Diseño y Configuración de IPS, IDS y SIEM en Sistemas de Control Industrial

CERT DE SEGURIDAD
E INDUSTRIA

certsi_

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

Noviembre 2017

CERTSI_GUIA_SCI_004_ConfiguracionIPSIDSySIEM_2017_v1

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 SOBRE ESTA GUÍA

Este estudio, de carácter técnico, se centra en una descripción del uso de sistemas de detección y prevención de intrusiones y de sistemas de recolección de eventos orientados a los sistemas de control.

Se detallan también el funcionamiento de algunas soluciones y las recomendaciones de seguridad a aplicar en estas tecnologías.

2 INTRODUCCIÓN

Actualmente, existe una estrecha relación entre la información y tecnología usada en las empresas. Con el tiempo han ido surgiendo y evolucionando nuevas técnicas que permiten el acceso de manera ilegítima por medio de vulnerabilidades encontradas en las redes OT.

Como respuesta a estas vulnerabilidades, se han desarrollado arquitecturas, técnicas y sistemas que detectan y previenen estos accesos indebidos. Así aparecen los IDS, con la función principal de detectar anomalías y usos indebidos (inicialmente pensados para el mundo IT). Las actuales amenazas contra las redes OT, hacen que se implemente el uso de estas herramientas en redes industriales, examinando detalladamente los protocolos y transmisiones que circulan por la red.

Ante la dificultad que supone para los IDS reaccionar frente a las alertas de intrusión, se desarrollaron los IPS que se encargan de reaccionar activamente a las intrusiones detectadas por el IDS. Hoy en día, los términos IDS e IPS se utilizan de modo indistinto y los equipamientos son idénticos, cambiando el modo de funcionamiento simplemente dependiendo del tipo de despliegue y de unos pocos parámetros de configuración.

Para avanzar más en la tecnología de defensa aparecen los sistemas SIEM, que no dependen de una sola fuente de información – como podría ser un IDS / IPS –. Además de centralizar la información, son capaces de relacionar (el verbo correlar se suele utilizar en este contexto en TI y se usará frecuentemente en este documento) eventos de diferentes fuentes para generar alertas personalizadas. Estos dispositivos aportarán la inteligencia necesaria para ir reduciendo paulatinamente el número de falsos positivos.

Existe una cierta ventaja en el uso de estos sistemas que combinan diferentes tipos de aprendizajes y gestión, debido a que en las redes industriales los eventos almacenados suelen presentar una menor variabilidad que en el mundo IT. Por este motivo, pueden resultar más efectivos y detectar un menor número de falsos positivos.

3 ORGANIZACIÓN DE ESTE DOCUMENTO

Este documento incluye dos apartados técnicos centrados en sistemas de control industrial y tecnologías IDS/IPS y SIEM, y dos anexos donde se detallan las tecnologías y los aplicativos relativos a los dos apartados técnicos anteriores.

En el primer apartado técnico (apartado 4) se recoge una arquitectura de red para sistemas de control industrial a modo de arquitectura base y a partir de esta otras arquitecturas de seguridad y recomendaciones para desplegar un entorno real con las tecnologías de seguridad analizadas en este documento; en el segundo apartado técnico (apartado 5) se presentan instrucciones precisas de instalación paso a paso de una infraestructura que cubre las tecnologías sobre las que trata este documento. Concretamente, se instruirá al lector para que pueda desplegar un sistema IDS/IPS en modo *Inline* así como un sistema de monitorización de eventos.

En los anexos se recoge un primera parte (ANEXO 1) con definiciones, características y ventajas de cada una de las tecnologías que forman parte del estudio, no sólo en el mundo TI, sino dando un matiz a nivel industrial. La segunda parte (ANEXO 2) enumera y detalla varias soluciones de seguridad de las tecnologías descritas que han sido probadas en laboratorio.

4 RECOMENDACIONES DE DESPLIEGUE

4.1 Introducción

En los siguientes puntos se detallarán diferentes tipos de despliegues usando las tecnologías descritas en este documento, IDS/IPS y SIEM. Se partirá de una arquitectura base que irá evolucionando para llegar a una arquitectura completa que contiene todos los elementos necesarios para disponer de un sistema de detección/prevención de intrusiones así como de un sistema de recolección y gestión de eventos.

4.2 Arquitectura base de sistemas de control

La arquitectura base seleccionada está basada en la propuesta ofrecida por la norma IEC 62443 [33]. En ella se definen diferentes zonas asociadas a los niveles en los que se divide un sistema de control industrial.

La arquitectura base presenta una segmentación basada en cortafuegos para separar las zonas de control y corporativa, contando además con dos DMZ para el intercambio de información entre ambas zonas.

Las arquitecturas siguientes propuestas presentas arquitecturas de seguridad para asegurar las comunicaciones y los dispositivos situados en la parte de control de la red. La seguridad de la parte corporativa no se ha tenido en cuenta en este estudio al quedar fuera del ámbito del mismo.

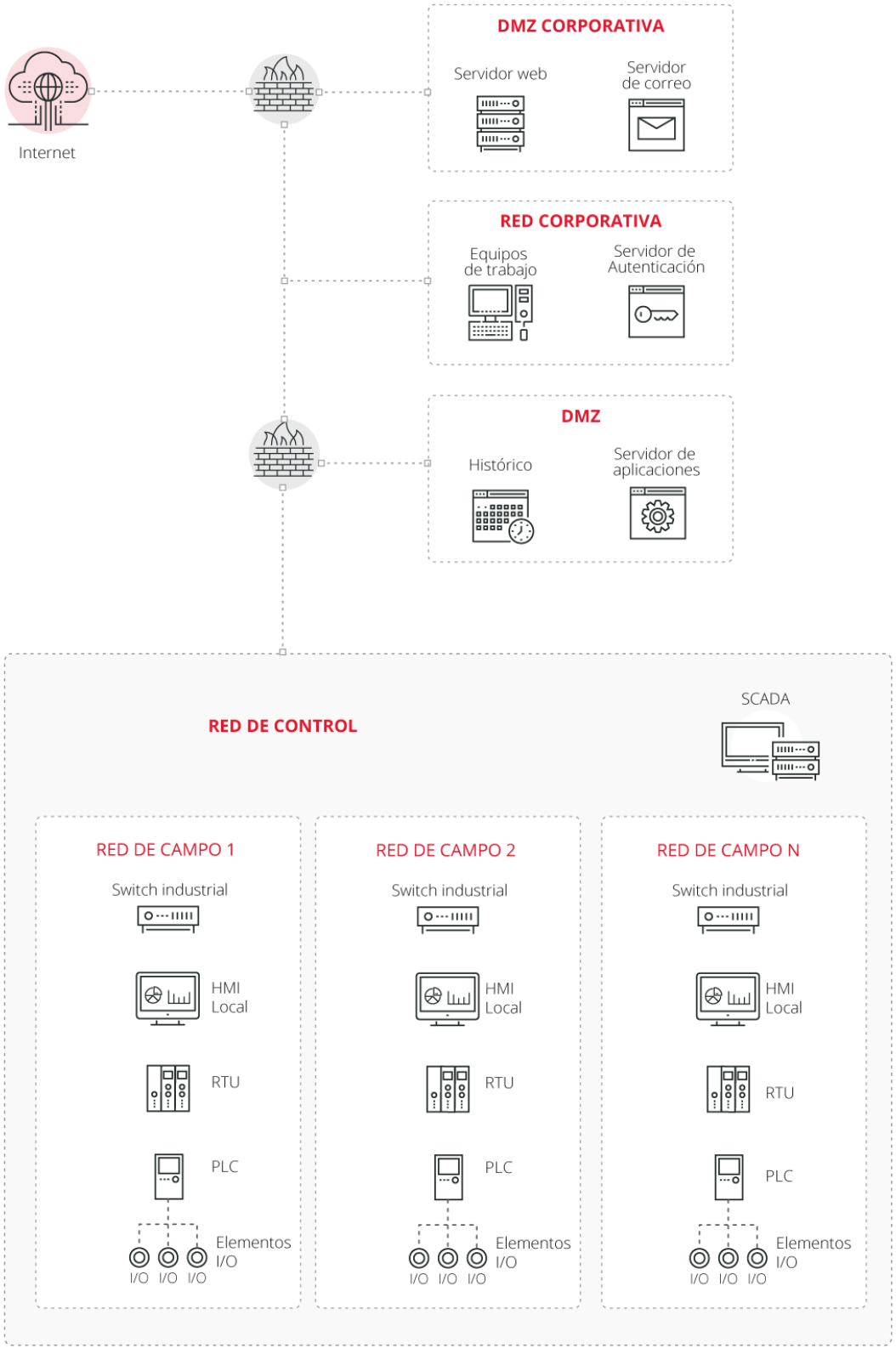

Figura 1: Arquitectura base para un sistema de control

4.3 Arquitecturas de seguridad para sistemas de control

La primera arquitectura, presentada en la Figura 2, describe la colocación de dispositivos de tipo IDS para monitorizar el tráfico dentro de la red de control. Para ello, todo el tráfico que pasa por los router/switches se lleva al sensor del IDS a través de puertos espejo (*mirror/SPAN*). También se añade una sonda para recibir información del cortafuegos y tener así controlado el tráfico intercambiado con la red correspondiente a la zona empresarial.

Los IDS deberán de disponer de las reglas adecuadas para generar las alertas oportunas que serán mostradas al operario o administrador de seguridad correspondiente a través de la consola.

La evolución de una arquitectura de seguridad con IDS pasa por bloquear tráfico. Para ello es necesario que los sensores pasen a estar en medio del tráfico, en lugar de escuchando el tráfico a través de los puertos espejo (*mirror/SPAN*), como refleja la Figura 3. La configuración de reglas debe ser adecuada para que no se interrumpa el flujo de tráfico de control habitual y solo se bloqueen las intrusiones y fallos de seguridad. La situación de los sensores IPS es similar a la de los sensores IDS, y el funcionamiento será exactamente el mismo, generando alerta que serán mostradas en la consola de IDS.

La Figura 4 representa la instalación de un SIEM dentro de los sistemas de control. Hay que tener en cuenta que el SIEM se dedica a recoger y gestionar eventos de log, por lo que las fuentes de datos provendrán de todos los dispositivos. En este caso hay que tener cuidado con las comunicaciones, ya que todos los dispositivos deben poder enviar sus registro de eventos hasta el SIEM, y esto puede implicar una sobrecarga de tráfico en la red. La mejor forma de solucionar esta sobrecarga es disponer de una red exclusiva para el envío de estos mensajes.

La representación final (Figura 5) muestra la puesta en conjunto de las tres tecnologías dentro de una arquitectura de red de sistemas de control. El IPS quedaría para los niveles superiores, controlando el tráfico intercambiado entre la parte de control y la parte corporativa o de negocio, los IDS gestionarían el tráfico entre la red de control y las de campo, informado de posibles anomalías en el tráfico; y el SIEM recogería la información del mayor número posible de dispositivos, incluyendo dispositivos de proceso y elementos de red, así como la información de las alertas tanto de los IDS como del IPS.

Las líneas rojas mostradas en las figuras indican los puntos donde tanto los sensores IDS como los sensores IPS se conectan para recabar el tráfico, y constituyen una conexión de red. La red de monitorización se utiliza como nexo de unión entre los sensores IDS/IPS y el núcleo central de gestión, y por este motivo no se requiere un acceso a dicha red desde ninguna otra parte de la arquitectura.

Las líneas marcadas en verde que finalizan el en SIEM muestran de dónde se obtiene información y no conexiones de red reales. La información se enviará a través de las conexiones existentes, habilitando en el cortafuegos (y en su caso en el IDS/IPS) las reglas correspondientes.

