INTEGRIGY

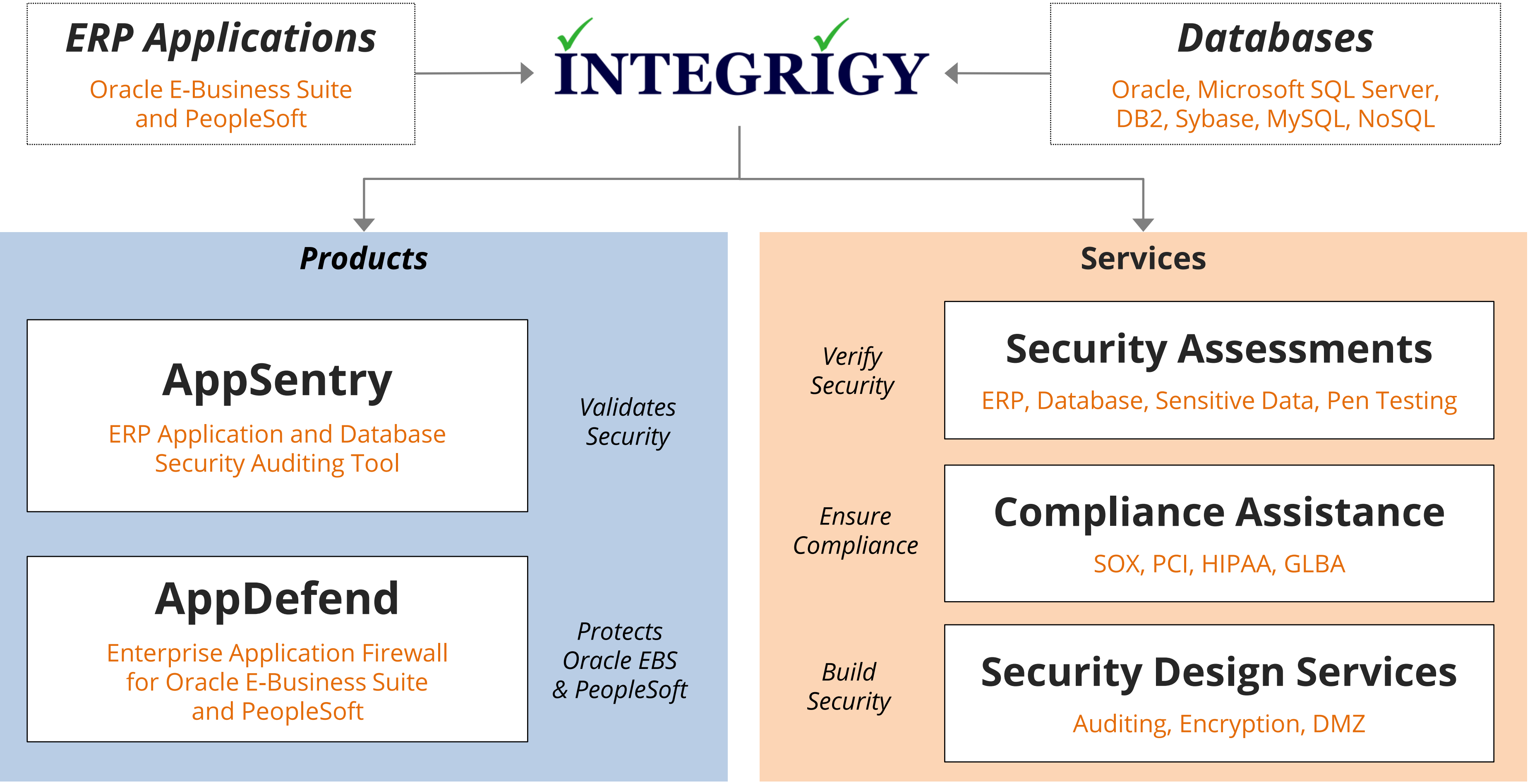
The Thrifty DBAs Guide to Open Source (or Free) Database Security Tools

June 4, 2020

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications

Oracle E-Business Suite and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Firewall for Oracle E-Business Suite and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE®
Gold Partner

Agenda

1 Introduction

2 Auditing

3 Assessment

4 Q & A

thrift·y [**thrif**-tee]

adjective

1. using money or other resources carefully and wastefully.
2. thriving, prosperous, or successful.
3. saving money by not buying unnecessary security products.

Agenda

1 Introduction

2 Auditing

3 Assessment

4 Q & A

Auditing Security Requirements

- Must audit key database security events and access by generic accounts
- Audit trail must be retained and protected centrally
- Alerts for potential security incidents must be raised
- Audit trail must be archived for forensic purposes
- May require auditing of access to key application tables that contain sensitive data

Commercial Auditing Solutions

There are a number of commercial database activity monitoring (DAM) solutions available at significant cost and implementation effort.

Oracle Audit Vault	▪ Licensing per processor monitored or audited ▪ $ 6,000 per processor license ▪ $ 1,320 per processor support and maintenance
Imperva	▪ Starting at $ 40,000 for 25 databases ▪ Starting at $ 6,400 per year support and maintenance
IBM Guardium	▪ Starting at about $ 60,000 including first year support and maintenance

Pricing is from the Oracle Technology Global Price List (12/16) and other sources. Actual cost will vary based on implementation, number of databases, and discounts.

