

# Oracle Database

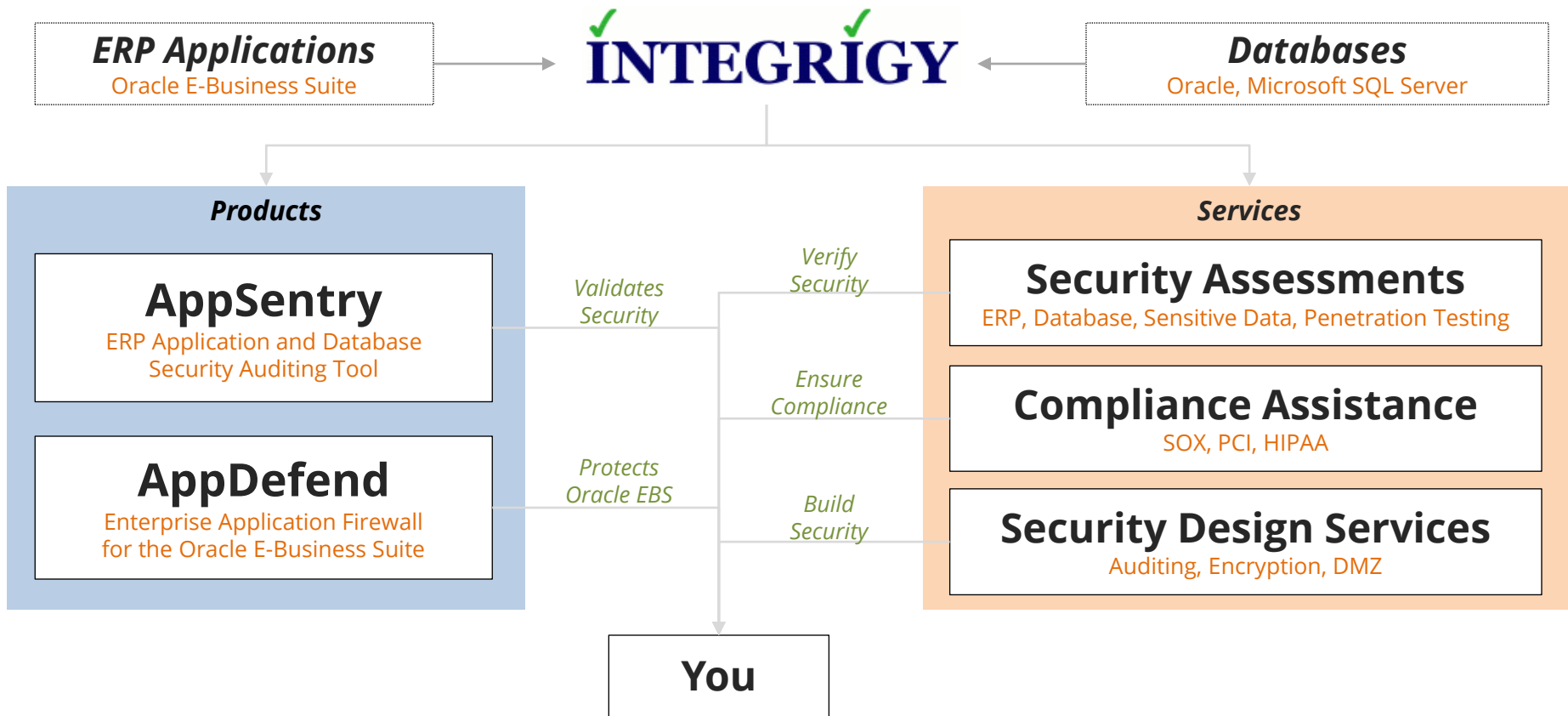
# *Security Myths*

December 13, 2012

Stephen Kost  
Chief Technology Officer  
Integrigy Corporation

Phil Reimann  
Director of Business Development  
Integrigy Corporation

# About Integrigy



# Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
<b>Critical Patch Update July 2011</b>	11.5.10 – 12.1.x	<ul style="list-style-type: none"> <li>Oracle E-Business Suite security configuration issue</li> </ul>
<b>Critical Patch Update October 2010</b>	11.5.10 – 12.1.x	<ul style="list-style-type: none"> <li>2 Oracle E-Business Suite security weaknesses</li> </ul>
<b>Critical Patch Update July 2008</b>	Oracle 11g 11.5.8 – 12.0.x	<ul style="list-style-type: none"> <li>2 Issues in Oracle RDBMS Authentication</li> <li>2 Oracle E-Business Suite vulnerabilities</li> </ul>
<b>Critical Patch Update April 2008</b>	12.0.x 11.5.7 – 11.5.10	<ul style="list-style-type: none"> <li>8 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update July 2007</b>	12.0.x 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>11 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update October 2005</b>	11.0.x, 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>Default configuration issues</li> </ul>
<b>Critical Patch Update July 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>SQL injection vulnerabilities</li> <li>Information disclosure</li> </ul>
<b>Critical Patch Update April 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>SQL injection vulnerabilities</li> <li>Information disclosure</li> </ul>
<b>Critical Patch Update Jan 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #68</b>	Oracle 8i, 9i, 10g	<ul style="list-style-type: none"> <li>Buffer overflows</li> <li>Listener information leakage</li> </ul>
<b>Oracle Security Alert #67</b>	11.0.x, 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>10 SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #56</b>	11.0.x, 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>Buffer overflow in FNDWRR.exe</li> </ul>
<b>Oracle Security Alert #55</b>	11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>Multiple vulnerabilities in AOL/J Setup Test</li> <li>Obtain sensitive information (valid session)</li> </ul>
