



Hacking an Oracle Database and How to Prevent It

February 12, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications

Oracle E-Business Suite,
PeopleSoft, Oracle Retail

**INTEGRIGY**

Databases

Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL

Products

AppSentry

ERP Application and Database
Security Auditing Tool

*Validates
Security*

AppDefend

Enterprise Application Firewall
for the Oracle E-Business Suite
and Oracle 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*

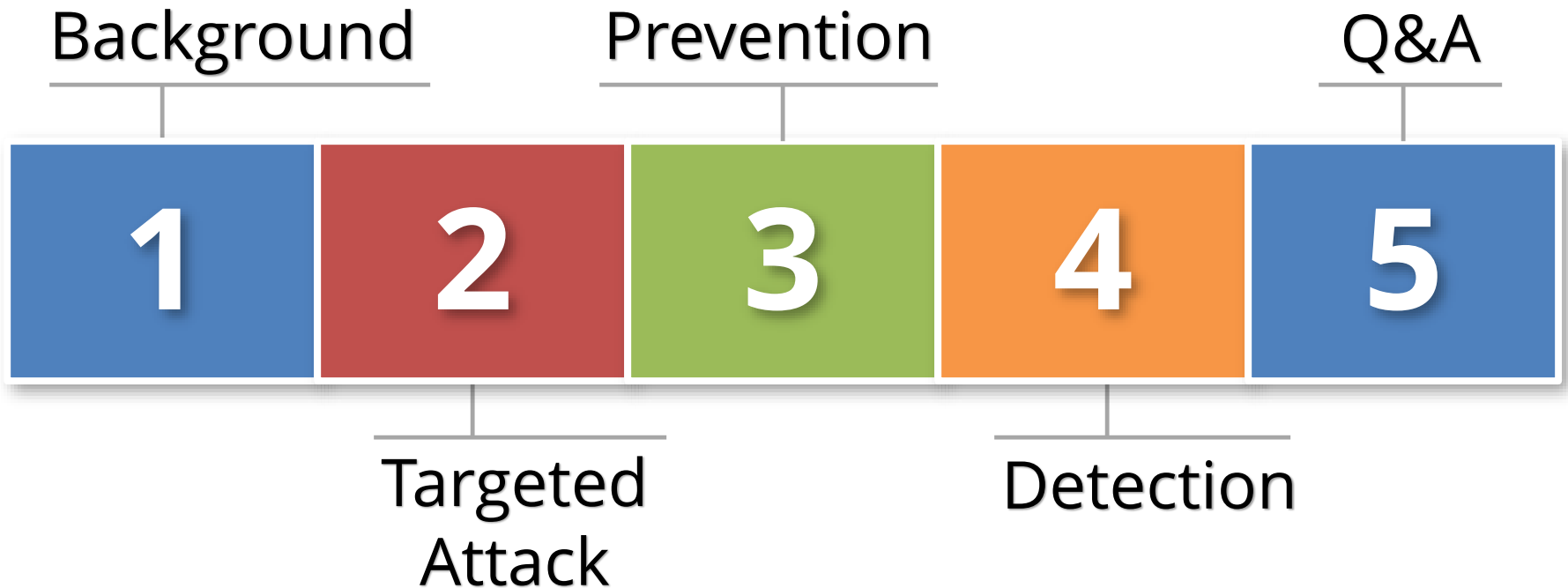
Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

Agenda



Agenda



Targeted Attack

Targeted Attack

Advanced Persistent Threat (APT)

State Sponsored

Anonymous, LulzSec, Legion of Doom, ...

