MENDEL Data Sheet

MENDEL, the network traffic analysis solution from GREYCORTEX offers advanced threat detection, deep network visibility, and robust response for enterprise, government, and critical infrastructure. MENDEL monitors and analyzes network traffic, helps to discover known and unknown threats; including data leaks, operation anomalies, disgruntled employees, and other difficult-to-detect threats. Because network traffic analysis uses mirrored traffic from backbone switches, MENDEL provides deep visibility for the full monitored network. MENDEL deploys in minutes and fills the gaps left by traditional security tools, decreasing the time and resources necessary to make network operations secure and reliable.

Detection Methods

MENDEL monitors network traffic and employs a number of advanced methods to detect malicious and anomalous behavior:

Prediction Analysis

Based on previously learned network behavior for all subnets, hosts, and services on each host, MENDEL predicts expected communications behavior. All traffic not in line with learned behavior models is reported as anomalous. Examples include: anomalous data transfer, volume of communication partners, number of communicating ports, number of flows, duration of communication, time of communication, etc. MENDEL updates its network behavior model each hour and uses 30 days worth of data.

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 communication between allowed and forbidden services based on preset policies.

Flow Analysis

Detects 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 long-term processing of stored data in the database, which enables MENDEL to detect communication by infected hosts which have been attacked by RATs, C&C malware, APTs, etc. This approach brings the advantage of 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.

MENDEL Detects Threats Using:

Intrusion Detection System

Inspects communication on the packet level, searching for known threats like trojans, malware, exploits, etc. MENDEL has more than 55,000 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

Our 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 URLs and files by their hashes. These feeds are delivered via STIX-TAXII format.

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 40Gbits/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
- 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 & 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 & 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)

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

Outputs

Graphical User Interface

- Web user interface (Firefox, Chrome, Opera, Edge)
- Easily customizable dashboards
- Managerial dashboards for simple overview
- Fast, rich filtering capabilities
- Two design themes (light and dark)

Reporting & 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 (2008 or newer) to identity users
- Email server
- Firewall (MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint)
- Integration with other infrastructure possible
- Customizable output format

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)

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

Sensor

- Up to 10Gbps monitored throughput
- Up to 8x 1GE interfaces or 4x 10GE interfaces
- Support for virtual appliances up to 1Gbps

Collector

- 50+ sensors per single collector
- Up to 30,000 monitored nodes per collector
- Up to 3 years of data history
- Support of virtual appliances for up to 20 connected sensors

All-in-One

- Single appliance containing sensor and collector
- Up to 10Gbps monitored throughput
- Up to 8x 1GE interfaces or 4x 10GE interfaces
- Up to 50 connected additional sensors per single All-in-One appliance
- Up to 30,000 monitored nodes per All-in-One appliance

Central Event Management

- Clustering of up to 20 collectors together