GREYCORTEX Mendel Data Sheet

Mendel, the network detection and response solution from GREYCORTEX, offers deep network visibility, advanced threat detection, and robust response for enterprise, government, and critical infrastructures.

Mendel monitors and analyzes network traffic, helps to discover known and unknown threats – including data leaks, operation anomalies, malicious activities of employees, and other difficult-to-detect threats. Thanks to its utilization of mirrored traffic from backbone switches, Mendel provides deep visibility of the entire monitored network. Deployable in minutes, it fills in the gaps left by traditional security tools, decreasing the time and resources necessary to make network operations secure and reliable.

Detection Methods

Prediction Analysis	Learn and anticipate network behavior for all subnets, hosts, and services on each host. All traffic not in line with learned behavior models is reported as anomalous (e.g., anomalous data transfer, volume of communication partners, number of communicating ports, number of flows, duration of communication, time of communication, etc.). Mendel re-adjusts its network behavior model every hour.
Discovery Analysis	Mendel maintains an up-to-date list of active services and hosts. If a new host (for example, BYOD) or a service appears in the monitored network segment, a discovery event is reported. The same method is used when services or hosts stop communicating, change their MAC addresses, or when DNS names change. Mendel also reports all communication between allowed and forbidden services based on preset policies.
Flow Analysis	Analysis of known and unwanted behavioral patterns in the network like port scans, brute force attacks, tunneled communication, blind communication, etc.
Repetitive Analysis	This method distinguishes between unpredictable human behavioral patterns and predictable machine-based behavioral patterns. This capability is based on the long-term processing of stored data in the database, which enables Mendel to detect communication by infected hosts that have been attacked by RATs, C&C malware, APTs, etc. This approach brings the advantage of having the ability to detect malware communication through various protocols, including HTTP/S, DNS, or ICMP.
Performance Analysis	Network performance monitoring and application performance monitoring modules analyze data transmission efficiency and SLA breaches for various protocols, including HTTP/S, MS-SQL, or SIP.
Rule-Based Analysis	Events are reported based on user-defined rules like data transfer, flows, packet throughput, thresholds on subnets, hosts, services, allowed or denied communication vectors (firewall audit), etc

Detection engines

Intrusion Detection System	Inspects communication on the packet level, searching for known threats like trojans, malware, exploits, etc. Mendel has more than 85,000 rules at hand to detect threats lurking in the network.
Correlation Engine	Correlates multiple events together, highlighting more serious issues by increasing the severity of the event. Multiple correlations are included in Mendel by default like malware spreading, detection of Tor networks, etc.
Threat Intelligence	The threat intelligence feeds include databases of black-listed IP addresses and their reputations, from both commercial and open sources (ProofPoint, SpamHouse, blocklist.de, abuse.ch, etc.). Mendel can also use feeds from ESET Threat Intelligence to detect malicious domains by their URLs and files by their hashes. These feeds are delivered in STIX-TAXII format.
Tagging Engine	The extended classification of devices and their roles. Dynamic visibility by tracking new activities or changes caused by devices communicating in the network. A completely new engine that brings a manual or automated way of tagging hosts or subnets through a system of user-defined rules with easy-to-understand syntax.
Log Processing	The ability to process received logs and generate security events from them by semi-passive approach (logs received by Mendel on a specified port).

GREYCORTEX

Traffic Processing and Analysis

Network Behavior Analysis

Flow-based analysis of network traffic with unsupervised machine learning and several detection techniques (see above).

Detection capabilities:

- Malware activity – propagation, downloading, spamming, etc.
- Attacker activity – scanning, brute-forcing, exploitation, etc.
- C&C activity – RAT, APT, AVT, bots, worms, rootkits, etc.
- Data exfiltration

Traffic Recording

- On-demand packet capture
- Based on source and destination IP, MAC, protocol, port etc.

Deep Packet Inspection

- Monitors any interaction with, or inside the internal network
- Allows to inspect traffic up to 100Gbits/sec
- Detection signatures for malware, policy violations, attacks, and other activity
- Malicious file detection by hashing
- Communication with blacklisted hosts
- Possibility to add user-created signatures

Performance Monitoring

Flow-based analysis of network and application performance (NPM, APM):

- Application awareness
- Monitoring current and average bandwidth
- Monitoring performance metrics such as application response times, round-trip time, user-experience time
- Rule-based detection (e.g. SLA)
- Automatic anomaly-based detection

Historical Metadata and Forensics

Mendel's Advanced Security Network Metrics (ASNM) protocol is security and performance-focused for advanced description of network traffic.

Capabilities include:

- Bi-directional flow recording (single flow contains both request and response)
- Metadata of application protocols for FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, SSL/TLS, Kerberos, etc.
- Metadata of industrial protocols for Modbus, DNP3, IEC 60870-5-104, IEC 61850 (GOOSE, MMS, SV), ENIP/CIP, CC-link, GE-SRTP
- Data can be stored for months or years (depending on storage capacity)

Main Benefits

Mirrored Traffic Analysis

- More sensitive behavioral detection than NetFlow (and similar protocols)
- Compared to NetFlow/IPFIX, records are enhanced by security parameters and performance metrics.

