DOAG

Deutsche ORACLE-Anwendergruppe e.V.

DOAG SIG Security 27.06.2018

Personenbezogene Daten in der Datenbank erkennen

DBSAT – DIE ORACLE DATENBANK BZGL. PII DATEN ANALYSIEREN

gunther@pipperr.de

Mein Blog

https://www.pipperr.de/dokuwiki/

Bergweg 14 - 37216 Witzenhausen/Roßbach

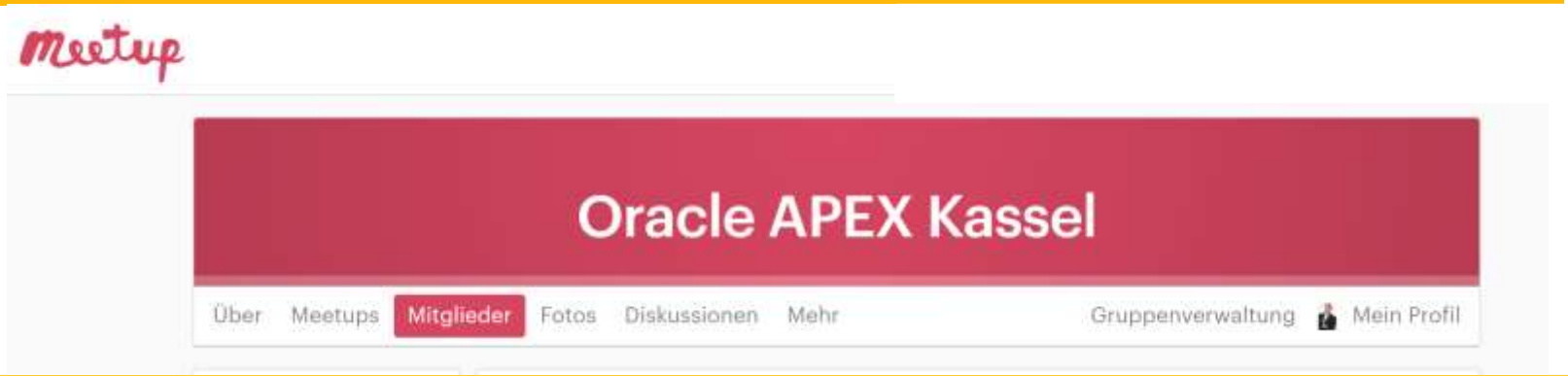
Freiberuflicher Oracle Datenbank Experte - Ich unterstütze Sie gerne in ihren Projekten.

APEX Meetup Gruppe Kassel

Raum für Veranstaltung in Kassel gesucht, können Sie unterstützen?

Mitglieder gesucht!

https://www.meetup.com/de-DE/Oracle-APEX-Kassel/



Agenda

1	**Aufgabe**
2	Idee
3	Praxis Beispiel
4	Erweitern und Konfigurieren
5	Fazit

Die Aufgabe

Personenbezogene Daten schützen, aber ….

Wo in meiner Umgebung werden Personen bezogene Daten (PII) gespeichert?

PII ⇒ **P**ersonally **I**dentifiable **I**nformation

Ein Ansatz

- Über das Data Dictionary Inhalte in einer Datenbank “erkennen”/”erahnen”/”erraten”
  - Oft werden Datenbank Objekte (Tabellen) so benannt, wie die Business Entitäten, die das Objekte später enthält
  - Gelegentlich werden Kommentare auf Tabellen und Spalten mit Hinweise auf die Bedeutung hinterlegt

In der Theorie jedenfalls

Die Annahme

- Eine Tabelle die „PERSONEN“ heißt, könnte mit hoher Wahrscheinlichkeit Personen-bezogene Daten enthalten

