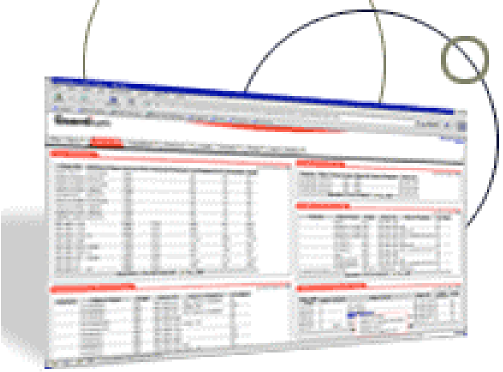


Beyond intrusion detection: The next frontier in safeguarding corporate assets

Ron Bennatan
CTO, Guardium Inc.

NYOUG Tech Journal
Sept, 2004

Databases - “The Crown Jewels”

- Databases are rich in content and functionality
  - Critical, sensitive and high integrity data is moving from applications to RDBMSs
  - Concentrate data and, therefore, risk
- Web Applications provide a high volume portal for database intrusions
  - Recent surveys indicate rising losses from database attacks (e.g. Evans Data)
- Generally weak implementation of data access/usage controls
  - Application bugs, non-current patches, lack of visibility and adherence to best practices
- Regulatory compliance enforcement - legal / regulatory pressure to protect information is increasing (eg. GLB, HIPPA, SOX)

Database Threats Are Increasing

- Pressures to deliver cause more holes
- Web applications (a portal to the database) are open to potentially every hacker in the world
- Hacker chatter about databases is rising
- Hacker conventions and workshops are focusing more on databases
- Surveys of database managers (e.g. Evans Data) indicate rising losses from database attacks
- Increasing class action lawsuits around privacy breaches

- So..
  - Database security is really important – and coming to the forefront
- But..
  - Doesn't a database have adequate security and audit capabilities?

Yes.. And No..

- Strategy/philosophy – defense-in-depth
- Databases have bugs
- Database security model is limited
  - Implicitly needs to trust the application – which really cannot be trusted
  - Based primarily of login name and user/role permissions
    - Not on programs, network info, ..
    - Cannot do baselining etc.
  - Dependent on its own configuration – cannot do introspection
- Auditing features exist but are sometimes hard to use
  - Taxes the CPU and IO
  - Not dynamic (will talk about it later)
  - Cannot support segregation of duties
- Application vulnerabilities become data access vulnerabilities

Example 1: App server conf files

```
<data-source name=”ORCL”
 class=”oracle.jdbc.pool.OracleConnectionPoolDataSource”
 username=”scott”
 password=”tiger”
 url=”jdbc:oracle:thin:@orclsrv”
 connection-driver=”oracle.jdbc.driver.OracleDriver”
 location=”jdbc/orcl” xa-location=”jdbc/xa/orcl”
 ejb-location=”jdbc/orcl”
 connection-retry-interval=”5”
 max-connect-attempts=”5”
 inactivity-timeout=”900”
 max-connections=”100”
 min-connections=”50”
 wait-timeout=”900”/>
```

```
weblogic.jdbc.connectionPool.eng=\
  url=jdbc:weblogic:oracle,\
  driver=weblogic.jdbc.oci.Driver,\
  loginDelaySecs=2,\
  initialCapacity=50,\
  capacityIncrement=10,\
  maxCapacity=100,\
  props=user=scott,password=tiger,server=ORCL
```

```
<ias-resources>
 <resource>
  <jndi-name>jdbc/ORCL</jndi-name>
  <jdbc>
   <database>ORCL</database>
   <datasource>ORCL</datasource>
   <username>scott</username>
   <password>tiger</password>
   <driver-type>ORACLE_OCI</driver-type>
  </jdbc>
 </resource>
</ias-resources>
```

Example 2 – SQL Injection & modification

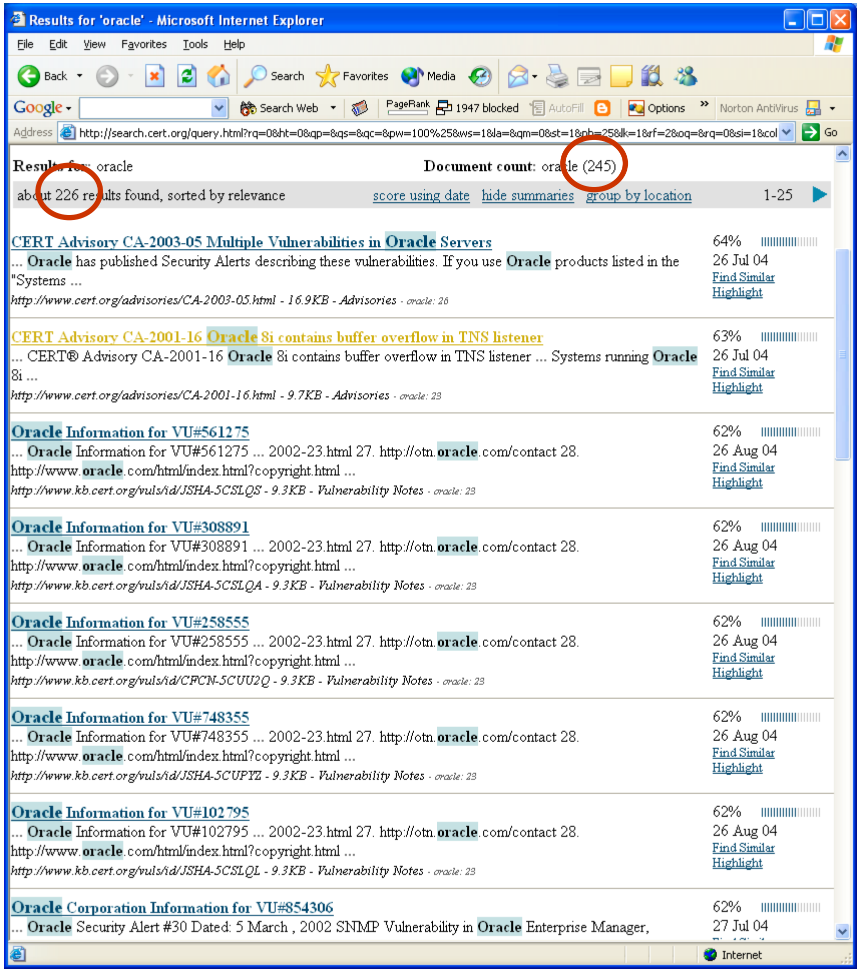
- SELECT username FROM users WHERE username=‘XYZ’ AND password=‘ABC’
  - SELECT username FROM users WHERE username=‘XYZ’ AND password=‘ABC’ OR ‘1’=‘1’
  - SELECT username FROM users WHERE username=‘XYZ’ AND password=‘ABC’ UNION ALL SELECT object_name FROM user_objects WHERE ‘’=‘’

