Setting up Compliance Enforcement, Monitoring, and Logging

Russ Thomas
DATABASE MANAGER

@sqljudo www.sqljudo.com

Real World Compliance

Abacos Administrator

Regulatory Auditors

Compliance Team

Summary

- Capture of Compliance Data
- Custom Approaches
  - Server level triggers
  - Database level triggers
  - Extended Events
  - Custom Code
  - Policy Based Approach
- Third Party Tools
- Implementing Monitoring in Production

Compliance Enforcement

Big Brother

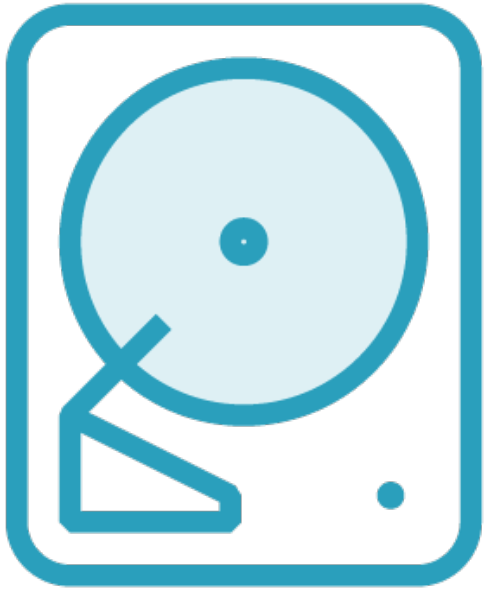
Little Brother

Compliance Auditing in Action

PCI Policy Rule

- No card holder data should exist on disk in plain text. All card holder data should be encrypted at rest.

Audit Process



SQL Server Triggers

Stored procedures that execute under specific circumstances or actions

- Server Level Triggers
- Database Level Triggers
- DDL Triggers
- DML Triggers

DDL and DML Statements

```
CREATE TABLE TestTable
(
  PKKey INT Primary Key Clustered,
  TestEntry VARCHAR(50)
);
```

```
INSERT INTO TestTable
(PKKey, TestEntry)
VALUES
(1,`this is a test`);
```

Common Uses for Triggers

- Capturing Meta Data
- Restricting Actions
- Help Avoid Accidental Data Destruction
- Trusting Your Triggers?