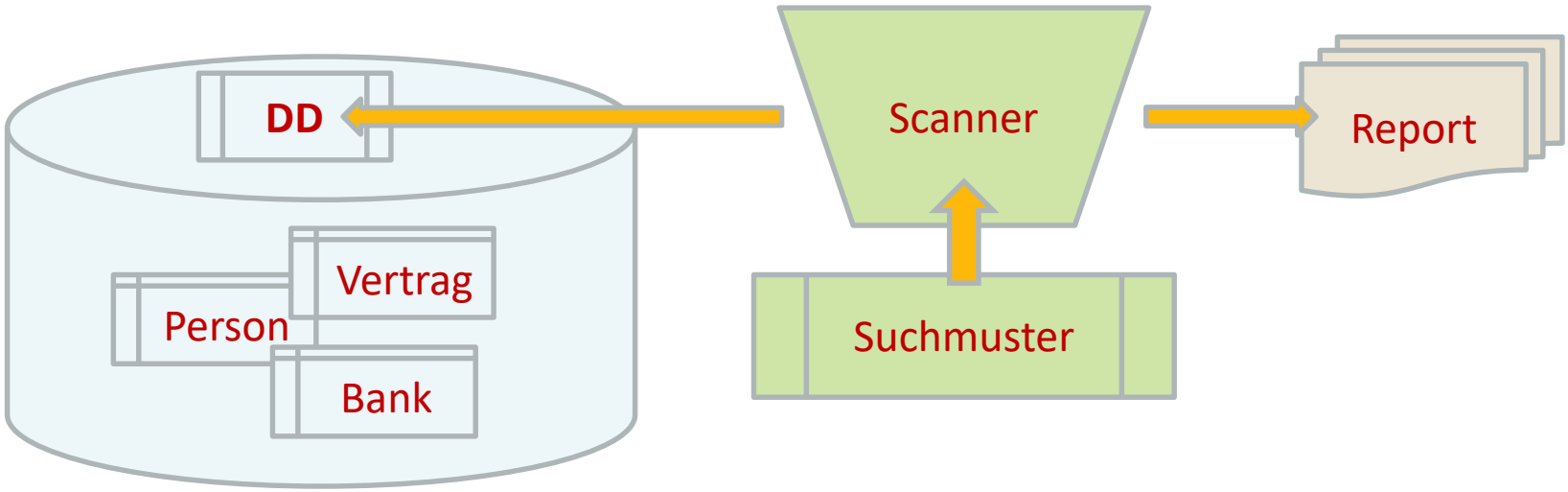
- Eine Spalte die „EMAIL“ heißt, könnte mit hoher Wahrscheinlichkeit tatsächlich eine E-Mail enthalten

- Kommentare, wie „Kreditkarten Nummer in Feld ZAHLWEGKID“, weist evtl. auf schützenswerte Daten hin

In der Theorie jedenfalls

Die Analyse

- Ein Scanner sucht nach bestimmten Mustern im Data Dictionary aller Datenbanken im Unternehmen



Bewertung

Vorteil	Nachteil
▪ Sehr Schnell ▪ Einfach umzusetzen ▪ Keine komplexe Software notwendig ▪ Geschätzt wird eine hohe Treffer-Quote erreicht	▪ Gewisse “False Positive” Rate wahrscheinlich (wie Spalten mit dem Namen “Position”) ▪ Optimierung auf die eigene Umgebung notwendig ▪ Keine echte Analyse auf den eigentlichen Daten

Werkzeuge für diese Aufgabe

- Selber bauen
  - Eigene Skripte entwickeln
- Kommerzielle Scannerlösungen
  - Wie die Lösungen von Herrn Kornbrust – Red Database Security - **GDPRSuite**
  - Die Oracle Lösung **DBSAT**
- Metadaten Handling einführen
  - Oracle Sensitive Data Discovery (Bestandteil des Database Masking and Subsetting Packs)
  - Oracle Enterprise Metadata Management **OEMM**

Die Oracle Lösung - DBSAT

- Ein Datenbank Scanner von Oracle
  - Kommandozeilen Werkzeug
  - Besteht aus 3 Elementen:
    - Collect => Skript für SQL*Plus für Security Frage Stellungen
    - Report => Reporting Werkzeug mit Python (ab 2.6)
    - **Discover** => DD Scanner auf Java Basis für PII Data
- Frei verwendbar für alle Kunden mit gültigen Support Vertrag

