CONFIGURACIÓN DE LABORATORIO SIEM: ALIENVAULT OSSIM

SIEM- GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD

La gestión de eventos e información de seguridad (SIEM) es un enfoque de la gestión de la seguridad que combina las funciones SIM (gestión de la información de seguridad) y SEM (gestión de eventos de seguridad) en un único sistema de gestión de la seguridad. El acrónimo SIEM se pronuncia "sim" con una e muda.

Los principios subyacentes de todo sistema SIEM son agregar datos relevantes de múltiples fuentes, identificar desviaciones de la norma y tomar las medidas adecuadas. En el nivel más básico, un sistema SIEM puede basarse en reglas o emplear un motor de correlación estadística para establecer relaciones entre las entradas de registro de eventos. Los SIEM avanzados han evolucionado para incluir análisis del comportamiento de usuarios y entidades (UEBA) y orquestación de la seguridad y respuesta automatizada (SOAR).

ALIENVAULT - OSSIM

OSSIM (Open Source Security Information Management) es un sistema de gestión de eventos e información de seguridad de código abierto que integra una selección de herramientas diseñadas para ayudar a los administradores de red en la seguridad informática, la detección y la prevención de intrusiones.

Como sistema SIEM, OSSIM pretende ofrecer a los analistas y administradores de seguridad una visión de todos los aspectos relacionados con la seguridad de su sistema, combinando la gestión de registros y la gestión y descubrimiento de activos con información procedente de controles de seguridad de la información y sistemas de detección dedicados. A continuación, esta información se correlaciona para crear contextos a la información no visibles desde una sola pieza.

- Descubrimiento de activos
- Evaluación de vulnerabilidades
- Detección de intrusiones en host
- Detección de intrusiones en la red
- Supervisión del comportamiento
- Correlación de eventos SIEM
- Acceso a la interfaz web
- Configuración Supervisión de red
- Detección de activos
- Despliegue de HIDS
- Gestión de registros
- Integración OTX API

INTEGRACIÓN OTX API

Ya viene con Open Threat Exchange (OTX). Esta comunidad abierta de inteligencia sobre amenazas proporciona inteligencia sobre amenazas generada por la comunidad y le permite colaborar con ella, además de automatizar el proceso de actualización de su infraestructura de seguridad con datos sobre amenazas procedentes de cualquier fuente.

CONFIGURACIÓN DE OSSIM

DESPLIEGUE

Podemos implementar AlienVault USM Appliance de dos maneras: simple o compleja.

IMPLEMENTACIÓN SIMPLE

Implementa todos los componentes de AlienVault USM Appliance -Sensor, Servidor y Registrador- en una sola máquina llamada USM Appliance All-in-One.

Este modelo de implementación es el más adecuado para entornos pequeños, pruebas y demostraciones.

DESPLIEGUE COMPLEJO/DISTRIBUIDO

Este modelo despliega cada componente de AlienVault USM Appliance -Sensor, Servidor y Registrador- como una máquina virtual o de hardware individual para crear una topología distribuida.

Optamos por un método de implementación simple

REQUISITOS DEL SISTEMA

USM Appliance Minimum Required Hardware Specifications

Name	Value
CPU Type	Intel® Xeon E5620
RAM Type	DDR3 1333 MHz
Disk Type	SAS 10000 RPM (204 MB/s)
Memory Performance (MEMCPY)	3310.32 MiB/s
Disk Performance (random read/write)	15.97 MB/s (120 Mb/s)

Este es el requisito básico de hardware del servidor OSSIM. El requisito de hardware o entorno virtual es:

USM Appliance Virtual Machine Requirements

	USM Appliance All-In-One		Remote Sensor		USM Appliance Standard		
	1TB	500GB	1TB	250GB	Server	Logger	Sensor
Total Cores[1]	8		4		8		
RAM (GB)	16		8		24		
Storage (TB)	1.0	0.5	1.0	0.25	1.2	1.8	1.2
Virtualization Environment	VMware ESXi 4.*x*, 5.*x*, 6.0, and 6.5[2] Hyper-V v3.0+ (Windows Server 2008 SP2 and later)						

NAVEGADORES COMPATIBLES

Supported Browsers

Browser/Platform	Windows	Mac OS X	Linux
Chrome	Yes	Yes	Yes
Edge	Yes	N/A	N/A
Firefox	Yes	Yes	Yes
Internet Explorer 11	Yes	N/A	N/A
Safari	N/A	Yes	N/A

INSTALAR ALIENVAULT OSSIM

En su máquina virtual, cree una nueva instancia VM utilizando la ISO como fuente de instalación.

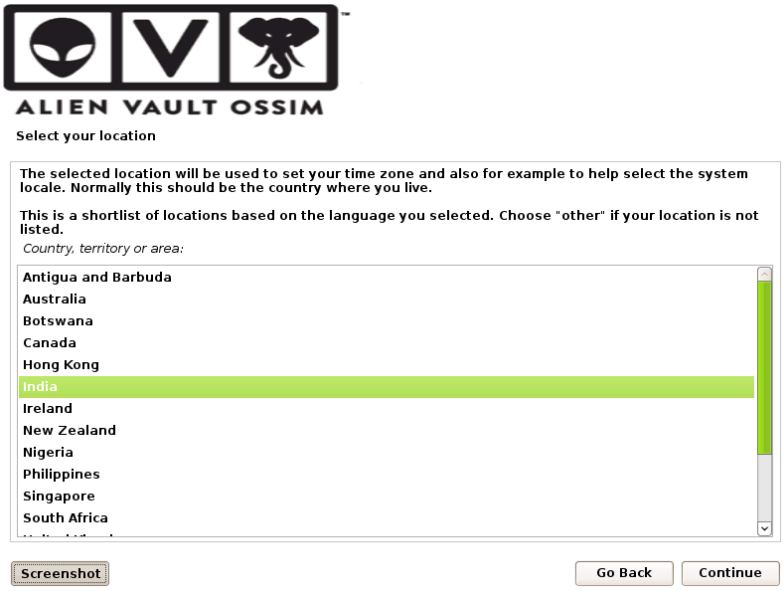
Enlace para descargar la ISO: https://dlcdn.alienvault.com/AlienVault_OSSIM_64bits.iso

Una vez iniciada la nueva instancia, seleccione Instalar AlienVault OSSIM (64 bits) y pulse Intro.

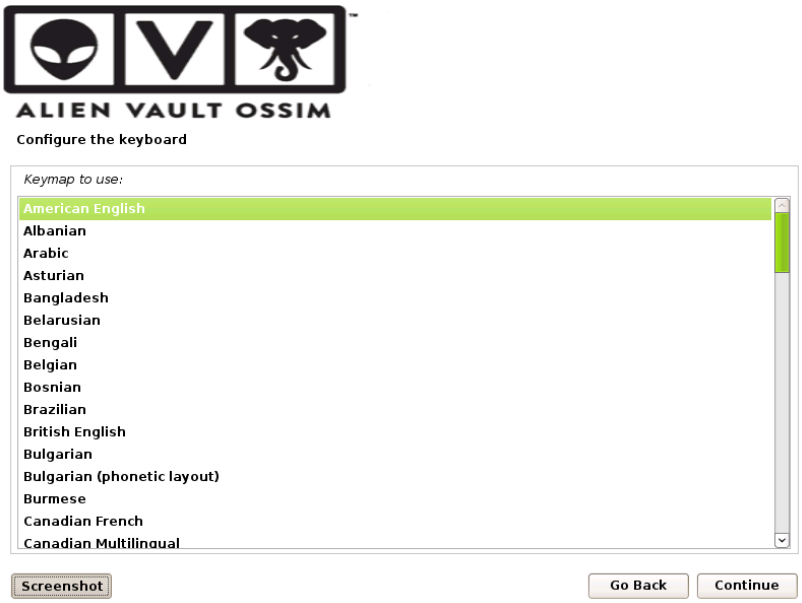
El proceso de instalación le llevará a través de una serie de opciones de configuración. Elija la opción primera.

Seleccionar idioma:

Seleccionar ubicación:

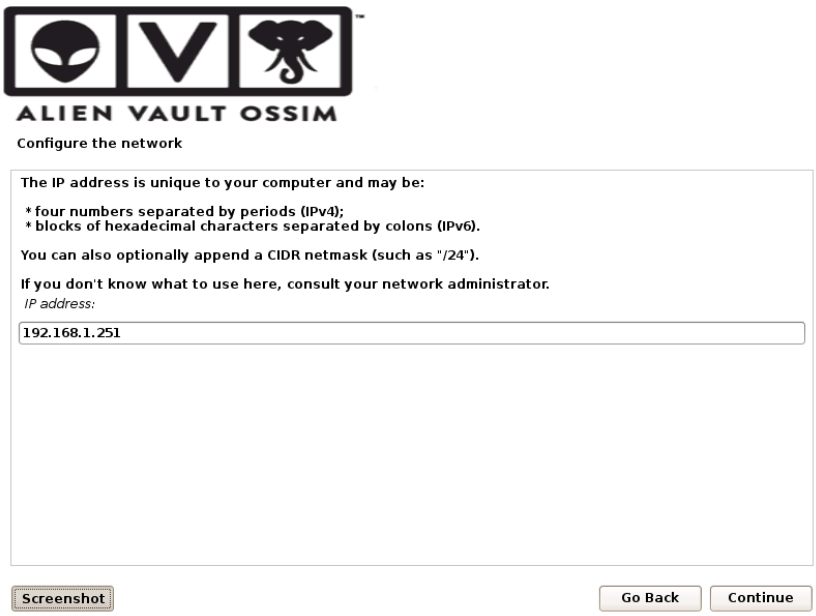


Mapa de teclado a utilizar:

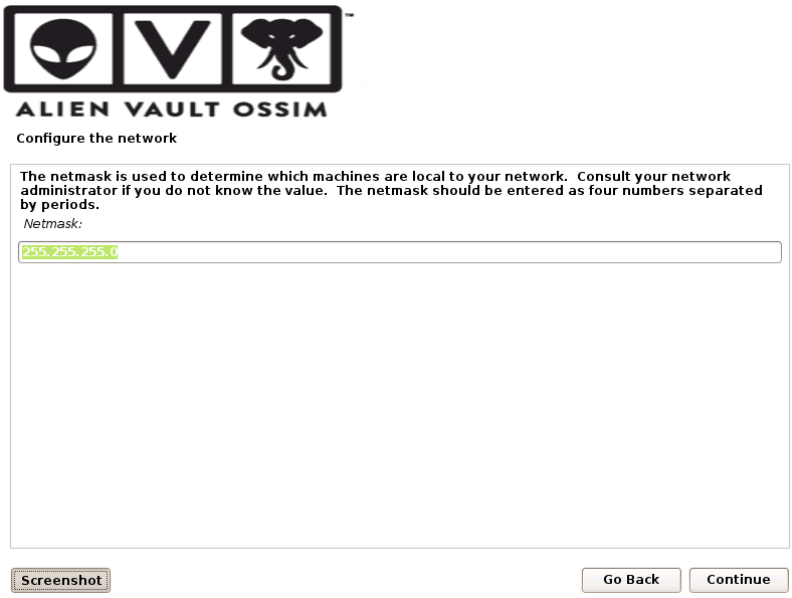


A continuación, la instalación carga los componentes necesarios y detecta la configuración.

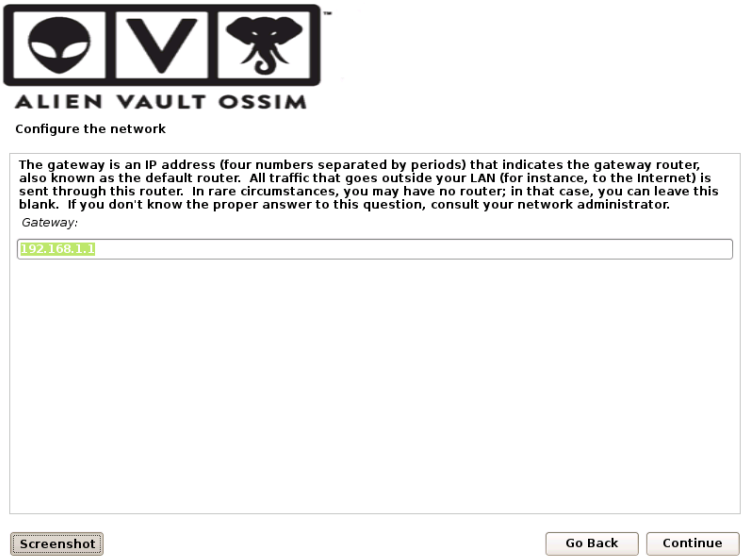
A continuación, configure la red asignando la siguiente Dirección IP:



Máscara de red



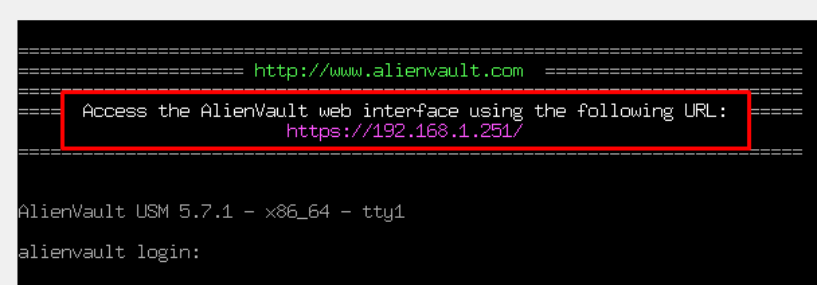
Puerta de enlace



Dirección del servidor DNS

La dirección IP será la dirección web que utilice para acceder a la interfaz de usuario web de AlienVault OSSIM.

