
ORACLE®

Oracle Database Security Assessment Tool 2.1

ハッカーに先を越される前に 自社のセキュリティ態勢を把握する

Pedro Lopes
製品マネージャー
Oracle Databaseセキュリティ
2019年3月1日

ORACLE

データ – もっとも貴重な資産

運転免許証番号、パスポート番号、
納税者ID、健康保険被保険者番号、…

クレジット/デビット・カード番号、
暗証番号、SSN、年齢、名前、誕生日、…

進化する規制の現状

- EU一般データ保護規則（EU GDPR）
- クレジット・カード業界のデータ・セキュリティ基準（PCI DSS）
- 米国サーベンス・オクスリー法（SOX）
- HIPAA/HITECH
- 多数の侵害通知法

誰が自社のデータを狙っているのか?

内部関係者

国家

元従業員

犯罪者

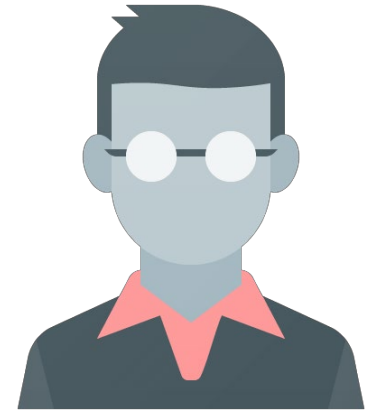
詮索好き

ハクティビスト

顧客

競合企業

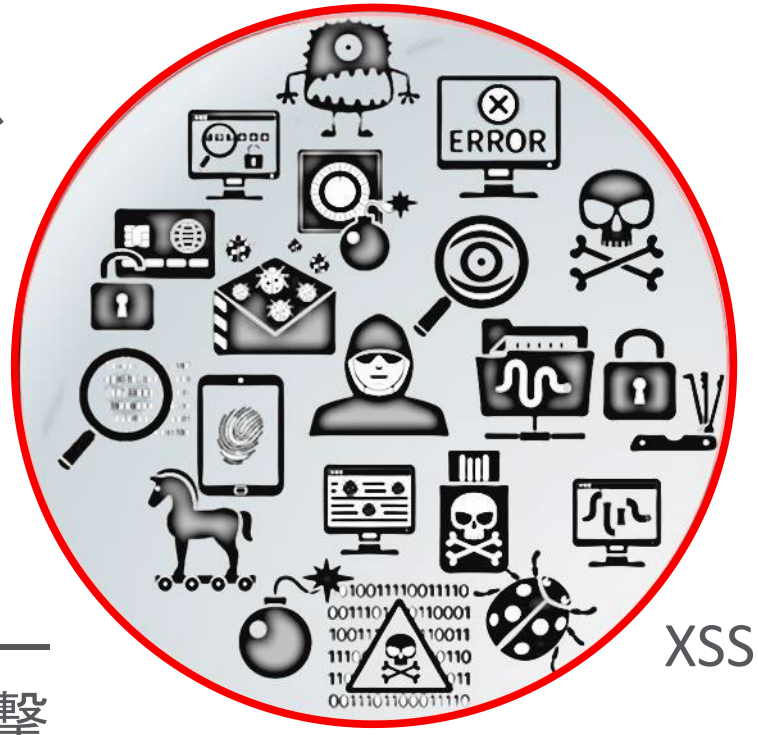
個人データ
財務データ
企業秘密
規制データ



進化する攻撃ツールとテクニック

盗んだ資格証明

フィッシング



SQLインジェクション

バッファ・
オーバーフロー

権限昇格

アプリケーション攻撃

XSS攻撃

パッチ未適用のシステム

思考の類似

攻撃者 vs データの所有者

内部関係者/部外者

オープン・ポート
データベースSID
既知のユーザー
一般的なパスワード
暗号化されたデータ
特権ユーザーに
対する監査
データベースの
バージョン
既知の脆弱性
有名なパッケージ・アプリ

開始点と探索対象

機密データはどこにあるのか?
ユーザーはだれで、そのエンタイトルメントは
何か?どんな制御機能を使用できるか?
使用中のデータベースはセキュアに構成されているか?

データベース・セキュリティ・チームは存在するか?
知識はどうか?分析時間はどうか?

