Impervaで実現するRDSの監査およびデータセキュリティ

株式会社Imperva Japan

2018年6月1日

IMPERVA®

Agenda

1. Impervaについて
2. 今、あなたのデータのリスク管理は万全ですか？
3. 膨大なDB監査ログを活用しませんか？
4. Imperva Database Security for Amazon RDS
5. まとめ

1

Impervaについて

IMPERVA®

会社概要

事業	セキュリティ製品の開発、販売
設立	2002年（2011年11月 NYSE上場）
本社	米国カリフォルニア州 Redwood Shores
CEO	Christopher Hylen
CTO	Terry Ray
創業者	Shlomo Kramer、Amichai Shulman、Mickey Boodaei
従業員数	1,100名
日本法人	株式会社Imperva Japan 2007年設立　　代表：長坂 美宏
パートナー	マクニカネットワークス、ソフトバンク・テクノロジー、NRIセキュアテクノロジーズ、ネットワークバリューコンポネンツ、富士通、NEC、日立など
実績	100カ国＋での500+パートナーと事業を展開
顧客	6,200社＋、100,000組織＋（クラウド）

IMPERVA®

IMPERVA®

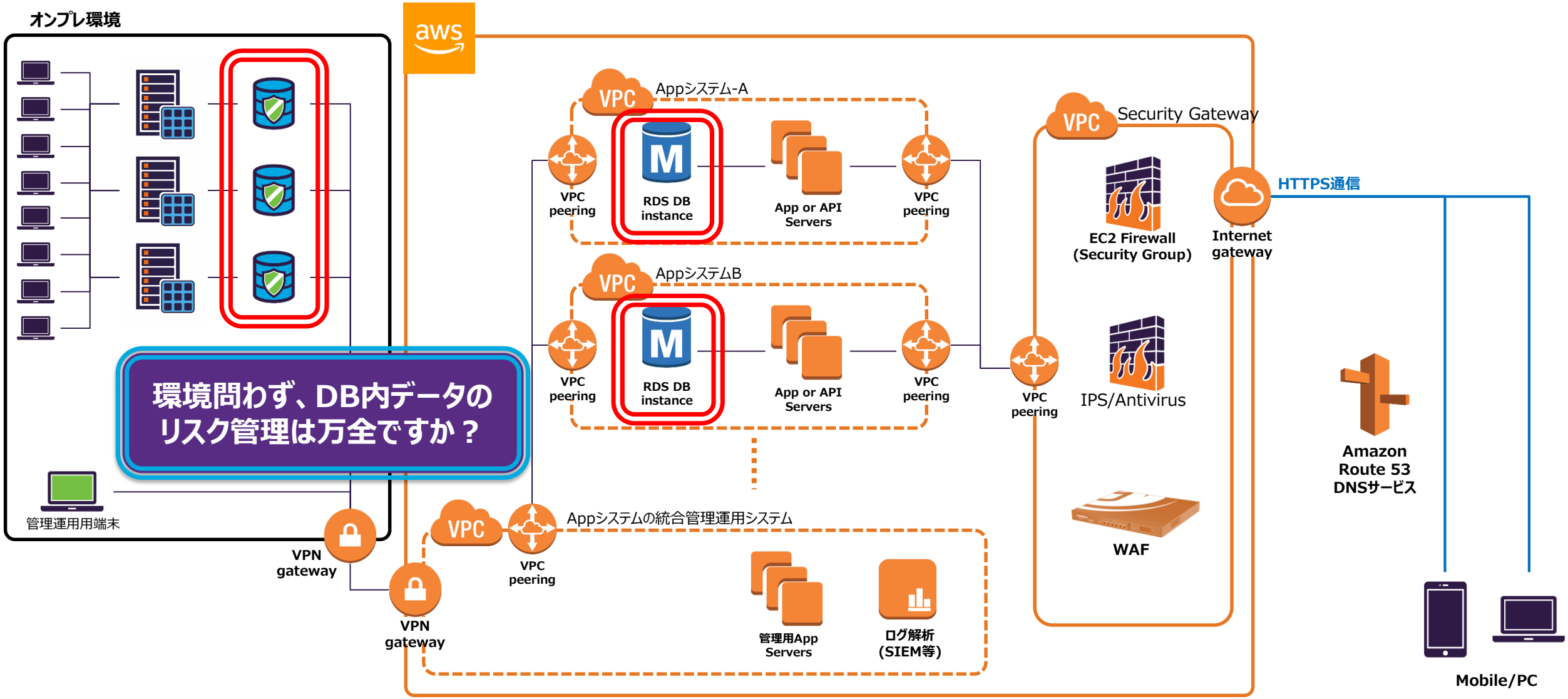
2

Impervaで実現するRDSの監査およびデータセキュリティ

今、あなたのデータのリスク管理は万全ですか？

IMPERVA®

セキュリティチェック - AWS上のDatabase vs オンプレのDatabase



IMPERVA®

AWSの責任共有モデル

	AWS	Customer
OS Maintenance	✓	
Database Maintenance	✓	
Durability/Availability	✓	✓
Performance	✓	✓
Data		✓

