Cátedra indra | minsait sociedad Digital

Máster Universitario en Ingeniería Informática

LOS IDS Y LA EVOLUCIÓN HACIA UN SIEM

MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA

Escuela Técnica Superior de Ingeniería Informática

ÍNDICE

1. INTRODUCCIÓN

2. IDS
   - Funciones
   - Clasificación
   - ¿Dónde colocarlo?
   - Limitaciones
   - Técnicas de evasión
   - NIDS vs Firewall

3. SIEM
   - OSSIM

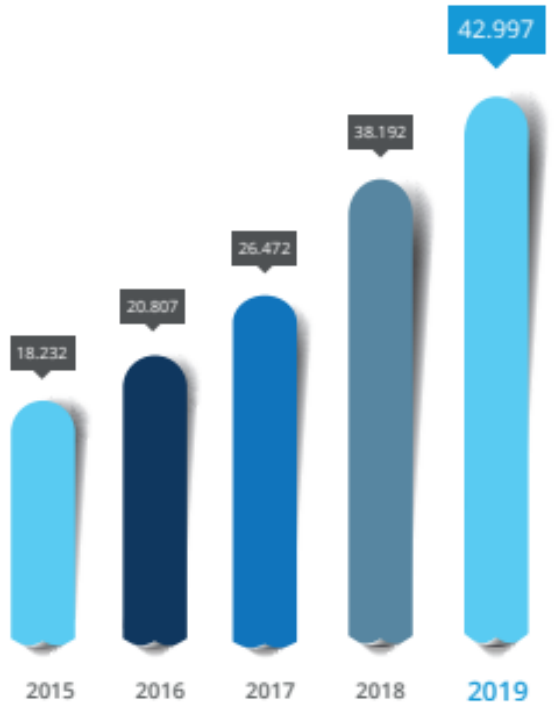
4. CASO PRÁCTICO

5. DEBATE

Jesús Herrera

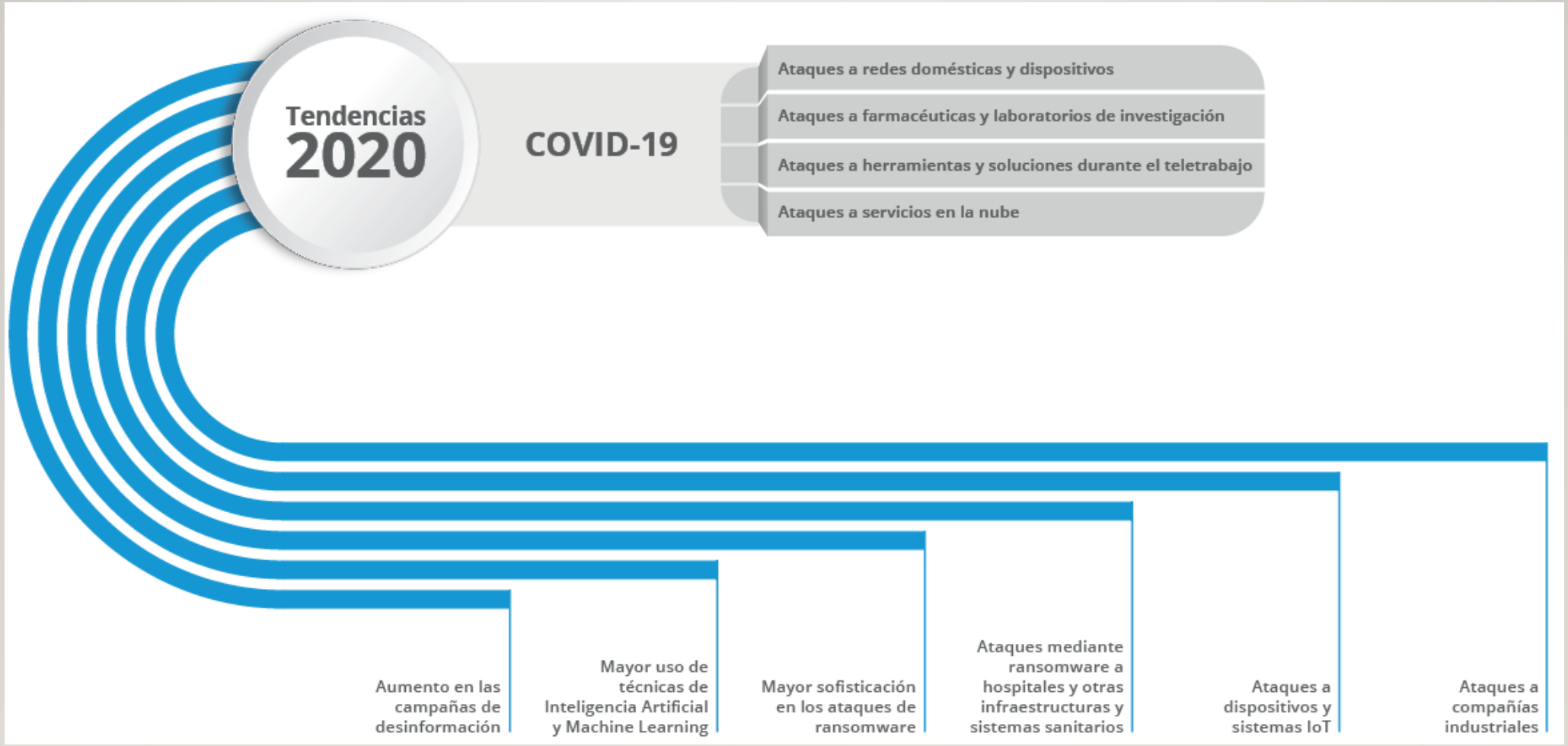
1. INTRODUCCIÓN

En 2019, el CCN-CERT gestionó **42.997 ciberincidentes** –más de un 11 % con respecto al año anterior–, de los cuales casi **un 7,5 %** fueron de **peligrosidad muy alta o crítica**, como se observa en las gráficas a continuación.



(Fuente: CCN-CERT) - 2020

1. INTRODUCCIÓN



(Fuente: CCN-CERT) - 2020

1. INTRODUCCIÓN

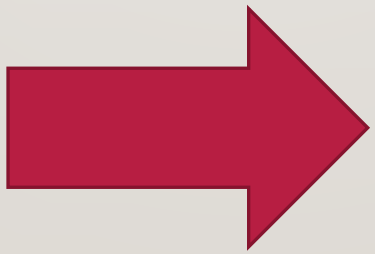
Hacker Tried Poisoning Water Supply After Breaking Into Florida's Treatment System

1. INTRODUCCIÓN

El mundo está en evolución

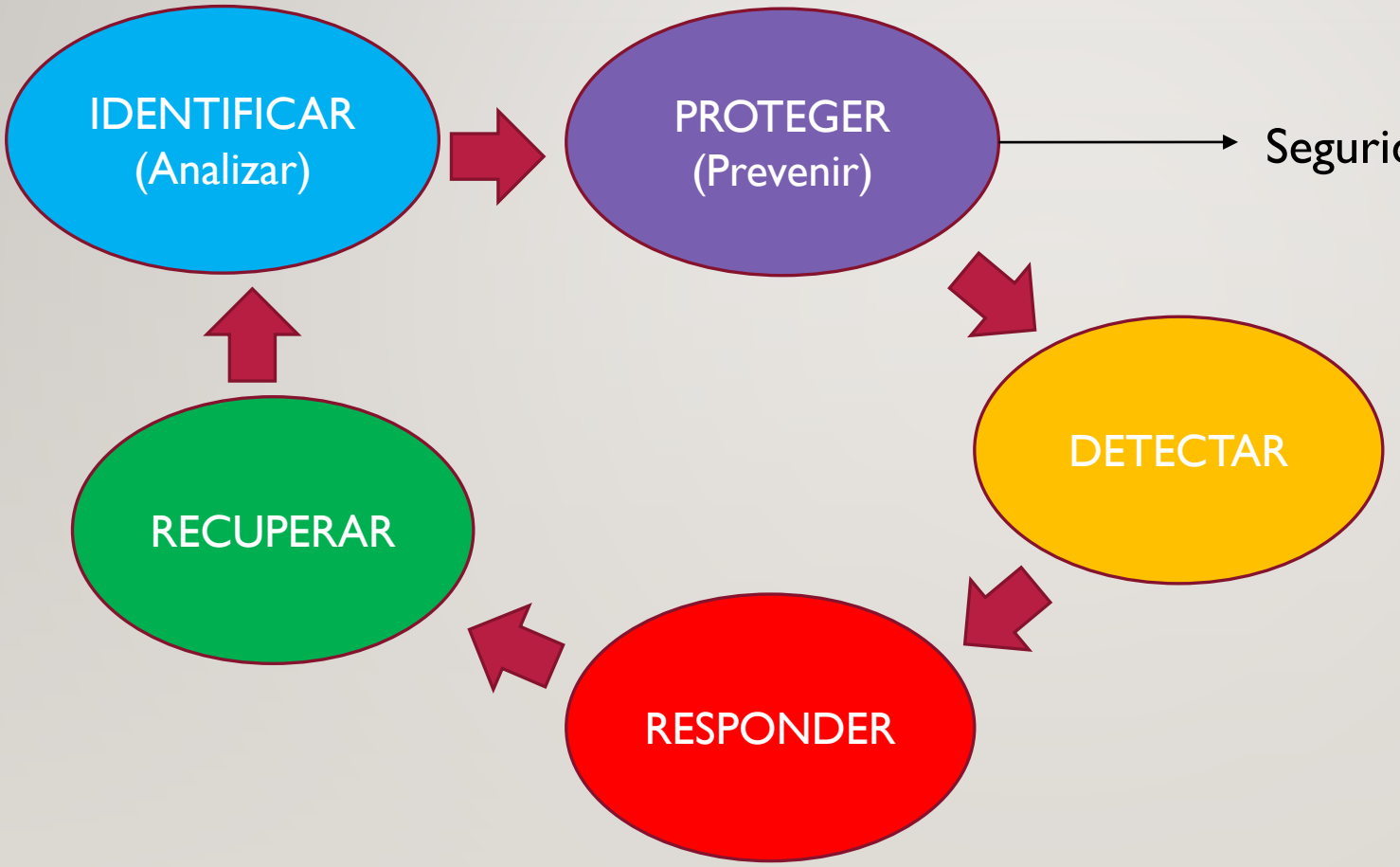
- IOT
- Teletrabajo
- Nuevos servicios
- Etc.

¿Dónde está la información?



1. INTRODUCCIÓN

1. INTRODUCCIÓN



Monitorización

Recolección, detección y análisis de amenazas en curso o compromisos previos.