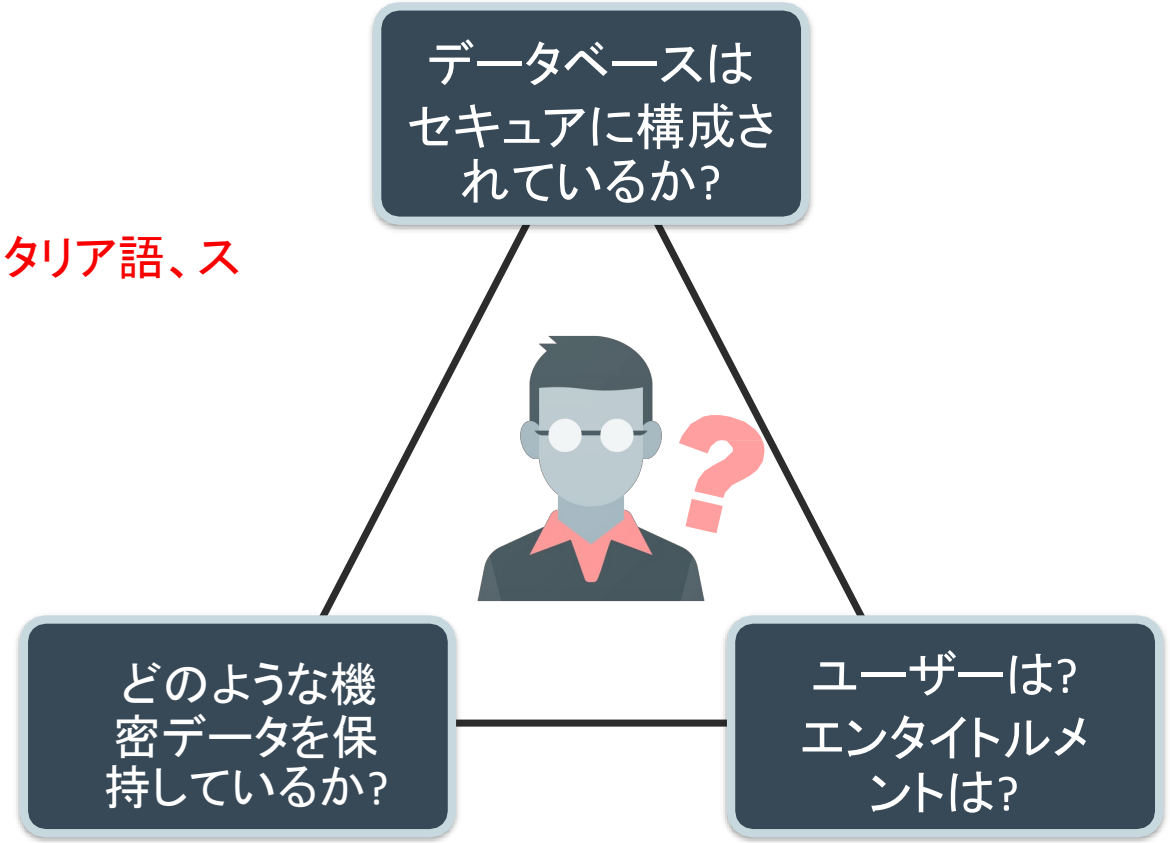
お試しください

Oracle Database Security Assessment Tool

Oracle Databaseセキュリティ評価ツール（DBSAT）

ハッカーに先を越される前に自社のセキュリティ態勢を把握する

- 自社のデータベースの安全性（脆弱性）を把握する
  - 全体的なセキュリティの現状を報告する
  - ユーザー、エンタイトルメント、リスクについて調べる
  - 機密データを英語、ドイツ語、オランダ語、フランス語、イタリア語、スペイン語、ポルトガル語 *で検索
- 実用的な評価レポート
  - サマリーと詳細情報
  - 優先順位付けされた推奨事項
  - EU GDPRおよびCISベンチマーク、STIG *との紐付け
- スタンドアロンの軽量なツール：迅速で、簡単
- 現在Oracleをご使用のお客様に無償提供



* 2.1の新機能

Oracle DBSATのチェック対象は?

1. **セキュリティ構成**
   - データ暗号化
   - 監査ポリシー
   - ファイングレイン・アクセス制御
   - データベースとリスナーの構成
   - OSファイル権限
   - セキュリティ・パッチ
2. **ユーザーとエンタイトルメント**
   - ユーザー・アカウント、権限、ロール
3. **機密データ**
   - どのような種類か、どこにあるか、どれほどあるか