Auditing Design

Use Integrigy Database Auditing and Logging Framework as starting point!

E1 - **Login**	*E8* - **Modify role**
E2 - **Logoff**	*E9* - **Grant/revoke user privileges**
E3 - **Unsuccessful login**	*E10* - **Grant/revoke role privileges**
E4 - **Modify auth mechanisms**	*E11* - **Privileged commands**
E5 - **Create user account**	*E12* - **Modify audit and logging**
E6 - **Modify user account**	*E13* - **Create, modify or delete object**
E7 - **Create role**	*E14* - **Modify configuration settings**

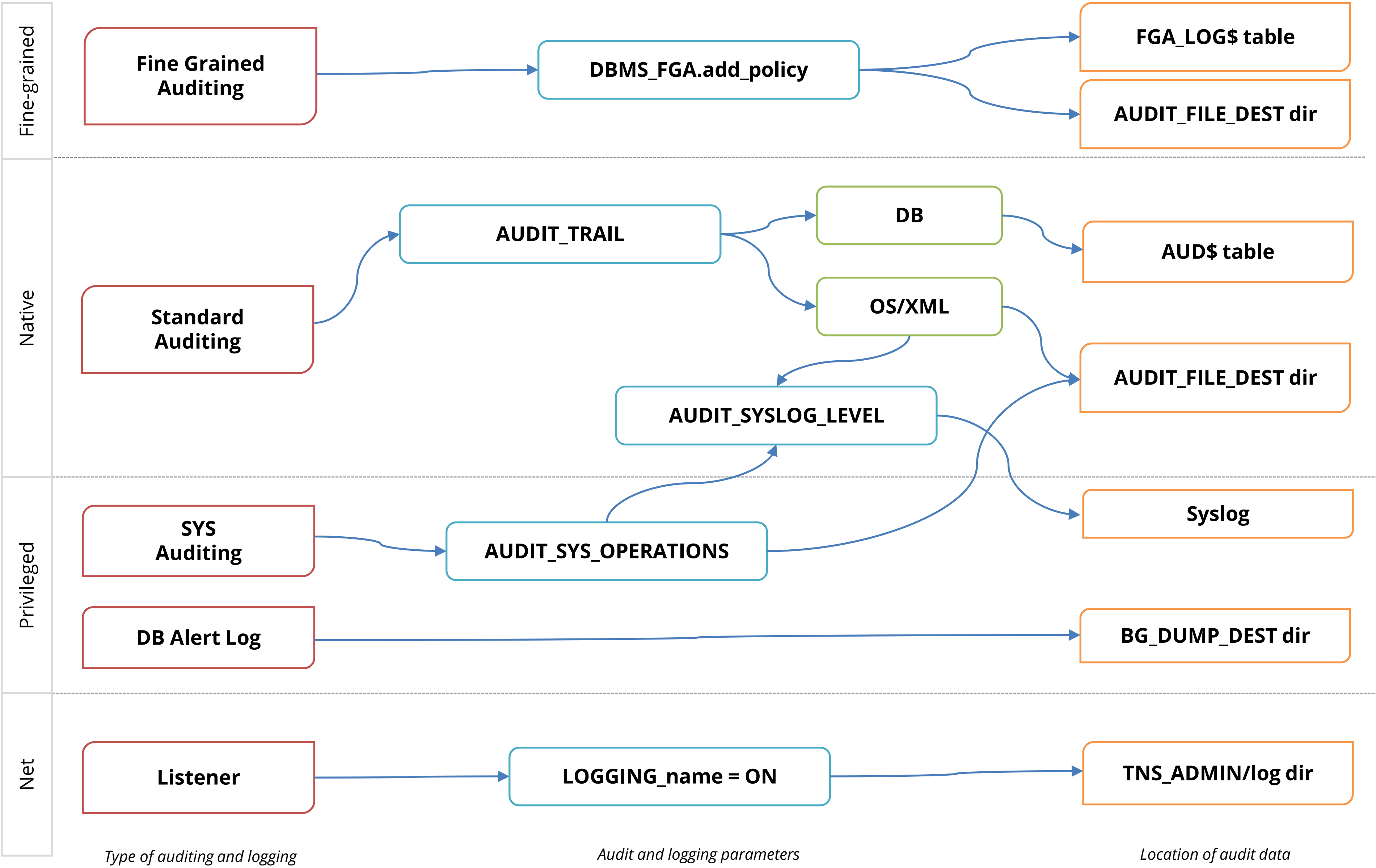
https://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

