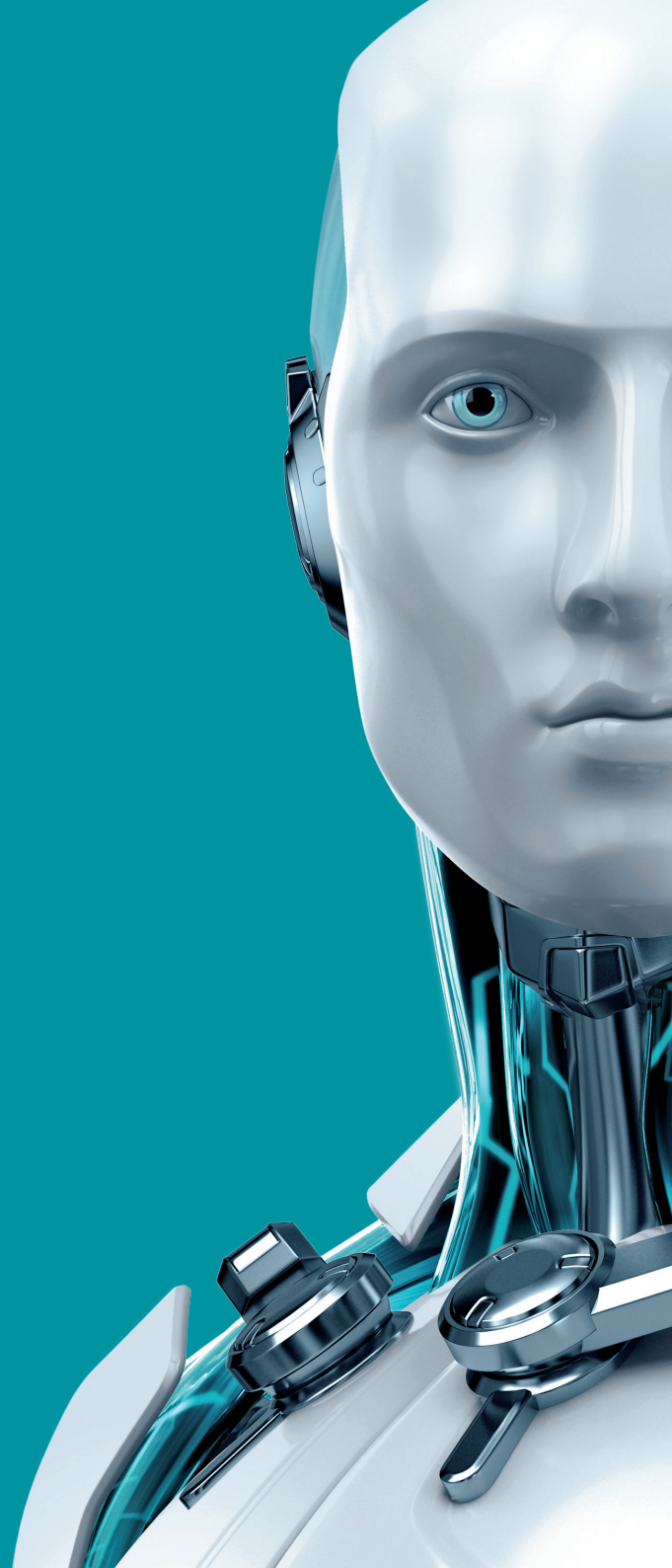
GREYCORTEX MENDEL

Análisis del tráfico de red

GREYCORTEX MENDEL
Descripción del producto

BUSINESS

ESET ALIANZA TECNOLÓGICA



GREYCORTEX MENDEL

Análisis del tráfico de red con GREYCORTEX MEDEL

GREYCORTEX MENDEL es un avanzado análisis de tráfico de red, monitorización, rendimiento, detección de amenazas y visibilidad profunda de la red para empresas, gobiernos e infraestructuras críticas. MENDEL utiliza inteligencia artificial de última generación, aprendizaje automático y análisis de big data para que la infraestructura de IT de las empresas sea segura y fiable.

