Co-funded by
the European Union

MERIT

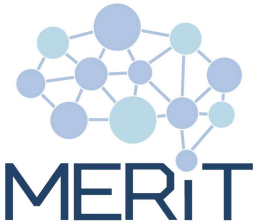
Database Security

Advanced Threats in Database Environments

Advanced Threats in Database Environments

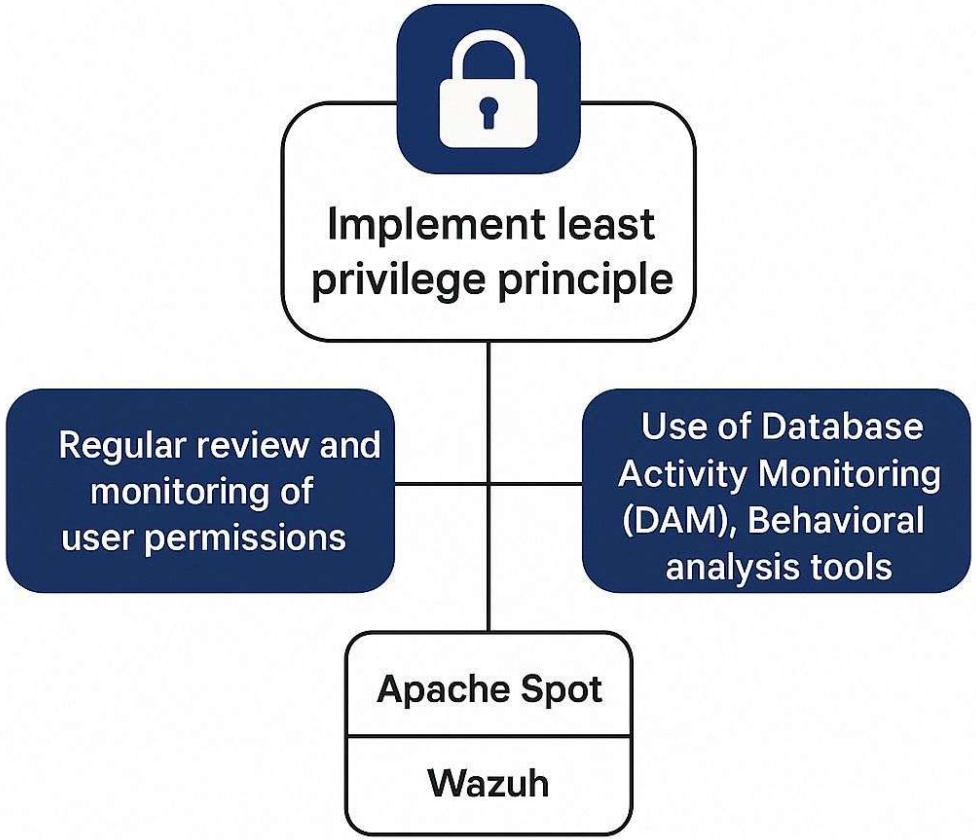
- Databases store critical, sensitive data, making them prime targets.
- Traditional security mechanisms may fail against sophisticated threats.
- Key advanced threats:
  - ✔ Insider Threats.
  - ✔ Data exfiltration.
  - ✔ Anomaly detection.
  - ✔ Honeypots.

Insider Threats and Privilege Abuse

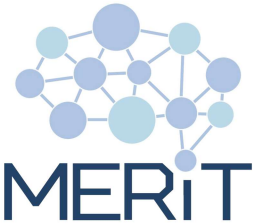


- Threats originating from within the organization.
- Employees or contractors with legitimate access may misuse privileges.
- Types:
  - ✔ Excessive privileges.
  - ✔ misuse of admin/root access.
  - ✔ unauthorized access/modification.

Mitigating Insider Threats



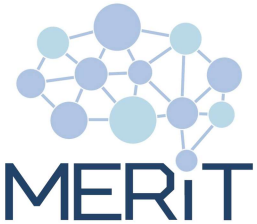
Mitigating Insider Threats



This table outlines key controls to ensure a secure and well-monitored database environment through least privilege, continuous auditing, and behavioral monitoring.