Foundation Security Events Mapping

Security Events and Actions	PCI DSS 10.2	SOX (COBIT)	HIPAA (NIST 800-66)	IT Security (ISO 27001)	FISMA (NIST 800-53)
E1 - Login	10.2.5	A12.3	164.312(c)(2)	A 10.10.1	AU-2
E2 - Logoff	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E3 - Unsuccessful login	10.2.4	DS5.5	164.312(c)(2)	A 10.10.1 A.11.5.1	AC-7
E4 - Modify authentication mechanisms	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E5 – Create user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E6 - Modify user account	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E7 - Create role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E8 - Modify role	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E9 - Grant/revoke user privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E10 - Grant/revoke role privileges	10.2.5	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E11 - Privileged commands	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2
E12 - Modify audit and logging	10.2.6	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-9
E13 - Objects Create/Modify/Delete	10.2.7	DS5.5	164.312(c)(2)	A 10.10.1	AU-2 AU-14
E14 - Modify configuration settings	10.2.2	DS5.5	164.312(c)(2)	A 10.10.1	AU-2

https://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

Oracle Database Auditing and Logging



Centralized Logging Solutions (Free, On-premise)

ELK (Elasticsearch, Logstash, Kibana)	▪ Open Source ▪ Visualizations using Kibana ▪ Add-ons for alerting and reporting
GrayLog	▪ Open Source ▪ Based on Elastic Search and MongoDB ▪ Alerting, dashboards, and searching
Splunk Free	▪ 500MB/day ▪ No signon security ▪ Splunk DB Connect add-on ▪ Splunk Oracle Database add-on

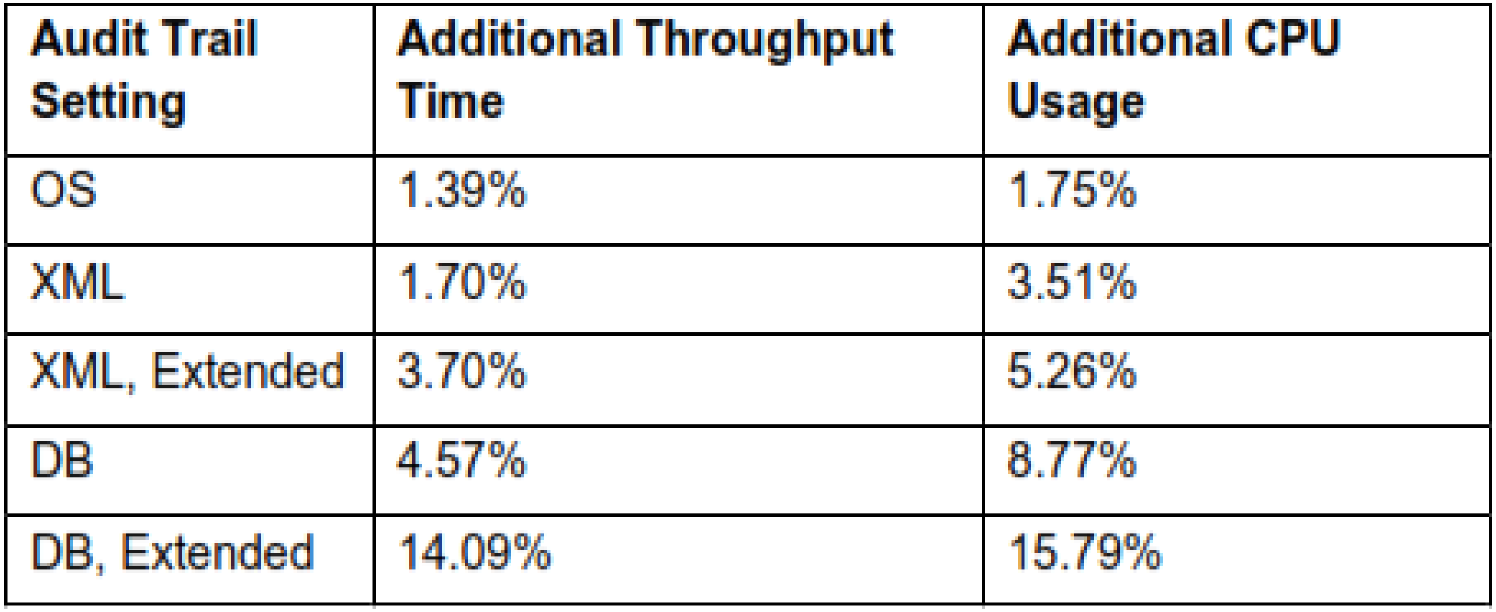
Database Audit Trail – SYSLOG

- **AUDIT_SYSLOG_LEVEL = "facility.priority"**
  - Available starting with 10.2
  - Set AUDIT_TRAIL=OS
  - Audit trail and SYS audit trail written to standard Unix/Linux Syslog
  - Can only be modified by root and completely protected from DBA, except disabling auditing
  - Send to external logging system using standard Syslog functionality (@<ip address>)

```
alter system set audit_syslog_level="local1.warning" scope=spfile;
```

See MOS Note ID 1528104.1 “How to read a SYSLOG audit trail record”

Oracle Auditing Performance



Audit Trail Setting	Additional Throughput Time	Additional CPU Usage
OS	1.39%	1.75%
XML	1.70%	3.51%
XML, Extended	3.70%	5.26%
DB	4.57%	8.77%
DB, Extended	14.09%	15.79%

