SISTEMAS DETECCIÓN Y PREVENCIÓN DE INTRUSIONES

QUE SON ?

- IDS, IPS y SIEM

- son sistemas de protección de las comunicaciones que actúan monitorizando el tráfico que entra o sale de nuestra red

IDS

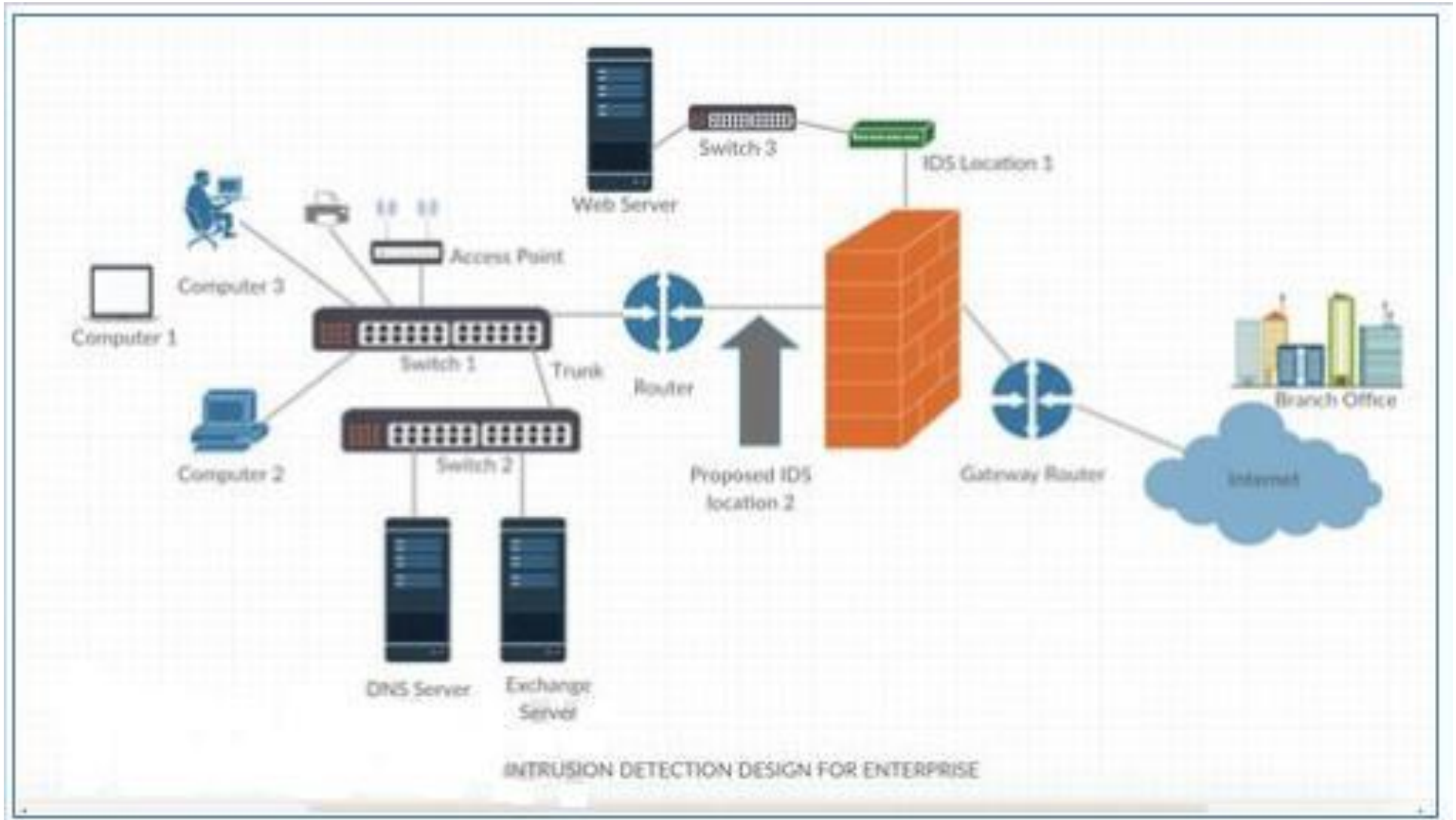
- **IDS (Intrusion Detection System)** o sistema de detección de intrusiones, es una aplicación que sirve para **detectar accesos que no han sido autorizados dentro de un ordenador o de una red**. En otras palabras, se trata de un sistema que monitoriza el tráfico que entra en la red, y lo contrasta con una base de datos actualizada para comprobar si tiene permitido el acceso.
- En caso de detectar actividad inusual o sospechosa, **el sistema emite automáticamente una alerta a los usuarios con permiso de administrador en el sistema**. Sin embargo, estos sistemas son meramente reactivos, lo que significa que no evitan la intrusión, sino que únicamente notifican al administrador de la misma.

