Database Activity Monitoring (DAM): How It Works, And What You Need To Know To Implement It

Charles Brodsky
April 2017

GIAC: GCIA, GCIH, GAWN, GSNA, GSEC, GLDR, GWAS

Goals of this presentation

- Explain what Database Activity Monitoring (DAM) is, how it works, and how it can be deployed
- Discuss the challenges, limitations, and 'gotchas' typically encountered
- Discuss how Imperva's SecureSphere product does this

Why do people audit databases?

- There are two primary reasons to audit a database
  - Recovery of Transactions
  - Investigation of Transactions

What is Database Activity Monitoring?

- Basically, it's tracking and auditing what someone did with their access/account
- Who would use this and why?

Database Activity Monitoring Fundamentals

- What are the types of monitoring?
  - Network Based (i.e. Network Sniffing)
  - Agent Based
- What are the Pros/Cons of each?
- How does this compare to "Native" Database Logging?

How do I know what to monitor?

- Typical first response: "Monitor Everything"
  - This doesn't work…ever.
- You need to answer the "hard" question
  - What do you really care about?

How do I know what to monitor?
(Cont.)

- Baseline what is normal for various user types
  - Queries and query types
  - Normal working hours
  - Size of typical data returned
- Look for anomalies from the baseline
  - Failed access attempts
  - Volume of queries
  - Unusual queries compared to what is typically used

What are the biggest challenges?

- Encryption (at rest and in transit)
- Data stored in multiple systems or locations
- Data access via applications and APIs
- Keeping up with database changes
- Finding people with enough DB and Info Sec knowledge to use the system

How do you get management 'buy in'?

- Look at your overall security program and see where this fits in
  - Risks addressed
  - Resources required (time, money, people…)
- Anticipate the concerns of the various stakeholders
  - These are typically the most critical databases in the organization

How do you get management 'buy in'? (cont.)

- Plan for multiple stages
  - Start with minimal risk to performance and stability (i.e. basic monitoring)
  - Progress to more enhanced monitoring as the teams become more confident
- "Sell" features that benefit them
  - Virtual patching
  - Blocking apps from using inefficient queries

Imperva SecureSphere

- This is one of the products you can use for Database Activity Monitoring
- Supports agent based and network monitoring
- Can do things like virtual patching, data classification, server discovery, etc.

Identifying what to monitor

- Hierarchical approach to server monitoring
  - Sites
  - Server Groups
  - Services
- Identify sensitive tables and columns
  - "Table Groups" are global objects used to define what is sensitive

Monitoring, Filtering, and Reporting

- This is where you tend to see the biggest differences between tools
  - Creating the monitoring policies and filtering to capture what you need
  - Determine what you will do with the data and the forms you will need it in
- Compare the capabilities of different tools to determine the most suitable

Summary

- Identify what you need to monitor
- Determine how this fits into your existing security program
- Plan for multiple stages to allow everyone to feel confident
- Evaluate tools based on criteria that is important to you
  - Reporting, features, resources, etc.

Goal Review

- Explain what Database Activity Monitoring (DAM) is, how it works, and how it can be deployed
- Discuss the challenges, limitations, and 'gotchas' typically encountered
- Discuss how to implement DAM with the Imperva's SecureSphere product

For more information: https://www.sans.org/reading-room/whitepapers/databases/database-activity-monitoring-dam-understanding-configuring-basic-network-monitoring-i-36577