【　重要！】お客様のデータに関するリスクはお客様が負う
パブリッククラウドでもオンプレミスと同様にリスク管理は必須

IMPERVA®

3

Impervaで実現するRDSの監査およびデータセキュリティ

膨大なDB監査ログを活用しませんか？

IMPERVA®

監査ログをImpervaが処理した結果

開発者が
1,100万レコード
を実環境DBから
取り出している

Developer pulls
11M records from
production DB

TOTAL NUM OF RECORDS
11,688,581

アナリストが
取引情報に
アクセスしている

Analyst accesses
trade information

TABLE/STORED PRCEDURE
exchangerate

データ管理者が
顧客のクレジットカード情報
にアクセスしている

DBA accesses
client credit
card records

TABLE/STORED PROCEDURE
client
clientcreditcard

契約社員が
人事情報に
アクセスしている

Contractor accesses
HR information

TABLE/STORED PROCEDURE
hrasurveyanswers

開発者が
管理者アカウント
を利用している

Developer uses
admin account

DB User:	besadmin
DB Name:	besmgmt

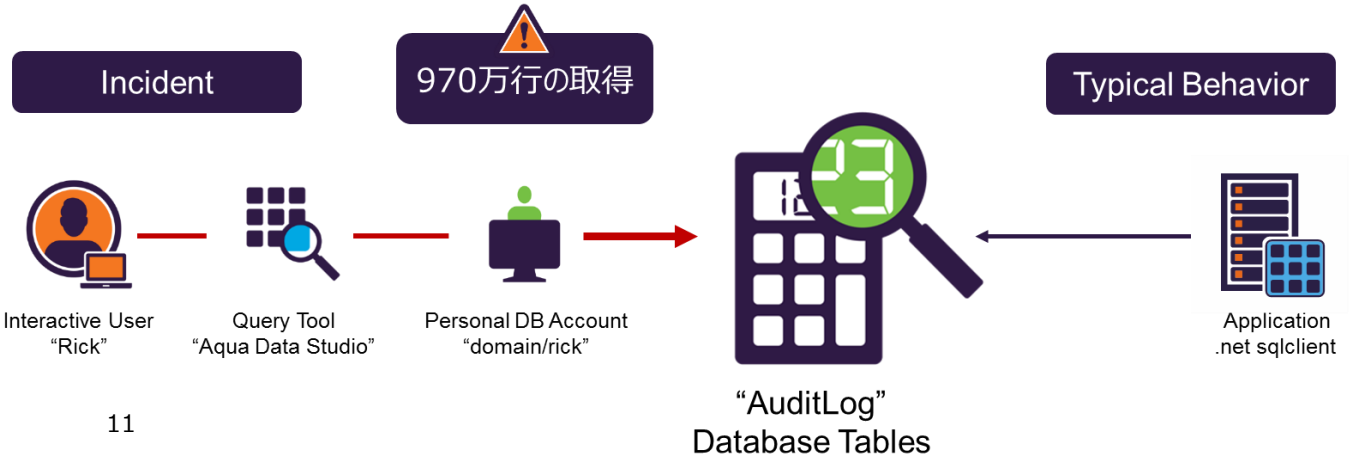
データ管理者が
200万レコード
の監査ログを見ている

DBA reads 2M
audit log records

NUM OF QUERIES	TOTAL NUM OF RECORDS
3	0
8	2,800,760

ユーザ事例：金融サービス

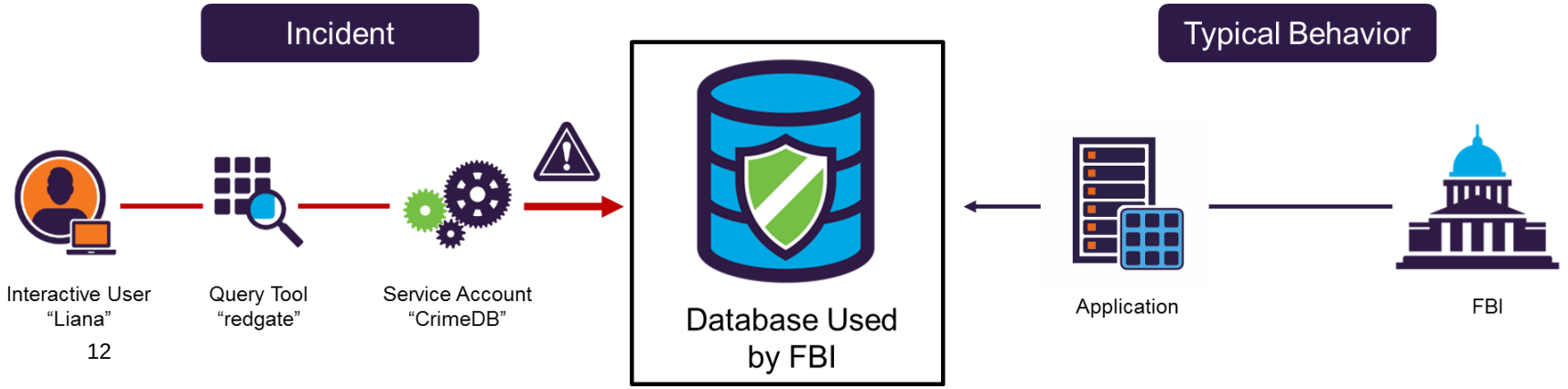
- **動機:** さまざまな規制対象のデータを保護しなければならない
- **課題:** 10万人以上の従業員のなかから、データ盗難を見つけ出さなければならない
  - DB にアクセス可能な特権ユーザ、DBA が最大の関心事
- **目的・効果:** 未知の内部脅威を発見するため、PoC を開始
- **所見:** Impervaソリューションによって、サービスアカウントを悪用したユーザによるインシデントを発見
  - ある特権ユーザが不適切にデータにアクセスしている疑いを発見
  - アプリケーションサーバからのログイン試行の失敗、および過剰な DB アクセスをインシデントとして検知



- サービスアカウント以外のインタラクティブユーザが auditlog テーブルから970万行を取得
- サービスアカウント以外のユーザでのクライアントツールからの直接アクセス
- 監査ログを改ざんしようとする試みを発見

ユーザ事例：公共交通機関

- **動機:** 大量の個人情報や知的財産を保有。取締役会、内部監査部門、法務部門から内部脅威への懸念が寄せられていた
- **課題:** SIEMでDB監査ログを分析。SIEMは多くのアラートと十分に利活用できない情報を提供
- **目的・効果:** PoVにおいて重大なインシデントを発見
- **所見:**
  - 悪意ある内部関係者による、FBI のみアクセスを許されている DB への直接アクセス
  - 重要な給与情報、人事情報などを含む DB への内部関係者による不適切アクセス



- 悪意ある内部関係者が高い権限を有するアカウントで重要 DB にアクセス
- アクセス制限を回避
- アクティビティが追跡不可能

DB監査ログをマシンラーニング、ピアグループ分析することにより ユーザデータアクセスのベースラインを構築

誰がデータベースに
アクセスしているか？

データベースへの
接続方法は？

どのデータに
アクセスしているか？

同僚も同じように
アクセスしているか？

どれくらいのデータに
アクセスしているか？

勤務時間は？

IMPERVA®

構築したベースラインによるプロファイリング～ユーザとデータ

アプリケーションからのアクセス？	Application 	or	Interactive User 
アカウントタイプは？	Service Account 	or	Personal DB Account 
アクセス先テーブルは？	Metadata 	or	Business Critical Data 
データベースの役割は？	Transaction Processing 	or	Data Warehouse 

継続的なデータアクセス監視

インシデント検知

インシデントタイプ
Database Access at Non-standard Time 標準時間外のデータベースアクセス
Database Service Account Abuse データベースサービスのアカウント濫用
Excessive Database Record Access 過度のデータベースレコードアクセス
Excessive Failed Logins 過度なログインの失敗
Excessive Failed Logins from Application Server アプリケーションサーバーからの過度なログインの失敗
Excessive Multiple Database Access 過度な複数データベースアクセス
Machine Takeover マシン（デバイス）の乗っ取り
Suspicious Application Data Access 不審なアプリケーションデータアクセス
Suspicious Database Command Execution 疑わしいデータベースコマンドの実行
Suspicious Dynamic SQL Activity 疑わしい動的SQLの実行