¿Cómo funciona un IDS?

- Un sistema de detección de intrusos analiza el tráfico de red o el uso de dispositivos conectados a esa red en busca de actividades sospechosas, que o bien compara con las firmas de amenazas que tiene en su base de datos, o bien busca comportamientos anómalos respecto al funcionamiento habitual de la red o dispositivos.
- Si el IDS detecta una amenaza o un comportamiento anómalo, emite una alerta para que los administradores del sistema tomen las acciones que estimen oportunas. En ese sentido, el IDS no bloquea o evita el ataque, pero sí ayuda a identificarlo cuando ocurre y lleva a tomar las medidas necesarias para mitigarlo.
-

- Algunos **ejemplos de sistemas de detección de intrusos (IDS) son Snort**, Suricata, Ossec, Samhain, Bro o Kismet.
-

Instalacion Sondas IDS



IPS

- **IPS (Intrusion Prevention System)** o sistema de prevención de intrusiones, es un software cuya finalidad es la de **proteger los sistemas de posibles ciberataques**. Para ello, llevan a cabo un análisis de las conexiones en tiempo real, lo que permite detectar (a veces incluso anticipar) las distintas intrusiones y, posteriormente, implementan políticas basadas en el contenido del tráfico monitorizado.
- En otras palabras, los IPS, a diferencia de los IDS, no sólo emiten alarmas cuando se producen intrusiones, sino que además también **pueden descartar paquetes y desconectar conexiones**.

- En algunas ocasiones p**odemos encontrar sistemas mixtos, llamados IPS/IDS**, **que se suelen integrar con cortafuegos y UTM** (**Unified Threat Management**), y que regulan el acceso en función de los protocolos y dependiendo del destino u origen del tráfico.
- La función principal de un **sistema de prevención de intrusos** es identificar cualquier actividad sospechosa y detectar y permitir (IDS) o prevenir (IPS) la amenaza. El intento se registra e informa a los administradores de red o al personal del Centro de operaciones de seguridad (SOC).

¿Por qué se deben utilizar los sistemas de prevención de intrusos (IPS)?

- Las tecnologías IPS pueden detectar o prevenir ataques de **seguridad de red**, como ataques de fuerza bruta, ataques de denegación de servicio (DoS) y vulnerabilidades de seguridad.
- Una vulnerabilidad es una debilidad en un sistema de software y una vulnerabilidad de seguridad es un ataque que aprovecha esa vulnerabilidad para obtener el control de un sistema.
- Cuando se anuncia una vulnerabilidad de seguridad, a menudo existe una ventana de oportunidad para que los atacantes aprovechen esa vulnerabilidad antes de que se aplique el parche de seguridad.
- En estos casos, se puede utilizar un **sistema de prevención de intrusos** para bloquear rápidamente estos ataques.

¿Por qué se deben utilizar los sistemas de prevención de intrusos (IPS)?

- Debido a que las tecnologías IPS vigilan los flujos de paquetes, también se pueden usar para hacer cumplir el uso de protocolos seguros y denegar el uso de protocolos inseguros como versiones anteriores de SSL o protocolos que utilizan cifrados débiles.

¿Cómo funcionan los sistemas de prevención de intrusos (IPS)?

- Las tecnologías IPS tienen acceso a paquetes donde se implementan, ya sea como sistemas de detección de intrusos de red (NIDS) o como sistemas de detección de intrusos de host (HIDS). El IPS de red tiene una vista más amplia de toda la red y puede implementarse en línea en la red o fuera de línea en la red como un sensor pasivo que recibe paquetes de un puerto TAP o SPAN de la red.

- El método de detección empleado puede estar basado en firma o anomalía. Las firmas predefinidas son patrones de ataques de red conocidos.