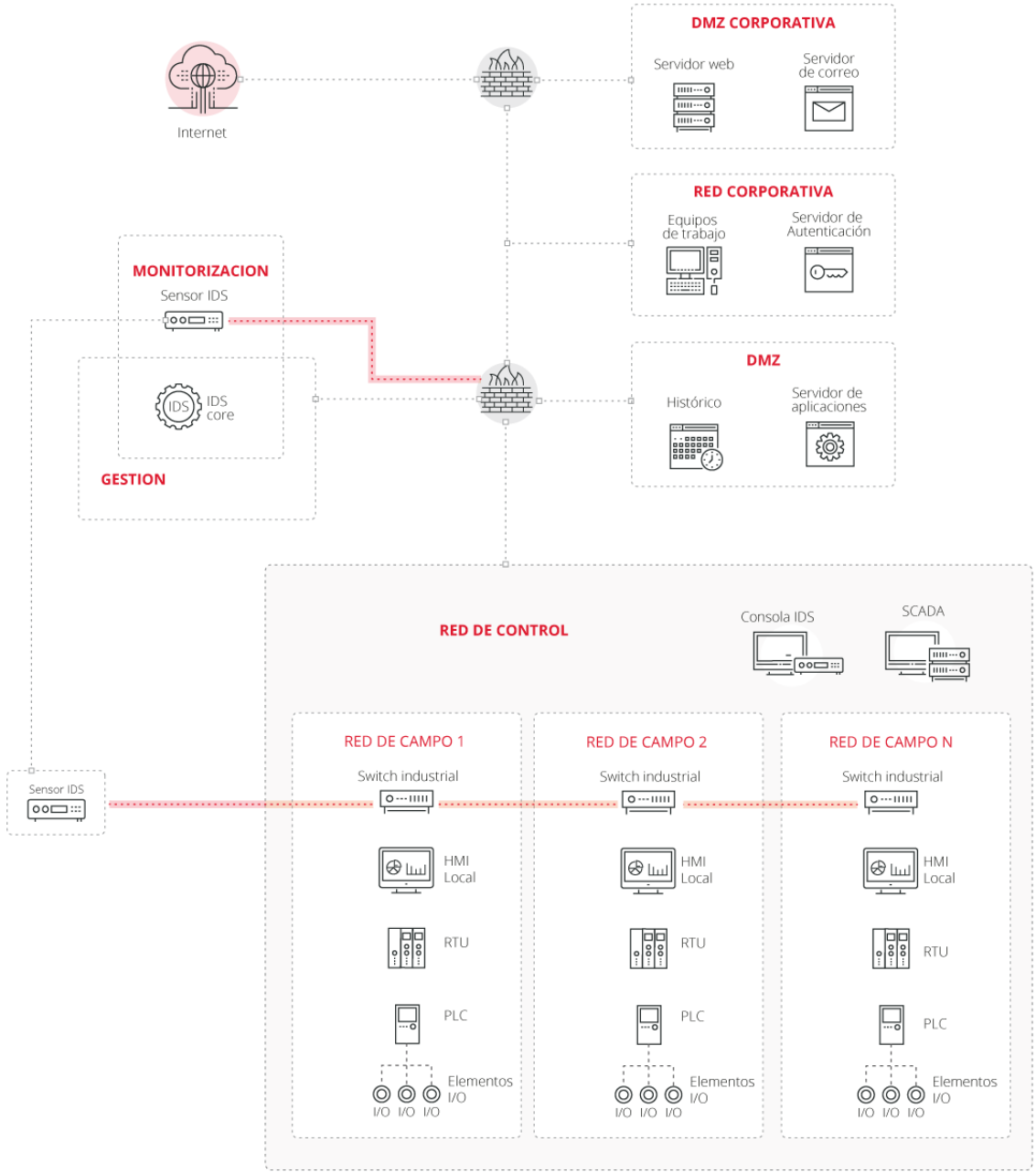

Figura 2: Arquitectura de seguridad con IDS

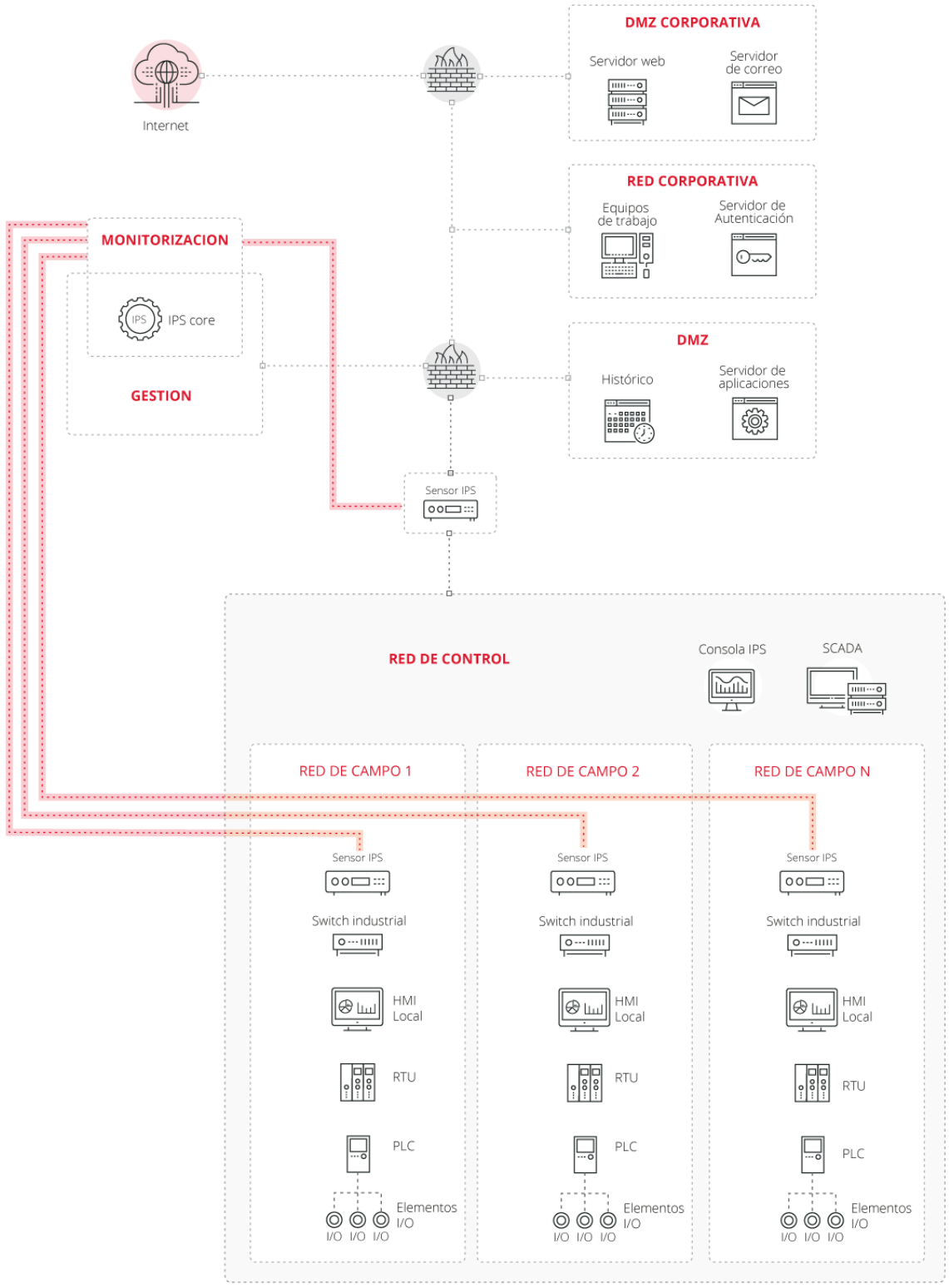

Figura 3: Arquitectura de seguridad con IPS

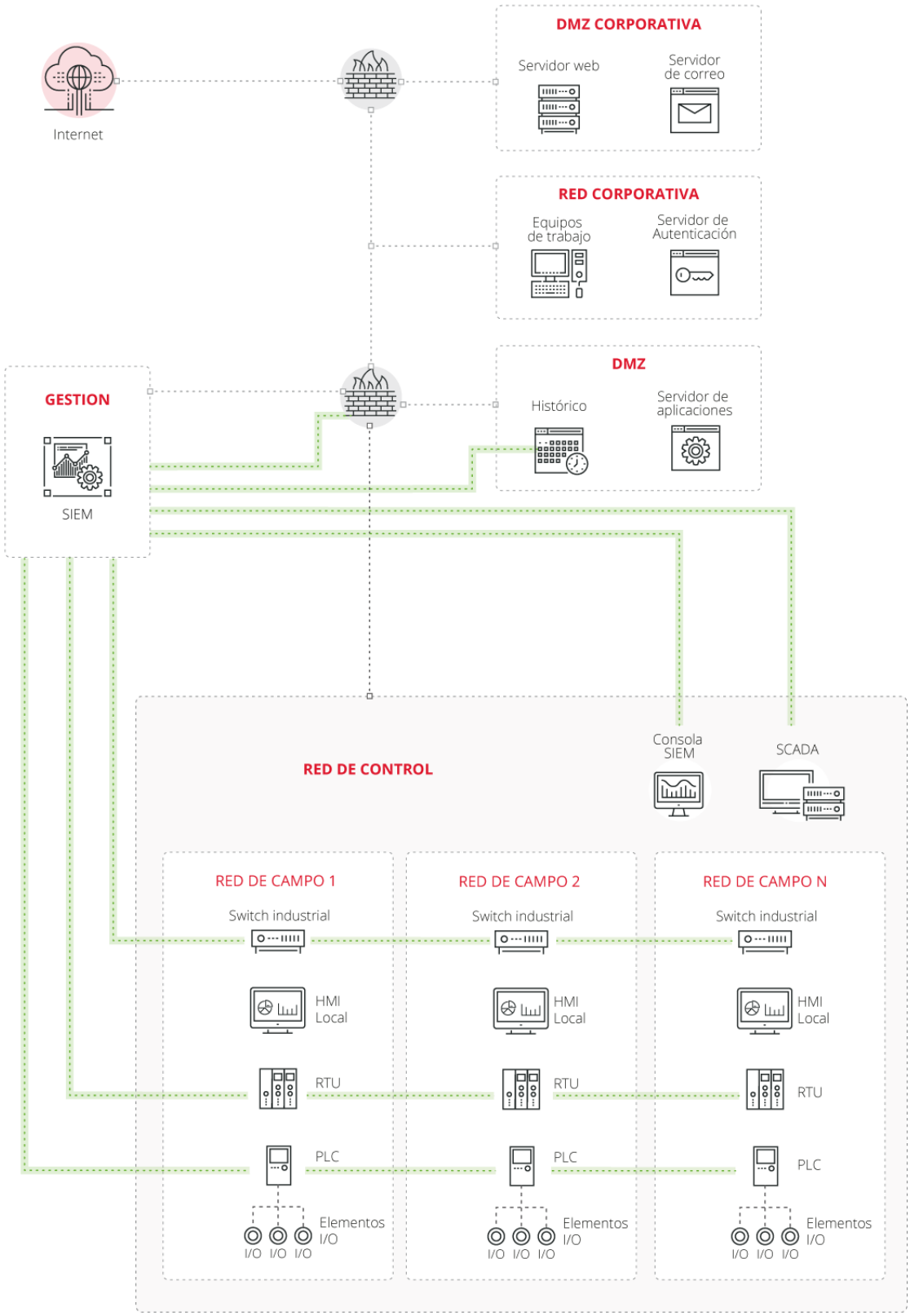

Figura 4: Arquitectura de seguridad con SIEM

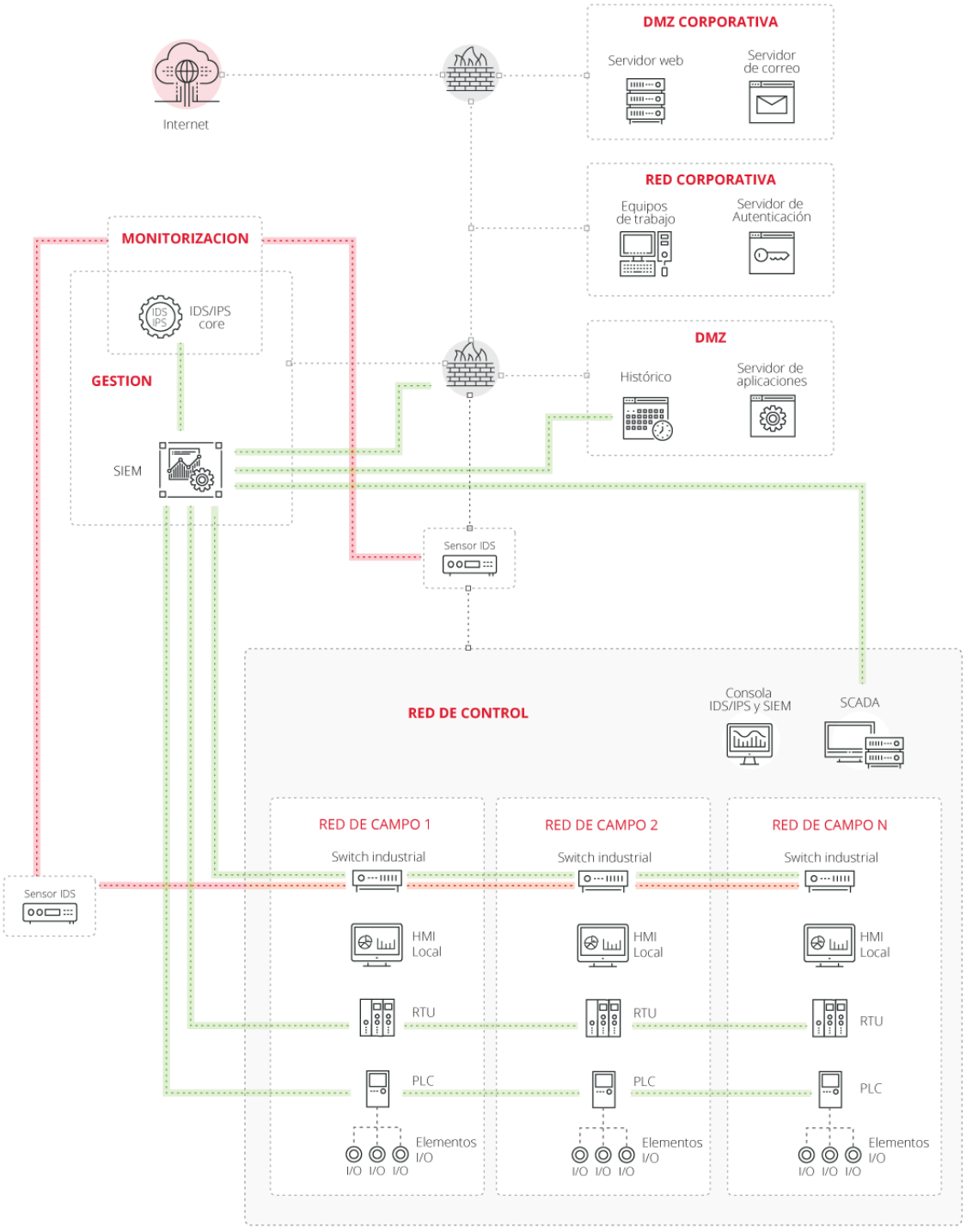

Figura 5: Arquitectura unificada con IDS, IPS y SIEM

5 MANUAL DE INSTALACIÓN

5.1 Introducción

En los siguientes apartados se darán instrucciones precisas paso a paso de cómo desplegar un entorno real que nos permita detectar eventos de seguridad (Snort) así cómo gestionarlos y visualizarlos con posterioridad (Snorby).

5.2 Diseño de arquitectura de laboratorio

La Figura 6 muestra la arquitectura de red desplegada en el laboratorio para comprobar la seguridad de las arquitecturas definidas previamente.

Los componentes utilizados en el despliegue son:

- IDS/IPS: Ubuntu Server 16.10 con Snort 2.9.8.3 en modo INLINE
- Gestor de eventos: Ubuntu Server 16.10 con Snorby
- PLC: Logitek TBox
- Router: Línux VyOS
- Simuladores: Microsoft Windows con ModBus Tools (maestro y esclavo)
- Atacante: equipo a situar en diferentes posiciones de la red para comprobar el funcionamiento de las reglas definidas en SNORT.

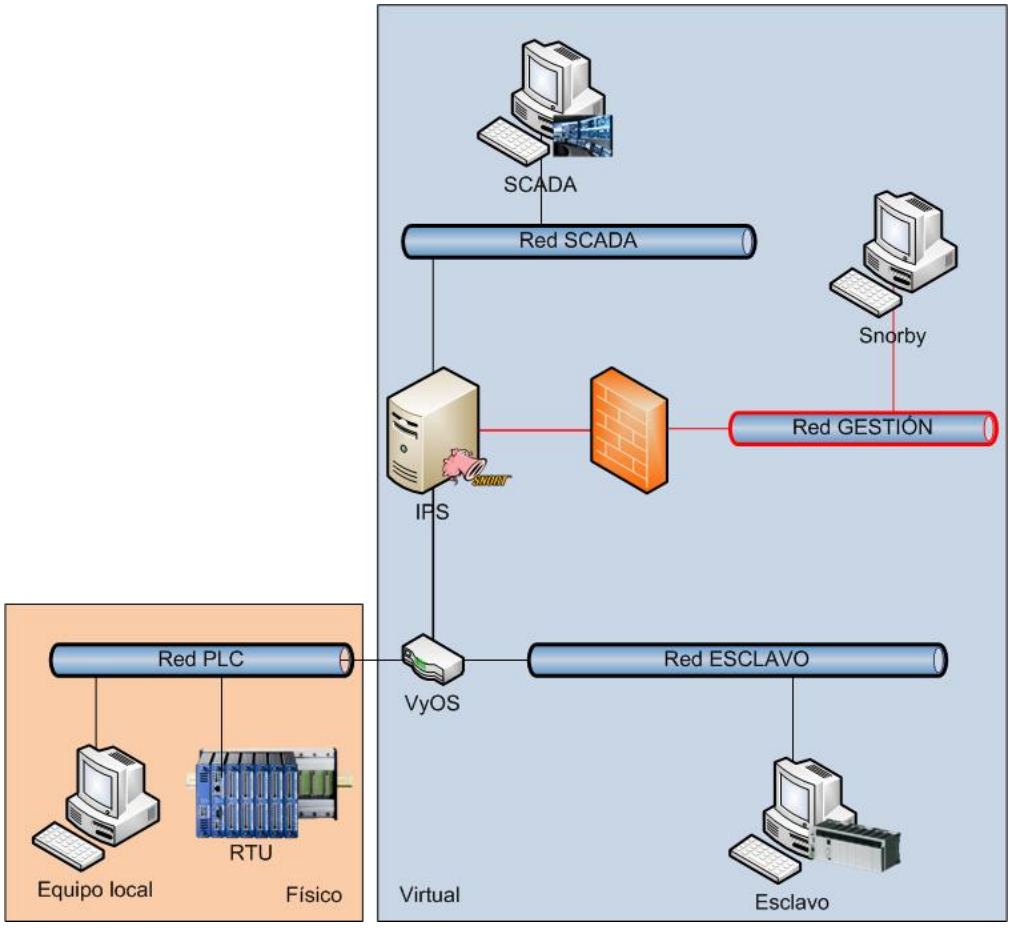

Figura 6: Arquitectura de despliegue en laboratorio

5.3 Diseño de redes

Para llevar a cabo una simulación lo más real posible se ha optado por una división en tres niveles. En el nivel 1, de acuerdo a la pirámide SCADA, se encuentran dos redes de campo separadas, una de nombre red PLC, que agrupa equipamientos reales; y otra de nombre red ESCLAVO, que agrupa a equipos de simulación virtuales. El nivel 2 se corresponde con la red SCADA, donde se sitúa el equipo que hace la recolección de todos los datos provenientes de campo. A nivel 3 se sitúa la red de gestión, donde se posiciona el equipo encargado de la gestión de los eventos producidos por el IPS.

El router es el encargado de realizar las comunicaciones entre los diferentes rangos de red.

El IPS se ha de configurar de manera que cuando no esté en funcionamiento el tráfico entre la red SCADA y las redes PLC y ESCLAVO se puedan seguir realizando de manera normal.

Para todas las máquinas de la red hay que determinar si se va a hacer uso de IPv6, en caso de que no sea necesario será conveniente desactivar este protocolo.

5.3.1 Creación de bridge

La máquina que alberga el IPS, en este caso Snort, requiere de la configuración de un bridge.

El IPS ha de ser trasparente para la red, de manera que no sea detectado ni interfiera en las comunicaciones. Para ello, las interfaces de red que utiliza no han de disponer de IP.

Para configurar el traspaso de información entre las dos interfaces que realizan el análisis se ha de definir un puente que las una para cuando el IPS no está en funcionamiento. Para ello hay que realizar cambios en la configuración de red.

Lo primero de todo es instalar el paquete que permite realizar los puentes.

```
apt install bridge-utils
```

Posteriormente hay que configurar la interfaz puente.

```
/etc/network/interfaces
auto br0
iface br0 inet manual
     bridge-ports eth0 eth1
     bridge_stp off
     bridge_fd 0
```

Cuando el IPS esté en funcionamiento, este puente debe ser desactivado, para lo que será necesario modificar algunos ficheros de configuración del IPS para que lo haga de forma automática o hacerlo de forma manual con los siguientes comandos:

```
ifconfig br0 down
"Ejecución del IPS"
ifconfig br0 up -arp
```

5.4 Instalación de Snort

Para instalación de SNORT en el laboratorio se ha utilizado un equipo Ubuntu Server 16.04. La instalación en Linux del IPS sigue el mismo proceso de instalación que cualquier otro paquete de Linux.

```
apt install snort
```

La carpeta de instalación del IPS es ***/etc/snort***, y ahí quedarán tanto los ficheros de configuración como los relacionados con las reglas de funcionamiento.

Como se pretende poner el IPS en modo INLINE, es necesario instalar también el complemento Data AcQuisition library (DAQ).

Hemos de recordar que un sistema IDS/IPS en un sistema de control puesto en modo INLINE bloqueando tráfico solo debe hacerse después de un estudio muy concienzudo de la información en tránsito para estar totalmente seguros de que no se va a bloquear en ningún momento ninguna orden de control. La habilitación del modo INLINE puede realizarse después de haber analizado el tráfico utilizando el modo IDS o el modo INLINE TEST.

El DAQ hay que descargarlo directamente de la página de Snort.

```
wget https://www.snort.org/downloads/snort/daq-X.X.X.tar.gz
tar zxf daq-X.X.X.tar.gz
cd daq-X.X.X
./configure
make && make install
ldconfig
```

Tener en cuenta que ha de indicarse la versión de DAQ a instalar.

5.4.1 Dependencias

Para la ejecución de Snort y DAQ son necesarias una serie de librerías. Éstas deben instalarse previamente a la instalación de los otros dos componentes, ya que sino fallarán.

```
apt install libdnet libdnet-dev libpcap-dev make automake gc flex bison libdumbnet-dev
```

Algunas librerías han cambiado de nombre y es necesario crear un enlace simbólico a una de ellas para que todo funcione de manera correcta.

```
ln -s /usr/include/dumbnet.h /usr/include/dnet.h
ldconfig
```

5.4.2 Configuración

La configuración general de Snort se encuentra en el fichero snort.conf. Además de los cambios realizados en este fichero es necesario realizar modificaciones en otros ficheros de configuración.

5.4.2.1 Snort.conf

Dentro del fichero de configuración de Snort es necesario modificar algunos parámetros para que el sistema pueda funcionar como un IPS INLINE. Buscar los valores y cambiarlos en el lugar correcto de **snort.conf**.

```
ipvar HOME_NET 192.168.1.0/24  #Modificar al rango de red concreto
ipvar EXTERNAL_NET !HOME_NET


config daq: afpacket
config daq_mode: inline
```

En este mismo fichero se han de configurar los ficheros de reglas a utilizar. Por defecto viene una selección preconfigurada de ficheros y reglas que podremos personalizar.

