



TECNOLÓGICO UNIVERSITARIO
RUMIÑAHUI
CES RPC - SO - 12 - Nro. 225-2020

INSTITUTO TECNOLÓGICO UNIVERSITARIO
“RUMIÑAHUI”
CARRERA DE REDES Y SEGURIDAD INFORMÁTICA.

**ANEXO 1 DEL PROYECTO DE TITULACIÓN: ANÁLISIS,
DISEÑO E IMPLEMENTACION DE UN SISTEMA SIEM**

AUTORES:
JAIME GRIJALVA GARCIA
DANILO SALAS JACOME
CESAR ALCOCER CEVALLOS

TUTOR:
ING. CAJAMARCA MÉNDEZ GERARDO IVÁN

Sangolquí, julio 2024

ANEXO 1 DEL PROYECTO DE TITULACIÓN: ANÁLISIS, DISEÑO E IMPLEMENTACION DE UN SISTEMA SIEM	1
1. Objetivos	3
2. Alcance	3
3. Justificación	4
4. Responsabilidad y Autoridades	4
5. Marco Jurídico	5
5.1 Cumplimiento Normativo:.....	5
5.2 Protección y privacidad de datos:	5
5.3 Gestión de riesgos:	5
6. Glosario	5
7. Análisis.	6
7.1 Análisis del Sistema Operativo SIEM	6
8 Diseño.	0
8.1 Levantamiento en Sitio	0
8.2 Arquitectura de Red.....	1
8.3 Infraestructura de Red.....	2
8.4 Equipos Tecnológicos.....	3
9 Implementación	6
9.1 Implementación de Alíen Valut OSSIM	6
9.2 Gestión de activos	23
9.3 Gestión de disponibilidad.....	31
9.4 Gestión de vulnerabilidades.....	41
9.4 Gestión de riesgo.....	49
9.5 Gestión de alarmas y eventos	54
9.6 Administración de tickets.....	57
9.7 Flujo de red.....	62
10 Bibliografía.....	65

CARTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

CT-ANX-2024-ISTER-6-6.1

Sangolquí, 21 de mayo de 2025

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

**INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE
UNIVERSITARIO**

Presente

Por medio de la presente, yo, CESAR MARCELO ALCOCER CEVALLOS declaro y acepto en forma expresa lo siguiente: Ser autor del trabajo de titulación denominado ANALISIS, DISEÑO Y IMPLEMENTACION DE UN SISTEMA SIEM, de la Tecnicatura Superior REDES Y SEGURIDAD INFORMATICA; y a su vez manifiesto mi voluntad de ceder al Instituto Superior Tecnológico Rumiñahui con condición de Universitario, los derechos de reproducción, distribución y publicación de dicho trabajo de titulación, en cualquier formato y medio, con fines académicos y de investigación.

Esta cesión se otorga de manera no exclusiva y por un periodo indeterminado. Sin embargo, conservo los derechos morales sobre mi obra.

En fe de lo cual, firmo la presente.

Atentamente,



Cesar Marcelo Alcocer Cevallos
C.I.: 172118618-5

FORMULARIO PARA ENTREGA DE PROYECTOS EN BIBLIOTECA INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO

CT-ANX-2024-ISTER-1

CARRERA:

TECNICATURA SUPERIOR REDES Y SEGURIDAD INFORMATICA

AUTOR /ES:

ALCOCER CEVALLOS CESAR MARCELO

TUTOR (METODOLÓGICO Y ACADÉMICO):

ING. CAJAMARCA MÉNDEZ GERARDO IVÁN

CONTACTO ESTUDIANTE:

0979183337

CORREO ELECTRÓNICO:

cescev@gmail.com

TEMA:

ANÁLISIS, DISEÑO Y IMPLEMENTACION DE UN SISTEMA SIEM

OPCIÓN DE TITULACIÓN:

PROYECTO TECNICO

RESUMEN EN ESPAÑOL:

EL ANÁLISIS DISEÑO E IMPLEMENTACION DE UN SISTEMA “SIEM” SE ENFOCA EN EL MONITOREO EN TIEMPO REAL LAS VULNERABILIDADES QUE PUEDA TENER LA RED TECNOLÓGICA EN DONDE SE IMPLEMENTARA EL “SIEM” CORRELACIONANDO DIFERENTES HERRAMIENTAS DE MONITOREO DE RED EN UNA SOLA PARA OBTENER LA MAYOR INFORMACION DE POSIBLE EVENTOS, VULNERABILIDADES EN TIEMPO REAL Y TOMAR MEJORES ACCIONES QUE MITIGUEN EL RIESGO TECNOLÓGICO.

PALABRAS CLAVE:

MONITOREO, TIEMPO REAL, EVENTOS, SEGURIDAD

ABSTRACT:

PALABRAS CLAVE:

SIEM, AlienVault, OSSIM

SOLICITUD DE PUBLICACIÓN DEL TRABAJO DE TITULACIÓN

CT-ANX-2024-ISTER-2
Sangolquí, 21 de mayo del 2025

Sres.-

**INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE
UNIVERSITARIO**

Presente

A través del presente me permito aceptar la publicación del trabajo de titulación de la Unidad de Integración Curricular en el repositorio digital “DsPace” del estudiante: CESAR MARCELO ALCOCER CEVALLOS, con C.I.: 172118618-5 alumno de la Carrera de TECNICATURA SUPERIOR REDES Y SEGURIDAD INFORMATICA

Atentamente,



Firma del Estudiante
Nombre del Estudiante
C.I.: 172118618-5

SÓLO PARA USO DEL ISTER

Han sido revisadas las similitudes del trabajo en el software “TURNITING” y cuenta con un porcentaje de; motivo por el cual, el Proyecto Técnico de Titulación es publicable. (EL PORCENTAJE DE SIMILITUD DEBE SER MÁXIMO DE 15%)

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

Fecha del Informe ____ / ____ / ____

MATRIZ SANGOLQUÍ: Av. Atahualpa 1701 y 8 de Febrero

Telf: 0960052734 / 023524576 / 022331628

 **www.ister.edu.ec / info@ister.edu.ec**

1. Objetivos

El objetivo de la implementación de un sistema SIEM en el área del laboratorio de redes y seguridad informática es proporcionar un entorno seguro y controlado para que los estudiantes puedan aprender y aplicar conceptos críticos de seguridad informática en un contexto práctico. Esto permitirá a los estudiantes experimentar y resolver problemas comunes asociados con la implementación y gestión de un sistema SIEM, como la correlación de eventos y la gestión de alertas.

La implementación ofrece la oportunidad para que los estudiantes trabajen con herramientas y tecnologías utilizadas en las industrias de la seguridad informática, y les permite trabajar en entornos controlados y prácticos, para que los estudiantes apliquen sus conocimientos teóricos aprendidos en clase.

Esta implementación ayudará a los estudiantes, a enfrentar desafíos reales en el campo de la seguridad informática al proporcionar un entorno que simula las condiciones y amenazas de seguridad que encontrarán en el ámbito profesional.

2. Alcance

Este documento permitirá establecer un esquema de seguridad complementario para analizar, controlar, rastrear y monitorear eventos e incidentes de seguridad en el área del laboratorio de redes y seguridad informática, un mecanismo que contribuya a tomar medidas de prevención que garanticen la protección de los activos de información

y que disminuya los riesgos de seguridad en la infraestructura del área del laboratorio de redes.

Este sistema ayudara con la búsqueda de la optimización en la gestión de control de eventos en tiempo real, aprovechando de manera integral las funcionalidades que incluye la herramienta SIEM, haciendo favorecer acciones para la gestión de los activos, gestión del flujo de red, gestión de vulnerabilidades, gestión de eventos y monitoreo, entre otras, de tal manera que permita el desempeño y desarrollo de las actividades con normalidad en la infraestructura del área del laboratorio de redes del instituto.

3. Justificación

La implementación de un sistema SIEM, demuestra por parte del instituto el compromiso de adquirir nueva tecnología para mantener la seguridad de la información en el área de redes, esto proporcionara una formación valiosa y practica a los estudiantes, ya que esto fomentara la investigación e innovación, y elevar la reputación y credibilidad del instituto. Ya que estos elementos combinados hacen que la implementación de un SIEM sea una inversión estratégica y beneficiosa para el instituto.

4. Responsabilidad y Autoridades

- **Nivel de Gobierno**

Rector

Vicerrectora administrativa

- **Máximo órgano Superior**

Presidente(a) de consejo de regente

- **Nivel de Asesoría**

Secretario(a) general

- **Nivel Académico**

Director(a) de docencia

- **Nivel de Apoyo**

Director(a) de tecnología

5. Marco Jurídico

5.1 Cumplimiento Normativo:

El Instituto como institución de educación superior, está obligado a cumplir con las normas emitidas por el Consejo para el Aseguramiento de la Calidad en la Educación Superior (CACES) en materia de seguridad de la información. La norma prevé la implantación de (SIEM) para detectar, analizar y dar respuesta a incidentes de seguridad del área de tecnología de redes de la Institución.

Además, el instituto debe cumplir con las políticas de seguridad de la información del Ministerio de Educación, que definen los lineamientos de protección de la información para el sector educativo.

5.2 Protección y privacidad de datos:

La implementación del SIEM debe cumplir con la ley de protección de datos personales, que regula la recolección, procesamiento y protección de datos personales.

5.3 Gestión de riesgos:

Al implementar el sistema SIEM se debe tener en cuenta que es una parte integral de la seguridad de riesgos de la información y el instituto debe cumplir con el estándar ISO/IEC 27001.

Esto facilitara al Institución establecer un sistema SIEM que permita proteger de forma adecuada sus sistemas de redes y cumplir con los estándares de control y regulación del sector educativo.

6. Glosario

- SIEM: Sistema de Gestión de Eventos e Información de Seguridad (Security Information and Event Management)
- OSSIM Open-Source System Information Management
- Dirección IP: Identificación única de un equipo, que se comunica a través de las redes mediante el protocolo IP.
- Ciber amenazas: Son ataques delictivos que se llevan a cabo con el objetivo de manipular, controlar y obtener información de un sistema.
- Software: Es el conjunto de componentes lógicos, cuyo destino es realizar tareas, utilizan la lógica aplicada.
- Puerto: Es un punto de conexión físico o virtual que permite la comunicación y transferencia de datos entre dispositivos.
- Capa: Este término se refiere a una división lógica o física que divide responsabilidades y facilita la modularidad y escalabilidad de los sistemas.
- Core: Núcleo que posee un Procesador
- Router: Conmutador de Red
- Switch: Es un dispositivo importante en una red local porque proporciona conexión y comunicación eficientes entre múltiples dispositivos.
- Servidor: Es un sistema o dispositivo que proporciona servicios, recursos o datos a otros dispositivos (clientes) a través de una red.

7. Análisis.

7.1 Análisis del Sistema Operativo SIEM

En el siguiente cuadro comparativo se mostrara los aspectos de los sistemas SIEM, mediante lo cual nos basaremos en sistemas SIEM de código abierto para esta implementación, los aspectos a tener en cuenta en esta comparativa, es medir la estabilidad del sistema, sus características principales, la capacidad de integración, el

soporte y mantenimiento del sistema, con cuales sistemas operativos es compatible el sistema, el rendimiento que tendrá el sistema, el manejo del sistema, al igual que el método de implementación en las cuales puede ser instalado el sistema SIEM.

Haga clic aquí para escribir texto.

Nombre del producto	Fabricante	Características Principales	Capacidad de Integración	Facilidad de Uso	Escalabilidad	Soporte y Mantenimiento	Método de Implementación	Sistemas Operativos Compatibles	Rendimiento	Comentarios de Usuarios	Coste
Splunk Enterprise Security	Splunk Inc.	Análisis de seguridad avanzado, búsqueda en tiempo real, informes personalizados	Alta	Alta	Alta	Excelente, soporte 24/7 disponible	On-premise, en la nube	Linux, Windows	Excelente	4,5/5	Desde \$2,000 por GB de datos ingeridos por año
IBM QRadar	IBM	Detección de amenazas, análisis de comportamiento, gestión de incidentes	Alta	Media	Alta	Excelente, soporte 24/7 disponible	On-premise, en la nube	Linux	Muy bueno	4,3/5	Desde \$10,700 por appliance virtual más \$800 por EPS (eventos por segundo) anual
ArcSight ESM	Micro Focus	Correlación de eventos, análisis forense, gestión de amenazas	Alta	Media	Alta	Bueno, soporte comercial disponible	On-premise, en la nube	Linux, Windows	Muy bueno	4,2/5	Desde \$10,000 por licencia más costos adicionales por EPS
LogRhythm	LogRhythm Inc.	Detección de amenazas, análisis de logs, inteligencia artificial	Alta	Alta	Alta	Excelente, soporte 24/7 disponible	On-premise, en la nube	Linux, Windows	Excelente	4,4/5	Desde \$28,000 por 500 EPS por año
OSSIM (AlienVault)	AT&T Cybersecurity	Correlación de eventos, monitoreo en tiempo real, cumplimiento	Media	Media	Media	Bueno, soporte comercial disponible	On-premise	Linux	Bueno	4,1/5	Gratis
McAfee Enterprise Security Manager	McAfee	Análisis en tiempo real, gestión de riesgos, cumplimiento normativo	Alta	Media	Alta	Bueno, soporte comercial disponible	On-premise, en la nube	Linux	Muy bueno	4,1/5	Desde \$25,000 por 500 EPS por año

Imagen 01: cuadro comparativo de sistemas SIEM

Referencia: Autor

Como se puede observar en el cuadro # 1, tenemos distintos sistemas SIEM, en lo cual hacemos la comparación con el sistema OSSIM, que es un sistema gratuito lo que lo hace ideal para instituciones con presupuestos limitados que es el caso de esta implementación. Ya que este no tiene costes de licencias, y se puede descargar e instalar sin ningún coste alguno.

Además de que este sistema OSSIM es una solución gratuita, este sistema ofrece una gama amplia de funcionalidades, incluyendo correlación de eventos, monitoreo en tiempo real, detección de intrusiones, análisis de vulnerabilidades y cumplimiento normativo.

Lo mejor de este sistema es que, se puede integrar con múltiples herramientas de seguridad de código abierto, lo que permite una expansión o personalización específica dependiendo de lo vallamos a necesitar en nuestra implementación.

Haciendo un poco la comparativa con los demás sistemas SIEM, OSSIM no es tan escalable como los demás sistemas SIEM que se muestran en la tabla, pero este sistema es los suficiente para nuestra implementación ya que este sistema es suficiente para medianas y pequeñas instituciones o empresas que no manejen un volumen extremo de datos. Además, que este sistema ofrece un rendimiento adecuado, que nos ofrece una seguridad decente y una buena capacidad para la detección de amenazas.

8 Diseño.

8.1 Levantamiento en Sitio



Imagen 02: imágenes del sitio donde se implementará el sistema SIEM.

Referencia: Autor

Para la implementación un sistema de gestión de eventos e información de seguridad (SIEM) de manera efectiva, es fundamental realizar el levantamiento de toda la información posible como, el sitio, infraestructura previa, las adecuaciones necesarias, medidas y estimaciones físicas de la Red. También se debe evaluar la postura de seguridad actual, incluyendo políticas, controles, herramientas y procesos, con el fin de determinar las áreas que necesitan mejoras para la adaptación del sistema SIEM.

8.2 Arquitectura de Red

En las visitas realizadas al laboratorio de Redes y Seguridad Informática de la Institución se pudo evidenciar la infraestructura de red interna, el área utilizada para analizar las conexiones de comunicación, montaje de estructuras de red, los elementos y equipos de comunicación, como también los servidores necesarios donde se instalarán los sistemas y herramientas necesarias para la implementación de SIEM.

En el siguiente esquema de red se detalla la Arquitectura de Red de las comunicaciones de datos, los equipos de red, servidores y equipos de comunicación, elementos necesarios que intervienen para levantar una red estructurada donde se implementara el gestor de eventos e información de seguridad SIEM.

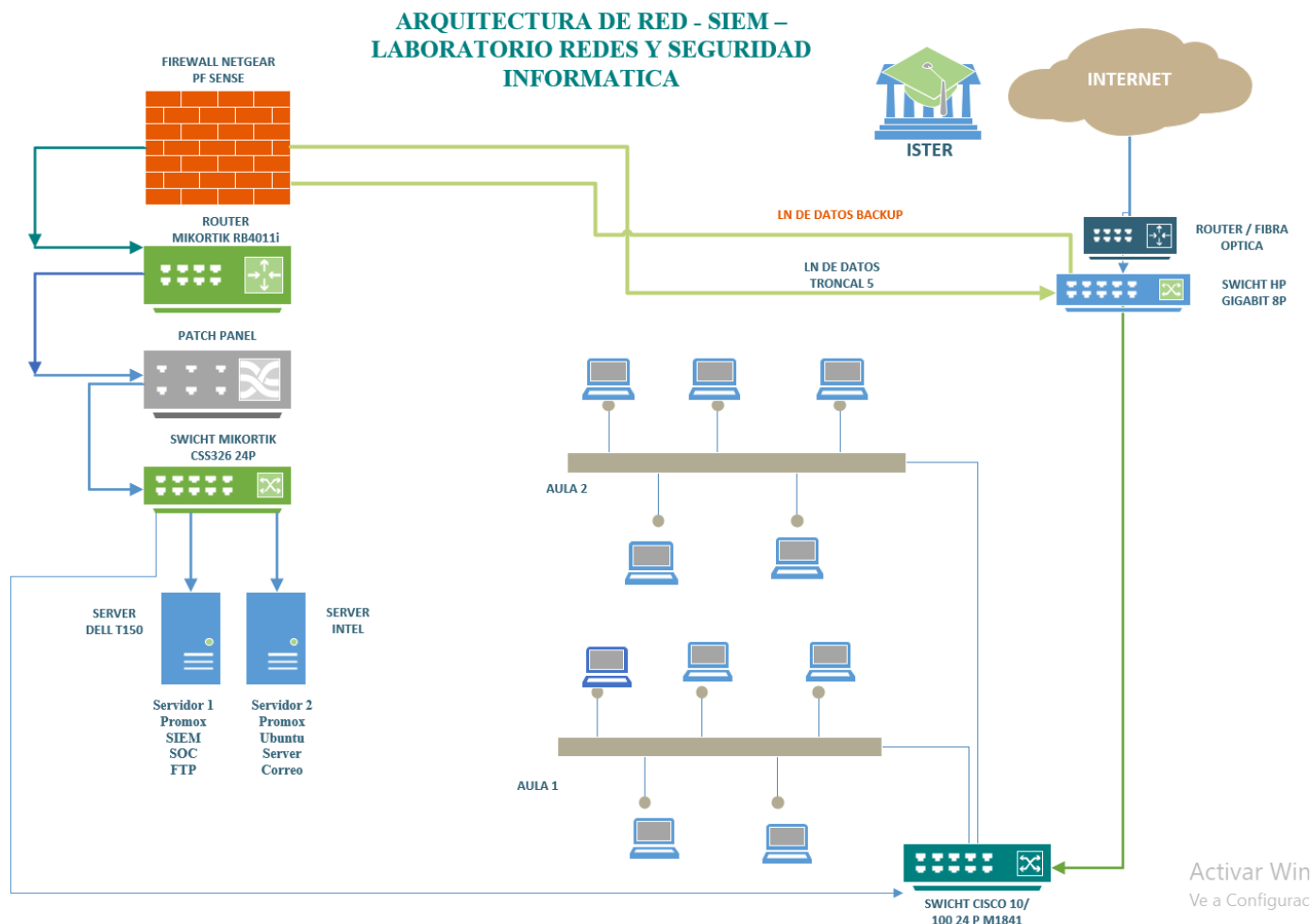


Imagen 03: Imagen Arquitectura de Red

Referencia: Autor

8.3 Infraestructura de Red

Al analizar la red del Laboratorio de Redes y Seguridad Informática del Instituto Rumiñahui tenemos que su infraestructura esta predispuesta en base a las necesidades académicas y docencia, sin embargo para Diseñar un sistema de gestión de eventos es necesario acoplarnos y ser parte de la red interna del Laboratorio, establecer conexiones con los equipos de comunicación y servidores configurados dentro del mismo segmento de red del laboratorio, tener configurados todos los parámetros dados por los equipos de Routing y Switching para que nuestro sistema pueda escanear la red interna del laboratorio. A continuación, nos vamos a ayudar de un esquema de configuraciones a los equipos dentro del segmento de red para nuestro sistema de monitoreo SIEM.

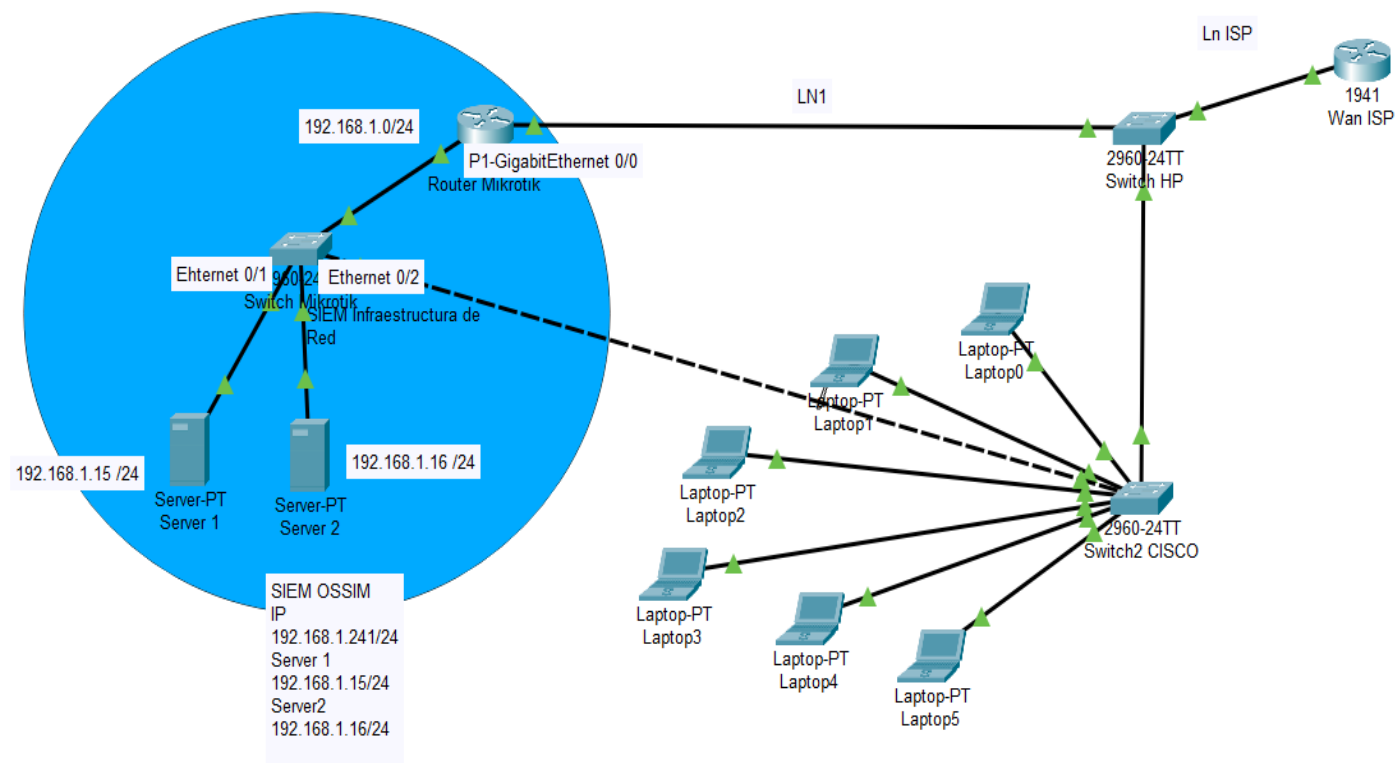


Imagen 04: topología de la red interna de la sala de redes y seguridad informática.

Referencia: Autor

8.4 Equipos Tecnológicos

Una vez realizado el levantamiento en la información en sitio y realizando los esquemas técnicos de la red podemos revisar los equipos que se van a utilizar para la implementación del SIEM, cabe recalcar que esta infraestructura de red más lo equipos tecnológicos presentados puede ayudar a que se integren otros servicios

de seguridad y operatividad como servicios de Mailin, FTP, Seguridad Forense, SOC, Switching y Routing. Y esta nueva infraestructura de red se comunicará con las demás subredes del laboratorio de seguridad del instituto, debemos instalar, cableado estructurado, rack de comunicaciones, elementos de rack y equipos tecnológicos de comunicación y servicios como detallaremos en la siguiente tabla de Equipos:

EQUIPOS MATERIALES DE INFRAESTRUCTURA DE RED PROYECTO SIEM			
ITEM	CANT.	DESCRIPCION	
1	1	GABINETE RACK NEXT PISO TECHO 42UR (205,5x60x80cm.)	
2	1	A/C 4 VENTILADORES DE TECHO PARA RACK	
3	1	ORGANIZADORES HORIZONTAL RACK 2UR 60X80	
4	1	MULTITOMAS HORIZONTAL 9 TOMAS	
5	1	PATCH PANEL 24 PUERTOS MODULAR CAT.6 NEXT	
6	5	PATCH CORD 1 FT CAT.6	

7	6	PACTHC CORD 3 FT CAT.6	
8	6	PATCH CORD 7 FT CAT.6	
	4	BANDEJAS 2U 30*45	
9	1	SERVIDOR DELL T50 2356 XENON 6CORES, 16 GB, 4TB SOLIDO.	
10	1	ROUTER RB4011iGS+RM MICROTIC	
11	1	SWITCH CRS326 24P +2S + RM MICROTICK	
12	2	CONMUTADORES DE FIBRA TP-LINK	
13	1	TECLADO INALAMBRICO	
14	1	MOUSE INALAMBRICO GENIUS	
15	1	UPS 2 KVA INTERACITVO 8 TOMAS	

Imagen 05: Equipos de la infraestructura de red de la sala de redes.

