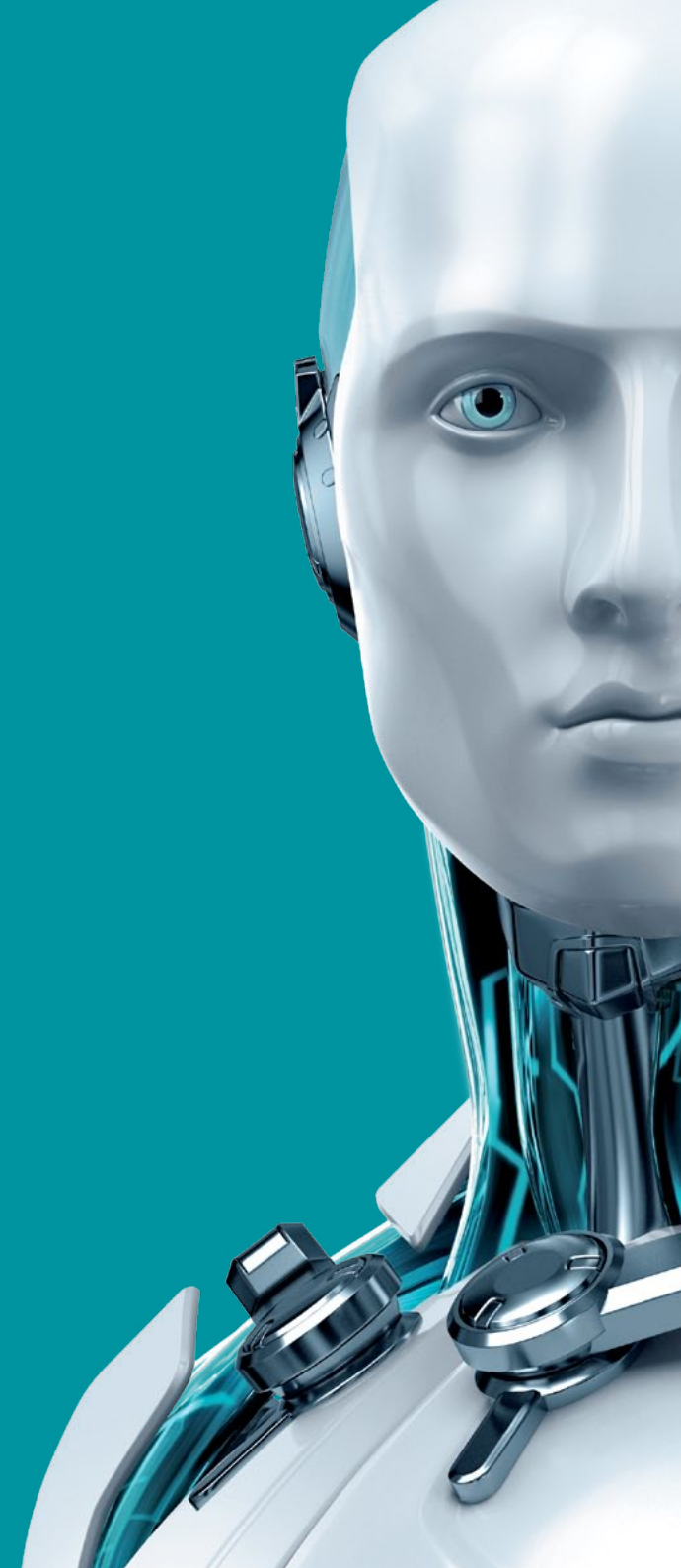
GREYCORTEX MENDEL

Análisis del tráfico de red

Información general del producto

BUSINESS

ESET TECHNOLOGY ALLIANCE



GREYCORTEX MENDEL

Análisis del tráfico de red con GREYCORTEX MENDEL

GREYCORTEX MENDEL es una solución avanzada que analiza el tráfico de red, monitorea el rendimiento, detecta amenazas y ofrece visibilidad detallada de la red para empresas, gobiernos e infraestructuras críticas. MENDEL utiliza inteligencia artificial, aprendizaje automático y análisis de grandes grupos de datos de última generación para garantizar la seguridad y confiabilidad de la infraestructura informática de las organizaciones.