Será importante añadir las reglas que correspondan a los sistemas industriales, que pueden descargarse del proyecto Quickdraw de DigitalBond.

```
#
#------------------------
# MODBUS TCP RULES
#------------------------
#
#
drop tcp !192.168.3.30 any -> 192.168.1.99 502 (content:"|00 00|"; offset:2; depth:2; pcre:"/[\S\s]{
3}(\x05|\x06|\x0F|\x10|\x15|\x16)/iAR"; msg:"Modbus TCP - Escritura desde maestro no autorizada"; cl
asstype:personalizado; sid:1000004; rev:1; priority:1;)
drop tcp 192.168.3.30 any -> !192.168.1.99 502 (msg:"Modbus TCP - Lectura de esclavo no autorizado";
 classtype:personalizado; sid:1000005; rev:1; priority:3;)
root@Snort:/etc/snort/rules#
```

Figura 7: Regla de bloqueo de determinados paquetes de tráfico Modbus

5.4.2.2 Otros cambios

Al estar en modo INLINE, también es necesario modificar el fichero **snort.debian.conf** (notar que este fichero puede variar de nombre dependiendo de la distribución Linux que se esté utilizando).

```
DEBIAN_SNORT_INTERFACES = "eth0:eth1" #poner las dos interfaces sobre las que va a
                                      #estar inspeccionando el tráfico Snort
```

5.4.2.3 Ejecución

Una vez realizados todos los cambios de configuración necesarios ya se puede iniciar Snort para que realice su función de IPS. Como se ha mencionado anteriormente, es necesario desactivar el bridge antes de la ejecución.

```
Snort -Q -i eth0:eth1 -c snort.conf
```

5.4.3 Barnyard

Snort genera alertas locales de las reglas que tenga configuradas. En una arquitectura de seguridad, las alertas generadas deben enviarse a un sistema de gestión de eventos. Para realizar esta tarea se va a utilizar el complemento de Snort denominado Barnyard2.

Barnyard2 es capaz de monitorizar el fichero de salida de alertas de Snort y enviarlo a una base de datos remota para su almacenamiento. Esta funcionalidad existía en las versiones antiguas de Snort, pero en las nuevas se ha suprimido.

Lo primero de todo es instalar barnyard2 y todas sus dependencias.

```
apt install libtool

git clone https://github.com/firnsy/barnyard2.git
```

Una vez descargado se ha de proceder a la instalación y configuración

```
./autogen.sh

./configure

make && make install
```

Posteriormente hay que indicarle a Barnyard dónde debe enviar las alertas. Esta configuración se recoge en el fichero **barnyard.conf**.

```
output database alert,mysql user=usuario password=contraseña dbname=nombre_bbdd
host=host_remoto
```

Dónde:

- Usuario: usuario definido en la base de datos mysql de destino
- Contraseña: contraseña del usuario
- Nombre_bbdd: Nombre de la base de datos definida en destino
- Host_remoto: IP o nombre del host remoto al que enviar las alertas

Ahora es necesario indicar a Snort que realice una salida en un formato que Barnyard pueda entender. Para ello es necesario modificar la salida en el fichero **snort.conf**.

```
output unified2: filename fichero limit 128
```

Dónde:

- Fichero: fichero de la salida de las alertas de snort

Para llevar un registro de las alertas que ya han sido enviadas a la base de datos entre diferentes ejecuciones de barnyard2 es necesario crear un fichero de persistencia, que dejaremos en la misma carpeta que los logs a enviar.

```
touch /var/log/snort/bardyar2.waldo
```

Una vez que se ha realizado toda la configuración ya se puede arrancar barnyard2 (notar que la base de datos a la que se envían los logs debe existir)

```
barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.conf -w
/var/log/snort/barnyard2.waldo
```

```
Opened spool file '/var/log/snort/snort.log.1481889496'
Waiting for new data
12/16-12:58:31.145903  [**] [1:1000005:1] Modbus TCP - Lectura de esclavo no autorizado [**] [Classi
fication: intento acceso modbus] [Priority: 1] {TCP} 192.168.3.30:1083 -> 192.168.1.91:502
INFO [dbProcessSignatureInformation()]: [Event: 1] with [gid: 1] [sid: 1000005] [rev: 1] [classifica
tion: 39] [priority: 3] Signature Message -> "[Modbus TCP - Lectura de esclavo no autorizado]"
        was not found in barnyard2 signature cache, this could mean its is the first time the signa
ture is processed, and will be inserted
        in the database with the above information, this message should only be printed once for ea
ch signature that is not  present in the database
        The new inserted signature will not have its information present in the sig_reference table
,it should be present on restart
        if the information is present in the sid-msg.map file.
        You can always update the message via a SQL query if you want it to be displayed correctly
by your favorite interface
```

Figura 8: Envío de alertas de Snort a Snorby a través de Barnyard2

5.5 Recogida y análisis de alertas y eventos

En todo sistema de seguridad que se precie, la recolección y análisis de las alertas generadas es algo muy valioso. Las alertas generadas por Snort son complejas de manejar al estar recogidas en un fichero de texto, por lo que para facilitar su manejo, se ha hecho uso de un sistema de gestión de eventos, en este caso Snorby.

5.5.1 Dependencias

Snorby requiere de varios paquetes accesorios para poder funcionar. Los principales son la base de datos para guardar toda la información que en será mysql, y el apache para poder desplegarlo, ya que se trata de una aplicación web.

Las dependencias previas necesarias a instalar:

```
apt install apache2 apach2-dev mysql-server libmysqlclient-dev ruby-full
postgreesql-server-dev-9.5 libcurl4-apoenssl-dev
```

5.5.2 Instalación y configuración Snorby

La instalación de Snorby comienza con la creación de la base de datos para almacenar toda la información de las alertas recibidas.

```
mysql -u root -p
> create database snorby;
> create user 'usuario@'%' identified by 'contraseña'
> grant all privileges on snorby.* to usuario@'%' with grant option;
> flush privileges;
> quit
```

Dónde:

- Usuario: nombre del usuario a utilizar por Snorby en la base de datos
- Contraseña: Contraseña seleccionada para el usuario definido.

Seguidamente descargaremos Snorby y lo copiamos a la carpeta de despliegue del apache.

```
git clone https://github.com/Snorby/snorby.git
cp -r snorby /var/www/html
```

Debido a cambios de versiones, es necesario modificar el fichero **Gemfile**

```
gem 'rake', '0.9.2' → gem 'rake', '> 0.9.2'
despues de gem 'json','X.X' añadir → gem 'thin'
en el apartado group (:development) to comentar → gem 'thin'
```

Y el fichero Gemfile.lock

```
rake (0.9.2) → rake (0.9.2.2)
```

Posteriormente es necesario instalar las gemas de ruby y crear los ficheros de configuración.

```
gem install rails bundler passenger wkhtmltopdf do_postgres -v '0.10.16'
bundle install
```

```
cp config/snorby_config.yml.example config/snorby_config.yml

cp config/database.yml.example config/database.yml
```

La configuración de acceso a la base de datos se encuentra en el fichero **database.yml**, donde habrá que especificar la base de datos y el usuario creados previamente.

Para que la integración de Snorby y ruby con Apache sea correcta es necesario instalar un módulo:

```
passenger-install-apache2-module
```

Al final de la instalación se mostrarán una serie de líneas que deberán ser añadidas al fichero **snorby.conf**. Este fichero no existe y debe ser creado previamente:

```
touch /etc/apache2/sites-available/snorby.conf
```

Las líneas serán similares a las siguientes:

```
LoadModule passenger_module /var/lib/gems/2.3.0/gems/passenger-5.0.30/buildout/apache2/mod_passenger.so

PassengerRoot /var/lib/gems/2.3.0/gems/passenger-5.0.30

PassengerDefaultRuby /usr/bin/ruby2.3
```

Además de las lineas anteriores, se han de añadir también las siguientes líneas al fichero **snorby.confs**:

```
Servername 192.168.1.200

DocumentRoot /var/www/html/snorby/public

<Directory /var/www/html/>

 AllowOverride all

 Order allow,deny

 Allow from all

 Options –MultiViews

</Directory>
```

Para que Snorby lea adecuadamente la configuración es necesario crear un enlace simbólico y eliminar el fichero de configuración por defecto.

```
ln -s /etc/apache2/sites-available/snorby.conf /etc/apache2/sites-enabled/snorby.conf

rm /etc/apache2/sites-enabled/000-default.conf
```

Ahora ya se puede arrancar Snorby para mostrar las alertas de Snort.

```
RAILS_ENV=production bundle exec rake snorby:setup
```

El acceso se realiza a través del navegador. El primer acceso se realiza con las credenciales:

- Usuario: snorby@example.com
- Contraseña: snorby

Una vez dentro es importante cambiar la contraseña a este usuario y crear todos aquellos nuevos que sean requeridos.

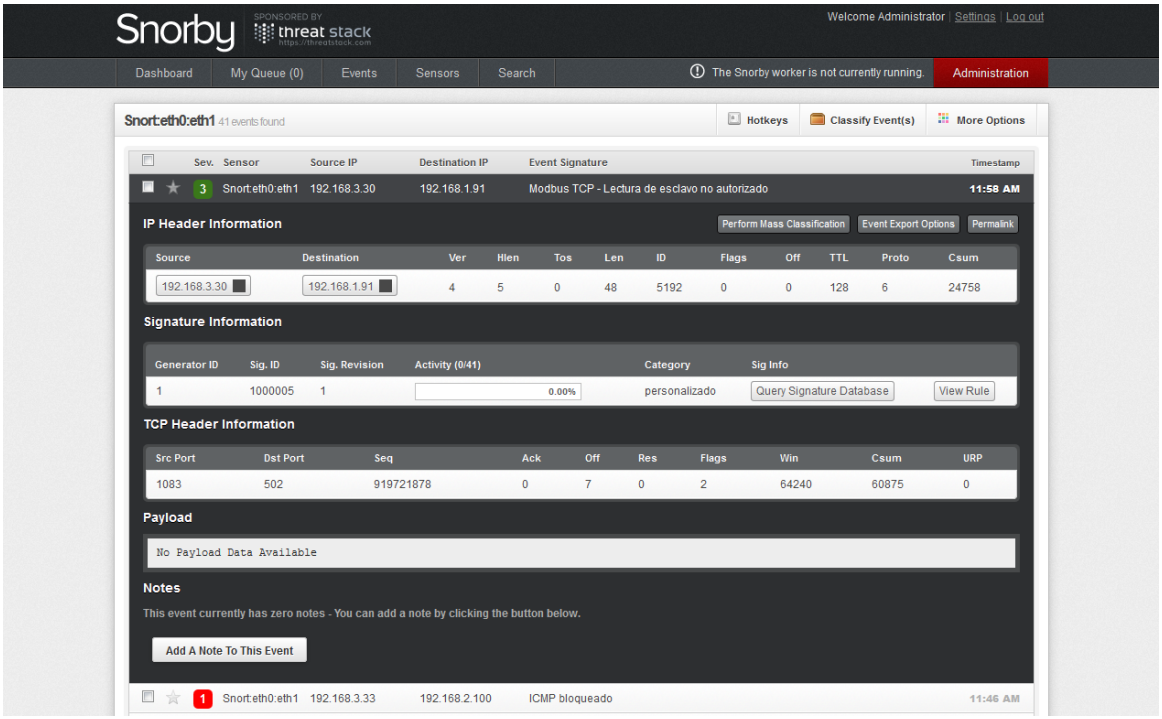

Figura 9: Alerta de Snort recogida en Snorby

6 CONCLUSIONES

Los sistemas de detección y prevención de intrusiones y los sistemas de tratamiento y gestión de eventos e incidentes aportan un nivel de seguridad a los sistemas de control siempre y cuando estén correctamente configurados y supervisados.

La configuración de un sistema de prevención puede implicar muchos problemas sobre un sistema de control en producción, por lo que deben ser correctamente valoradas todas las implicaciones, así como realizar todas las posibles pruebas previamente, incluyendo las de mantener el sistema sólo en modo detección hasta estar totalmente seguros de que no se bloqueará tráfico crítico para el sistema e ir afinando progresivamente el sistema para que sólo detecte o informe de eventos importantes.

Los SIEM proporcionan información del estado del sistema a los operadores de seguridad, pero sólo son útiles si la información recogida es correctamente analizada. Centralizar todos los eventos en un único equipamiento tiene la ventaja de que todas las acciones ocurridas van a ser controladas en el mínimo tiempo y no se van a perder por tener que revisar múltiples aplicaciones.

La inclusión de estas herramientas en la arquitectura de los sistemas de control puede ser compleja dependiendo del sistema que se quiera controlar, pero los beneficios van a compensar todo el esfuerzo invertido en el despliegue, ganando un control en la red y que permite asegurar el correcto funcionamiento del sistema sin intrusiones.

ANEXO 1. FUNDAMENTOS DE LAS TECNOLOGÍAS MONITORIZACIÓN

ANEXO 1.1. DEFINICIONES

Todos los sistemas que se tratan en el presente estudio son conocidos por el personal de seguridad lógica de los sistemas empresariales, pero no todo el personal involucrado en los sistemas de control industrial los conoce. Por ello es necesario realizar una definición de cada uno de los sistemas a tratar.

ANEXO 1.1.1. IDS

El sistema de detección de intrusiones consiste en un conjunto de métodos y técnicas para revelar actividad sospechosa sobre un recurso o recursos informáticos. Es decir, eventos que sugieran un comportamiento anómalo, incorrecto o inapropiado sobre un sistema.

ANEXO 1.1.2. IPS

Los IPS son dispositivos de hardware o software encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. La respuesta consiste en descartar o modificar los paquetes procedentes del ataque de tal manera que se anule su propósito. Este comportamiento los clasifica como dispositivos proactivos debido a su reacción automática a situaciones anómalas.

ANEXO 1.1.3. SIEM

Las soluciones SIEM son una solución híbrida de las categorías de productos como SIM (*Security Information Management*) y SEM (*Security Event Manager*). La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red. Las soluciones SIEM pueden venir como software, aplicaciones, o administración de servicios, y también son utilizados para registrar datos de seguridad y generar reportes para fines de cumplimiento.

ANEXO 1.2. IDS

Un sistema de detección de intrusiones (*Intrusion Detection System*) puede ser descrito como un proceso de detección y monitorización de eventos que suceden en una red. Este sistema escucha y analiza toda la información que circula por una red, permite ayudar a entender los ataques, estimar los daños causados y tratar de prevenir otros ataques.

Para detectar intrusiones en un sistema, los IDS utilizan tres tipos de información: un histórico de eventos, la configuración actual del sistema y, finalmente, procesos activos del sistema o reglas.

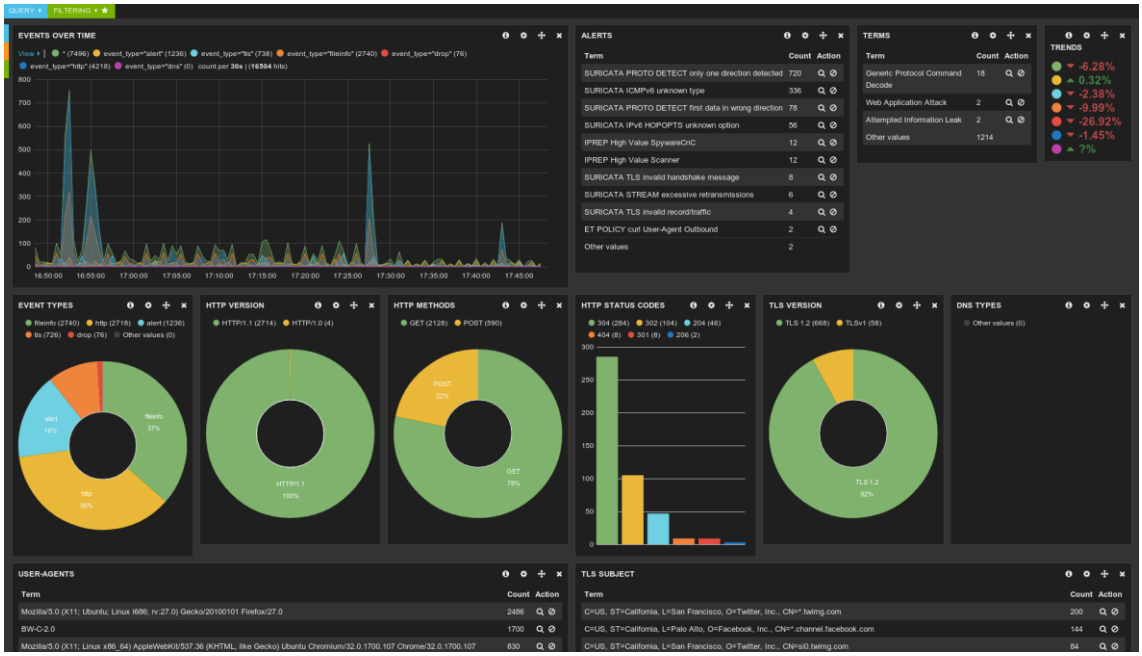

Figura 10: Panel de control de Suricata. Fuente: https://suricata-ids.org/tag/dns/

ANEXO 1.2.1. Tareas de un IDS

Un IDS realiza dos tareas fundamentales:

- Prevención: se realiza por medio de herramientas que escuchan el tráfico en la red o en un ordenador, denominados sensores, e identifican los ataques aplicando reglas, reconocimiento de patrones o técnicas inteligentes.
- Reacción: trata de detectar patrones de intrusión en las trazas de los servicios de red o en el comportamiento del sistema.

Existen indicadores estadísticos de sensibilidad, especificidad y precisión que permiten comprobar la efectividad del IDS, se basan en los siguientes conceptos:

- Verdaderos positivos (TP): Intrusión existente y correctamente detectada.
- Falsos positivos (FP): Intrusión no existente e incorrectamente detectada.
- Falsos negativos (FN): Intrusión existente y no detectada.
- Verdaderos negativos (TN): Intrusión no existente y no detectada.

ANEXO 1.2.2. Tipos de IDS

Existen distintas clasificaciones de los IDS, según sea su enfoque, origen de datos, estructura y comportamiento.

