



enigmedia

Introducción a la Ciberseguridad Industrial

Gerard Vidal, PhD
CSO

www.enigmediasecurity.com



Agenda

Conocimientos requeridos: ninguno específico de ciberseguridad

Para quién: instaladores, integradores, usuarios finales

1. Por qué es importante la ciberseguridad
2. Particularidades del entorno industrial
 - a. Diferencias entre IT y OT
 - b. Amenazas
3. Qué podemos hacer?
 - a. Buenas prácticas
 - b. La norma IEC-62443
4. Cómo generar negocio?
 - a. Diferenciación
 - b. Inventariado
5. Q&A



POR QUÉ LA
CIBERSEGURIDAD ES
IMPORTANTE?



Retrospectiva



El principal reclamo comercial son las nuevas funcionalidades



Situación actual

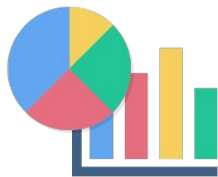


La normativa exige
unas medidas de
ciber-seguridad
en función del nivel
de riesgo



Importancia a nivel de cada empresa

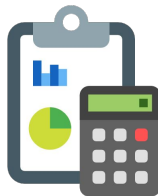
La información gobierna todos los aspectos de la empresa



Ventas



Operaciones



Contabilidad



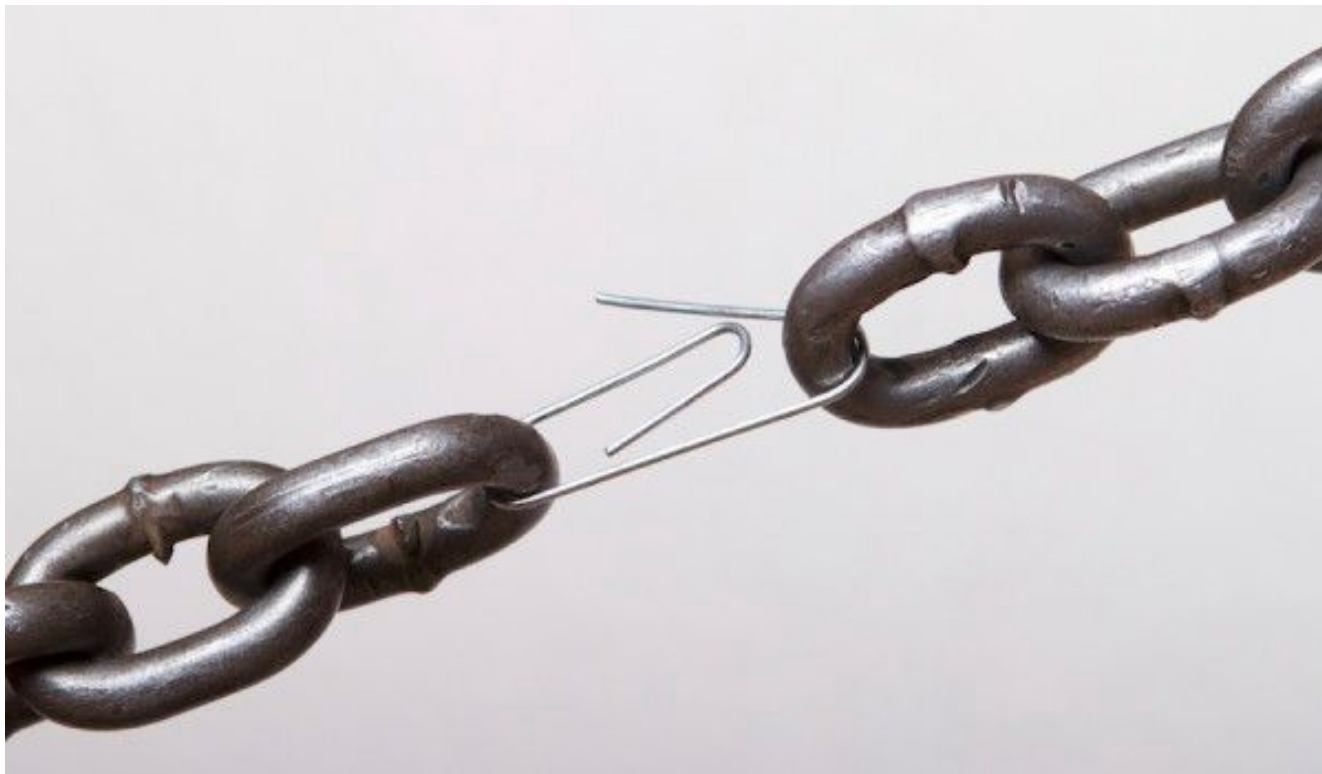
Personal



Compras



Importancia a nivel de cadena de suministro

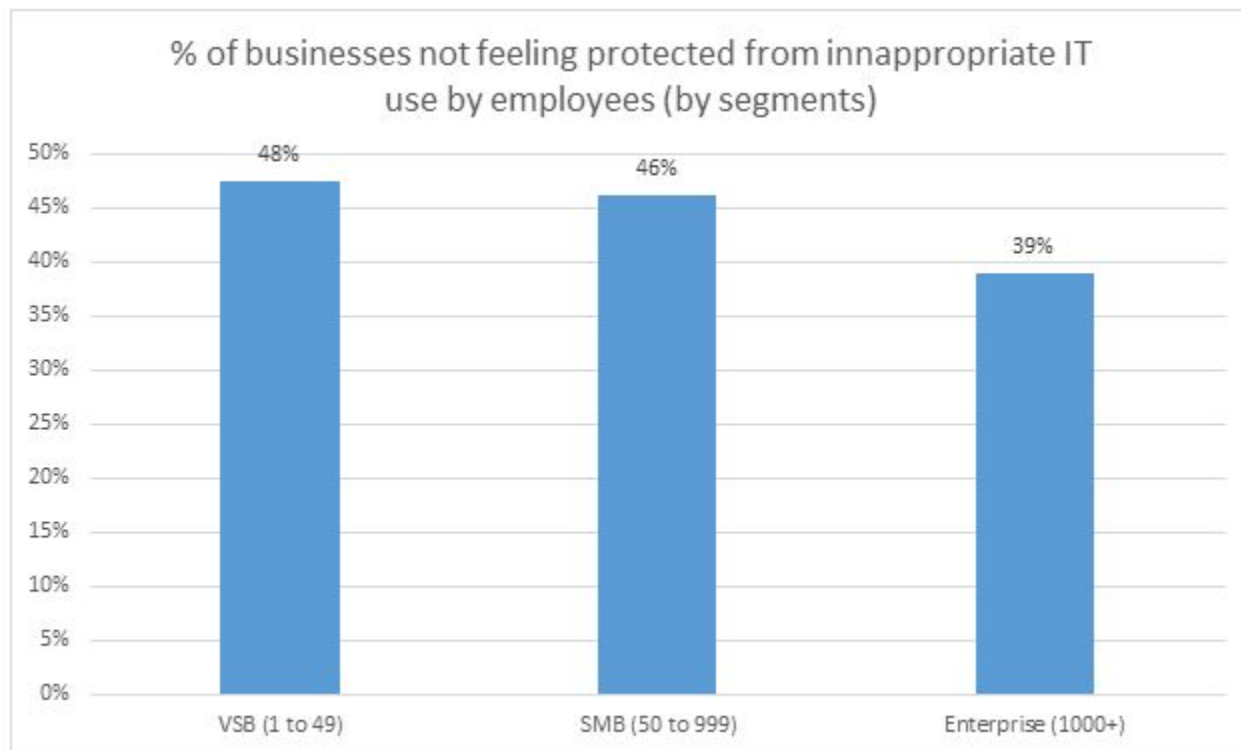


La fuerza de una cadena se mide por el eslabón más débil.

Por eso la regulación acaba afectando a todos.



