Oracle DB Security with the Use of AI

Exploring the Potential and Limitations of AI-Enhanced Database Protection

Stefan Oehrli

Stefan Oehrli – Modern Data Platforms

Modern Data Platforms

stefan.oehrli@accenture.com

SYMBOLIT

Oracle ACE Director

Tech Architecture Manager

- Since 1997 active in various IT areas
- More than 25 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
  - Security assessments and reviews
  - Database security concepts and their implementation
  - Oracle Backup & Recovery concepts and troubleshooting
  - Oracle Enterprise User and Advanced Security, DB Vault, …
  - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)

Terraform ASSOCIATE – HashiCorp CERTIFIED

2025 Oracle ACE Director

oradba.ch

@stefanoehrli

Oracle ACE

450+ technical experts helping peers globally

The **Oracle ACE Program** recognizes and rewards community members for their technical and community contributions to the Oracle community

3 membership tiers

Oracle ACE Director | Oracle ACE Pro | Oracle ACE Associate

For more details on Oracle ACE Program:
ace.oracle.com

Oracle ACE

Nominate
yourself or someone you know:
ace.oracle.com/nominate

Connect: **aceprogram_ww@oracle.com** Facebook.com/OracleACEs @oracleace Oracle ACE Program Group

Modern Data Platforms
VISON & MISSION

WHY? We are the game changer for our client's data platform projects

HOW? Maximum automation, maximum efficiency, maximum quality!

WHAT? We build innovative data platforms based on our blueprints and licensable assets and tools.

3 key benefits

1 Architecture expertise from hands-on projects

2 Delivery of tailor-made data platforms

3 Integrated Teams - Like a rowing team, perfect alignment and interaction.

Tools and Blueprints

Key enabler for the implementation of modern data platforms at a high speed and quality.

Continuous Optimization

Tools and Blueprints are continuously optimized to the customer and project’s needs.

Expertise & Light Towers

Expert group for modern data platforms from technical implementation to project management and organization

AI in Oracle DB Security

From Concept to Future Possibilities

1 Motivation & Challenges

2 AI Concept & First Steps

3 Natural Language in Action

4 Future Ideas

5 One More Thing

6 Summary & Conclusion

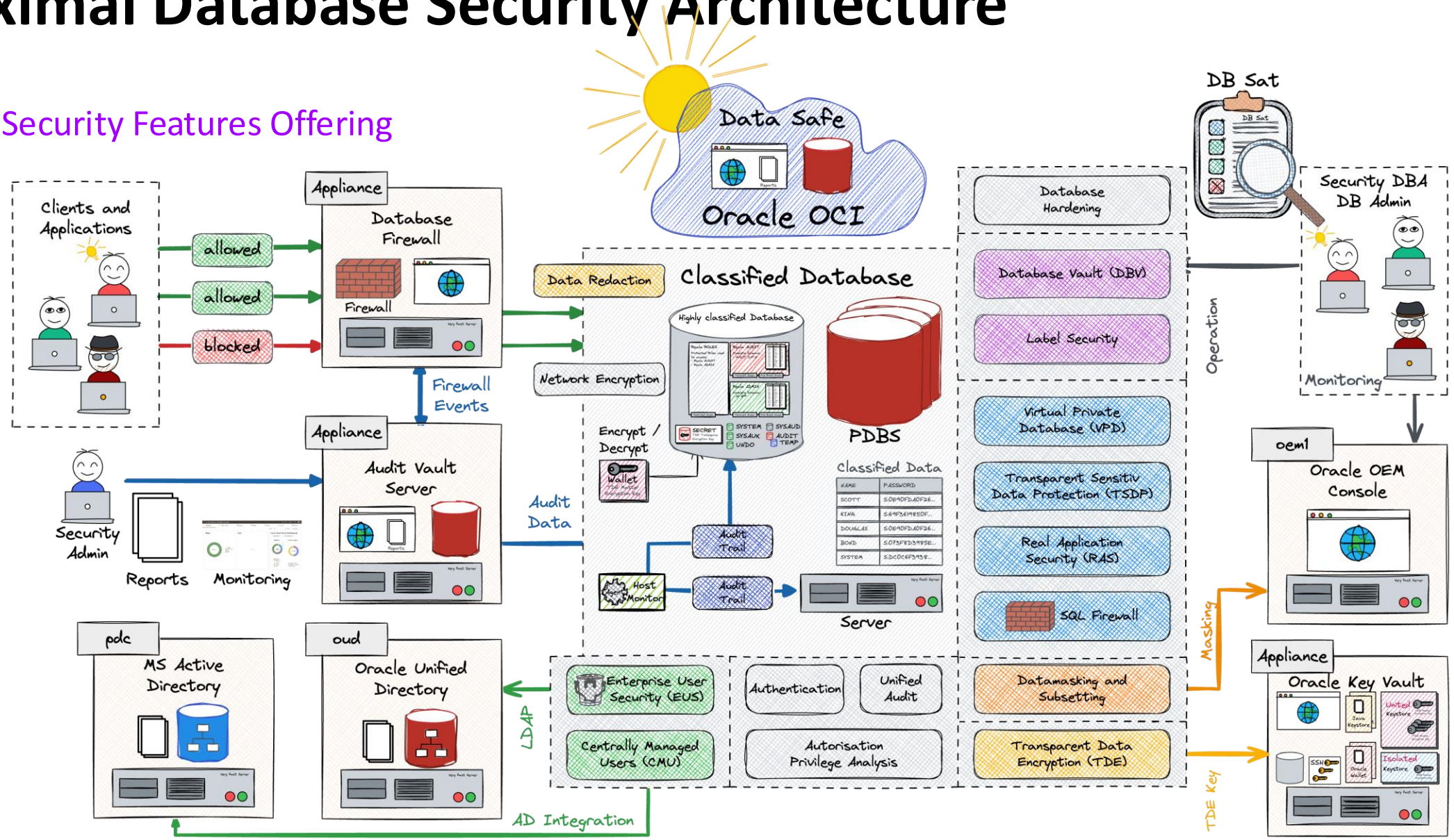
1

Motivation & Challenges

Why AI could bridge current security gaps.

