Obtaining Value from Your Database Activity Monitoring (DAM) Solution

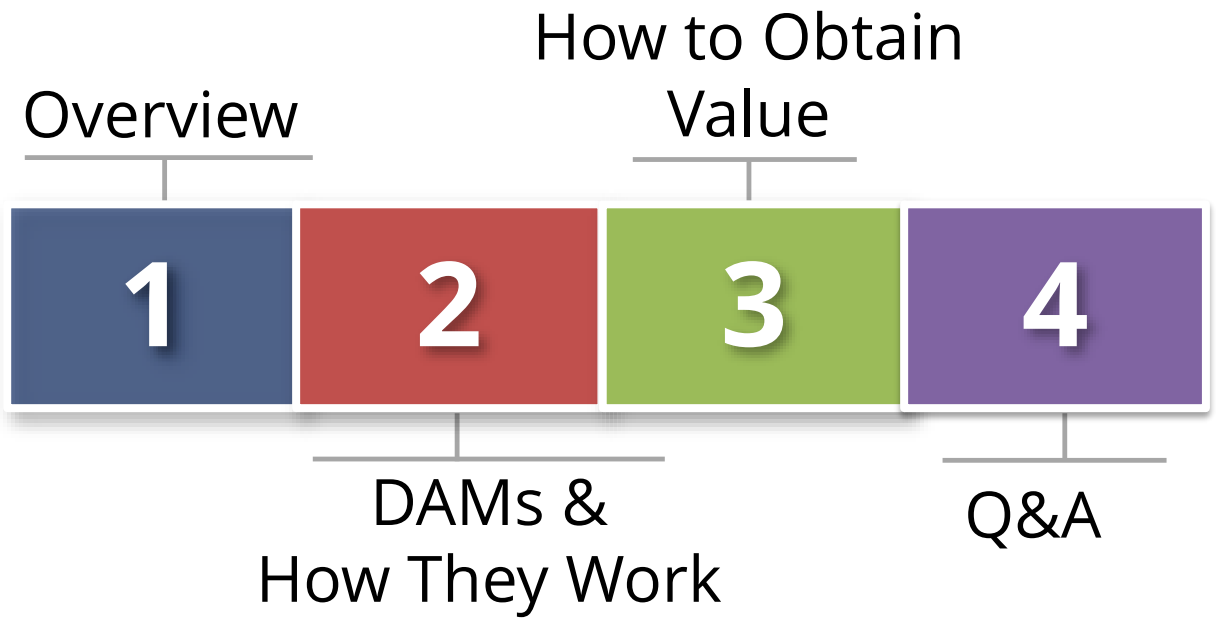
September 23, 2015

Mike Miller
Chief Security Officer
Integrigy Corporation

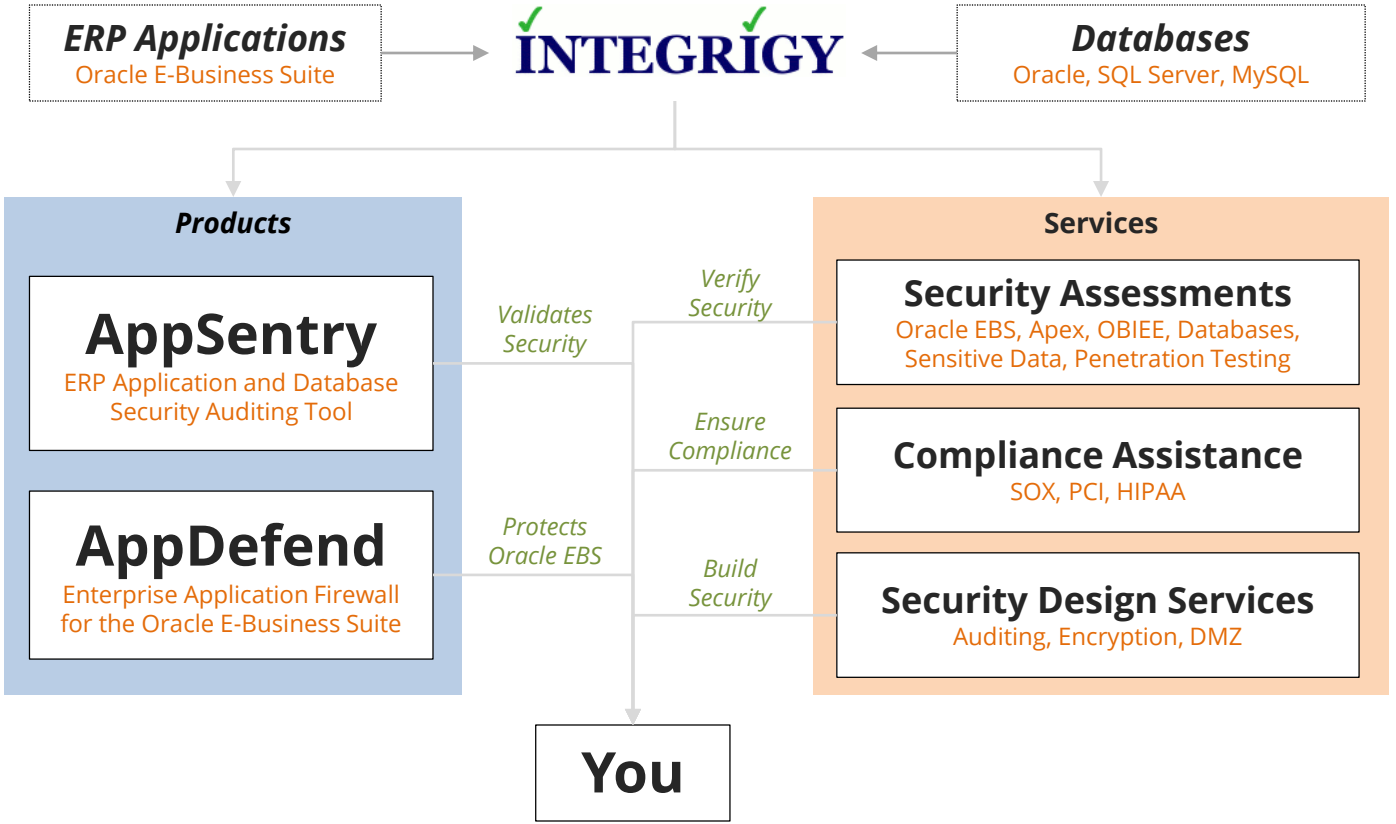
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

