Universidad Autónoma de Madrid

Proyecto SinMalos

Victor Barahona (UAM)

GGTT 2018 – Ciudad Real

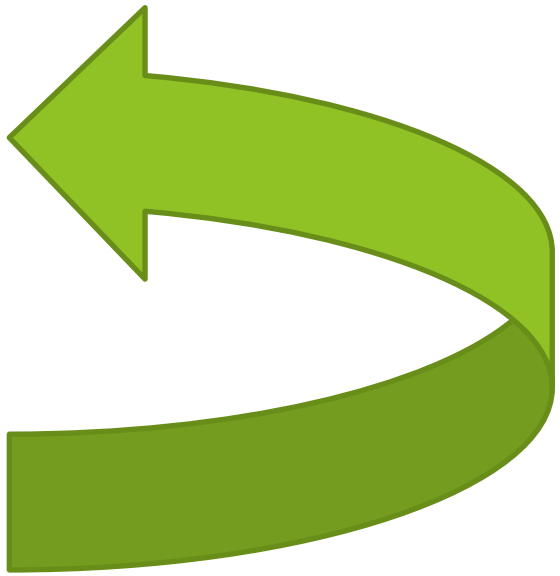
Universidad Autónoma de Madrid

Red de la UAM

- Direccionamiento público
- 20K dispositivos conectados
- Usuarios modo CPSC
- Red abierta
- Superficie de exposición masiva
- Aprox 200M conex/dia desde internet
- Escaneos masivos (ssh, telnet, SIP, 80, 443)
- Botnets (Mirai, Reaper, Hajime, Satori, etc)
- Impacto en los FWs
- Impacto en los SIEM

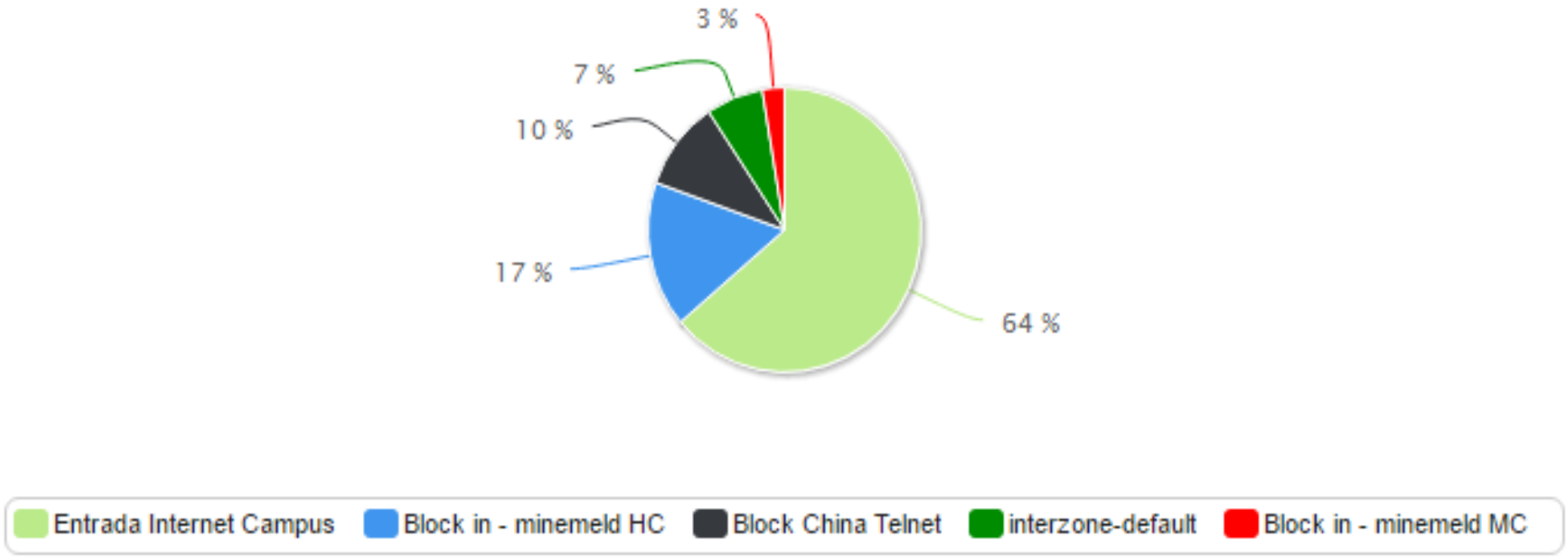
Política de protección 2016

- 2 x PaloAlto 5050
  - Desde 2012
  - Core de red y seguridad
  - Políticas anti DDoS
- Minemeld
  - Fuentes públicas



