SearchInform updated its DCAP solution FileAuditor

MOSCOW, RUSSIAN FEDERATION, December 22, 2020 / EINPresswire.com/ -- Almost a year has passed since the release of Serchinform FileAuditor. Within this period, the system has been enriched with new tools, such as tools for scanning directories and tools for configuring rules for automatic detection and a manual search for incidents.


CEO, Sergey Ozhegov

Flexible scanning and reporting

FileAuditor has added additional settings that allow you to analyze file storage in the corporate network faster and better.

In order to save software resources you can exclude files and folders from scanning based on the specified attributes.

Now the system supports scanning directories using symbolic links. Even in case the server stores only file paths, FileAuditor will analyze these files and protect their confidential content. If you don't need this functionality, you can easily disable this feature.

To satisfy their needs risk managers can either use ready-made templates in the settings or create their own, the latter will enable them to configure rules that are more detailed. Manually designed rules will allow to scale and easily replicate similar rules for different tasks.

Finally, viewing all progress information becomes possible. You can also view general statistics for all computers and network resources as well as detailed reports on PC scanning. Now risk managers have a detailed information featuring the exact time of last scan, its duration; how many files were checked and how much space they occupy; moreover, the information in the files is divided into categories.

Another new report shows a list of errors that occurred during the last scans. This report will also indicate the reason for their occurrence: for example, a password-protected file can not be indexed that is why it has not been analyzed by the system. Another new feature displays the list of owners of file resources. It is especially useful for controlling the appearance of new objects in the file system and distributing access rights to them.

Classification rules and manual analytics

More search types are now available in the classification rules settings. Based on extended search opportunities the system would be more accurate in classifying the information type in storages.

Attribute and phrase search are now accompanied by character sequence search. This function allows you to search documents for information containing special characters and signs (foreign language inserts, @, №, $, %, etc.).

When you are setting up scan rules you can now set the search criteria in the dictionary. For example, you can train the system to identify whether documents that contain more than 5 words from the accounting terminology dictionary belong to the "financial reporting" category.

In new version of FileAuditor the regular expression search functionality has also been improved. The query window has converted into a convenient virtual keyboard editor with search element templates. All search element templates are specified with detailed comments. The editor is also enabled to create complex regular expressions, by which we mean a situation when multiple conditions are combined in a single search. For example, in the classification rule FileAuditor can consider the files where at least 5 card number combinations and three-digit CVC/CVV codes occur simultaneously, moreover, a user can immediately verify the request is working correctly. There is a check field, where you can set an example of the searched combination of characters and test whether the system recognizes it.

There is also a new manual search viewing mode: "text only". In this mode the system highlights all matches with the query (e.g. words, phrases, regular expressions) in the text. This mode is especially convenient to figure out why the document was included in the search results and to specify the exact fragment location.

Incidents auto-search

In order to track user actions with the specified data categories a new FileAuditor can set up automated search for violations in security policies by any parameter, namely: file or folder category, location, type, extension, user access rights, date of creation or modification, and so on. For example, a risk manager can create a policy according to which all changes made to documents that fall under the "trade secret" category will be reported. FileAuditor also notifies when a certain file no longer falls into the specified category (covers the situation when a user

has deleted significant content or the file itself).

Thus, FileAuditor policies allow specialists responsible for data protection be aware of all changes made to important data in the corporate network since the last scan. This includes monitoring employee violations when working with confidential files.

When the policy is violated, the system immediately sends an alert to the risk manager, in addition to this it saves the search results on the "Incidents" tab. In the tab a responsible specialist can find a detailed info on a violation and a file itself. The info includes the file path, specifies the category it belongs to and shows access rights.

Mihajlo Prerad
SearchInform Ltd.
+381 69 44 210 44
m.prerad@searchinform.com
Visit us on social media:
Facebook
Twitter
LinkedIn