Referencia: Autor

9 Implementación

9.1 Implementación de AliénValut OSSIM

La instalación de la herramienta OSSIM AlienVault requerirá información sobre la arquitectura de red de la sala de redes, así como las configuraciones que permitirán que el programa funcione eficazmente.

Las configuraciones de la máquina virtual, para nuestro sistema SIEM es la siguiente; como podemos ver en la imagen ya tenemos las especificaciones en las cuales va a trabajar nuestro sistema las cuales son:

- 6 de memoria RAM.
- Uno 4 Cores de procesador.
- 40 gigas de memoria de almacenamiento.

Estas son las especificaciones por defecto del sistema, también cabe decir que este es un sistema Linux de Debian de (64-bit)

Agregar ▾ Eliminar Editar Acción de disco ▾ Revertir		
Memoria	5.86 GiB	
Procesadores	4 (1 sockets, 4 cores) [x86-64-v2-AES]	
BIOS	Por defecto (SeaBIOS)	
Pantalla	Por defecto	
Maquina	Por defecto (i440fx)	
Controlador SCSI	Por defecto (LSI 53C895A)	
Dispositivo CD/DVD (ide2)	storage01:iso/AlienVault_OSSIM_64bits.iso,media=cdrom,size=721M	
Disco duro (scsi0)	storage01:108/vm-108-disk-0.qcow2,size=40G	
Dispositivo de red (net0)	virtio=BC:24:11:7F:BD:C4,bridge=vibr0,firewall=1	

Imagen 06: configuración de OSSIM – Especificaciones de la máquina virtual del sistema.

Referencia: Autor

Para la instalación del sistema OSSIM nos dará a escoger dos opciones las cuales la primera opción es la instalación completa (Install AlienVault OSSIM), ya la otra opción es para instalar el sensor (Install AlienVault Sensor). La opción que escogeremos es la primera que nos permite trabajar no sólo con un servicio centralizado, sino que nuestro servidor va a recoger datos de varios sensores a escala de la infraestructura de la sala de redes.



Imagen 07: configuración de OSSIM – Inicio de la instalación.

Referencia: Autor

Al seleccionar nos saldrá esta opción que es la configuración del idioma a escoger de acuerdo a como queramos.

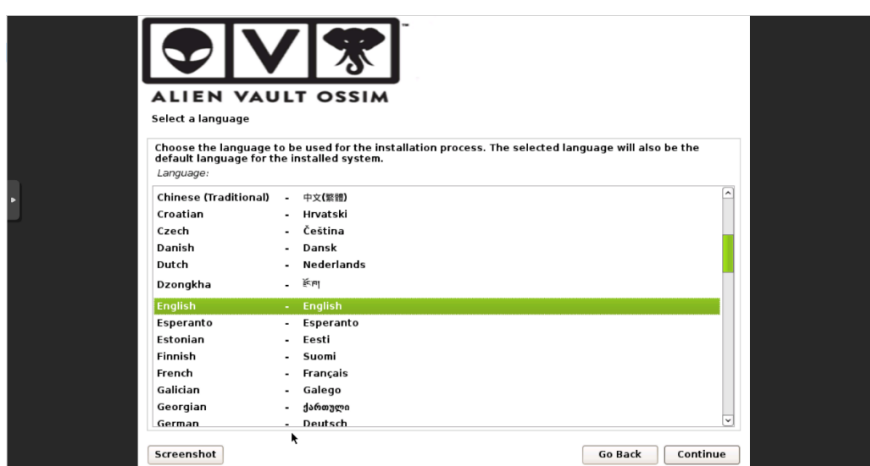


Imagen 08: configuración de OSSIM – Seleccionando el idioma.

Referencia: Autor

Se mostrara la ubicación o el país de residencia en donde estemos realizando al instalación.

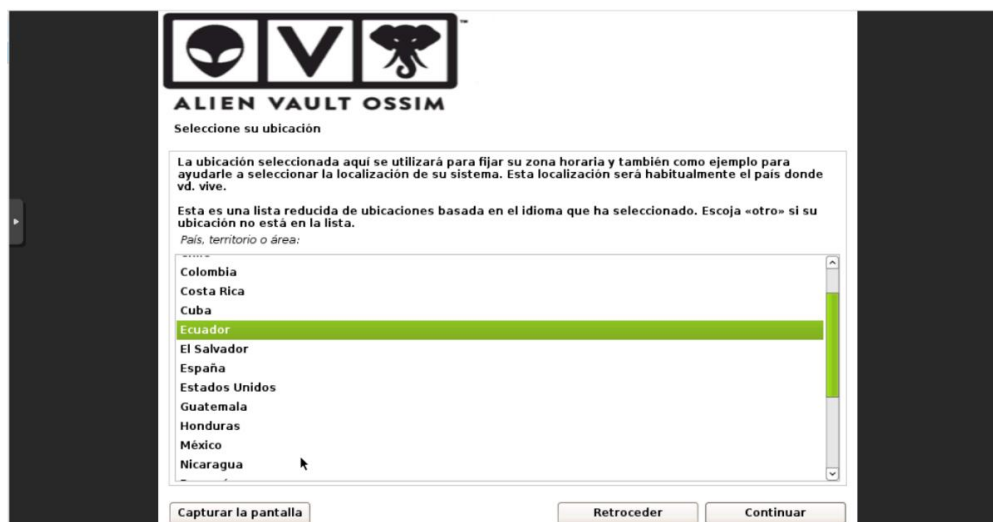


Imagen 09: configuración de OSSIM – Escoger la ubicación.

Referencia: Autor

Seleccionaremos el idioma del teclado en cual estemos utilizando.

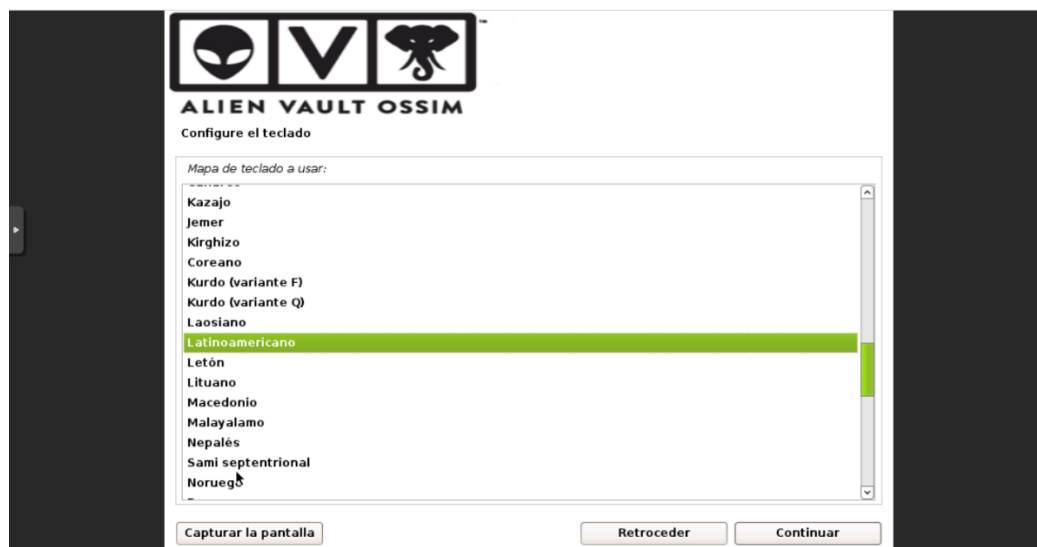


Imagen 10: configuración de OSSIM – Selección del teclado.

Referencia: Autor

Después de darle a continuar, se procederá a la descarga de unos elementos necesarios para la instalación del sistema SIEM.



Imagen 11: configuración OSSIM – Instalación de elementos.

Referencia: Autor

Después de que se descarguen los componentes la siguiente ventana en aparecer es la asignación de la dirección IP de OSSIM para nuestra máquina virtual, en este apartado se debe de tener en consideración cual es el segmento de nuestra red para poder asignarle una dirección IP a nuestro sistema.



Imagen 12: configuración OSSIM – Asignación de la dirección IP del OSSIM

Referencia: Autor

Al continuar la siguiente ventana se especificará la máscara de red de la dirección IP que se configuro previamente en la máquina virtual.



Imagen 13: configuración OSSIM – configuración de mascara de red.

Referencia: Autor

Al seguir el proceso se nos muestra la dirección IP de la puerta de enlace (Gateway), que tiene nuestro servidor. Cabe decir que la dirección nos salda automática ya que al poner la dirección IP en nuestro servidor automáticamente el sistema resuelve e identifica cual es la dirección IP del Gateway.



ALIEN VAULT OSSIM

Configurar la red

La pasarela es una dirección IP (cuatro números separados por puntos) que indica el encaminador de pasarela, también conocido como encaminador por omisión. Todo el tráfico que se envía fuera de su LAN (por ejemplo, hacia Internet) se envía a este encaminador. En algunas circunstancias anormales, puede no tener un encaminador; si es así lo puede dejar en blanco. Si no sabe la respuesta correcta a esta pregunta, consulte al administrador de red.

Pasarela:

Capturar la pantalla Retroceder Continuar

Imagen 14: configuración OSSIM – configuración del Gateway.

Referencia: Autor

A continuación, la siguiente pestaña es la asignación de la dirección DNS, esto es para la solución del nombre de dominio, además de comenzar con la asignación de la red correspondiente.



The screenshot shows the 'Configurar la red' (Configure the network) section of the Alien Vault OSSIM web interface. At the top, there is a logo with three icons: an alien head, a 'V', and an elephant, followed by the text 'ALIEN VAULT OSSIM'. Below the logo, the section is titled 'Configurar la red'. A text box contains instructions in Spanish: 'Los servidores de nombres se utilizan para buscar los nombres de las máquinas de la red. Por favor, introduzca la dirección IP (no el nombre de sistema) de hasta tres servidores de nombres, separados por espacios. No utilice comas. Se consultarán los servidores en el orden en que se introduzcan. Si no quiere utilizar ningún servidor de nombres deje este campo en blanco.' Below this text, there is a label 'Direcciones de servidores de nombres:' followed by a large, empty text input field. At the bottom of the form, there are three buttons: 'Capturar la pantalla' (Screenshot), 'Retroceder' (Back), and 'Continuar' (Continue).

Imagen 15: configuración OSSIM – configuración de DNS.

Referencia: Autor

La siguiente pestaña en salir es la configuracion de nuestra contraseña que debe de ser una robusta ya que esta contraseña es para nuestro super usuario (root).

ALIEN VAULT OSSIM

Configurar usuarios y contraseñas

Necesita definir una contraseña para el superusuario («root»), la cuenta de administración del sistema. Podría tener graves consecuencias que un usuario malicioso o un usuario sin la debida cualificación tuviera acceso a la cuenta del administrador del sistema, así que debe tener cuidado y elegir un la contraseña para el superusuario que no sea fácil de adivinar. No debería ser una palabra que se encuentre en el diccionario, o una palabra que pueda asociarse fácilmente con usted.

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

La contraseña del usuario «root» (administrador) no debería estar en blanco. Si deja este valor en blanco, entonces se deshabilitará la cuenta de root creará una cuenta de usuario a la que se le darán permisos para convertirse en usuario administrador utilizando la orden «sudo».

Tenga en cuenta que no podrá ver la contraseña mientras la introduce.

Clave del superusuario:

☐ Mostrar la contraseña en claro

Por favor, introduzca la misma contraseña de superusuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

☐ Mostrar la contraseña en claro

Imagen 16: configuración OSSIM – configuración de contraseña.

Referencia: Autor

La siguiente pestaña nos muestra la zona horaria según a las asignaciones previas.

ALIEN VAULT OSSIM

Configurar el reloj

Si la zona horaria deseada no está en la lista entonces vuelva atrás al paso «Escoja el idioma» y seleccione un país que utilice la zona horaria deseada (el país donde vive o está ubicado).

Seleccione una ubicación en su zona horaria:

- Guayaquil
- Islas Galápagos

Imagen 16: configuración OSSIM – Asignación de zona horaria.

Referencia: Autor

Una vez configurada la zona horaria, se iniciará la instalación base del sistema OSSIM en el disco duro de la máquina virtual.



Imagen 17: configuración OSSIM – Instalación base del sistema.

Referencia: Autor

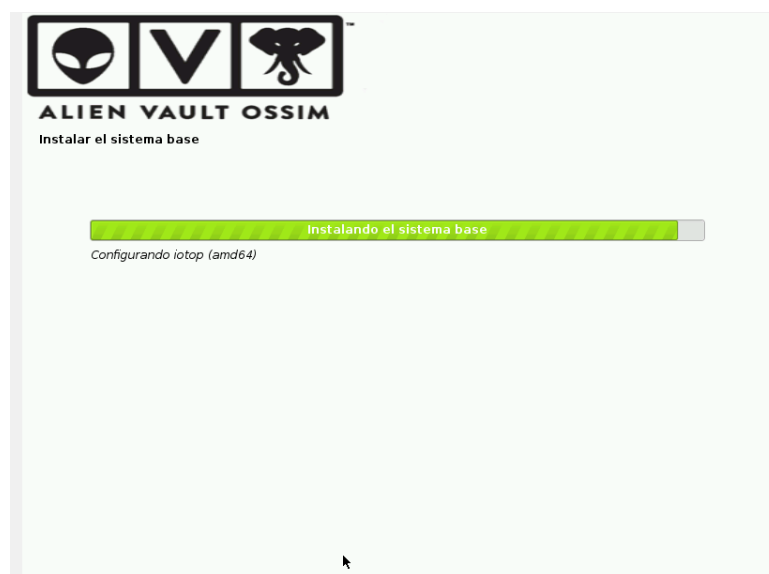


Imagen 18: configuración OSSIM – Instalación base del sistema.

Referencia: Autor

Una vez completada la instalación base de nuestro sistema OSSIM, la máquina virtual se reiniciará para cargar la pantalla de arranque.



Imagen 19: configuración OSSIM – inicio del sistema base.

Referencia: Autor

Al terminar todas las instalaciones del OSSIM AlienVault, ya se podría acceder al sistema.

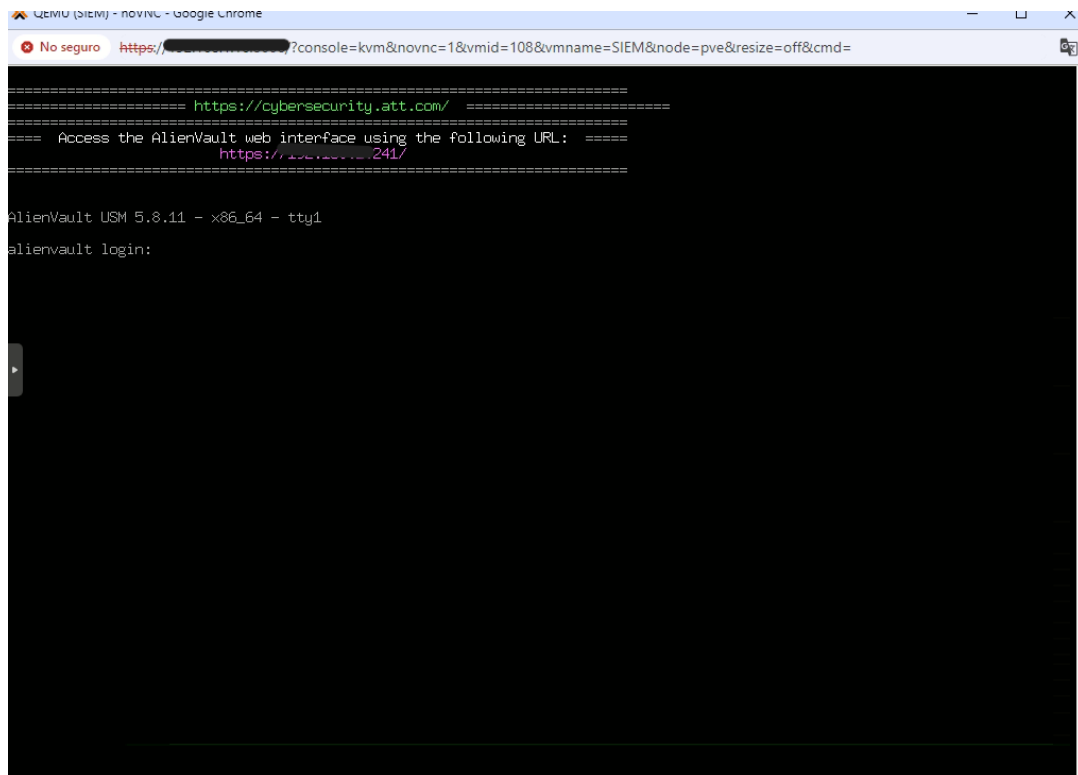


Imagen 20: configuración OSSIM – Inicio del sistema.

Referencia: Autor

Para comprobar que podremos acceder, introduciremos las claves que configuramos anteriormente, es decir, el superusuario (root), y la contraseña que se colocó previamente, al ingresar estas credenciales se nos abrirá un menú de opciones de configuraciones disponible.



Imagen 21: configuración OSSIM – Menú de opciones del sistema.

Referencia: Autor

Para acceder a la página web de nuestro sistema OSSIM, debemos introducir la dirección IP previamente configurada, esta dirección la colocaremos en un navegador web del equipo que estemos utilizando y se encuentre en el mismo segmento de red.

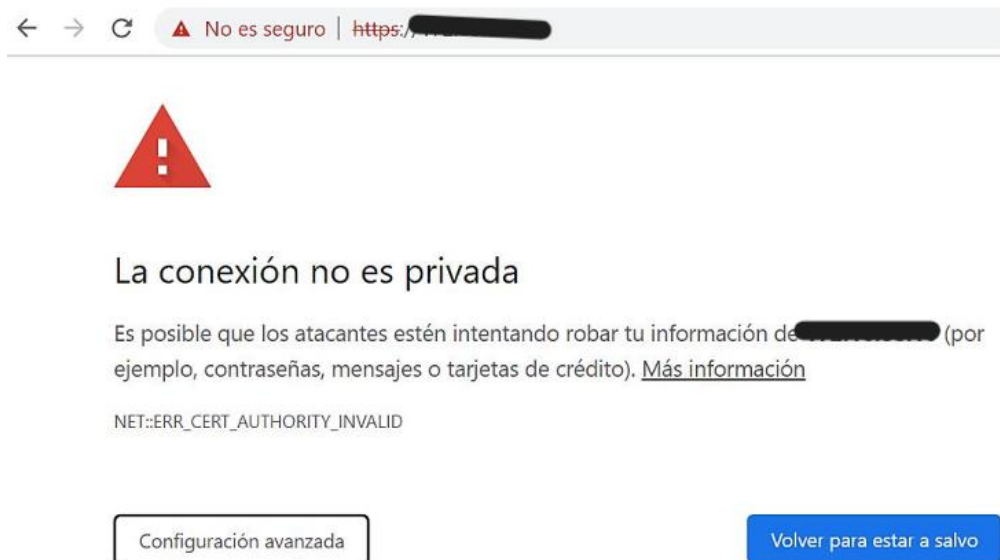


Imagen 22: configuración OSSIM – Acceso a la página web del sistema.

Referencia: Autor

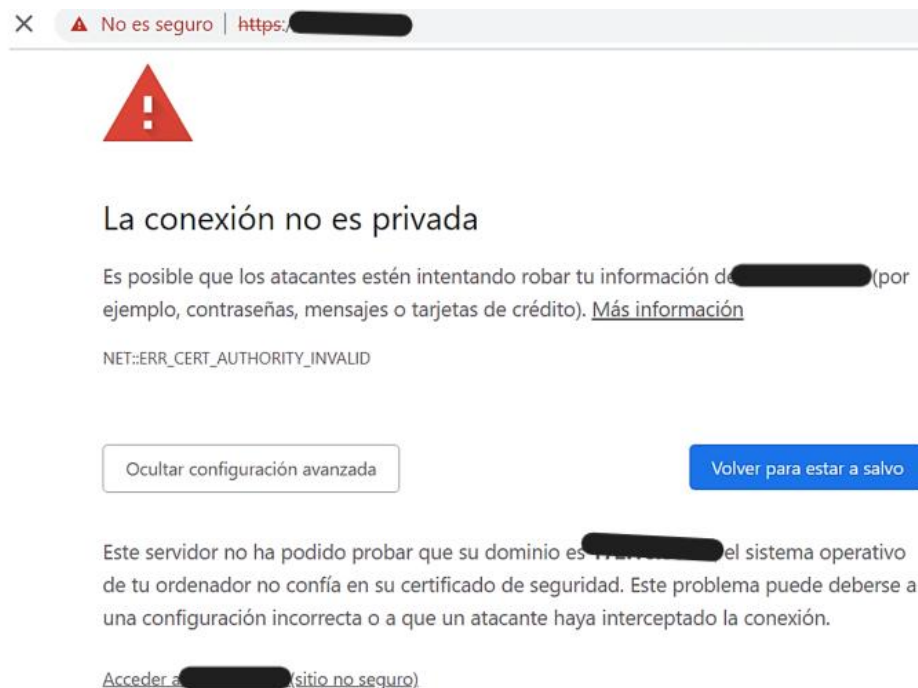
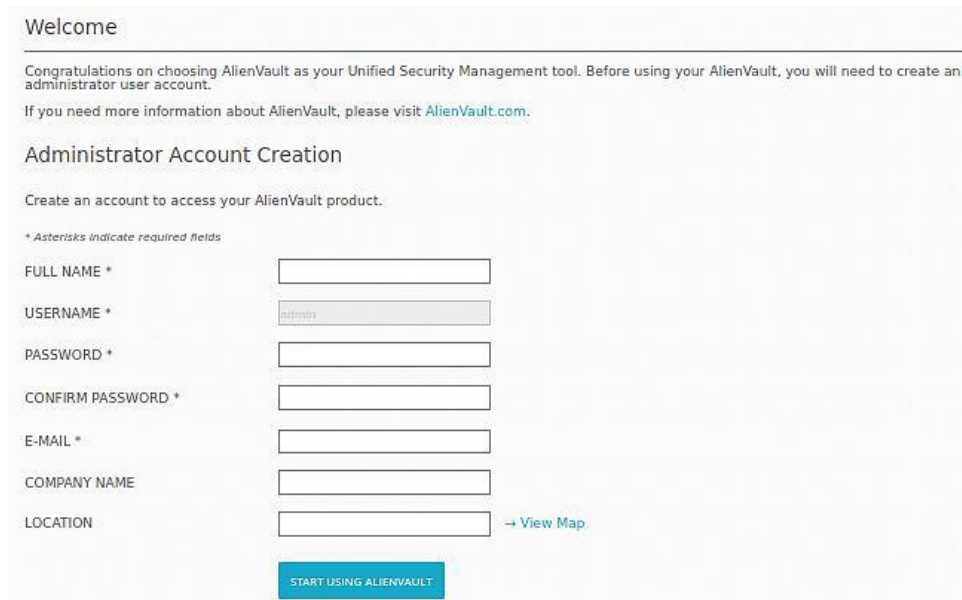


Imagen 23: configuración OSSIM – Acceso a la página web del sistema.

Referencia: Autor

Al aceptar la opción de acceder al sitio web, se podría ver la siguiente página en la cual se ingresará los datos o información requerida en el formulario de creación de cuenta.

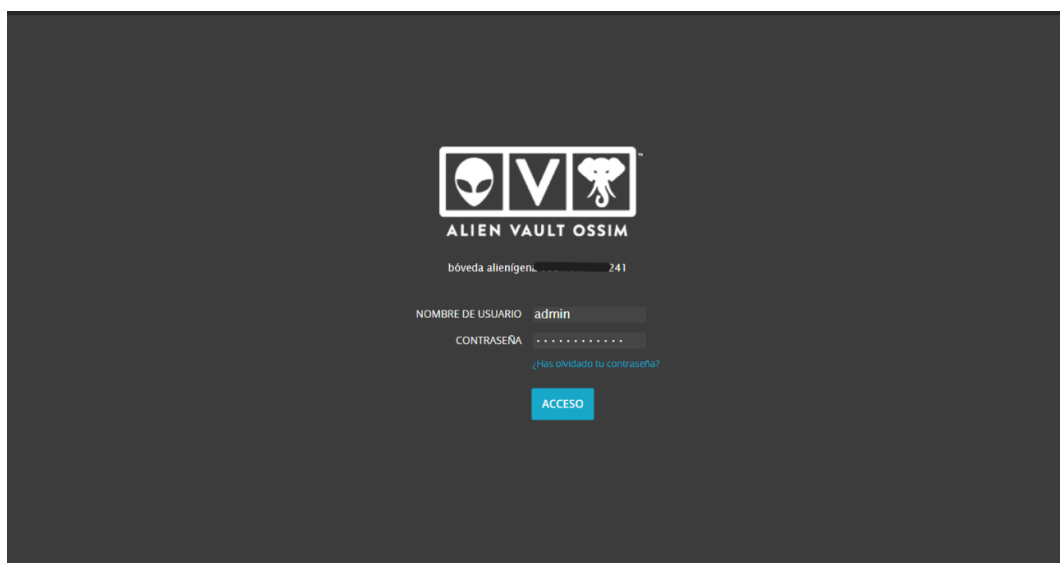


The screenshot shows the 'Administrator Account Creation' page of AlienVault OSSIM. At the top, a 'Welcome' message congratulates the user for choosing AlienVault and instructs them to create an administrator account. Below this, a link to 'AlienVault.com' is provided. The main section is titled 'Administrator Account Creation' and asks the user to 'Create an account to access your AlienVault product.' A note states '* Asterisks indicate required fields'. The form contains several input fields: 'FULL NAME *', 'USERNAME *' (with 'admin' pre-filled), 'PASSWORD *', 'CONFIRM PASSWORD *', 'E-MAIL *', 'COMPANY NAME', and 'LOCATION'. A '→ View Map' link is next to the 'LOCATION' field. At the bottom, there is a blue button labeled 'START USING ALIENVAULT'.

