responsiv
simple · effective · distinctive

www.responsiv.co.uk

STREAMLINE DATA AUDIT REPORTING AND MONITORING WITH IBM GUARDIUM

AT A GLANCE

Challenges

- Required to create regulatory and internal data reports
- Limited access to database activity information across multiple systems
- Limited visibility of potential database threats and vulnerabilities

Benefits

- Configured monitoring and reporting for GDPR, PCI, SOX, HIPAA, and other data security regulations
- Accelerators for PCI compliance
- Investigation dashboard to easily assess issues
- Threat detection analytics for SQL injected or Stored Procedure attacks
- Reports can be saved to a dashboard for easy access
- Configure reports to update automatically

BENEFITS

Time and Effort Reduced

Reduce the time and effort required to collate and create regulatory reports using workflows and predefined report templates.

Access and Distribution

Easily access your reports by saving to a dashboard, or by automating distribution to the relevant auditors and stakeholders.

Custom Alerts

Create custom alerts with appropriate actions, for example, raise an alert ticket in the service desk when a file is accessed.

CHALLENGE

Teams are required to report on data protection and user access across distributed sources where the exact data source is unknown, unclear, or difficult to access. The time and effort is adding up.

Regulatory reports and internal updates on database security rely on this information to demonstrate compliance and assess threats, making it a priority for data governance and audit teams, as well as any other key stakeholders including auditors, CISOs, Heads of IT, and Cyber Risk teams.

SOLUTION

IBM Guardium *audit process builder* streamlines compliance workflows by consolidating information about asset discovery; vulnerability assessment and hardening; database activity monitoring and audit reporting; report distribution; sign off by key stakeholders; and escalations.

Processes can include tasks for:

- **Reporting** - create custom or utilise predefined reports.
- **Security assessments** - detect and alert teams of vulnerabilities.
- **Entity audit trails** - report on activity relating to a specific entity.
- **Discovering sensitive data** - scan data and metadata to suggest potentially sensitive data that should be kept secure.

Take advantage of the IBM Guardium *predefined reports* to streamline regulatory compliance and internal threat reporting, including:

- SQL errors
- Failed logins
- Policy violations
- Compliance reports (PCI, SOX, GDPR)
- Compliance monitoring (BASEL II, HIPAA, PII)

Automate report generation and distribution to save staff time, effort, and cost whilst improving efficiency and collaboration. Distribute reports to receivers based on role, or to an individual user or defined user groups. Schedule report generation to run immediately or at regular intervals as desired.

Click here to see how to create an audit process.

*information courtesy of IBM