Importancia a nivel individual



Source: IT Security Risks Survey 2017, global data

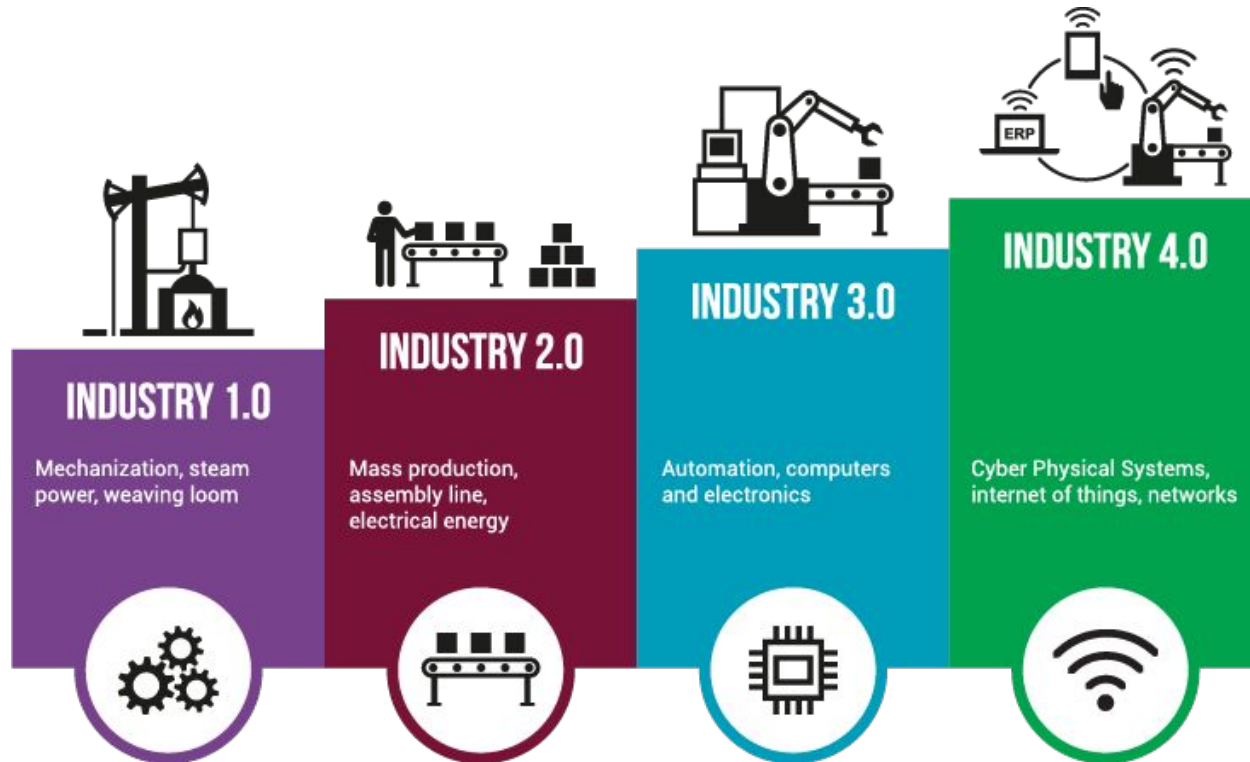
El ser humano
suele ser el
eslabón más
débil.



CIBERSEGURIDAD INDUSTRIAL

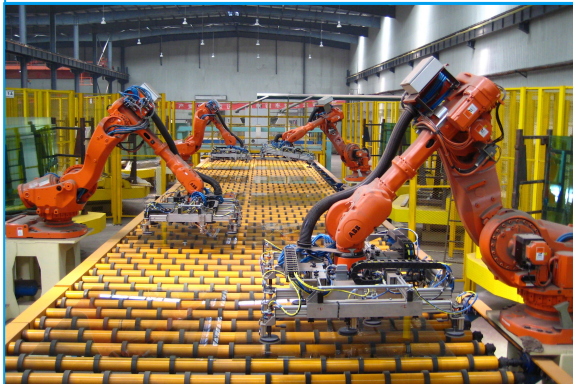


Cuál es el problema?



Incremento de ciberataques con consecuencias en sistemas físicos

Sistemas Industriales (OT):
Protección de los medios y
recursos productivos



Vida media de los equipos de
más de 20 años.
Difícil de actualizar.

Los conceptos
de seguridad IT
no se aplican
directamente
al mundo OT

Oficina e Informática (IT):
Protección de los equipos y
servicios IT.



Vida media de 3 - 5 años.
Fácil de actualizar.

Seguridad IT vs Seguridad OT

Seguridad IT

CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

Vida media de 3 - 5 años.
Fácil de actualizar.

La información sobre amenazas y vulnerabilidades en IT es fácilmente accesible: firewalls, IDS, IPS,..

+

PRIORIDAD

-



Seguridad OT

CONTROL

DISPONIBILIDAD

INTEGRIDAD

CONFIDENCIALIDAD

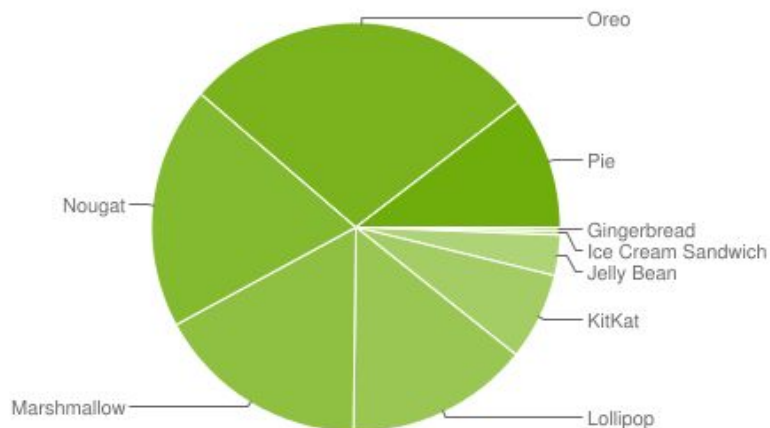
Vida media de los equipos de más de 20 años.
Difícil de actualizar

Las soluciones para IT, no funcionarán en OT

A lioness is shown in profile, running towards a herd of buffalo. The buffalo are running away from the lioness, kicking up a cloud of dust. The scene is set in a dry, open savanna with sparse vegetation. A small bird is visible in the upper left corner of the frame.

**BONUS TRACK:
LEGACY**

Sistemas desactualizados: una fuente de problemas



*Datos recopilados durante un período de 7 días hasta el May 7, 2019.
No se muestran versiones con una distribución inferior al 0.1%.*

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0		26	12.9%
8.1	Oreo	27	15.4%
9		28	10.4%

<https://developer.android.com/about/dashboards/>



Una parada inesperada puede llegar a costar 2M €

AMENAZAS	RIESGOS
• Diseño y segmentación de red inadecuado • Errores en la conexión de dispositivos • Dispositivos industriales inseguros • Escalado de ataques desde la red IT • Malware industrial (industroyer, petya, etc.)	• Paradas de líneas de producción • Reducción de la productividad • Avería de equipos • Accidentes • Espionaje de competidores • Fugas de información (know-how)



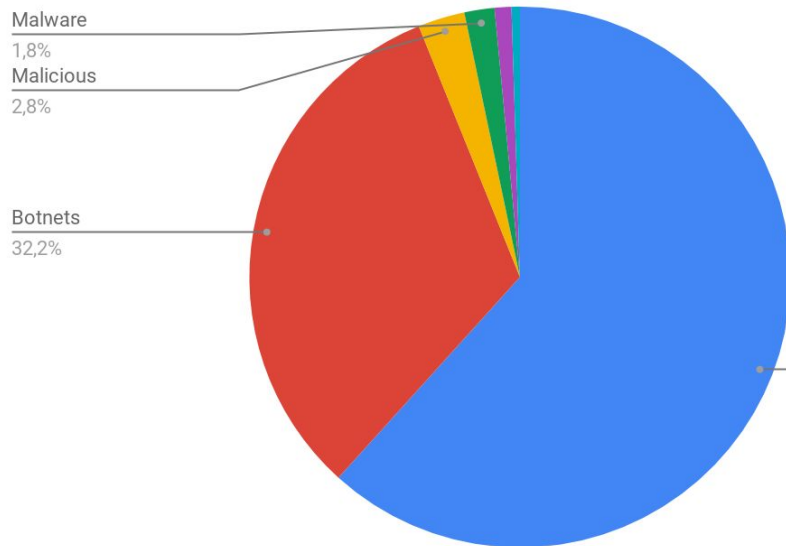
Un fallo típico puede costar unos

20.000 € por minuto

al cliente.

