ESET TECHNOLOGY ALLIANCE

GREYCORTEX

Detección y respuesta en red

Progress. Protected.

FICHA TÉCNICA

Mendel, la solución de detección y respuesta de red de GREYCORTEX, colaborador de ESET Technology Alliance, proporcionará a tu empresa una gran visibilidad de la red, detección avanzada de amenazas y sólidas capacidades de respuesta gracias a la integración con XDR.

La detección y respuesta de redes es una herramienta esencial para empresas, gobiernos y operadores de infraestructuras críticas: Mendel monitoriza y analiza el tráfico de red, ayuda a descubrir amenazas conocidas y desconocidas, como fugas de datos, anomalías en el funcionamiento, actividades maliciosas de los empleados y otras amenazas difíciles de detectar. Gracias a la utilización de tráfico en espejo procedente de los conmutadores troncales, Mendel proporciona una visibilidad profunda de toda la red monitorizada. Implementable en cuestión de minutos, llena los vacíos dejados por las herramientas de seguridad tradicionales, reduciendo el tiempo y los recursos necesarios para que las operaciones de red sean seguras y fiables.

VISIBILIDAD ÚNICA

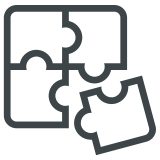
de tus redes de IT y OT

- Visibilidad de todos los dispositivos y usuarios de tu red
- Visualización de todas tus comunicaciones, hasta el nivel de aplicación
- Monitorización del comportamiento de los dispositivos BYOD e IoT
- Identidad de usuario, etiquetado de dispositivos y detalles de inventario
- Monitorización del rendimiento de aplicaciones, dispositivos y de la red
- Grabación y descifrado del tráfico
- Compatibilidad con redes definidas por software (SDN)/Cisco ACI
- Información histórica y contextualizada

POTENTE DETECCIÓN

de amenazas y anomalías en sus primeras fases

- Ciberdelincuencia, actividades de hackers, ransomware, malware no detectado
- Comprobación del funcionamiento del cortafuegos, la seguridad de los terminales o la VPN
- Errores y cambios en la configuración de la red
- Infracciones de la política de seguridad
- Múltiples métodos de detección de comportamiento, incluyendo machine learning, análisis estadístico y correlación de eventos
- Inteligencia sobre amenazas y firmas IDS
- Análisis de tráfico cifrado
- Análisis mediante datos totalmente filtrables con múltiples opciones de visualización



FÁCIL INTEGRACIÓN XDR

gracias a la integración de EDR, cortafuegos y mucho más

- Máxima visibilidad de toda la infraestructura
- Correlación de detecciones de tráfico malicioso
- Lista priorizada de detecciones sospechosas y configuraciones vulnerables
- Identificación rápida de la causa de los problemas
- Tiempos de respuesta a incidentes reducidos
- Bloqueo automático de comunicaciones no deseadas
- Envío de datos, alertas y eventos a la plataforma XDR, SIEM o SOAR
- Mejora de la eficacia del trabajo de los equipos de vigilancia de la seguridad

Métodos de detección

ANÁLISIS DE PREDICCIONES

Aprender y anticipar el comportamiento de la red para todas las subredes, hosts y servicios en cada host. Todo el tráfico que no se ajusta a los modelos de comportamiento aprendidos se notifica como anómalo (por ejemplo, transferencia de datos anómala, volumen de interlocutores de comunicación, número de puertos en comunicación, número de flujos, duración de la comunicación, hora de la comunicación, etc.). Mendel reajusta su modelo de comportamiento de red cada hora.

ANÁLISIS DE DESCUBRIMIENTO

Mendel mantiene una lista actualizada de los servicios y servidores activos. Si aparece un nuevo host (por ejemplo, BYOD) o servicio en el segmento de red monitorizado, se notifica un evento de descubrimiento. El mismo método se utiliza cuando los servicios o hosts dejan de comunicarse, cambian sus direcciones MAC, o cuando los nombres DNS cambian. Mendel también informa de todas las comunicaciones entre servicios permitidos y prohibidos basándose en políticas preestablecidas.

