

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

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で実現するRDSの監査およびデータセキュリティ

Impervaについて

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 Hysten
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）





セイコーインスツル株式会社

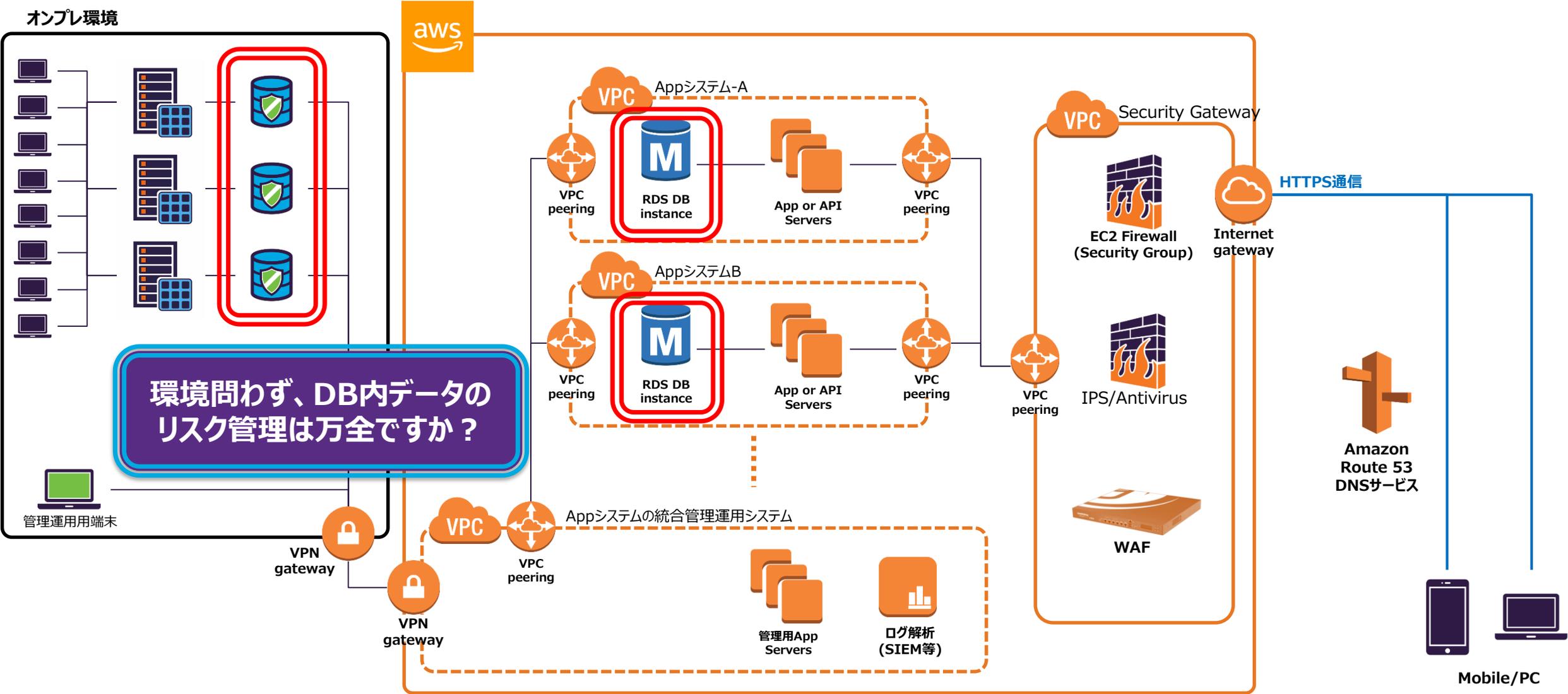


2

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？

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



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

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？

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 PROCEDURE
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:	besgmt