MENDEL no es otra herramienta más para monitorear el comportamiento de la red: combina el análisis de amenazas, el aprendizaje automático, la inteligencia artificial, la inspección de paquetes, la correlación de eventos y otras herramientas para identificar actividades sospechosas dentro de una red. Esto les permite a los equipos de seguridad encontrar amenazas con mayor certeza y actuar más rápido que con las soluciones tradicionales de seguridad de red.

Identificación de amenazas antes de que ocasionen daños

La mayoría de los demás proveedores se enfocan en los métodos de ataque o los códigos maliciosos conocidos. En cambio, MENDEL usa métodos avanzados de inteligencia artificial para llegar más allá de las amenazas conocidas, de modo que detecta e identifica los síntomas de comportamiento malicioso a nivel atómico. Las amenazas se identifican en sus primeras fases, lo que disminuye el tiempo de respuesta a los incidentes, evita daños adicionales y reduce el riesgo general.

MENDEL también suministra en forma integrada la detección basada en firmas y la inteligencia de amenazas conocidas; esto aumenta sus capacidades de detección, al tiempo que reduce la tasa de falsos positivos.

de 8 a 16 horas
es el tiempo que necesita un atacante para entrar en la red

8 meses
es el tiempo promedio en que una amenaza persistente avanzada (APT) permanece sin ser detectada en la red de la víctima

98 días
es el tiempo promedio para detectar un ataque de una APT

71%
de las organizaciones no detectan con sus recursos las brechas de seguridad

Adaptación automática

El motor de Análisis de comportamiento de red (NBA) exclusivo de MENDEL utiliza cálculos matemáticos avanzados en aprendizaje automático para generar y adaptar las reglas de detección del tráfico anterior. Integra las entradas de sus otros motores de detección e incluye algoritmos especializados que, entre otras funciones, distinguen el comportamiento de una máquina del comportamiento humano. El motor NBA de MENDEL es la única solución en el mercado con esta capacidad.

Detección sensible

El protocolo métricas avanzadas de seguridad de red de MENDEL permite monitorear más de 70 características en cada flujo de red individual. Gracias a este nivel avanzado de análisis, MENDEL es más efectivo para detectar conductas maliciosas y otras amenazas que las demás soluciones actualmente disponibles en el mercado.

Sus técnicas avanzadas de minería de datos permiten procesar muchas más características de flujo de datos en tiempo real que las soluciones basadas en protocolos NetFlow. Además, MENDEL es capaz de escalar hasta 10 Gbps en una sola configuración de sensor y recopilador, y hasta 40 Gbps por recopilador.

MENDEL detecta las amenazas ocultas

– Malware en dispositivos móviles o integrados
– Fugas de datos con DNS, SSH, HTTP(S), etc.
– Tráfico de túnel
– Anomalías en protocolos
– Ataques enmascarados
– Spam
– Preparación para el robo y la extracción de datos
– Recopilación automatizada de datos
– Robo de datos
– Ataques de phishing

Mejor monitoreo del rendimiento

MENDEL proporciona información detallada sobre el rendimiento de las aplicaciones tanto desde el punto de vista del usuario como de la red. Su diseño sin agente ofrece la capacidad de monitorear todas y cada una de las transacciones, a través de múltiples tipos de aplicaciones. Dichas transacciones se muestran en una amplia gama de modos de visualización, con capacidades completas de clasificación y filtrado, lo que les proporciona a los equipos datos detallados para salvaguardar y optimizar los procesos críticos corporativos, y les permite analizar las causas de origen en forma fácil y rápida; todo en tiempo real. Esto significa que las organizaciones no solo ven mejoras en la seguridad de la red, la eficiencia y la visibilidad, sino también notan un retorno de la inversión considerable.