Table 3 – Oracle Database 11.2.01 Standard Audit Trail with 50% CPU System Load

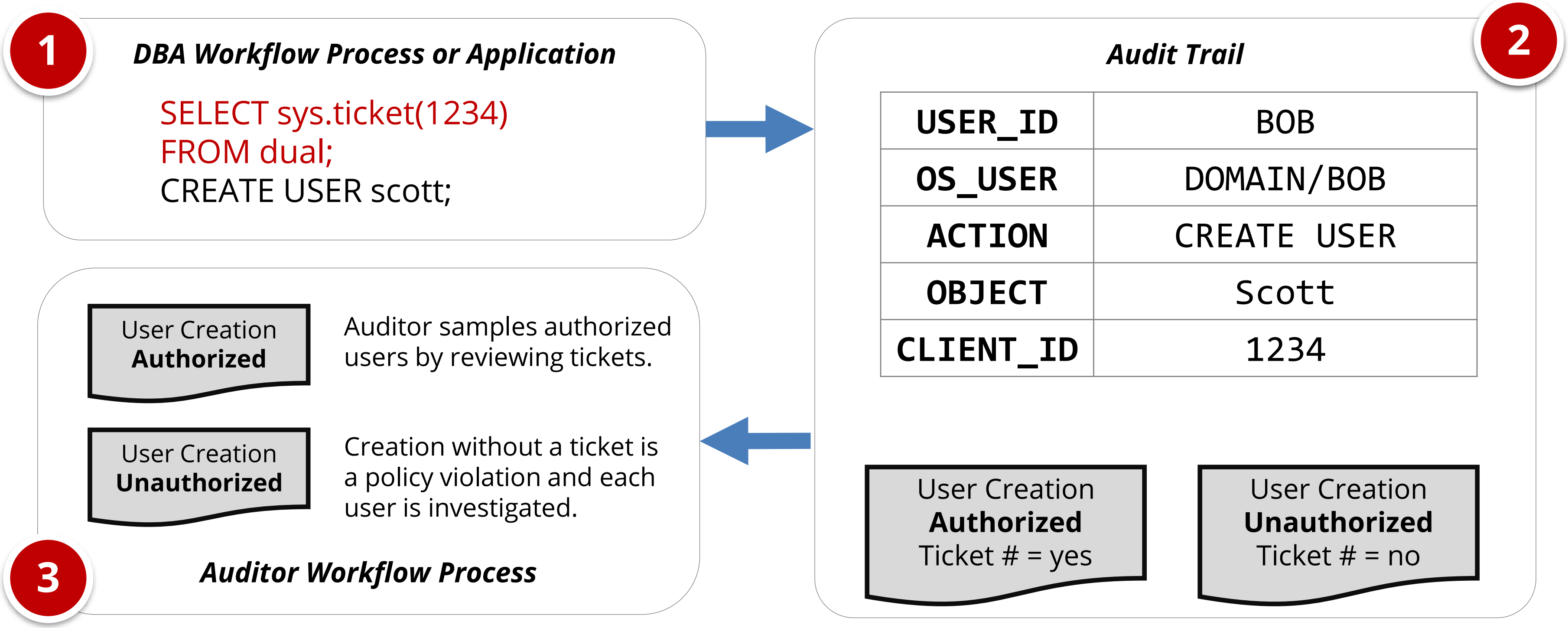
Source: Oracle Database Auditing: Performance Guidelines, August 2010

Oracle Client Identifier

Application	Example of how used
E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the FND_USER.USERNAME of the user logged on. Prior to Release 12, follow Support Note How to add DBMS_SESSION.SET_IDENTIFIER(FND_GLOBAL.USER_NAME) to FND_GLOBAL.APPS_INITIALIZE procedure (Doc ID 1130254.1)
PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.
SAP	With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.
Oracle Business Intelligence Enterprise Edition(OBIEE)	When querying an Oracle database using OBIEE the connection pool username is passed to the database. To also pass the middle-tier username, set the user identifier on the session. Edit the RPD connection pool settings and create a new connection script to run at connect time. Add the following line to the connect script: CALL DBMS_SESSION.SET_IDENTIFIER('VALUEOF(NQ_SESSION.USER)')

Change Management Tracking – Create User Example

Capture change ticket numbers and other information for a database session based on special SQL executed by database users or applications.



1

DBA Workflow Process or Application

```
SELECT sys.ticket(1234)
FROM dual;
CREATE USER scott;
```

2

Audit Trail

USER_ID	BOB
OS_USER	DOMAIN/BOB
ACTION	CREATE USER
OBJECT	Scott
CLIENT_ID	1234

User Creation **Authorized** Ticket # = yes

User Creation **Unauthorized** Ticket # = no

3

User Creation **Authorized**

Auditor samples authorized users by reviewing tickets.