データ管理者が
200万レコード
の監査ログを見ている



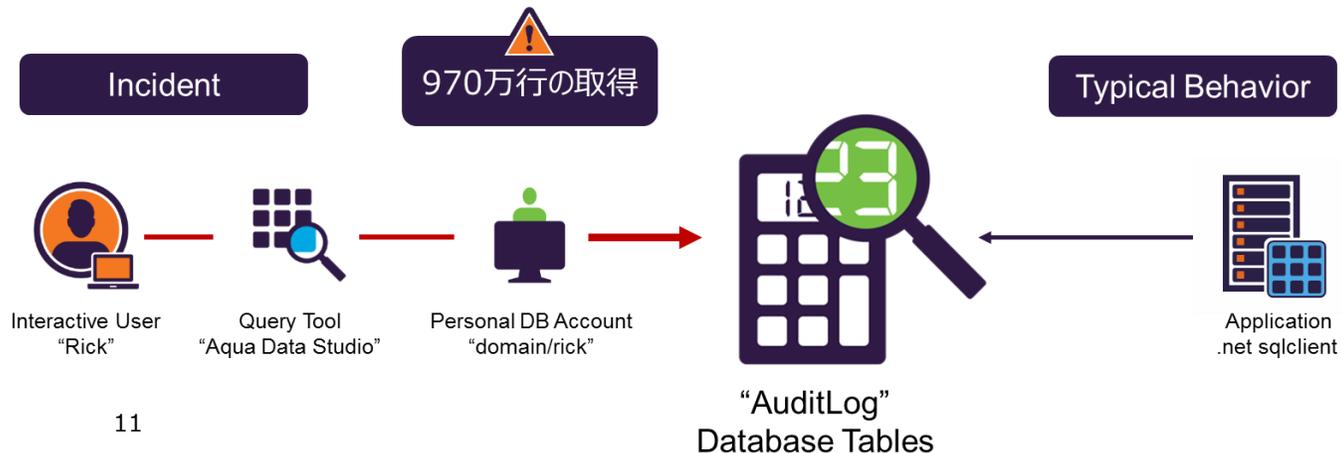
DBA reads 2M
audit log records

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中から、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



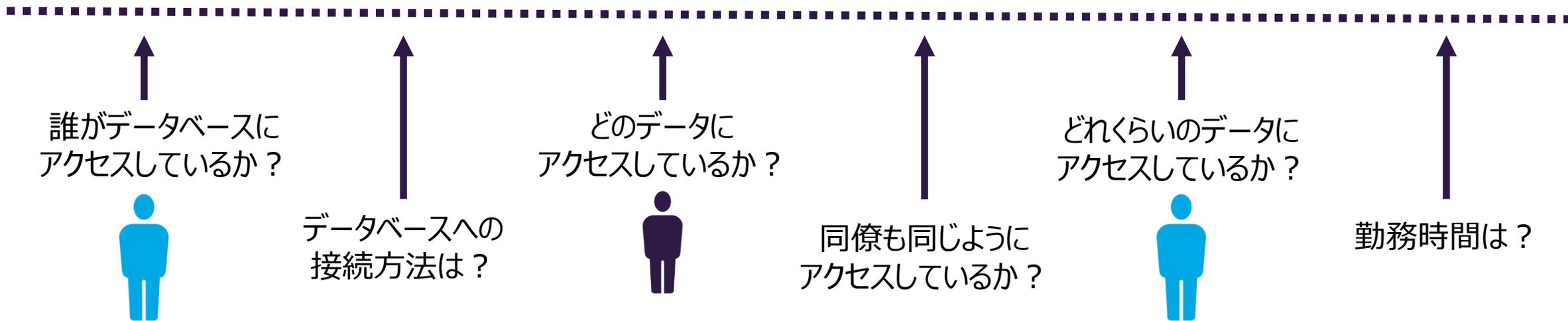
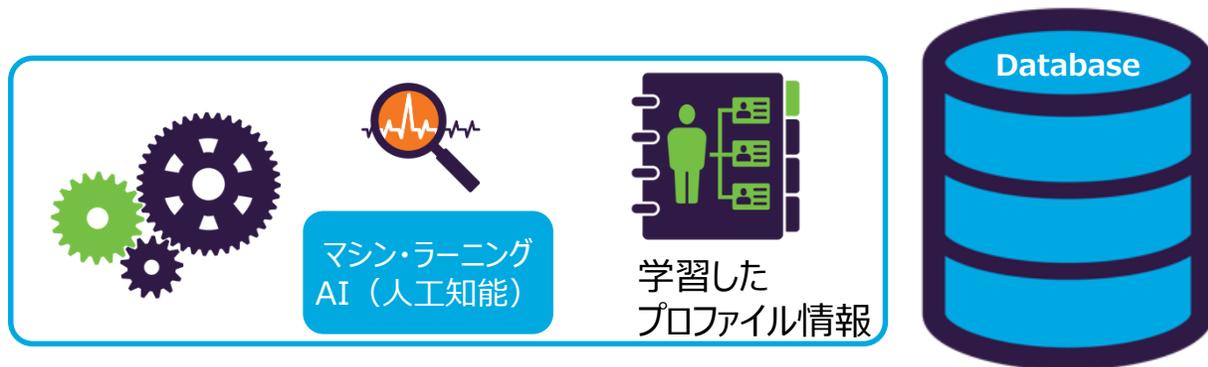
ユーザ事例：公共交通機関

