Automatically Find and Fix Insecure Database settings with Oracle Management Cloud

PRO4284

David Wolf
Snr Dir of Product Management - Oracle

Oct 25, 2018
Session : PRO4284

Title: Automatically Find and Fix Insecure Database settings with Oracle Management Cloud

Description : Automated attacks necessitate an automated defense, and there is no defense-in-depth without continuous compliance monitoring of your Oracle Databases. In this session explore best practices for database security posture maintenance and see strategies for prioritizing violation remediation using policies applied across both on-premises and cloud deployments. In addition explore automated policy violation remediation at the moment of detection, narrowing vulnerability windows.
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle’s products may change and remains at the sole discretion of Oracle Corporation.
Program Agenda

1  Why secure configuration matters so much for databases
2  Challenges with finding and fixing insecure databases
3  Automating secure configurations of databases with OMC
4  Demo
5  Q & A
Let’s get the obvious and infeasible goal of “Don’t get compromised” out of the way. A focus on understanding what data types are likely to be targeted and the application of controls to make it difficult (even with an initial device compromise) to access and exfiltrate is key.

Top asset involved in breaches

$76\%$ of breaches were financially motivated

Source: 2018 Verizon Data Breach Investigations Report
Sources of Cyber Security Controls

Top 6 (of 20) CIS Critical Security Controls

1: Inventory and Control of Hardware Assets
2: Inventory and Control of Software Assets
3: Continuous Vulnerability Management
4: Controlled Use of Administrative Privileges
5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6: Maintenance, Monitoring and Analysis of Audit Logs

Finding & Fixing Insecure Assets (Databases)

Cyber Security Frameworks
Finding and Fixing insecure database configurations

Common Challenges

Finding

• Knowledge of secure settings
• Changing application topologies
• Hybrid cloud deployments
• New instances

Fixing

• Lack of knowledge
• Time consuming
• Lengthy response times
Configuration and Compliance Cloud Service
Continuous secure configuration assessment and enforcement

• **Automated assessments** across deployments
  – On-demand and recurring evaluation with alerting on newly discovered issues and anomalies
  – Topology aware assessment ensures accurate evaluation

• **Analyze deviations from best practice and custom policies**
  – Rich out of box content: Industry best practices from DISA (STIG), CIS and Oracle
  – Execute & score custom scripts without modification
  – Retain compliance results for auditors and for use in Security Monitoring and Analytics
  – Upload and execute additional benchmarks

• **Enforce standards**
  – Guided manual remediation procedure embedded in each violation
  – Auto remediation via Orchestration channel
Trusted sources of secure state guidance

- **Consensus-based industry best practices**
- **Benchmark**
  - Technology specific hardening steps
- **Document guides freely available**
- **Primarily commercial usage**

- **Vendor assisted industry best practices**
- **STIG - Secure Tech Implementation Guide**
  - Technology specific hardening steps
- **Document guides freely available**
- **Primarily US Federal and state government**

- **Secure best practice recommendation whitepapers, MOS documents, etc.**
Automated Secure Config knowledge for Oracle DB and more

- OMC is Certified by the Center for Internet Security to assess the following:
  - CIS Benchmark for Oracle Database 12c v2.0.0, Level 1 RDBMS Traditional Profile

- OMC ships with rule-sets based on
  - Oracle Database 12c STIG
  - Oracle Linux 6 and 7 STIGs

- OMC includes secure best practice recommendation for:
  - EBS 12.X
  - Oracle Database 18c

### Rule Set Table

<table>
<thead>
<tr>
<th>Rule Set Name</th>
<th>Entity Type</th>
<th>Rule Set Type</th>
<th>Enabled</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Security Configuration For Oracle Database 18c [v1]</td>
<td></td>
<td></td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>Oracle Database 12c Single Instance Database STIG Configuration [v2]</td>
<td></td>
<td></td>
<td></td>
<td>83</td>
</tr>
<tr>
<td>Oracle E-Business Suite with Oracle Database 12.1 Best Practices [v1]</td>
<td></td>
<td></td>
<td></td>
<td>30</td>
</tr>
<tr>
<td>CIS Oracle Database 12c Benchmark- Level 1 - RDBMS using Traditional Auditing [v2.0.0]</td>
<td></td>
<td></td>
<td></td>
<td>117</td>
</tr>
<tr>
<td>Basic Security Configuration For Oracle Database [v1]</td>
<td></td>
<td></td>
<td></td>
<td>34</td>
</tr>
</tbody>
</table>
Dynamic Application Topology intelligence

• Single Assessment for entire topology
  – Pick the Rule Sets, Pick the App – Let Service figure out which to apply

• Topology evaluated at start of each assessment

• Investigate and Report violations in application context reduces time to action
Unified security posture for hybrid cloud deployments

- Comprehensive configuration intelligence across multiple cloud and multiple on-premise deployments
- Ensure consistency and security of cloud migrated databases and apps
- Integrated Security and ITOM services enhances security and maximizes investments
Automatic assessment of new database instances

• Groups can be used instead of specifying specific entities

• Groups can be:
  – Static – manually membership
  – Dynamic – auto membership based on attributes – Tag, size, etc

• Example – All databases with tag=Production should be assessed hourly against CIS rule-set.

• What if you want to assess ALL databases?

• Tip: All databases will be included IF you leave the entities/group list blank and select database rule-set.
Detailed guidance for manual remediation

• Oracle provided rule-sets have detailed descriptions, rationales and remediation instructions

• Prescriptive enough for junior administrators to be successful
Create run-books (workflows) for common remedies

• Orchestration CS’s workflow library to create library of common, time-consuming remedial actions

• Multistep workflows can support complex requirements like starting and stopping database if required for configuration change to take effect.

• Comprehensive graphical user interface to build, test and publish workflows.
Auto remediation for critical or time-sensitive fixes

- Automatically submit Orchestration workflow based on rule violation

- Integration via standard alert rules

- Create per rule or single “fix all” workflow depending on needs
Demonstration
Configuration and Compliance
Cloud Service
OMC Configuration and Compliance Service
Find and fix insecure database configurations automatically

**Finding**
- Ready to use secure configuration rule-sets for Oracle Databases and apps
- Dynamic application topology intelligence
- Unified security posture across hybrid cloud deployments
- Dynamic group and All features ensure complete coverage

**Fixing**
- Prescriptive remediation steps for Oracle database rule-sets
- Orchestration workflow library for common time-consuming runbooks
- Auto-remediation for critical or time-sensitive violations
Q & A