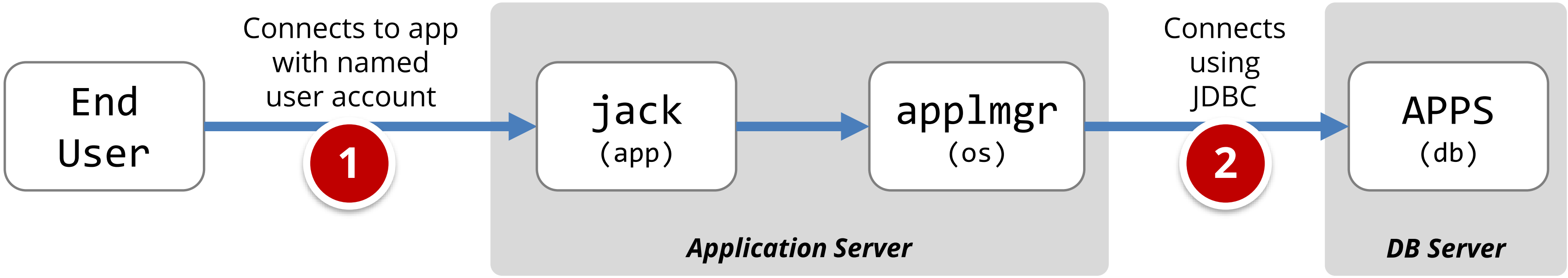
User Creation **Unauthorized**

Creation without a ticket is a policy violation and each user is investigated.

Auditor Workflow Process

Application End User Tracking – Solution

Database auditing tools are able to capture web application end-users and correlate the application end-user to SQL statements. Support depends on the application and includes both package and custom applications.



DAM Audit Record with “Application User” Feature Enabled

DB User	OS User	Machine	Program	SQL	Application User
APPS	applmgr	APPSERVER1	JDBC	select * from credit_cards	jack

This example is Oracle E-Business Suite R12

Splunk Free Demonstration

Agenda

1 Introduction

2 Auditing

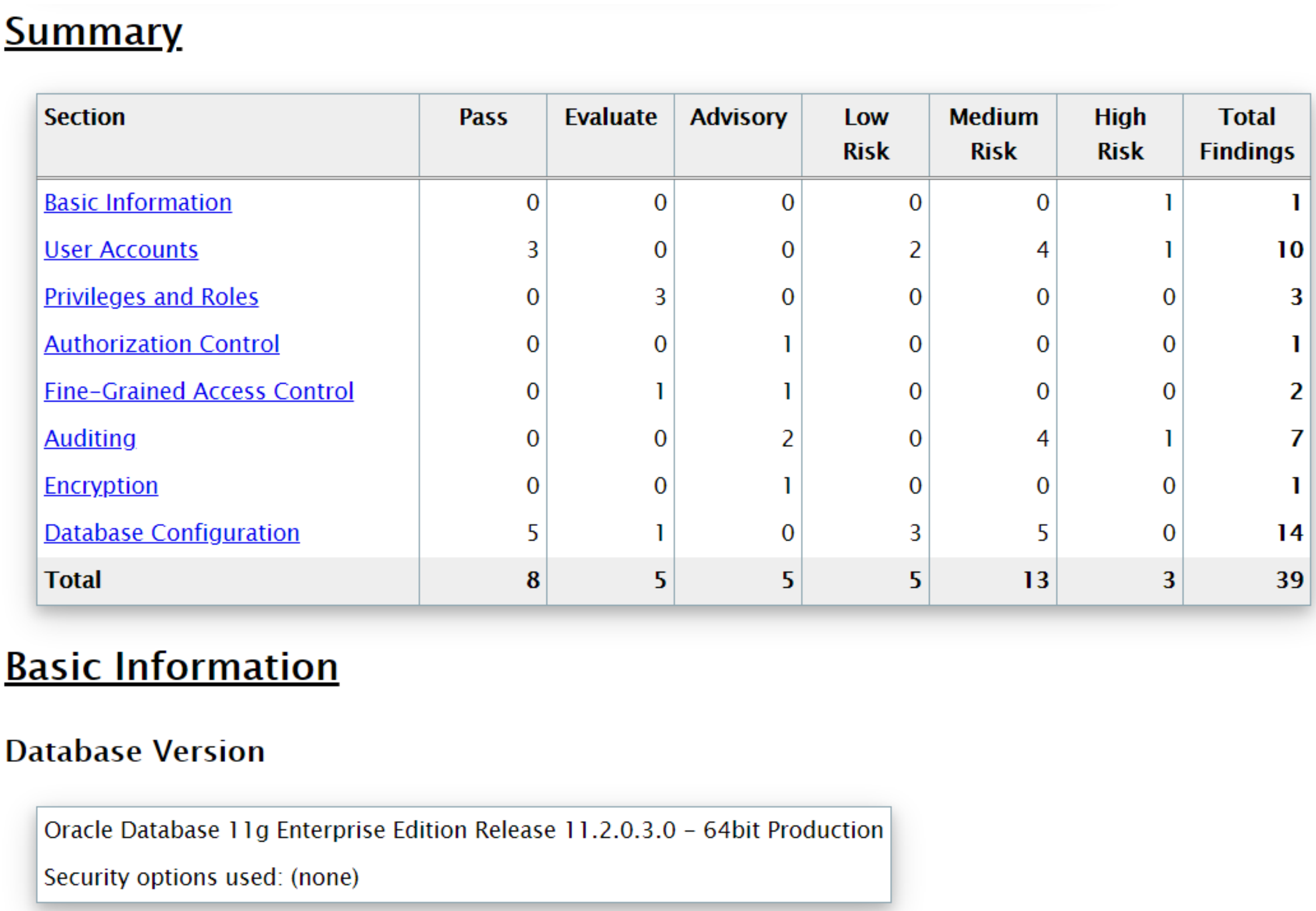
3 Assessment

4 Q & A

Database Security Assessment Tool (DBSAT)

