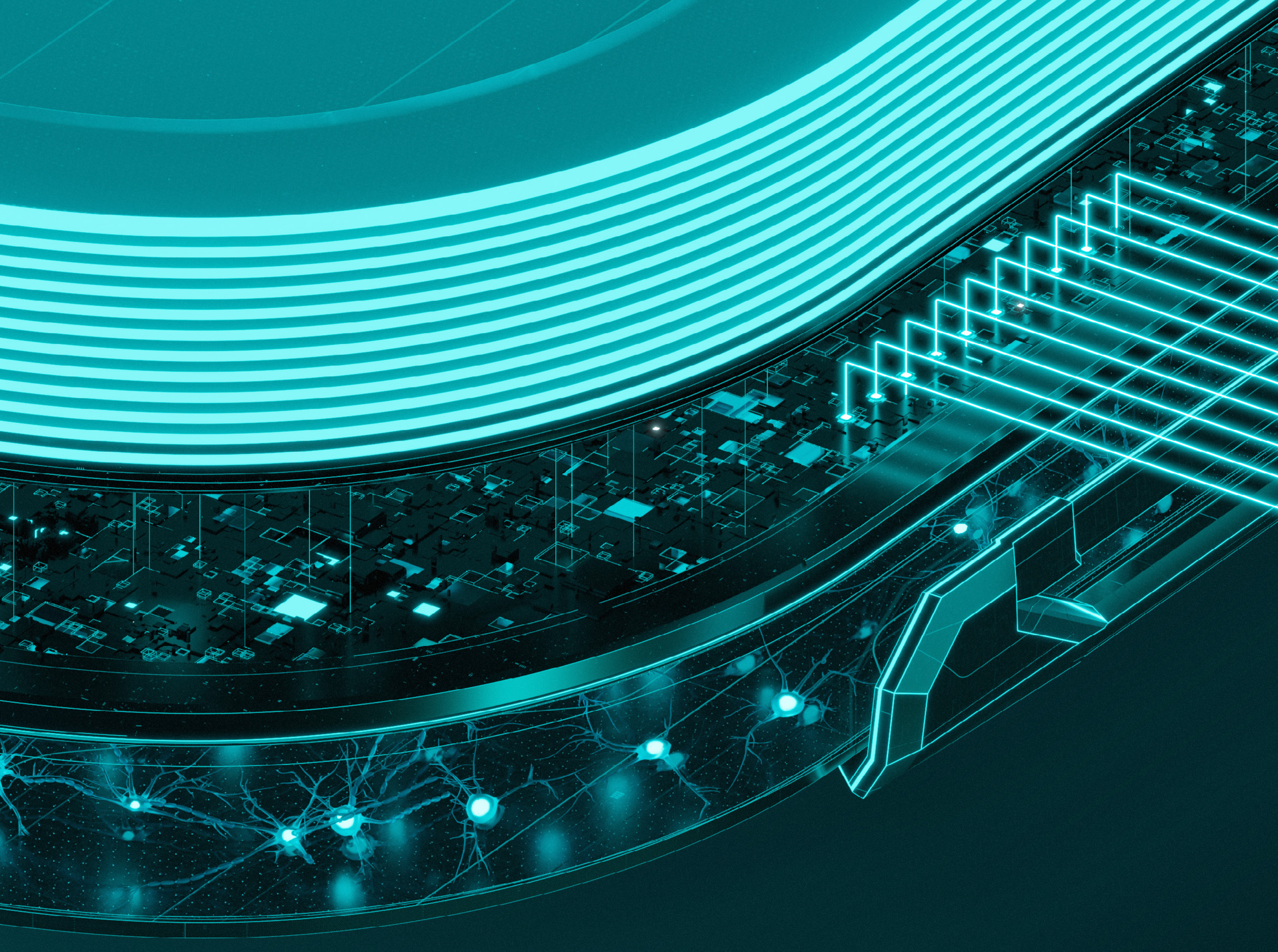
ESET TECHNOLOGY ALLIANCE

GREYCORTEX

Network Detection and Response



Progress. Protected.

DATASHEET

Mendel, the network detection and response solution from ESET Technology Alliance partner GREYCORTEX, will provide your organization with deep network visibility, advanced threat detection, and robust response capabilities thanks to XDR integration.

Network detection and response is an essential tool for enterprise, governments and operators of critical infrastructure: Mendel monitors and analyzes network traffic, helps to discover known and unknown threats – including data leaks, operation anomalies, malicious activity by employees, and other difficult-to-detect threats. Thanks to its utilization of mirrored traffic from backbone switches, Mendel provides deep visibility into 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.

UNIQUE VISIBILITY

into your IT and OT networks

- Visibility of all devices and users in your network
- Visualization of all their communications – up to application level
- Monitoring of BYOD and IoT device behavior
- User identity, device tagging and inventory details
- Performance monitoring of applications, devices and your network
- Traffic recording and decryption
- Support for software-defined networking (SDN)/Cisco ACI
- Historical, context-relevant reporting

POWERFUL DETECTION

of threats and anomalies in their early stages

- Cyber crime, hacker activities, ransomware, undetected malware
- Verification that your firewall, endpoint security or VPN is functioning
- Misconfigurations and changes to your network configuration
- Security policy violations
- Multiple behavioral detection methods, including unsupervised machine learning, statistical analysis and event correlation
- Threat intelligence and IDS signatures
- Encrypted traffic analysis
- Analysis using fully filterable data with multiple viewing options

EASY XDR INTEGRATION

thanks to integration of EDR, firewalls and more

- Maximum visibility into the entire infrastructure
- Correlation of malicious traffic detections
- Prioritized list of suspicious detections and vulnerable configurations
- Quick identification of the root cause of problems
- Minimized incident response times
- Automatic blocking of unwanted communications
- Forwarding of data, alerts and events to the XDR platform, SIEM or SOAR
- Improved work efficiency of security surveillance teams

eset® Digital Security
Progress. Protected.

GREYCORTEX

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 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.

RULES-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 at 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.

LOG PROCESSING

The ability to process received logs and generate security events from them via a semi-passive approach (logs received by Mendel on a specified port).

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.

THREAT INTELLIGENCE

Utilized 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.

Traffic Processing and Analysis

DEEP PACKET INSPECTION

- Monitors any interaction with, or inside, the internal network
- Allows inspection of 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)

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.

Main Benefits

INCIDENT MANAGEMENT

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

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

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.)

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

NETWORK INVENTORY

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