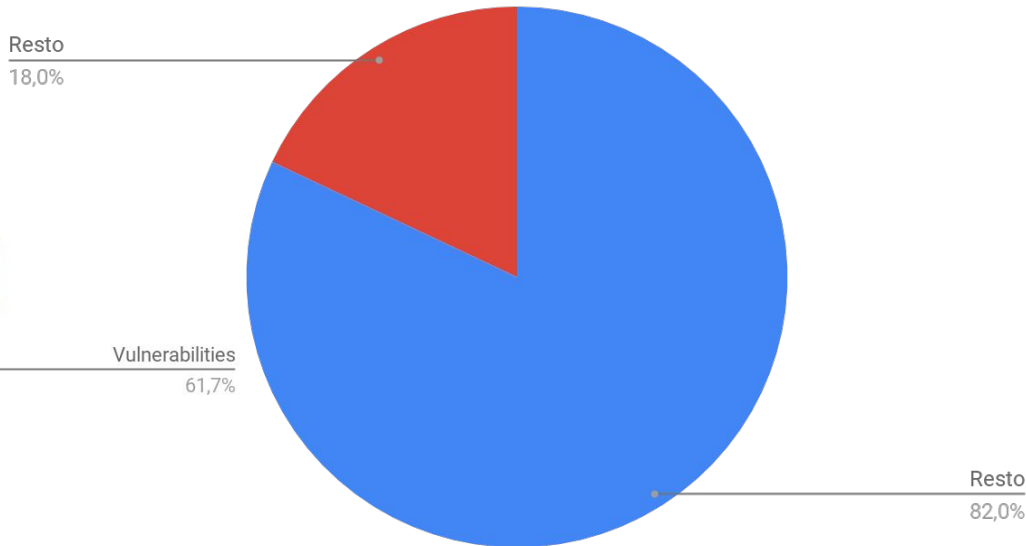
Esto es de verdad? Cómo de grande es el problema?

Incident classification



Datos de INCIBE

ICS comprometidos a Feb 2020



Datos de Kaspersky



AMENAZAS





Crash Override, el malware que puede dejar sin electricidad a ciudades enteras



junio 15 15:35
2017

por Fernanda Ortiz
0 comentarios

Bloomberg

Merck Cyberattack's \$1.3 Billion Question: Was It an Act of War?

In a world where a keyboard can cause more harm than a gunship, a legal dispute between the drug giant and its insurers could determine who pays for cyber damage.

By **David Voreacos**, **Katherine Chiglinsky**, and **Riley Griffin**

3 de diciembre de 2019 6:01 CET Updated on 3 de diciembre de 2019 23:03 CET

From **Bloomberg Markets**





Hacking

The Norsk Hydro cyber attack is about money, not war

Aluminium maker shows the importance of manual overrides as a way to cope when hackers cripple your systems



By **KELLY FIVEASH**

Thursday 21 March 2019

It has been widely speculated – although not confirmed by Norsk Hydro – that the ransomware used in the highly targeted attack was a relatively new and difficult-to-detect strain, dubbed LockerGoga, which criminals use to quickly encrypt computer files, before demanding payment to unlock them.

Delincuentes con recursos y capacidades limitadas

De Centro de tratamiento de Denuncias Automatizadas
Asunto **Multa** 10:39
A [redacted] ★ Otras acciones ▾

Para: [redacted]

Asunto: Multa

Motivo de no entrega en el acto: medios de captación de imágenes.

Hecho denunciado: circular entre 71 y 80 KM/H, estando limitada la velocidad a 50 KM/H generica para la via. 77 Normativa aplicable: Reglamento General de Circulación APT. 50 APDO. 1 Clasificación jurídica: Grave. Puntos = 2.

Sanción propuesta: 300.00

Encuentre la foto en el archivo adjunto.

1 adjunto: Multa_N_Expediente_19-002-923.doc 211,2 KB Guardar ▾

Re:SAFTY CORONA VIRUS AWARENESS WHO



World Health Organization



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong

Specialist wuhan virus advisory

FAKE

El correo electrónico malicioso vinculado al coronavirus apareció por primera vez a principios de febrero. (Sophos)

Hack-cidentes



En ocasiones la gente se confía en el trabajo y asume riesgos innecesarios



Hack-cidentes



- 🔍 como recuperar
- 🔍 como recuperar **fotos del movil**
- 🔍 como recuperar **a tu ex**
- 🔍 como recuperar **contraseña gmail**
- 🔍 como recuperar **fotos borradas**
- 🔍 como recuperar **la voz**
- 🔍 como recuperar **una cuenta de instagram**
- 🔍 como recuperar **conversaciones whatsapp**
- 🔍 como recuperar **puntos**
- 🔍 como recuperar **archivos borrados**
- 🔍 como recuperar **videos borrados**

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

En ocasiones la gente se confía en el trabajo y asume riesgos innecesarios

Ejemplo ataque remoto a servicio Carga EV

Shodan

Developers Monitor View All...

SHODAN

circulife

Explore Downloads Reports Pricing Enterprise Access

My Account Upgrade

The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

1:24

Ejemplo ataque remoto a servicio Carga EV

circarlife country:"ES" -S x +

https://www.shodan.io/search?query=circarlife+country%3A"ES"&page=2

SHODAN

Exploits Maps Share Search Download Results Create Report

Explore Downloads Reports Pricing Enterprise Access

TOTAL RESULTS

83

TOP COUNTRIES



Spain 83

TOP CITIES

Barcelona	13
Sant Cugat Del Valles	5
Zaragoza	4
Calafell	3
Tarragona	2

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

225.red-213-97-51.staticip.rna-ide.net
Telefonica de Espana Static IP
Added on 2019-05-29 08:58:47 GMT
Spain, Barcelona

HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.2.4
Connection: keep-alive
Date: Wed, 29 May 2019 8:58:46 GMT
Content-Length: 0
Location: html/setup.html

7.red-63-40-114.staticip.rna-ide.net
Telefonica de Espana Static IP
Added on 2019-05-30 19:30:17 GMT
Spain, Madrid

HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.3.1
Connection: keep-alive
Date: Thu, 30 May 2019 19:28:31 GMT
Content-Length: 0
Location: html/setup.html

Ejemplo ataque remoto a servicio Carga EV

Data

City	Madrid
Country	Spain
Organization	Telefonica de Espana Static IP
ISP	Telefonica de Espana Static IP
Last Update	2019-06-01T06:39:04.167810
Hostnames	[REDACTED]
ASN	AS3352