- **DBSAT is a free tool for assessment Oracle Database security**
  - Introduced January 2018
  - Free download from oracle.com
  - https://www.oracle.com/database/technologies/security/dbsat.html
- **Run locally on database server or remotely**
  - Locally also checks OS file permissions and Listener
- **Checks Oracle Database against a fixed security policy**
  - Shows latest CPU patch
  - Check DBA_USERS_WITH_DEFPWD
  - Initialization parameters
  - Auditing configuration
  - Excessive user privileges
  - Sensitive data search

Database Security Assessment Tool (DBSAT)



Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	**1**
User Accounts	3	0	0	2	4	1	**10**
Privileges and Roles	0	3	0	0	0	0	**3**
Authorization Control	0	0	1	0	0	0	**1**
Fine-Grained Access Control	0	1	1	0	0	0	**2**
Auditing	0	0	2	0	4	1	**7**
Encryption	0	0	1	0	0	0	**1**
Database Configuration	5	1	0	3	5	0	**14**
Total	**8**	**5**	**5**	**5**	**13**	**3**	**39**

Basic Information

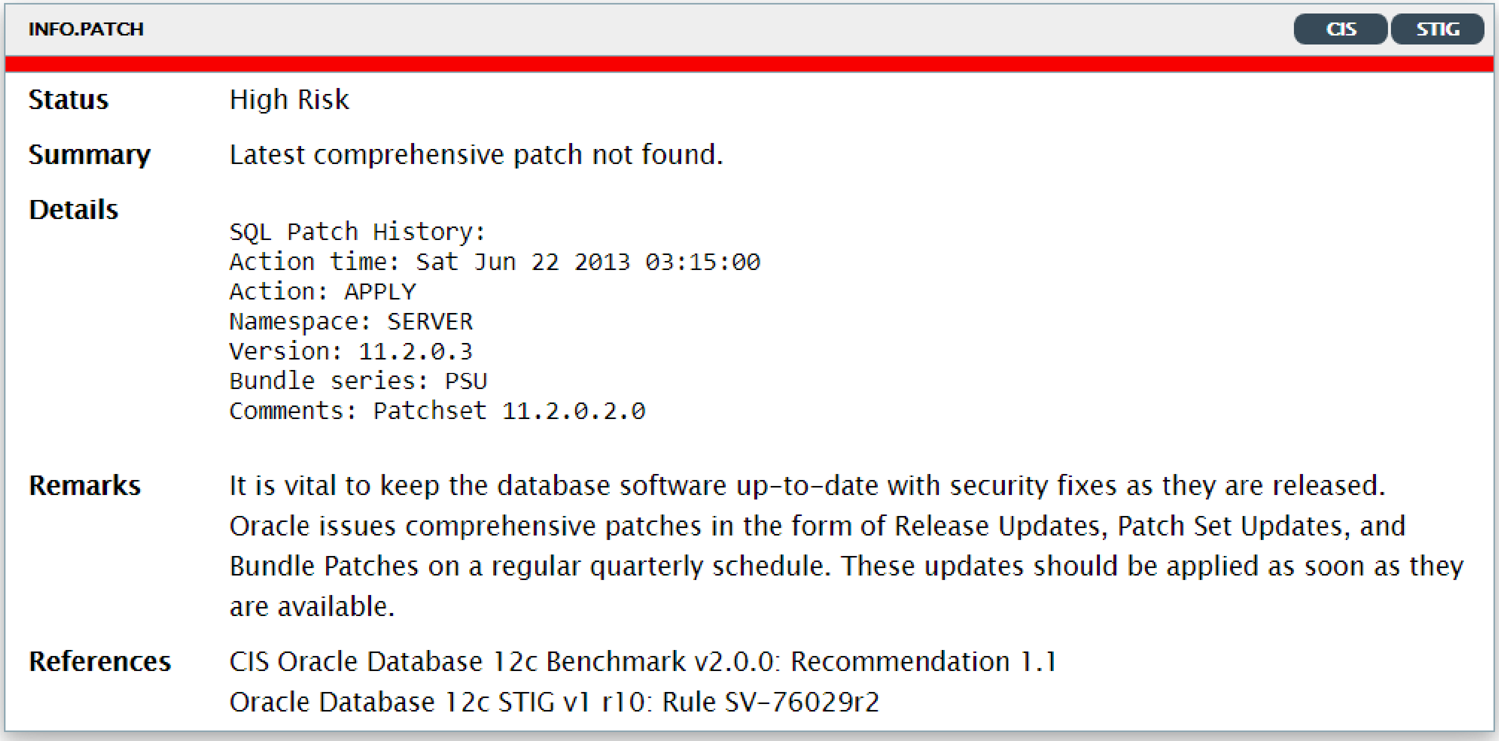
Database Version

Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production

Security options used: (none)

Database Security Assessment Tool (DBSAT)

Patch Check



Status High Risk

Summary Latest comprehensive patch not found.

