



## Top 6 Security Events to Monitor in SQL Server

Sponsored by  
**LOGbinder SQL**

© 2013 Monterey Technology Group Inc.



Thanks to

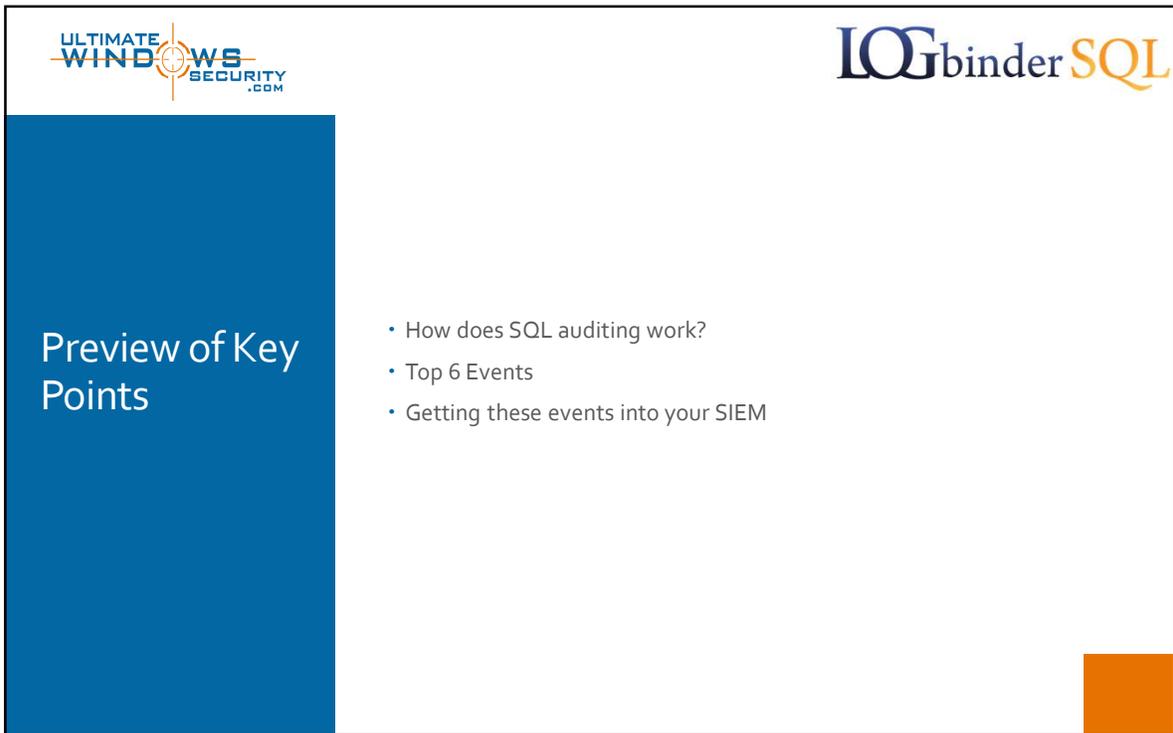
• Made possible by

**LOGbinder SQL**

<http://www.logbinder.com/products/logbindersql>

A Randy Franklin Smith Company

© 2013 Monterey Technology Group Inc.



ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

Preview of Key Points

- How does SQL auditing work?
- Top 6 Events
- Getting these events into your SIEM

This slide features a blue vertical bar on the left containing the title 'Preview of Key Points'. The main content area is white and contains a bulleted list of three items. The logos for 'ULTIMATE WINDOWS SECURITY .COM' and 'LOGbinder SQL' are positioned at the top left and top right respectively. A small orange square is located in the bottom right corner of the slide.



ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

How SQL auditing works

- What can you audit?

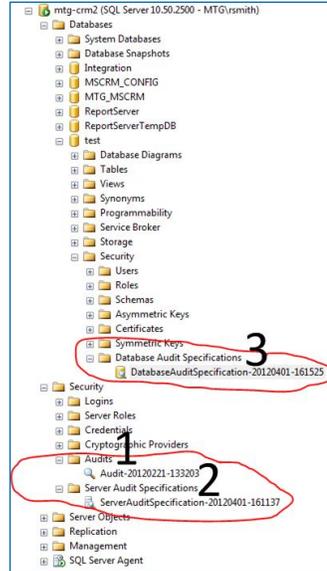
Everything

This slide features a blue vertical bar on the left containing the title 'How SQL auditing works'. The main content area is white and contains a single bulleted item. The word 'Everything' is written in large, bold, orange letters with a yellow glow effect across the bottom of the slide. The logos for 'ULTIMATE WINDOWS SECURITY .COM' and 'LOGbinder SQL' are positioned at the top left and top right respectively. A small orange square is located in the bottom right corner of the slide.

