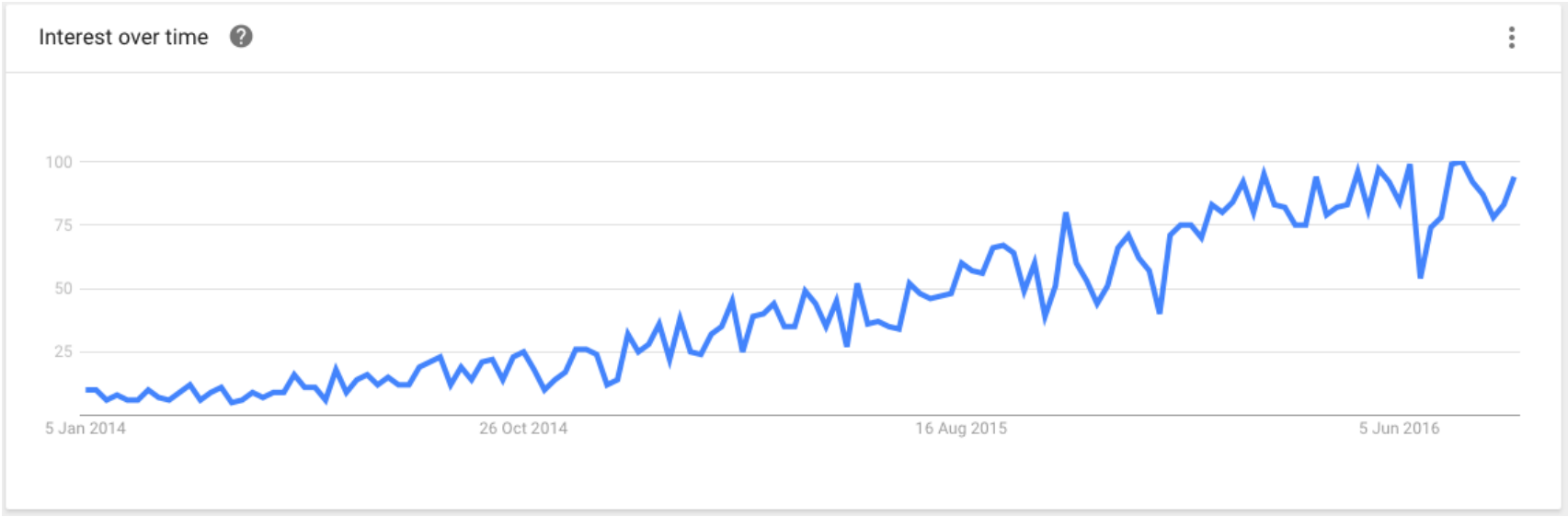
ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

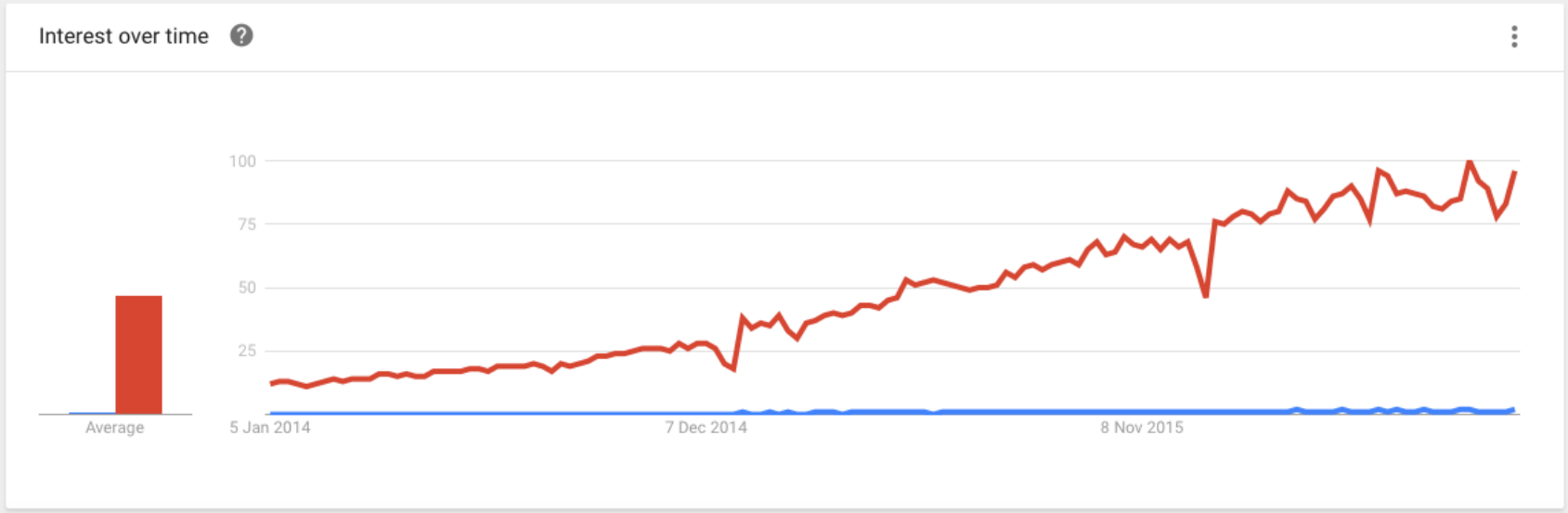
El papel del operador en la Seguridad IoT