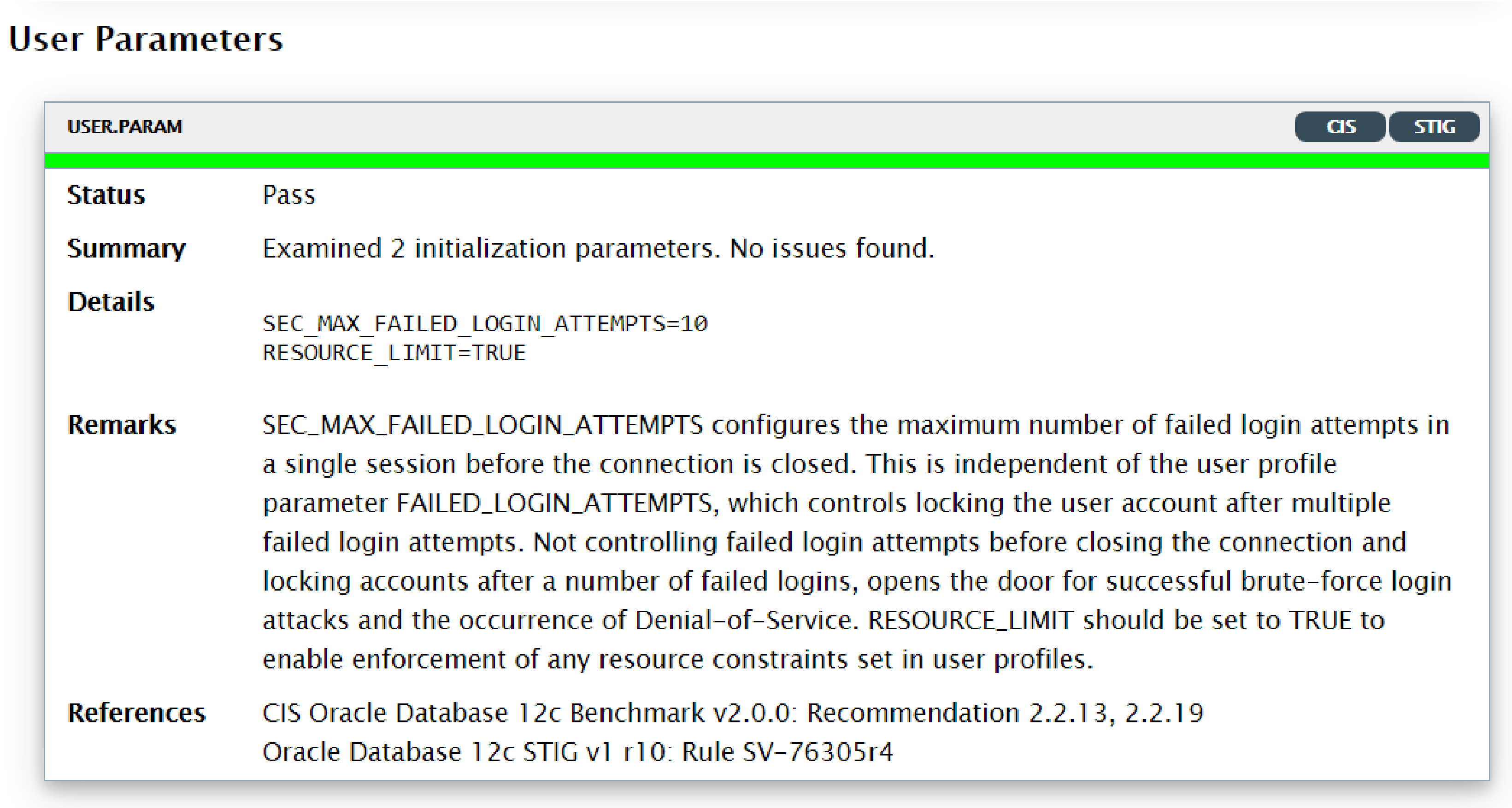
Details

```
SQL Patch History:
Action time: Sat Jun 22 2013 03:15:00
Action: APPLY
Namespace: SERVER
Version: 11.2.0.3
Bundle series: PSU
Comments: Patchset 11.2.0.2.0
```

Remarks It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates, Patch Set Updates, and Bundle Patches on a regular quarterly schedule. These updates should be applied as soon as they are available.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.1
Oracle Database 12c STIG v1 r10: Rule SV-76029r2

Database Security Assessment Tool (DBSAT)



User Parameters

USER.PARAM

Status Pass

Summary Examined 2 initialization parameters. No issues found.

