



Inplexus offers a complete Oracle database environment security assessment. This assessment identifies vulnerabilities and recommends solutions that will improve the security of the database environment against denial of service attacks and unauthorized access.

This Oracle Security Assessment can be performed on one or more databases. The actual assessment creates little strain on the database and the database machine. Therefore, these activities can be performed on a production database during normal operation. However, the customer chooses the database and the time for the assessment. The assessment involves four different security evaluations: customer interviews, a database penetration test, a database vulnerability evaluation and an Oracle environment evaluation of the database server operating system.

Inplexus begins the assessment by interviewing the customer staff and gathering information about the databases, hosts and network connectivity. In addition, these interviews collect information about database security policies, guidelines, responsibilities and procedures. The information gathered from the interviews are used for database security examination and reviewed for potential security improvement.

The second step in the Oracle assessment is a penetration test. During the penetration test, the assessment attempts to find users with predictable or easily guessed user name and password combinations. This test is conducted using default password, dictionary and brute force attempts. Typically, user and password combinations are found that allow easy access to the database.

The third step in the assessment is a database vulnerability assessment. During the database vulnerability assessment, the database is examined for potential vulnerabilities where the database does not conform to security best practices. A secure database follows the principal of "least privilege". This means that users and programs should only have access to the database objects required. Typical problems uncovered are vulnerabilities that provide valid users more access than required, potential for denial of service attacks and unneeded access to internal database information. This portion of the assessment performs more than fifty tests on the database.

The fourth step in the assessment is an operating system review of the Oracle database environment. During this review, configuration and permissions on Oracle files and directories are checked. This step examines Oracle executables, database files, configuration files and Oracle environment variables.

Once the interviews, penetration tests, vulnerability assessments and operating system investigation are complete, Inplexus staff reviews the results and provides the assessment findings and a recommendation report to the customer noting methods to mitigate the risks that have been identified. Inplexus delivers both a printed version and an electronic version of the report to the customer and conducts an in-depth meeting with the key staff members to review the report and define critical risks and associated remedies. The customer can then use the findings and recommendations to address the security concerns defined in the report. All findings and recommendations are kept confidential.

The Oracle Security Assessment offers value to the customer by identifying database vulnerabilities, recommending for security-based changes and providing explanation of remedies.

If you would like more information about an Oracle database system assessment from Inplexus, please call 770-864-7222 or send an email to info@inplexus.com.