Después de la instalación, se reinicia automáticamente y la página de inicio de sesión tiene el siguiente aspecto,



Inicie sesión con las credenciales de la cuenta root.

CONFIGURAR LA INTERFAZ DE SUPERVISIÓN DE REGISTROS

Después de iniciar sesión correctamente, debe configurar la interfaz de gestión de registros.

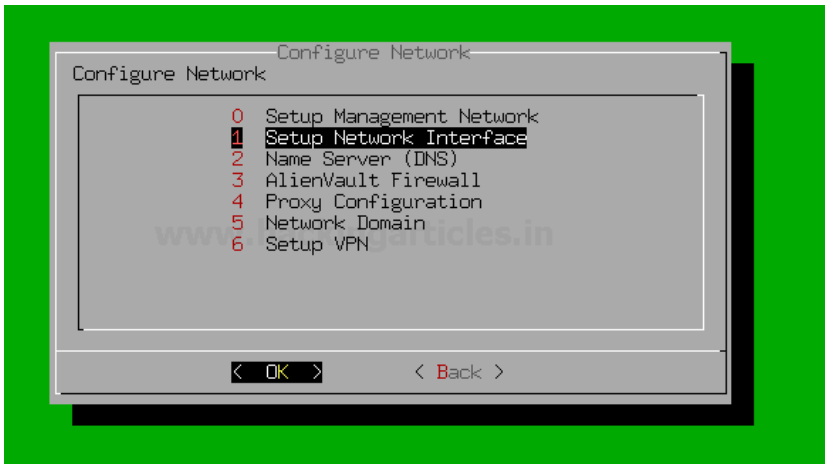
Para configurar una interfaz de red para la gestión y el análisis de registros, siga los pasos que se describen a continuación.

Haga clic en Preferencias del Sistema > Configurar red > Configurar interfaz de red > eth1 > dirección IP > máscara de red.

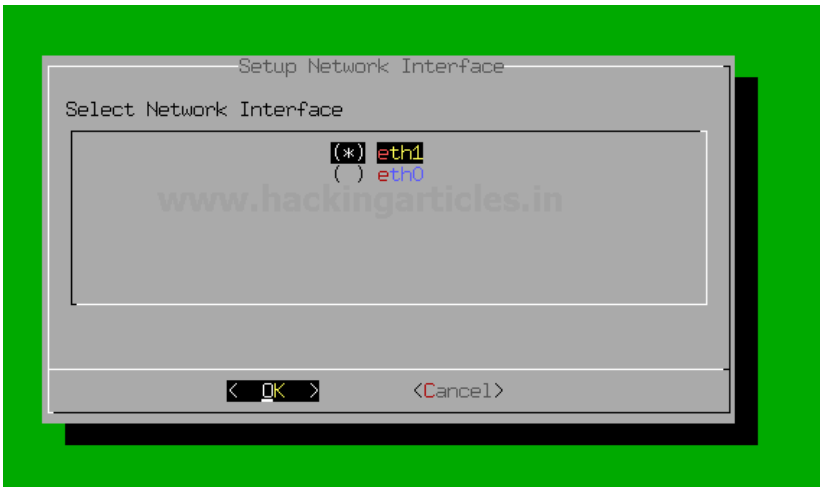
Vaya a Preferencias del Sistema

Seleccione Configurar red

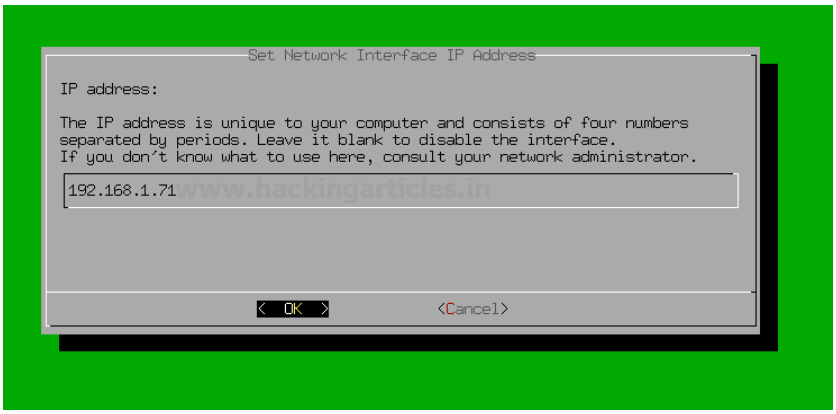
Seleccione la interfaz de red



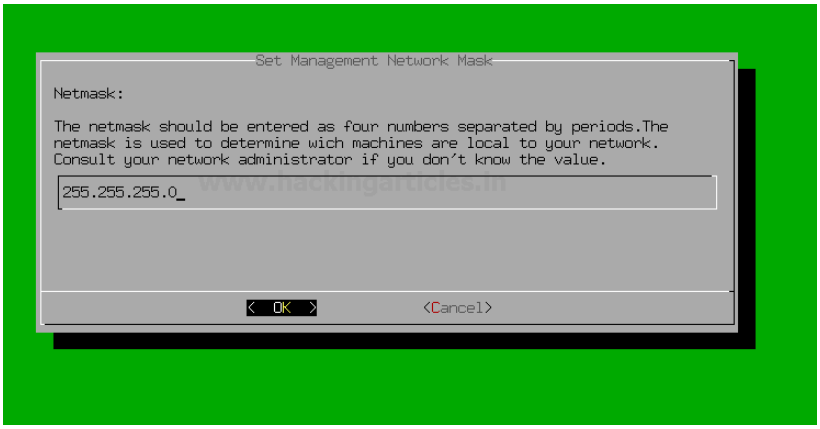
Seleccione eth1 para la gestión y escaneo de logs.



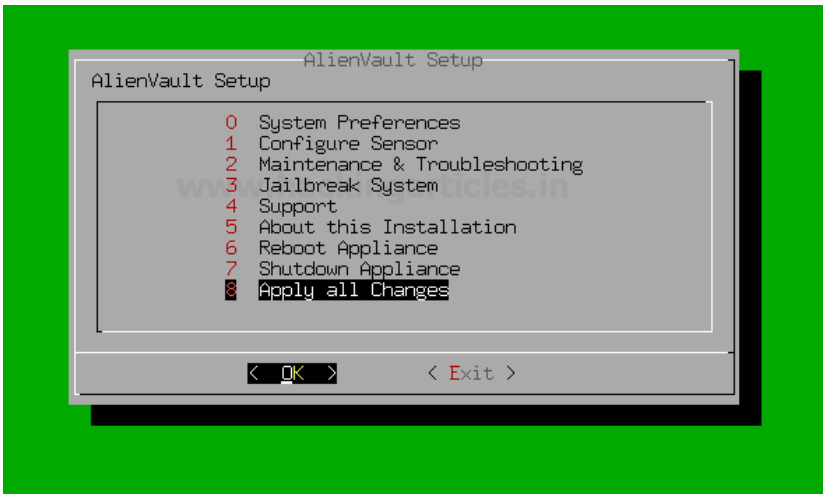
Asignar una dirección IP única para configurar una interfaz de gestión de red



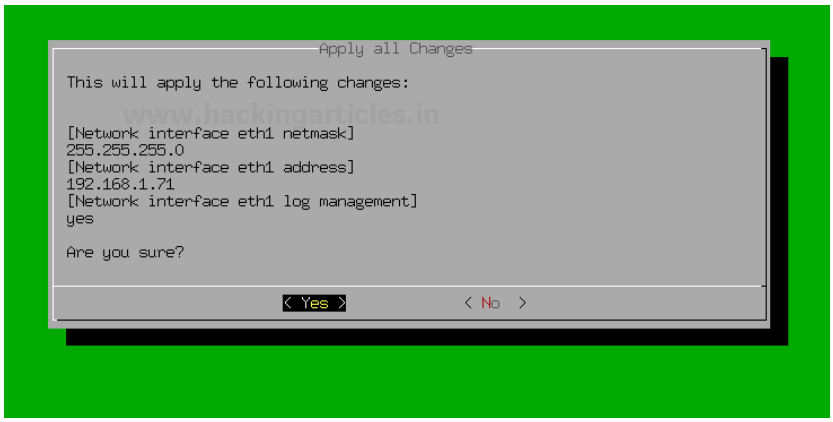
Asigna la máscara de red de la dirección IP designada.



Y luego vuelva a la configuración de AlienVault seleccionando atrás y atrás y luego seleccione Aplicar todos los cambios como se muestra a continuación.



Verifique los cambios que ha realizado, si son correctos seleccione sí.



Ahora ya ha configurado correctamente la interfaz de red para la gestión de registros.

ACCESO A LA INTERFAZ WEB

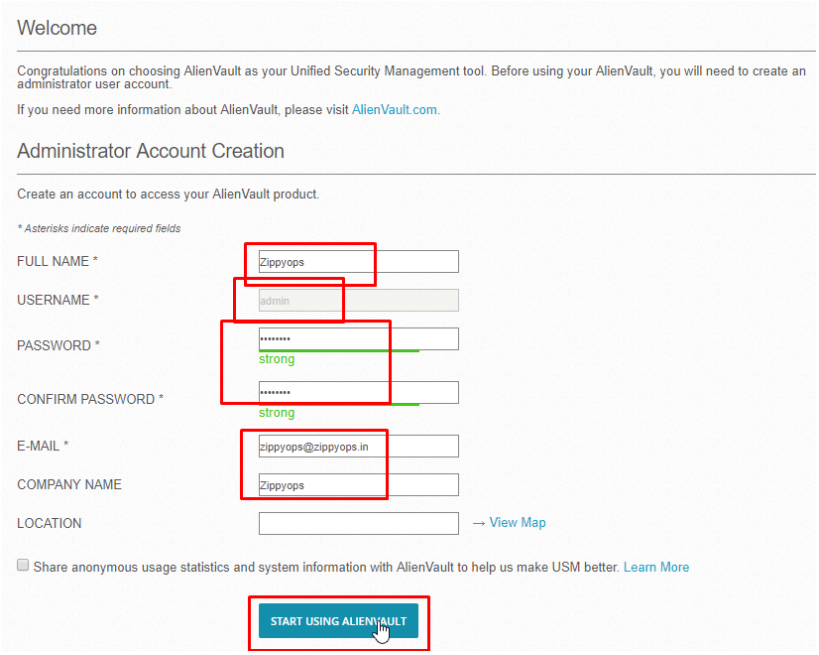
Ahora podemos acceder a la interfaz web a través de la IP, pero tenemos que configurar las credenciales de administrador.

Vaya a su WebUI e introduzca sus credenciales como,

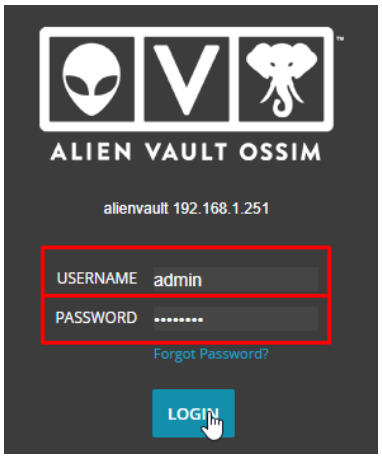
Una vez completado el proceso de instalación, podrás acceder a la interfaz web y configurar tu cuenta de administrador.