Oracle Database 10g
以降が対象

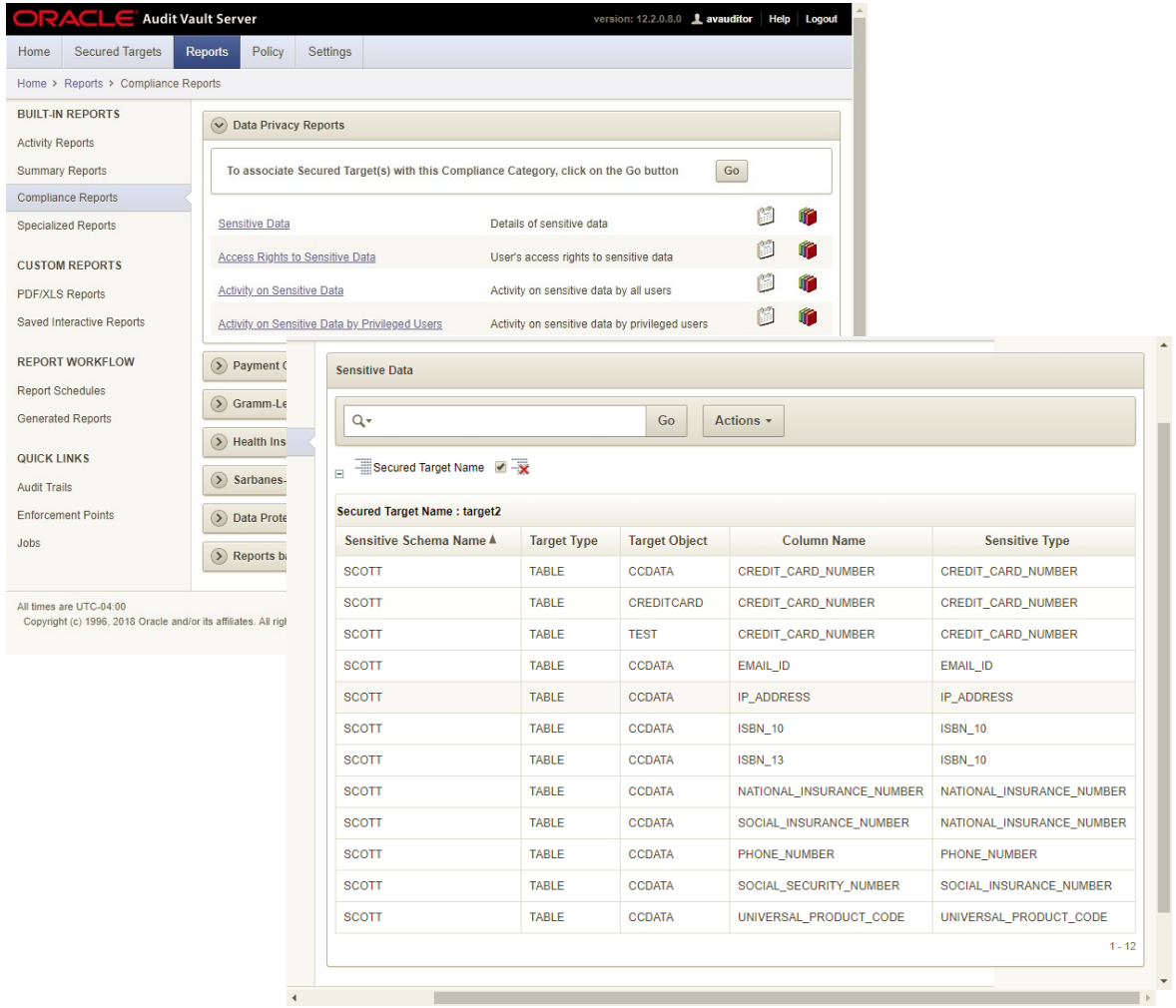
2.0.1 DBSATの新機能

- CISベンチマークの推奨事項への参照
- GDPRの条項/備考への参照
- 他のツールとの統合に使用できるJSON出力
- 機密データ検出機能の導入
  - 英語のパターン・ファイルが標準で付属
  - カスタマイズ可能

2.0.2 DBSATの新機能

7月に導入

- Discovererとデータベース・サーバーのSSLチャネル経由での接続をサポート
- Exadata Express Cloud ServiceおよびAutonomous Data Warehouseでの機密データの検出
- 検出された機密データ列をAudit Vault and Database Firewallにインポートして新しいデータ・プライバシー・レポートを作成可能



2.1.0 DBSATの新機能

NEW

- STIGルールの強調表示
- パスワード・ファイル、グローバル名、インスタンス名、RMANバックアップ等に対する新しい評価結果
- 直接付与されたシステム権限の特定の簡素化
  - (D)マークで明示
- Oracle Database 18c、19cおよびAutonomous Databasesに対する動作保証

- ドイツ語、オランダ語、フランス語、スペイン語、イタリア語、ポルトガル語に対応した機密情報パターン・ファイルが付属
- 新しい機密タイプ、カテゴリ、サブカテゴリ
- 機密データのカテゴリをリスク・レベルでグループ化
- リスク・レベルに応じた注釈および推奨される制御をレポートに掲載

操作方法

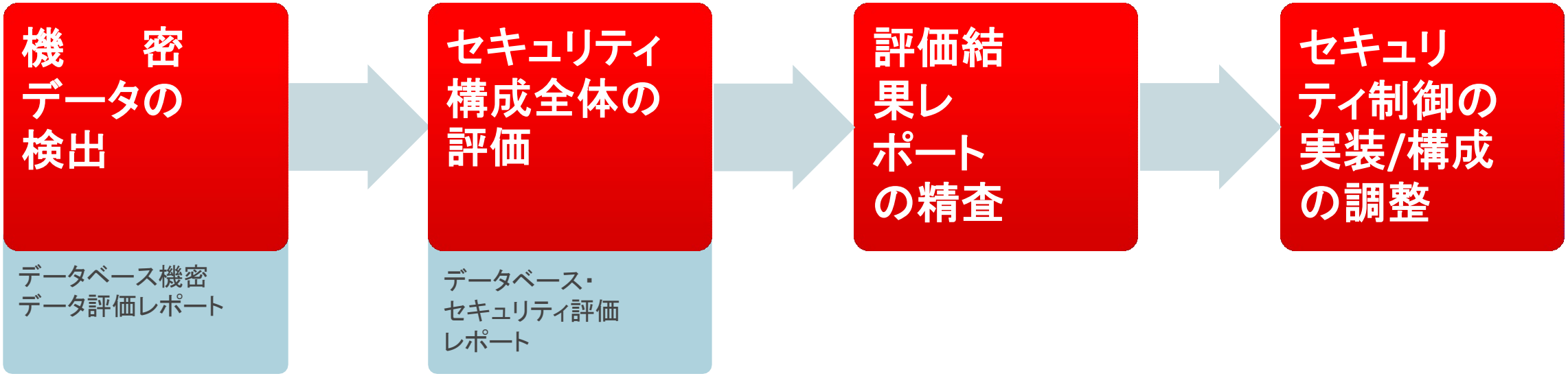
Oracle Database Security Assessment Tool

