ALIEN VAULT OSSIM

OSSIM

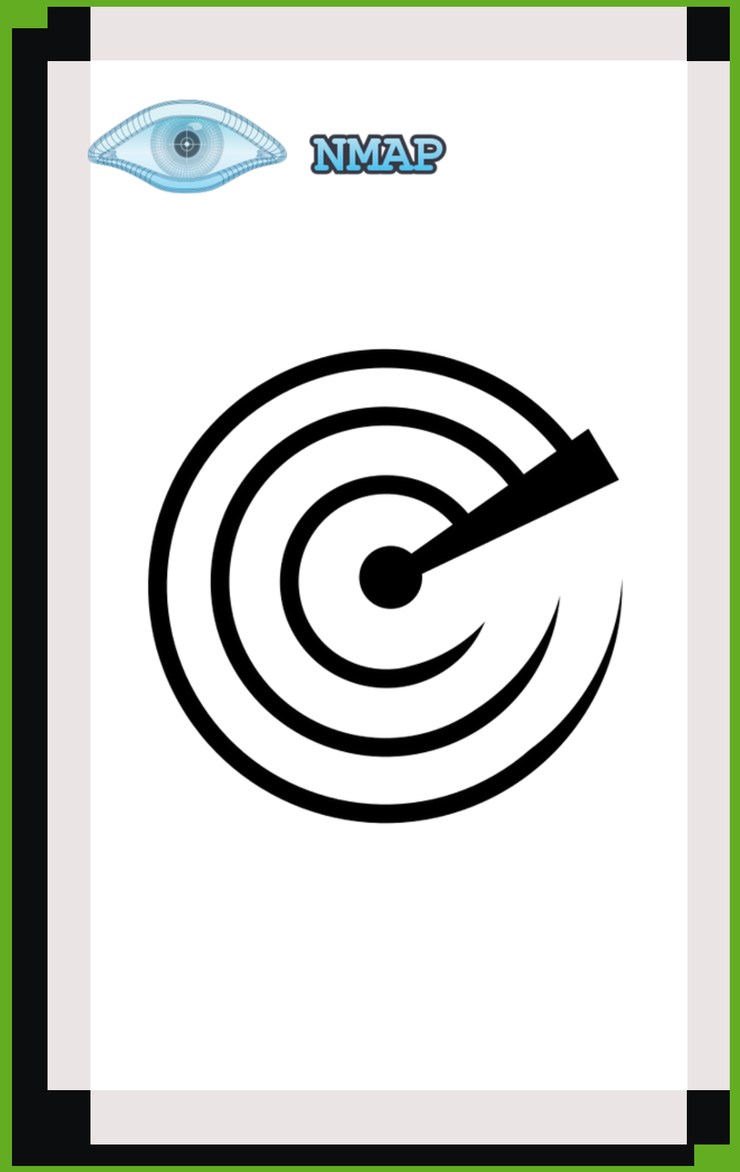
OPEN SOURCE SECURITY INFORMATION MANAGEMENT

BTR Consulting

Usos de Alien Vault OSSIM:

- Asset discovery
- Vulnerability assessment
- Threat detection
- Behavioral monitoring
- Security Intelligence