Bitcoin/Monero Mining

Sensitive Data in Databases

| | |
|--|---|
| <p><i>Credit Card Fraud</i></p> <p>Credit Card Data</p> | <ul style="list-style-type: none">▪ Credit Card Number<ul style="list-style-type: none">▪ <i>Primary Account Number (PAN)</i>▪ CVV/CV2/CID<ul style="list-style-type: none">▪ <i>3 digits on the back for Visa/MC</i>▪ <i>4 digits on the front for AMEX</i>▪ Magnetic Stripe Data (very rare) |
| <p><i>Identify Theft/Tax Fraud</i></p> <p>Personally Identifiable Information (PII)</p> | <ul style="list-style-type: none">▪ First and last name▪ Date of Birth▪ Plus one of the following:<ul style="list-style-type: none">▪ Social security number▪ Bank account number▪ Financial account number▪ Driver license or state ID number |
| <p><i>Health Insurance Fraud</i></p> <p>Health Information</p> | <ul style="list-style-type: none">▪ First and last name▪ Plus one of the following (Protected Health Information)<ul style="list-style-type: none">▪ “the past, present, or future physical or mental health, or condition of an individual”▪ “provision of health care to an individual”▪ “payment for the provision of health care to an individual” |

**Last three years, the
health care industry
accounted for 42.5%
of all breaches**

- Identity Theft Resource Center

What is your data worth? Identify Theft

| | | |
|---------------------|---|---|
| \$1 - \$5 | <ul style="list-style-type: none">▪ First and last name▪ Social Security number | Tax information (e.g., 1099) |
| \$20 - \$40 | <ul style="list-style-type: none">▪ First and last name▪ Social Security number▪ Current address▪ Date of birth | Health care Human Resources |
| \$30 - \$100 | <ul style="list-style-type: none">▪ First and last name▪ Social Security number▪ Current address▪ Date of birth▪ Bank account number or credit card number▪ Salary | Payroll |

- **2017 – 1.1 million potentially fraudulent tax returns**
- **2017 – IRS paid \$4.4 billion in fraudulent tax refunds**
- **3,000 IRS employees dedicated to tax Fraud**

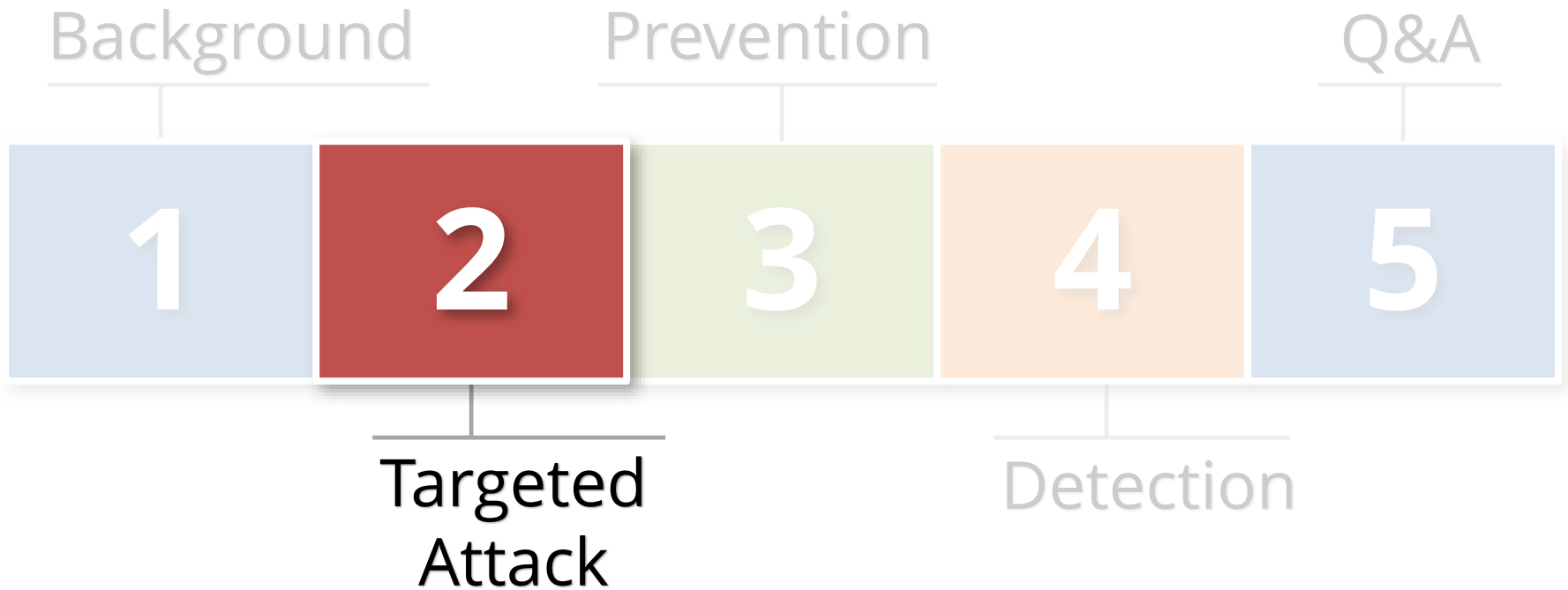
- General Accounting Office (GAO) Report

