An Open Source DBMS, Employs Role-Based Access Control

Detect insider attacks

Phases of operation

1- Training phase
- Create profiles for roles
- Use valid queries in the Audit Log
- Statistics collector process to report statistics during the DB operation
- Different ranges for information extraction: coarse, medium and fine

2- Detection phase
- Query should match profile of user's role
- Use naïve Bayes classifier
- Max. Aposteriori role for classification
- Response (currently): Drop Query

Screen-shots

- PostgreSQL
  - Open Source DBMS, Employs Role-Based Access Control
  - Detect insider attacks

- Anomaly Detection and Data Collection Hooks in PostgreSQL

- Profile creator process to report statistics during the DB operation
- Different ranges for information extraction: coarse, medium and fine

- Query should match profile of user's role
- Use naïve Bayes classifier
- Max. Aposteriori role for classification
- Response (currently): Drop Query