- El **dispositivo IPS** compara los flujos de paquetes con la firma para ver si hay una coincidencia de patrones. Los sistemas de detección de intrusos basados en anomalías utilizan heurística para identificar amenazas, por ejemplo, comparando una muestra de tráfico con una línea de base conocida.

Ventajas IDS

- Permite identificar incidentes de seguridad gracias al registro que hace de ellos.
- Puede ayudar a identificar problemas o errores de seguridad en la red o en los dispositivos.
- Permite el monitoreo de la red y los dispositivos en tiempo real.
- Puede ayudar a automatizar nuevos patrones de búsqueda de amenazas en los paquetes de datos enviados a través de la red.

Ventajas IDS

- Ayuda con el cumplimiento normativo en materia de ciberseguridad y seguridad de la información.
- Mientras que sus principales desventajas son:
- No pueden prevenir o bloquear ataques, ya que su función es reactiva y no proactiva.
- Son vulnerables a ataques DDoS, puesto que pueden causar que el IDS deje de funcionar.
- Pueden dar falsos positivos.

¿Cuál es la diferencia entre IDS e IPS?

- Las implementaciones tempranas de la tecnología se desarrollaron en modo de detección en dispositivos de seguridad exclusivos.

- A medida que la tecnología ha madurado y se ha movido a un firewall de última generación o dispositivos UTM integrados, la acción predeterminada se establece para evitar el tráfico malicioso.
- Si bien ambos sistemas monitorean y analizan la red y los dispositivos en busca de amenazas con anomalías, la principal diferencia entre un IDS y un IPS, es que el segundo sí puede bloquear ataques, puesto que tiene una función preventiva y proactiva.

¿Cuál es la diferencia entre IDS e IPS?

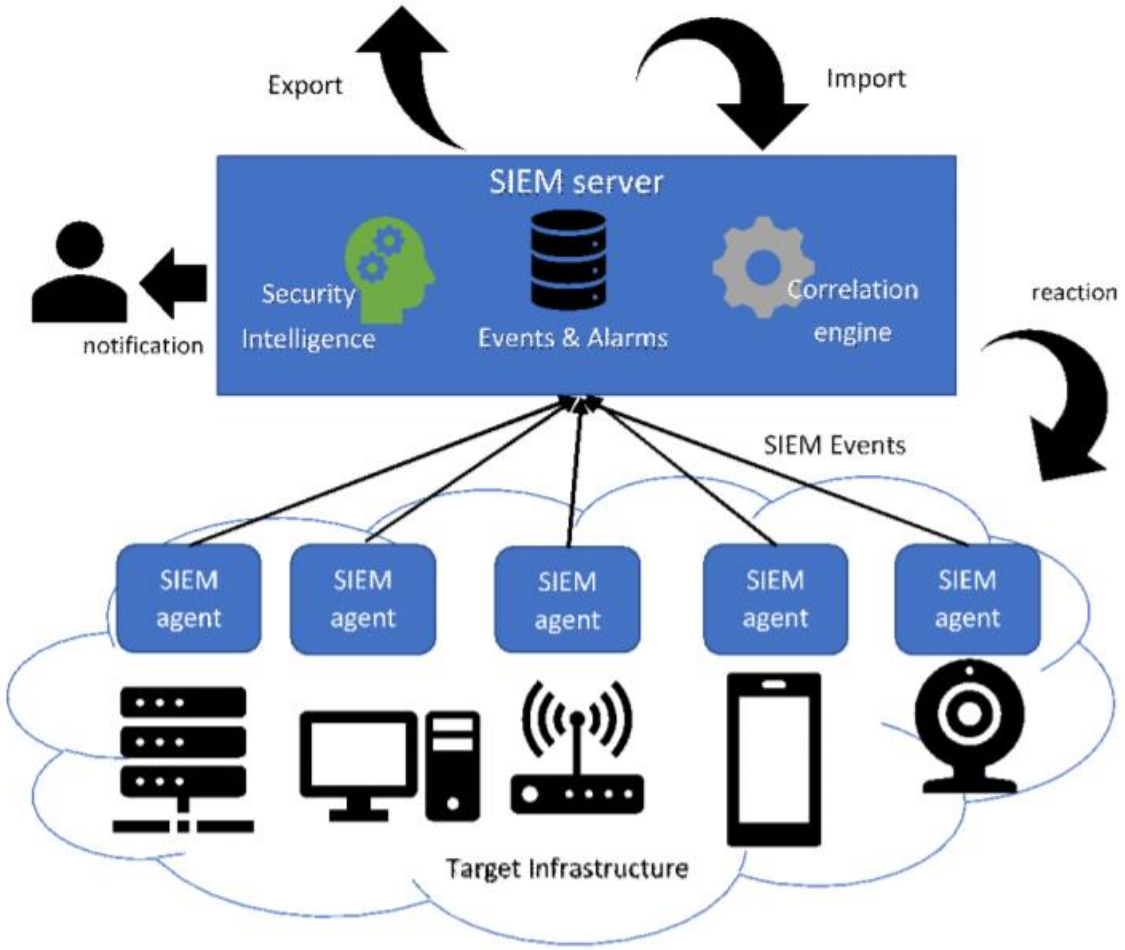
- ¿Y el firewall?
- este lo que hace es bloquear todo el tráfico, filtrando solo aquel tráfico o paquetes de datos permitido en su configuración. Un IDS hace lo opuesto, es decir, permite el paso de todo el tráfico, lo analiza para detectar actividad o datos maliciosos. Por ello, el IDS y el firewall deben trabajar de forma conjunta, de manera que el segundo filtra el tráfico permitido y el primero lo analiza en busca de amenazas o anomalías.