<b>Oracle Security Alert #53</b>	10.7, 11.0.x 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>No authentication in FNDDFS program</li> <li>Retrieve any file from O/S</li> </ul>



# Myth: The Oracle Database is **secure** out of the box

Started as Project Oracle at the CIA, Unbreakable marketing campaign, ...



# Reality: The Oracle Database requires **significant effort** to make it secure and compliant

Oracle has significantly improved in 11g the default installation by setting passwords, locking accounts, including better password profiles, and enabling default auditing, but ...

#2

**Myth: An Oracle Database is secure if you implement most items in a **security checklist****

Oracle's Database Security Checklist, Department of Defense STIG, Center for Internet Security Oracle Benchmark, SANS Oracle Database Security Checklist, etc.

#2

Reality: All items in the security checklists are a **base minimum** and additional steps are required

A good starting point but must be tailored to the organization and application and expanded to be effective.













# Database Security Checklists

**Database security checklists** are used to secure databases one at a time.

- Excellent baseline and starting point
- Often in conflict with application configuration
- Too many exceptions required to handle application limitations
- Need to validate compliance with checklist



# Oracle Database Security Checklists

Security Checklist	Versions	Last Updated	Installation	Configuration	Administration
<b>1. Oracle's Database Security Checklist</b>	Oracle 9i Oracle 10g Oracle 11g	Oct 2011			
<b>2. DOD DISA STIG</b>	Oracle 9i Oracle 10g Oracle 11g	Aug 2010			
<b>3. Center for Internet Security (CIS) Oracle Benchmarks</b>	Oracle 9i Oracle 10g Oracle 11g	Dec 2011			
<b>4. SANS Database Security Checklist</b>	Oracle 9i Oracle 10g	Nov 2006			

# DB Security Standards - Content

**What**

What needs to be secured in the database?

**Why**

Why is this a security issue? What's the impact?

**How**

What are the exact steps required to secure this? Step by step

**Verification**

How is this setting verified precisely? A single SQL statement

**Mitigation**

Besides an exception, what else can be done? Auditing?