NIST cybersecurity framework

2. IDS

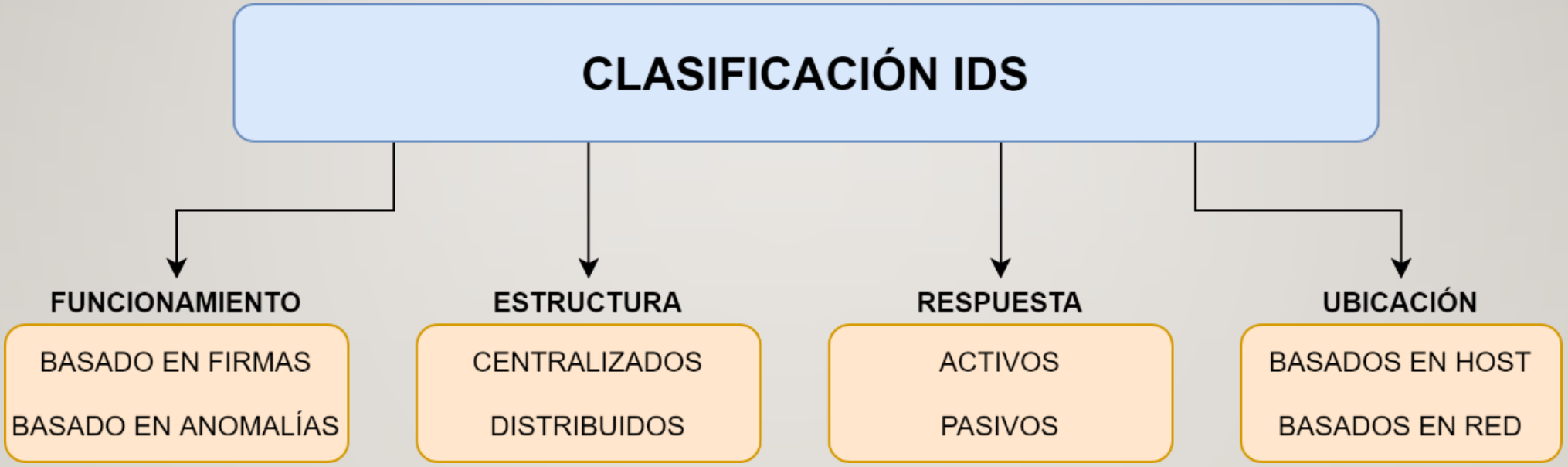
¿Qué es un IDS? *Intrusion Detection System*

Monitorizar, analizar y generar alertas de intrusión

Funciones de un IDS

- Detectar intrusiones.
- Disuasorias.
- Realización de auditorías.
- Búsqueda de nuevospatrones.
- Monitorización de actividad.

2.1. IDS


CLASIFICACIÓN IDS
FUNCIONAMIENTO
BASADO EN FIRMAS
BASADO EN ANOMALÍAS
ESTRUCTURA
CENTRALIZADOS
DISTRIBUIDOS
RESPUESTA
ACTIVOS
PASIVOS
UBICACIÓN
BASADOS EN HOST
BASADOS EN RED

2.1. IDS – FIRMAS VS ANOMALÍAS

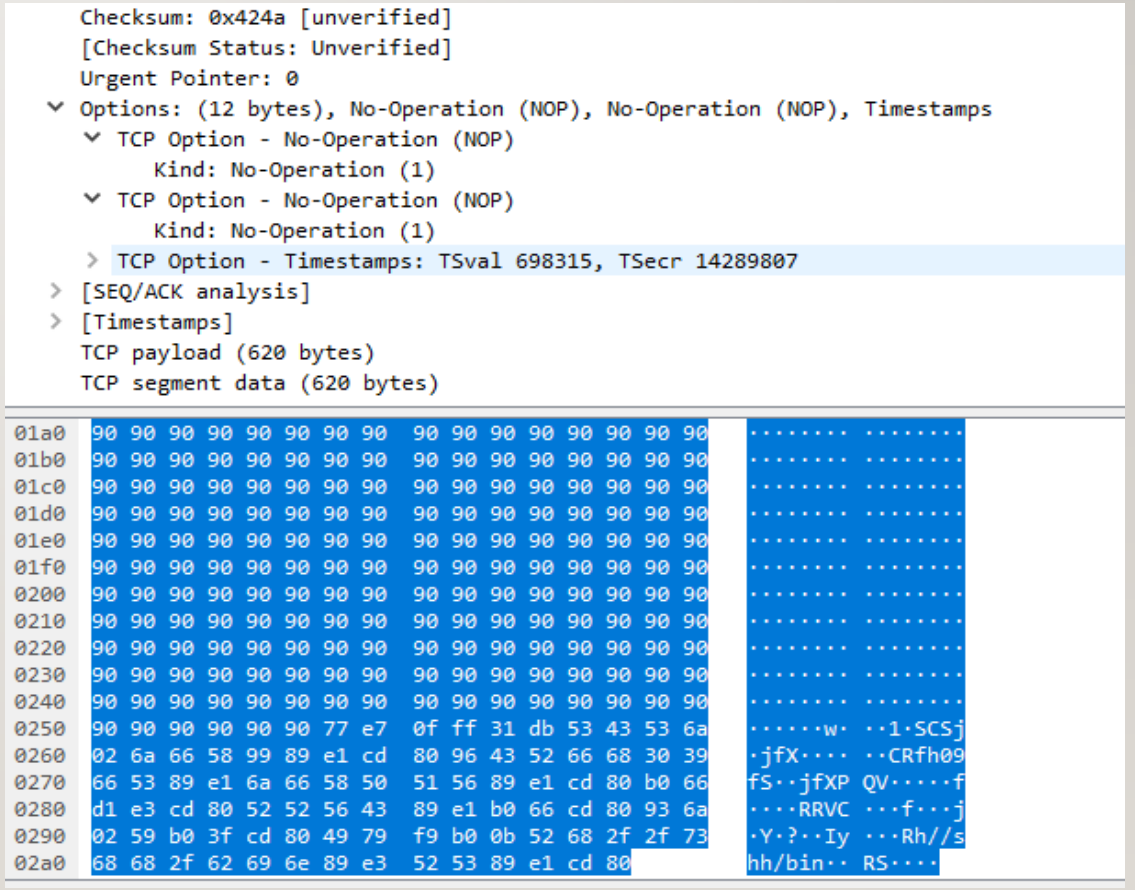
Firmas

- Patrones de ataques conocidos
- Bastante precisos
- Menos falsos positivos

¿Mala definición?

¿Actualización?

¿Ataques 0-day?



2.1. IDS – FIRMAS VS ANOMALÍAS

Anomalías

- Búsqueda de desviaciones de lo "normal"
- Técnicas heurísticas - Perfiles
- Detectar nuevos ataques

¿Qué es lo "normal"?

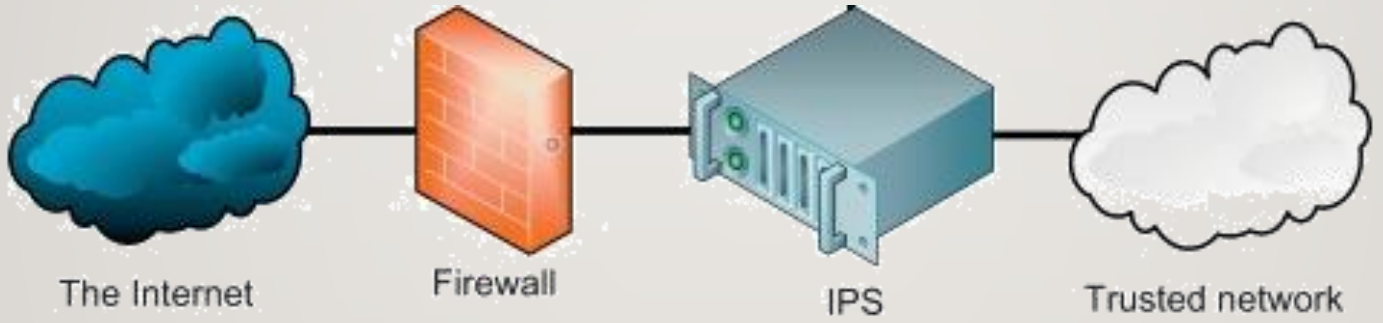
Falsos positivos

Campo de investigación amplio

En combinación con los basados en firmas

2.1. IDS - ACTIVOS VS PASIVOS

ScienceDirect



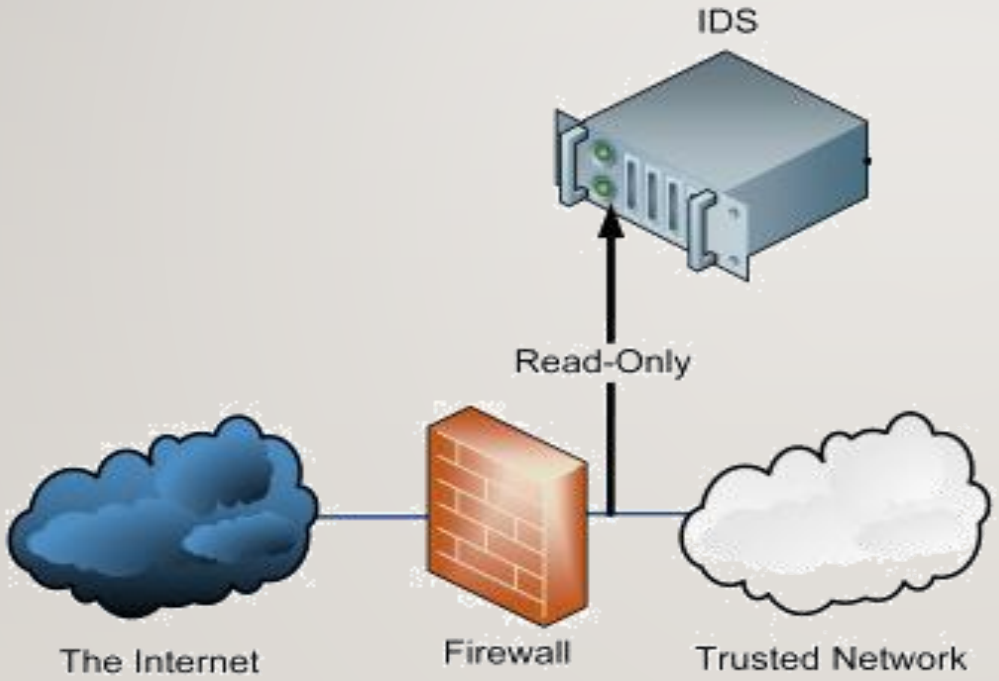
IPS: Sistema de Prevención de Intrusiones

Respuesta activa

¿Falso Positivo? → Evento inesperado

2.1. IDS - ACTIVOS VS PASIVOS

ScienceDirect



Generan alertas.

No eliminan la amenaza.