Permission Type	Auditable Actions	Recommended Controls	Frequency
Administrative Access	Login/logout, configuration changes	DAM, behavioral monitoring, multi-factor authentication (MFA)	Continuous, Real-time
Schema/Table Modification	Creation, alteration, deletion	DAM monitoring, regular privilege reviews	Weekly
Access to Sensitive Data	Read, modify, delete, export	DAM monitoring, behavioral analysis	Continuous, Daily
Execution of Critical Queries	Queries impacting performance or security	DAM monitoring, anomaly detection alerts	Continuous, Real-time
Backup/Restore Permissions	Creation, restoration, deletion	DAM monitoring, role-based restrictions	Monthly
Data Transfer or Export	Mass data export, remote transfers	Behavioral analysis, DLP integrated with DAM	Continuous, Immediate alerts
Audit or Log Changes	Modification of audit records	DAM monitoring, independent audits	Continuous, Daily
User Creation and Privilege Assignment	User additions, deletions, privilege changes	Regular privilege reviews, DAM activity monitoring	Weekly

Data Exfiltration and Covert Channels



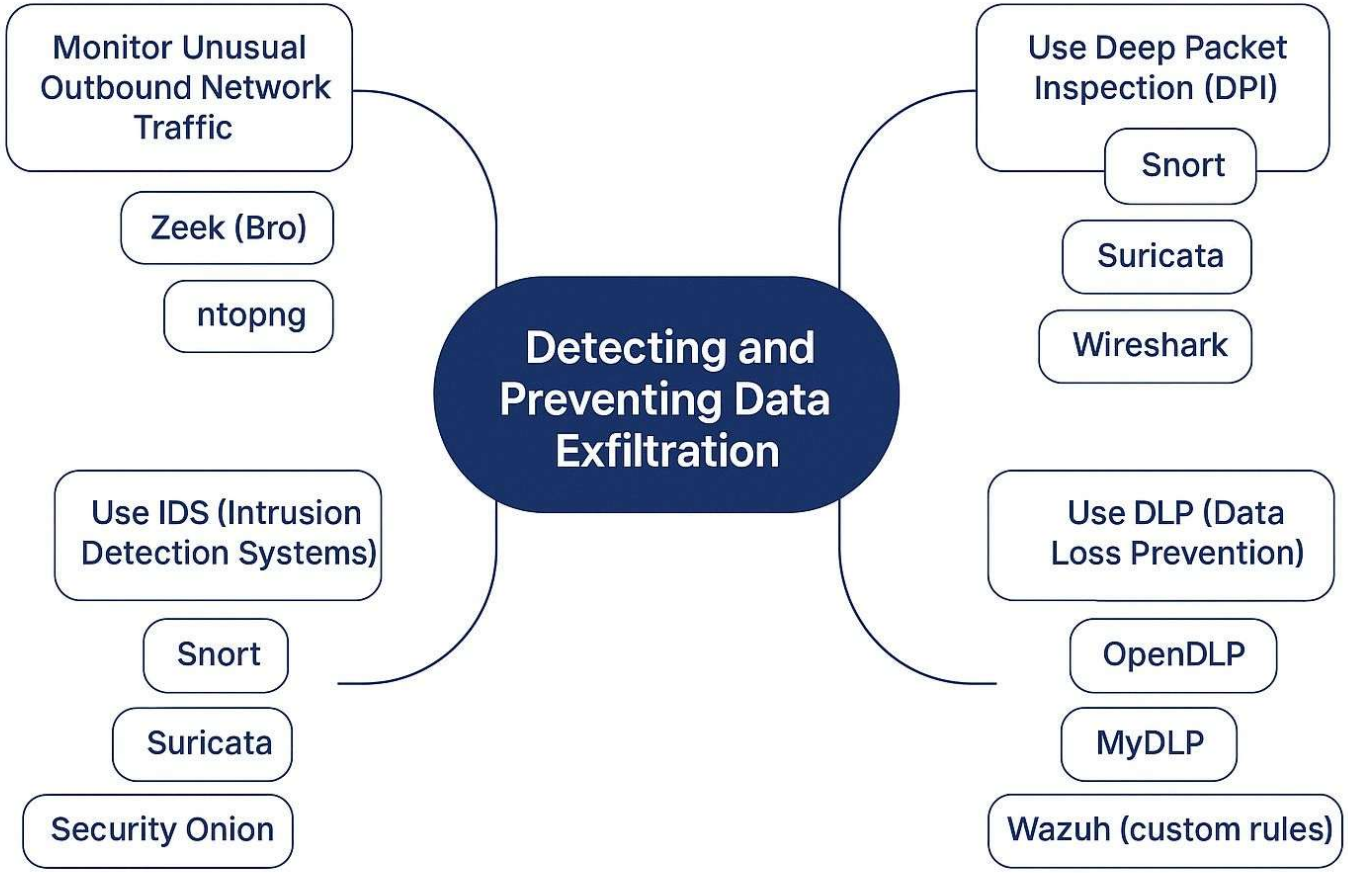
🟦 Data Exfiltration Techniques

- **File exports**
  Direct export of data to local or remote files, often using SQL commands or administrative tools.
- **Encrypted channels**
  Use of encrypted channels (such as HTTPS, VPN, or SSL/TLS) to conceal the transfer of stolen data.
- **DNS tunneling**
  Encapsulation of data within DNS requests/responses to bypass firewalls and network controls.
- **SQL injection**
  Injection of malicious commands into SQL queries to access, modify, or extract data without authorization.

