GREYCORTEX Mendel 4.1.0

MAIN FEATURES

New look

The new user interface (UI) is a new redesigned look. It has been created to reduce visual complexity, provide easy access to essential data and progressively disclose complex functionality as needed – resulting in a cleaner look and feel. #light #dark

Extended integration for (not only) XDR coverage

EDR integration / stage 1

- Generic (vendor plugin based) solution to cooperate with different brands of endpoint clients (APIs)
- Extended host/device/endpoint information in Mendel UI
- Events from EDR visible in Mendel´s UI with hyperlinks to EDR console
- Response capability triggered (manually/automatically) by Mendel and executed by EDR client

CISCO ACI/APIC integration

- Extended visibility with applied definitions of the software defined infrastructure/network (e.g. host/subnet tags corresponding to ESG/EPG information)

API version 2

Current API coverage:

- Events
- IDS and log processing signatures, IDS variables
- UnTE signatures (4.1.0)
- Raw flows (4.1.0)
- Malicious domains
- Data captures (a direct connection into the database where all captured network data is stored)
- False positive management
- Blacklists based on IP addresses (including MISP)
- Malicious Files

Important: With the new version 4.1.0 the product (Mendel) is using a higher version of the API = v2. This version comes with a unified language and new set of keywords.

Advanced filtering with powerful queries

Master the data outputs with queries based on rich syntax with the new fulltext filter.

OTHER FEATURES

New OT parsers for BACnet and Profinet on DCE/RPC

LACP bonding on Mendel interfaces

IoC validation in history using API

Improved processing of ERSPAN communication (decapsulation on Mendel interfaces)

ENHANCEMENTS

System profiles are now configurable by users with administrator role

Upgraded Napatech drivers for wider compatibility

Newly discovered subnets are now reported in events

Optimization of hosts/services tab

Add interface to Asset Survey Configuration

Single page for AD + ISE + Identity logs settings

Official Mendel Product Support

With the release of version 4.1.0, full-service support will be provided for versions 4.1.x and 4.0.x. Limited service support is provided for the previous version, 3.9.x. Versions 3.8.x and older are no longer supported. End-users with valid support and maintenance or an active software subscription are advised to upgrade to a supported version(s).

Release Notes

For speeding up and improving system updates and data updates, we are preparing a new update/upgrade server. To be prepared for further use of the new server, please allow IP address 46.28.107.158 on your firewall. Current IP 89.221.218.75 (update.greycortex.com) needs to be preserved as well.