Imagen 24: configuración OSSIM – Formulario de creación de cuenta.

Referencia: Autor

Una vez que haya introducido la información solicitada por el formulario, se le dará paso a iniciar sesión en su cuenta con el nombre de usuario y la contraseña asignados previamente en la página anterior.



The screenshot shows the login page of AlienVault OSSIM. At the top, the AlienVault logo (an alien head, a 'V', and an elephant) is displayed above the text 'ALIEN VAULT OSSIM'. Below the logo, the text 'bóveda alienígena.' is followed by a redacted IP address '241'. The login form includes two fields: 'NOMBRE DE USUARIO' with 'admin' pre-filled, and 'CONTRASEÑA' with masked characters. A link for '¿Has olvidado tu contraseña?' is located below the password field. At the bottom, there is a blue button labeled 'ACCESO'.

Imagen 25: configuración OSSIM – Ingreso de inicio de sesión.

Referencia: Autor

Una vez establecidas las credenciales, entraremos en la interfaz web de OSSIM, donde se mostrará una pantalla que nos dará la bienvenida para iniciar la programación del servidor.



Imagen 26: configuración OSSIM – Inicio del sistema.

Referencia: Autor

Al continuar en la interfaz web, aparece una ventana que es el asistente OSSIM, en el cual nos indica las configuraciones preliminares del sistema.

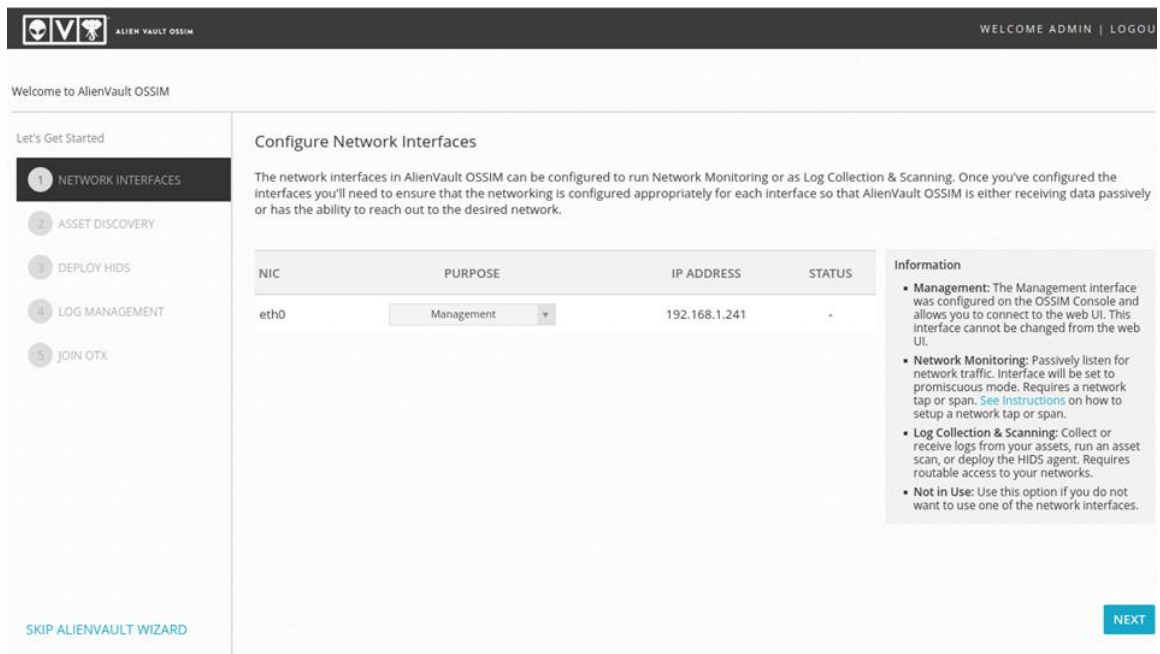


Imagen 27: configuración OSSIM – Interfaces de red.

Referencia: Autor

La siguiente pantalla nos indica los activos que hay en la red, así como la posibilidad de añadir otros activos o equipos de red, también aquí se puede realizar un escaneo de la red para poder añadir más activos.

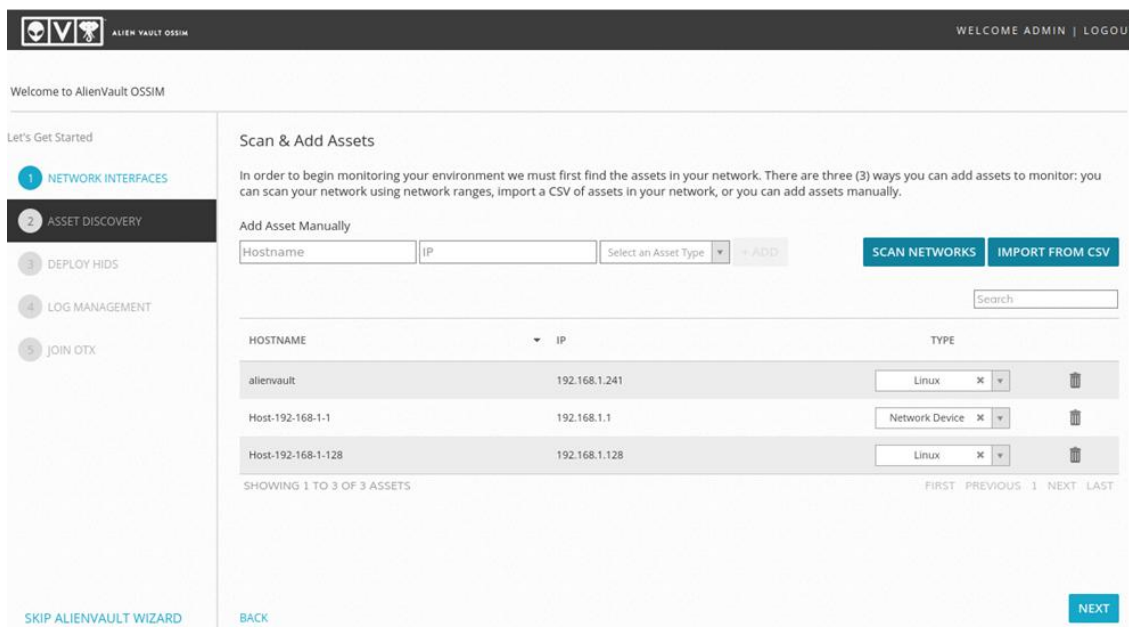


Imagen 28: configuración OSSIM – Descubrimiento de activos.

Referencia: Autor

A continuación, se nos enseña el despliegue de la implementación del HIDS (Host-based Intrusion Detection System) en ordenadores y servidores para su control, donde es necesario incluir un nombre de usuario, contraseña y dominio, este último es opcional.

The screenshot shows the 'Deploy HIDS to Servers' configuration page in the AlienVault OSSIM interface. The top navigation bar includes the AlienVault logo, 'ALIEN VAULT OSSIM', and a 'WELCOME ADMIN | LOGOUT' link. The main content area is titled 'Deploy HIDS to Servers' and includes a sub-header 'Let's Get Started' with a sidebar menu containing five steps: 1. NETWORK INTERFACES, 2. ASSET DISCOVERY, 3. DEPLOY HIDS (selected), 4. LOG MANAGEMENT, and 5. JOIN OTX. The main panel contains a 'Deploy HIDS to Servers' section with a sub-header 'UNIX / LINUX (2)'. Below this, a text block states: 'For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.' Below this text are two input fields for 'Username' and 'Password', and a 'DEPLOY' button. To the right of these fields, a section titled 'Deploy to the following hosts:' shows a list of hosts with a plus icon and the text 'Local 192.168.1.0_24'. At the bottom of the page, there are three buttons: 'SKIP ALIENVAULT WIZARD', 'BACK', and 'NEXT'.

Imagen 29: configuración OSSIM – Despliegue HIDS.

Referencia: Autor

Al continuar, verá esta ventana en la que se le pedirá que realice el registro de una cuenta para introducir el código OTX, ya que permite la incorporación del programa de detección de amenazas. Este código se obtendrá al registrar una cuenta que será corroborada. Este apartado es opcional ya que este apartado requiere unas configuraciones adicionales, lo recomendable es excluir esto e iniciar la interfaz web de OSSIM.

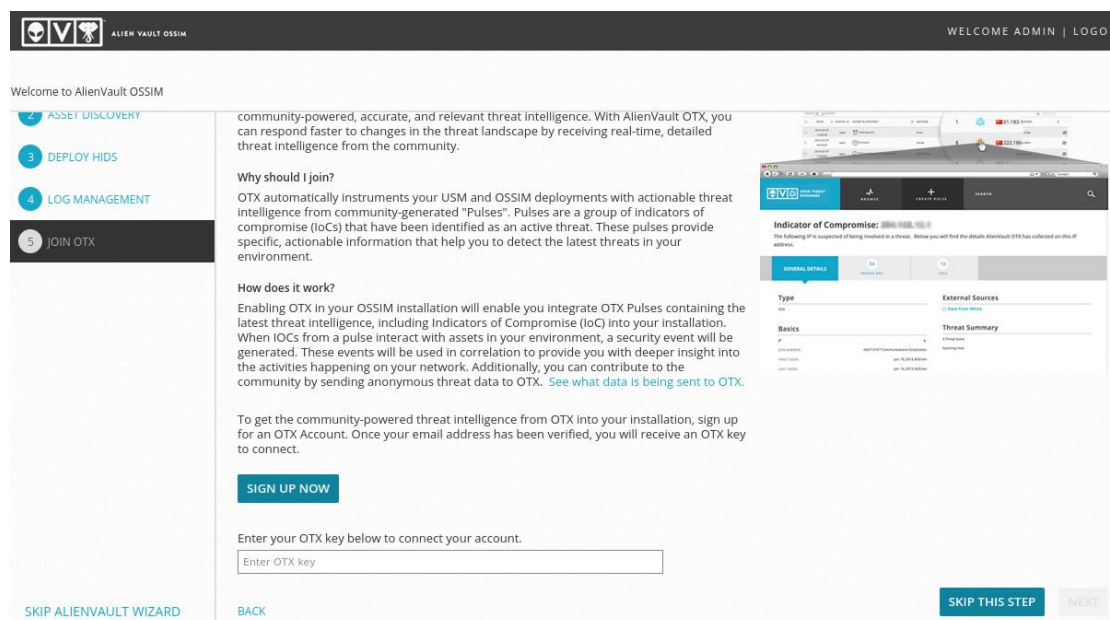


Imagen 30: configuración OSSIM – Registro de código OTX.

Referencia: Autor

Y la última ventana nos muestra un mensaje de finalización de registro.

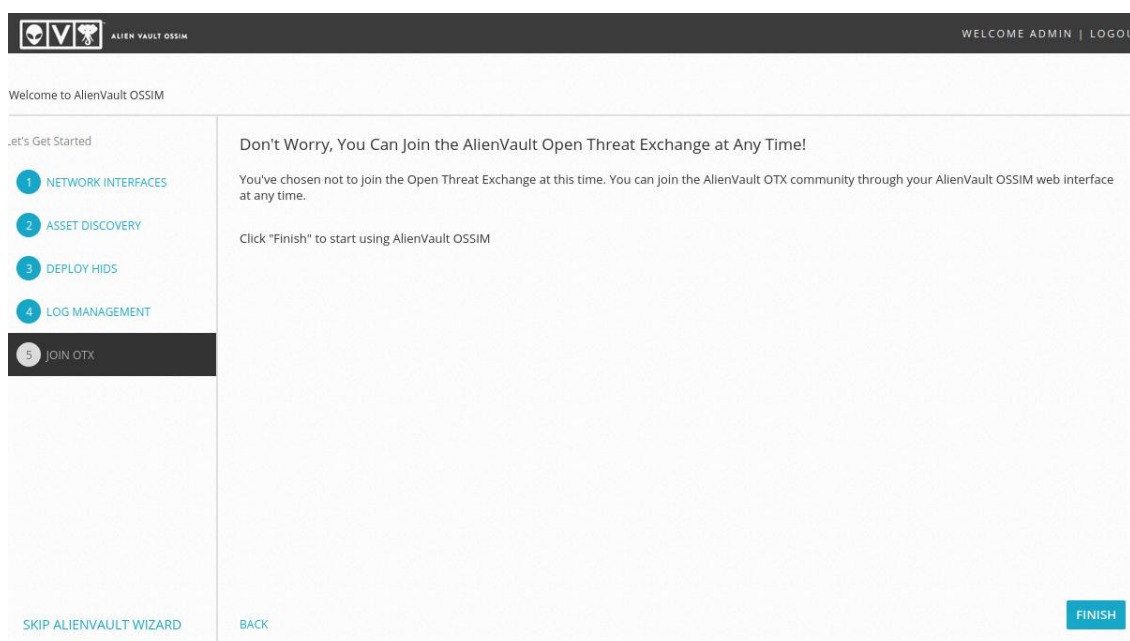


Imagen 31: configuración OSSIM – Finalización de registro.

Referencia: Autor

Al final, se cargará una interfaz web con diferentes elementos de configuración.

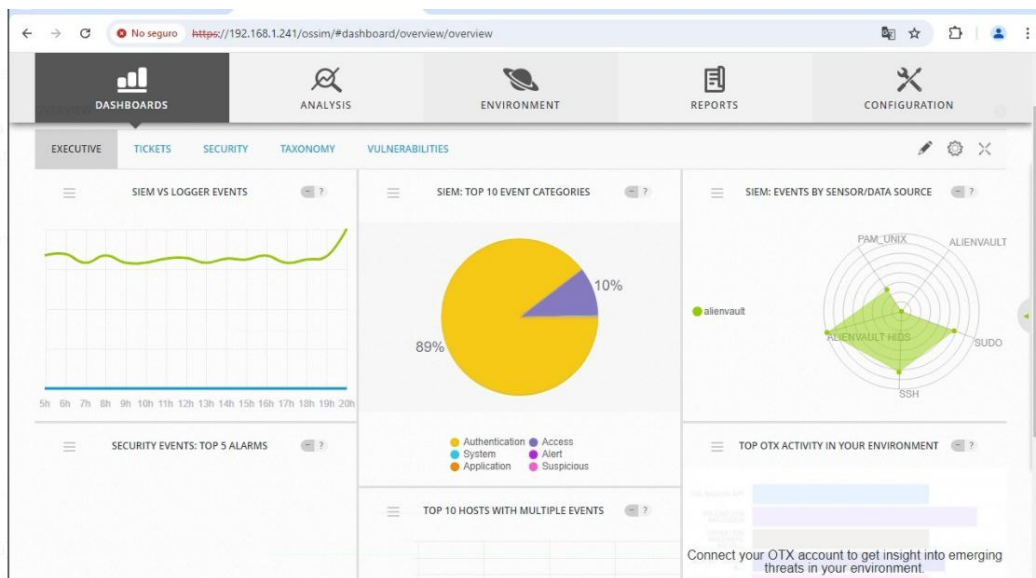


Imagen 32: configuración OSSIM – Interfaz web.

Referencia: Autor

9.2 Gestión de activos

Accediendo con las claves a la interfaz web de OSSIM, nos vamos a donde dice ‘Activos y Grupos’ que está ubicado en el apartado de ‘Ambiente’, en el cual aquí nos muestra los valores (Activos o dispositivos) detectados por el sistema OSSIM. Se pueden añadir más activos si es necesario, para ello nos vamos donde dice ‘Agregar activos’ y después seleccionamos donde dice ‘Escanear en busca de nuevos activos’.

<

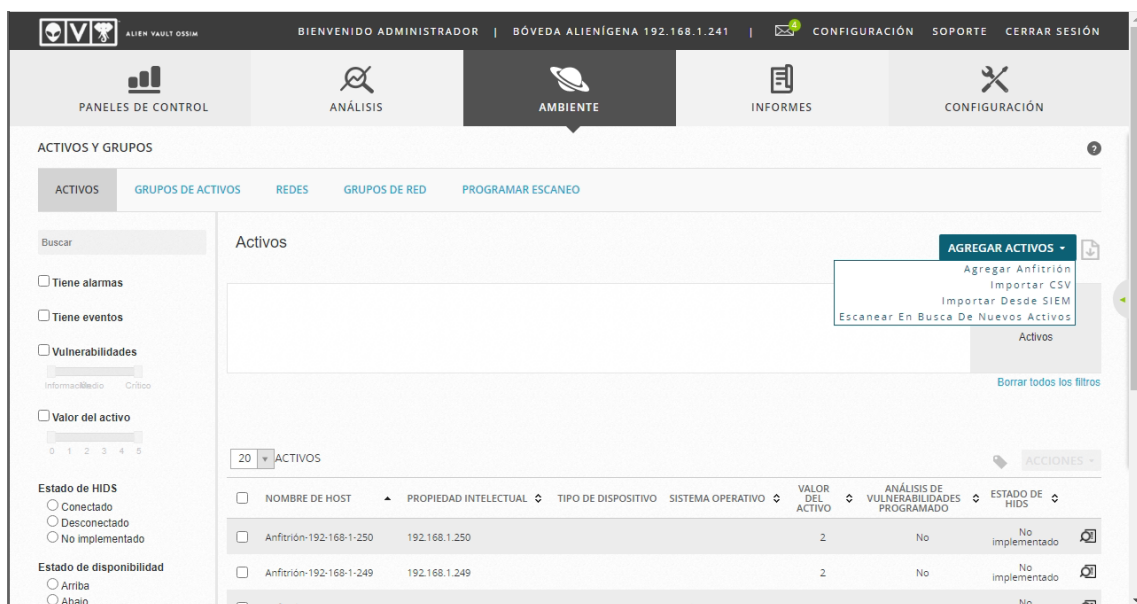


Imagen 33: interfaz web OSSIM – Gestión de activos.

Referencia: Autor

Al seleccionar la función de búsqueda de nuevos activos se abrirá un campo para agregar los activos que se van a explorar en la red, también en este apartado se podrá seleccionar el sensor que queramos utilizar ya sea el sensor colocado en el servidor OSSIM, también en este apartado de podría seleccionar el tipo de escaneo, que tan rápido queremos que sea el escaneo, el detectar el sistema operativo y servicios, la utilización de la resolución DNS invertida para conocer los nombres de los distintos equipos. Además, el periodo de escaneado vendrá determinado por el tamaño y la cantidad de servidores, ordenadores y dispositivos conectados a la red. Esto se hace para recopilar información y guardarla en la base de datos OSSIM con el objetivo de descubrir posibles peligros y vulnerabilidades.

SCAN FOR NEW ASSETS

TARGET SELECTION

Please, select the assets you want to scan:

192.168.1.1 (Host-192-168-1-1)

192.168.1.128 (Host-192-168-1-128)

Type here to search assets

All Assets

Assets

Asset Groups

Networks

Network Groups

[X]

DELETE ALL

SENSOR SELECTION

Local sensor Launch scan from the local sensor

Automatic sensor Launch scan from the first available sensor

SELECT A SPECIFIC SENSOR

alienvault [192.168.1.241]

ADVANCED OPTIONS

Scan type:

Fast Scan

Fast mode will scan fewer ports than the default scan

Timing template:

Normal

Autodetect services and Operating System

Enable reverse DNS Resolutions

Privileged Mode

START SCAN

Imagen 34: interfaz web OSSIM – Ingreso de activos y escaneo de activos.

Referencia: Autor

Los resultados obtenidos del escaneo de estos activos, fue una lista de los activos encontrados, si queremos actualizar la administración de estos activos hacemos click en ‘Update managed assets’.

SCAN RESULTS								
☒	HOST	HOSTNAME [?]	FQDN [?]	DEVICE TYPES	MAC [?]	OS [?]	SERVICES [?]	☐ FQDN AS HOSTNAME [?]
☒	192.168.1.1	Host-192-168-1-1	-	General Purpose	00:50:56:C0:00:02	FreeBSD 6.X	mysql	☐
☒	192.168.1.128	Host-192-168-1-128	-	-	00:0C:29:25:2F:48	-		☐

CLEAR SCAN RESULT

UPDATE MANAGED ASSETS

Imagen 35: interfaz web OSSIM – Resultados de escaneo de activos.

Referencia: Autor

☒	HOST	HOSTNAME [?]	FQDN [?]	DEVICE TYPES	MAC [?]	OS [?]	SERVICES [?]	☐ FQDN AS HOSTNAME [?]
☒	192.168.1.1	Host-192-168-1-1	-	General Purpose	00:50:56:C0:00:02	FreeBSD 6.X	mysql	☐
☒	192.168.1.128	Host-192-168-1-128	-	-	00:0C:29:25:2F:48	-	-	☐
☒	192.168.1.241	alienvault	alienvault.alienvault	General Purpose	-	Linux 2.6.X	ssh, mysql, https, http, otp	☐
☒	192.168.1.254	Host-192-168-1-254	-	-	00:50:56:F3:E7:CD	-	-	☐

Imagen 36: interfaz web OSSIM – Actualización de gestión de activos.

Referencia: Autor

Los datos habilitados corresponden al nombre del grupo que incluirá los activos conectados, junto con una breve descripción. El valor de crítico del activo se expresará en una escala de 1 a 5 en función del tipo o clase de activos gestionados por la red. El sensor o red de sensores distribuidos se utilizará para administrar el grupo de servidores especificado. Además, deberá indicarse que el «activo» no corresponde a una entidad externa, y cualquier modificación deberá guardarse para garantizar que la información del registro esté actualizada.

Please, fill these global properties about the assets you've scanned

Values marked with () are mandatory*

Optional group name	Description
Servicios	test
Asset Value *	External Asset *
5	☐ Yes ☒ No
Sensors *	
☒ 192.168.1.241 (alienvault)	

Imagen 37: interfaz web OSSIM – Nombre del grupo de activos.

Referencia: Autor

Al darle al ‘Save’ se actualizará el listado en un resumen descriptivo de los activos nuevos de la red.

Asset information successfully updated

SCAN SUMMARY			
IP ADDRESS	HOSTNAME	STATUS	DETAILS
192.168.1.254	Host-192-168-1-254	Success	-
192.168.1.241	alienvault	Warning	
OS could not be saved [More relevant OS was previously inserted]			
192.168.1.128	Host-192-168-1-128	Success	-
192.168.1.1	Host-192-168-1-1	Success	-

SHOWING 1 TO 4 OF 4 ASSETS

FIRST PREVIOUS 1 NEXT LAST

Imagen 38: interfaz web OSSIM – Activos y grupos.

Referencia: Autor

Una vez actualizado el inventario con la información del grupo de servidores creado, aparecerá en la opción «Grupos de activos» dentro de la sección «Entorno», mostrando el número de activos asociados al grupo, pero sin datos estadísticos sobre vulnerabilidades, alarmas y disponibilidad.

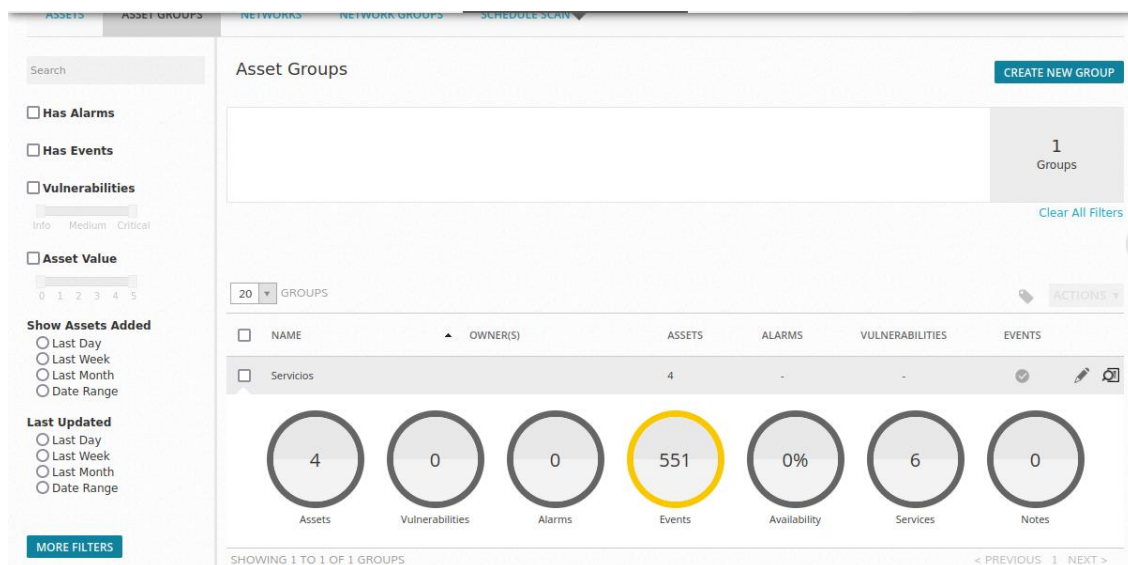


Imagen 39: interfaz web OSSIM – Grupos de activos

Referencia: Autor

En esta pestaña llamada ‘Networks’, aquí se muestra las redes que podrán configurarse y ser monitoreadas por el OSSIM.