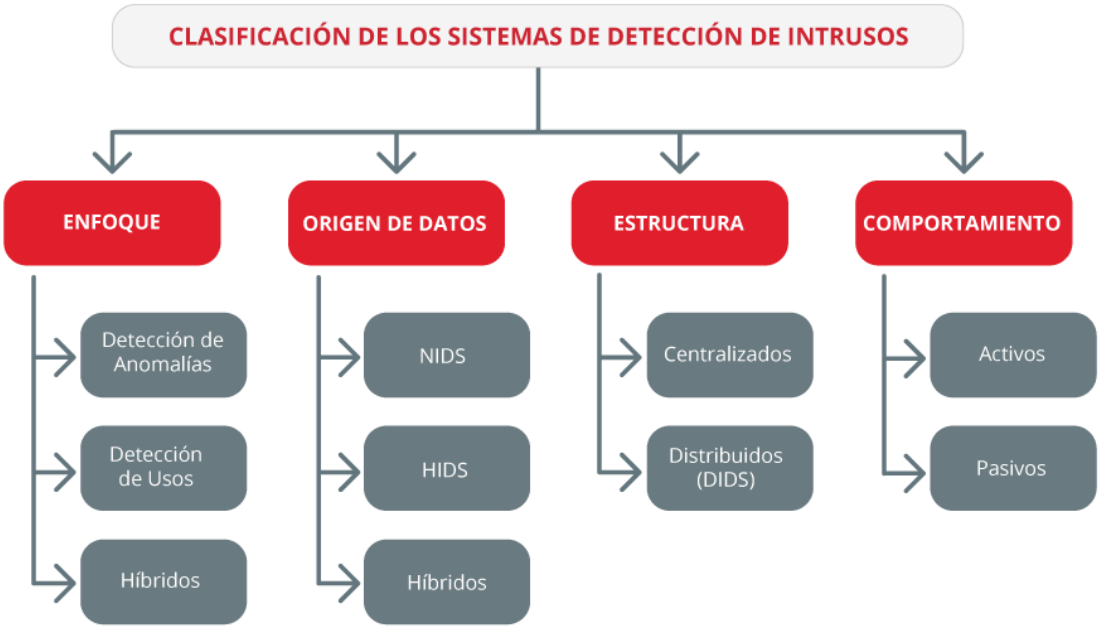

Figura 11: Clasificación de los IDS. Fuente [1]

ANEXO 1.2.3. En función del enfoque

Se presentan dos grupos: Los sistemas de detección de usos indebidos, que comparan las firmas con la información recogida; y los de detección de anomalías, que usan técnicas estadísticas para distinguir el comportamiento usual del anormal.

- **Detección de anomalías:** Es necesario definir cuál es el comportamiento normal de un sistema por medio de un aprendizaje de actividades, para clasificar los comportamientos que se desvíen de lo normal como sospechosos.

  Estos sistemas son propensos a dar falsos positivos, que son producidos cuando se dispara una alerta con actividad normal. Tienen la desventaja de que depende de la calidad del proceso de aprendizaje.

  Existen tres técnicas diferentes para realizar la detección de anomalías en un sistema:

  - Sistemas basados en conocimiento: Representa el inicio en los IDS, y se basa en las violaciones de seguridad detectadas mediante el uso de reglas. Resultan más fiables y proporcionan mejores rendimientos frente a ataques conocidos, con el inconveniente de su baja capacidad para detectar nuevos ataques no incluidos en la base de datos de firmas.
  - Sistemas basados en métodos estadísticos: Basado en perfiles de actividad que vienen definidos por el comportamiento del usuario, con respecto a ficheros, programas, registros, etc. Se realiza mediante el establecimiento de métricas y modelos estadísticos.
  - Sistemas basados en aprendizaje automático: Son los más desarrollados para el modelado de comportamientos normales y buscan mejorar los resultados en cuanto a detección, reducción de falsos positivos y tiempo de computación. Una ventaja reside en recoger las características de un ataque y añadirlo a una base de datos como firmas nuevas, permitiendo actualizar la base de firmas en un breve lapso de tiempo.

- **Detección de usos incorrectos (detección por firma/regla):** Los sistemas de detección basados en uso indebido monitorizan las actividades que ocurren en un sistema y las compara con una base de datos de firmas de ataques. Cuando se encuentra una actividad que coincide con una de estas firmas, se genera una alarma.

  Presentan una facilidad de adaptación ya que basta con actualizar la base de datos, ya sea, escribiendo la nueva regla u obteniéndola de un tercero.

  - Sistemas Expertos: Conocimiento codificado mediante reglas de implicación (condición-acción), si se cumplen todas las condiciones se aplica la acción o regla. Presenta la desventaja de que las reglas no son secuenciales, lo que dificulta aislar pasos de intrusiones en el tiempo.
  - Detección de firmas: Realiza comparaciones entre los eventos que ocurren en el sistema y las firmas almacenadas en la base de datos en busca de similitudes.
  - Análisis de transacción de estados: Los ataques se representan como una secuencia de transiciones (máquina de estados finitos). Cuando se alcanza un estado considerado como intrusión se lanza una alarma.

- **Híbridos:** Los IDS basados en firmas resultan más fiables y proporcionan mejores rendimientos frente a ataques conocidos, pero presentan una deficiencia ante nuevos ataques. Los IDS basados en anomalías presentan la capacidad de detectar ataques desconocidos, pero su rendimiento es inferior. Los sistemas híbridos serán una mezcla de ambos, y por lo tanto, pueden ajustarse para operar como ambos tipos de detectores, mejorando la funcionalidad, la detección de ataques y la mejora de rendimiento.

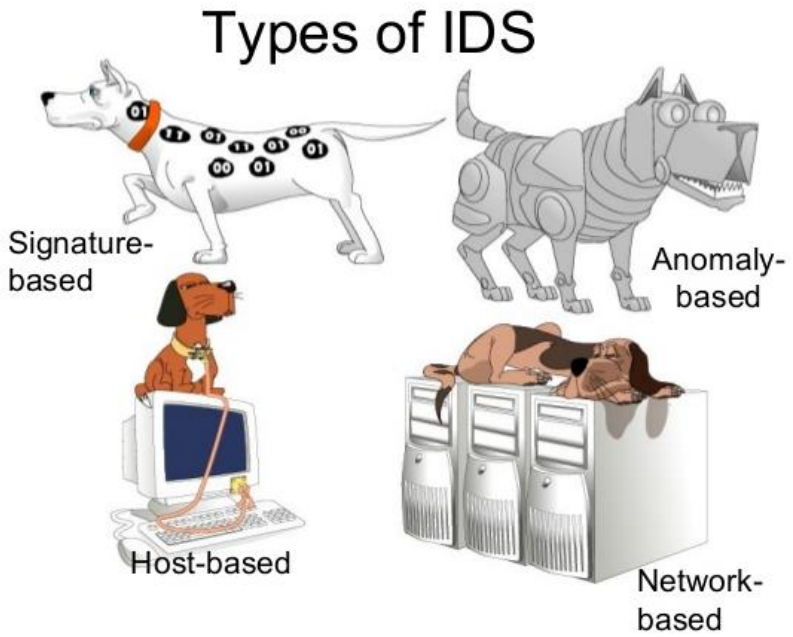

Figura 12: Tipos de IDS [2]

ANEXO 1.2.4. En función del origen de los datos

Se encuentran tres tipos de IDS atendiendo a las fuentes de información que se utilicen:

- **HIDS (*Host-based Intrusion Detection Systems*):** Los IDS basados en el host solo procesan información de las actividades de los usuarios y servicios en una

máquina determinada. Permite monitorizar los datos generados por un usuario, mediante el uso de *syslog*[1], e identificar amenazas e intrusiones a nivel de host.

Una desventaja proviene del requerimiento de confianza en el sistema, que puede estar infectado anteriormente a la instalación, y lo hace vulnerable ante ataques directos.

- **NIDS (*Network Intrusion Detection Systems*):** Los NIDS son instalados en un dispositivo en modo promiscuo, realizan una escucha pasiva sobre la red de forma que no interfieren en su uso, analizando el tráfico en tiempo real, pero por contra, resultan inútiles ante ataques locales.

  Los nuevos sistemas, basados en agentes inteligentes, permiten una detección de nuevos ataques usando el concepto de centinelas, que supervisan el sistema para recoger toda la información necesaria para la detección.

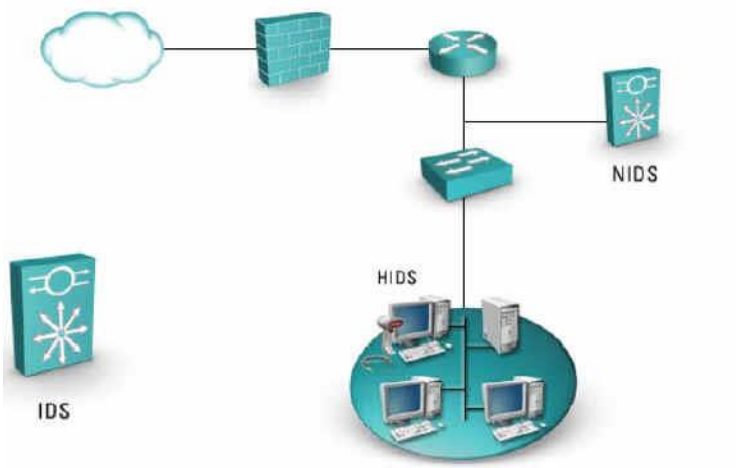

Figura 13: IDS en función de los orígenes de datos. Fuente: Internet [2]

- **IDS Híbridos:** Los sistemas híbridos recogen lo mejor de ambos tipos HIDS y NIDS. Permiten una detección local de los sistemas y un sensor en cada segmento de red se encarga de la vigilancia. De esta forma se cubren las necesidades HIDS con las del NIDS, permitiendo el aprovechamiento de las ventajas de ambas arquitecturas.

ANEXO 1.2.5. En función de su estructura

Clasificación basada en las estrategias de control:

- **Sistema de Detección de Intrusión Distribuido (DIDS):** Se basa en la instalación en un sistema distribuido, ubicando sensores repartidos por varios equipos de la red. Estos sensores se comunican con un nodo central donde se recibirá toda la información y donde se cruzan los datos, lo que nos permitirá detectar los ataques con fiabilidad y obtener una visión global mejorando la detección de incidentes.

[1] http://www.ietf.org/rfc/rfc3164.txt

[2] https://hndsanjaya.wordpress.com/category/certified-information-systems-auditor-cisa/

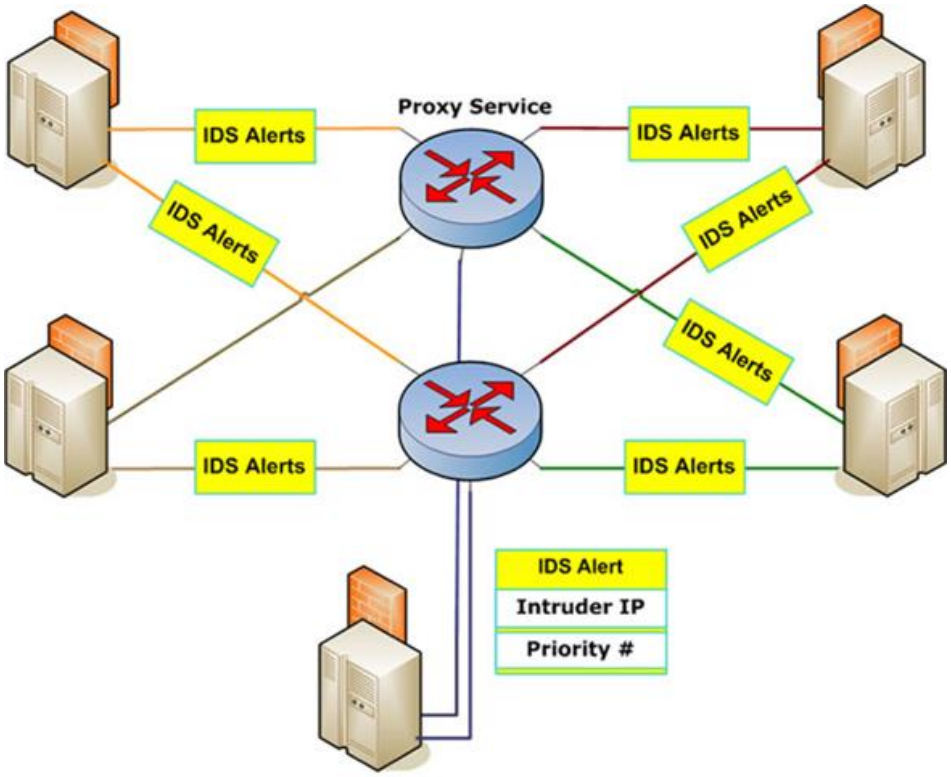

Figura 14: Esquema de un DIDS. Fuente: Internet[3]

- **Sistema de Detección de Intrusión Centralizado:** Emplea sensores que transmiten información a un sistema central que realiza el control, permitiendo ahorrar en equipamientos.

[3] http://monalisa.cern.ch/monalisa__Service_Applications__Intrusion_Detection.html

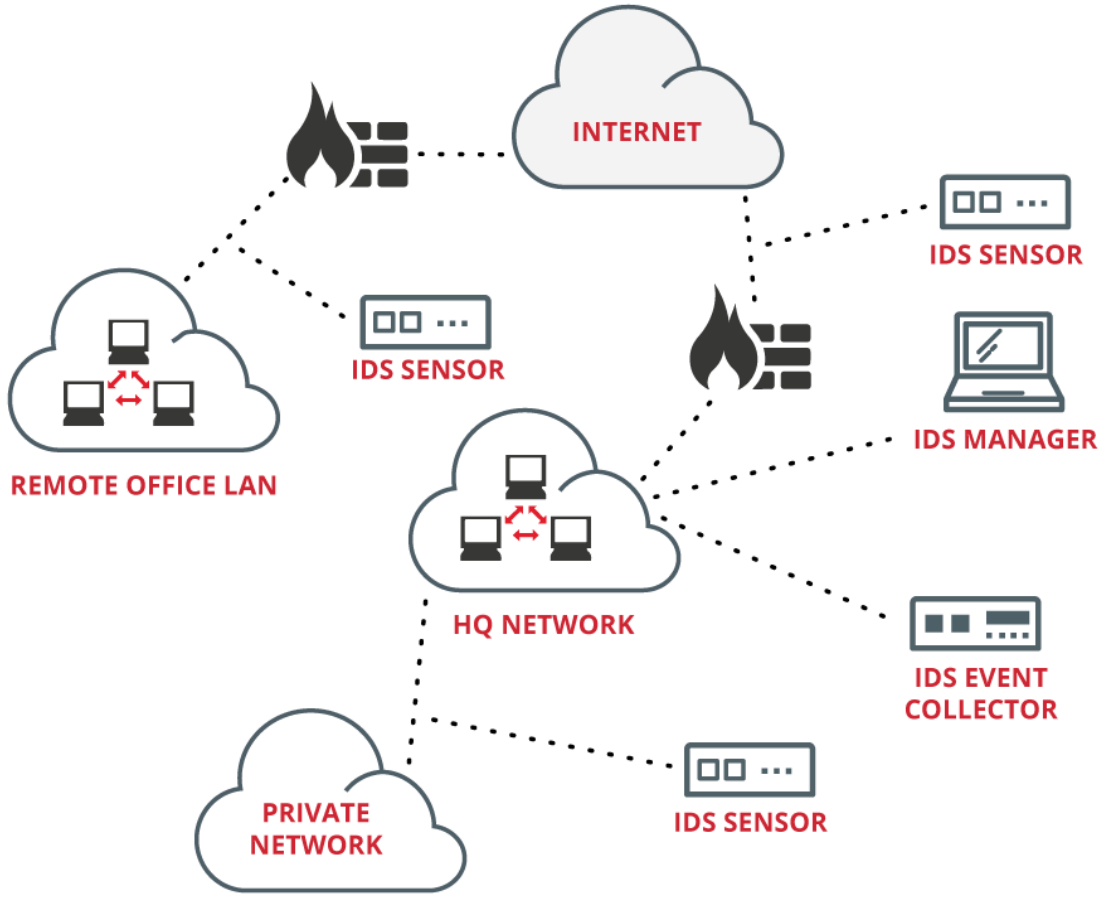

Figura 15: Ejemplo de IDS Centralizado. Fuente: Internet[4]

Anexo 1.2.5.1. En función de su comportamiento

Encontramos dos tipos de IDS según si realizan la prevención escuchando el tráfico o si se elabora una respuesta defensiva cuando se detecta un ataque.

- **IDS Pasivo:** Sólo notifican al administrador de la red pero no actúan sobre el ataque. Únicamente procesan la información en busca de intrusiones, y una vez detectada se genera una alerta.
- **IDS Activos:** Es un tipo de IDS denominado Sistema de Prevención de Intrusión (IPS). A diferencia de los IDS, esta tecnología no se limita a escuchar el tráfico de la red y a mandar alertas, sino que permite establecer reglas, como se lo hace en los cortafuegos, para detener las intrusiones.

ANEXO 1.3. IPS

Los IPS se asemejan el comportamiento de los cortafuegos, ambos toman decisiones sobre la aceptación de paquetes en un sistema. Sin embargo, los cortafuegos basan sus decisiones en los encabezados de paquetes entrantes, capas de red y de transporte, mientras que los IPS basan sus decisiones tanto en los encabezados como en el contenido de datos del paquete.

[4] http://www.xanatech.net/products/index.htm

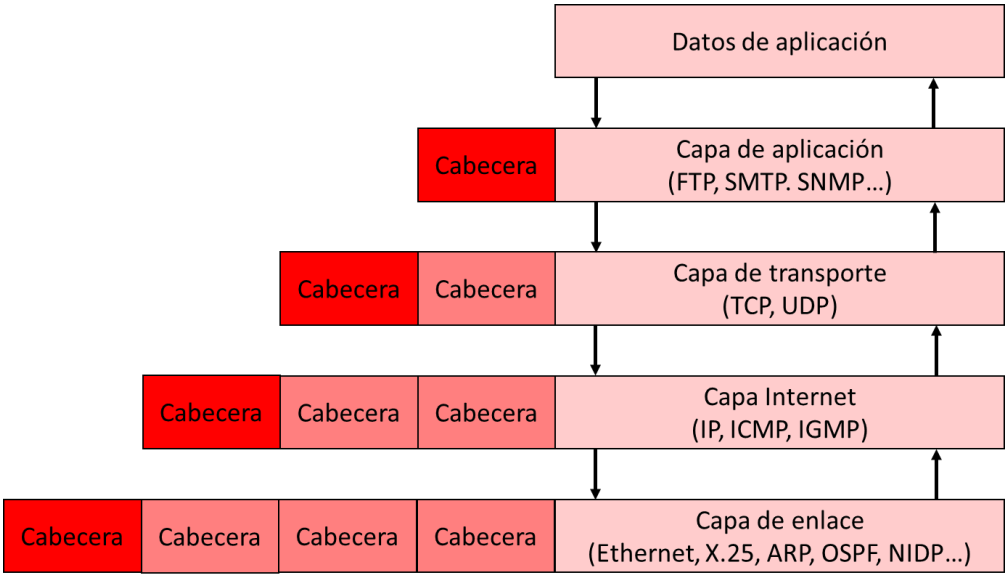

Figura 16: Encabezado y contenido de paquetes dependiendo del protocolo.

