APPLICATION SECURITY, INC.

Securing Databases With an SCAP Compatible Toolset

Josh Shaul – Director, Systems Engineering
Application Security, Inc.

Agenda

- Corporate Background
- The Database Security Challenge
- SCAP for the Database

Corporate Background

Deloitte. 2006 Technology Fast 50 New York Rising Star

RED HERRING 100 WINNER N. AMERICA

06 AO100 Stanford Summit

SQL Server Central.com Readers' Choice Award 2004 Winner

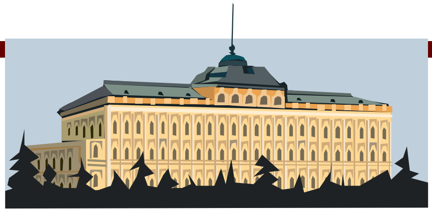
SECURE ENTERPRISE TESTER'S CHOICE

WINNER 2006 BEST OF INTEROP Network Computing

- Database security software company
- Headquartered in NY
  - Offices: U.S., U.K., France and Belgium
- Industry-leading Database Security & Auditing solution
  - Most awarded database security solution on the market
  - Solution of choice for auditors and security consultants
  - Complete Database Security
    - Discovery, vulnerability assessment, activity monitoring, auditing
  - Common Criteria in process
- Industry-leading customer base
  - **900+ customers**
- Top-tier investors and partners
  - Visa (financial), Paladin (national security)…..
- Strategic Relationships:
  - Security Technology Vendors – McAfee, ArcSight, etc.

VISA ORACLE Microsoft IBM SYBASE

Sample Government Customers



DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

U.S. DEPARTMENT OF HOMELAND SECURITY Homeland Security

DEPARTMENT OF THE NAVY UNITED STATES OF AMERICA

U.S. AIR FORCE

U.S.ARMY

SRA INTERNATIONAL, INC.

U.S. DEPARTMENT OF THE INTERIOR BUREAU OF LAND MANAGEMENT

U.S. DEPARTMENT OF THE INTERIOR MARCH 3, 1849

UNITED STATES POSTAL SERVICE®

NATIONAL PARK SERVICE

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

GSA U.S. General Services Administratio

U.S. Department of Education

Promoting educational excellence for all Americans.

DEPARTMENT OF JUSTICE QUI PRO DOMINA JUSTITIA SEQUITUR

SOCIAL SECURITY USA ADMINISTRATION

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

EDS

CACI EVER VIGILANT

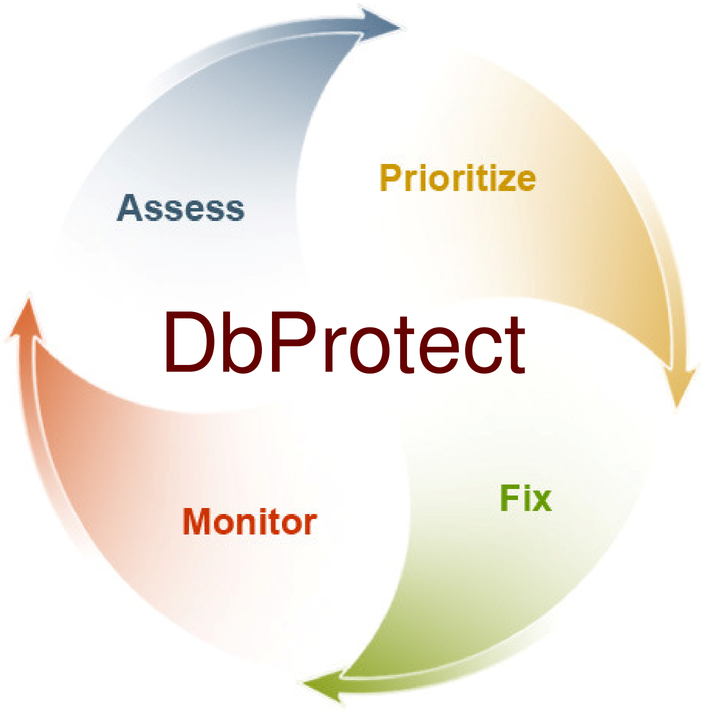
ERNST & YOUNG Quality In Everything We Do

PRICEWATERHOUSECOOPERS

KPMG

Deloitte.

Database Security Best Practices



1. Discovery
2. Vulnerability assessment and prioritization
3. Remediation
4. Residual vulnerability mapping
5. Monitoring policy deployment
   - Patch-gap policies
   - Privileged user monitoring policies
   - User and behavior policies
6. Report customization and publishing
7. ASAP update scheduling and policy tuning
8. Integration: SIM/SEM etc.

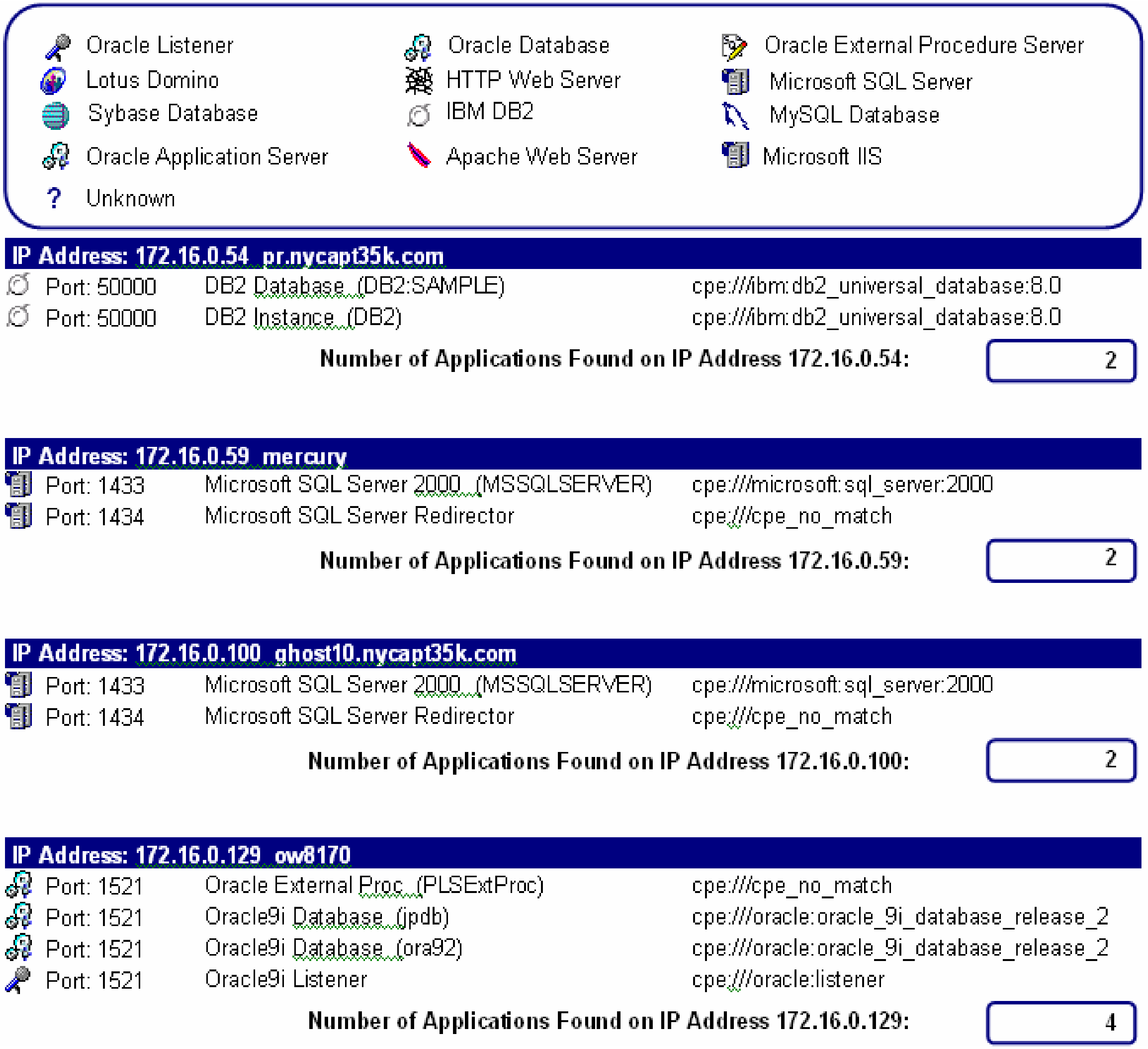
SCAP Components – Database Readiness

- **CVE**: In good shape. Many database vulnerabilities listed, more being added.
- **CPE**: Looking good with v2, high-level database platforms are covered.
- **CCE**: Currently no elements defined for database configurations.
- **CVSS**: Ready. Oracle using CVSS today to score all new vulnerabilities.
- **XCCDF**: Open Framework, can be used to describe database scan policies.
- **OVAL**: Not ready to implement database checks yet

Application Security – Getting Involved

- Working to become SCAP compatible in 2007.
  - Focus on CVE, CPE, and CCE Infrastructure
  - Follow up with CVSS and XCCDF
- Driving SCAP to the database
  - Engaged with MITRE on entering new CVEs