Database Valuation

Calculate the black market value of the data contained in your database to help evaluate risk.

| <i>Data Type</i> | <i>Formula</i> |
|--------------------------------|---|
| Credit Cards | (number of unique, unexpired cards) * \$10 |
| Social Security Numbers | (number of unique SSN + Name + DoB) * \$20 or (number of unique SSN + Bank) * \$50 |

Agenda



Anatomy of the Targeted Attack

| | | |
|----------|---------------------------------|--|
| 1 | Point of Entry | Breach the perimeter network through a network compromise, phishing attack, or social engineering. |
| 2 | Persistence | Once inside, establish a “beach-head” and maintain the compromise over time (days, months, years). |
| 3 | Lateral Movement | Expand the compromise to more devices and systems. |
| 4 | Asset and Data Discovery | <p>The Targeted Attack has already identified “data of interest” and will be searching for it.</p> <p><i>How to do this without detection?</i></p> |
| 5 | Data Exfiltration | <p>Once the “data of interest” has been gathered, it must be transferred externally without being detected.</p> <p><i>How do you quietly steal gigabytes or terabytes of data?</i></p> |

Asset and Data Discovery Techniques

| | |
|----------------|--|
| Passive | <ul style="list-style-type: none">▪ Search internal knowledge repositories for architecture diagrams, design documents, code repositories, etc.▪ Find TNSNAMES.ORA files |
| Active | <ul style="list-style-type: none">▪ Compromise DBA credentials through phishing or social engineering attacks▪ Install malware on DBA machines and steal credentials, such as saved in SQL Developer▪ Use Nmap to scan internal network for Oracle Databases on default port 1521 – very noisy |

Demo – Search Engine (Internal)

- Findings tnsnames.ora files using internal search engines
- www.google.com
- `search: tnsnames filetype:ora`

Demo – Source Code Repositories

Obtaining passwords from internal source code repositories

www.github.com

search: "alter user" "identified by"

<http://www.github.com>

Note: To search all code repositories, but be signed into Github with free account.

Decrypt SQL Developer passwords

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

Use extension in SQL Developer

Demo – Network Scanning – Find Databases

If the attacker can't find databases through other means, then the old fashioned way by scanning the network.

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
```

Demo – Determine the SID if Unknown

To connect to a database need IP address/hostname, TNS port number, and SID/Service Name.

Using Nmap to brute force SID

www.nmap.com

```
nmap -p 1521 -v --script oracle-sid-brute 192.168.56.10
```

Note: To search all code repositories, but be signed into Github with free account.

Next Step – Login into Database

| Database Account | Default Password | Exists in Database % | Default Password % |
|------------------|-------------------|----------------------|--------------------|
| SYS | CHANGE_ON_INSTALL | 100% | 3% |
| SYSTEM | MANAGER | 100% | 4% |
| DBSNMP | DBSNMP | 99% | 52% |
| OUTLN | OUTLN | 98% | 43% |
| 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% |
| CTXSYS | CTXSYS | 54% | 32% |

* Sample of 120 production databases – mostly production ERP databases such as SAP, Oracle EBS, and PeopleSoft

Demo – 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
```