**High percentage of  
exceptions or variances**

**= FAILURE**

*Database security standards must  
anticipate common exceptions*

#3

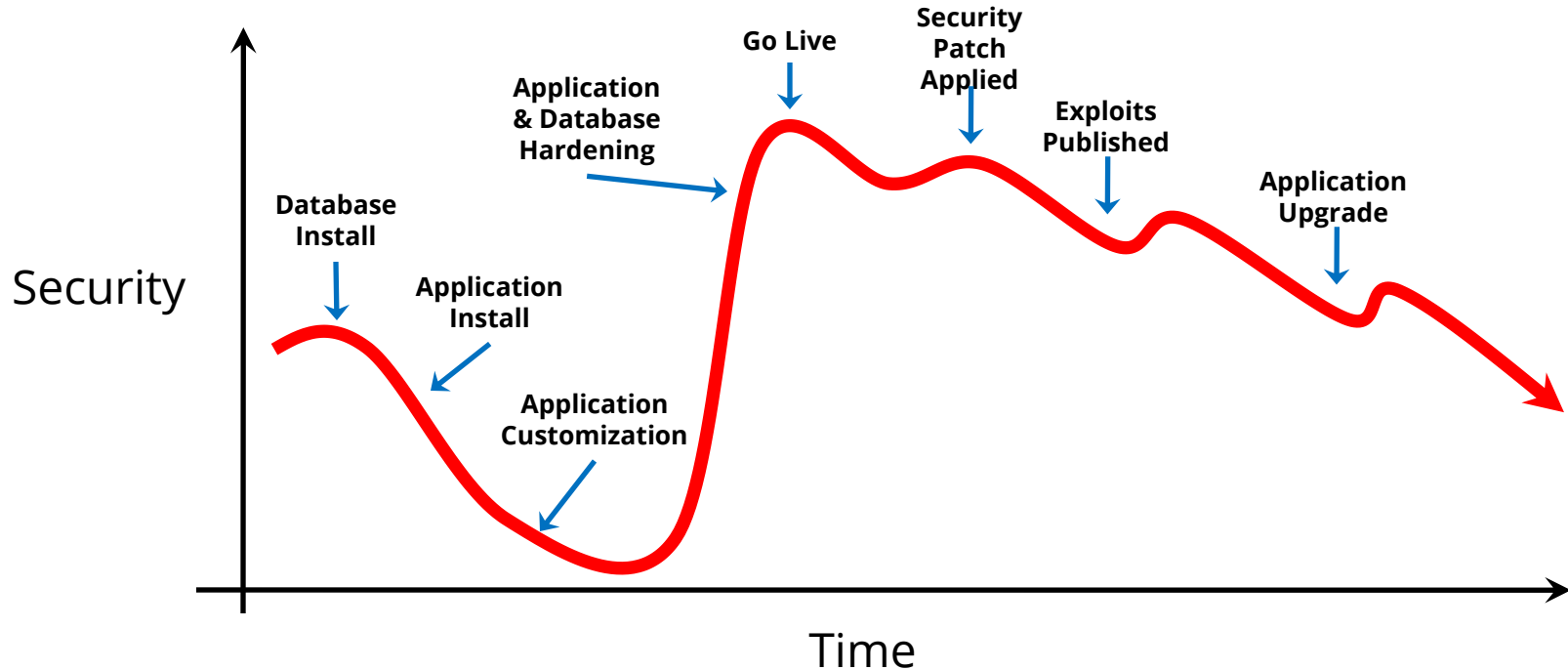
Myth: We **harden** all our Oracle databases at go-live – so we are secure today

#3

Reality: Oracle Database security decays over time and steps must be taken routinely to **validate security**

# Database Security Decay

Database and application security decays over time due to complexity, usage, application changes, upgrades, published security exploits, etc.



# Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
<b>DBSNMP</b>	<b>DBSNMP</b>	<b>99%</b>	<b>52%</b>
<b>OUTLN</b>	<b>OUTLN</b>	<b>98%</b>	<b>43%</b>
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
<b>CTXSYS</b>	<b>CTXSYS</b>	<b>54%</b>	<b>32%</b>

\* Sample of 120 production databases

# How to Check Database Passwords

- Use Oracle's **DBA\_USERS\_WITH\_DEFPWD**
  - Limited set of accounts
  - Single password for each account
- **Command line tools** (orabf, etc.)
  - Difficult to run – command line only
- **AppSentry**
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords



#4

Myth:

- (i) Your **IT Security team** is protecting Oracle Databases
- (ii) Your **DBAs** are protecting your Oracle Databases

#4

**Reality: Securing Oracle  
Databases is hard and requires  
a focused effort from a  
multidisciplinary team**

Oracle DBAs, application teams, IT Security, and Internal Audit must work together to make Oracle Databases secure and compliant

# Organizational Misalignment

Oracle Database technical security often not effectively handled in most organizations and **“falls between the cracks.”**

- ❖ **Database and Application Administrators**

Priority is performance, maintenance, and uptime

- ❖ **IT Security**

No understanding of Oracle Database security

- ❖ **Internal Audit**

Focused on application controls, segregation of duties

# What should you do?

- ❖ **Ensure the database is securely configured**

Work with DBAs to understand what has been done and not done

- ❖ **Understand how data is accessed and protected**

Learn what sensitive data is in each Oracle database, who accesses it, and what is done to protect it

- ❖ **Periodically validate security and configuration**

Security and configuration is changing over time

# Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-08 03.13.45.093449 PM	UPGRADE	10.2.0.3.0	Upgraded from 9.2.0.8.0
18-JAN-09 06.51.32.425375 AM	APPLY	10.2.0.4	CPUJan2009
09-APR-09 04.48.14.903718 PM	UPGRADE	10.2.0.4.0	Upgraded from 10.2.0.3.0
18-JUL-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-10 07.18.57.042620 AM	APPLY	10.2.0.4	CPUOct2010
30-OCT-10 06.42.55.108783 AM	UPGRADE	11.1.0.7.0	Upgraded from 10.2.0.4.0

**What CPU Level is this database patched to?**

- A. January 2007      B. January 2009      C. January 2010      D. October 2010**

# Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-08 03.13.45.093449 PM	UPGRADE	10.2.0.3.0	Upgraded from 9.2.0.8.0
18-JAN-09 06.51.32.425375 AM	APPLY	10.2.0.4	CPUJan2009
09-APR-09 04.48.14.903718 PM	UPGRADE	10.2.0.4.0	Upgraded from 10.2.0.3.0
18-JUL-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-10 07.18.57.042620 AM	APPLY	10.2.0.4	CPUOct2010
30-OCT-10 06.42.55.108783 AM	UPGRADE	11.1.0.7.0	Upgraded from 10.2.0.4.0

**What CPU Level is this database patched to?**

- A. January 2007   **B. January 2009**   C. January 2010   D. October 2010

#5

Myth: When installing or upgrading, the latest Oracle **Critical Patch Updates (CPU)** are already included

#5

**Reality: For the Oracle Database, only the latest CPU at time of release is included**

Almost always have to install the latest CPU when doing a fresh installation or upgrade to the database



# Critical Patch Updates Baselines

Database Version Upgrade Patch	Included CPU
10.2.0.4	April 2008
10.2.0.5	October 2010
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011
11.2.0.3	July 2011

**At time of release, usually the latest available CPU is included**

#6

Myth: **A database security tool** will address our database security issues

#6

Reality: **No silver bullet** exists to address all necessary aspects for database security

Significant security impact as Oracle EBS has a massive footprint

# Traditional Database Security Approaches

**The database security tool** is purchased to solve the database security problem.

- Database monitoring and auditing tools are only part of the solution
- Expensive and time consuming to implement
- Complex applications cause deployment problems

# Database Security Program Components

## Inventory

- Review existing database inventories
- Define scope of database discovery
- Perform hybrid database discovery

## Configuration

- Review existing database configuration standards
- Define database security and compliance requirements
- Develop measurable database security standards

## Access

- Define database access management definition
- Select and implement access solutions or policies for privileged and end-user accounts

## Auditing

- Development auditing requirements for DAM
- Define baseline auditing for all databases
- Define auditing for key applications and databases based on compliance and data

## Monitoring

- Development monitoring requirements for DAM
- Define and implement database IDS
- Define and implement log monitoring integration