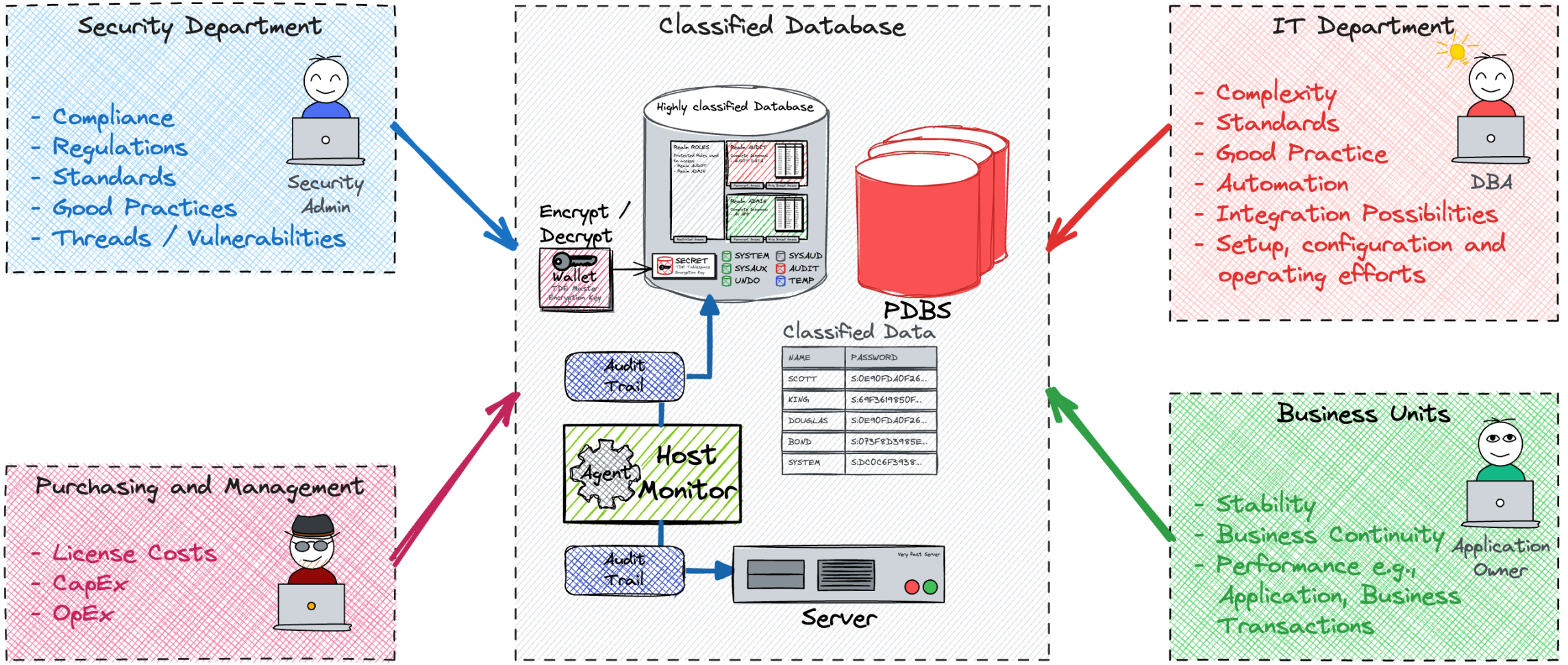
Maximal Database Security Architecture

Oracle Security Features Offering



The Critical Role of Oracle Database Security

Understanding the Needs and Contributions of Key Stakeholders



Bridging the Gap: Security vs. Operations

Can AI Simplify Oracle DB Security for All Stakeholders?

DBAs Focus:

- Typically centered on **performance**, **stability**, and **operational** tasks.
- Security monitoring and continuous reviews are often **not a primary** focus.
- Complexities of database security are easily **overlooked in day-to-day** operations.

Security Teams Dilemma:

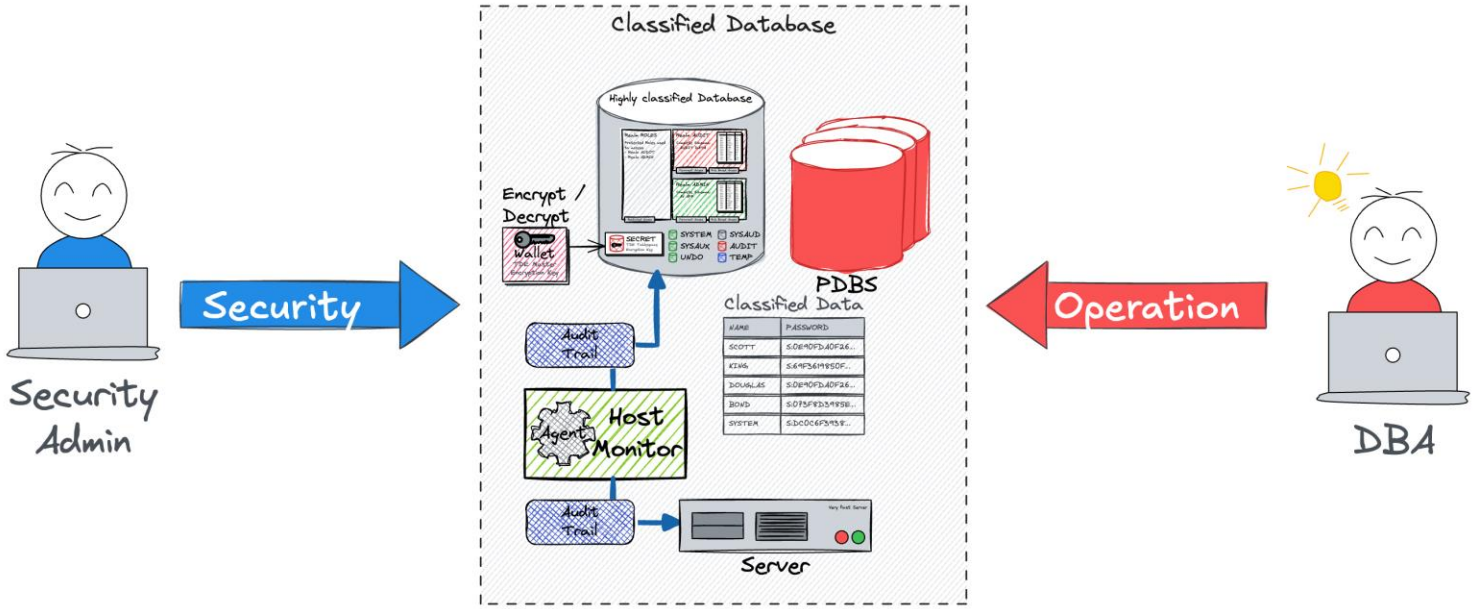
- Security teams **often lack** in-depth expertise to analyze privileges, audit trails, etc.
- **Relying** on DBAs for detailed database insights can delay risk detection and response.

Bridging the Gap: Security vs. Operations

Can AI Simplify Oracle DB Security for All Stakeholders?

The Question:

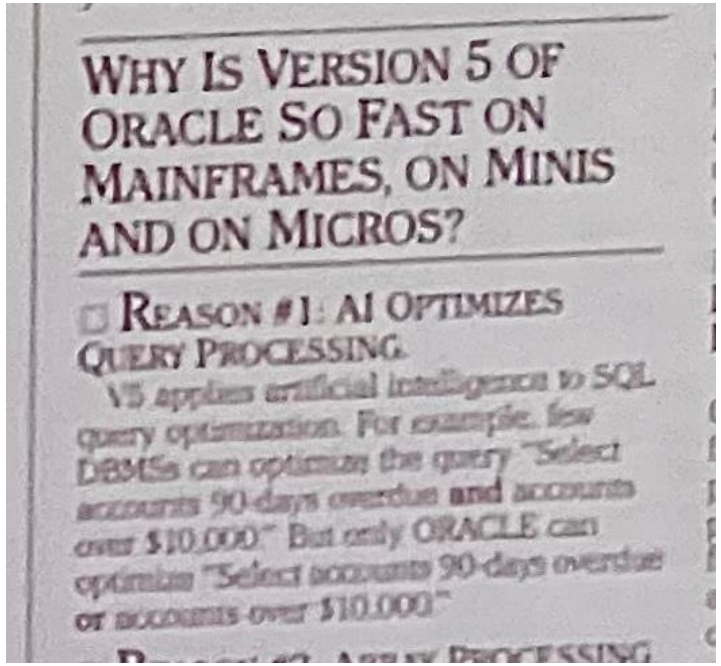
- What if security monitoring and analysis could be simplified?
- Could AI handle tasks like privilege analysis, auditing, and anomaly detection?
- How much more efficient could DBAs and security teams be with AI tools?



Oracle AI

Something new for Oracle Database?