- SELECT name,ssec FROM customers WHERE id=‘XYZ’
  - SELECT name,ssec FROM customers where id LIKE ‘%’

- SELECT name,ssec FROM customers WHERE id=‘1’
  - SELECT name,ssec FROM customers WHERE id=‘2’
  - SELECT name,ssec FROM customers WHERE id=‘3’
  - SELECT name,ssec FROM customers WHERE id=‘4’
  - …

Oracle Vulnerabilities

- www.cert.org
- http://www.oracle.com/technology/deploy/security/alerts.htm



Address http://search.cert.org/query.html?rq=0&ht=0&qp=&qs=&qc=&pw=100%25&ws=1&la=&qm=0&st=1&nh=25&lk=1&rf=2&oq=&rq=0&si=1&col

Results for: oracle **Document count:** oracle (245)

about 226 results found, sorted by relevance score using date hide summaries group by location 1-25

CERT Advisory CA-2003-05 Multiple Vulnerabilities in Oracle Servers
... Oracle has published Security Alerts describing these vulnerabilities. If you use Oracle products listed in the "Systems ...
http://www.cert.org/advisories/CA-2003-05.html - 16.9KB - Advisories - oracle: 26
64% 26 Jul 04 Find Similar Highlight

CERT Advisory CA-2001-16 Oracle 8i contains buffer overflow in TNS listener
... CERT® Advisory CA-2001-16 Oracle 8i contains buffer overflow in TNS listener ... Systems running Oracle 8i ...
http://www.cert.org/advisories/CA-2001-16.html - 9.7KB - Advisories - oracle: 23
63% 26 Jul 04 Find Similar Highlight

Oracle Information for VU#561275
... Oracle Information for VU#561275 ... 2002-23.html 27. http://otn.oracle.com/contact 28. http://www.oracle.com/html/index.html?copyright.html ...
http://www.kb.cert.org/vuls/id/JSHA-5CSLQS - 9.3KB - Vulnerability Notes - oracle: 23
62% 26 Aug 04 Find Similar Highlight

Oracle Information for VU#308891
... Oracle Information for VU#308891 ... 2002-23.html 27. http://otn.oracle.com/contact 28. http://www.oracle.com/html/index.html?copyright.html ...
http://www.kb.cert.org/vuls/id/JSHA-5CSLQA - 9.3KB - Vulnerability Notes - oracle: 23
62% 26 Aug 04 Find Similar Highlight

Oracle Information for VU#258555
... Oracle Information for VU#258555 ... 2002-23.html 27. http://otn.oracle.com/contact 28. http://www.oracle.com/html/index.html?copyright.html ...
http://www.kb.cert.org/vuls/id/CFCN-5CUU2Q - 9.3KB - Vulnerability Notes - oracle: 23
62% 26 Aug 04 Find Similar Highlight

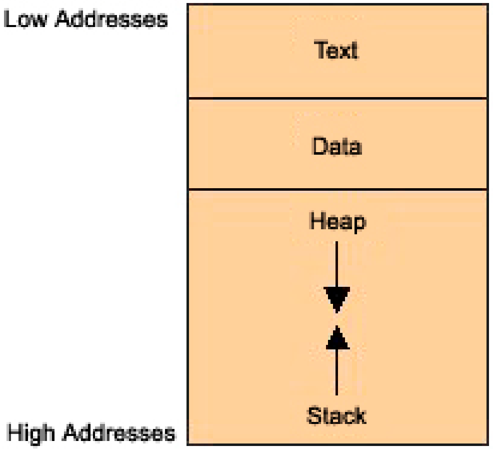
Oracle Information for VU#748355
... Oracle Information for VU#748355 ... 2002-23.html 27. http://otn.oracle.com/contact 28. http://www.oracle.com/html/index.html?copyright.html ...
http://www.kb.cert.org/vuls/id/JSHA-5CUPYZ - 9.3KB - Vulnerability Notes - oracle: 23
62% 26 Aug 04 Find Similar Highlight

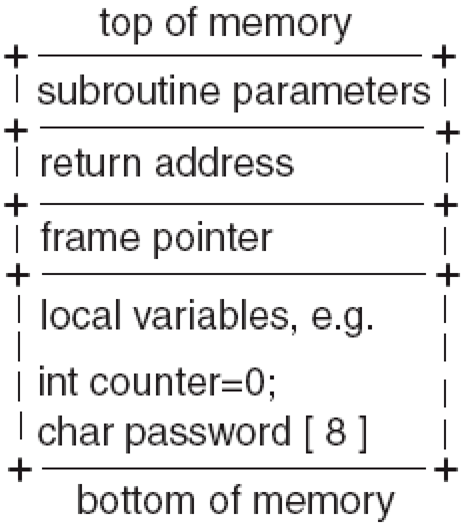
Oracle Information for VU#102795
... Oracle Information for VU#102795 ... 2002-23.html 27. http://otn.oracle.com/contact 28. http://www.oracle.com/html/index.html?copyright.html ...
http://www.kb.cert.org/vuls/id/JSHA-5CSLQL - 9.3KB - Vulnerability Notes - oracle: 23
62% 26 Aug 04 Find Similar Highlight

Oracle Corporation Information for VU#854306
... Oracle Security Alert #30 Dated: 5 March , 2002 SNMP Vulnerability in Oracle Enterprise Manager,
62% 27 Jul 04