🟦 Covert Channels

- **Storage channels**
  Hiding data inside unused fields or legitimate database structures (e.g., comments, metadata).
- **Timing channels**
  Transmitting data by manipulating the timing between events (e.g., faster or slower responses encode bits of information).

Detection Techniques for Data Exfiltration



Anomaly Detection in Databases

🟦 **Identifies Deviations from Normal Behaviors**

What it is:
Detects activity that significantly deviates from the usual user or system patterns, helping to uncover insider threats or novel attacks.

🛠️ Techniques

Machine Learning Algorithms

Automatically model normal behavior and detect outliers without predefined rules.

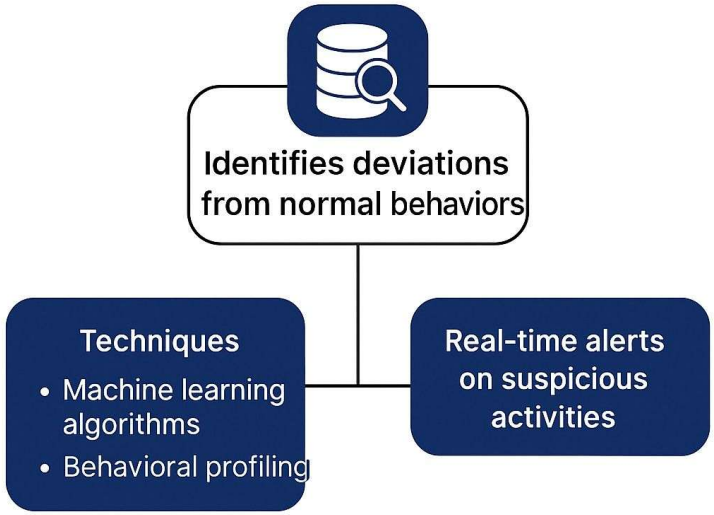
Behavioral Profiling

Tracks and builds patterns based on user roles, access times, query types, and resource usage.

🚨 Real-Time Alerts on Suspicious ActivitiesTriggers immediate notifications when deviations from expected behavior are detected, such as:

- ✔ Unusual login time or location
- ✔ Access to uncommon tables or large volumes
- ✔ Query anomalies or privilege escalations

Anomaly Detection in Databases



Tool	Type	Notes
Apache Spot	Open Source, ML-based	Detects anomalies using big data pipelines
ELK + Machine Learning (X-Pack)	Commercial / Open Hybrid	Detects unusual patterns in logs
Splunk (with UEBA)	Commercial	Powerful analytics with user behavior profiling
Wazuh (with custom rules)	Open Source	Limited anomaly detection via rule logic

Honeypots and Deception Techniques

🛡️ Decoy Databases to Detect Attackers Early

What it is:

Simulated databases designed to look real and attract malicious users.

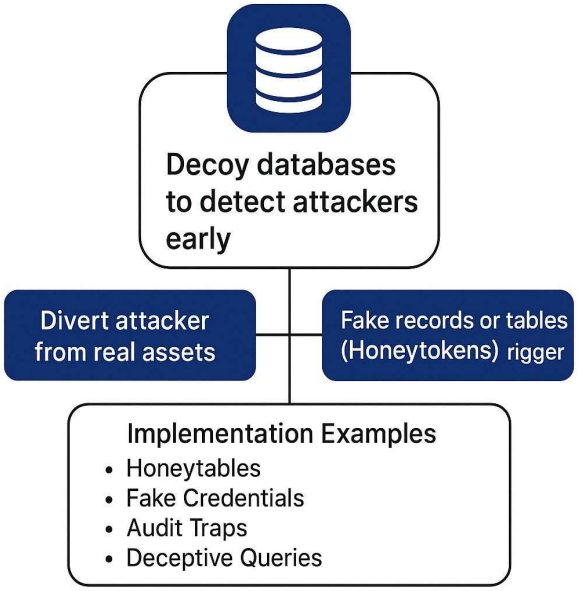
🎯 Goals of Deception

- **Divert Attacker from Real Assets**

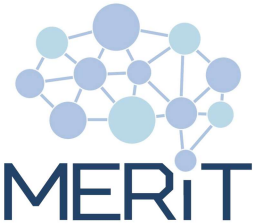
Attackers waste time on fake data while alerts are triggered silently.

