REPÚBLICA DE GUATEMALA **EJÉRCITO DE GUATEMALA**

“II Curso Internacional de Informática y Ciberdefensa”

Asignatura:

Seguridad informática

ALIENVAULT OSSIM

Oficial Alumno:

TTE. DE INF. HUGO MORALES BATZ

INDICE

INTRODUCCIÓN

En un mundo de amenazas cibernéticas en constante crecimiento, la elección de la herramienta adecuada para gestionar la seguridad de la información se vuelve crucial. La Seguridad de la Información y la Gestión de Eventos (SIEM) es esencial para proteger los sistemas y datos de una organización. En este contexto, AlienVault OSSIM emerge como una solución potente y de código abierto. En esta exploración, analizaremos las características y ventajas de AlienVault OSSIM, centrándonos en su capacidad para detectar, analizar y responder a amenazas en tiempo real, También consideraremos sus desafíos y cómo se adapta a las necesidades de seguridad únicas de cada organización.

I. ¿QUÉ ES EL SIEM?

El SIEM es una herramienta esencial en ciberseguridad que se encarga de centralizar la recopilación, correlación y análisis de datos de seguridad procedentes de diversas fuentes en una red o sistema. Su objetivo es identificar patrones de comportamiento, detectar eventos anómalos y potenciales amenazas, y emitir alertas en tiempo real para una respuesta inmediata. Al brindar visibilidad sobre actividades maliciosas o sospechosas, el SIEM fortalece la postura de seguridad de una organización y contribuye al cumplimiento de regulaciones al generar informes detallados. También facilita el análisis forense en caso de incidentes, proporcionando datos históricos para comprender la naturaleza y alcance de los mismos, permitiendo así una mejora continua de la estrategia de seguridad de la organización.

II. ¿QUÉ ES ALIENVAULT OSSIM?

AlienVault OSSIM es una herramienta de seguridad de código abierto que se enfoca en la detección, análisis y respuesta a amenazas en tiempo real, AlienVault OSSIM ofrece un conjunto completo de capacidades diseñadas para abordar los desafíos de seguridad que enfrentan las organizaciones en el entorno digital actual.

Esta solución integral no solo proporciona visibilidad en tiempo real sobre eventos y comportamientos sospechosos, sino que también permite la correlación de datos de seguridad de diversas fuentes. AlienVault OSSIM se destaca por su enfoque en la detección proactiva, su integración con ELK Stack y su capacidad de automatizar respuestas ante eventos de seguridad. Además, su naturaleza de código abierto proporciona flexibilidad y personalización, lo que permite adaptar la herramienta a las necesidades únicas de cada organización.

En resumen, AlienVault OSSIM se presenta como una opción valiosa para fortalecer la seguridad en un mundo digital en constante evolución, al brindar una plataforma eficiente y adaptable para enfrentar las amenazas cibernéticas y proteger los sistemas y datos de una organización.

AlienVault OSSIM tiene la capacidad de recolectar y gestionar una amplia variedad de registros (logs) de eventos provenientes de diversas fuentes en una red. Esta capacidad es fundamental para su función de detección y respuesta a amenazas, así como para el análisis forense y la generación de informes.

III. FUNCIONALIDADES Y VENTAJAS DE ALIENVAULT OSSIM

A. Funcionalidades:

1. Detección en Tiempo Real: AlienVault OSSIM ofrece una supervisión constante en tiempo real. Monitoriza eventos y registros de forma continua para identificar patrones y comportamientos sospechosos en el momento en que ocurren.
2. Integración con ELK Stack: La colaboración con ELK Stack (Elasticsearch, Logstash y Kibana) facilita la administración de datos de seguridad. Esta integración no solo garantiza un almacenamiento eficiente, sino que también simplifica el procesamiento y la visualización de información para comprender mejor la actividad de seguridad.