¿Falsos Positivos? → Ruido

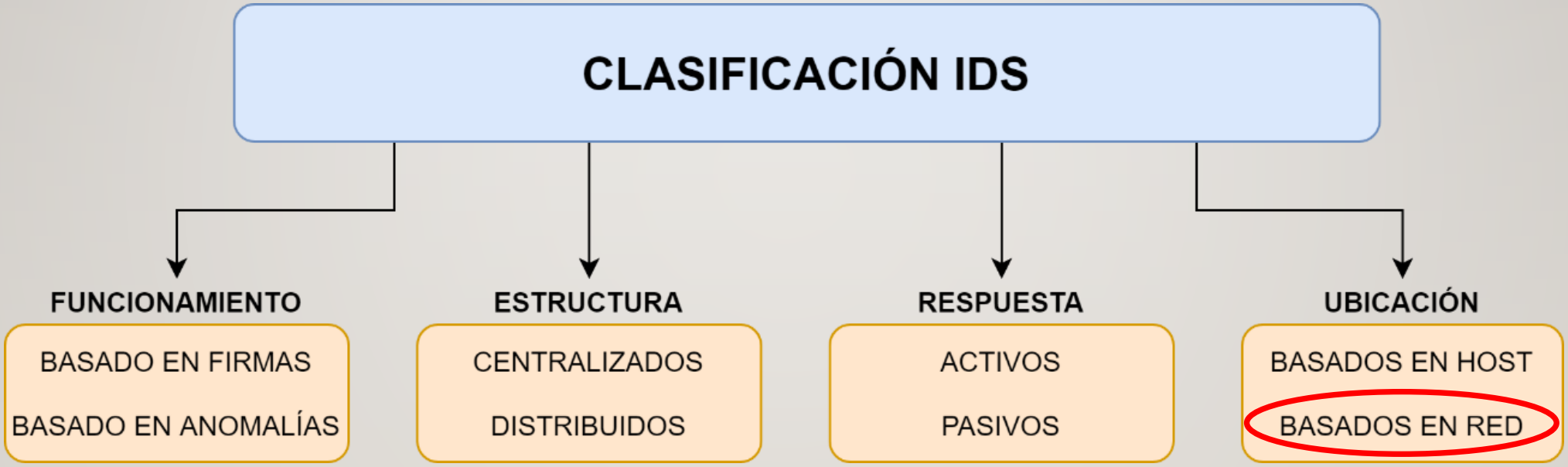
2.1. IDS - HIDS VS NIDS

	Ventajas	Desventajas
HIDS	• Comprueban el comportamiento de comunicaciones cifradas. • No se precisa de hardware adicional. • Comprueban el sistema de archivos, llamadas al sistema y diferentes eventos.	• Consumen recursos del host. • Es necesario que se instalen en cada host. • Solo detectan ataques producidos en el equipo donde se encuentran instalados.

2.1. IDS - HIDS VS NIDS

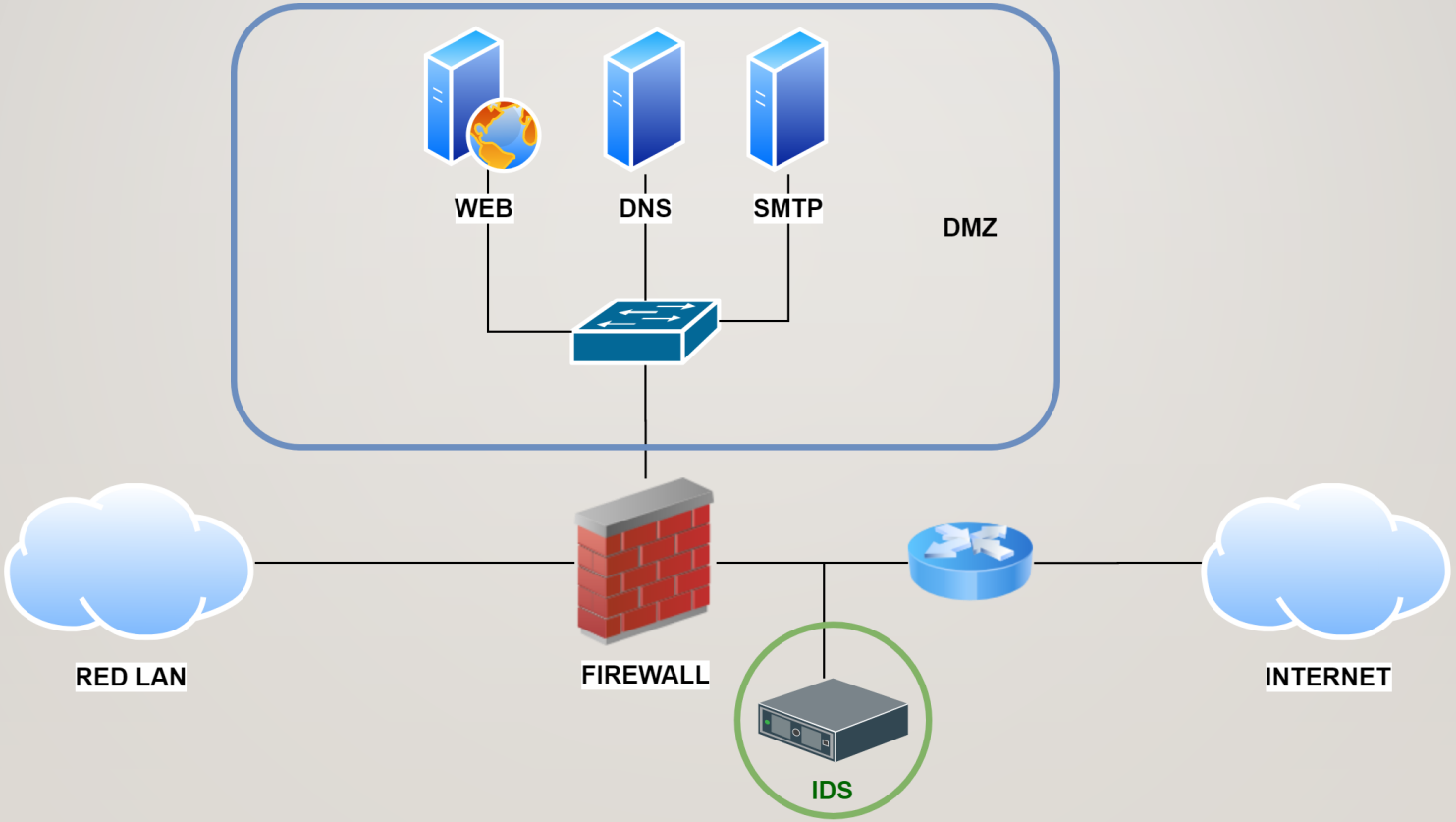
	Ventajas	Desventajas
NIDS	• Comprueban los paquetes de red. • No requiere que se instalen en cada máquina. • Pueden analizar múltiples equipos.	• Presentan carencias al tratar de detectar ataques en tráfico cifrado. • Se requiere hardware dedicado. • Dificultad en redes de alta velocidad.

2.1. IDS

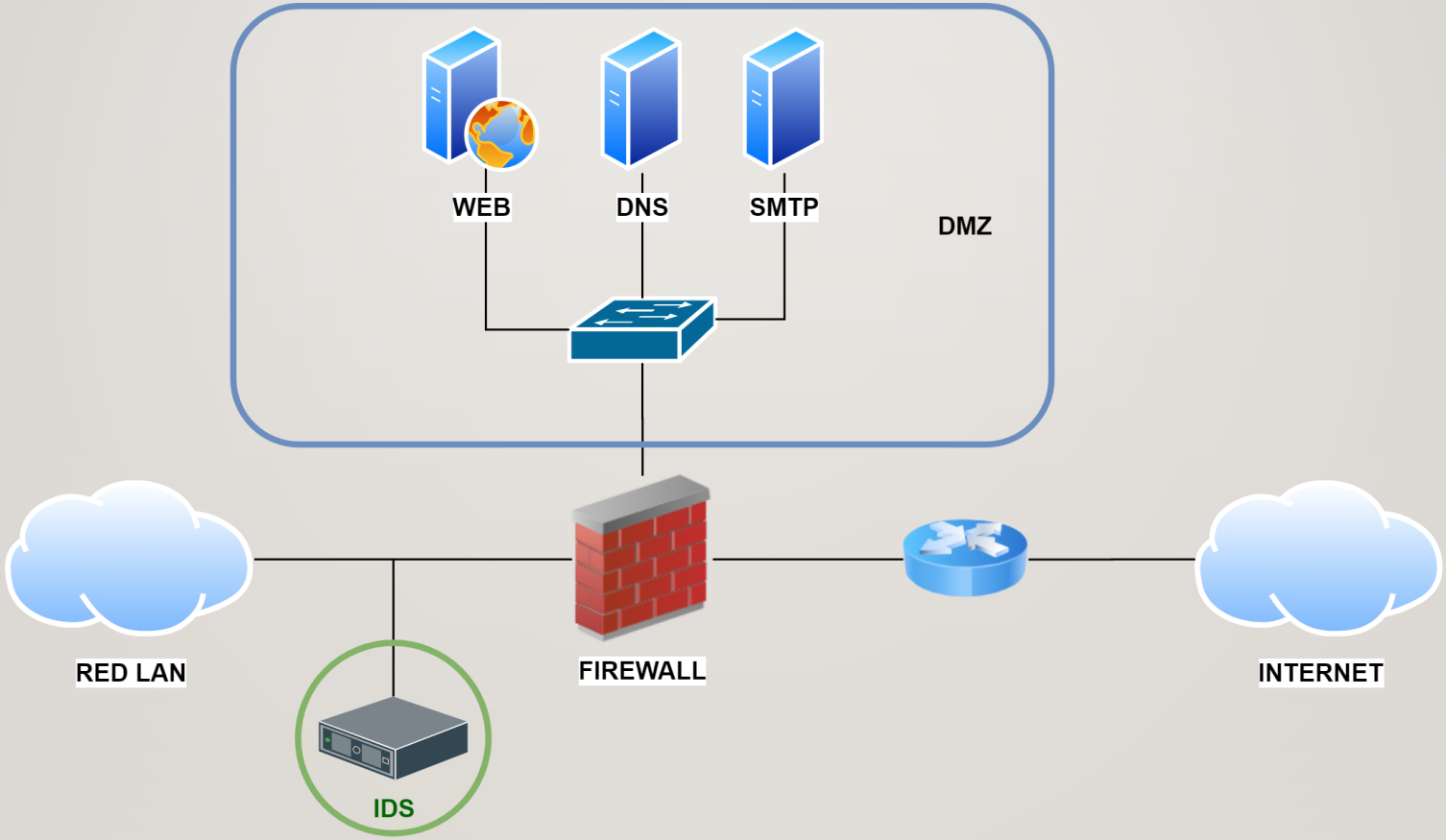


IDS basados en red o NIDS (Network-based IDS)