Resultados de 2016

- Beneficios:
  - entre el 15 - 20% del tráfico de internet era (felizmente) descartado.
  - >300-500 drop/sec.



Conclusiones en 2016

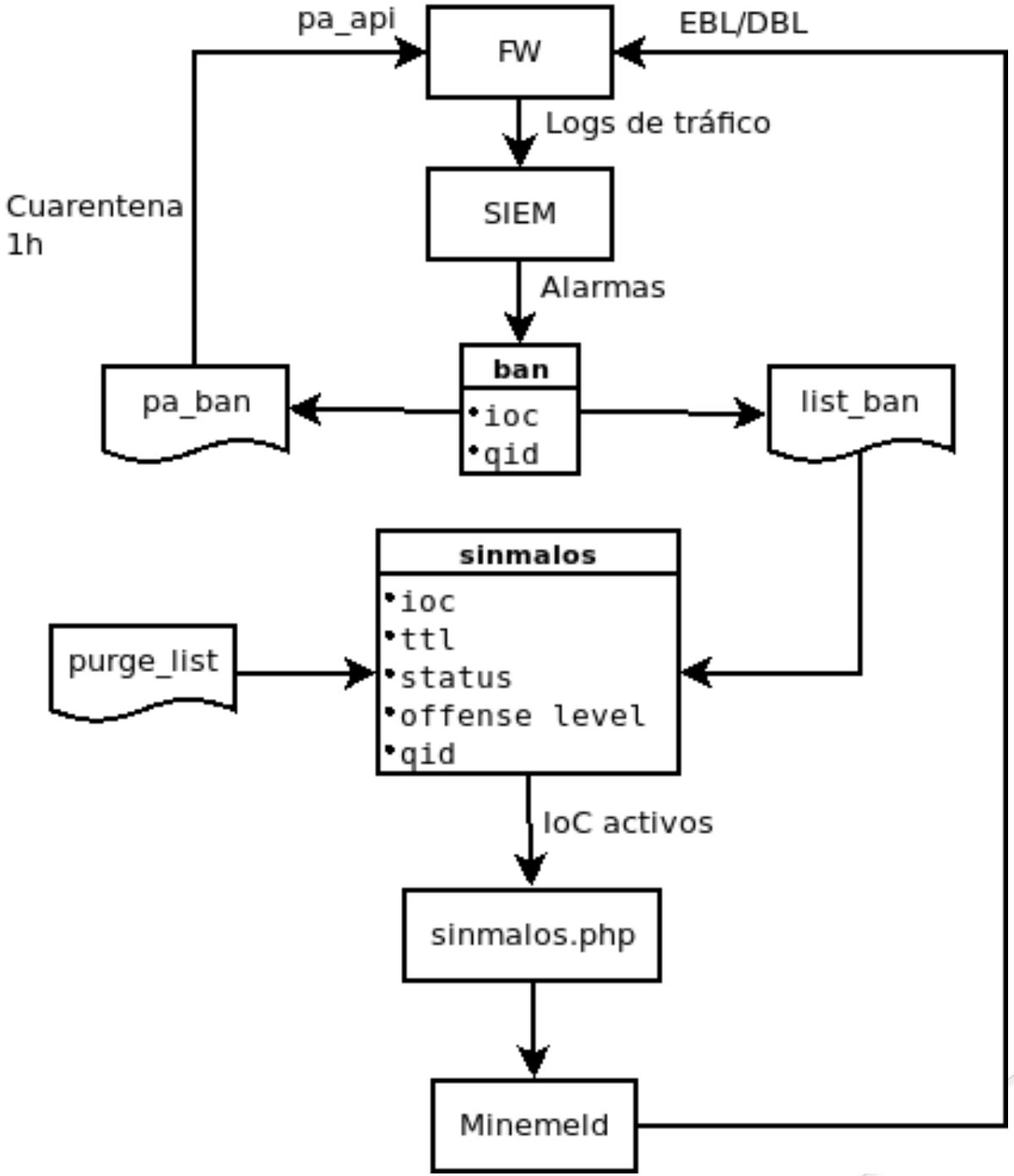
- Pros
  - Minemeld es fácil de montar
  - Beneficios inmediatos
  - Riesgo bajo
- Contras
  - Poco control de los orígenes de los feed
  - Alto nivel de trafico malicioso aun permitido