Para acceder a la Web UI, abre tu navegador favorito y teclea:

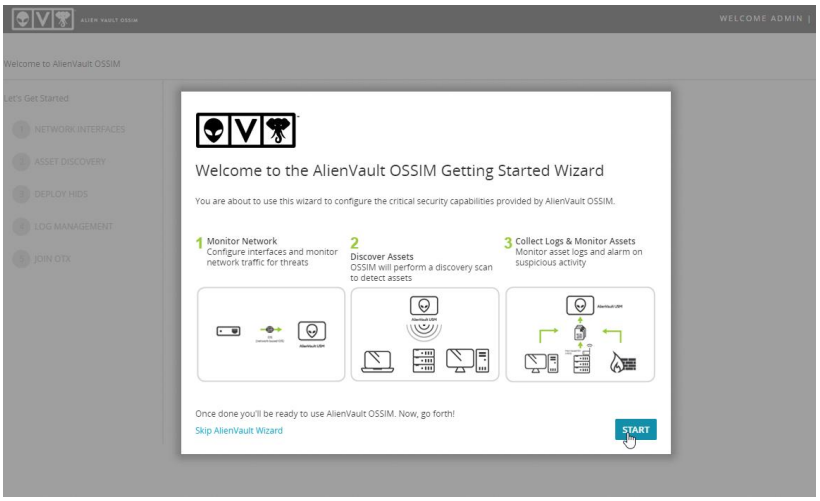
https://ip_establecida_anteriormente



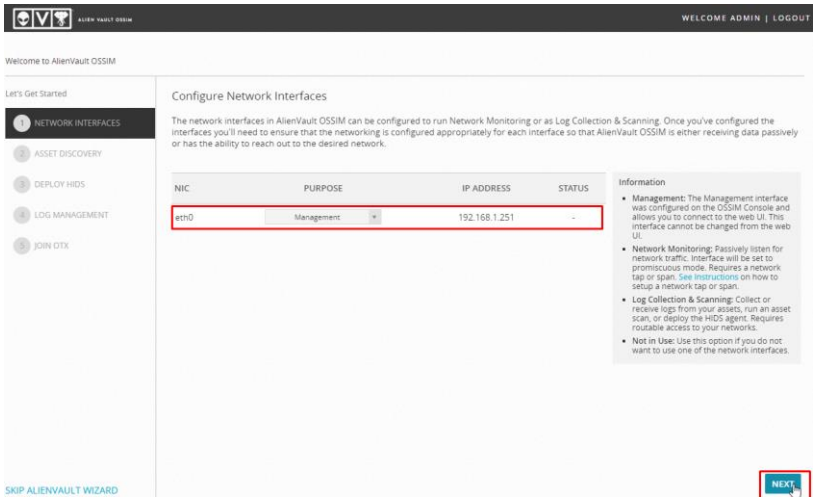
Ahora haga clic en Inicio Uso AlienVault y ahora la interfaz de usuario como,



Haga clic en Inicio para configurar una bóveda alienígena para configurar el sensor y el monitoreo de red,

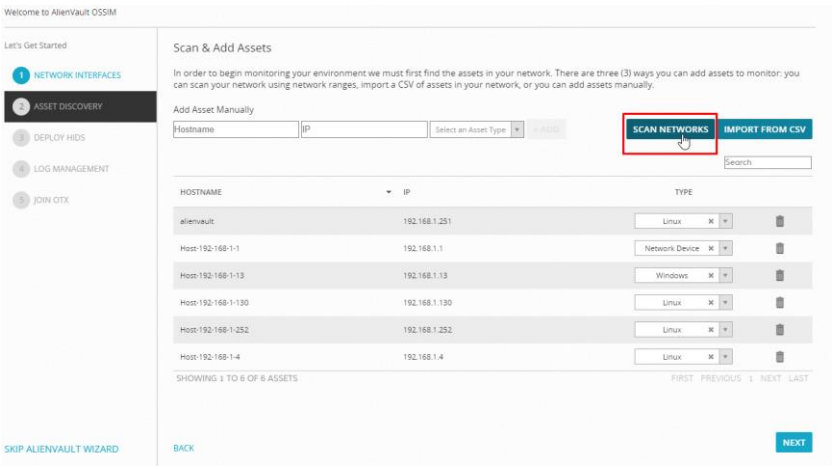


Ahora seleccione el dispositivo de red para escanear el tráfico de red y haga clic en siguiente,

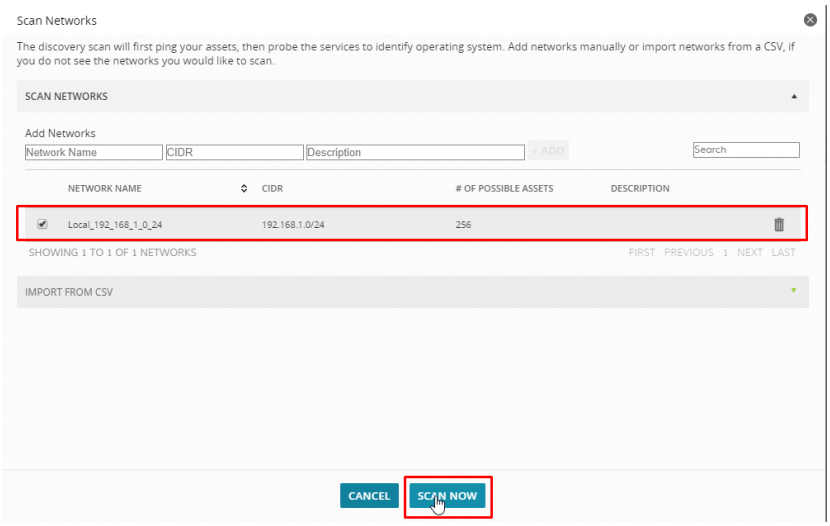


Ahora se hizo una exploración rápida básica y mostrar la lista de dispositivos que podemos añadir activos a través del descubrimiento a través de la exploración de red y la carga de archivos CSV. Es fácil descubrir activos a través de escaneos de red.

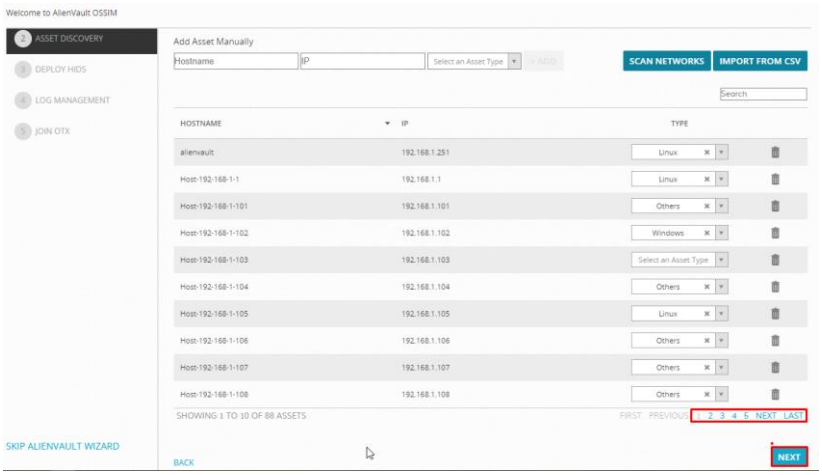
Para ello, seleccione la opción Escanear red y seleccione los dispositivos de red para escanear la red,



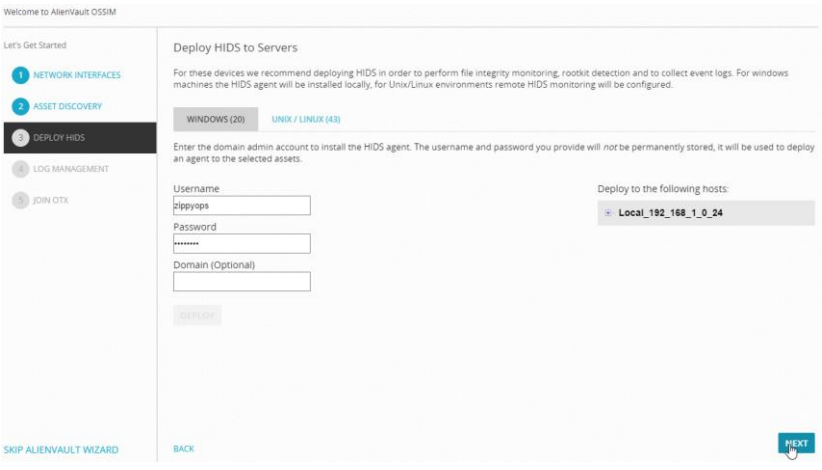
A continuación, haga clic en Escanear ahora para escanear la red,



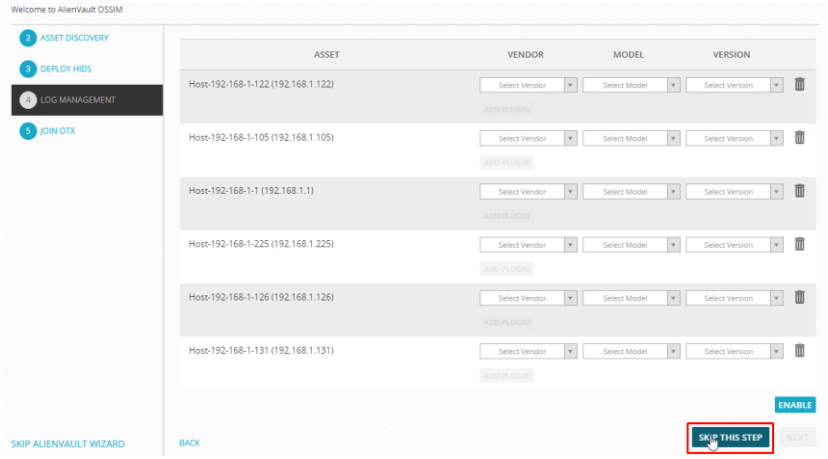
Después del escaneo, descubre la mayoría de los dispositivos conectados a la red.



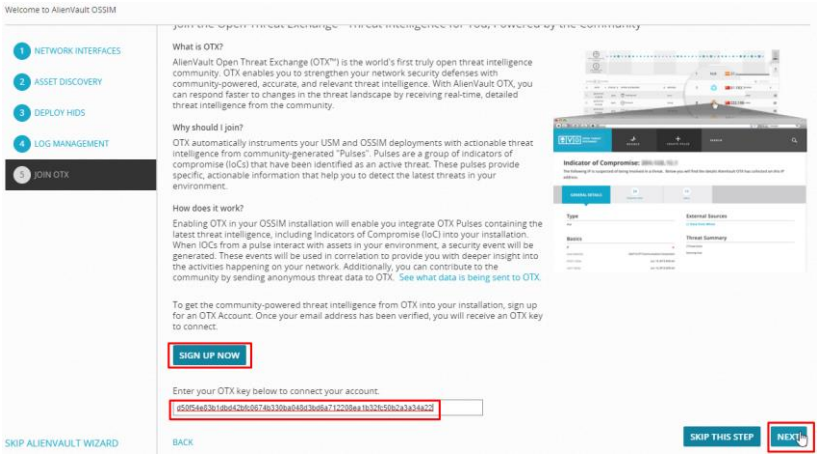
Inicialmente, intenta desplegar el HIDS en todas las IPs descubiertas, para ello necesitamos el mismo nombre de usuario y contraseña para todas las máquinas con privilegios de root. Introduzca el nombre de usuario y la contraseña (si no, tiene que crear un usuario con privilegios de root con el mismo nombre y contraseña). Luego pulse siguiente



Se muestra una lista de dispositivos para agregar plugins para ello seleccione el tipo de proveedor, modelo y versión si no ve su modelo entonces omita el paso haciendo clic en Omitir el paso.



El paso final del asistente de configuración de OSSIM es añadir la clave OTX a OSSIM a través de la cual podemos obtener actualizaciones y soporte.



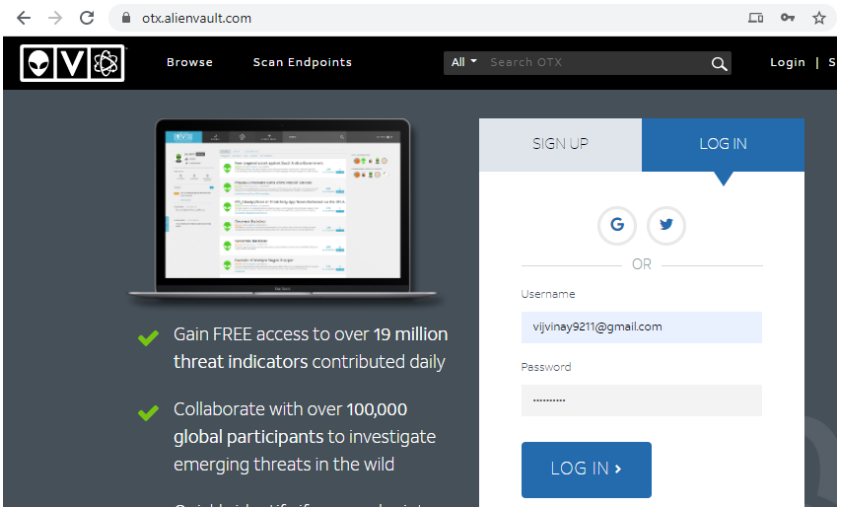
INTEGRACIÓN DE LA API OTX

En la siguiente ventana, se solicitará el token de registro OTX (Open Threat Exchange).

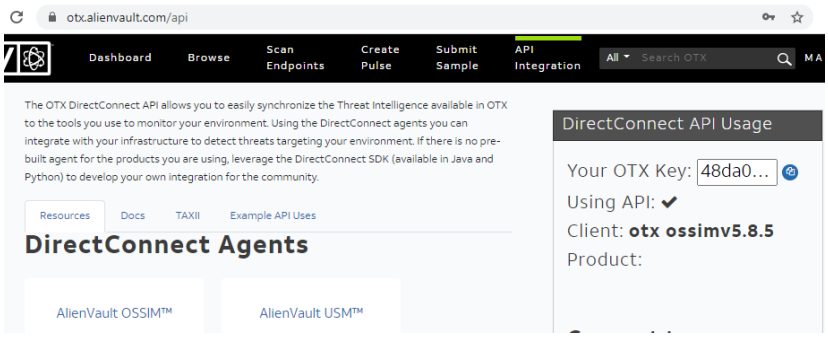
El registro sigue siendo gratuito, y es necesario para indicar o actualizar automáticamente las últimas firmas de amenazas.

