



# Using Splunk and LOGbinder to Monitor SQL Server, SharePoint and Exchange Audit Events

Sponsored by



© 2015 Monterey Technology Group Inc.

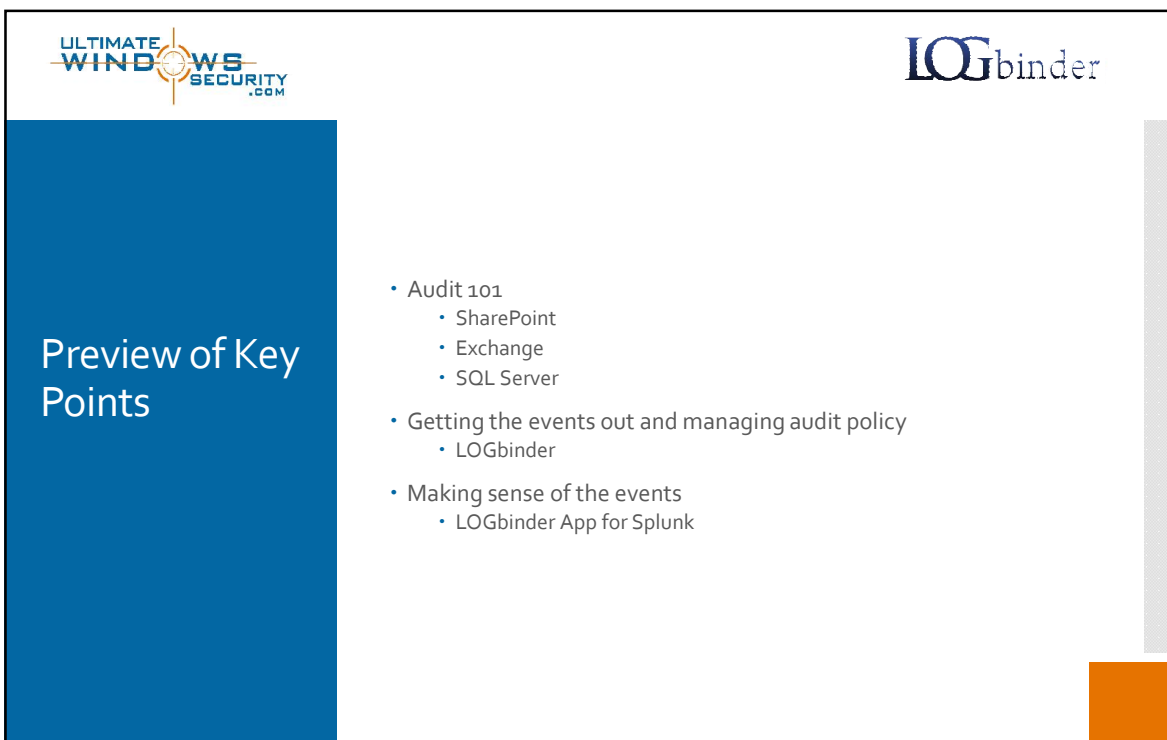


Thanks to

• Made possible by



© 2015 Monterey Technology Group Inc.