¿Cuál es la diferencia entre IDS e IPS?

- En algunos casos, la decisión de detectar y aceptar o prevenir el tráfico se basa en la confianza en la protección IPS específica.
- Cuando existe una menor confianza en una protección IPS, hay una mayor probabilidad de falsos positivos.

SIEM

- **es una solución híbrida centralizada que engloba la gestión de información de seguridad (*Security Information Management*) y la gestión de eventos (*Security Event Manager*).**

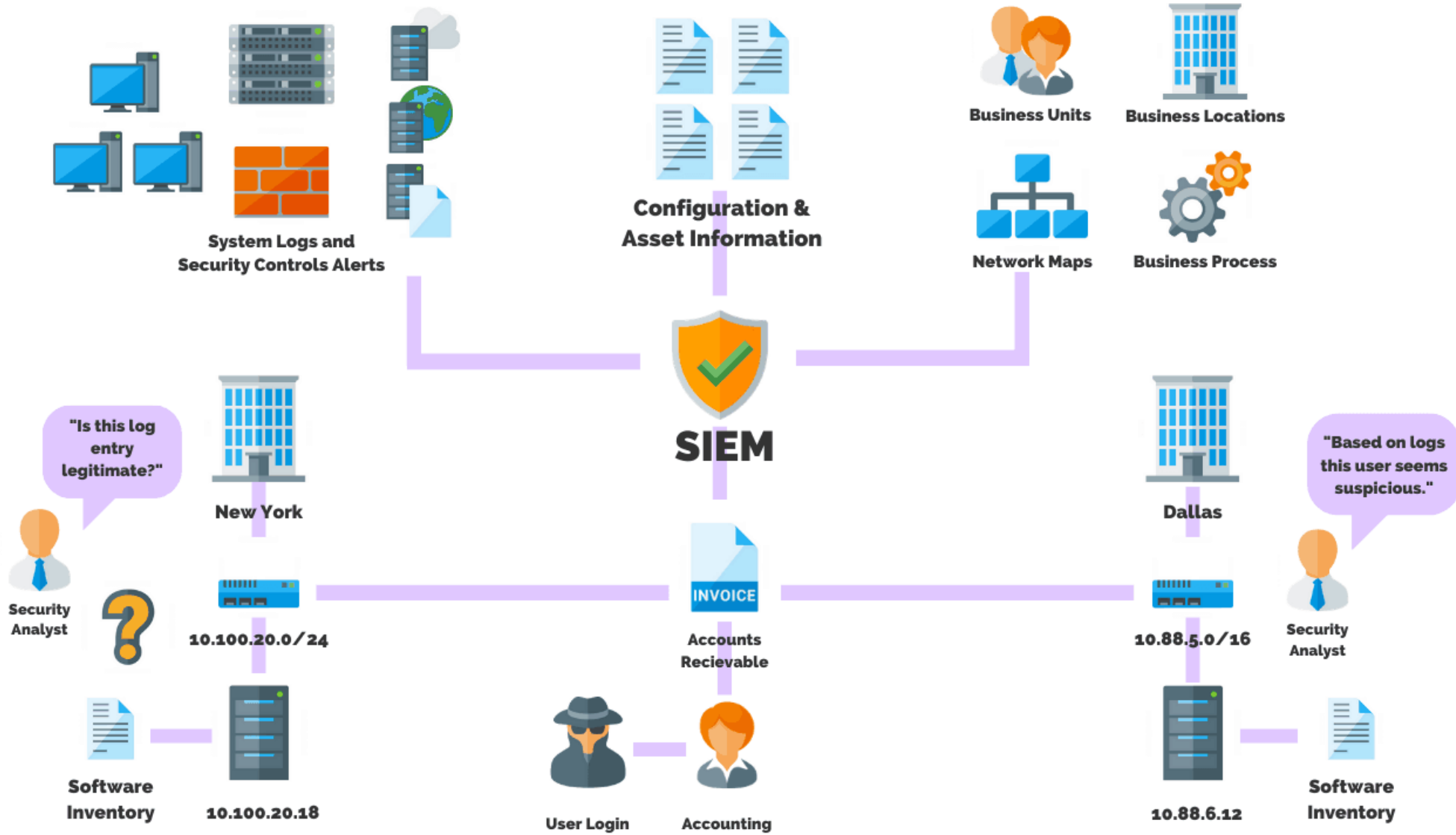


