SPIRION

Spirion Extensions

Scan All Files and Remediate based on Data Retention

Table of Contents

Scan All Files and Remediate based on Data Retention

(Created, Modified, Access)

Introduction

On occasion it may not be possible to simply search for sensitive data based solely on the actual content of which exists in a file. The scenario arises when it becomes necessary to archive or destroy all files in a folder as result of the date criteria such as created, modified, or access dates. This extension shows how to search all files in a folder and remediate them based on a retention date.

Requirements

This process requires the following prerequisites in which to make this process possible. These include:

- Current versions of the SDM product(s).
- All Files "SDD".
- "Workflow" rule.
- Search "Policy".

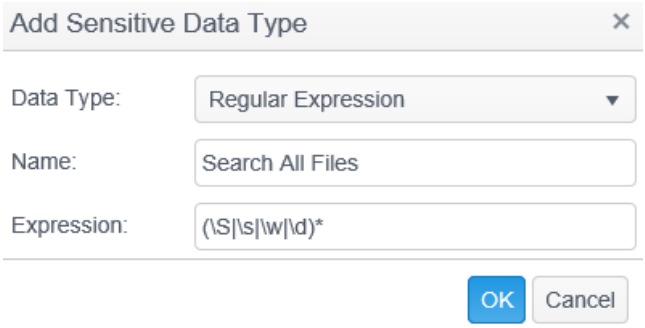
Important Notes

Note that proceeding with the following "could" override the true content-based classifications for any file in these respective locations. This Cool Solution applies to Sensitive Data Manager (SDM).

Process

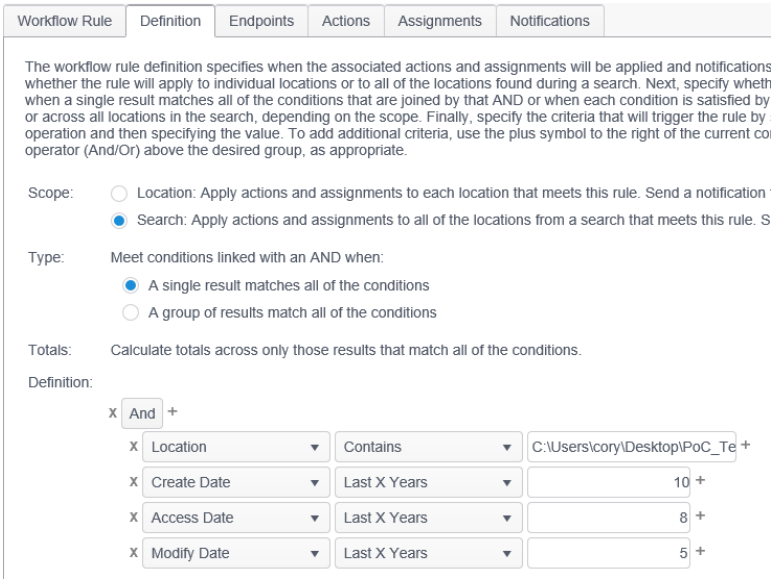
STEP 1 (SDD)

1. Import or create a RegEx to capture all files in a location using the expression.
2. From within the Spirion SDM Console Admin > Sensitive Data Types > Add > Select Data Type = Regular Expression > Name = Search All Files > Expression = (\S|\s|\w|\d)*



STEP 2 (Workflow)

1. Import or create a new workflow from within the Spirion SDM Console Admin > Classification > Add > Name = XXXX.
2. Select optionally a color, icon, or weight.
    a. Click OK.
3. Highlight the new Classification, from within the Spirion ribbon Select Rule > Add.
    a. Workflow Rule
        i. Provide a workflow rule name and other options
    b. Definition
        i. Select from the dropdown options the following, see the image below.
            1. “Location”, “Contains”, Path to folder which all files from within should be classified as XXXX.
        ii. Select from the dropdown options the following, see the image below.
            1. “Create\Access\Modify Date”, “Last X Years”, and time frame.

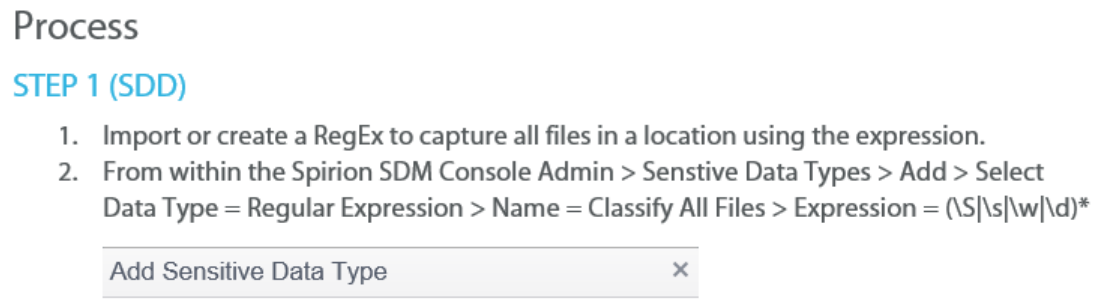


c. Endpoints
    i. Select the appropriate endpoint from where the local files are being searched.
d. Actions
    i. The Classification tag will be automatically selected, if not from the drop down for “Classify results as:” select the XXXX classification name from step 3. a. i.
    ii. Select from the “Execute classification rules:” “Directly on the endpoint”.
e. Click Finish
    i. Bottom right area of the page to save the new rule.

STEP 3 (Search Policies)

1. Import or create a new workflow from within the Spirion SDM Console Admin > Policies.
2. Create a new Policy by clicking Policy > Create.
    a. On the Policy Tab provide a name and optionally a description.
        i. For Policy Type select Scheduled Task.
        ii. On the Endpoints Tab select the same endpoint chosen for the workflow created previously.
        iii. On the Data Types Tab deselect all.
        iv. On the Location Tab deselect all.
    b. Click Finish

3. Select the policy name just created > expand the tree view > expand Search Locations and Select Custom Folders.
    a. Click Add from the Ribbon
    b. In the new Folder Location field place the same Share name as done in workflow, for example (C:\Location\PoC_Test_Data or the UNC path).
    c. Select "Include in Search" to the right of the folder patch for the Scope.
    d. Click the green check mark to the left of the folder path to save the changes.
4. Select the policy name just created > expand the tree view > Select Sensitive data Types.
    a. From within the resulting list select "Classify All Files" as created in this document "Step 1, 2.".

    b. 

5. Select the policy name just created > expand the tree view > Select "Scheduled Tasks" or "Search > Initiate Search" to search and classify all files from within the target folder location.

Outcomes

As result of the following detailed procedural steps for all files from within a location will be reported to the console matching the time specifications regardless of the content of the file "purely on the date criteria" and any remediation actions such as Shred or Quarantine will be invoked.