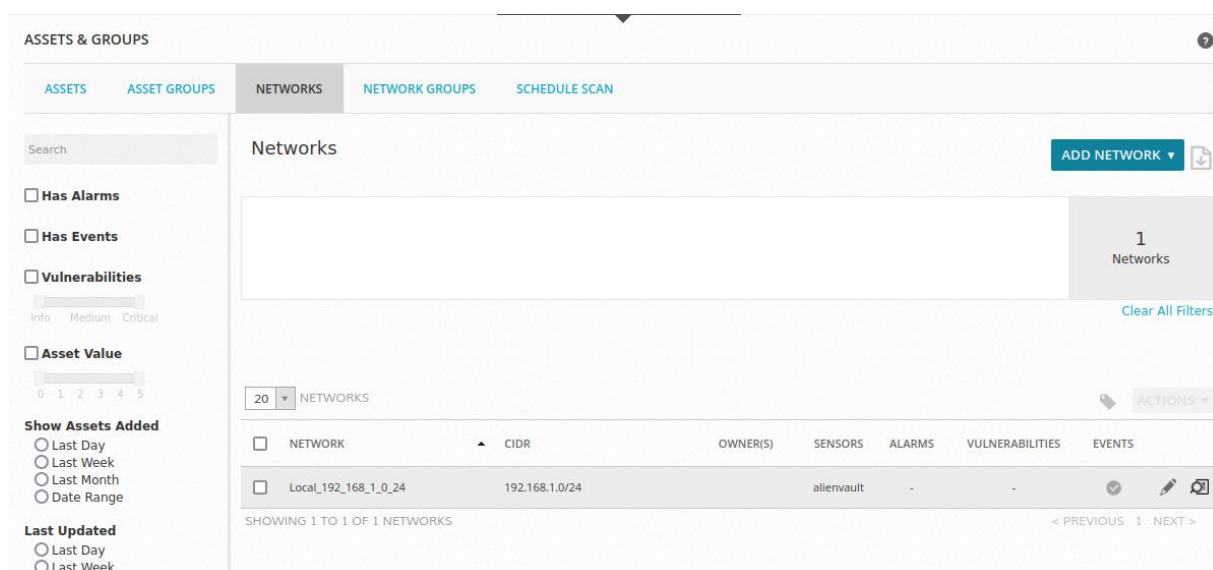


Imagen 40: interfaz web OSSIM – Redes

Referencia: Autor

En esta pestaña llamada ‘Networks Groups’, se muestra el conjunto de redes que se pueden agruparse.

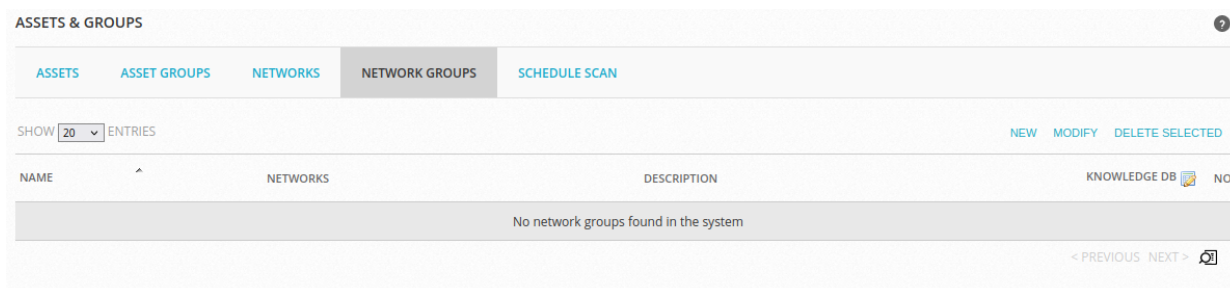


Imagen 41: interfaz web OSSIM – Grupos de redes.

Referencia: Autor

Del mismo modo, si se necesitan otros grupos de activos, se pueden construir y añadir para conmutadores, enrutadores, VPN y estaciones de trabajo para organizar la red y producir un mapa de los activos disponibles para la empresa o entidad. Para ver información sobre cada host (activo), seleccione la opción «Activos» en la sección «Entorno» y, a continuación, seleccione un activo.

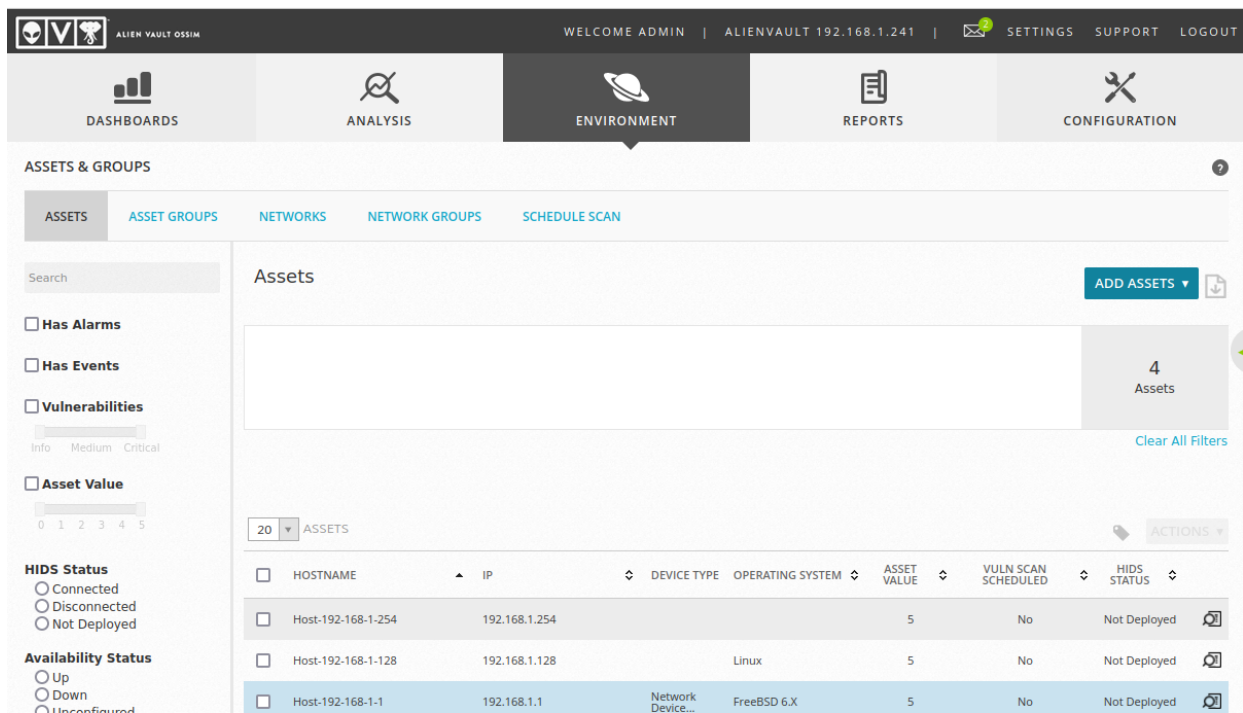


Imagen 42: interfaz web OSSIM – Activos

Referencia: Autor

Al elegir cualquier activo de la lista que aparece, se puede verificar la información que presenta dicho activo, y si de ser necesario se puede realizar algunas modificaciones mediante donde dice ‘Actions’, para poder editar el activo seleccionado.

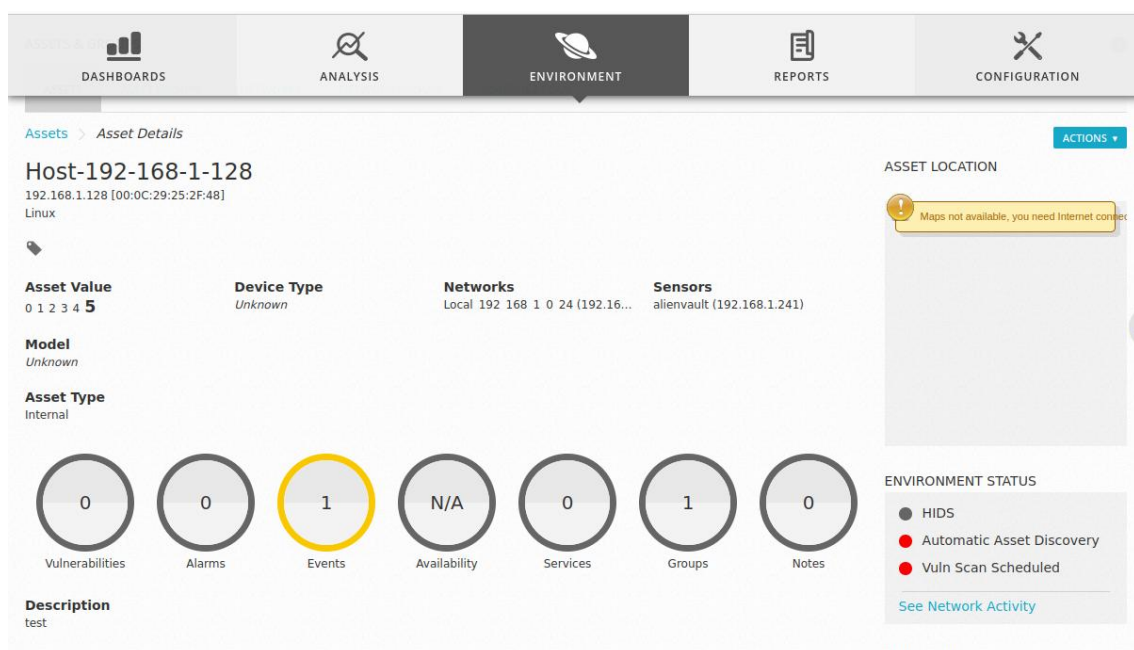


Imagen 43: interfaz web OSSIM – Detalles de activos.

Referencia: Autor

Para editar el activo seleccionado nos vamos donde dice ‘Actions’, y seleccionamos donde dice ‘Edit’.

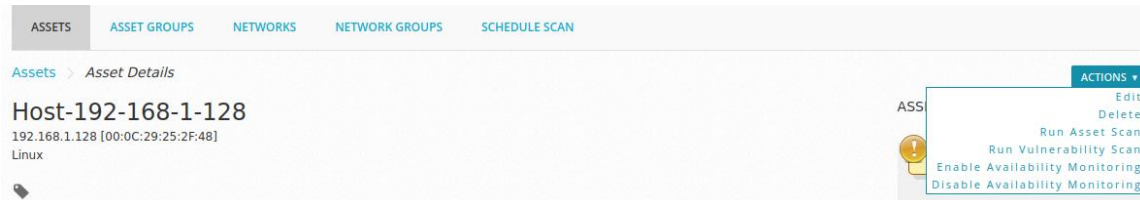


Imagen 44: interfaz web OSSIM – Edición de los detalles del activo

Referencia: Autor

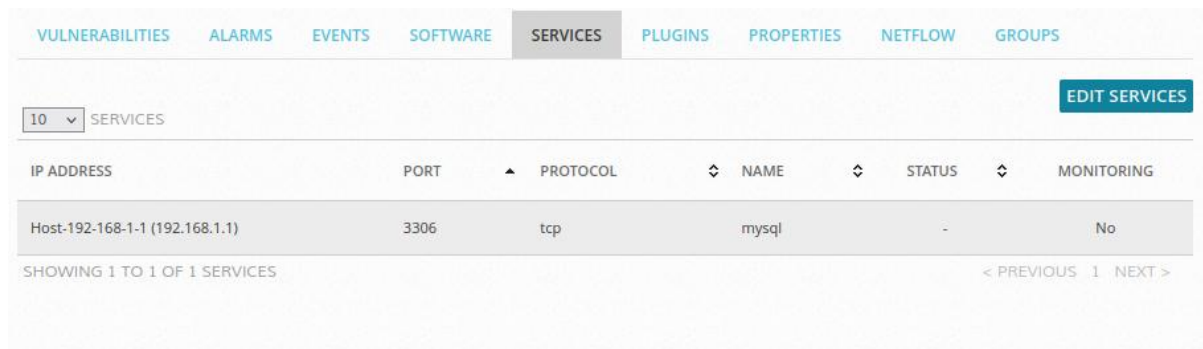
Al darle a editar nos saldrá una ventana en la cual nos permitirá la actualización y configuración del activo seleccionado.

The screenshot shows the 'Edit Asset' form in the OSSIM web interface. The form has a title bar 'Edit Asset' with a close button. Below the title bar, there is a note 'Values marked with (*) are mandatory'. The form is divided into several sections. The first section contains 'Name *' (Host-192-168-1-128), 'IP Address *' (192.168.1.128), and 'FQDN/Aliases'. The second section contains 'Asset Value *' (5), 'External Asset *' (Yes/No), and 'Latitude/Longitude'. The third section contains 'Operating System' (Linux), 'Model', and 'Description' (test). The fourth section contains 'Sensors *' (192.168.1.241 (alienvault)). There is also a 'Location' field and a 'Devices Types' section with '-- Devices --' and 'Types' dropdowns, and an 'ADD' button. A yellow warning message with an exclamation mark icon states 'Maps not available, you need Internet connection'.

Imagen 45: interfaz web OSSIM – Edición del activo.

Referencia: Autor

También dentro de la información obtenida del activo, se puede seleccionar donde dice ‘Services’, en este apartado se pueden visualizar los servicios que están activos, al igual estos servicios también se pueden editar y mostrar información como protocolos, puertos, nombres, monitoreo y estado.



SERVICES					
IP ADDRESS	PORT	PROTOCOL	NAME	STATUS	MONITORING
Host-192-168-1-1 (192.168.1.1)	3306	tcp	mysql	-	No

Imagen 46: interfaz web OSSIM – Servicios de los activos.

Referencia: Autor

9.3 Gestión de disponibilidad

Donde dice ‘Environment’ en la interfaz web del OSSIM, nos ingresamos a la sección de ‘Assets’ y seleccionamos cualquier activo en la lista y ingresamos a la información del activo y una vez dentro no vamos donde dice ‘Actions’ para habilitar el monitoreo de disponibilidad en ‘Enable Availability Monitoring’, con una configuración de que el monitoreo ha sido habilitado, es decir que se activó el monitoreo en el activo.

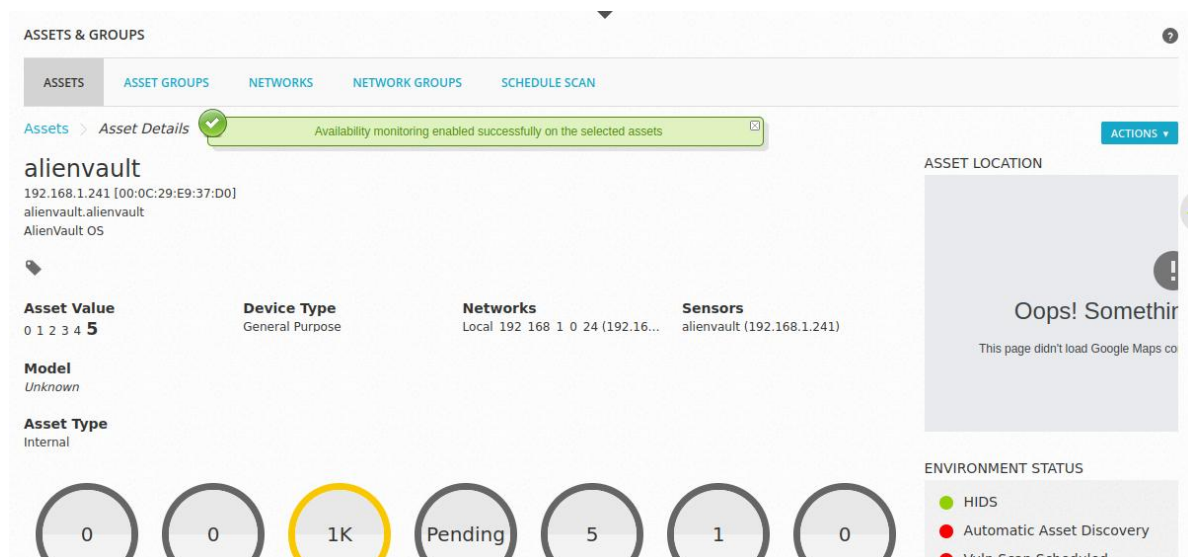


Imagen 47: interfaz web OSSIM – Gestión de monitoreo de disponibilidad.

Referencia: Autor

Ahí mismo en el activo habilitaremos el monitoreo de los servicios en el apartado ‘Services’ en la sección de ‘Description’ del activo que este seleccionado.

VULNERABILITIES	ALARMS	EVENTS	SOFTWARE	SERVICES	PROPERTIES	NETFLOW	GROUPS
10 SERVICES EDIT SERVICES							
IP ADDRESS	PORT	PROTOCOL	NAME	STATUS	MONITORING		
alienvault (192.168.1.241)	22	tcp	ssh	-	No		
alienvault (192.168.1.241)	80	tcp	http	-	No		
alienvault (192.168.1.241)	443	tcp	https	-	No		
alienvault (192.168.1.241)	3306	tcp	mysql	-	No		
alienvault (192.168.1.241)	9390	tcp	gvmd	-	No		
SHOWING 1 TO 5 OF 5 SERVICES						< PREVIOUS 1 NEXT >	

Imagen 48: interfaz web OSSIM – Servicios del activo.

Referencia: Autor

Después ingresamos en la opción ‘Edit Services’, para la edición del monitoreo de los servicios correspondiente que contine el servidor. Esto depende de la criticidad, ya bien se podrían monitorear algunos servicios o todos a la vez, para activar el servicio seleccionamos ‘yes’ del apartado ‘Monitoring’ en cada uno de los servicios.

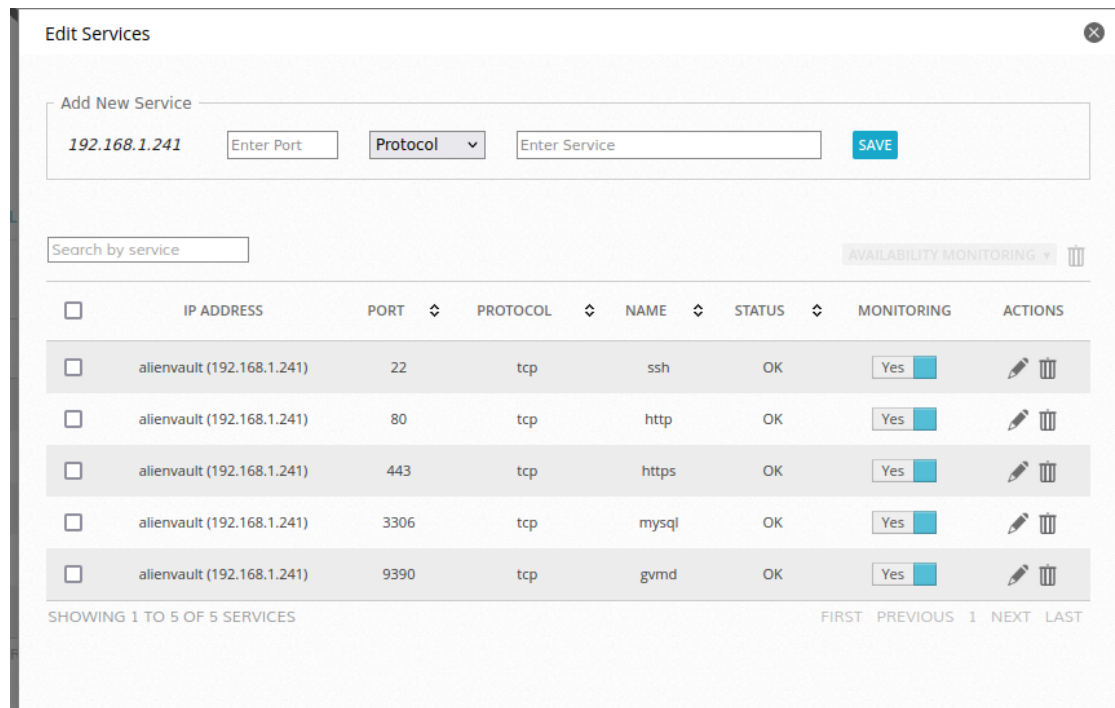


Imagen 49: interfaz web OSSIM – Habilitación de servicios del activo

Referencia: Autor

Al levantarse el monitoreo de los servicios, se actualizará la información de las estadísticas del activo.

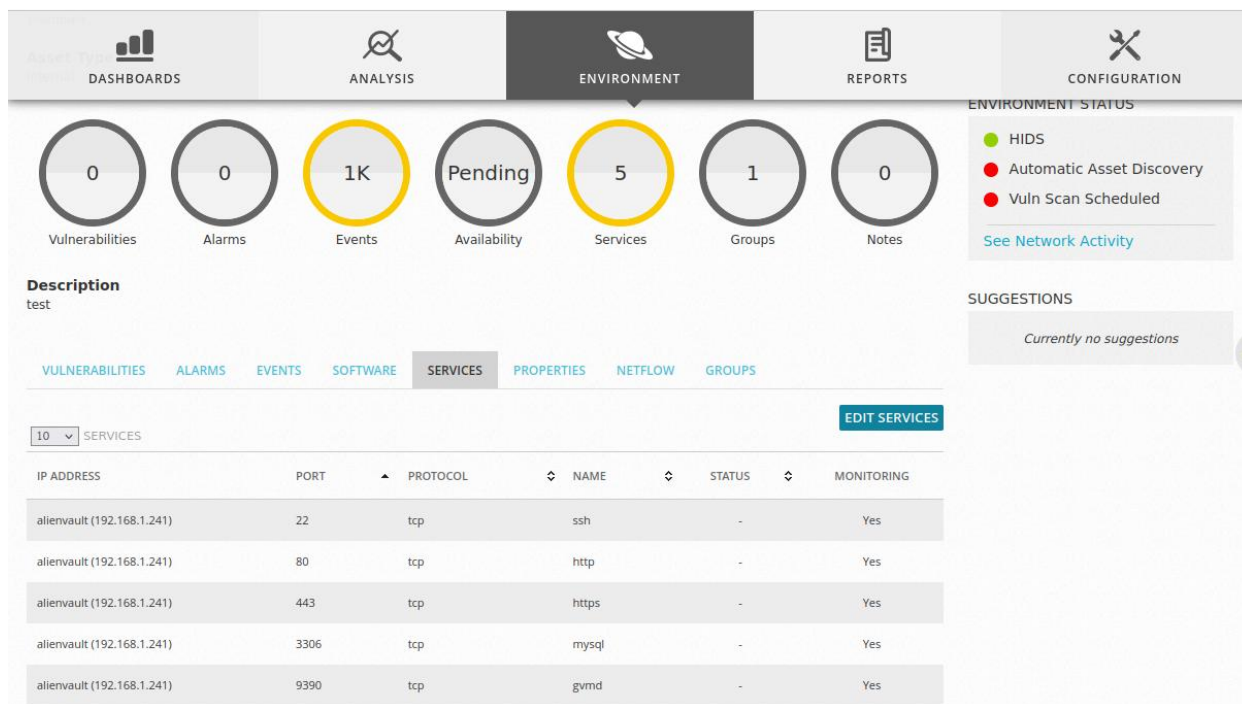


Imagen 50: interfaz web OSSIM – Actualización de información del activo.

Referencia: Autor

Previamente, nos vamos al apartado de ‘Enviroment’, en el apartado ‘Availability’, en este apartado se puede monitoriar los servicios previamente configurados.

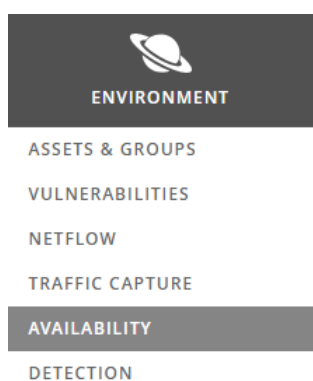


Figura 51: interfaz web OSSIM – Opción de acceso a la disponibilidad.

Referencia: Autor

Una vez ingresados en el apartado ‘Availability’, se nos desplegara la información de los activos que se encuentren monitorizados.