- Newspaper advertisement for **Oracle 5**
- Mentioning…
  - **Reason #1**
    AI Optimizes Query Processing



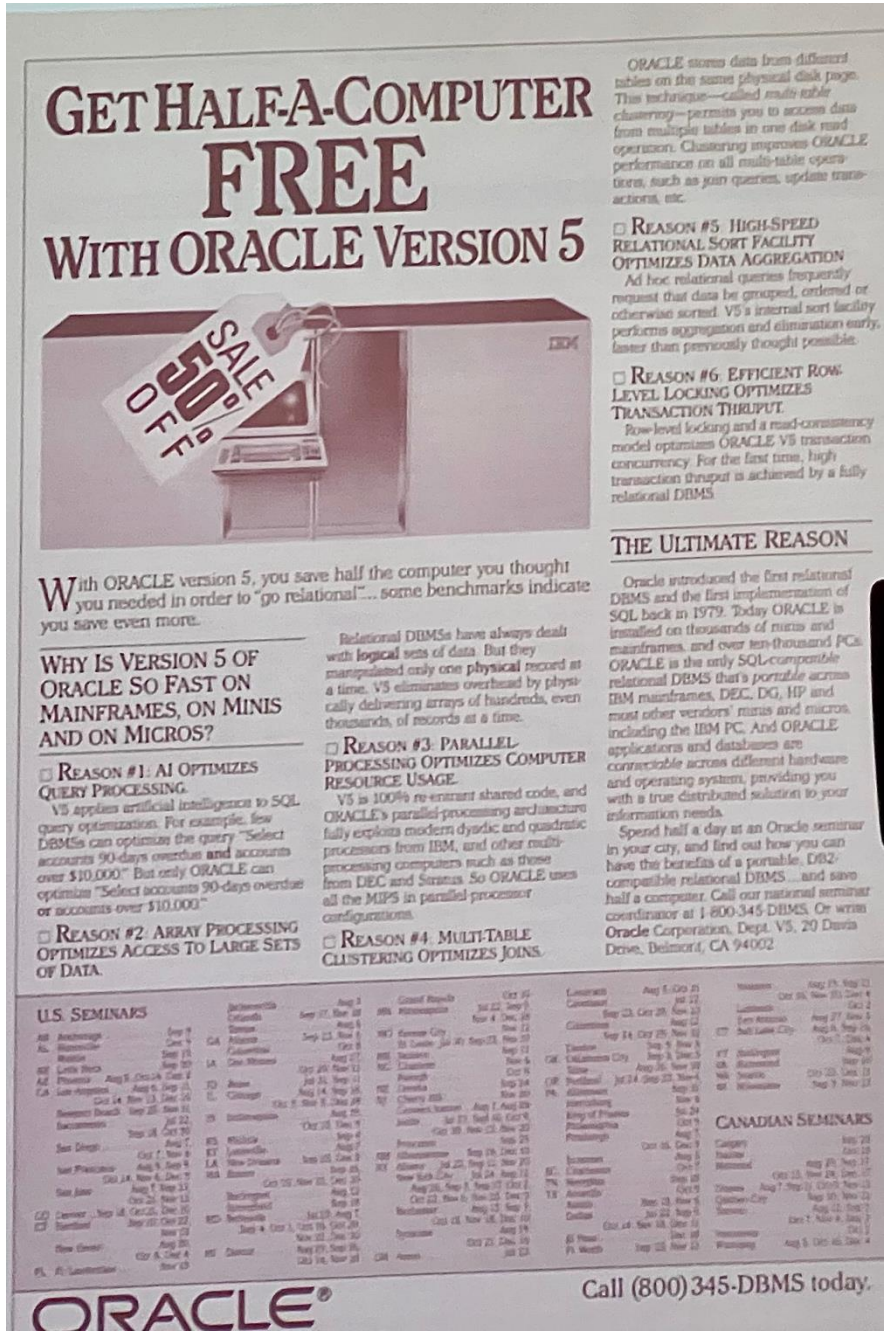
WHY IS VERSION 5 OF ORACLE SO FAST ON MAINFRAMES, ON MINIS AND ON MICROS?

☐ REASON #1: AI OPTIMIZES QUERY PROCESSING.

V5 applies artificial intelligence to SQL query optimization. For example, few DBMSs can optimize the query "Select accounts 90-days overdue and accounts over $10,000." But only ORACLE can optimize "Select accounts 90-days overdue or accounts over $10,000."

☐ REASON #2: ARRAY PROCESSING

Found in a presentation by Markus Michalewicz



GET HALF-A-COMPUTER FREE WITH ORACLE VERSION 5

With ORACLE version 5, you save half the computer you thought you needed in order to "go relational"... some benchmarks indicate you save even more.

WHY IS VERSION 5 OF ORACLE SO FAST ON MAINFRAMES, ON MINIS AND ON MICROS?

☐ REASON #1: AI OPTIMIZES QUERY PROCESSING.

V5 applies artificial intelligence to SQL query optimization. For example, few DBMSs can optimize the query "Select accounts 90-days overdue and accounts over $10,000." But only ORACLE can optimize "Select accounts 90-days overdue or accounts over $10,000."

☐ REASON #2: ARRAY PROCESSING OPTIMIZES ACCESS TO LARGE SETS OF DATA.

Relational DBMSs have always dealt with **logical** sets of data. But they manipulated only one **physical** record at a time. V5 eliminates overhead by physically delivering arrays of hundreds, even thousands, of records at a time.

☐ REASON #3: PARALLEL PROCESSING OPTIMIZES COMPUTER RESOURCE USAGE.

V5 is 100% re-entrant shared code, and ORACLE's parallel-processing architecture fully exploits modern dyadic and quadratic processors from IBM, and other multi-processing computers such as those from DEC and Stratus. So ORACLE uses all the MIPS in parallel processor configurations.

☐ REASON #4: MULTI-TABLE CLUSTERING OPTIMIZES JOINS.

ORACLE stores data from different tables on the same physical disk page. This technique—called *multi-table clustering*—permits you to access data from multiple tables in one disk read operation. Clustering improves ORACLE performance on all multi-table operations, such as join queries, update transactions, etc.

☐ REASON #5: HIGH-SPEED RELATIONAL SORT FACILITY OPTIMIZES DATA AGGREGATION

Ad hoc relational queries frequently request that data be grouped, ordered or otherwise sorted. V5's internal sort facility performs aggregation and elimination early, faster than previously thought possible.

☐ REASON #6: EFFICIENT ROW-LEVEL LOCKING OPTIMIZES TRANSACTION THRUPUT.

Row-level locking and a read-consistency model optimizes ORACLE V5 transaction concurrency. For the first time, high transaction thruput is achieved by a fully relational DBMS.

THE ULTIMATE REASON

Oracle introduced the first relational DBMS and the first implementation of SQL back in 1979. Today ORACLE is installed on thousands of minis and mainframes, and over ten-thousand PCs. ORACLE is the only SQL-compatible relational DBMS that's *portable* across IBM mainframes, DEC, DG, HP and most other vendors' minis and micros, including the IBM PC. And ORACLE applications and databases are *connectable* across different hardware and operating system, providing you with a true distributed solution to your information needs.

Spend half a day at an Oracle seminar in your city, and find out how you can have the benefits of a portable, DB2-compatible relational DBMS... and save half a computer. Call our national seminar coordinator at 1-800-345-DBMS. Or write **Oracle** Corporation, Dept. V5, 20 Davis Drive, Belmont, CA 94002

U.S. SEMINARS

CANADIAN SEMINARS

ORACLE®

Call (800) 345-DBMS today.

