GREYCORTEX Mendel 3.9.0

MAIN FEATURES

Threat Visualization

An interactive dashboard based on GREYCORTEX's and MITRE ATT&CK®'s knowledge in the field of cyber security. A clear and comprehensive view of specific threat models and methodologies in accordance with detection in supervised networks. For both IT and OT environments.

API / stage 2

Higher integration potential with a new ability to connect Mendel with external information sources or provide processed data to recipients (SIEMs, etc.) for further processing. #restful

Current API coverage:

- Data captures (a direct connection into the database where all captured network data is stored)
- False positives management
- Blacklists based on IP addresses (including MISP)
- Malicious Files

Offline upgrade

Native capability to upgrade itself and the whole cascade (sensor via collector) via the user interface (UI) without the need of a live connection to the update server. Supports local (removable device) or remote (Samba) storage.

User activity log

To ensure the higher level of internal security of the monitoring tool itself, there is now the possibility to monitor the activity of users within their work.

ENHANCEMENTS

Network Analysis improvements for a better user experience

- Added the new metric "All" for the sum of the source and destination values
- Added new operators (is empty, is not empty, etc.)
- Added "Save as" and "To filter" buttons
- Import/export functionality for saved predefined views

Added support in the UI for downloading PCAPs from sensors

- Full support in the user interface for creating (conditional recording), storing and downloading raw traffic data from the sensor appliance

UnTE (Tagging) enhancements

- Dashboards based on the new tagging system
- Richer rule-making syntax
- Optimization for higher traffic speed (20 Gbps and higher)

Compressed data on the fast primary storage

- Capability to compress stored data on the fast (SSD) primary storage
  This feature is available only for a multipartition appliance setup.

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

GREYCORTEX

Netflow processing for higher speeds and from a scaled number of netflow sources

Import/Export of (custom) IDS rules via the Settings page (UI)

User defined time settings for data update distribution

Hardened DCOM remote protocol by authentication level with packet integrity + Windows 2022 support

Multidomain mapping in Suricata to handle proxy pairing in flows

Support for Intel E810 network cards

Support for Broadcom 10/25GbE cards

Changed visualization of event details for better comprehensibility

Geoip detection in IDS rules

Official Mendel Product Support

With the release of version 3.9.0, full-service support will be provided for versions 3.9.x and 3.8.x. Limited service support is provided for the previous versions, 3.7.x. Versions 3.6.x and older are no longer supported. End-users with valid support and maintenance or active SW subscription are advised to upgrade to a supported version(s).

New Support SLA

Professional PLUS Support – same as Professional Support with additional:

- Priority solution times – support tickets are responded to before waiting or open non-priority tickets.
- Priority software fix times – SW issues are fixed before other/non-priority tickets.
- Proactive Care – active system health monitoring by GREYCORTEX systems, including preventive identification of potential issues and problems (only performance statistics are analyzed, no specific network data and no sensitive data at all are collected).
- Priority handling of feature requests – via a special form sent to feature@greycortex.com.
- On-demand consulting, training and security services provided by GREYCORTEX – 4 hours per quarter (16 hours per year) by default.
- Available for All-in-ones and Collectors only.

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