FOREGENIX

What does Mark As False Alarm w/Exclusion do?

rdavis@foregenix.com - 2017-01-24 - Comments (0) - Malware

When dealing with events, the marking with exclusion allows you to mark that file off so that it wont be scanned again unless the contents of the file is changed in any way. It does this by taking a hash of the "clean" file and then storing this value.

Everytime the system runs a scan in the future it will compare the file's hash with the one that is stored, if they match then the file wont be scanned as the contents hasn't changed since the previous scan. This way there will be a lot less alerts being flagged. The more you tell our scanners about exclusions in your enviroment, the more helpful the alerts will be for you.

Tags
Basehunter
events
Malware