Services

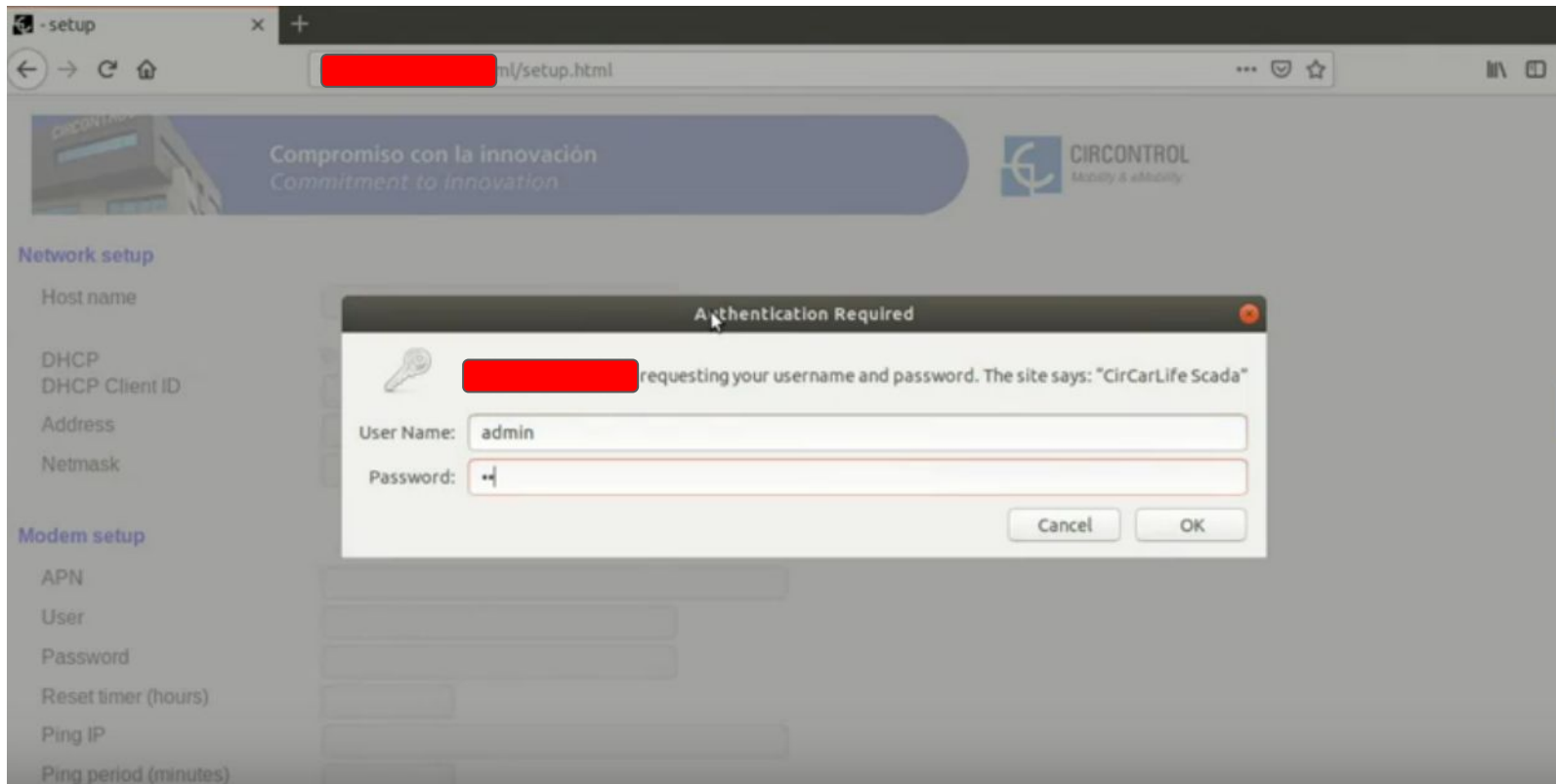


[REDACTED] Temporary Redirect
Server: CirCarLife Scada v4.3.1
Connection: keep-alive
Date: Thu, 30 May 2019 19:28:31 GMT
Content-Length: 0
Location: html/setup.html



[REDACTED] authorized
Content-type: text/html; charset=iso-8859-1
Accept-Ranges: bytes
Connection: close
WWW-Authenticate: Basic realm="GeneralUser/Administrator"

Ejemplo ataque remoto a servicio Carga EV



Ejemplo ataque dirigido - 1

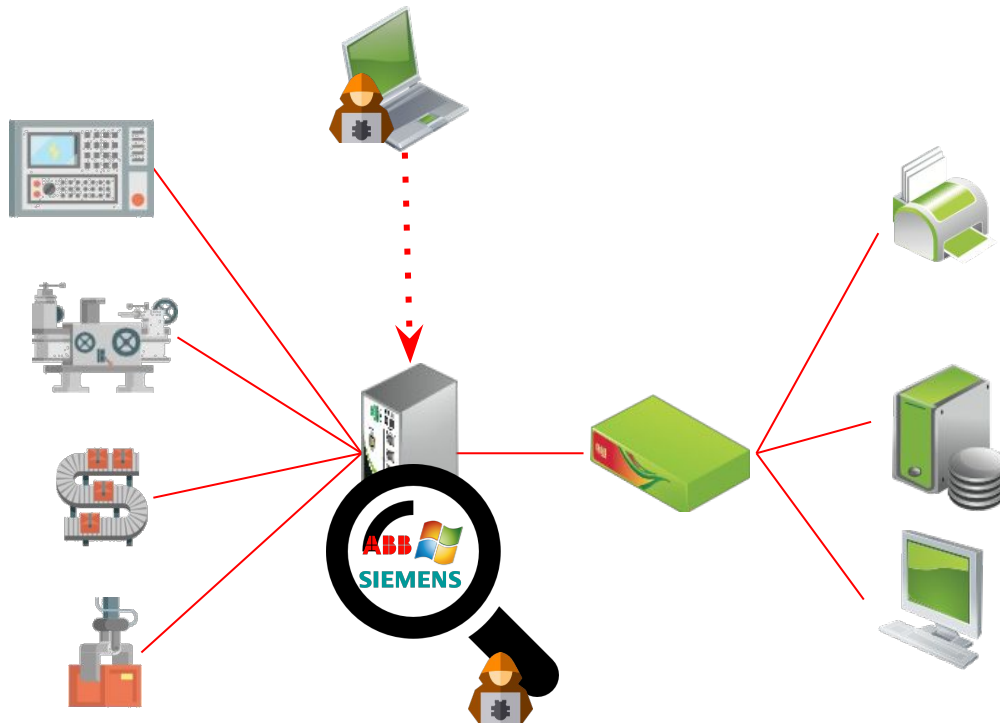


1

Maintenance contractor's laptop is infected



Ejemplo ataque dirigido - 1

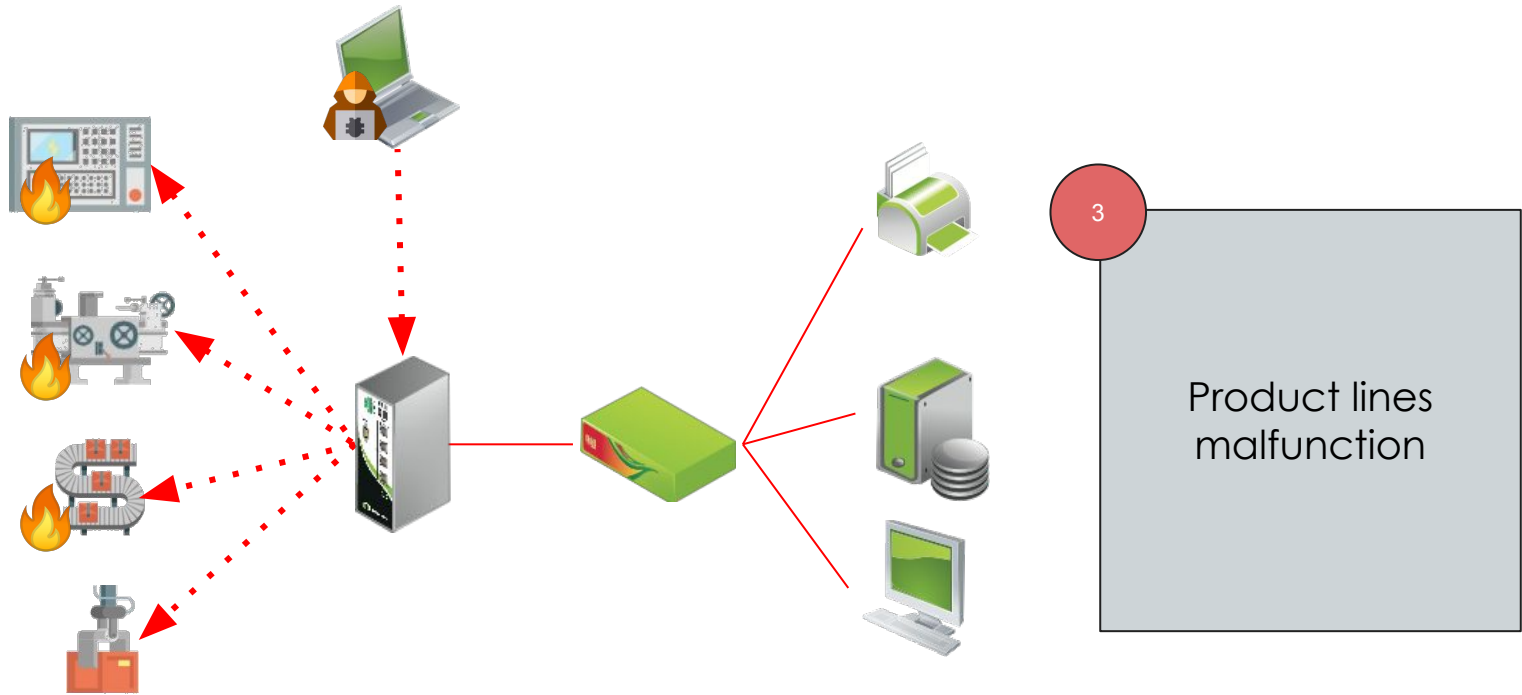


2

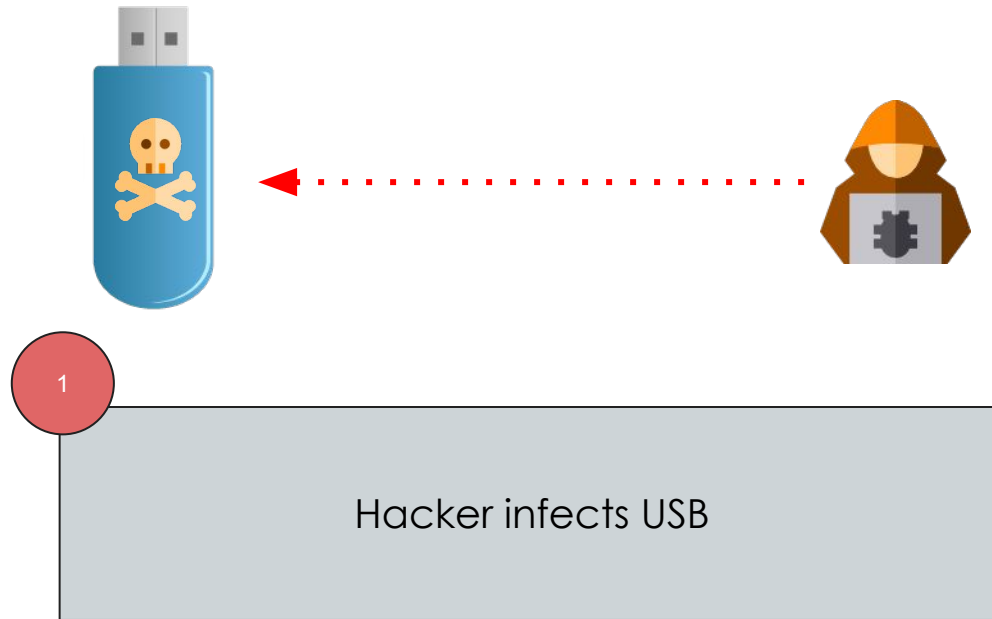
Attacker scans OT network to detect vulnerable devices



