ORACLE Database

Oracle Database Security Assessment Tool

データ侵害が日々増え続け、データ保護やプライバシーに関する一連の規制が進化し続けている中で、ビジネスの機密データと規制対象データを保護することは不可欠です。しかしながら、データベースはセキュアに構成されているのか、どのようなユーザーがそのデータベースにアクセスできるのか、また機密の個人データはどこに保存されているのかを、ほとんどの組織が把握しきれずにいます。オラクルの多層防御機能の一部であるOracle Database Security Assessment Tool（DBSAT）は、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定し、リスクを緩和するために必要な変更内容と制御方法を提案します。

進化する規制の順守

セキュリティ構成の調査は、EU一般データ保護規則（EU GDPR）、PCIデータ・セキュリティ・スタンダード（PCI DSS）、多数の侵害通知法をはじめとする多くの規制において、重要な要素となっています。Center for Internet Security（CIS：米国インターネット・セキュリティー・センター）、米国国防総省など、さまざまな組織も、セキュリティ構成のベスト・プラクティスに関する推奨事項を設けています。新たな規制が発表され、多くの組織のもっとも価値ある資産、すなわちデータを保護するべく既存の規制が進化している中で、セキュリティ制御の重要性を軽視することはできません。

新たな制御を実装する前に組織が直面する最大の課題の1つは、自社のデータベースのセキュリティ対策状況を把握することです。組織は、データベースがどのようにセキュアに構成されているか、機密データがどこに保存されているか、機密データをどの程度保持しているか、どのユーザーが機密データにアクセスできるか、それらのユーザーはどのような権限を有しているか、そしてどのようなセキュリティ制御が実装されているかを迅速に特定する必要があります。

データベースがオンプレミスで実行されていようと、クラウドで実行されていようと、Oracle Database Security Assessment Tool（DBSAT）は、潜在的な機密データを発見し、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定します。DBSATは、異なる種類のデータをデータベースから収集し、分析することで、セキュリティ・リスクを特定します。さらに、それらのリスクを緩和するために必要な変更内容と制御方法を提案します。

ビジネス上のおもなメリット

- 現在のセキュリティ状態を迅速に評価し、Oracle Database内の機密データを特定
- 実績のあるOracle Database Securityのベスト・プラクティス、STIG、CISベンチマークの推奨事項を使用して、リスクの発生を低減
- セキュリティ評価結果を活用して、EU GDPRや他の規制の順守を迅速化
- 価値あるレポートを数分以内にインストールして提供
- オラクルのお客様には追加費用なしで提供

おもな機能

- リスクの発生を増加させる可能性のある構成の設定を特定
- 慎重に扱うべきユーザー・アカウントとその権限、およびセキュリティ・ポリシーを特定
- 英語のデータ・ディクショナリと欧州の主要言語による機密データの発見
- 適切なセキュリティ制御を推奨および優先順位付け

ORACLE

ハッカーのように考える

攻撃者は通常、標的を理解するために相当な時間を費やします。データベース、オープン・ポート、既知の脆弱性、および特権ユーザー・アカウントの発見を自動化するツールを複数使用する可能性があります。その後で、パスワード窃盗、総当たりパスワード・クラッキング、権限昇格攻撃、SQLインジェクション攻撃など、さまざまな攻撃を仕掛けます。厳密な調査が終了すると、もっとも脆弱なリンクを特定し、次のステップを決定します。攻撃者は、基本的にまず現在のセキュリティ状態を評価し、捕まることなく機密データにアクセスできるもっとも容易な方法を見つけます。

たとえば、データが暗号化されている場合は、おそらく権限を持つユーザーとしてデータベースにアクセスする必要があります。デフォルトのパスワードを使用しているユーザーはいますか?権限を昇格できますか?監査が実施されていますか?どのユーザーがDBAと同様の権限を持っていますか?このデータベース・バージョンにはどのような既知の脆弱性がありますか?その脆弱性にはパッチが当てられていますか?どのようなパッケージ・アプリケーションが実行されていますか?それらのアプリケーションは強力なシステム権限を使用して実行されていますか?どのような種類の機密データを処理しますか?このような問いのほかにも数多くの問いがハッカーの頭の中にあり、その解答が、データベースに侵入し、データを盗むための計画を思いつくのに役立ちます。

