GREYCORTEX Mendel 4.5

Main Features

Extensive User Management Overhaul Plus New Identity Integration

Complete rework of user and permissions handling, delivering native, comprehensive integration with identity services in your network infrastructure - such as Active Directory, and others.

- Centralized user access control through existing identity providers
- Onboarding and offboarding with directory-based authentication
- Granular permission management aligned with organizational roles
- Supports SSO and MFA if used in your organization

This enhancement strengthens security, simplifies administration and ensures the deployment fits seamlessly into your enterprise environment.

Precomputed Dashboards

Instant Insights with precomputed network analysis for complex queries, generated automatically from stored metadata—so you get immediate access to critical insights.

With this update, you benefit from faster investigations with on-demand access to key network behavior patterns, and reduced system load thanks to pre-analyzed, ready-to-use data based on pre-defined network analysis filters.

High Availability

Full protection and operational continuity with data and settings redundancy for your appliance. Two modes to ensure that critical configurations, detection rules, and captured network data are continuously synchronized to a secondary unit. In the event of a failure, your backup system resumes operation with no loss of visibility or historical data—ensuring seamless monitoring and fast recovery.

First Seen Communication

A new detector flags previously unseen communication between two peers. It alerts on the first occurrence of any inbound or outbound connection and is best used selectively on critical systems (e.g., domain controllers, DNS, OT).

Other Features

Extended Backup Options

- Hitachi HCP and AWS S3
- Local backup/restore of the settings to USB or network mounted storage

Visibility into Kubernetes Traffic – stage 1

Network monitoring and analysis of your Kubernetes environments, whether in the cloud or on-premises. Gain full visibility into east-west traffic between pods and services, detect anomalies across microservices, and uncover threats hidden inside your containerized infrastructure.

Faster Threat Response with Reworked Real-Time Event Reporting

An enhanced real-time event reporting engine, that was redesigned for speed, clarity, and actionability. Security events are now delivered instantly with enriched context, smart categorization, and prioritized alerts, ensuring your team can respond to threats the moment they emerge.

Huge Number of Flows Protection (DDoS & Scanners)

New DDoS & scanner mitigation mode that keeps Mendel responsive when a single IP starts generating (or receiving) a huge volume of flows. Mendel automatically summarizes bursts into aggregate events so you keep visibility without storing millions of near-identical records.

GREYCORTEX Mendel 4.5

Enhancements

- Sensor-Collector connection enabled on system interfaces
- System interface accept and reply ICMP (echo) packets
- Flow direction swapping based on heuristic data from network model
- Detection for Enterprise backup solutions
- Detect file share services as an application
- Implemented BPF filtering per interface
- Added support for JA4
- More precise OS detection for Windows
- Allow ignoring NTP server
- Processing ERSPAN version 2 type III
- Make hostname default option for FP
- Signatures for Polish personal ID (PESEL)

Event Correlation — UnTE Migration

The legacy correlation engine was removed. All rules were rewritten and moved to the improved UnTE engine, delivering better filtering, grouping, and deduplication with less noise and clearer context.

UI & UX Enhancements

We are constantly improving the user experience in our solution to make threat detection and investigation faster, clearer, and more intuitive. You can benefit from new abilities:

- Reworked filter manager page and predefined filters
- Enable/Disable napatech cards support in UI
- Display host risk in topology graph
- Added metrics into Peers graph
- Show OS Icon in UI for corresponding OS
- False positives - IMPORT
- IDS variables import
- Export policies/subnets/hosts in setting pages
- Add comments to Incident reports (PDF)
- Add comments to Incident export
- Subnets exported into .csv file should be compatible with Subnet import
- Improve advanced filter help
- Update glossary for the search function in the ME settings
- Add a function to disable Plugin sign check
- Optimize space on peers graph in FullHD
- Managerial&Security reports - small enhancements
- Icons in Tag management
- Improve accuracy of search in Settings

And refactored:

- Samba backup dialog to dynamic dialog
- Refactor EM page
- Refactor FP page
- Refactor UNTE page
- Refactor NBA page
- Refactor IDS page
- Refactor share link dialog to dynamic dialog
- Refactor whois dialog to dynamic dialog
- Refactor company dialog to dynamic dialog
- Refactor plugin dialog to dynamic dialog
- Refactor download system logs dialog to dynamic dialog
- Disconnect Icon label from button
- DataTable: add lazy attribute
- Implement dynamic dialog to upload certificat

OT

Extended Host/Asset Inventory Information

Enhance network visibility with external operational data. By correlating real-time security events with extended information about assets, you gain deeper context for every situation, faster root cause analysis, smarter prioritization, and reduced alert fatigue. Benefit from manually or automatically added data or tags to leverage the power of unified monitoring to make informed decisions and respond with precision.

Added new OT protocol coverage

- DICOM protocol parser
- HL7 protocol parser
- Ether-S-Bus protocol parser
- PROFINET Realtime (PN-IO) detection

Enhancements of the OT protocols

- LLDP parser extension with MED-extention capabilities
- SIP protocol improvements
- Inter-Control Center Communications Protocol (ICCP) support inside MMS parser
- PROFINET, unified service naming
- PROFINET over DCE/RPC, parser enhancement
- PROFINET, Alarm messages of the service PN-IO-RT
- PROFINET DCP parser enhancement
- PROFINET acyclic Real Time, enhanced PN-PTCP detection
- OPC/UA, protocol parser improvement for functions
- IEC-104, improved protocol detection and parsing
- IEC-104, OT metrics enhancements
- MODBUS, reworked signatures

Fixed Issues

THE FULL LIST WILL BE ADDED IN PRODUCTION BUILD OF 4.5.0 STABLE VERSION

Official GREYCORTEX Mendel Product Support

With the release of version 4.5.0, full-service support is provided for versions 4.5.x and 4.4.x.

Versions 4.3.x and older are no longer supported. End-users with valid support and maintenance or an active software subscription are highly advised to upgrade to a supported version(s).