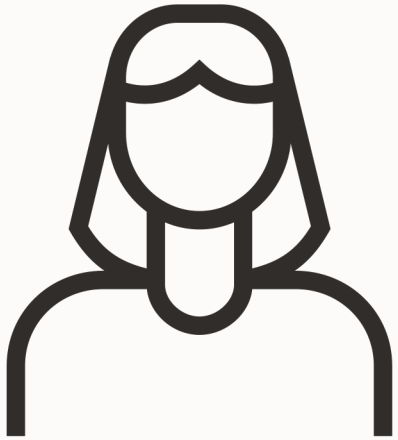
XSS Attacks

Unpatched Systems

Think like a hacker

Attacker

Privileged users?
Known users?
Common passwords?
Open ports?
Database configuration?
Encrypted data?
Auditing on?
Known vulnerabilities?
Known packaged apps?



Data Owner

What you don’t know can hurt you

Is the database configured according to best practices?

What security controls are already in place?

What users are in the database?

What access do users have?

What sensitive data is in this database?

Top 10 findings

From database security assessments

- No Database Security policies/strategy in place
- No patching/patch management policy in place
- No personalized accounts; No separation of duties; Over-privileged accounts
- No encryption of sensitive/regulated data
- No monitoring/auditing in place
- No password policies; Weak password management
- Non-Production (DEV/TEST/TRAINING) systems with production data
- No cleanup of test/sample accounts
- No anonymization of data sent to third parties
- No OS hardening

Introducing

Database Security Assessment Tool

Assess your database security before hackers come knocking

Assess Configuration

Patches

Data Encryption

Auditing policies

OS file permissions

Database configuration

Listener configuration

Fine-grained access control

Identify Risky Users

Database accounts

User privileges

User roles

Discover Sensitive Data

What type, where, and how much?

Sample pattern files for Greek, German, Dutch, French, Spanish, Italian, and Portuguese based data models as well.

Assessment Reports

Summary and detailed information

Prioritized, actionable and target specific recommendations

Mapping to EU GDPR, STIG and CIS Benchmark

Runs on 11g to 21c Oracle Databases

New features in DBSAT 2.2.2 (June 2021)

Specific checks and targeted recommendations for on-premises Oracle Database EE, Autonomous Databases and DBCS (EE/HP/EP DB Systems)

The PDB_DBA role is now included for all checks where the DBA role was previously being considered.

New Findings

- **USER.GPR**
  Provides recommendations for the Gradual Password Rollover profile parameter
- **CRYPT.DBFIPS**
  Checks if parameter DBFIPS_140 = TRUE. This parameter enables TDE and DBMS_CRYPTO PL/SQL package program units to run in a FIPS-compliant mode.

Updated Severity for

- INFO.PATCH, USER.VERIFIER, AUTH.DV, ACCESS.REDACT, AUDIT.ADMIN, AUDIT.CONN, CONF.BKUP, NET.CRYPT, OS.LISTEN

Enhanced Findings

- **INFO.PATCH**
  Now considers Autonomous Databases specifics.
- **CONF.BKUP**
  Improved accuracy. Checks were also improved to better assess the frequency of backups in Autonomous Databases.
- **CRYPT.TDE**
  Now lists how many days have passed since the master encryption key was last rotated.
- **CONF.DIR**
  Directory objects that pose a risk are now identified at the top of the details section.
- **AUTH.DV**
  Improved to focus on user created policies, realms, command rules, and protected objects. Users with Database Vault default roles are displayed. Database Vault Operations Control status is displayed.

How can DBSAT Help?

Assess your database security before hackers come knocking

Assess your database security before hackers come knocking

Know your overall database security posture

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	**1**
User Accounts	5	0	0	3	2	2	**12**
Privileges and Roles	5	15	0	1	1	0	**22**
Authorization Control	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	1	4	0	0	0	**5**
Auditing	1	4	1	0	7	0	**13**
Encryption	0	1	1	0	0	0	**2**
Database Configuration	5	3	0	3	2	2	**15**
Network Configuration	1	1	0	0	3	0	**5**
Operating System	1	1	0	2	1	0	**5**
Total	**18**	**27**	**7**	**9**	**16**	**5**	**82**

Security Features

Feature	Currently Used
USER AUTHENTICATION	
Password Authentication	Yes
Global Authentication	No
External Authentication	No
AUTHORIZATION CONTROL	
Database Vault	No
Privilege Analysis	Yes
ENCRYPTION	
Tablespace Encryption	No
Column Encryption	No
Network Encryption	No
AUDITING	
Unified Audit	Yes
Fine Grained Audit	No
Traditional Audit	Yes
FINE-GRAINED ACCESS CONTROL	
Virtual Private Database	No
Real Application Security	No
Label Security	No
Data Redaction	Yes
Transparent Sensitive Data Protection	No