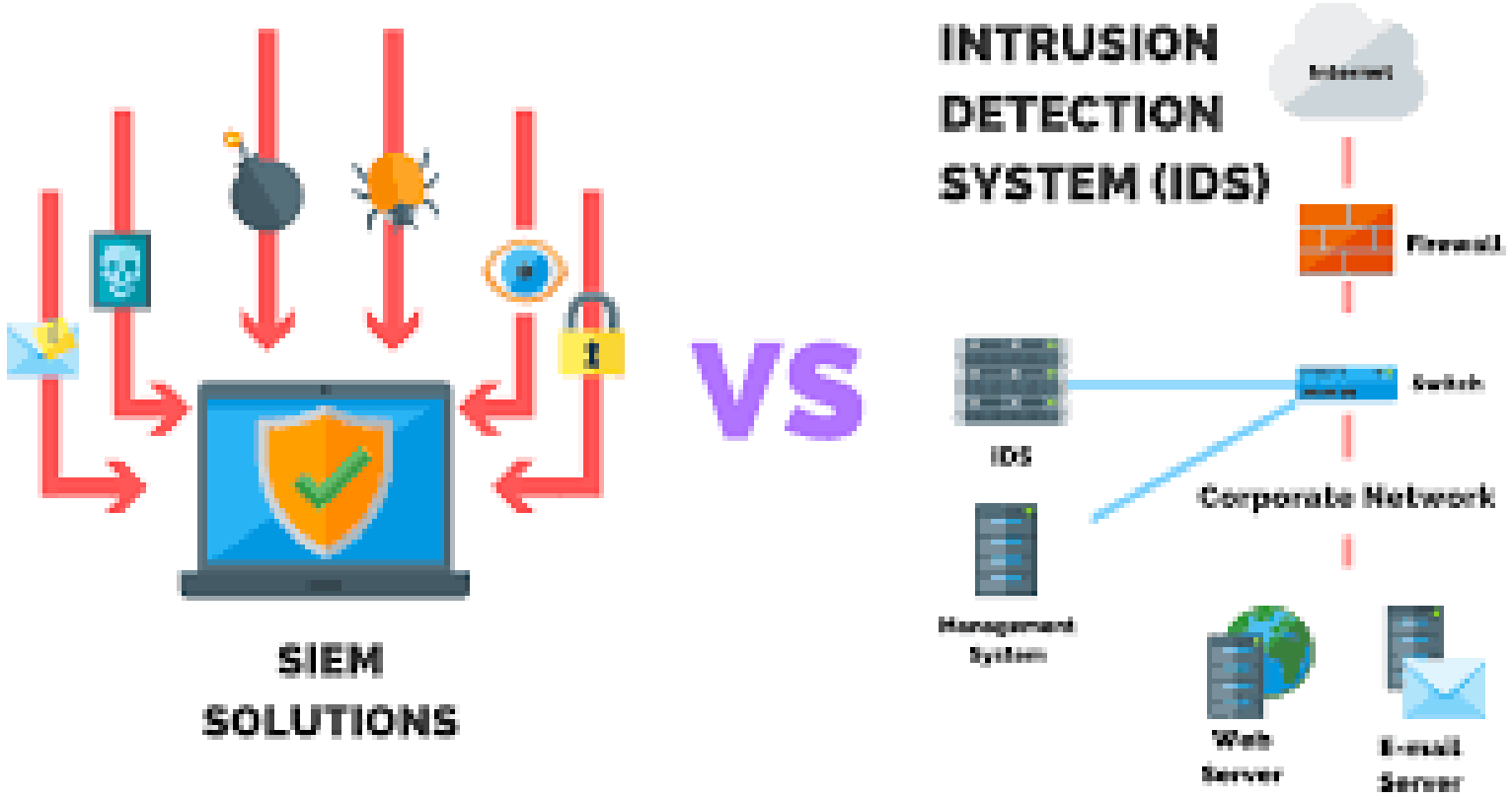
SIEM

- **SIEM (Security Information and Event Management)** o sistema de gestión de eventos e información de seguridad, es una **solucion híbrida centralizada que integra la gestion de la información de seguridad, y la gestión de eventos**. El SIEM es el complemento perfecto para el IDS y el IPS, dado que lleva a cabo un análisis en tiempo real de todas las alertas emitidas por estos sistemas, y los categoriza para distinguir intrusiones de accidentes o falsos positivos.