Trigger Concerns

Can be hard to administer or troubleshoot

- Especially instead of triggers

Can impact performance

- Deeply nested triggers or triggers that take many locks

Make sure your triggers are documented

Extended Events

SQL Trace Deprecated

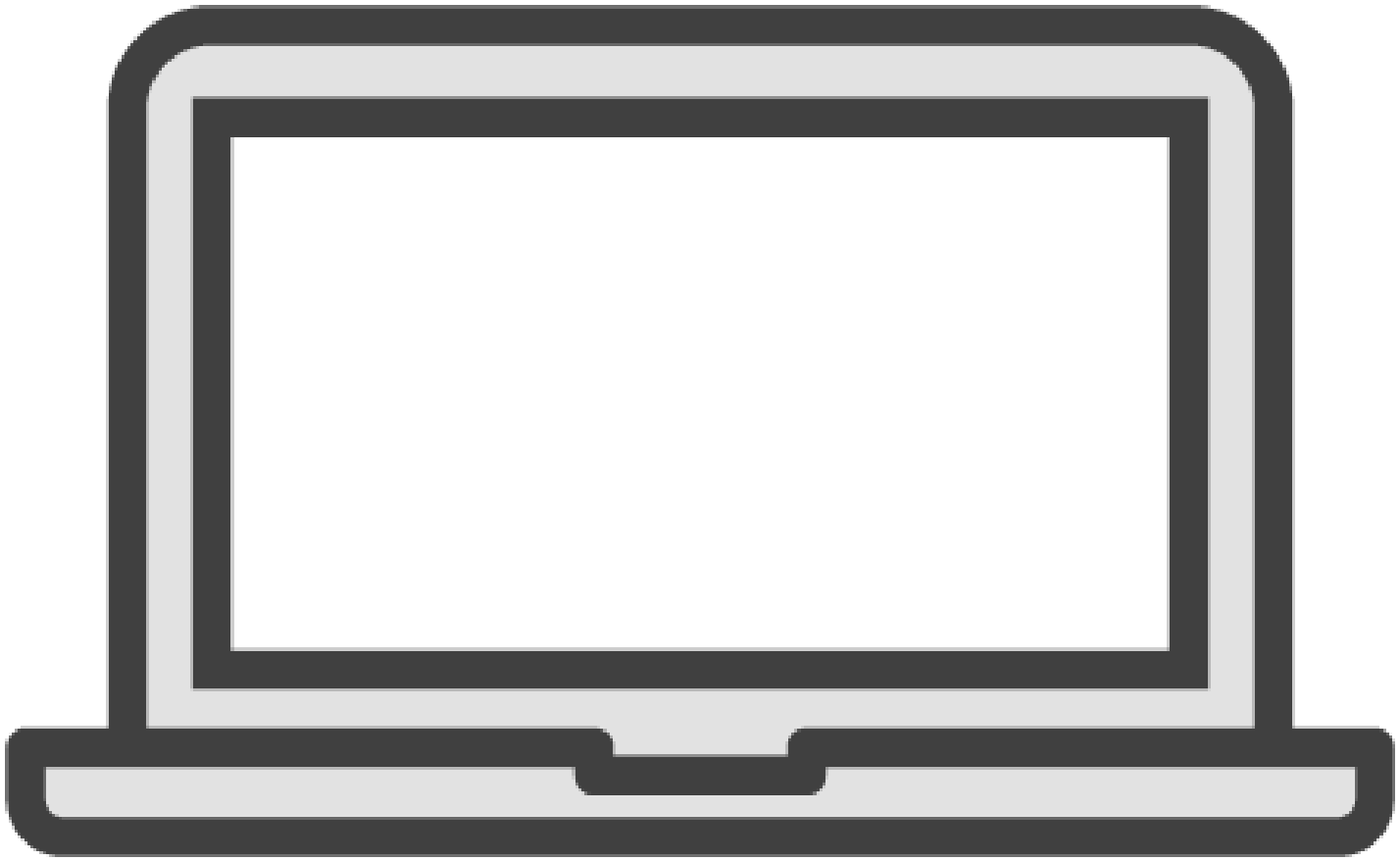
