GREYCORTEX Mendel 4.0.0

MAIN FEATURES

Network Inventory

The Visibility and Detection layers have been merged into one clear view. Have a complete overview of your network infrastructure with the added value of subnet and host detailed information colored with calculated risk and a security view. See the data as a sortable table or a scalable graphical interpretation.

API/stage 3

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

Current API coverage:

- Events (4.0.0)
- IDS and log processing signatures, IDS variables (4.0.0)
- Malicious domains (4.0.0)
- Data captures (a direct connection into the database where all captured network data is stored)
- False positive management
- Blacklists based on IP addresses (including MISP)
- Malicious Files

Integration

- Utilize threat intelligence platforms and enrich your security feeds. #MISP
- Extract identity information about logged users from logs from firewalls or domain controllers and pair them with hosts. #Radius
- **Community ID Flow Hashing**: Blue-team security specialists often use a variety of monitoring applications to correlate network flows from each of them. It's often desirable to pivot quickly from one dataset to another. In Mendel 4.0, GREYCORTEX introduces the industry standard Community ID in its flows, decreasing the workload of such dataset "joins" for blue-team members working with Mendel.
  - Security Tooling Supporting Community ID: Arkime, Elasticsearch, **GREYCORTEX Mendel (v4.0+)**, Security Onion, VAST, Wireshark, Zeek and many others.

ENHANCEMENTS

Scalable **NetFlow** processing

- Up to 50 Gb of origin traffic
- Up to one thousand NetFlow sources
- Stores HTTP, TLS and DNS fields from IPFix
- Detects blacklisted IPs in traffic
- Extracts performance metrics and parameters (e.g., incoming interface/port)
- Supports performance profiles to optimize deployment and processing
- Receivies and processes NetFlow on multiple network interfaces of a single machine

Estimatated source of data anomalies on outliers with the capability to define false positives and reduce invalid detection.

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

GREYCORTEX

Custom rules defined (added or imported) by the user for **Log processing** = Log processing is now in full production stage with UI support.

Failsafe mode with enhanced performance to solve infrastructure connection issues.

Flow identifier string to quickly and simply represent a given network flow. #Community ID

User interface enhancements for better UX

- Top events and services in a (small) host info dialog box
- A copy button for IP and MAC in the host info dialog box
- Common services rendered into flows detailed information
- Handover of the Supervisor role to another account
- User defined data retention

Network capture enhancements

Signatures are capable of testing TCP flags in flows

GE-SRTP OT parser

Support for the latest network card drivers

Official Mendel Product Support

With the release of version 4.0.0, full-service support will be provided for versions 4.0.x and 3.9.x. Limited service support is provided for the previous version, 3.8.x. Versions 3.7.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).

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