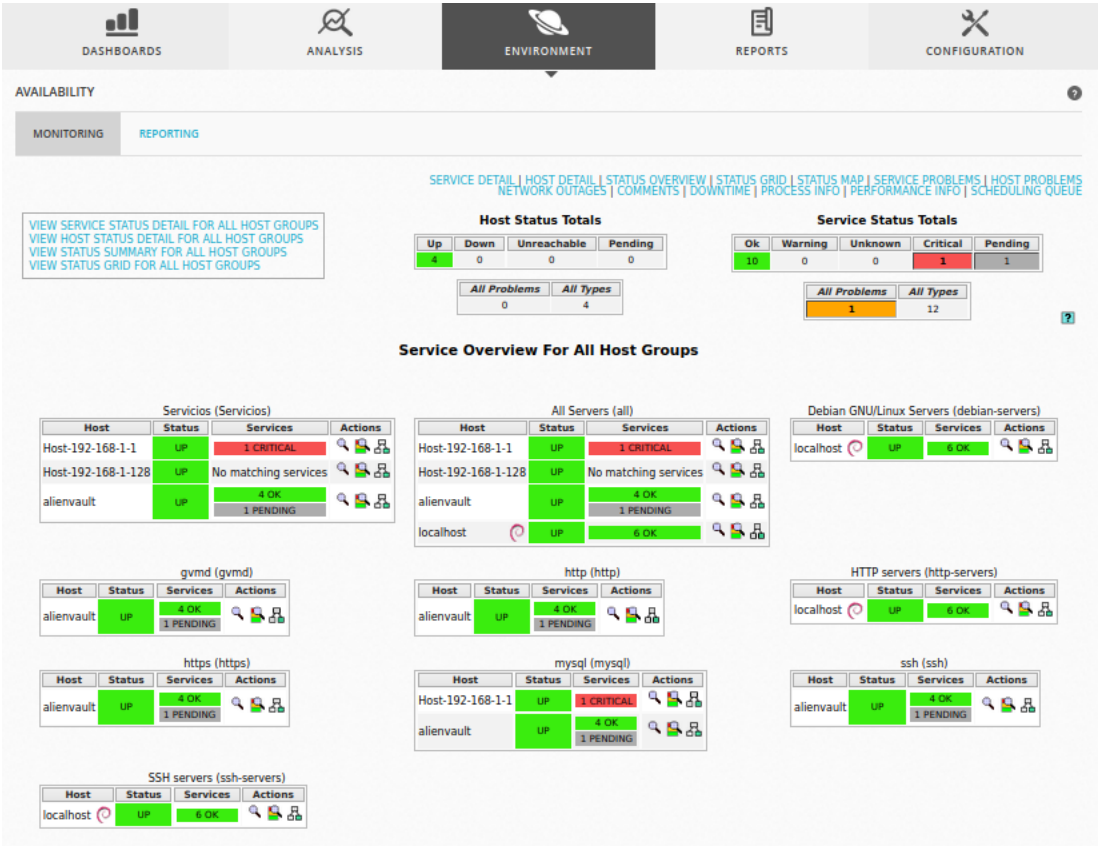


Imagen 52: interfaz web OSSIM – Monitoreo de disponibilidad de activos.

Referencia: Autor

La información obtenida, con su estado activo o inactivo se continuará actualizando mientras se sigan explorando nuevos activos. Para la revisión de las alertas, aquí se considera que el color verde indica que el servicio de un determinado activo se encuentra disponible o habilitado, y según su grado de criticidad, el color podrá ser gris, rojo, naranja o amarillo con la información referente al estado.

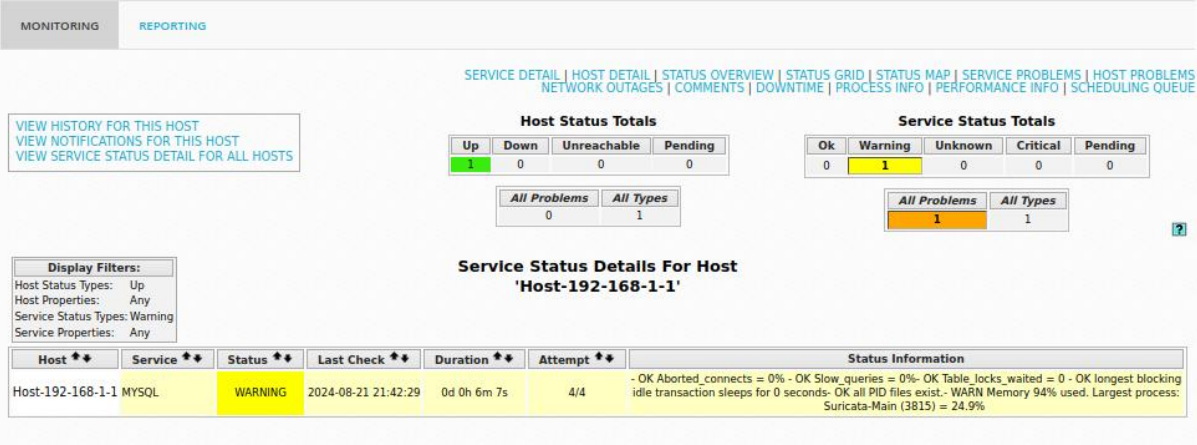


Imagen 53: interfaz web OSSIM – Estado del servicio de un activo.

Referencia: Autor

Al seguir agregando más activos, estos se verán reflejados en el apartado ‘Availability’ con el respectivo estado de criticidad.

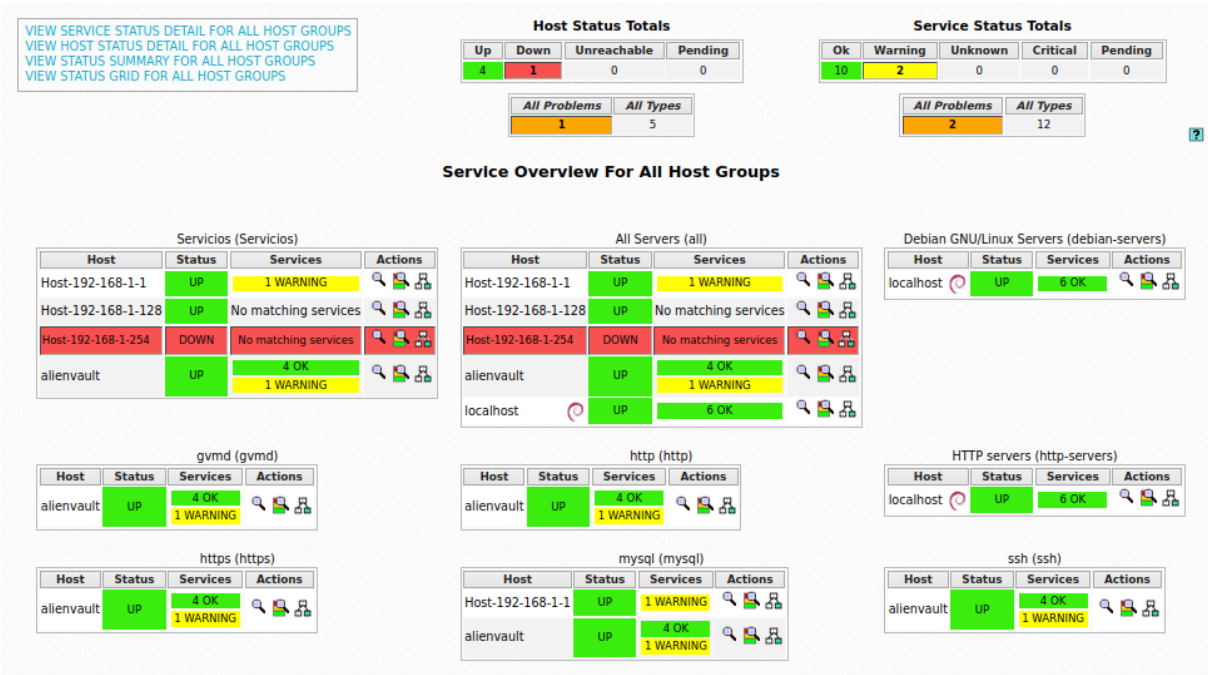


Imagen 54: interfaz web OSSIM – Monitoreo del estado de activos.

Referencia: Autor

Para poder obtener más información detallada sobre los activos que están siendo monitoreados, seleccionamos la opción ‘Service detail’, dentro mismo de ‘Monitoring’ en el apartado ‘Availability’, en el cual nos muestra un listado de información de los servicios.

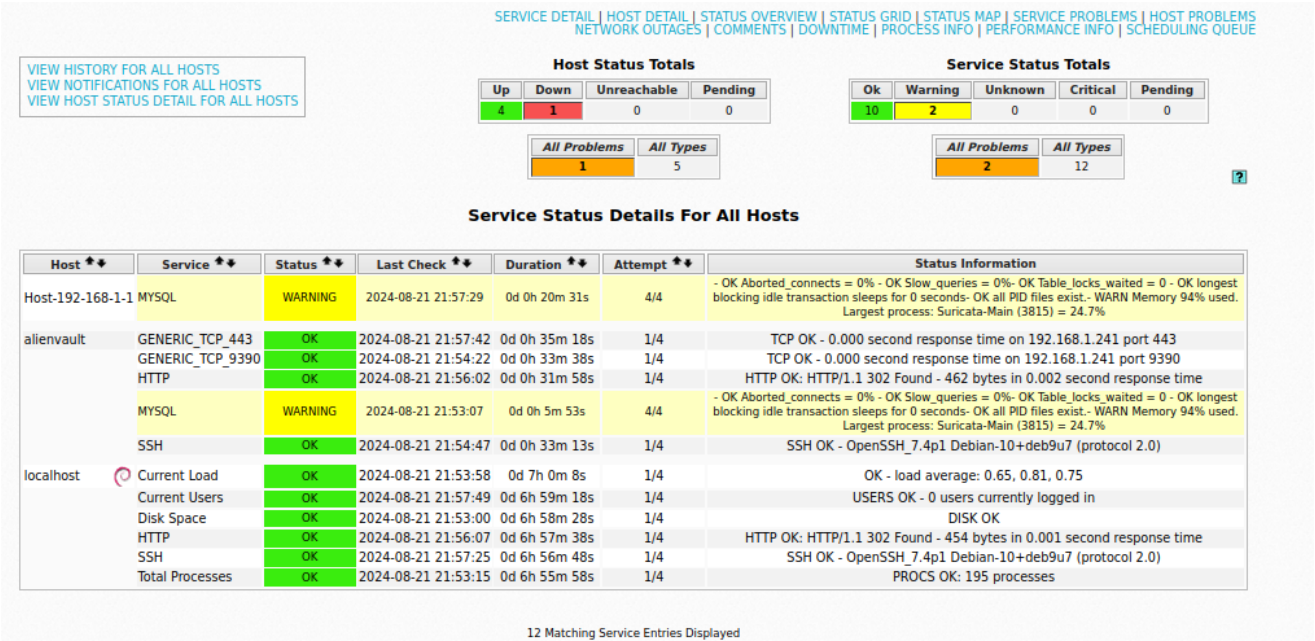


Imagen 55: interfaz web OSSIM – Detalle de servicios.

Referencia: Autor

Para nosotros obtener información de los (host), seleccionamos ‘Host detail’, en donde nos nuestros los equipos que se encuentran activos con su respectiva información sobre su última información de estado, su revisión y su duración.

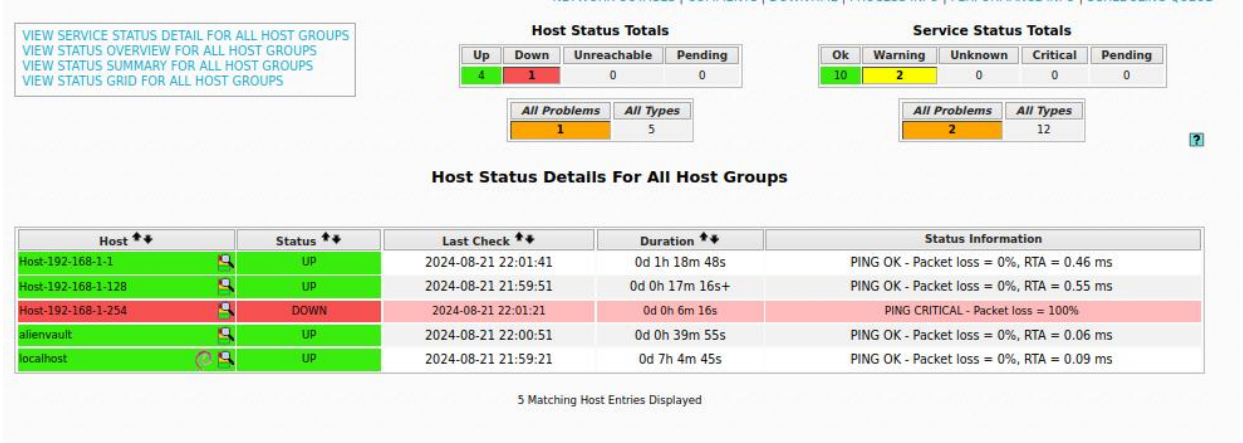


Imagen 56: interfaz web OSSIM – Detalle del estado de los servicios.

Referencia: Autor

Se puede también revisar los apartados: ‘Status overview’ (Descripción del estado), ‘Status grid’ (Malla de estado), ‘Status map’ (Mapa de estado), ‘Service problems’ (Problemas de servicio), ‘Host problems’ (Problemas de equipos), ‘Network outages’ (Interrupciones en la red), ‘Performance info’ (Información de funcionamiento), ‘Scheduling queue’ (Lista de programación), ‘Comments’ (Comentarios), ‘Downtime’ (Tiempo muerto), y ‘Process info’ (Información de procesos).

Si se presentara algún problema con un servidor (host), se puede visualizar en el apartado ‘Monitoring’, en el cual si hay un mensaje cualitativo de ‘Down’ (Caído o inactivo) se mostrara este de color rojo.

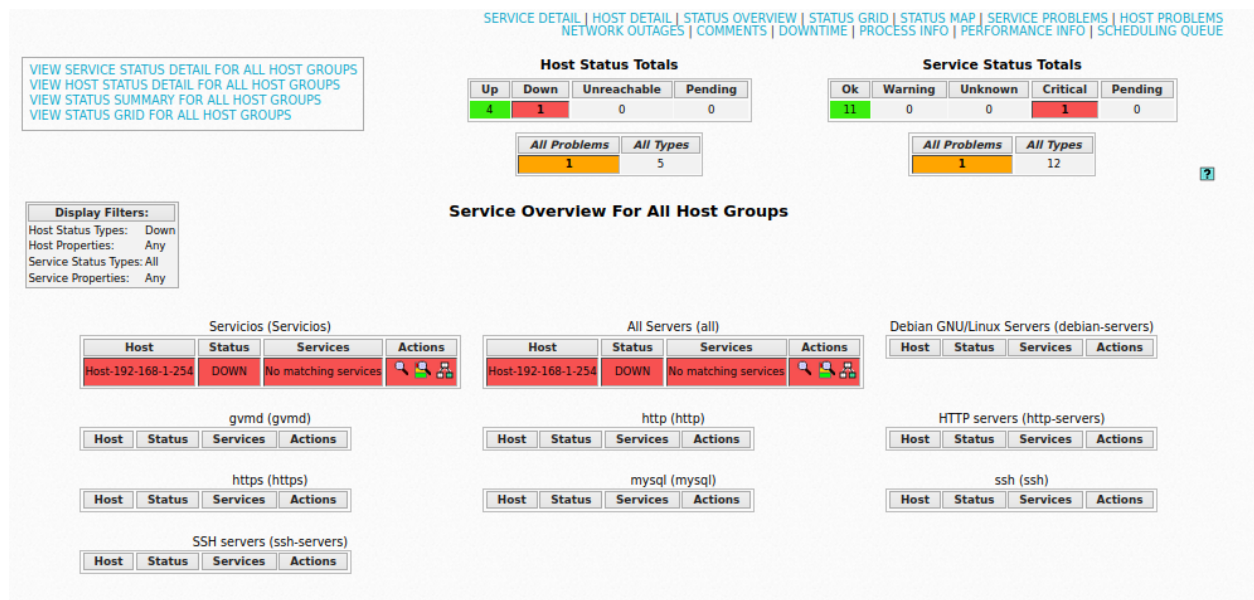


Imagen 57: interfaz web OSSIM – Monitoreo y revisión de disponibilidad.

Referencia: Autor

Dentro del apartado ‘Host detail’ (Detalle del equipo) se puede hacer la validar los resultados del monitoreo.

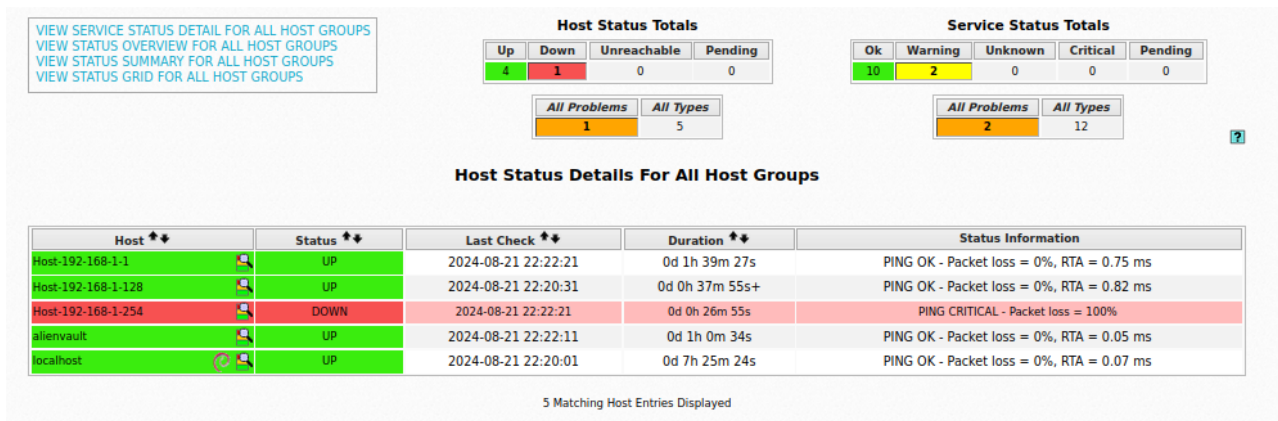


Imagen 58: interfaz web OSSIM – Detalle del estado del activo detenido.

Referencia: Autor

Dentro del apartado ‘Availability’, hay una función que permite la generación de reportes a nivel de dispositivos, grupos de servicios o grupos de dispositivos y servicios, para generar dicho reporte nos vamos donde dice ‘Reporting’ este reporte nos permite obtener un porcentaje de disponibilidad de acuerdo a un determinado tiempo, y esto también depende de que tan requeridos sean los reportes, lo primero es acceder a ‘Trends’ para seleccionar el tipo de informe ya sea por equipo (host) o por servicio (service).

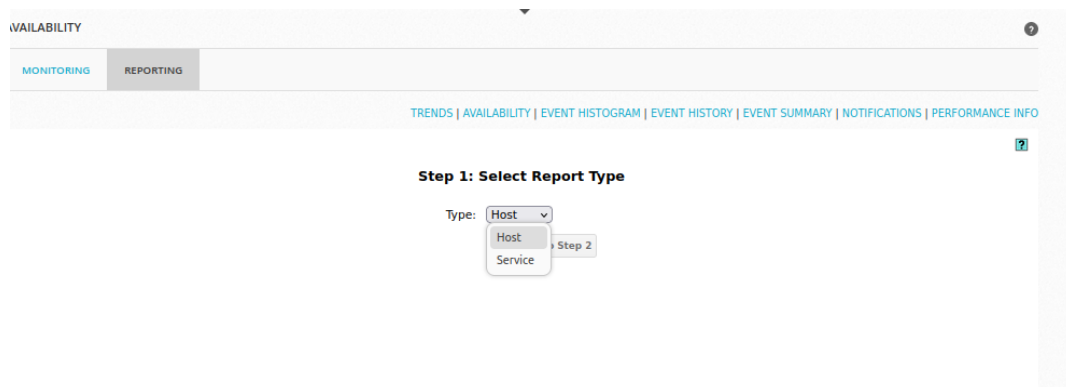


Imagen 59: interfaz web OSSIM – Selección del tipo de informe.

Referencia: Autor

Después de seleccionar el tipo de informe se selecciona el equipo o servicio para generar el informe correspondiente.

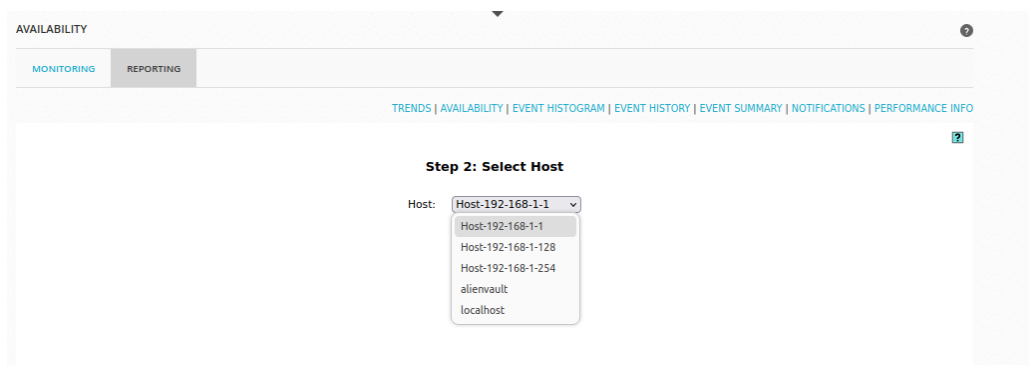


Imagen 60: interfaz web OSSIM – selección del host del reporte.

Referencia: Autor

El siguiente punto es especificar el periodo que tendrá el reporte o si será personalizado, y después de determinar eso se procede a crear el reporte.

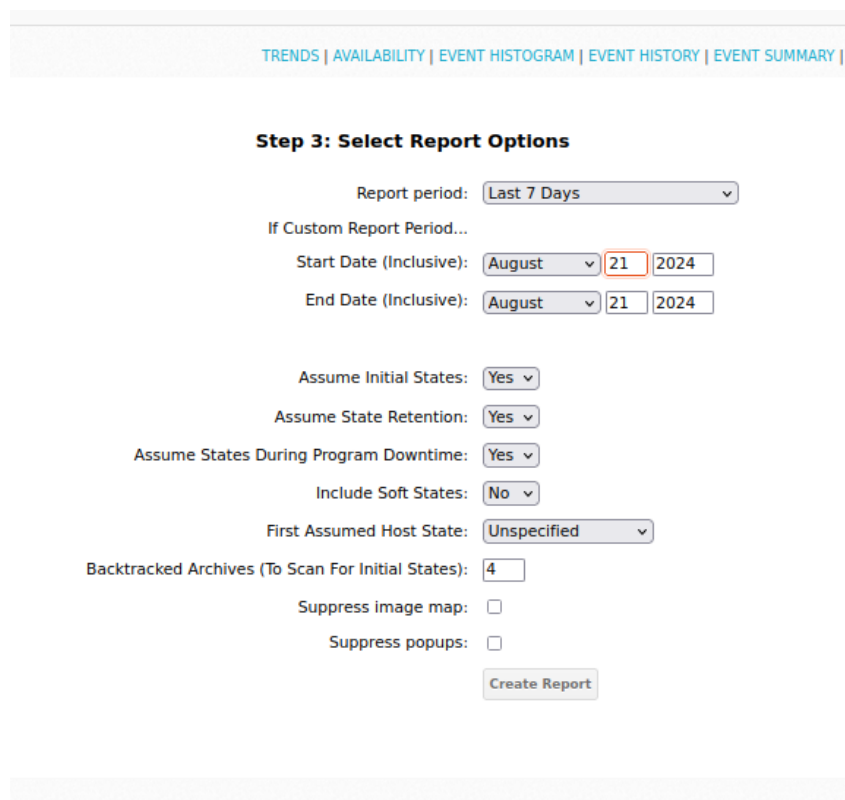


Imagen 61: interfaz web OSSIM – Selección de opciones de reporte.

Referencia: Autor

Después de la creación del reporte, en este se puede visualizar los porcentajes del estado inicial de los servicios dentro del servidor o host selecciono. Como el reporte creado es de un lapso periodo de tiempo el grafico no mostrara mayores cambios, solo considerando los indicadores ‘Up’ (Activo), ‘Down’ (Inactivo), ‘Unreachable’ (Inalcanzable), ‘Indeterminate’ (Indeterminado).

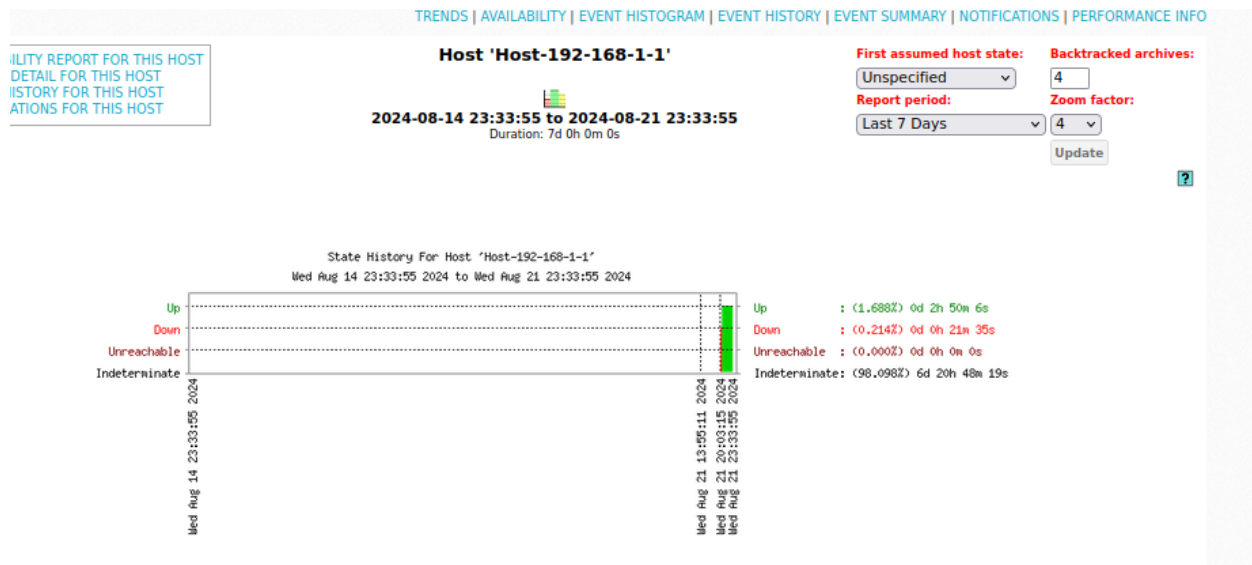


Imagen 62: interfaz web OSSIM – Informes de disponibilidad.

