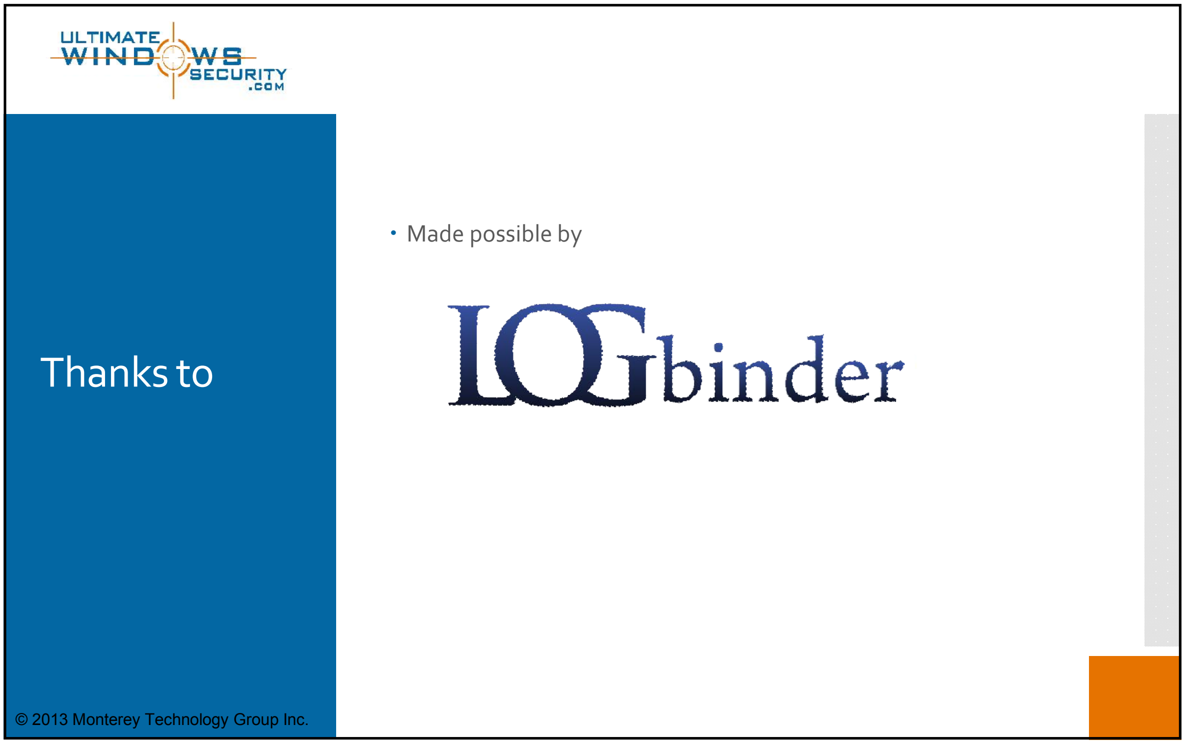
Not Monitoring SQL Server with Your SIEM is Close to Negligent: What are Your Options?