Proyecto SinMalos (Jul 2017): Objetivos

- Parar más...
- Mucho mas...
- Pero sin impacto
- Sin falsos positivos (tras un periodo de ajuste)
- Autogestionado
- Plug & forget
- Not perfect BUT good enough

Ingredientes

- Logs del Firewall (PaloAlto)
- Flujos de red (Nprobe)
- SIEM (Qradar)
- MySQL
- PERL
- PHP


pa_api
FW
EBL/DBL
Logs de tráfico
Cuarentena
1h
SIEM
Alarmas
ban
•ioc
•qid
pa_ban
list_ban
sinmalos
•ioc
•ttl
•status
•offense level
•qid
purge_list
IoC activos
sinmalos.php
Minemeld

In and out

- Se entra por ser Malo
- Se sale por ser Bueno

Offese Level	Tiempo de Baneo
1	1d
2	2d
3	4d
4	16d

Reglas

- Regla pensada para drops en red Campus, donde casi todo está permitido

Excessive Firewall Denies from Remote Host

- when the event context is Remote to Local **(from internet)**
- and when any of these BB:CategoryDefinition: Firewall or ACL Denies with the same source IP more than 5 times, across more than 15 destination IP within 5 minutes **(5x15x5)**
- and NOT when any of Rulename (custom) match sinmalos **(evito reglas sinmalos)**
- and NOT when the destination network is Server_Network.TI **(evitamos servidores)**

Reglas

- Regla pensada para accepts en la red de Campus

Excessive Firewall Accepts Across Multiple Host form Remote

- when the event context is Remote to Local **(from internet)**
- and when any of these BB:CategoryDefinition: Firewall or ACL Accept with the same source IP more than 2 times, across more than 30 destination IP within 5 minutes **(2x30x5)**
- and NOT when an event matches any of the following BB:HostDefinition: Servers **(evita servidores)**

Reglas

Excessive Firewall Accepts with no answer

- Firewall or ACL Accept with the same source IP more than 2 times, across more than 15 destination IP within 15 minutes **(2x15x15)**
- and when the event context is Remote to Local **(from internet)**
- and when the IP protocol is one of the following TCP **(TCP)**
- and when any of Packets (custom) match ^[1|2]$ **(conex sin respuesta)**

Too many Firewall accepts with no answer

- when the event Excessive Firewall Accepts with no answer
- and when at least 2 events are seen with the same Source IP in 4 hour(s) **(2x4h)**