2

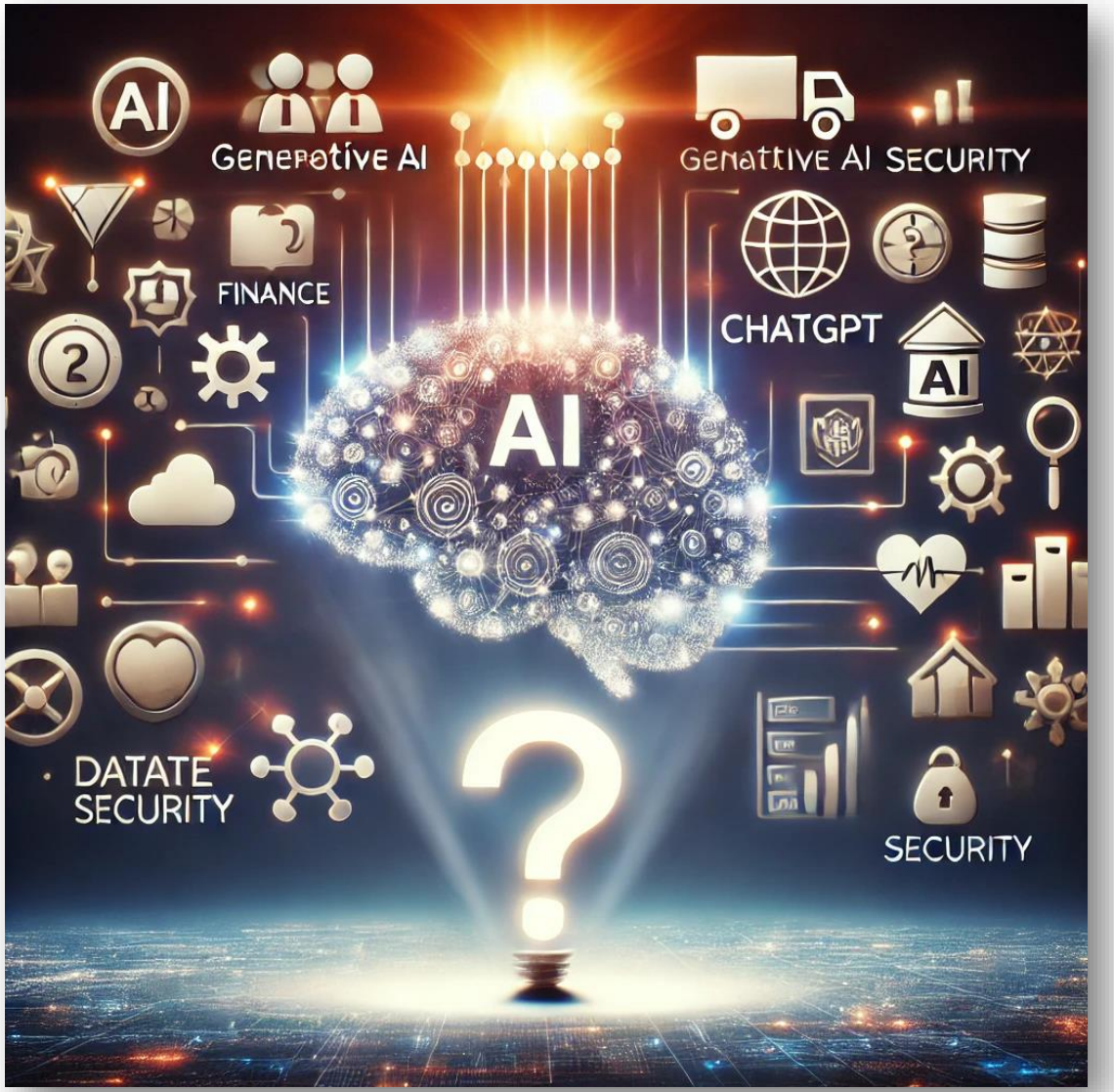
AI Concept & First Steps

Initial explorations and trials with AI for DB security.

AI in the Spotlight

Why Not Apply It to Database Security?

- **Generative AI (GenAI)**, **LLMs**, and **ChatGPT** are transforming industries.
- The question is:
  - *Can we leverage AI to simplify complex security activities?*



Use Case 1: Creating Security Configurations

Can AI Help Build Secure Code?

Scenario:

- Need to create a **password verify function** for database security.

Goal:

- Use AI to quickly generate the required code and streamline the process.

Demo:

- Showcasing AI (ChatGPT) generating the **password verify function** code.

```
create a password verify function for Oracle including the following checks for upper / lower case, min 1 digit, min 1 special character and a string distance of 5 characters, name the function soug_test_pvf
```

Use Case 1: AI-Generated Code

Conclusion: AI Assistance, but Not Perfect

Conclusion:

- AI-generated code is **not always perfect**.
- Requires validation and security expertise.
- You need to **know what you're doing** before applying it.

Use Case 2: Analyzing Code & Errors

Can AI Simplify Debugging and Analysis?

Scenario:

- Need to analyze and debug a **password verify function**.

Goal:

- Use AI to help **analyze code**, understand potential issues, and assist with documentation.

Demo:

- Showcasing AI (ChatGPT) analyzing the password verify function.
- Analysis: AI explains the code, highlights any issues, and offers solutions.

```
create a password verify function for Oracle including the following checks for upper / lower case, min 1 digit, min 1 special character and a string distance of 5 characters, name the function soug_test_pvf
```

Use Case 2: AI-Assisted Analysis

Conclusion: AI as a Documentation and Learning Aid

Conclusion:

- AI simplifies **documentation** and **code analysis**.
- Helpful when your **knowledge is limited**.
- AI bridges the gap but still requires a basic **understanding**.

3

Natural Language in Action

Demos showing privilege and audit analysis using natural language queries.

Natural Language in Action

Introducing Oracle Natural Query Language

Oracle Natural Query Language:

- Enables database interaction through **natural language queries**.
- Integration with **Large Language Models (LLMs)** for enhanced query understanding.

Potential for Simplifying Security:

- Translate complex SQL queries into **natural language**.
- Integrate with LLMs like **OpenAI**, **Cohere**, **Azure**, **OCI**, and **Google**.
- Empowers the security team to analyse data without in-depth SQL knowledge.

Basic Requirements

What You Need to Get Started

Cloud Environment:

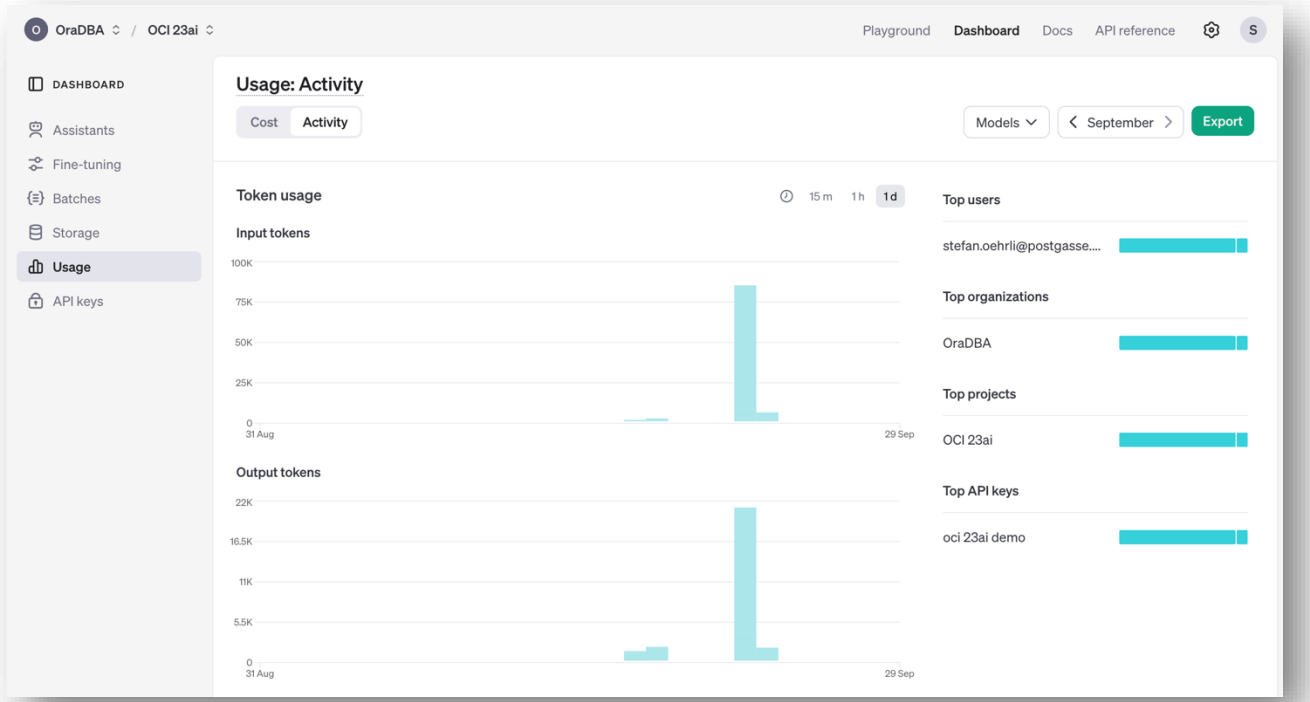
- Oracle 23ai cloud setup.
- Oracle Autonomous Database