Facilidad de uso sin afectar el rendimiento de la red

MENDEL no es solamente un conjunto de herramientas, métodos y capacidades avanzadas. Se implementa rápidamente, ahorra tiempo administrativo y recopila datos sin afectar la velocidad de la red. Los administradores de TI adoran MENDEL porque:

- La instalación y configuración básica de MENDEL requiere 30 minutos. MENDEL realiza un estudio de la red y el motor del sistema de detección de intrusiones (IDS) comienza a informar los resultados de inmediato. Los datos accionables están disponibles después de siete días, y el ciclo de aprendizaje para el motor de Análisis de comportamiento de red (NBA) se completa en 28 días.
- MENDEL facilita la generación de informes y la comprensión de las amenazas identificadas, con herramientas de filtrado y clasificación, informes personalizables y una interfaz Web intuitiva para ahorrar tiempo.
- MENDEL supervisa y permite visualizar el tráfico de red (en vez de interrumpirlo) a la vez que registra información sobre cada flujo de datos. Esto significa que los usuarios pueden identificar fácilmente cada flujo en tiempo real y descubrir quién usa ciertos servicios, nodos de red y ancho de banda. MENDEL evalúa el rendimiento de las aplicaciones y de la red, y lleva a cabo un análisis de la causa de origen, sin crear demoras en el tiempo de respuesta de la red.

Análisis de comportamiento de red

El motor NBA de MENDEL utiliza cálculos matemáticos avanzados en aprendizaje automático, métodos de clasificación supervisados y no supervisados, agrupación en clústers y análisis de valores atípicos:

– Modelos de comportamiento normal en la red, todas las subredes, los hosts, los servicios y los flujos de datos individuales
– Análisis Bayesiano de funcionalidades modificadas.
– Modelos probabilísticos de mezclas (Algoritmo de esperanza-maximización (EM) de Gauss).
– Técnicas de razonamiento ad hoc .

Acerca de GREYCORTEX

GREYCORTEX utiliza inteligencia artificial, aprendizaje automático y métodos de minería de datos avanzados para que las operaciones informáticas de las organizaciones sean seguras y confiables. MENDEL, la solución de análisis del tráfico de red que ofrece GREYCORTEX, ayuda a las corporaciones, los gobiernos y los sectores de infraestructuras críticas a proteger su futuro mediante la detección de amenazas cibernéticas a datos confidenciales, redes, secretos comerciales y reputaciones, que otros productos de seguridad de red pasan por alto.

GREYCORTEX eligió el nombre "MENDEL" para su software en honor a Gregor Johan MENDEL, el padre de la genética moderna, que hizo sus descubrimientos en la ciudad de Brno, en el sur de Moravia, República Checa, donde GREYCORTEX tiene su casa matriz.

ESET TECHNOLOGY ALLIANCE

El objetivo de la **Alianza tecnológica de ESET** es mejorar la protección corporativa mediante una serie de soluciones de seguridad informática. Les proporcionamos a los clientes una mejor opción en el entorno de seguridad, que se halla en cambio constante, mediante la combinación de nuestra tecnología de confianza comprobada por el tiempo con otros productos que constituyen los mejores en su campo.

Información técnica

Arquitectura	La arquitectura de empresa de MENDEL está conformada por sensores y recopiladores. Los sensores se utilizan para detectar amenazas conocidas y entregar datos sobre el tráfico de red para el motor NBA del recopilador. Los recopiladores se utilizan para transformar estas métricas en información. Los sensores MENDEL admiten hasta 10 Gbps, y los recopiladores manejan hasta 40 Gbps. En casos de grandes implementaciones con muchas ubicaciones se usa un recopilador capaz de admitir 10 o más sensores (tanto físicos como virtuales).
Entradas	Flujos de datos de red desde el tráfico en un mirror (SPAN o TAP) y reputaciones IP como botnets conocidas, fuentes de spam, nodos TOR, proxies y más.
Salidas	Interfaz gráfica del usuario en la Web y archivos descargables .pcap, informes personalizables en .pdf y .doc (entregados por correo electrónico), exportaciones a SIEM en CEF y en IDEA.
Implementación	GREYCORTEX MENDEL puede implementarse como un dispositivo de hardware o como un dispositivo virtual pero con ciertas limitaciones. Otras posibilidades incluyen MENDEL en un entorno de SECaaS, modelos de centros de operaciones de seguridad o como una auditoría de seguridad única de la red de un cliente.
Despliegue	**Despliegue único:** MENDEL se puede implementar como un único appliance, conformado por un solo sensor de red y recopilador. **Despliegue distribuido:** MENDEL se puede implementar con varios recopiladores y sensores que comparten conocimientos sobre el tráfico y las amenazas de la red (para monitorear ubicaciones geográficamente distantes y/o procesar grandes volúmenes de tráfico).