Gran Alternativa
Siem "Open source"
ofrecido por AT&T



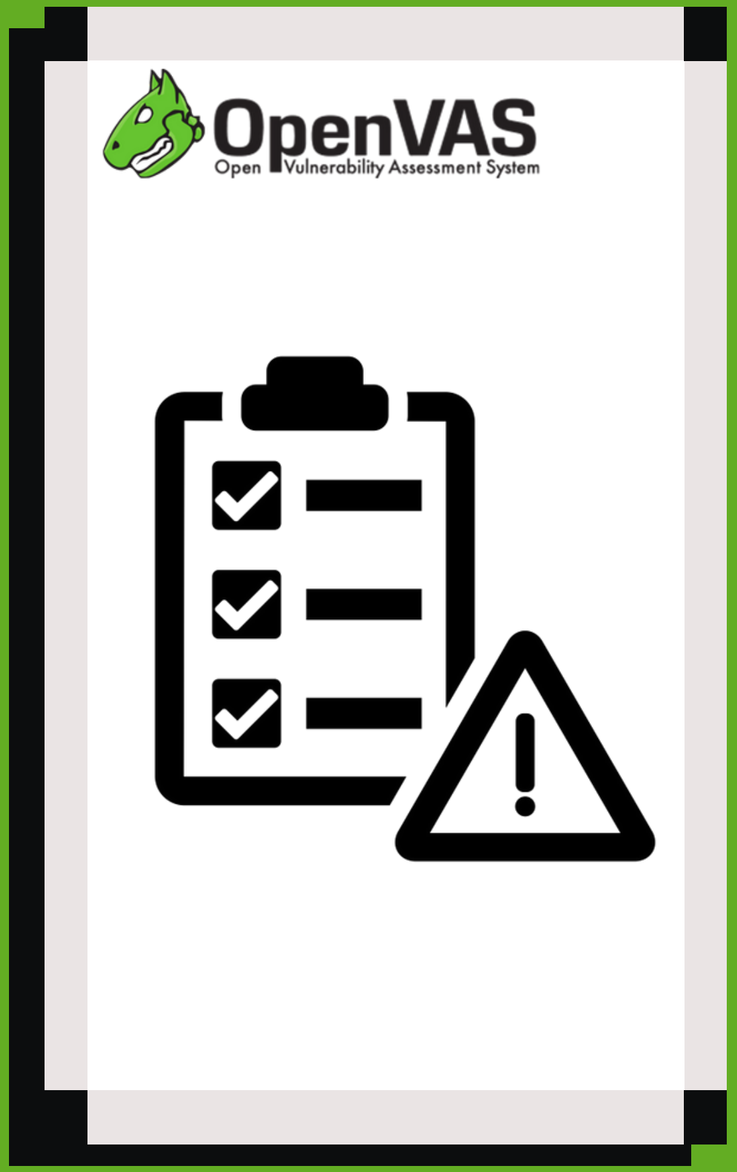
Asset discovery

(Descubrimiento de activos)

- **Escaneo de red activo**
- **Escaneo de red pasivo**
- **Inventariado de assets**
- **Inventario de sofware baseado en host**

Para saber a qué eventos dar prioridad necesitaremos conocer la lista de sistemas críticos de una red, y qué software está instalado en ellos.

Necesita entender el entorno actual entorno existente para evaluar la criticidad de los incidentes como parte del proceso de orientación/tratamiento, ossim emplea el uso de NMAP y PRADS para realizar esto.