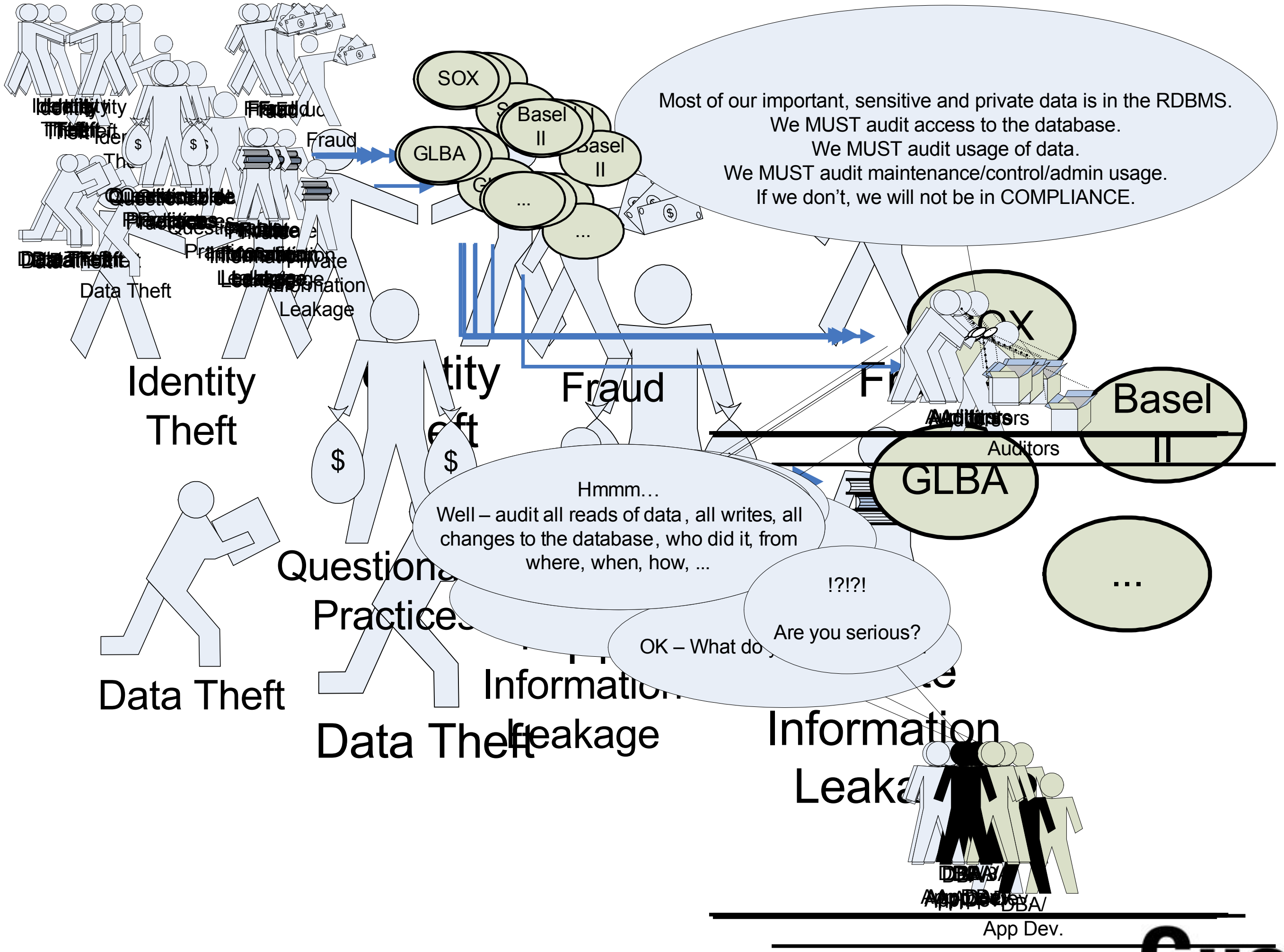
Example 3: Double Whammy

- SELECT FROM_TZ(TIMESTAMP ‘2004-09-07 18:00:00’, ‘5:00’) FROM DUAL;
- SELECT FROM_TZ(TIMESTAMP ‘2004-09-07 18:00:00’, ‘well crafted long string @(*#&$%^*@#$sdfnhjkhsdfkhjfdhgkh9283748’) FROM DUAL;





Example 4: Auditing semantic gap


Identity Theft
Fraud
Questionable Practices
Data Theft
Private Information Leakage
SOX
Basel II
GLBA
...
Most of our important, sensitive and private data is in the RDBMS. We MUST audit access to the database. We MUST audit usage of data. We MUST audit maintenance/control/admin usage. If we don't, we will not be in COMPLIANCE.
Auditors
Hmmm… Well – audit all reads of data, all writes, all changes to the database, who did it, from where, when, how, ...
OK – What do
!?!?! Are you serious?
DBA/ App Dev.

What does the security world have to offer?

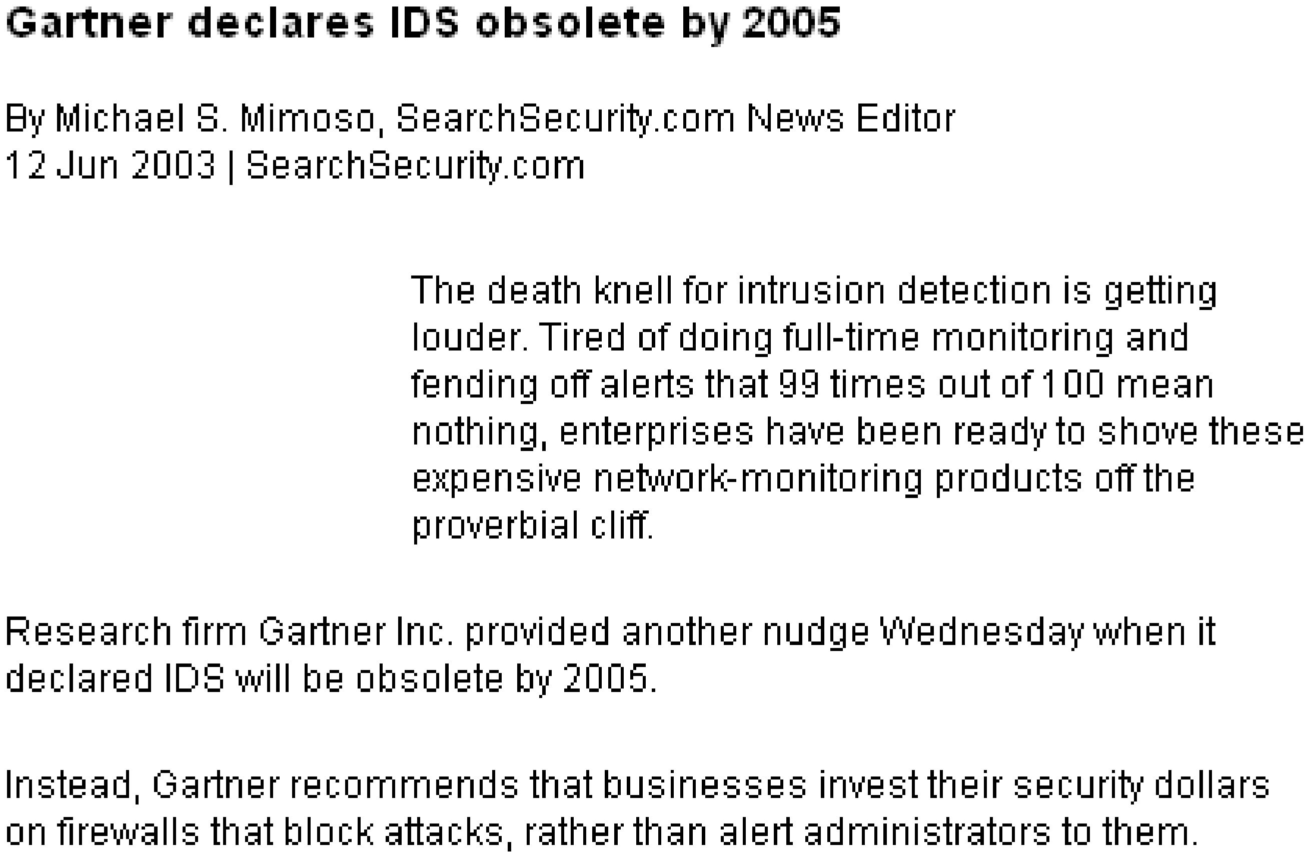
- Firewalls
  - TCP/IP access control

```
TCP.INVITED_NODES=(<Client IP-ADDRESS 1>, <Client IP-ADDRESS 2>)
TCP.EXCLUDED_NODES=(<Client IP-ADDRESS 3>, <Client IP-ADDRESS 4>)
TCP.VALIDNODE_CHECKING=yes
```