MENDEL no es otra herramienta de monitorización del comportamiento de la red. Utiliza una combinación de análisis de amenazas, aprendizaje automático, inteligencia artificial, inspección de paquetes, correlación de eventos, y otras herramientas para identificar la actividad sospechosa dentro de una red. Esto permite a los equipos de seguridad encontrar amenazas con mayor certeza y tomar medidas más rápidamente que con las soluciones tradicionales de seguridad de la red.

Identifica las amenazas antes de que se produzcan los daños

Muchos otros proveedores se centran en métodos de ataque conocidos o piezas de código malicioso. Utilizando métodos avanzados de inteligencia artificial, MENDEL va más allá de las amenazas conocidas para detectar e identificar síntomas de comportamiento malicioso a nivel atómico. Las amenazas se identifican en sus primeras etapas, disminuyendo el tiempo de respuesta a los incidentes, previniendo daños mayores y reduciendo el riesgo en general.

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

8 – 16 horas
es el tiempo que un adversario necesita para entrar en una red

8 meses
es el tiempo medio que una APT pasa desapercibida en la red de la víctima

98 días
el tiempo medio para detectar un ataque APT

71%
de las empresas no detectan una brecha por sí mismas

Adaptación automática

El exclusivo motor de análisis del comportamiento de la red (NBA) de MENDEL utiliza un avanzado análisis matemático de aprendizaje automático para generar y adaptar reglas de detección a partir del tráfico anterior. Integra entradas de sus otros motores de detección e incluye algoritmos especializados que, en otras funciones, distinguen entre el comportamiento de la máquina y el humano. El motor NBA de MENDEL es la única solución del mercado que ofrece esta capacidad.

Detección más sensible

El protocolo de métricas de red de seguridad avanzada de MENDEL permite monitorizar más de 70 características de cada flujo de red individual. Este nivel avanzado de análisis hace que MENDEL sea más eficaz en la detección de comportamientos maliciosos y otras amenazas que las soluciones del mercado actual.

Las avanzadas técnicas de minería de datos de MENDEL garantizan que pueda procesar muchas más características de flujo de datos que las soluciones basadas en protocolos NetFlow, en tiempo real. Además, MENDEL puede escalar hasta 10Gbps en una configuración de sensor y compilador único, y hasta 40Gbps por compilador.

Mendel detecta amenazas ocultas

- El malware en dispositivos móviles o integrados
- Fugas de datos con DNS, SSH, HTTP(S), etc.
- Tráfico en túnel
- Anomalías de protocolo
- Ataques ocultos
- Detección de spam
- Preparación para el robo de datos y exfiltración
- Compilación automática de datos
- Robo de datos
- Ataques de phishing

Mejor control del rendimiento

MENDEL proporciona una visión detallada del rendimiento de las aplicaciones tanto desde el punto de vista del usuario como de la red. Su diseño sin agentes ofrece la capacidad de monitorizar todas y cada una de las transacciones, a través de múltiples tipos de aplicaciones. Estas transacciones se muestran en una amplia gama de visualizaciones con capacidades completas de clasificación y filtrado, proporcionando a los equipos datos detallados para salvaguardar y optimizar los procesos críticos del negocio, además de permitir un análisis fácil y rápido desde la raíz de las causas; todo ello en tiempo real. Esto significa que las empresas no solo ven una mejora en la seguridad de la red, la eficiencia y la visibilidad, sino también un retorno de la inversión considerable.