Assess your database security before hackers come knocking

Know your users, roles, and privileges

Users with Default Passwords

USER.DEFPWD — CIS STIG

Status	High Risk
Summary	Found 2 unlocked user accounts with default password.
Details	`Users with default password: HR, SCOTT`
Remarks	Default passwords for predefined Oracle accounts are well known and provide a trivial means of entry for attackers. Well-known passwords for locked accounts should be changed as well.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2 Oracle Database 12c STIG v1 r10: Rule SV-76031r1, SV-76339r1

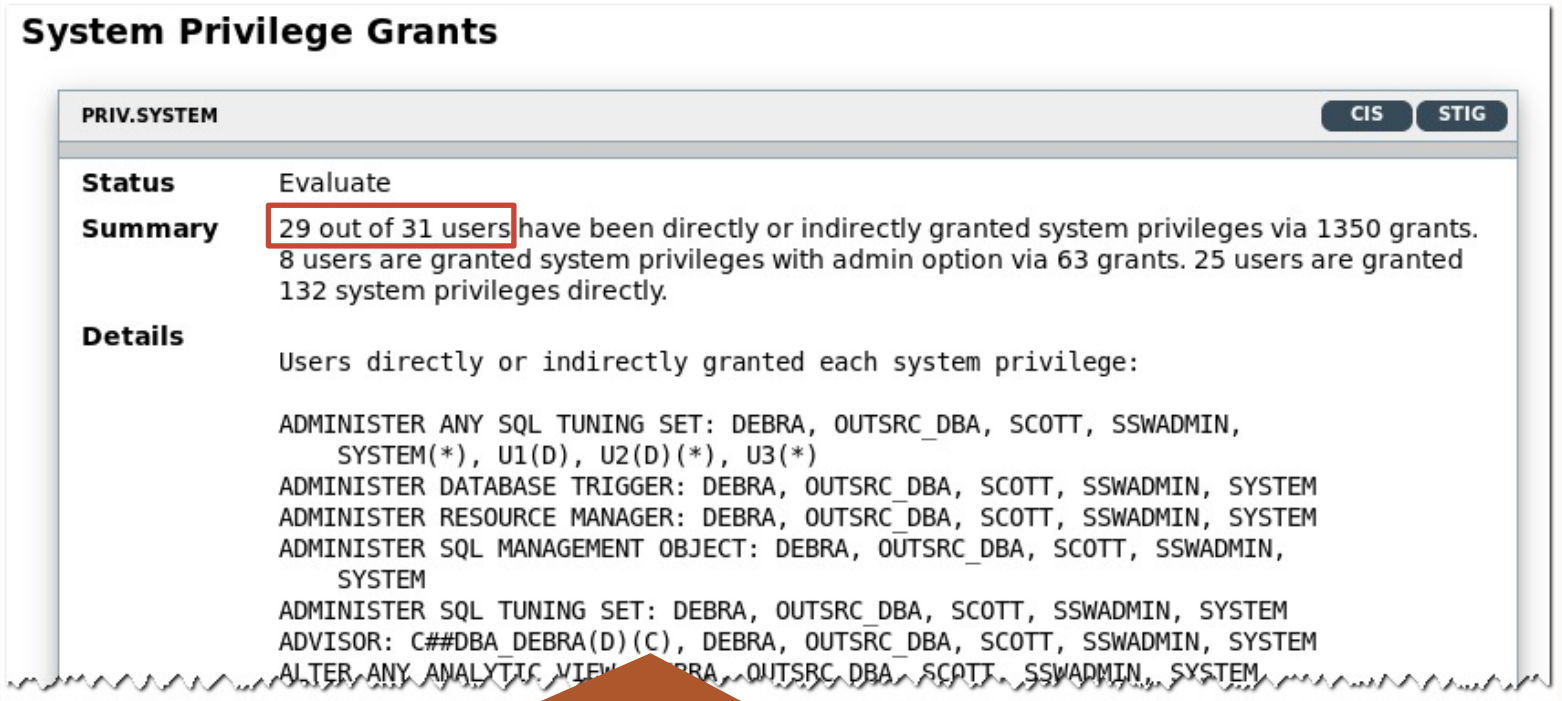
Know your users, roles, and privileges

Password Verification Functions

USER.PASSWD CIS STIG

Status	Medium Risk
Summary	Found 27 users not using password verification function.
Details	Profiles with password verification function: ORA_STIG_PROFILE(ORA12C_STIG_VERIFY_FUNCTION) Profiles without password verification function: DEFAULT Users without password verification function: APEX_180200, APEX_INSTANCE_ADMIN_USER, APEX_LISTENER, APEX_PUBLIC_USER, APEX_REST_PUBLIC_USER, APPUSER, DBJSON, DBSAT, DEBRA, FINACME, FLOWS_FILES, HCM1, HR, HRREST, MYDBA, OBE, ORDS_PUBLIC_USER, OUTSRC_DBA, PDBADMIN, SCOTT, SSWADMIN, U1, U2, U3, XDBEXT, XDBPM, XFILES
Remarks	Password verification functions are used to ensure that user passwords meet minimum requirements for complexity, which may include factors such as length, use of numbers or punctuation characters, difference from previous passwords, etc. Oracle supplies several predefined functions, or a custom PL/SQL function can be used. Every user profile should include a password verification function.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 3.8 Oracle Database 12c STIG v1 r10: Rule SV-76209r1, SV-76213r1, SV-76215r1 , SV-76217r1, SV-76219r1, SV-76221r1, SV-76225r1