3. Detección de Amenazas: Equipado con reglas predefinidas, AlienVault OSSIM amplía su capacidad para identificar comportamientos maliciosos. Estas reglas abarcan diversas amenazas, incluyendo

intrusiones y ataques cibernéticos conocidos, brindando una sólida defensa inicial.

4. Automatización de Respuestas: AlienVault OSSIM permite configurar respuestas automáticas o manuales a eventos de seguridad, permitiendo una acción rápida y proactiva para minimizar el impacto de las amenazas potenciales.

5. Personalización: Una ventaja distintiva es la capacidad de AlienVault OSSIM para adaptarse a las necesidades específicas de cada organización. Además de las reglas predefinidas, la herramienta permite crear reglas personalizadas que se ajusten a los requisitos únicos de seguridad.

6. Cumplimiento Normativo: AlienVault OSSIM simplifica el cumplimiento de regulaciones y normativas de seguridad al proporcionar reglas y plantillas predefinidas que ayudan a cumplir con los requisitos establecidos.

A. Ventajas:

1. Detección Proactiva: La capacidad de AlienVault OSSIM para detectar comportamientos anómalos en tiempo real ayuda a anticipar amenazas y a tomar medidas preventivas.

2. Integración Avanzada: La colaboración con ELK Stack mejora la gestión y visualización de datos de seguridad, permitiendo una comprensión más profunda de la actividad en línea.

3. Eficiencia en Respuestas: La automatización de respuestas a eventos de seguridad agiliza la mitigación de amenazas, minimizando su impacto en el sistema.

4. Personalización Flexible: La adaptabilidad de AlienVault OSSIM a las necesidades únicas de cada organización permite una seguridad más enfocada y precisa.

5. Cumplimiento Simplificado: Con reglas y plantillas predefinidas, AlienVault OSSIM facilita el proceso de cumplimiento normativo.

6. Registro Integral: La sólida capacidad de generación y administración de registros contribuye al análisis forense, la revisión de incidentes y la detección temprana de problemas.

IV. DESVENTAJAS

A. Requerimientos Técnicos Avanzados: La configuración y administración de AlienVault OSSIM pueden ser complejas y requieren un nivel significativo de conocimiento técnico. Organizaciones con recursos limitados o equipos no familiarizados con ciberseguridad podrían enfrentar dificultades en la implementación y operación.

B. Curva de Aprendizaje: Aunque es una herramienta de código abierto, el aprendizaje de todas las funcionalidades de AlienVault OSSIM puede llevar tiempo. La necesidad de capacitación y familiarización con la plataforma podría requerir recursos adicionales.

C. Escalabilidad Limitada: A medida que la cantidad de eventos y datos aumenta, AlienVault OSSIM puede enfrentar desafíos en términos de

escalabilidad. Requiere ajustes y optimizaciones para mantener un rendimiento óptimo en entornos de alta demanda.

D. Actualizaciones y Mantenimiento: Al igual que cualquier software, AlienVault OSSIM necesita actualizaciones regulares para corregir vulnerabilidades y agregar nuevas características. Mantener la herramienta actualizada puede requerir recursos y pruebas para minimizar interrupciones.

E. Dependencia de la Comunidad: Aunque es respaldada por una comunidad activa, la evolución futura de AlienVault OSSIM podría depender de la comunidad de desarrollo. Esto podría generar incertidumbre en cuanto a la disponibilidad continua de soporte y actualizaciones.

F. Complejidad en la Configuración: La riqueza de opciones de configuración y personalización puede resultar en una mayor complejidad para implementar AlienVault OSSIM de manera eficiente. Requiere una planificación cuidadosa y una comprensión profunda de las funcionalidades.

G. Necesidad de Soporte Adicional: Aunque es de código abierto, algunas organizaciones podrían requerir asistencia adicional en forma de capacitación o soporte especializado para maximizar el valor de AlienVault OSSIM.

H. Posibles Limitaciones de Información: La calidad de las alertas y la precisión de la detección dependen en parte de la calidad y cantidad de datos que la herramienta recopila. En algunos casos, podría haber limitaciones en la disponibilidad o calidad de la información recopilada.