- **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

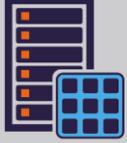


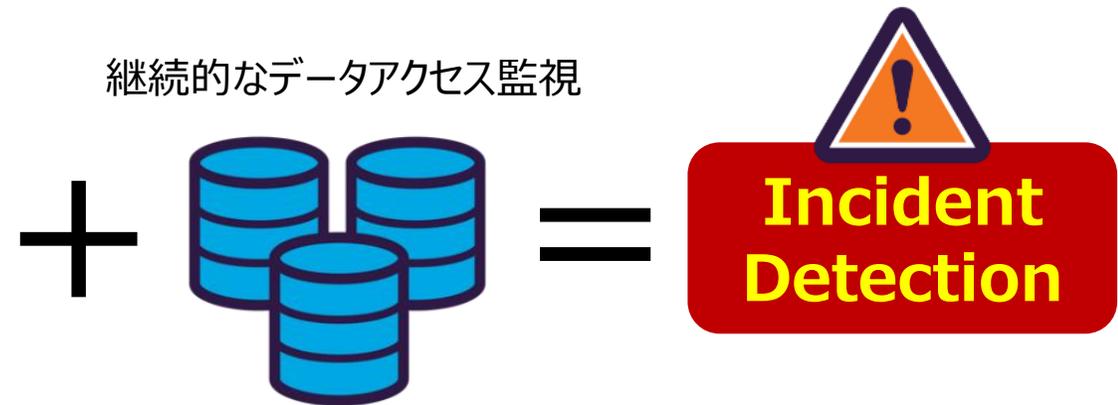
- 悪意ある内部関係者が高い権限を有するアカウントで重要DBにアクセス
- アクセス制限を回避
- アクティビティが追跡不可能

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



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 



インシデント検知



SQL



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

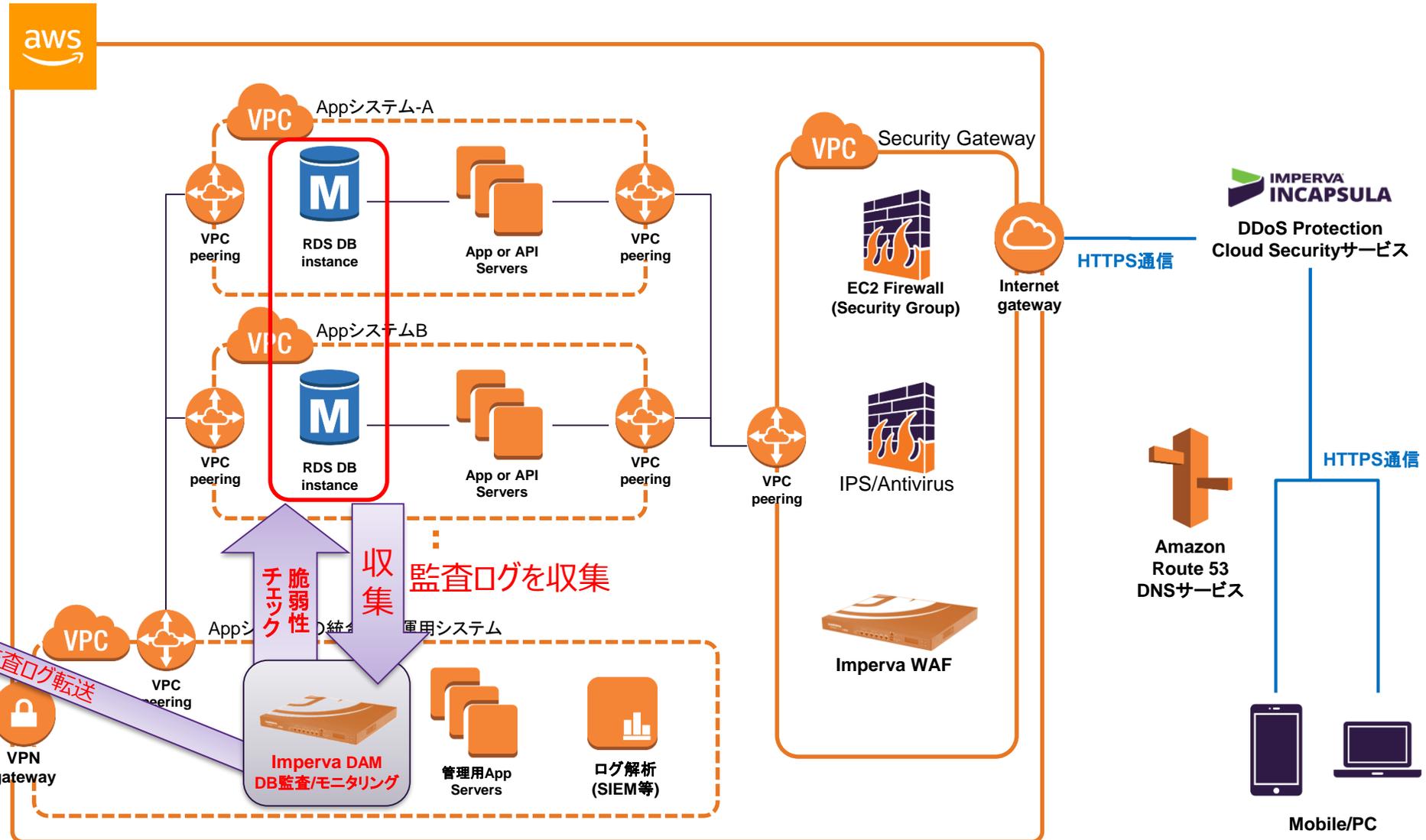
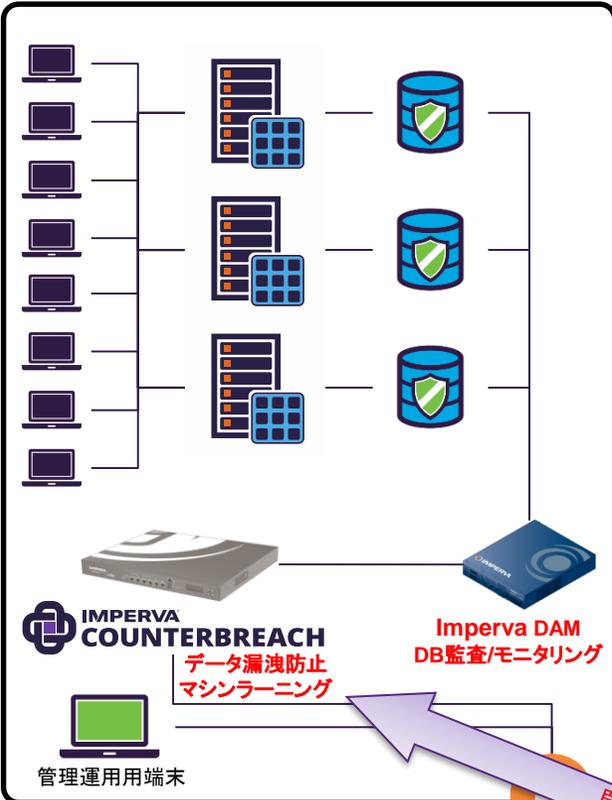
4