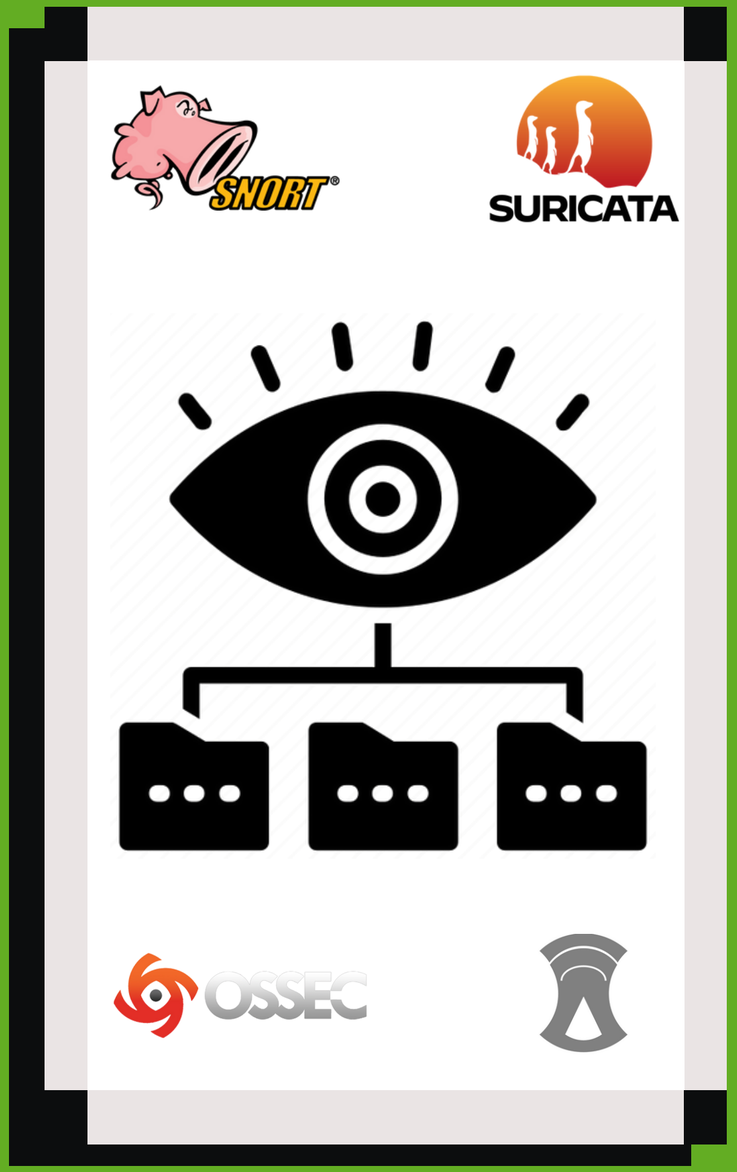
Vulnerability assessment

(Gestion de vulneravilidades)

- **Monitoreo continuo de vulnerabilidades**
- **Escaneo activo autenticado/no autenticado**

Los escáneres de vulnerabilidad permiten identifican posibles vulneravilidades y ayudan a evaluar la superficie de ataque global de una organización, de modo que se puedan implementar tareas de remediación.

