ULTIMATE WINDOWS SECURITY .COM™

Detecting Information Grabs of Confidential Documents in SharePoint

Sponsored by

LOGbinder SP

ULTIMATE WINDOWS SECURITY .COM

Thanks to

- Made possible by

LOGbinder SP

© 2013 Monterey Technology Group Inc.

Preview of Key Points

- How to audit all view access for a given site collection
- How to limit view auditing to documents only in order to eliminate massive amounts of "page view noise"
- How to report on document view access from within SharePoint
- How to connect SharePoint to your log management/SIEM solution
- Abnormal access patterns
- How to automatically manage audit policy on new site collections as they are created
- How to safely purge SharePoint's internal audit log after exporting to your SIEM

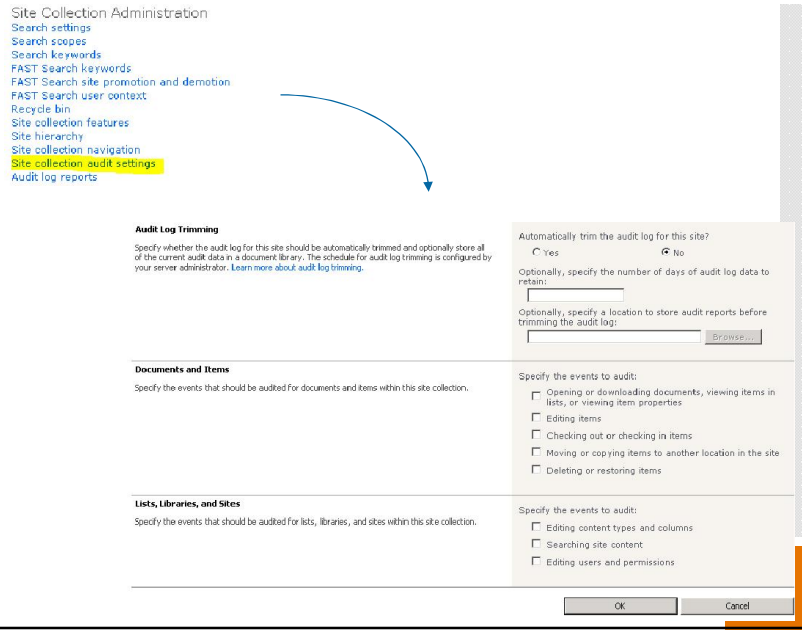
Overview

- SharePoint is constantly growing
  - Unstructured data
  - Confidential documents
  - Self-service
- Windows security log doesn't address SharePoint access
- SharePoint does have an application level audit ability

ULTIMATE WINDOWS SECURITY .COM

LOGbinder SP

How to audit all view access for a given site collection



ULTIMATE WINDOWS SECURITY .COM

LOGbinder SP

Problem / Solution

- Problem
  - Enabling View at the Site Collection level will create an explosion of "page view noise"
- Solution
  - Control View auditing at the content Content Type level
  - By default all files in SharePoint document libraries are the default "Document" content type
  - Site Settings\Gallery\Site Content Types
    - Choose Document
    - Information Management Policy Settings

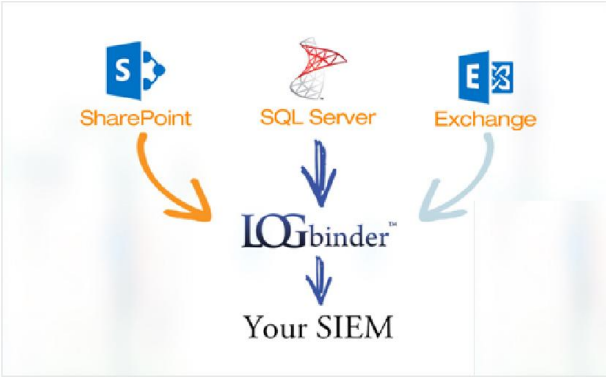
How to report on document view access from within SharePoint

- View some documents
- Site Collection Administration
  - Audit Log Reports
  - Content Viewing

How to connect SharePoint to your log management/ SIEM solution

- Information grabs are **time sensitive**
- You can't hope to catch them by running a report every day and perusing an Excel spreadsheet
- You need to get SharePoint audit events into your SIEM
- Not possible with native functionality
  - SharePoint audit log is stored in the Content Database
  - Completely internal to SharePoint

How to connect SharePoint to your log management/ SIEM solution



Abnormal access patterns

- Now that you have SharePoint audit events in your SIEM
- What indicates an information grab?
  - Unlikely number of Document View events within a short period of time
  - >10 documents within 1 minute?
  - You have to know your sites

Other SharePoint audit needs

- How to automatically manage audit policy on new site collections as they are created
- How to safely purge SharePoint's internal audit log after exporting to your SIEM

Bottom line

- SharePoint is host to massive amounts of sensitive unstructured data
- Internal SharePoint audit log only way to track access to this information
  - Enable view auditing at Site Collection level
  - Or Content Type level to avoid page view noise
- LOGbinder bridges the gap between SharePoint and your SIEM
- Now your SIEM can detect information grabs within seconds
- Download a free trial at
  - www.logbinder.com