La tecnología IPS ofrece una visión más exhaustiva de las operaciones de la red proporcionando información sobre todo tipo de actividades maliciosas, malas conexiones, contenido inapropiado y otras funciones, con una mínima vigilancia.

Las principales características de esta tecnología son:

- Capacidad de reacción automática ante incidentes.
- Aplicación de nuevos filtros conforme detecta ataques en progreso.
- Bloqueo automático frente a ataques efectuados en tiempo real.
- Disminución de falsas alarmas de ataques a la red.
- Protección de sistemas no parcheados.
- Optimización en el rendimiento del tráfico de la red.

ANEXO 1.3.1. Los IPS como evolución de los IDS

Mientras el IDS se limita a detectar y notificar la intrusión al administrador del sistema, y éste se encarga de recibir y responder las alertas; el IPS detecta la intrusión y la detiene de algún modo ya predefinido, comprobando ciertos comportamientos en la red previamente configurados como anómalos. Gracias a este hecho, el nivel de alertas de un IPS es considerablemente menor que el nivel de alertas producido por un IDS.

La diferencia principal entre los IDS activos y los IPS es que estos últimos están en capacidad de inutilizar los paquetes involucrados en el ataque modificando su contenido.

Una desventaja de los IPS viene por parte de la reacción proactiva ante las intrusiones. Por una parte, se tiene una disminución en el tiempo de reacción ante un ataque, pero también puede provocar efectos inesperados e inconvenientes cuando éste reacciona ante un falso positivo (FP), lo que podría llevar a una denegación de servicio o incluso al aislamiento de la máquina. Por ello, el uso de IPS en sistemas de control industrial ha de ser bien estudiado o en su defecto utilizar un cortafuego que posea inspección profunda de paquetes para mayor seguridad en las comunicaciones.

Las arquitecturas actuales centralizan el funcionamiento del IPS, lo que facilita su operación y administración, pero disminuye la escalabilidad del sistema y convierte al IPS en un punto crítico.

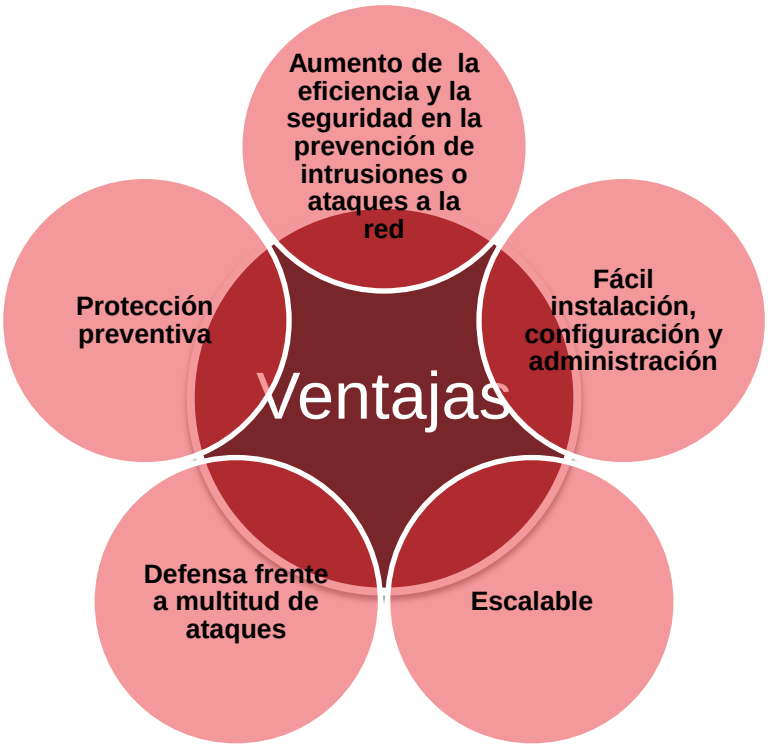

Figura 17: Ventajas de los IPS

ANEXO 1.3.2. Tipos de IPS

Básicamente, los diferentes tipos de IPS se distinguen por su ubicación.

- **IPS basados en host (HIPS):** Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los host.
- **IPS basadas en red (NIPS):** Monitorizan la red en busca de tráfico sospechoso.
- **IPS basado en red Wireless (WIPS):** Monitorizan redes inalámbricas, al igual que hacen los NIPS con redes LAN.
- **IPS basado en Análisis de Comportamiento de Red (NBA):** Examina el tráfico de red para identificar amenazas que generan tráfico inusual, como ataques de DoS o malware.

ANEXO 1.3.3. IPS basado en red (NIPS) vs IPS basado en host (HIPS)

Un HIPS puede manejar el tráfico cifrado y sin cifrar por igual, ya que puede analizar los datos después de que hayan sido descifrados en el host.

Por otra parte, un NIPS no utiliza el procesador y la memoria del host, por lo que no impacta en el rendimiento de la máquina.

Un NIPS puede detectar eventos dispersos a través de la red y puede reaccionar fácilmente, mientras que con un HIPS se tardaría demasiado tiempo en informar a un motor central y posteriormente informar al resto de los equipos.

ANEXO 1.3.4. La evolución y las categorías de los IPS

Es posible distinguir dos generaciones históricas de los IPS:

- Los IPS de primera generación, al detectar un ataque proveniente de una dirección IP determinada, descartaban todos los paquetes de esa dirección, estuvieran o no involucrados en el ataque.
- La evolución de los IPS se debe a la capacidad de descartar únicamente los paquetes relacionados con el ataque identificado, permitiendo el tráfico de otros paquetes provenientes de la IP del atacante, siempre y cuando no estuvieran relacionados con el ataque.

Se pueden distinguir cinco categorías de IPS dependiendo de su funcionamiento, sus capacidades y su ubicación en la arquitectura de la red [9].

ANEXO 1.3.5. IPS *inline*

Estos IPS suponen la evolución de los NIDS basados en firmas y hacen la función de un Bridge a nivel de capa dos, revisando todos los paquetes que circulan por la red en busca de firmas. En caso de detectar alguna anomalía automáticamente es almacenado en un log, o incluso puede permitir el paso de un paquete alterando su contenido para de esta manera frustrar un ataque, sin que el atacante se dé cuenta. Este proceso es realizado mediante *Scrubbing*[5], que consiste en la detección de errores por medio de verificación *checksum* o por redundancia con copias de datos.

Habitualmente son conocidos como IPS de red o NIPS.

Anexo 1.3.5.1. Switches a nivel de la capa de Aplicación (nivel 7 del modelo OSI)

Los switches trabajan de forma habitual en el nivel 2 (enlace) pero cada vez son más habituales también los switches a nivel 7 o aplicación debido a la alta demanda de ancho de banda. La tarea principal de estos switches es balancear la carga de las aplicaciones distribuidas entre varios servidores, tomando decisiones de enrutamiento o conmutación a partir del contenido de los datos de la capa de aplicación. Hasta este punto no hay diferencia con un balanceador de carga.

El funcionamiento como IPS es similar a un NIPS basado en firmas, sirviendo para bloquear ataques. La posición de estos equipos suele ser delante de los cortafuegos, de manera que protejan la red completa. Al ser similares a un NIPS, sólo pueden parar ataques que conocen, pero permiten bloquear ataques de tipo DoS o DDoS que el resto de IPS no pueden parar y sin afectar al resto de la red.

Se pueden configurar de forma redundante, en modo levantamiento en caliente o como balanceador de carga (característica que los diferencia de cualquier otro IPS).

Anexo 1.3.5.2. Cortafuegos/IDS de Aplicación

[5] https://en.wikipedia.org/wiki/Data_scrubbing

Los cortafuegos/IDS de aplicación se instalan en cada host que se desea proteger, teniendo en cuenta las aplicaciones que corren en él, por lo que también son conocidos como HIPS. Para su correcto funcionamiento será necesario hacer una fase de entrenamiento, que consiste en el proceso de identificación de patrones normales de funcionamiento en el host.

Por medio de este entrenamiento se crea un perfil de relaciones frecuentes entre las aplicaciones y los componentes del sistema, como: el sistema operativo, otras aplicaciones, la memoria y los usuarios.

Los HIPS se comportan de forma similar a los IDS basados en detección de anomalías a la hora de detectar las intrusiones, pero deben identificar todos los procesos exhaustivamente, puesto que de no ser así pueden bloquear una aplicación válida.

Debido a que se apoyan en la detección de comportamientos anómalos y no en la coincidencia de firmas, es posible prevenir intrusiones muy recientes para las cuales todavía no existe una definición de sus firmas específicas.

Anexo 1.3.5.3. Switches Híbridos

Los switches híbridos son una combinación entre los HIPS y los switches de nivel de aplicación. Son dispositivos hardware como los switches de nivel de aplicación pero usan políticas similares a las utilizadas por los HIPS.

Los switches híbridos se basan en el análisis de patrones de comportamiento. La fortaleza radica en el conocimiento detallado del tráfico que debe aceptar.

Anexo 1.3.5.4. Aplicaciones engañosas

Este tipo de tecnología analiza todo el tráfico de red y de cada dispositivo en particular para disponer de un conocimiento de cuál es el tráfico permitido y correcto, similar a como realiza los patrones un HIPS.

En el modo de funcionamiento, cuando detecta un tráfico que no está permitido para la red (acceso a un puerto no permitido) o para un servidor concreto (acceso a un puerto SSH a un servidor que no lo tiene abierto), envía una respuesta marcada al atacante, de manera que el IPS puede detectar otro tráfico de esa misma fuente y bloquearlo.

ANEXO 1.4. SIEM

Las siglas SEM, SIM y SIEM se han usado a menudo, aunque el significado correcto del termino SIEM es una combinación de los dos primeros.

- **SEM**: Es el primer área de gestión de la seguridad, se ocupa de la monitorización en tiempo real, correlación de eventos, notificaciones y vistas de la consola que comúnmente se conoce como **Gestión de Eventos de Seguridad (*Security Event Management*)**.
- **SIM**: Ofrece almacenamiento a largo plazo, análisis y comunicación de los datos de eventos, y se conoce como **Gestión de Seguridad de la Información (*Security Information Management*)**.

El término Gestión de la Información de Seguridad y de Eventos (***Security Information and Event Management***) describe múltiples capacidades como la recopilación, análisis y presentación de información de la red y los dispositivos de seguridad. A esto se le añaden

las aplicaciones de gestión de identidades y accesos, gestión de vulnerabilidades y los instrumentos de política de cumplimiento, sistema operativo, base de datos, logs, y datos de amenazas externas.

La clave es monitorizar y ayudar a controlar los privilegios de usuario y de servicio, servicios de directorio y otros cambios de configuración del sistema, así como proporcionar datos para auditoría de eventos, revisión y respuesta a incidentes.

La detección de eventos de interés puede ser a través de cualquiera de los grupos funcionales, con el soporte SEM, capaz de monitorizar en tiempo real; y el SIM, que proporciona un medio eficaz para comparar la gran cantidad de eventos recopilados.

Los SIEM están diseñados para recopilar eventos de seguridad a partir de una amplia variedad de fuentes dentro de una organización. Una vez que el SIEM tiene los eventos, procesa los datos para estandarizarlos, lleva a cabo el análisis de los datos "normalizados", genera alertas cuando detecta actividad anómala, y produce informes a petición de los administradores. Algunos productos SIEM también pueden actuar para bloquear las actividades maliciosas.

ANEXO 1.4.1. Capacidades de detección en tiempo real

La gestión de eventos de seguridad (SEM) proporciona herramientas y funcionalidades en tiempo real o casi para facilitar la gestión de los eventos relacionados con la seguridad, mediante la evaluación de los eventos y la correlación de la información procedente de diferentes fuentes. Al no depender de una sola fuente de información, como lo hacen los IDS / IPS, la función de gestión de eventos puede ayudar a reducir el número de falsos positivos, asegurando que el evento que haya sido descubierto se comunique al resto de sistemas. A medida que la base de datos se actualiza se vuelve más eficaz y diferencia mejor los incidentes de seguridad de los patrones habituales de eventos.

Las tecnologías avanzadas SEM soportan capacidades de visualización de datos, que pueden ayudar al analista de seguridad a evaluar rápidamente los acontecimientos y tendencias. Las funciones de análisis de amenazas y la priorización de eventos proporcionan una asistencia extra al personal de operaciones de seguridad, ya que pueden concentrar sus esfuerzos en la investigación de los eventos que tienen las clasificaciones de amenaza más altas.

Anexo 1.4.1.1. SEM en industria

Las herramientas y funcionalidades proporcionadas por el gestor de eventos de seguridad son a menudo muy competitivas en el sector industrial. Debido al uso de protocolos propietarios de los elementos industriales, se requiere llevar a cabo un aprendizaje exhaustivo; pero gracias a los pocos cambios ocurridos en la red y su alta estabilidad proporciona una seguridad elevada, al poder detectar fácilmente cualquier conexión o mensaje fuera de la transmisión habitual entre las máquinas.

ANEXO 1.4.2. Gestión de archivos de eventos

Las funciones del SIM se caracterizan por el análisis de datos en tiempo no real, a través de la recopilación y estandarización de sistemas dispares y la información centralizada de aplicaciones (por ejemplo, eventos del sistema, pistas de auditoría, registros de eventos y registros de transacciones).

El analista de seguridad puede consultar el archivo y recuperar información a través de consultas estandarizadas; almacenando la información de diferentes sistemas en un solo lugar, de manera cronológica y formalizada.

Las tecnologías avanzadas SIM pueden evaluar estos eventos guardados, a medida que se recogen o bajo demanda, con el fin de examinar comportamientos anómalos en futuros análisis.

El análisis forense se favorece por las funciones de gestión de eventos, mientras que los eventos centralizados ayudan a gestionar los tiempos de retención para cumplir con las leyes y normas aplicables. La capacidad de generación de informes puede simplificar las evaluaciones internas y los ciclos de auditoría de una organización.

Los sistemas SIEM proporcionan detección de eventos por medio de la evaluación en tiempo real de la información y por el análisis forense de eventos previamente almacenados.

Anexo 1.4.2.1. SIM en la industria

Las funciones de recopilación de datos son perfectas para los procesos de auditoría. Por suerte, los datos registrados por los sensores suelen ser muy homogéneos en redes donde los equipos no se modifican durante grandes periodos de tiempo. Es fácilmente detectable cualquier anomalía en los protocolos, valores o tiempos, viendo al instante los cambios producidos por posibles ataques a la red.

ANEXO 1.4.3. Entendiendo un SIEM

Los SIEM requieren de una gran cantidad de planificación antes de que comience la ejecución, identificación y prevención de las violaciones de seguridad. La implementación suele declararse como desalentadora para gran cantidad de empresas, muchas veces siendo externalizada, por ser difícil de ajustar y puede llevar un tiempo considerable antes de obtener resultados deseados.

Existen varias razones que podrían conducir a una empresa a poner en práctica un SIEM, desde el cumplimiento de una norma de gobierno o de industria, pasando por haber sido la víctima de un ataque cibernético, o tal vez obtener un cierto nivel de seguridad antes de firmar un contrato. Independientemente de la convicción, cuando una compañía se decide a implementar un SIEM, tendrá que realizar grandes esfuerzos antes de que comience a ver los resultados.

ANEXO 1.4.4. Implantación del SIEM en redes industriales

La implementación de un SIEM en una red OT conlleva varias dificultades:

- **Ciclos de vida muy largos:** El problema más habitual en los sistemas industriales viene por el ciclo de vida, muchas veces entre 20 y 40 años dependiendo del tipo de industria. Añadir elementos de seguridad a la red o a equipo, pueda afectar, modificar o retrasar la señal de comunicaciones de los PLC u otros equipos, debido a la baja potencia de procesado con la que cuenta. Esto puede conllevar a una problemática asociada a la compatibilidad y al funcionamiento entre los equipos de esa red.

- **Prestaciones:** Los ordenadores que se encuentran en las redes industriales, así como los propios dispositivos industriales, suelen ser equipos poco potentes, desfasados y desactualizados, con las capacidades justas para las tareas de control asignadas. Un antivirus moderno, las herramientas IDS/IPS y otras que son necesarias para el procesamiento de los logs, pueden conllevar incompatibilidades, disminución de potencia los dispositivos o incluso el mal funcionamiento general del sistema.
- **Personal:** Los empleados y técnicos necesarios para la gestión de los SIEM deben tener además los conocimientos suficientes para entender los protocolos y equipos de la red industrial para poder interpretar correctamente los eventos generados.

Anexo 1.4.4.1. Consideraciones de implantación de un SIEM

La implantación de un SIEM requiere un profundo conocimiento de la topología de red y de sus protocolos, y de una comprensión clara de lo que se espera que haga. La mejor manera de implantar un SIEM es por medio de sus dos componentes más importantes por separado, la gestión de las capacidades de registro y seguimiento por una parte y la respuesta ante las alertas por otra.

La primera tarea para la organización será conocer que considera como activo crítico y posteriormente se pasará al estudio de su protección.

Algunas compañías disponen de una variedad de eventos que recopilar y procesar de manera diferente. Antes de que el sistema SIEM sea capaz de proporcionar informes útiles, los diversos eventos deberán ser normalizados para que los datos sean coherentes.