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 Database Security for Amazon RDS 構成イメージ

オンプレ環境



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

監査ログ

Default Rule - All Events - Audit Events

Reported Period: 05/11/2018, 00:00- 05/14/2018, 16:22 (3 Days, 16 hrs)

Base Filter: Empty

Filter: Empty

Select Columns | Page 1 of 1 | Showing records 1-17 out of 17 available

Event Date and Time	Event ID	Source IP	User	Destination IP	Service	Object	Operation	Query
May 14, 2018 4:16:02 PM	249108103185	172.23.2.249	sys	10.0.1.78	Oracle RDS	v\$archive_dest	Select	select 'ERROR: error '.as error,'LOG SE
May 14, 2018 4:16:02 PM	249108103184	172.23.2.249	sys	10.0.1.78	Oracle RDS			COMMIT
May 14, 2018 4:16:02 PM	249108103183	172.23.2.249	sys	10.0.1.78	Oracle RDS			COMMIT
May 14, 2018 4:16:02 PM	249108103182	172.23.2.249	sys	10.0.1.78	Oracle RDS		Login	
May 14, 2018 4:15:12 PM	249108103181	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS		Logout	
May 14, 2018 4:15:12 PM	249108103180	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist order by id;
May 14, 2018 4:15:12 PM	249108103179	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist;
May 14, 2018 4:09:14 PM	249108103178	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist;
May 14, 2018 4:09:14 PM	249108103177	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist;
May 14, 2018 4:09:14 PM	249108103176	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist order by id;
May 14, 2018 4:09:14 PM	249108103175	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist order by id;
May 14, 2018 4:09:14 PM	249108103174	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS	userslist	Select	select * from userslist;
May 14, 2018 4:09:14 PM	249108103173	10.0.11.102	damtest	10.0.1.28	PostgreSQL RDS		Login	
May 14, 2018 4:02:04 PM	249108103172	172.23.2.249	sys	10.0.1.78	Oracle RDS	v\$archive_dest	Select	select 'ERROR: error '.as error,'LOG SE
May 14, 2018 4:02:04 PM	249108103171	172.23.2.249	sys	10.0.1.78	Oracle RDS			COMMIT

いつ

誰が

どこのテーブルへ

何をしたか

アラートログ

Alert 1: Test SecurityPolicy

Actions: None

Policy: Test SecurityPolicy (Policy Description)

Edit Policy Knowledge Base

Aggregated from 16:15:18 (0 hour(s), 0 minute(s)), 2 alerts (last updated 16:15:18)

Alert aggregated by:

Distinct value for:	Value
Custom Rule	Test SecurityPolicy
Immediate Action	None
Server Group	amazon rds
Source IP	10.0.11.102

Statistical Information:

Key	Value
OS Hosts	1
Source Applications	1
SQL Users	1
Tables	1

Violations:

User	OS User	OS Host
damtest		10.0.11.102

Event 249108103180: Custom Rule Violation

Key	Value
Violation Type	sql
Severity	Medium
Policy Name	Test SecurityPolicy (Policy Description)
Alert Number	1
Violation Description	Test SecurityPolicy
Violated Item	Custom Violation
Immediate Action	None
Matched Patterns	

Event Details:

Event Time	Gateway
May 14, 2018 4:14:39 PM	1-0ac4566af202d962e

Server Group	Service	Application
amazon rds	PostgreSQL RDS	Default PostgreSQL Application

Connection	Source of Activity	User	DB Application	OS User	OS Host
10.0.11.102:43945 → 10.0.1.28:5432	Remote	damtest	psql		10.0.11.102

Affected Rows	Response Size	Response Time
0	0 Records	0 msec.