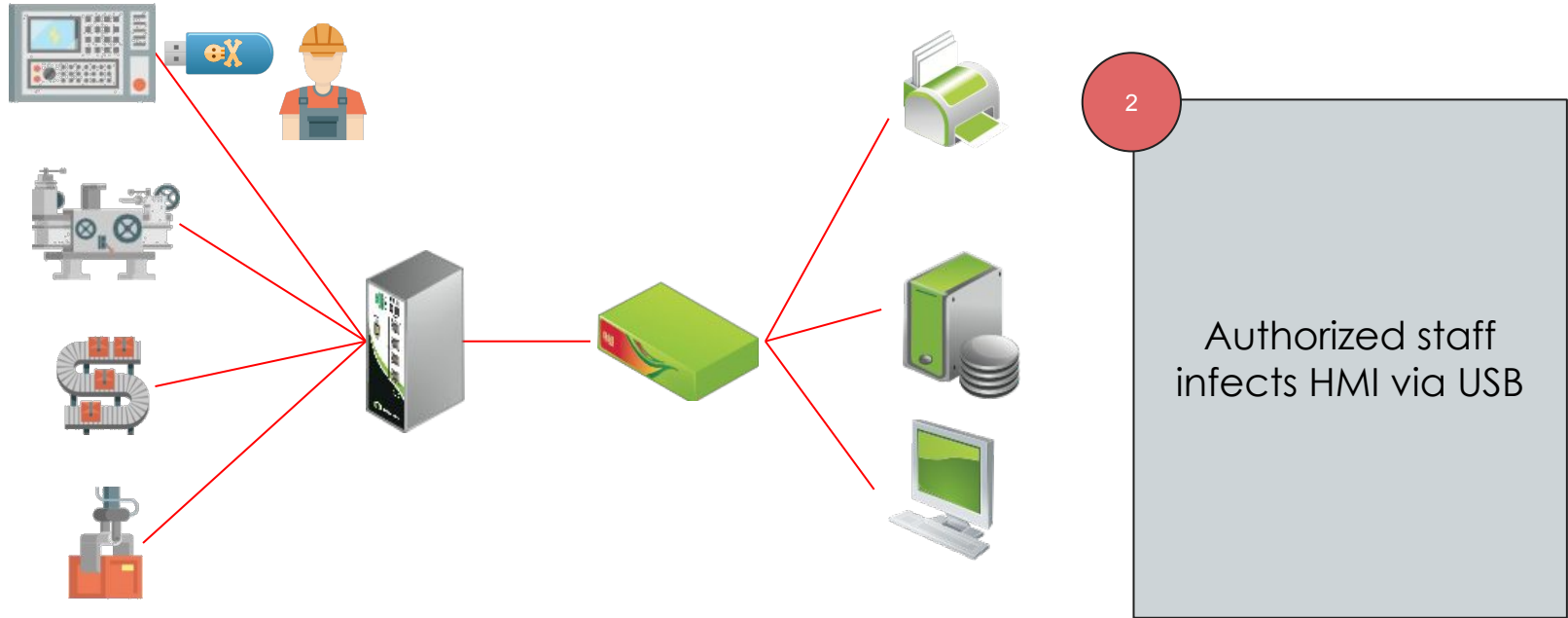
Ejemplo ataque dirigido - 1



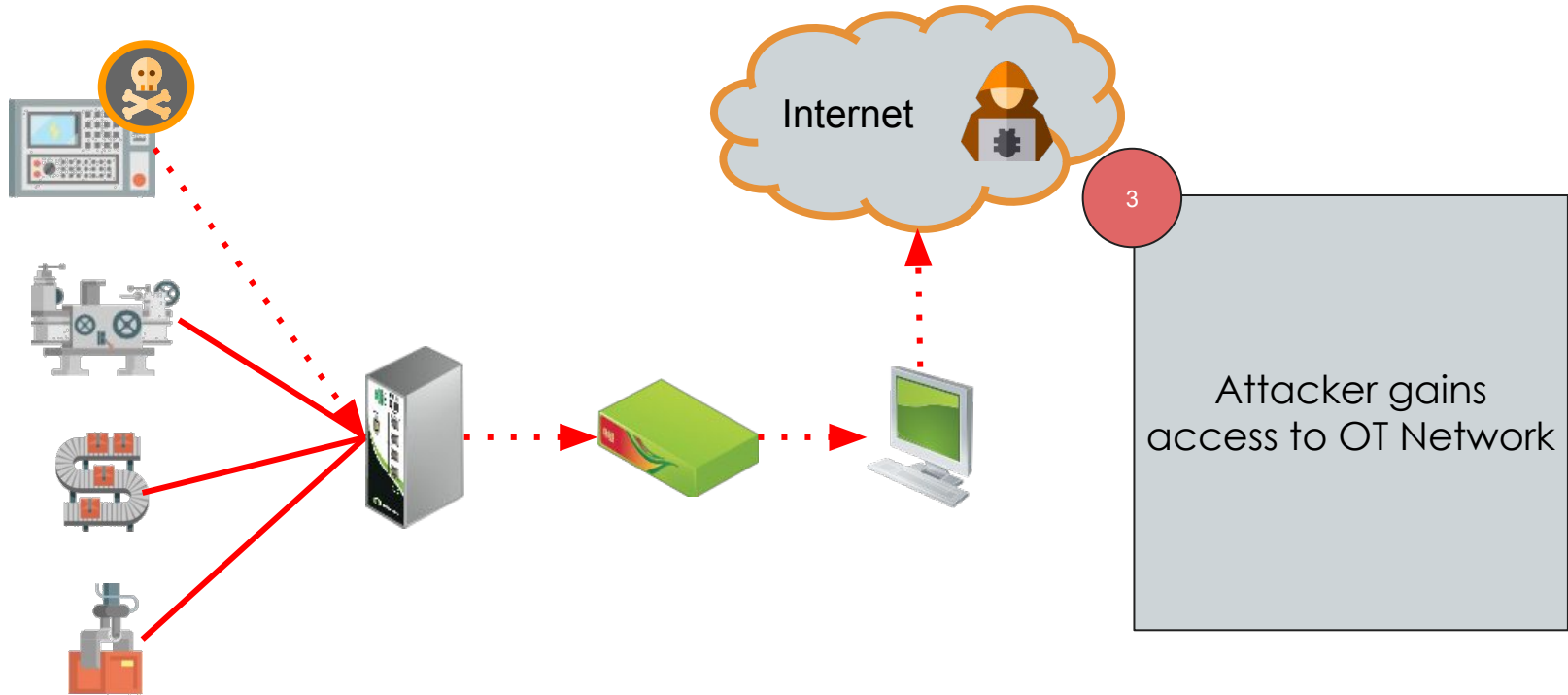
Ejemplo ataque dirigido - 2



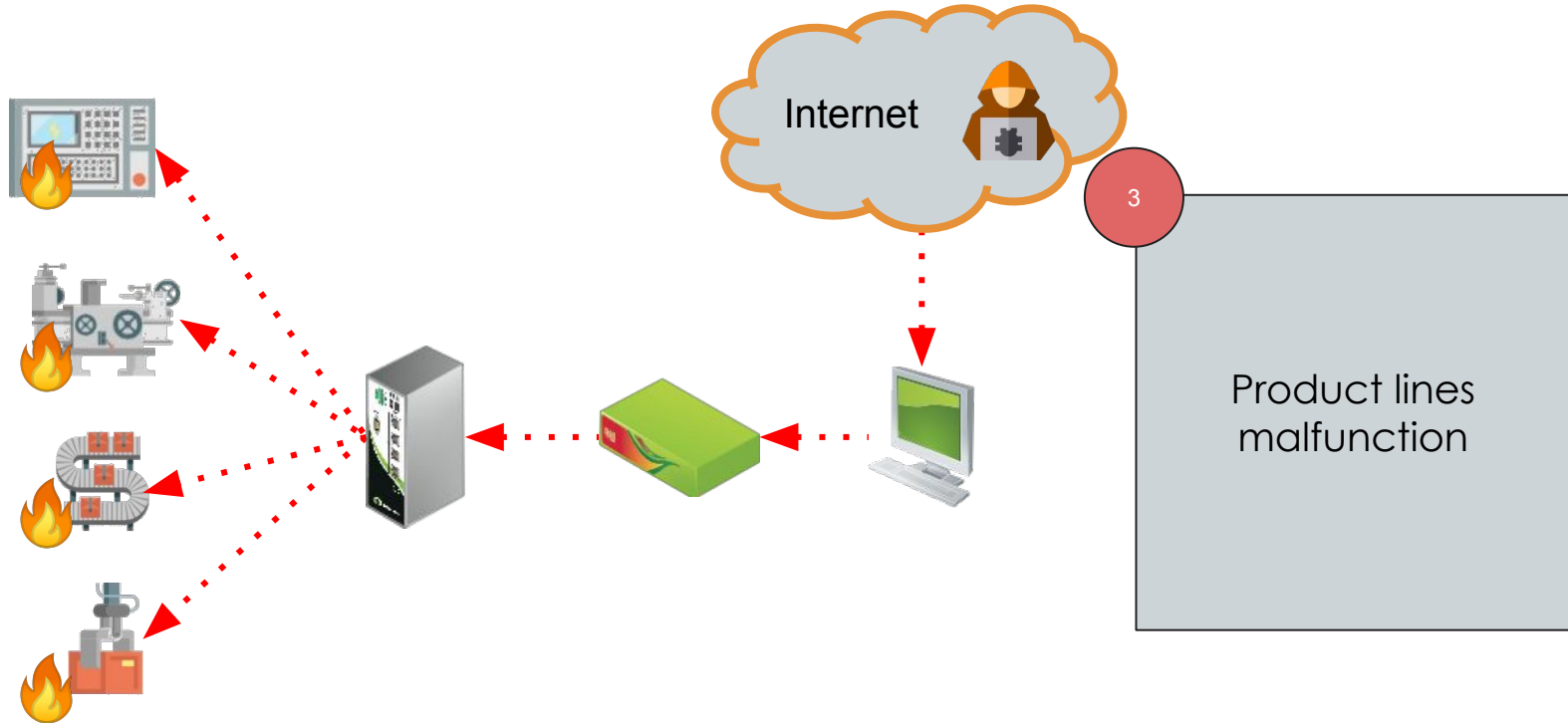
Ejemplo ataque dirigido - 2



Ejemplo ataque dirigido - 2



Ejemplo ataque dirigido - 2



QUÉ PODEMOS
HACER?



Seguir las buenas prácticas recomendadas



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Tu ayuda en ciberseguridad: 017

La Línea de Ayuda en ciberseguridad de INCIBE ya está disponible en el número 017. Un servicio gratuito y confidencial disponible los 365 días del año de 9:00 y 21:00
¡Si tienes dudas, llámanos!

Más info sobre el 017