protocol.ora for Oracle 8i   sqlnet.ora for Oracle 9i

- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems
  - Detect/prevent misuse of network or computer resources
    - Sensors and rules
    - Libraries of signatures
    - “Deep packet inspection”

IDS Success – or lack-of



Gartner declares IDS obsolete by 2005

By Michael S. Mimoso, SearchSecurity.com News Editor
12 Jun 2003 | SearchSecurity.com

The death knell for intrusion detection is getting louder. Tired of doing full-time monitoring and fending off alerts that 99 times out of 100 mean nothing, enterprises have been ready to shove these expensive network-monitoring products off the proverbial cliff.

Research firm Gartner Inc. provided another nudge Wednesday when it declared IDS will be obsolete by 2005.

Instead, Gartner recommends that businesses invest their security dollars on firewalls that block attacks, rather than alert administrators to them.

Problem in applying IDS and deep packet inspection to database security

- Payload inspection is not enough – full SQL parsing and full protocol analysis is needed

```
00000000 : 01 67 00 00 06 04 00 00 00 00 11 6b 04 09 00 00 .g.........k....
00000010 : 00 b8 17 00 00 01 00 00 00 03 5e 05 f9 82 00 00 ..........^.....
00000020 : 00 00 00 00 38 a3 06 08 4e 00 00 00 60 3e 06 08 ....8...N...`>..
00000030 : 0c 00 00 00 00 00 00 00 90 3e 06 08 00 00 00 00 .........>......
00000040 : 01 00 00 00 16 00 00 00 b0 56 06 08 01 00 00 00 .........V......
00000050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000060 : 92 3e 06 08 b0 56 06 08 03 00 00 00 fe 40 73 65 .>...V.......@se
00000070 : 6c 65 63 74 20 65 6e 61 6d 65 20 2c 73 61 6c 20 lect ename ,sal
00000080 : 2c 63 6f 6d 6d 20 69 6e 74 6f 20 3a 73 32 3a 73 ,comm into :s2:s
00000090 : 31 20 2c 3a 73 34 3a 73 33 20 2c 3a 73 36 3a 73 1 ,:s4:s3 ,:s6:s
000000a0 : 35 20 20 20 66 72 6f 6d 20 45 4d 50 20 77 0e 68 5   from EMP w.h
000000b0 : 65 72 65 20 45 4d 50 4e 4f 3d 3a 62 32 00 01 00 ere EMPNO=:b2...
000000c0 : 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000d0 : 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 ................
000000e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 ................
000000f0 : 00 00 16 00 00 00 00 00 00 00 01 00 00 00 00 00 ................
00000100 : 00 00 00 00 00 00 00 00 00 00 00 01 01 00 00 14 ................
00000110 : 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 ................
00000120 : 00 b2 00 01 00 00 00 00 02 01 00 00 16 00 00 00 ................
00000130 : 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 ................
00000140 : 00 00 00 00 00 02 01 00 00 16 00 00 00 00 00 00 ................
00000150 : 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000160 : 00 00 07 03 c2 4a 46                             .....JF
```

UPDATE TEST_SQL SET TEXT='SELECT * FROM USER_OBJECTS UNION SELECT * FROM USER_OBJECTS WHERE 1=1'

