GREYCORTEX Mendel 3.8.0

MAIN FEATURES

Extended classification of devices and their roles (Tagging)

Dynamic visibility by tracking new activities or changes caused by devices communicating in your network. A completely new engine that brings a manual or automated way of tagging hosts or subnets through a system of user-defined rules with easy-to-understand syntax.

New categorization of detected security events

Mendel interprets all events captured in your network with more clarity thanks to the MITRE ATT&CK® tactics and techniques, Proofpoint rules and Top events (most relevant events at the top).

Analysis module

Deeper and more advanced data analysis thanks to the redesigned Analysis module. You can define any view over the processed and stored data using attributes, metrics and other variables.

Cloud support

New ability for Partners or Customers to deploy Mendel into the Cloud environment without support by utilization of our pre-prepared image ISO file. AWS is fully supported (sensor, AiO, collector). MS Azure and Google Cloud ready (support for collector deployment).

System profiling for speeds up to 100Gb

Mendel now officially supports 4×10Gbit on Intel X710 network cards, 10/25/40/100 Gbit on Napatech network cards and experimentally Nvidia Mellanox network cards

Subnet Discovery

Simplify the post deployment process by automatically identifying subnets in the monitored infrastructure.

Enhanced Dashboard settings

Added ability to import/export, clone and move dashboards to a different layout.

Added text field with wysiwyg editor and addition of text-only dashboard component.

Log Processing BETA

Ability to process received logs and generate security events from them by semi-passive approach (logs received by Mendel on specified port).

OT/ICS/SCADA FEATURES

Asset Discovery as a Mendel feature or standalone application BETA

CVE matching for vulnerable assets BETA

Implementation of OT/ICS parsers based on Siemens S7 and OPC protocols

Implementation of KNX and BACnet discovery into Asset Discovery tool

Added detection of DICOM and KNX protocol

UI tab displaying data from industrial networks renamed to OT metrics (former Scada)

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com, www.greycortex.com

GREYCORTEX

ENHANCEMENTS

Optimized database processing for better UI response

Added description of common service in service info dialog box

Added interface for IDS variables adjustment in UI

Added option to export event alerts in separate emails

Added response plugin to send email about the detected response request

Added option to generate application data in IPFIX flow export

Added option to insert subnet to multiple sensors

Added signature for detection SMB broadcast request

Added support for new arguments in firewall plugins

Added ability to import csv files for importing subnets

Added option to merge multiple netflow sources

Added capability to process IPv4 over IPv4 tunnel

Added support for parsing GENEVE Protocol

Added view over application data for application IDS events

Added option to merge span traffic from multiple interfaces to process separated RX and TX

Enhanced validation and error reporting for new IDS signatures

Enhanced local service detection on flows with errors

Enhanced Checkpoint firewall plugin

Enhanced scan detector for ARP scans

Improved Netflow processing to scale to higher speeds

Improved filtering in UI (autocomplete, port number for undefined services and more)

Improved scan detection to ignore common antivirus scans

Improved service descriptions

Improved reporting events to external systems on multiple sensors

All dialog windows are now movable

Official Mendel Product Support

With the release of version 3.8.0 full-service support will be provided for the versions 3.8.x and 3.7.x. Limited service support is provided for the previous version 3.6.x. Versions 3.5.x and older are no longer supported. End-users with valid support and maintenance or active software subscription are advised to upgrade to a supported version(s).

IMPORTANT

Please note that upgrading to version 3.8.0 will replace the system kernel and result in a reboot of the appliance. We recommend having direct or remote access to the appliance in order to be able to restart it if necessary.

If you are using the standalone Greycortex upgrade proxy application as a replacement for access to the update server, then you need to upgrade this proxy solution to a newer version first, to make the Mendel product upgrade (3.8.0) available.

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com, www.greycortex.com

GREYCORTEX