Materiales - Línea de ayuda - Recursos gratuitos y para todo tipo de públicos

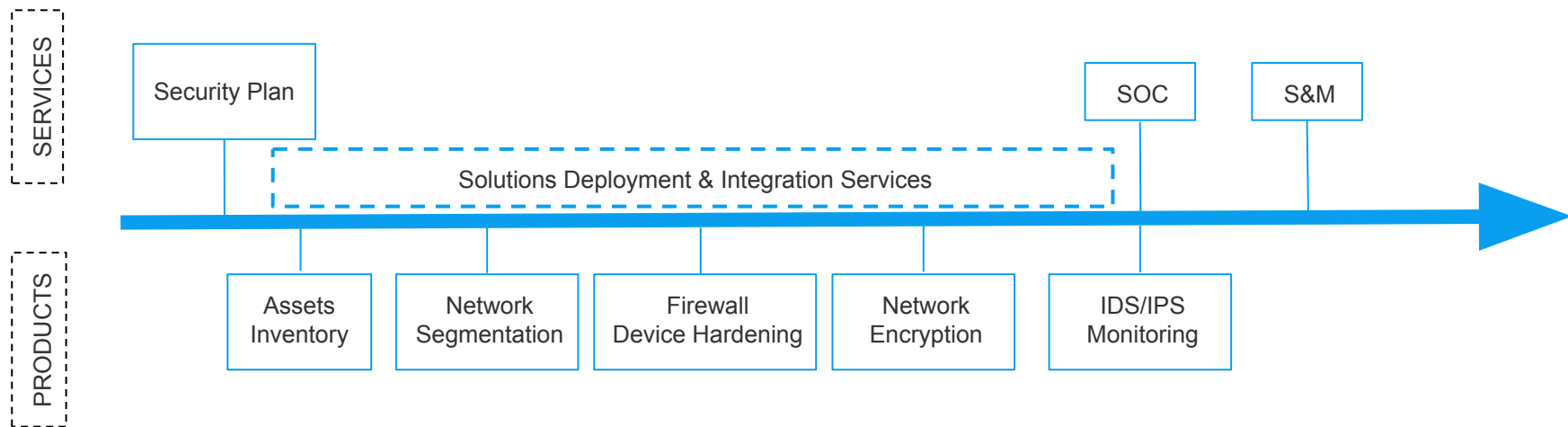


IEC 62443-3-3 y 62443-2-4

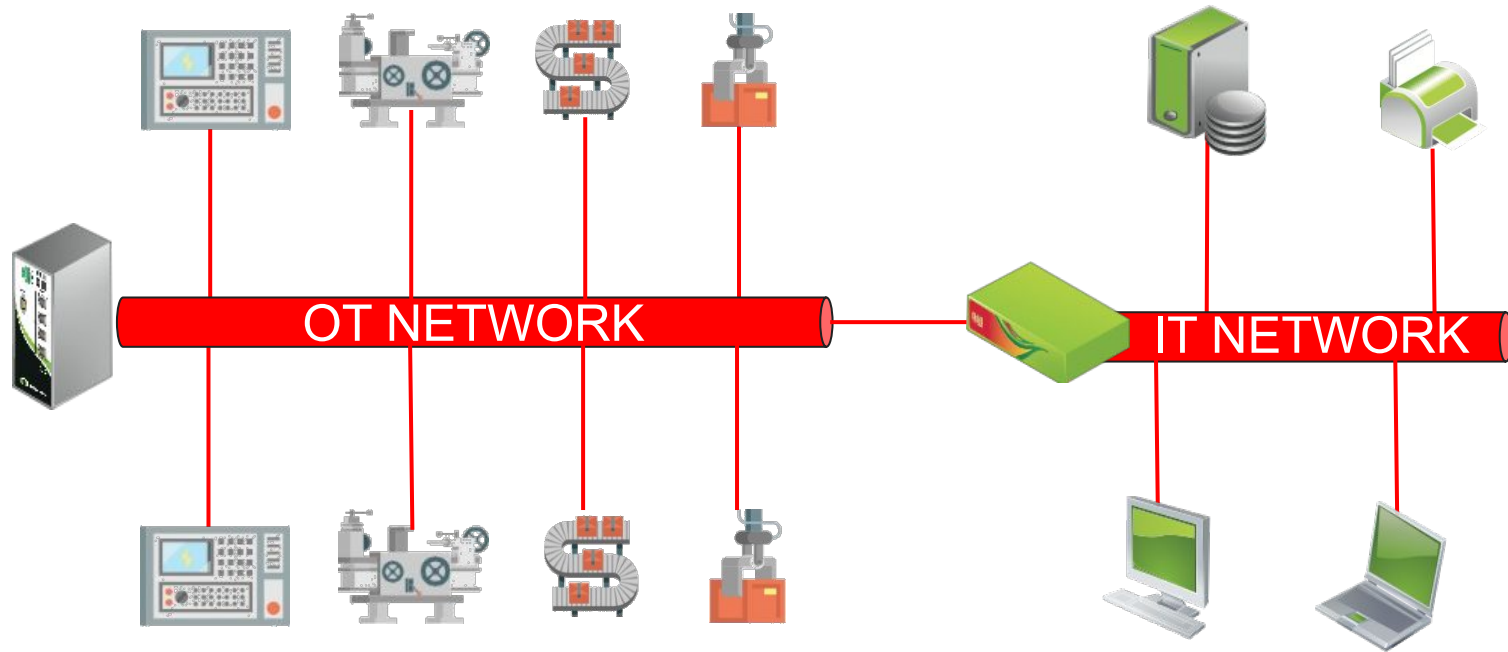
- 62443-2-4: orientada a proveedores de servicio
 - Define qué capacidades y requisitos son necesarios para los diversos grandes de riesgos o amenaza que debe afrontar un cliente
- 62443-3-3: orientada a la infraestructura
 - Qué debe de implementar un cliente final para que su red sea segura en función de los niveles de riesgo a los que está expuesta.
 - Hay 4 niveles de “amenaza”. El primero son “accidentes” y el último naciones-estado.



