GREYCORTEX Mendel 4.3

Main Features

OT metrics in production – stage 1

With OT Metrics, you gain real-time insights into key metrics that drive your operational success. Monitor critical parameters with precision and accuracy. Our intuitive visualisation provides a holistic view of your OT environment, allowing you to identify alarming trends, and potential security issues and make informed decisions. All this is for the most used protocols such as Modbus, MMS, SNMP, BACnet, and IEC-104 with the potential to enlarge the OT protocol coverage in future versions upon your interest and request.

Built up OT capabilities

- New OT parsers for Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), GE-SRTP, and Mitsubishi MELSEC
- Enhanced SNMP parser to version 3
- User configuration of OT protocol ports using variables
- Specific IDS detection rules for protocols in OT environment
  - Energy Distribution
  - Industrial Manufacturing and Processing
  - Facility management networks
- Up to 100 small sensors managed by one collector

- Our latest product for quick asset inventory is the GREYCORTEX Microsensor. This tool allows our partners to quickly make an overview of a network with all it's OT-assets, without the deployment complexity of a full GREYCORTEX Mendel-product
- OT POST deployment guides for:
  - Energy Distribution
  - Industrial Manufacturing and Processing

PCAP recorder 2.0 with more reliable data capture and better UX

We are introducing enhanced reliability and UX in data capture. Our new PCAP recorder now leverages primary keys from the database for flawless PCAP naming and compatibility across languages and charsets. With innovative LST_ flags, database signaling ensures real-time tracking of PCAP changes for each sensor. Recording all packets with matching filtering options, even across multiple PCAPs, ensures comprehensive data capture. We've broadened the recording criteria to include Ethernet type, MPLS, tunnels, protocol, and source port. Plus, all PCAP definitions and database interactions are seamlessly managed through specialised database functions, guaranteeing secure and efficient data operations.

UX improvements related to optimised PCAP recording and storage management.

- The file rotation system supports both one-time pass recordings and continuous recording with FIFO-based erasing of the oldest files.
- PCAP rotation across the entire storage partition, giving you the flexibility to protect specific files from deletion and choose between FIFO rotation or halting recording when the volume is full.
- Information about overall disk volume and available space

NetFlow enhancements

- Maximum processing efficiency by sharing output threads across multiple NetFlow pipelines to ensure optimal resource utilization, reducing overhead and enhancing throughput for faster, more reliable data processing.
- Significant memory savings with optimised ParsedFlow class to reduce memory consumption.
- Dedicated flow enrichment pipeline component, designed to operate independently for enhanced modularity. This allows for more flexible deployment, easier maintenance, and the ability to scale or update components without impacting the entire system.
- Overall improvement accelerates data processing, enhances code readability, and reduces CPU load, providing a smoother and more efficient operation.
- And for all these changes there is a new NetFlow configuration in the UI to manage NetFlow settings across multiple pipelines easily.

Other Features

UI changes for better UX

- Visual changes in CEM to distinguish it from other types of appliances
- Whisperer in Main filter for Applications data type
- Policies, Subnets, and Host in Settings with reworked tables and filters
- An option to manage users by multiple administrators (user managers)
- Filtering by network interfaces and NetFlow sources
- Improved import function for subnet’s settings and added bulk operations
- The incident filter was adjusted to work with False positives and Long Term labels as attributes
- Default (system) subnets in settings reworked to be more comprehensible
- Plugins in Settings with code visualisation
- Group operations in Subnets and Hosts
- PDF reports in the Czech language
- Training forbidden ports on subnets
- Tag rendering

API extension to provide support for

- Incidents
- Custom categories in Signatures
- Saved views in Network Analysis
- Audit (user activity) logs

Improved Unte signatures

- Matching Mac addresses for vendor recognition
- New predicate when tag does not exist on host

Integration with Zabbix monitoring platform to enrich host/device information

Cloning Mendel instances from templates in VMware for automatic multiple locations installation using Ansible

GREYCORTEX Mendel 4.3

Enhancements

Logs in LEEF and CEF format support substitution of empty fields

Added UnTE filtering by subnet tag

Jitter and Delay metrics + RTP header

Official Mendel Product Support

With the release of version 4.3.0, full-service support is provided for versions 4.3.x and 4.2.x. Limited service support is provided for the previous version, 4.1.x. Versions 4.0.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).