組織は、データの所有者、管理者、処理者として、ハッカーと同じように考える必要がありますが、その目的は、ハッカーが自社のデータベースを標的にする前に、セキュリティ態勢を改善することです。

現在のセキュリティ状況を評価し、不意を突かれないようにするために何が必要であるかを把握しているにもかかわらず、多くの組織は、データベース・セキュリティ専門家がいない、時間が不足している、適切な優先順位付けができない、リスクを誤解しているなどの理由から、自社のデータベース・セキュリティを評価することに苦心しています。データベースの保護方法に関する知識が、DBAと、ネットワークやエンドポイントの保護をもっとも重視しているITセキュリティ・チームとに、組織的に分散されている場合もあります。

Oracle DBSATは、適切な種類の構成情報をデータベースから収集し、現在のセキュリティ状態を評価することで、評価プロセスを迅速化させるとともに、特定されたリスクを緩和する方法を提案します。DBSATは、データベースがどの程度セキュアに構成されているか、どのようなユーザーがデータベースにアクセスでき、それらのユーザーはどのような権限を有しているか、どのようなセキュリティ・ポリシーが導入されているか、どのようなセキュリティ制御が実装されているか、機密データはどこに保存されているかを素早く表示します。以下の図は、サンプル・データベースのセキュリティ状態をまとめたものであり、評価結果をリスク・レベルで分類しています。

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**

図1：Oracle Databaseの現在のセキュリティ状態の概要

DBSATは、一連の評価結果という形で、分析の結果を報告します。それぞれの評価結果では、ステータスの概要、リスク・レベル、サマリー、詳細、および参考資料を必要に応じて提供します。また、結果がOracle DatabaseのSTIGルール、Center for Internet Security（CIS）ベンチマークの推奨事項、またはGDPRの条項/備考に関連しているかを指摘します。以下の2つの評価結果は、どのユーザーが強力なDBAロールを有しているか、そのロールはどのように取得されたか（直接付与、他のロール経由の付与）、およびパスワードがデフォルトのままのユーザーを示しています。

関連製品
Oracle Databaseの多層防御セキュリティ製品：

- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting
- Oracle Label Security
- Oracle Audit Vault and Database Firewall

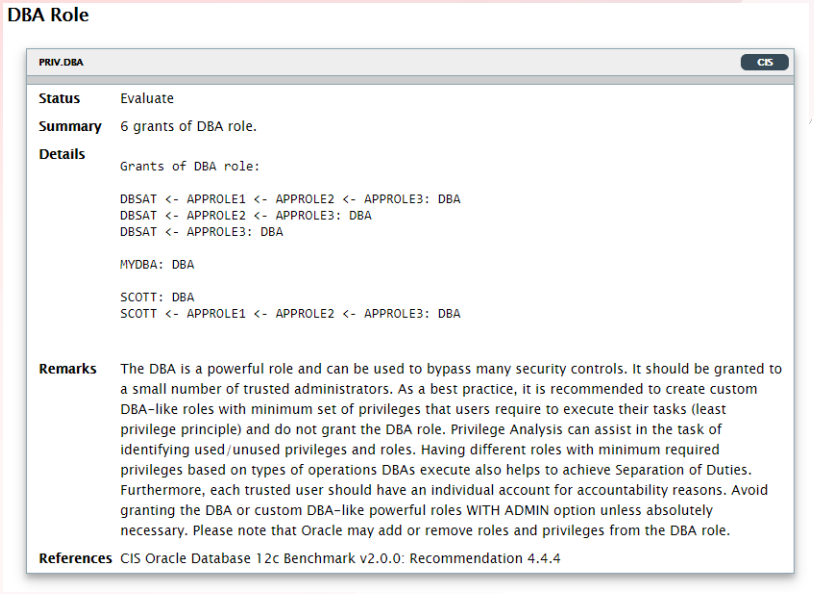

図2：強力なDBAロールを有するユーザー

上の例では、ユーザーSCOTTは他のロールが付与されたことによって（APPROLE3、APPROLE2、APPROLE1の順で）間接的にDBAロールを取得しており、MYDBAユーザーはDBAロールを直接付与されていることがDBSATのレポートに示されています。