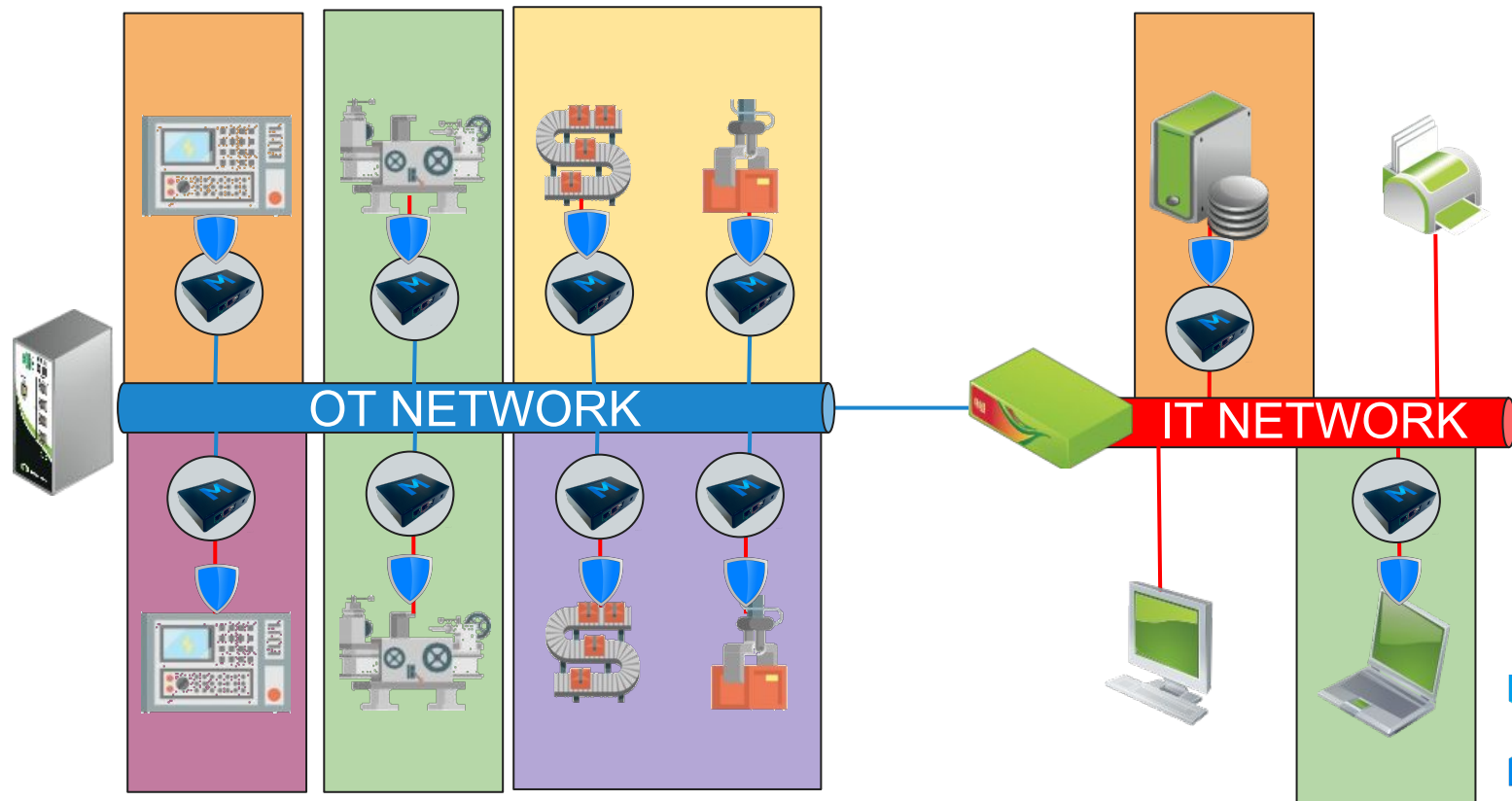
ICS Cybersecurity Customer Roadmap



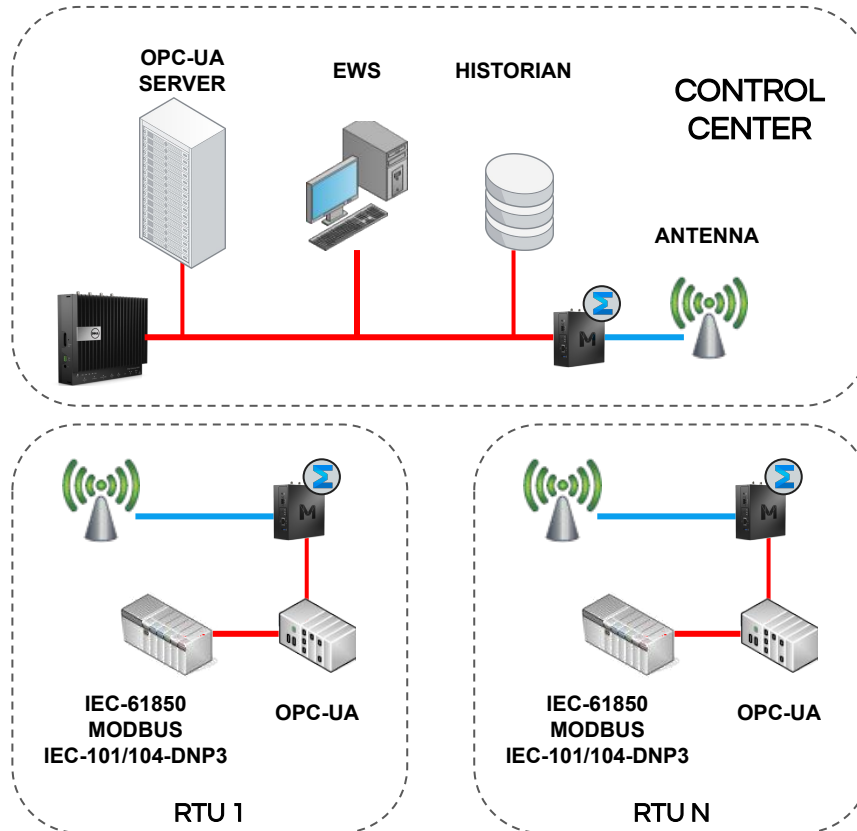
Escenario inicial: una red plana



Cumplimiento IEC-62443-3-3

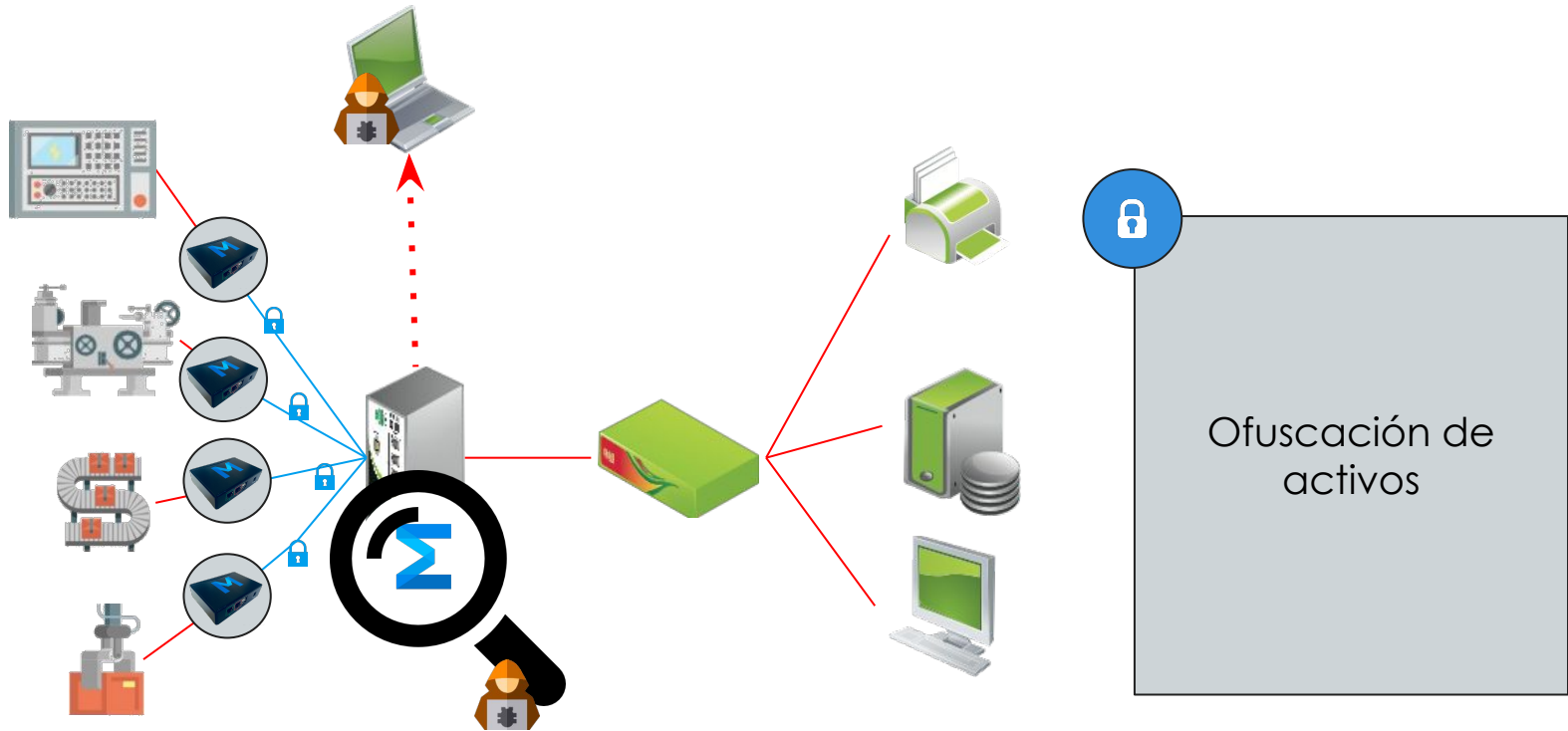


Ejemplo ataque dirigido - Ataque a acceso remoto

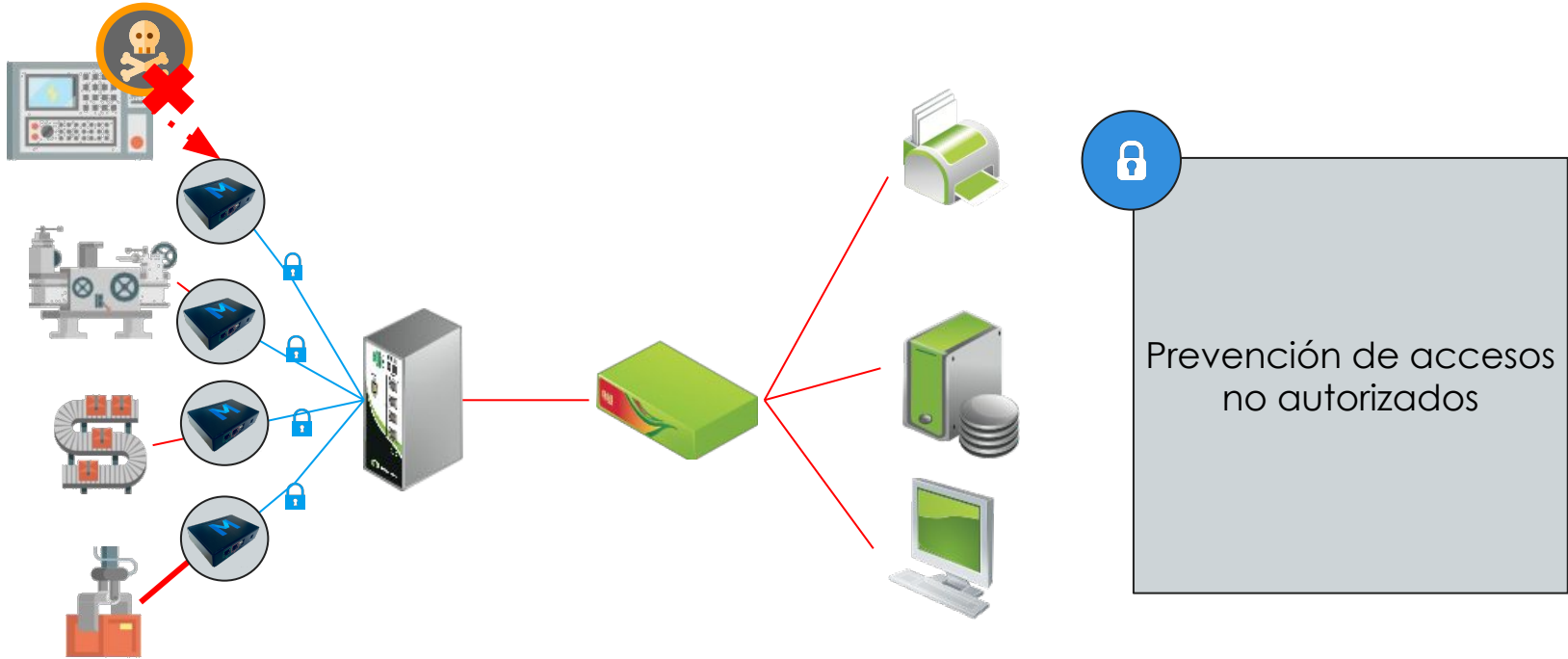


Autenticación y
cifrado de los
canales de
comunicación

Ejemplo ataque dirigido - Atacante con acceso a la red



Ejemplo ataque dirigido - USB



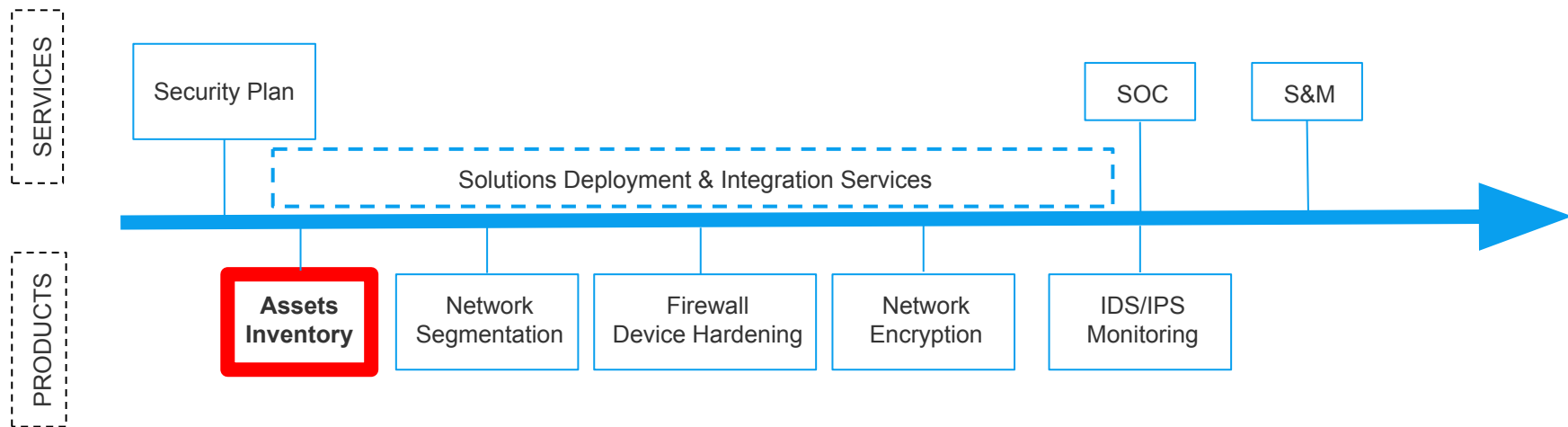
CÓMO PUEDO
GENERAR
NEGOCIO?



Diferenciación de la competencia

- El mercado es inmaduro y lleno de oportunidades
- Empieza a haber demanda en pliegos de ciberseguridad industrial
- Poder acreditar conocimientos en el campo se valora positivamente
- Tanto los fabricantes industriales como las empresas de ciberseguridad buscan alianzas

ICS Cybersecurity Customer Roadmap



Gestión de activos

- El primer paso de cualquier proyecto de ciber es conocer el número de equipos en la red y hacer un diagrama de red.
- Este proceso lo puede hacer el integrador.
- Existen múltiples herramientas disponibles.