  - Joined CCE WG
  - Examining implementing the first Database Scanning Policy in XCCDF
  - Working with Oracle and other database vendors to assign CVSS scores to new vulnerabilities

SCAP Report Example – Database Inventory Report



Oracle Listener	Oracle Database	Oracle External Procedure Server
Lotus Domino	HTTP Web Server	Microsoft SQL Server
Sybase Database	IBM DB2	MySQL Database
Oracle Application Server	Apache Web Server	Microsoft IIS
? Unknown		

IP Address: 172.16.0.54 pr.nycapt35k.com

Port: 50000	DB2 Database (DB2:SAMPLE)	cpe://ibm:db2_universal_database:8.0
Port: 50000	DB2 Instance (DB2)	cpe://ibm:db2_universal_database:8.0

Number of Applications Found on IP Address 172.16.0.54: 2

IP Address: 172.16.0.59 mercury

Port: 1433	Microsoft SQL Server 2000 (MSSQLSERVER)	cpe:///microsoft:sql_server:2000
Port: 1434	Microsoft SQL Server Redirector	cpe:///cpe_no_match

Number of Applications Found on IP Address 172.16.0.59: 2

IP Address: 172.16.0.100 ghost10.nycapt35k.com

Port: 1433	Microsoft SQL Server 2000 (MSSQLSERVER)	cpe:///microsoft:sql_server:2000
Port: 1434	Microsoft SQL Server Redirector	cpe:///cpe_no_match