Para el registro de OTX visite en: -

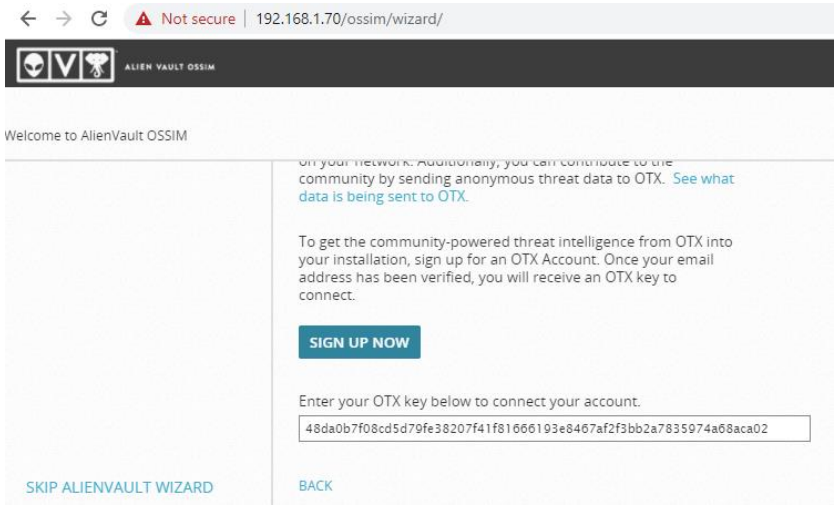
https://otx.alienvault.com/



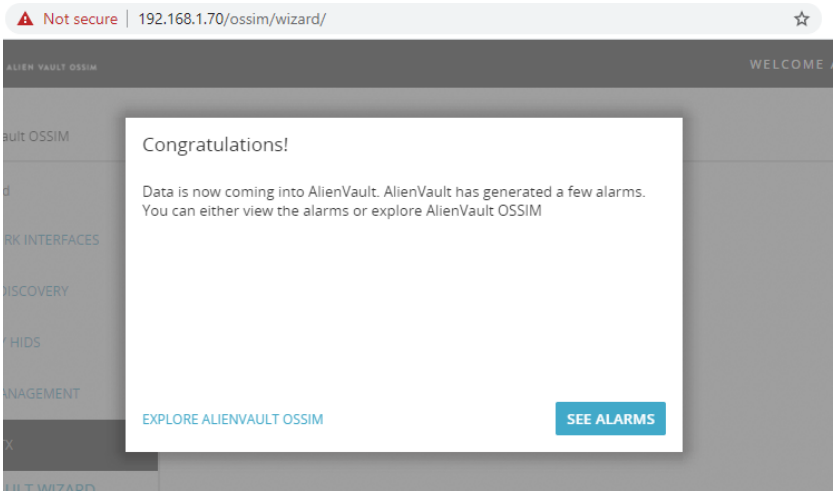
Después de crear la cuenta ingrese a la consola OTX de AlienVault y localice la integración API y luego copie la Clave API OTX como se muestra a continuación



A continuación, vuelva a la interfaz web de OSSIM y pegue la "clave OTX" copiada en el lugar de "Introducir token" como se muestra a continuación



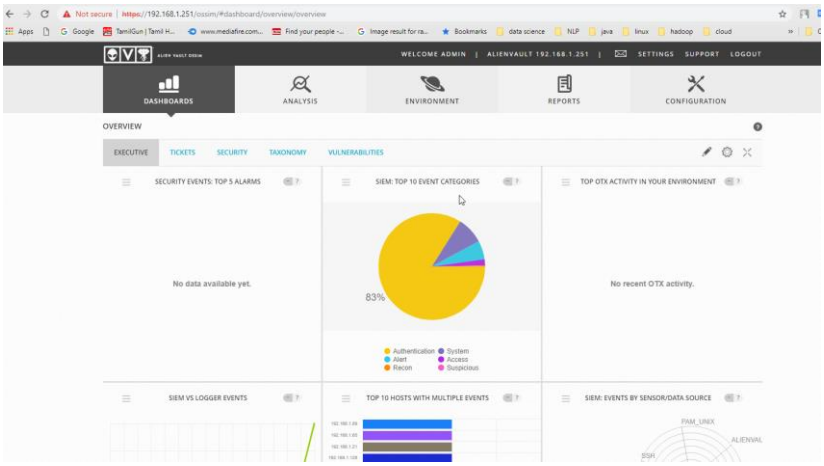
A continuación, haga clic en "Finalizar" u "Omitir" para omitir este paso y finalizar el asistente de configuración.



Ya hemos configurado correctamente la Web UI de AlienVault

Naveguemos por el panel de control de OSSIM.

Como podemos ver, se generaron algunas alarmas que podemos explorar seleccionando Explorar AlienVault OSSIM.



Eso es todo, ahora tienes un servidor OSSIM básico configurado en tu red. Necesitamos añadir un agente para la máquina OSSIM para desplegar HIDS. Podemos instalarlo tanto en sistemas Windows como Linux.

Por defecto, la Interfaz Web muestra una colección de gráficos y diagramas de alto nivel que resumen la actividad de su red.

Desde este panel principal, puede elegir diferentes opciones de menú o hacer clic en otros enlaces y botones seleccionables.

Menú principal: proporciona acceso a las principales funciones u operaciones de USM Appliance. Entre ellas se incluyen:

> **Dashboards**: *Cuadros de mando,* visualización de todos los cuadros, tablas y gráficos de seguridad de la red; estado de despliegue y global del sistema, la red y los dispositivos de USM Appliance; y visualizaciones de amenazas e impulsos OTX.
>
> **Analysis**: *Análisis,* visualización que proporciona búsqueda, clasificación, selección filtrada y visualización de Alarmas, Eventos de seguridad (SIEM), Registros sin procesar y Tickets.

Environment: *Entorno*, Proporciona visualización y gestión de Activos y Grupos, Vulnerabilidades, Datos NetFlow, Captura de Tráfico, Disponibilidad y Detección.

Reports: *Informes,* Proporciona visualización y gestión de varios informes integrados y personalizados seleccionables por categorías, como alarmas, activos, cumplimiento, registros sin procesar, operaciones de seguridad, tickets y actividades de usuario.

Configuration: Configuración, ofrece opciones para ver y gestionar los componentes desplegados de OSSIM Appliance; las opciones de administración permiten gestionar usuarios, la configuración del sistema y los ajustes de copia de seguridad y restauración.

Menú secundario (o submenú): para cada selección del menú principal, suele haber opciones secundarias o de submenú adicionales específicas de un tema concreto que se muestran al hacer clic en la selección principal, por ejemplo, **Dashboard > overview** > **Tickets**.

DESPLIEGUE DEL AGENTE OSSIM-HIDS

DESPLIEGUE EN WINDOWS

Para hosts Microsoft Windows, USM Appliance genera un archivo binario que contiene la configuración apropiada del servidor y la clave de autenticación. Puede dejar que USM Appliance instale el archivo por usted o descargarlo e instalarlo usted mismo en el host.

Antes de desplegar un agente HIDS en el equipo Windows, asegúrese de que cumple los siguientes requisitos.

Si utiliza algún dispositivo acelerador de red en el entorno, debe añadir el sensor de USM Appliance a su lista blanca. Esto se debe a que el USM Appliance Sensor utiliza SMB (Server Message Block) para transferir el paquete de instalación del agente HIDS a la máquina Windows. Si el acelerador de red intenta optimizar el tráfico del USM Appliance Sensor, puede hacer que falle la implementación de HIDS.

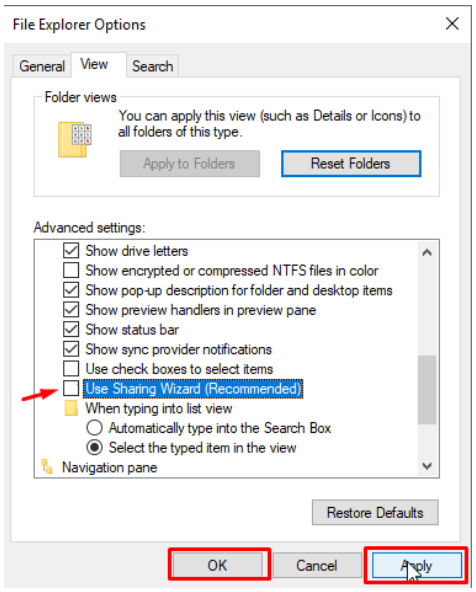
El sistema operativo debe ser uno de los siguientes:

- Microsoft Windows XP
- Windows 7, 8 o 10
- Windows Server 2003, 2008R2 o 2012R2

Debe utilizar una cuenta de usuario que pertenezca al mismo grupo de Administradores que la cuenta de Administrador local.

1. Vaya a Panel de control > Apariencia y personalización > Opción Explorador de archivos > Ver.

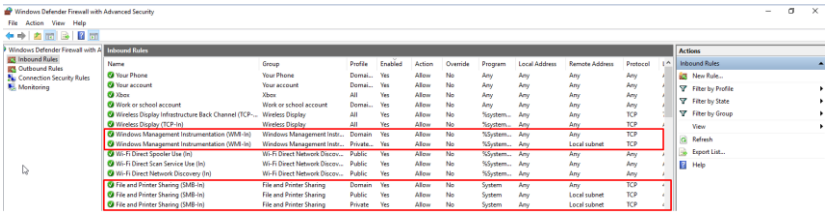
2. Deseleccione Usar asistente para compartir (recomendado).



3. Vaya a Panel de control > Sistema y seguridad > Firewall de Windows > Configuración avanzada > Reglas de entrada.

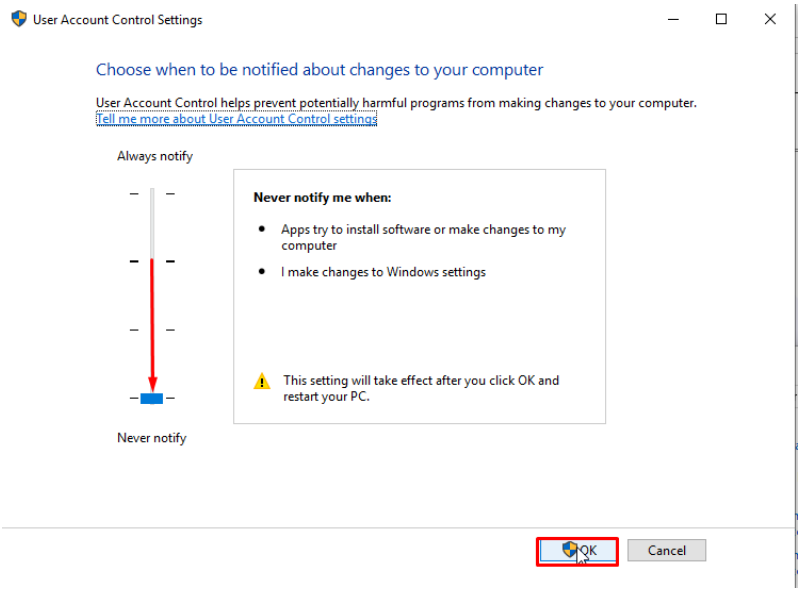
4. Active Compartir archivos e impresoras (SMB-In).

5. Habilite la entrada Instrumental de administración de Windows (WMI).



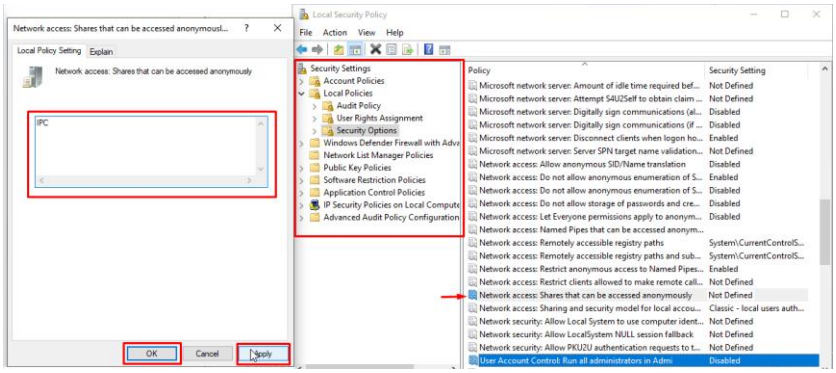
6. Vaya a Panel de control > Cuentas de usuario > Cambiar configuración de control de cuentas de usuario.

7. Mueva el control deslizante a No notificar nunca.



8. Abra la Política de seguridad local.

a. Vaya a Políticas locales > Opciones de seguridad
b. Configure Acceso a la red: Recursos compartidos a los que se puede acceder de forma anónima a IPC.
c. Establezca Control de cuentas de usuario: Ejecutar todos los administradores en Modo de Aprobación Admin en Desactivado (recomendado).



9. Aplique los cambios y reinicie el equipo.

Para implementar el agente AlienVault HIDS en un host Windows

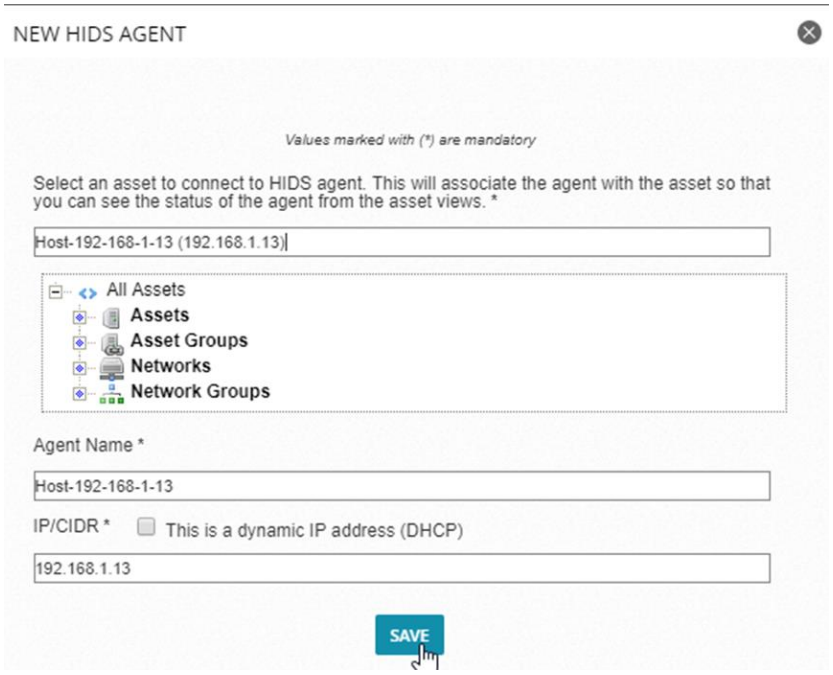
1. Navegue hasta Entorno > Detección.