IMPERVA®

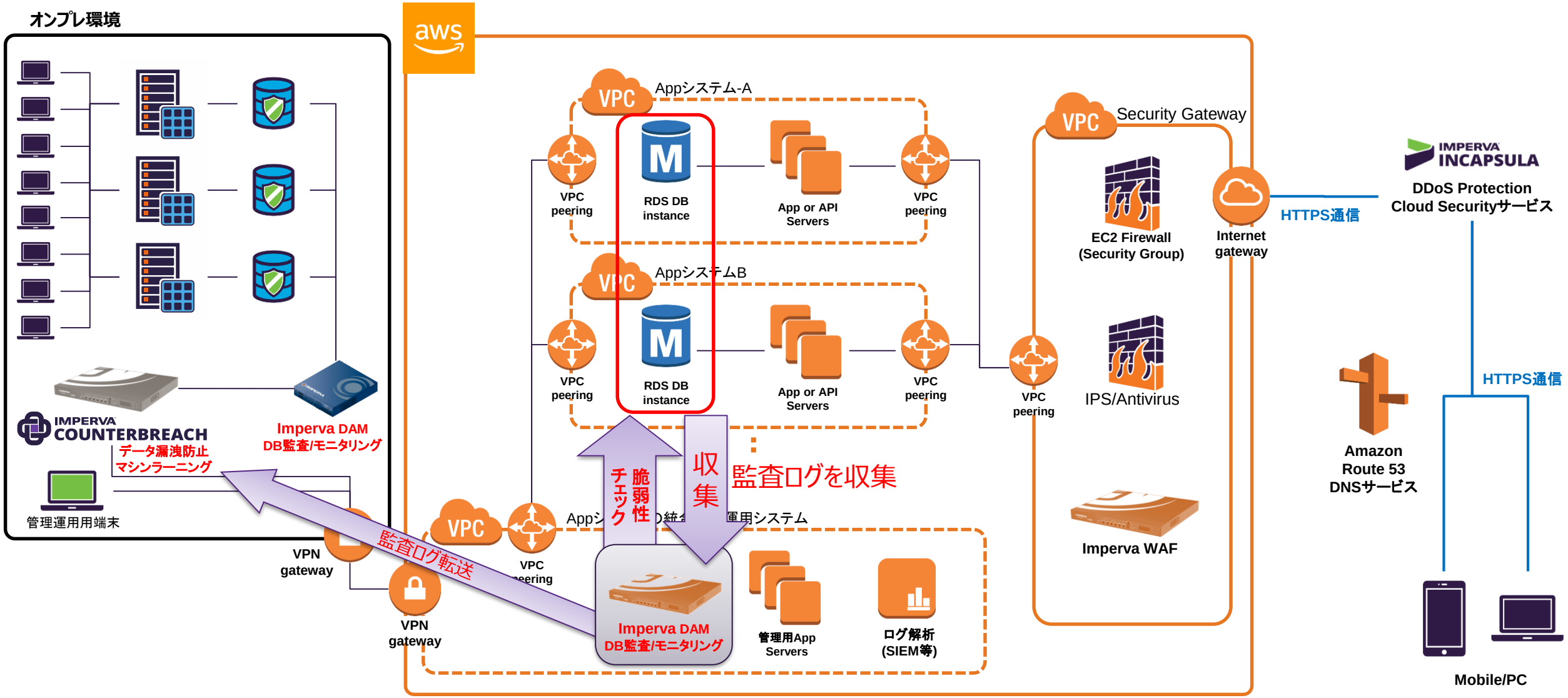
4

Impervaで実現するRDSの監査およびデータセキュリティ

Imperva Database Security for Amazon RDS

IMPERVA®

Imperva Database Security for Amazon RDS 構成イメージ



Imperva SecureSphere DAM for Amazon RDS 概要

- Ver 12.3よりAmazon RDSに対応
- セキュリティ機能は従来の仕様を継承
- 複数のDAMを管理サーバで一元管理
- 「ログコレクタ」を用いてDB監査ログを収集
  - DB側での監査ログ出力が必須

Model	AV2500 DAM	AVM150 MX 管理サーバ
スループット	500Mbps	-
ディスクスペース	80GB以上	80GB以上
インスタンスタイプ	c4.xlarge以上	c4.xlarge以上
提供方法	BYOL	BYOL

※BYOL=ライセンス課金

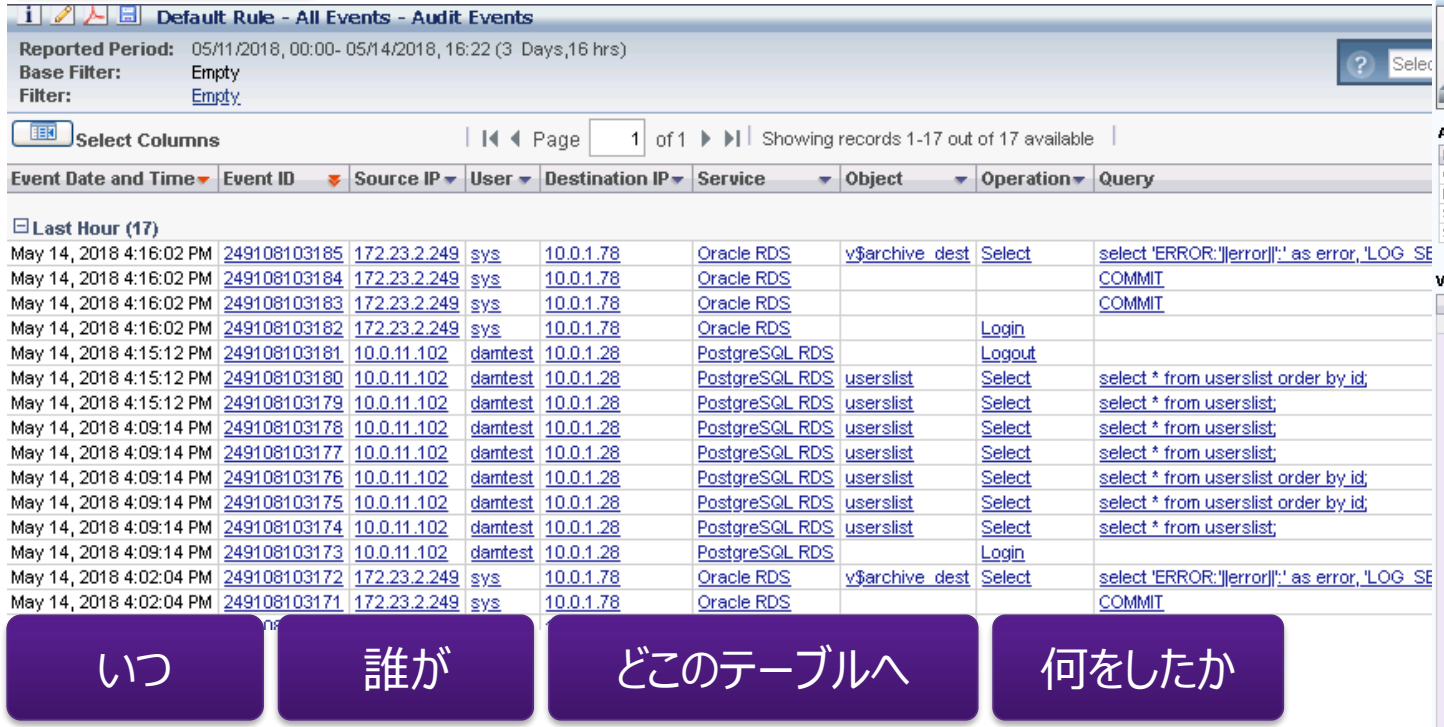
Imperva SecureSphere DAM for Amazon RDS 対応状況