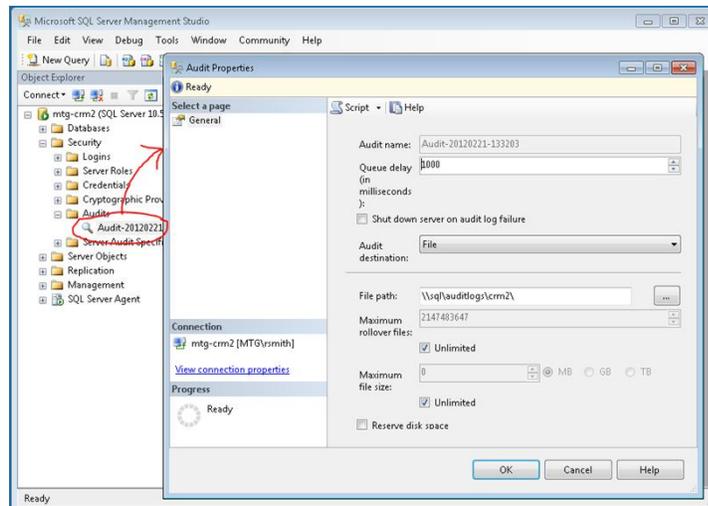


# SQL Server Auditing

- 3 audit policy objects
  1. Server Audit
  2. Server Audit Specification
  3. Database Audit Specification



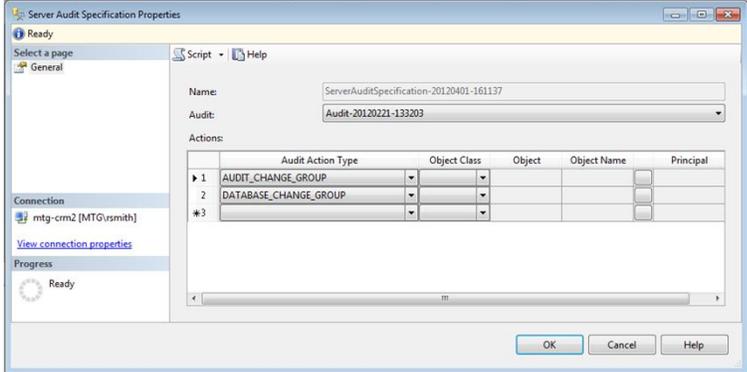
# SQL Server Auditing







## SQL Server Auditing



The screenshot shows the 'Server Audit Specification Properties' dialog box. The 'Name' field contains 'ServerAuditSpecification-20120401-161137' and the 'Audit' dropdown is set to 'Audit-20120221-133203'. The 'Actions' section contains a table with the following data:

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

The 'Connection' section shows 'mtg-crm2 [MTG\smith]' and the 'Progress' section shows 'Ready'. Buttons for 'OK', 'Cancel', and 'Help' are at the bottom right.





## SQL Server Auditing

- Audit action groups
  - Categories of auditable activity
  - Assigned at the
    - Server level
    - Database level




## SQL Audit Logs

- Windows Event Log
  - Application or Security
- Binary file
  - Readable by any edition of SQL Server
  - <audit\_name>\_<audit\_guid>\_nn\_<timestamp\_as\_bigint>.sqlaudit
  - SELECT \* FROM fn\_get\_audit\_file('E:\SqlAudits\\*', default, default)
  - Over 2 dozen columns




## SQL Audit Logs

```

event_time:2010-09-16 12:35:30.0787755
sequence_number:1
action_id:APRL
succeeded:true
permission_bitmask:0
is_column_permission:false
session_id:54
server_principal_id:260
database_principal_id:1
target_server_principal_id:0
target_database_principal_id:0
object_id:7
class_type:RL
session_server_principal_name: ACME\SPAdministrator
server_principal_name: ACME\SPAdministrator
server_principal_sid:0
database_principal_name: dbo
target_server_principal_name: ACME\SPAdministrator
target_server_principal_sid: 0
target_database_principal_name: John Smith
server_instance_name: SPDEV\SQLo8ENT
database_name: AuditTest
schema_name:
object_name: Human Resources
statement: EXEC sp_addrolemember N'Human Resources', N'John Smith'
            
```

**At 12:35AM on 9/16/2010, ACME\SPAdministrator added John Smith to the Human Resources role in the AuditTest database on SQL Server SPDEV\SQLo8ENT**

ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

## SQL Audit Logs

- For best performance and security
  - Generate binary audit logs
  - Can target a remote shared folder
- But how do you get that to your SIEM?
  - Stand by...

ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

## Top 6 Events to Monitor

1. Admin authority changes
2. Permission changes
3. Role membership changes
4. Failed logons
5. Data exports by privileged users
6. New logins/principals



# #1

## Admin authority changes

- Changes to built-in roles at the server and database level
- Add to Server Audit Specification
  - SERVER\_ROLE\_MEMBER\_CHANGE\_GROUP
  - DATABASE\_ROLE\_MEMBER\_CHANGE\_GROUP
- Monitor for
  - action\_id = APRL
  - object\_name =

Server roles	Database roles
bulkadmin	db_accessadmin
dbcreator	db_backupoperator
diskadmin	db_datareader
processadmin	db_datawriter
<u>public</u>	db_ddladmin
securityadmin	db_denydatareader
serveradmin	db_denydatawriter
setupadmin	db_owner
sysadmin	db_securityadmin
	<u>public</u>

- Who got or lost permissions
  - target\_server\_principal\_name
  - target\_database\_principal\_name
- Database (if applicable) = database\_name
- Who did it = server\_principal\_name



# #2

## Permission and owner changes

- Add to Server Audit Specification
  - SERVER\_OBJECT\_PERMISSION\_CHANGE\_GROUP,
  - SERVER\_PERMISSION\_CHANGE\_GROUP,
  - DATABASE\_PERMISSION\_CHANGE\_GROUP,
  - SCHEMA\_OBJECT\_PERMISSION\_CHANGE\_GROUP,
  - DATABASE\_OBJECT\_PERMISSION\_CHANGE\_GROUP,
  - DATABASE\_OWNERSHIP\_CHANGE\_GROUP,
  - SCHEMA\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP,
  - DATABASE\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP,
  - SERVER\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP



## Permission changes

- Monitor for
  - action\_id = G, GWG, R, RWG, RWC
- Who got or lost permissions
  - target\_server\_principal\_name
  - target\_database\_principal\_name
- Object whose permissions changed = object\_name
  - Database (if applicable) = database\_name
  - Schema (if applicable) = schema\_name
- Who did it = server\_principal\_name
- Which permissions = statement



## Owner changes

- Monitor for
  - action\_id = TO
- Who got ownership
  - target\_server\_principal\_name
  - target\_database\_principal\_name
- Object whose ownership changed = object\_name
  - Database (if applicable) = database\_name
  - Schema (if applicable) = schema\_name
- Who did it = server\_principal\_name

# #3

## Role membership changes

- Changes to built-in roles at the server and database level
- Add to Server Audit Specification
  - SERVER\_ROLE\_MEMBER\_CHANGE\_GROUP
  - DATABASE\_ROLE\_MEMBER\_CHANGE\_GROUP
- Monitor for
  - action\_id = APRL
- Who got or lost permissions
  - target\_server\_principal\_name
  - target\_database\_principal\_name
- Database (if applicable) = database\_name
- Who did it = server\_principal\_name

# #4

## Failed logons

- Add to Server Audit Specification
  - SERVER\_ROLE\_MEMBER\_CHANGE\_GROUP
  - DATABASE\_ROLE\_MEMBER\_CHANGE\_GROUP
- Monitor for
  - action\_id = LGIF
- User name attempted = server\_principal\_name
- Reason = statement



# #5

## Database backed up privileged users

- Add to Server Audit Specification
  - BACKUP\_RESTORE\_GROUP
- Monitor for
  - action\_id = BA
- Who did it = server\_principal\_name
  - Filter out backups by backup applications
- Are there more operations?