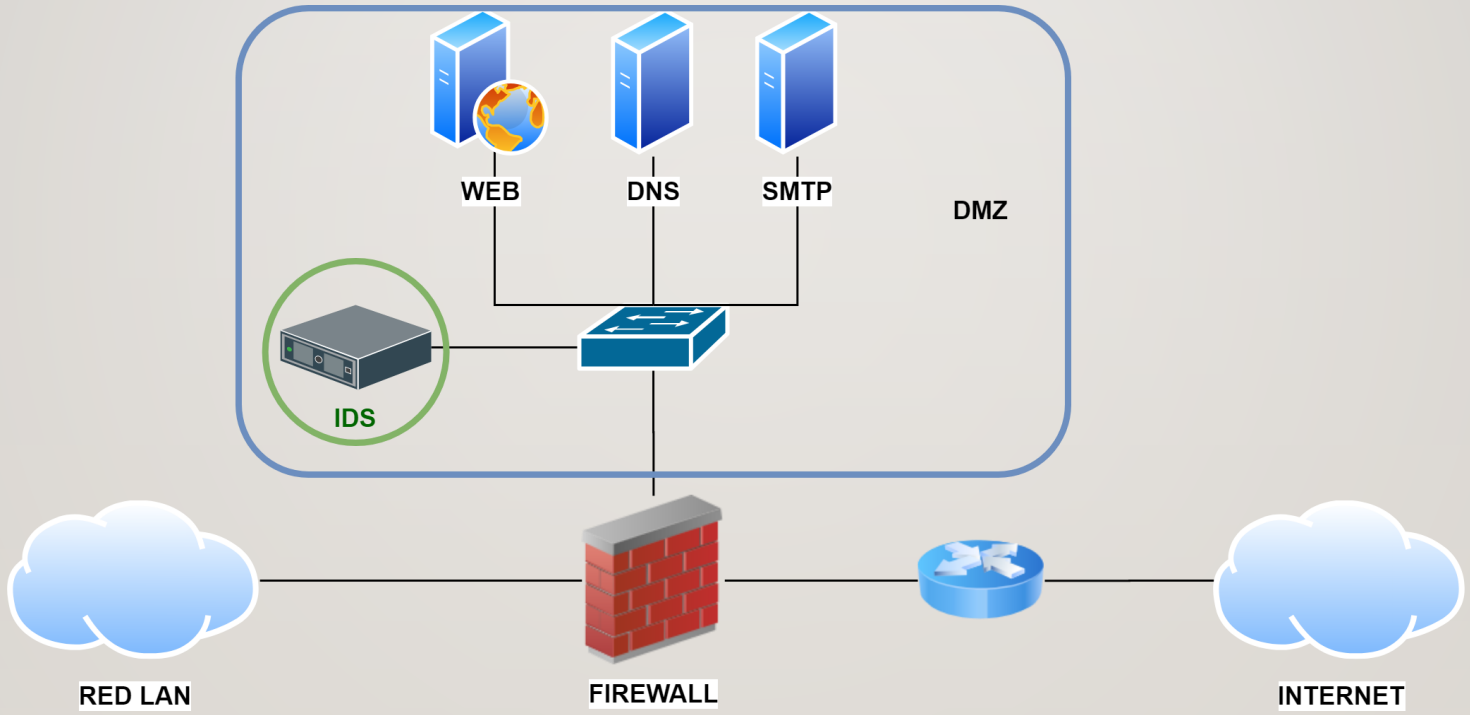
2.2. NIDS - ¿DÓNDE COLOCARLO?



2.2. NIDS - ¿DÓNDE COLOCARLO?



2.2. NIDS - ¿DÓNDE COLOCARLO?



2.2. NIDS - LIMITACIONES

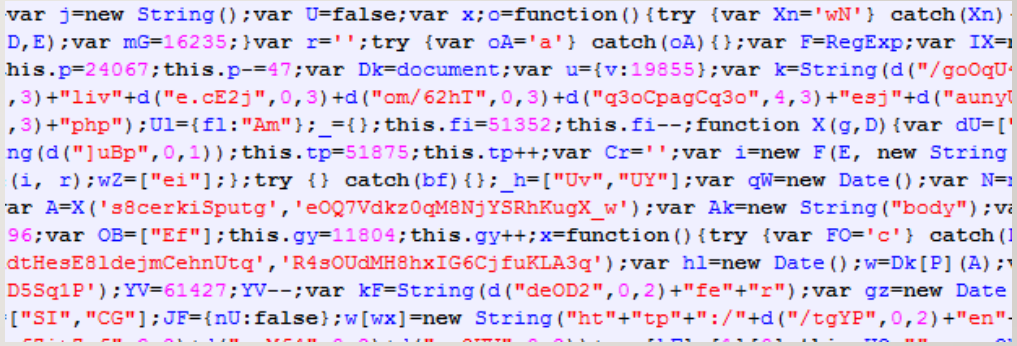
¿Rendimiento?

Procesamiento del tráfico – Bajo throughput

¿Tráfico cifrado?

2.2. NIDS – TÉCNICAS DE EVASIÓN

- Fragmentación
- Inundación – DOS
- Evitar valores por defecto
- Ofuscación
- Tráfico cifrado



2.3. NIDS OPENSOURCE

2.3. NIDS VS FIREWALL

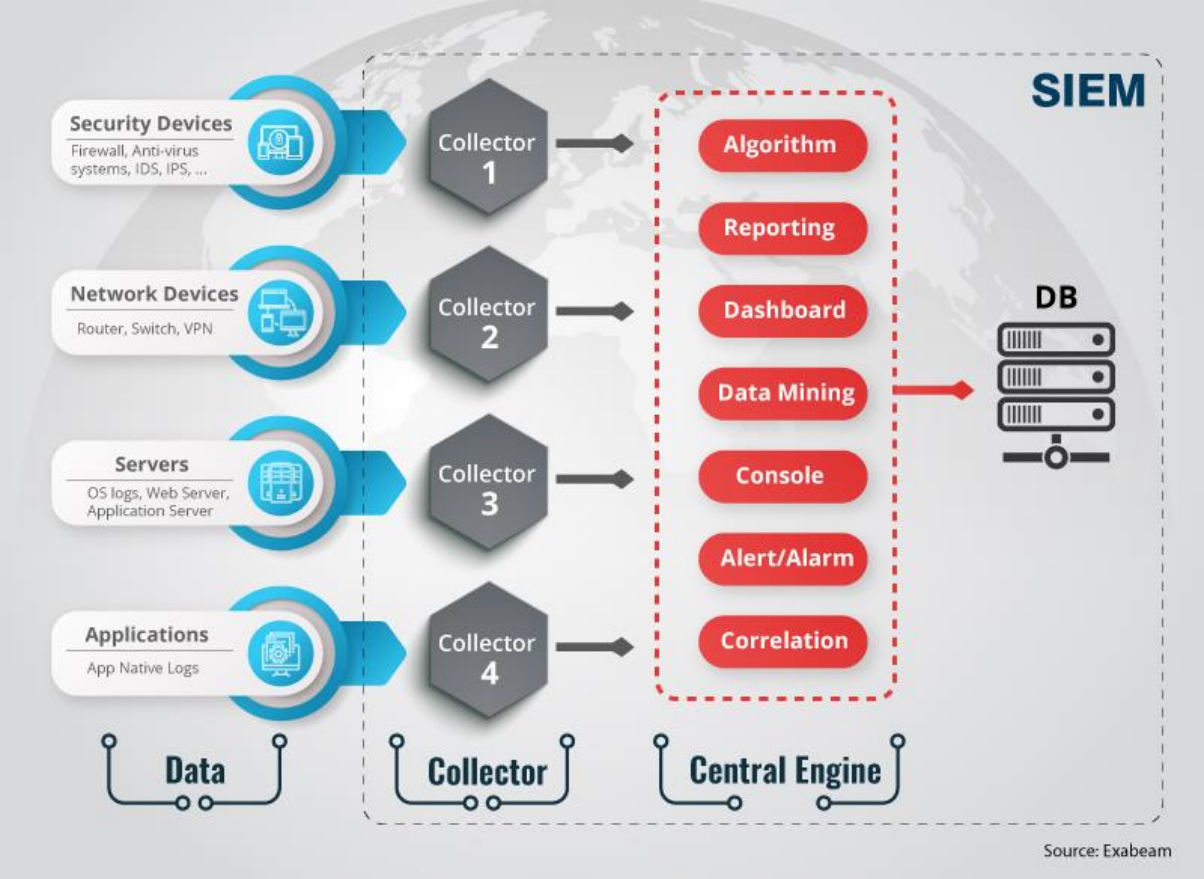
2.3. NIDS VS FIREWALL

90% DEL PRESUPUESTO EN PROTEGER EL PERÍMETRO

¡ SÓLO EL 24% DE LOS ATAQUE!