DBSAT – Zwei Teilbereiche

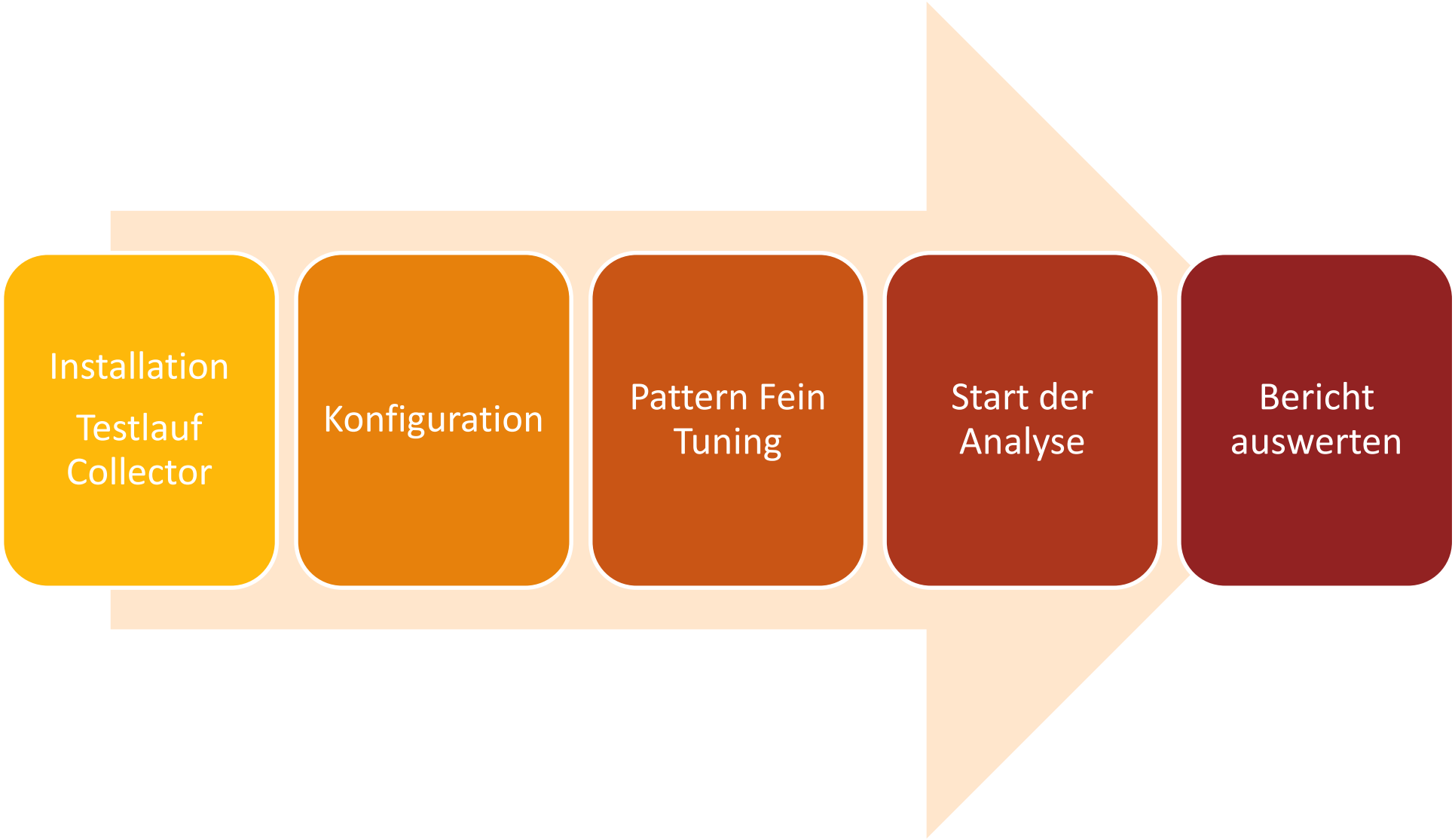
DB Security

- Sicherheits-Analyse der Datenbank Umgebung
- Analyse mit fest hinlegten SQL Abfragen per SQL*Plus
  - Analyse der DB Umgebung (z.B. der Listener) nur bei Linux/Unix möglich!
- Erzeugt übersichtliche Berichte und Hinweise zu Sicherheitsthemen der DB

DB “Sensible” Daten

- Suche im Data Dictionary mit Hilfe von Mustern nach “interessanten”, ”schützenwerten”, “persönlichen” Daten Speicherorten
- Frei definierbare Pattern werden für die Suche eingesetzt

Demo – Analyse einer DB auf PII Data



Download (1)

- Herunterladen über => Oracle Database Security Assessment Tool (DBSAT) (**Doc ID 2138254.1**)
  - Kostenlos für alle Oracle Kunden mit Zugang zum Oracle Support Portal mit aktuellen Support Vertrag