## Vulnerability

- Development vulnerability assessment requirements for DAM
- Implement monitoring and compliance of configuration standard
- Implement periodic scanning

## Encryption

- Define encryption requirements
- Select and implement encryption solution for initial databases
- Develop on-going encryption implementation

### Outputs

- Database inventory
- Data inventory for key databases

- Database security and compliance requirements
- Database security standards

- Database access management
- Policies for database account management

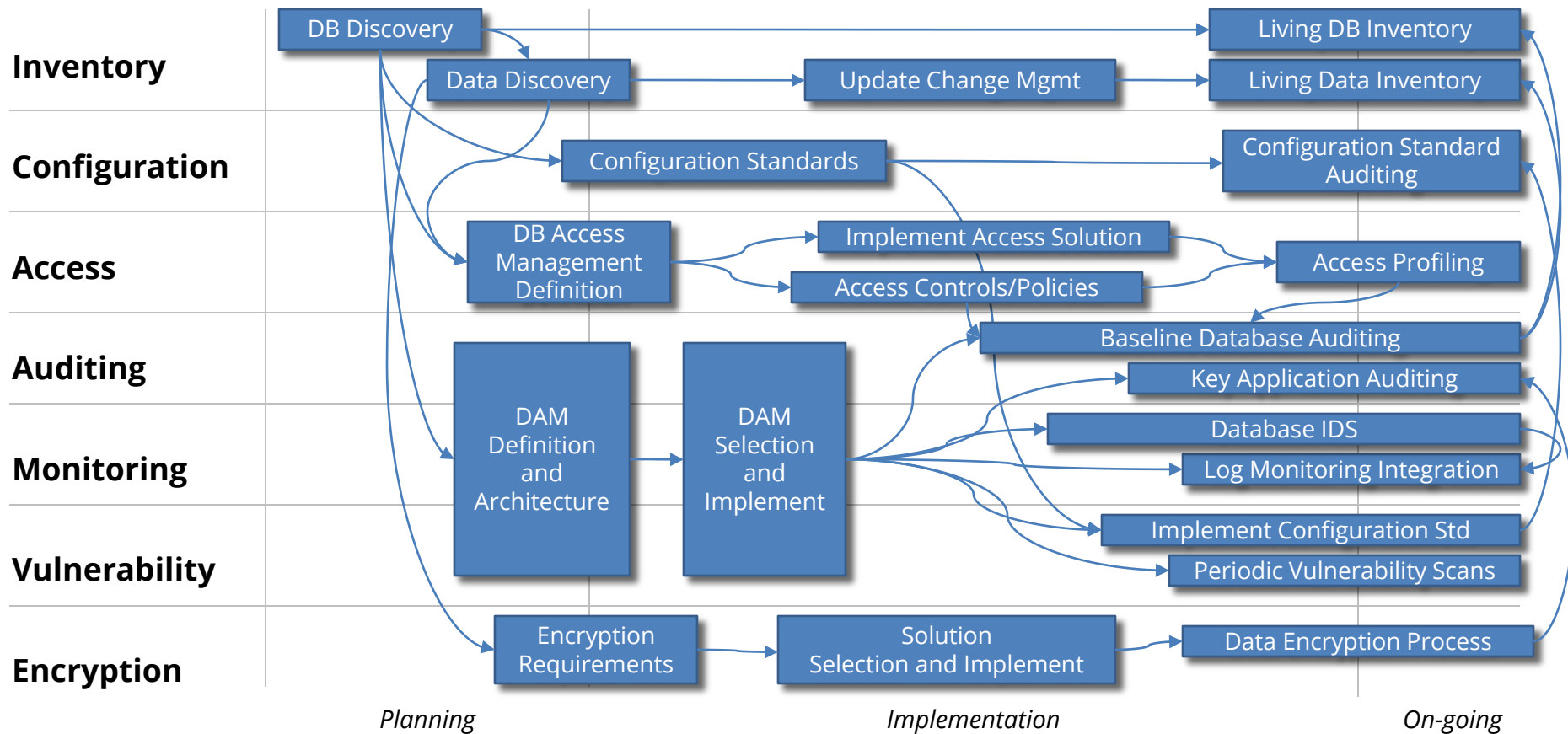
- Database auditing definition for (1) all databases and (2) key databases