Antes de que una empresa pueda sacar el máximo provecho de su SIEM, deberá configurar el sistema para hacer frente a los datos que se recogen en cada tipo de dispositivo, cómo y dónde se almacenan los datos, y cómo los incidentes crean los avisos, además de gestionar el horario, que también puede ser condicionante a la hora de generar los avisos.

Cada SIEM tiene su propio conjunto de requisitos para la recopilación de eventos. Hay muchos tipos de fuentes de eventos, pero syslog y los registros de eventos de Windows generalmente cubren el 75 por ciento o más del entorno de una empresa.

La seguridad es un proceso y no una operación táctica. Con el fin de obtener los mejores resultados medibles para la inversión en el SIEM deberán elegir las mejores situaciones para incorporar sus sensores distribuidos por la red.

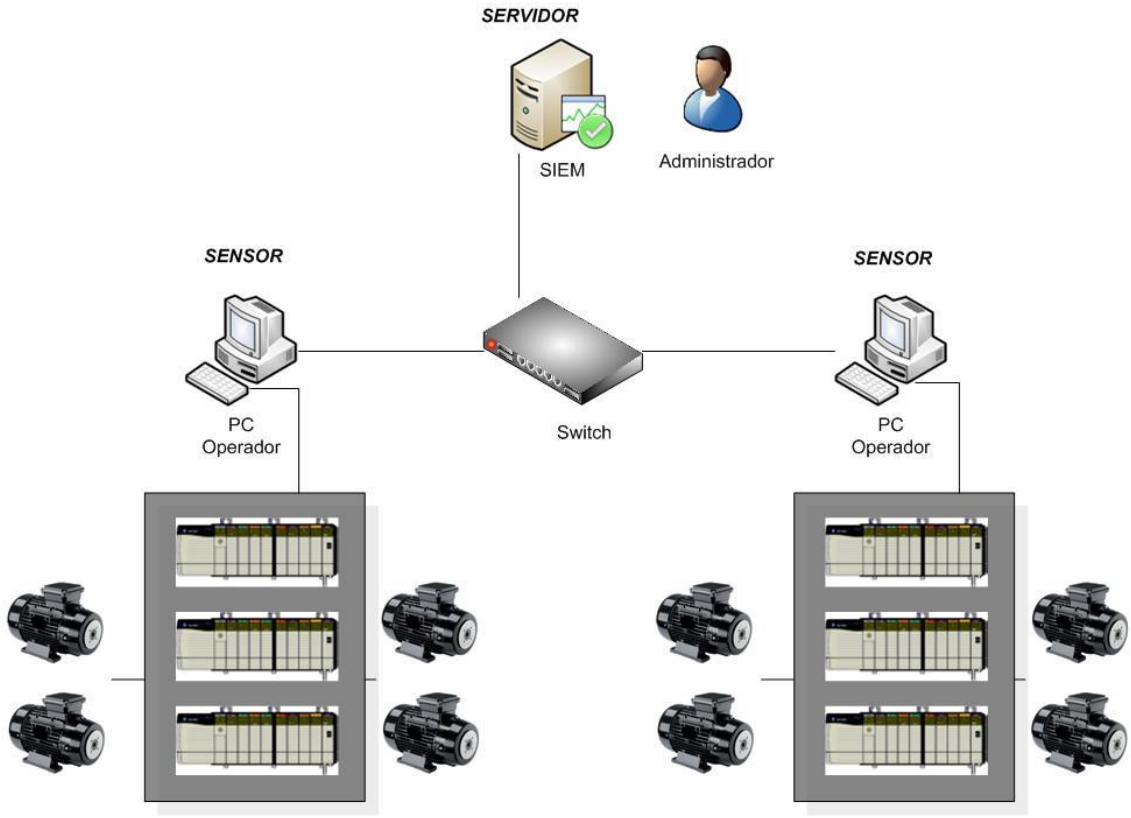

Figura 18: Ejemplo de SIEM en una red industrial

Anexo 1.4.4.2. El camino hacia el éxito SIEM

Hacer funcionar correctamente un SIEM para que sea eficiente y efectivo para la empresa requiere de una serie de pasos y medidas a tener en cuenta:

- Recoger los eventos de las fuentes de seguridad estándar.
- Enriquecer los eventos con datos suplementarios provenientes de otras fuentes.
- Aplicar inteligencia de global de amenazas (listas negras).
- Correlar la información recogida.
- Investigar los eventos generados, realizando seguimiento y corrección.
- Documentar las acciones a realizar, los procedimientos operativos estándar, acuerdos de nivel de servicio, tickets de problema.
- Incorporar nueva información al SIEM mediante la creación de listas blancas o nuevos contenidos.

En algunos casos, una organización podría optar por la gestión externalizada SIEM sobre una empresa especializada en seguridad. En los sistemas IT la gestión se llevaría desde las propias instalaciones de la empresa de seguridad, pero en los sistemas OT es más común que un técnico o más de la empresa de seguridad se desplacen a trabajar conjuntamente en la industria.

Anexo 1.4.4.3. Gestión interna vs externalizada

El beneficio de SIEM dedicado hace que los datos de la empresa nunca salgan al exterior, la empresa tiene control sobre el hardware y los eventos almacenados. Tienen la capacidad de configurar las correlaciones (reglas), la presentación de informes, los períodos de

retención, y otros ajustes para satisfacer sus necesidades. Los SIEM administrados internamente, pueden problemas en la dotación de personal o que el personal asignado pueda ser requerido para otros proyectos o funciones.

La gestión de un SIEM requiere una formación especializada y de unos procedimientos de trabajo normalizados que deben ser creados y mantenidos para cada entorno. Un enfoque fuera de las instalaciones requiere que los eventos se envíen al administrador, y con esto, se pierde la visibilidad.

Las desventajas a las que un cliente se enfrenta cuando se trata de un SIEM externalizado son: la falta de visibilidad y la incapacidad para moverse entre proveedores y mantener los eventos más antiguos. Esta falta de visibilidad provoca problemas con la búsqueda de nuevas amenazas.

Dado que los proveedores de servicios gestionados se suelen especializar en un fabricante de SIEM, son mucho más eficientes y por lo general tienen una mayor experiencia para recurrir a operaciones.

Anexo 1.4.4.4. Capacidades de un SIEM

- **Agregación de datos**: SEM / LM (administración de logs) soluciones para administración de logs desde muchas fuentes, incluyendo redes, seguridad, servidores, bases de datos, aplicaciones, proporcionando la capacidad de consolidar los datos monitorizados para ayudar a evitar la pérdida de los acontecimientos cruciales.
- **Correlación**: busca atributos comunes y relaciona eventos en paquetes o incidentes. Esta tecnología realiza técnicas de correlación para integrar diferentes fuentes, con el fin de convertir los datos en información.
- **Alerta**: el análisis automatizado de eventos correlacionados y la producción de alertas, que serán enviadas al administrador.
- **Cuadros de mando**: SIEM / LM herramienta para transformar los datos y convertirlos en tablas y gráficas informativas que ayuden a reconocer patrones o identificar actividades anómalas.
- **Cumplimiento**: Las aplicaciones SIEM se pueden emplear para automatizar la recopilación de datos y en la elaboración de informes adaptados a normativas existentes.
- **Retención**: SIEM / SIM emplea soluciones a largo plazo de almacenamiento de datos, que constituyen un proceso crítico en la investigación forense, ya que es poco probable que el descubrimiento de una violación de la red sea en el instante en el que se produzca.
- **Redundancia**: Los motores de correlación no requieren ser redundantes, sin embargo, es muy aconsejable que la base de datos si esté redundada para no perder información.
- **Escalabilidad**: Permitir que el sistema sea configurado jerárquicamente, de manera que pueda crecer atendiendo a las necesidades.

Anexo 1.4.4.5. Opciones SIEM basadas en la nube

Un enfoque que está empezando a crecer es el SIEM como un servicio en la nube. Mientras que los proveedores en la nube podrían ofrecer programas especiales para los clientes

SIEMaaS (SIEM as a Service) por primera vez, los proveedores más grandes quieren ofrecer también soluciones SIEM.

Los proveedores deben reconocer que los eventos son propiedad del cliente, y los clientes tienen que entender que los eventos pueden contener información confidencial de la empresa.

Se recomienda que si la empresa recoge datos protegidos, se ha de firmar un acuerdo entre ambos para asegurar que los datos se manejan apropiadamente.

A diferencia tradicional, en el software SIEM basado en la nube generalmente se factura en función del modelo de uso, y no por servidor o por usuario. Sin embargo, si el software SIEM envía todos los eventos a la nube, o de lo contrario se configura incorrectamente, el costo del ancho de banda del proveedor de la nube podría ser alto.

Las empresas más pequeñas pueden encontrar mayores beneficios en la utilización de un proveedor de servicios que ofrece seguridad basada en SaaS o un proveedor de servicios de seguridad gestionada (MSSP) que va a proporcionar algunas de las demandas en curso.

Anexo 1.4.4.6. SIEM Open Source

Existe una gran multitud de ofertas y opciones, en este estudio nos centraremos en uno de los SIEM más conocidos y populares, se trata de Security Onion, desarrollado por Doug Burks, creando una implementación o unión de todos los programas libres para el trabajo con IDS/IPS de una forma muy sencilla de instalar, permitiendo instalar software de terceros como Splunk por medio de aplicaciones.

Existen otros muchos SIEM, también efectivos contra amenazas, pero pueden llevar asociados costes o quizá puedan ser menos usados. Por hablar de otras posibilidades, tenemos a modo de ejemplo: AlienVault Open Source SIEM (OSSIM)[6], EMC RSA Security Analytics[7], HP ArcSight Enterprise Security Manager (ESM)[8], IBM Security QRadar SIEM[9], LogRhythm Security Intelligence Platform[10], McAfee Enterprise Security Manager[11], SolarWinds Log & Event Manager[12], Splunk Enterprise[13], Lookwise Enterprise Manager[14], Graylog 2[15], LOGanalize[16], entre otros.

[6] https://www.alienvault.com/products/ossim

[7] http://spain.emc.com/security/security-analytics/security-analytics.htm

[8] http://www8.hp.com/es/es/software-solutions/arcsight-esm-enterprise-security-management/

[9] http://www-03.ibm.com/software/products/es/qradar-siem

[10] https://logrhythm.com/es/

[11] http://www.mcafee.com/es/products/enterprise-security-manager.aspx

[12] http://www.solarwinds.com/log-event-manager

[13] https://www.splunk.com/en_us/products/splunk-enterprise.html

[14] http://www.lookwisesolutions.com/index.php/es/productos/lookwise-enterprise-manager

[15] https://www.graylog.org/

[16] http://loganalyzer.adiscon.com/

ANEXO 2. SOLUCIONES TECNOLÓGICAS

ANEXO 2.1. Herramientas IDS/IPS

ANEXO 2.1.1. Snort

Snort es un "*sniffer*" de software libre construido sobre libpcap y tcpdump, que permite capturar todo el tráfico que llega al equipo donde está instalado. Snort está diseñado para ser preciso en el registro de actividades en la red y está en continua búsqueda de posibles coincidencias entre el flujo de datos y los ataques que tiene registrados en base a diferentes reglas.

Figura 19: Logotipo de Snort

Snort tiene una base de datos de ataques que se está actualizando constantemente, que, además, permite añadir o actualizar a través de Internet. Los usuarios pueden crear 'firmas' basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort[17]. Esta comunidad ha convertido a Snort en uno de los IDS más populares, actualizados y robustos.

Otra de las características más importantes de Snort es que los principales fabricantes de IDS/IPS lo utilizan, pudiendo utilizarse sus firmas en casi cualquier dispositivo.

Anexo 2.1.1.1. Quickdraw

Quickdraw es un conjunto de reglas para Snort realizado por la empresa Digital Bond, y sirve para aprovechar los IDS existentes mediante el desarrollo de firmas para el control del tráfico de determinados protocolos utilizados en los sistemas de control. Además, también incluye reglas para detectar dispositivos y vulnerabilidades.

Las firmas Quickdraw (reglas en el argot de Snort), identifican solicitudes no autorizadas, solicitudes y respuestas erróneas del protocolo, comandos peligrosos, y otras situaciones que son probables o posibles ataques. En este momento tienen firmas disponibles para cuatro protocolos de sistemas de control, un conjunto de firmas para identificar los ataques

[17] http://www.snort.org/lists.html

a las vulnerabilidades del sistema de control, y un grupo de firmas que identifican eventos de seguridad.

ANEXO 2.1.2. Suricata

Suricata es el nombre de un proyecto de software libre, desarrollado por la comunidad OISF (*Open Information Security Foundation*). Es un motor basado en un conjunto de reglas IDS/IPS para monitorizar el tráfico en la red y proporcionar alertas al administrador del sistema cuando ocurre un evento que considera sospechoso. Está diseñado para ser compatible con otros componentes de seguridad existentes y, además, acepta llamadas desde otras aplicaciones.

Figura 20: Logotipo de Suricata[18]

Anexo 2.1.2.1. Características

Suricata puede funcionar como IDS de tiempo real, IPS, monitorizador de seguridad de la red (NSM) y como analizador de ficheros pcap (ficheros con capturas de tráfico).

El funcionamiento para analizar la red se basa en reglas y firmas, aunque también dispone de soporte para crear nuevos scripts mediante el lenguaje LUA.

Dispone de entradas y salidas estandarizadas a formatos como YAML que le permiten integrarse fácilmente con otras herramientas como SIEM o bases de datos.

Al involucrar a la comunidad de código abierto y el conjunto de los recursos más importantes de reglas IDS/IPS disponible, OISF ha construido el motor Suricata para simplificar el proceso de mantenimiento del nivel de seguridad óptimo. A través de asociaciones estratégicas, OISF está aprovechando la experiencia de Amenazas Emergentes[19] y otros recursos importantes en la industria para proporcionar las reglas más actualizadas y completas disponibles.

[18] https://suricata-ids.org/

[19] www.emergingthreats.net

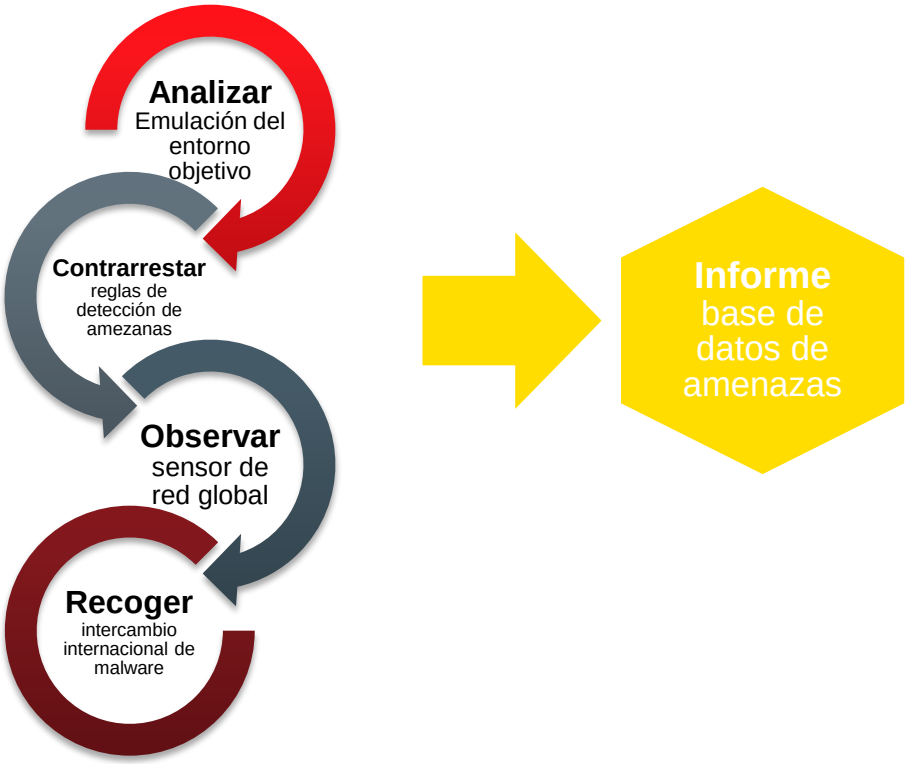

Figura 21: Fases en la gestión de amenazas

ANEXO 2.1.3. Bro

Bro es otra herramienta que sirve de IDS/IPS, debido a sus características de análisis de red, al igual que Snort y Suricata. Se basa en un potente motor de análisis que permite un alto rendimiento en la monitorización de la red, analiza protocolos, y la información de la capa de aplicación en tiempo real.

Figura 22: Arquitectura de Bro

Al igual que otras herramientas, Bro también hace uso de la librería libpcap para su funcionamiento, además es capaz de funcionar en varias redes.

Además de la portabilidad adquirida mediante el uso de libpcap, Bro también puede ser una herramienta de red pasiva, lo que significa que puede actuar supervisando una red sin que sea un nodo con una dirección IP asignada.

Bro está conceptualizado en dos capas:

- **Motor de eventos:** Analiza y guarda el tráfico de la red para generar eventos neutros, que se basan en inicios o paradas de transmisiones, detección de puertos y protocolos.
- **Política de programa**: Analiza los acontecimientos para crear políticas de acción. Bro registra los eventos, pero también puede ser configurado para tomar acciones

como el envío de alertas, ejecuciones de comandos, actualizaciones y llamadas a otros programas.

ANEXO 2.1.4. OSSEC

OSSEC es un IDS basado en Hosts (HIDS). Realiza análisis de logs, comprobación de la integridad, la supervisión del registro de eventos de Windows, detección de rootkits, alerta basada en tiempo y respuesta activa. Proporciona detección de intrusiones para la mayoría de sistemas operativos, incluyendo Linux, OpenBSD, FreeBSD, OS X, Solaris y Windows. OSSEC tiene una arquitectura centralizada, multiplataforma que permite a varios sistemas ser controlados y manejados fácilmente.

OSSEC se basa en nombrar a cada hosts como server o sensor, según sean sus características. Será necesario un sensor en cada zona que se quiera inspeccionar la red en busca de amenazas, y un servidor al menos para poder leer los datos que llegan de los sensores.