Telefónica

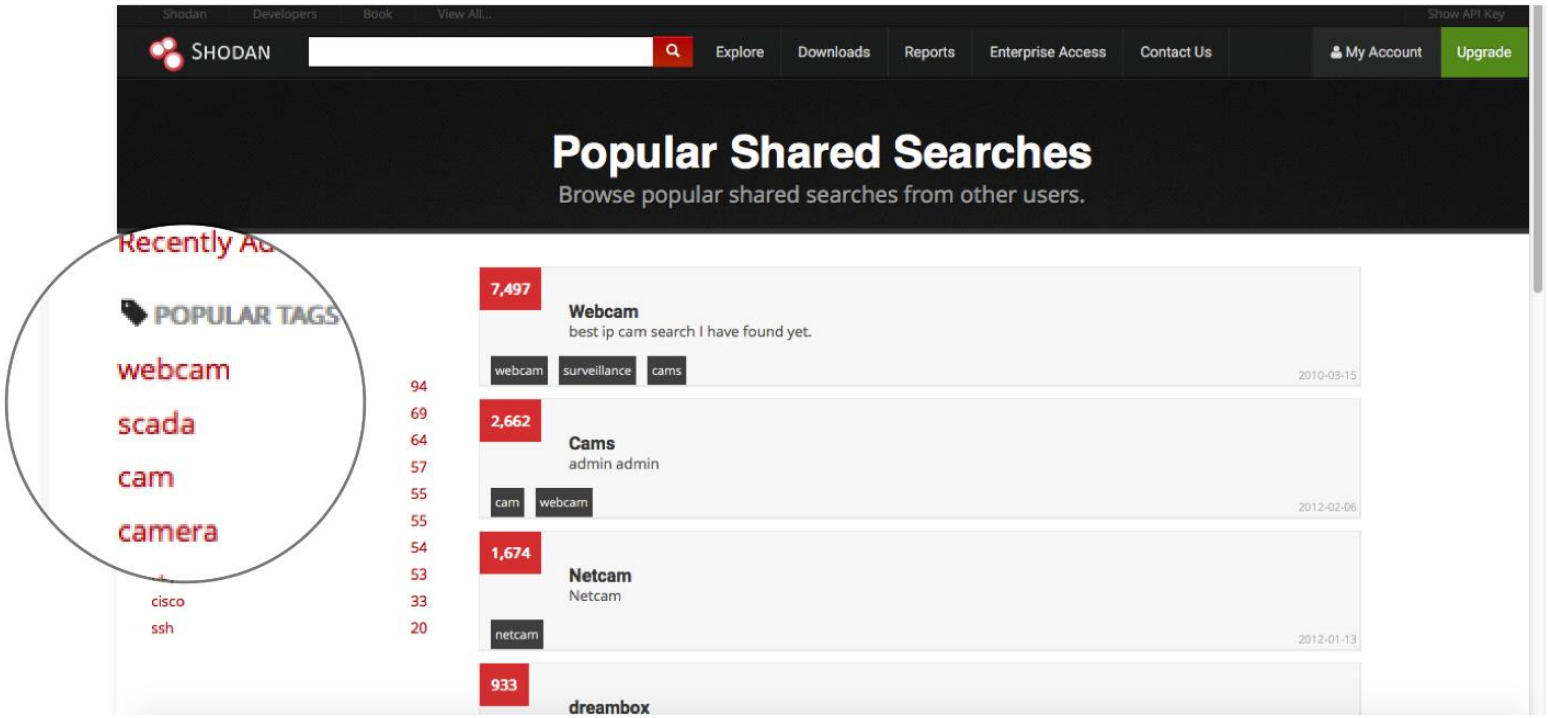
El interés en la Seguridad IoT está creciendo si miramos Google Trends