Details

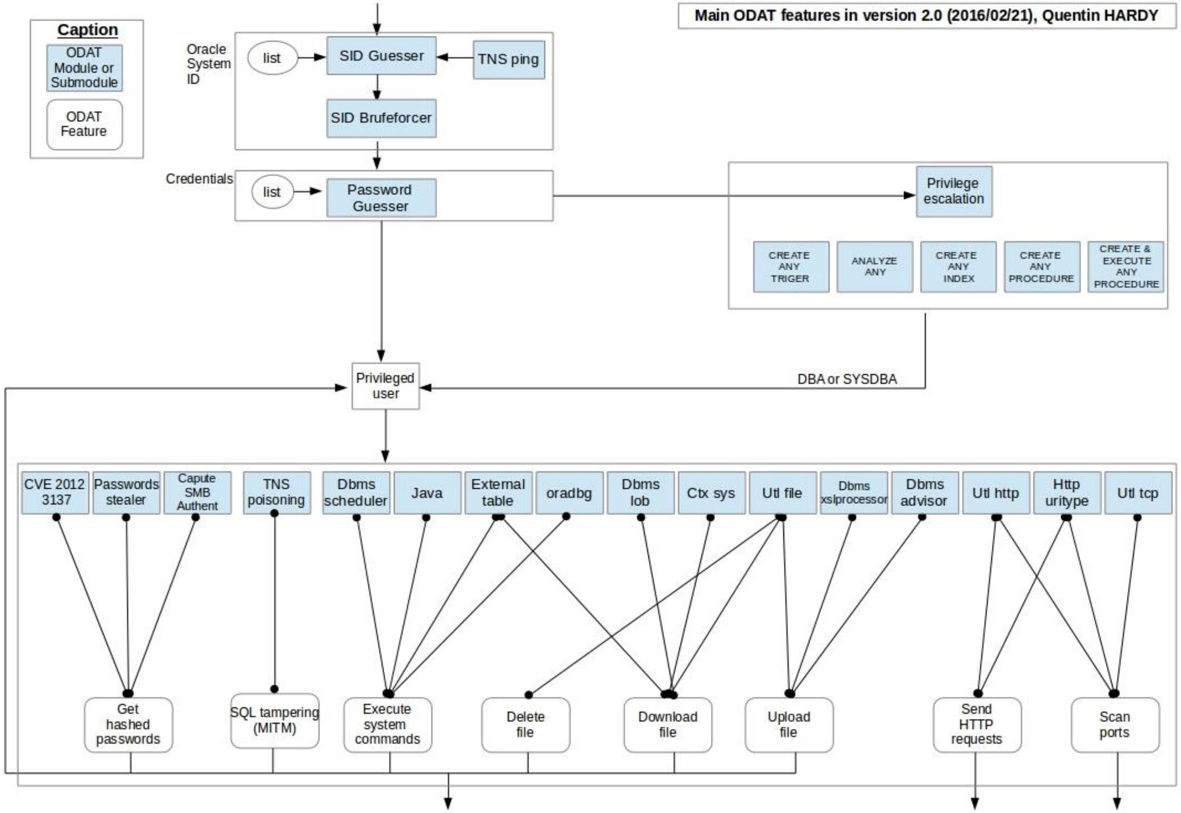
```
SEC_MAX_FAILED_LOGIN_ATTEMPTS=10
RESOURCE_LIMIT=TRUE
```

Remarks SEC_MAX_FAILED_LOGIN_ATTEMPTS configures the maximum number of failed login attempts in a single session before the connection is closed. This is independent of the user profile parameter FAILED_LOGIN_ATTEMPTS, which controls locking the user account after multiple failed login attempts. Not controlling failed login attempts before closing the connection and locking accounts after a number of failed logins, opens the door for successful brute-force login attacks and the occurrence of Denial-of-Service. RESOURCE_LIMIT should be set to TRUE to enable enforcement of any resource constraints set in user profiles.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.13, 2.2.19
Oracle Database 12c STIG v1 r10: Rule SV-76305r4

ODAT – Security Testing Oracle Databases

ODAT (https://github.com/quentinhardy/odat) is a free and open source Oracle Database penetration testing tool.   Includes features to find databases, compromise database accounts, and elevate privileges.



ODAT – Penetration Testing

Using ODAT to automatically test database

```
python3 ./odat.py all -s 192.168.2.16 -p 1521
```

Nmap – Security Testing Oracle Databases

Nmap (nmap.com) is a free and open source network discovery and security testing tool. Nmap has a number of Oracle specific “scripts”.

oracle-brute	▪ Brute-force Oracle passwords using a pre-defined list of usernames and passwords
oracle-brute-stealth	▪ Exploit O5Login security vulnerability (CVE-2012-3137) in 11.x and brute-force a pre-defined list of database accounts using a password list
oracle-enum-users	▪ List database accounts in the database from a pre-defined list of database accounts by exploiting the O5Login vulnerability.
oracle-sid-brute	▪ Brute-force the Oracle SID if not known for an IP address and port number against a pre-defined list
oracle-tns-version	▪ Display the version of the TNS listener

Nmap – Network Scanning – Find Databases

Using Nmap to find Oracle databases

www.nmap.com

```
nmap -sT -sV -p 1521-1529 -T4 -v -n -Pn –open 192.168.2.11-50
```

Nmap – Brute Force Database Accounts

Using Nmap for Database Password Guessing

www.nmap.com

```
nmap -p 1521 -v --script oracle-brute

--script-args oracle-brute.sid=ORCL 192.168.56.10
```

Show SQL Developer Passwords

Decrypt SQL Developer passwords

`https://github.com/tomecode/show-me-password-sqldev-jdev`

Use extension in SQL Developer

Agenda

1 Introduction

2 Auditing

3 Assessment

4 Q & A

Integrigy Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**