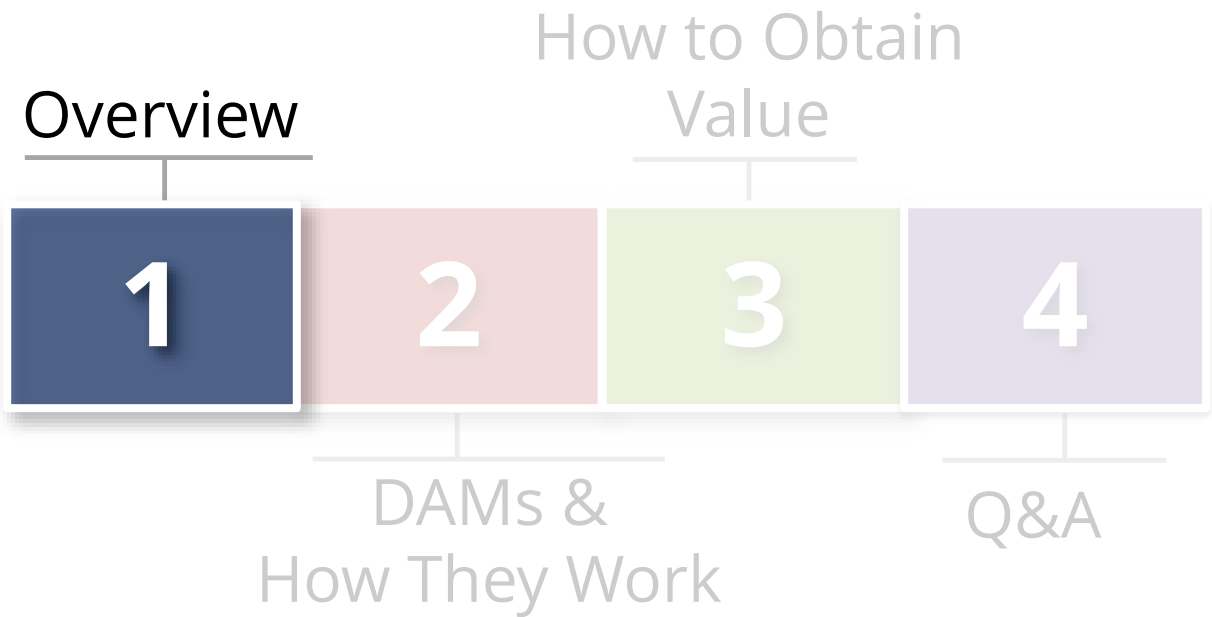
Agenda



About Integrigy



Agenda



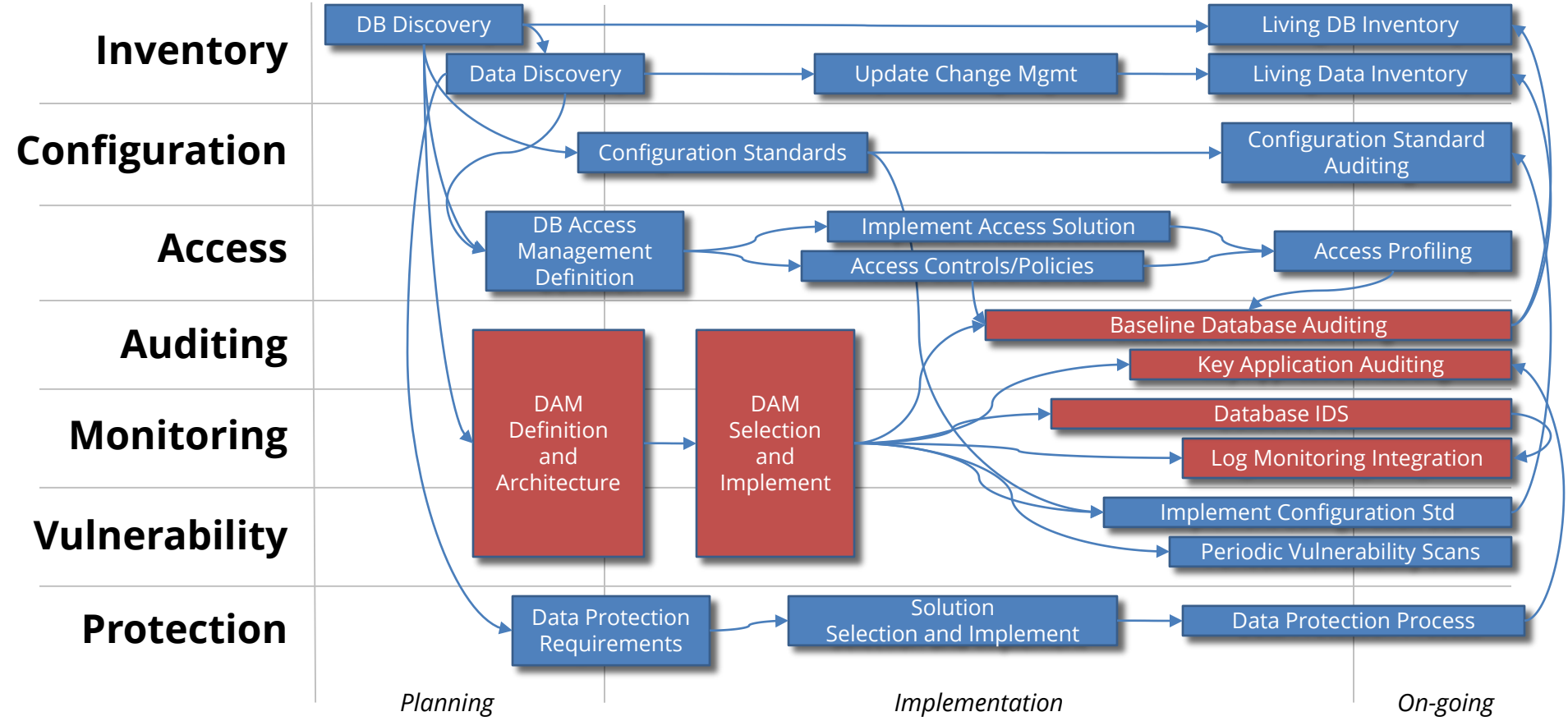
Security is a Process

- **Tools do not provide security, people do**
  - Tools only enable and automate
- **Security is not provided by any one product, upgrade, or patch**
  - Security provided by on-going lifecycle and configuration management
- **Database security is a process**
  - Monitoring and auditing are only one of several components required to secure a database

Database Security Program Components

Inventory	▪ An inventory of all databases and sensitive data locations ▪ Methods and processes to maintain the inventories
Configuration	▪ A measureable database security standard and baseline ▪ Periodic validation with compliance to the standard
Access	▪ Database access management policies, procedures, and tools ▪ Database access profiling and monitoring
Auditing	▪ Database auditing requirements, processes, and definitions ▪ Centralized auditing retention and reporting solution
Monitoring	▪ Database real-time security monitoring and intrusion detection ▪ Database monitoring definition and tools
Vulnerability	▪ Vulnerability assessment and management for databases ▪ Vulnerability remediation strategy and processes
Protection	▪ Sensitive data protection strategy – encryption, data masking, redaction, scrambling ▪ Data protection policies, procedures, and tools