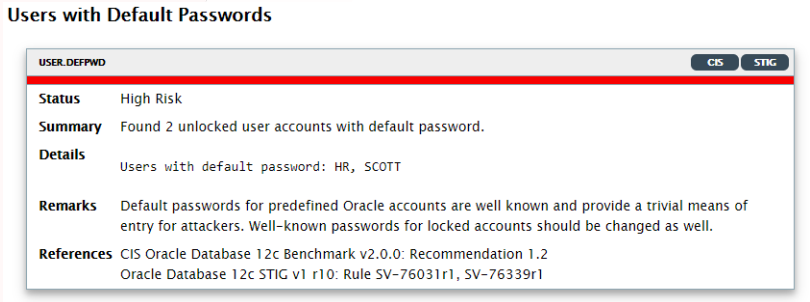

図3：デフォルトのパスワードを使用しているユーザー

評価結果は、HTML、Microsoft Excel、JSON、テキスト・ファイルなど、複数の形式で提供されるため、組織はこのデータを構成やリスク管理ツールの一部として組み込むことができます。

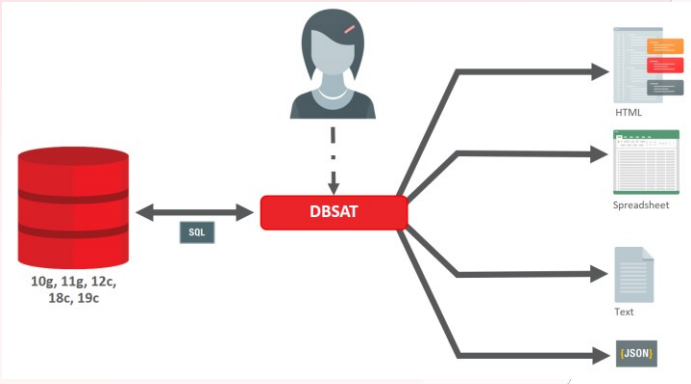

図4：DBSATレポート

機密データの発見

EU GDPRなどの規制により、組織は個人情報（PII）データを保護することが義務付けられていますが、まずどのような個人データがどこに保存されているかを把握する必要があります。

DBSATは、カスタマイズ可能な正規表現パターンを使用して機密データのデータベース・メタデータをスキャンし、発見された機密データの量と種類を報告します。機密データは、英語のデータ・ディクショナリ（列名およびコメント）を使用して検索できるほか、ヨーロッパの主要言語（オランダ語、フランス語、イタリア語、ドイツ語、ポルトガル語、スペイン語など）でも検索できます。これにより、保有している機密データの量とその存在場所についてより詳しく把握できるため、アクセス制御、監査、マスキング、暗号化を適切に実施してデータベースを保護できます。以下の図は、データベース・メタデータのスキャンを基に作成されたサマリー・レポートです。

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**

図5：機密データ状況のサマリー

まとめ

機密データがどこにあり、どのように構成されているかを把握することは、多層防御戦略を実装する上での基礎となります。100 %セキュアなシステムはありませんが、基礎に目をつぶることは、攻撃者の侵入を容易にするだけです。

Oracle Database Security Assessment Tool（DBSAT）は、機密データを素早く発見し、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定します。

DBSATは、有効なサポート契約を結んでいるオラクルのお客様には追加費用なしで提供されます。
詳細およびDBSATのダウンロードについては、www.oracle.com/jp/database/technologies/security/dbsat.htmlを参照してください。

CONNECT WITH US

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。
北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services