Release Announcement: Enterprise Inspector v1.4.1364

2020-06-15 - Steef | ESET Nederland - Reacties (0) - Releases

It is with great pleasure that I would like to announce the release of ESET Enterprise Inspector v1.4. It is an important milestone in terms of the maturity of our EDR solution and we have introduced multiple features which really improves its competitiveness among the fierce competition in this market segment.

Changelog

General

Added: macOS support - EI Agent now available also for macOS

Added: Public REST API - Detections can now be managed via API

EI Web console changes

Added: 2FA support for login into the EEI console (currently using out own ESET Secure Authentication 2FA solution)

Added: Tagging of Objects - users now have the option of creating custom tags and adding to various objects

Improved: New Filter Bar and Improved Filters

Improved: Various aspects of Search - Rename, Tooltip, Process search

Improved: Custom order of columns - columns in all table views can now easily be reordered by mouse dragging

Added: Events Load view and Event storage filter to be able to precisely see and select which event types should or should not be stored

Added: Alerts view to Computer details - to see system related information, such as ability to detect alive, but non-reporting clients

Added: Auto resolving of alarms/detections matched by an exclusion

Improved: OS aware Computer actions and menus - to see exactly which functionality is available for which endpoints based on OS type

New detection capabilities

Improved: User account monitoring

Added: Visibility into WMI

Added: Visibility into scripts executed by PowerShell, CScript, WScript and MS Office for rule engine and investigation

Added: Credential dumping monitoring

Added: DNS requests monitoring

Added: SHA-256 and MD-5 hashes - additional hash value types can now be calculated

New or improved remediation capabilities

Added: Network Isolation of endpoints - ability to isolate endpoints from the rest of the network while keeping connection to management consoles intact

Added: Terminal (remote PowerShell interface)

Added: Possibility to block hashes automatically

Other

Added: Necessary internal changes to be compatible with upcoming Windows OS builds to be released in H1 2021

Improved: Performance and scaling

Known Issues:

- Some events may not have parent process information on macOS and the analysis tree may be incomplete (i.e. ModuleDrop, formerly known as PEDrop, event not generated on macOS, lack of process tree and accessing process, username info). This will be fixed with system extensions in our Endpoint Security product (expected in October) and compatible only with macOS 10.15 or newer.
- EEI license is not needed to activate EI Agent on mac (endpoint itself has to be activated with standard endpoint license).
- Search doesn't support DNS responses
- Some macOS specific rules could potentially cause a higher number of false positives in some environments. These rules will be specifically categorized as "Experimental" (within the Rules section) and if needed can be simply turned off. Please note that FPs in an EDR context are not the same as in an Endpoint product context and the tolerance/norm for FPs is much higher/normal.

Installation packages for the Global Availability build 1.4.1364 can be found on the official Download section of our webpage here

Installation notes:

1. upgrade MySQL/ MsSQL
2. upgrade EI server
3. upgrade endpoint security product
4. upgrade EI agents