Mandiant

FILE LIBRARY

Overview

You can quickly and easily create custom security content using files included in the file library. Alternatively, you can upload your own files (from your sandbox, for example) as a basis for file transfer-related Actions.

From the File Library page, you can also download unrestricted files for review, use them to create file transfer Actions, apply a template, or delete the file entry.

Note the following important information about the file library.

- You can have multiple files with the same name, however, the SHA256 hash must be unique. For example, you can have multiple versions of the Mimikatz exploit file.
- You cannot download a file that is labeled Restricted Malicious or that is labeled Pending Approval.
- You cannot modify the Malicious file classification of files linked to A1xx-xxx Actions.
- Unless you have the appropriate permissions, you cannot approve a file for use (see **Approving Files for Use (https://docs.mandiant.com/home/approving-files-for-use)**).
- You can use User Tags to label the files. To categorize the files into groups, start the User Tag with the string "Group:" (see **Grouping Files in the File Library (https://docs.mandiant.com/home/grouping-files-in-the-file-library)**). For example, "Group: Partners" will place the file into the Partners group.

The Endpoint Files Library is used to transfer Files to Protected Theater and Endpoint Actors. See the Admin Guide or Protected Theater Guide for more information about the Endpoint File Library.