Security => MD5 Hash der Datei ist dort hinterlegt ! Immer genau auch prüfen

Download (2)

- Integrity Check durchführen!

```
PS C:\oracle\products> Get-FileHash -Algorithm SHA256 dbsat.zip

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          A485CFBF14AC9FFCF70CD0F0A8C101055B27EB30EDB54CB8040A4B4BBFB71165       C:\oracle\products\dbsat.zip
```

INTEGRITY CHECK

DBSAT zip file integrity

To make sure that the content is transferred correctly and has not been tampered or damaged during the download process you can validate if the SHA256 checksum o

DBSAT Release	SHA256 checksum
2.0.1 (December 2017)	a485cfbf14ac9ffcf70cd0f0a8c101055b27eb30edb54cb8040a4b4bbfb71165
1.0.2 (October 2016)	cca0d9fa7d446d837472e2321310a6b3342d420da7b34225507cc91db59d5a2e
1.0.1 (June 2016)	0ea517275102742e4b98679ff54e6ec317d02c2c4c316d68717132693beb7a33

If the values do not match, your downloaded dbsat.zip file is broken or was tampered. Please try the download again, and recheck.

Voraussetzungen

- Installation von Python Version 2 (>= 2.6) für die Reporter Komponente

- Java Runtime Environment (JRE) ab 1.6 für die Discoverer Komponente

- zip und unzip Kommando
  - Unter Windows einfach die mit der DB gelieferten Version unter $ORACLE_HOME/bin verwenden, wird mit gesetzten Oracle Home automatisch erkannt

Installation (1)

- Software auspacken

```
Expand-Archive
   The archive file 'C:\oracle\products\dbsat.zip' expansion is in progress...
   [ooooooooooooooooooooooooooooo
```

```
PS C:\oracle\products> Expand-Archive C:\oracle\products\dbsat.zip  -DestinationPath C:\oracle\products\dbsat
```

Installation (2)

- Umgebung (ORACLE_HOME und JAVA_HOME) setzen und starten

```
set-item -path ENV:ORACLE_HOME -value
C:\oracle\products\12.1.0.2\dbhome_1\

set-item -path env:JAVA_HOME -value "C:\Program
Files\Java\jre1.8.0_144"

.\dbsat.bat

Database Security Assessment Tool version 2.0.1 (December 2017)


Usage: dbsat collect [ -n ] <database_connect_string> <output_file>
       dbsat report [ -a ] [ -n ] [ -x <section> ] <input_file>
       dbsat discover [ -n ] -c <config_file> <output_file>

Options:
   -a          Run the reports for all the database accounts
   -n          No encryption for output
   -x          Specify sections to exclude from report (may be repeated for
               multiple sections)
   -c          Configuration file used for discoverer
```

Sicherheitsüberlegungen

- Das Tool über das Betriebssystem schützen!
  - Ein perfekter Ort um Schadcode zu hinterlegen, eine Manipulation der Dateien wird von der Software nicht selbstständig erkannt
  - ABER => Im Bericht des Reporters wird ein andere HASH angezeigt!

DBSAT Reporter integrity

The generated reports includes the checksum of the Reporter used to generate it (4 digits in the Reporter Version column). reinstall.

DBSAT Release	Checksum	Notes
2.0.1 (December 2017)	**d526**	* Added Discoverer module to find sensitive data.

Ein schöner Platz für ein Easter Egg

Datenbank User für die Analyse

- Einen User für die Analyse anlegen

```
sqlplus / AS sysdba

CREATE USER SECDBA IDENTIFIED BY "<this_is_a_real_secret_pasword_like_secdba>";

GRANT CREATE SESSION TO SECDBA ;

-- only read rights
GRANT select_catalog_role TO SECDBA ;
GRANT SELECT ON sys.registry$history TO SECDBA ;

-- 11g
GRANT SELECT ON sys.dba_users_with_defpwd TO SECDBA ;

-- 12c only
GRANT SELECT  ON audsys.aud$unified TO SECDBA ;
GRANT audit_viewer      TO SECDBA ;
GRANT capture_admin     TO SECDBA ;

-- Data Vault
GRANT DV_SECANALYST     TO SECDBA ;
```

Ein erster Aufruf bzgl. der DB Sicherheit

- Datenbank Daten einsammeln

```
.\dbsat collect secdba@oragpi collect_27_06_2018_db_gpi
```