Database Security Process



Database Activity Monitoring

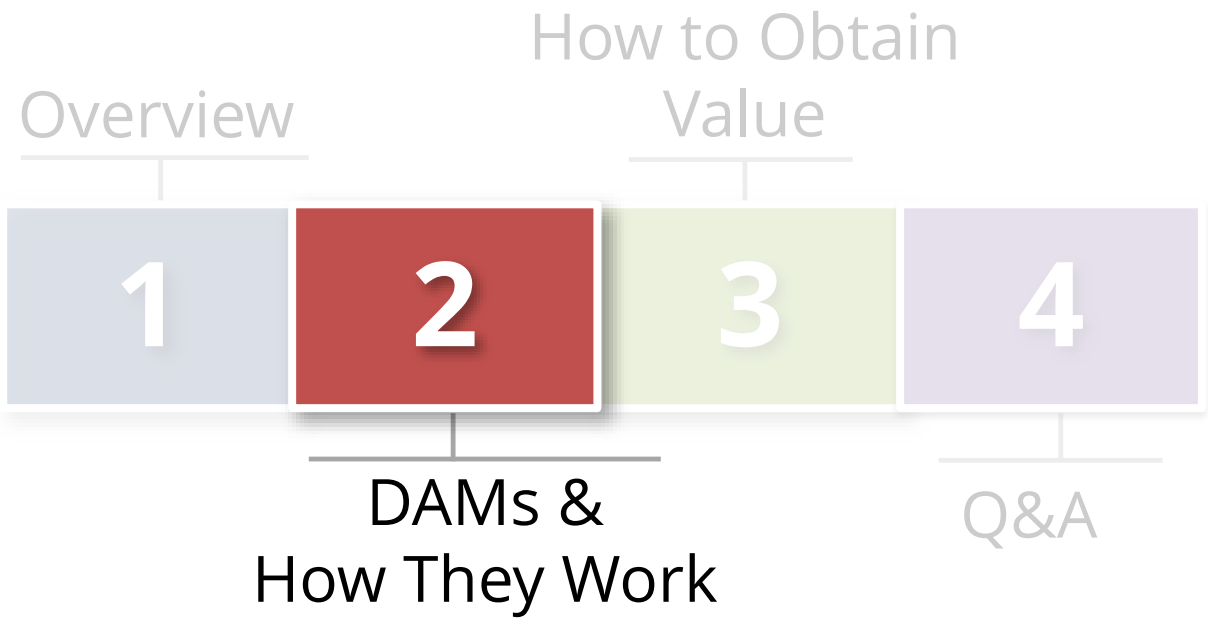
- **Auditing, monitoring, and alerting**
  - Related but separate disciplines
- **Defining requirements is difficult**
  - Technical, compliance, audit, and security
- **Need information as basis for action**
  - **Most organizations ignore or underutilize auditing**

Zero Value Database Activity Monitoring

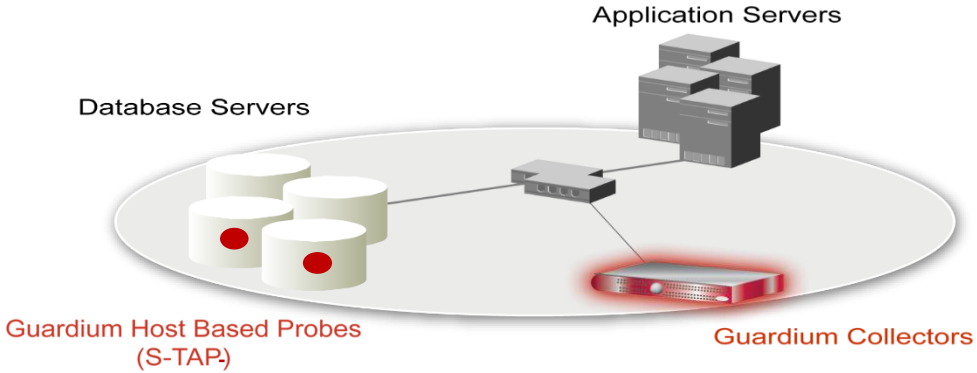
Database auditing and monitoring in most organizations is done simply for a **compliance checkbox**.

- **Not using auditing**
- **Auditing poorly defined**
- **No review of audit data**
- **No mapping of business requirements to auditing, alerts, or reports**
- **Audit data is not actionable**
- **Zero or limited value to the organization**

Agenda



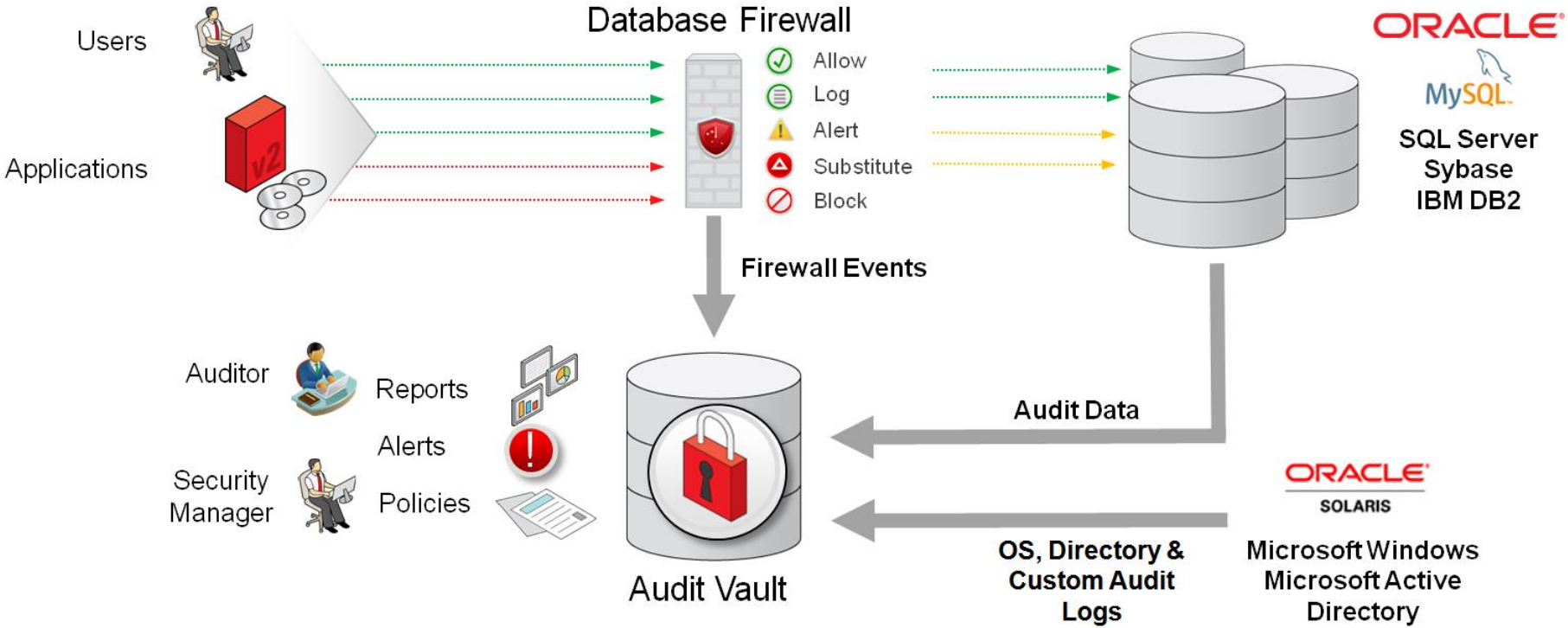
DAMs Provide Non-Invasive, Real-Time Database Security



- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS audit logs
- Minimal performance impact (2-3%)
- No DBMS or application changes

- Supports Separation of Duties
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

Oracle Audit Vault and Database Firewall



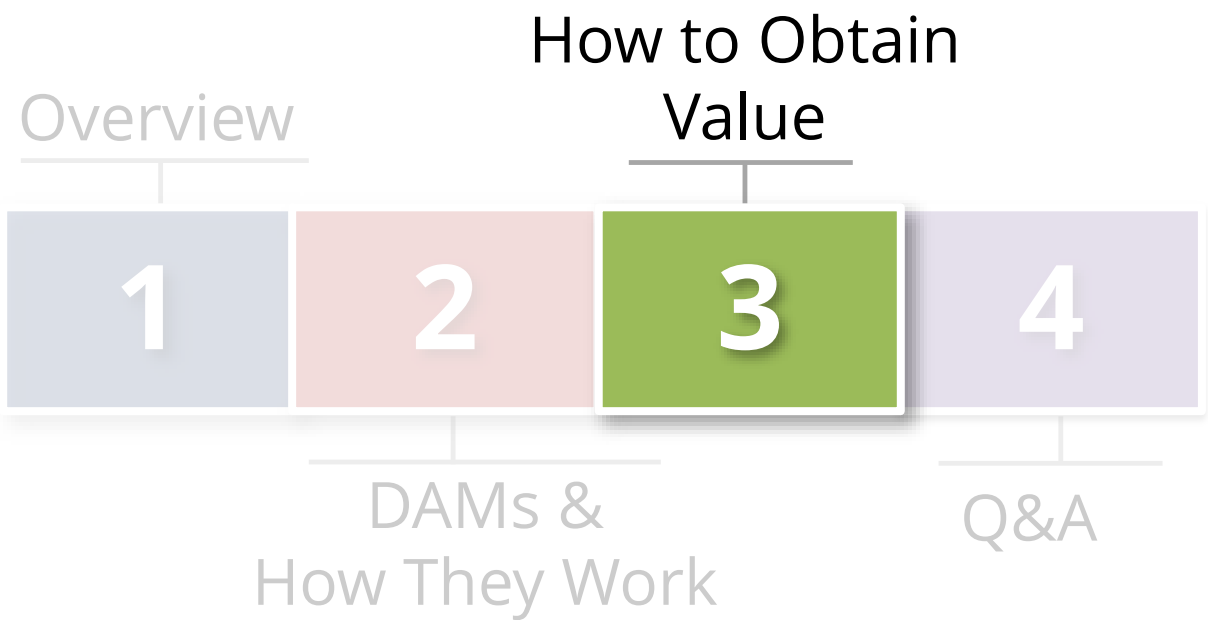
Key DAM Vendors

- **Imperva**
  - SecureSphere for Databases
- **IBM**
  - IBM Security Guardium
- **Oracle**
  - Audit Vault and Database Firewall (AVDF) (formerly Secerno)
- **McAfee**
  - Data Center Security for Databases (formerly Sentrigo)

DAM Advanced Features and Capabilities

Blocking	▪ Block incoming SQL statements based on policy
Masking	▪ Mask sensitive data being returned to client based on policy
Inventory	▪ Find databases on network and sensitive data within databases
Vulnerability Scanning	▪ Scan database for security vulnerabilities and misconfigurations
Configuration & Change Auditing	▪ Monitor configuration and tables for changes

Agenda



DAM Implementation Steps

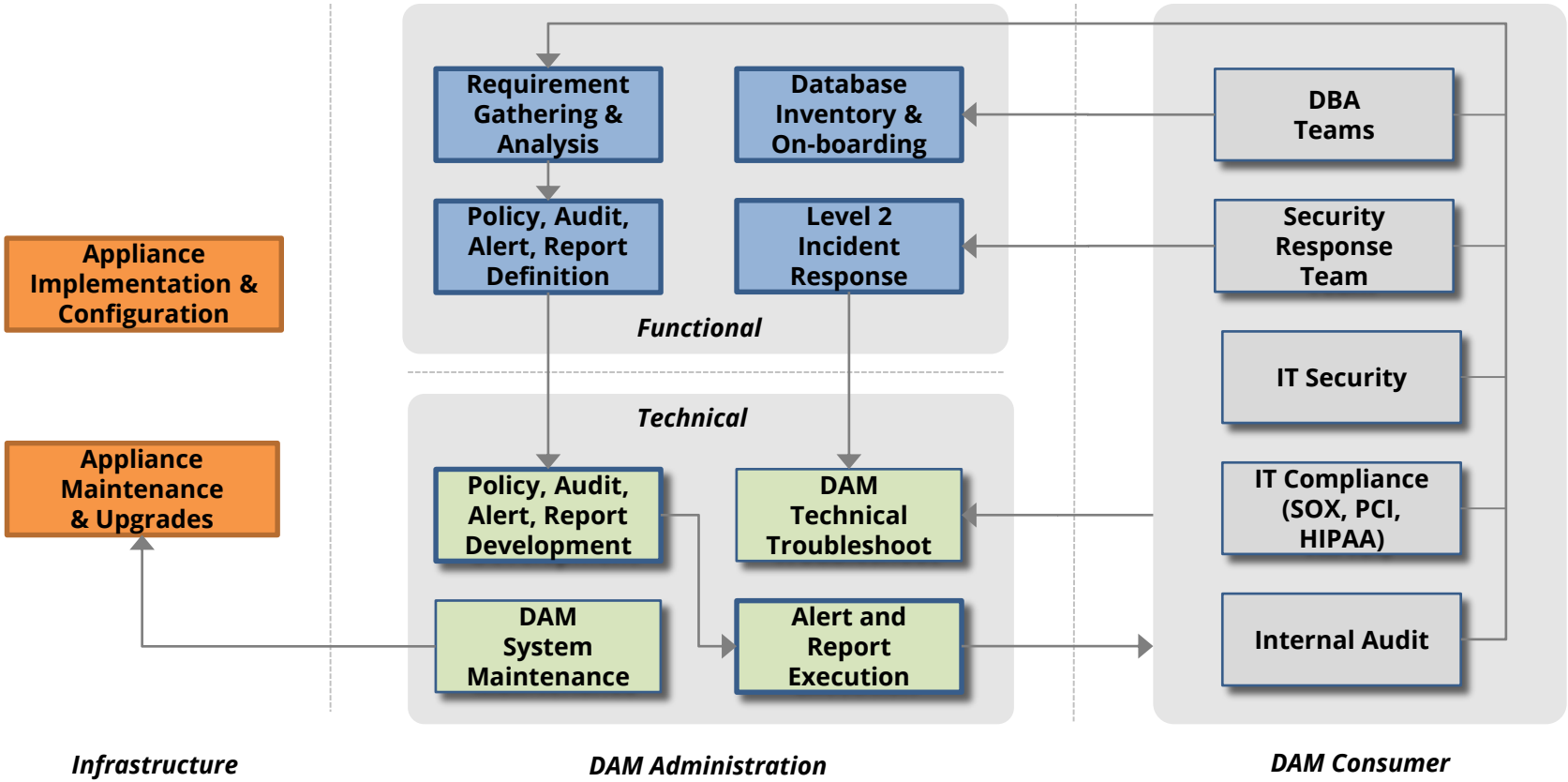
- **Planning**
  - Requirements definition
- **Pilot**
  - Phase 1 - Infrastructure
  - Phase 2 - Pilot & *Initial policy design*
- **Production**
  - Phase 3 - Agent rollout & *tune policies to reality*
  - Phase 4 - Go-Live
  - Phase 5 - Advanced DAM features
  - Phase 6 - Outlier detection & Bayesian learning