2. Vaya a HIDS > Agentes > Control de agentes > Agregar agente.

3. En Nuevo agente HIDS, seleccione el host del árbol de activos.

USM Appliance rellena Nombre de agente con el nombre del host e IP/CIDR con la dirección IP del host automáticamente.

4. Haga clic en Guardar.



USM Appliance añade el nuevo agente a la lista.

Necesitamos una herramienta de agente OSSEC para conectar ambos modos windows y Linux como agente con despliegue HIDS. Para Windows descargue la herramienta desde el enlace:

https://updates.atomicorp.com/channels/atomic/windows/ossec-agent-win32-3.2.0-6132.exe

Vaya a Entorno > Detección > Agente > haga clic en el icono de extracción de clave para obtener la clave.

Instálela en su equipo Windows y ejecútela como administrador. A continuación, introduzca la IP del servidor OSSIM en la pestaña IP del servidor OSSEC y pegue la clave en la pestaña de claves, pegue la clave copiada del panel del servidor. En el agente OSSEC haga clic en Administrar > Iniciar OSSEC.

5. Para desplegar el agente

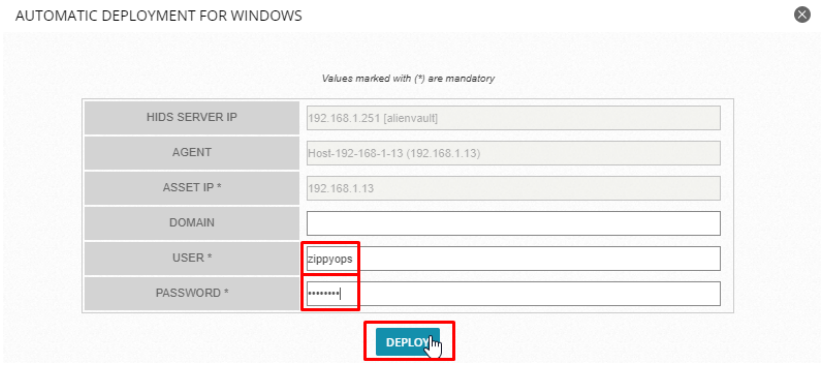
Haga clic en el botón:

https://www.alienvault.com/documentation/resources/images/usm-ids/autodeploy-button.png

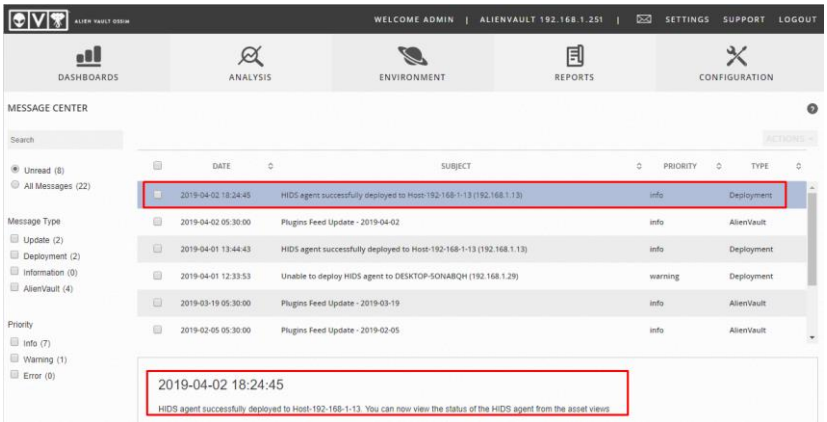
en la columna Acciones.

6. En Despliegue automático para Windows, escriba el Dominio (opcional), el Usuario y la Contraseña del host; a continuación, haga clic en Guardar.

USM Appliance ensambla un archivo binario preconfigurado y lo despliega en el host.



Ahora podemos ver el resultado del despliegue en el centro de mensajes.



7. Alternativamente, para descargar el archivo binario preconfigurado,

Haga clic en el botón:

https://www.alienvault.com/documentation/resources/images/usm-ids/download-deployment-button.png

de la columna Acciones.

Su navegador descargará el archivo automáticamente o le pedirá que lo descargue.

8. Transfiera el archivo, denominado ossec_installer_.exe, al host Microsoft Windows.

9. En el host Windows, haga doble clic para ejecutar el ejecutable.

El instalador se ejecuta brevemente en una consola y, a continuación, muestra una barra de progreso hasta que finaliza.

INSTALACIÓN EN LINUX

También es similar al despliegue de windows HIDS como un lado del agente en el servidor de forma similar añadir agente utilizando su IP

Descargue el archivo tar del agente OSSEC desde el siguiente enlace:

https:/codeload.github.com/ossec/ossec-hids/tar.gz/3.2.0

1. Actualice su sistema Linux utilizando yum update -y

2. Descargue el agente OSSEC mediante el comando wget

https:/codeload.github.com/ossec/ossec-hids/tar.gz/2.8.3

3. Ahora deshabilita SELinux y firewalld en tu sistema usando systemctl stop firewalld y setenforce 0

4. Extraiga el archivo tar descargado utilizando el comando tar -zxvf ossec-hids-2.8.3.tar.gz

5. Goto el ossec-hids-2.8.3

6. Ejecute ./install.sh

[root@nodo ossec-hids-2.8.3]# ./install.sh

which: no host in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin)

** Para instalarlo en portugués, elija [br].

** 要使用中文进行安装, 请选择 [cn].

** Para una instalación alemana, diríjase a [de].

** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].

** Para instalar en inglés, elija [en].

** Para instalar en Español , eliga [es].

** Pour une installation en français, choisissez [fr].

** A Magyar nyelvű telepítéshez válassza [hu].

** Para la instalación en italiano, seleccione [it].

** 日本語でインストールします．選択して下さい． [jp].

** Para la instalación en los Países Bajos, consulte [nl].

** Para instalar en polaco, visite [pl].

** Для инструкций по установке на русском ,введите [ru].

** Za instalaciju na srpskom, izaberi [sr].

** Türkçe kurulum için seçin [tr].

(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: es

A continuación, pulse Intro

7. Introduzca las respuestas a las preguntas formuladas (como seleccionar tipo como agente).

8. Ejecute el archivo manage-agent como ./manage-agents y luego introduzca I

9. Ahora pega la clave extraída del dashboard del servidor ossim y luego pulsa enter

10. Luego ejecute ./ossec-agent start para iniciar el agente.

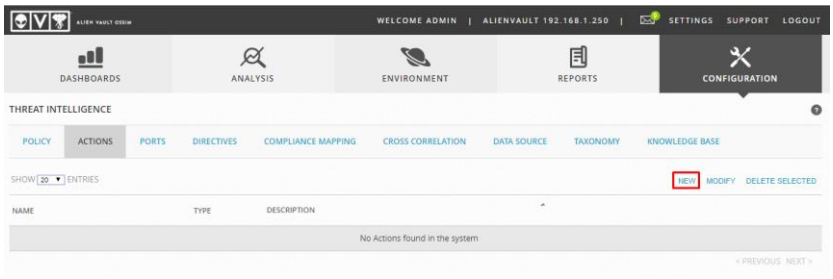
Ahora ve al dashboard y despliega el HIDS en la pestaña agent y comprueba la pestaña message y comprueba el estado del nodo.

CREACIÓN DE ALERTA DE CORREO ELECTRÓNICO

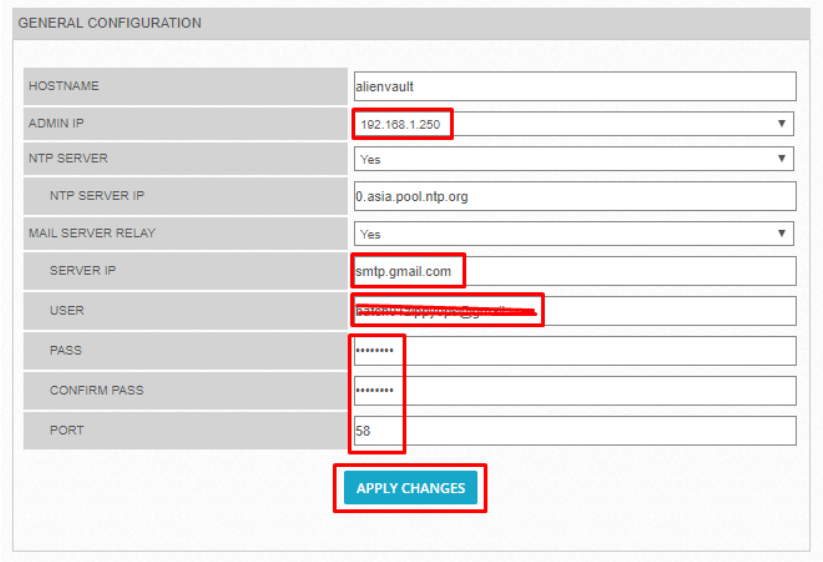
Es una necesidad para cada herramienta SIEM generar una alerta de correo electrónico en caso de ataques y violación de seguridad. Se puede hacer fácilmente en Alienvault OSSIM utilizando Grupos de Políticas. Siga los siguientes pasos para crear un grupo de políticas para generar una alerta de correo electrónico.

CREAR GRUPO DE POLÍTICAS

Vaya a Configuración > Inteligencia de Amenazas > Acciones > Nuevo



Ahora, en la ventana emergente, seleccione Tipo como Enviar un mensaje de correo electrónico y, a continuación, introduzca los valores de Dirección de origen y destino, Condición, Nombre, Asunto, Mensaje y haga clic en Guardar. Ahora vaya a Configuración > Implementación > Componentes > Detalles del servidor y seleccione la pestaña Retransmisión de correo. Introduzca las credenciales y haga clic en Aplicar cambios para guardar las credenciales de correo.



Ahora hemos creado correctamente una alerta de correo para las alarmas.

ALARMAS

AlienVault OSSIM proporciona una vista centralizada de sus alarmas. Vaya a ACTIVIDAD > ALARMAS. La página de alarmas muestra información sobre las alarmas. A la izquierda, encontrará las opciones de búsqueda y filtro. Utilice los filtros para delimitar su búsqueda. Para más información, consulte Búsqueda de alarmas. En la parte superior, puede ver los filtros que ha aplicado y tiene la opción de crear y seleccionar diferentes vistas de las alarmas. La parte principal de la página es la lista de alarmas. Cada fila describe una alarma individual e incluye una casilla de verificación a la izquierda de cada una para seleccionarla. Puede seleccionar todas las alarmas de la misma página haciendo clic en la casilla de verificación de la primera columna de la fila de cabecera.

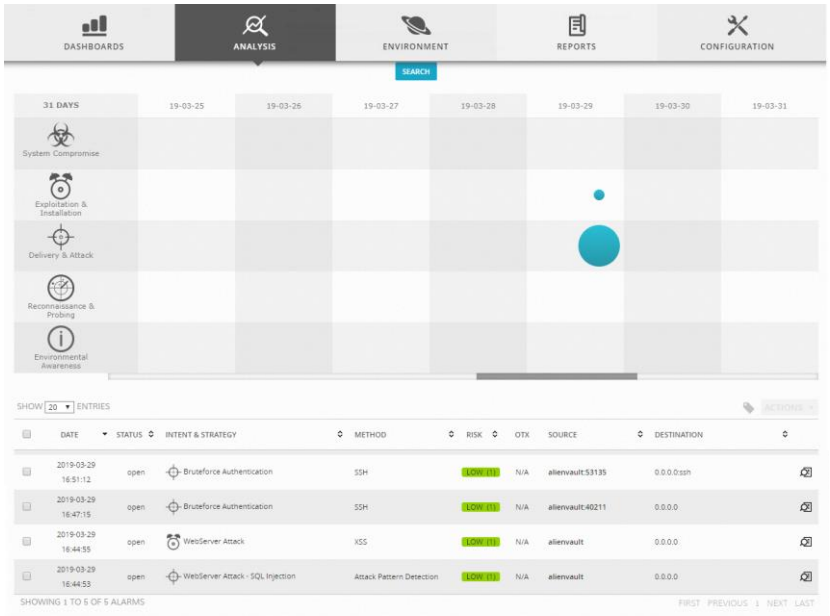
GRÁFICO DE RESUMEN DE ALARMAS

La sección superior de la página incluye un gráfico de burbujas que ofrece una representación gráfica de las alarmas por intención. Los círculos azules indican el número de veces que se mostró una alarma en una intent. Un círculo más grande indica un mayor número de alarmas. Puede pasar el ratón por encima de cada uno de los círculos para obtener el número real de los distintos tipos de intent. Además, si haces clic en cualquiera de los círculos azules, USM Anywhere muestra sólo las alarmas correspondientes a ese círculo. Puedes cambiar el periodo de tiempo mostrado haciendo clic en Creado durante el filtro. Las

alarmas graficadas por intención se clasifican en cinco categorías diferentes, que están representadas por los iconos gráficos de la pantalla