ダウンロードして3ステップを実行するだけ

1. ダウンロード
   https://www.oracle.com/jp/database/technologies/security/dbsat.html
2. データベース・セキュリティ評価レポートを入手
   - DBSAT Collectorを実行
   - DBSAT Reporterを実行
3. データベース機密データ評価レポートを入手
   - DBSAT Discovererを実行

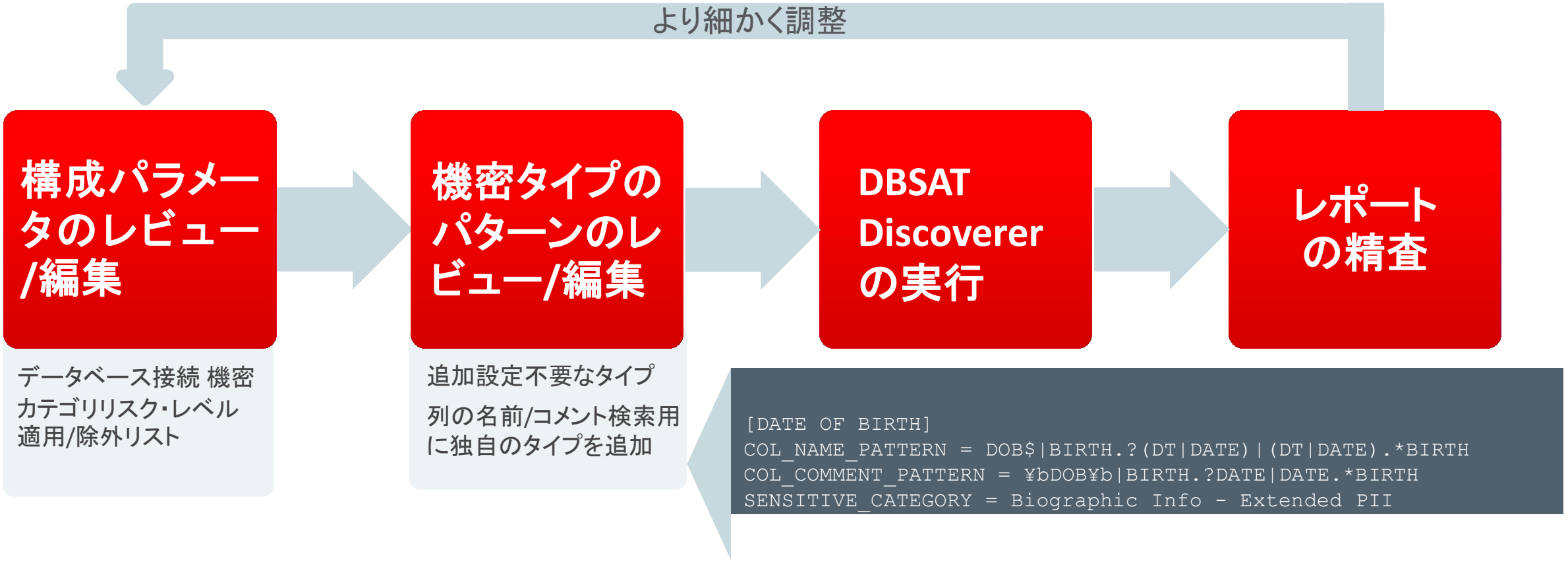
例：データ・プライバシーへの取組みを進めるための評価フロー・ステップ

検出から推奨事項まで



機密データの検出

何を、どこに、どのくらい持っているかを把握する



レポート：どのような機密データを、どのくらい保持しているか?

機密データの状況

カスタマイズ
可能なカテゴリ

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****

* 機密データが含まれる一意の表数
** 機密データが含まれる一意の行数

レポート：推奨される制御

NEW

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***

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

例

機密情報の操作を監査する データを暗号化する
テスト/開発時はデータをマスクする

レポート:どのテーブルに、どれくらいの機密データが含まれているか?

機密情報を含む表のサマリー

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
HCM1	EMP_EXTENDED	3	3	107	FINANCIAL INFO – CARD DATA, IDENTIFICATION INFO – PERSONAL IDS, JOB INFO – EMPLOYEE DATA

暗号化 /特権ユーザー・アクセス/プロセッサ制限の候補表?