Reglas

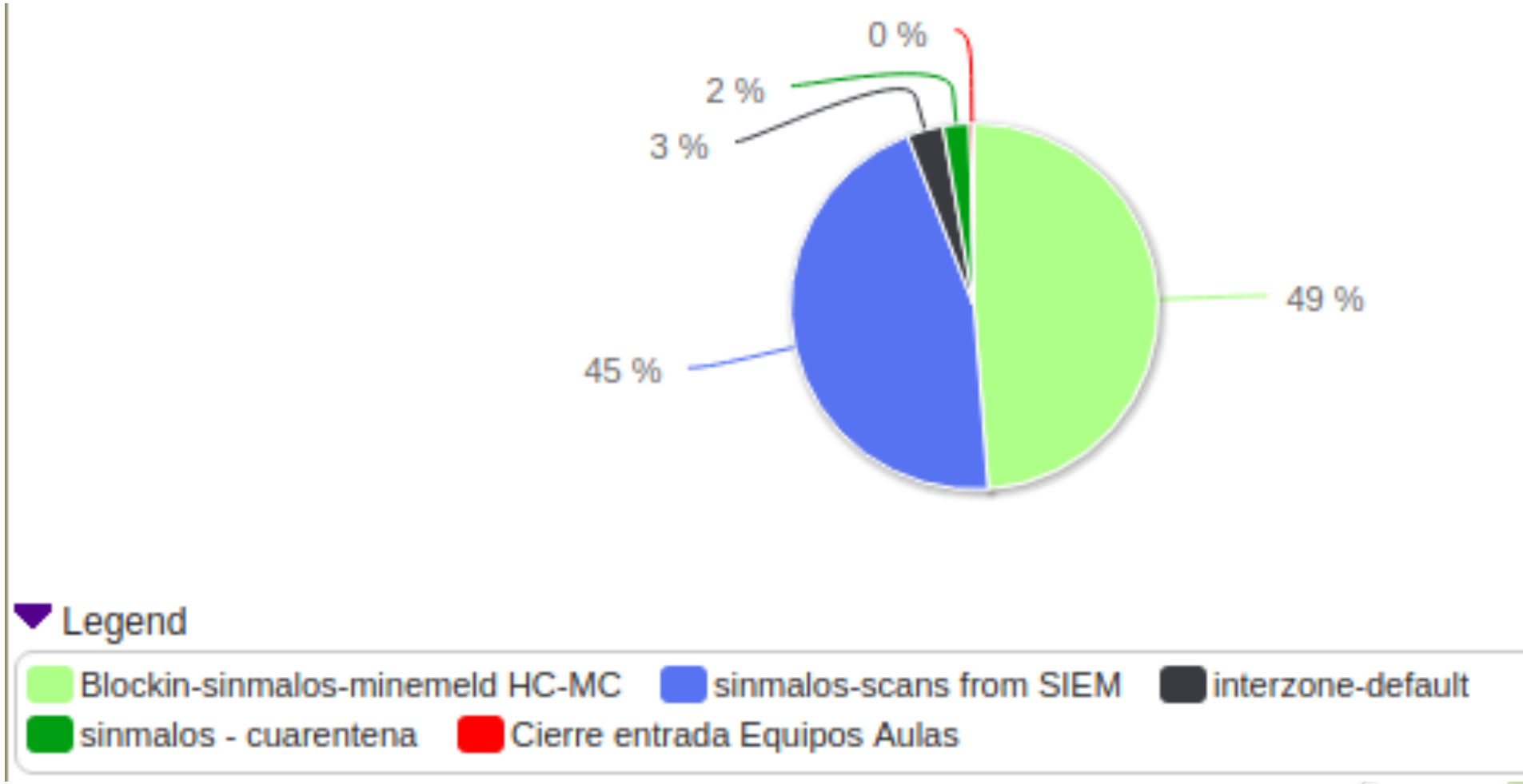
Excessive Firewall Accepts with no answer Slow

- when any of these BB:CategoryDefinition: Firewall or ACL Accept with the same source IP more than 2 times, across more than 40 destination IP within 24 hours **(2x40x24h)**
- and when the event context is Remote to Local **(from internet)**
- and when the IP protocol is one of the following TCP **(TCP)**
- and when any of Packets (custom) match ^[1|2]$ **(conex sin respuesta)**

