GREYCORTEX Mendel 4.6

Main Features

Hostname History

Visibility into **hostname identity changes** is provided through continuous collection of hostname data **from multiple sources** such as DNS, mDNS, NetBIOS, DHCP, and TLS SNI. This data is correlated with host timelines, enabling analysts to trace hostname evolution, investigate identity shifts, and link activity even when IPs or names change. Historical **hostname values can** now **be searched, filtered, and viewed** for enhanced understanding of host behavior and network relationships.

How It Works

- Aggregates **hostname data from multiple sources** DNS, DHCP, NetBIOS, mDNS, TLS SNI.
- Each hostname is **timestamped** and stored **with source information** in the host timeline database.
- Historical hostnames can be viewed, filtered, and searched in a dedicated **host dialog grid**.
- Timeline correlations allow analysts to follow **identity changes over time**.

Enhanced Network Visibility with Structured Metadata

Network visibility is enhanced by structuring and analyzing **application-layer metadata** for easier access and interpretation. Key **protocol attributes** are extracted and stored in a dedicated structure. Analysts can more quickly recognize device roles — for example, distinguishing printers, DNS servers, or user workstations **based on communication patterns**. Identifiable attributes accelerate host identification, improve context for detections, and provide deeper understanding of network activity.

How It Works

- Application-layer metadata is extracted from monitored traffic and stored in a dedicated table.
- Previously hidden application-layer details are made searchable and linked to hosts.
- Focus is placed on identifying meaningful protocol attributes to **reveal device types** and behaviors.
- Data extracted from both IT and OT protocols: SNMP, SMB, DHCP, mDNS, HTTP, TLS.
- Based on the metadata, the Universal Tagging Engine creates tags in the host dialog.
- Users can define their own UnTE rules over these metadata to create their custom tags.

Packet Capture & Analysis Module

A unified Packet Capture & Analysis module consolidates the previous Data Capture and PCAP Analyzer into a single workspace. Users can access PCAPs from all connected sensors, replay them directly, and analyze results without extra steps. Enhanced controls, including full replay cancellation and improved UI organization, increase usability and workflow efficiency. The module lays the foundation for future expert-level traffic analysis in both IT and OT environments.

How It Works

- **Single workspace**: All PCAP-related activities are now accessible under Packet Capture & Analysis.
- **Integrated sensor support**: Mendel connects directly to sensors to retrieve capture data.
- Users can replay packets directly on the sensor, or analyze stored files as needed.
- A new “Cancel Replay” function ensures users can stop processing anytime.

Identity protocol extension “SAML” + “SSO”

SAML support has been added alongside LDAP, Kerberos, and OAuth, enabling enterprise Single Sign-On (SSO) integration. **The authenticator UI has been enhanced** with expandable sections, advanced options, and OAuth2 quick login. Editing authenticator domains is simplified, and API client authentication now supports OAuth2 scopes, improving usability, compatibility, and security in enterprise identity

infrastructures.

How It Works

- **SAML authentication** and authorization flows supported for web-based access.
- Integration with external Identity Providers (IdP) and Service Providers (SP) for secure Single Sign-On.
- Redesigned authenticator UI dialogs with expandable sections and advanced options.
- OAuth2 **quick login button** added to simplify access via federated identity systems.
- Ability to edit authenticator domains without recreating the configuration.

EULA & Account Roles

End users are now required to individually review and **accept the EULA** upon first login, ensuring consent is tied to actual system users. **Administrative roles are focused on system maintenance**, while operational users handle daily analysis and configuration under their own credentials. Use of administrative accounts for regular tasks triggers reminders to switch to personal accounts, improving compliance, traceability, and separation of roles.

How It Works

- Installation and upgrade processes now require explicit end-user EULA acceptance.
- Administrator and Support accounts are limited to system configuration; they cannot accept the EULA.
- End-User accounts are required for daily operations such as analysis or configuration tasks.
- Admin account usage triggers reminder messages to use personal accounts.
- All EULA-related actions are logged and traceable for compliance auditing.

Shared Threat Intelligence Framework

A secure data-sharing framework enables the collection of anonymized operational insights to **improve threat intelligence and detection quality**. Anonymized metrics from customer deployments support research, refine detection models, and strengthen protection against emerging threats. Data transfer is encrypted, strictly limited, and activated only with explicit user consent, ensuring privacy, transparency, and security.

How It Works

- Periodic sharing of anonymized detection and communication statistics.
- Data serialized in structured formats (JSON) and sent over encrypted HTTPS channels.
- Cloud storage in AWS S3 enables secure, scalable processing.
- Internal tools analyze aggregated data to enhance threat intelligence, detection coverage, and system reliability.
- Collection is strictly opt-in and enabled only after user approval via the EULA confirmation.

Flow-Preserving Hardware Bypass for Napatech

High-performance sensors equipped with Napatech adapters can now use a refined hardware **bypass mode that preserves flow information while reducing CPU load**. This improvement addresses large-scale environments (e.g., 50+ Gbit/s links) where full hardware bypass previously caused incomplete flow data and reduced visibility. The new flow-preserving mode allows the system to skip deep payload inspection when resource limits are reached — while keeping flow size, timing, and key metadata intact. This ensures that even when inspection depth is limited, network visibility and detection context remain accurate.