Anexo 2.1.4.1. Arquitectura OSSEC

OSSEC se compone de múltiples piezas:

- **Servidor:** El servidor es la pieza central del despliegue OSSEC. Almacena la integridad de los archivos de bases de datos, comprobación de los registros, eventos y entradas de auditoría del sistema. Todas las reglas, decodificadores, y las principales opciones de configuración se almacenan de forma centralizada en el administrador; por lo que es fácil de administrar incluso con un gran número de agentes.
- **Agentes/sensores:** El agente es un pequeño programa o conjunto de programas, instalado en el sistema que va a ser monitorizado. El agente recopilará información y la transmitirá al gestor para su análisis y para llevar a cabo una correlación de información. Parte de la información se recoge en tiempo real, otra será recogida periódicamente. Tiene un pequeño uso de memoria y CPU por defecto, que no afecta el uso del sistema.

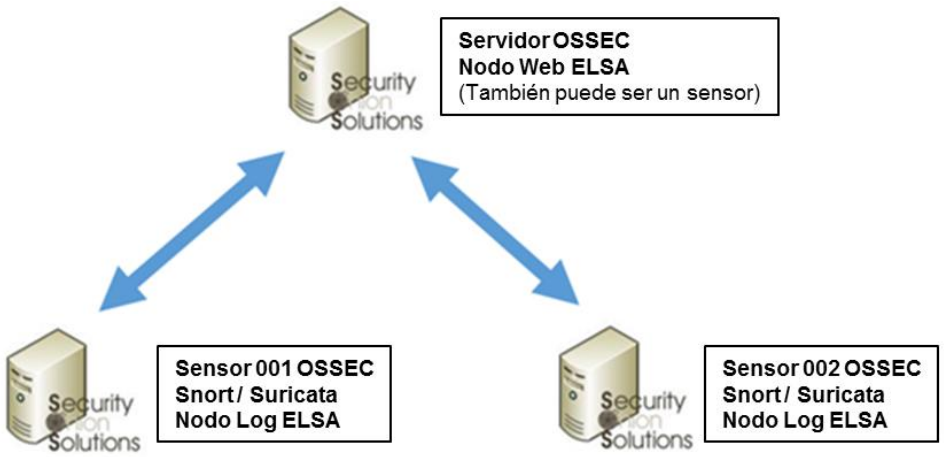

Figura 23: Arquitectura OSSEC

Anexo 2.1.4.2. OSSEC en redes industriales

A modo de resumen, e implementando este sistema en una red industrial, se puede incluir una lista blanca con la IP de cada equipo industrial, routers y switches que puedan estar conectados a la red, denegando la inyección de tráfico a cualquier otro equipo que no esté registrado en esta lista.

De esta forma, se consigue una seguridad efectiva, de forma gratuita y sencilla. Igualmente se puede crear en otros sistemas operativos, en un Linux como se ha visto, o en Windows, que se presenta a continuación. Al funcionar adecuadamente con equipos con bajo rendimiento, nos permite realizar la instalación en redes industriales donde se suelen encontrar equipos más antiguos.

La inclusión de integridad del servidor, detección de rootkits y detección activa, es un añadido a la seguridad de una red industrial, siendo un requisito indispensable para aumentar la defensa de una empresa.

ANEXO 2.1.5. Comparación entre varios IDS/IPS

La Tabla 1 refleja una comparación de las características de algunos de los sistemas IDS/IPS que se han tratado en este estudio.

Características	Bro	Snort	Suricata
Multi Hilo	No	v3.0	Si
Soporte para IPv6	Sí	Sí	Sí
Reputación IP	Parte	No	Sí
Detección Automática de Protocolos	Sí	v3.0	Sí
Aceleración con GPU	No	No	Sí
Variables globales/Flowbits	Sí	No	Sí
GeoIP	Sí	No	Sí
Análisis Avanzado de HTTP	Sí	No	Sí
HTTP Acces Logging	Sí	No	Sí
SMB Access Logging	Sí	No	Sí
Gratis	Sí	Sí	Sí

Tabla 1: Comparación de IDS/IPS

ANEXO 2.2. Herramientas SIEM

ANEXO 2.2.1. Snorby

Snorby es un interfaz para la monitorización de alertas basado en Ruby[20]. La ventaja clave es la flexibilidad, es decir, se puede configurar la interfaz para que acepte eventos provenientes de diferentes aplicaciones, siendo solo necesario añadir determinados códigos. Snorby se utiliza para supervisar la seguridad de red gracias a la incorporación de eventos de IDS/IPS como Snort o Suricata.

[20] https://www.ruby-lang.org/es

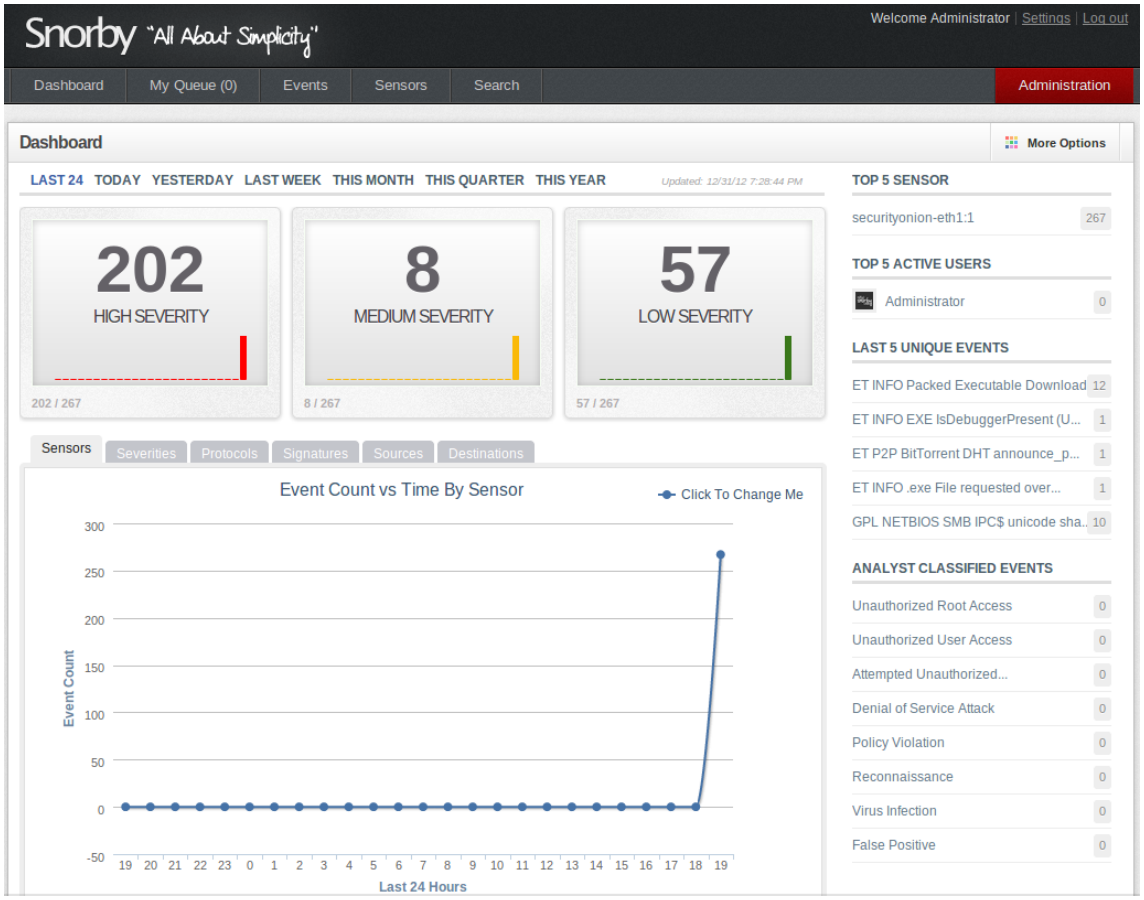

Figura 24: Interfaz de Snorby

Mediante la captura de paquetes (CapME[21]) proporcionados por Snorby, se puede hacer un filtrado con las características que se deseen, por ejemplo seleccionar dirección del equipo y destino, el protocolo de transmisión, la fecha y hora en la que queremos buscar en la base de datos para obtener todos los eventos relacionados. De esta forma, se simplifica la búsqueda y permite centrar el análisis en los eventos necesarios.

ANEXO 2.2.2. Sguil

La herramienta Sguil está construida por y para los analistas de seguridad de red. El principal componente de Sguil es una interfaz gráfica de usuario que proporciona acceso a los eventos en tiempo real, datos de sesión, y capturas de paquetes. Sguil facilita el seguimiento y análisis de eventos en la red. El cliente Sguil se puede ejecutar en multitud de sistemas operativos, incluyendo Linux, BSD, Solaris, MacOS y Windows.

[21] https://github.com/Security-Onion-Solutions/security-onion/wiki/CapMe

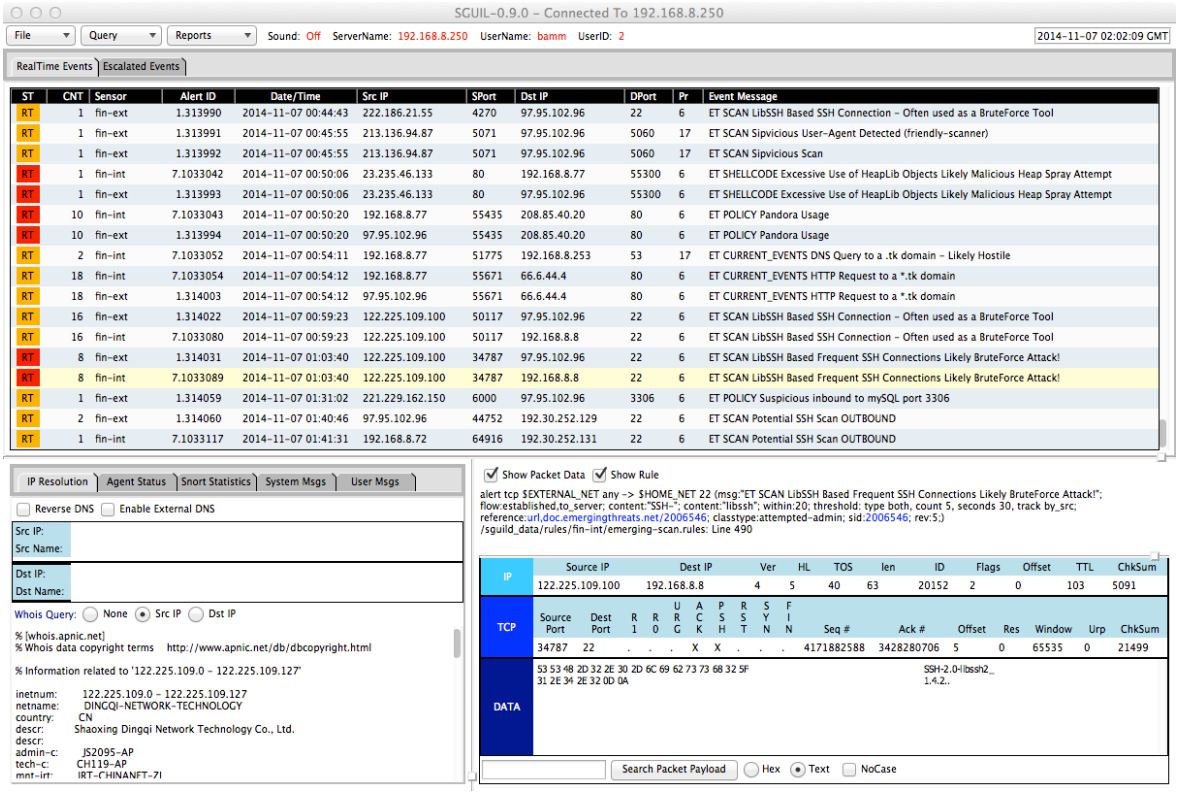

Figura 25: Interfaz de Sguil[22]

Sguil proporciona visibilidad sobre los datos de evento recogidos y el contexto para validar la detección. Proporciona una única interfaz gráfica de usuario, en cual, se ven las alertas de Snort o Suricata, alertas OSSEC, eventos HTTP Bro, y las alertas del sistema de detección pasivo de activos en tiempo real (PRADS[23]).

Más importante aún, Sguil permite ver todo el tráfico asociado a una alerta, consultar todos los paquetes capturados, y también el tráfico que no tiene porqué pertenecer a esa alerta, pero podría estar asociado con la actividad maliciosa o no deseada.

Sguil se diferencia de otras interfaces de alerta en que permite la colaboración entre los analistas permitiendo comentar las alertas

[22] http://bammv.github.io/sguil/index.html

[23] http://manpages.ubuntu.com/manpages/trusty/man1/prads.1.html

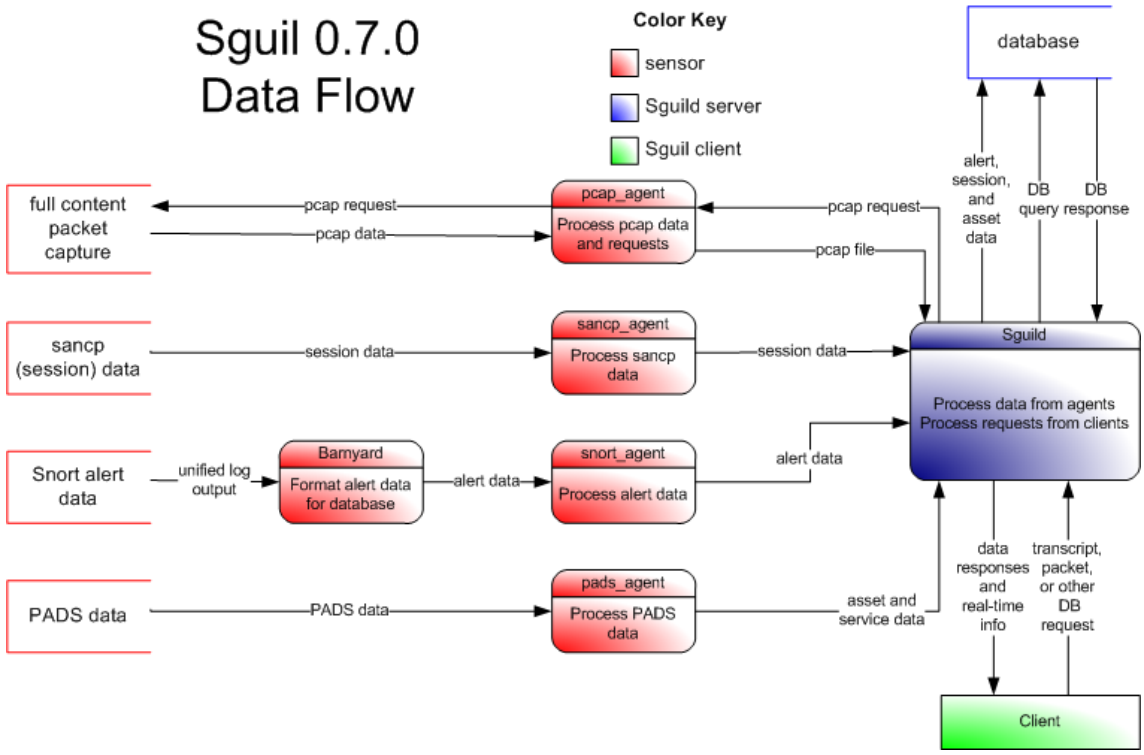

Figura 26: Flujo de datos de Sguil[24]

ANEXO 2.2.3. Squert

Squert es una aplicación web que se utiliza para consultar y ver eventos de datos almacenados en una base de datos Sguil (por lo general son breves datos de alerta). Squert es una herramienta visual que intenta proporcionar información adicional a los eventos a través del uso de metadatos, representaciones de series de tiempo, ponderaciones y conjuntos de resultados agrupados de forma lógica.

[24] http://nsmwiki.org

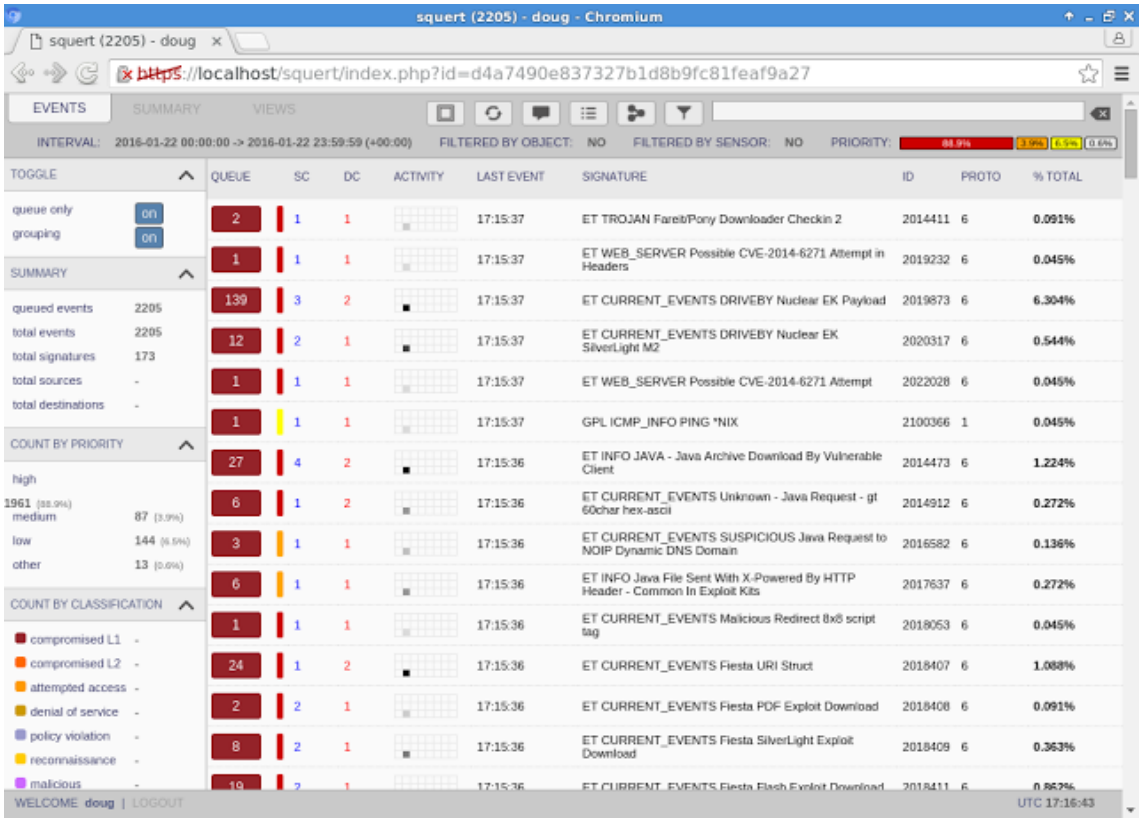

Figura 27: Cola de alertas en la pestaña de eventos de Squert[25]

ANEXO 2.2.4. ELSA

La herramienta para búsqueda y almacenado de logs de empresa (ELSA - Enterprise Log Search and Archive) es un analizador de eventos que opera en tres niveles: receptor de log, base de datos o almacenador e interfaz web para syslog entrantes. Aprovecha un analizador basado en una base de patrones para la normalización de eventos y usa el motor de búsqueda Sphinx[26] para la indexación de texto completo para realizar la búsqueda de eventos.