- Entrega y ataque
- Conocimiento del entorno
- Explotación e instalación
- Reconocimiento y sondeo
- Compromiso del sistema

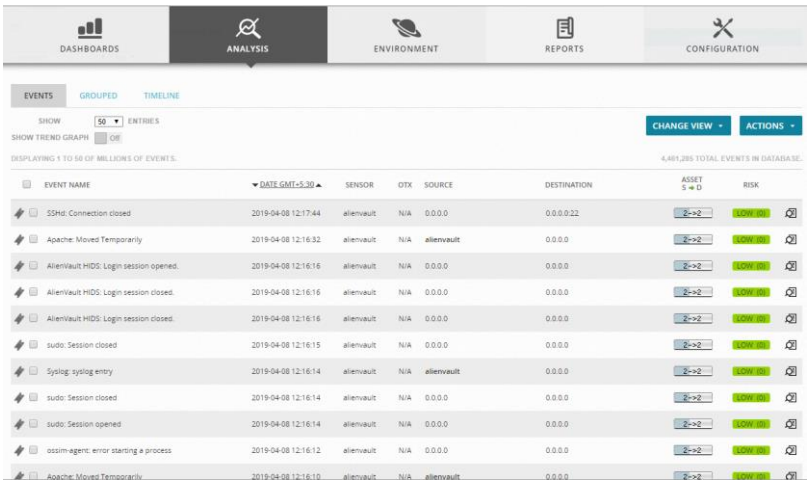
Si desea analizar los datos y ver las columnas adicionales sin tener que desplazarse a izquierda y derecha, puede maximizar la pantalla y ocultar el panel de filtrado. Haga clic en el icono para ocultar el panel de filtrado. Haga clic en el icono para ampliar el panel de filtrado.



SIEM - GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD

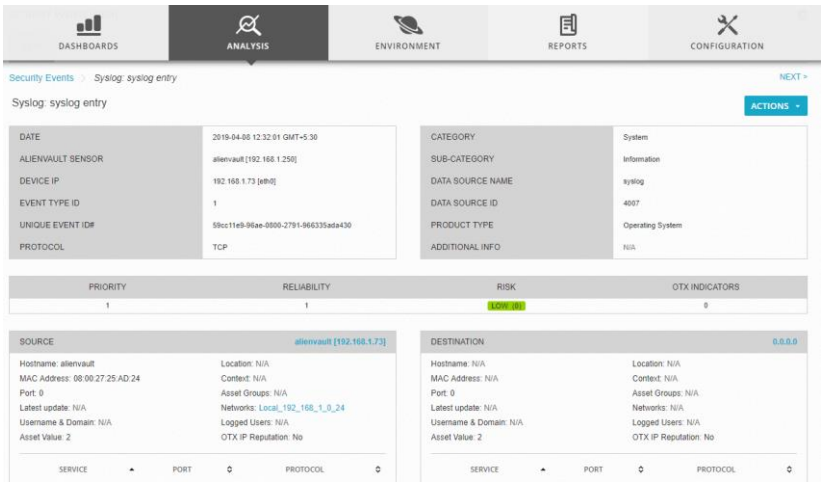
EVENTO DE SEGURIDAD

En alien vault OSSIM, SIEM se realiza a través de un evento de Seguridad. Esa pestaña muestra todos los eventos como informes y podemos obtener informes en nuestra propia vista personalizada. El evento de Seguridad también muestra eventos en tiempo real. Para obtenerlo vaya a Análisis > SIEM



Seleccione Cambiar vista para filtrar las columnas del informe.

Para ver un evento en particular, haga clic en SIEM > Eventos y haga doble clic en el evento para ver todos los detalles.

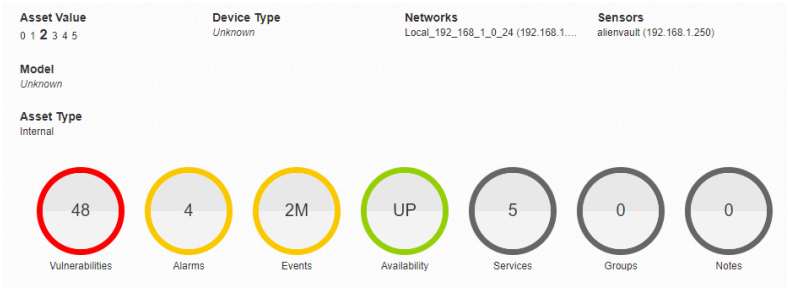


La pestaña En tiempo real contiene la lista de eventos en tiempo real. Muestra los eventos ocurridos en la red en ese momento. Cada 10 segundos, refresca la red y obtiene detalles de registro de todos los activos, luego filtra y muestra los eventos.

ACTIVOS Y GRUPOS

Desde la configuración de nuestro adaptador de red, OSSIM escanea todas las IP y muestra las máquinas y dispositivos asignados como activos. Si despliega el agente HIDS - OSSEC en los activos, se convertirá en el agente de OSSIM (no podemos añadir dispositivos de red como agente).

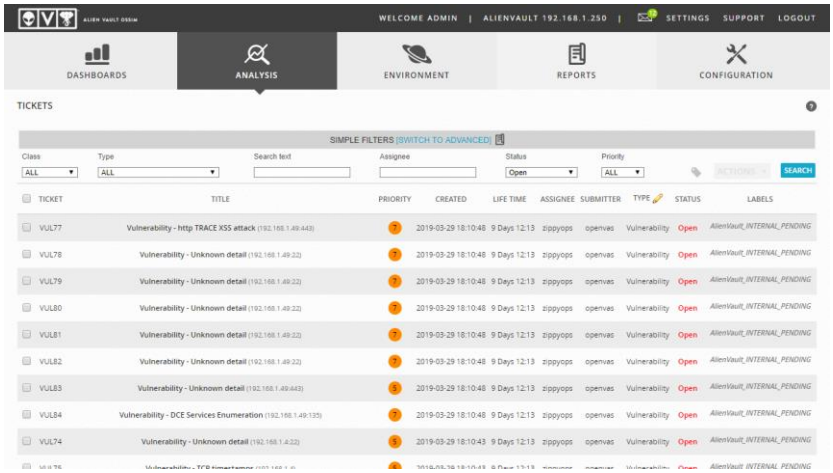
Si hace clic en un activo concreto, se mostrarán los detalles del activo, como eventos, vulnerabilidades, alarmas y servicios.



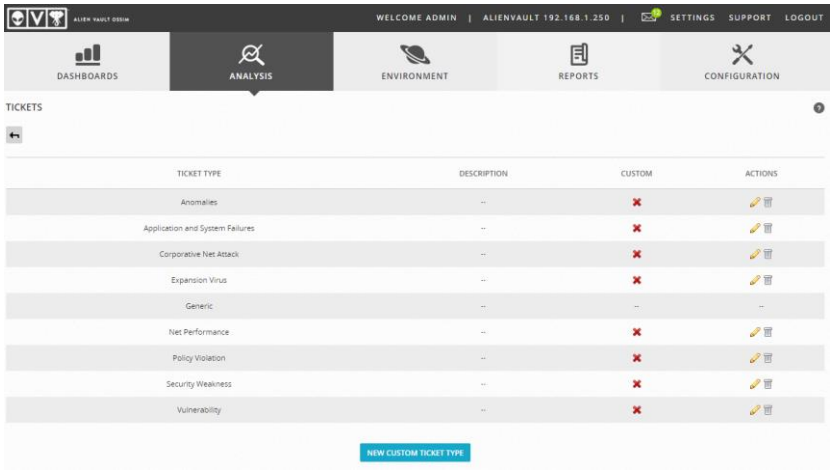
TICKETS

GENERACIÓN DE TICKETS

Normalmente OSSIM genera automáticamente tickets para 8 actividades principales del sistema como ataques y SIEM Para ver esto vaya a DashBoard > OverView > Tickets > Ticket Status ahora puede ver el estado de los tickets en un gráfico circular, haga clic en él para ver los tickets abiertos y se mostrará una lista de tickets como,



Si necesita configurar un ticket personalizado, haga clic en Nuevo tipo de ticket personalizado.

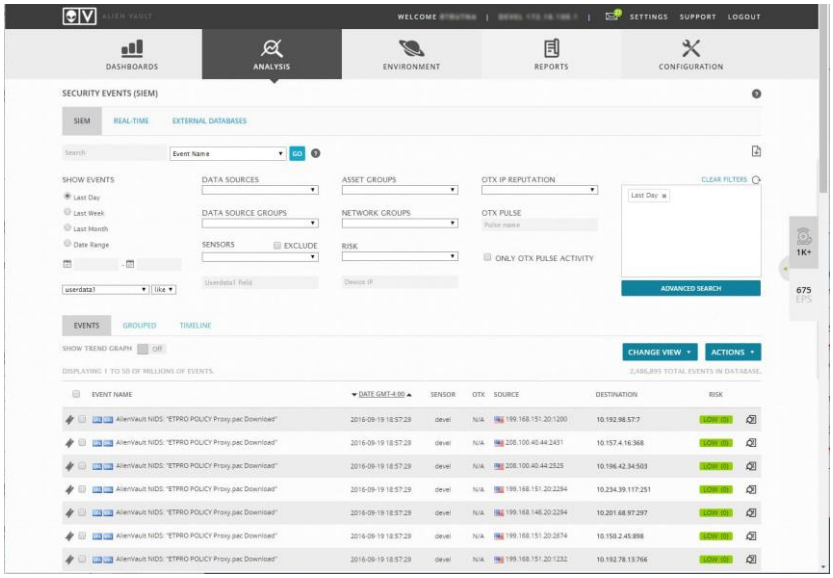


DASHBOARDS

Al iniciar por primera vez la interfaz de usuario web de USM Appliance, se muestra la página principal de paneles.

Esta vista de alto nivel de información resumida muestra el estado general de su red, de modo que puede obtener una indicación inmediata de los niveles de eventos y alarmas que se producen en su entorno.

Confirme que los eventos de seguridad se están recopilando y rellenando correctamente la base de datos de USM Appliance. Para ver los eventos en la base de datos, vaya a la vista Análisis > Eventos de seguridad (SIEM).



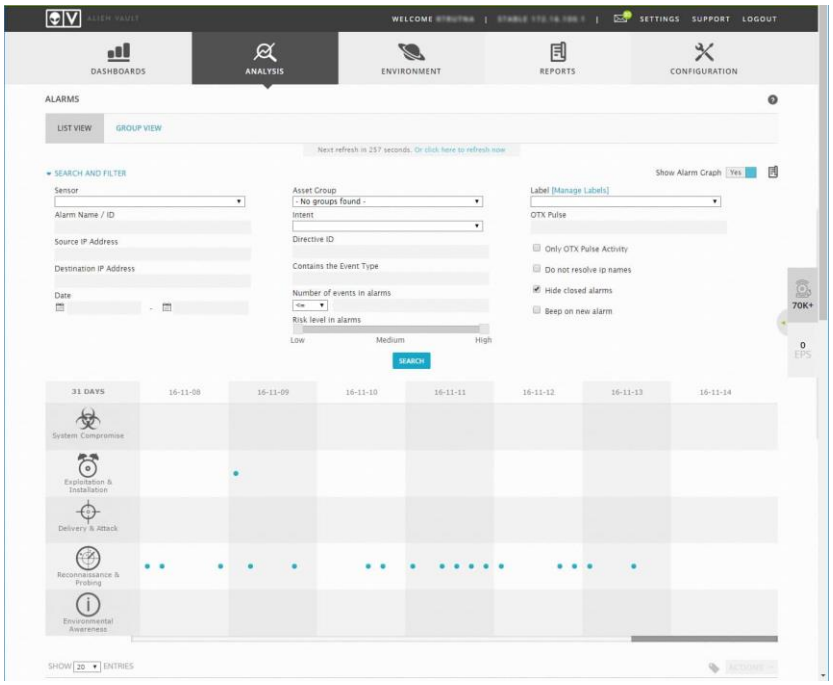
EVENTOS DE SEGURIDAD (SIEM)

En esta pantalla, cualquier evento de registro normalizado, o cualquier otro evento recibido o generado por cualquier sensor de USM Appliance a nivel de aplicación, sistema o red, aparece en la parte inferior de la pantalla, a menos que una política de USM Appliance lo haya filtrado. En la parte superior de la pantalla, se pueden buscar y filtrar eventos específicos mediante intervalos de tiempo y otros criterios de búsqueda. En la lista tabular de eventos, que se muestra en la parte inferior de la pantalla, puede hacer clic en una fila de evento específica para mostrar información adicional sobre el evento seleccionado, en

una ventana emergente. Puede ver y examinar todos los detalles de un evento, en una ventana completa del navegador, haciendo clic en el icono de la última columna de la fila del evento.