Know your users, roles, and privileges



SQL> grant advisor to C##DBA_DEBRA container=all;

(*) With Admin Option
(D) Direct Grant
(C) Common Grant

Know your users, roles, and privileges

PRIV.DBA CIS

Status	Evaluate
Summary	5 out of 30 users have been directly or indirectly granted highly sensitive DBA role via 5 grants.
Details	Grants of DBA role: DEBRA <- APP_ROLE: DBA OUTSRC_DBA: DBA SCOTT: DBA SSWADMIN: DBA SYSTEM: DBA
Remarks	The DBA is a powerful role and can be used to bypass many security controls. It should be granted to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with minimum set of privileges that users require to execute their tasks (least privilege principle) and do not grant the DBA role. Privilege Analysis can assist in the task of identifying used/unused privileges and roles. Having different roles with minimum required privileges based on types of operations DBAs execute also helps to achieve Separation of Duties. Furthermore, each trusted user should have an individual account for accountability reasons. It is recommended to audit users with the DBA roles to detect any unauthorized activity. Avoid granting the DBA or custom DBA-like powerful roles WITH ADMIN option unless absolutely necessary. Please note that Oracle may add or remove roles and privileges from the DBA role.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 4.4.4

Direct and Indirect grants

Assess your database security before hackers come knocking

Know your sensitive data

Sensitive Data Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO - ADDRESS	7	18	244
FINANCIAL INFO - CARD DATA	2	2	256
HEALTH INFO - PROVIDER DATA	1	1	149
IDENTIFICATION INFO - PERSONAL IDS	3	3	356
IDENTIFICATION INFO - PUBLIC IDS	3	12	321
IT INFO - USER DATA	1	1	149
JOB INFO - COMPENSATION DATA	7	10	527
JOB INFO - EMPLOYEE DATA	12	25	569
JOB INFO - ORG DATA	7	8	412
TOTAL	**21***	**80**	**989****

* Number of Unique Tables with Sensitive Data.

** Number of Unique Rows with Sensitive Data.

Know your sensitive data

Recommended Security Controls

Risk Level: High Risk

Security for Environments with High Value Data: Detective plus Strong Preventive Controls
Highly sensitive and regulated data should be protected from privileged users, and from users without a business need for the data. Activity of privileged accounts should be controlled to protect against insider threats, stolen credentials, and human error. Who can access the database and what can be executed should be controlled by establishing a trusted path and applying command rules. Sensitive data should be redacted on application read only screens. A Database Firewall ensures that only approved SQL statements or access by trusted users reaches the database - blocking unknown SQL injection attacks and the use of stolen login credentials.

Recommended controls include:

- **Audit all sensitive operations including privileged user activities**
- **Audit access to application data that bypasses the application**
- **Encrypt data to prevent out-of-band access**
- **Mask sensitive data for test and development environments**
- **Restrict database administrators from accessing highly sensitive data**
- **Block the use of application login credentials from outside of the application**
- **Monitor database activity for anomalies**
- **Detect and prevent SQL Injection attacks**
- ***Evaluate: Oracle Audit Vault and Database Firewall, Oracle Advanced Security, Oracle Data Masking and Subsetting, Oracle Database Vault***

Know your sensitive data

Summary per
Risk Level and Category

Tables Detected within Sensitive Category: BIOGRAPHIC INFO - ADDRESS

Risk Level	High Risk
Summary	Found BIOGRAPHIC INFO - ADDRESS within 18 Column(s) in 7 Table(s)
Location	Tables: FINACME.COMPANY_DATA, HCM1.COUNTRIES, HCM1.LOCATIONS, HR.COUNTRIES, HR.LOCATIONS, HRREST.COUNTRIES, HRREST.LOCATIONS

Tables Detected within Sensitive Category: FINANCIAL INFO - CARD DATA

Risk Level	High Risk
Summary	Found FINANCIAL INFO - CARD DATA within 2 Column(s) in 2 Table(s)
Location	Tables: HCM1.EMP_EXTENDED, HCM1.SUPPLEMENTAL_DATA