ELSA permite realizar una exploración que puede estar escalada en los diferentes nodos que tenga un sistema distribuido. El proceso de normalización asigna a cada usuario entrante un identificador según la clase de usuario.

Los usuarios pueden conceder permisos (listas blancas) granulares para un host o programa, es decir, un usuario puede limitarse a uno o varios hosts pero es capaz de consultar cualquier programa o clase en estos equipos.

ELSA se divide en tres componentes principales: los nodos finales, el DAEMON[27] (proceso demonio) que se ejecuta en el servidor web, y el propio sitio Web. Los nodos no tienen conocimiento de la interfaz web y responden a cualquier petición a su puerto de escucha.

[25] https://github.com/Security-Onion-Solutions/security-onion/wiki/Squert

[26] http://sphinxsearch.com

[27] https://es.wikipedia.org/wiki/Demonio_(inform%C3%A1tica)

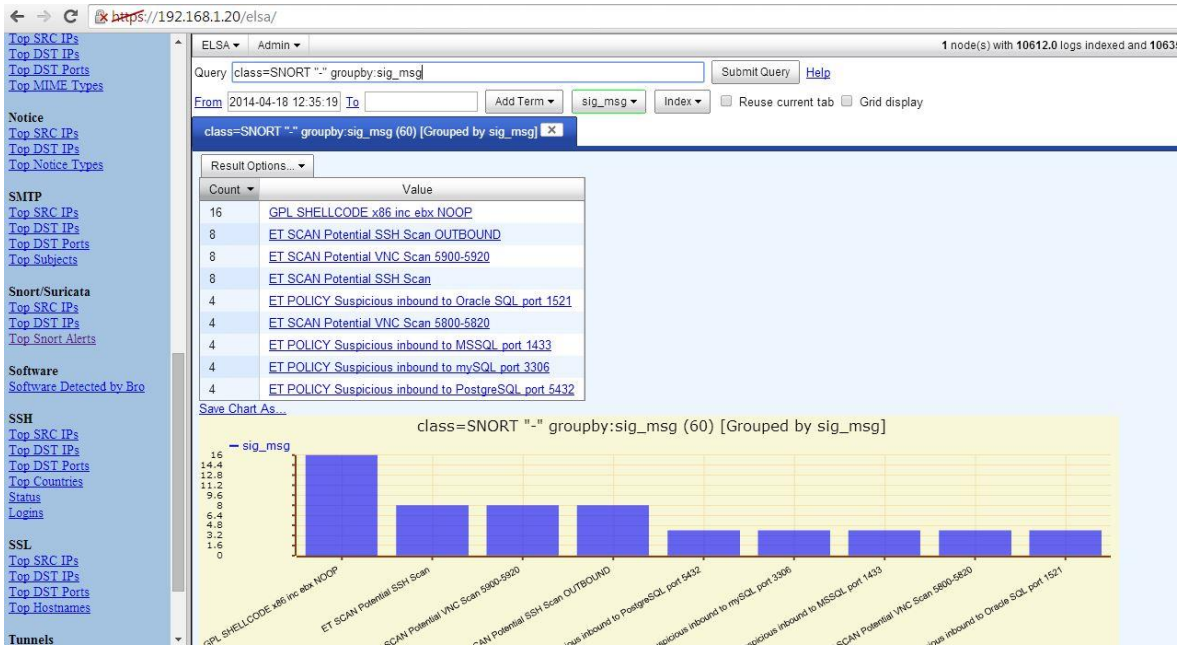

Figura 28: Interfaz gráfica de ELSA[28]

ELSA permite realizar búsquedas de logs igual que si fuera un navegador web, tan solo insertar un espacio de tiempo para realizar un filtrado de todos los logs e indicar un filtro ya predefinido para realizar la búsqueda.

Anexo 2.2.4.1. ELSA en redes industriales

Los filtros configurados en ELSA no permiten hacer filtrado de protocolos industriales por defecto. Los protocolos industriales no son reconocidos, pero como se ve en el apartado que trata el IDS Snort, la implementación de las reglas Quickdraw permite reconocer y filtrar por ejemplo, el puerto 502 o por protocolo ModBus, sin que se encuentre como filtro por defecto.

ANEXO 2.2.5. SPLUNK

Splunk es un sistema que permite la correlación de eventos y la incorporación de los datos de campo e informes para sguil, Bro IDS y OSSEC, e incluye varios cuadros de mando e interfaz de búsqueda para correlar eventos.

Proporciona una plataforma altamente escalable para los datos generados por todos los dispositivos de los sistemas de control, sensores, sistemas SCADA, redes, aplicaciones y usuarios finales conectados a estas redes industriales.

Splunk eleva la eficiencia operativa por medio de:

- La integración y agregación de datos a través de tecnología operativa.
- Busca, explora y correlaciona a través de múltiples fuentes para diagnosticar rápidamente los problemas operativos más costosos.
- Aprovecha la analítica avanzada, proporcionando la capacidad de detectar patrones, tendencias y anomalías.

[28] https://ttcshelbyville.wordpress.com/2014/04/20/security-onion-ids-nsm-and-log-management/

- Entrega rápidamente valores a través de modelos de implementación flexibles.

Figura 29: Aplicación Splunk para seguridad empresarial e ICS [3]

ANEXO 2.3. Security Onion

Security Onion es una distribución de Linux para la detección de intrusiones sobre la que se basa este estudio con el fin de controlar la seguridad de la red y de gestionar los eventos. Creada por Doug Burks, esta distribución ha sido la elegida por tener como objetivo la monitorización de anomalías y detección de problemas de seguridad, dada la cantidad de las herramientas libres (Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, Network Miner, etc.) incluidas en la misma y sin obviar su fácil instalación y puesta en marcha.

Figura 30: Pantalla de inicio de Security Onion

La idea de Doug Burks es crear un Gestor de Seguridad de Red NSM (Network Security Manager) por medio de la compilación de varios programas libres, creando como un conjunto de seguridad de fácil instalación.

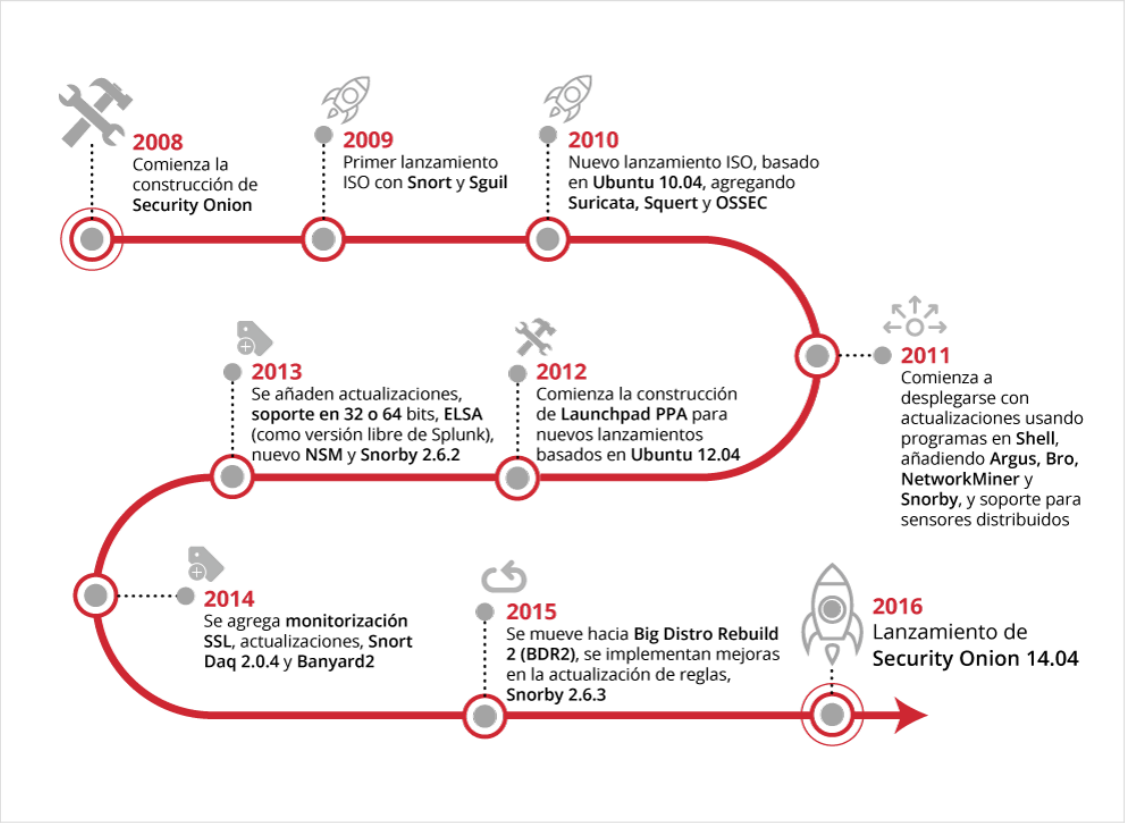

Figura 31: Historia de Security Onion

Las características de Security Onion favorecen su actuación en redes industriales, primero por el bajo coste de la solución, y después por la capacidad de introducir reglas definidas en Snort para monitorizar los protocolos industriales.

ANEXO 2.3.1. Componentes Principales

Security Onion se compone fundamentalmente de tres funcionalidades básicas:

- Captura de paquetes
- Sistemas de detección de intrusiones basado en host y basado en la red y (HIDS y NIDS)
- Herramientas de análisis con gran capacidad y potencia

La captura de paquetes completa se logra a través netsniff-ng, wireshark y otros programas que poseen el mismo objetivo, capturando todo el tráfico de los sensores definidos en Security Onion. La información capturada permite identificar no sólo de dónde o adónde van los paquetes, sino también dónde han sido almacenados (esto permite explotar payloads, correos electrónicos de phishing, exfiltración de archivos).

Los HIDS y NIDS analizan el tráfico que pasa por el host y la red y proporcionan datos de alerta, registro de eventos y actividades detectadas. Security Onion ofrece múltiples opciones de IDS:

- **NIDS:** Security Onion dispone de Snort y Suricata.
- **Análisis guiado por NIDS:** Para la detección de intrusiones de red impulsada por el análisis, se incluye Bro.
- **HIDS:** Security Onion ofrece OSSEC.

ANEXO 2.3.2. Visión de conjunto

Una Gestión de Seguridad de Red (NSM) se refiere a la monitorización de la red obteniendo los eventos relacionados con la seguridad. Puede ser que sea proactivo, cuando se utiliza para identificar las vulnerabilidades o los certificados SSL que expiran, o podría ser reactivo, tal como en la respuesta a incidentes y análisis forense de red. Ya sea porque esté realizando el seguimiento a un adversario o tratando de mantener a raya el malware, un NSM proporciona el contexto, la inteligencia y el conocimiento de la situación de la red.

Security Onion proporciona visibilidad en el tráfico de la red y el contexto en torno a las alertas y eventos anómalos, pero requiere un compromiso hacia el administrador o analista, el cual, deberá revisar las alertas y supervisar la actividad de la red. Security Onion integra para este cometido las herramientas Sguil, Squert y ELSA.

ANEXO 2.3.3. Implantación

Security Onion se basa en un modelo cliente-servidor distribuido. Un sensor de Security Onion es el cliente y otro un servidor. Los componentes del servidor y de los sensores se pueden ejecutar en una única máquina física o virtual, o múltiples sensores pueden ser distribuidos a través de una infraestructura y configurados para informar a un solo servidor designado.

Los siguientes son los tres escenarios de implantación de Security Onion:

- **Independiente (*Standalone*):** Una instalación independiente consiste en una única máquina física o virtual en la que se ejecuta tanto el servidor como los componentes de los sensores y los procesos relacionados. Una instalación independiente puede controlar múltiples segmentos de red con diferentes interfaces de red para la monitorización. Una instalación independiente es el método más fácil y más conveniente para monitorizar una red o redes que son accesibles desde una misma ubicación.
- **Servidor-Sensor:** Una instalación de servidor-sensor consta de una máquina que ejecuta el servidor y una o más máquinas separadas que ejecutan la detección y notifican de nuevo al servidor. Los sensores ejecutan todos los procesos de búsqueda y almacenan los paquetes asociados a la captura, alertas IDS y bases de datos para Sguil y ELSA. El analista se conecta al servidor desde una máquina cliente independiente y todas las consultas enviadas al servidor se distribuyen a los sensores apropiados, la información solicitada se envía al cliente. Este modelo reduce el tráfico de red, manteniendo la mayor parte de los datos recogidos en los sensores hasta que es solicitado por el cliente. Todo el tráfico entre el servidor, los sensores y el cliente están protegidos con túneles cifrados por SSH.
- **Híbrido:** Una instalación híbrida consiste en una mezcla de las dos arquitecturas presentadas, es una instalación independiente que también tiene uno o más sensores separados para informar al servidor de la máquina independiente.

BIBLIOGRAFÍA

[1] Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas. Gómez López, Julio. 10/2009. ISBN: 9788482409313
[2] Introduction to network Security. Debabrata Dash. http://www.slideshare.net/patelvinil/network-security-52257967
[3] https://conf.splunk.com/session/2015/conf2015_TMcCorkle_Splunk_SecurityCompliance_SplunkForIndustrialControl.pdf
[4] IDS gratuitos, pros y contras: https://www.upguard.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise
[5] Añade OSSEC y OpenWIPS-NG http://searchsecurity.techtarget.com/tip/Top-five-free-enterprise-network-intrusion-detection-tools
[6] Free Intrusion Detection (IDS) and Prevention (IPS) Software http://netsecurity.about.com/od/intrusiondetectionid1/a/aafreeids.htm
[7] Introduction to Intrusion Detection Systems (IDS) http://netsecurity.about.com/cs/hackertools/a/aa030504.htm
[8] What is the Difference Between an IPS and a Web Application Firewall? https://www.sans.org/security-resources/idfaq/what-is-the-difference-between-an-ips-and-a-web-application-firewall/1/25
[9] Intrusion Prevention Systems: the Next Step in the Evolution of IDS. https://www.symantec.com/connect/articles/intrusion-prevention-systems-next-step-evolution-ids
[10] Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial https://www.dspace.espol.edu.ec/bitstream/123456789/19502/1/Diapositivas_tesina.pdf
[11] Proyecto final de carrera http://www.adminso.es/images/0/03/Pfc_Carlos_cap1.pdf
[12] IDS vs IPS módulo ciberseguridad http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf
[13] Herramientas de Detección y Prevención de Intrusos http://www.jessland.net/JISK/IDS_IPS/Tools_(Es).php
[14] IDS e IPS Universidad Politécnica http://www.criptored.upm.es/guiateoria/gt_m142w.htm
[15] What is the Difference Between an IPS and a Web Application Firewall? https://www.sans.org/security-resources/idfaq/what-is-the-difference-between-an-ips-and-a-web-application-firewall/1/25
[16] Introducción a las Web Application Firewalls (WAF) http://wiki.elhacker.net/seguridad/web/introduccion-a-los-web-application-firewalls-waf
[17] A Practical Guide to Security Assessments. Sudhanshu Kairab. 2004
[18] Advances in swarm and computational intelligence: 6th International Conference, ICSI 2015 held in conjunction with the second BRICS Congress, CCI 2015, Beijing, June 25-28, 2015, Proceedings. Part II
[19] What is The Role of a SIEM in Detecting Events of Interest? https://www.sans.org/security-resources/idfaq/what-is-the-role-of-a-siem-in-detecting-events-of-interest/5/10
[20] SIEM https://securitcrs.wordpress.com/knowledge-base/siem-security-information-and-event-management/
[21] A Guide to Security Information and Event Management http://www.tomsitpro.com/articles/siem-solutions-guide,2-864.html
[22] Suricata https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_User_Guide
[23] Security Analytics with Big Data, https://securosis.com/assets/library/reports/SecurityAnalytics_BigData_V2.pdf

[24] Splunk & Pcap
https://www.sans.org/reading-room/whitepapers/detection/security-analytics-fun-splunk-packet-capture-file-pcap-34580
[25] Introduction to wireless intrusion prevention systems in the enterprise
http://searchsecurity.techtarget.com/feature/Introduction-to-wireless-intrusion-prevention-systems-in-the-enterprise
[26] Comparing the top wireless intrusion prevention systems
http://searchsecurity.techtarget.com/feature/Comparing-the-top-wireless-intrusion-prevention-systems
[27] Snort vs Suricata
http://wiki.aanval.com/wiki/Snort_vs_Suricata
[28] Security Onion - Canal youtube Doug Burks
[29] Squert
http://www.squertproject.org/
[30] OSSEC Architecture. https://ossec.github.io/docs/manual/ossec-architecture.html
[31] Quickdraw SCADA IDS. http://www.digitalbond.com/tools/quickdraw/
[32] Bro. https://en.wikipedia.org/wiki/Bro_(software)
[33] IEC 62443-2-1. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program
[34] Snorby
https://github.com/Snorby/snorby
[35] Barnyard2
https://github.com/firnsy/barnyard2

CERT DE SEGURIDAD E INDUSTRIA