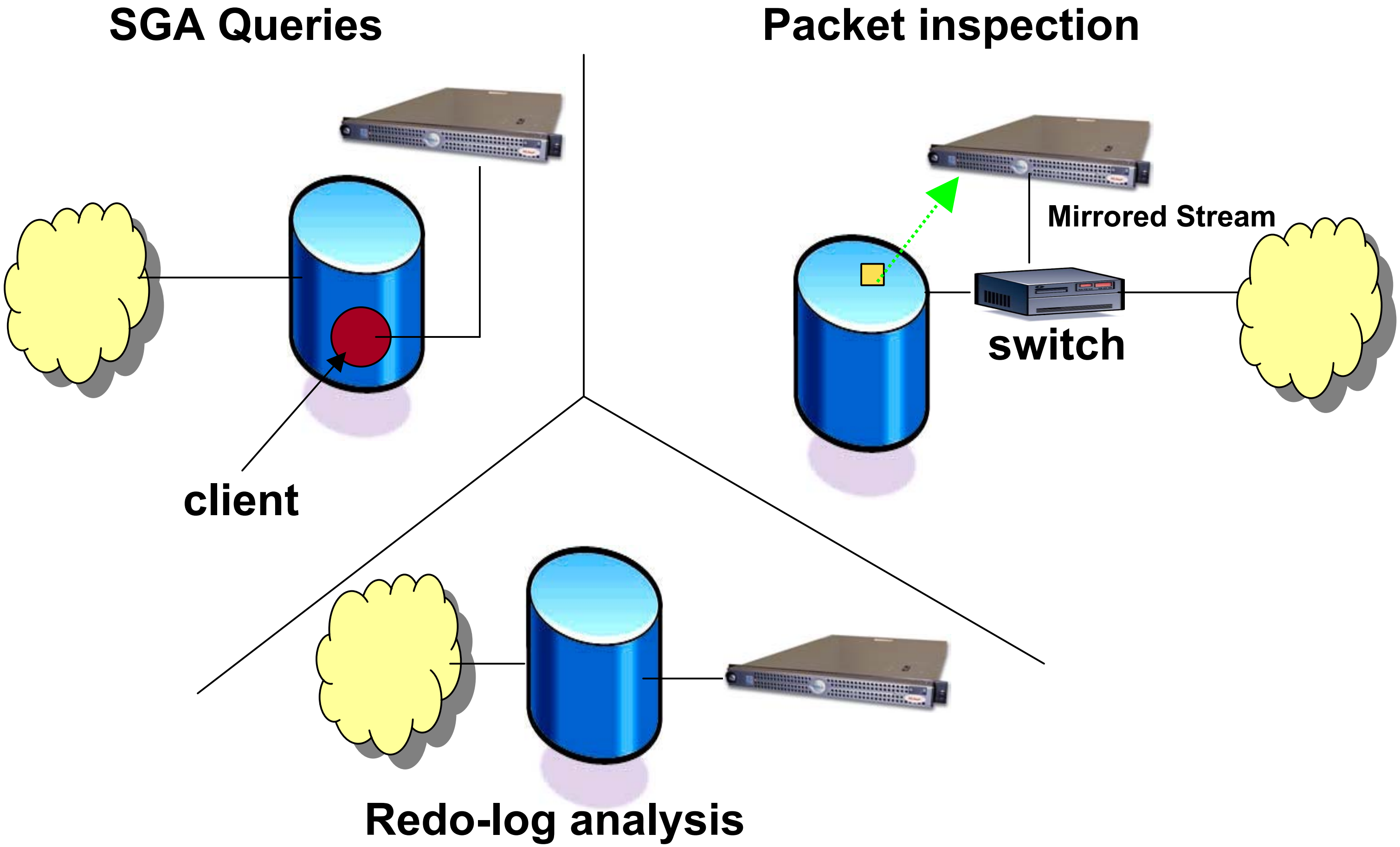
More importantly

- Any attack can take on an infinite number of ways – signatures are pretty much useless in a SQL environment
  - 1=1, 2=2, 1<2, ‘ron’ like ‘ron%’, string concatenation, build in functions, …
- Bottom line: generic IDS/IPS are not effective for database protection
- Function-focused vs. environment-focused
  - IDS/IPS try to provide a function for many environments
  - Database environment requires multiple security/audit functions

Key Success Factors

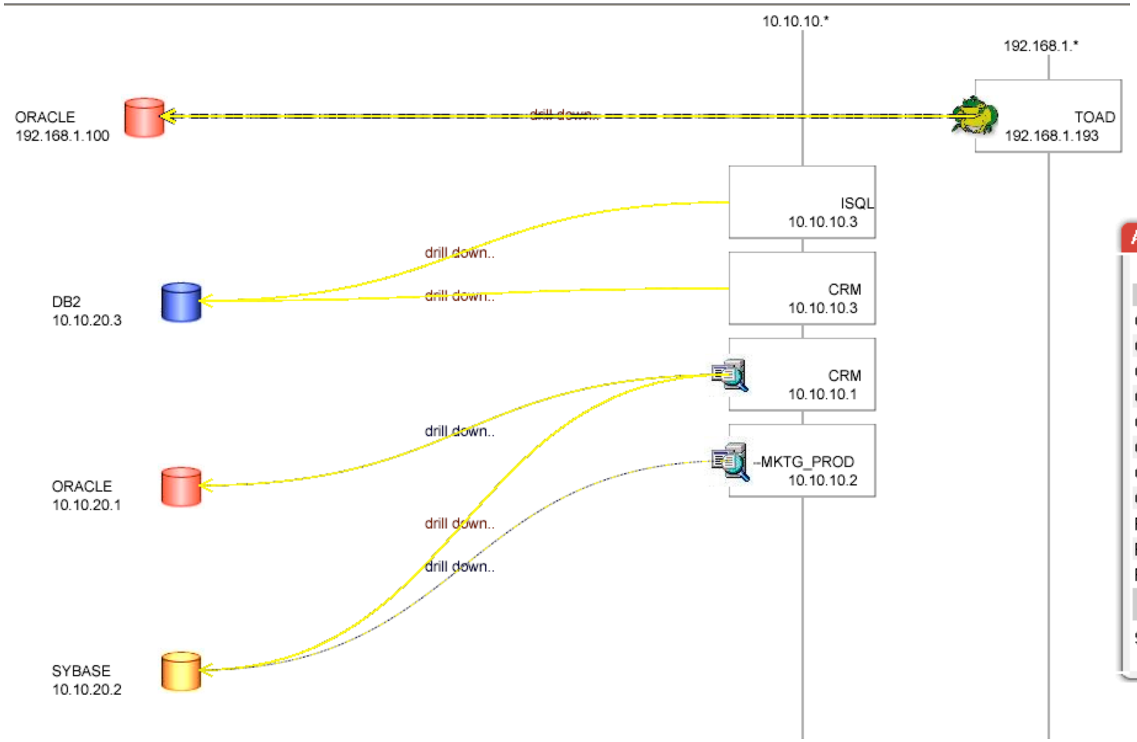
- Full understanding and fit with the database and the DBA environment
  - Continuous SQL-level inspection
  - Full coverage of database options
  - SQL and other – based policies, alerts, etc.
  - Non intrusive
  - Complex access environments
  - Complex rules and configurations
- Breadth of functionality for database security and auditing
  - Policy-based real-time alerting and prevention
    - Before-the-fact or after-the-fact
  - Data access monitoring
  - Assessments
  - Auditing
    - …
  - Error monitoring and alerting
  - Investigations and forensic analysis
- Quick implementation and ability to be utilized with limited skill sets
  - Non-intrusive; zero risk
  - Many tasks do not require DBA skills
    - Stop overloading the DBA
    - Segregation of duties – put your money where your mouth is