Supported LLMs:

- Integration with OpenAI, Cohere, Azure, OCI, Google.
- https://platform.openai.com

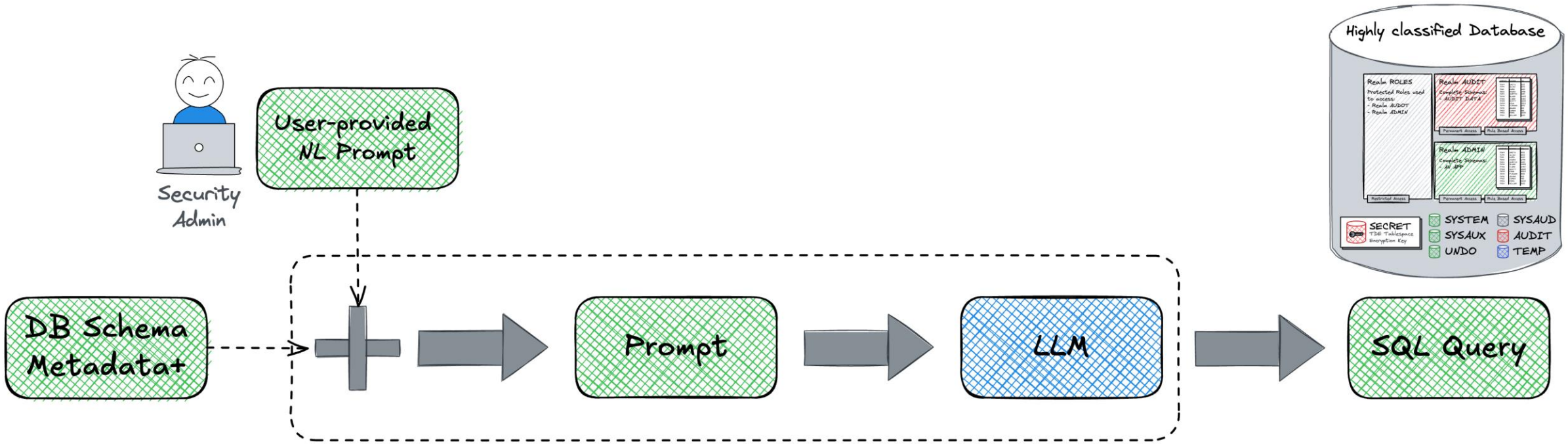
Database User Requirements:

- Corresponding DB user with **AI profiles**.
- Set up **ACLs** (Access Control Lists) for AI access.



Architecture Overview

How Natural Language Queries Work with Oracle



Demo Use Case 1: Privilege Analysis

Using Natural Language to Analyze Privileges

- **Step 1:** Configure a user for AI with privileges and ACLs.

```
BEGIN
    DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(
         host => 'api.openai.com',
         ace  => xs$ace_type(privilege_list => xs$name_list('http'),
                             principal_name => 'OEHRLI2',
                             principal_type => xs_acl.ptype_db));
END;
/
```

- **Step 2:** Create credentials for AI interaction.

```
BEGIN
    dbms_cloud.create_credential(
        credential_name => 'OpenAI_oci23ai',
        username        => 'stefan.oehrli@postgasse.ch',
        password        => 'sk-proj-08bxQiiZ2cruLkgm9cBq_...');
END;
/
```

Demo Use Case 1: Privilege Analysis

Using Natural Language to Analyze Privileges

- **Step 3:** Create an AI profile for the user.

```
BEGIN
    dbms_cloud_ai.create_profile(
        profile_name    => 'SECPRIV_AI',
        attributes      => '{"provider": "openai",
                             "model": "gpt-4",
                             "credential_name": "OpenAI_oci23ai",
                             "object_list": [{"owner": "SYS", "name": "DBA_ROLES"},
                                             {"owner": "SYS", "name": "DBA_TAB_PRIVS"},
                                             {"owner": "SYS", "name": "DBA_ROLE_PRIVS"},
                                             {"owner": "SYS", "name": "DBA_SYS_PRIVS"}]}');
END;
/
```

- **Step 4:** Set the profile and run the natural language query to analyze privileges.

```
EXEC dbms_cloud_ai.set_profile(profile_name => 'SECPRIV_AI');
SELECT AI list roles not maintained by oracle;
```

Demo Conclusion

Key Takeaways from Privilege Analysis

Efficient Privilege Analysis:

- Simplifies the complexity of privilege reviews.

Human-Friendly Queries:

- Removes the need for complex SQL.

Good Basis for Browsing:

- Useful for quick browsing of database content.

Challenges in Finding the Correct Prompt:

- It can be tricky to phrase the natural language prompt correctly for the intended outcome.

Not Necessarily **Reproducible**:

- Results may vary slightly with different wording of prompts.

Limitations:

- Cannot handle complex subqueries or recursive queries effectively.

Demo Use Case 2: Audit Trail Analysis

Using Natural Language to Review Audit Data

- Set up everything for AI interaction (similar to use case 1).
- No Data when query the audit trail

```
Sorry, unfortunately a valid SELECT statement could not be generated for your natural language prompt.
Here is some more information to help you further:

To find out how many unified audit events exist, you can use the following Oracle SQL query:

SELECT COUNT(*) AS "Total Audit Events"
FROM "SYS"."UNIFIED_AUDIT_TRAIL""
```

- Create a temporary table for analysis.

```
CREATE TABLE unified_audit_trail
    AS
        SELECT
            *
        FROM
            audsys.unified_audit_trail;
```