Error Code	Error Message
	select * from userslist order by id;

DB Assessments Scan機能 for Amazon RDS サンプル

Assessment Result - Summary View

Filter: Result is one of [Info, Failed] and Last Scan in Each Policy is [True]

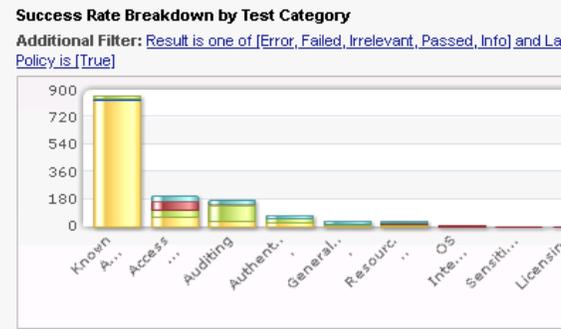
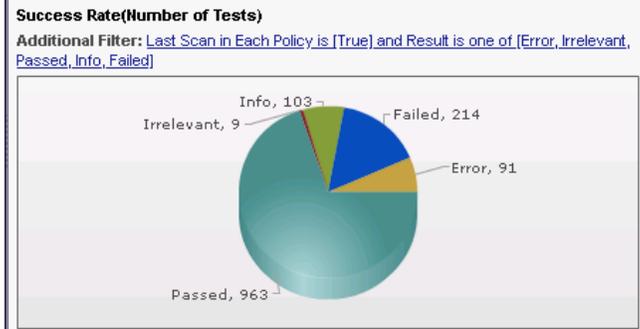
Scanning Coverage

Additional Filter: Result is one of [Failed, Passed, Error, Irrelevant, Info] and Last Scan in Each Policy is [True]

Page 1 of 1 Showing records 1-8 out of 8 available

Policy	Scan Name	Scan Run Date	# Tests Failed	# Tests Passed	Result Count Info	# Tests with errors	# Irrelevant Tests
CIS - Security Configuration Benchmark For Oracle Database Server 12c	CIS - Latest Database Security Benchmark	05/09/2018 4:28:59 PM	89	54	1		
DISA (STIG) - Database Checklist and Procedures for Oracle 11g and Above (DISA Version 8, Release 20). See the note under Policy Description.	DISA (STIG) - Latest Database Security Benchmark	05/09/2018 4:03:50 PM	28	24	16		
DISA (STIG) - Database Checklist and Procedures for Oracle 12c (DISA Version 1, Release 8).	DISA (STIG) - Latest Database Security Benchmark	05/09/2018 4:03:50 PM	16	17	47		
DISA (STIG) - Database Checklist and Procedures for PostgreSQL 9.0 and Above	DISA (STIG) - Database Checklist and Procedures for PostgreSQL 9.0 and Above: default scan	05/09/2018 3:59:56 PM	34	14	19		
DISA (STIG) - Database Checklist and Procedures for PostgreSQL 9.0 and Above	DISA (STIG) - Latest Database Security Benchmark	05/09/2018 4:03:50 PM	34	14	19		
Missing Security Patches for Oracle	Missing Security Patches	05/09/2018 4:27:57 PM	1	0	0		
Oracle Known Vulnerabilities	Known Vulnerabilities	05/09/2018 4:28:21 PM	0	607	0		
PCI-DSS Compliance - Oracle	PCI-DSS Compliance for Oracle	05/09/2018 6:04:52 PM	12	233	1		

結果サマリー



Assessment Results

Filter: Result is one of [Info, Failed] and Last Scan in Each Policy is [True]

Page 1 of 7 Showing records 1-50 out of 317 available

Result	Category	Test Name	IP	Asset
High Info	Access Control	Users Assigned DBA Role	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Info	Access Control	List of users that have access to DBMS_B...	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Access Control	Unauthorized Users Have Access to DBA %...	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Access Control	Unauthorized Users Granted DBA Role (CIS...	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Access Control	Unauthorized Users Granted EXECUTE_CATAL...	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Access Control	Unauthorized Users Granted GRANT ANY OBJ...	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Access Control	Unauthorized Users Granted GRANT ANY ROL...	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Authentication and User Management	Users with Default Passwords	10.0.1.78	Default Site - amazon rds - Oracle RDS
High Failed	Known Attacks	Latest PostgreSQL patch not installed	10.0.1.28	Default Site - amazon rds - PostgreSQL RDS
High Info	Resource Control	PostgreSQL enforce authorized access to ...	10.0.1.28	Default Site - amazon rds - PostgreSQL RDS

脆弱性詳細

Test: Users Assigned DBA Role

Overview Recommended Fix Technical Details

Vulnerability Information

ID (CVE)	Vulnerability Type	Severity
	Users Assigned the DBA Role	9.03

Source Policy

DISA (STIG) - Database Checklist and Procedures for Oracle 11g and Above (DISA Version 8, Release 20). See the note under Policy Description.