Referencia: Autor

9.4 Gestión de vulnerabilidades

Para poder gestionar las vulnerabilidades nos debemos ir a ‘Environment’ en el apartado ‘Vulnerabilidades’.

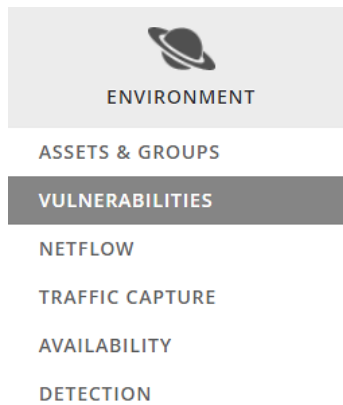


Imagen 63: interfaz web OSSIM – Opción de acceso a vulnerabilidades

Referencia: Autor

Ya dentro de esta opción, tendremos acceso al tablero general de configuraciones para la administración y generación de reportes.

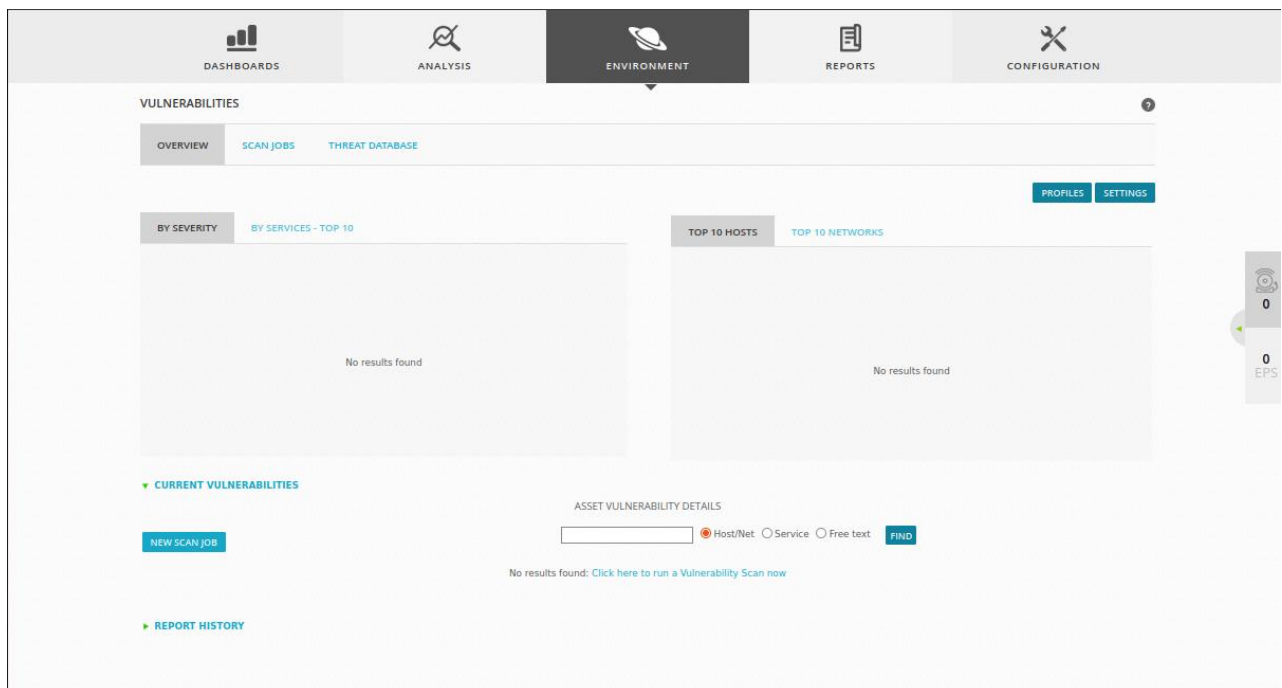


Imagen 64: interfaz web OSSIM – Tablero general de vulnerabilidades.

Referencia: Autor

En la pestaña ‘Scan jobs’ (Trabajos de escaneo) en este apartado se puede llevar a cabo la programación de escaneo de vulnerabilidades de acuerdo a los activos existentes y esto también puede depender de los requisitos disponibles al momento de realizar dicho proceso.

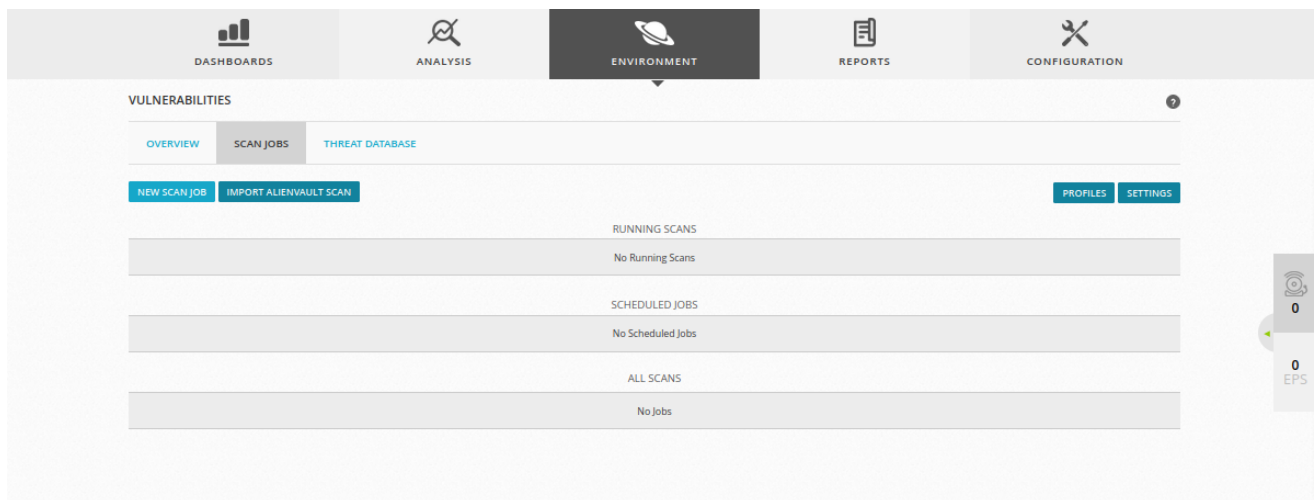


Imagen 65: interfaz web OSSIM – Trabajos de escaneo.

Referencia: Autor

Para poder realizar un escaneo en este apartado nos vamos donde dice ‘New scan jobs’ ya dentro de este apartado nos mostrara una serie de parámetros para llenar y poder realizar el escaneo de vulnerabilidades del activo que vallamos a seleccionar.

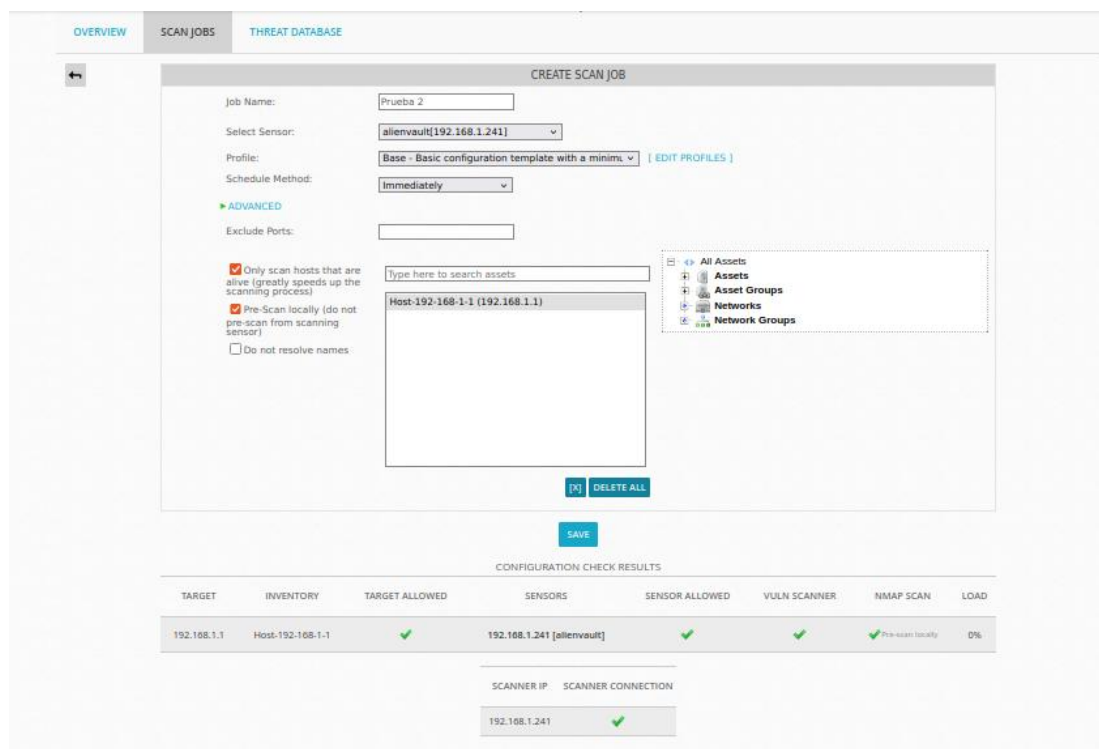


Imagen 66: interfaz web OSSIM – Creación del trabajo de escaneo.

Referencia: Autor

Después de guardar los cambios (Save) la creación de este trabajo que hemos realizado se ejecutara automáticamente, es decir que el escaneo se realizara de manera automática al activo que hemos seleccionado.

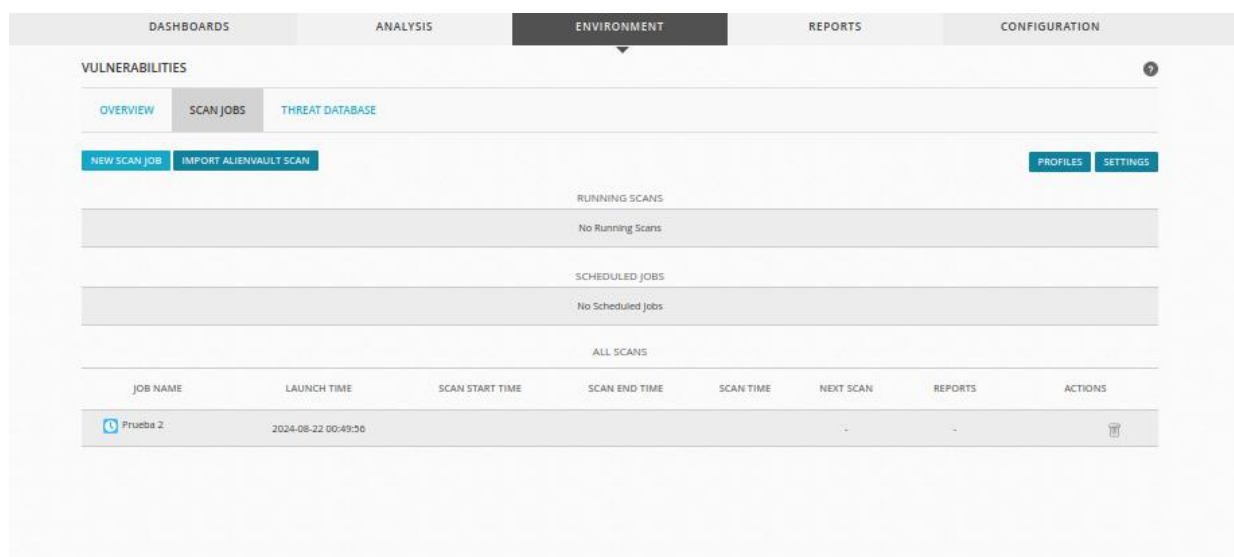


Imagen 67: interfaz web OSSIM – Trabajo de escaneo programado.

Referencia: Autor

Al haber programado este trabajo de escaneo, tendremos que esperar el inicio del proceso para que presente su reporte del escaneo de vulnerabilidades.

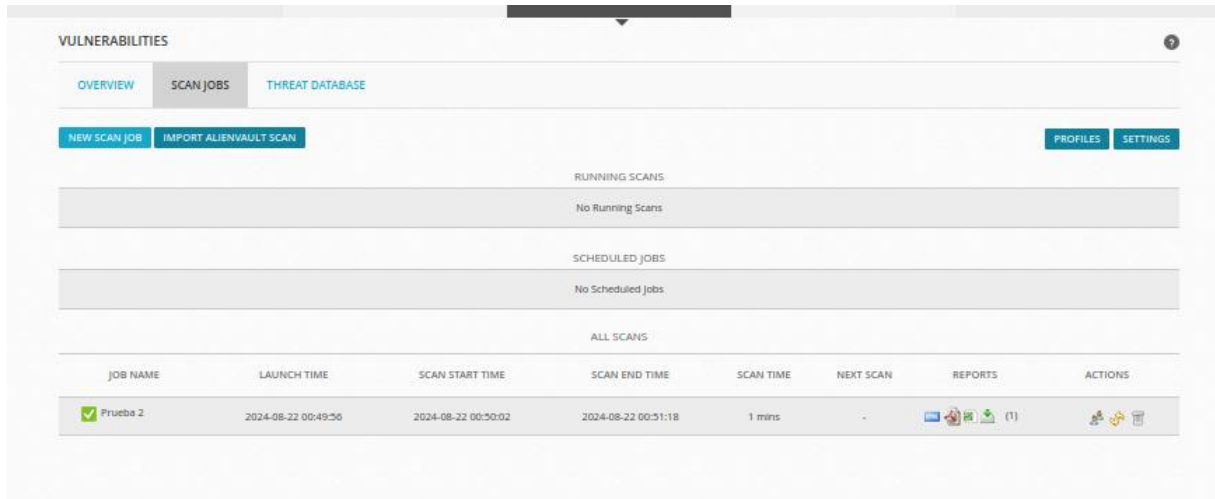


Imagen 68: interfaz web OSSIM – Finalización del trabajo de escaneo.

Referencia: Autor

Este trabajo de escaneo programado mostrara un resumen preliminar referente a la detección inicial de vulnerabilidades, adema de incluir reporte por puertos.

En el reporte generado se ve un grafico en forma de pastel en el cual se puede ver el estado general de vulnerabilidades, donde el tipo de vulnerabilidades se representa por categorías y colores.

- Vulnerabilidades criticas (Critical)
- Vulnerabilidades altas (High)
- Vulnerabilidades medias (Medium)
- Vulnerabilidades bajas (Low)
- Vulnerabilidades informativas (Info)

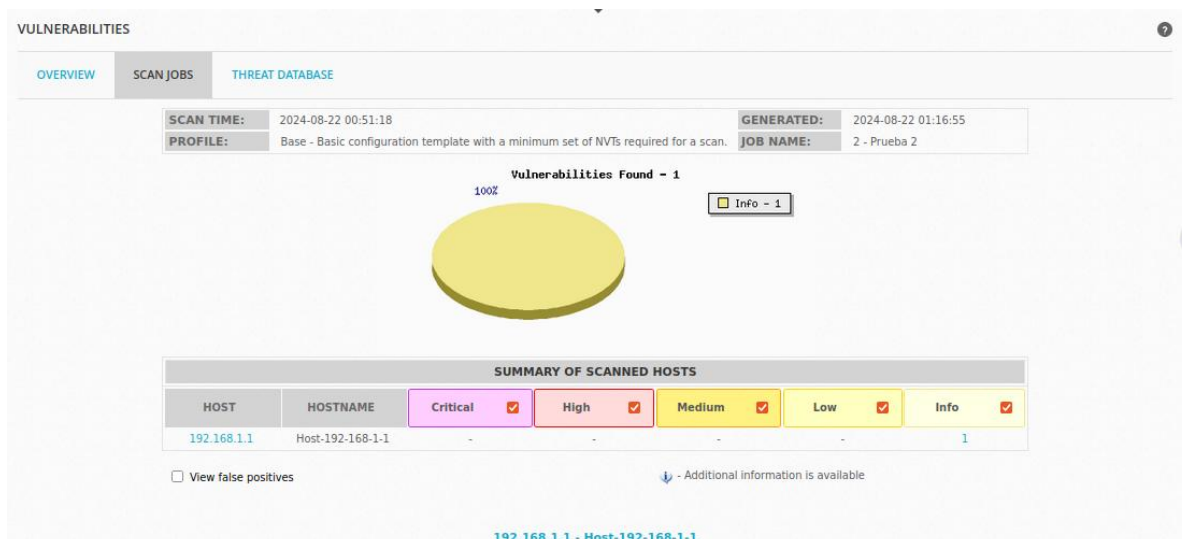


Imagen 69: interfaz web OSSIM – Resultados preliminares de escaneo 1

Referencia: Autor

VULNERABILITY NAME	VULNERABILITY ID	SERVICE	SEVERITY
Hostname Determination Reporting	108449	general (tcp)	Info
References: Vulnerability Detection Result: Hostname determination for IP 192.168.1.1: Hostname Source 192.168.1.1 IP-address CVSS Base Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N Summary: The script reports information on how the hostname of the target was determined. CVSS Base Score: 0.0	Family name: Service detection Category: end Created: 2018-07-05T06:03:26Z Modified: 2018-11-19T11:11:31Z		

Imagen 70: interfaz web OSSIM – Resultados preliminares de escaneo 2

Referencia: Autor

De acuerdo con el diagrama de tipo pastel, aquí muestra el grado de severidad de las vulnerabilidades encontradas de acuerdo con el activo analizado.

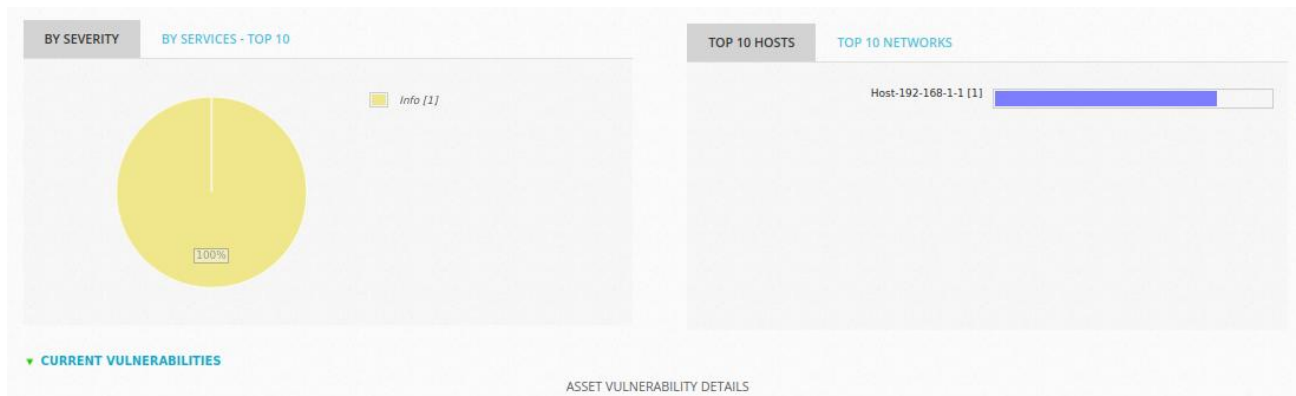


Imagen 71: interfaz web OSSIM – Diagrama de severidad del activo seleccionado.

Referencia: Autor

Aquí la categorización de los colores se establece de la siguiente manera:

- Vulnerabilidades criticas CRIT (Morado)
- Vulnerabilidades altas HIGH (Rojo)
- Vulnerabilidades medias MEDI (Amarillo)
- Vulnerabilidades bajas LOW (Azul)
- Vulnerabilidades INFO (Verde)

El resultado del escaneo de vulnerabilidades aquí el sistema exporta la información en los formatos ‘html’, ‘pdf’, y ‘xlsx’ respectivamente.

NEW SCAN JOB					☒ Host/Net ☐ Service ☐ Free text FIND				
HOST - IP	DATE/TIME	OWNER	PROFILE	CRIT	HIGH	MEDI	LOW	INFO	
All	-	-	-	0	0	0	0	1	
Host-192-168-1-1 (192.168.1.1)	-	-	-	0	0	0	0	1	
	2024-08-22 00:51:18	admin	Base	0	0	0	0	1	
	2024-08-22 00:51:18	admin	Full and fast	0	0	0	0	1	
	2024-08-22 00:51:18	admin	System Discovery	0	0	0	0	1	

Imagen 72: interfaz web OSSIM – Detalles de vulnerabilidades de activos.

Referencia: Autor

Para configurar un trabajo de escaneo programado que se ejecute un cierto tiempo, ingresamos a la pestaña ‘Scan Jobs’ en la sección de ‘Vulnerabilities’ en la opción ‘New scan Job’ donde aquí configuraremos un nuevo trabajo de escaneo para un determinado activo de la red, en el cual el proceso de ‘scanning’ será para un escaño de un activo que requiera un escaneo diario.

CREATE SCAN JOB

Job Name:

Activo critico

Select Sensor:

alienvault[192.168.1.241]

Profile:

Base - Basic configuration template with a minimu

[EDIT PROFILES]

Schedule Method:

Daily

BEGIN IN

Year

2024

Month

8

Day

22

FREQUENCY

Every

2

 day(s)

TIME

2

 Minutes

0

ADVANCED

Exclude Ports:

☒ Only scan hosts that are alive (greatly speeds up the scanning process)

☒ Pre-Scan locally (do not pre-scan from scanning sensor)

☐ Do not resolve names

Type here to search assets

Host-192-168-1-128 (192.168.1.128)

All Assets

Assets

Asset Groups

Networks

Network Groups

[X] DELETE ALL

SAVE

CONFIGURATION CHECK RESULTS

TARGET	INVENTORY	TARGET ALLOWED	SENSORS	SENSOR ALLOWED	VULN SCANNER	NMAP SCAN	LOAD
192.168.1.128	Host-192-168-1-128	✓	192.168.1.241 [alienvault]	✓	✓	✓ Pre-scan locally	0%

SCANNER IP

SCANNER CONNECTION

192.168.1.241

✓

Imagen 73: interfaz web OSSIM – Programación de trabajo de escaneo.

Referencia: Autor

Al guardar los cambios, en el panel de trabajos se puede evidenciar que el estado está habilitado para realizar un escaneo programado.

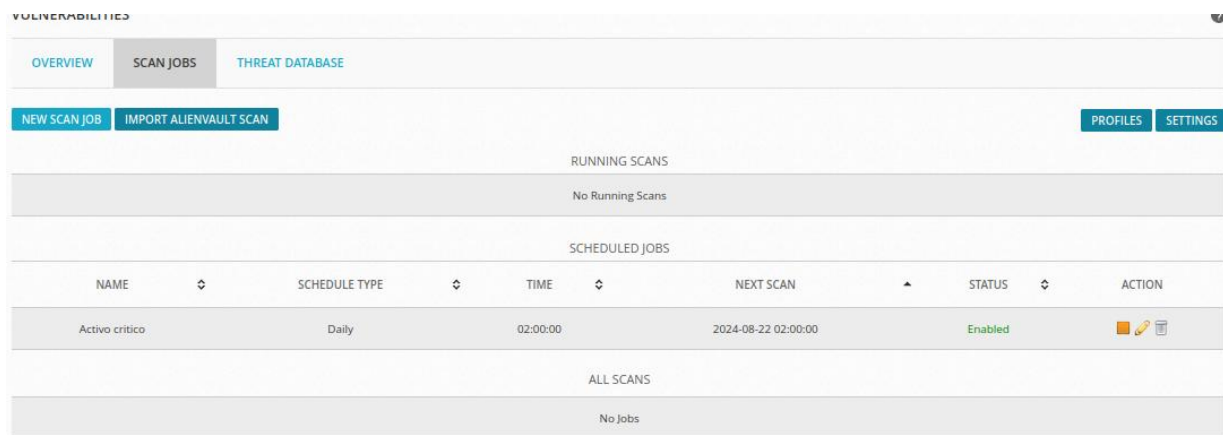


Imagen 74: interfaz web OSSIM – Programación automática del trabajo.

Referencia: Autor

9.4 Gestión de riesgo

La herramienta SIEM, gestiona el riesgo al que esta expuesto cada uno de nuestros activos de la red, esta gestión la hace mediante un IDS (Intrusion Detection System) o más conocido como Sistema de detección de intrusos, aunque el sistema no bloquea el tráfico anómalo que se recibe, con lo que el sistema alerta de estos posibles eventos de riesgos. Para poder gestionar el riesgo, nos vamos a ‘Analysis’ y seleccionamos la opción ‘Security events (SIEM)’.

