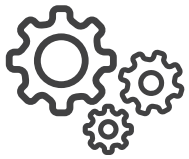
Servidor AlienVault

La automatización de la seguridad, la gestión unificada y el conocimiento simplifican y aceleran su capacidad para detectar y responder a las amenazas

El Servidor USM de AlienVault, la piedra angular de la plataforma Gestión Unificada de la Seguridad (USM™), combina la automatización de la seguridad, la gestión unificada y el conocimiento de amenazas para correlacionar los datos, identificar las amenazas de su red, proporcionar una guía para la remediación y mejorar su eficiencia operativa.

USM de AlienVault le permite configurar, gestionar y controlar rápida y eficazmente las cinco características esenciales de seguridad que no deberían faltar en ninguna empresa: descubrimiento de activos, evaluación de vulnerabilidades, detección de intrusiones, monitorización de comportamientos y SIEM. Al unificar estas cinco capacidades en una sola plataforma USM, AlienVault simplifica su gestión y reduce la complejidad, permitiéndole emplear más tiempo en asegurar su red y menos tiempo en implementar y configurar herramientas, escribir reglas de correlación y buscar amenazas.



Automatización de la seguridad: acelera su respuesta ante las amenazas

El Servidor USM de AlienVault automatiza actividades esenciales para simplificar el proceso de detección de amenazas y proporcionarle la información que necesita en ese mismo instante para dar respuesta a eventos que están ocurriendo en su red. La plataforma USM recopila y correlaciona la información sobre activos, vulnerabilidades, amenazas y conductas, reunidas en sus fuentes de datos integradas para crear una visión que abarca toda la red para detectar actividades sospechosas o maliciosas. Las reglas de correlación preconfiguradas usan todos los datos de eventos de sus archivos de registro para identificar los incidentes de seguridad que son más importantes. La automatización de la seguridad del Servidor USM produce alertas altamente precisas y utilizables, permitiéndole emplear su valioso tiempo en dar respuesta a las amenazas de mayor prioridad a las que se enfrenta su red, en lugar de buscar manualmente los archivos de registro e investigar las amenazas.

Gestión unificada: reduce el coste y la complejidad de asegurar su red

La gestión unificada reduce la complejidad de intentar mantenerse por delante de las amenazas a las que se enfrenta su red. Esto le permite emplear más tiempo monitorizando su red, en lugar de intentar gestionar herramientas de seguridad independientes. Al diseñar la plataforma USM como una solución unificada, AlienVault le permite hacerlo todo desde una sola consola: identificar un ataque, aislar la brecha de seguridad, determinar el éxito de su acción y definir el alcance del compromiso. La existencia de un marco de informes unificado con programas asistentes fáciles de usar y plantillas para informes personalizables acelera también su cumplimiento normativo, proporcionando a los auditores la información que necesitan.

Conocimiento de amenazas: elimina la necesidad de realizar su propia investigación

El conocimiento de amenazas integrado en USM de AlienVault Labs elimina la necesidad de que los equipos de TI empleen su tiempo llevando a cabo su propia investigación sobre amenazas emergentes o atendiendo alarmas desencadenadas por sus propias herramientas de seguridad. El equipo de AlienVault Labs envía regularmente a la plataforma USM su conocimiento de amenazas en forma de un conjunto coordinado de actualizaciones, lo que acelera y simplifica la detección de amenazas y su remediación. La plataforma USM integra también datos de OTX, la primera comunidad de conocimiento de amenazas verdaderamente abierta del mundo, que permite la defensa colaborativa con datos de amenazas utilizables proporcionados por la comunidad.