Regulation Section Name	Regulation Section No.
Oracle DBA role assignment	DO3440

Description

The DBA role is very powerful and access to it should be restricted. Verify that any database account granted the DBA role is explicitly authorized by the IAO. In addition to full access to database objects, access to the DBA role by unauthorized accounts may provide full access to the

Attribute	Value
Asset	Default Site - amazon rds - Oracle RDS
IP	10.0.1.78
Port	1521
DB	Oracle
Schema	orcl

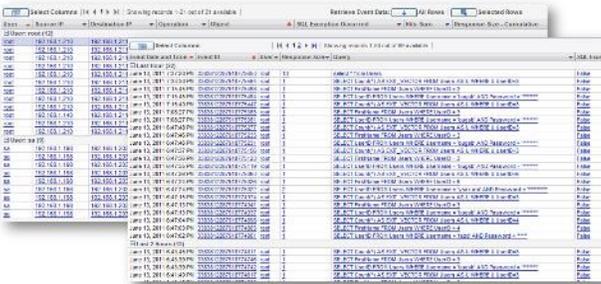
CounterBreachによる次世代ピア・グループ分析

監視

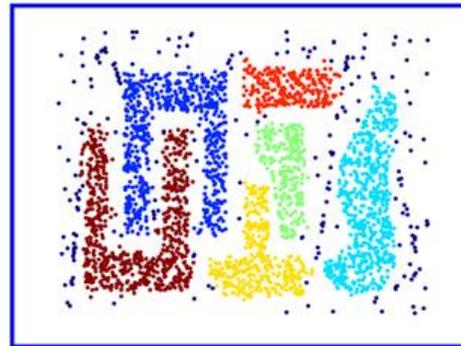
学習・分析

検知

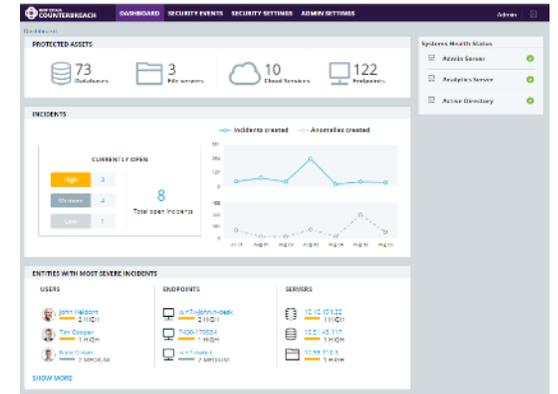
監査ログ収集



マシン・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

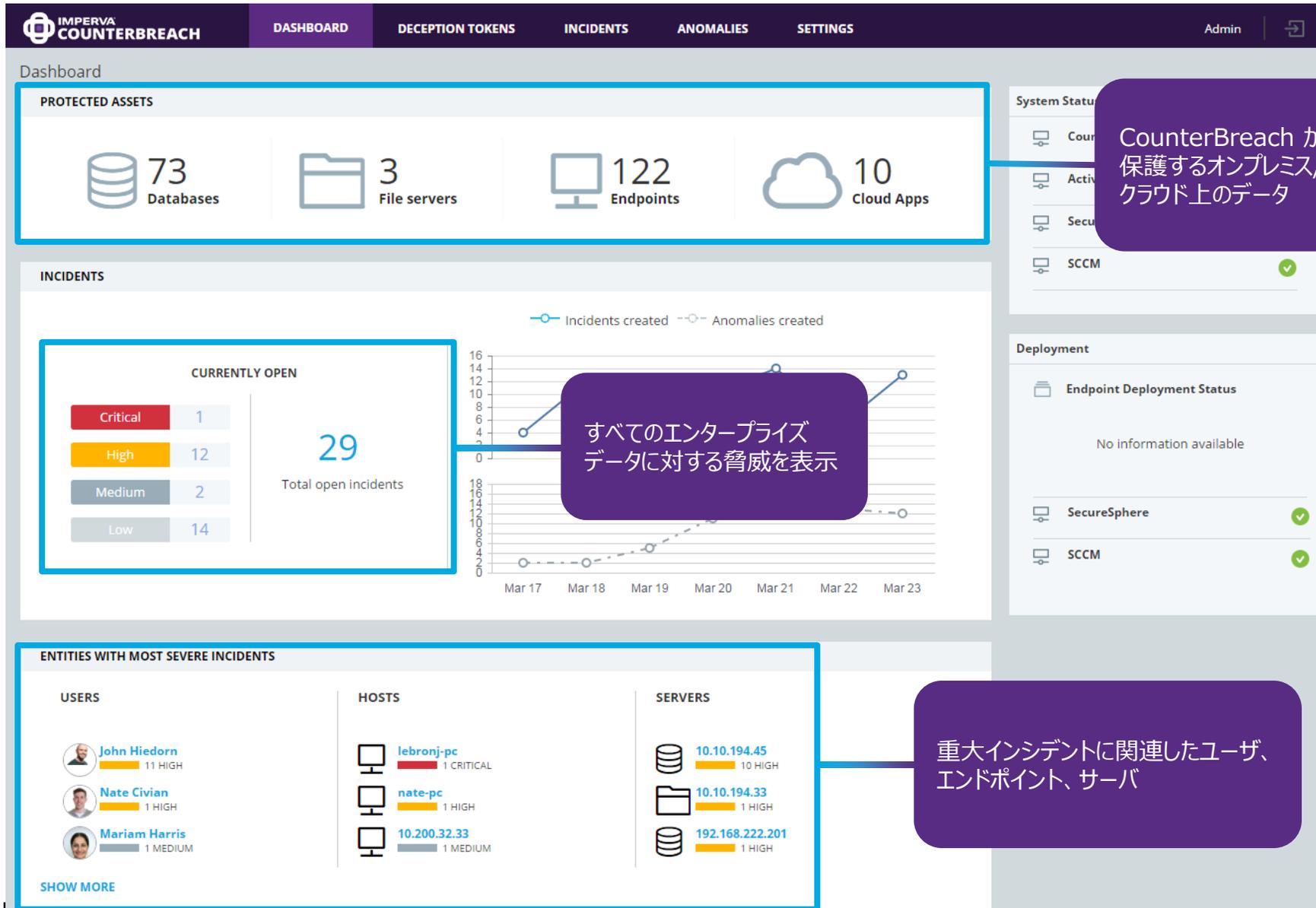


A

Appendix

CounterBreach プロダクトツアー

CounterBreach ダッシュボード



CounterBreachが
保護するオンプレミス/
クラウド上のデータ

すべてのエンタープライズ
データに対する脅威を表示

重大インシデントに関連したユーザ、
エンドポイント、サーバ

CounterBreach ユーザスクリーン

IMPVERA COUNTERBREACH

DASHBOARD DECEPTION TOKENS INCIDENTS ANOMALIES SETTINGS Admin

Employee Profile

John Hiedorn
Contractor
Information Technology

DASHBOARD

EMPLOYEE DETAILS

EMAIL
john.hiedorn@impvcu.com

PHONE
1 (650) 345 9998

OFFICE
HQ

INCIDENTS

CRITICAL	0
HIGH	11
MEDIUM	0
LOW	14
TOTAL OPEN INCIDENTS	25

ANOMALIES

41 ANOMALIES

LOW HIGH

Behavior profile for LAST 165 DAYS

ENDPOINTS ACTIVITY

2
Endpoints used to access resources

Last used
lebronj-pc
Jan 09 2016 09:24 AM

DATABASES ACTIVITY

3
Databases accessed

Recently accessed
192.168.222.201 / MSSQL
Jan 09 2016 09:24 AM

FILE ACTIVITY

105
Files accessed daily

Recently accessed
\\192.168.220.19\impvcu
Nov 16 2015 16:47 PM

CLOUD ACTIVITY

105
Cloud services accessed

Recently accessed
Salesforce
Jan 09 2016 11:45 AM

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？

CounterBreach インシデントスクリーン

INCIDENTS

CRITICAL	0