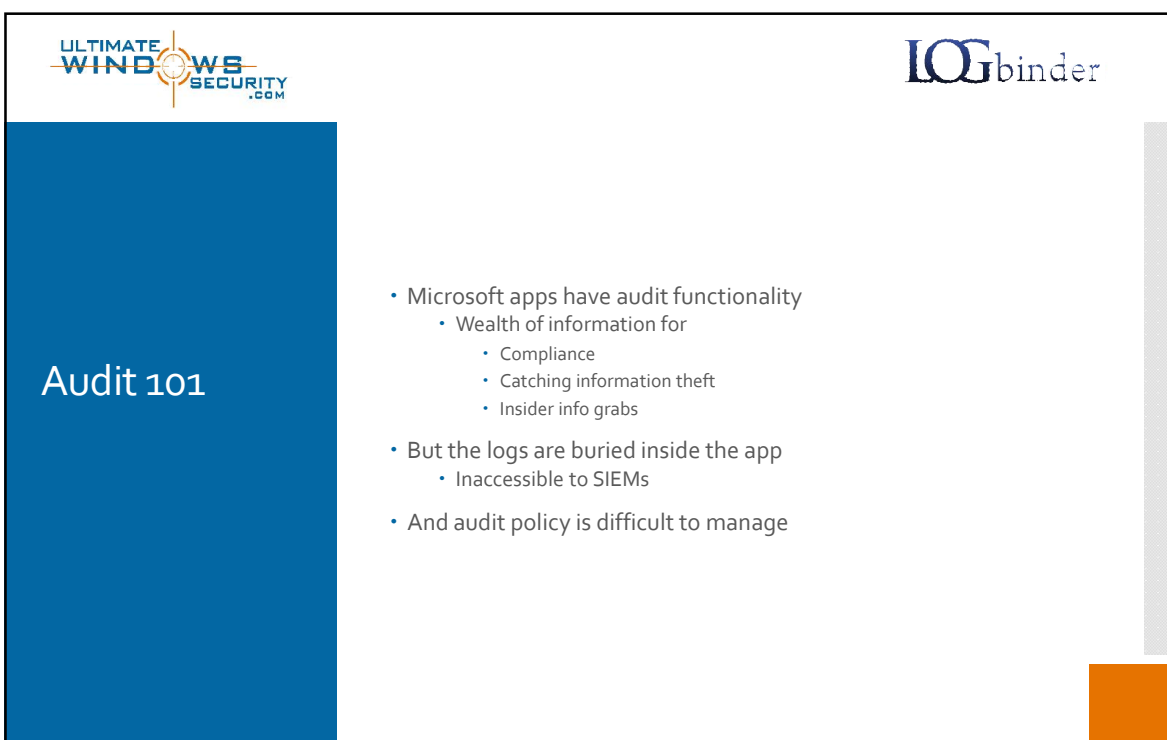


ULTIMATE  
WINDOWS  
SECURITY  
.COM

LOGbinder

## Preview of Key Points

- Audit 101
  - SharePoint
  - Exchange
  - SQL Server
- Getting the events out and managing audit policy
  - LOGbinder
- Making sense of the events
  - LOGbinder App for Splunk



ULTIMATE  
WINDOWS  
SECURITY  
.COM

LOGbinder



## Audit 101

- Microsoft apps have audit functionality
  - Wealth of information for
    - Compliance
    - Catching information theft
    - Insider info grabs
- But the logs are buried inside the app
  - Inaccessible to SIEMs
- And audit policy is difficult to manage



SharePoint

- Webinars
  - [Detecting Information Grabs of Confidential Documents in SharePoint](#)
  - [Top 10 Security Events to Monitor in SharePoint](#)
  - [SharePoint Defense-In-Depth Monitoring: What to Watch at the App, DB and OS Level – and How?](#)
- More info
  - [Comparing SharePoint 4 Audit Logs for Security and SIEM Integration](#)
  - [Top 6 Security Events to Audit in SharePoint](#)
  - [SharePoint Audit Events List](#)
  - More at <https://www.logbinder.com/Resources/>
  - And <https://www.ultimatewindowssecurity.com/sharepoint>



SharePoint

- What types of activity?
  - Content viewed
    - Information grabs
  - Documents downloaded
  - Content modified
  - Document library and list permissions changed
  - SharePoint groups changed
  - Administrators access granted
  - Document deletion
  - Export of data
  - Check in/Check out



# SharePoint


- Where are the events?
  - Trapped inside SharePoint
  - In the SharePoint content database
  - Not in
    - Simple table
    - Log file
    - Event log
  - Only accessible
    - SharePoint admin web pages
    - SharePoint server-side API




# SharePoint

- Even if you do create an audit log report...

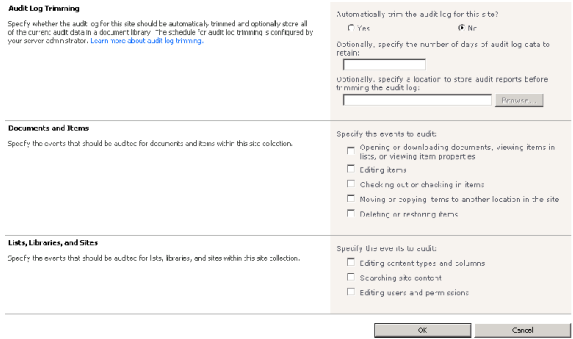
Site ID	Item ID	Item Type	Document	Occurred (GMT)	Event	Event Data
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Group Create	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <groupname>=New Group
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Group Update	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <groupname>=New Group; <updateinfo>=New Group
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Group Member Add	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <groupname>=New Group; <username>=New Group
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Group Member Remove	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <groupname>=New Group; <username>=New Group
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Group Member Add	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <groupname>=New Group; <username>=New Group
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Group Member Remove	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <groupname>=New Group; <username>=New Group
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role
223c500a-4773-4166-8784-c08b1813c0	223c500a-4773-4166-8784-c08b1813c0	Site Collection		2011-11-22T08:05:19	Security Role End Break	<siteid>=223c500a-4773-4166-8784-c08b1813c0; <roleid>=New Role