Robust Detection

- Zero-day and advanced threats (APTs, etc.)
- Remote Access Trojans (RATs)
- Data leakage (misused DNS, SSH, HTTP(S), ICMP, etc.)
- Tunneled traffic (DNS, SSH, HTTP(S), ICMP, etc.)
- Protocol anomalies
- Port scans
- Dictionary and brute-force attacks
- Data theft and other internal threats
- Breach of internal security policies
- Network misconfigurations
- DoS, DDoS
- Automatic data harvesting (e.g. e-shop)
- Encrypted traffic analysis (SSL certificates, fingerprinting, etc.)

Detailed Network Visibility

- All subnets, hosts, services, and flows with detailed information
- Metadata provides sufficient information on network behavior for forensic investigation, regulatory compliance, etc.
- Tunneled traffic
- Decrypts encrypted traffic with decryption key
- Automatic identification of critical devices in the network like Active Directory, Email server, etc.
- Months of historical data are indexed and quickly accessible
- Powerfully search collected data using filtering

Incident Management

- Incident Management capabilities to mark events as incidents and track investigation process reporting
- Simple managerial and analyst reports for different time intervals

Network inventory

- Merged Visibility and Detection layer into one clear view.
- Network infrastructure with added value of subnet and host detailed information flavored with calculated risk and security view.
- Data represented as a sortable table or scalable graphical interpretation.

NetFlow

- up to 50 Gbits of origin traffic
- up to 1,000 of external sources (switches)
- store HTTP, TLS and DNS fields from IPFix
- extract performance metrics
- extract parameters e.g. incoming interface
- detect blacklisted IP addresses
- performance profiles
- support for multiple appliance interfaces

GREYCORTEX

Outputs

Graphical User Interface

- Web user interface (Firefox, Chrome, Opera, Edge)
- Main interactive dashboard based on GREYCORTEX's and MITRE ATT&CK®'s frameworks
- Easily customizable dashboards
- Managerial and security dashboards for simple overview
- Fast and rich filtering capabilities
- Two design themes (light and dark)
- Context help and wide user documentation

Reporting and Alerting

- Conditional reporting (alarms)
- Customizable output format with custom links to the GUI
- Human-readable formats: email (HTML), and PDF

Integration

- SIEM: Based on CEF format (Common Event Format), CEF Standard, LEEF (Long Extended Event Format), Syslog, or the IDEA reporting protocol
- Export of flows in IPFIX format
- Active Directory, Cisco ISE and common external logs for user identity
- Firewall (MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint, etc.)
- Customizable output format
- Generic RESTful API to integrate with other infrastructure for Events, Data captures, False positives management, Blacklists based on IP addresses (including MISP), Malicious Files and Malicious Domains
- Community ID

Inputs

Network Data

- Mirrored traffic (TAP, SPAN, or other type of mirrored data port)
- Link layer support
- Network layer support including IPv6 protocols
- Transport layer support
- Application layer support
- Other Mendel appliances (sensor or collector)
- Flow-based protocols (NetFlow family, IPFIX)

Security Intelligence

- IDS signatures from Proofpoint and others
- Other databases (IP reputation, domain reputation, GEO IP, WHOIS, ...)
- Malicious Files Feed (e.g. ESET Threat Intelligence, MISP)
- Mitre ATT&CK Enterprise and ICS frameworks

Network Awareness

- Definition of policies by segments/subnets that share the same patterns of network behavior e.g. management, sales, servers, WiFi, VoIP, printers, DMZ, etc.
- IP to host name (using DNS records)

User Awareness

- IP to domain user (using domain controller event logs, LDAP)

Scalability

Deployment scalability may vary according to specific conditions and combinations in the infrastructure.

Sensor

- Up to 100Gbps monitored throughput
- Up to 8× 1GE interfaces or 4× 10GE interfaces or 2× 100GE
- Support for virtual or Cloud appliances up to 4Gbps

Collector

- 40+ sensors per single collector
- Up to 50,000 monitored nodes per collector
- Up to 3 years of data history
- Virtual appliances (including Cloud) with up to 20 connected sensors
- Multi-partition storage with fast disks support (NVMe, SSD, SAS
- Online and offline capability to upgrade itself or connected sensors

All-in-One

- Single appliance containing sensor and collector at once
- Up to 100Gbps monitored throughput
- Up to 8× 1GE interfaces or 4× 10GE interfaces or 2× 100GE
- Up to 20 connected additional sensors per single All-in-One appliance
- Up to 50,000 monitored nodes per All-in-One appliance
- Multi-partition storage with fast disks support (NVMe, SSD, SAS)
- Online and offline capability to upgrade itself or connected sensors

Central Event Management

- Clustering of up to 20 collectors together
- One-site event overview from whole infrastructure

GREYCORTEX