Demo Use Case 2: Audit Trail Analysis

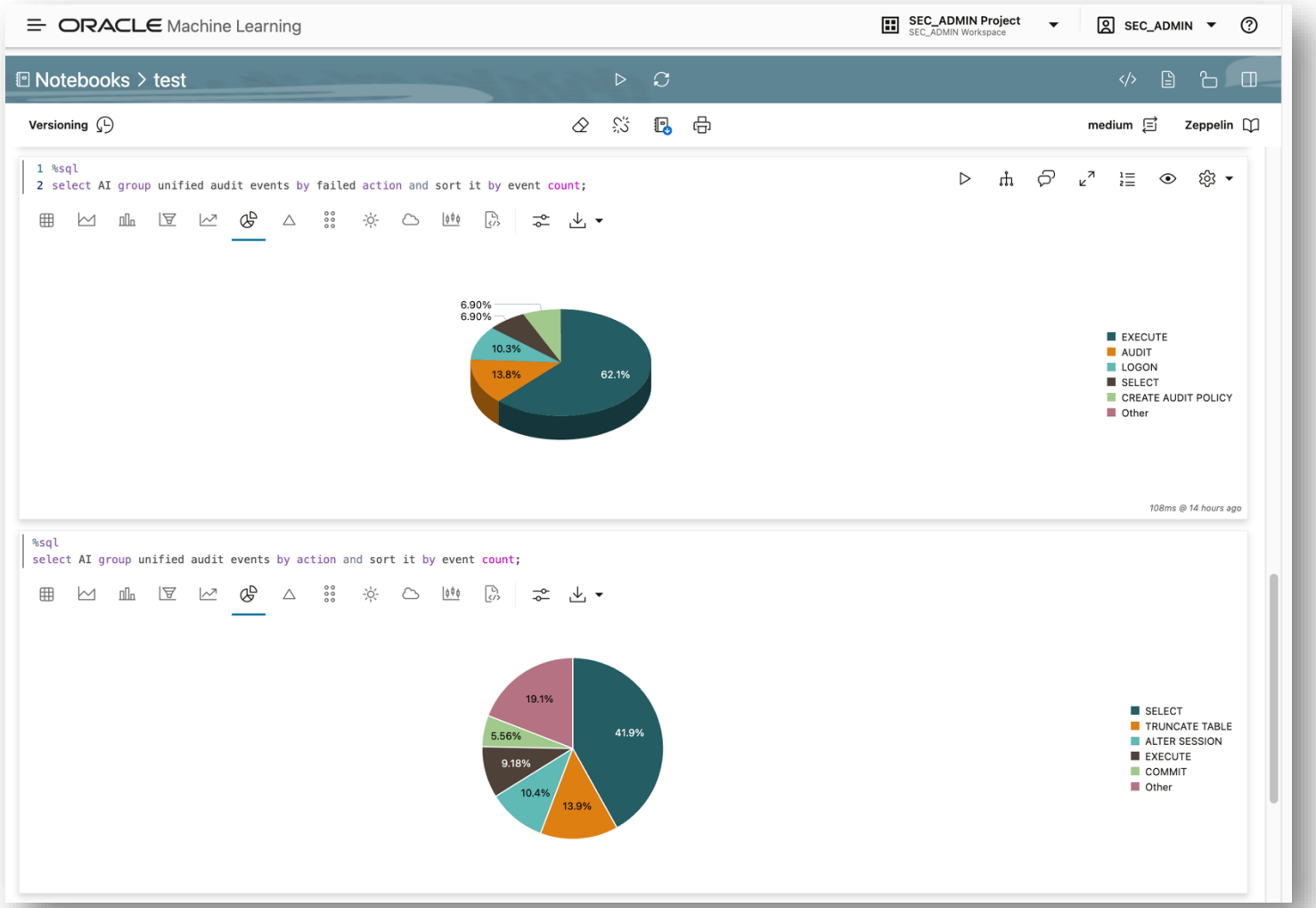
Using Natural Language to Review Audit Data

- Recreate the AI profile for the new table
- Run the **natural language query** to analyze the audit trail.

```
select AI what is latest audit event in SEC_ADMIN.UNIFIED_AUDIT_TRAIL table;
select AI what is the user host with the most unified audit events;
select AI list all unified audit events of dbusername SEC_ADMIN order by EVENT_TIMESTAMP;
```

Demo Use Case 2: Audit Trail Analysis

OML Notebooks to query the data



Challenges in Audit Trail Analysis

Issues Faced in Natural Language Query Setup

Direct Grants Missing:

- Somehow SELECT AI does not work if object is not granted directly

Temp Table for Simulation:

- Simplifies audit analysis but introduces temporary complexities.
- In particular additional storage requirements for audit trail

Natural Language interesting approach to start the Process:

- Once configured, simple analysis does work
- It can be tricky to phrase the natural language prompt correctly for the intended outcome.

Sum Up: Issues and Challenges

Potential and Limitations of Natural Language Queries

Configuration Challenges:

- Proper setup for AI interaction is crucial.

Natural Language:

- Reduces complexity in privilege and audit analysis.
- It can be tricky to phrase the natural language prompt correctly for the intended outcome.
- Cumbersome to find issues when SELECT AI does not work

Potential for Broader Use:

- Could be expanded to handle more complex security tasks in the future.

4

Future Ideas

A brief look at potential applications of machine learning in security.

Future Ideas: Machine Learning in Security

Exploring the Potential of Oracle Machine Learning for Audit Analysis

Oracle Machine Learning for Audit Data

- Leverage Oracle Machine Learning (OML) to analyze audit trails.

Analyzing Patterns

- Understand usual/regular user activity and access patterns.

Identifying Anomalies

- Use ML to detect irregularities in behavior and data access.

Traffic Light System

- **Green:** Normal activity
- **Yellow:** Unusual activity (e.g., increased administrative tasks)
- **Red:** Potential security breach (e.g., exceeded privilege use, password guessing, attacks)

Currently just an idea...

5

One More Thing

A sneak peek at a potential upcoming Oracle feature.

Simplifying Database Security

Fewer Complex Queries, More Actionable Insights

What if…

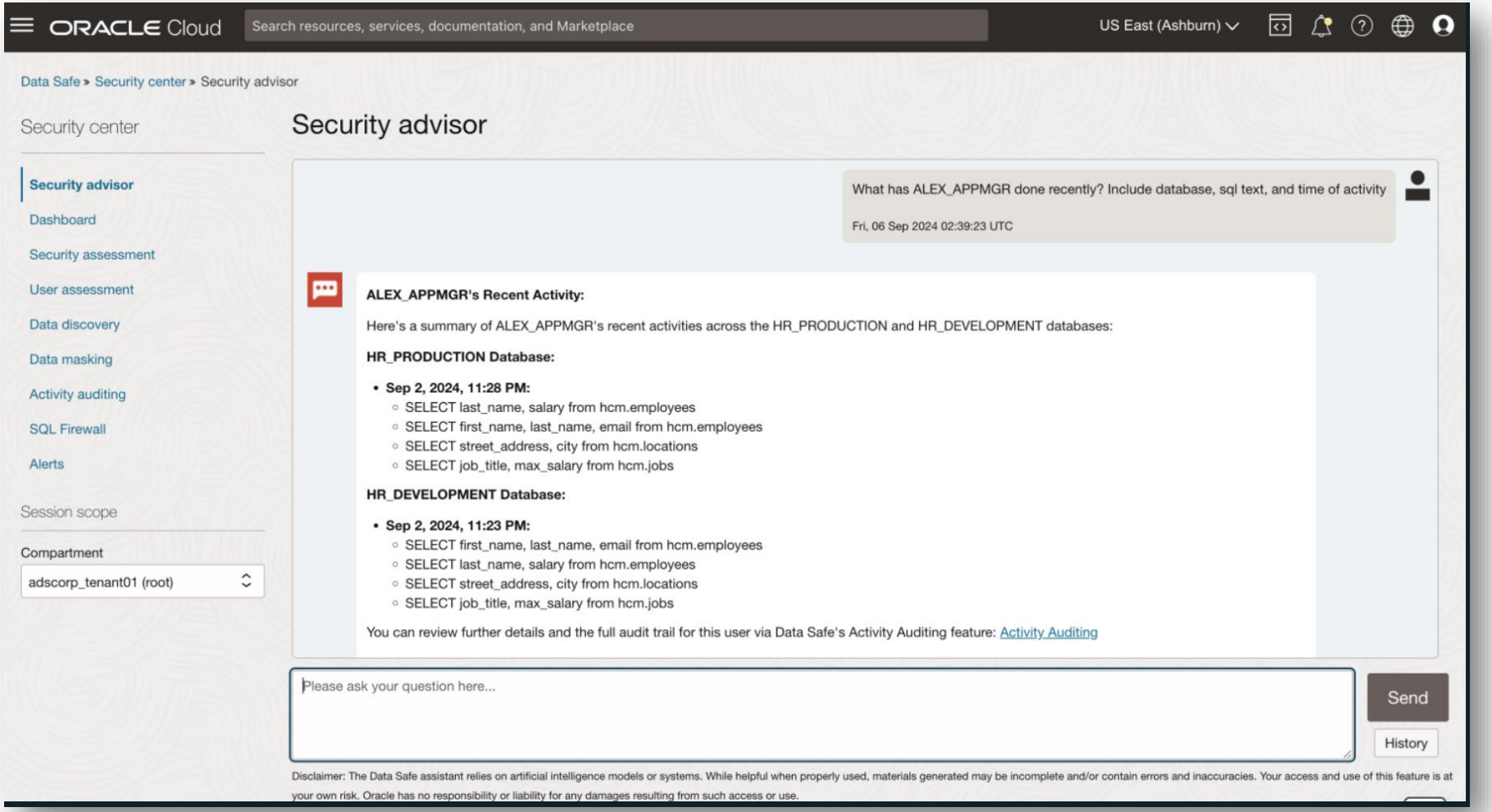
- You could instantly know the security status of your database?
- Get insights into unusual or risky activity inside your DB?
- Simplify the work of a security operator or analyst?
- All this could be achieved without the need for complex SQL queries or in-depth technical know-how?