Know your sensitive data

Table level details

Table Summary

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
FINACME	COMPANY_DATA	9	4	100	BIOGRAPHIC INFO - ADDRESS, IDENTIFICATION INFO - PERSONAL IDS
HCM1	COUNTRIES	3	1	25	BIOGRAPHIC INFO - ADDRESS
HCM1	DEPARTMENTS	4	1	27	JOB INFO - ORG DATA
HCM1	EMPLOYEES	11	8	107	IDENTIFICATION INFO - PUBLIC IDS, JOB INFO - COMPENSATION DATA, JOB INFO - EMPLOYEE DATA, JOB INFO - ORG DATA

Know your sensitive data

Column level details

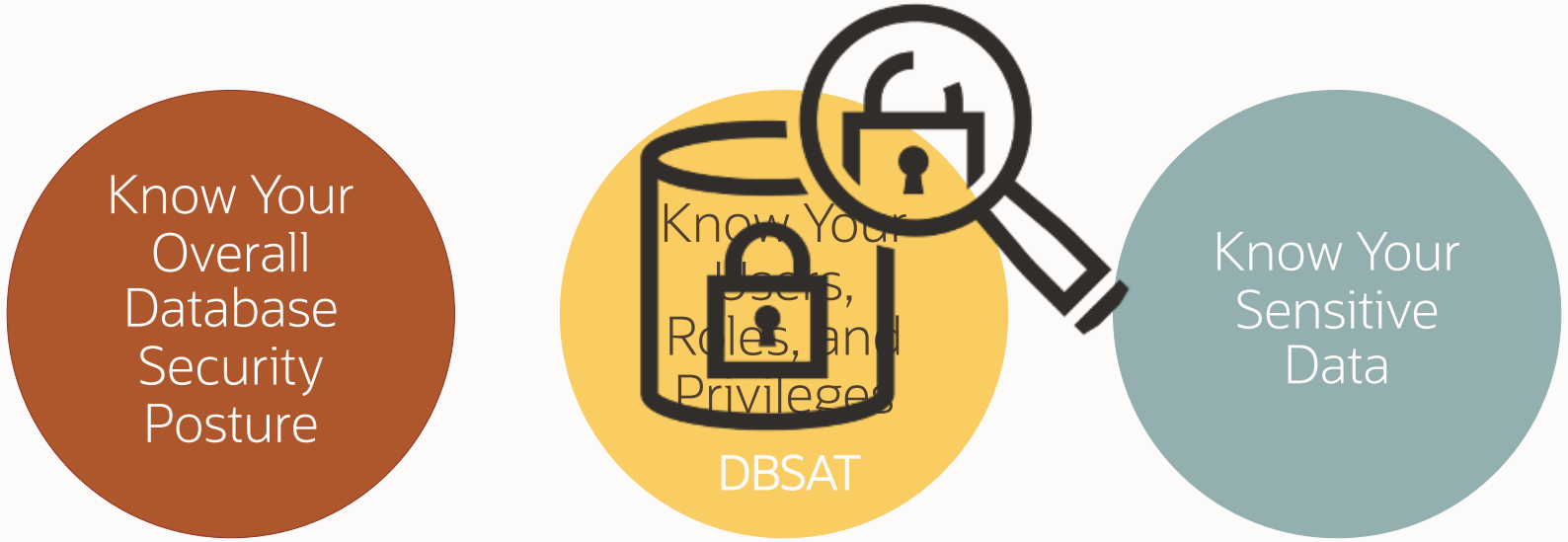
Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
FINACME	COMPANY_DATA	CITY	--	BIOGRAPHIC INFO - ADDRESS	CITY	High Risk
FINACME	COMPANY_DATA	STATE	--	BIOGRAPHIC INFO - ADDRESS	STATE	High Risk
FINACME	COMPANY_DATA	TAX_PAYER_ID	--	IDENTIFICATION INFO - PERSONAL IDS	TAX ID NUMBER (TIN)	High Risk
FINACME	COMPANY_DATA	ZIP	--	BIOGRAPHIC INFO - ADDRESS	POSTAL CODE	High Risk
HCM1	COUNTRIES	COUNTRY_NAME	--	BIOGRAPHIC INFO - ADDRESS	COUNTRY	High Risk

TIP

The csv file can be loaded into Oracle Audit Vault and Database Firewall to get reports on activity on sensitive data, user's access rights to sensitive data, activity on sensitive data by privileged users, and others.

Assess your database security before hackers come knocking



Stand-alone lightweight tool: quick and easy
FREE to current Oracle customers

How to Get Started?

Quick & Simple!

