



WEBINAR

MINIMIZA LOS RIESGOS,
ASEGURA TU NEGOCIO.

(Empezamos en unos minutos. Este webinar va a ser grabado)



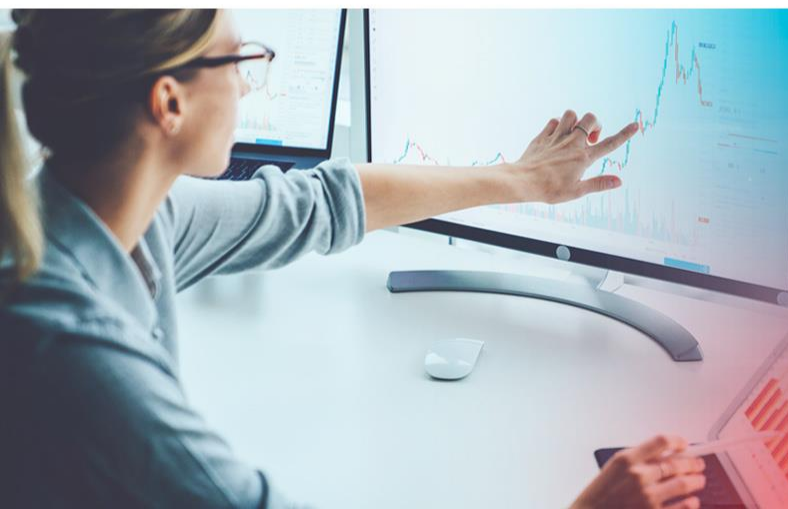
BITSIGHT

RISKMEDIA



Gobierna tu seguridad IT

Conócete, valorízate, cúbrete



José María Ochoa
Area Manager | OneseQ - Cybersecurity

BITSIGHT

RISKMEDIA

... y lo primero a asumir es

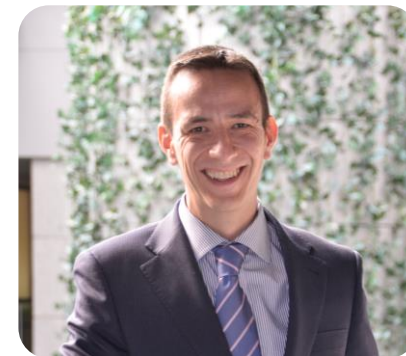


“ El verdadero conocimiento es conocer la medida de la propia ignorancia”

Autor: Confucio

“ ... para actuar en consecuencia”

Anexo: Jose María Ochoa



BITSIGHT™

RISKMEDI

Un poco de visibilidad del contexto ... “ ver para creer = conocer ”



ATTACK ORIGINS

COUNTRY
United States
China
Pakistan
Switzerland
Turkey
Netherlands
South Korea
Italy
Spain

ATTACK TYPES

#	PORT	SERVICE TYPE
61	25	smtp
25	23	telnet
12	53413	netis-router
7	8123	unknown
7	123	ntp
5	50864	xsan-file-system
4	3389	ms-wbt-server
4	443	https
3	5900	rfb

ATTACK TARGETS

#	COUNTRY
109	United States
24	United Arab Emirates
10	France
3	Spain
3	Belgium
2	Saudi Arabia
2	Italy
1	Romania
1	Norway

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
11-12-09.756	Dslam Infrastructure South	182.180.160.97	Lahore, PK	Aix-En-Provenc...	netis-router	53413
11-12-09.342	Microsoft Corporation	65.55.169.247	Washington, US	De Kalb Junctio...	smtp	25
11-12-08.875	Dslam Infrastructure South	182.180.160.97	Lahore, PK	Aix-En-Provenc...	netis-router	53413
11-12-08.411	Microsoft Corporation	157.56.111.246	Redmond, US	De Kalb Junctio...	smtp	25
11-12-08.156	Microsoft Corporation	157.56.110.248	Redmond, US	De Kalb Junctio...	smtp	25
11-12-07.811	Microsoft Corporation	65.55.169.253	Washington, US	De Kalb Junctio...	smtp	25
11-12-07.412	American National Insurance Co	50.200.102.48	League City, US	De Kalb Junctio...	https	443
11-12-07.126	ChinaNet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	unknown	8123
11-12-06.941	As29073 Ecatel Ltd	80.82.65.120	The Hague, NL	Brussels, BE	unknown	8090



HOME

EXPLORE

WHY NORSE?

Interpretemos bien lo que hemos visto

- ✓ Somos un país con un grado de destino de ataques altísimo.
- ✓ Y con un grado de origen de ataque también enorme.

