InsiderSecurity

Database Activity Monitor

Detect Unauthorized Access to your Data

How does **Database Activity Monitor** help you?

With data security regulations such as Singapore's PDPA and EU's GDPR, organisations increasingly need to keep the data in their databases safe.

Database Activity Monitor uses machine learning and smart cybersecurity algorithms to look for breaches in your databases.

Database Activity Monitor's users include government, healthcare institutions and other large enterprises today.

How is **Database Activity Monitor** Different?

Monitor does not require rules to be written/maintained, and significantly reduces the need for manual monitoring and analysis. This enables earlier and greater threat detection.

Monitor provides database activity monitoring that detects for:

1. Suspicious database administrator activity
2. Suspicious data access (data theft) in the database
3. Unusual network activity in the database server

Database Activity Monitor Detects

1.  **Unusual Login Behaviour**

2.  **Risky Administrator Commands**

3.  **Suspicious SQL Commands**

4.  **Unusual Data Access**

5.  **Suspicious Failed Queries**

6.  **Malicious network traffic in the server, beyond database traffic**

Database Activity Monitor Use Cases

1 

Database account credentials has been leaked or stolen

A hacker managed to gain access to a company network, and steal the database account credentials. When the hacker uses the stolen credentials, InsiderSecurity is able to detect the suspicious login activity, abnormal account actions and data theft.

2 

Database is accidentally left exposed to internet

A hacker who logins to an exposed database is detected as a login anomaly. Unusual SQL commands by this hacker are detected. Furthermore, via network behavior analytics, InsiderSecurity detects early port scanning attempts.

Database Activity Monitor Use Cases

3

Insider threat

An insider threat is a disgruntled employee that is authorized to access the database, but abuses his/her account. InsiderSecurity detects for suspicious data access, eg, accessing an unusually high number of records, or accessing tables that are not normally accessed.

4

Rogue administrator

The rogue database administrator is similar to an insider threat, except that it can do more damage as it has greater privileges. InsiderSecurity logs and analyses for risky privileged commands, eg drop table, add user etc. InsiderSecurity checks for suspicious login behavior. InsiderSecurity also detects unusual SQL queries by the administrator, eg, dumping data from database.

5

Vulnerable application that uses the database

A vulnerability or bug in the application allows a hacker to make unauthorised access to data stored in the database. This may be due to SQL injection or broken access control. When there is a deviation from the usual data access pattern, InsiderSecurity detects the anomaly. First-time access or permission errors in accessing the database are also detected.

6

Backdoor installed in database

A vulnerability in the server OS or database allows a hacker to install a malware/backdoor in the server. When the malware establish command-and-control (C2) connections back to the hacker, this C2 traffic is detected by InsiderSecurity via network behavior analytics. Note that InsiderSecurity does not rely on ip address blacklists to do such detection, as ip address blacklists are often outdated.

InsiderSecurity

+65 6270 4029

hello@insidersecurity.co

https://insidersecurity.co

81 Ayer Rajah Crescent, #03-48,
Singapore 139967