El conocimiento de amenazas en acción

Imagine una consola de gestión que puede proporcionar las siguientes funciones de forma impecable: Su firewall detecta un escaneo de puerto, y su servicio de reputación de IP identifica la dirección de origen del escaneo como host malicioso activo. Entonces, su SIEM correlaciona dicha dirección maliciosa de origen como la dirección de destino de una sesión SSH procedente de un host interno. Una búsqueda en su base de datos de activos identifica el perfil de riesgo del host interno: el host es esencial para las operaciones de la empresa, por lo que crea un incidente crítico de seguridad. A continuación, su herramienta de evaluación de vulnerabilidades escanea el host comprometido buscando otras vulnerabilidades, descubriendo que falta un patch de seguridad crítico. Su consola de gestión crea un ticket en un sistema externo de gestión de patches para dar instrucciones al administrador del sistema de que use un patch en el host comprometido y lo devuelva al servicio. Un análisis forense completo del host comprometido durante los últimos 30 días determina que no se necesita ninguna acción correctiva adicional.

Puede tener esta funcionalidad hoy mismo con la plataforma de Gestión Unificada de la Seguridad de AlienVault, y beneficiarse de poder configurar y gestionar todas estas funciones desde una única consola. Y, dado que se remite automáticamente un informe con la información sobre la dirección IP de origen y el comportamiento del ataque al intercambio abierto de amenazas (OTX, Open Threat Exchange) de AlienVault, todos aquellos que reciban actualizaciones de conocimientos de amenazas de OTX podrán protegerse frente a un amenaza similar.

FUNCIÓN	BENEFICIO
GESTIÓN UNIFICADA	
Gestión unificada de herramientas de seguridad	Costeo reducido de propiedad mediante monitorización y configuración centralizadas para sensores y registradores.
Gestión federada	Admite la separación necesaria de tareas debido a requisitos organizativos o normativos; admite entornos multiempresa para proveedores de servicios.
Más de 200 informes de amenazas y cumplimiento de normativas predefinidos	Genera fácilmente informes sobre incidentes, alarmas, vulnerabilidades, tickets de problemas, activos, disponibilidad de servicios y salud de la red.
Más de 2.500 módulos de informes	Reducción del tiempo empleado en crear informes personalizados mediante la reutilización de informes existentes.
Generación de informes dirigido por asistente	Cumplimenta rápidamente los informes requeridos sobre cumplimiento de normativa y operaciones específicos para una organización.
Paneles configurables y ampliables	Crea vistas personalizadas de amenazas, cumplimientos y datos operativos para cada usuario.
AUTOMATIZACIÓN DE SEGURIDAD	
Correlación en tiempo real	Mejora la productividad de las operaciones de seguridad al convertir eventos sin modificar en alertas utilizables.
Más de 2.000 reglas de correlación predefinidas	Asegura la máxima efectividad de los controles de seguridad integrados.
Asistente para crear reglas de correlación personalizadas	Crea fácilmente reglas de correlación para cumplir los requisitos de seguridad y cumplimiento de normativas específicos de su organización u empresa.
Análisis contextual de comportamientos	Evaluación del riesgo de la actividad anómala correlacionándola con la información del entorno, como la importancia del activo.
Reconocimiento de patrones y análisis de comportamientos	Acelera las acciones correctivas al correlacionar el conocimiento de amenazas actual con el incidente de seguridad.
Validación de eventos dinámicos	Automatiza la solución inicial de problemas al consultar las herramientas de seguridad integradas para reunir más información sobre el estado de la red y de los activos.
CONOCIMIENTO DE AMENAZAS	
Conocimiento de amenazas de AlienVault Labs	Las actualizaciones regulares del conocimiento de amenazas enviadas a la plataforma USM eliminan la necesidad de que usted tenga que llevar a cabo su propia investigación, acelerando y simplificando la detección de amenazas y su remediación.
Datos de amenazas integrados proporcionados por la comunidad de OTX	OTX es la primera comunidad de conocimiento de amenazas verdaderamente abierta del mundo que permite la defensa colaborativa con datos de amenazas utilizables, proporcionados por la comunidad, que ofrecen una visión global de las tendencias de los ataques y de los actores maliciosos.

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM