SIEM Integration with SharePoint: Monitoring Access to the Sensitive Unstructured Data in SharePoint

Sponsored by

Thanks to

- Made possible by

www.logbinder.com

Preview of Key Points

- Why important?
- Good news
- Bad news
- The solution

Why important?

- Sensitive information in unstructured format abounds in SharePoint
- If you are only monitoring the Windows Security Log you'll never know
  - Persistent attacker progressively downloading every document you have
  - Insider performing a "Snowdown" (Edward Snowden Download)
- Or be able to answer
  - Who looked at this document before that information was leaked to the press?
  - Who modified this document?
- What information is subject to compliance requirements in SharePoint?

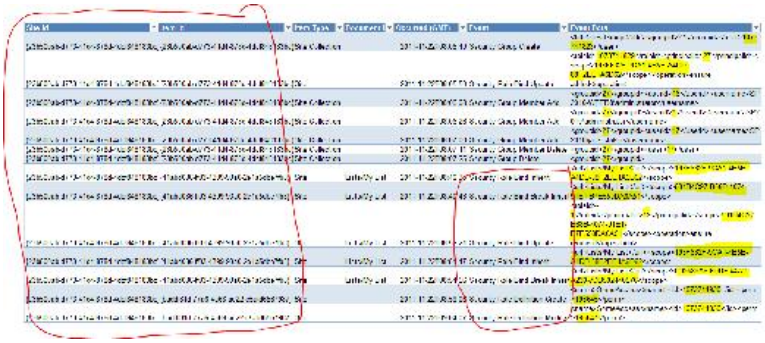
Monitoring document access in SharePoint

- Good news
  - SharePoint has an audit log
  - Can monitor all types of access to documents
    - What document was accessed?
    - Who accessed it?
    - When was it accessed?
    - How was it accessed?
  - Can also monitor
    - Permission changes
    - SharePoint group membership changes
    - Admin authority changes

Monitoring document access in SharePoint

- Bad news
  - The audit log isn't really a log
    - It's accessible manually inside SharePoint via browser
    - Or by .NET API in C#
  - The raw audit log isn't readable
    - Users, groups and other objects are labeled by ID code instead of actual name
  - Each site has it's own audit policy that must be configured manually
    - Self service site creation
  - Audit log integrity
    - Audit events can be purged by SharePoint before collected
    - Privileged users can erase events
  - SIEMs can't access the SharePoint audit log
    - Even if they could the information wouldn't be valuable
    - Don't confuse the SharePoint audit log with SharePoint's other non-security logs
      - Comparing SharePoint's 4 Audit Logs for Security and SIEM Integration

The raw audit log accessed manually



LOGbinder bridges the gap between SharePoint and your SIEM

LOGbinder

- Translates unreadable raw audit data into easy-to-read events
- Outputs in over 6 formats and protocols for any SIEM to consume
- Easy to integrate on your own but many SIEMs
  - Already have built-in support
    - QRadar, RSA, LogRhythm, LogPoint, SolarWinds, and more
  - Are supported by LOGbinder developed resources
    - ArcSight
    - Splunk
- Automates site audit policy configuration
- Automates purging of old events after sending to SIEM
- Within minutes
  - Correlate activity in SharePoint with everything else going on in your network
    - SQL Server and Exchange, too
  - Alert on
    - Information grabs
    - Tripwires

Set tripwires in SharePoint

- How to get late stage but reliable detection of intruders?
- Set tripwires
- In SharePoint these are called honey-sites or honey-documents

Bottom line

- SharePoint monitoring is part of the next era of application level security intelligence
  - SQL Server and Exchange
- The audit data is buried in SharePoint
- Get it out and send it to your SIEM with LOGbinder

More information on SharePoint audit logging

- https://www.ultimatewindowssecurity.com/sharepoint
  - Audit Policy
  - Audit Log
  - LOGbinder SP
  - Webinars
- https://www.logbinder.com/Resources/
  - Whitepapers
    - Comparing SharePoints 4 Audit Logs for Security and SIEM Integration
    - Comparison: ArcSight Connector for SharePoint DB and LOGbinder for SharePoint
    - SharePoint Audit Logging With HP ArcSight and LOGbinder
    - Top 6 Security Events to Audit in SharePoint
  - SharePoint Audit Events List
  - LOGbinder for SharePoint Datasheet
  - SIEM Integration Resources
    - ArcSight CEF Configuration Guide
    - ArcSight Content Pack for LOGbinder for SharePoint
    - Installing GFI EventsManager
    - LOGbinder for SharePoint Compliance Guidance
    - LogRhythm and LOGbinder for SharePoint Solution Brief
    - Recommended Reports and Alerts Designs for LOGbinder for SharePoint
    - Splunk App for LOGbinder
    - Splunk App for LOGbinder Integration Guide

Next steps

- Download LOGbinder for SharePoint
  - https://www.logbinder.com/Form/LBSPDownload
- Schedule a demo
  - https://www.logbinder.com/Form/Ask