Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM™

Monitoring Access to Confidential Information in SharePoint

- Made possible by both: LOGbinder SP™

LOGbinder SP™

Brought to you by

LOGbinder SP™

http://www.logbinder.com/products/logbindersp/

Speaker

- Randy Franklin Smith, Creator of LOGbinder

LOGbinder SP™

Preview of Key Points

- Audit policy
- Reporting
- Building on the foundation

LOGbinder SP™

Confidential Information in SharePoint

- What kind of confidential information do you have in SharePoint?
- Do you have a log management solution?
- Is encryption a requirement for SharePoint?
  - CipherPoint
  - first provider of transparent content encryption solutions for Microsoft SharePoint
  - www.cipherpointsoftware.com

LOGbinder SP™

Native SharePoint audit foundation

- **Available in**
  - WSS 3.0
    - Not exposed in the interface
  - SharePoint 2007
  - SharePoint Foundation
    - Not exposed in the interface
  - SharePoint 2010

LOGbinder SP™

Native SharePoint audit foundation

- **Audit policy defined at the site collection level**
  - Changes to audit policy
  - Permission changes
  - Group membership changes
  - View
  - Check in/out
  - Delete/Update
  - Schema changes
  - Workflow
  - Search

LOGbinder SP™

Monitoring Access to Confidential Information

- **Events to monitor**
  - Audit integrity
  - Access control changes
  - View

LOGbinder SP™

Reporting

- **Audit report for individual document**
  - Compliance Details
- **For document library**
  - Custom Report
    - Select document library
  - Other criteria
    - Time/date
    - User
    - Location

LOGbinder SP™

Native SharePoint audit foundation

- **Audit records written to internal table within content database**
  - Inaccessible to log management solutions
  - Consumes expense SQL/SharePoint storage
  - Insecure to store audit logs on same system where they are generated
- **Rudimentary Excel reports available**
  - Audit codes, object ID numbers, user and group ID numbers not translated
    - Not readable or actionable
  - Criteria extremely limited
- **No alerting**
- **Audit log purging introduced with SP2010**
  - No archival capability

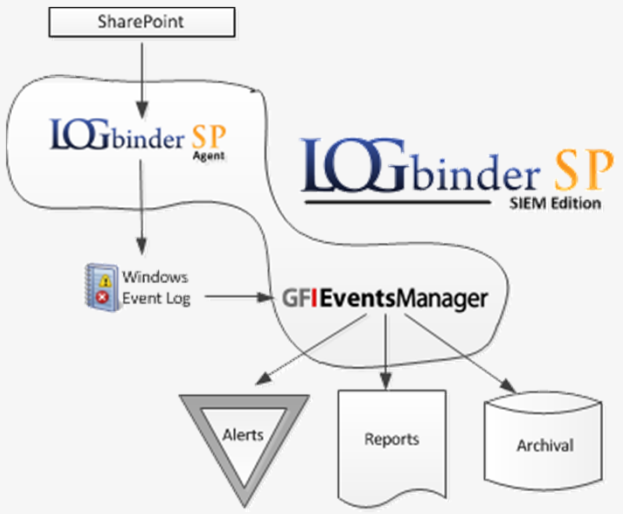
LOGbinder SP™

Native SharePoint audit foundation

- **Limitations in WSS and Foundation**
  - Audit engine present but
    - Audit policy not exposed in the UI
    - No reporting
  - Auditing only possible through application that interfaces with SharePoint API

LOGbinder SP™

Building on the foundation



LOGbinder SP™

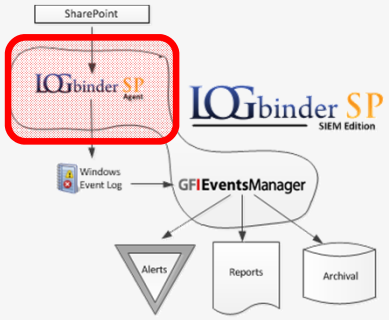
Demo

- LOGbinder SP SIEM Edition

LOGbinder SP™

Building on the foundation

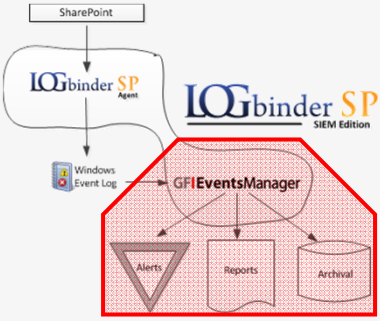
- **LOGbinder SP**
  - Translates SharePoint audit records into human readable audit trail
  - Sends SharePoint audit events to the Windows event log
  - Purges events after export



LOGbinder SP™

Take action on the data

- **GFI EventsManager**
  - Secure log archival
    - Filter on specific fields in events
    - Assign different levels of importance to certain files/users
  - Alerting
    - Critical events can trigger email/SMS/Network message
    - Send alerts to responsible parties for event type
  - Reporting
    - Export events from Event Browser in HTML
    - Schedule reports daily, weekly, monthly



LOGbinder SP™

Bottom Line

- SharePoint increasingly used to store and process sensitive information
- Becoming an IT audit and compliance target
- Auditing, Alerting, Reporting is a must for any technology like SharePoint
- SharePoint native auditing is a foundation technology
- LOGbinder SP SIEM Edition build on that foundation to provide fully managed audit and security monitoring for SharePoint

LOGbinder SP™

- Brought to you by

LOGbinder SP™

http://www.logbinder.com/products/logbindersp/

- Speaker
  - Randy Franklin Smith, Creator of LOGbinder