FIREEYE TECHNICAL DOCUMENTATION

HXTool 4.0

Release Notes

2018-10-09

FireEye
SECURITY REIMAGINED

HXTool 4.0 – Release notes

NEW FEATURES

- Extended scheduler functionality
- Bulk acquisitions now fully utilizes scheduler allowing acquisitions to be run immediately, at a specific point in time or on an interval.
- Enterprise search now fully utilizes scheduler allowing acquisitions to be run immediately, at a specific point in time or on an interval.
- Enterprise search now support “skip unsupported terms” if you are using FireEye Endpoint security 4.5 or later
- Task-processors added which allows bulk acquisitions to be forwarded to files or TCP/UDP stream in the JSON format
- Full acquisition script builder added allowing you to build acquisition scripts directly in HXTool.
- Bulk acquisition now supports a comment to help track your acquisitions
- Improved logging capabilities (new log messages and reworked message format)
- Reworked scheduler UI allowing you to see scheduler activity and delete unwanted tasks
- Updated navigation bar and drop-down menus
- Implemented TinyDB cache which helps performance
- Docker support added

BUGFIXES

- A large number of bugfixes have been committed as part of the 4.0 release
- When an Enterprise Search script submission fails due to an invalid script, the error message will be shown in the console
- Syslog log handlers in conf.json are now parsed correctly
- When background credentials are unset, any associated API sessions are closed
- HXTool now properly handles relative paths and relative paths
- Timestamps now pass through a single function which properly handles precision. Resolves issues with timestamp parsing on session serialization/deserialization
- HXTool initialization code has been moved to its own function: app_init(), providing for compatibility with mod_wsgi/gunicorn
- Failed or aborted hosts as part of a bulk acquisition job will be removed from the download job (when download is required) so they no longer count against the total progress.

- When viewing bulk acquisition details, a bad bulk acquisition ID no longer results in application crash

KNOWN LIMITATIONS

- Alert investigation panel can take a long time to load on an endpoint with many alerts. This is due to the time is takes to retrieve the alerts via the API and depends on network performance between HXTool and the HX Controller
- Some features greatly depend on the number of alerts/acquisitions or other type of data contained in your FireEye endpoint controller. We have limited means of testing with very large configurations so certain panels or tables might take a while to load. The reason behind this is that we need to poll certain data from the endpoint API which depends on resources, hardware specification where you run HXTool and network performance.
- Data stacking does currently not have any limitations of the number of rows that can be returned. Very large data stacking jobs can potentially return too much data causing long load times and high memory use in your web browser
- Scheduler is multi-threaded and the number of threads can be controlled in the configuration file. When using the feature bulk acquisition with task-processor profiles each thread can allocate up to 800Mb of memory usage. Make sure you have enough memory in your system to accommodate each thread.
- With the addition of task processors HXTool can now potentially use much more system resources than earlier versions due to the fact that we are ingesting and processing each acquisition result. If this feature is heavily used we recommend running HXTool on a dedicated server