Release announcement: ESET Enterprise Inspector 1.3.1124.0

2019-09-18 - Mitchell | ESET Nederland - Reacties (0) - Releases

Release date: September 17, 2019

ESET Enterprise Inspector version 1.3.1124.0 has been released and is available for download at our download section and in ESMC repository.

Main highlights:

- Support for MS SQL server version 2017 or newer
- Increased and supported scalability up to 18 000 endpoints when using MySQL and 5 000 endpoints when using MS SQL
- UI improvements
- New and improved Search functionality
- Cross referencing of MITRE ATT&CK(TM) Framework
- Scoring system
- Commenting
- Option to search for hash value on VirusTotal and other 3rd party sources
- Auditing
- Expanded Exclusion system
- And many others including performance improvements

Other advanced functionality improvements:

- Better sorting of Alarms
- Extended information in Alarms View (more details for Alarms)
- Ability to detect inter process injection (CreateRemoteThreat + new Rules)
- IP ranges can now be defined in rules, this allows to define external/internal network connections (+ relevant rules added/changed)
- Ability to detect attempts to write suspicious content to registry (e.g. by file-less malware), since we are now able to check length of values written to registry database (+ new rules)
- Ability to evaluate actual values written to registry database, which allows to write more precise rules
- Ability to evaluate DLL in exclusions, which enables users to write exclusions for FPs connected with suspicious DLLs (many customers reported this problem)
- Ability to evaluate not only parent process, but any preceding process in process tree. This functionality can be also used in exclusions which greatly helps to eliminate complicated FP cases
- Raw events can be exported to CSV file and analyzed offline (e.g. in Excel or other tools)
- Ability to detect suspicious “file move” operations by evaluating source and destination name for the RenameFile operation
- In Aggregated Events view, under Network Connections it is now possible to see resolved domain names in addition to just IP addresses
- Integration with Network Protection module in Endpoint to provide more details about network events for better detection quality
- EI tracks which processes loaded a DLL

Known Issues

For a detailed list of known issues, see Known Issues for ESET Enterprise Inspector.

Support Resources

- Online Help (user guide): ESET Enterprise Inspector