Trustwave®

# Database Risk Assessment

## INDEPENDENT DATABASE RISK & COMPLIANCE ANALYSIS

### Objectives

Provide recipient with the knowledge of their Risk Exposures and Compliance posture for their databases, prioritize them and understand how a continuous process would improve an organization's database security & compliance program's effectiveness.

### A Diagnostic Exercise to Assess

1. Awareness of all discoverable databases
2. Current Database Security and Risk Posture
3. User Entitlement Review
4. Access to Sensitive Data
5. Compliance and Audit readiness

### Description

Databases contain an organization's valuable information, but the complexity of database functionality and the lack of technical awareness regarding database security, results in database applications being one of the most commonly misconfigured applications. A Database Risk Assessment (DRA) discovers database platforms within your infrastructure and then assesses their risk exposure.

1. During a Database Risk Assessment, a Trustwave consultant performs testing in three phases:
2. Identify discoverable database instances within a defined IP range or domain in your infrastructure
3. Assess one or two representative database(s) against Industry best practices. For this phase, a vulnerability assessment scan is configured to assess the database instance using credentials to access the information needed to complete the audit. This approach provides actionable information on inherent vulnerabilities and database configuration elements which may cause your databases to be vulnerable to attack, lead to regulatory compliance issues, or cause them to fail to comply with your information security policy.
4. Conduct a User Entitlement Review against a handful of objects that contain sensitive data, to identify who has access to this data and how those rights were obtained.

### Outcome

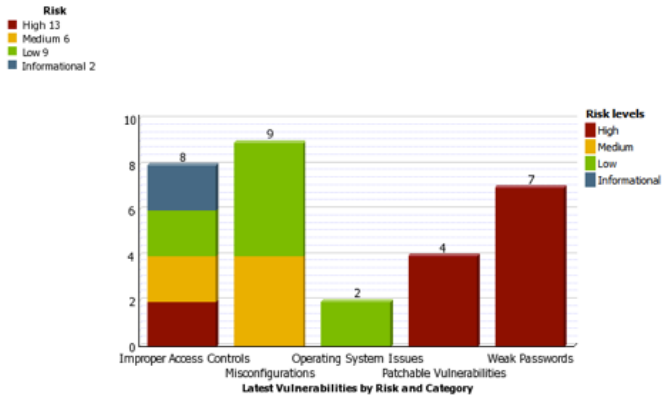
The Trustwave consultant will provide a comprehensive presentation that outlines key vulnerabilities, prioritizes them by risk level, and explains what they mean, the impact and suggested remediation. The Risk Assessment findings are presented and reviewed with you and your designated personnel to ensure they are well understood.

At the end of the DRA engagement, Trustwave will leave behind the assessment software used to run the initial vulnerability scans, so that the client can run subsequent scans against other databases over the next month.

#### The presentation will cover the following topics:

- DRA Objectives
- Environment Description
- Summary findings
  - Databases
  - Vulnerabilities
  - User Rights Review
- Analysis of Top 5-8 issues
- Root Causes, Enablers
- Detailed Findings Report
- Key Recommendations / Conclusion

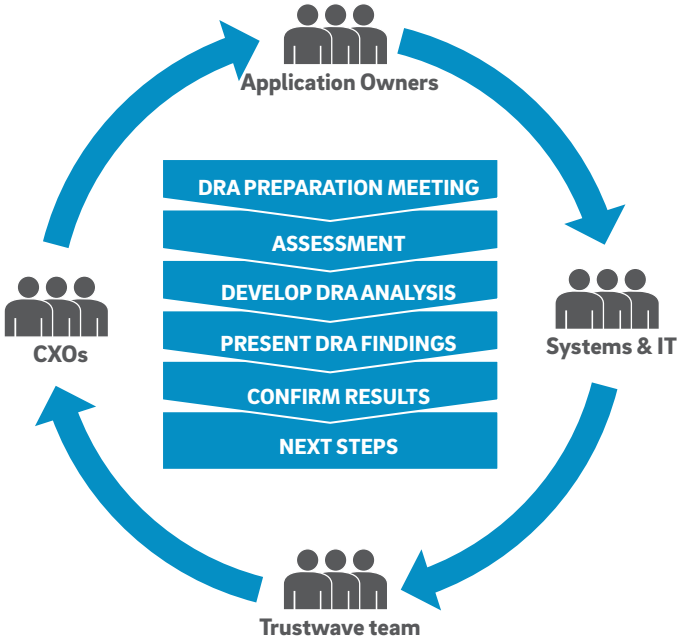
#### Latest Vulnerabilities by Risk & Category



## DRA Process

- Pre-call (Qualification)
- Preparation Con Call – 1 Hour
- Day 1
  - Onsite meeting
  - Conduct Assessment
- Offsite Work (1-3 Days)
  - Develop DRA Analysis
- Day 2
  - Present Findings and Confirm results

## Management Sponsorship




## DRA Preparation

- Logistics
  - Pre-call
  - NDA in place
  - Scheduling – enough notice 2-3 weeks out
  - Pre-questionnaire Completed (one week prior)
- Database access
- Network access
- Etc.
  - Preparation Con Call (one week prior)
- Database(s) to be assessed
- IP Range to be used for discovery
- Logistics discussion

## Prerequisites

- Project team members should have a working knowledge of Databases and Security.
- Appropriate system access for consultant must be in place

## Pricing

The Database Risk Assessment is a Time and Materials project of up to 5 days, and includes an unlimited use 30 day license for AppDetectivePRO, at a cost of $15,000 USD. This pricing assumes 1 full-time Database Risk Assessment Technical Expert. Scope and project deliverables will be detailed in an SOW. Travel and accommodation expenses are billed separately.

Trustwave®

For more information: www.trustwave.com