SharePoint

- How to enable?
  - Each site collection has it's own audit policy







Exchange

- What can you audit?
  - Privileged user activity
    - Admin audit log
  - Non-owner mailbox access
    - Mailbox audit log
- Configuration
  - Admin audit log
    - Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets \* -AdminAuditLogParameters \*
  - Mailbox audit
    - Must turn on auditing on each mailbox individually

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Exchange

- Where are the logs?
  - System mailbox for admin audit log
  - Inside each user's mailbox
- How do you access the logs?
  - Run reports interactively from the Exchange Control Panel
  - Request reports via PowerShell to be delivered by email
  - There is no log file to monitor

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

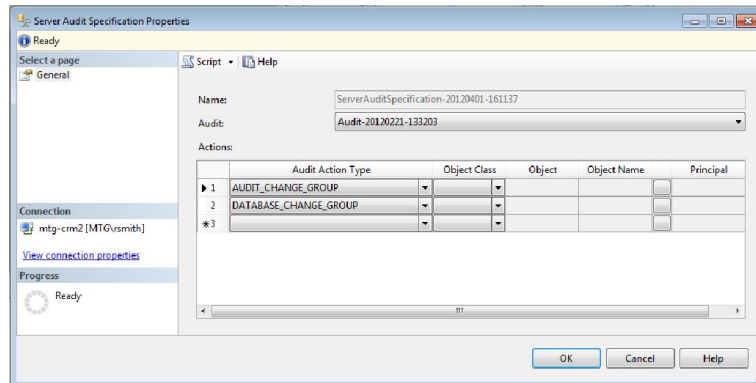
Exchange

- Webinars
  - [Managing Mailbox Audit Policy in Exchange 2013](#)
  - [Detecting Non-Owner Mailbox Access with Exchange Mailbox Auditing](#)
  - [Understanding Exchange 2010 Audit Logging](#)
- More info
  - [Comparing Exchanges 3 Audit Logs for Security and SIEM Integration](#)
  - [Exchange Audit Events List](#)
  - More at <https://www.logbinder.com/Resources/>
  - And <https://www.ultimatewindowssecurity.com/exchange>

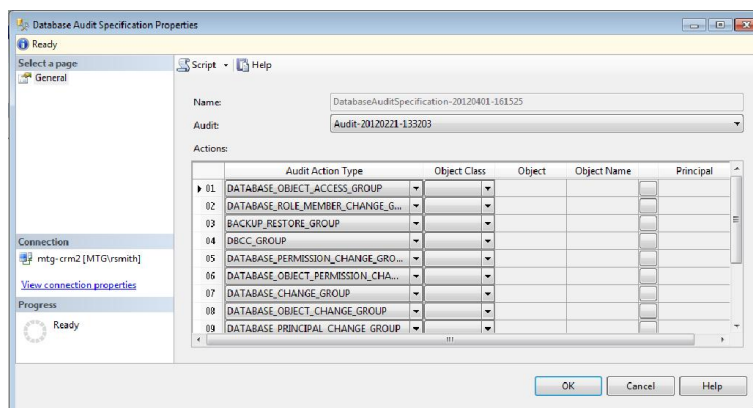
## SQL Server

- 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



## SQL Audit



## SQL Server



- SQL Audit can send logs
  - To a binary log file elsewhere on network
  - Directly to local Windows Security Log
- Here's why that doesn't work for enterprise log management
  - Performance
  - Stability
  - Security
  - Agent
- SQL Audit binary logs
  - Fast
  - Agentless
  - Secure
  - Stable
  - DB admins much happier
- But how do you read binary audit logs into your SIEM?





## SQL Server

- Webinars
  - [Top 6 Security Events to Monitor in SQL Server](#)
  - [Not Monitoring SQL Server with Your SIEM is Close to Negligent: What are Your Options?](#)
- More info
  - [Comparison: SQL Server Audit and SQL Trace](#)
  - More at <https://www.logbinder.com/Resources>
  - And <https://www.ultimatewindowssecurity.com/sqlserver>



## Getting the Logs Out

- Getting these logs out of SQL Server, Exchange and SharePoint is difficult
  - Cryptic
  - Require enrichment
  - Methods are weird and complex

## Getting the Logs Out

splunk >

## LOGbinder

- 5 minutes to install
- Configure input
  - SQL Servers to monitor
  - Exchange environment URLs
  - SharePoint farms
- Configure output
  - Log format
  - Destination path or IP address
- Done!