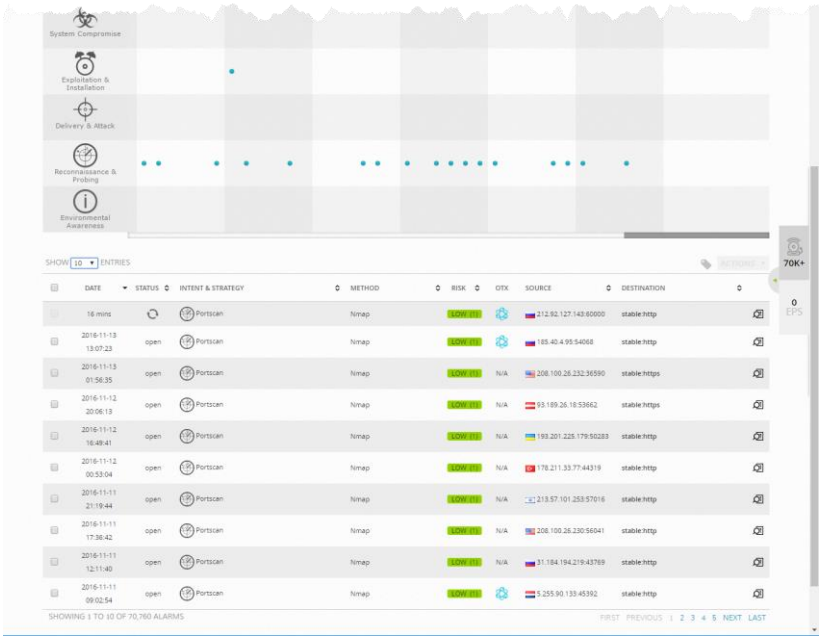
Confirme que USM Appliance está creando alarmas y que éstas se muestran correctamente. El servidor de USM Appliance utiliza una fórmula basada en el valor del activo, la prioridad del evento y la fiabilidad del evento para calcular el riesgo de un evento individual. Cualquier evento con un riesgo de 1 o superior generará una alarma. (Consulte Conceptos y terminología de seguridad de red de USM Appliance para obtener una descripción de cómo se calcula el riesgo de los eventos).

Para ver las alarmas de su sistema, vaya a Análisis > Alarmas.



Por defecto, la parte central de la pantalla proporciona una representación gráfica de las alarmas actuales que se están generando en su entorno. Los círculos azules indican el número de alarmas de una categoría que están apareciendo en un momento determinado. Un círculo más grande indica un mayor número de alarmas. Las alarmas se priorizan por categorías que reflejan los métodos típicos utilizados por los atacantes. (Consulte Gestión de alarmas para obtener más información sobre la categorización de alarmas).

La parte inferior de la ventana muestra una lista tabular de alarmas.



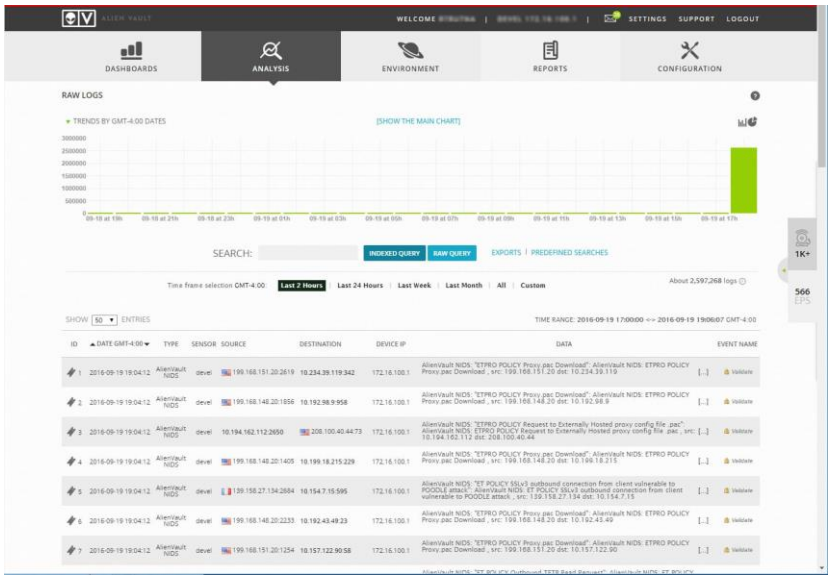
Al hacer clic en una fila de alarma, se muestran todos los detalles sobre la alarma, como los eventos que la activaron, las direcciones IP de origen y destino, y las vulnerabilidades asociadas a la alarma.

En la parte superior de la pantalla, puede buscar y filtrar las alarmas que se muestran en esta página. Por ejemplo, puede elegir que sólo se muestren las alarmas originadas por un sensor concreto, que tengan un determinado nivel de riesgo o que sólo afecten a determinados grupos de activos.

Confirme que la información de registro sin procesar (normalizada) se está almacenando en el USM Appliance Logger.

El USM Appliance Logger proporciona un repositorio de archivo basado en ficheros que está especialmente diseñado para almacenar información de registro de seguridad para su archivo y recuperación a largo plazo. Cada hora, los archivos de registro se indexan, comprimen y firman digitalmente para garantizar su integridad. Puede comprobar si el componente USM Appliance Logger está recibiendo eventos de registro sin procesar de los dispositivos de red visualizando los datos en la pantalla Registros sin procesar.

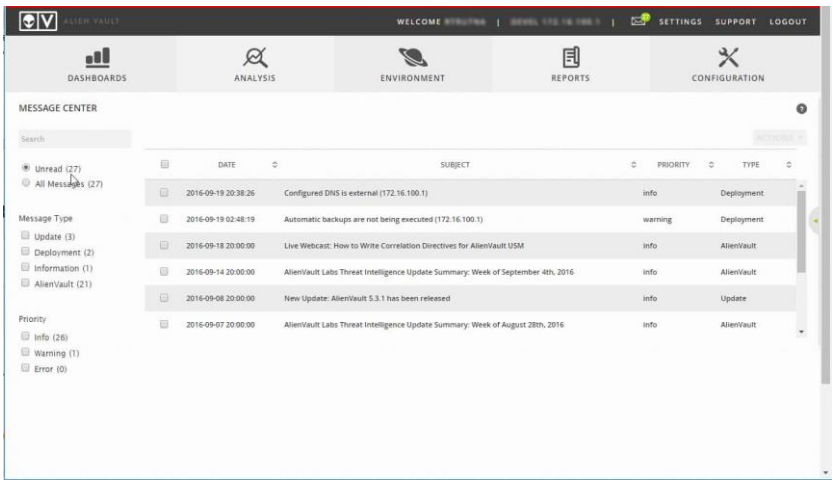
Para ver los registros, vaya a Análisis > Registros sin procesar.



La parte superior de la ventana muestra un gráfico en el que puede ver las tendencias de los registros en el intervalo de tiempo que haya establecido.

Los registros se muestran en la parte inferior de la ventana. Puede ver los detalles de cada registro haciendo clic en el elemento correspondiente de la lista. También puede utilizar el cuadro de búsqueda para buscar entradas de registro específicas, por ejemplo, podría buscar el nombre o la ubicación de un archivo de registro, o las direcciones IP de origen o destino implicadas en un evento registrado. También puede seleccionar un intervalo de tiempo para mostrar las entradas de registro sólo para el intervalo de tiempo seleccionado.

Haga clic en el icono Centro de mensajes para observar cualquier información del sistema, error o mensaje de advertencia en el Centro de mensajes para determinar si hay algún problema pendiente notificado por el servidor de USM Appliance. La pantalla también informa de cualquier problema que se haya producido con los componentes del sistema de USM Appliance o con las operaciones de recopilación de registros.



En el Centro de mensajes se pueden recibir mensajes sobre posibles problemas con el funcionamiento del Servidor de USM Appliance u otros componentes. El Centro de mensajes también proporciona información sobre las actualizaciones disponibles del sistema. La interfaz de usuario web de USM Appliance muestra una lista de mensajes relacionados con cualquier problema potencial que detecte, además de otros mensajes informativos y de actualización del sistema.

ESTABLECIMIENTO DEL COMPORTAMIENTO BÁSICO DE LA RED

Cuando empieces a utilizar USM Appliance por primera vez, es una buena idea dejarlo funcionar durante unos días para determinar qué eventos y alarmas puedes considerar "ruido" y cuáles debes investigar más a fondo. Por ruido, nos referimos a falsos positivos que ocultan los verdaderos positivos, o a eventos que pueden indicar un comportamiento realmente malicioso.

Dado que ningún sistema es perfecto, debe asegurarse de tener alarmas procesables e informes útiles, no cientos de cosas que revisar. Lo que aprenda de la recopilación de líneas de base y de la evaluación de esos eventos le ayudará a crear políticas que indiquen a USM Appliance lo que es importante, o no.

LÍNEA DE BASE

Para poder ajustar el sistema, es necesario crear una línea de base de lo que constituye un comportamiento normal en la red. Esto se denomina baselining. Las alarmas y eventos generados durante este periodo inicial representan el comportamiento normal actual, en otras palabras, una instantánea en el tiempo. Por supuesto, puede haber cosas que quiera filtrar de inmediato. Pero, en general, debe resistir la tentación y esperar hasta que haya tenido la oportunidad de observar cualquier patrón en su red.

EVALUACIÓN DE LOS RESULTADOS

Después de recopilar estos puntos de datos, hay que empezar a tomar decisiones sobre ellos, basándose en los siguientes criterios:

¿Qué eventos tienen valor y aplicabilidad para mi sistema?

¿Qué eventos tienen que ver con la política de la red y, por tanto, no son amenazas potenciales?

¿Se ha evaluado correctamente el riesgo?

¿Qué sucesos tienen valor para la notificación?

¿Quién debe recibir una notificación cuando se produce este evento?

Para responder a estas preguntas por primera vez, lo mejor es hacerlo en grupo con las partes interesadas. En iteraciones posteriores de este proceso, normalmente sólo participan los analistas, porque las preguntas fundamentales para cada evento pueden aplicarse mediante taxonomía. Dado que AlienVault lanza nuevas firmas con frecuencia, este proceso de decisión debe repetirse a intervalos regulares.

FILTRAR EL RUIDO

Algunos falsos positivos deben ser identificados y filtrados inmediatamente. Un ejemplo podría ser una alarma que indique el escaneo de hosts en la red. Dicha actividad puede ser completamente legítima si la realiza un mapeado de red interno. Por otro lado, puede ser actualmente benigna, pero también puede ser precursora de un ataque real. USM Appliance trata ambos eventos por igual.

Si examina una alarma y determina que el evento que la activó era ruido y no una amenaza real, considere tomar las siguientes medidas:

Cree una política que impida que USM Appliance procese nuevos eventos del origen. Por ejemplo, supongamos que USM Appliance ha detectado correctamente un escaneado de vulnerabilidades procedente de un escáner interno, pero esos eventos no le interesan.

Si no está interesado en alarmas específicas, puede hacer lo siguiente:

- Reconfigure la fuente de datos externa para que no envíe tales eventos.
- Utilice una política para descartar dichos eventos.
- Desactivar la regla de correlación.
- Eliminar todas las apariciones de la alarma de SIEM.
- Creación de nuevas políticas

También puede crear una política para reducir el número de falsos positivos. Por ejemplo, puede crear una directiva para que USM Appliance deje de procesar eventos del host específico que es el origen de los falsos positivos.

Supongamos que USM Appliance ha detectado correctamente un escáner de vulnerabilidades procedente de un escáner de vulnerabilidades dentro de su sistema. Si no le interesan estos eventos, porque su entorno controla el escáner de vulnerabilidades, puede crear una política que excluya los eventos procedentes de él, para que el servidor de USM Appliance no los procese.

Después de realizar una de estas tareas, o ambas, debe eliminar todas las apariciones de la alarma de USM Appliance. Para obtener información sobre cómo hacerlo, consulte Revisión de alarmas como grupo.

Para obtener más información sobre el ajuste de las reglas de correlación y la gestión de políticas, consulte Reglas de correlación y gestión de políticas.

AJUSTE DE LAS REGLAS DE CORRELACIÓN

Ajuste sus reglas de correlación, si es necesario, para ajustar la prioridad o la fiabilidad, o ambas, para cambiar el nivel de riesgo. Si el riesgo tiene un valor inferior a 1, USM Appliance no genera una alarma.

Un ejemplo en el que podría hacer esto sería una regla de correlación que detecte la mensajería instantánea. Si la política de seguridad de su empresa permite la mensajería instantánea, no es necesario que reciba advertencias sobre este tipo de eventos.

Si la alarma ha sido un falso positivo, es decir, se ha disparado por un tráfico que no debería haberlo hecho, deberá personalizar la regla de correlación que ha disparado la alarma. Una vez personalizada la regla, etiquete la alarma existente como falso positivo y ciérrela. (Para obtener más información, consulte Revisión de alarmas como grupo).

RESPUESTA A INCIDENTES

Las organizaciones se ven bombardeadas cada día con amenazas potenciales. No es probable que la mayoría de los sucesos o incidentes que suponen amenazas causen daños en su entorno, pero aun así es necesario investigarlos. Para investigar y responder rápida y eficazmente a las amenazas, necesita un plan. Un plan de respuesta a incidentes define su respuesta, no sólo para abordar eficazmente incidentes concretos e individuales, sino también para examinar secuencias de sucesos y determinar si pueden coincidir con los pasos que podría dar un atacante para poner en peligro la seguridad de su entorno.