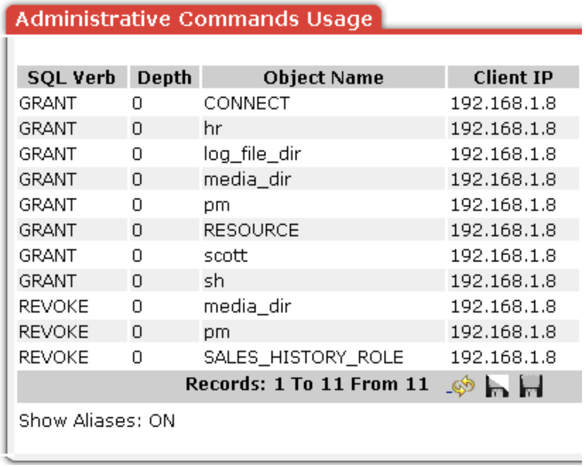
Three approaches to "non-intrusive" monitoring



Guardium

Monitoring



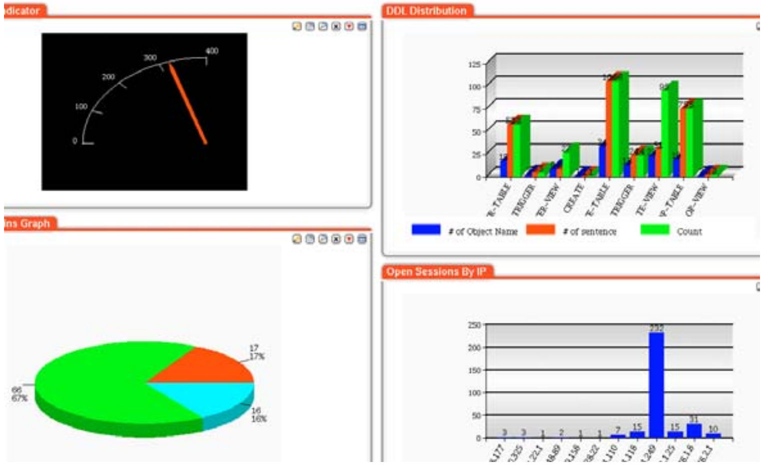


Administrative Commands Usage

SQL Verb	Depth	Object Name	Client IP
GRANT	0	CONNECT	192.168.1.8
GRANT	0	hr	192.168.1.8
GRANT	0	log_file_dir	192.168.1.8
GRANT	0	media_dir	192.168.1.8
GRANT	0	pm	192.168.1.8
GRANT	0	RESOURCE	192.168.1.8
GRANT	0	scott	192.168.1.8
GRANT	0	sh	192.168.1.8
REVOKE	0	media_dir	192.168.1.8
REVOKE	0	pm	192.168.1.8
REVOKE	0	SALES_HISTORY_ROLE	192.168.1.8

Records: 1 To 11 From 11

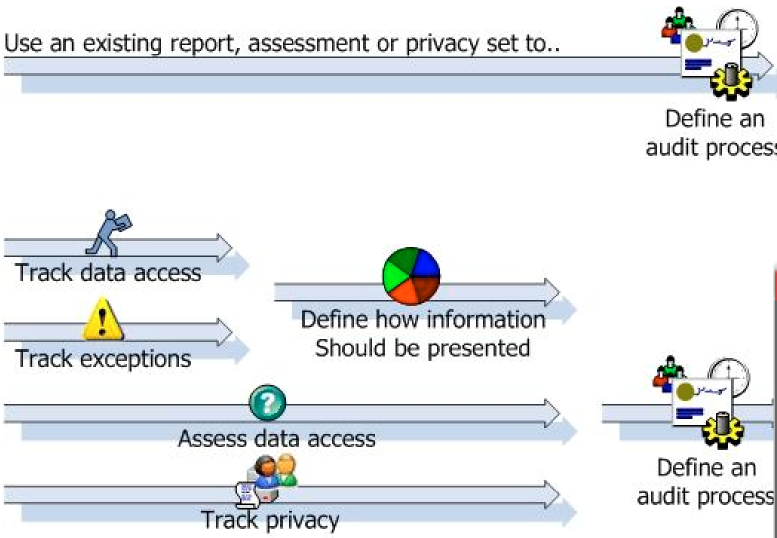
Show Aliases: ON



Company Confidential

Guardium

Auditing



Use an existing report, assessment or privacy set to..