2.3. NIDS VS FIREWALL

3. SIEM

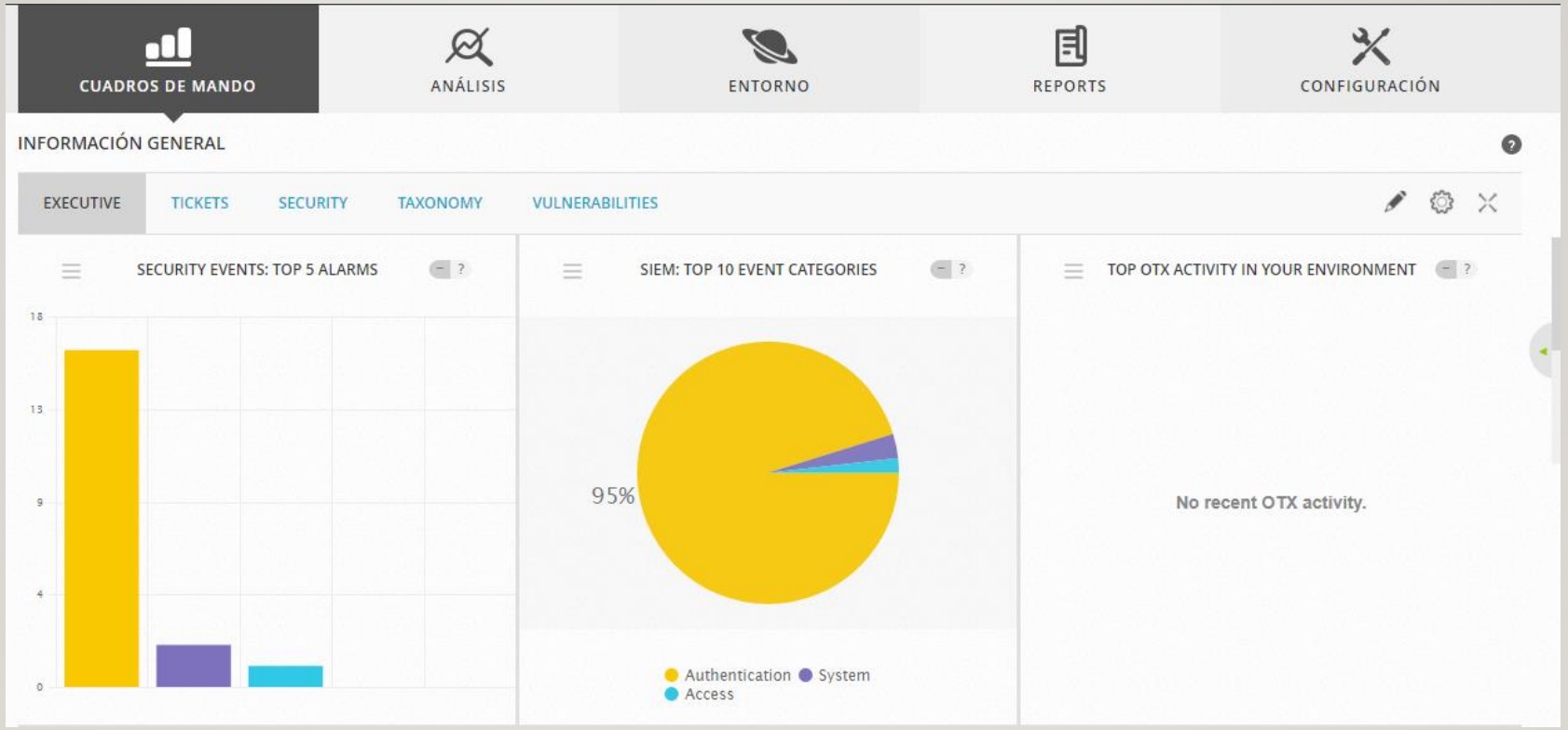

SIEM
Security Devices
Firewall, Anti-virus systems, IDS, IPS, ...
Network Devices
Router, Switch, VPN
Servers
OS logs, Web Server, Application Server
Applications
App Native Logs
Collector 1
Collector 2
Collector 3
Collector 4
Algorithm
Reporting
Dashboard
Data Mining
Console
Alert/Alarm
Correlation
DB
Data
Collector
Central Engine
Source: Exabeam

3. SIEM


```
","src_port":53,"dest_ip":"192.168.0.101","dest_port":38370,"proto":"UDP","dns":{"version":2,"type":"answer","id":27614,"flags
"8180","qr":true,"rd":true,"ra":true,"rrname":"detectportal.firefox.com","rrtype":"AAAA","rcode":"NOERROR","answers":[{"rrname
"detectportal.firefox.com","rrtype":"CNAME","ttl":32,"rdata":"detectportal.prod.mozaws.net"},{"rrname":"detectportal.prod.moza
.net","rrtype":"CNAME","ttl":1323,"rdata":"detectportal.firefox.com-v2.edgesuite.net"},{"rrname":"detectportal.firefox.com-v2.
gesuite.net","rrtype":"CNAME","ttl":2132,"rdata":"a1089.dscd.akamai.net"},{"rrname":"a1089.dscd.akamai.net","rrtype":"AAAA","t
":19,"rdata":"2a02:26f0:013c:0000:0000:0000:0216:7e88"},{"rrname":"a1089.dscd.akamai.net","rrtype":"AAAA","ttl":19,"rdata":"2a
:26f0:013c:0000:0000:0000:0216:7e8a"}],"grouped":{"CNAME":["detectportal.prod.mozaws.net","detectportal.firefox.com-v2.edgesui
.net","a1089.dscd.akamai.net"],"AAAA":["2a02:26f0:013c:0000:0000:0000:0216:7e88","2a02:26f0:013c:0000:0000:0000:0216:7e8a"]}}}
{"timestamp":"2020-06-22T10:44:01.257171+0200","flow_id":1257929069121864,"in_iface":"eth1","event_type":"dns","src_ip":"8.8.8
","src_port":53,"dest_ip":"192.168.0.101","dest_port":38370,"proto":"UDP","dns":{"version":2,"type":"answer","id":27595,"flags
"8180","qr":true,"rd":true,"ra":true,"rrname":"detectportal.firefox.com","rrtype":"A","rcode":"NOERROR","answers":[{"rrname":"
tectportal.firefox.com","rrtype":"CNAME","ttl":59,"rdata":"detectportal.prod.mozaws.net"},{"rrname":"detectportal.prod.mozaws.
t","rrtype":"CNAME","ttl":3566,"rdata":"detectportal.firefox.com-v2.edgesuite.net"},{"rrname":"detectportal.firefox.com-v2.edg
uite.net","rrtype":"CNAME","ttl":1156,"rdata":"a1089.dscd.akamai.net"},{"rrname":"a1089.dscd.akamai.net","rrtype":"A","ttl":19
rdata":"95.100.101.72"},{"rrname":"a1089.dscd.akamai.net","rrtype":"A","ttl":19,"rdata":"95.100.101.97"}],"grouped":{"A":["95.
0.101.72","95.100.101.97"],"CNAME":["detectportal.prod.mozaws.net","detectportal.firefox.com-v2.edgesuite.net","a1089.dscd.aka
i.net"]}}}
{"timestamp":"2020-06-22T10:44:07.022256+0200","flow_id":610857886635760,"in_iface":"eth1","event_type":"dns","src_ip":"192.16
0.101","src_port":46196,"dest_ip":"192.168.0.1","dest_port":53,"proto":"UDP","dns":{"type":"query","id":37247,"rrname":"es-es.
cebook.com","rrtype":"A","tx_id":0}}
{"timestamp":"2020-06-22T10:44:07.022339+0200","flow_id":610857886635760,"in_iface":"eth1","event_type":"dns","src_ip":"192.16
0.101","src_port":46196,"dest_ip":"192.168.0.1","dest_port":53,"proto":"UDP","dns":{"type":"query","id":53640,"rrname":"es-es.
cebook.com","rrtype":"AAAA","tx_id":1}}
{"timestamp":"2020-06-22T10:44:07.031186+0200","flow_id":124424923085266,"in_iface":"eth1","event_type":"dns","src_ip":"192.16
0.101","src_port":60754,"dest_ip":"8.8.8.8","dest_port":53,"proto":"UDP","dns":{"type":"query","id":37247,"rrname":"es-es.face
ok.com","rrtype":"A","tx_id":0}}
{"timestamp":"2020-06-22T10:44:07.031239+0200","flow_id":124424923085266,"in_iface":"eth1","event_type":"dns","src_ip":"192.16
0.101","src_port":60754,"dest_ip":"8.8.8.8","dest_port":53,"proto":"UDP","dns":{"type":"query","id":53640,"rrname":"es-es.face
ok.com","rrtype":"AAAA","tx_id":1}}
{"timestamp":"2020-06-22T10:44:07.065805+0200","flow_id":124424923085266,"in_iface":"eth1","event_type":"dns","src_ip":"8.8.8.
,"src_port":53,"dest_ip":"192.168.0.101","dest_port":60754,"proto":"UDP","dns":{"version":2,"type":"answer","id":37247,"flags"
8180","qr":true,"rd":true,"ra":true,"rrname":"es-es.facebook.com","rrtype":"A","rcode":"NOERROR","answers":[{"rrname":"es-es.f
ebook.com","rrtype":"CNAME","ttl":3567,"rdata":"star.facebook.com"},{"rrname":"star.facebook.com","rrtype":"CNAME","ttl":3418,
data":"star.c10r.facebook.com"},{"rrname":"star.c10r.facebook.com","rrtype":"A","ttl":59,"rdata":"179.60.192.3"}],"grouped":{"
AME":["star.facebook.com","star.c10r.facebook.com"],"A":["179.60.192.3"]}}}
{"timestamp":"2020-06-22T10:44:07.066763+0200","flow_id":124424923085266,"in_iface":"eth1","event_type":"dns","src_ip":"8.8.8.
,"src_port":53,"dest_ip":"192.168.0.101","dest_port":60754,"proto":"UDP","dns":{"version":2,"type":"answer","id":53640,"flags"
8180","qr":true,"rd":true,"ra":true,"rrname":"es-es.facebook.com","rrtype":"AAAA","rcode":"NOERROR","answers":[{"rrname":"es-e
facebook.com","rrtype":"CNAME","ttl":3567,"rdata":"star.facebook.com"},{"rrname":"star.facebook.com","rrtype":"CNAME","ttl":34
,"rdata":"star.c10r.facebook.com"},{"rrname":"star.c10r.facebook.com","rrtype":"AAAA","ttl":59,"rdata":"2a03:2880:f01f:0002:fa
:b00c:0000:0002"}],"grouped":{"CNAME":["star.facebook.com","star.c10r.facebook.com"],"AAAA":["2a03:2880:f01f:0002:face:b00c:00
:0002"]}}}
```


Logs producidos por Suricata

3. SIEM



¿Alertas relevantes? → ¿Qué riesgo suponen?

3. SIEM


CHALLENGERS
LEADERS
Splunk
IBM
Exabeam
Securonix
LogRhythm
Rapid7
Dell Technologies (RSA)
FireEye
AT&T Cybersecurity
Micro Focus
McAfee
HanSight
Fortinet
ManageEngine
SolarWinds
LogPoint
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of February 2020
© Gartner, Inc

