SharePoint Defense-In-Depth Monitoring: What to Watch at the App, DB and OS Level – and How?

Sponsored by

LOGbinder

Thanks to

- Made possible by

LOGbinder
Application Security Intelligence for your SIEM
www.logbinder.com

Preview of key points

- The SharePoint "Stack"
  - Application
  - Web server
  - Database
  - Operating system
- 4 Questions
  - What types of activity
  - Where are the events
  - How to enable
  - Accessible to SIEM

Operating System

- What types of activity?
  - Windows system security events
    - Top 12 Security Events To Monitor on Member Servers
      - https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=29
  - Authentication
    - SharePoint uses Windows authentication
    - No "logon" event or "logon session" in SharePoint
    - Logged to Windows security log as Event ID 4624 with Logon Type 3

Operating System

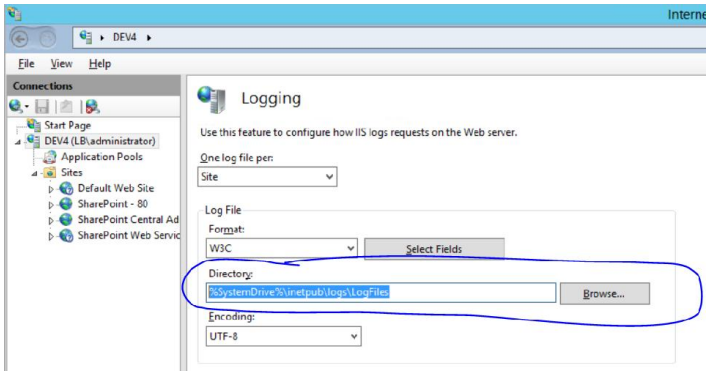
- Where are the events?
  - Windows Security Log
- How to enable?
  - Group Policy or auditpol
  - Subcategories
    - Audit Logon
    - Audit User Account Management
    - Audit Security Group Management
    - Audit Process Creation
    - Audit Policy Change
    - Audit Authentication Policy Change
    - Audit Authorization Policy Change
    - Audit Security State Change
    - Audit Security System Extension
    - Audit System Integrity
- Accessible to SIEM?
  - Yes
  - Must collect from each server in farm

Web Server

- Basic understanding of HTTP
  - Client request
    - verbs
  - Server response
    - Status codes
  - URI
    - Especially parameters
      - ?param=value
- Attack methods and tactics
  - http://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-web-applications-log-files-2074
- What types of activity?
  - Web page requests
    - Client
    - Server
    - URL
    - Response

Web Server

- Where are the events and how to enable?



- Accessible to SIEM?
  - Yes
  - Must collect from each server in farm

Web Server

- Catching Web Based Attacks with W3C Logs from IIS
  - https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=272

Database

- What types of activity
  - SQL Server level security events
  - Database level security configuration changes
  - Privileged user access
- Top 6 events
  - https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=213
  - Admin authority changes
  - Permission changes
  - Role membership
  - Security setting changes
  - Failed logons
  - Data exports by privileged users

Database

- Where are the events
  - Depends on version of SQL Server
  - Prior to SQL 2008
    - No true audit log
    - SQL Trace
      - All or nothing
      - Big performance hit
      - Tremendous noise
  - SQL Server 2008 and later
    - New SQL Audit function
    - Define exactly what to audit
      - Who
      - What objects
      - Which actions

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Database

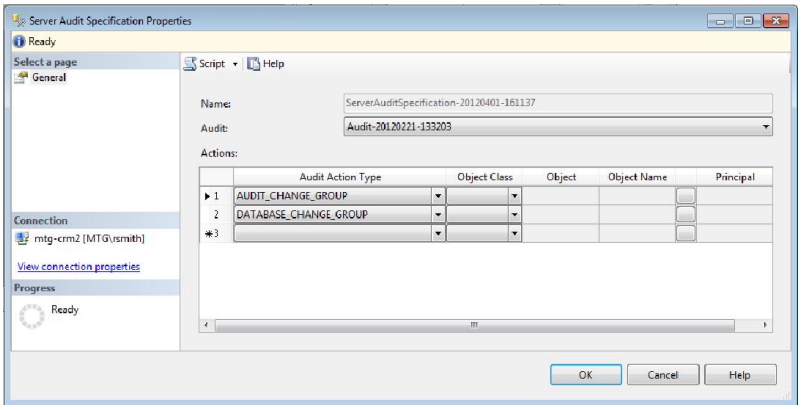
- SQL Server Audit allows you to track administrator, application and user level activity across all types of objects and operations. You can track
  - security operations involving logins, roles and permissions
  - maintenance of tables, stored procedures and any other object
  - database operations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