Amazon RDS Database Engines

IMPERVA

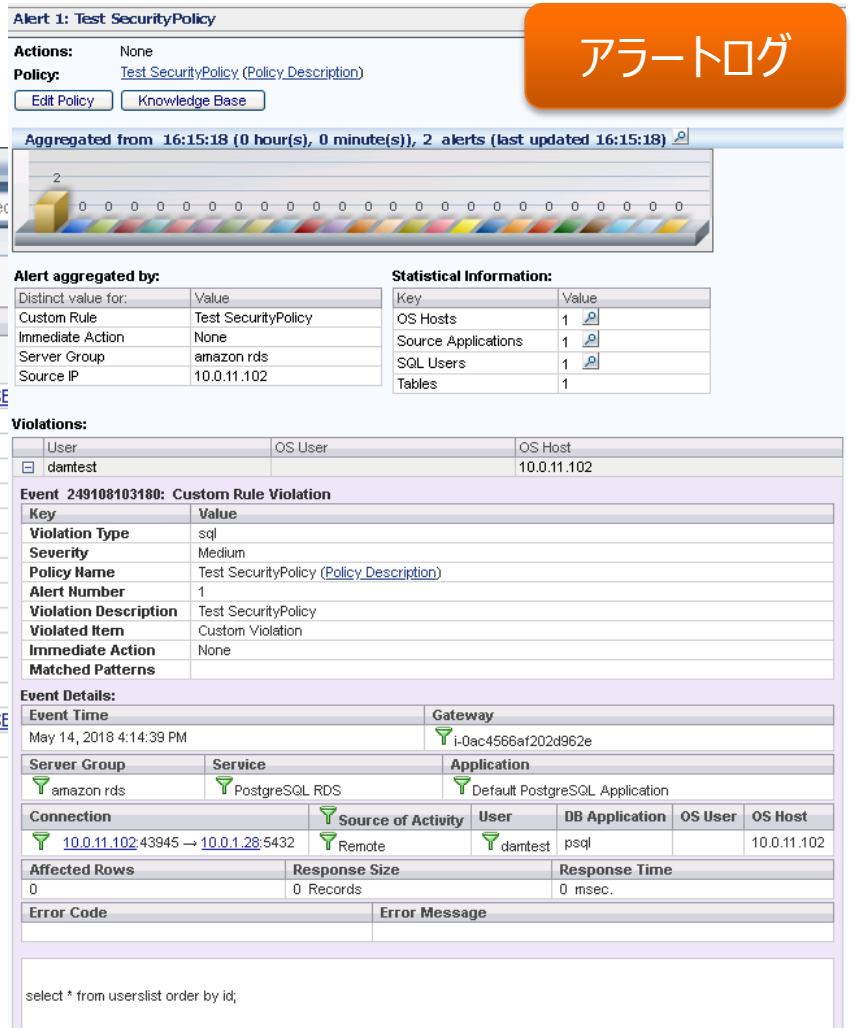
Imperva SecureSphere DAM for Amazon RDS
監査ログ・アラート