3.1 SIEM - OSSIM

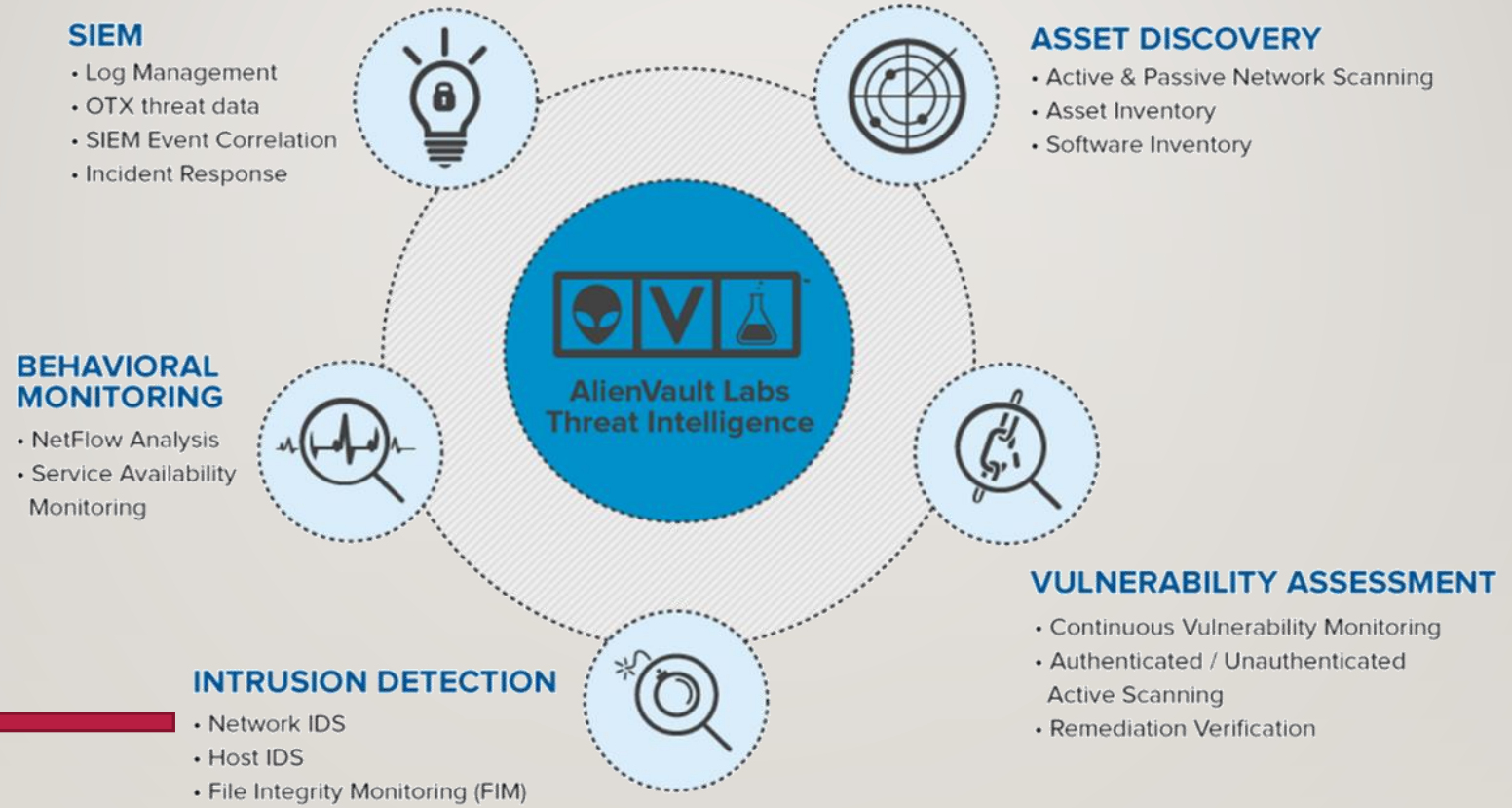
AT&T CYBERSECURITY

Threat Detection and Response

- USM Anywhere

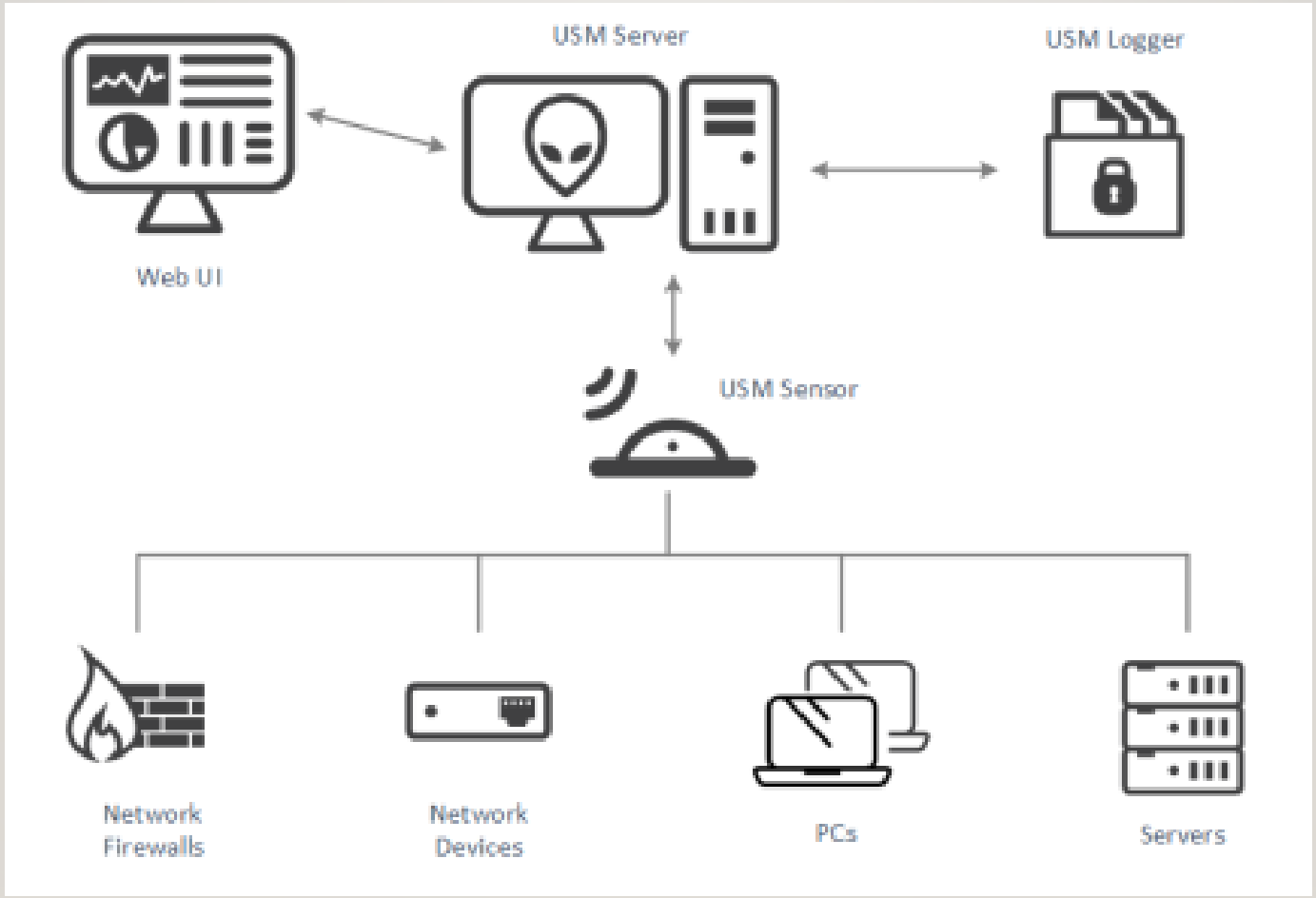
- AlienVault OSSIM
  - Opensource
  - Gratuito
  - Herramientas GPL(OpenVas, Nmap, Suricata…)

3.1 SIEM - OSSIM

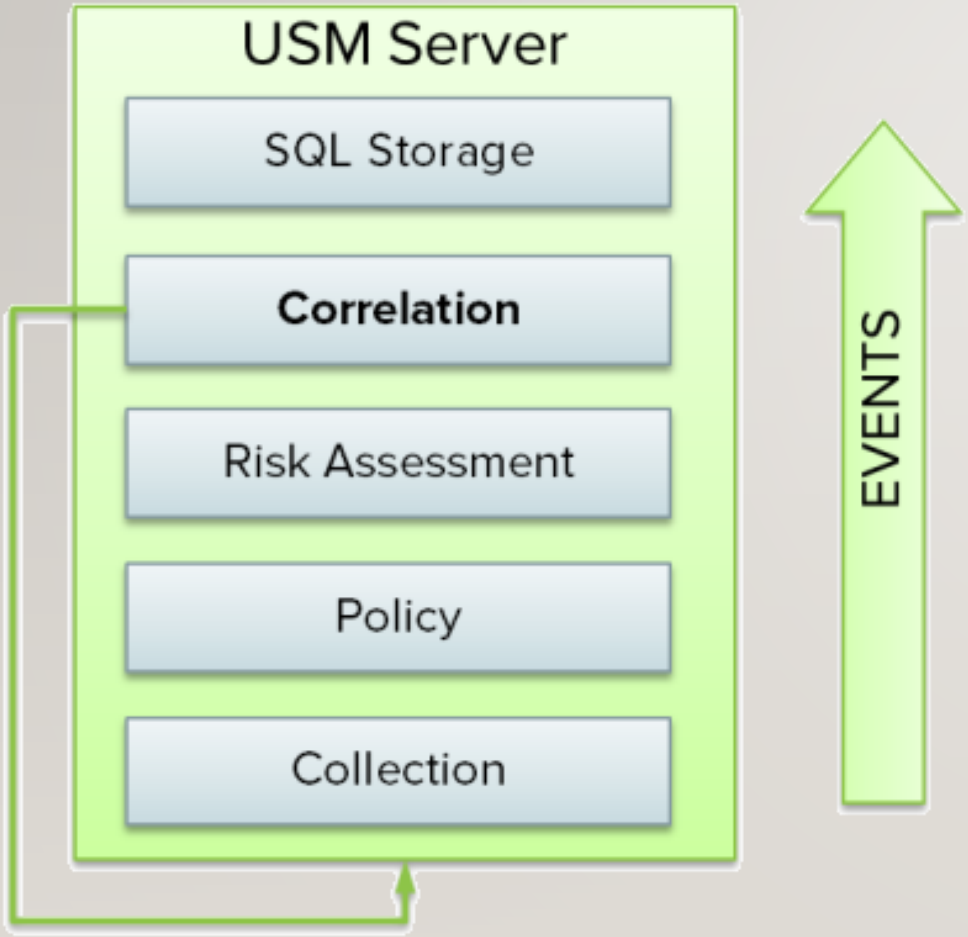


Suricata

3.1 SIEM - OSSIM



3.1 SIEM - OSSIM



Recopilación de datos y normalización.

- Logs de diversas fuentes.
- Normalización y estandarización (Plugins)

Procesamiento de eventos.

- Prioridad y fiabilidad.
- Valor del activo.
- Clasificación taxonómica.
- Cruce de datos – Reputación.