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

LOGbinder



- Audit policy managed for you
  - SharePoint site collections
  - SQL Audit Policy Wizard
  - Exchange mailbox audit policy controlled by group or OU

ULTIMATE WINDOWS SECURITY .COM

LOGbinder



Splunk

- Not a SIEM
- But
  - Easy
  - Fun
  - Powerful
  - Free
    - 500 MB a day
    - No alerting and other "enterprise" features
- Splunk Light
  - Affordable for SMBs
- Splunk Enterprise
  - Expensive; price by GB indexed per day
- The secret to making Splunk affordable
  - Filtering out the noise

## LOGbinder App for Splunk

- Teaches Splunk how to understand audit logs from
  - SharePoint
  - SQL Server
  - Exchange
- Delivered by LOGbinder
- Includes
  - 4 Dashboards
  - 30+ Reports

## Deployment

- Install LOGbinder
  - Configure output to shared folder
  - Getting started guides: <https://www.logbinder.com/Resources/>
- Install Splunk
  - [http://www.splunk.com/en\\_us/download/splunk-enterprise.html](http://www.splunk.com/en_us/download/splunk-enterprise.html)
- Install LOGbinder App for Splunk
  - [LOGbinder for Splunk Beta](#)
- Configure Splunk to consume logs in shared folder


**splunk>** Apps


Files & directories  
Data inputs > Files & directories

New

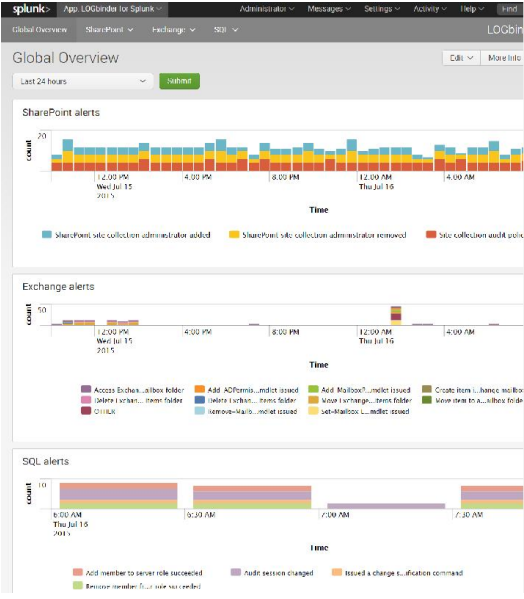
Showing 19 of 3 items

Full path to your data	Set host	Source type	Set the destination index
\$SPLUNK_HOME\var\log\splunk\version	Constant Value	splunk_version	_internal
\$SPLUNK_HOME\var\log\input\ospection	Constant Value	Automatic	introspection
\$SPLUNK_HOME\var\log\splunk	Constant Value	Automatic	_internal
\$SPLUNK_HOME\var\log\pool\splunk	Constant Value	Automatic	default
\$SPLUNK_HOME\var\log\pool\splunk_stash_new	Constant Value	stash_new	default
\$WINDIR\System32\DRIVE1	Constant Value	DriveSysLog	windows
\$WINDIR\System32\log	Constant Value	WindowsUpdateLog	windows
C:\Users\log\log	Constant Value	logbinder\syslog	logbinder
C:\Users\log\log	Constant Value	logbinder\syslog	logbinder







## LOGbinder App for Splunk



The screenshot shows the Splunk interface for the LOGbinder app. It features a 'Global Overview' section with three stacked bar charts: 'SharePoint alerts', 'Exchange alerts', and 'SQL alerts'. Each chart shows the count of alerts over time, with a legend below each chart identifying specific alert types. The SharePoint alerts chart shows events like 'SharePoint site collection administrator added', 'SharePoint site collection administrator removed', and 'Site collection audit policy'. The Exchange alerts chart shows events like 'Access Schedules... folder', 'Add ACForms... folder', 'Add Mailbox... folder', 'Create Item L... folder', 'Delete Outlook... folder', 'Delete Outlook... folder', 'Move Exchange... folder', and 'Move Item to... folder'. The SQL alerts chart shows events like 'Add member to server role succeeded', 'Audit session changed', and 'Issued a charge... command'.





## Bottom line

- Don't be blind to what's happening inside your most important applications
- SQL, SharePoint and Exchange audit logs are important
- LOGbinder bridges the gap and brings application security intelligence to your SIEM
- If you can't afford a SIEM, try Splunk Free or Splunk Light
- If you already have and love Splunk
- Get the LOGbinder App for Splunk
- Monitor and respond to security events inside your apps
- Correlate application security intelligence with all the other security intelligence in your enterprise
- Comply and stop attacks and info grabs



LOGbinder

**SIEM Synergy Partners**

These valuable partners have built support for LOGbinder into their SIEM solutions.



**Integrations by LOGbinder**

We have developed integrations for the SIEM solutions listed below.