SQL Trace Implemented Via

- SQL Profiler
- Server Side Tracing

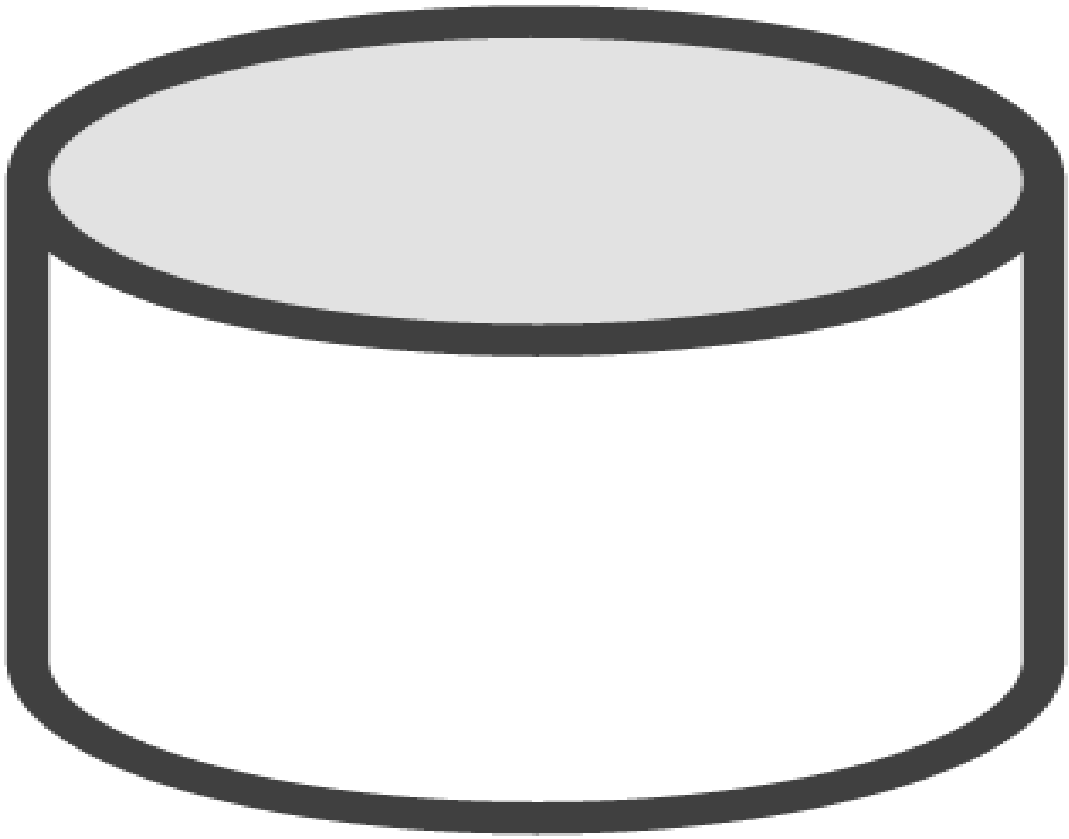
Extended Event to SQL Trace Equivalents

- http://bit.ly/2dWbRvw

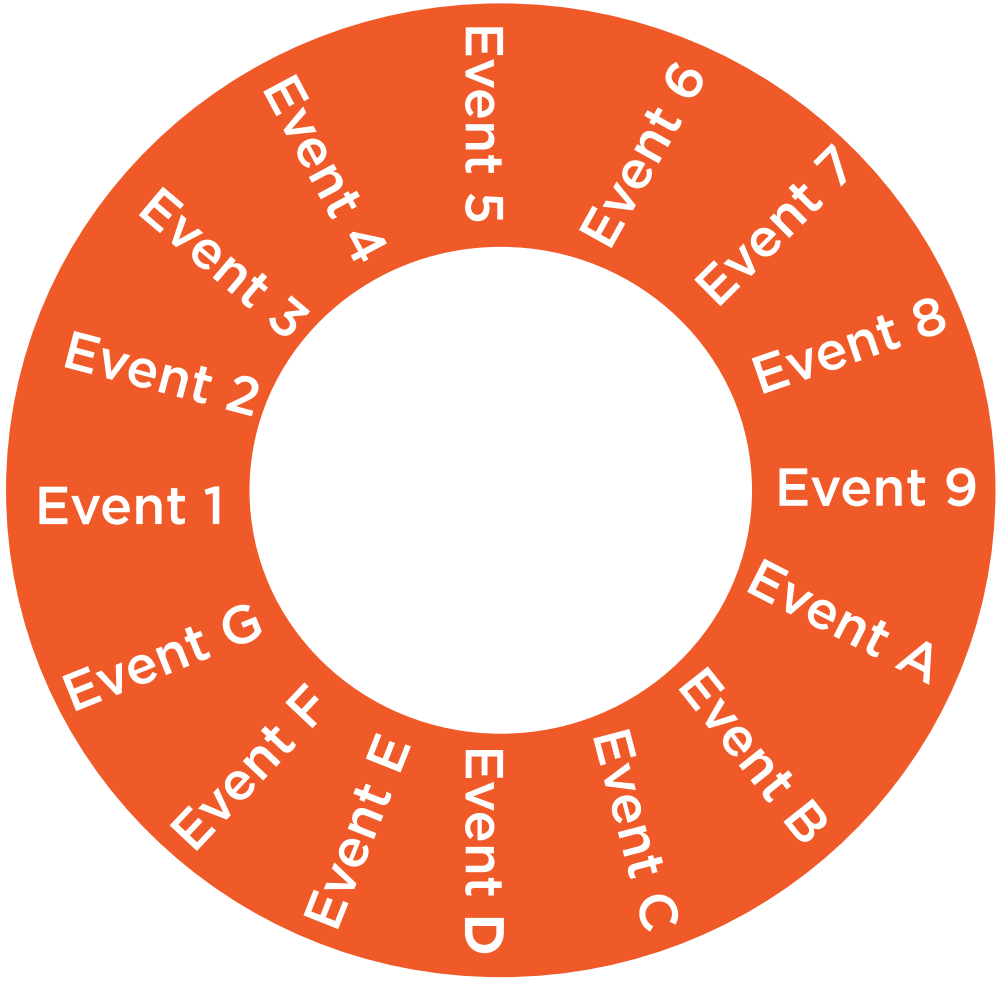
Extended Events



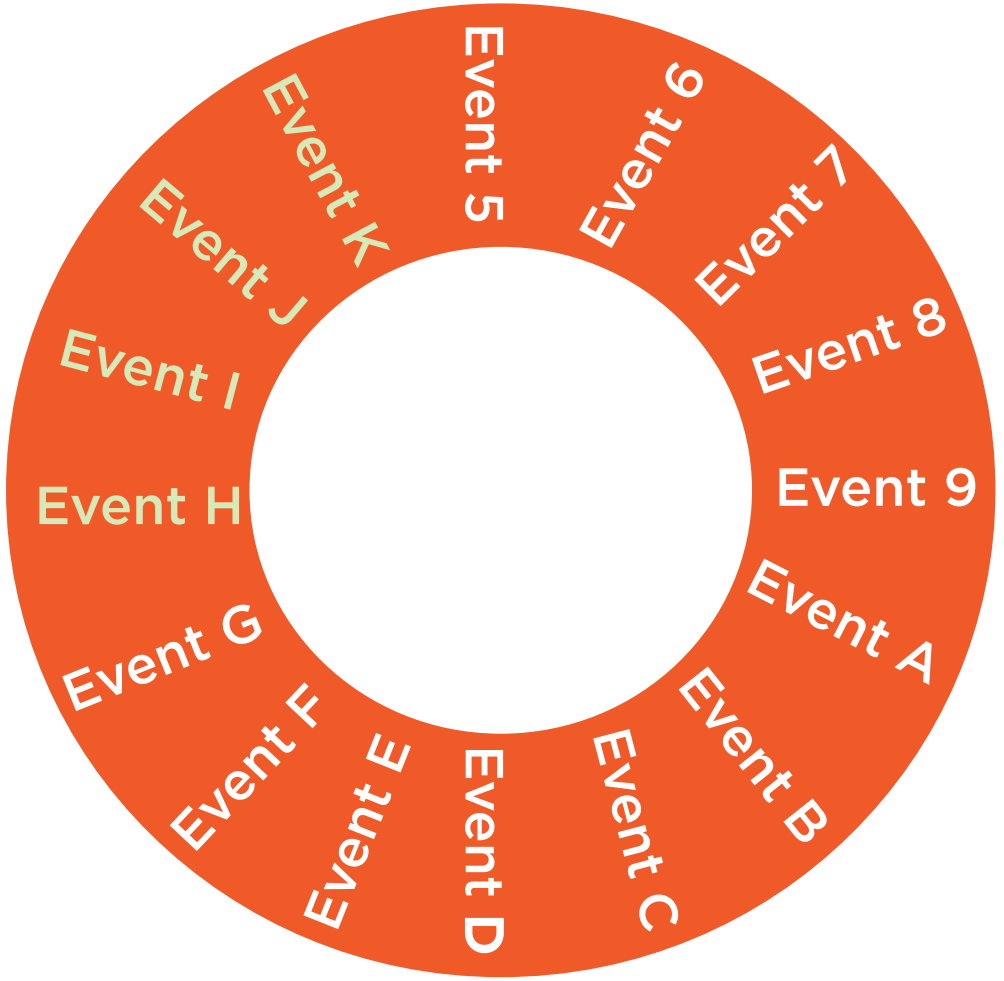
Extended Events



Extended Event Ring Buffer Storage



Extended Event Ring Buffer Storage



Managing Compliance at Scale

Policy Based Management

- Automated policy verification
- Log and report
- Block out of policy actions
- Verifies settings
- Verifies configurations
- Verifies object

Policy:

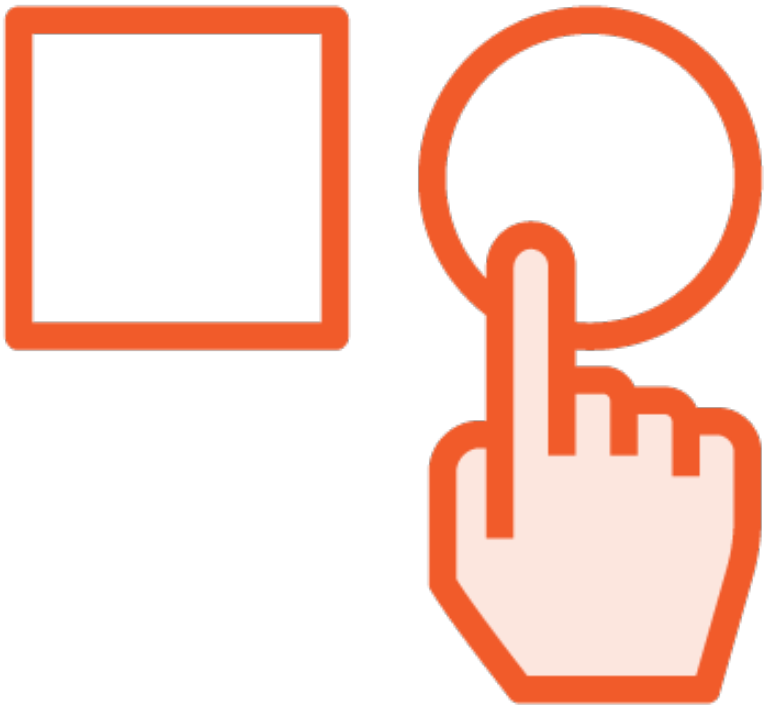
Windows logins only – mixed mode authentication is not allowed

Policies:

- Defined rules to be checked
- On demand
- Automated
- Log only or block action

Targets:

- Scope of the policy verification
- Instances
- Databases
- Individual objects



Conditions:

- Expression or logic

- Evaluated for Boolean result

Facets:

- Properties with categories of scope

Example:

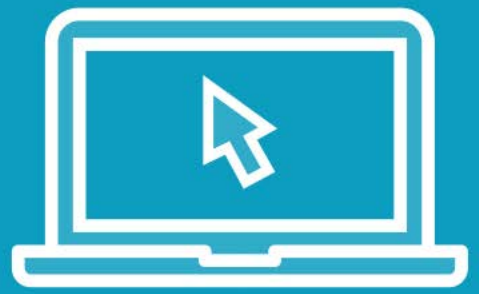
- Login name
- Create date
- Password expired
- Disabled
- ...

```
select count(*)
from sys.databases
    where name='model'
    and
    recovery_model_desc
    = 'SIMPLE‘;
```

- Any logical expression that you can write with TSQL can be used within a policy

- Check your sql server instances for any model databases that are in simple recovery

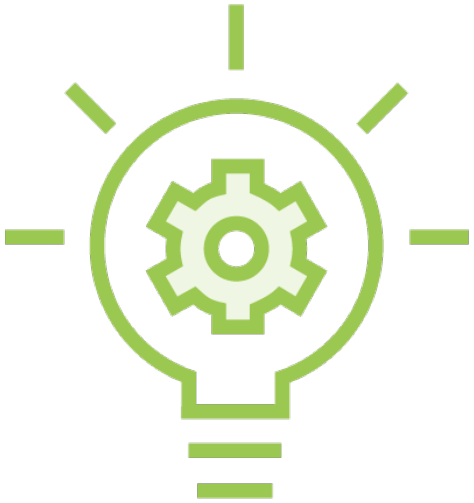
Demo



Abacos Widgets

Policy Based Management Demo

Compliance Monitoring and Enforcement



Custom Approaches

Third Party Tools

Third Party Solutions

Pros	Cons
Less up front effort	Larger up front cost
Leverage trusted technologies	More features than needed
May offer industry standards	Still require management and support

3rd Party Compliance Tools

- Production efficiency is critical
- Be proficient with your tools
- Leverage industry resources

Up Next

Who watches the watchers?

Separation of power!