Pero todavía es muy bajo si lo comparamos con el interés en IoT



Sin embargo, en Shodan, SCADA es el #2 en popular tags

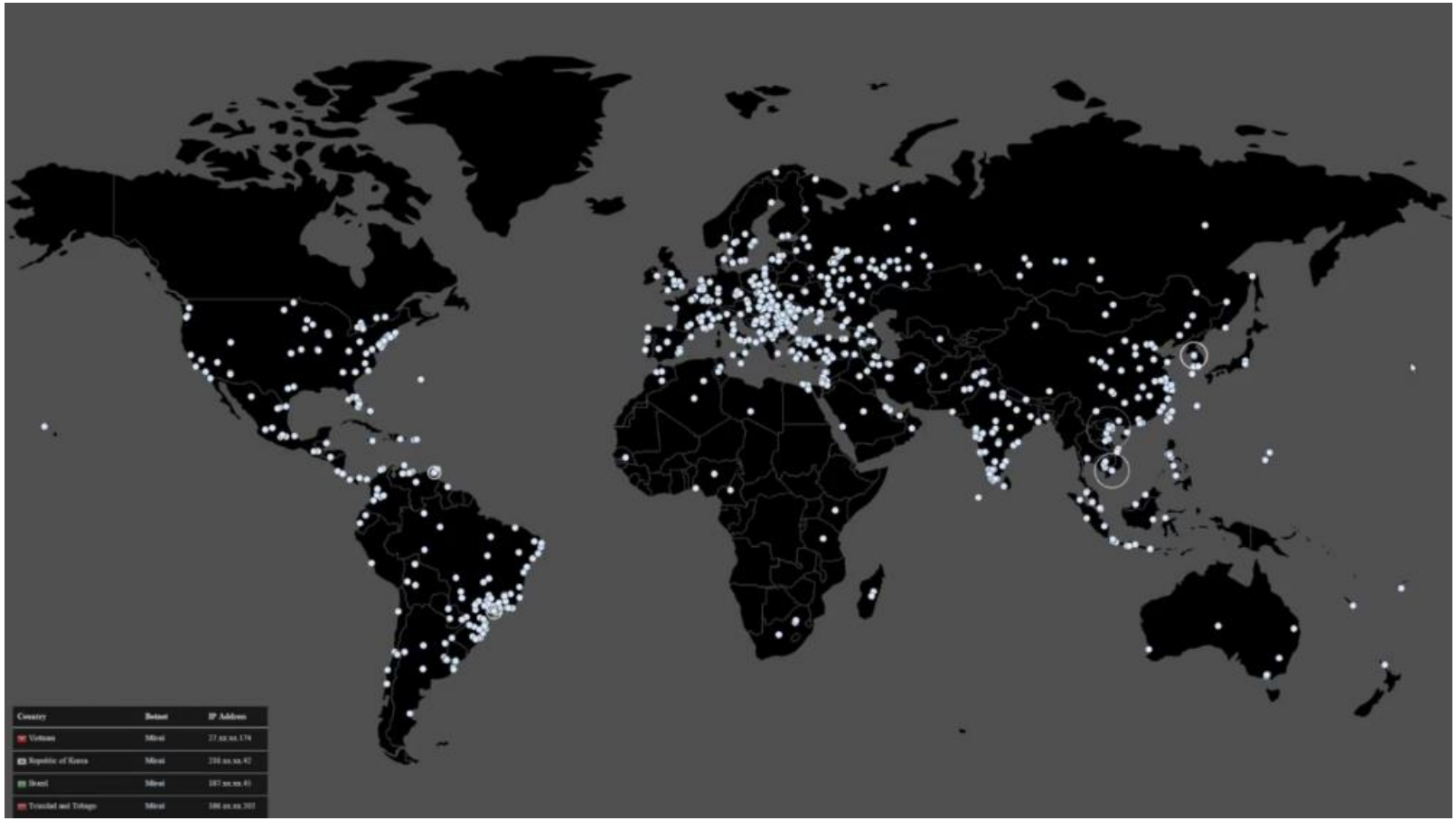