# #6

## New logins and users

- Add to Server Audit Specification
  - SERVER\_PRINCIPAL\_GROUP
  - DATABASE\_PRINCIPAL\_GROUP
- Monitor for
  - action\_id = CR

• class=

class_type	class_type_desc	securable_class_desc
US	USER	USER
LX	LOGIN	LOGIN
AU	ASYMMETRIC KEY USER	USER
CU	CERTIFICATE USER	USER
GU	GROUP USER	USER
SU	SQL USER	USER
WU	WINDOWS USER	USER
AL	ASYMMETRIC KEY LOGIN	LOGIN
CL	CERTIFICATE LOGIN	LOGIN
SL	SQL LOGIN	LOGIN
WG	WINDOWS GROUP	LOGIN
WL	WINDOWS LOGIN	LOGIN

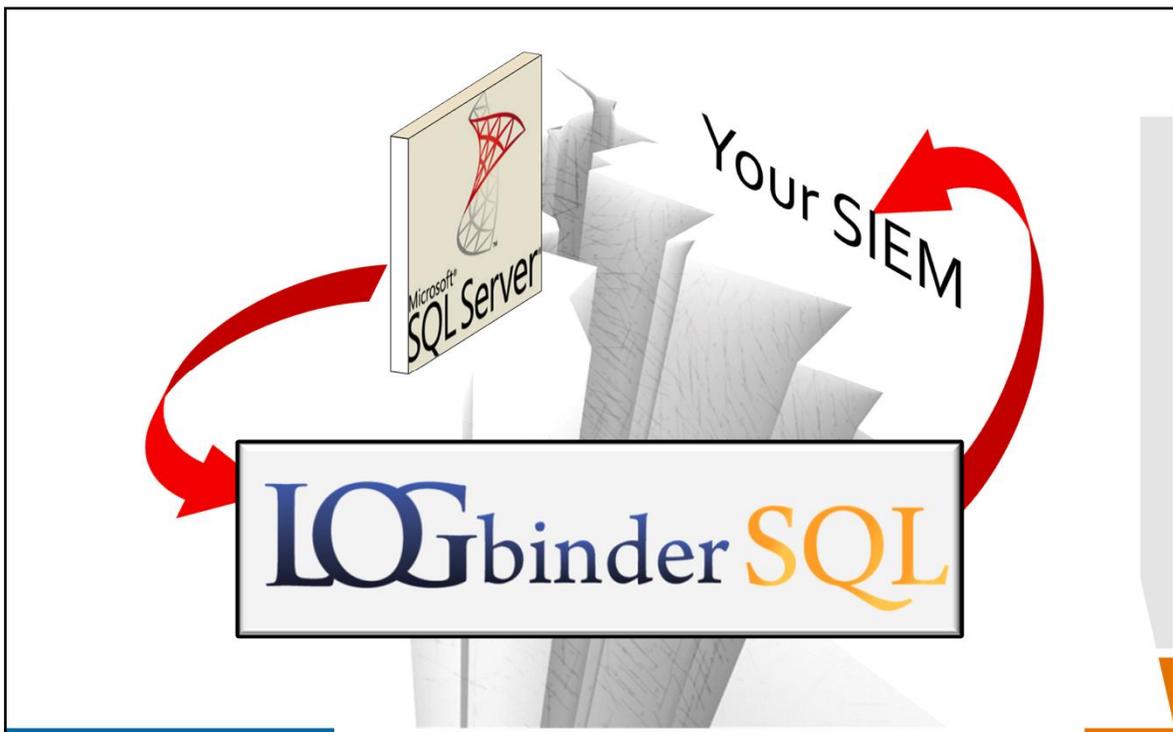
- Who did it = server\_principal\_name
- New login/user = object\_name





## Bottom Line

- Awesome audit logging
  - Comprehensive, consistent, flexible
- Log management and security issues
  - To be consumed by SIEM solutions directly
    - Must use lower performance Windows event log
    - Usually agent required = push back by db admins
  - Binary logs preferable for performance, security and db admin acceptance
  - Either way you have 349 different audit events reflected in one message structure
    - Cryptic and complicated to interpret



ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

Bridge the gap

- LOGbinder SQL
  - No agent on your SQL Servers
  - Higher performance binary log format
  - Translates cryptic, raw audit data into easy-to-understand audit messages
  - Resolves cryptic Action IDs
  - Outputs to
    - Windows Security Log
    - Syslog
    - Common Event Format (for ArcSight)

ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

LOGbinder SQL

[www.logbinder.com](http://www.logbinder.com)

Bridge the Gap Between Exchange and Your SIEM