3-Step flow

1 Run
./dbsat collect

2 Run
./dbsat report

3 Run
./dbsat discover

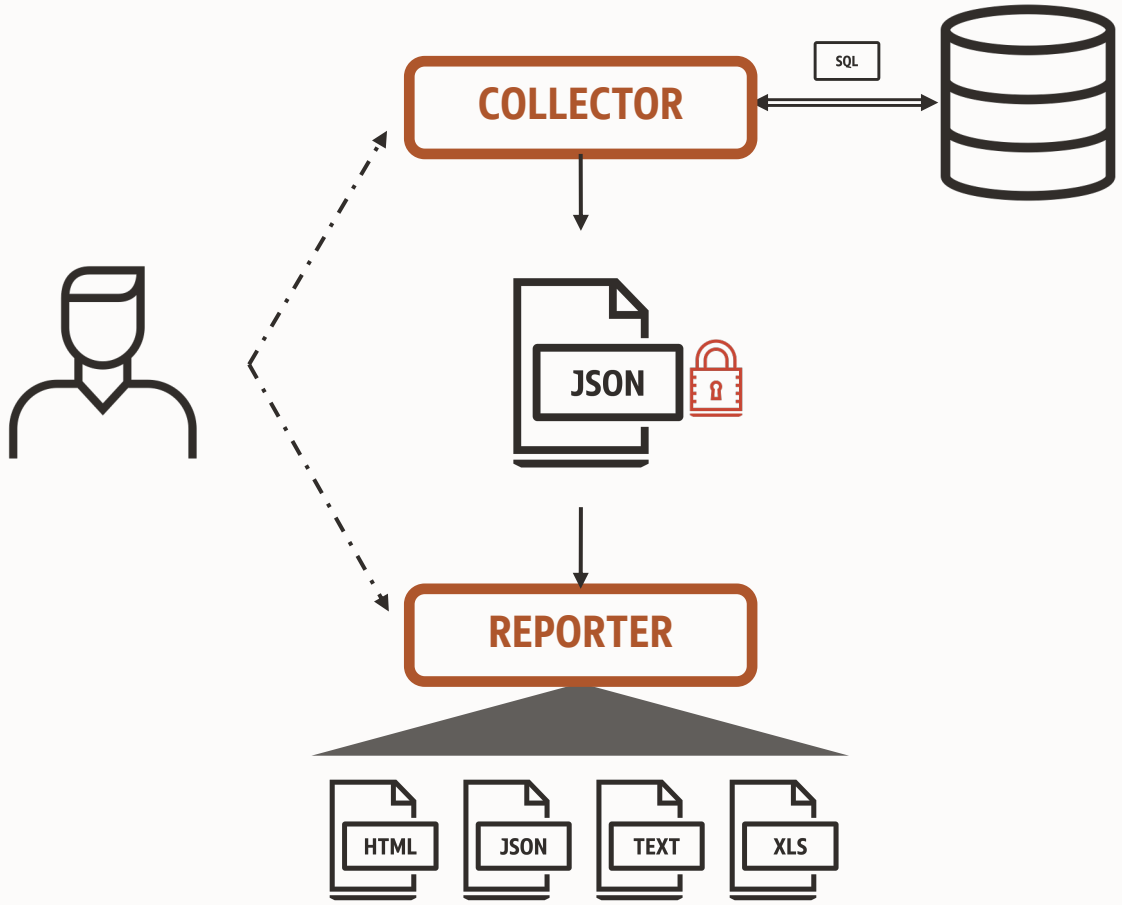
Collector & Reporter

Collects metadata information on users, roles, privileges, security configuration, and policies in place

Generates summary output with prioritized findings

Over 80 detailed findings with remarks

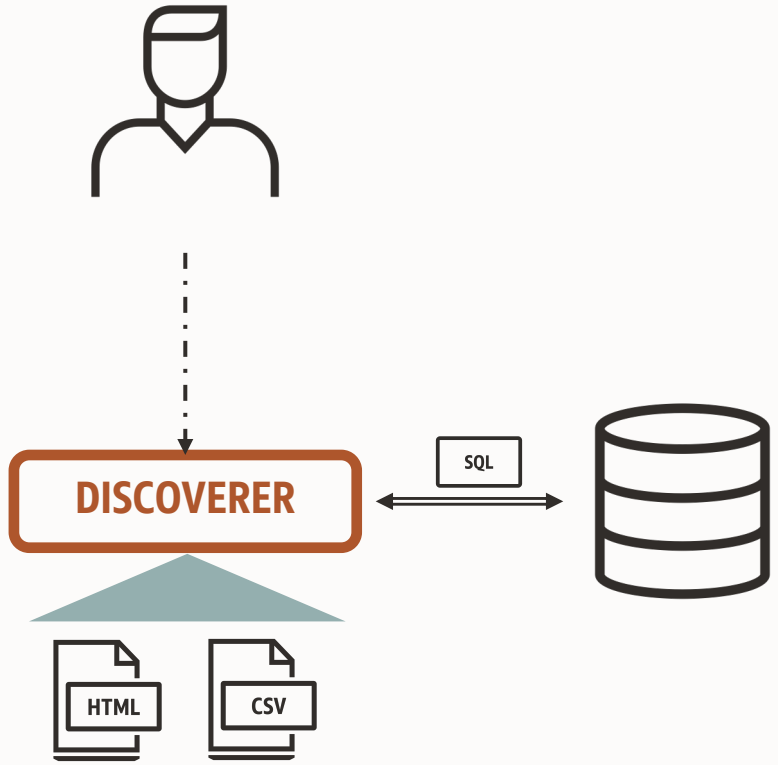
References to CIS Benchmark, STIG Rules and GDPR articles/recitals



Discoverer

Get summary and details on Sensitive Data Categories and Types (125+), tables, columns, rows, and risk levels

Get recommendations on which security controls to put in place to protect your sensitive data



What Else?