レポート:どの列に、どれくらいの機密データが含まれているか?

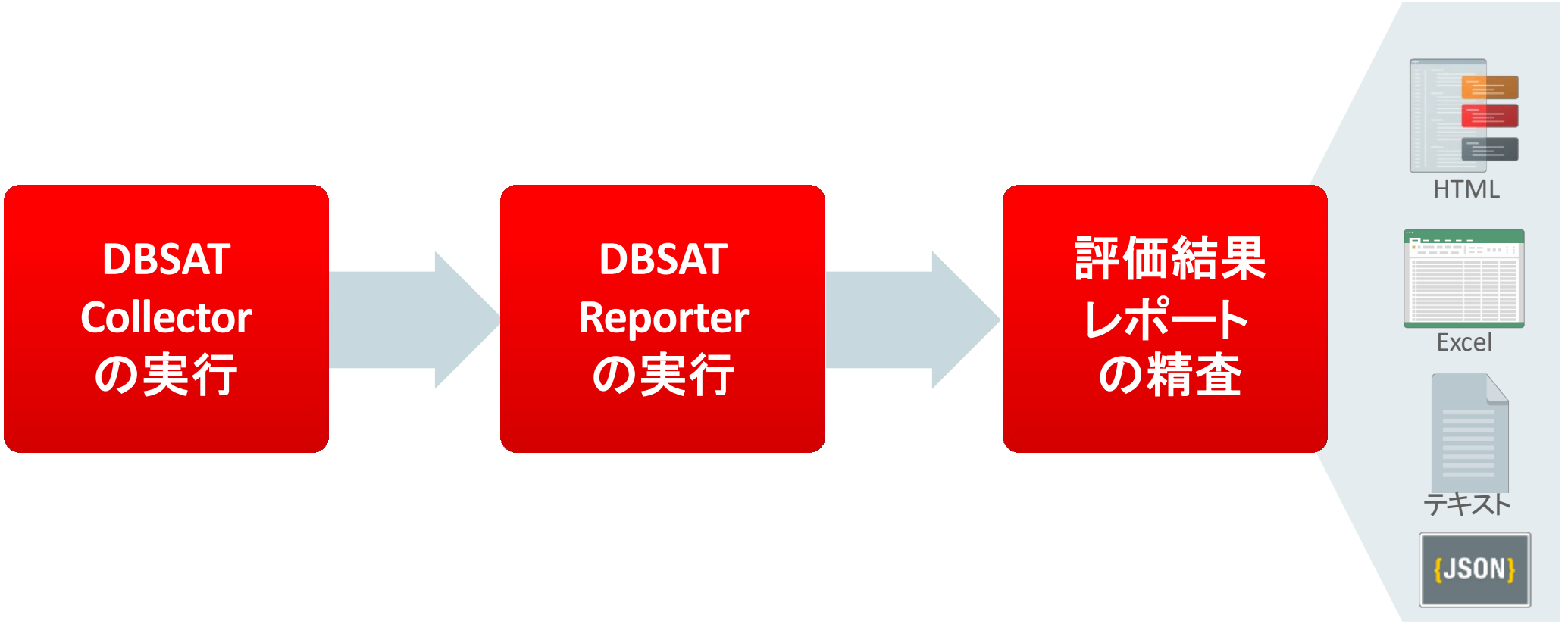
機密データのある列の詳細

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
HCM1	DEPARTMENTS	DEPARTMENT_NAME	--	JOB INFO - ORG DATA	DEPARTMENT NAME	Low Risk
HCM1	EMPLOYEES	EMAIL	This is the email ad...	IDENTIFICATION INFO - PUBLIC IDS	EMAIL ADDRESS	High Risk
HCM1	EMPLOYEES	EMPLOYEE_ID	This is the unqiue e...	JOB INFO - EMPLOYEE DATA	EMPLOYEE ID NUMBER	High Risk
HCM1	EMPLOYEES	FIRST_NAME	--	IDENTIFICATION INFO - PUBLIC IDS	FIRST NAME	High Risk