HIGH	11
MEDIUM	0
LOW	14
TOTAL OPEN INCIDENTS	25

ANOMALIES

41 ANOMALIES

LOW HIGH

SHOW MORE

<input type="checkbox"/>	SEVER										
<input type="checkbox"/>	High	#5540									
<input type="checkbox"/>	Low	#5104									
<input type="checkbox"/>	Medium	#4514	Database Service Account Abuse	An interactive (non-application) user 'mharris' logged in to the d...	Jan 14, 2016 7:24:02 AM	Jan 9, 2016 7:00:00 AM	Open	jhiedhorn	john-macbook	192.168.10.200	10.10.194.30
<input type="checkbox"/>	High	#3250	Slow Rate File Access	User 'incivian' accessed 3253 files at an unusu...		2015 PM	Open	jhiedhorn	nate-pc	10.10.34.143	10.10.194.33

John に関するすべてのインシデントを表示

CounterBreach インシデントスクリーン

IMPVERA COUNTERBREACH

DASHBOARD DECEPTION TOKENS INCIDENTS ANOMALIES SETTINGS Admin

Incidents

4 OPEN 0

インシデントを表示

CLOSE SELECTED MANAGE WHITELIST RULES

Showing 1 - 4 of 4 Incidents | Show closed incidents (3467) Show suppressed events (0)

SEVERITY	TYPE	LOG TIME	EVENT TIME	STATUS	USER	HOST	SOURCE IP	DESTINATION IP
High #5540	Suspicious Application Data Access Interactive (non-application) user 'jhiedhorn' directly accessed s...	Feb 28, 2016 11:01:39 AM	Feb 28, 2016 11:00:00 AM	Open	jhiedhorn	john-macbook	192.168.10.200	192.168.222.201
Low #5104	Excessive Database Record Access An abnormally high number of records were accessed by user '...	Feb 25, 2016 5:08:35 AM	Feb 24, 2016 4:00:00 PM	Open	jhiedhorn	nate-pc	10.10.34.143	192.168.222.201
Medium #4514	Database Service Account Abuse An interactive (non-application) user 'mharris' logged in to the d...	Jan 14, 2016 7:24:02 AM	Jan 9, 2016 7:00:00 AM	Open	jhiedhorn	john-macbook	192.168.10.200	10.10.194.30
High #3250	Slow Rate File Access User 'ncivian' accessed 3253 files at an unusually slow rate	Jan 5, 2016 12:03:51 AM	Nov 10, 2015 2:06:02 PM	Open	jhiedhorn	nate-pc	10.10.34.143	10.10.194.33