ANÁLISIS DE FLUJO

Análisis de patrones de comportamiento conocidos y no deseados en la red, como análisis de puertos, ataques de fuerza bruta, ataques de túnel, etc.

ANÁLISIS REPETITIVO

Este método distingue entre patrones de comportamiento humano impredecibles y patrones de comportamiento basados en máquinas predecibles. Esta capacidad se basa en el procesamiento a largo plazo de los datos almacenados en la base de datos, lo que permite a Mendel detectar la comunicación de hosts infectados que han sido atacados por RATs, malware C&C, APTs, etc. Este enfoque aporta la ventaja de tener la capacidad de detectar la comunicación de malware a través de varios protocolos, entre ellos HTTP/S, DNS o ICMP.

ANÁLISIS DEL RENDIMIENTO

Los módulos de monitorización del rendimiento de la red y de las aplicaciones analizan la eficacia de la transmisión de datos y los incumplimientos de los acuerdos de nivel de servicio para varios protocolos, como HTTP/S, MS-SQL o SIP.

ANÁLISIS BASADO EN REGLAS

Los eventos se notifican basándose en reglas definidas por el usuario, como transferencia de datos, flujos, rendimiento de paquetes, umbrales en subredes, hosts, servicios, vectores de comunicación permitidos o denegados (auditoría de cortafuegos), etc.

Motores de detección

SISTEMA DE DETECCIÓN DE INTRUSIONES

Inspecciona la comunicación a nivel de paquetes, buscando amenazas conocidas como troyanos, malware, exploits, etc. Mendel dispone de más de 85.000 reglas para detectar las amenazas que acechan en la red.

MOTOR DE CORRELACIÓN

Correlaciona múltiples sucesos entre sí, destacando los problemas más graves al aumentar la gravedad del suceso. En Mendel se incluyen correlaciones múltiples por defecto, como la propagación de malware, la detección de redes Tor, etc.

PROCESAMIENTO DE REGISTROS

La capacidad de procesar los registros recibidos y generar seguridad a través de un enfoque semi-pasivo (logs recibidos por Mendel en un puerto especificado).

MOTOR DE ETIQUETADO

La clasificación ampliada de los dispositivos y sus funciones. Dinámica visibilidad mediante el seguimiento de nuevas actividades o cambios provocados por los dispositivos que se comunican en la red. Un motor completamente nuevo que aporta una forma manual o automatizada de etiquetar hosts o subredes mediante un sistema de reglas definidas por el usuario con una sintaxis fácil de entender.

INFORMACIÓN SOBRE AMENAZAS

Las fuentes de inteligencia sobre amenazas utilizadas incluyen bases de datos de direcciones IP en listas negras y sus reputaciones, tanto de fuentes comerciales como abiertas (ProofPoint, SpamHouse, blocklist.de, abuse.ch, etc.). Mendel también puede utilizar fuentes de ESET Threat Intelligence para detectar dominios maliciosos por sus URL y archivos por sus hashes. Estas fuentes se entregan en formato STIX-TAXII.

Tratamiento y análisis del tráfico

INSPECCIÓN PROFUNDA DE PAQUETES

- Monitoriza cualquier interacción con, o dentro de la red interna
- Permite la inspección de tráfico de hasta 100Gbits/seg
- Firmas de detección de malware ataques y otras actividades
- Detección de archivos maliciosos mediante hashing
- Comunicación con hosts incluidos en listas negras
- Posibilidad de añadir firmas creadas por el usuario

CONTROL DEL RENDIMIENTO

Análisis basado en flujos del rendimiento de redes y aplicaciones (NPM, APM):

- Conocimiento de las aplicaciones
- Monitorización del ancho de banda actual y promedio
- Monitorización de métricas de rendimiento como los tiempos de respuesta de la aplicación, el tiempo de experiencia del usuario
- Detección basada en reglas (por ejemplo, SLA)
- Detección automática basada en anomalías

METADATOS HISTÓRICOS Y ANÁLISIS FORENSES

El protocolo Advanced Security Network Metrics (ASNM) de Mendel se centra en la seguridad y el rendimiento para la descripción avanzada del tráfico de red.