Define an audit process

Track data access

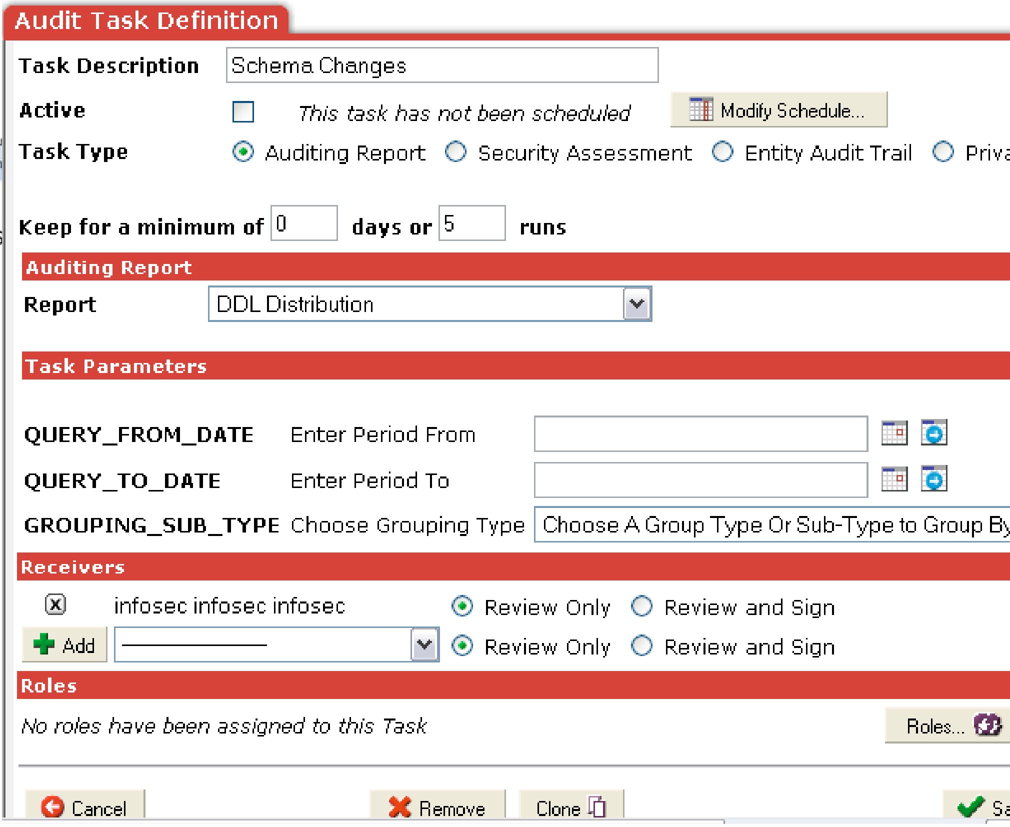
Track exceptions

Define how information Should be presented

Assess data access

Track privacy

Define an audit process



Audit Task Definition

Task Description: Schema Changes

Active: □ *This task has not been scheduled*

Task Type: ● Auditing Report ○ Security Assessment ○ Entity Audit Trail ○ Priva

Keep for a minimum of 0 days or 5 runs

Auditing Report

Report: DDL Distribution

Task Parameters

QUERY_FROM_DATE	Enter Period From	
QUERY_TO_DATE	Enter Period To	
GROUPING_SUB_TYPE	Choose Grouping Type	Choose A Group Type Or Sub-Type to Group By

Receivers

☒ infosec infosec infosec ● Review Only ○ Review and Sign

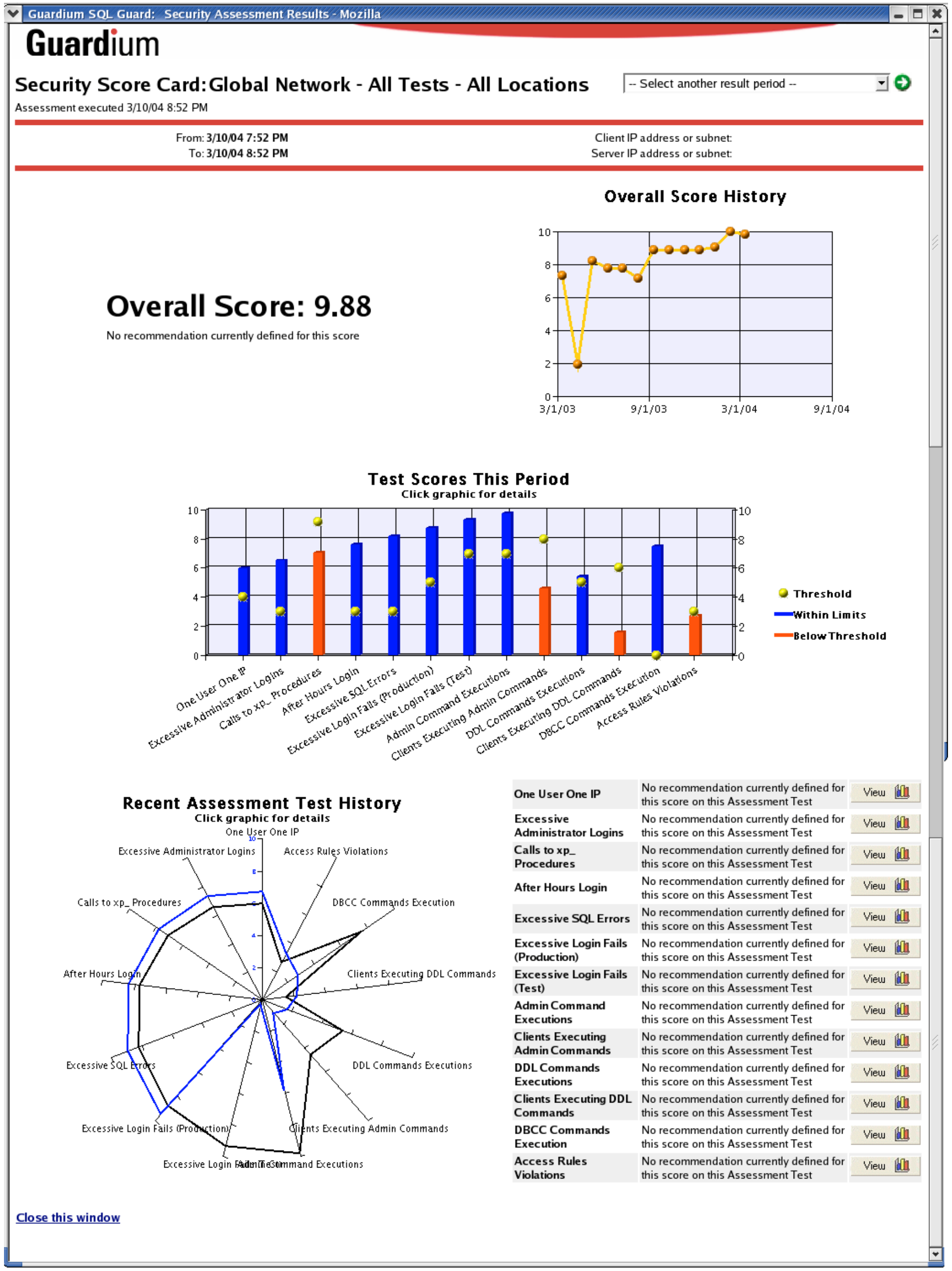
Add ● Review Only ○ Review and Sign

Roles

No roles have been assigned to this Task

Company Confidential

Assessments



Guardium SQL Guard: Security Assessment Results - Mozilla

Guardium

Security Score Card:Global Network - All Tests - All Locations

-- Select another result period --

Assessment executed 3/10/04 8:52 PM

From: **3/10/04 7:52 PM**
To: **3/10/04 8:52 PM**

Client IP address or subnet:
Server IP address or subnet:

Overall Score: 9.88

No recommendation currently defined for this score

Overall Score History

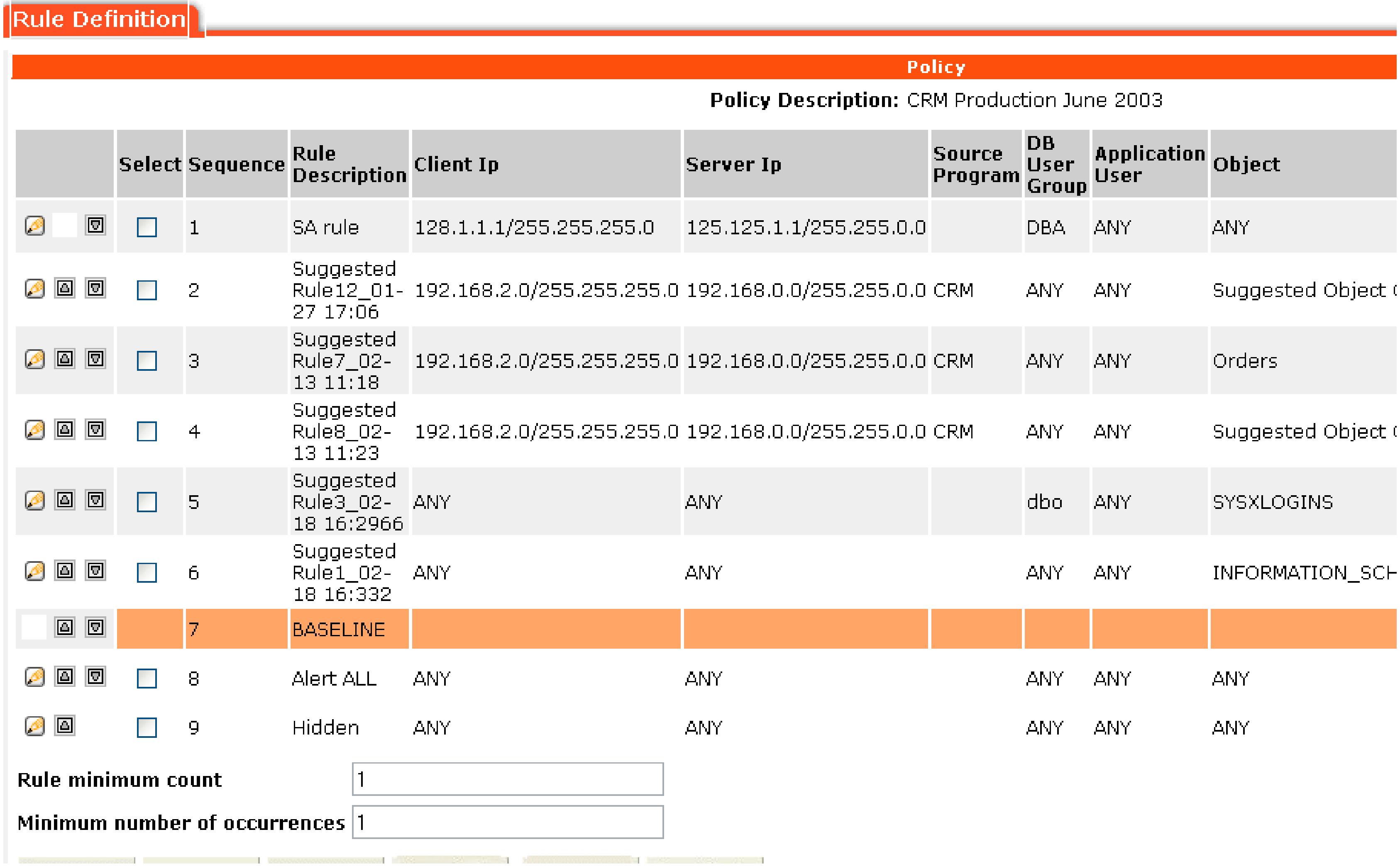
Test Scores This Period
Click graphic for details

Recent Assessment Test History
Click graphic for details

One User One IP	No recommendation currently defined for this score on this Assessment Test	View
Excessive Administrator Logins	No recommendation currently defined for this score on this Assessment Test	View
Calls to xp_ Procedures	No recommendation currently defined for this score on this Assessment Test	View
After Hours Login	No recommendation currently defined for this score on this Assessment Test	View
Excessive SQL Errors	No recommendation currently defined for this score on this Assessment Test	View
Excessive Login Fails (Production)	No recommendation currently defined for this score on this Assessment Test	View
Excessive Login Fails (Test)	No recommendation currently defined for this score on this Assessment Test	View
Admin Command Executions	No recommendation currently defined for this score on this Assessment Test	View
Clients Executing Admin Commands	No recommendation currently defined for this score on this Assessment Test	View
DDL Commands Executions	No recommendation currently defined for this score on this Assessment Test	View
Clients Executing DDL Commands	No recommendation currently defined for this score on this Assessment Test	View
DBCC Commands Execution	No recommendation currently defined for this score on this Assessment Test	View
Access Rules Violations	No recommendation currently defined for this score on this Assessment Test	View

Close this window

Policies



Rule Definition

Policy

Policy Description: CRM Production June 2003

	Select	Sequence	Rule Description	Client Ip	Server Ip	Source Program	DB User Group	Application User	Object
	□	1	SA rule	128.1.1.1/255.255.255.0	125.125.1.1/255.255.0.0		DBA	ANY	ANY
	□	2	Suggested Rule12_01-27 17:06	192.168.2.0/255.255.255.0	192.168.0.0/255.255.0.0	CRM	ANY	ANY	Suggested Object (
	□	3	Suggested Rule7_02-13 11:18	192.168.2.0/255.255.255.0	192.168.0.0/255.255.0.0	CRM	ANY	ANY	Orders
	□	4	Suggested Rule8_02-13 11:23	192.168.2.0/255.255.255.0	192.168.0.0/255.255.0.0	CRM	ANY	ANY	Suggested Object (
	□	5	Suggested Rule3_02-18 16:2966	ANY	ANY		dbo	ANY	SYSXLOGINS
	□	6	Suggested Rule1_02-18 16:332	ANY	ANY		ANY	ANY	INFORMATION_SCH
		7	BASELINE						
	□	8	Alert ALL	ANY	ANY		ANY	ANY	ANY
	□	9	Hidden	ANY	ANY		ANY	ANY	ANY

Rule minimum count 1

Minimum number of occurrences 1

DATABASE SECURITY STARTS WITH KNOWLEDGE™

SQL Guard™

Ron Bennatan
Guardium, Inc.
230 Third Avenue
Waltham, MA 02451

phone 781-684-6282
fax 781-684-6299

ron_bennatan@guardium.com

Guardium