Watching the Watcher with SQL Server Audit

Russ Thomas
DATABASE MANAGER

@sqljudo www.sqljudo.com

SQL Audit

- Capture events of interest
- Log those events reliably
- Runs on extended events
- Guarantee Accuracy
- Separation of Power

SQL Audit is one item in a toolbox of various other tools

Gaining proficiency with all tools gives us the best of all worlds

SQL Audit can protect it's own logs as well as custom approaches

Audit Specification

Single action or a group of focused actions to be audited or logged

It is assumed a specification is complete, accurate, and consumable

Many specifications can make up a single audit solution

Module

Demo Heavy

Server Audit Specification

Database Audit Specification

Audit Specification Targets

Protection and Reliability of Targets

Your ability to configure and consume

The volume of audit data

Your ability to guarantee protection

Staff resources

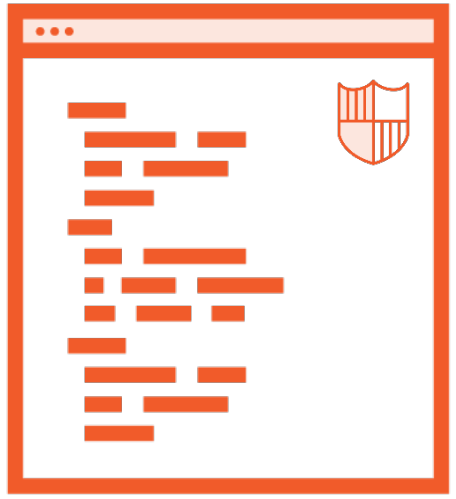
Initial Configuration and Consumption

Binary File

Ongoing maintenance and consumption harder

Application Log

Easy to set up and write to



Security Log

Slightly more difficult to configure an consume than application log

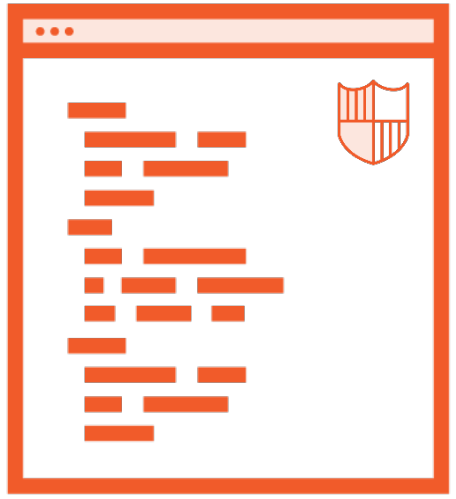
Initial Configuration and Consumption

Binary File

Much better performance for high volume logging

Application Log

Slower and requires more ongoing maintenance under load



Security Log

Same as application log

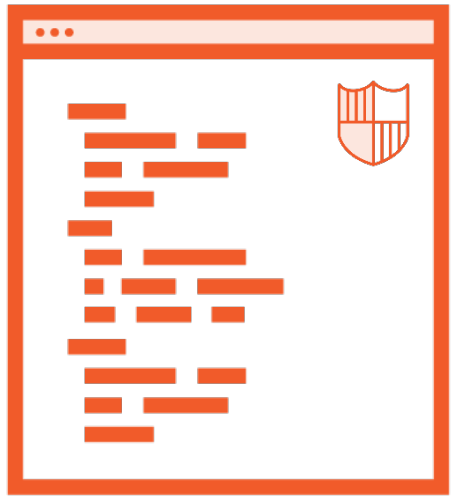
Initial Configuration and Consumption

Binary File

Custom approaches for consupmtion

Application Log

Native tools or third party tools



Security Log

Same as application log

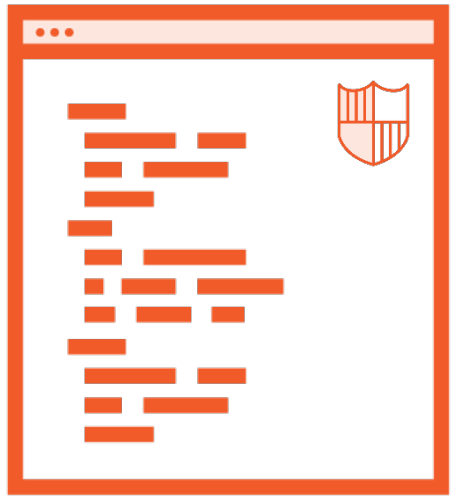
Protection of Data

Binary File

Very flexible for complex security approaches and administration

Application Log

Least secure but can be used with third party tools like splunk



Security Log

Requires more privileges to update

These jobs are easier with more staff at your disposal

One-person shops might need to rely more on technologies and third party products

Up Next

Compliance Reports and Documentation