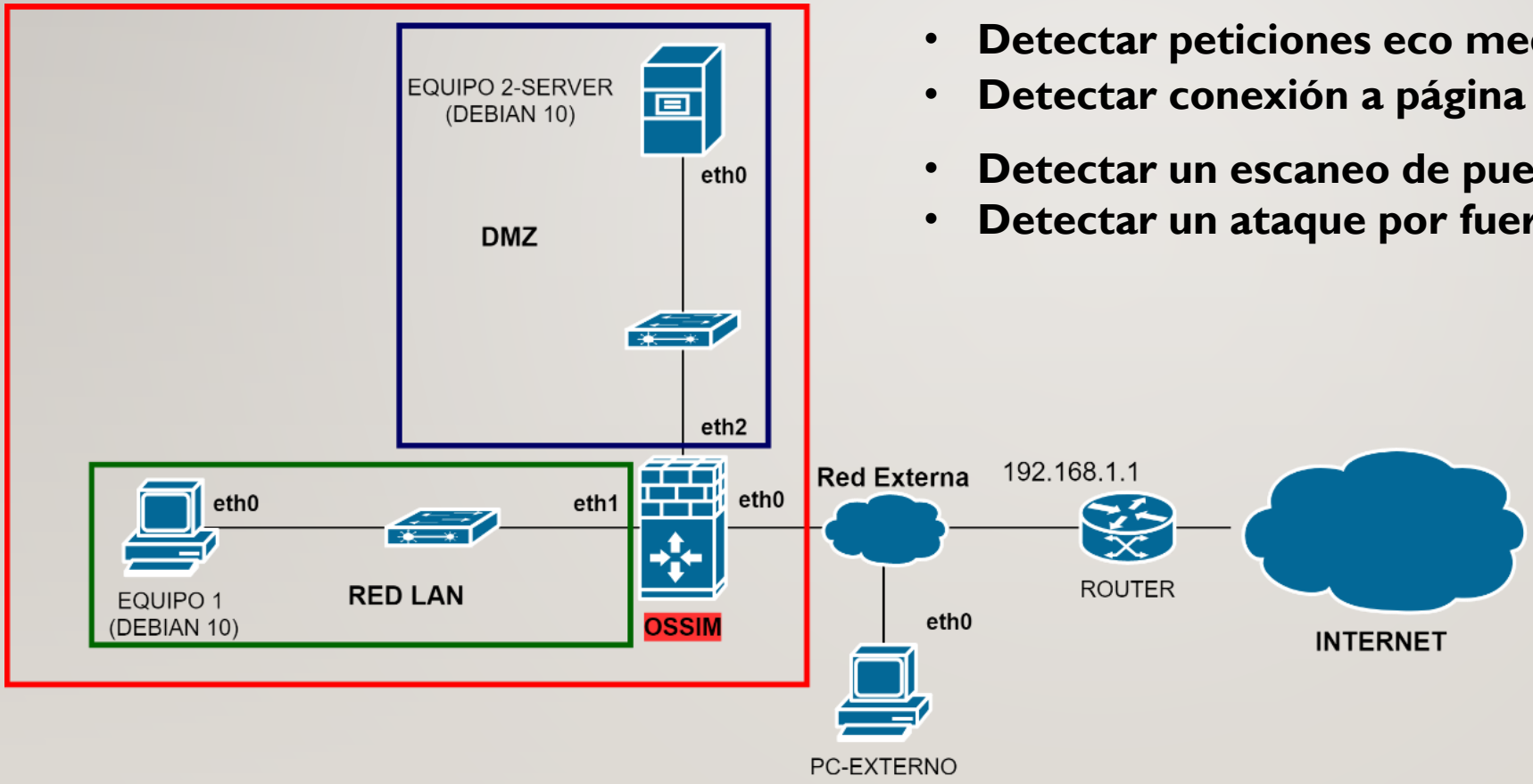
Correlación de eventos y alarmas.

- Motor de correlación. Reglas de correlación
- Directivas de correlación. Conectar o no ciertos eventos.
- Generación de alarmas en función del riesgo.

Gestión de políticas.

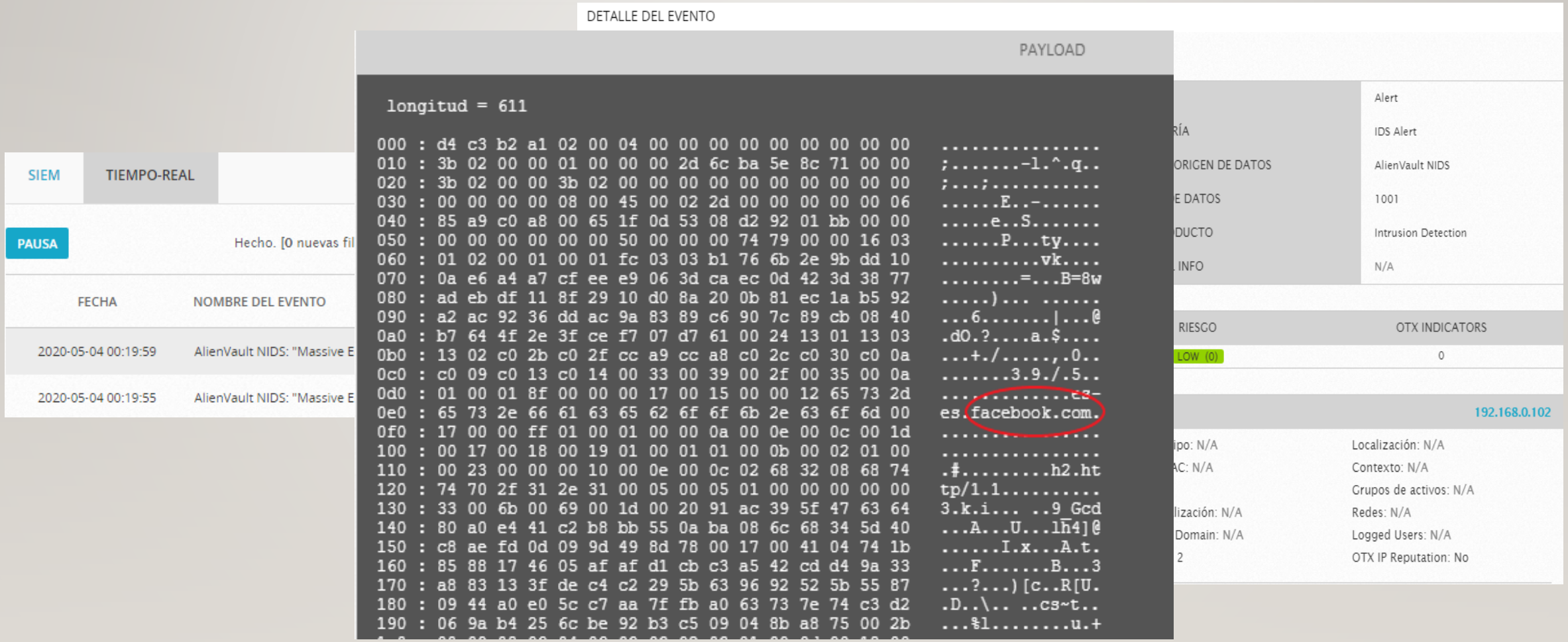
- Enviar notificaciones
- Elevar nivel de riesgo de un evento.
- Descartar evento.

4. CASO PRÁCTICO – ESCENARIO1

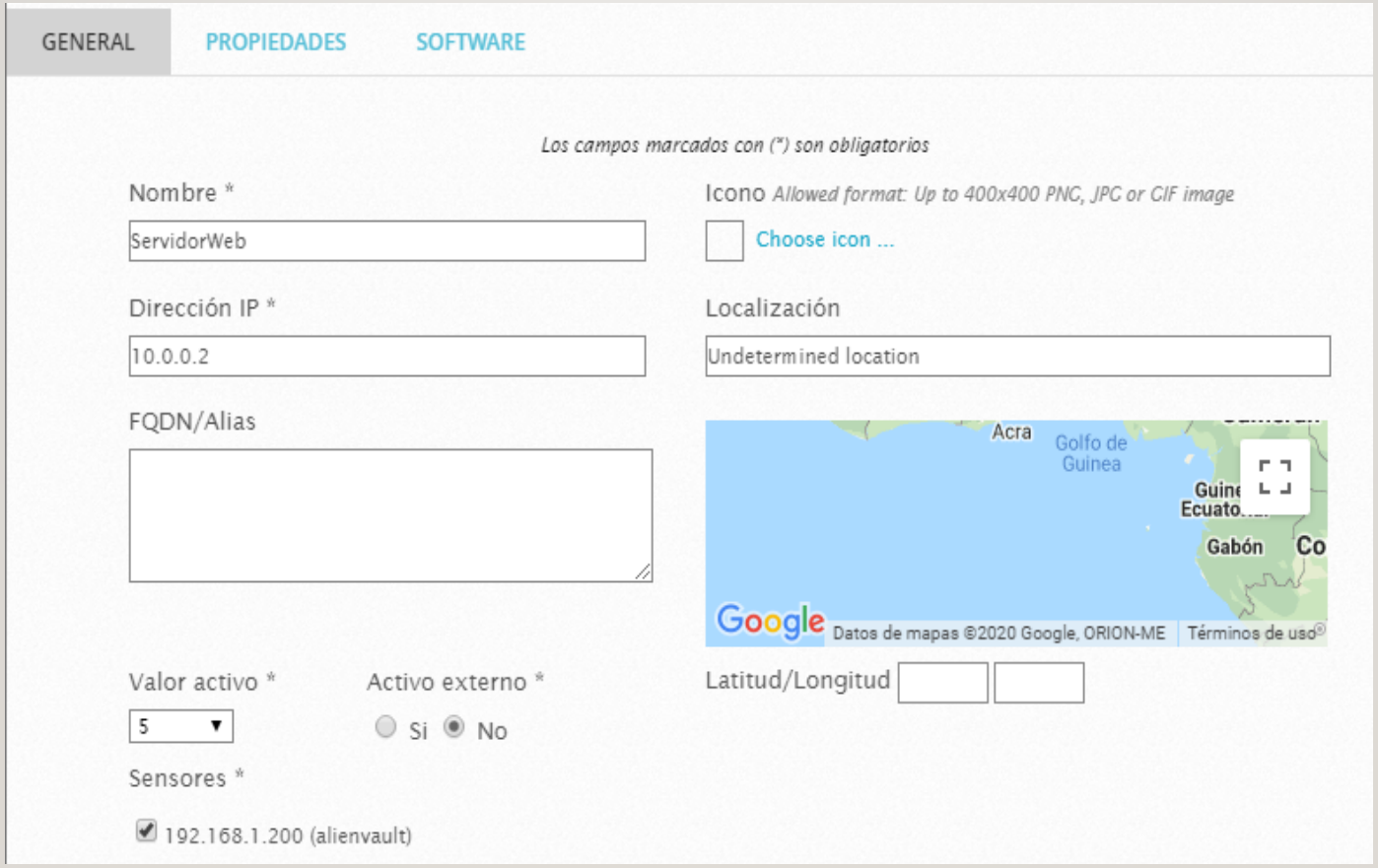


- **Detectar peticiones eco mediante el protocolo ICMP.**
- **Detectar conexión a página web no autorizada.**
- **Detectar un escaneo de puertos con Nmap.**
- **Detectar un ataque por fuerza bruta a través de SSH.**