Sponsored by

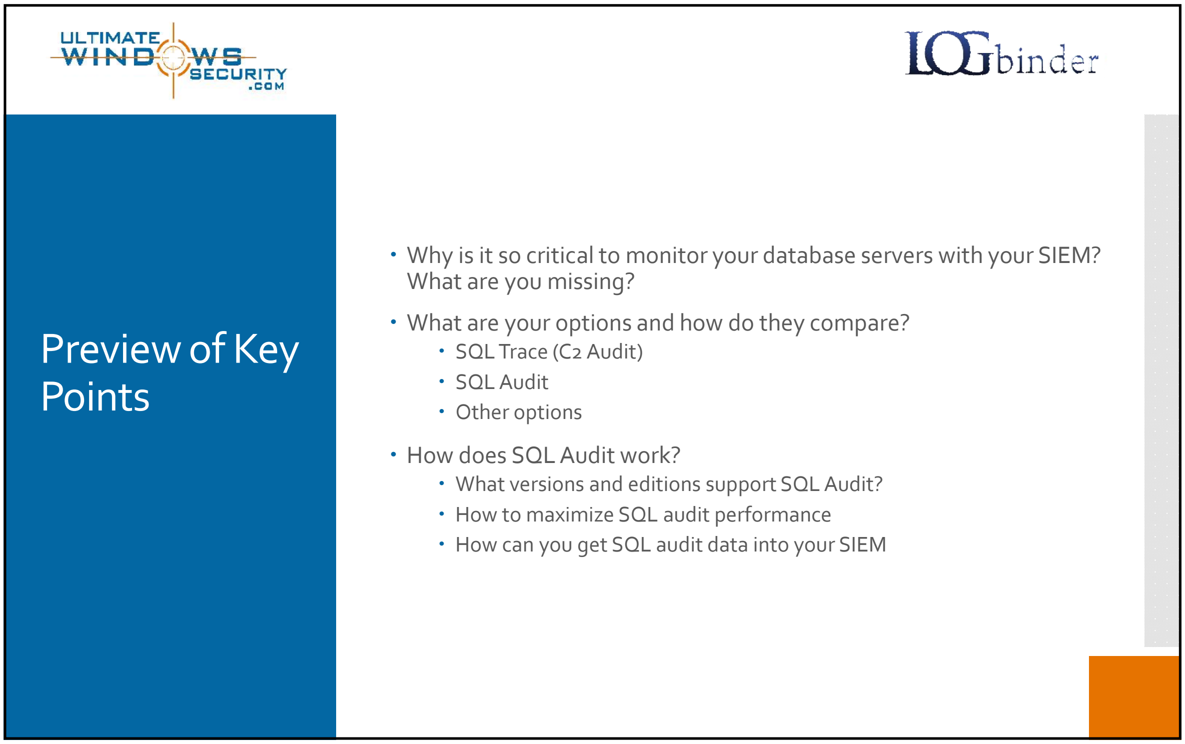
LOGbinder



Thanks to

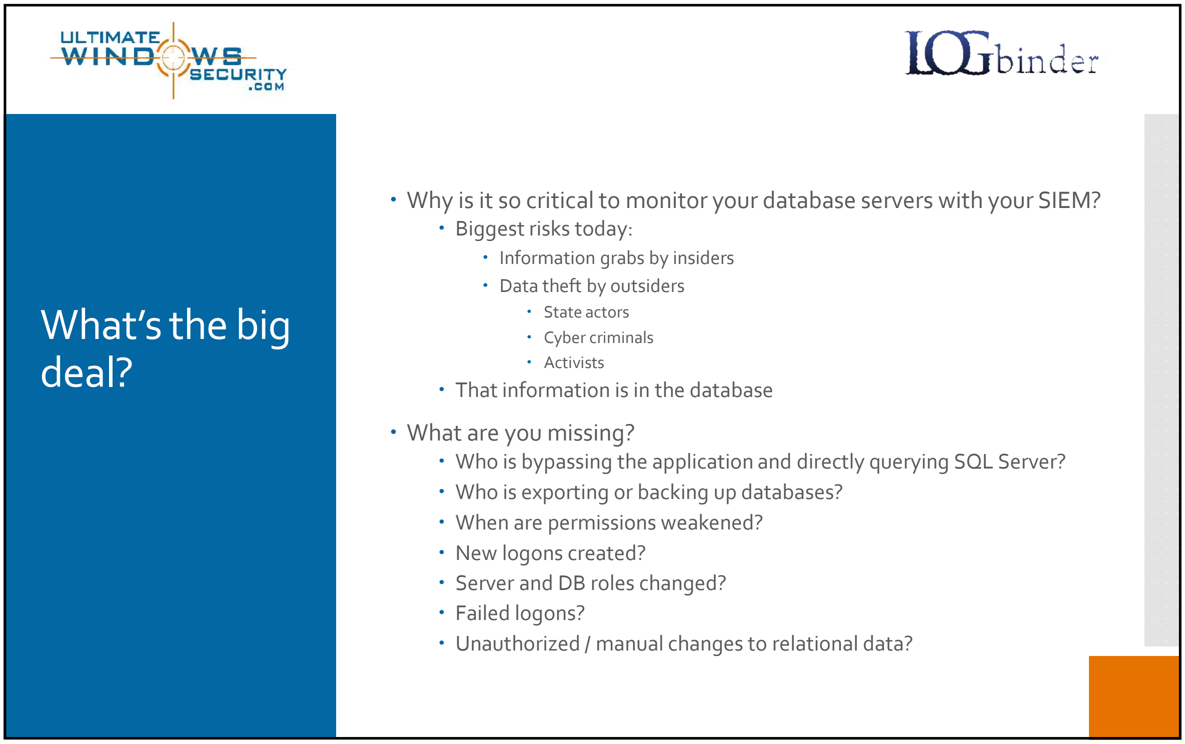
- Made possible by

LOGbinder



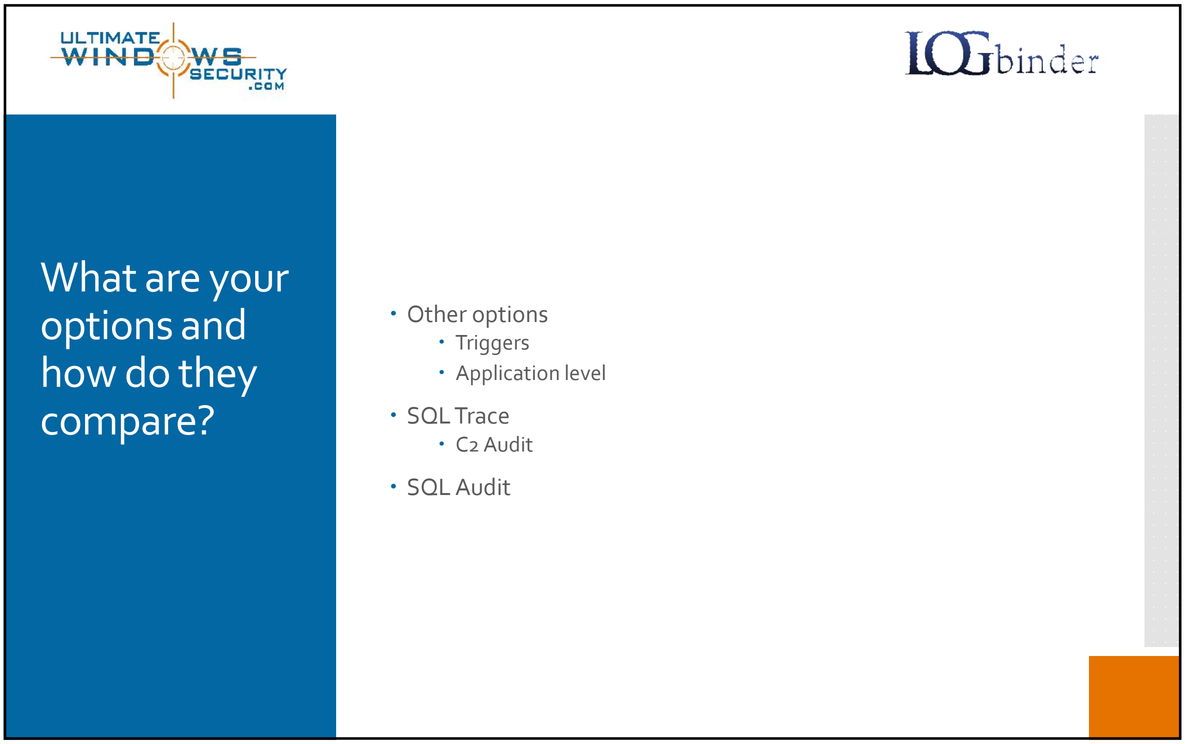
Preview of Key Points

- Why is it so critical to monitor your database servers with your SIEM? What are you missing?
- What are your options and how do they compare?
  - SQL Trace (C2 Audit)
  - SQL Audit
  - Other options
- How does SQL Audit work?
  - What versions and editions support SQL Audit?
  - How to maximize SQL audit performance
  - How can you get SQL audit data into your SIEM



What's the big deal?

- Why is it so critical to monitor your database servers with your SIEM?
  - Biggest risks today:
    - Information grabs by insiders
    - Data theft by outsiders
      - State actors
      - Cyber criminals
      - Activists
  - That information is in the database
- What are you missing?
  - Who is bypassing the application and directly querying SQL Server?
  - Who is exporting or backing up databases?
  - When are permissions weakened?
  - New logons created?
  - Server and DB roles changed?
  - Failed logons?
  - Unauthorized / manual changes to relational data?

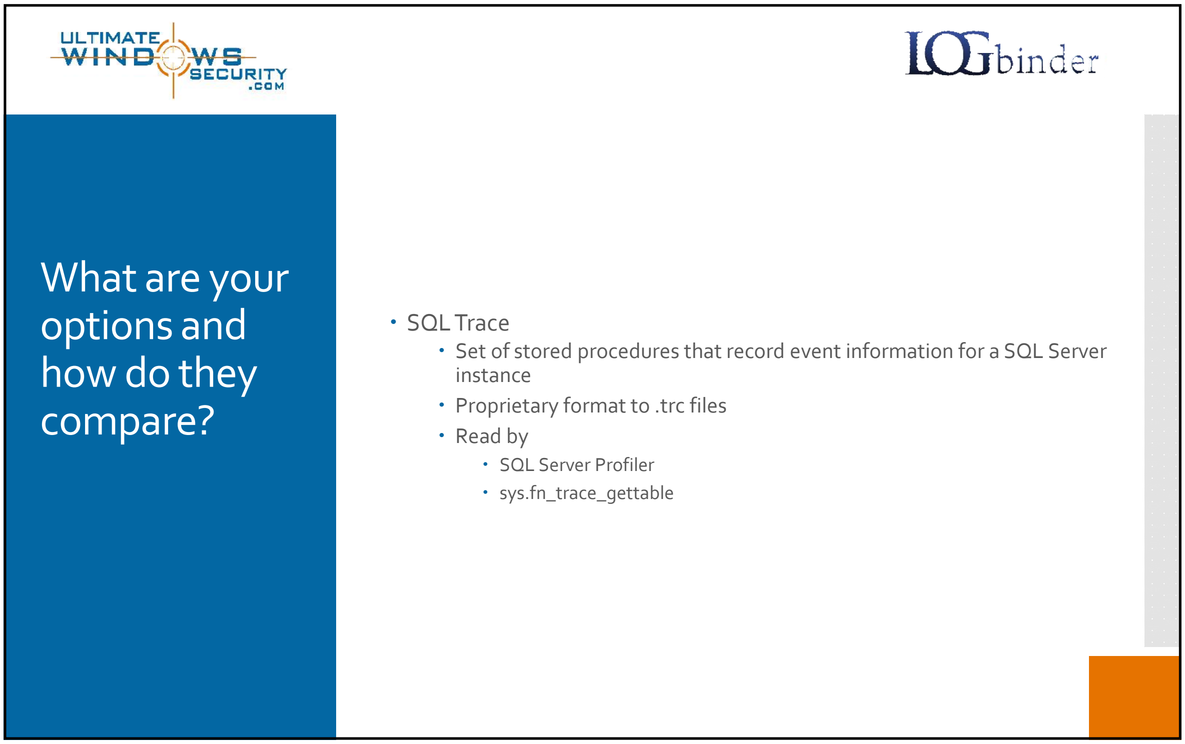


What are your options and how do they compare?