En Shodan podemos encontrar desde taxímetros conectados …

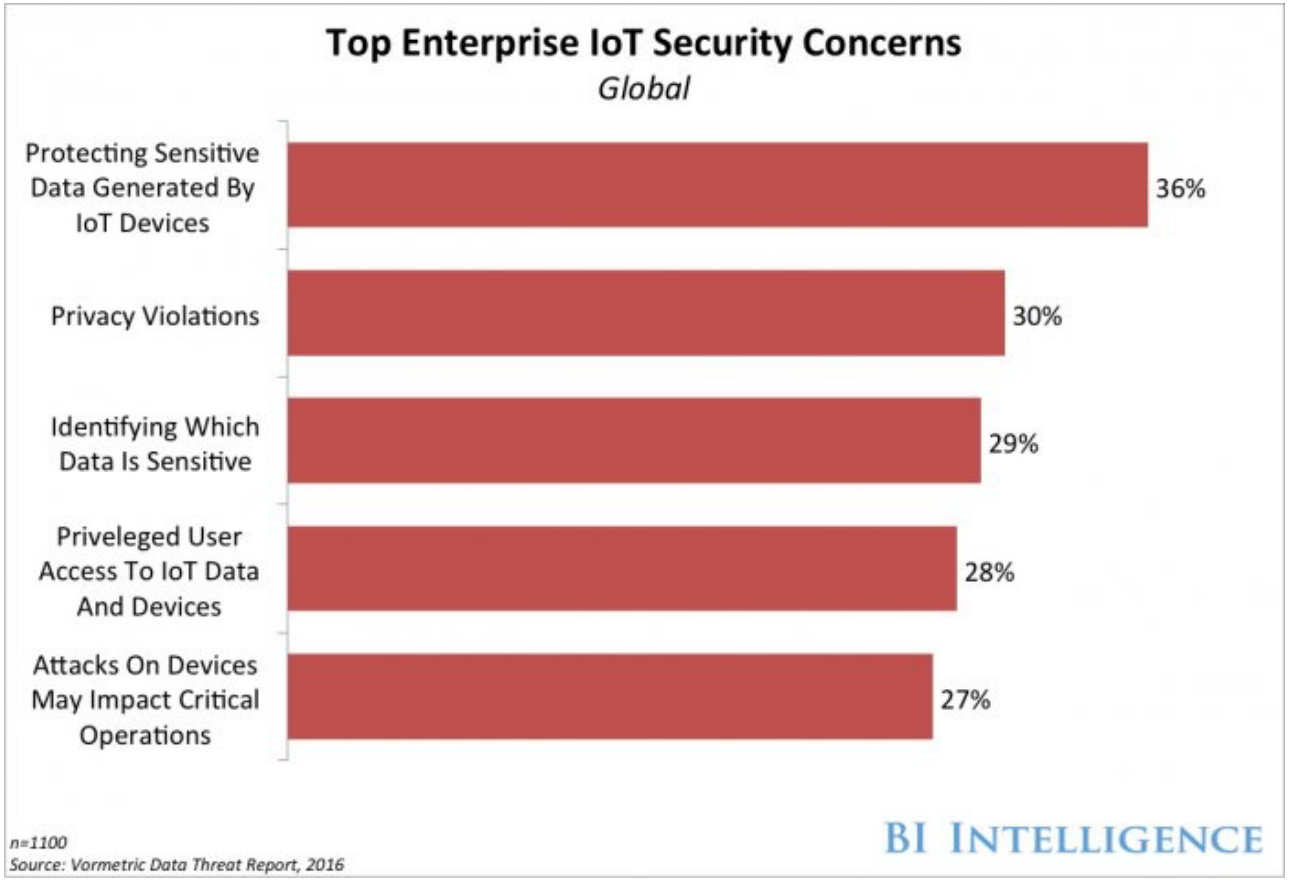
Source: http://www.elladodelmal.com/2016/05/hacking-de-taximetros-en-espana-via.html