- Database monitoring and alerting definition
- Log monitoring integration

- Rules for measuring compliance with database security standards

- Encryption requirements with policies
- Encryption implementation process

# Program Implementation



#7

Myth: Oracle Database  
**passwords** are safe and secure

#7

Reality: Oracle Database  
password hashes **can be**  
**brute forced**



# Brute Forcing Database Passwords

## A number of efficient password brute forcing programs exist for Oracle

- Speed is at least 1 million passwords per second for desktop/laptop
- Speed is around 100 million passwords per second for specialized hardware (FGPA/GPU)
- Only the username and hash are required
- Estimated time to brute force a password of x length –

<b>Length</b>	<b>Permutations</b>	<b>Time (desktop)</b>	<b>Time (GPU)</b>
1	26 (26)	0 seconds	0 seconds
2	1,040 (26 x 39)	0 seconds	0 seconds
3	40,586 (26 x 39 x 39)	0 seconds	0 seconds
4	1,582,880	1.5 seconds	0 seconds
5	61,732,346	2 minute	6 seconds
6	2,407,561,520	40 minutes	24 seconds
7	93,894,899,306	1 day	15 minutes
8	3,661,901,072,960	42 days	10 hours
9	142,814,141,845,466	1,600 days	16 days

# Oracle Database Passwords

- ❖ **Oracle Database password algorithm published**

Oracle 11g – hash changed to SHA-1 – old DES hash also stored

- ❖ **Hash is unique to the username, but common across all versions and platforms of the Oracle database**

SYSTEM/MANAGER is always D4DF7931AB130E37 in every database in the world

- ❖ **Database password hashes cloned to development**

Security and configuration is changing over time

#8

Myth: Oracle Database **audit data** is always accurate and reliable

#8

Reality: Most Oracle  
Database audit data fields  
can be spoofed

# Audit Trails Destinations and Values

Session Value	V\$SESSION View	SYS_CONTEXT Function	SYS.AUD\$ DBA_AUDIT_*	FGA_LOG\$ AUDIT_TRAIL	Audit Vault
DB User Name	✓	✓	✓	✓	✓
Schema Name	✓	✓			
OS User Name	✓	✓	✓	✓	✓
Machine	✓	✓	✓	✓	✓
Terminal	✓	✓	✓		✓
Program	✓				✓
IP Address		✓	✓		✓
Client Process ID	✓				
Module	✓	✓			
Action	✓	✓			
Client Info	✓	✓			✓
Client ID	✓	✓	✓	✓	✓

# Auditing Session Data

<b>Database User Name</b>	<b>OS User Name</b>	<b>Schema Name</b>
<b>IP Address</b>	<b>Machine/ User host</b>	<b>Terminal</b>
<b>Program</b>	<b>Client Process ID</b>	<b>Module</b>
<b>Action</b>	<b>Client Info</b>	<b>Client ID</b>

# Auditing Session Data – Spoofable

<b>Database User Name</b>	<del><b>OS User Name</b></del>	<del><b>Schema Name</b></del>
<b>IP Address</b>	<del><b>Machine/ User host</b></del>	<del><b>Terminal</b></del>
<del><b>Program</b></del>	<del><b>Client Process ID</b></del>	<del><b>Module</b></del>
<del><b>Action</b></del>	<del><b>Client Info</b></del>	<del><b>Client ID</b></del>

# Contact Information

**Stephen Kost**

Chief Technology Officer

Integrigy Corporation

web: [www.integrigy.com](http://www.integrigy.com)

e-mail: [info@integrigy.com](mailto:info@integrigy.com)

blog: [integrigy.com/oracle-security-blog](http://integrigy.com/oracle-security-blog)

youtube: [youtube.com/integrigy](http://youtube.com/integrigy)