監査ログ

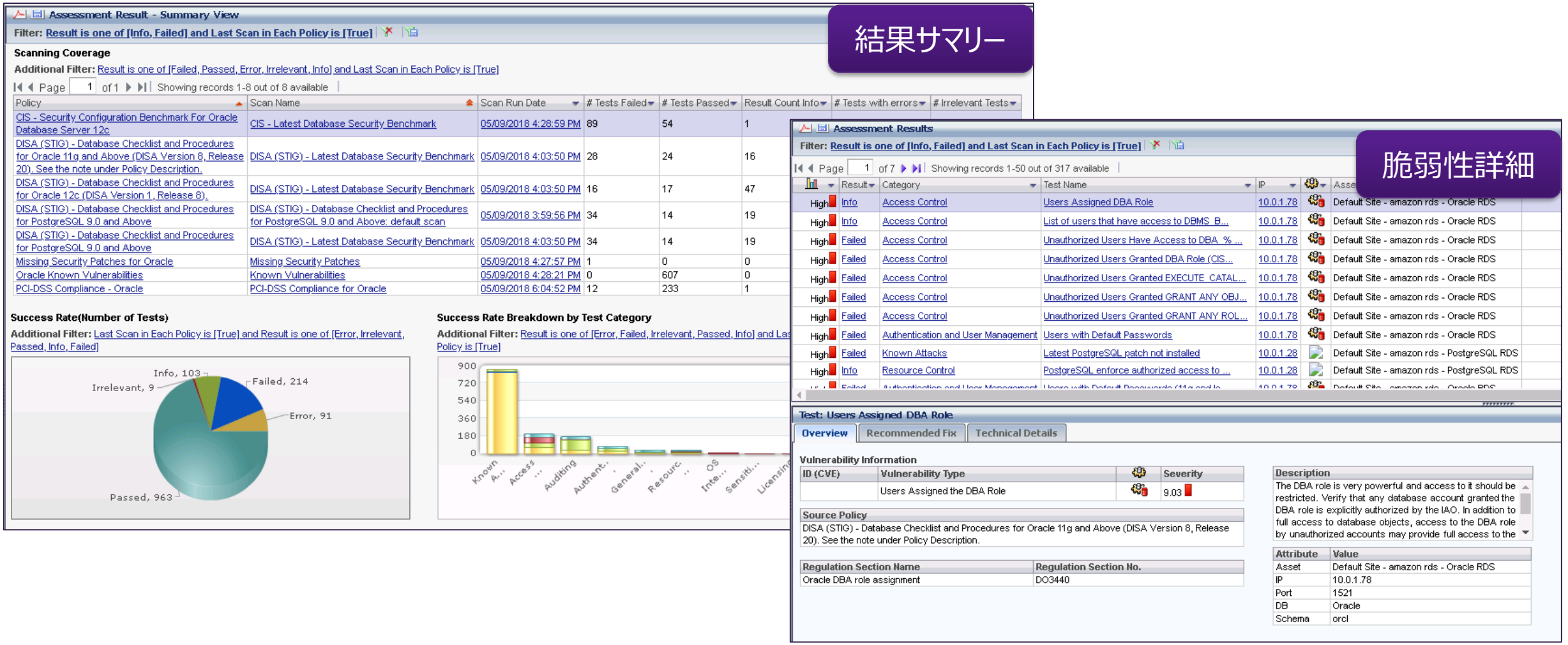


いつ　誰が　どこのテーブルへ　何をしたか

アラートログ



DB Assessments Scan機能 for Amazon RDS サンプル

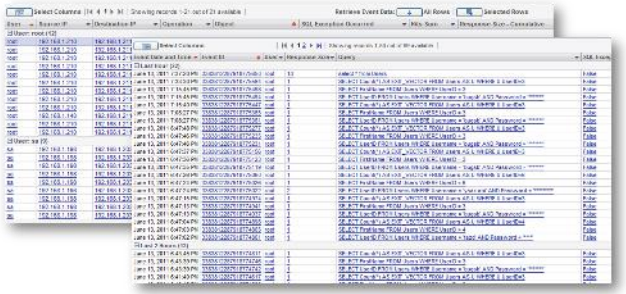


IMPERVA®

CounterBreachによる次世代ピア・グループ分析

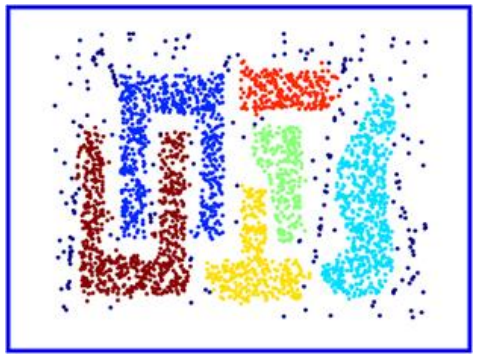
監視 → 学習・分析 → 検知

監査ログ収集

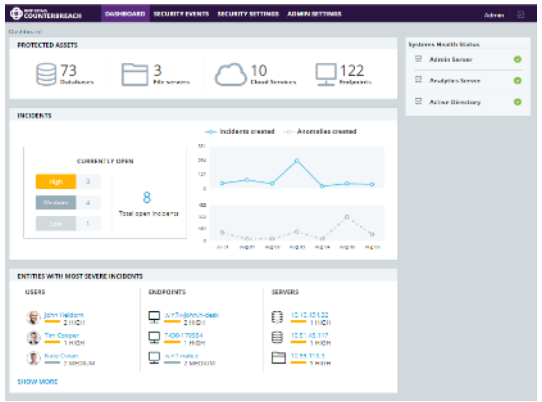


aws

マシーン・ラーニングと
“仮想”ピア・グループ分析



異常行動のインシデント
を発報



IMPERVA®

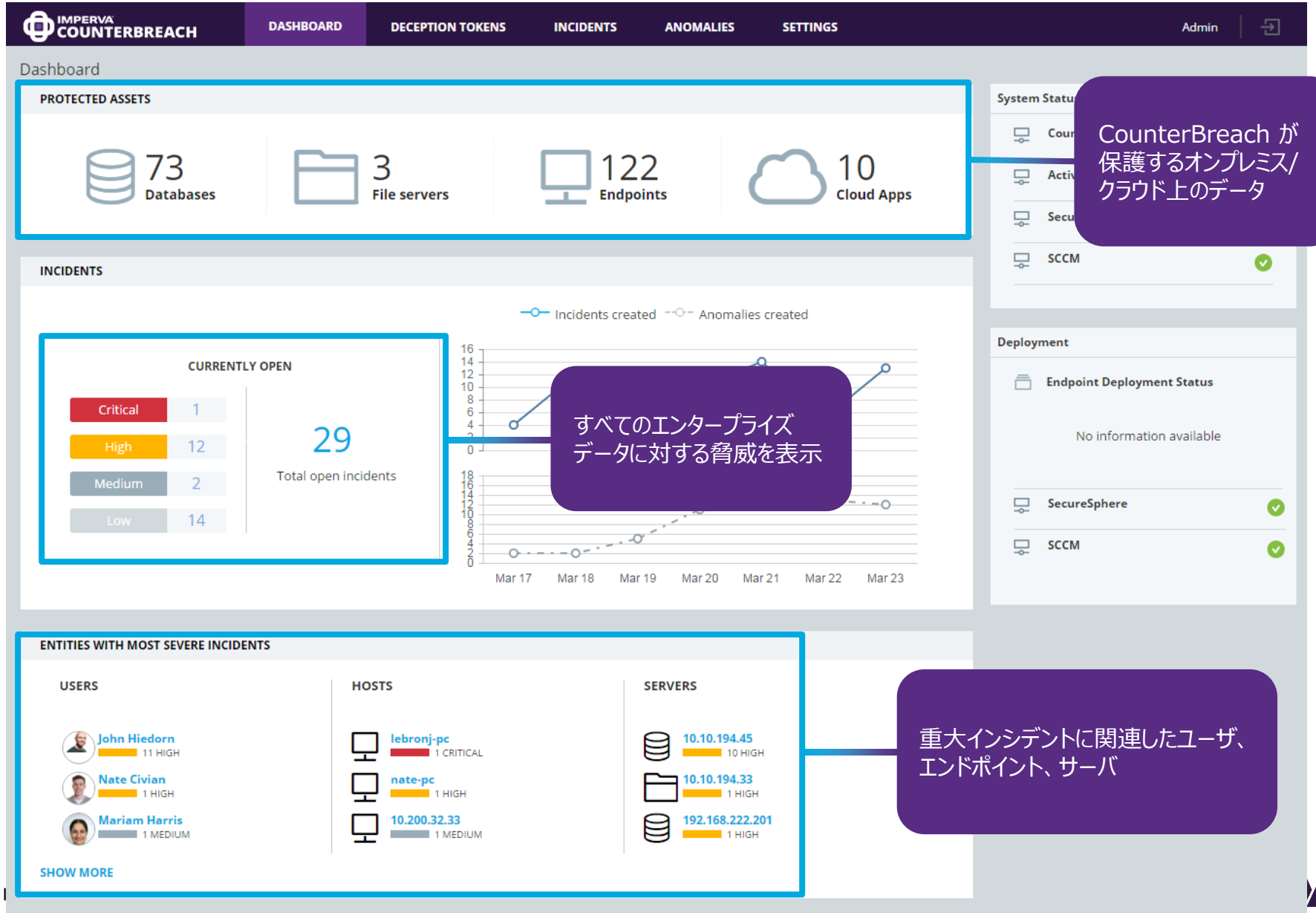
A

Appendix

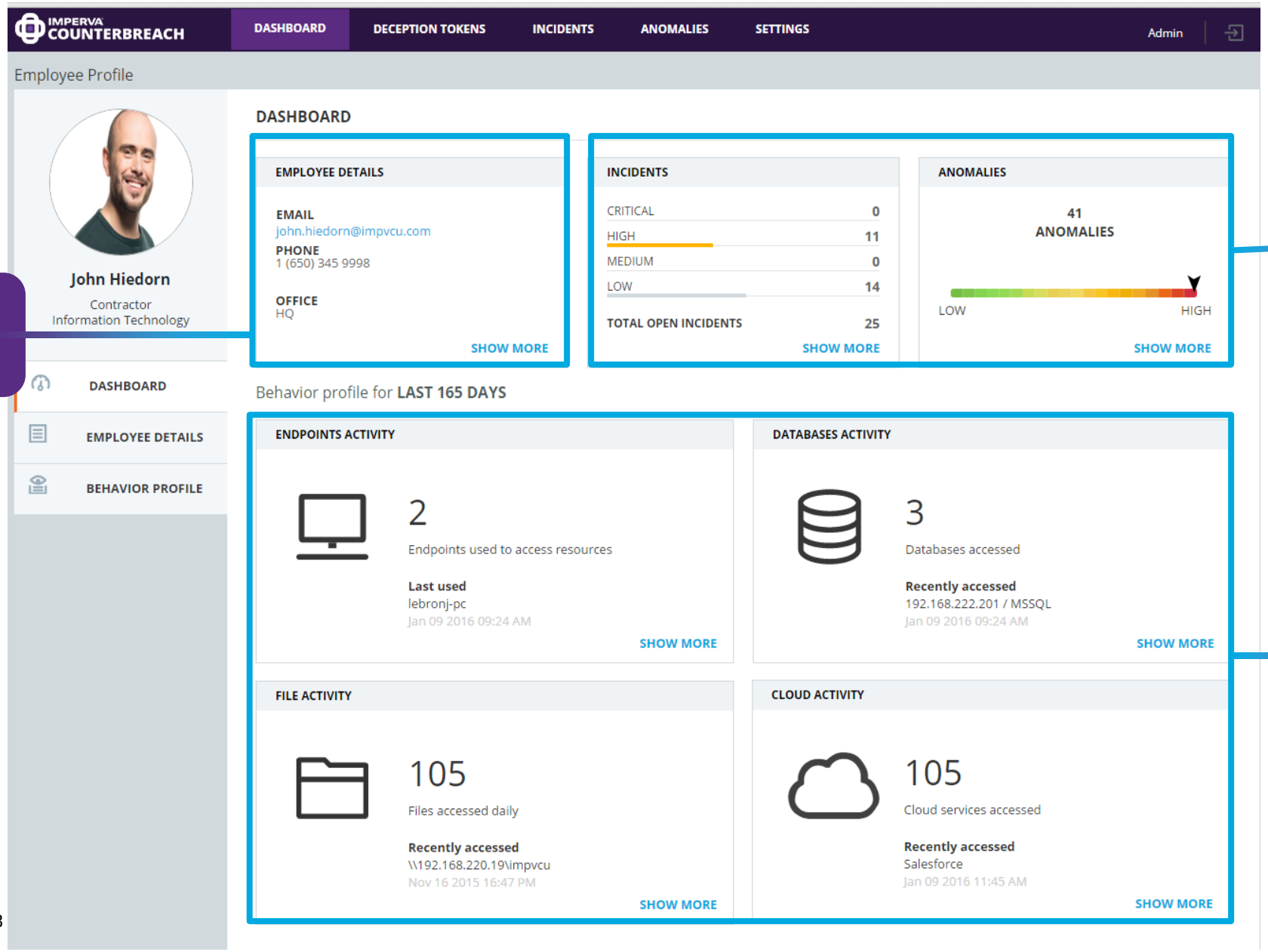