=> SQL*Plus Script wird abgearbeitet

- Report erstellen

```
.\dbsat report collect_27_06_2018_db_gpi
```

Date of Data Collection	Date of Report	Reporter Version
Mon Jun 25 2018 23:20:00	Mon Jun 25 2018 23:22:59	2.0.1 (December 2017) - d526

Security Bericht auswerten (1)

- Auf die Checksum im Bericht achten

Oracle Database Security Assessment Tool (DBSAT) (**Doc ID 2138254.1**)

DBSAT Reporter integrity

The generated reports includes the checksum of the Reporter used to generate it (4 digits in the Reporter Version column). reinstall.

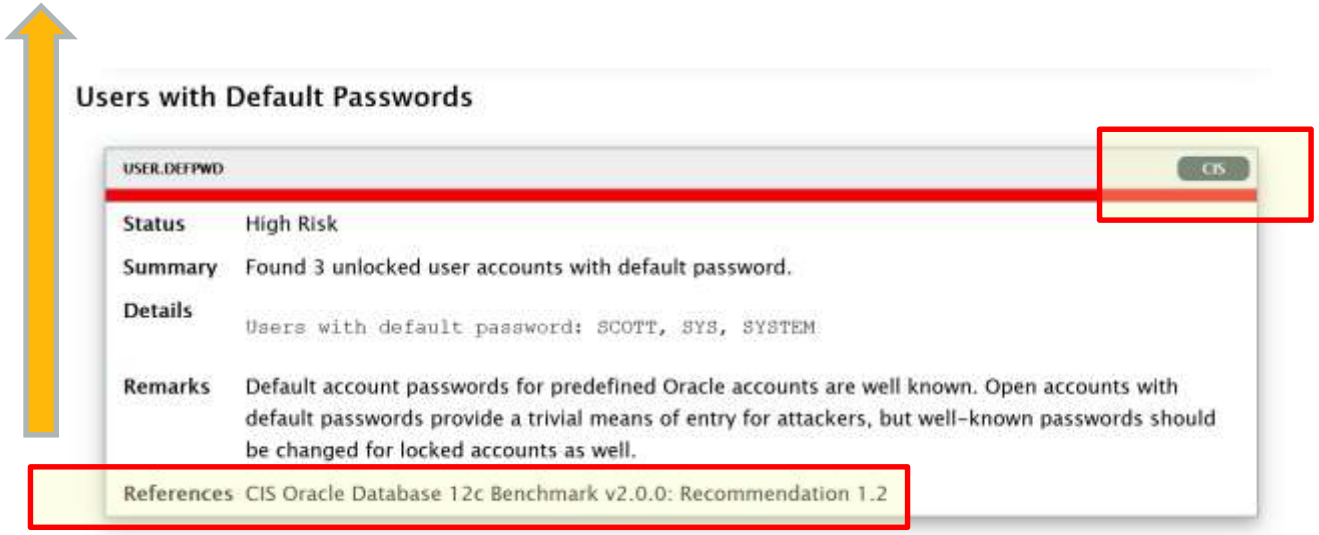
DBSAT Release	Checksum	Notes
2.0.1 (December 2017)	**d526**	* Added Discoverer module to find sensitive data.

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Wed Jun 27 2018 14:16:00	Wed Jun 27 2018 14:19:02	2.0.1 (December 2017) - d526

Security Bericht auswerten (2)

- Auf die Referenzen im Bericht achten
  - CIS Liste - Siehe => https://www.cisecurity.org/benchmark/oracle_database/



Discover Konfiguration für die PII Data Analyse

- Datei dbsat.config erstellen/anpassen
  - Kopie von sample_dbsat.config erstellen und anpassen