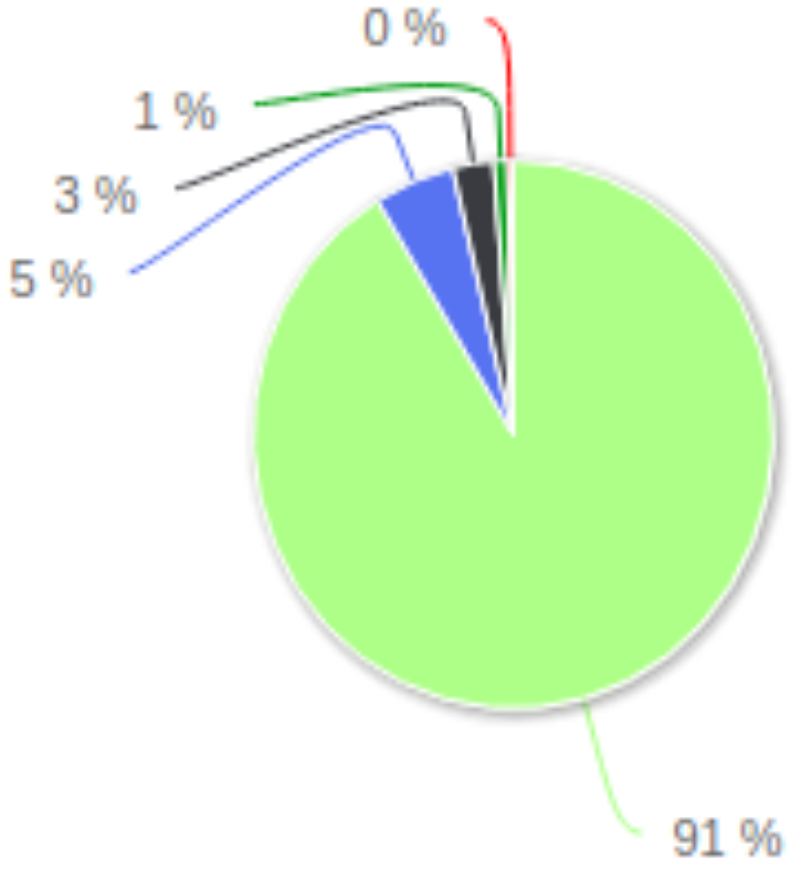
Resultados 2018

- Filtramos usando PBF
- Recibimos unos 200Mill de conexiones diarias (src Zona Internet)
  - Filtramos unas 140M conx/dia
  - Permitimos unas 60M conx/dia
- Si solo miramos conex a las redes de usuarios (dst Zona Campus)
  - Filtrando el 92-97% de las conexiones.
  - Permitiendo entre el 3-8% de las conexiones