Periodic scheduled assessments?

Baselining?

Drift report?

Assessment history?

User risk assessment?

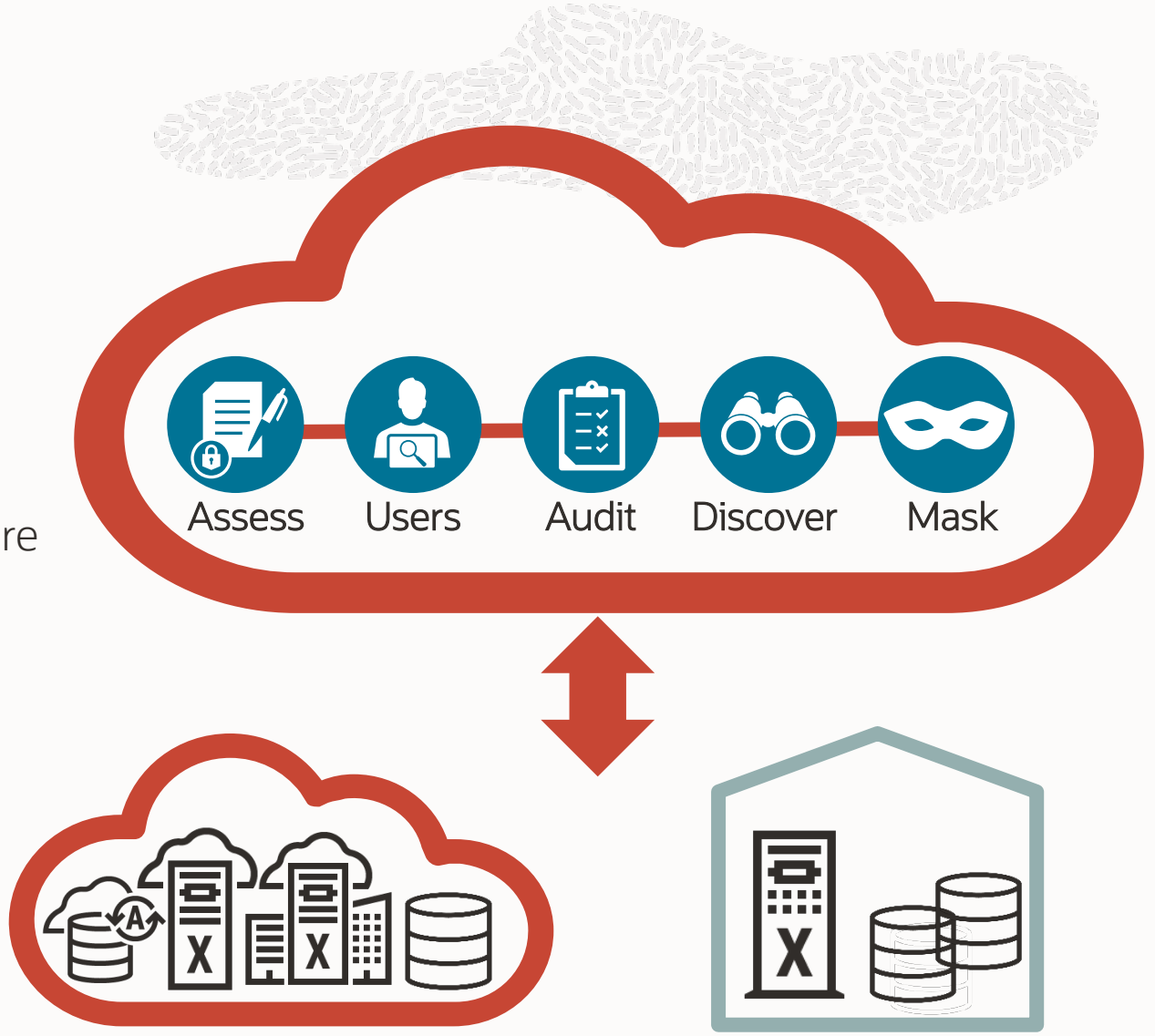
Oracle Data Safe

Unified database security control center

- Risk dashboard: configuration, data, users
- Monitor user activity
- Discover sensitive data and mask data

Benefits

- ✓ No special expertise needed: click-and-secure
- ✓ Saves time and mitigates security risks
- ✓ Defense-in-depth security for all customers

