Sensor USM de AlienVault

¿Qué está pasando y dónde? ¿Cuál es el impacto sobre sus datos y aplicaciones esenciales? ¿Cuáles son los mayores riesgos que están sucediendo en su red ahora mismo?

El Sensor USM es el módulo de seguridad que actúa en primera línea de defensa en la plataforma unificada de gestión de la seguridad AlienVault Unified Security Management (USM™), y ofrece visibilidad detallada de sus activos, vulnerabilidades, comportamiento malicioso, vectores de ataques y servicios de red. Es uno de los tres componentes de la plataforma USM AlienVault (logger, sensor y servidor). El Sensor USM ejecuta cuatro de las cinco funcionalidades esenciales de USM AlienVault: descubrimiento de activos, análisis de vulnerabilidades, detección de intrusos y monitorización de comportamientos.

Los Sensores USM reciben los datos sin modificar de los logs que generan distintos dispositivos, el tráfico de red, los Agentes USM y los escaneos activos y se encargan de normalizarlos y reenviarlos Servidor USM para proceder a la correlación de eventos y su análisis mediante el servicio Inteligencia de Amenazas de AlienVault Labs, que se actualiza continuamente. Puede implementar el Sensor USM como aplicación independiente o como parte de un appliance todo en uno. Lo ofrecemos tanto como appliance físico y appliance virtual. El Sensor USM proporciona estas funcionalidades esenciales threat intelligence. The USM Sensor delivers these essential capabilities:

Descubrimiento de activos — Realiza automáticamente el inventario de activos

El descubrimiento automático de activos implica que usted no tendrá que supervisar los sistemas y los datos de su red, ni siquiera en los entornos actuales tan cambiantes. Las técnicas de escaneo activo y pasivo de red crean un inventario de los activos desplegados en su red, un primer paso esencial para poner en marcha con éxito un programa exhaustivo de seguridad. Con un detallado mapa de red, podrá evaluar las vulnerabilidades, detectar amenazas y monitorizar su red y sus servicios para localizar conductas maliciosas o poco usuales.

Análisis de vulnerabilidades — Detecta qué activos son vulnerables a los ataques

El coste y la complejidad pueden dejar determinadas tecnologías esenciales, como el análisis de vulnerabilidades, fuera del alcance de muchos equipos de IT con recursos limitados. El análisis de vulnerabilidades identifica el software y los sistemas vulnerables, lo cual ayuda a priorizar sus acciones de remediación y mejora su seguridad. Mediante la combinación del descubrimiento de activos y el análisis de vulnerabilidades, la plataforma USM pone al alcance de los equipos de IT de cualquier tamaño la visibilidad de redes y la toma de conciencia en materia de seguridad, ambas esenciales.

Detección de intrusos — Identifica los hosts acechados y las amenazas activas

El sistema de detección de intrusos en redes (IDS) del Sensor USM monitoriza activamente su tráfico de red para detectar tráfico malicioso y patrones de ataque dentro de su red. También utiliza el conocimiento exhaustivo de las vulnerabilidades del sistema, generado a partir de los datos del Análisis de Vulnerabilidades, para alertarle de las amenazas que acechan a sus sistemas vulnerables.

Monitorización de comportamientos — Identifica cambios en las condiciones normales de funcionamiento

Los cambios en el comportamiento de su red, sus sistemas y sus servicios pueden indicar que hay un ataque en marcha o que hay un sistema comprometido. El Sensor USM combina el análisis de flujo de red (NetFlow) para monitorizar cambios en el tráfico de red y para la captura de paquetes para análisis forenses, la monitorización activa del servicio para verificar de forma proactiva los cambios en los servicios, y la recopilación de logs para detectar anomalías reportadas por otros elementos de su infraestructura.

Gestión ininterrumpida del ciclo vital de la seguridad

Securizar su infraestructura es un proceso continuo, no un evento puntual. Diseñamos el Sensor AlienVault para reducir el coste y la complejidad de implementar una solución exhaustiva de seguridad basada en el ciclo de vida de su infraestructura. La arquitectura flexible del USM de AlienVault le permite implementar su sensor de forma centralizada junto con otros elementos del USM, o distribuido en puntos estratégicos de su red. Independientemente del modelo de implementación que elija, USM mantiene un flujo ininterrumpido de trabajo basado en el ciclo de vida. Ofrece toda la potencia y flexibilidad sin el coste ni la complejidad de las soluciones puntuales: lo mejor de ambos mundos.

FUNCIÓN	BENEFICIO
DESCUBRIMIENTO DE ACTIVOS	
Monitorización pasiva de red	Observa el tráfico de red de forma no intrusiva para identificar los hosts y los paquetes de software instalados.
Escaneo activo de red	Encuentra sistemas que no estén activos actualmente sondeando la red, descubriendo hosts y enumerando los servicios en ejecución.
Inventario de software basado en host	Mantiene un inventario detallado de las configuraciones de hardware y software.
Descubrimiento de red	Descubre y mapea automáticamente la topología de la red para identificar dispositivos desconocidos.
ANÁLISIS DE VULNERABILIDADES	
Escaneo autentificado	Ofrece el método más preciso para detectar vulnerabilidades mediante el acceso directo al sistema de archivos del host y la inspección del software instalado.
Escaneo no autentificado	Amplía los beneficios del escaneo a los hosts cuando no sea posible la autenticación.
DETECCIÓN DE INSTRUSIONES	
Detección de intrusión en red	Visibilidad inmediata de los ataques contra su sistema.
Integridad de archivos e IDS basados en el host	Monitoriza los sistemas internos de un host para proporcionar visibilidad del ataque y hacer cumplir las políticas de seguridad.
MONITORIZACIÓN DE COMPORTAMIENTOS	
Análisis de flujo de red	Proporciona una valiosa visión del uso del ancho de banda y de las aplicaciones en ejecución en su red.
Captura de paquetes	Captura datos de paquetes para evaluar tráfico concreto con el fin de realizar un análisis detallado de amenazas.
Monitorización activa del servicio	Asegura que solo los servicios deseados estén en ejecución de forma activa y que no haya alteraciones del servicio, o servicios no deseados en ejecución.
Recolección de logs	Consolidación de logs de infraestructuras remotas e integración con herramientas de terceros para acelerar y simplificar la detección de amenazas y su remediación.

CONTÁCTENOS PARA SABER MÁS

WWW.ALIENVAULT.COM