- **Trigger Alerts Using Fake Records (Honeytokens)**

Embedded fake tables, users, or credentials alert defenders when accessed.



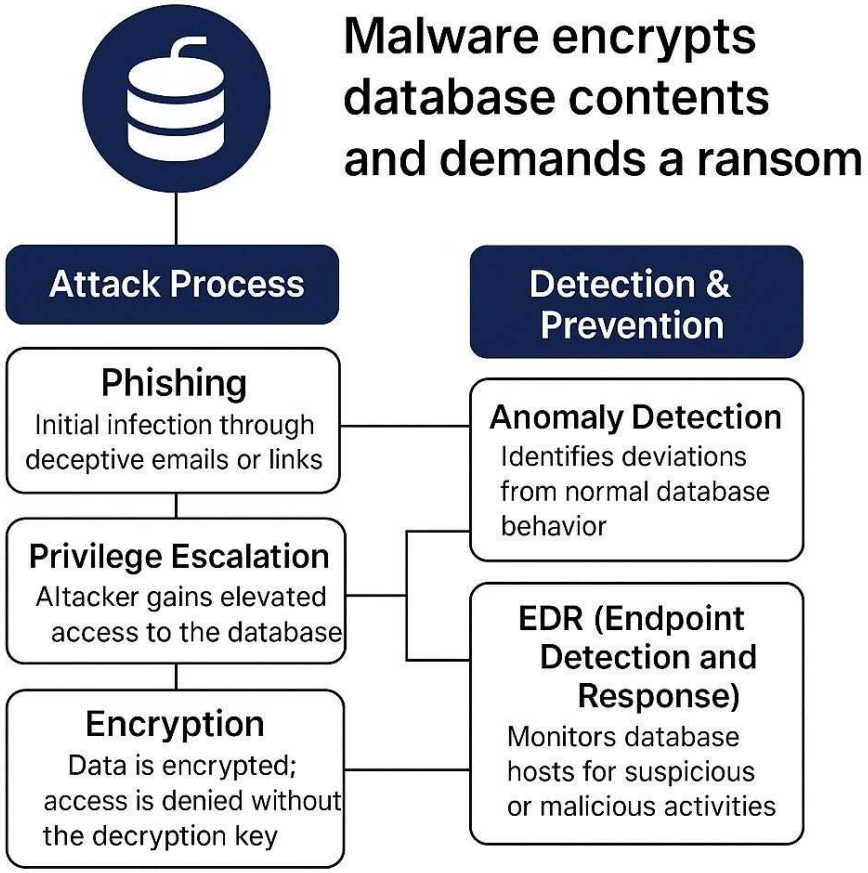
Integrating Honeypots into Security



🔧 Implementation Examples

Strategy	Description
Honeytables	Tables filled with plausible but fake data.
Fake Credentials	Fake users with logs and permissions that bait intruders.
Audit Traps	Queries or access attempts to certain tables raise alarms.
Deceptive Queries	Logs generated by fake queries reveal attacker behavior.

Database Ransomware Attacks



Database Ransomware Attacks

🦠 What is it?
Malware encrypts database contents and demands a ransom.The attacker denies access to critical data until payment is made.

🧬 Attack Process
Phishing
Initial infection through deceptive emails or links.
Privilege Escalation
The attacker gains elevated access to the database system.
Encryption
Data is encrypted; access is denied without the decryption key.

🚨 Detection & Prevention

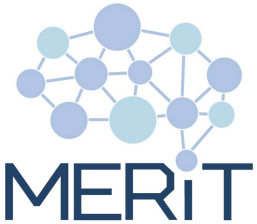
Technique	Description
Anomaly Detection	Identifies unusual database activity or access patterns.
EDR (Endpoint Detection and Response)	Monitors and contains suspicious host behavior.

Mitigating Database Ransomware

Protection Measures

- **Secure Database Backups**
  Maintain offline and immutable backups.
- **Privilege Limitation**
  Apply the principle of least privilege to user roles.
- **Multi-Factor Authentication (MFA)**
  Prevent unauthorized administrative access.

Summary



Key Topics Covered

- **Insider Threats & Privilege Abuse**
  → Misuse of legitimate access by internal actors.
- **Data Exfiltration & Covert Channels**
  → Hidden extraction via file exports, DNS tunneling, SQL injection, etc.
- **Anomaly Detection**
  → Behavioral profiling & machine learning to detect suspicious activity.
- **Honeypots & Deception**
  → Fake databases and honeytokens to detect and divert attackers.
- **Database Ransomware Attacks**
  → Encryption of data for ransom; prevention via MFA, backups, and EDR.