A Preview

- A future feature currently in highly alpha state
- Still uncertain on final capabilities and release dates
- All information subject to change

Data Safe – Security Advisory

Preview of Future Data Safe Feature – Highly Experimental, Subject to Change



6

Summary & Conclusion

Key takeaways and final thoughts.

Data Safe for Security Enhancements

Leverage Data Safe for Comprehensive Security Management

The use of Data Safe for ADB is straight forward

Security Assessments

- Identify vulnerabilities and misconfigurations.

Audit Configuration and Reporting

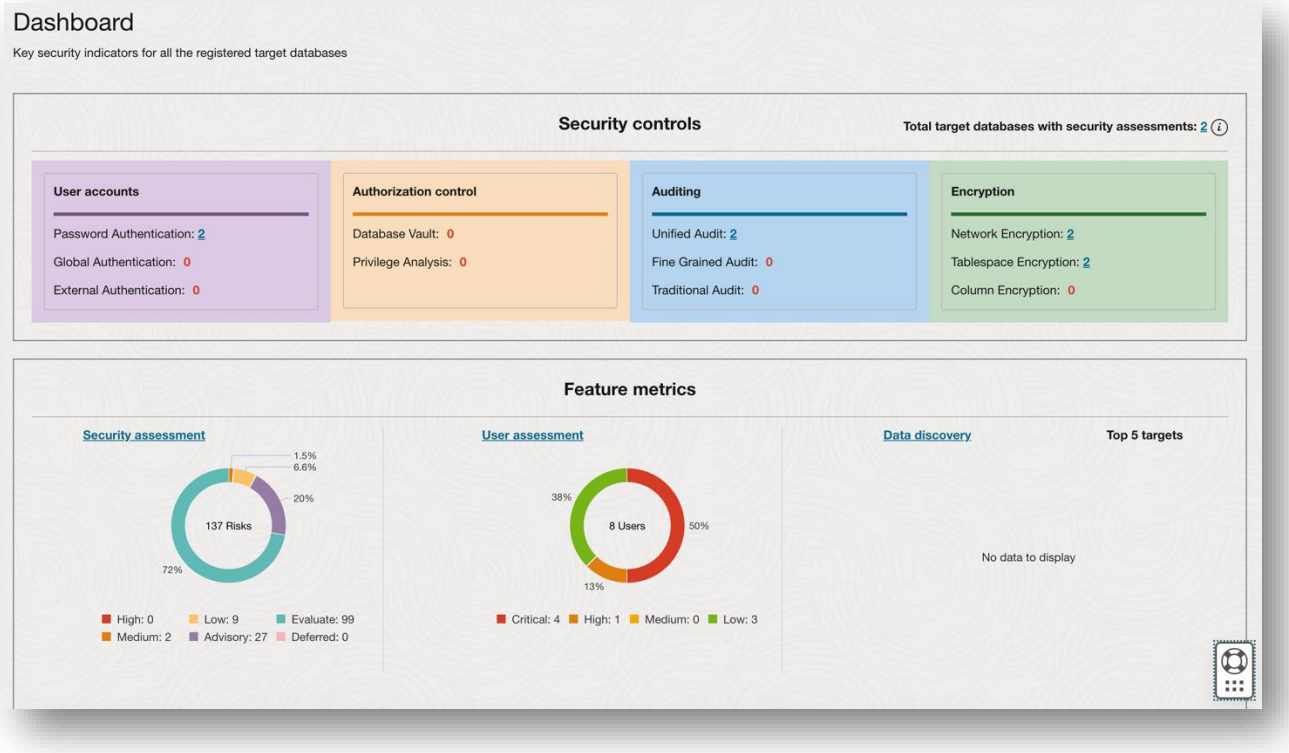
- Automate audit setup and reporting to ensure compliance.

User Assessments

- Monitor and analyze user access patterns.

Sensitive Data Discovery

- Identify and protect sensitive data automatically.



Infrastructure Protection with Cloud Guard

Extend Security to OCI with Cloud Guard

Cloud Guard

- Monitor and remediate OCI infrastructure threats.