Hasta webcams con usuario y password por defecto …

Capaces de generar un DDoS de 600 GB/s



La industria ya tiene conciencia de las implicaciones de Seguridad IoT



La seguridad IoT debe considerarse una cuestión de negocio

Preocupación en seguridad como barrera

Es el principal obstáculo para el desarrollo de productos conectados

VDC Research – Dic 2014

Los incidentes afectan al negocio

Fiat hizo un recall de 1.4M Jeep Grand Cheerokee tras el hacking

Wired (Jul 2015)

La operadora como partner de Seguridad

Como proveedor de la conectividad el operador puede aportar aislamiento y monitorización del tráfico.

Retos de la seguridad IoT

Diversidad

Los dispositivos, redes de conectividad, los protocolos de aplicación, métodos de autenticación y plataformas en la nube son muy diversos.

Recursos

Los dispositivos están computacionalmente muy limitados con el fin de adaptarse a las restricciones de coste y de la batería en despliegues masivos de IoT.

Identidad

Asignar a los dispositivos una identidad que permita establecer un canal seguro de comunicación.

Operación

Asegurar la disponibilidad de los dispositivos que han sido diseñados para ser desatentidos en localizaciones remotas.

Muchos retos pueden afrontarse con los activos del operador

VPN y APNs privados	Aislando dispositivos de Internet evitando que sean accesibles por cualquiera
Monitorización Comunicaciones	Monitorizando el tráfico para detectar, reportar y eventualmente bloquear la actividad inesperada
Autenticación de red	Detectando el MSISDN de que se conecta a un servicio y permitiendo validar su identidad.

Debe considerarse E2E en todas las etapas del ciclo de vida de un producto

PREVENCIÓN

Prevenir o disuadir ataques para evitar o al menos minimizar las pérdidas

DETECCIÓN

La identificación de ataques para permitir una respuesta rápida y completa

RESPUESTA

Minimizar las pérdidas y volver a la actividad normal

La GSMA ha publicado recomendaciones de seguridad IoT

La GSMA ha publicado recomendaciones de seguridad IoT

La GSMA ha concentrado estas recomendaciones en una checklist

- Estructurada
- Referenciada
- Consisa

3.3.2 Checklist For Service Platforms

3.3.2.1 General Recommendations For Service Platforms

The following recommendations are taken from CLP.11 [1].

GSMA Recommendations from CLP12 [2]		Question(s)	Control(s)	Response				Notes
ID	Recommendations			Yes	Part	No	N/A	
CLP11_7.2	11.7.2 Review the current product or service's Security Model	11.7.2.1 Have you reviewed the current product or service's Security Model?	11.7.2.1.1 We have reviewed the security model for our service platform as per document CLP.12 [2].					
CLP11_7.3	11.7.3 Review and evaluate Recommendations	11.7.3.1 Have you reviewed and evaluated the recommendations?	11.7.3.1.1 We have reviewed all of the service ecosystem security recommendations contained in document CLP.12 [2].					
CLP11_7.4	11.7.4 Implementation and Review	11.7.4.1 Have you implemented and reviewed the recommendations?	11.7.4.1 We have created a clear plan to secure each component of our service.					
			11.7.4.2 We have used our risk assessment process to develop a threat model for each component, incorporating the recommendations and risks that are appropriate for each component and security task.					
			11.7.4.4 We have reviewed the recommendations contained in CLP.12 [2] and we have ensured that our implementation fulfils the requirements set forth by this document.					
			11.7.4.5 We have ensured that the implementation solves the security risks with regard to the context in which the component is designed in our organization's product or service.					

3.3.2.2 Specific Recommendations For Service Platforms

The following recommendations are taken from CLP.12 [2].


Take part in the
GSMA IoT Security Self-Assessment