CounterBreach プロダクトツアー

IMPERVA®

CounterBreach ダッシュボード



CounterBreach ユーザスクリーン



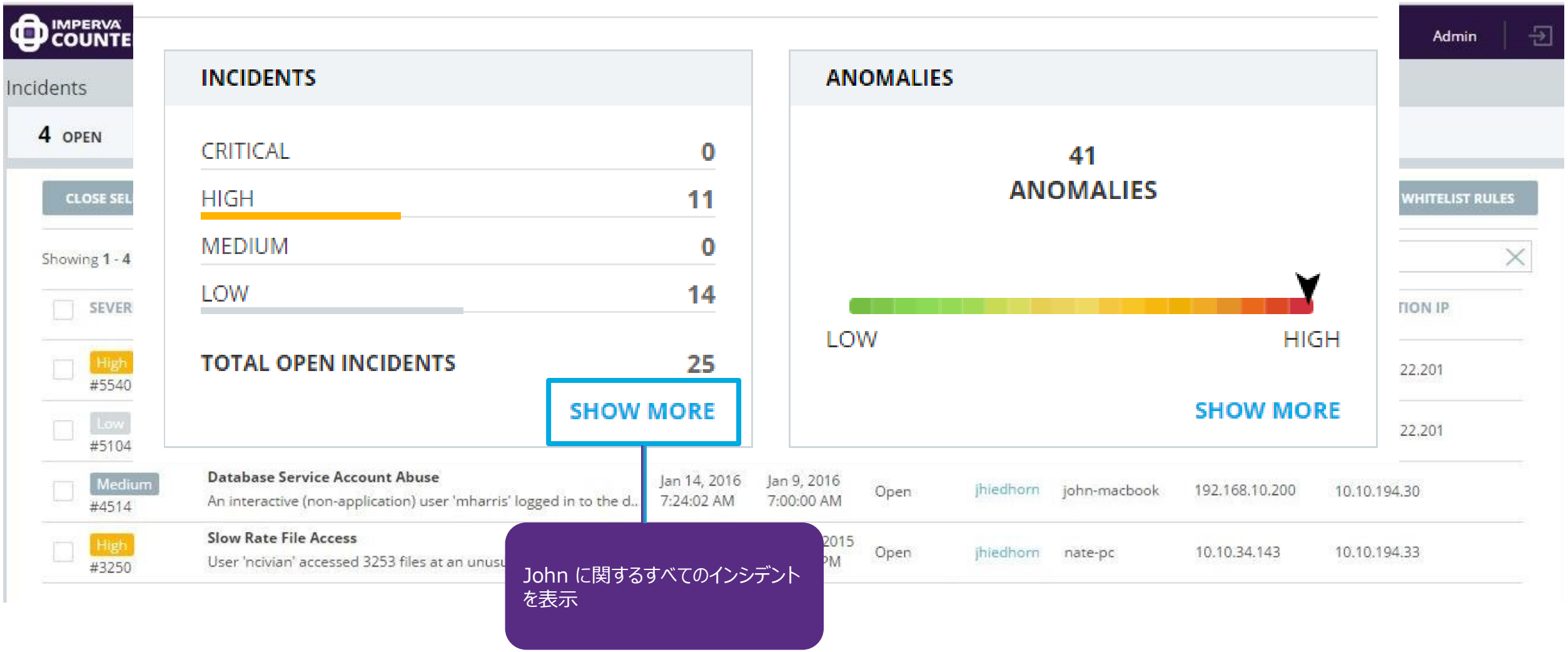
Johnの詳細なユーザ情報を表示

インシデントと不審な振る舞い

Johnがどのデータにアクセスしたか？

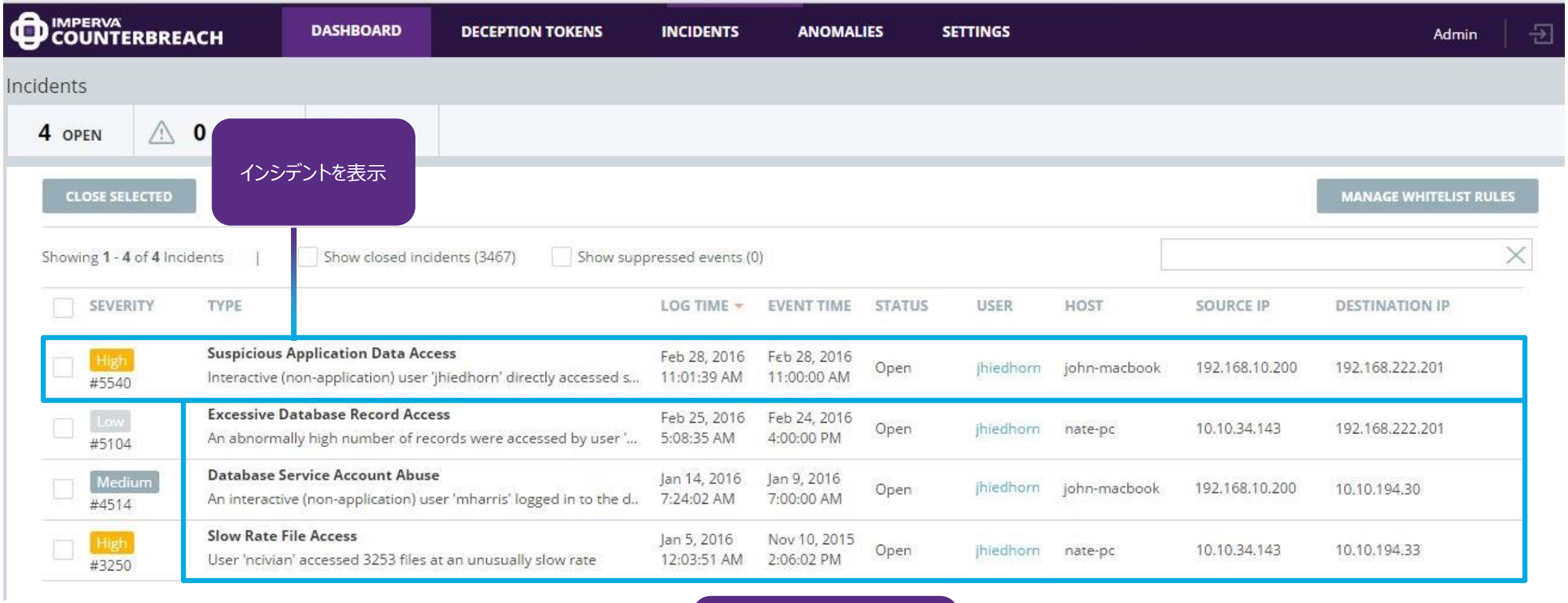
IMPERVA®

CounterBreach インシデントスクリーン



IMPERVA

CounterBreach インシデントスクリーン



IMPERVA®

インシデントスクリーン詳細

インシデントの情報と考えられる影響

DESCRIPTION
Interactive (non-application) user 'John Hiedorn' directly accessed sensitive application table data on the database on '192.168.222.201'.

