Suscripción AlienVault Threat Intelligence

Le proporcionamos en el momento la información que necesita

Las amenazas cambian constantemente con el descubrimiento casi diario de nuevas vulnerabilidades, técnicas de ataque y nuevas cepas de malware. Usted no tiene el tiempo ni los recursos para investigar estas amenazas emergentes, o para determinar si su entorno está en riesgo o ya se ha visto comprometido. En lugar de hacerlo ellos mismos, los equipos de seguridad de TI más activos acuden a la suscripción Threat Intelligence de AlienVault Labs para mantenerse al día con la última información sobre los agentes maliciosos y sus herramientas, infraestructura y métodos.

La suscripción Threat Intelligence ofrecida por el equipo de AlienVault Labs permite que organizaciones de todos los tamaños se centren en dar respuesta a las amenazas de las que informa la plataforma Unified Security Management (USM™) de AlienVault, en lugar de tener que investigar por sí mismos. Al alertarle de las amenazas más significativas que tienen su red como objetivo, la plataforma USM maximiza la efectividad de cualquier equipo de TI y le permite responder rápida y eficazmente.

Mantenga su plataforma USM protegida frente a las amenazas más recientes

La plataforma USM proporciona cinco características esenciales de seguridad que no deberían faltar en ninguna empresa: descubrimiento de activos, gestión de vulnerabilidades, detección de intrusiones, monitorización de comportamientos e información de seguridad, y gestión de eventos (SIEM). El equipo de AlienVault Labs utiliza varias técnicas, tanto manuales como automatizadas, para ayudar a desarrollar el conocimiento de amenazas, como por ejemplo: honeypots (equipos trampa), análisis de malware realizado en la misma empresa y análisis del big data.

Con la unificación de estas características esenciales de seguridad en una sola plataforma y el suministro continuo de conocimiento de amenazas actualizado, la plataforma USM le proporciona respuestas a las siguientes preguntas críticas:

- Soy vulnerable a esta amenaza?
- ¿Puede mi sistema detectar esta amenaza?
- ¿Soy un objetivo de la amenaza?

Al automatizar el proceso de detección de amenazas, USM le permite emplear más tiempo dando respuesta a las amenazas y menos tiempo aprendiendo, implementando y configurando herramientas. USM de AlienVault le proporciona todo lo que necesita para manejar las amenazas y lograr el cumplimiento regulatorio.

Validación de amenazas

Para que nuestros clientes puedan eliminar la necesidad de llevar a cabo su propia investigación, el equipo de investigación de amenazas de AlienVault Labs emplea innumerables horas trazando mapas de los distintos tipos de ataques, las amenazas más recientes, los comportamientos sospechosos, las vulnerabilidades y los exploits que descubren por todas las amenazas.

Dado que somos propietarios tanto de las fuentes de datos como de la plataforma de gestión, nuestros expertos en amenazas poseen una comprensión exhaustiva de las interacciones entre los distintos tipos de datos que se están correlacionando y analizando, así como las últimas técnicas de ataque. Incluimos esta experiencia en los controles de seguridad integrados y en el conocimiento ininterrumpido de amenazas integrado que proporcionamos, para permitirle detectar las amenazas más recientes, así como enseñarle cómo mitigar las amenazas rápida y eficazmente, independientemente de su entorno de red.

El equipo de AlienVault Labs envía regularmente a la plataforma USM conocimiento de amenazas en forma de conjunto coordinado de actualizaciones, lo que acelera y simplifica la detección de amenazas y su remediación:

- **Directivas de correlación:** USM se envía con más de 2,500 reglas predefinidas que traducen los eventos sin modificar en información sobre amenazas específica y utilizable, al relacionar eventos dispares de toda su red.
- **Firmas IDS de red:** detecte el tráfico malicioso más reciente de su red
- **Firmas IDS del host:** identifique las amenazas más recientes cuyo objetivo son sus sistemas esenciales
- **Firmas de descubrimiento de activos:** detecte la información más reciente sobre sistemas operativos, aplicaciones y dispositivos
- **Firmas de evaluación de vulnerabilidades:** revela las vulnerabilidades más recientes de sus sistemas
- **Módulos de informes:** reciba nuevas visualizaciones de los datos críticos de su entorno para gestionar y satisfacer las demandas de los auditores
- **Plantillas dinámicas de respuesta a incidentes:** guía personalizada sobre cómo responder a cada alerta
- **Plugins para fuentes de datos ahora compatibles:** amplíe su capacidad de monitoreo al integrar datos de dispositivos y aplicaciones de seguridad antiguos

Investigación continua de amenazas

AlienVault Labs constantemente monitoriza, analiza, hace ingeniería inversa e informa sobre amenazas sofisticadas que incluyen ataques desde el día cero, malware avanzado, botnets, campañas de phishing y más. Mediante este equipo de expertos en seguridad renombrados y con dedicación exclusiva, AlienVault contribuye de varias formas con código, documentación, análisis y resultados de investigación a la comunidad dedicada a la seguridad, a su educación y a hacer del mundo un lugar más seguro para todos nosotros.

La investigación sobre amenazas proporcionada por AlienVault incluye la información más reciente en las áreas siguientes:

- Exploits y vulnerabilidades
- Ataques de fuerza bruta
- Ataques de denegación de servicio (DoS)
- Detección de malware
- Ataques a nivel de red
- Ataques a sistemas SCADA
- Escaneo y sondeo del sistema
- Actividad maliciosa

La Suscripción Threat Intelligence de AlienVault incorpora las últimas investigaciones sobre amenazas del equipo de AlienVault Labs. Para saber más sobre las actualizaciones que proporciona la suscripción Threat Intelligence, visite la sección de actualizaciones de AlienVault Labs en los foros de AlienVault. Para saber más acerca de las demás investigaciones sobre seguridad que publica este equipo, visite el blog de AlienVault Labs.

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM