



Databases

Benefits:

- » Continuous auditing of all databases activities without relying on local audit logging capabilities
- » Enforce Separation of Duties: independent auditing that tracks all privileged users
- » Reduced impact on databases and applications
- » Correlation of all enterprise platform logs and alerts
- » Simplified management across enterprise platforms
- » Business dashboard and drill downs provide better visibility into users activities
- » Minimize risk and impact of a data breach through real-time alerts and controls

SecureSphere DAM and SIEM Integration

Audit Database Activity, Protect Against Emerging Threats

Integration between SecureSphere Database Activity Monitoring (DAM) and SIEM solutions enables organizations to gain a comprehensive view of data usage, and provides advanced protection against emerging threats. Unlike collection of native DBMS logs, which in many cases is impractical due to performance overhead, partial data and separation of duties, SecureSphere provides a practical and cost-effective solution for database security and compliance.

SecureSphere DAM monitors and analyzes database activities in real-time providing a detailed audit trail and real time security alerts. SIEM solutions combine the database audit trail and alerts with log information from other systems such as IPS, IDS, firewalls, network, identity and access management systems and physical security devices. Through correlation of events across platforms, organizations gain in-depth visibility, and as a result, improved incident prioritization, handling and reporting.

Comprehensive Audit with Minimal Impact

SecureSphere provides full visibility, detailed audit data and real-time alerts with minimal impact on monitored servers. This is enabled through SecureSphere's hybrid architecture which combines network monitoring appliances and light-weight agents. Unlike native logging solutions that cause significant performance degradation, SecureSphere agents typically consume 2-4% CPU resources, and network monitoring has zero impact on the database server. Integrating SecureSphere with SIEM ensures safe collection of database audit and security details with continuous visibility across enterprise platforms.

Monitor Privileged Users, Enforce Separation of Duties

Database activity auditing solutions that rely on local logging allow privileged users to control the audit process (stop, start and change audit policies) and enable access to the audit data stored locally on the database server. This allows privileged database users to carry out malicious activities and conceal evidence in the audit trail, violating the concept of Separation of Duties (SOD). The integration of SecureSphere and SIEM overcomes this challenge as SecureSphere provides a complete, independent, tamper-proof audit trail of all database activities, including privileged user activities.

Establish Continuous Processes, Minimize Risk and Achieve compliance

The integrated SecureSphere and SIEM solution enables implementation of continuous and repeatable processes for mitigating risk and meeting regulatory mandates. A business dashboard view and drill down capabilities show who is accessing your critical enterprise data and how that data is being used. Vulnerability assessments and configuration audits included with SecureSphere help harden databases and ensure compliance with enterprise policies. Detailed alerts, audit and assessment data enable further mitigation of risk, enforcement of governance controls and reduction of compliance costs.

Automated Policy Enforcement and Real-Time Protection

For effective protection SecureSphere users can add the Firewall option which allows them to automatically block unauthorized activity. In addition to audit policies, SecureSphere includes highly granular security policies which identify known attacks in real-time. Behavior analysis based on the patented Dynamic Profiling technology identifies abnormal behaviors which may indicate an attack. Custom policies can easily be implemented for enforcement of access controls and prevention of unauthorized access.

Simplified Management across Enterprise Platforms

Most enterprise networks include a variety of platforms and network devices, each providing different logging and alerting capabilities. This is especially true for databases: native audit tools, which are included with most databases, vary in maturity levels and capabilities. SecureSphere streamlines auditing through centralized audit management and enables users to apply audit policies across heterogeneous databases. It does not require database expertise or SQL scripting for enablement or maintenance. SecureSphere provides a complete detailed audit trail for all platforms, regardless of native capabilities, and alerts in real-time on unauthorized access or malicious activity. SIEM correlates this information with other logs generating a full picture of enterprise activity.

Database Security and Compliance	SIEM + SecureSphere DAM	SIEM + collection of DBMS logs
Basic audit details about database activities	✓	✓
Selective audit policies	✓	✓
A detailed audit trail that includes information about the end-user, source applications and more	✓	✗
Real-time alerts on database events, ability to block unauthorized activities and attacks	✓	✗
Centralized management console for administrating all audit policies and reports	✓	✗
Doesn't allow database users to change audit policies or data to ensure separation of duties	✓	✗
Minimal impact on database performance and availability	✓	✗

Imperva

Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com

© Copyright 2011, Imperva

All rights reserved. Imperva, SecureSphere, and "Protecting the Data That Drives Business" are registered trademarks of Imperva. All other brand or product names are trademarks or registered trademarks of their respective holders. #TB-DAM-SIEM-INTEGRATION-0111rev1