- Other options
  - Triggers
  - Application level
- SQL Trace
  - C2 Audit
- SQL Audit

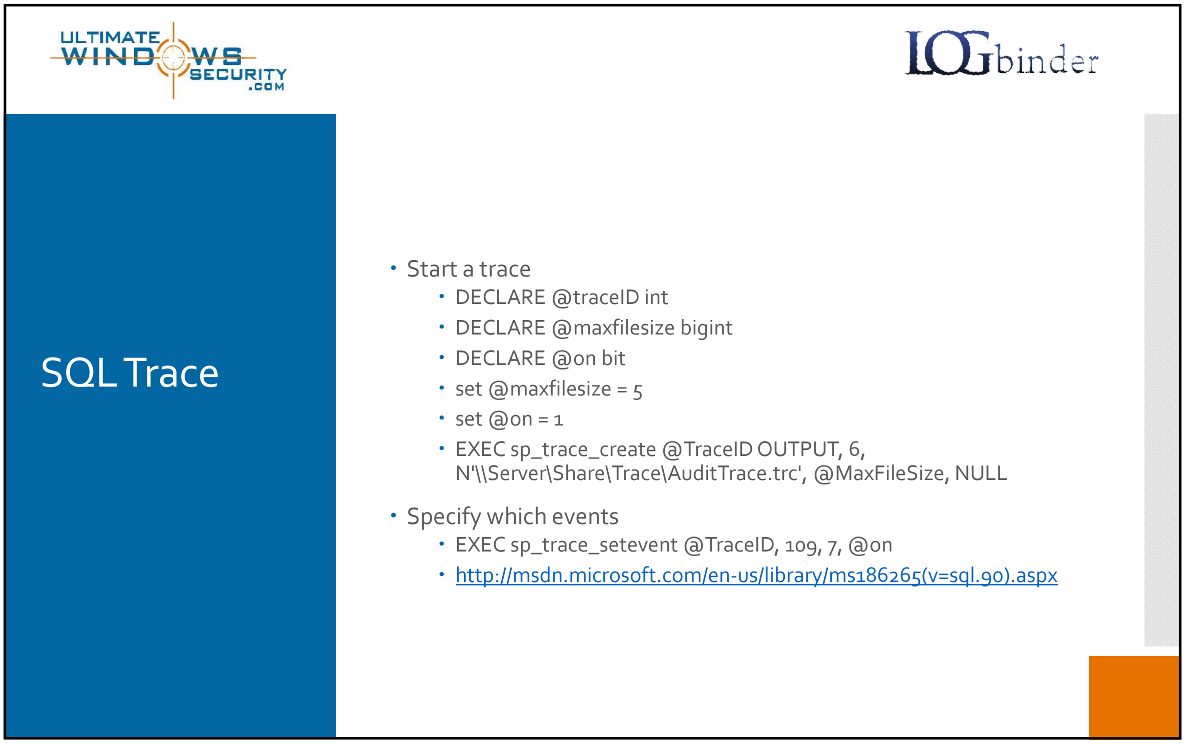
What are your options and how do they compare?

- Other options
  - Triggers
    - Requires DB programmer
  - Application level
    - Require application programmer
    - Access to source code
- Case specific
- Laborious
- Maintenance headache
- Impractical



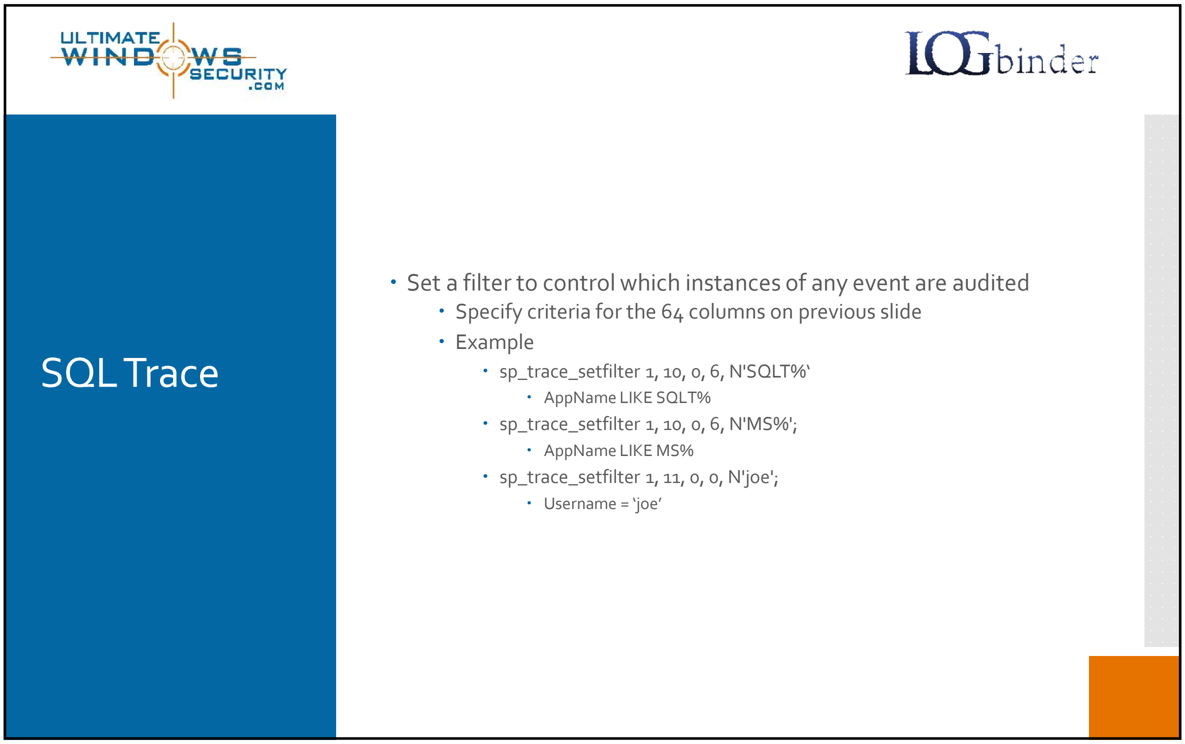
What are your options and how do they compare?

- SQL Trace
  - Set of stored procedures that record event information for a SQL Server instance
  - Proprietary format to .trc files
  - Read by
    - SQL Server Profiler
    - sys.fn_trace_gettable



SQL Trace

- Start a trace
  - DECLARE @traceID int
  - DECLARE @maxfilesize bigint
  - DECLARE @on bit
  - set @maxfilesize = 5
  - set @on = 1
  - EXEC sp_trace_create @TraceID OUTPUT, 6, N'\\Server\Share\Trace\AuditTrace.trc', @MaxFileSize, NULL
- Specify which events
  - EXEC sp_trace_setevent @TraceID, 109, 7, @on
  - http://msdn.microsoft.com/en-us/library/ms186265(v=sql.90).aspx



SQL Trace

- Set a filter to control which instances of any event are audited
  - Specify criteria for the 64 columns on previous slide
  - Example
    - sp_trace_setfilter 1, 10, 0, 6, N'SQLT%‘
      - AppName LIKE SQLT%
    - sp_trace_setfilter 1, 10, 0, 6, N'MS%';
      - AppName LIKE MS%
    - sp_trace_setfilter 1, 11, 0, 0, N'joe';
      - Username = ‘joe’

