Trustwave®

Database Risk Assessment

▶ INDEPENDENT DATABASE RISK & COMPLIANCE ANALYSIS

Benefits

- External verification of your database security program

- Preparing for an audit by having a dry run with our Trustwave SpiderLabs security consultants

- Finding rogue or abandoned databases that may have Personally Identifiable Information (PII) or Organization Identifiable Information (OII)

- Discover over-privileged users that could lead to breaches

Databases often contain sensitive and confidential information and are attractive targets for cyber criminals. They also need to meet stringent compliance, regulatory and audit requirements. Conducting regular databases regular health checks ensure that their security meets their standards. They also help identify gaps and how to remediate them.

The Database Risk Assessment (DRA) program is a key component of the Trustwave Database Security Process. The goal of the DRA is to identify risk exposure and compliance posture on the databases, prioritize them and understand how a continuous process would improve the organization's database security & compliance program effectiveness. This program is ideal for organizations in the following situations:

- Preparing for an audit and need expertise to assess their current database security program
- Need to conduct database inventory as they don't know where all their databases are located
- Need external verification of their database security program
- Lack of in-house database security expertise and seek an expert assessment

Overview

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.

During a Database Risk Assessment, a Trustwave consultant performs testing in three phases:

1. Identify discoverable database instances within a defined IP range or domain within your infrastructure
2. Assess representative database(s) against industry best practices. A vulnerability assessment scan using credentials is configured to assess the database instance and to access the information needed to complete the audit. This approach provides actionable information on inherent vulnerabilities and database configuration elements that may make your databases vulnerable to attack, lead to regulatory compliance issues, or make them fail to comply with your information security policy.
3. 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.

At the end of a Database Risk Assessment a comprehensive presentation and documentation are created that outlines key vulnerabilities and configuration issues, prioritization of each by risk level, as well as explanations of what they are, their impact and appropriate next steps. Trustwave will provide deep analysis on the top five to ten issues, the root causes or enablers of those issues and detailed findings reports on them. As part of the Database Risk Assessment we additionally provide a 30-day license of AppDetectivePRO so that you can retest and ensure a more secure database.

Check Results Summary

As of Today (Oct 4, 2018)
For Organization: patterson.home
Including Descendants: Yes
For Asset Types: Any
For Check Categories: Any
For Result Status: Any
For Risks: Any
Include Attributes: No
KB Articles Included: No

A security review has been run on a number of applications on your network. This review consisted of probing the application and comparing the results to a knowledge base of Trustwave vulnerabilities. This report displays a summary of all check results. Drill down to view more detailed results.

By Risk / By Category / By Asset Type

Legend: High, Medium, Low, Informational

Results Summary (904 checks)

Asset	IP Address, Port, Instance	Result Status	Check Category	Risk	Check	Occurrences
DVD Rental	192.168.1.18 3, 5432, dvdrental	Fact	Improper Access Controls	⚠	Ensure only DBAs has SUPERUSER, CREATEDB, CREATEROLE privileges	1

High, Medium, Low, Informational

Check Status

As of Today (Oct 4, 2018)
For Organization: patterson.home
Including Descendants: Yes
For Asset Types: Any
For Check Categories: Any
For Result Status: Any
For Risks: Any
Include Attributes: No
KB Articles Included: No

A number of penetration tests and audits were performed on the assets in your network. Below is a list of checks that were executed along with an indication of whether any violations of the check were found.

By Check Status / By Asset Type / By Category

Check Category: Improper Access Controls, Misconfigurations, Operating System Issues, Other, Patchable Vulnerabilities, Weak Passwords

Legend: Completed, Failed, Skipped

Results (904 checks)

Asset	IP Address, Port, Instance	Result Status	Check Category	Risk	Check	Check Start Date	Check End Date
DVD Rental	192.168.1.18 3, 5432, dvdrental	Fact	Improper Access Controls	⚠	Ensure only DBAs has SUPERUSER, CREATEDB, CREATEROLE privileges	May 1 2018 20:41	May 1 2018 20:41
				⚠	Ensure password aren't stored in plaintext	May 1 2018 20:41	May 1 2018 20:41
				ⓘ	Ensure that the number of connection are limited	May 1 2018 20:40	May 1 2018 20:40
				ⓘ	Periodic review of PostgreSQL databases	May 1 2018 20:40	May 1 2018 20:40
				⚠	Review database objects for correct ownership	May 1 2018 20:41	May 1 2018 20:41
				⚠	Review PostgreSQL users and roles	May 1 2018 20:41	May 1 2018 20:41

High, Medium, Low, Informational

Trustwave®