Aplicando Minemeld y luego SinMalos



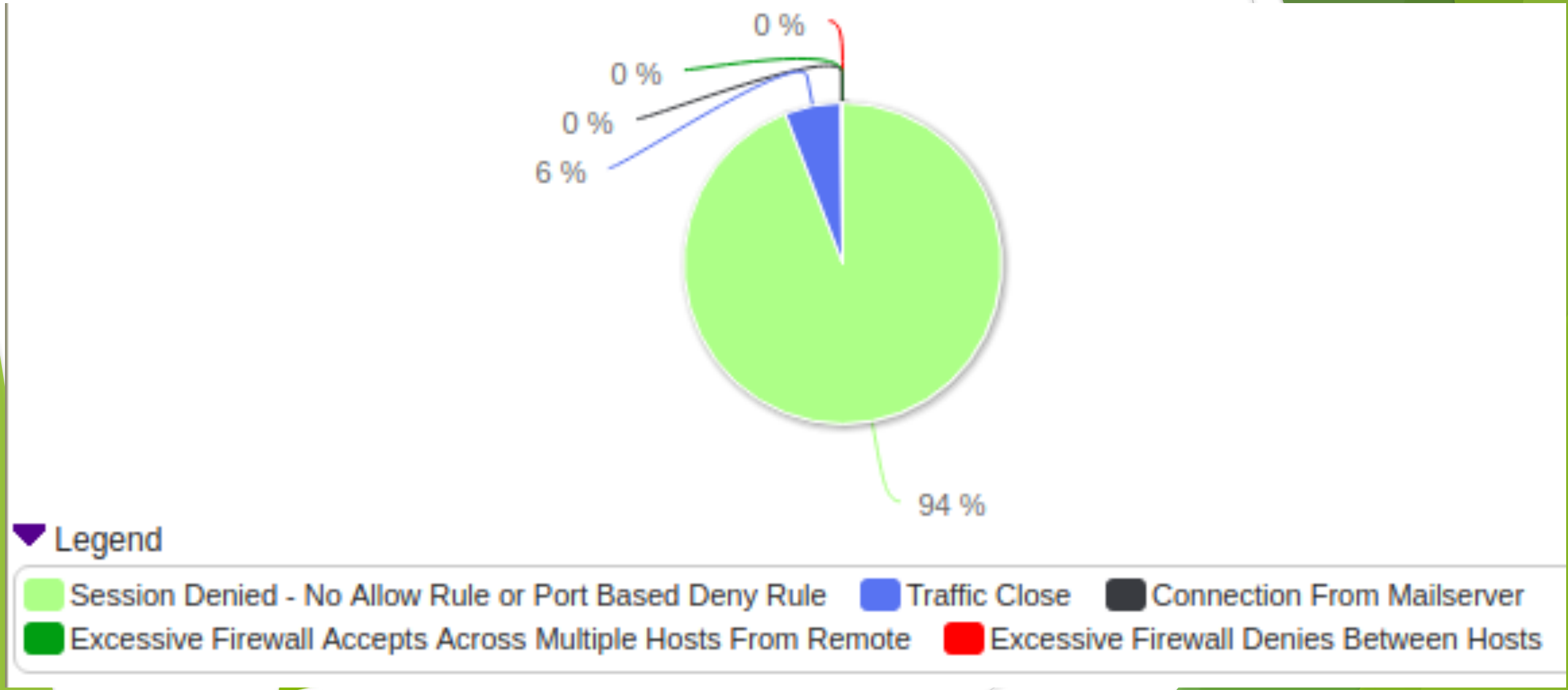
Aplicando SinMalos y luego Minemeld



Legend

sinmalos-scans from SIEM
interzone-default
sinmalos - cuarentena
Block in - minemeld HC-MC
Cierre entrada Equipos Aulas

Dst Red Campus: Filtrado vs Permitido



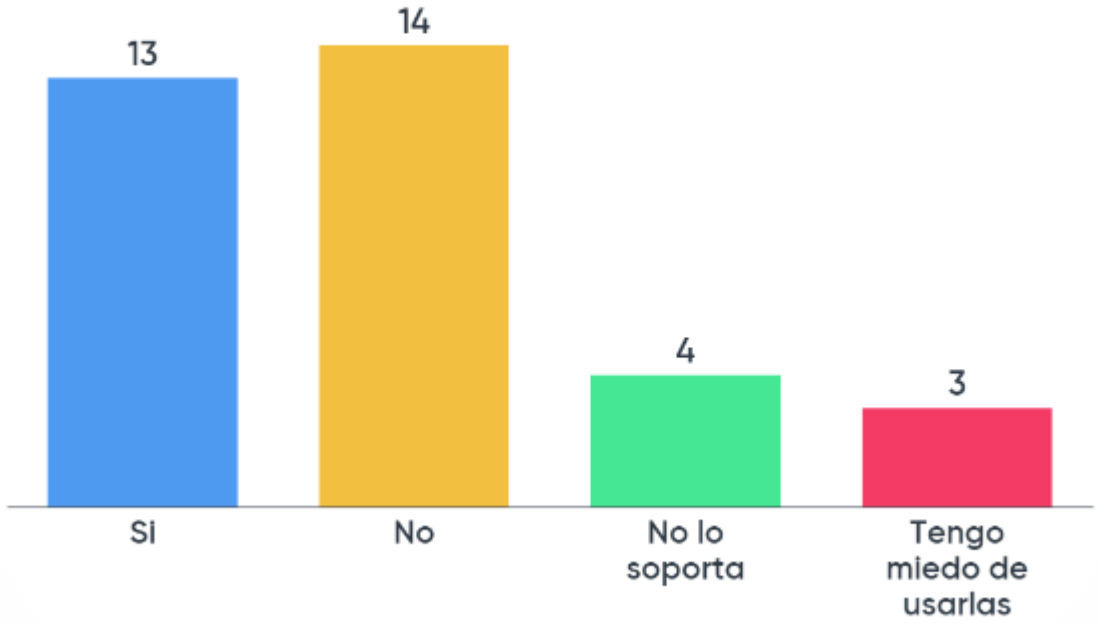
Conclusiones

- Minemeld mola
- Minemeld + SinMalos mola más
- Estamos mucho mejor que en el 2016
- No hemos vuelto a tener impacto en los FW por DoS
- Nuestra implementación de SinMalos no es exportable
- Pero la idea de SinMalos si
- Intelligence Gathering Network
- Compartir es amar

Resultados de la encuesta

¿Usas listas negras dinámicas en tu FW?