El objetivo último de un plan de respuesta a incidentes no es sólo abordar con eficacia incidentes concretos y aislados, sino también identificar posibles amenazas originadas por una secuencia de sucesos o incidentes que podrían utilizarse para llevar a cabo un ataque más amplio. Es importante disponer de un plan completo con procedimientos y procesos para hacer frente a diferentes situaciones, ya que, incluso si se acepta que nada saldrá exactamente según lo previsto, proporcionará una valiosa lista de comprobación y referencia para todo lo que hay que hacer. Esto puede ser muy valioso, sobre todo en momentos de crisis muy estresantes.

¿QUÉ DEFINE UN INCIDENTE?

Un incidente es un suceso imprevisto que requiere una cierta inversión de tiempo y recursos para rectificarlo. Con el tiempo, usted desarrollará su propio sistema interno de clasificación de incidentes, pero ésta es la medida con la que la mayoría de las organizaciones deberían empezar.

Los incidentes en el mundo de la seguridad normalmente implican que una parte hostil externa (aunque a veces interna) tiene acceso no autorizado o control de los sistemas que soportan los procesos centrales de tu organización. Muchas organizaciones pueden verse comprometidas durante mucho tiempo antes de que se descubra. Por regla general, la mayoría de las organizaciones declaran que algo es un incidente en el momento en que hay que recurrir a analistas de seguridad externos para remediar la situación.

¿QUÉ ES UNA VIOLACIÓN?

En términos legales, las violaciones representan una pérdida significativa de datos a una parte externa no autorizada, y pueden requerir la divulgación pública de la pérdida de acuerdo con la ley. Una red puede ser atacada miles de veces sin preocupación, verse comprometida (y recuperarse de ello) muchas veces a lo largo del año, pero seguir haciendo negocios ininterrumpidamente, siempre que no se produzca una brecha.

QUÉ INCLUIR EN SU PLAN DE REPARACIÓN DE INCIDENTES

Una de las grandes ventajas de la supervisión de la seguridad es que no sólo detecta cuándo han fallado los controles de seguridad, sino cómo han fallado, y luego vuelca esa información en la mejora de la seguridad general.

Cuando un host se ve comprometido por medio de un sitio web malicioso, limpiar el host infectado es sólo una parte de la respuesta. Por otro lado, bloquear el sitio web malicioso para evitar nuevas infecciones demuestra el verdadero valor de la supervisión de la seguridad.

La supervisión de la seguridad sin este tipo de análisis de la causa raíz sólo trata los síntomas, no la enfermedad. Por esta razón, asegúrese de que, al planificar los resultados de su plan de respuesta a incidentes, no sólo hace hincapié en reparar los sistemas comprometidos, sino también en recopilar información para remediar los problemas que causaron el compromiso y evitar que vuelvan a ocurrir.

DESARROLLO DE UNA ESTRATEGIA DE TRIAJE EFICAZ

El término triaje se utiliza más comúnmente en la comunidad médica, donde significa salvar vidas ayudando al personal médico de emergencia a evaluar rápidamente la gravedad de una herida o enfermedad, y establecer los protocolos adecuados, en el orden correcto para reducir el trauma y mantener la salud y recuperación del paciente. Sin embargo, estos mismos principios pueden aplicarse también al análisis de seguridad. Algunas pautas que le ayudarán a perfeccionar su capacidad de triaje de los tipos de incidentes de seguridad de la información podrían ser las siguientes:

Cómo identificar los distintos tipos de incidentes de seguridad, comprendiendo cómo se desarrollan los ataques.

Cómo priorizar los esfuerzos de reparación, por ejemplo, para identificar qué incidentes investigar primero según qué amenazas potenciales podrían causar el mayor daño a su empresa.

Cómo responder eficazmente en situaciones de crisis.

Estas son sólo algunas ideas a tener en cuenta a la hora de definir los esfuerzos de triaje dentro de su planificación de respuesta a incidentes. Probablemente querrá considerar más prácticas de triaje y respuesta a incidentes basadas en su entorno específico, y sus requisitos específicos de cumplimiento y seguridad de la red.

¿CÓMO DESCUBRO UN ATAQUE POSIBLEMENTE MAYOR EN CURSO?

La mayor parte del trabajo diario de supervisión de la seguridad consiste en detectar dónde han fallado los controles de seguridad y un sistema se ha visto comprometido por malware o exploits. Sin embargo, siempre existirán situaciones que requieran más investigación, con razones para creer que un host comprometido puede haber sido usado para comprometer otros, o una secuencia más compleja de eventos específicos puede ser usada para llevar a cabo un ataque o exploit, comúnmente referido como un vector de ataque.

INDICADORES DE COMPROMISO (IOC)

Los indicadores de compromiso, o IoCs, representan piezas de información sobre un vector de ataque. Un IoC puede utilizarse para observar una relación con otros ataques. De hecho, si ve un IoC responsable de varias infecciones de malware que reciben instrucciones del mismo host remoto en Internet, debería rastrearlo. Esto le permitirá desactivar muchas infecciones al mismo tiempo bloqueando ese servidor.

VECTORES DE ATAQUE COMUNES Y ESTRATEGIAS PARA COMBATIRLOS

La mejor manera de determinar la respuesta adecuada ante incidentes en cualquier situación dada es comprender a qué tipos de ataques puede enfrentarse su organización de forma más lógica.

El Instituto Nacional de Estándares y Tecnología

(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) publica la siguiente lista de vectores de ataque comunes:

- Medios externos/extraíbles: Un ataque ejecutado desde un medio extraíble (por ejemplo, una unidad flash, un CD) o un dispositivo periférico.
- Desgaste: Ataque que emplea métodos de fuerza bruta para comprometer, degradar o destruir sistemas, redes o servicios.
- Web: Ataque ejecutado desde un sitio web o una aplicación basada en web (por ejemplo, drive-by download).
- Correo electrónico: Ataque ejecutado a través de un mensaje de correo electrónico o un archivo adjunto (por ejemplo, infección por malware).
- Uso indebido: Cualquier incidente resultante de la violación por parte de un usuario autorizado de las políticas de uso aceptable establecidas por una organización, excluyendo las categorías anteriores.
- Pérdida o robo de equipos: Pérdida o robo de un dispositivo o soporte informático utilizado por la organización, como un ordenador portátil o un teléfono inteligente. Identifique qué equipos supondrían el mayor riesgo para la empresa en caso de pérdida o robo. En la mayoría de las empresas, se incluiría el portátil perteneciente al director financiero junto con cualquier disco duro de servidor que contenga IP u otros datos sensibles.
- Otros: Un ataque que no encaja en ninguna de las otras categorías.

Revise la lista anterior para asegurarse de que dispone de políticas y controles de seguridad para mitigar la mayoría de los riesgos de estos vectores de ataque. Además, utilice esta lista para guiar a su equipo a la hora de determinar cómo clasificar los distintos tipos de incidentes de seguridad.

TAXONOMÍA DE ALERTAS

Una taxonomía de alertas puede ayudarle a ordenar las alertas relacionadas en una imagen de un ataque mayor en curso, ya que el atacante hace lo siguiente:

- Realiza un reconocimiento.
- Lleva el ataque a muchos sistemas.
- Explota con éxito algunos de ellos.
- Utiliza el sistema comprometido como base desde la que atacar a otros.

ENTRAR EN LA MENTE DEL ATACANTE A TRAVÉS DE LA CATEGORIZACIÓN DE EVENTOS DE SEGURIDAD

La seguridad de la información tradicional asume falsamente que usted sabe qué camino tomará un atacante a través de su red. Por ejemplo, los atacantes rara vez entran por la puerta principal o, en este contexto, por el cortafuegos de la puerta de enlace. Por otro lado, cada ataque suele seguir un patrón determinado, o lo que Lockheed Martin denomina Cyber Kill Chain®.

La Cyber Kill Chain es una secuencia de etapas necesarias para que un atacante consiga infiltrarse en una red y extraer datos de ella. Cada etapa demuestra un objetivo específico a lo largo del camino del atacante. Diseñar su plan de vigilancia y respuesta en torno al modelo Cyber Kill Chain es un método eficaz, porque se centra en cómo se producen los ataques reales.

Cyber Kill Chain model	
Intención	**Objetivo del atacante**
Reconocimiento y sondeo	• Encontrar el objetivo. • Desarrollar un plan de ataque basado en las oportunidades de explotación.
Entrega y ataque	• Poner en línea el mecanismo de entrega. • Utilizar la ingeniería social para conseguir que el objetivo acceda al malware o a otro exploit.
Explotación e instalación	• Aprovechar las vulnerabilidades de los sistemas objetivo para obtener acceso. • Elevar los privilegios del usuario e instalar la carga útil de persistencia.

Cyber Kill Chain model	
Intención	**Objetivo del atacante**
Compromiso del sistema	• Filtrar datos de gran valor de la forma más silenciosa y rápida posible. • Utilizar el sistema comprometido para obtener acceso adicional, "robar" recursos informáticos y/o utilizarlo en un ataque contra otra persona.

A la hora de elaborar un plan de respuesta a incidentes, puede resultarle útil establecer un orden de prioridad entre los incidentes o alarmas de seguridad.

Ejemplo de hoja de cálculo de respuesta a incidentes:

Tipo de incidente	Etapa de la cadena de muerte	Nivel de prioridad	Acción recomendada
Escaneo de puertos	Reconocimiento y sondeo	Bajo	Puede ignorar estos a menos que AlienVault OTX IP Reputation le de al IP responsable un mal puntaje. OTX IP Reputation almacena informes sobre cualquier actividad IP sospechosa, que puede o no ser maliciosa.
Infección de malware	Entrega y ataque	Bajo-Medio	Remedie las infecciones de malware lo antes posible antes de que progresen. Analice el resto del sistema en busca de IoC relacionados, por ejemplo, hashes MD5.
Denegación de servicio distribuida	Explotación e instalación	Alta	Configure los servidores web para protegerlos contra las peticiones HTTP y SYN flood. Coordine con su proveedor de servicios de Internet (ISP) durante un ataque para bloquear las IP responsables.
Acceso no autorizado	Explotación e instalación	Medio	Detectar, supervisar e investigar los intentos de acceso no autorizado, dando prioridad a los que son de misión crítica y/o contienen datos sensibles.
Violación de información privilegiada	Compromiso del sistema	Alto	Identifique las cuentas de usuario privilegiadas de todos los dominios, servidores, aplicaciones y dispositivos críticos. Asegúrese de que ha activado la supervisión de todos los sistemas y de todos los eventos del sistema.

Tipo de incidente	Etapa de la cadena de muerte	Nivel de prioridad	Acción recomendada
			Compruebe que su infraestructura de registro en bruto de USM Appliance está registrando activamente todos los eventos.
Escalada de privilegios no autorizada	Explotación e instalación	Alta	Mediante sus directivas de correlación integradas, USM Appliance registra automáticamente todos los eventos de escalada de privilegios y envía alarmas en caso de intentos no autorizados. En función de las necesidades, también puede mejorar su entorno de USM Appliance añadiendo directivas de correlación personalizadas.
Ataque destructivo a sistemas y datos.	Puesta en peligro del sistema	Alta	Realice copias de seguridad de todos los datos y sistemas críticos; pruebe, documente y actualice los procedimientos de recuperación del sistema. Durante un ataque al sistema, capture cuidadosamente las pruebas. Documente todos los pasos de recuperación y todos los datos probatorios.
Amenaza persistente avanzada (APT) o ataque en varias fases	Representa todas las fases, desde el reconocimiento hasta el compromiso del sistema	Alta	Cualquiera de los sucesos individuales ilustrados podría representar parte de una APT, el tipo más peligroso de amenaza a la seguridad. Por esta razón, considere cada evento como parte de un contexto más amplio, incorporando la inteligencia sobre amenazas más reciente. Las directivas de correlación de USM Appliance suelen tener en cuenta cuántos eventos de una naturaleza específica se han producido antes de generar una alarma, aumentando así su fiabilidad. Los pulsos OTX, por otro lado, sólo requieren un evento para hacerlo.
Falsas alarmas	Representa todas las etapas	Bajo	Gran parte del trabajo de quien responde a un incidente consiste en eliminar la información irrelevante y eliminar los falsos positivos. Este proceso es continuo. Para obtener más información, consulte Establecimiento del comportamiento base de la red y también Gestión de políticas.
Otras	Todas las etapas	Alta	La respuesta a incidentes nunca se detiene y constituye una fuente de mejora continua. Con el tiempo, a medida que los incidentes se convierten en alarmas, se adquieren conocimientos que ayudan a

Tipo de incidente	Etapa de la cadena de muerte	Nivel de prioridad	Acción recomendada
			descubrir nuevas formas de clasificar los incidentes y evitar que se conviertan en alarmas.

ACERCA DE LAS ALARMAS DE ESCANEO DE PUERTOS

Puede estar seguro de que los atacantes no están obteniendo información útil de sus escaneos. Sin embargo, si los escaneos de sus sistemas externos parecen ser detallados y exhaustivos, puede asumir razonablemente que tienen la intención de seguir el reconocimiento con intentos de ataque más adelante.

Si el escaneado se origina en las redes de una organización legítima, lo mejor es ponerse en contacto con su equipo de seguridad, si lo tienen, o con el personal de gestión de la red.

Si no hay detalles de contacto aparentes, busca detalles sobre el dominio en WHOIS, cuyo enlace está disponible al final de la lista de Eventos de Seguridad de USM Appliance y también en las páginas web OTX aplicables para tales IoCs.