Demo – Able to Connect and Access USER\$

**Brute forcing Oracle Database
Passwords**

Integrigy internal tool

google: oracle password cracker

free tools: woraauthbf, orabf

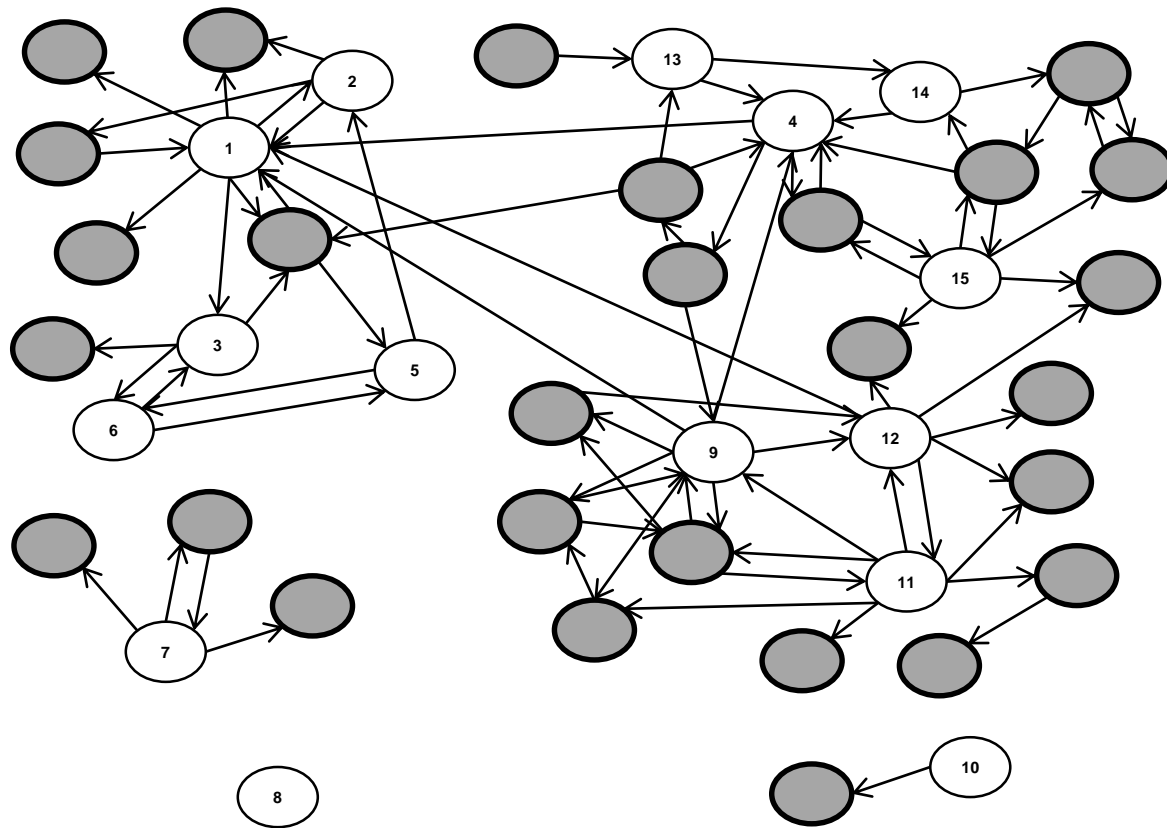
Final Step – Privilege Escalation

Last step is to escalate privileges by exploiting an unpatched vulnerability. Applying Critical Patch Updates provided no protection until this point. Database hardening and configuration are as important.

The compromised database account privileges and the skill and creativity of the attacker matter most for this last step.

google: oracle database privilege escalation

Lateral Movement After Database Compromise



Overview

- Organization with about 150 production Oracle Databases
- Assessed 15 key SOX and PCI compliance Oracle databases
- Reviewed database links for connectivity and appropriateness

Conclusion

- Compromised 28 other databases just through database links.