- En resumen, el SIEM e**s el sistema en el que se centraliza toda esta información, y se integra con los otros sistemas de detección de intrusiones**.

SIEM

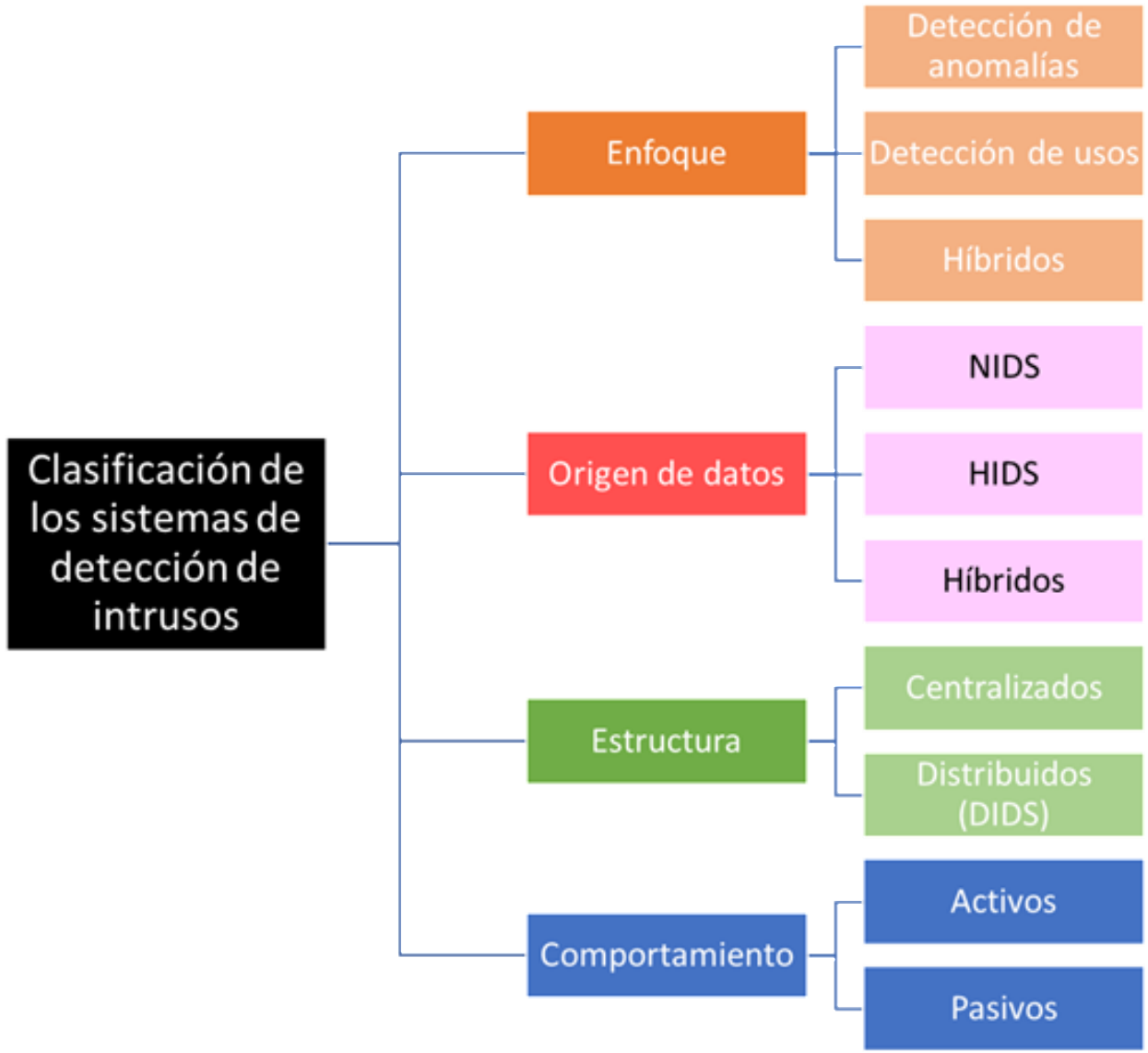
- La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos *hardware* y *software* de la red. Recoge los registros de actividad (*logs*) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una **herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas**.


System Logs and
Security Controls Alerts
Configuration &
Asset Information
Business Units
Business Locations
Network Maps
Business Process
SIEM
"Is this log entry legitimate?"
New York
Dallas
"Based on logs this user seems suspicious."
Security Analyst
10.100.20.0/24
INVOICE
Accounts Recievable
10.88.5.0/16
Security Analyst
Software Inventory
10.100.20.18
User Login
Accounting
10.88.6.12
Software Inventory


SIEM
SOLUTIONS
VS
INTRUSION
DETECTION
SYSTEM (IDS)
Internet
Firewall
Switch
IDS
Corporate Network
Management
System
Web
Server
E-mail
Server

Tipos de sistemas IDS

- Los sistemas de detección de intrusiones se pueden clasificar en diferentes tipos, en función del sistema que monitorean (NIDS e HIDS) y en función de cómo se implementan (SIDS y SIDA).


Clasificación de los sistemas de detección de intrusos
Enfoque
Detección de anomalías
Detección de usos
Híbridos
Origen de datos
NIDS
HIDS
Híbridos
Estructura
Centralizados
Distribuidos (DIDS)
Comportamiento
Activos
Pasivos

- **Sistema de detección de intrusos en la red (NIDS)**
- El sistema de detección de intrusos basados en la red o NIDS se ocupa de monitorear todo el tráfico de red en un segmento estratégico de la red o en un dispositivo, analizando la red y la actividad de los protocolos en busca de actividades maliciosas o sospechosas, al comparar los datos del tráfico con una biblioteca de ataques conocidos.

- **Sistema de detección de intrusos en host (HIDS)**
- El IDS basado en host o HIDS monitorea las características de un host y los eventos que ocurren en él en busca de actividades maliciosas o sospechosas. Un host es un equipo o dispositivo conectado a la red. El HIDS puede identificar tanto el tráfico malicioso que entra en el host como el que origina en el propio host y que un sistema de detección basado en red no podría detectar.

- **Sistema de detección de intrusos basados en firmas (SIDS)**
- Un SIDS es un sistema de detección basado en firmas, es decir, analiza los paquetes de datos que entran en la red y los compara con firmas de amenazas conocidas almacenadas en su base de datos, para alertar sobre ellas si detecta una coincidencia.

- **Sistema de detección de intrusos basado en anomalías (SIDA)**
- El sistema de detección de intrusiones basado en anomalías o SIDA monitoriza el tráfico de red en busca de comportamientos o actividades anómalas, es decir, que no coinciden con firmas, pero que se consideran extraños para el funcionamiento habitual de la red respecto al ancho de banda, protocolos, puertos y otros dispositivos que estén conectados.
- Este sistema basado en anomalías emplea el aprendizaje automático para detectar nuevas amenazas desconocidas.