SQL Trace

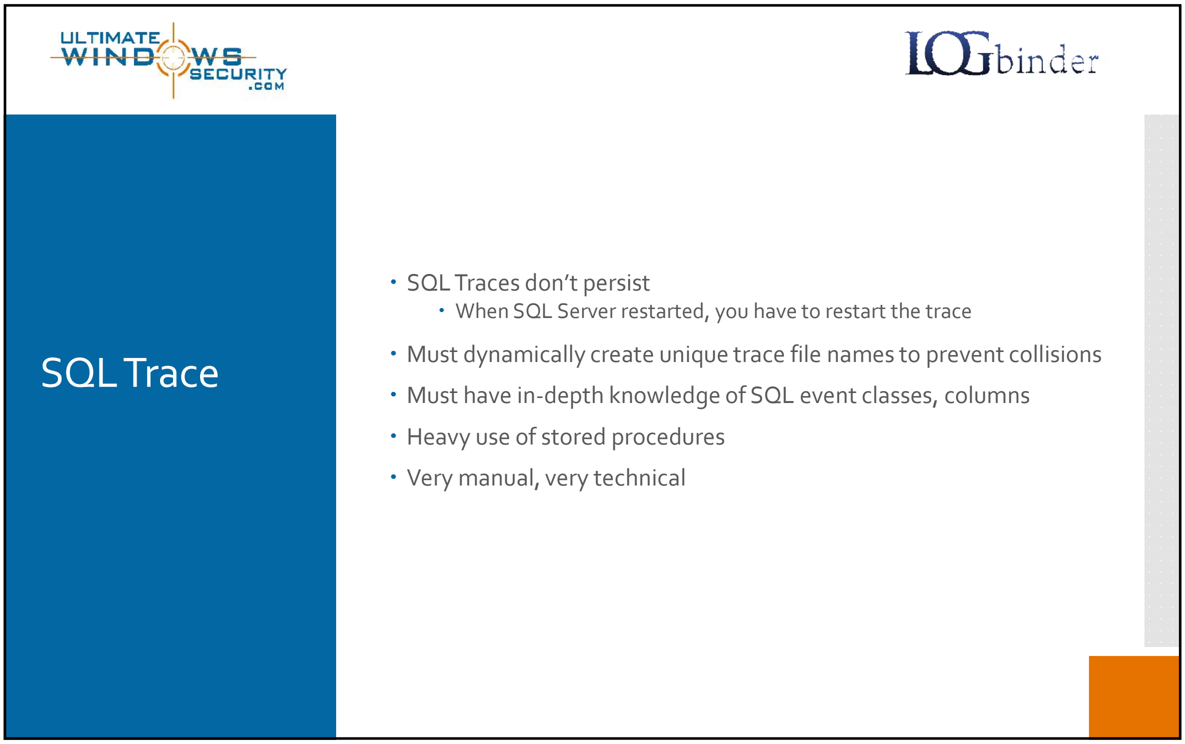
- Read a trace
  - sys.fn_trace_gettable
  - Columns

ApplicationName 1
BigintData1
BigintData2
Binary Data
ClientProcessID 1
ColumnPermissions
CPU
Database ID 1
DatabaseName
DBUserName 1
Duration
EndTime
Error
EventClass 1

EventSequence
EventSubClass 1
GUID
FileName
Handle
HostName 1
IndexID
IntegerData
IntegerData2
IsSystem
LineNumber
LinkedServerName
LoginName
LoginSid 1
MethodName
Mode
NestLevel
NTDomainName 1
NTUserName 1
ObjectID
ObjectID2

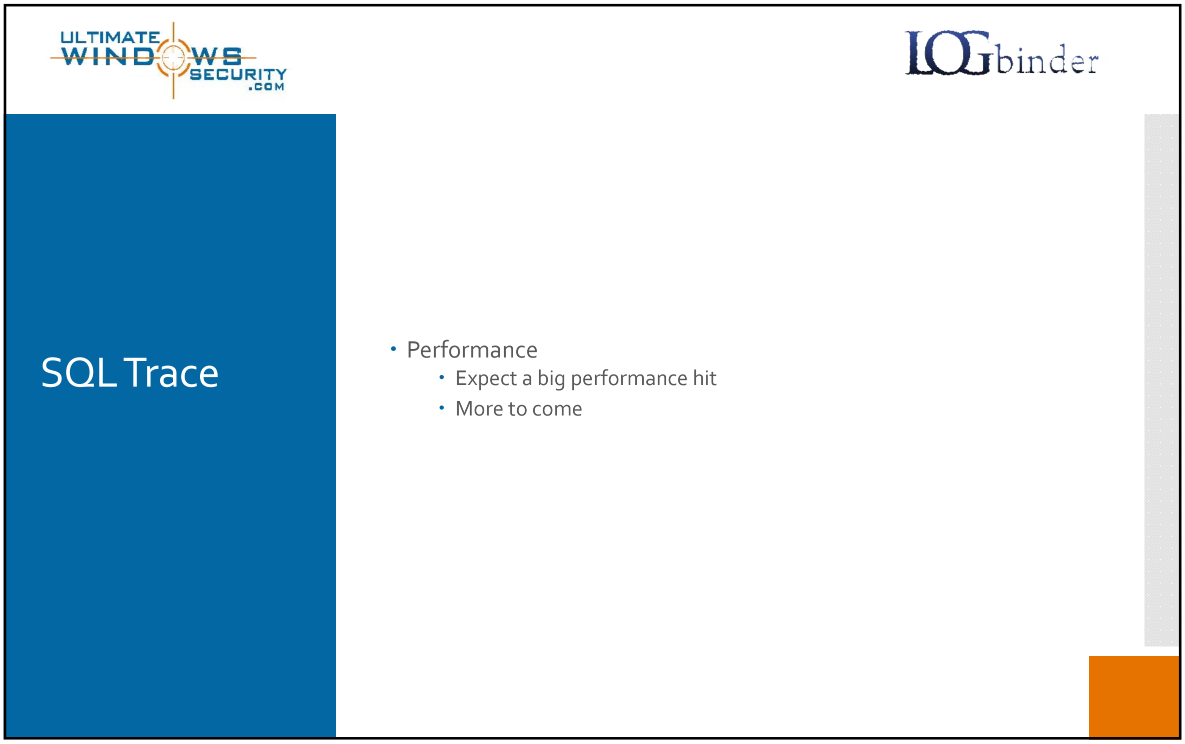
ObjectName
ObjectType 2
Offset
OwnerID
OwnerName
ParentName
Permissions
ProviderName
Reads
RequestID
RoleName
RowCounts
ServerName 1
SessionLoginName
Severity
SourceDatabaseID
SPID
SqlHandle
StartTime 1
State

Success
TargetLoginName
TargetLoginSid
TargetUserName
TextData
Transaction ID
Type
Writes
XactSequence