Las capacidades incluyen:

- Registro bidireccional de flujos (un único flujo contiene tanto la solicitud como la respuesta)
- Metadatos de protocolos de aplicación para FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, SSL/TLS, Kerberos, etc.
- Metadatos de protocolos industriales para Modbus, DNP3, IEC 60870-5-104, IEC 61850 (GOOSE, MMS, SV), ENIP/CIP, CC-link, GE-SRTP
- Los datos pueden almacenarse durante meses o años (dependiendo de la capacidad de almacenamiento)

ANÁLISIS DEL COMPORTAMIENTO DE LA RED

Análisis del tráfico de red basado en flujos con machine learning no supervisado y varias técnicas de detección (ver más arriba).

Capacidad de detección:

- Actividad de malware - propagación, descarga, envío de spam, etc.
- Actividad de los atacantes: análisis, fuerza bruta, explotación, etc.
- Actividad de C&C - RAT, APT, AVT, bots, gusanos, rootkits, etc.
- Exfiltración de datos

GRABACIÓN DE TRÁFICO

- Captura de paquetes a demanda
- Basada en IP de origen y destino MAC, protocolo, puerto, etc.

Principales ventajas

GESTIÓN DE INCIDENTES

- Funciones de gestión de incidentes para marcar sucesos como incidentes y realizar un seguimiento del proceso de investigación
- Informes sencillos de gestión y análisis para distintos intervalos de tiempo

VISIBILIDAD DETALLADA DE LA RED

- Todas las subredes, hosts, servicios y flujos con información detallada
- Los metadatos proporcionan suficiente información sobre el comportamiento de la red para investigación forense, cumplimiento normativo, etc.
- Tráfico en túnel
- Descifra el tráfico cifrado con clave de descifrado
- Identificación automática de dispositivos críticos de la red, como Active Directory, servidor de correo electrónico, etc.
- Meses de datos históricos indexados y rápidamente accesibles
- Búsqueda potente de los datos recopilados mediante filtrado

ANÁLISIS DEL TRÁFICO DUPLICADO

- Detección de comportamiento más sensible que NetFlow (y protocolos similares)
- En comparación con NetFlow/ IPFIX, los registros se mejoran con parámetros de seguridad y métricas de rendimiento

DETECCIÓN ROBUSTA

- Amenazas de día cero y avanzadas (APT, etc.)
- Troyanos de acceso remoto (RAT)
- Fuga de datos (uso indebido de DNS, SSH, HTTP(S), ICMP, etc.)
- Tráfico tunelizado (DNS, SSH, HTTP(S), ICMP, etc.)
- Anomalías de protocolo
- Análisis de puertos
- Ataques de diccionario y de fuerza bruta
- Robo de datos y otras amenazas internas
- Infracción de las políticas internas de seguridad
- Desconfiguraciones de la red
- DoS, DDoS
- Recogida automática de datos (por ejemplo, tienda electrónica)
- Análisis de tráfico cifrado (certificados SSL, fingerprinting, etc.)

FLUJO DE RED

- hasta 50 Gbits de tráfico de origen
- hasta 1.000 de fuentes externas (conmutadores)
- almacenar campos HTTP, TLS y DNS de IPFix
- extraer métricas de rendimiento
- extraer parámetros, por ejemplo, interfaz entrante
- detectar direcciones IP en listas negras
- perfiles de rendimiento
- soporte para múltiples interfaces de dispositivos

INVENTARIO DE RED

- Capa de visibilidad y detección fusionadas en una visión clara
- Infraestructura de red con valor añadido de información detallada de subredes y hosts, aderezada con una visión calculada de riesgos y seguridad
- Datos representados en forma de tabla ordenable o interpretación gráfica escalable