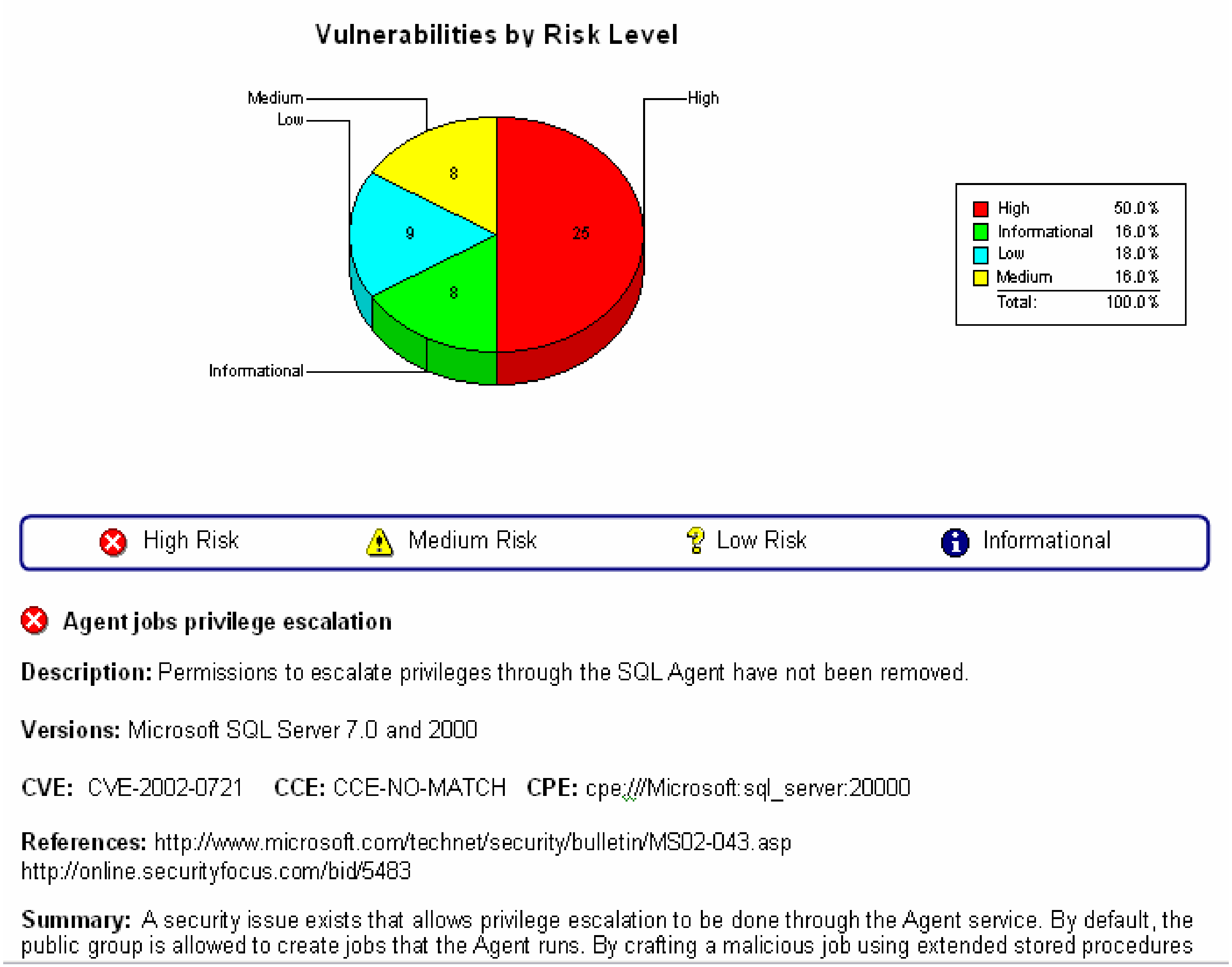
Number of Applications Found on IP Address 172.16.0.100: 2

IP Address: 172.16.0.129 ow8170

Port: 1521	Oracle External Proc (PLSExtProc)	cpe:///cpe_no_match
Port: 1521	Oracle9i Database (jpdb)	cpe:///oracle:oracle_9i_database_release_2
Port: 1521	Oracle9i Database (ora92)	cpe:///oracle:oracle_9i_database_release_2
Port: 1521	Oracle9i Listener	cpe:///oracle:listener

Number of Applications Found on IP Address 172.16.0.129: 4

SCAP Report Example – Database Vulnerability Report



🟥	High	50.0 %
🟩	Informational	16.0 %
🟦	Low	18.0 %
🟨	Medium	16.0 %
	Total:	100.0 %

⊗ High Risk ⚠ Medium Risk ? Low Risk ℹ Informational

⊗ Agent jobs privilege escalation

Description: Permissions to escalate privileges through the SQL Agent have not been removed.

Versions: Microsoft SQL Server 7.0 and 2000

CVE: CVE-2002-0721 **CCE:** CCE-NO-MATCH **CPE:** cpe:///Microsoft:sql_server:20000

References: http://www.microsoft.com/technet/security/bulletin/MS02-043.asp
http://online.securityfocus.com/bid/5483

Summary: A security issue exists that allows privilege escalation to be done through the Agent service. By default, the public group is allowed to create jobs that the Agent runs. By crafting a malicious job using extended stored procedures