Planning – Decide Before You Do Anything

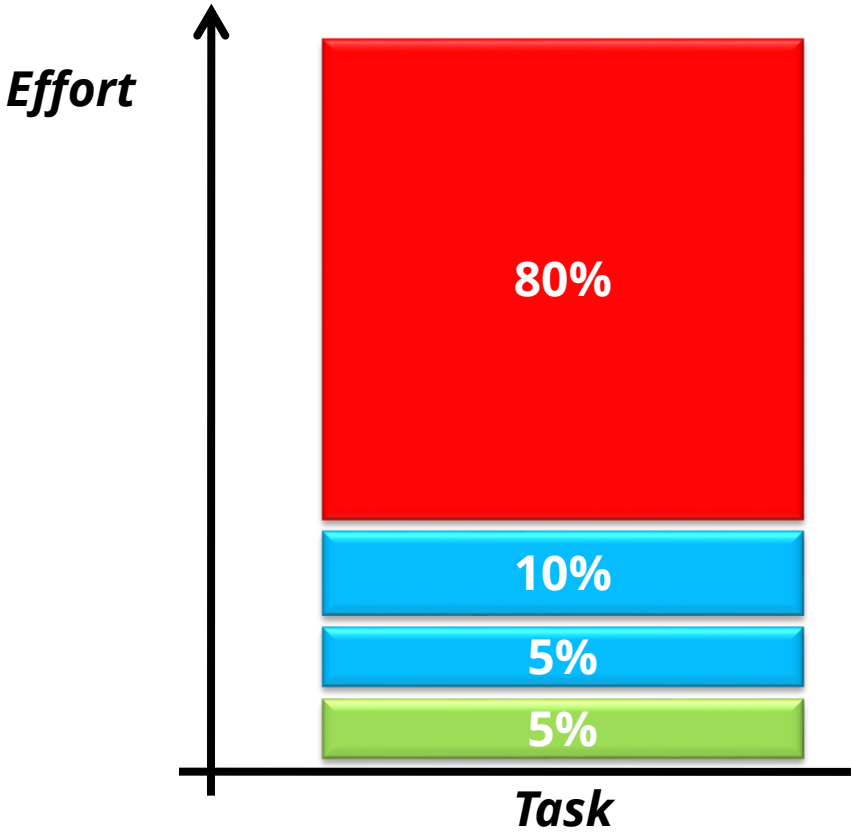
- **Who is going to own what?**
  - Support model
- **Who will be monitoring**
  - IT Security, DBA, Audit, or 3rd party?
    (e.g., who will decide a granted user privilege is legitimate?)
  - Security is a process – integrate into security fabric

Don't proceed until these two decisions are resolved!

Planning – Who Owns What? DAM Support Model



Long Term DAM Implementation Effort by Task



Monitoring, Alerting, Reporting, Reviewing

Archiving & Purging

Installation

Design

Pilot Phase 1 – Infrastructure

- **Deploy infrastructure**
  - Collectors, Central Managers, and Aggregators
- **Obtain inventory of all in-scope databases**
  - Ports, host name and IP, service names, install paths
- **Deploy agents to QA/test servers**
  - Include sampling of each platform and database vendor
  - Must be free to bounce databases and execute test SQL
  - Address performance fears – stress testing may be required
  - Create run books

Pilot Phase 2 – Pilot & Initial Policy Design

- **Focus on basics first**
  - Explore out-of-box policies & rules
    - Oracle, SQL-Server, Hadoop, Oracle E-Business, PeopleSoft, SAP
    - PCI, SOX, and HIPAA
  - Develop local reports to review data
  - No forwarding of alerts, blocking, masking, or encryption
  - Enable learning/Bayesian outlier detection

Pilot Phase 2 – Pilot & Initial Policy Design

- **Implement Integrigy Framework**
  - Systematic and focused policies for key security events
  - Out-of-box policies are too generic
  - Out-of-box policies capture way too much data and noise
  - Must be free to create test transactions
  - Suggest test scripts and data be used
  - Should test on all future platforms and database vendors

Create Value With Layered Design Approach

All Databases

Common Events

Database Events
- Database logins
- Database logoffs
- Failed database logins
- Database configuration changes

Security Events
- Create/Update/Delete User
- Grants and Revokes
- Security profile changes
- SQL Errors (defined list)

Anomalous and Intrusion Detection
- Defined anomalous events
- Known security vulnerabilities

DAM Events and Activity
- User logins and activity
- Security changes
- Infrastructure alerts

Compliance DBs

Compliance Events

SOX
- Database object changes
- Privileged account access by global list of accounts

PCI
- Requirement 10.2
- Access to card data in global list of tables
- Privileged account access by global list of accounts

GLBA
- Privileged account access by global list of accounts

HIPAA
- Privileged account access by global list of accounts
- Access to HIPAA data based on global list of tables

Per Database

Per Database Events (defined during database on-boarding)

Access to SHR/Confidential Data
- Tables and columns containing SHR/Confidential Data
- Select, Insert, Update, and/or Delete based on requirements

Privileged Account Access
- Definition of accounts per application or database
- Exceptions to monitoring based on location or type of access