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Database

- How to enable



ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Database

- Accessible to SIEM?
  - Output – 2 different formats available
    - Windows event log
    - binary file format readable through a stored procedure
  - 5 reasons why you shouldn't use the event log
    - Performance
    - Security
    - Stability
    - Hard to understand
    - DB admin push back

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Database

- 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
  - LOGbinder for SQL Server to the rescue
    - https://www.logbinder.com/Products/LOGbinderSQL/
- Not Monitoring SQL Server with Your SIEM is Close to Negligent: What are Your Options?
  - https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=282

Application

- 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

Application

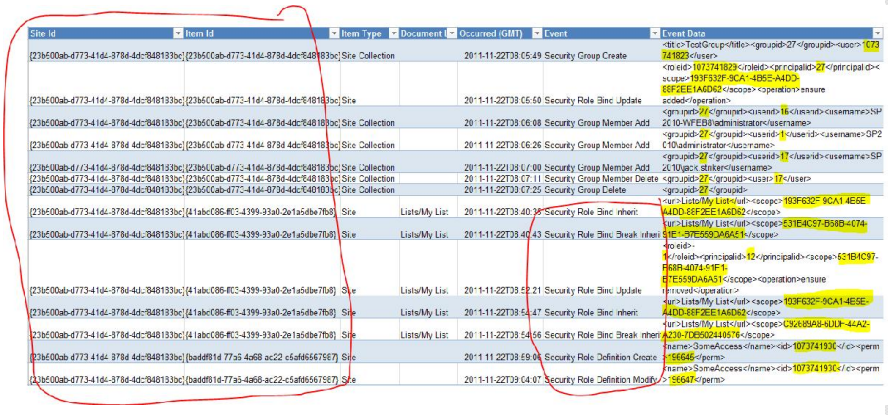
- Where are the events?
  - Trapped inside SharePoint
  - In the SharePoint content database
  - Not in
    - Simple table
    - Log file
    - Event log
  - Only accessible
    - SharePoint admin web pages
    - SharePoint server-side API