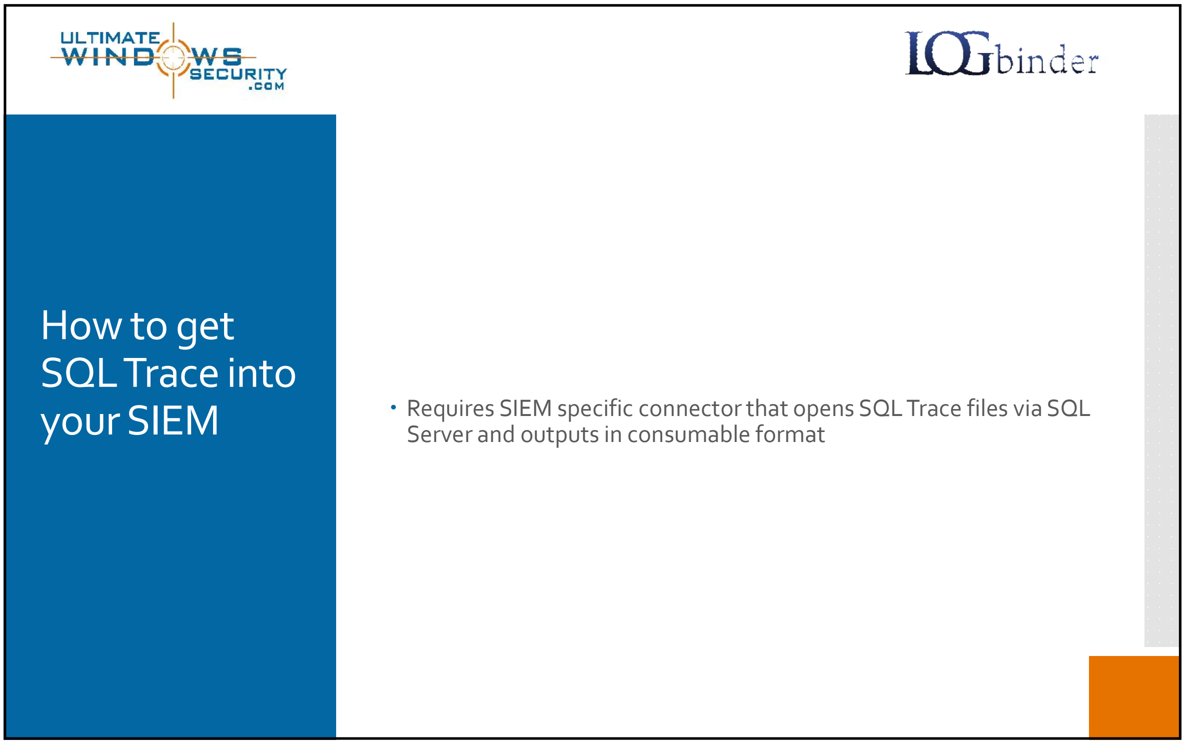
SQL Trace

- SQL Traces don't persist
  - When SQL Server restarted, you have to restart the trace
- Must dynamically create unique trace file names to prevent collisions
- Must have in-depth knowledge of SQL event classes, columns
- Heavy use of stored procedures
- Very manual, very technical



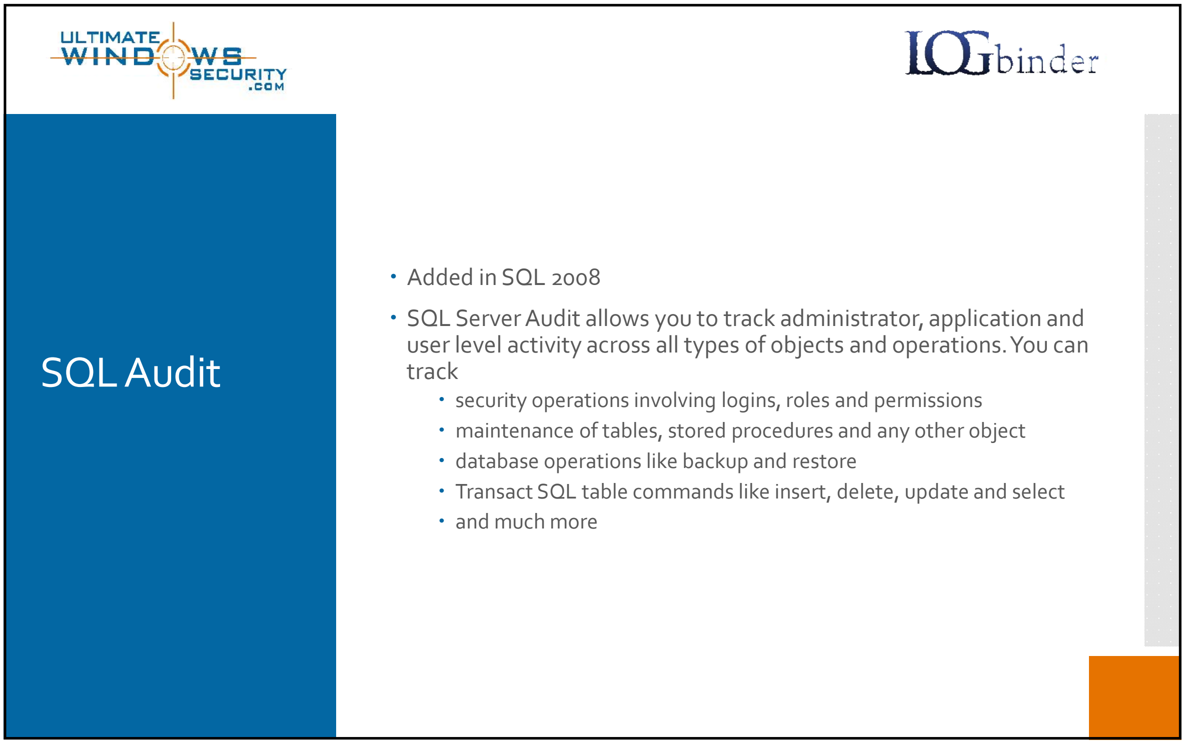
SQL Trace

- Performance
  - Expect a big performance hit
  - More to come



How to get SQL Trace into your SIEM

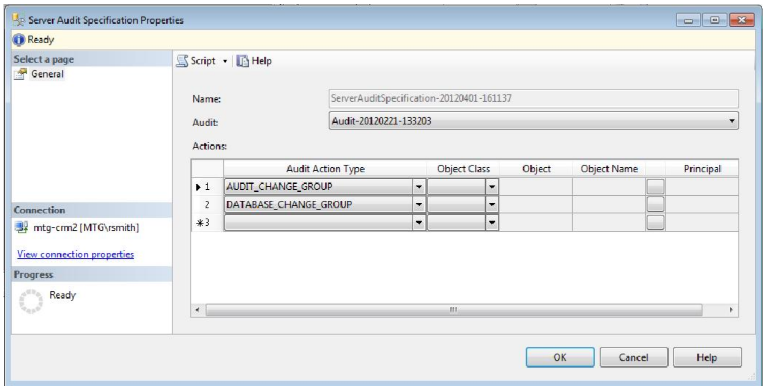
- Requires SIEM specific connector that opens SQL Trace files via SQL Server and outputs in consumable format



SQL Audit

- Added in SQL 2008
- SQL Server Audit allows you to track administrator, application and user level activity across all types of objects and operations. You can track
  - security operations involving logins, roles and permissions
  - maintenance of tables, stored procedures and any other object
  - database operations like backup and restore
  - Transact SQL table commands like insert, delete, update and select
  - and much more

SQL Audit



mtg-crm2 [MTG\rsmith]

Ready

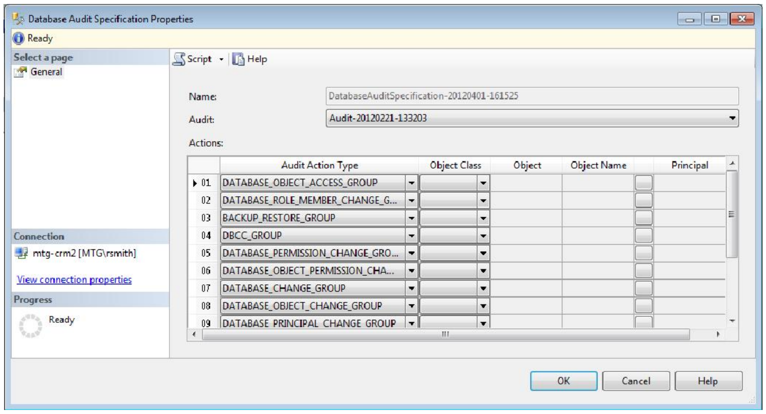
Name: ServerAuditSpecification-20120401-161137

Audit: Audit-20120221-133203

Actions:

	Audit Action Type	Object Class	Object	Object Name		Principal
1	AUDIT_CHANGE_GROUP					
2	DATABASE_CHANGE_GROUP					
*3						

SQL Audit



Database Audit Specification Properties
Ready
Select a page
General
Script
Help
Connection
View connection properties
Progress
OK
Cancel
Help

mtg-crm2 [MTG\rsmith]