Mentimeter

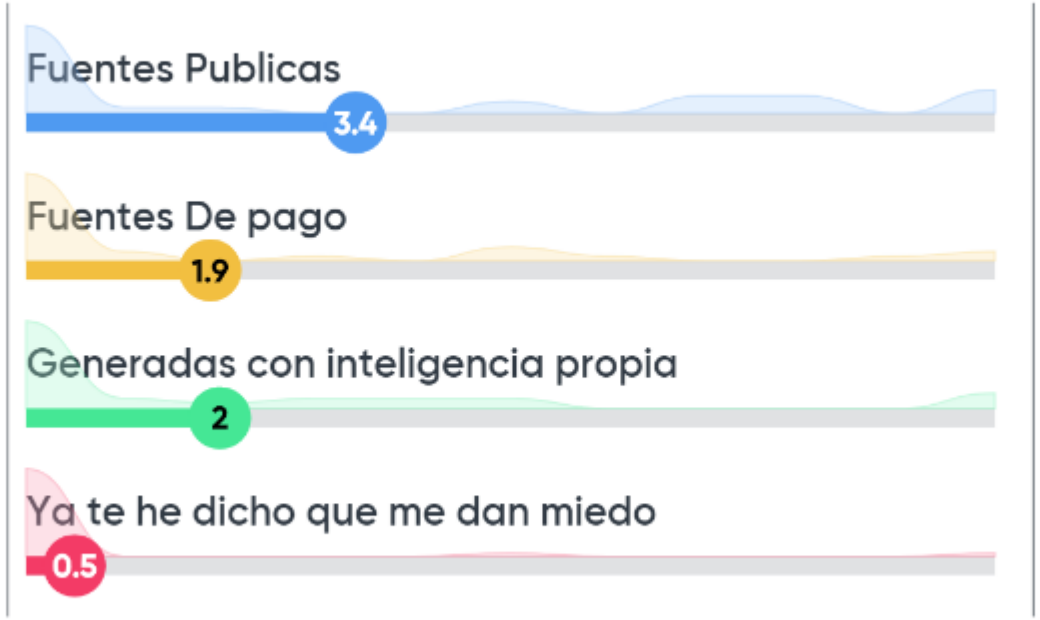


34

UAM Universidad Autónoma de Madrid

¿Cual es el origen de las listas que consultas?

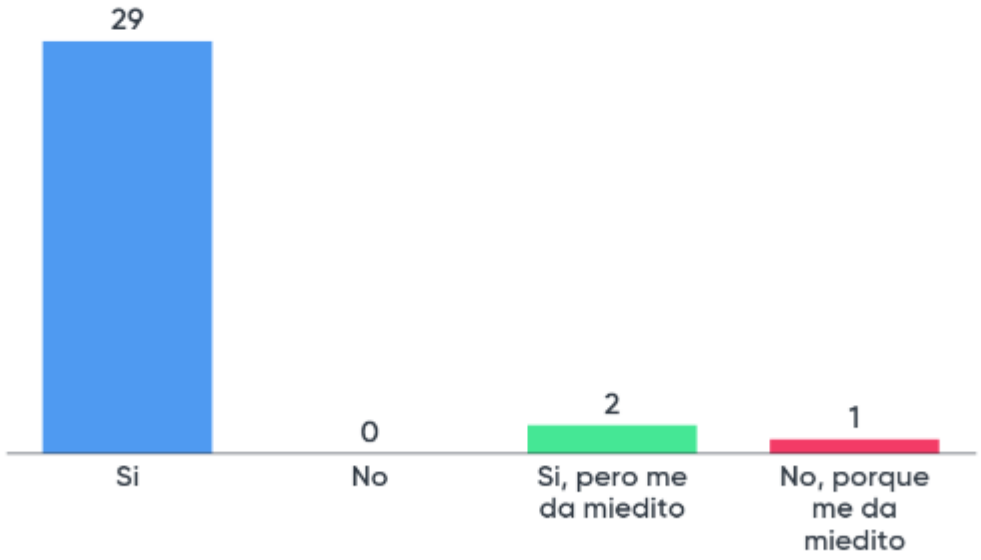
Mentimeter



32

¿Considerías util la creación de una lista negra colaborativa en RedIRIS?

Mentimeter



32

?