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Application

- Even if you do create an audit log report…



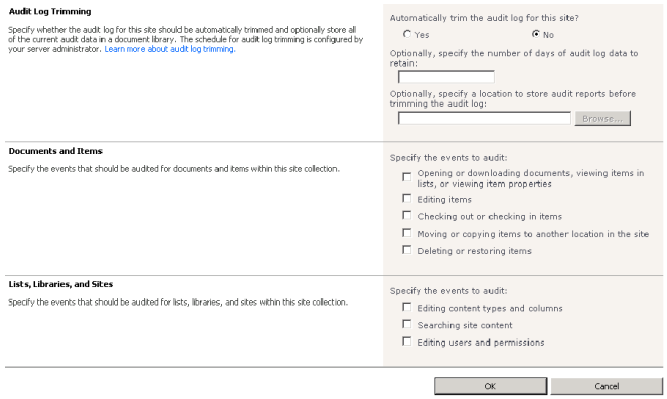
Site Id	Item Id	Item Type	Document I	Occurred (GMT)	Event	Event Data
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site Collection		2011-11-22T38:05:49	Security Group Create	<title>TestGroup</title><groupid>27</groupid><uco>"C73741823</user>
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site		2011-11-22T38:06:50	Security Role Binc Update	<ro eid>1073741829</roleid><principalid>27</principalid><scope>193F532F-9CA1-4B65-A4DD-68F2EE1A6D62</scope><operation>ensure added</operation>
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site Collection		2011-11-22T38:06:08	Security Group Member Add	<groupid>27</groupid><userid>16</userid><username>SP2010-WFEB8\administrator</username>
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site Collection		2011-11-22T38:06:26	Security Group Member Add	<groupid>27</groupid><userid>1</userid><username>SP2010\administrator</username>
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site Collection		2011-11-22T38:07:00	Security Group Member Add	<groupid>27</groupid><userid>17</userid><username>SP2010\jack stinker</username>
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site Collection		2011-11-22T38:07:11	Security Group Member Delete	<groupid>27</groupid><user>17</user>
{23b600ab-d773-41d4-378d-4dc8481838c}	{23b600ab-d773-41d4-873d-4dc8481838c}	Site Collection		2011-11-22T38:07:25	Security Group Delete	<groupid>27</groupid>
{23b600ab-d773-41d4-378d-4dc8481838c}	{41abc086-ff03-4399-93a0-2e1a5dbe7fb8}	Site	Lists/My Lis:	2011-11-22T38:40:36	Security Role Binc nheri:	<ur>Lists/My List</url><scope>193F532F-9CA1-4E6E-A4DD-68F2EE1A6D62</scope>
{23b600ab-d773-41d4-378d-4dc8481838c}	{41abc086-ff03-4399-93a0-2e1a5dbe7fb8}	Site	Lists/My Lis:	2011-11-22T38:40:43	Security Role Binc Break nheri	<ur>Lists/My List</url><scope>E31E4C67-B58B-4C74-81E1-57E559DA6A51</scope>
{23b600ab-d773-41d4-378d-4dc8481838c}	{41abc086-ff03-4399-93a0-2e1a5dbe7fb8}	Site	Lists/My Lis:	2011-11-22T38:52:21	Security Role Binc Update	<ro eid><roleid>12</roleid><principalid><scope>621B4C97-F58B-4074-81F1-57E559DA6A51</scope><operation>ensure removed</operation>
{23b600ab-d773-41d4-378d-4dc8481838c}	{41abc086-ff03-4399-93a0-2e1a5dbe7fb8}	Site	Lists/My Lis:	2011-11-22T38:54:47	Security Role Binc nheri:	<ur>Lists/My List</url><scope>193F532F-9CA1-4E6E-A4DD-68F2EE1A6D62</scope>
{23b600ab-d773-41d4-378d-4dc8481838c}	{41abc086-ff03-4399-93a0-2e1a5dbe7fb8}	Site	Lists/My Lis:	2011-11-22T38:54:56	Security Role Binc Break nheri	<ur>Lists/My List</url><scope>C52E89A8-6UUF-4CA2-A236-7DE502449576</scope>
{23b600ab-d773-41d4-378d-4dc8481838c}	{baddf81d-77a5-4a68-ac22-c5afd66675E7}	Site		2011-11-22T38:59:03	Security Role Definition Create	<name>SomeAccess</name><id>1073741930</id></c><perm>56646</perm>
{23b600ab-d773-41d4-378d-4dc8481838c}	{baddf81d-77a5-4a68-ac22-c5afd66675E7}	Site		2011-11-22T38:04:07	Security Role Definition Modify	<name>SomeAccess</name><id>1073741930</id></c><perm>56647</perm>

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Application

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

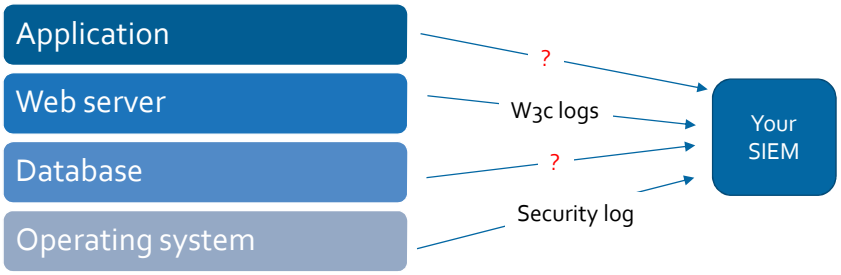


Application

- Accessible to SIEM?
  - No
  - LOGbinder for SharePoint to the rescue
    - https://www.logbinder.com/Products/LOGbinderSP/

LOGbinder

- The SharePoint "Stack"