マスキング、仮名化、監査ポリシーの候補列

データベース・セキュリティ評価レポート

セキュリティ構成ステータス、ユーザーとそのエンタイトルメント



評価結果の分析

Evaluate、Advisory、Pass、Low Risk、
Medium Risk、High Riskのいずれか

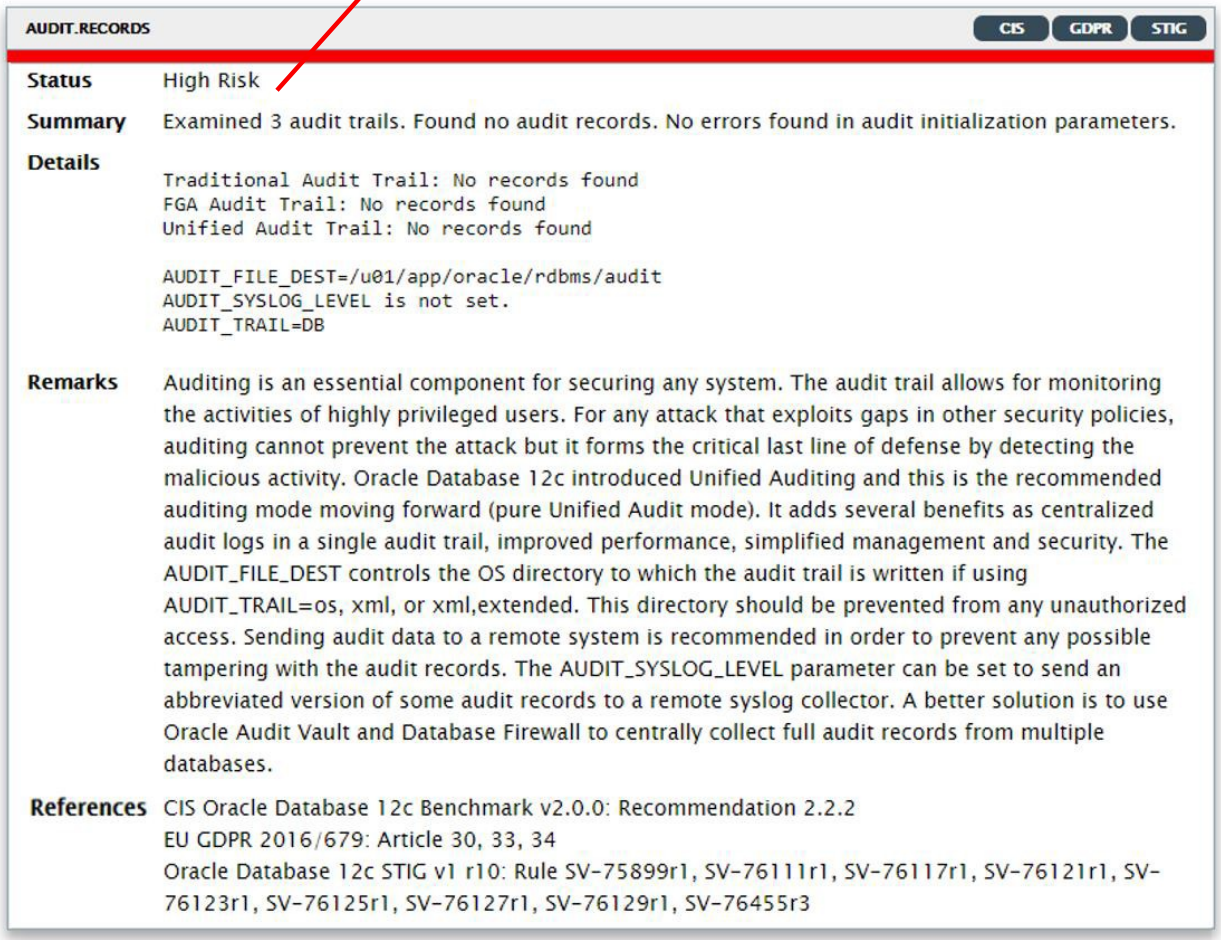
評価結果の
カテゴリ

関連する
可能性が
ある規制

評価結果の詳細

根拠と推奨事項

規制との
マッピング



ユースケース：データベースはセキュアに構成されているか?

評価結果のサマリー表示、優先度別

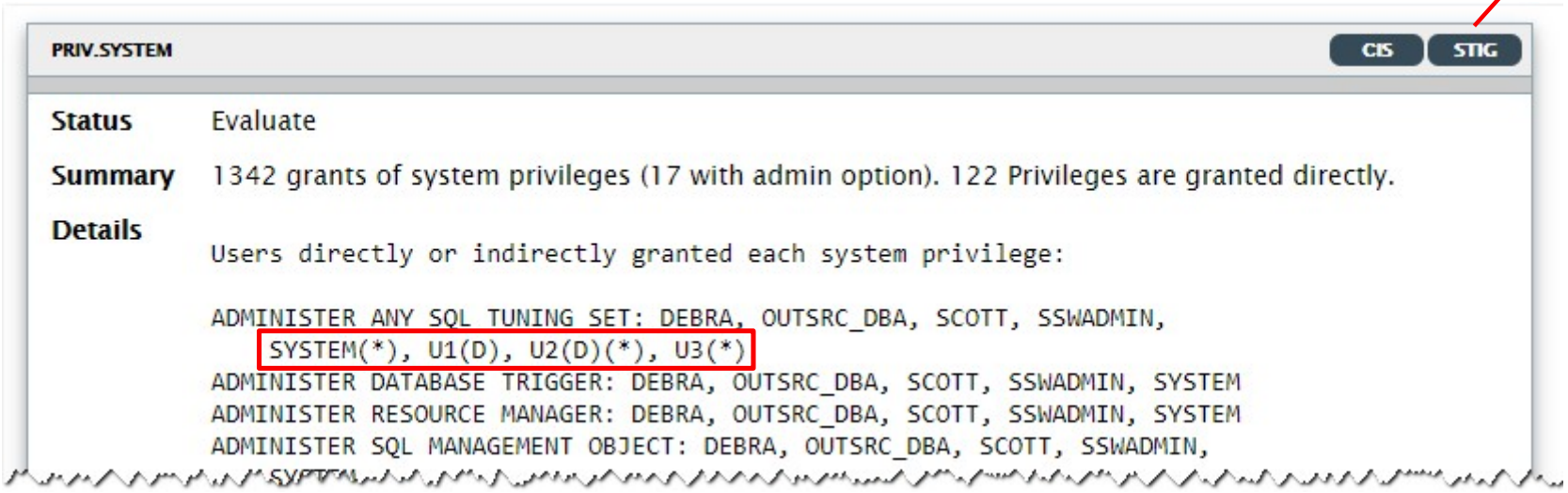
Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	**1**
User Accounts	5	0	0	4	2	1	**12**
Privileges and Roles	5	16	0	0	0	0	**21**
Authorization Control	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	1	4	0	0	0	**5**
Auditing	0	4	2	0	6	0	**12**
Encryption	0	1	1	0	0	0	**2**
Database Configuration	5	3	0	3	2	1	**14**
Network Configuration	1	1	0	0	3	0	**5**
Operating System	1	0	0	2	1	1	**5**
Total	**17**	**27**	**8**	**9**	**14**	**4**	**79**