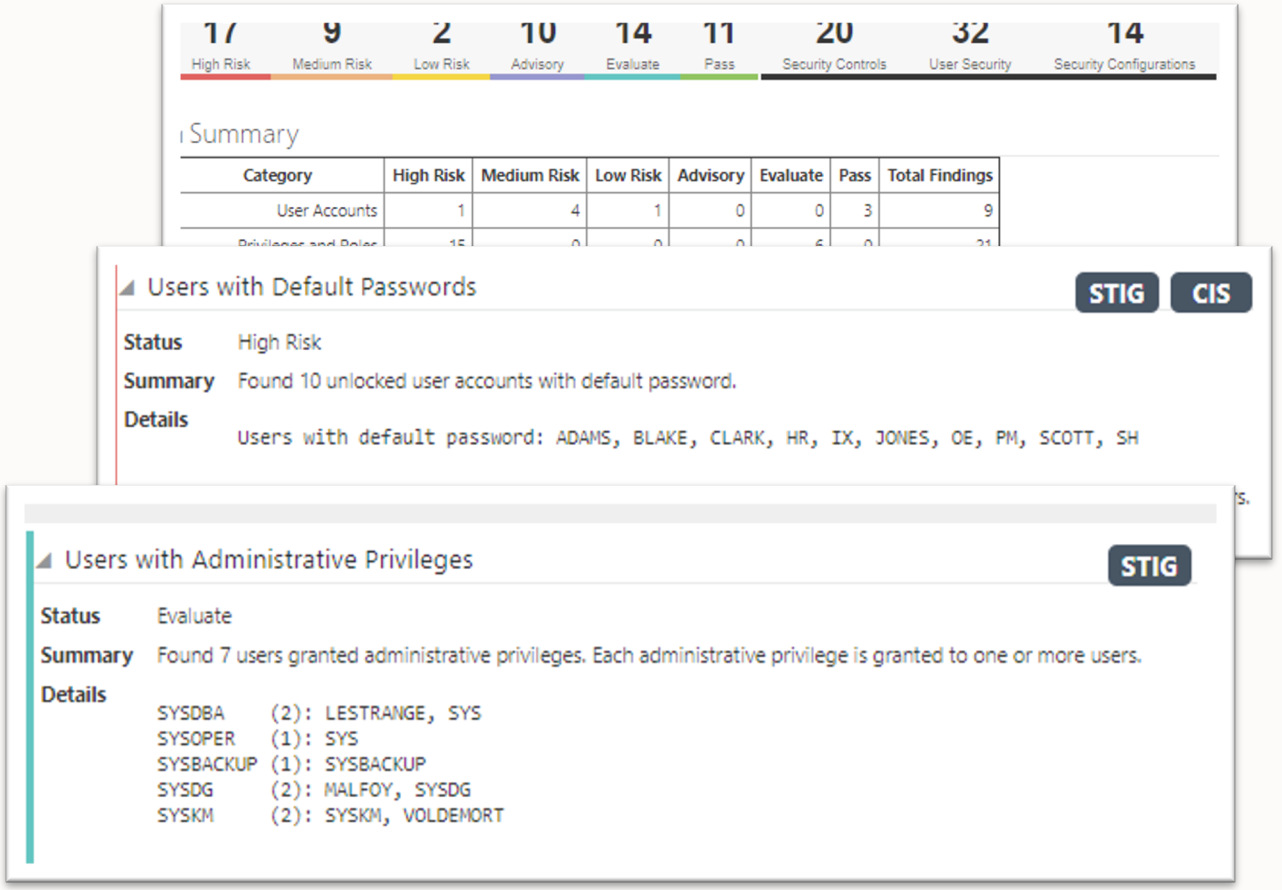


Securing cloud and on-premises Oracle databases

Database Security Assessment

Instant feedback on configurations that may introduce unnecessary risk

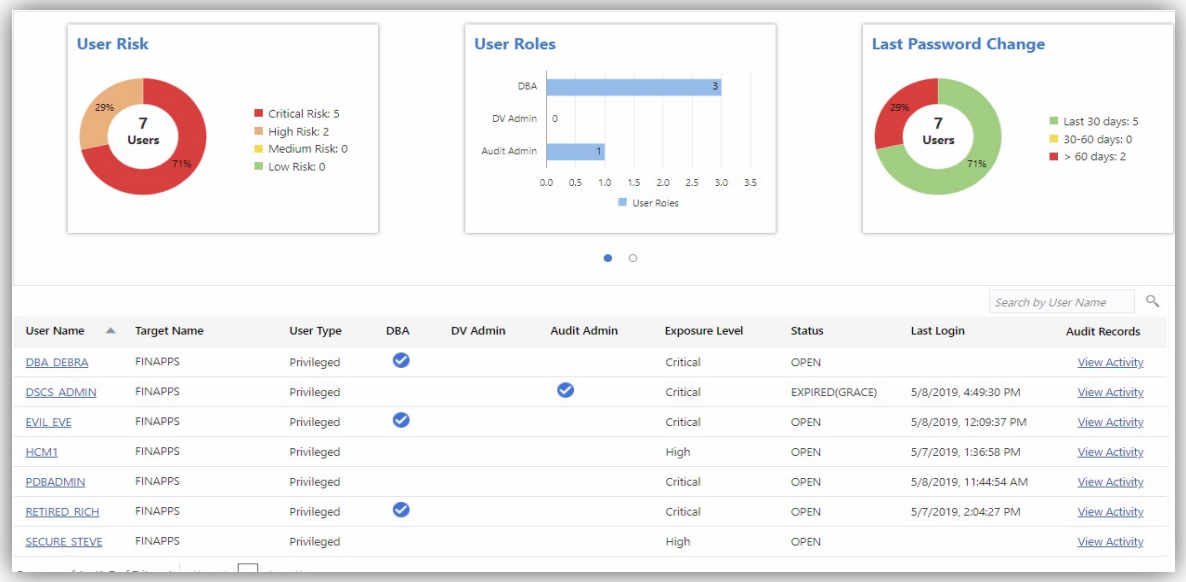
- Comprehensive assessment
  - Security parameters
  - Security controls in use
  - User Roles and Privileges
- Identify drift from best practices
- Actionable reports
  - Prioritized recommendations
  - Compliance mappings (GDPR, STIG, CIS)



User Risk Assessment

Reduce user risk by managing roles/privileges and policies

- Identify over-privileged risky users
- Evaluate static profile:
  type of user, password policies, …
- Evaluate dynamic profile:
  last login / IP / password change, audit data, …



Data Safe vs. DBSAT Capabilities

Capabilities	Data Safe	DBSAT
Overall security configuration status	Yes	Yes
Configuration drift detection and reporting	Yes	-
User Risk Assessment	Yes	-
Sensitive Data Discovery	Yes	Yes*
Centralized management of assessment on multiple targets	Yes	-
Historical reports and management	Yes	-
Supports cloud, on-premises and Cloud@Customer targets	Yes	Yes
Supports column names in Spanish, German, Greek, Italian, French, Dutch, Portuguese		Yes

* Checks only for column names and comments, but not data

Summary

Easy to install and run

Download DBSAT 2.2.2 today from
https://www.oracle.com/database/technologies/security/dbsat.html