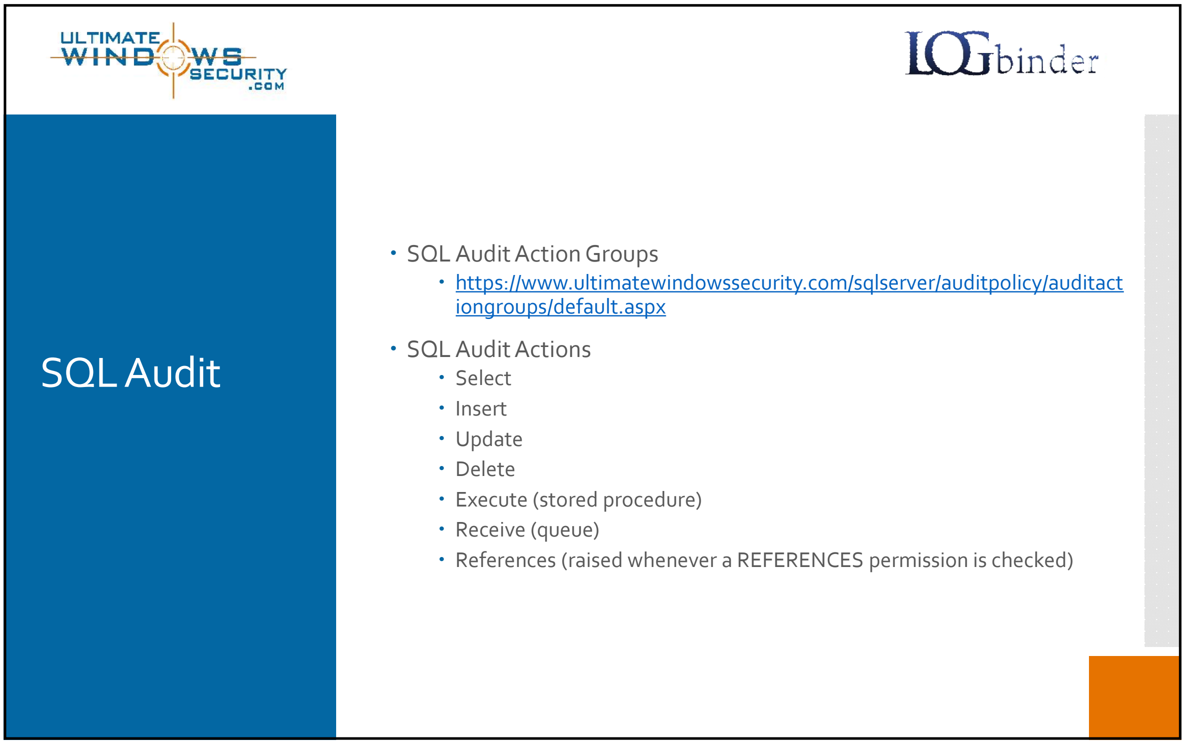
Ready

Name: DatabaseAuditSpecification-20120401-161525

Audit: Audit-20120221-133203

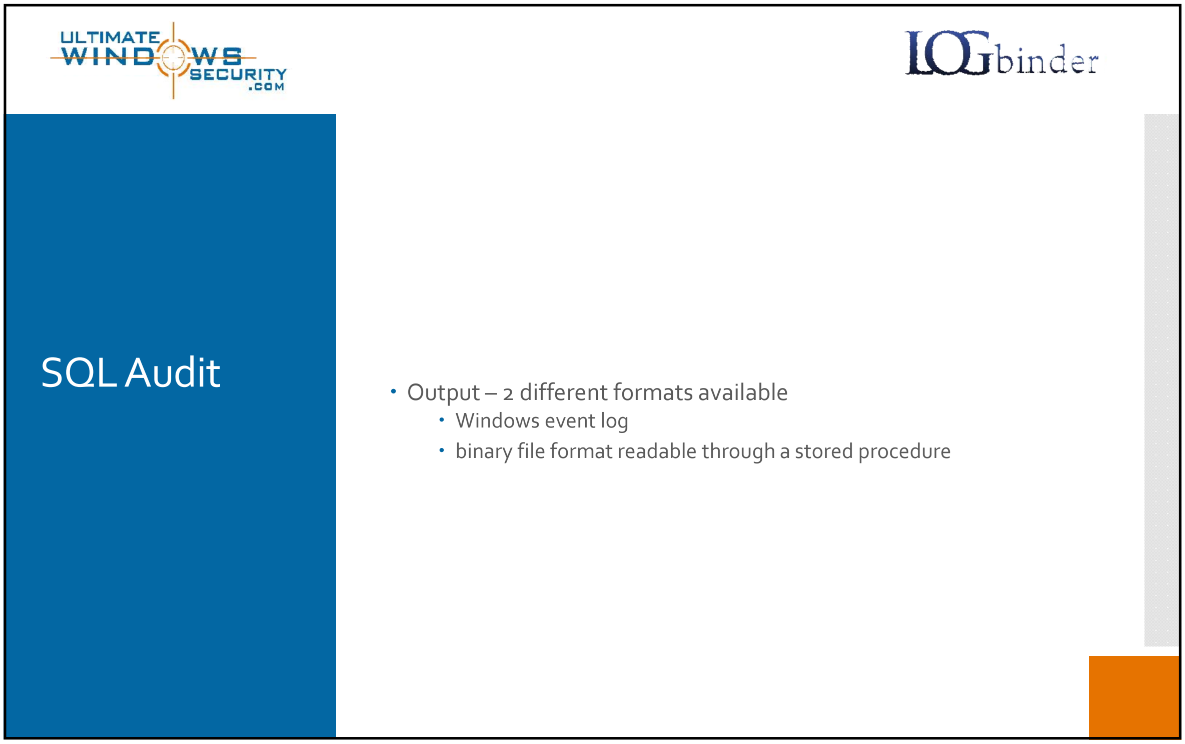
Actions:

	Audit Action Type	Object Class	Object	Object Name		Principal
01	DATABASE_OBJECT_ACCESS_GROUP					
02	DATABASE_ROLE_MEMBER_CHANGE_G...					
03	BACKUP_RESTORE_GROUP					
04	DBCC_GROUP					
05	DATABASE_PERMISSION_CHANGE_GRO...					
06	DATABASE_OBJECT_PERMISSION_CHA...					
07	DATABASE_CHANGE_GROUP					
08	DATABASE_OBJECT_CHANGE_GROUP					
09	DATABASE_PRINCIPAL_CHANGE_GROUP					



