TACHTECH
ACCELERATE SECURITY

Database Activity Monitoring Best Practices

info@tachtech.net | tachtech.net

Database Activity Monitoring Best Practices

TachTech offers an Imperva Database Activity Monitoring Best Practice Assessment to help ensure that Imperva users are gaining optimal value from their Imperva investment.

Network firewalls typically have dedicated staff and standard operating procedures to ensure they are providing the security intended. These include the following tasks:

- Add, Change or Modify Rules
- Policy & Configuration Review
- Updates and Upgrades
- Configuration Backups
- System Checks: CPU, Disk, Memory
- Log Reviews

Why is the same rigor not applied to database activity monitoring?

The biggest issue with the management of database activity monitoring (DAM) is the balancing of audit or regulatory requirements with finite resources available for monitoring, reporting and storage. Combined with the need to involve network, system, DBA, security and compliance teams, DAM management creates a great deal of complexity.

TachTech provides a complimentary assessment of leading DAM technologies to provide Imperva customers a measured analysis of their environment relative to best practices.

This health check includes the following components:

- Platform Assessment
- Configuration Assessment
- Deployment Score Card

The Deployment Score Card will clearly display areas that can be improved to increase your overall security posture and help your organization utilize Imperva's SecureSphere platform to its full potential.

About TachTech

TachTech is a group of security professionals that provides managed security programs, creating operationalized, measured programs benefitting information security, compliance and the business overall.

Platform Score Card

Design Check	ABC Company has DAM gateways placed in locations effective in monitoring database activity	🟢
Performance Check	ABC Company management server (MX) is operating according to company expectations	🟢
Capacity and High Availability (HA) Check	ABC Company has adequate gateways to monitor database activity during normal operation and through possible outage events	🟢
Version Check	ABC Company is running the latest recommended version of software	🟢
System Events Check	ABC Company does not have CPU Utilization Alerts, State Change Alerts or Hardware Failure Alerts configured for the MX and DAM. TachTech recommends those system events be configured to notify via syslog and email	🟡
Action Sets Check	ABC Company does not have syslog integrated with the MX. TachTech recommends that all MX and System Events should be sent to an external syslog sever or SIEM	🟡
Authentication Check	ABC Company does not use active directory (AD) authentication for MX GUI logins	🔴
Backups Check	ABC Company has a CIFS based backup location configured	🟢
ADC Updates Check	ABC Company checks for ADC updates once a week and TachTech recommends doing this check daily	🟡

Database Activity Monitoring (DAM) Score Card

Monitored Database Services Check	ABC Company has production application databases monitored. TachTech recommends adding monitoring for non-production databases that could house copies of production data	🟡
Site Tree Check	ABC Company has a well-designed site tree	🟢
Agent Check	ABC Company has agents deployed to monitor both network and local database activity. Currently each agent is registered to one gateway, TachTech recommends registering each agent to two gateways for redundancy	🟡
Profile Check	ABC Company does not monitor the database profile. TachTech recommends tuning so that the profile of users and user groups is kept to a manageable size	🔴
Alerts Check	ABC Company has database alerts being sent to their SIEM	🟢
Audit Policy Check	ABC Company is utilizing a monitor all policy to meet audit requirements causing an unnecessary drain on Imperva system and network storage resources. TachTech recommends configuring audit policies in a targeted fashion to meet audit, compliance and/or other monitoring needs	🟡
Archive Settings Check	ABC Company is archiving audit data on a monthly basis. TachTech recommends archiving daily for policies with high activity and weekly for policies with moderate activity	🟡
Reports Check	ABC Company has automated reports scheduled and sent to the necessary audience	🟡