POSSIBLE IMPLICATIONS
Individuals that directly access sensitive application data violate access privileges and expose the organization to the risk of a data breach.

SOURCE AND DESTINATION

SOURCE DETAILS

jhiedhorn

Johnの振る舞いプロファイル

IP
192.168.10.200

Source Application
dbeaver

DESTINATION DETAILS

Database Server

DB Username
c_lebronj

IP
192.168.222.201

Database
impvcuprod

ADDITIONAL INFORMATION

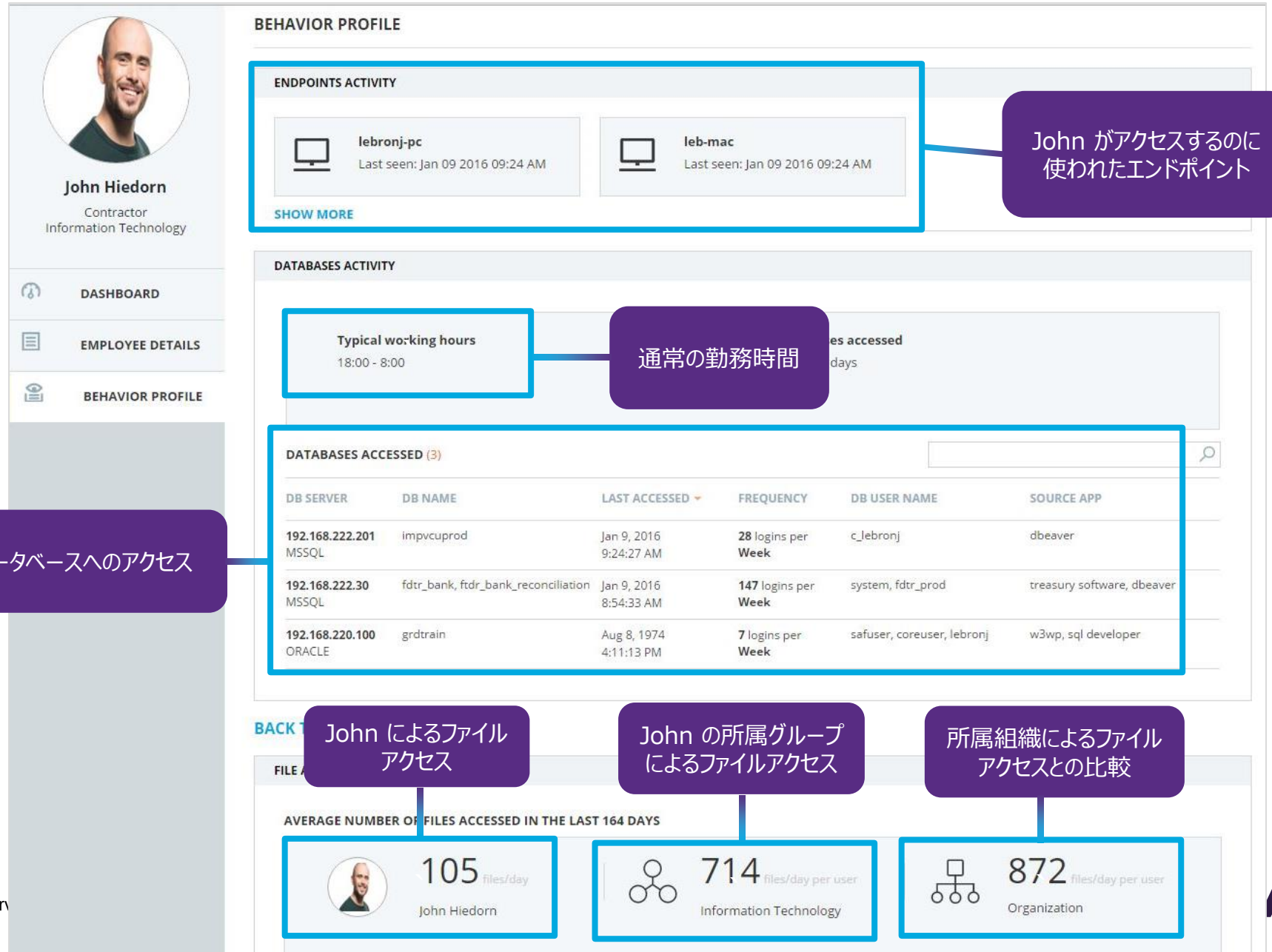
DB OPERATIONS (5)

