GREYCORTEX Mendel 4.2

Main Features

PCAP playback and analysis

An extension to Mendel's core capabilities not only to analyse mirrored traffic in real-time but offers the same power to do it over earlier recorded data with the built-in PCAP recorder or captured by any other tool you have. Replayed PCAPs are processed and stored separately to any other data in Mendel to ensure the highest user experience during retrospective analysis with a maximum focus on data consistency and security.

XSOAR integration

An integration pack that connects Mendel and XSOAR and enables native data ingestion. This integration streamlines the flow of data from Mendel directly into XSOAR, the security orchestration, automation, and response platform.

IDS rule wizard

With this new step-by-step tool, you are able to tailor the rules in no time with significantly less knowledge the same way as a skilled professional, and can use the time saved more effectively.

New reporting module

A redesigned way to create and visually process reports in PDF format. Using the new and more effective engine, you can select added options for every part of the report to make it exactly meet your expectations. Use any predefined dashboard and filter, with the ability to define the number of rows for table type content, comes as standard. This is the foundation for a broad and unified powerful reporting service, streamlining the process of making comprehensive reports from any data available in the product.

User activity log

Audit every step of a Mendel user or API queries to comply with legislative requirements or internal policies.

User event categorization BETA

A brand new option to configure user-accounts as IT or OT users. This categorizes events faster and more efficiently with an emphasis on different needs and the focus of IT and OT security and operational specialists. This allows both user-groups to collaborate via the same Mendel, while still having their own perspective.

OT Metrics prototype for BACnet EXPERIMENTAL

The ability to visualize parsed values or metrics, derived from your OT protocols network flows within Mendel, offers you an unprecedented window into understanding your industrial equipment's behaviour. This exclusive experimental feature brings a new dimension to monitoring and comprehension.
Contact us to explore this non-public offering and gain a deeper understanding of your industrial systems.

GREYCORTEX Mendel 4.2

Other Features

UI changes for better UX

- Detection part in settings (a merged view for system and customer rules + TI)
- Group operations in the detection part
- LACP settings applicable via the UI
- The MITRE page as a regular dashboard
- Import subnets with tags

API extension to provide support over data related to:

- hosts
- users (persons)
- reports

Calculated delay and jitter from VoIP time metrics

File extraction from analyzed traffic for external analysis in the Sandbox BETA

Processing AWS FlowLogs protocol in the NetFlow module EXPERIMENTAL

Enhancements

Network capture parsers and enhancements

- Parsers (PostgreSQL, Bittorrent , IKE1/IKE2, QUIC and HTTP2)
- VOIP and delay metrics, improved ART/RTT
- MPLS and VLAN tags filtering from the recorded PCAPs

Improved OT protocol parsers

- BACnet
- OPC-UA
- S7

NetFlow export enhancements

- export version 5/9
- application data
- time metrics

Extended UnTE engine to support event correlations BETA

Official Mendel Product Support

With the release of version 4.2.0, full-service support is provided for versions 4.2.x and 4.1.x. Limited service support is provided for the previous version, 4.0.x. Versions 3.9.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).