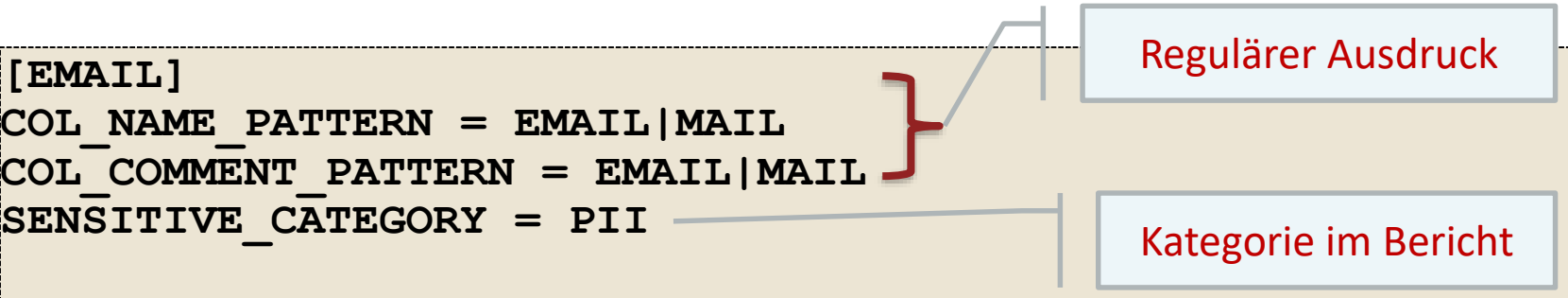
Datenbank Verbindung konfigurieren

```
#Configuration File for DBSAT Discoverer Tool
# Copyright (c) 2017, 2018, Oracle and/or its affiliates. All rights reserved.

############################################################

#Database Section: Allows the user to provide DB server details
[Database]

#DB_IP is the IP address or FQDN for the DB Server
#default is localhost

    DB_HOSTNAME = 10.10.10.1

#DB_PORT is the port at which the DBSat tool needs to connect to
#default is 1521

        DB_PORT = 1521

#DB_SERVICE_NAME is the service Name for the DB
#default is empty

        DB_SERVICE_NAME = GPI

############################################################

```

Fein Tuning – Pattern File anpassen

- Pattern Datei sensitive_en.ini anpassen

```
[EMAIL]
COL_NAME_PATTERN = EMAIL|MAIL
COL_COMMENT_PATTERN = EMAIL|MAIL
SENSITIVE_CATEGORY = PII

[PHONE]
COL_NAME_PATTERN =
PHONE|^TEL|^CELL|MOBILE|((WORK|OFFICE|CONTACT).*(NUM|NO|NBR))
COL_COMMENT_PATTERN = Phone|Telephone|Cellphone|Mobile N|Work N|Office
N|Contact N
SENSITIVE_CATEGORY = PII
```



Analyse

- Aufruf des Werkzeuges dbsat

```
 set-item -path env:JAVA_HOME -value "C:\Program Files\Java\jre1.8.0_144"

.\dbsat discover -c .\Discover\conf\dbsat.config discover_gpi_db_28_05_2018

..


Enter username: secdba
Enter password:
DBSAT Discover ran successfully.
.
Calling c:\oracle\products\12.2.0.1\dbhome_1\bin\zip.exe to encrypt the generated reports
.
Enter password:
Verify password:
  adding: discover_gpi_db_28_05_2018_discover.html (200 bytes security) (deflated 82%)
  adding: discover_gpi_db_28_05_2018_discover.csv (200 bytes security) (deflated 79%)
zip completed successfully.
```

Auswertung

Summary

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
JOB DATA	6	15	55969
PII	4	13	55930
PII – ADDRESS	6	25	55891
PII – IT DATA	7	8	677
PII-LINKED	2	4	55819
PII-LINKED – BIRTH DETAILS	1	1	319
TOTAL	16*	66	56380**

* Number of unique Tables with Sensitive Data.

** Number of unique Rows with Sensitive Data.

Sensitive Data

Schemas with Sensitive Data

Risk Levels	High Risk, Medium Risk
Summary	Found 7 schemas with sensitive data.
Location	Schemas with sensitive data: CONBOOK, HR, OE, PM, SCOTT, SH, SPA

Tables Detected within Sensitive Category: PII

Risk Level	High Risk
Summary	Found PII within 13 Column(s) contained in 4 Table(s)
Location	Tables: HR.EMPLOYEES, OE.CUSTOMERS, PM.PRINT_MEDIA, SH.CUSTOMERS