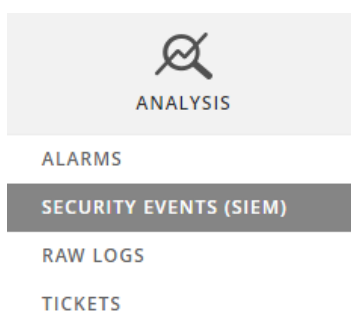


Imagen 75: interfaz web OSSIM – Acceso a eventos de seguridad.

Referencia: Autor

Al ingresa a esta ventana se nos despliega una lista de incidencias que están relacionada a la seguridad, en la cual nosotros podremos verificar información de diversos eventos que han sido detectado por el OSSIM, estos eventos nos permiten conocer parámetros de nombre del evento en cuestión, el origen, la fecha, el destino y el nivel de riesgo asociado. Estos eventos se pueden mostrar por mes, semanas, días o por un determinado rango de tiempo.

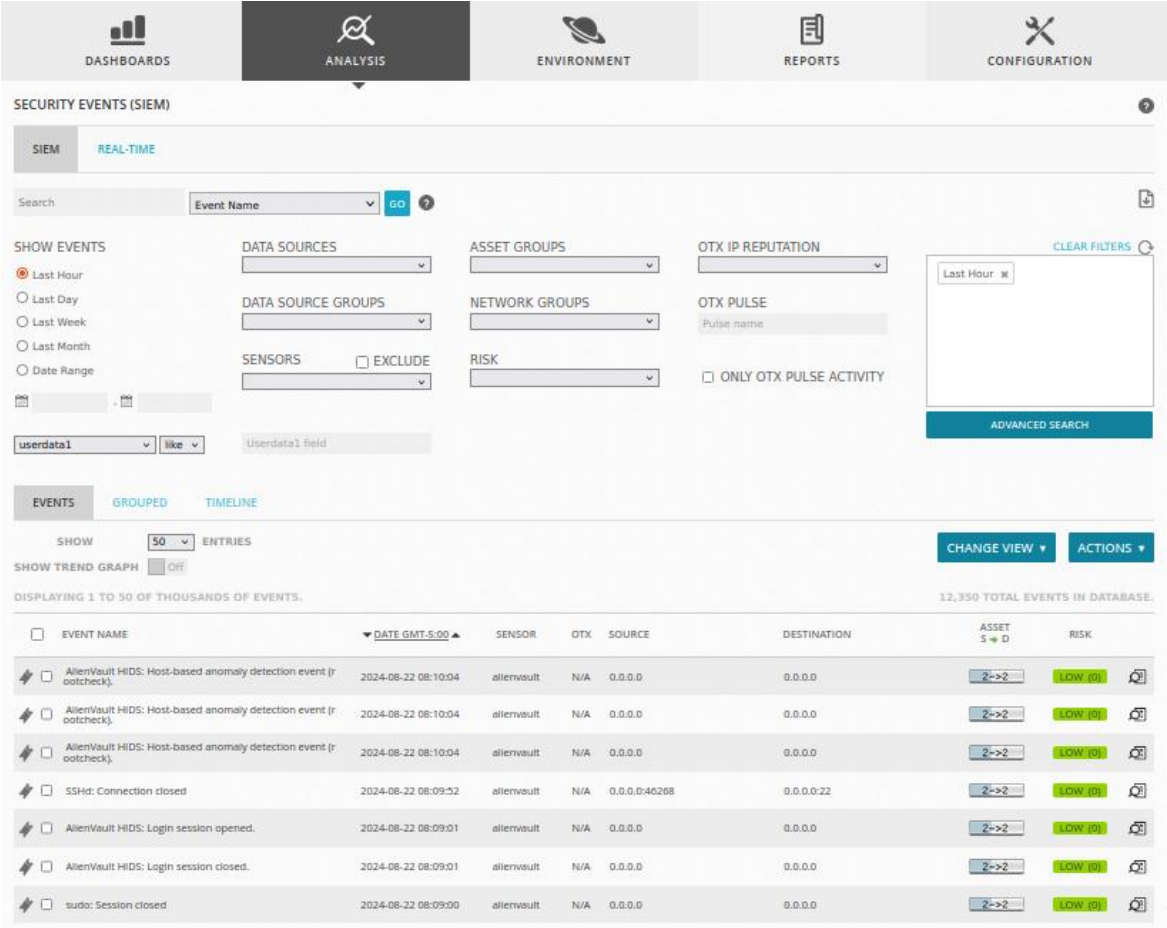


Imagen 76: interfaz web OSSIM – Eventos de seguridad SIEM.

Referencia: Autor

En el apartado donde dice ‘Real Time’ en la sección de ‘Security events (SIEM)’, aquí podemos ver en tiempo real lo que es la captura del tráfico, que también nos muestra intentos fallidos de conexión de un usuario inexistente dentro de un activo de la red.

DASHBOARDS	ANALYSIS	ENVIRONMENT	REPORTS	CONFIGURATION
------------	----------	-------------	---------	---------------

SECURITY EVENTS (SIEM)

SIEM

REAL-TIME

PAUSE

Done. [0 new rows]

DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	CTX	SOURCE IP	DEST IP
2024-08-22 08:13:55	SSHd: Connection closed	0	ssh	allenvault	N/A	0.0.0.0:47278	0.0.0.0:22
2024-08-22 08:13:29	SSHd: Connection closed	0	ssh	allenvault	N/A	allenvault:55938	0.0.0.0:22
2024-08-22 08:13:13	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:12	sudo: Session closed	0	sudo	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:12	SSHd: Session disconnected	0	ssh	allenvault	N/A	allenvault:55912	allenvault:22
2024-08-22 08:13:11	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:10	SSHd: Session disconnected	0	ssh	allenvault	N/A	allenvault:55910	allenvault:22
2024-08-22 08:13:10	sudo: Session opened	0	sudo	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	sudo: Session closed	0	sudo	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	sudo: Session opened	0	sudo	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	sudo: Session closed	0	sudo	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	allenvault	N/A	0.0.0.0	0.0.0.0
2024-08-22 08:13:09	AlienVault HIDS: Login session opened.	0	AlienVault HIDS-authentication_success	allenvault	N/A	0.0.0.0	0.0.0.0

FILTERS

Source IP:

Destination IP:

Imagen 77: interfaz web OSSIM – Lista de eventos en tiempo real.

Referencia: Autor

Al ingresar a dicho evento por autenticación aquí podemos verificar el detalle del evento, con información relevante, que contiene fecha, la dirección IP, el ID del tipo de evento, la categoría, el protocolo, el tipo de producto, el origen de datos e información adicional al evento. También en este apartado se muestra la fiabilidad, prioridad y riesgo analizado.

DASHBOARDS

ANALYSIS

ENVIRONMENT

REPORTS

CONFIGURATION

SIEM

REAL-TIME

Security Events

AlienVault HIDS: Login session closed.

NEXT >

AlienVault HIDS: Login session closed.

ACTIONS

DATE

2024-08-22 08:21:02 GMT-5:00

ALIENVault SENSOR

alienvault [192.168.1.241]

DEVICE IP

192.168.1.241 [eth0]

EVENT TYPE ID

5502

UNIQUE EVENT ID#

608911ef-a44b-000c-29e9-37d060aca82c

PROTOCOL

TCP

CATEGORY

Authentication

SUB-CATEGORY

Logout

DATA SOURCE NAME

AlienVault HIDS-syslog

DATA SOURCE ID

7001

PRODUCT TYPE

Operating System

ADDITIONAL INFO

N/A

PRIORITY

1

RELIABILITY

1

RISK

LOW (0)

OTX INDICATORS

0

SOURCE

0.0.0.0

Hostname: N/A

Location: N/A

MAC Address: N/A

Context: N/A

Port: 0

Asset Groups: N/A

Latest update: N/A

Networks: N/A

Username & Domain: N/A

Logged Users: N/A

Asset Value: 2

OTX IP Reputation: No

SERVICE

PORT

PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES

FIRST PREVIOUS NEXT LAST

DESTINATION

0.0.0.0

Hostname: N/A

Location: N/A

MAC Address: N/A

Context: N/A

Port: 0

Asset Groups: N/A

Latest update: N/A

Networks: N/A

Username & Domain: N/A

Logged Users: N/A

Asset Value: 2

OTX IP Reputation: No

SERVICE

PORT

PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES

FIRST PREVIOUS NEXT LAST

USERNAME

USERDATA1

USERDATA2

USERDATA3

USERDATA5

root

/var/log/auth.log

Login session closed.

pam.syslog.

3

RAW LOG

AV - Alert - "i724332862" --> RID: "5502"; RL: "3"; RG: "pam.syslog."; RC: "Login session closed."; USER: "None"; SRCIP: "None"; HOSTNAME: "alienvault"; LOCATION: "/var/log/auth.log"; EVENT: "[INIT]Aug 22 08:21:00 alienvault sudo: pam_unix(sudo:session): session closed for user root[END]";

Imagen 78: interfaz web OSSIM – Detalle del evento suscitado.

Referencia: Autor

Dentro donde dice SIEM, aquí podemos visualizar que se puede incluir un tipo de filtrado según sea necesario las necesidades de los eventos suscitados, esto lo podemos ver en el apartado de ‘Grouped’ aquí podemos visualizar estos eventos agrupados por tipo de evento.

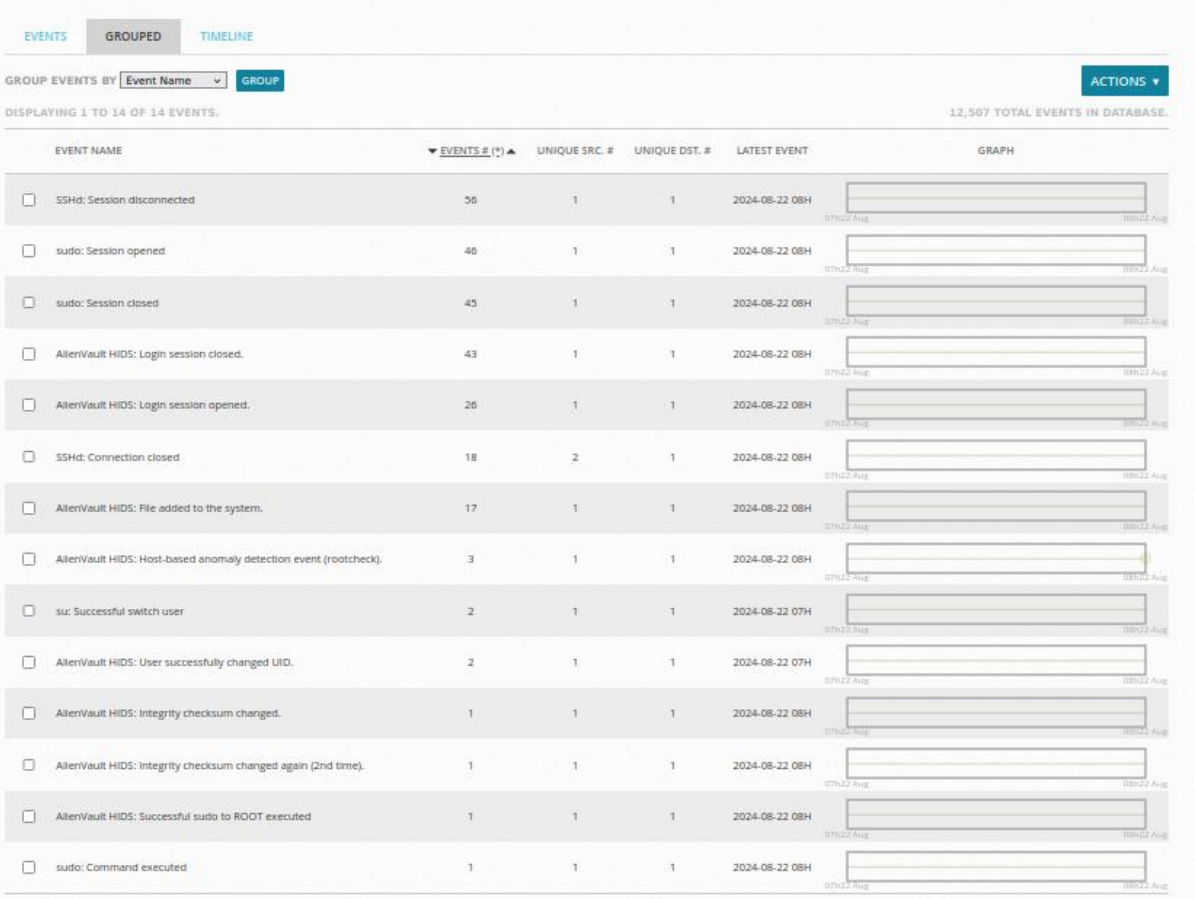


Imagen 79: interfaz web OSSIM – Agrupación de eventos.

Referencia: Autor

La siguiente ventana es ‘Timeline’, en esta nos muestra donde se puede determinar la resolución de la línea de tiempo sobre eventos que se hayan suscitados.

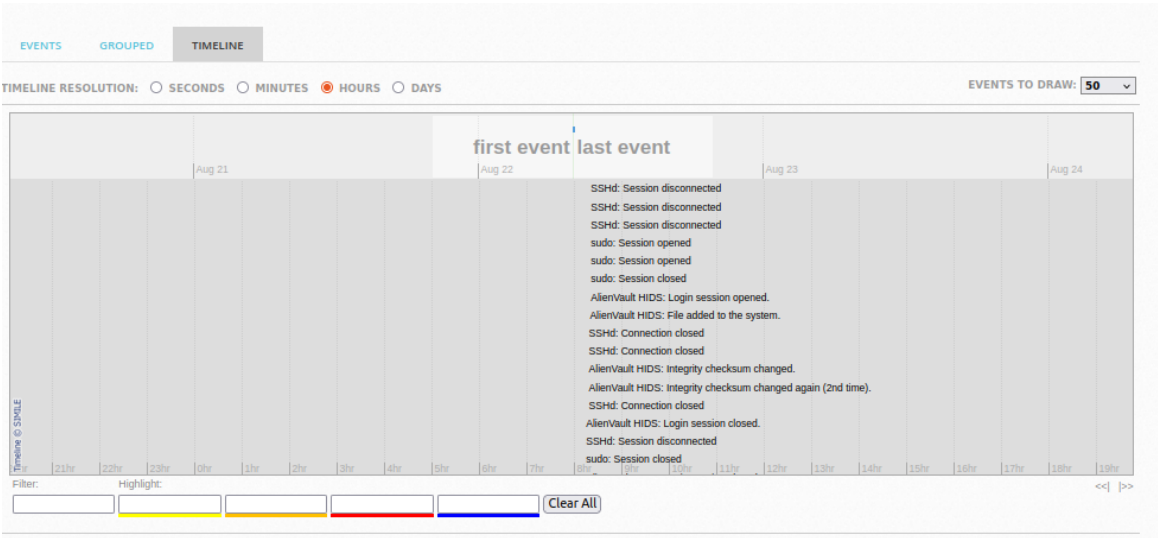


Imagen 80: interfaz web OSSIM – Línea de tiempo de eventos.

Referencia: Autor

Para nosotros poder aplicar un filtrado de un evento en específico de la red en la opción ‘SIEM’ que corresponde a ‘Security events (SIEM)’, aquí ingresamos la dirección IP de origen y el tiempo para verificar la cantidad de eventos que puedan ocurrir en el activo (host). En lo que nos muestra un listado general de eventos y incidentes con un nivel LOW (un riesgo bajo).

EVENTS

GROUPED

TIMELINE

SHOW

50

ENTRIES

SHOW TREND GRAPH

Off

CHANGE VIEW

ACTIONS

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.

12,972 TOTAL EVENTS IN DATABASE.

☐	EVENT NAME	▼ DATE GMT-5:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
☐	sudo: Command executed	2024-08-22 08:34:12	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	su: Successful switch user	2024-08-22 08:32:04	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	su: Successful switch user	2024-08-22 08:32:04	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 08:17:16	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	su: Successful switch user	2024-08-22 07:58:27	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	su: Successful switch user	2024-08-22 07:58:27	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 02:00:18	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 02:00:18	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 02:00:02	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 01:51:34	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 01:51:11	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 01:48:52	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 01:34:11	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	su: Successful switch user	2024-08-22 01:32:04	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	su: Successful switch user	2024-08-22 01:32:04	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 01:17:10	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)
☐	sudo: Command executed	2024-08-22 00:52:09	alienvault	N/A	0.0.0.0	0.0.0.0	2→2	LOW (0)

Imagen 81: interfaz web OSSIM – Eventos filtrados de un activo.

Referencia: Autor

9.5 Gestión de alarmas y eventos

Al inicio de la interfaz web del OSSIM, se tiene un ‘banner’ al lado derecho de la pantalla principal que nos indica un breve resumen sobre las alarmas que se encuentran activas o que aún no han sido resueltas.

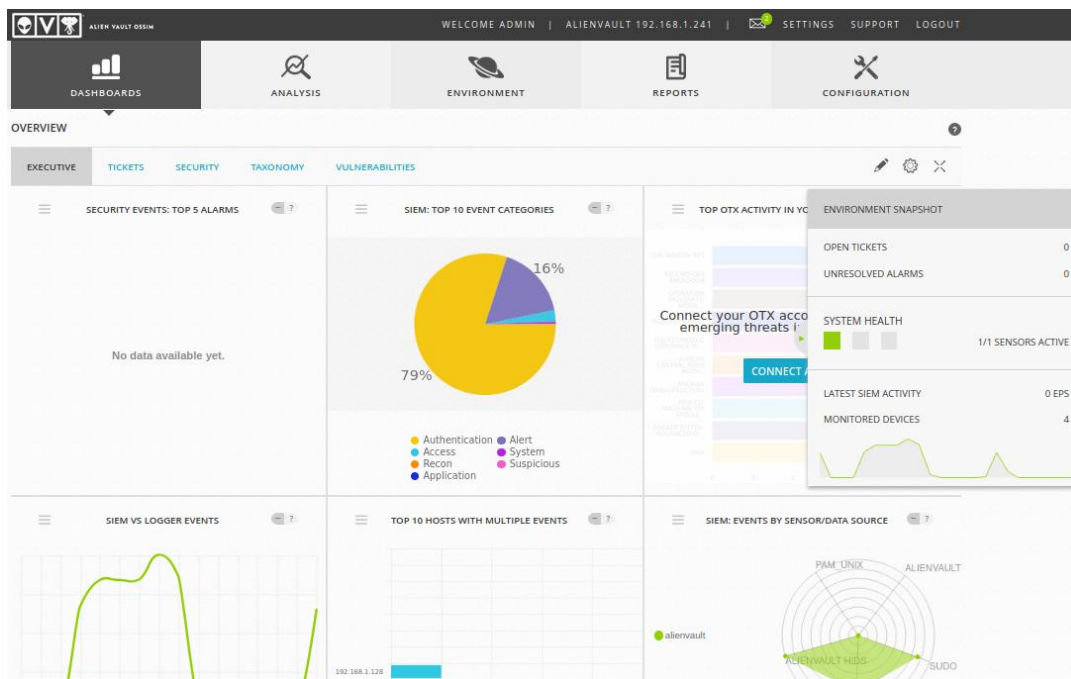


Imagen 82: interfaz web OSSIM – Banner de alarmas.

Referencia: Autor

Para poder acceder a las configuraciones de las alarmas nos ingresamos en la ventanita ‘Analysis’, en el apartado ‘Alarma’ (Alarmas).

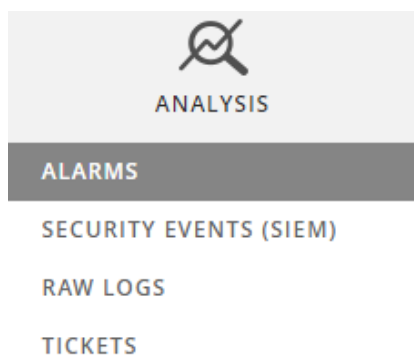


Imagen 83: interfaz web OSSIM – Opción de alarmas.

Referencia: Autor

Ya dentro de este apartado se puede ver la información con todas las alarmas generadas.

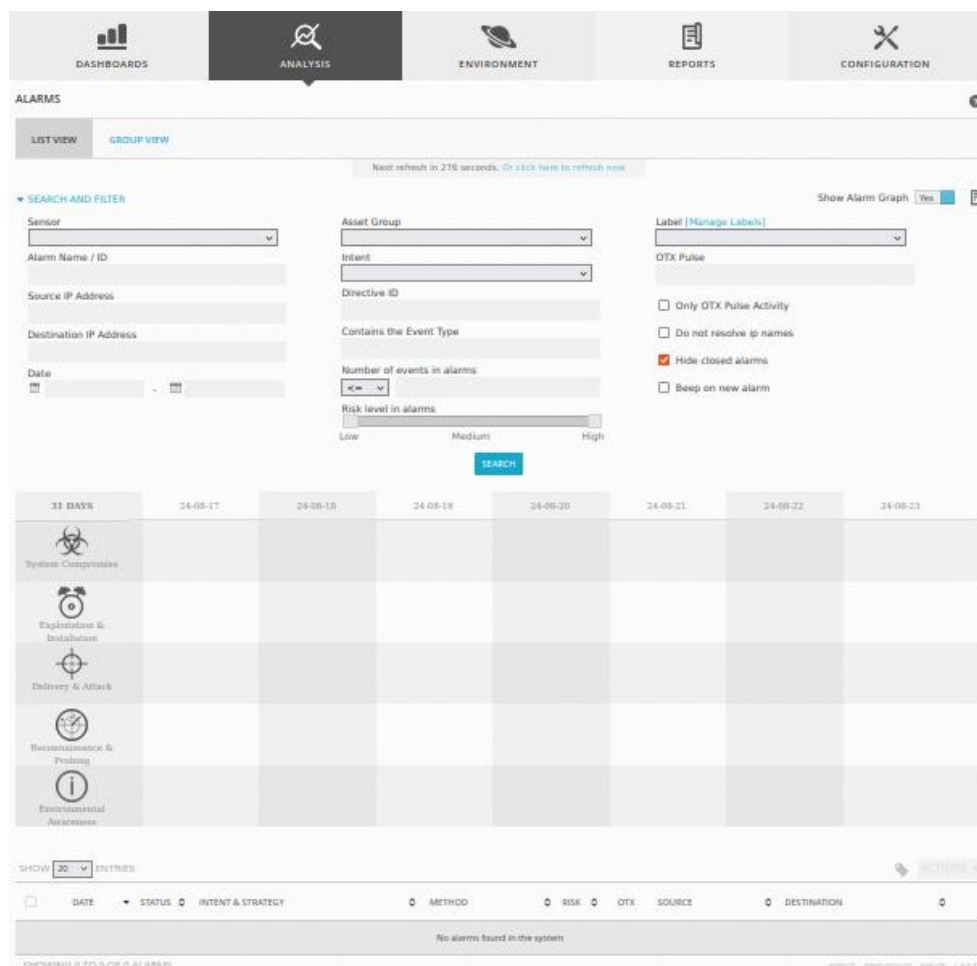


Imagen 84: interfaz web OSSIM – Vista de la lista de alarmas.

Referencia: Autor

También se puede visualizar el listado de las alarmas de manera agrupada en el apartado ‘Group view’ (Vista agrupada), aunque de momento no se visualiza ninguna alarma ya que no se han realizado configuración de ellas.

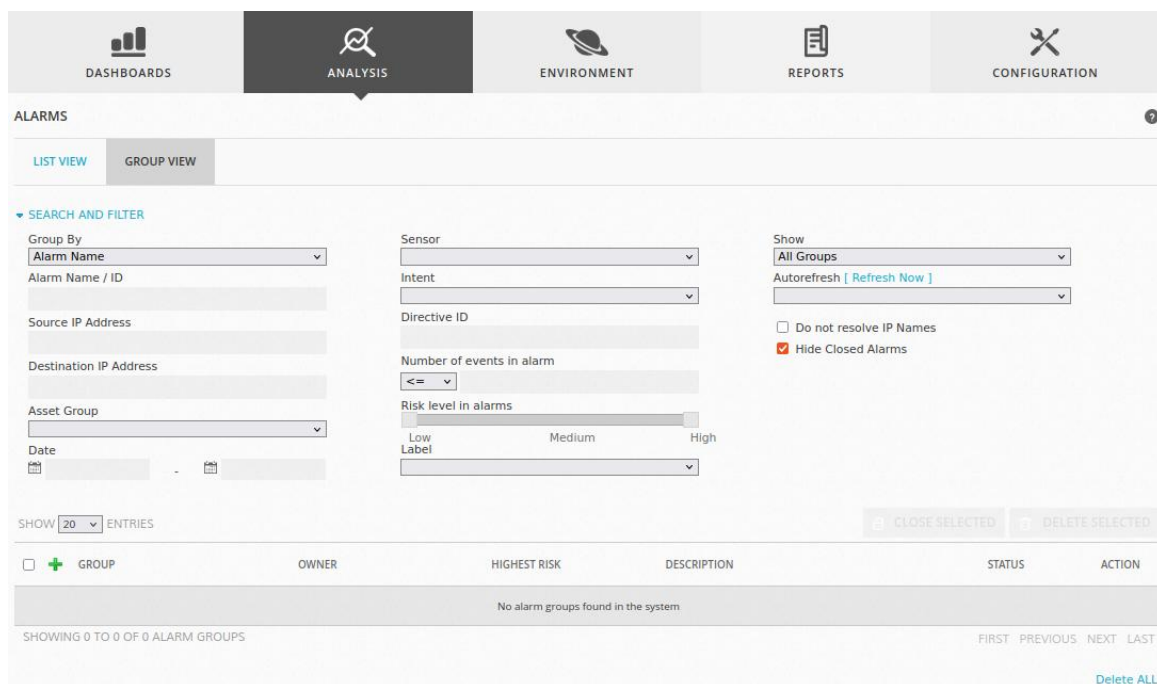


Imagen 85: interfaz web OSSIM – Vista agrupada de la lista de alarmas.