NEW

ユースケース：ユーザーとそのエンタイトルメントは?

直接付与されたシステム権限

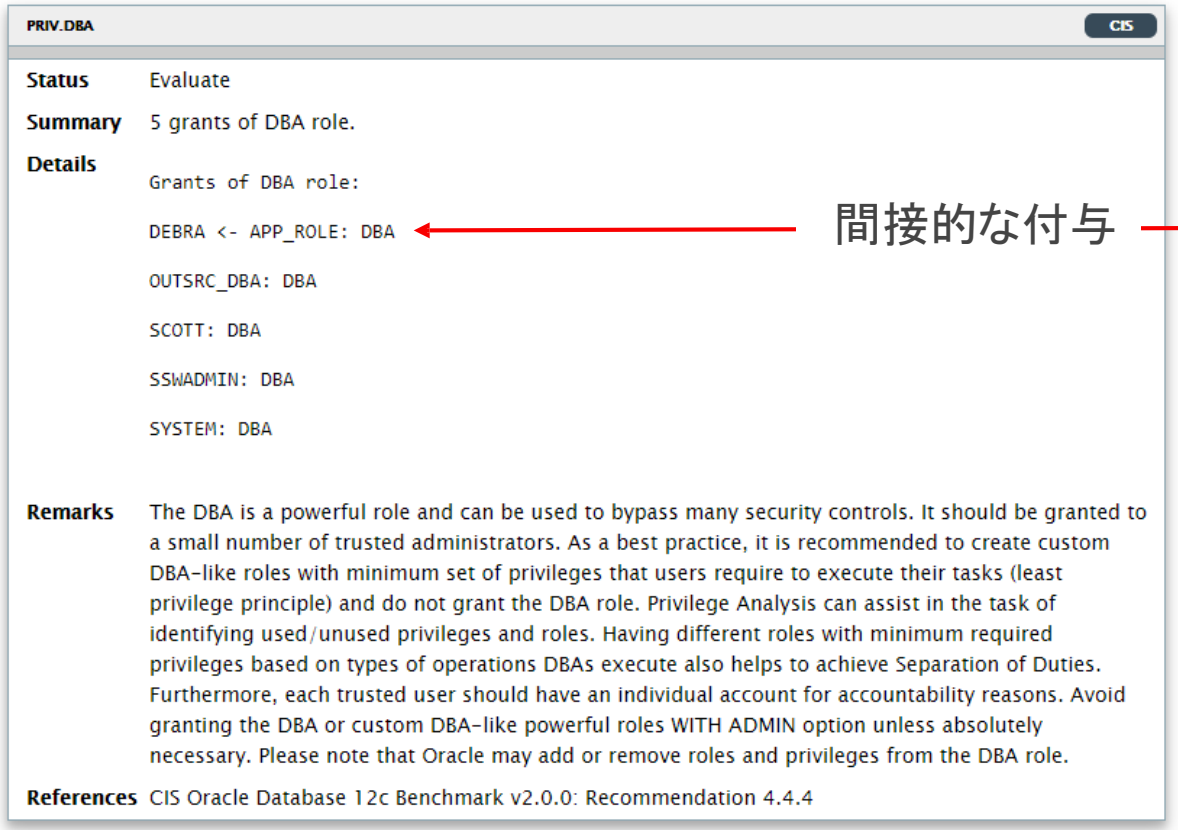
STIGの強調表示



(D) – 直接付与 (*) – 管理者オプション付き

ユースケース：ユーザーとそのエンタイトルメントは?