すべてのインシデントを表示

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の振る舞いプロフィール

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)

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

操作の種類、アクセスされた
レコード数

ユーザ振る舞いプロフィールスクリーン

BEHAVIOR PROFILE

ENDPOINTS ACTIVITY

- lebronj-pc (Last seen: Jan 09 2016 09:24 AM)
- leb-mac (Last seen: Jan 09 2016 09:24 AM)

DATABASES ACTIVITY

Typical working hours: 18:00 - 8:00

DATABASES ACCESSED (3)

DB SERVER	DB NAME	LAST ACCESSED	FREQUENCY	DB USER NAME	SOURCE APP
192.168.222.201 MSSQL	impvcuprod	Jan 9, 2016 9:24:27 AM	28 logins per Week	c_lebronj	dbeaver
192.168.222.30 MSSQL	fdtr_bank, fdtr_bank_reconciliation	Jan 9, 2016 8:54:33 AM	147 logins per Week	system, fdtr_prod	treasury software, dbeaver
192.168.220.100 ORACLE	grdtrain	Aug 8, 1974 4:11:13 PM	7 logins per Week	safuser, coreuser, lebronj	w3wp, sql developer

John Hiedorn
Contractor
Information Technology

John によるファイルアクセス

John の所属グループによるファイルアクセス

所属組織によるファイルアクセスとの比較

AVERAGE NUMBER OF FILES ACCESSED IN THE LAST 164 DAYS

- John Hiedorn: 105 files/day
- Information Technology: 714 files/day per user
- Organization: 872 files/day per user

John がアクセスするのに使われたエンドポイント

通常の勤務時間

データベースへのアクセス

関連するユーザと影響を受けるサーバに関する詳細

The screenshot displays a detailed view of database access patterns. It is divided into two main sections: Client Details and Server Details.

Client Details:

- User:** john.heidorn, Information Technology Contractor.
- Host:** win7x-john.h-desk (Personal Device).
- IP Address:** 10.10.32.41.
- Source Application:** aqua_data_studio (Interactive Tool).

Server Details:

- DB User:** app-db (Service Account).
- DB Name:** db05-assement.

USER Access Statistics:

- john.heidorn:**
 - User **john.heidorn** accesses the database **db05-assement** only from this single host.
 - User **john.heidorn** accesses **15** databases. Only **9%** of the interactive users access more databases than this user.

HOST/IP ADDRESS Access Statistics:

- win7x-john.h-desk:**
 - Host **win7x-john.h-desk** is used to access **15** databases. Only **13%** of the hosts are used to access more databases than this host.

DB NAME Access Statistics:

- db05-assement:**
 - Database **db05-assement** is accessed by **2** interactive users. Only **less than 1%** of the databases are accessed by less interactive users.

Annotations:

- A callout box explains that the source application **aqua_data_studio** is an interactive tool typically used only by humans.
- A purple box highlights the database access details: データへのアクセス方法の詳細.
- Another purple box highlights the access trends and comparison with peer groups: アクセス傾向とピアグループとの比較について.

At the bottom, there are tabs for Incident Details and Typical Behavior, and a 'Hide details' link.

インシデントの詳細と一般的なアクセス傾向との比較

Incident Details | Typical Behavior

8 Applicative tables ('customers_tab', 'contract'...) accessed on this DB server

9 Operations performed on this DB server

ユーザによってアクセスされた DB テーブル

オペレーション種別とアクセスされたレコード数

発生インシデントの詳細

一般的なアクセス傾向とインシデントとの比較

DB NAME	DB USER	SCHEMA	TABLE/STORED PROCEDURE	TYPE	CONTENT TYPE	OPERATION	NO. OF QUERIES	TOTAL NO. OF RECORDS
db_gen09	john.heidorn	dbo	customers_tab	table	APPLICATION CONTENT	select	19	221,775
db_gen09	john.heidorn	dbo	contract	table	APPLICATION CONTENT	select	148	209,774
db_gen09	john.heidorn	dbo	customer	table	APPLICATION CONTENT	select	60	59,864
db_gen09	john.heidorn	dbo	asset	table	APPLICATION CONTENT	select	130	36,423
db_gen09	john.heidorn	dbo						

Incident Details | Typical Behavior

5 Applications typically access these applicative tables

APPLICATIONS TYPICALLY ACCESSING THESE TABLES (5)

USER NAMES	SOURCE HOSTS/IPS	SOURCE APPLICATIONS	DB USERS
admin	srv-host-2	mssql.exe	db-admin
admin	srv-host-1	sap.exe	db-admin
admin	srv-host-3	bbna.exe	db-admin
admin	srv-host-4	sas 9	db-admin

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[®]