Detecting New Programs and Modifications to Executable Files with Windows File Access Auditing and File Integrity Monitoring

Sponsored by solarwinds

© 2015 Monterey Technology Group Inc.

Thanks to

- Made possible by solarwinds LOG & EVENT MANAGER

www.solarwinds.com

© 2015 Monterey Technology Group Inc.

Preview of Key Points

- Preparation
- Events to monitor
- Compare to File Integrity Monitoring
- SolarWinds Log & Event Manager

Preparation

- Compile list of extensions
- Enable auditing of
  - All file creation
    - Then check extension in events
  - File modification
    - Either enable auditing only on certain
      - Extensions
      - Folders
    - Monitor all file modifications
    - What if files renamed?
    - How

Events to monitor

- Criteria
  - Event ID 4663
  - Accesses
    - WriteData and/or AppendData
  - Object Type: File
  - Object Name: *.exe
    - Or other extension
  - Subject identifies Who

Events to monitor

- Important information fields
  - Object Name
    - The file!
  - Subject
    - Whodunnit
  - Process Name
    - Identifies what program used
    - Often Explorer

Programs

- Whitelisting program names not required the way it is with monitoring program execution
- Instead, whitelist who and what programs should be creating new programs or modifying them
  - Installers
  - System management agents
  - Patch management processes

Challenges

- Can't tell difference between file creation and modification
- Copies are audited but moves are not
- Must audit all file modifications and creations
  - A LOT of data
  - Can't filter with Windows event forwarding

Advantages File Integrity Monitoring

- Easy to configure
- Easy to optimize
  - Cut out all the noise
- No inflexible Windows file audit policy to configure
- Easy to understand events