Referencia: Autor

Para configurar alarmas en la opción ‘List view’, se puede programar alarmas dentro de los parámetros de configuración de ‘Search and filter’, estas alarmas se deben de configurar en función de un determinado activo de la red, ya que esto nos permite gestionar algún tipo de evento que consideremos de alto riesgo.

9.6 Administración de tickets

La generación de tickets está relacionada sobre los eventos y alarmas reportadas en el OSSIM, y estas están asociadas a la gestión de vulnerabilidades, ya que al haber alguna detección de vulnerabilidades se podrá generar un ticket para ser notificado al operador del sistema SIEM. Para ver la lista de eventos nos vamos donde es ‘Analysis’ en el apartado ‘Security events (SIEM)’, en este podremos visualizar un listado de eventos ocurridos.

DASHBOARDS

ANALYSIS

ENVIRONMENT

REPORTS

CONFIGURATION

SECURITY EVENTS (SIEM)

SIEM

REAL-TIME

Search

Event Name

GO

SHOW EVENTS

DATA SOURCES

ASSET GROUPS

OTX IP REPUTATION

DATA SOURCE GROUPS

NETWORK GROUPS

OTX PULSE

SENSORS

EXCLUDE

RISK

ONLY OTX PULSE ACTIVITY

Clear Filters

Advanced Search

EVENTS

GROUPED

TIMELINE

SHOW

50

ENTRIES

CHANGE VIEW

ACTIONS

SHOW TREND GRAPH

Off

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.

13,830 TOTAL EVENTS IN DATABASE.

☐	EVENT NAME	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S > D	RISK	
☒	SSHd: Connection closed	2024-08-22 10:28:11	alienvault	N/A	0.0.0.0:56590	0.0.0.0:22	2->2	LOW (0)	
☒	AlienVault HIDS: Login session closed.	2024-08-22 10:28:09	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	
☒	AlienVault HIDS: Login session closed.	2024-08-22 10:28:09	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	
☒	sudo: Session closed	2024-08-22 10:28:08	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	
☒	SSHd: Session disconnected	2024-08-22 10:28:08	alienvault	N/A	alienvault-54056	alienvault:22	5->2	LOW (0)	
☒	AlienVault HIDS: Login session closed.	2024-08-22 10:28:07	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	
☒	AlienVault HIDS: Login session closed.	2024-08-22 10:28:07	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	

Imagen 86: interfaz web OSSIM – Lista de eventos ocurridos.

Referencia: Autor

Nosotros podremos generar un ticket mediante la selección de un determinado evento, seleccionando el generador de ticket, en el cual se abrirá una ventanita, en el cual nos pedirá que ingresemos el usuario, tipo, datos de titulo y prioridad.

New Event ticket

Values marked with (*) are mandatory

NEW TICKET	
TITLE *	SSHD: Connection closed
ASSIGN TO *	User: jaime grijalva garcia
PRIORITY *	5
TYPE *	Policy Violation
SOURCE IPS	0.0.0.0
DEST IPS	0.0.0.0
SOURCE PORTS	57496
DEST PORTS	22
START OF RELATED EVENTS	2024-08-22 15:34:52
END OF RELATED EVENTS	2024-08-22 15:34:52
SAVE	

Imagen 87: interfaz web OSSIM – Generación de nuevo ticket.

Referencia: Autor

Al guardar los cambios, este ticket será incluido a la lista de tickets con un estado de abierto (Open), en sí que este ticket debe ser cerrado posteriormente.

DASHBOARDS	ANALYSIS	ENVIRONMENT	REPORTS	CONFIGURATION
TICKETS				
SIMPLE FILTERS [SWITCH TO ADVANCED]				
Class	Type	Search text	Assignee	Status
ALL	ALL			Open
SEARCH				
☐	TICKET	TITLE	PRIORITY	CREATED
☐	EVE02	SSHD: Connection closed	5	2024-08-22 10:36:02
		LIFE TIME	ASSIGNEE	SUBMITTER
		05:00	jaime grijalva garcia	jaime grijalva garcia
		TYPE	STATUS	LABELS
		Policy Violation	Open	
Pag. 1				
Open a new ticket manually: Alarm CREATE				

Imagen 88: interfaz web OSSIM – Esquema de tickets generados.

Referencia: Autor

Para ingresar a la lista de tickets creados nos vamos a la ventanita ‘Analysis’ y seleccionamos ‘Tickets’, y aquí es donde podremos visualizar la lista de tickets creados dentro del OSSIM. También se pueden revisar cada uno a detalle.

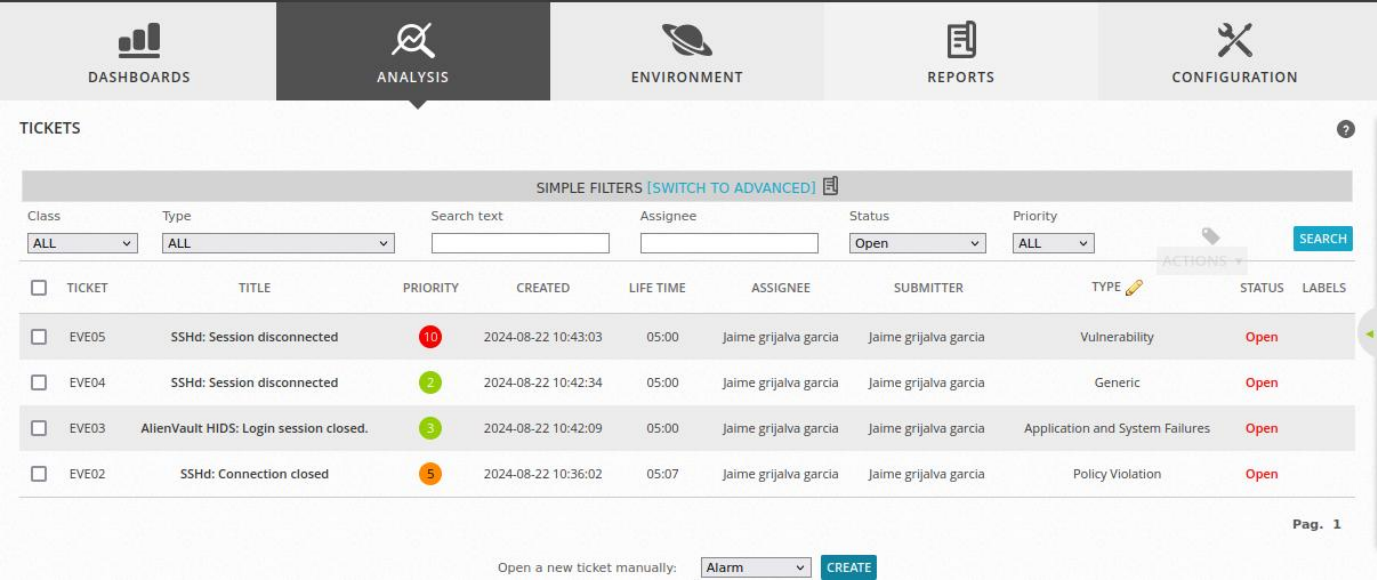


Imagen 89: interfaz web OSSIM – Tickets.

Referencia: Autor

Para visualizar la información de los tickets los seleccionamos para poder observar y conocer la información referida del ticket.

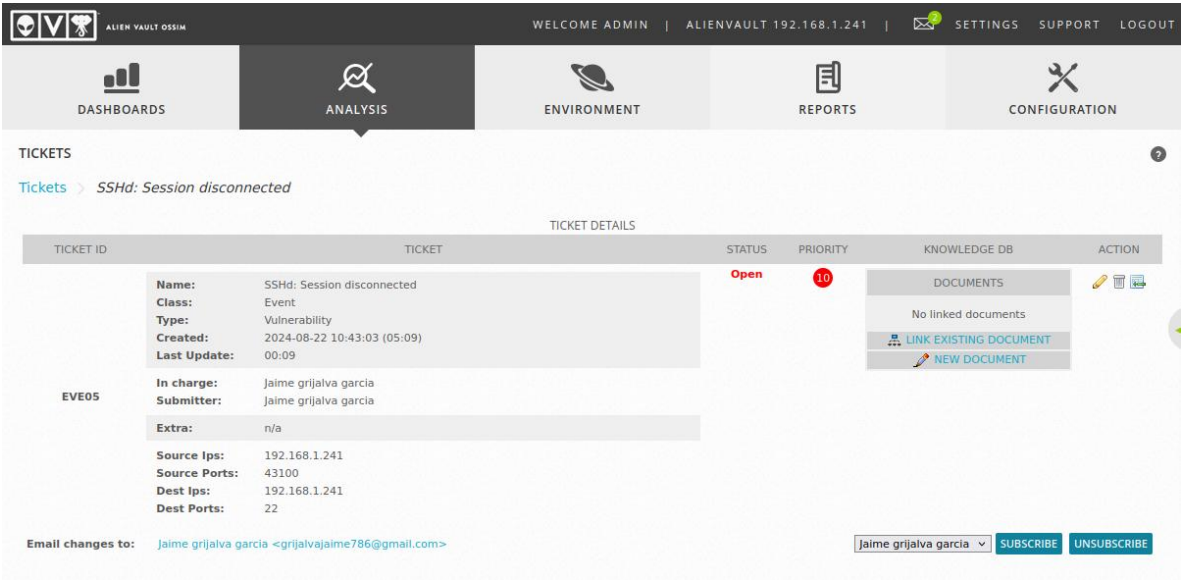


Imagen 90: interfaz web OSSIM – Detalle del ticket.

Referencia: Autor

De ser necesario después de analizar el ticket, se puede concluir cerrando el estado de este, seleccionando el ticket en la opción ‘Status’ seleccionando ‘Closed’ (Cerrado) y guardando los cambios con la opción ‘Save ticket’.

STATUS: Open
PRIORITY: 10
TRANSFER TO: User: - No users found -
ATTACHMENT: Browse... No file selected.

DESCRIPTION *
Resultado

ACTION

SAVE TICKET

Imagen 91: interfaz web OSSIM – Configuración del ticket

Referencia: Autor

Se actualiza la lista de los tickets, y como vemos uno de los tickets ya está en el estado de cerrado (Closed).

TICKETS										
SIMPLE FILTERS [SWITCH TO ADVANCED]										
Class	Type	Search text	Assignee	Status	Priority					
ALL	ALL			ALL	ALL	ACTIONS SEARCH				
TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	ASSIGNEE	SUBMITTER	TYPE	STATUS	LABELS	
☐	ALA06 New Alarm incident	10	2024-08-22 10:58:11	00:07	Jaime grijalva garcia	Jaime grijalva garcia	Vulnerability	Closed (2024-08-22 11:05:23)		
☐	EVE05 SSHd: Session disconnected	10	2024-08-22 10:43:03	05:23	Jaime grijalva garcia	Jaime grijalva garcia	Vulnerability	Open		
☐	EVE04 SSHd: Session disconnected	2	2024-08-22 10:42:34	05:24	Jaime grijalva garcia	Jaime grijalva garcia	Generic	Open		
☐	EVE03 AllenVault HIDS: Login session closed.	3	2024-08-22 10:42:09	05:24	Jaime grijalva garcia	Jaime grijalva garcia	Application and System Failures	Open		
☐	EVE02 SSHd: Connection closed	5	2024-08-22 10:36:02	05:30	Jaime grijalva garcia	Jaime grijalva garcia	Policy Violation	Open		

Pag. 1

Imagen 92: interfaz web OSSIM – Actualización de los estados del listado de tickets.

Referencia: Autor

9.7 Flujo de red

Para poder ver el detalle del flujo de la red, nos iremos a la opción ‘Netflow’ que está en la ventanita de ‘Environment’. Este apartado que es NetFlow es un protocolo publicado y diseñado por Cisco Systems que nos permite registra y transmitir información sobre los datos que se registran en la red.

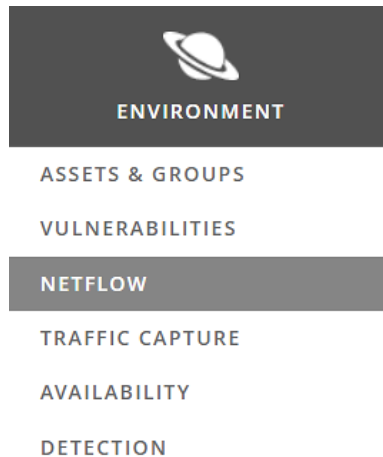


Imagen 93: interfaz web OSSIM - Flujo de red.

Referencia: Autor

En esta opción se tendrá toda la información del flujo de la red en tiempo real, con la opción de alternativas de tiempo. Aquí podremos ver gráficos de flujo de red, paquetes de red para los protocolos TCP, UDP, ICMP y otros, además de ver el trafico de la red.

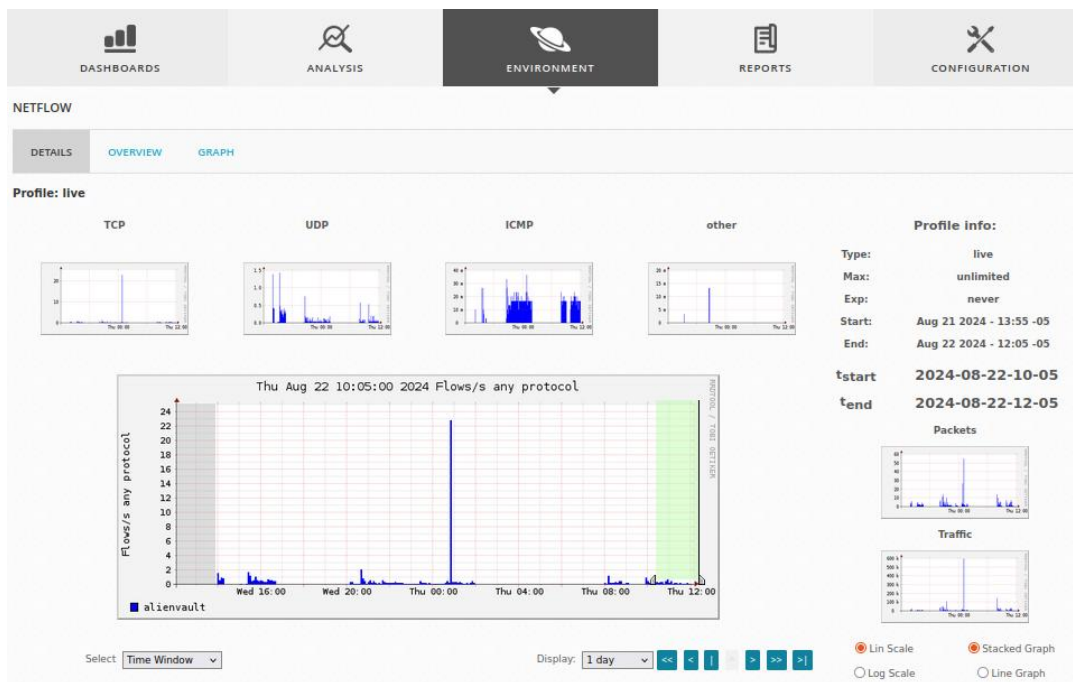


Imagen 94: interfaz web OSSIM – Detalles del flujo de red.

Referencia: Autor

En la otra pestaña que es resumen (Overview), en esta se podrá visualizar el resumen del flujo de la red que ha sido generado por la herramienta.

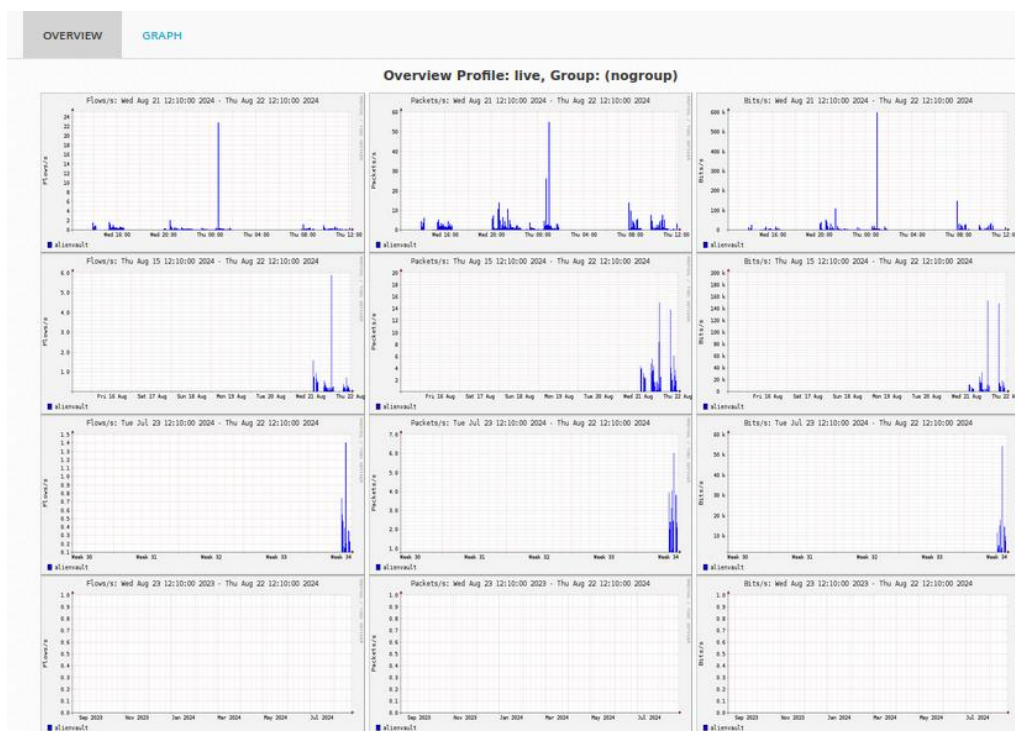


Imagen 95: interfaz web OSSIM – Resumen del fujo de red.

Referencia: Autor

En la ultima pestaña que es grafico (Graph), aquí se muestra los gráficos por paquetes, flujo y tráfico de la red generado.

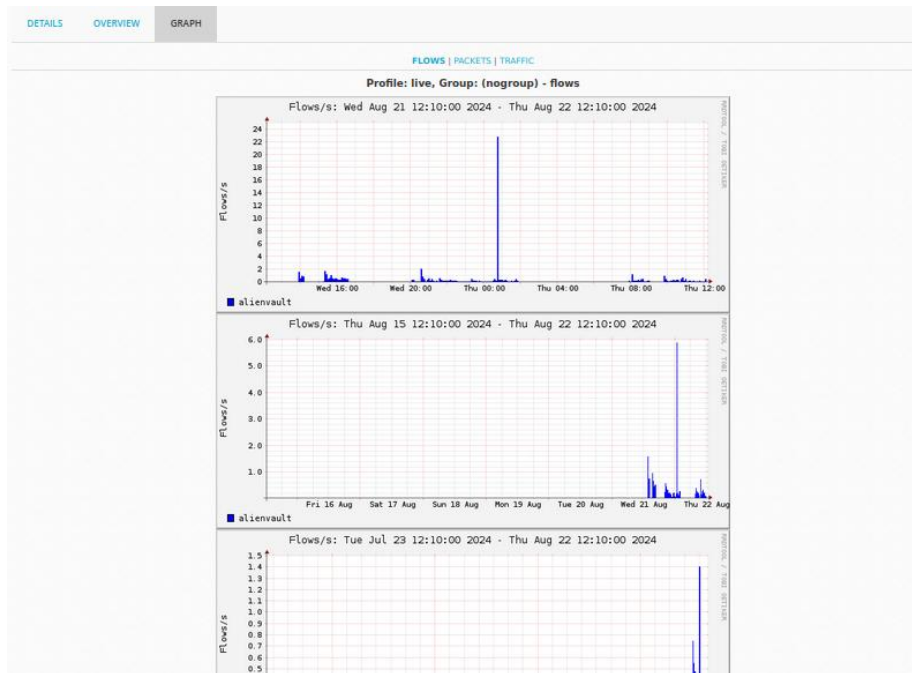


Imagen 96: interfaz web OSSIM – Gráficos de flujo de red.

Referencia: Autor

Después de realizar las configuraciones en los distintos módulos del sistema SIEM, en la pantalla principal de la interfaz web del OSSIM, veremos que presenta nuevos cambios en la visión general de los procesos.

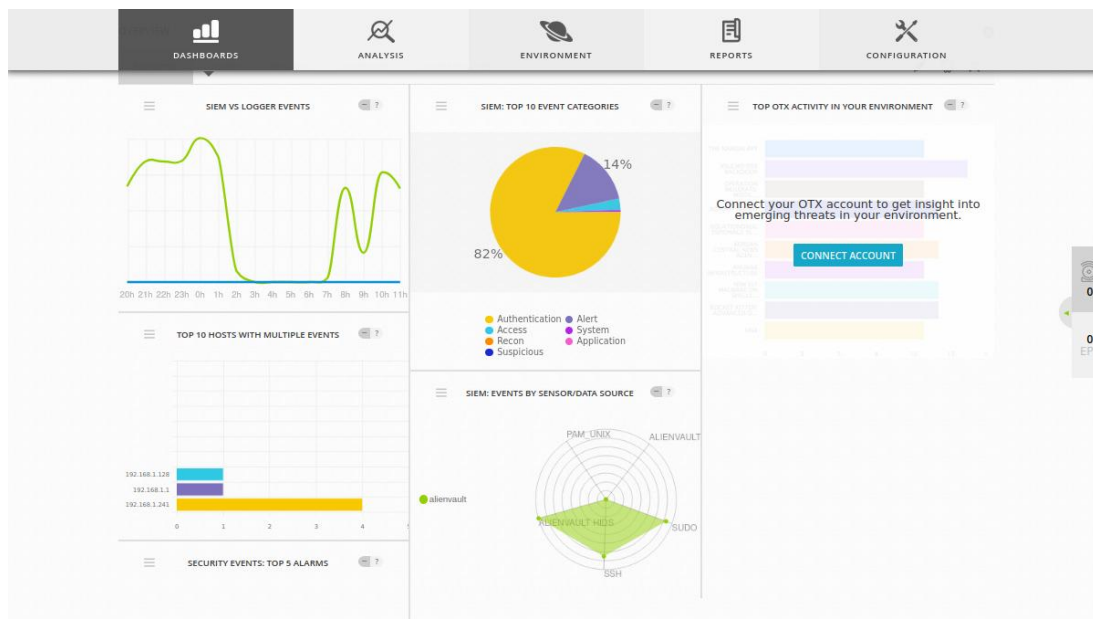


Imagen 97: interfaz web OSSIM – Visión general del SIEM.

Referencia: Autor

10 Bibliografía

Buscar. (s/f). Recuperado el 18 de julio de 2024, de Wwww.hp.com website:

<https://www.hp.com/ec-es/search.html>

Cisco 220 series smart switches data sheet. (2020, febrero 13). Recuperado el 18 de julio de 2024,

de Cisco website: <https://www.cisco.com/c/en/us/products/collateral/switches/small-business-220-series-smart-plus-switches/datasheet-c78-731284.html>

Cisco 890 Series Integrated Services Routers data sheet. (2022, noviembre 17). Recuperado el 18

de julio de 2024, de Cisco website:

https://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html

Crs326-24g-2s+rm. (s/f). Recuperado el 18 de julio de 2024, de Mikrotik.com website:

<https://mikrotik.com/product/CRS326-24G-2SplusRM>

Linksys official Support - Linksys SE2800 8-port gigabit Ethernet switch. (s/f). Recuperado el 18

de julio de 2024, de Linksys.com website: <https://store.linksys.com/support-product?sku=SE2800>

Linksys SE2800-EU 8-Port Gigabit Ethernet Switch. (s/f). Recuperado el 18 de julio de 2024, de

Ciudadwireless.com website: https://www.ciudadwireless.com/linksys_se2800-eu_8-port_gigabit_ethernet_switch-p-5039.html?currency=ESP

RB4011iGS+RM. (s/f). Recuperado el 18 de julio de 2024, de Mikrotik.com website:

https://mikrotik.com/product/rb4011igs_rm

Switches DGS-1510 Series. (2018, abril 13). Recuperado el 18 de julio de 2024, de D-Link

Latinoamérica website: <https://la.dlink.com/la/switches/dgs-1510-series/>

Técnica, G. (s/f). Dell EMC PowerEdge T150. Recuperado el 18 de julio de 2024, de Dell.com

website: https://i.dell.com/sites/csdocuments/Product_Docs/es/mx/dell-emc-poweredge-t150-technical-guide-es-xl.pdf

(S/f). Recuperado el 18 de julio de 2024, de Lenovo.com website: [https://www.le-](https://www.lenovo.com/us/en/p/servers-storage/servers/racks/thinksystem-sr250-v2/7d7qa01yna)

[novo.com/us/en/p/servers-storage/servers/racks/thinksystem-sr250-v2/7d7qa01yna](https://www.lenovo.com/us/en/p/servers-storage/servers/racks/thinksystem-sr250-v2/7d7qa01yna)