Schema View

Table Summary

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
CONBOOK	KUNDEN	7	1	2	PII – IT DATA
HR	COUNTRIES	3	3	25	PII – ADDRESS
HR	DEPARTMENTS	4	1	27	PII – IT DATA
HR	EMPLOYEES	11	9	107	JOB DATA, PII
HR	JOBS	4	3	19	JOB DATA
HR	JOB_HISTORY	5	1	10	JOB DATA
HR	LOCATIONS	6	6	23	PII – ADDRESS, PII – IT DATA
OE	CUSTOMERS	15	10	319	JOB DATA, PII, PII – ADDRESS, PII – IT DATA, PII-LINKED, PII-LINKED – BIRTH DETAILS
OE	PRODUCT_INFORMATION	11	1	288	PII – IT DATA
OE	WAREHOUSES	5	2	9	PII – IT DATA
PM	PRINT_MEDIA	10	1	4	PII
SCOTT	EMP	8	4	14	JOB DATA
SH	COUNTRIES	10	10	23	PII – ADDRESS
SH	CUSTOMERS	23	12	55500	JOB DATA, PII, PII – ADDRESS, PII-LINKED
SPAREPORT_STB	COMPONENT_SCHEMA_INFO	11	1	9	PII – IT DATA
SPAREPORT_STB	SERVICETABLE	6	1	1	PII – ADDRESS

Sensitive Column Details

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type
CONBOOK	KUNDEN	GEBURTSDATUM	--	PII – IT DATA	LOCATION
HR	COUNTRIES	COUNTRY_ID	Primary key of c...	PII – ADDRESS	COUNTRY
HR	COUNTRIES	COUNTRY_NAME	Country name	PII – ADDRESS	COUNTRY
HR	COUNTRIES	REGION_ID	Region ID for th...	PII – ADDRESS	COUNTRY
HR	DEPARTMENTS	LOCATION_ID	Location id whe...	PII – IT DATA	LOCATION

Exclude Liste anlegen

- Falls zu viel gefunden wird – Ausnahme-Datei erstellen
  - Ignore ini Datei anlegen - ignore_tables.ini

```
#EXCLUSION_LIST_FILE contains schemas, tables and columns to be excluded from the scan
#This file contains one entry per line.
#An entry is presented as SchemaName OR
#                         SchemaName.TableName OR
#                         SchemaName.TableName.ColumnName
#To exclude all tables in that schema include SchemaName
#To exclude all columns in that table include SchemaName.TableName
#To exclude a specific column from scan, list SchemaName.TableName.ColumnName
GPI
IX
GPI.TOAD_PLAN_TABLE
GPI.HTMLDB_PLAN_TABLE
HR.TOAD_PLAN_TABLE
GPI.TOAD_PLAN_TABLE
GPI.HTMLDB_PLAN_TABLE
```

  - Parameter Datei anpassen - dbsat.config

```
55
56      EXCLUSION_LIST_FILE = ignore_tables.ini
57
```

Deutsche Pattern Datei

- Inoffizielle Version über den Oracle Vertrieb erhältlich
  - Ansprechpartnerin
    Justyna Biernat justyna.biernat@oracle.com
  - DBSAT Tool EMEA Produkt Manager, Herr Pedro Lopes

Integration in Audit Vault

- Erzeugte CSV Daten in Audit Valut integrieren
  - Norman Sibbing fragen .-)
  - Zum Beispiel die Spalten aus dem Bericht erweitert auditieren – Stichwort „Fine grained auditing“

Diskussion

Hilft das bei der DSGVO?

Wie halten Sie es mit Metadaten Handling in Ihrem Unternehmen?

Konnten Sie schon Erfahrungen mit dbsat sammeln?

Werden Sie das Tool einsetzen?

Fazit

- **Pro:**
  - Einfach und komfortabel im Einsatz ohne Installations-aufwand
  - Kostenlos für Kunden mit gültigen Oracle Support Vertrag
  - Einheitlich alle Oracle Datenbanken überwachen
  - Übersichtliches Reporting der wichtigsten Grund-voraussetzungen
  - Analyse des DD mit regulären Ausdrücken erweiterbar

- **Contra:**
  - Standard Sicherheitsregeln nicht als Pattern hinterlegt, Standard Regeln nicht einfach zu erweitern

Mehr

- Siehe
  - Webinar => http://www.doag.org/go/newsletter/180620/cw_link1
  - Blog: => https://www.pipperr.de/dokuwiki/doku.php?id=dba:oracle_dbsat
- Wieder mal eine andere Skript Library
  - https://github.com/gpipperr/OraPowerShell
- Bildmaterial : https://pixabay.com

F & A

Fragen

Fragen zu DBSAT ?