	País	Riesgo de amenaza (100-0)	Softwares de seguridad instalados	Amenazas de malware	Legislación sobre ciberdelincuencia	Ranking
1	EEUU	100,0	89,9%	12,6%	✓	100,0
2	Alemania	31,6	90,1%	14,7%	✓	33,4
3	España	30,2	90,4%	20,2%	✓	32,8
4	Francia	24,9	91,8%	19,1%	✓	26,8
5	Suiza	14,2	90,2%	12,8%	✓	15,1
6	Polonia	11,9	89,2%	21,2%	✓	14,6
7	Reino Unido	13,1	91,0%	13,4%	✓	13,9
8	Japón	12,7	90,4%	11,9%	✓	13,4
9	Italia	8,7	90,4%	17,1%	✓	10,2
10	Bélgica	1,3	91,9%	16,8%	X	8,2

Actualidad Cloud Endpoint Infraestructuras críticas Normativa Vulnerabilidades
 ITDS TV IT Whitepapers IT Webinars Content Marketing Revistas digitales IT Trends

España es el tercer país con más riesgo de sufrir ciberataques

Actualidad 30 DIC 2020



LOS CIBERDELINCUENTES SE APROVECHAN DE LA CRISIS

España es uno de los cinco países del mundo con más ciberataques a autónomos y a pequeños negocios



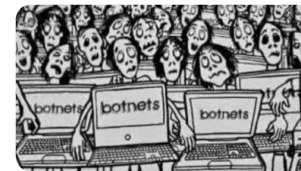
Nuestra situación



- ✓ Tenemos un capacidad de red muy alta comparada con otros países.
- ✓ Somos atacados porque somos facilones
 - Nuestro grado de madurez en protección no es muy elevado
- ✓ Y por ello tenemos dos vertientes para los atacantes:



- Atacarnos para robarnos
- Usarnos para atacar a otros destinos (zombies)



Por lo tanto somos ... ¡ muertos vivos !

OneseQ
by alhambra



Gestionamos
Servicios

Gestionamos
Impactos



¿Nos hemos preocupado por nuestra empresa y su exposición y riesgo?

- ¿Hemos mirado nuestra exposición desde el exterior?
- ¿Nos hemos comparado con compañías similares?
- ¿Sabemos valorizar el riesgo?
- ¿Nos hemos cubierto con seguros específicos de ciber-riesgo?



Valorizamos nuestros análisis de seguridad

Veamos el riesgo, midámonos y obtengamos un rating que nos proporcione datos a nosotros y datos a terceros para posicionarnos en mejores condiciones para; pólizas, contratos, compliance, normas, etc ...

BITSIGHT

SECURITY RATINGS



Download your Security Ratings report



Download ratings data

BITSIGHT SECURITY RATING

700

COMPARE

Our ratings measure a company's relative security effectiveness.

ADVANCED

900-740

INTERMEDIATE

740-640

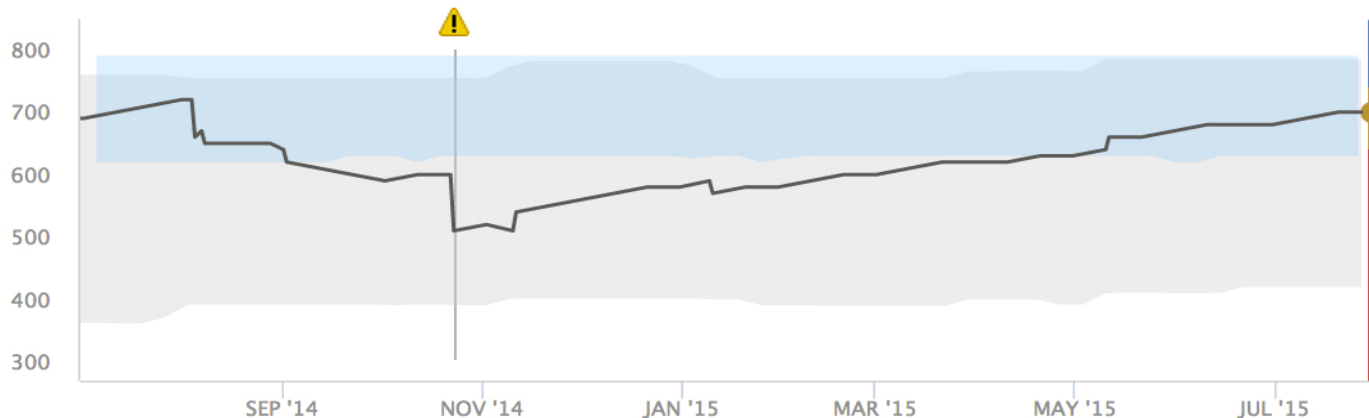
BASIC

640-250

LAST 12 MONTHS

Portfolio Range

Finance Industry Range



y si no ... ¿nos abandonamos en manos de la suerte?



y si no ... cubrámonos

Hay tres cosas que uno SIEMPRE tiene que tener a mano:

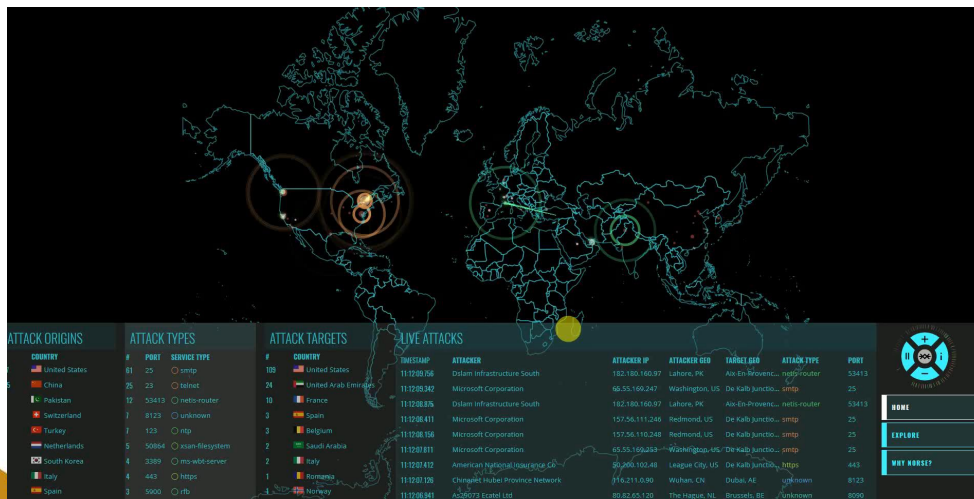
- Un buen amigo médico
- Un buen amigo abogado
- Un **BUEN SEGURO**

RISKMEDI 



... y nosotros insistimos | Gobernanza de servicios

El éxito de las medidas de seguridad IT integradas en nuestras infraestructuras, dependen de la **inteligencia de amenazas y la sincronía de la detección y respuesta**, y ésta a su vez genera las capacidades de: **conocer, comprender y perfilar a los atacantes** de manera que podamos anticipar y detectar nuevos impactos que escapan a nuestras soluciones defensivas. Tener **visibilidad y sincronía en los ámbitos de detección y gestión**, nos da las capacidades de actuar de modo temprano.



Según Gartner, la **inteligencia de amenazas** es el **“conocimiento basado en la evidencia, incluyendo información de contexto, las implicaciones, y demás variables que giran en torno a una amenaza, peligro existente o emergente sobre los activos, y que se puede utilizar para la toma de decisiones”**.

MSSP | SOC (Centro de Operaciones de Seguridad)

- > Te ayuda a **conocer las amenazas externas e internas** a las que te expones.
- > **Monitoriza** eventos e incidencias de seguridad
- > Almacena eventos de seguridad como **evidencias para un posible forense**, proceso judicial, etc.
- > **Previene posibles amenazas en el futuro** a través de la aplicación de las medidas **correctivas** correspondientes.
- > **Genera mayor visibilidad sobre incidentes** de seguridad externos que pueden impactar en tus infraestructura.
- > Evidencia la “**preocupación**” por el control de la **seguridad** de cara a normativa (GDPR, etc...)



Imagen de nuestro SOC (Madrid)



Garantía de Calidad | OneseQ



ISO 14001

¿Qué valor aportamos desde el SOC de OneseQ?

- > El servicio de nuestro SOC se basa en **tecnologías que ayudan a gestionar grandes cantidades de datos** e interpretarlos como eventos o incidentes de seguridad
- > Es operado por **personal muy cualificado** en servicios de ciberseguridad
- > **Múltiples SOC**s en distintas zonas geográficas (**implantación internacional**)
- > Nuestros SOC's además operan y **colaboran compartiendo información con otros SOC**s
- > Al ser operadores virtuales de comunicaciones, OneseQ posee un **NOC (Network Operation Center)** con una experiencia de más de **20 años**
- > Operado con tecnología **multi-SIEM y macro-correlación sobre tecnología cloud** que se ofrece en modo SaaS y tarifado por EPS (Eventos Por Segundo)
- > Tenemos las **máximas acreditaciones** en buenas prácticas y seguridad IT



ISO 27018



ISO 27001



ISO 22301



ISO 20001



ISO 9001



CMMI (N3)



ENS



BITSIGHT

RISKMEDI

Una red de conocimiento | generación de VALOR



RED de SOC



SOC Propios y socios

Madrid

Brasil

Santa Cruz de Tenerife



SOC Colaboradores

Barcelona

Chile

Casa Blanca (Marruecos)

Dubai (Emiratos Árabes)

Riyadh (Arabia Saudí)





OneseQ
by alhambra

BITSIGHT

RISKMEDIA

www.oneseq.es | www.bitsight.com | www.riskcyber360.com