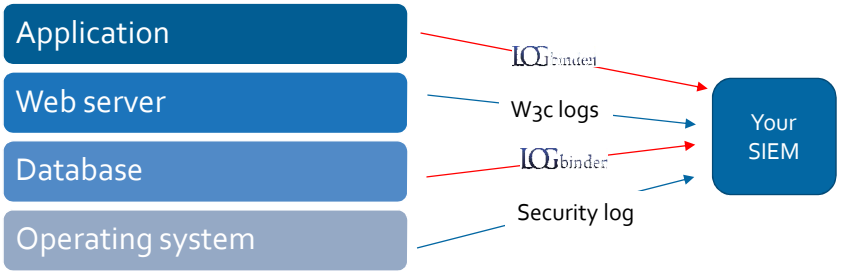


ULTIMATE WINDOWS SECURITY .COM

LOGbinder

LOGbinder

- The SharePoint "Stack"

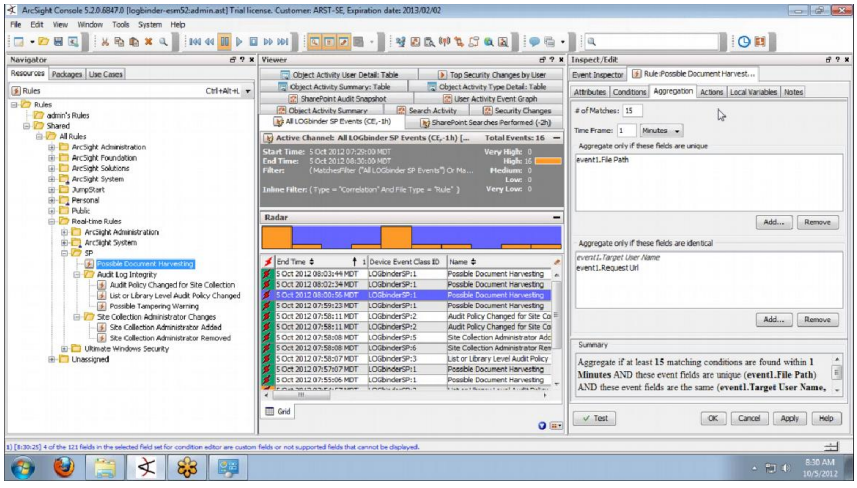


ULTIMATE WINDOWS SECURITY .COM

LOGbinder

LOGbinder

- SQL and SharePoint Events show up in your SIEM within seconds



LOGbinder

SIEM Synergy Partners

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

logpoint solarwinds LogRhythm
EventTracker www.eventtracker.com GFI McAfee
IBM RSA

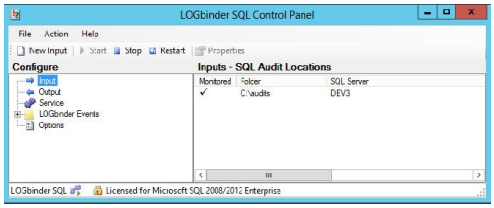
Integrations by LOGbinder

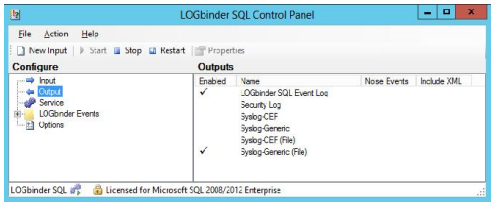
We have developed integrations for the SIEM solutions listed below.

ArcSight An HP Company splunk>

LOGbinder

- 5 minute setup

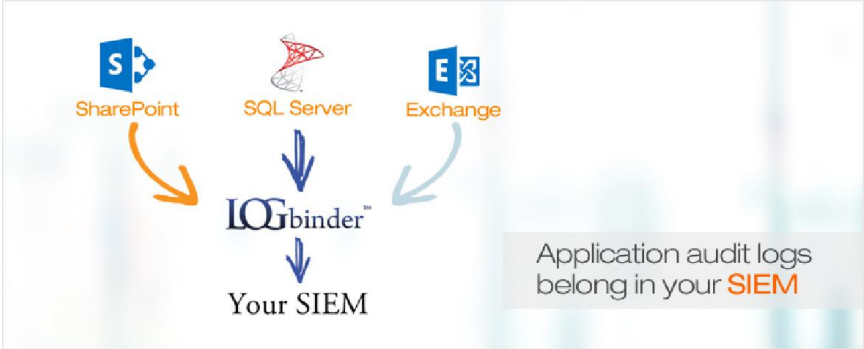




ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Bottom Line



- Contact sales
  - https://www.logbinder.com/Form/Ask
- Download free trial, learn more
  - https://www.logbinder.com/Resources/