V. ¿POR QUÉ ELEGIR ALIENVAULT OSSIM?

La elección de AlienVault OSSIM como nuestra herramienta de elección para implementar SIEM se basa en una evaluación exhaustiva en comparación con otras opciones disponibles. Sus características y ventajas destacan de manera significativa, especialmente en áreas clave que son esenciales para nuestra estrategia de seguridad.

VI. CARACTERISTICAS DE ALIENVAULT OSSIM

A. Detección en Tiempo Real: AlienVault OSSIM monitoriza continuamente eventos y registros en tiempo real para identificar comportamientos anómalos y actividades sospechosas en la red.

B. Integración con ELK Stack: La plataforma utiliza la combinación de Elasticsearch, Logstash y Kibana (ELK Stack) para almacenar, procesar y visualizar los datos de seguridad de manera eficiente.

C. Correlación de Eventos: AlienVault OSSIM utiliza técnicas de correlación para analizar eventos y registros de múltiples fuentes y determinar si hay patrones o comportamientos que podrían indicar una amenaza.

D. Detección de Amenazas: La herramienta viene con reglas predefinidas para detectar una amplia gama de amenazas, como intrusiones, malware y comportamientos sospechosos.

E. Automatización de Respuestas: Permite configurar respuestas automáticas a eventos de seguridad, lo que permite una acción rápida para mitigar amenazas y minimizar su impacto.

F. Personalización de Reglas: Además de las reglas predefinidas, AlienVault OSSIM permite crear reglas personalizadas adaptadas a las necesidades únicas de la organización.

G. Cumplimiento Normativo: Proporciona reglas y plantillas predefinidas para ayudar a cumplir con regulaciones y normativas de seguridad, simplificando el proceso de auditoría.

H. Generación y Administración de Registros: La herramienta registra eventos y actividades de seguridad, lo que es esencial para el análisis forense, la revisión de incidentes y el cumplimiento normativo.

I. Gestión de Vulnerabilidades: AlienVault OSSIM puede identificar y rastrear vulnerabilidades en los sistemas y activos de la red, ayudando a priorizar las acciones de mitigación.

J. Mapa de la Red y Topología: Proporciona una vista visual de la topología de la red y los activos, lo que ayuda en la identificación rápida de posibles puntos de entrada de amenazas.

K. Integración de Fuentes de Datos: Puede integrar datos de diversas fuentes, como firewalls, sistemas de detección de intrusiones y más, para una visión holística de la seguridad.

L. Análisis Forense: Facilita la investigación de incidentes al proporcionar datos históricos y contexto para comprender la naturaleza y el alcance de los ataques.

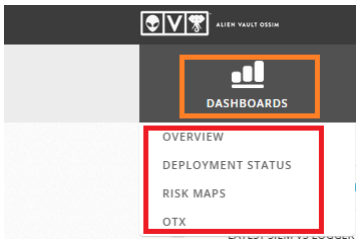
M. Generación de Informes: AlienVault OSSIM puede generar informes detallados sobre eventos de seguridad, actividades y tendencias, lo que es valioso para la toma de decisiones y la auditoría.

VII. Interfaz web

La interfaz web del servidor OSSIM consta de las siguientes opciones en la GUI principal.

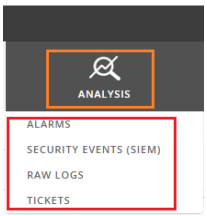
A. Tablero

Muestra una vista completa de todos los componentes del servidor OSSIM, como la gravedad de la amenaza, las vulnerabilidades en el host de la red, el estado de implementación, los mapas de riesgo y las estadísticas de OTX. El submenú del tablero se muestra en la siguiente figura



B. Análisis

El análisis es un componente muy importante de cualquier dispositivo SIEM. El servidor OSSIM analizó los hosts en función de sus registros. Este menú muestra las alarmas, SIEM (eventos de seguridad), tickets y registros sin procesar. El menú de análisis se divide en el siguiente submenú.