4. CASO PRÁCTICO – ESCENARIO 1



4. CASO PRÁCTICO – ESCENARIO 1



4. CASO PRÁCTICO – ESCENARIO 1

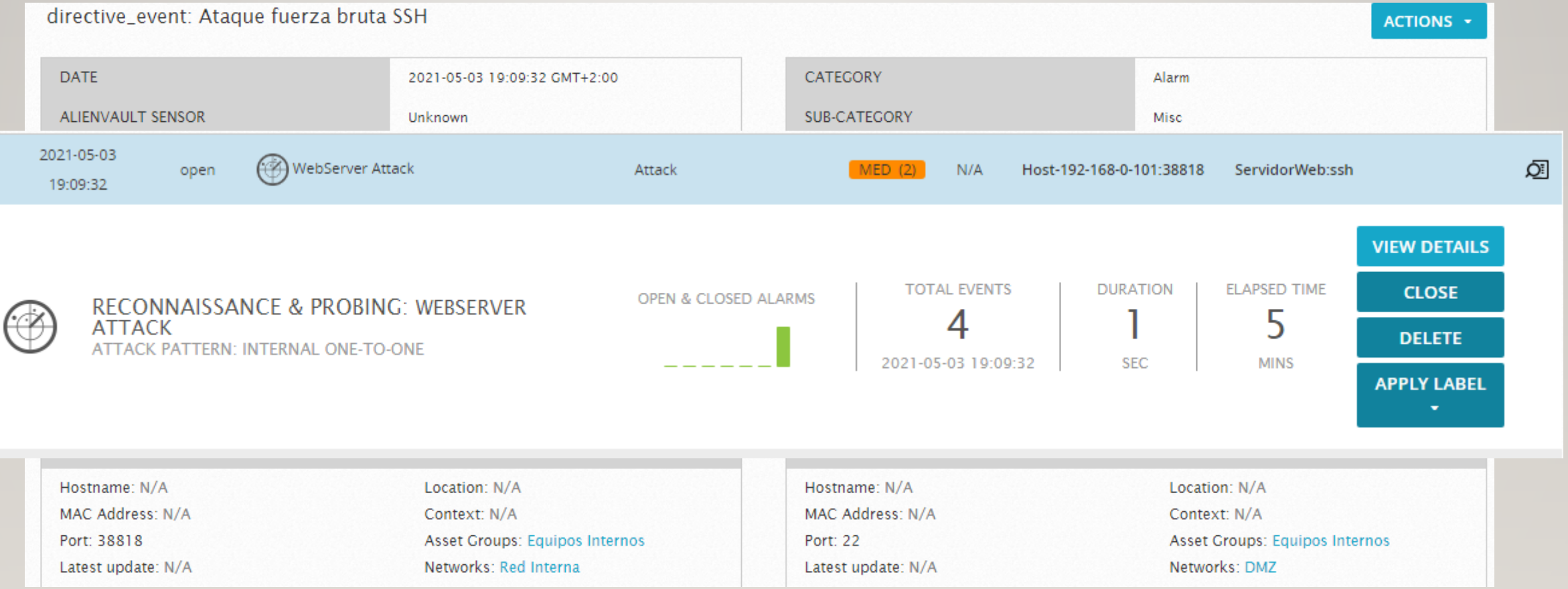
User Contributed [1 directiva]

Ataque fuerza bruta SSH
Reconnaissance & Probing, WebServer Attack, Attack - Prioridad 4

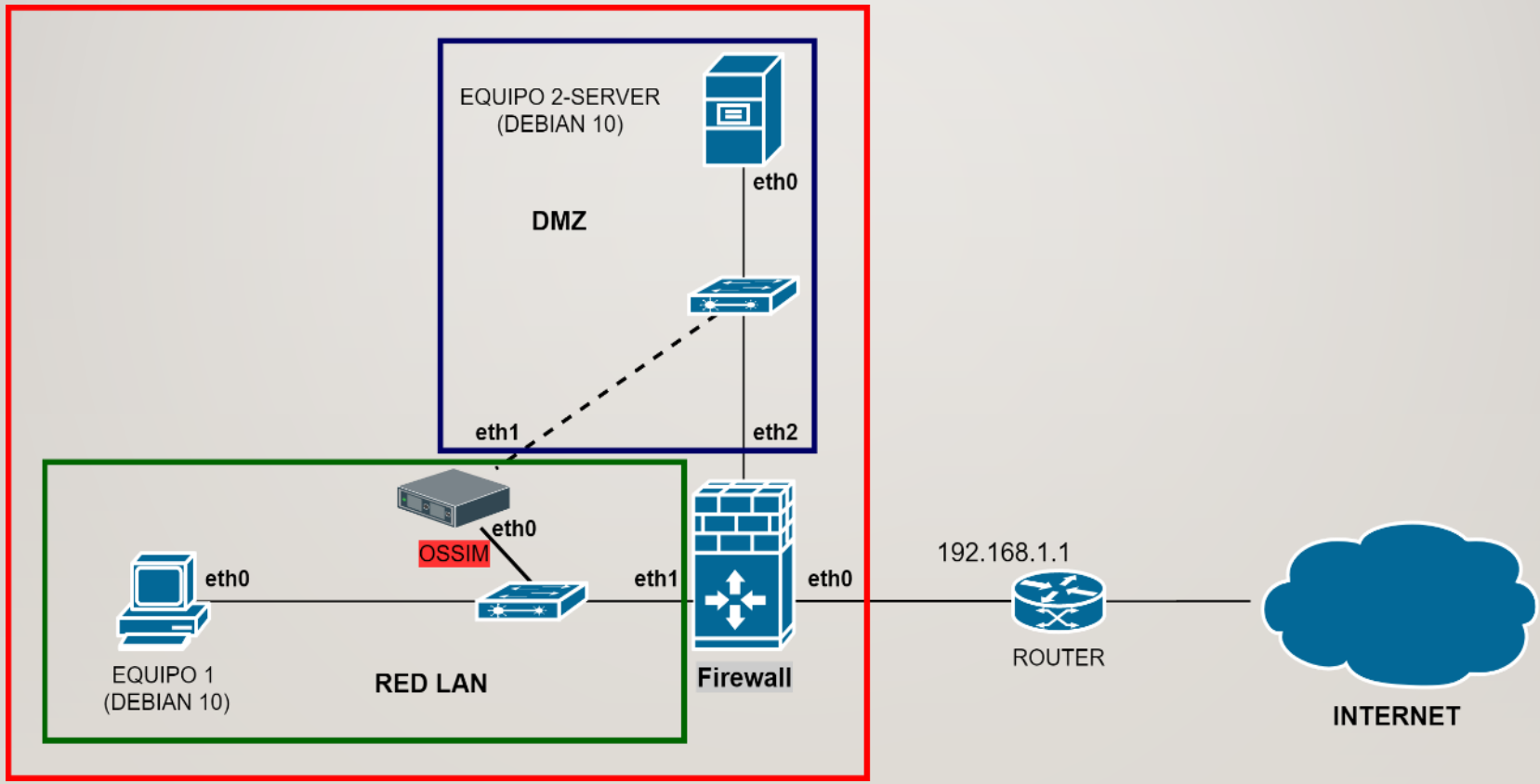
REGLAS

NOMBRE	FIABILIDAD	TIMEOUT	OCURRENCIA	DESDE	PARA	ORIGEN DE DATOS	TIPO DE EVENTO	[...]
Intento de acceso ssh	2	Ninguno	1	ANY	ServidorWeb:22	AlienVault NIDS (1001)	SIDs: 2001219 2003068	Más
Intento de acceso ssh	7	60	3	1:SRC_IP	1:DST_IP:1:DST_PORT	AlienVault NIDS (1001)	SIDs: 1:PLUGIN_SID	Más

4. CASO PRÁCTICO – ESCENARIO 1

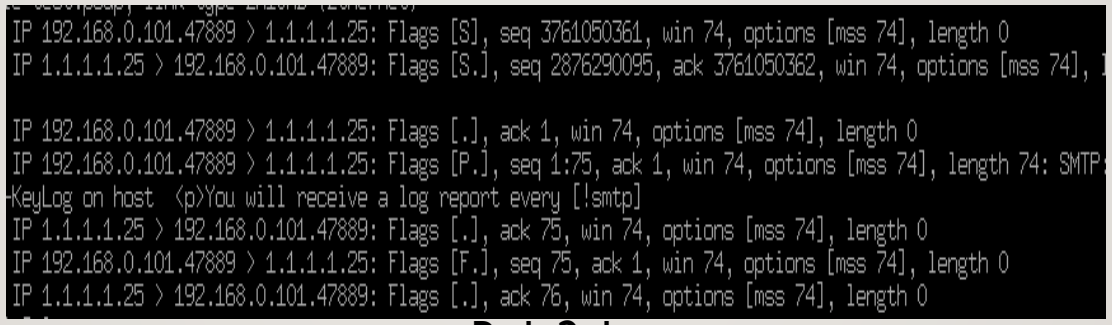


4. CASO PRÁCTICO – ESCENARIO 2

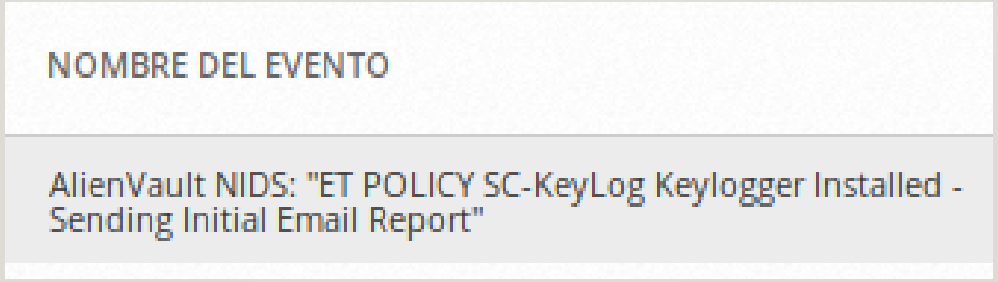


4. CASO PRÁCTICO – ESCENARIO 2

Detectar troyano.



Rule2alert



4. CASO PRÁCTICO – ESCENARIO 2

EVE17	Troyano detectado	10	2021-05-03 19:29:14	00:00	Jesús Herrera	admin	Generic	Open
EVE16	Troyano detectado	10	2021-05-03 18:17:06	00:00	Jesús Herrera	Jesús Herrera	Generic	Open

5. DEBATE

- ✓ ¿Necesidad de monitorización?
- ✓ ¿Cuándo desplegamos un SIEM?
- ✓ ¿Merecen la pena este tipo de sistemas? ¿Y los NGFW?
- ✓ ¿Contamos con el factor productivo? ¿Y el económico?
- ✓ IA
- ✓ Big Data. Tratamiento masivo de datos. ELK
- ✓ Endpoint security

Muchas gracias por la atención.

jesusherrerapalacios0@gmail.com
jherrera@pulsia.es