Ossim utiliza Openvas para poder realizar este tipo de escaneos



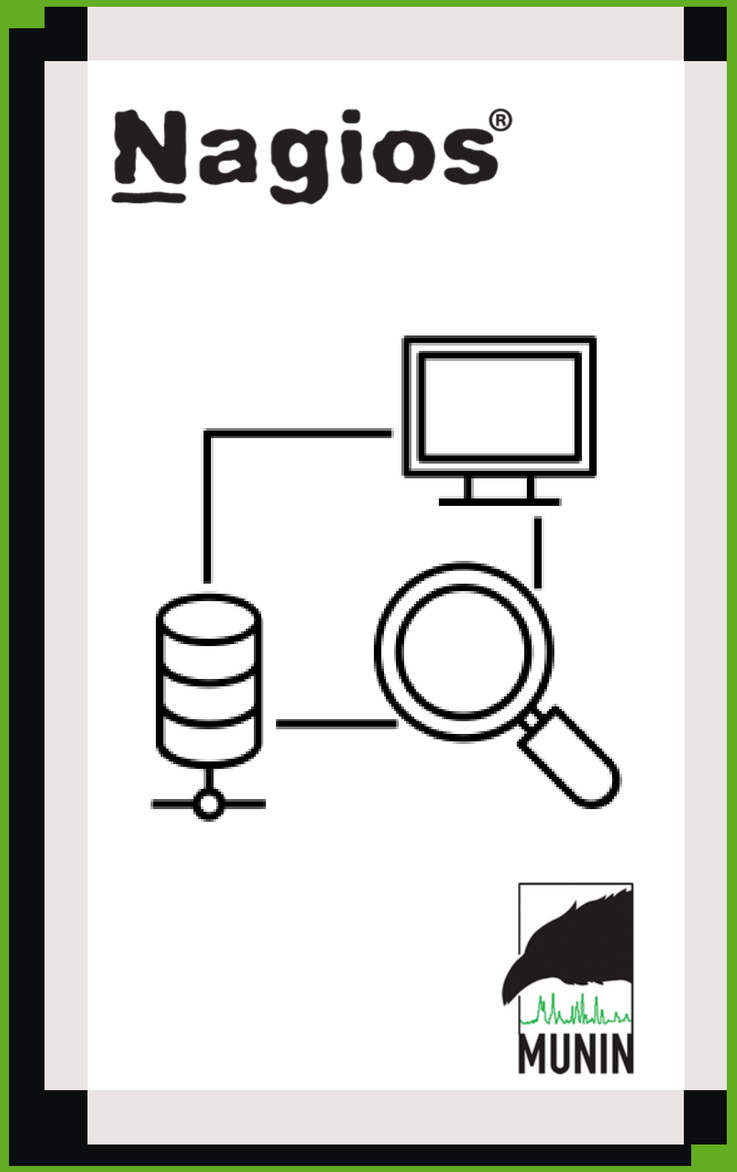
Threat detection

(Detecion de Amenazas)

- **Network IDS**
- **Host IDS**
- **Wirelees IDS**
- **Monitoreo de integridad de archivos**

Los IDS (HIDS y NIDS) supervisan la actividad del servidor y de la red en tiempo real, suelen utilizar firmas de ataque o baseline para identificar y emitir una alerta cuando se producen ataques conocidos o actividades sospechosas en un en un servidor (HIDS) o en una red (NIDS).

OSSIM utiliza Tcptrack, Suricata (IDS) o Snort (NIDS), OSSEC (HIDS), Kismet (WIDS)



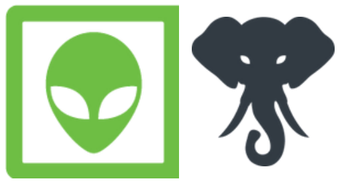
Behavioral monitoring

(Supervisión de comportamiento)

- **Recoleccion de logs**
- **Analisis de netflow**
- **Disponibilidad de servicios**

Uno de los objetivos de la respuesta a incidentes es evitar el tiempo de inactividad en la medida de lo posible, acegurar de la disponibilidad es crucial porque podría ser la primera señal de un incidente en curso.

Ossim utiliza Nagios (Disponibilidad de activos), Munin (Analisis de trafico), NFSen/NFDump (recoleccion y analisis de NetFlow)



Security Intelligence

(Correlacion de eventos)

- **Correlacion de eventos SIEM**
- **Respuestas a incidentes**

Los logs son la fuente más rica para entender lo que está pasando en su red, pero necesitará una herramienta De respuesta a incidentes que dé sentido a todos esos Logs

OSSIM incluye herramientas de desarrollo propio, siendo la más importante el motor de correlación genérico con soporte de directivas lógicas e integración de Logs con plugins