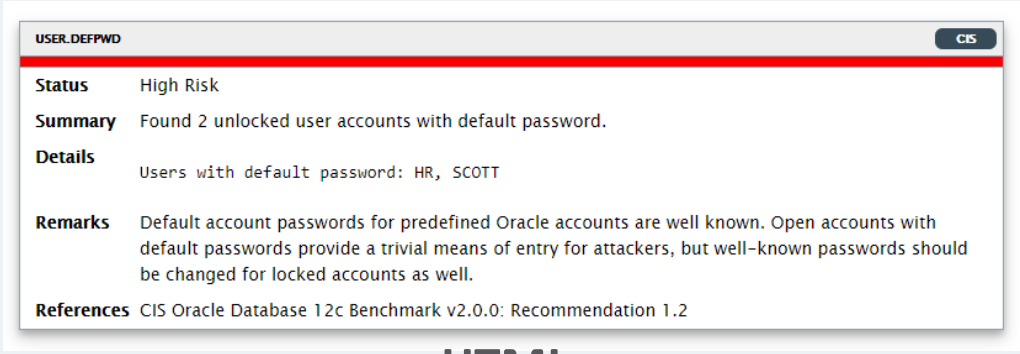
DBAロール（直接または間接付与）のあるユーザー



間接的な付与

ユーザーDEBRAはロールAPP_ROLE経由でDBAロールを間接的に付与されている

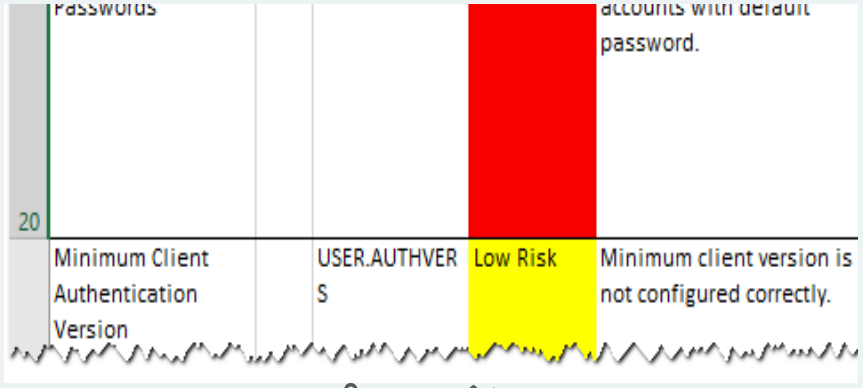
複数のレポート形式



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



スプレッドシート

```
205
206  * Users with Default Passwords *
207  Status: High Risk
208  Summary:
209      Found 2 unlocked user accounts with default password.
210  Details:
211      Users with default password: HR, SCOTT
212  Remarks:
213      Default account passwords for predefined Oracle accounts are well
214      known. Open accounts with default passwords provide a trivial means of
215      entry for attackers, but well-known passwords should be changed for
216      locked accounts as well.
217  References:
218      CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2
219
```

テキスト

すぐに始めましょう
攻撃はすでに始まっています!

インストールと実行が容易

- 下のURLからDBSAT 2.1を今すぐダウンロードする
  https://www.oracle.com/jp/database/technologies/security/dbsat.html
- サポート契約が有効なすべてのOracleデータベースのお客様がダウンロード可能

- ターゲットで'dbsat collect'を実行してセキュリティ構成データを収集する
- ターゲットまたは他の場所で‘dbsat report’　　を実行する
- ターゲットで‘dbsat discover’を実行して機密データ・レポートを生成する
- 機密データが含まれるため、生成されたレポートへのアクセスを制限する

開始点と探索対象

機密データはどこにあるのか?
ユーザーはだれで、そのエンタイトルメントは何か?
どんな制御機能を使用できるか?
使用中のデータベースはセキュアに構成されているか?

データベース・セキュリティ・チームは存在するか?
知識はどうか?分析時間はどうか?

まとめ

- ハッカーに先を越される前に、データベースの現在のセキュリティ状態を迅速に評価する
- 機密データを特定して、リスクと適切なセキュリティ管理を見極める
  - 英語および欧州の主要言語に対応
- 効果が証明されているベスト・プラクティス（CISおよびSTIG）を使用して、リスクへの露出を減らす
- EU GDPRや他の規制の順守を推進する
- Oracle Database 10g、11g、12c、18c、19cおよびAutonomous DBをサポート
- 追加費用なしで提供
- すぐにデプロイして使用できる

今すぐダウンロードしてください

- OTNのページ
- ソーシャル・ネットワークでは**#DBSAT**をご利用ください

- **データベース・セキュリティとGDPRホワイト・ペーパー**
  https://go.oracle.com/LP=54366
- **GDPRに関する詳細情報**
  www.oracle.com/goto/gdpr
- **データベース・セキュリティに関する詳細情報**
  http://oracle.com/database/security

Q & A

オラクルの情報を発信しています

/OracleDatabase
#DBSAT

/OracleSecurity

blogs.oracle.com/
SecurityInsideOut

Oracle Database Insider

/Oracle/database

/OracleLearning

oracle.com/database/security

oracle.com/technetwork/database/security

Integrated Cloud

Applications & Platform Services