Agenda



Integrigy #1 Security Recommendation

- **Limit direct database access whenever possible**
 - Much harder to hack database if an attacker can not connect to it
 - Would have to use another avenue such as a web application or reporting tool (e.g., OBIEE)
- **Use firewalls in front of data center, network ACLs, TNS invited nodes, Oracle Connection Manager, Oracle Database Firewall, etc.**
 - DBAs should use bastion hosts to manage databases

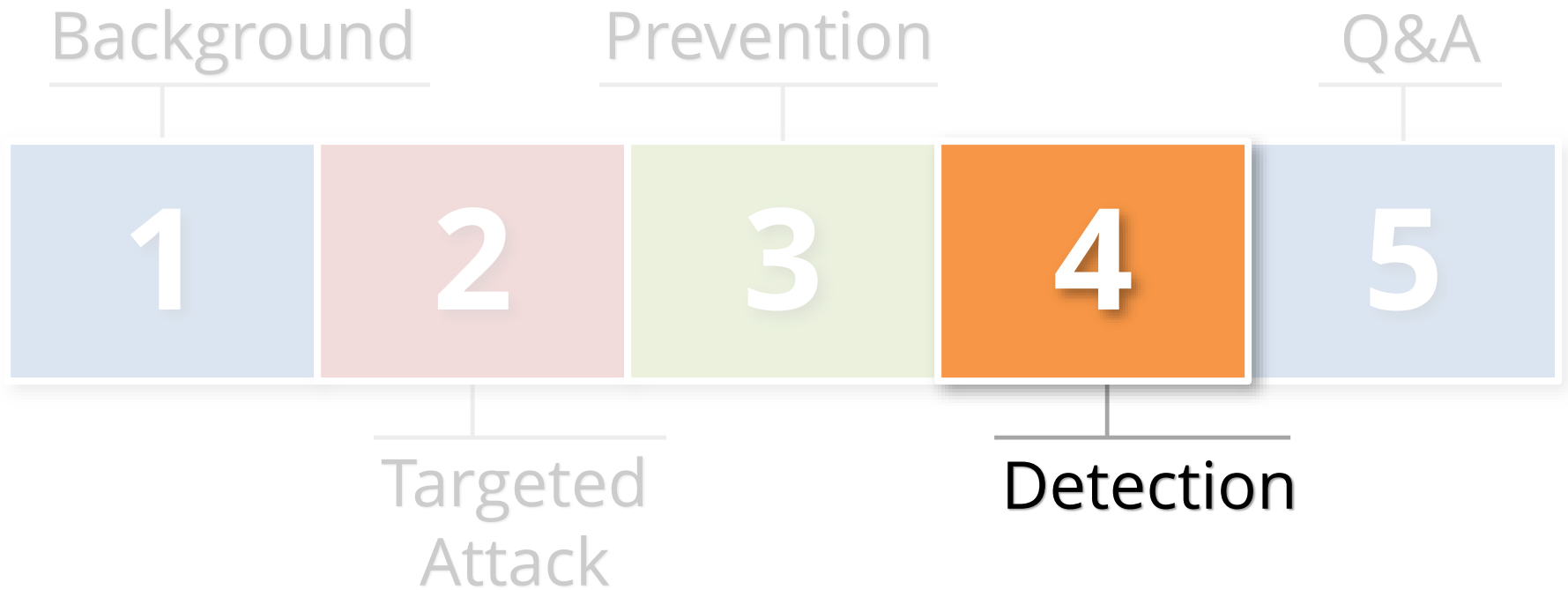
Database Security Preventative Controls

- **Apply Oracle Critical Patch Updates on a regular basis on all databases**
 - Reduce risk of compromise and escalation of privileges
- **Check for default and weak passwords constantly**
 - Use multiple tools to check passwords
 - Install database profiles to enforce strong passwords
- **Harden database configurations**
 - Validate configurations on regular basis

Routinely Check for Default 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