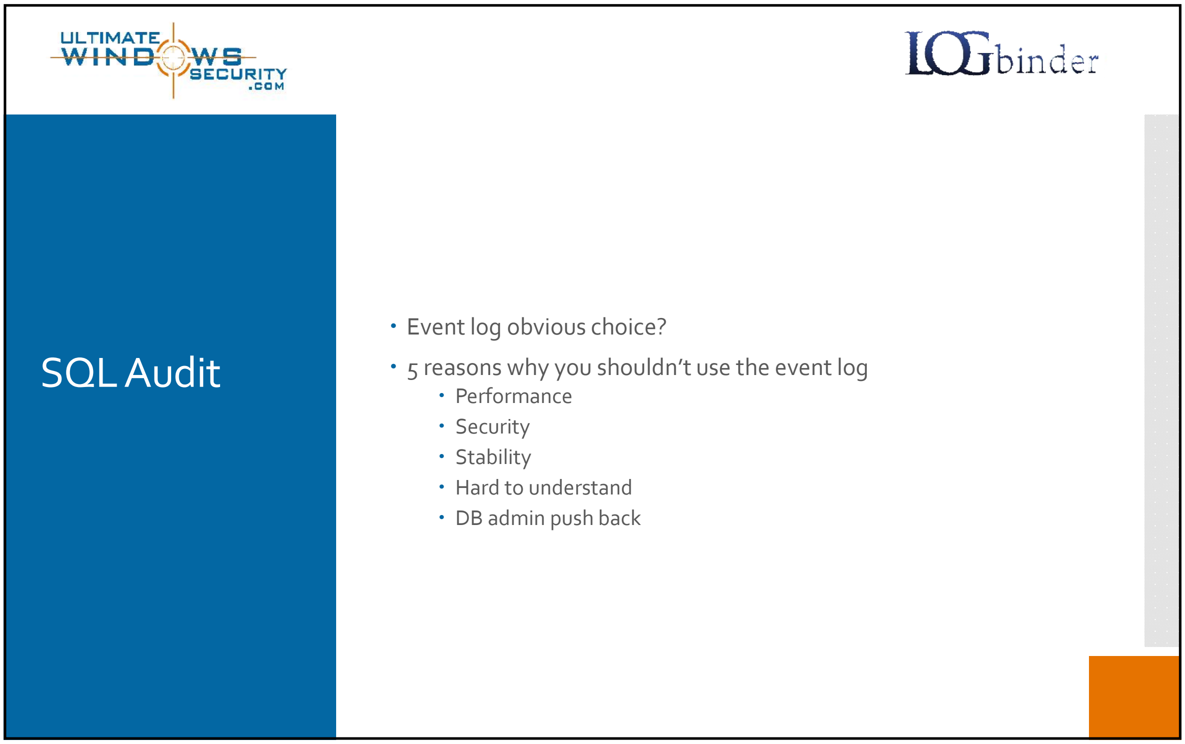
SQL Audit

- SQL Audit Action Groups
  - https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/auditactiongroups/default.aspx
- SQL Audit Actions
  - Select
  - Insert
  - Update
  - Delete
  - Execute (stored procedure)
  - Receive (queue)
  - References (raised whenever a REFERENCES permission is checked)



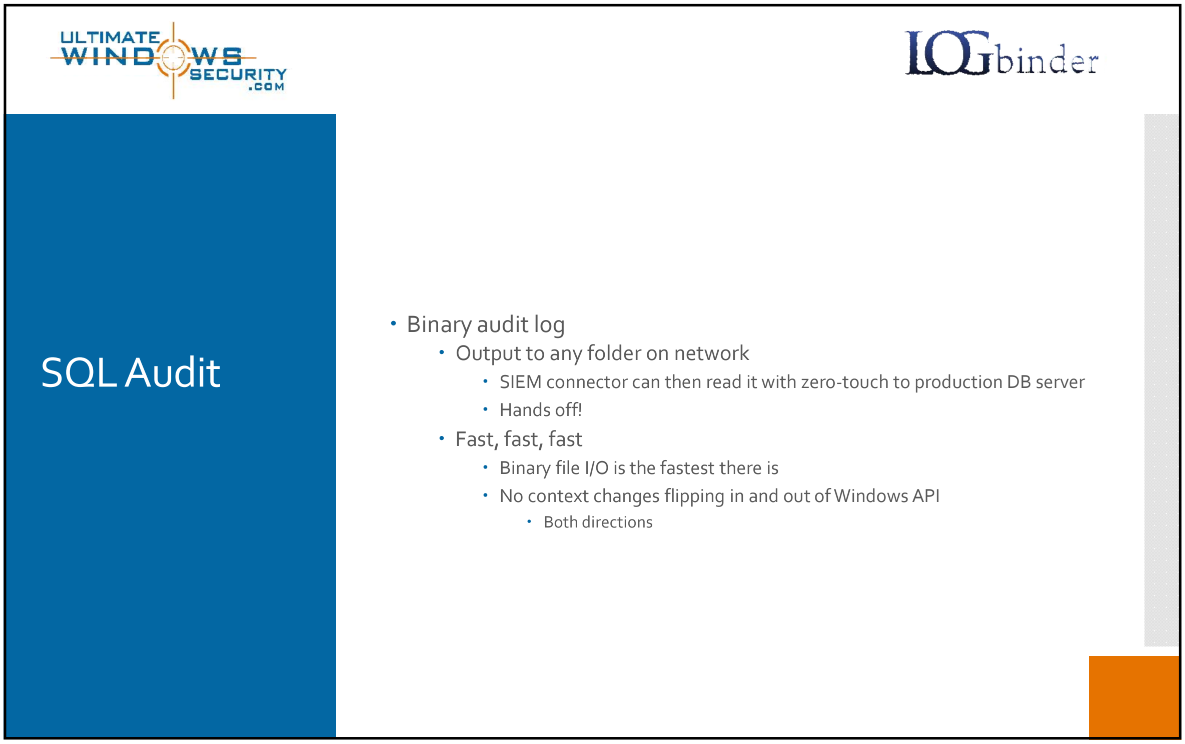
SQL Audit

- Output – 2 different formats available
  - Windows event log
  - binary file format readable through a stored procedure



SQL Audit

- Event log obvious choice?
- 5 reasons why you shouldn’t use the event log
  - Performance
  - Security
  - Stability
  - Hard to understand
  - DB admin push back



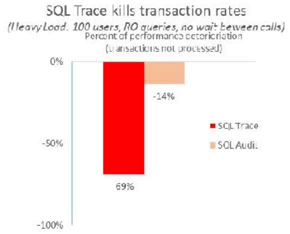
SQL Audit

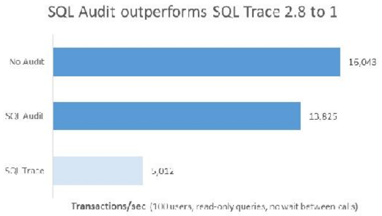
- Binary audit log
  - Output to any folder on network
    - SIEM connector can then read it with zero-touch to production DB server
    - Hands off!
  - Fast, fast, fast
    - Binary file I/O is the fastest there is
    - No context changes flipping in and out of Windows API
      - Both directions

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Trace vs Audit Performance



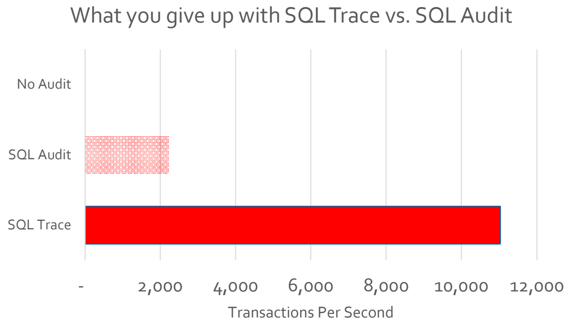


Source: http://sqlblog.com/blogs/linchi_shea/archive/2012/01/24/performance-impact-sql2008-r2-audit-and-trace.aspx

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

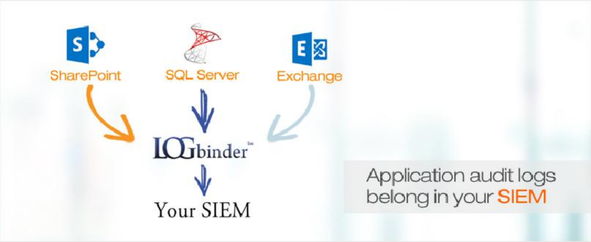
Trace vs Audit Performance



Source: http://sqlblog.com/blogs/linchi_shea/archive/2012/01/24/performance-impact-sql2008-r2-audit-and-trace.aspx