THE ESSENTIAL CONTROLS

Analytics & Intelligence

EMERGING THREATS

ALIEN VAULT OSSIM

Asset Discovery

PRADS

PADS

open source alternatives for each of the 5 categories

Behavioral Monitoring

nfsp

OpenFPC

P0F

NFSen

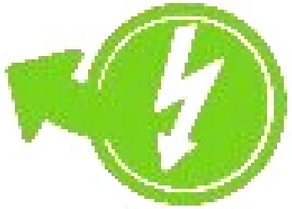
Nagios

openNMS

Vulnerability Assessment

OpenVAS

OVALdi



Threat Detection

OSSEC

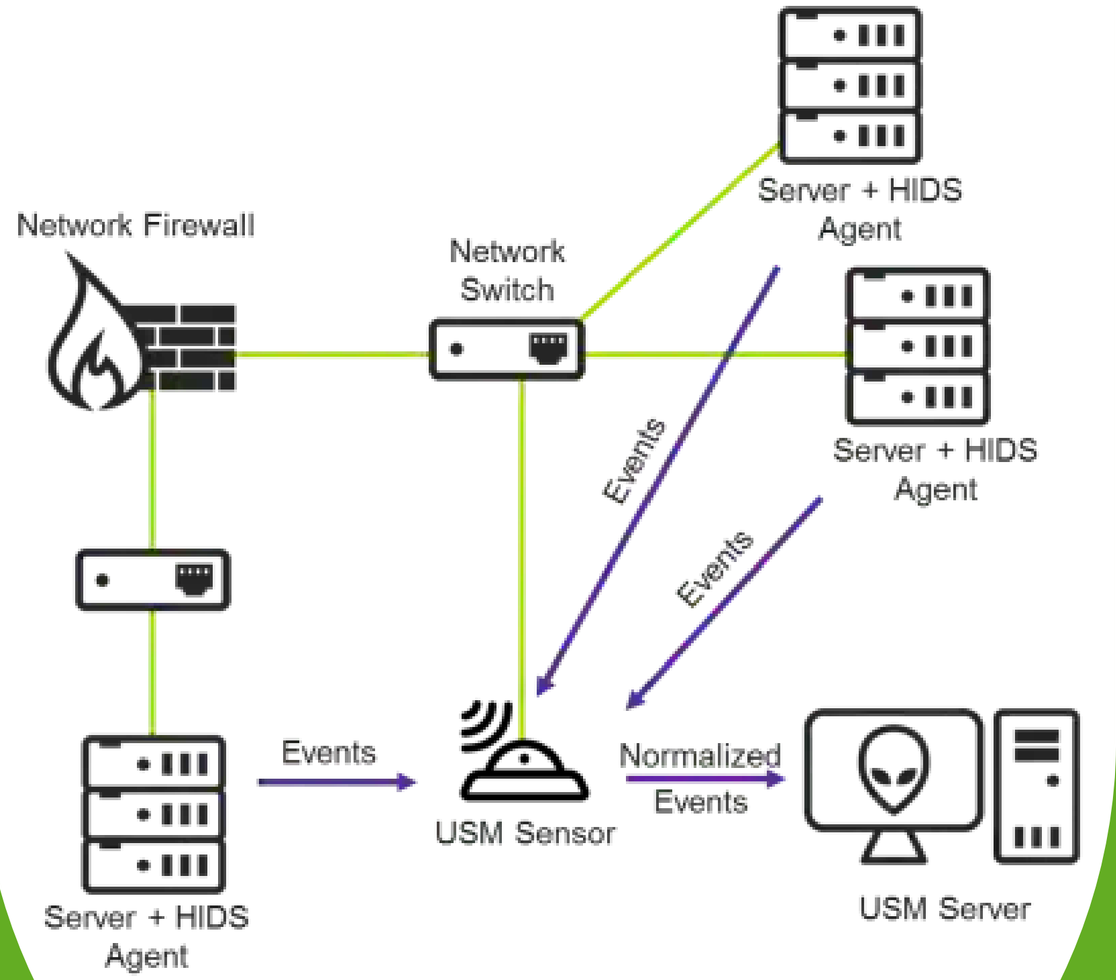
KISMET

SURICATA

SNORT

AlienVault HIDS

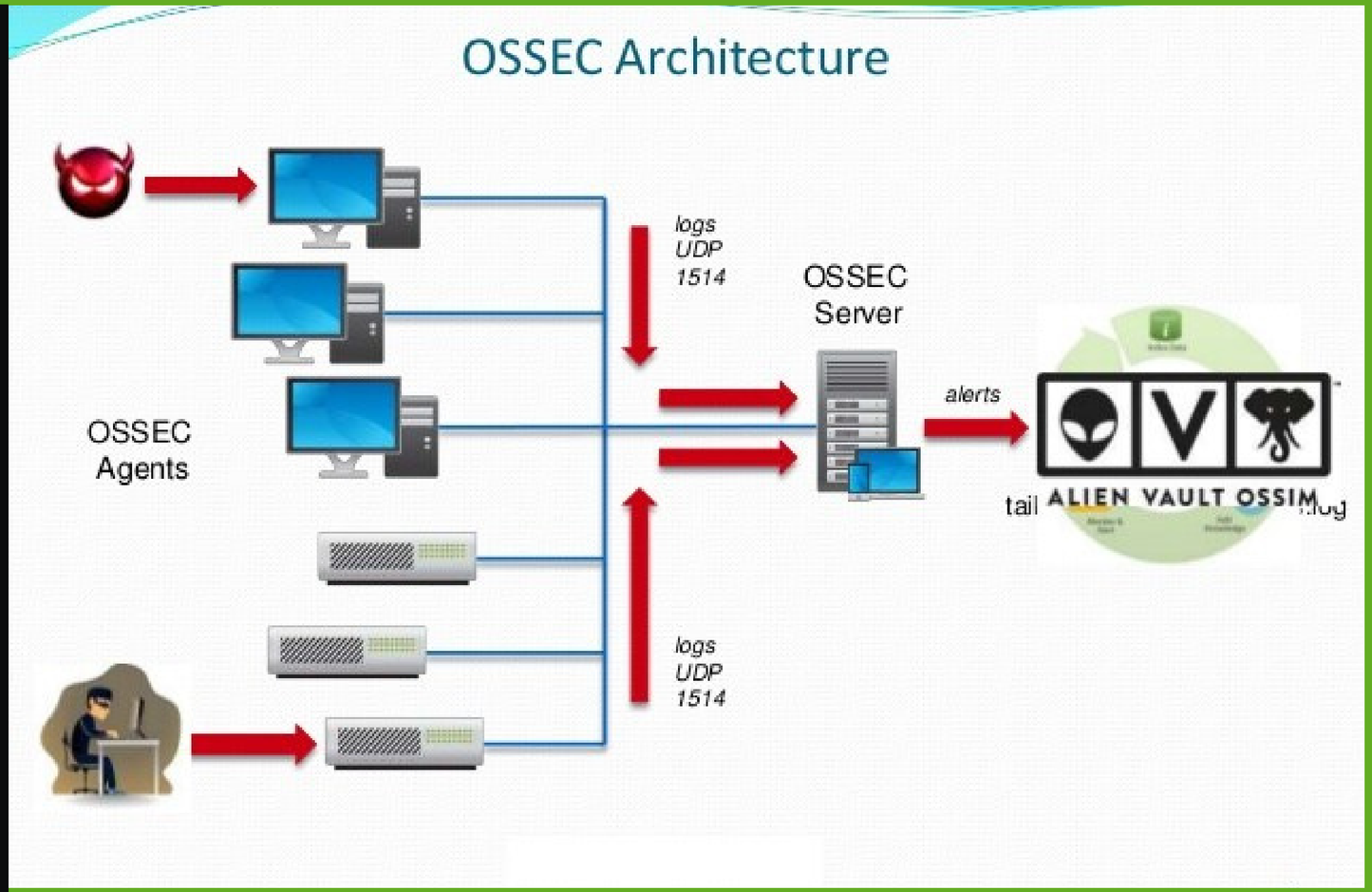
AlienVault HIDS utiliza una arquitectura de servidor/agente, en la que el agente HIDS reside en los hosts que desea monitorear y el servidor HIDS reside en el USM Appliance Sensor. El USM Appliance Sensor recibe los eventos de los agentes HIDS, los normaliza y los envía al USM Appliance Server para su análisis, correlación y almacenamiento.



OSSEC

Ossim utiliza OSSEC host-based IDS (HIDS) que permiten:

- Recoleccion y Monitoreo de Logs
- Deteccion de Rootkit
- Control en Integridad de archivos
- Control de registros de Windows
- Respuesta Activa



¿Preguntas?

Presentacion por:
BTR consulting