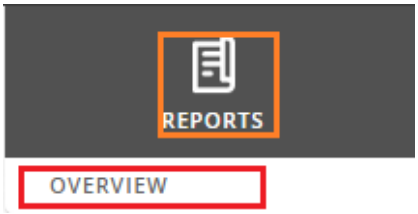


C. Ambiente

En este menú del servidor OSSIM, la configuración está relacionada con los activos de la organización. Muestra los activos, el grupo y la red, las vulnerabilidades, el flujo de red y la configuración de detección. El submenú para todos estos ajustes se muestra en la figura.

D. **Informes**

Los informes son un componente importante de cualquier servidor de registro. El servidor OSSIM también genera informes que son muy útiles para la investigación detallada de cualquier host específico.



E. Configuración.

En la configuración meHow to Install and Configure AlienVault SIEM (OSSIM) nu, el usuario puede cambiar la configuración del servidor OSSIM, como cambiar la dirección IP de la interfaz de administración, agregar más host para monitorear y registrar y agregar / eliminar diferentes sensores / complementos. El submenú de todos los servicios se muestra a continua

VIII. Sensor USM de AlienVault

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.

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.

A. 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.

B. 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.

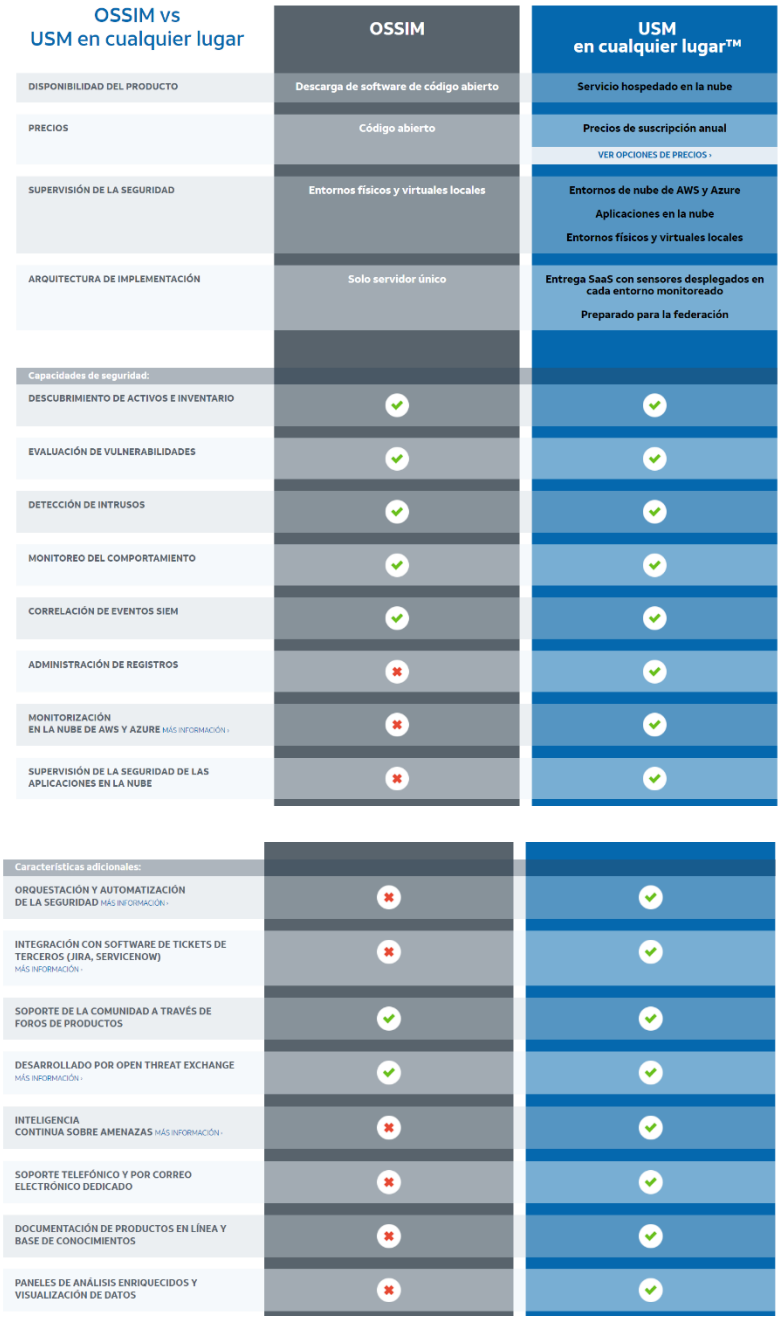
C. Detección de intrusos — Identifica los hosts acechados y las amenazas activas