How It Works

- Two new per-sensor options define bypass behavior:
  - **Hardware Stream Bypass** skips payload data beyond the configured depth but preserves flow attributes (duration, size, endpoints).
  - **Hardware TLS Bypass** offloads encrypted traffic processing to Napatech hardware while keeping TLS metadata.
- A new setting allows administrators to disable hardware bypass for testing or fallback scenarios.
- Sensor configuration UI now includes two additional checkboxes next to the existing Stream Bypass option.
- Changes are applied per sensor upon restart or config reload.

Zabbix Integration Update for Asset Information

Zabbix integration has been updated to use the new Asset Information tag structure introduced in version 4.5, improving host management and visualization. Asset data retrieved from Zabbix — including vendor, model, firmware, and device type — is now mapped directly to standardized Mendel tags, providing a clearer and more consistent view of network assets.

The integration continues to use a lightweight, display-only approach similar to the SentinelOne connector, showing collected data in the host information dialog without additional storage or filtering. This enhancement ensures better alignment between external asset inventories and Mendel's internal asset representation, simplifying correlation and future expansion of IT/OT visibility.

OpenAppID Framework Upgrade

Mendel has been updated to support the latest OpenAppID framework used in new signatures. This ensures that the system can correctly identify and classify applications and protocols based on updated detection rules.

- The framework upgrade allows Mendel to recognize new application patterns and behaviors.
- Latest signatures have been incorporated, improving coverage and detection accuracy.
- The upgrade ensures ongoing compatibility with evolving threat intelligence and helps analysts respond to new application-layer threats more effectively.

Enhancements

Default Attributes for Email Data Exports

Email-based **data exports now include a predefined set of attributes** by default. The default configuration now automatically includes key analytical and contextual fields — such as timestamps, source and destination identifiers, severity, and MITRE category — ensuring that essential information is always part of the exported dataset.

UI and Configuration Simplification for Flow Source Management

The configuration process for adding new flow sources has been simplified. **The updated design now focuses flow input configuration exclusively on collectors (or all-in-one appliances)**, as they are the only components capable of processing NetFlow data. The "Sensor" option has been removed from both the UI and configuration files, and the related setting in mshell is disabled.

Use Configured Base URL in Data Exports

Data exports now correctly **use the globally configured Base URL** when generating download links. Previously, export links were based on individual sensor names, which could lead to inconsistencies in multi-

sensor or distributed environments. This update ensures all exported data references a unified, system-defined Base URL — improving link accuracy, consistency, and integration with external tools or portals.

UUID Information Added to the Settings Views

Unique system identifiers (UUIDs) are now visible directly in the Settings interface, improving transparency and simplifying troubleshooting. The mapped UUID is displayed in *Settings → Overview and under Settings → System → Sensors & Collectors → [machine] → License* for all devices. This enhancement eliminates the need to access Mshell for UUID lookup.

Update IPVOID Link with Selected IP Address

The IPVOID integration now automatically includes the selected IP address in the redirect URL. Instead of opening a generic IPVOID page showing the user's own IP, the system now displays information directly related to the analyzed IP from Mendel's interface. This improvement streamlines investigations and eliminates the need to manually copy or re-enter the IP address when checking external threat intelligence sources.

Update Modbus Configuration Hints and Documentation

The Modbus configuration has been improved to make setup and data import more intuitive. Updates include clearer guidance in the user interface and enhanced documentation, helping users correctly define register information and avoid configuration errors.

UI enhancements

Exclude Option Returned to Host and Subnet Tags in Filters

Filtering capabilities are extended with the option to **exclude Host and Subnet Tags** directly within the filter manager. Analysts can now refine searches by omitting specific tagged hosts or subnets, improving precision during incident investigation and data exploration. The feature reintroduces the Exclude operator for tag-based filters, aligned with existing host and subnet filtering logic and optimized to avoid previous performance issues.

MAC Vendor Icons from Database

MAC vendor icons are now displayed directly from the database, rather than being stored in the filesystem. This ensures that the icons always match the latest vendor information.

- The system automatically uses database records to determine which vendor a MAC address belongs to and shows the correct icon.
- Frequently used icons are cached for faster display.

Refactor Threat Intelligence Page

The **Threat Intelligence** page has been restructured into **three tabbed subpages** under a single parent page. Improvements include:

- Dynamic dialogs for adding or editing entries
- Enhanced filtering, searching, and sorting capabilities
- Updated tag glossary for consistent term management

Refactor Detection Section

The **Detection** section in Mendel has been reorganized to follow the same design principles as the other

pages. This refactor introduces a consistent user experience with:

- Filters for fast access to relevant items
- Group operations for bulk actions
- Import/export functionality
- Customizable columns for user-specific views

Category Filter Enhancement for Signature Pages

The category filter in signature settings pages has been redesigned. Instead of loading all available categories at once — which could slow down the interface on large deployments — the new version introduces an **autocomplete component** with grouped suggestions.

Other enhancements

PowerShell Flow Exporter Script

A new PowerShell script has been implemented to export all flows, meeting requirements provided by a potential customer. The script accepts a **start date** and **end date** as input parameters and generates **one CSV file per day** within the specified range. This script is included in the documentation as a reference example for users.

Official GREYCORTEX Mendel Product Support

With the release of version 4.6.0, full-service support will be provided for versions 4.6.x and 4.5.x., plus basic support for the version 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).