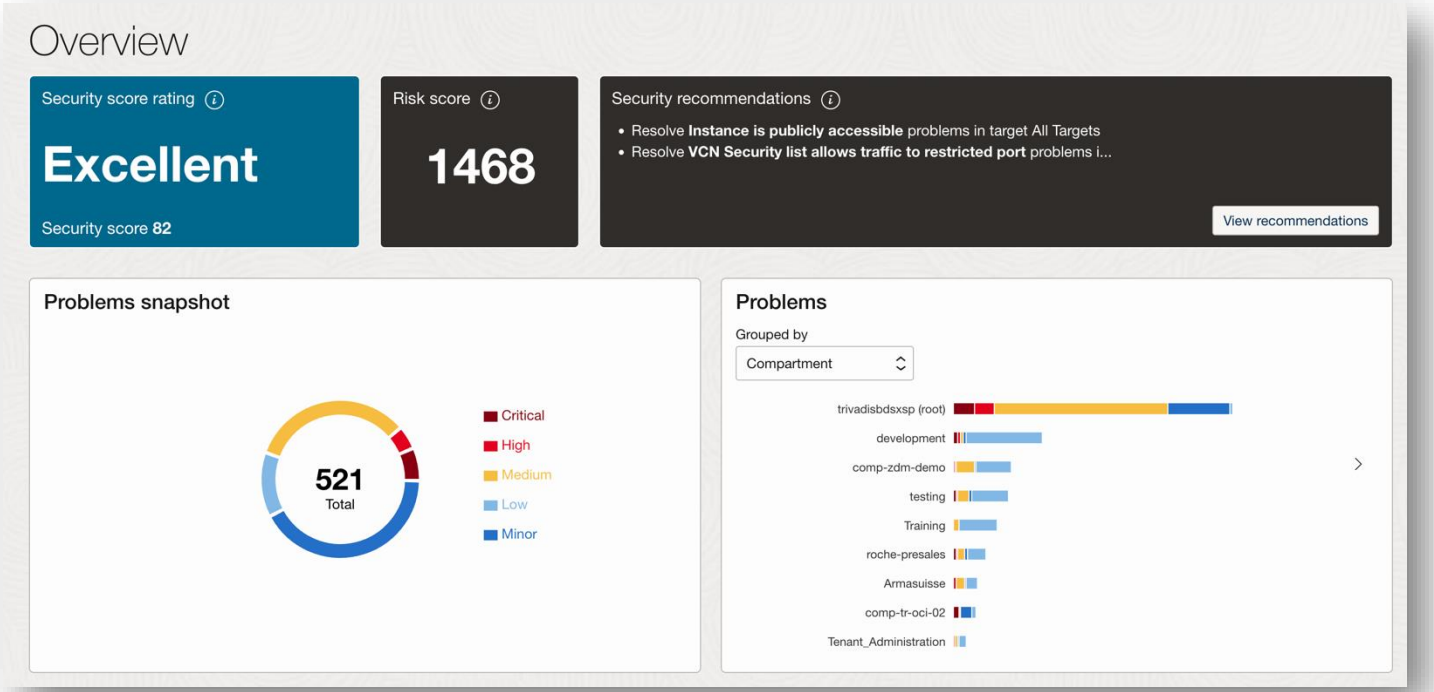
Automated Risk Detection

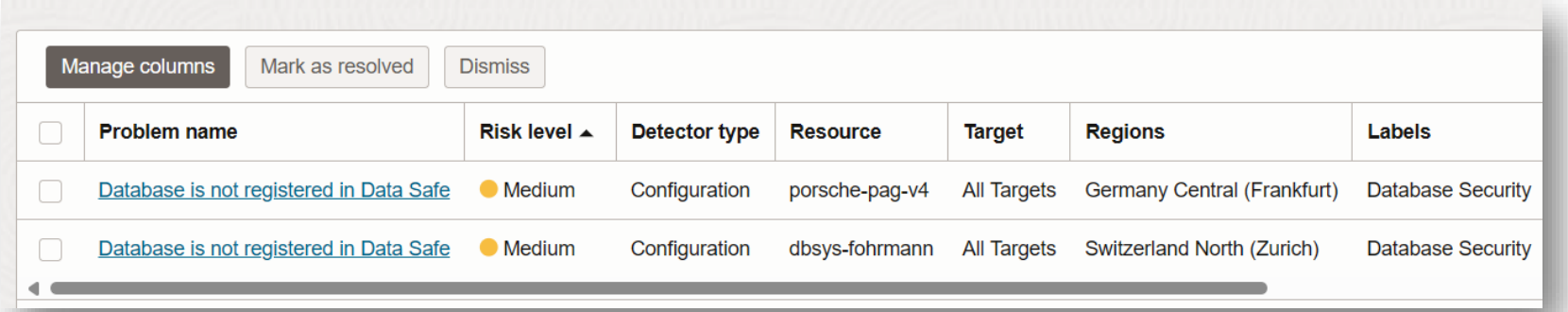
- Identify suspicious activity across OCI resources.

Threat Remediation

- Automatically apply fixes or alert administrators.

Example: Database has an old version, is public accessible, not registered in Data Safe

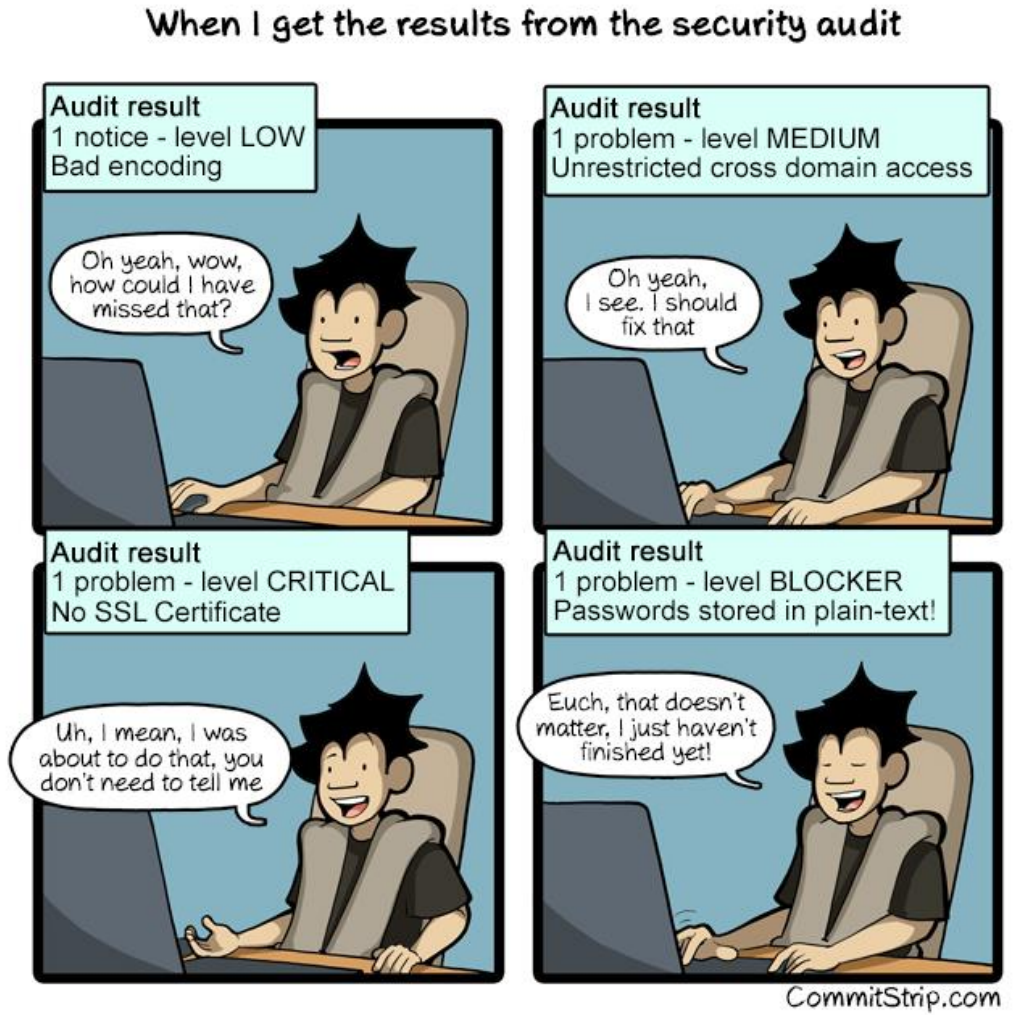




Conclusion

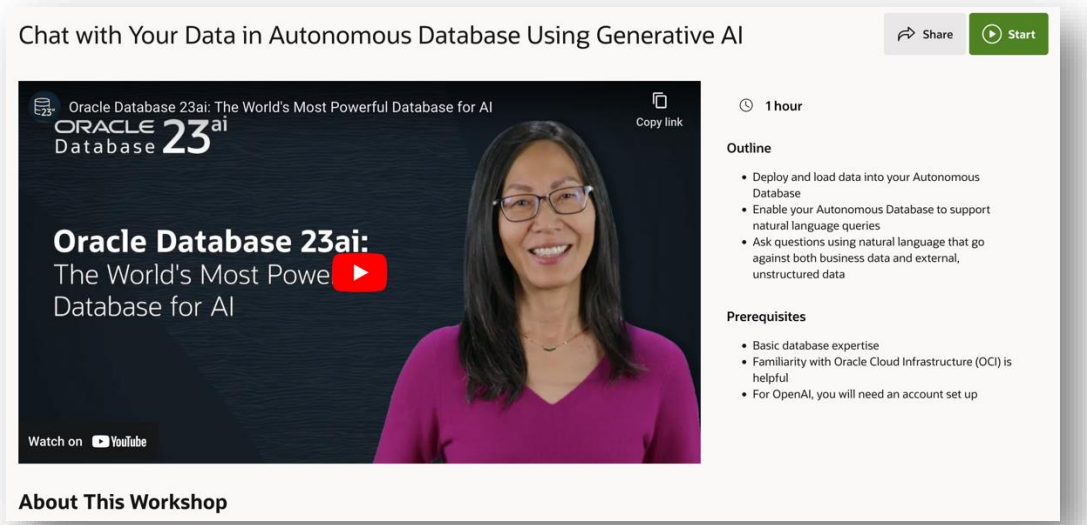
GenAI, Natural Query Language,… Do they simplify DB Security?

- AI **holds promise** for Oracle DB security
- **Early stages**, primarily cloud-based.
- **May simplifies** tasks (privilege and audit analysis).
- Security expertise **remains essential**.
- Technical challenges ahead; not fully mature.
- **Defined reports**, SQL queries, and tools like **Data Safe** still deliver faster, more accurate, and reliable results.
- Exciting **future opportunities**, but progress will take time.



Oracle LiveLabs – DB Security

Trial the ADB and GenAI in just a few minutes…



Chat with Your Data in ADB – ID 3875

- Deploy and load data into your ADB
- Enable your ADB to support natural language queries
- Ask questions using natural language
- https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=3831

AI is promising for Oracle DB security but is still at an early stage and only available in the cloud.

In-depth security expertise is still the key to success.

Thank You