Facilidad de uso sin ralentizar la red

MENDEL no es solo herramientas, métodos y capacidades avanzadas. Se implementa rápidamente, ahorra tiempo administrativo y recoge datos sin ralentizar la velocidad de la red. Los responsables de IT adoran MENDEL porque:

- Instalar y configurar los parámetros básicos en MENDEL lleva 30 minutos. MENDEL estudia la red, y el motor IDS comienza a informar de los resultados inmediatamente. Los datos procesados están disponibles después de siete días, y un ciclo de aprendizaje completo para el motor NBA se termina en 28 días.
- MENDEL facilita la elaboración de informes y la comprensión de las amenazas identificadas, con filtrado y clasificación, informes personalizables y una interfaz web intuitiva para ahorrar tiempo.
- MENDEL monitoriza y visualiza, en lugar de interrumpir el tráfico de la red mientras registra la información de cada flujo de datos. Esto significa que los usuarios pueden identificar fácilmente cada flujo en tiempo real y averiguar quién utiliza determinados servicios, nodos de red y ancho de banda. Evalúa el rendimiento de las aplicaciones y de la red, y lleva a cabo un análisis de la raíz de la causa, sin crear un inconveniente en el tiempo de respuesta de la red.

El análisis del comportamiento de la red se une al aprendizaje automático

El motor NBA de MENDEL emplea análisis matemáticos avanzados en el aprendizaje automático, métodos de clasificación supervisados y no supervisados, clustering y análisis de valores atípicos:

- Modelos de comportamiento normal en la red, todas las subredes, los hosts, los servicios y el flujo de datos individuales
- Análisis bayesiano de características transformadas
- Modelos de mezcla probabilística (algoritmo gaussiano de maximización de expectativas (EM))
- Diversas técnicas de razonamiento ad hoc

Acerca de GREYCORTEX

GREYCORTEX utiliza métodos avanzados de inteligencia artificial, aprendizaje automático y minería de datos para ayudar a las empresas a que sus operaciones de IT sean seguras y fiables. MENDEL, la solución de análisis de tráfico de red de GREYCORTEX, ayuda a corporaciones, gobiernos y al sector de las infraestructuras críticas a proteger su futuro detectando las ciberamenazas en datos sensibles, redes, secretos comerciales y reputaciones, que otros productos de seguridad de la red.

GREYCORTEX ha bautizado su software con el nombre de "MENDEL", en honor a Gregor Johan MENDEL, el padre de la genética moderna, que realizó sus descubrimientos en la ciudad de Brno, Moravia del Sur, República Checa, donde GREYCORTEX tiene su sede.

ESET

ALIANZA TECNOLÓGICA

La alianza tecnológica de ESET tiene como objetivo proteger mejor a las empresas con una gama de soluciones complementarias de seguridad informática. Proporcionamos a los clientes una mejor opción a la hora de estar protegidos en el entorno de seguridad en constante cambio, combinando nuestra tecnología probada y de confianza con otros de su clase.

Información técnica

Arquitectura	La arquitectura empresarial de MENDEL se compone de sensores y compiladores. Los sensores se utilizan para detectar amenazas conocidas y entregar datos de tráfico de red para el motor de la NBA en el compilador. Los compiladores se utilizan para transformar estas métricas en información. Los sensores de MENDEL pueden soportar hasta 10Gbps, y los compiladores pueden manejar hasta 40Gbps. Las grandes implementaciones en muchas ubicaciones se diseñan con un compilador que puede soportar 10 o más sensores (tanto físicos como virtuales).
Inputs	Flujos de datos de red procedentes del tráfico en espejo (SPAN o TAP), y reputaciones IP como redes de bots conocidas, fuentes de spam, nodos TOR, proxies, etc.
Outputs	GUI web y archivos .pcap descargables, informes personalizables en .pdf y .doc (entregados por correo electrónico), exportaciones a SIEM en CEF e IDEA.
Implementación	GREYCORTEX MENDEL puede implementarse como un dispositivo de hardware o, con algunas limitaciones, como un dispositivo virtual. Otras posibilidades incluyen MENDEL en un entorno SECaaS, modelos de centro de operaciones de seguridad o como una auditoría de seguridad puntual de la red de un cliente.
Implementación	**Implementación única:** MENDEL puede implementarse como un único sensor de red y compilador en un único dispositivo. **Implementación distribuida:** MENDEL puede implementarse con varios compiladores y sensores que comparten conocimiento sobre el tráfico de la red y las amenazas (para monitorizar lugares geográficamente distantes y/o procesar grandes volúmenes de tráfico).