Sample Alerts and Reports Design

Imperva Alerts and Reports — Last Update: 3/9/2010

Summary						Alert/Report			Compliance		
#	Group	Type 1. Audit 2. Security 3. Assessment	Requirement/Report/Alert 1. All alerts have corresponding report 2. All e-mail reports have ad hoc report	Description	Scope Apply to	Frequency	Format	Target	SOX Control	PCI-DSS 1.2.1	ArcSight Req
Security											
S1	Security	Security	Failed Database Login	All failed database logins	All	Real time	CEF	ArcSight	5.1	10.2.4	A2
S2	Security	Audit	Database Logins	All successful database logins	All	Real time	CEF	ArcSight	3.6	10.2.5	A1
S3	Security	Audit	Database Logoffs	All database logoffs	All	Real time	CEF	ArcSight	3.6	10.2.5	A1
S4	Security	Audit	Database Account Creation, Modification, Deletion	All CREATE, ALTER, DROP user and role statements	All	Real time	CEF	ArcSight	4.1	10.2.5	A3
S5	Security	Audit	Database Privileges Grant or Revoke	All GRANT and REVOKE statements	All	Real time	CEF	ArcSight	4.1	10.2.5	A4
S6	Security	Audit	Database Object Creation, Modification, Deletion	All CREATE, ALTER, and DROP statements	All	Real time	CEF	ArcSight	4.1	10.2.7	A5
S7	Security	Security	Stream Signature - Recommended Signatures Policy for General Applications	Imperva default signatures - false positives disabled	All	Real time	CEF	ArcSight	8.2	11.4	
S9	Security	Security	SQL Protocol Signatures - Recommended Signatures Policy for Database Applications	Imperva default signatures - false positives disabled	All	Real time	CEF	ArcSight		11.4	
S10	Security	Security	Oracle Protocol Validation - Oracle SQL Protocol Policy	Imperva default signature for alert session vulnerability	All	Real time	CEF	ArcSight		11.4	
S11	Security	Security	Database Connection Report	Report of all connections not in DB profile	All	Ad hoc	Imperva	Security	3.6	10.2.5	
S12	Security	Security	Direct Changes to Data Dictionary	Any external direct changes to data dictionary tables - if done, should only be done through patches from database server	All	Real time	CEF	ArcSight	4.1	11.4	
S13	Security	Security	Usage of Default Database Account	Usage of any default, not normally used DB account	All	Real time	CEF	ArcSight	3.7	2.1	
S14	Security	Assessment	Default Database Passwords	Check for accounts with default passwords	All	Weekly	CEF	ArcSight	2.1	2.1	
S15	Security	Assessment	Latest Oracle Critical Patch Update	Check for latest Oracle Critical Patch Update	All	Monthly	E mail/PDF	Security/DBA	2.2	6.1	
S16	Security	Security	Suspicious SQL Exceptions	Check for SQL exceptions that may be suspicious	All	Real time	CEF	ArcSight	8.9	11.4	
S17	Security	Audit	Audit of all PSECDBAUDIT activity	Audits the audit account	All	Ad hoc	Imperva	Imperva	10.1		

Production Rollout

- **Phase 3 – Begin to Digest Reality**
  - Agent deployment usually by platform
  - Expect agent deployment rate of 60 to 100 a week
  - Tune and adjust initial policies to reality
  - Dispel fears about performance impact
  - Design reports & dashboards
  - Keep alert relay off

Production Rollout

- **Phase 4 – Go Live**
  - Draft run books – focus on response matrix*
  - Enable alert relay
  - Size backup and archive to reality
  - Communicate to management that you are live

**Why implement if never going to use it*

Production Rollout

- **Phase 5 – Sensitive data and other**
  - Continued policy tuning
  - Log, mask and block sensitive data
  - Vulnerability scanning
- **Phase 6 – Learning / Bayesian outliers**
  - Each database may need 4 to 6 weeks of observation BEFORE results are shown
  - Models need to be trained (“who is going to play pac-man?”)
  - Include in your DAM procedures only well after initial implementation

Don’t Build Your DAM to be an Information Dam

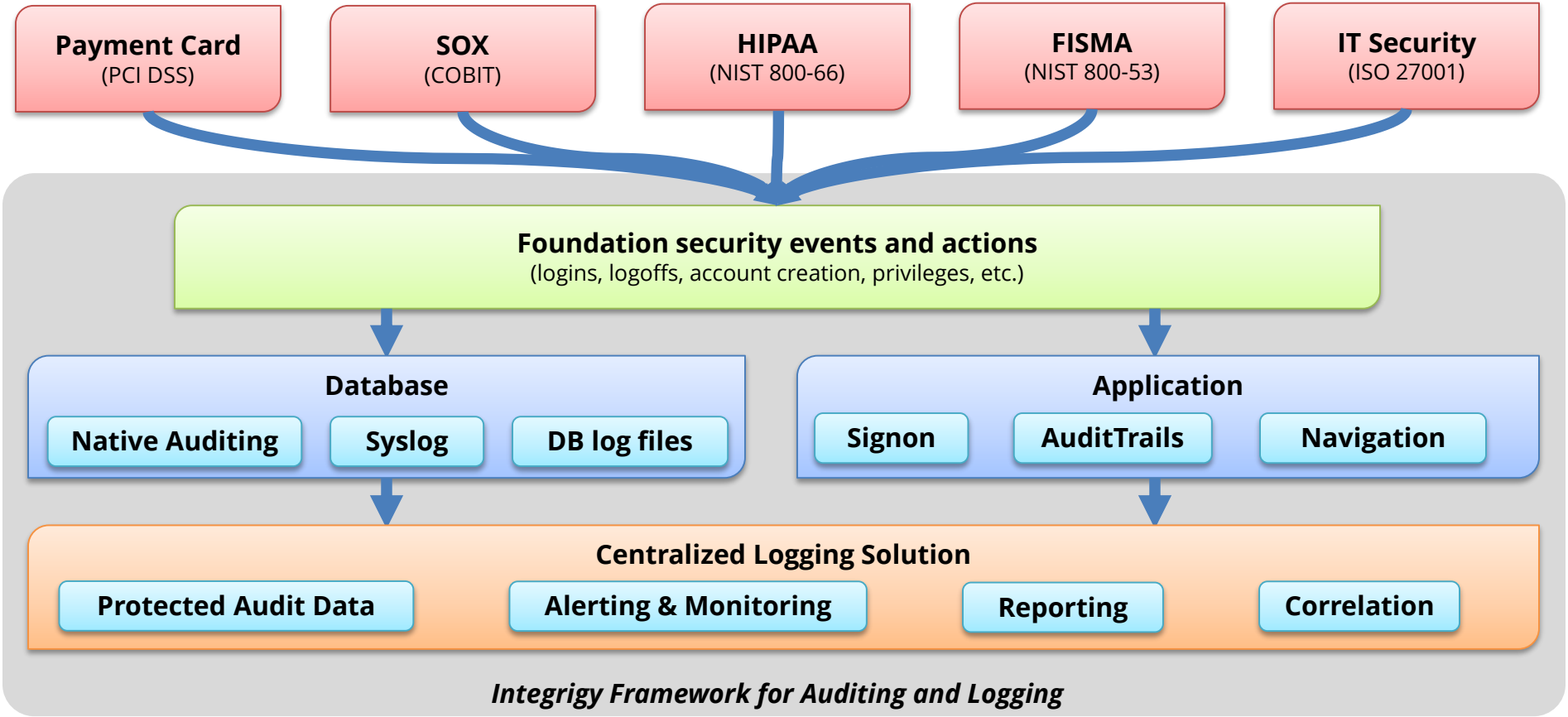
- **Goal of Database Activity Monitoring**
  - Transform activity into actionable information
  - Use as mitigating and detective controls
  - Harmony with overall database security program to proactively identify non-compliance
  - Solve compliance and security challenges – change ticket tracking and workflow

Why Do You Need an Auditing Framework?