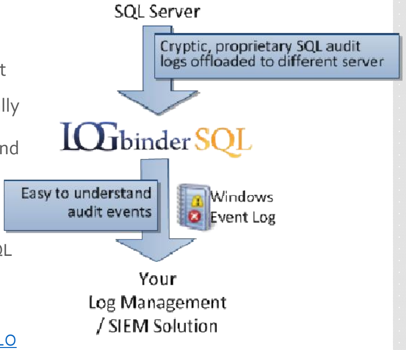
SQL Audit

- But how do you get the binary audit log into your SIEM?
  - LOGbinder SQL



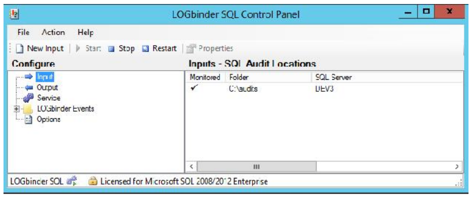
LOGbinder

- Small efficient Windows service that runs on any Windows server on your network
- One instance of LOGbinder SQL can process logs from many SQL Servers
- LOGbinder SQL can coexist with other LOGbinder products like LOGbinder EX for Exchange and LOGbinder SP for SharePoint
- Simply configure each SQL Server (optionally with our free SQL Server Audit Wizard) to write its audit events to a specified folder and then provide those folders to LOGbinder SQL.
- LOGbinder SQL
  - 1. Processes events as they appear in SQL Server binary audit log files
  - 2. Translates them into easy-to-read events
    - http://www.logbinder.com/Products/LOGbinderSql/EventsGenerated
  - 3. Forwards to your SIEM solution in its native format
    - ArcSight, Qradar, McAfee, EventTracker, LogRhythm, LogPoint, SolarWinds, Splunk and many, many more


SQL Server
Cryptic, proprietary SQL audit logs offloaded to different server
LOGbinder SQL
Easy to understand audit events
Windows Event Log
Your Log Management / SIEM Solution

LOGbinder

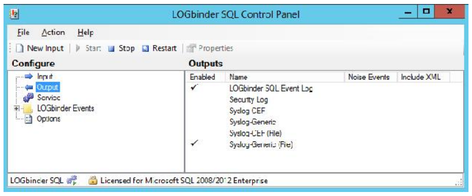
- 5 minute setup



Inputs - SQL Audit Locations

Monitored	Folder	SQL Server
✓	C:\audits	DEV3

LOGbinder SQL Licensed for Microsoft SQL 2008/2012 Enterprise



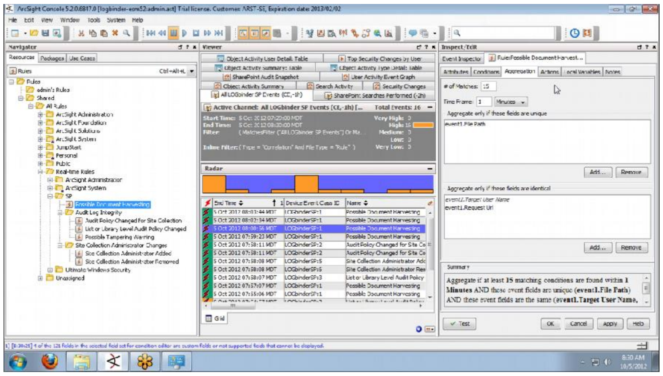
Outputs

Enabled	Name	Noise Events	Include XML
✓	LOGbinder SQL Event Log		
	Security Log		
	Syslog CEF		
	Syslog-Generic		
	Syslog-CEF (File)		
✓	Syslog-Generic (File)		

LOGbinder SQL Licensed for Microsoft SQL 2008/2012 Enterprise

LOGbinder

- SQL Events showing up in your SIEM within seconds


ArcSight Console 5.2.0.6817.0 [logbinder-esm52:admin.ast] Trial license. Customer: ARST-SE, Expiration date: 2013/02/02
File
Edit
View
Window
Tools
System
Help
Navigator
Resources
Packages
Use Cases
Rules
Ctrl+Alt+L
Rules
admin's Rules
Shared
All Rules
ArcSight Administration
ArcSight Foundation
ArcSight Solutions
ArcSight System
JumpStart
Personal
Public
Real-time Rules
ArcSight Administration
ArcSight System
SP
Possible Document Harvesting
Audit Log Integrity
Audit Policy Changed For Site Collection
List or Library Level Audit Policy Changed
Possible Tampering Warning
Site Collection Administrator Changes
Site Collection Administrator Added
Site Collection Administrator Removed
Ultimate Windows Security
Unassigned
Viewer
Object Activity User Detail: Table
Top Security Changes by User
Object Activity Summary: Table
Object Activity Type Detail: Table
SharePoint Audit Snapshot
User Activity Event Graph
Object Activity Summary
Search Activity
Security Changes
All LOGbinder SP Events (CE,-1h)
SharePoint Searches Performed (-2h)
Radar
Grid
Inspect/Edit
Event Inspector
Rule:Possible Document Harvest...
Attributes
Conditions
Aggregation
Actions
Local Variables
Notes
Add...
Remove
Test
OK
Cancel
Apply
Help
8:30 AM
10/5/2012

Active Channel: All LOGbinder SP Events (CE,-1h) [... Total Events: 16

Start Time: 5 Oct 2012 07:29:00 MDT
End Time: 5 Oct 2012 08:30:00 MDT
Filter: (MatchesFilter ("All LOGbinder SP Events") Or Ma...
Inline Filter: (Type = "Correlation" And File Type = "Rule")

Very High: 0
High: 16
Medium: 0
Low: 0
Very Low: 0

End Time	Device Event Class ID	Name
5 Oct 2012 08:03:44 MDT	LOGbinderSP:1	Possible Document Harvesting
5 Oct 2012 08:02:34 MDT	LOGbinderSP:1	Possible Document Harvesting
5 Oct 2012 08:00:56 MDT	LOGbinderSP:1	Possible Document Harvesting
5 Oct 2012 07:59:23 MDT	LOGbinderSP:1	Possible Document Harvesting
5 Oct 2012 07:58:11 MDT	LOGbinderSP:2	Audit Policy Changed For Site Co
5 Oct 2012 07:58:11 MDT	LOGbinderSP:2	Audit Policy Changed For Site Co
5 Oct 2012 07:58:08 MDT	LOGbinderSP:5	Site Collection Administrator Adc
5 Oct 2012 07:58:08 MDT	LOGbinderSP:6	Site Collection Administrator Rer
5 Oct 2012 07:58:07 MDT	LOGbinderSP:3	List or Library Level Audit Policy
5 Oct 2012 07:57:07 MDT	LOGbinderSP:1	Possible Document Harvesting
5 Oct 2012 07:55:06 MDT	LOGbinderSP:1	Possible Document Harvesting

# of Matches: 15
Time Frame: 1 Minutes

Aggregate only if these fields are unique
event1.File Path

Aggregate only if these fields are identical
event1.Target User Name
event1.Request Url

Summary
Aggregate if at least **15** matching conditions are found within **1 Minutes** AND these event fields are unique (**event1.File Path**) AND these event fields are the same (**event1.Target User Name,**

1] [8:30:25] 4 of the 121 fields in the selected field set for condition editor are custom fields or not supported fields that cannot be displayed.

LOGbinder

- Benefits
  - Application security intelligence for SQL Server
  - Fill the audit gap in your compliance efforts
  - Catch APTs that have penetrated upstream defenses
  - Less push back from database admins
  - Zero Impact
    - Use SQL Server's fastest, most efficient audit log output method and thereby offload all subsequent log processing from busy database servers to a server of your choice.
    - No agent required. LOGbinder SQL does not require an agent to be installed on your SQL Servers. In fact, LOGbinder SQL doesn't even need to send a single packet to your database servers.
  - Know what's happening inside of SQL Server including
    - Security operations involving logins, roles and permissions
    - Maintenance of tables, stored procedures and any other object
    - Database operations like backup and restore
    - Transact SQL table commands like insert, delete, update and select
  - Correlate SQL Server security activity with related events from the rest of your environment
  - No data silos or additional consoles to monitor

Bottom line

- SQL Server is where your is
  - Not monitoring it with your SIEM is risky and non-compliant
- LOGbinder bridges the gap between SQL Server and your SIEM
- Now your SIEM can detect database intrusions within seconds
  - Without impacting your DB
- Download a free trial at
  - www.logbinder.com
- Free whitepaper
  - **Comparison: SQL Server Audit and SQL Trace**
  - http://1drv.ms/1w96eNw