Agenda



Auditing Design

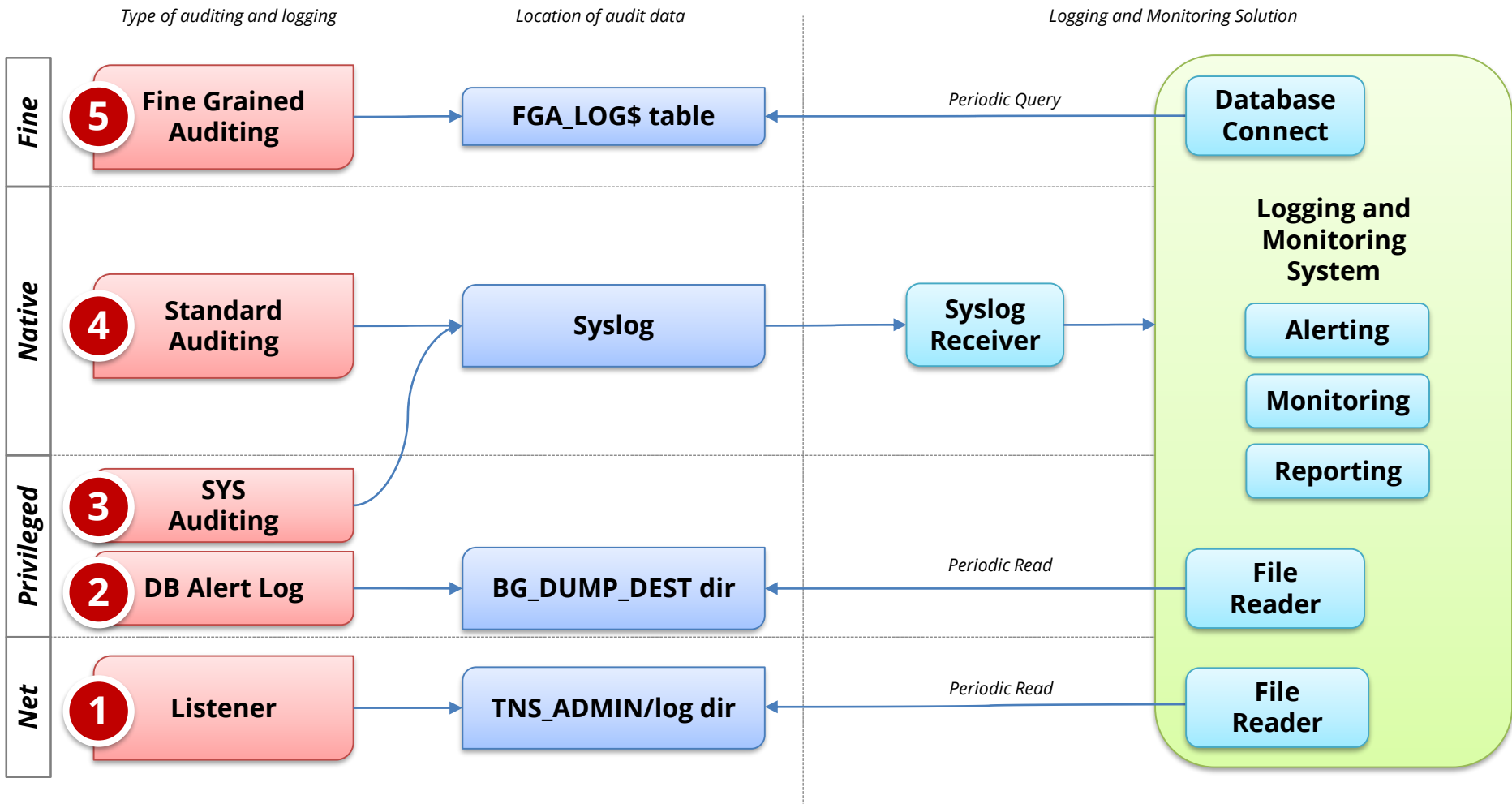
Use Integrigy Database Auditing and Logging Framework as starting point!

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

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 |

Traditional Database Auditing (pre 12c, 12c Mixed Mode)



Agenda



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