   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.

D. 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.

IX. DIFERENCIAS ENTRE ALIENVAULT OSSIM VS USM



OSSIM vs USM en cualquier lugar	OSSIM	USM en cualquier lugar™
DISPONIBILIDAD DEL PRODUCTO	Descarga de software de código abierto	Servicio hospedado en la nube
PRECIOS	Código abierto	Precios de suscripción anual VER OPCIONES DE PRECIOS ›
SUPERVISIÓN DE LA SEGURIDAD	Entornos físicos y virtuales locales	Entornos de nube de AWS y Azure Aplicaciones en la nube Entornos físicos y virtuales locales
ARQUITECTURA DE IMPLEMENTACIÓN	Solo servidor único	Entrega SaaS con sensores desplegados en cada entorno monitoreado Preparado para la federación
Capacidades de seguridad:		
DESCUBRIMIENTO DE ACTIVOS E INVENTARIO	✓	✓
EVALUACIÓN DE VULNERABILIDADES	✓	✓
DETECCIÓN DE INTRUSOS	✓	✓
MONITOREO DEL COMPORTAMIENTO	✓	✓
CORRELACIÓN DE EVENTOS SIEM	✓	✓
ADMINISTRACIÓN DE REGISTROS	✗	✓
MONITORIZACIÓN EN LA NUBE DE AWS Y AZURE MÁS INFORMACIÓN ›	✗	✓
SUPERVISIÓN DE LA SEGURIDAD DE LAS APLICACIONES EN LA NUBE	✗	✓
Características adicionales:		
ORQUESTACIÓN Y AUTOMATIZACIÓN DE LA SEGURIDAD MÁS INFORMACIÓN ›	✗	✓
INTEGRACIÓN CON SOFTWARE DE TICKETS DE TERCEROS (JIRA, SERVICENOW) MÁS INFORMACIÓN ›	✗	✓
SOPORTE DE LA COMUNIDAD A TRAVÉS DE FOROS DE PRODUCTOS	✓	✓
DESARROLLADO POR OPEN THREAT EXCHANGE MÁS INFORMACIÓN ›	✓	✓
INTELIGENCIA CONTINUA SOBRE AMENAZAS MÁS INFORMACIÓN ›	✗	✓
SOPORTE TELEFÓNICO Y POR CORREO ELECTRÓNICO DEDICADO	✗	✓
DOCUMENTACIÓN DE PRODUCTOS EN LÍNEA Y BASE DE CONOCIMIENTOS	✗	✓
PANELES DE ANÁLISIS ENRIQUECIDOS Y VISUALIZACIÓN DE DATOS	✗	✓

CONCLUSIÓN:

AlienVault OSSIM ofrece una solución valiosa para la Seguridad de la Información y la Gestión de Eventos. A pesar de algunas desventajas, sus capacidades de detección proactiva, integración con ELK Stack, automatización de respuestas y personalización lo hacen una opción sólida. Su capacidad para centralizar la recopilación y análisis de registros de eventos de diversas fuentes permite identificar amenazas en tiempo real y fortalecer la seguridad cibernética.