- **Value is generated through auditing**
  - Need information as basis for action

- **Integrigy's Framework for Database Auditing is a Methodology**
  - Defines what should be logged and audited
  - Defines what should be alerted and reported on
  - Starting point and direction for database logging

Integrigy Framework for Database Auditing



Foundation Security Events and Actions

The foundation of the framework is a set of key security events and actions derived from and mapped to compliance and security requirements that are critical for all organizations.

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**

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

Change Ticket Tracking – Create User Example

DAM solutions are able to capture 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 ticket_1234
CREATE USER scott
```

2

DAM Solution

USER_ID	BOB
OS_USER	DOMAIN/BOB
ACTION	CREATE USER
OBJECT	Scott
TICKET	1234
PROGRAM	SQL Developer

User Creation **Authorized** Ticket # = yes

User Creation **Unauthorized** Ticket # = no

3

Auditor Workflow Process

User Creation **Authorized**

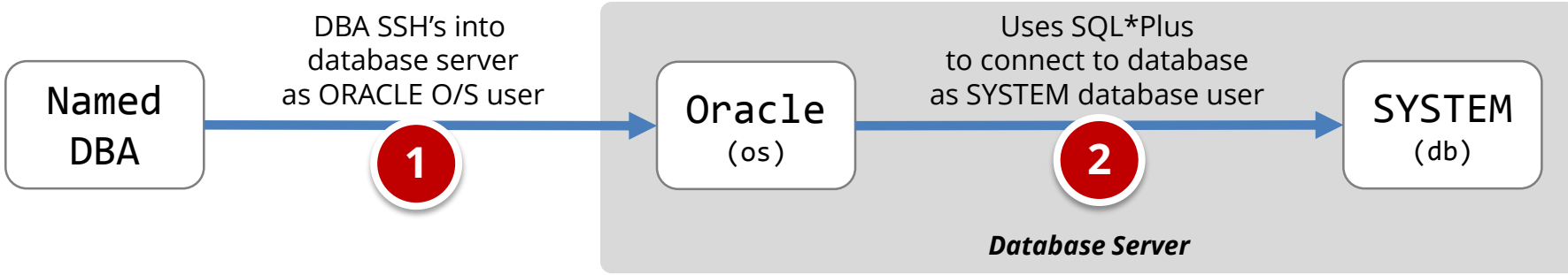
Auditor samples authorized users by reviewing tickets.

User Creation **Unauthorized**

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

Generic User Tracking – Problem

Database audit trail often only captures generic user information at the operating system and database level. Not able to identify the named person performing the SQL.

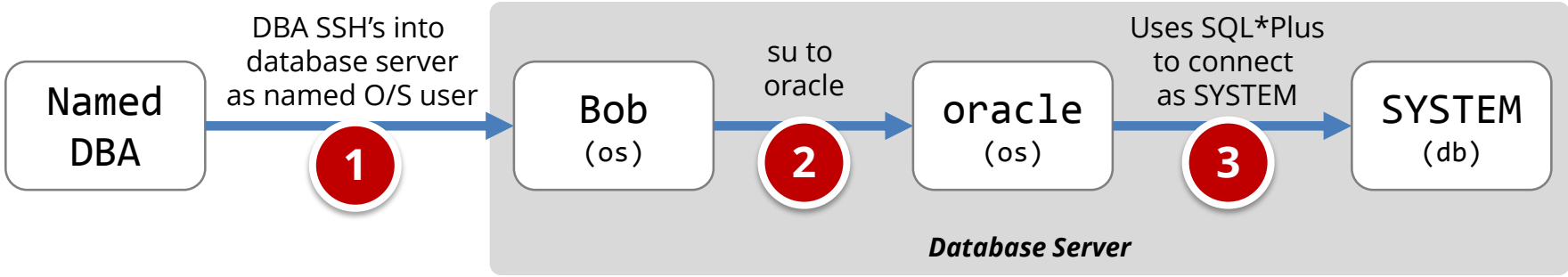


Sample Native Database Auditing and DAM Solution Audit Record

DB User	OS User	Machine	Program	SQL
SYSTEM	oracle	DBSERVER1	SQL*Plus	CREATE USER

Generic User Tracking – Solution

DAM solutions are able to capture OS user information on a DB server across user transition events such as **su** or **sudo**. The user "chain" can be included in the audit trail.

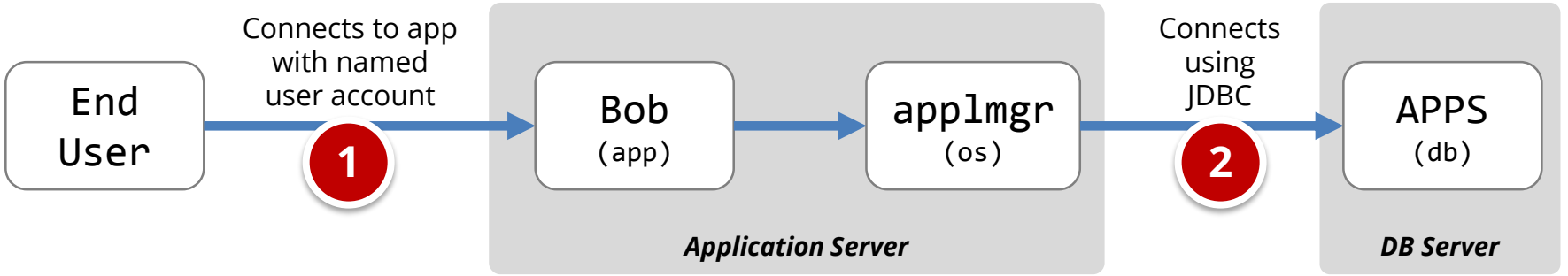


DAM Solution Audit Record with "User Tracking" Feature

DB User	OS User	Machine	Program	SQL	OS Chain
SYSTEM	oracle	DBSERVER1	SQL*Plus	CREATE USER	bob -> oracle

Application End User Tracking – Solution

DAM solutions are able capture web application end-users and correlate the application end-user to SQL statements. Support depends on the application.



DAM Solution Audit Record with "Application User" Feature Enabled

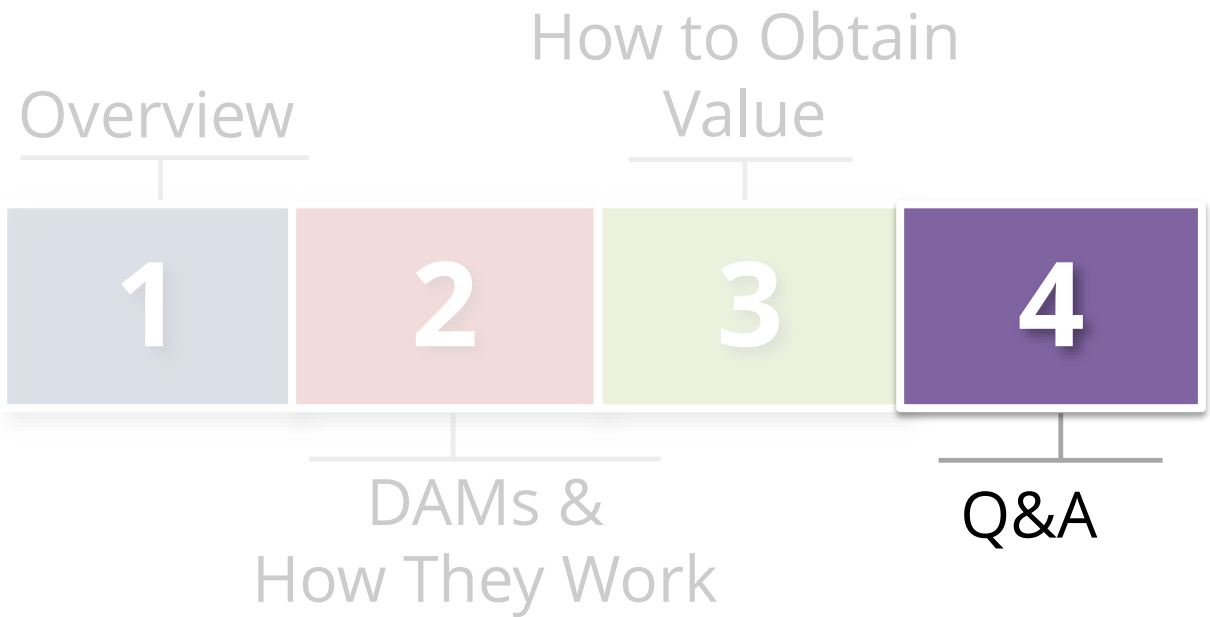
DB User	OS User	Machine	Program	SQL	Application User
APPS	applmgr	APPSERVER1	JDBC	select * from credit_cards	bob

This example is Oracle E-Business Suite R12

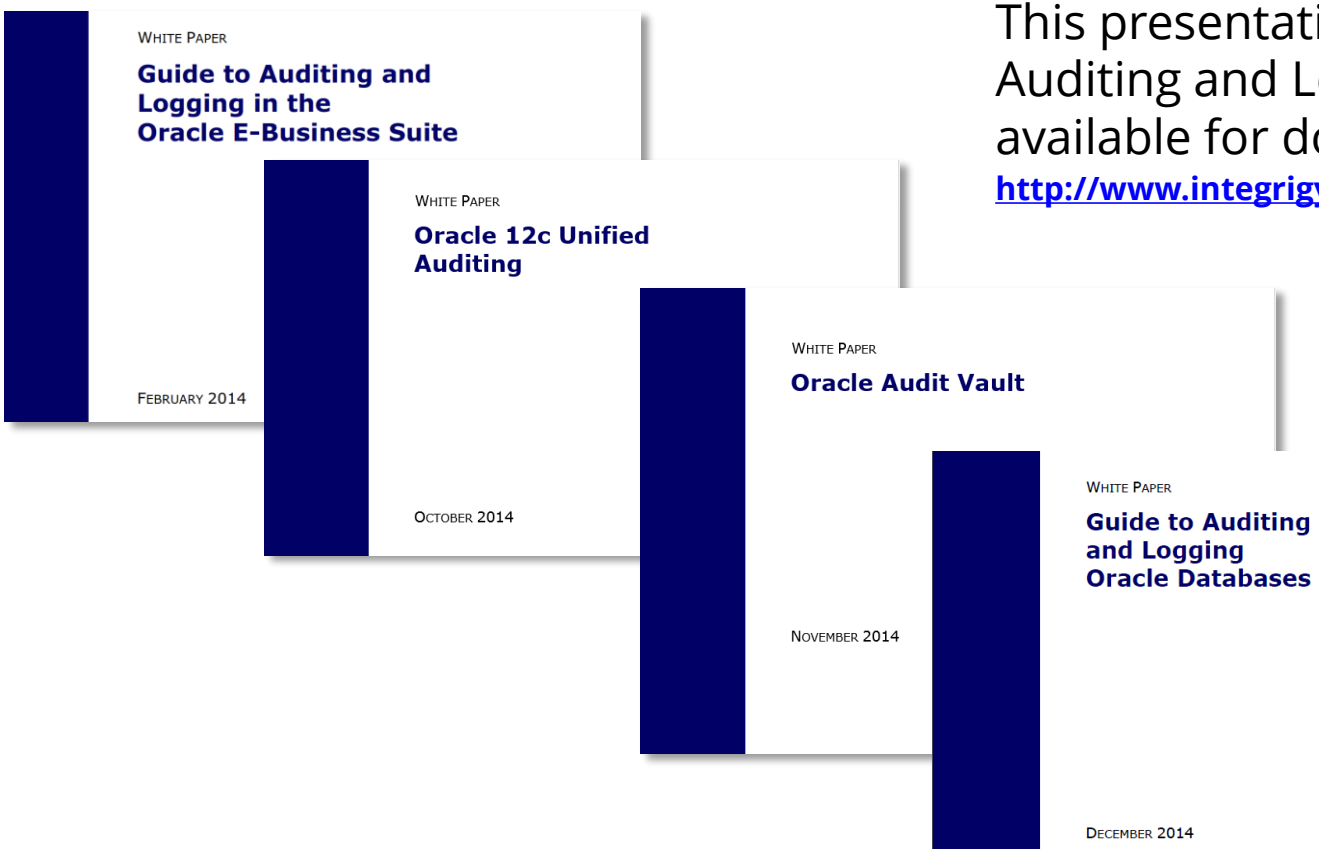
Oracle Client Identifier Examined

Application	Example of how used
Oracle 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's 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)')

Agenda



Integrigy Oracle Whitepapers



This presentation is based on our Auditing and Logging whitepapers available for download at – http://www.integrigy.com/security-resources

Contact Information

Michael Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

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

youtube: **youtube.com/integrigy**