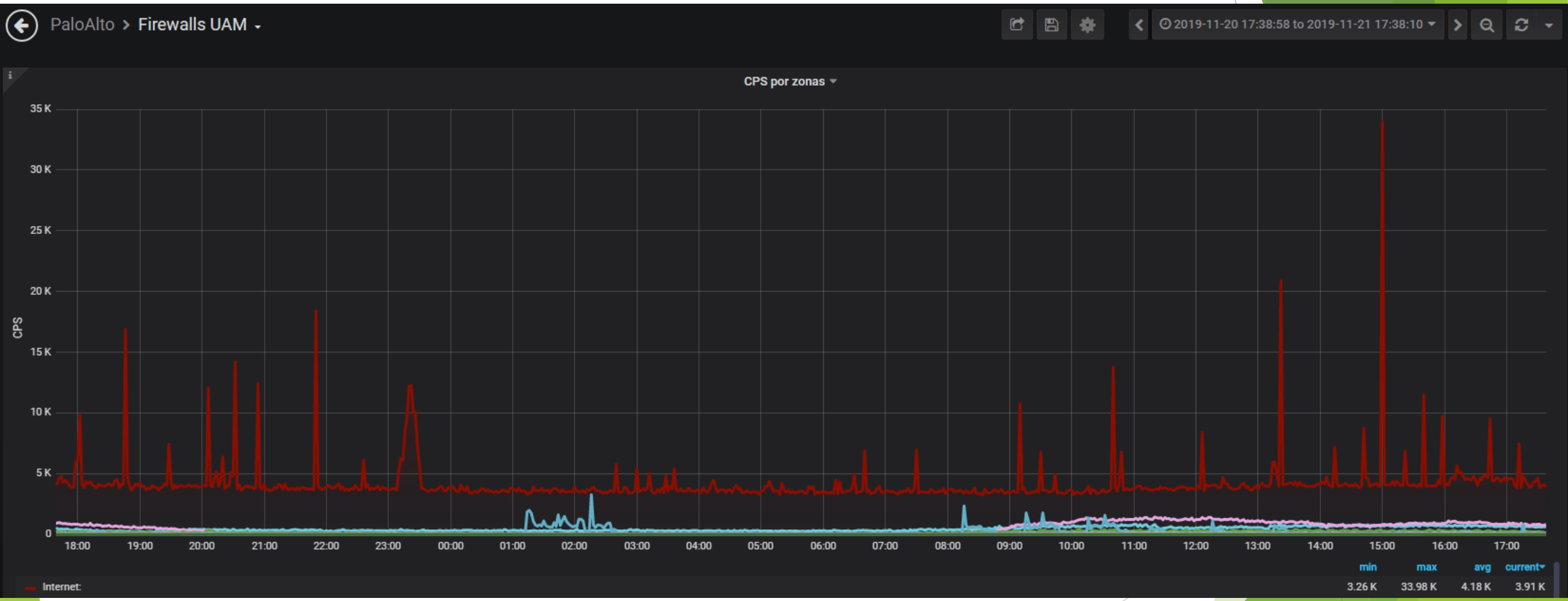
Universidad Autónoma de Madrid

Proyecto SinMalos

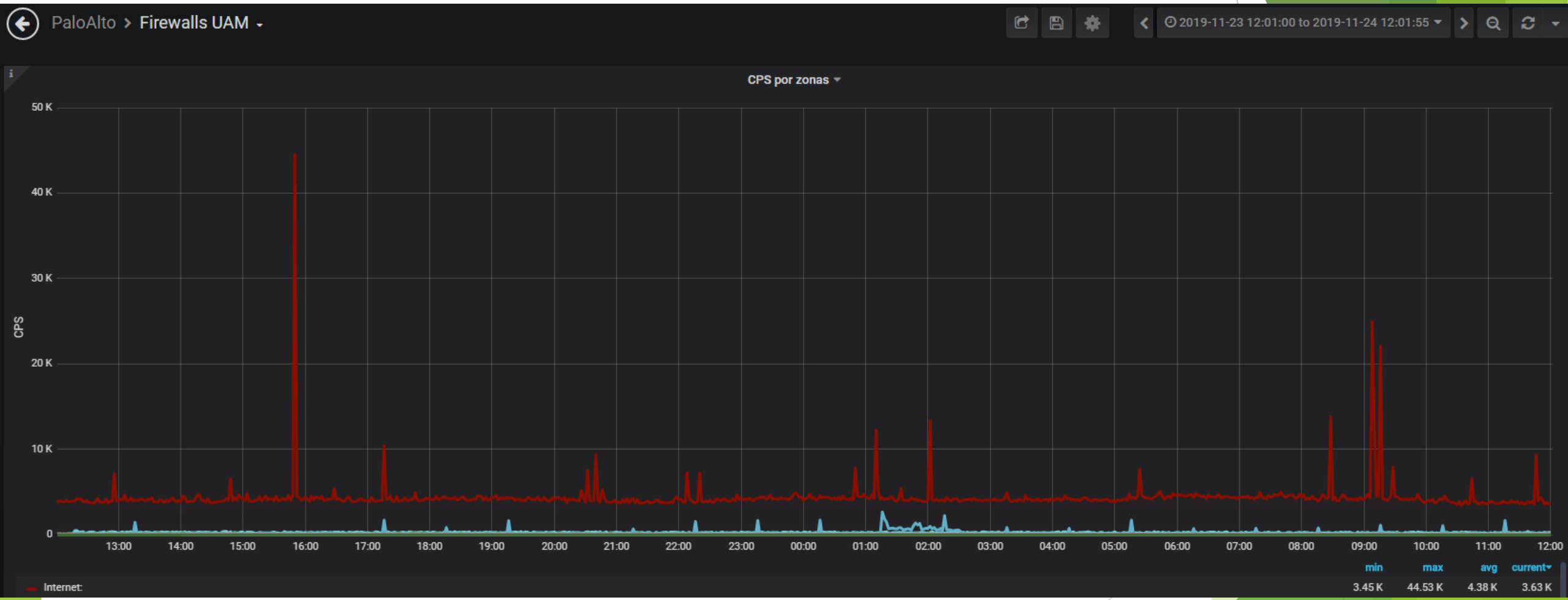
Victor Barahona (UAM)

GGTT 2019 - Valladolid

El “ruido” de Internet



El “ruido” sonando en weekend



Proyecto SinMalos

- Minemeld fuentes públicas 2016
- SinMalos UAM 2017
- GGTT Ciudad Real 2018
- SinMalos-UAM:
  - Basadas en correlación ataques recibidos (SIEM)
  - Autogeneradas
  - Autogestionadas
- Propuesta de compartición de listas en la comunidad

Lo que es malo para uno
es probable que lo sea para todos

Lo que es malo para varios
SEGURO que lo es para todos

Feeds Disponibles

Feed	Criterio	Num de IoCs	Confianza
SinMalosRootValues	Todos los IoCs	120-140K	Media
SinMalosValues	Todos los IoCs	120-140K	Media
SinMalos-MultiSource	IoCs >= 2 fuentes	10-20K	Alta

Instituciones Participantes (so far)

Institución	Feed
UC3M	SinMalos-Chunguitos
UIB	SinMalos-UIB
UAM	SinMalos-UAM

$> man sinmalos

- ¿Como **consumo** SinMalos?
  - Instala Minemeld
  - Escribe a seguridad@rediris.es
- ¿Cómo **colaboro** con mi feed?
  - Instala Minemeld (debe ser alcanzable desde Rediris)
  - Escribe a seguridad@rediris.es

Consideraciones

- Disclaimer: ¡Filtrad solo en Inbound!
- No consumáis directamente SinMalos desde vuestros FW.
- Usad minemeld para gestionar las listas.
- Configurad listas blancas de vuestra infraestructura.
- Not perfect but Good Enough
- ¿Es mi feed Good Enough? Si lo usas para ti si
- El valor está en la intersección de listas
- No uséis los IoCs de SinMalos en vuestras reglas de correlación de generación de listas. ¡Nos cargamos el valor!

WE WANT YOUR FEEDS!!