Collect security config data by running ‘dbsat collect’ on the target
Run ‘dbsat report’ to generate security assessment report
Run ‘dbsat discover’ to generate sensitive data report

Available to all Oracle database customers with active support contract

Action plan

Monday Morning

Run DBSAT to assess your current database security state.

What is measured gets done!

Next 30 days

Fix obvious mistakes and high risk findings.

A data breach impacts your business.

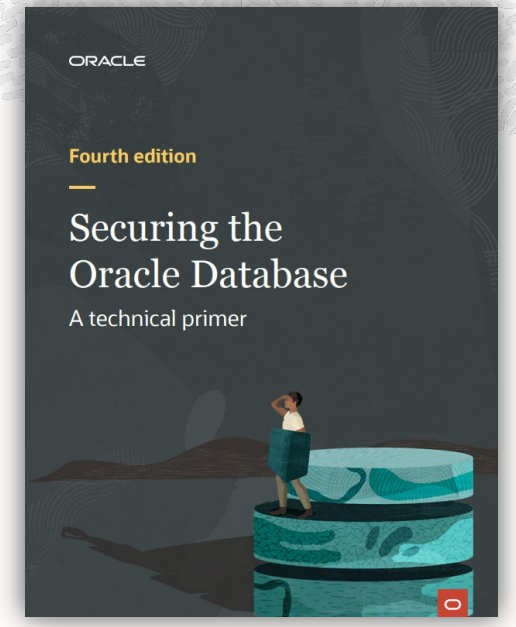
Next 90 days

Update Data Security strategy to include database security best practices.

Plan. Trust is hard to build and easy to lose.

Learn more

O.com: www.oracle.com/security/database-security/
OTN: www.oracle.com/database/technologies/security.html
Blog: http://blogs.oracle.com/cloudsecurity/db-sec
NEW: eBook 4th Edition: www.oracle.com/securingthedatabase



Oracle LiveLabs - Try it yourself:

- DBSAT: https://bit.ly/3w1wwVy
- Data Safe: https://bit.ly/3ykd8oS
- All Database Security: https://bit.ly/3tTZ6XQ

Database Security Office Hours offers free, open Q&A sessions with Oracle Database experts. We hold two LIVE sessions on the second Wednesday of each month, one at 14:00 UTC, the other at 23:00 UTC.

https://bit.ly/asktomdbsec

Ask Tom Database Security

Thank You

Pedro Lopes
Product Manager
Database Security


ORACLE

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.