



Detecting Information Grabs of Confidential Documents in SharePoint

Sponsored by

LOGbinder SP

© 2013 Monterey Technology Group Inc.



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

How to audit
all view access
for a given site
collection

Site Collection Administration

- Search settings
- Search scopes
- Search keywords
- FAST Search keywords
- FAST Search site promotion and demotion
- FAST Search user context
- Recycle bin
- Site collection features
- Site hierarchy
- Site collection navigation
- Site collection audit settings
- Audit log reports

Audit Log Trimming

Specify whether the audit log for this site should be automatically trimmed and optionally store all of the current audit data in a document library. The schedule for audit log trimming is configured by your server administrator. [Learn more about audit log trimming.](#)

Automatically trim the audit log for this site?
☐ Yes ☒ No
 Optionally, specify the number of days of audit log data to retain:



 Optionally, specify a location to store audit reports before trimming the audit log:
 Browse...

Documents and Items

Specify the events that should be audited for documents and items within this site collection.

Lists, Libraries, and Sites

Specify the events that should be audited for lists, libraries, and sites within this site collection.

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



LOGbinder SP

How to report on document view access from within SharePoint

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



LOGbinder SP

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