ユーザーにアクセスされたDB テーブル

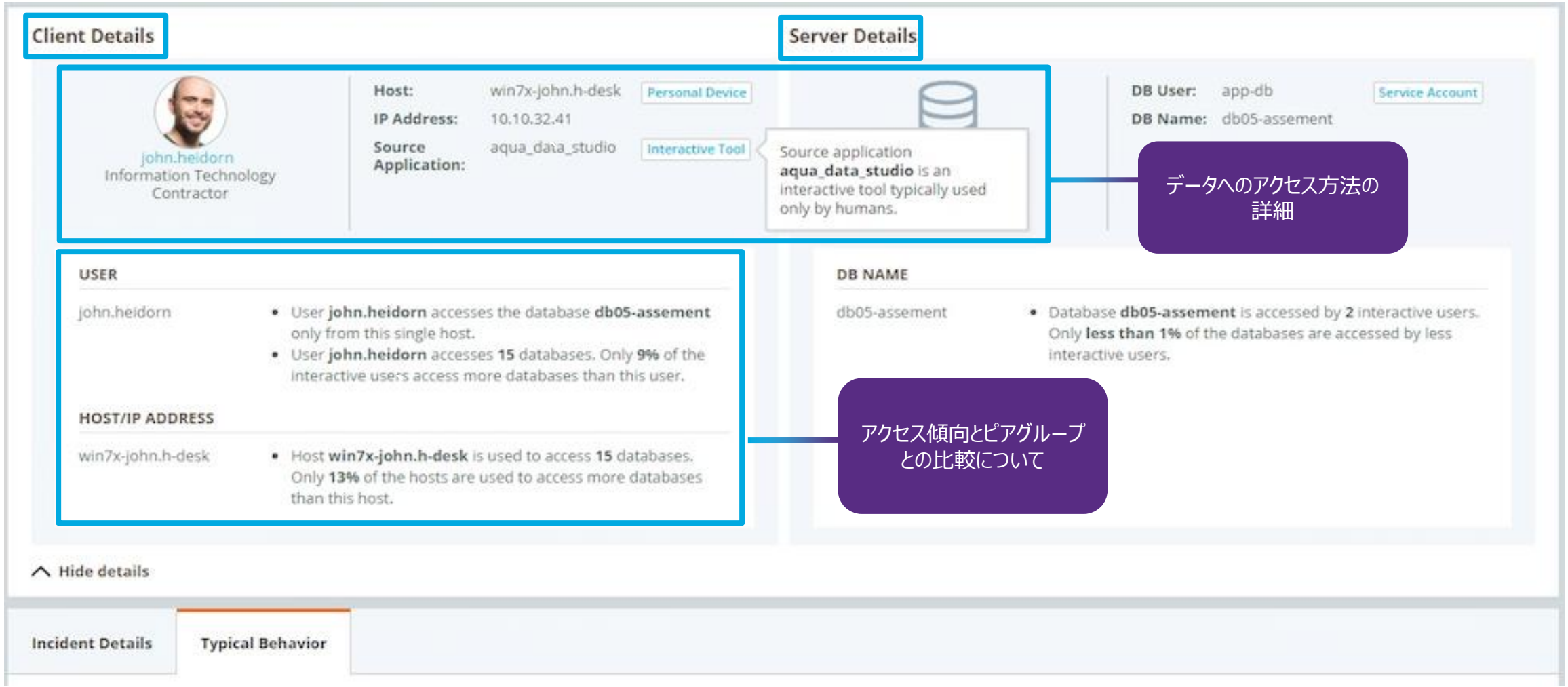
操作の種類、アクセスされたレコード数

DATABASE	SCHEMA	TABLE/STORED PROCEDURE	APPLICATION TABLE	TYPE	OPERATION	NO. OF QUERIES	TOTAL NO. OF RECORDS
impvcuprod	dbo	fldencryptedaccountnumber	yes	table	select	3	1443254
impvcuprod	dbo	tblcreditcards	yes	table	select	4	38199

ユーザ振る舞いプロファイルスクリーン

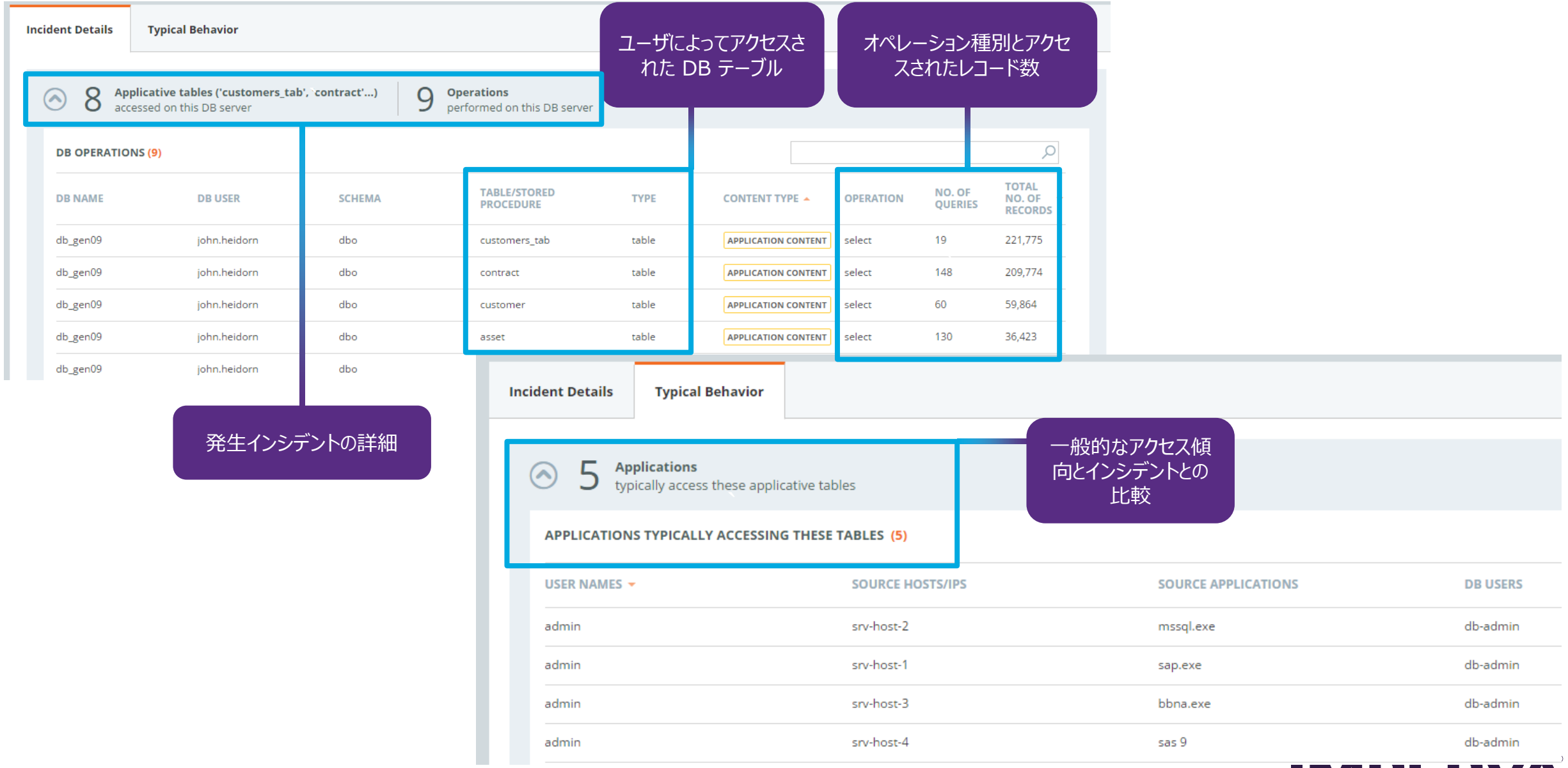


関連するユーザと影響を受けるサーバに関する詳細



IMPERVA®

インシデントの詳細と一般的なアクセス傾向との比較



まとめ　RDSの監査およびデータセキュリティ

1. 責任共有モデルとして、RDS内のデータ管理責任はお客様側

2. RDSの統合リスク管理や運用にエコ・システムを活用

3. アクセスログのチェック、アラートの解析はAI、機械学習に任せる

IMPERVA®

IMPERVA®