NUEVOS RETOS DE CIBERSEGURIDAD

23 de Octubre 2025 Barcelona

Sergio Martínez
Director de Iberia
Sonicwall

SONICWALL

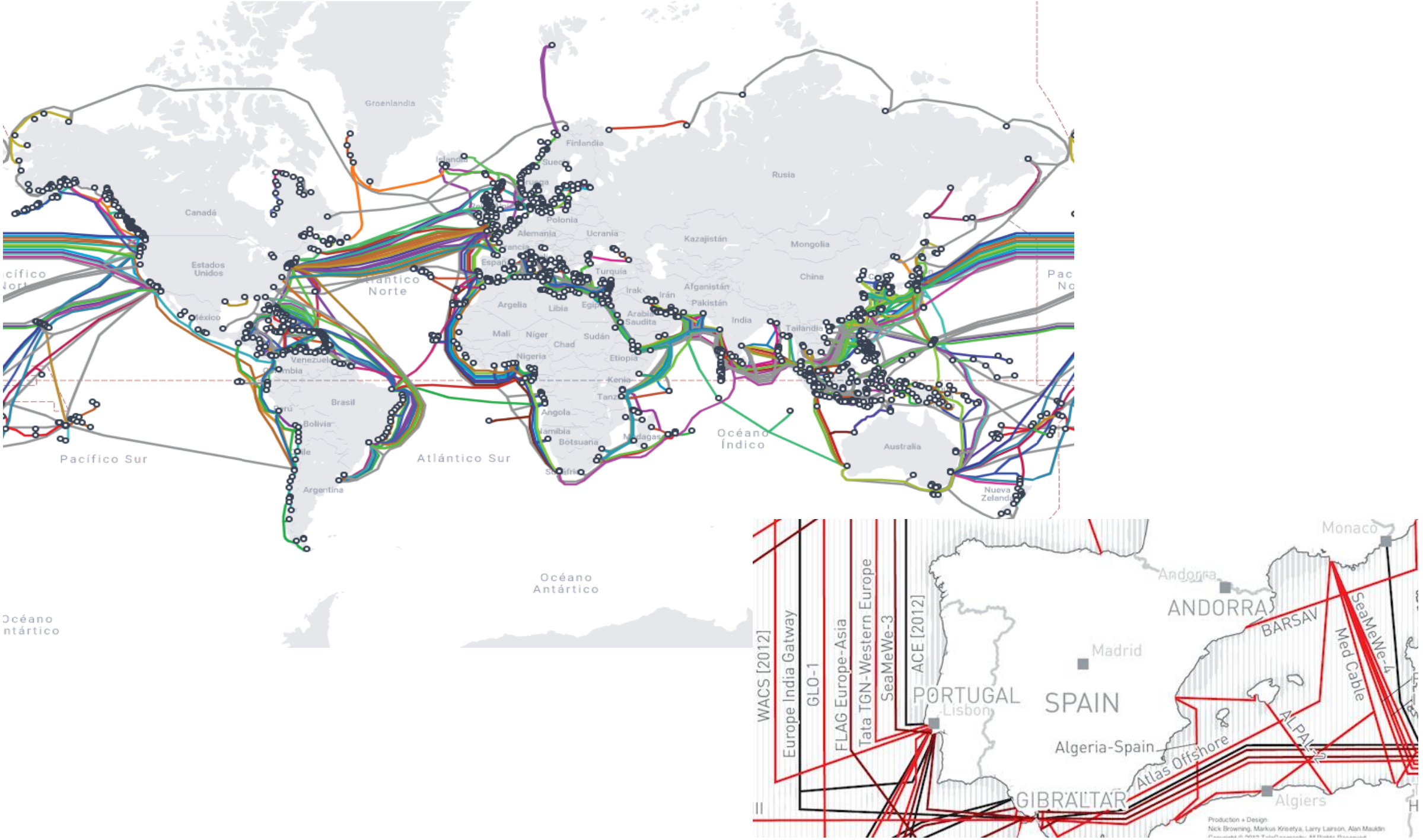
AGENDA

Nuevos retos de ciberseguridad

23th octubre. Barcelona

1. **Introducción a la Ciberseguridad**
2. **Estado de la ciberseguridad: tendencias**
3. **NIS2: Responsabilidad de los consejeros**
4. **Nuevas amenazas en el horizonte**
5. **Preguntas y respuestas**

¿INTERNET? ¿DÓNDE ESTÁ?


Groenlandia
Canadá
Estados Unidos
México
Venezuela
Brasil
Bolivia
Argentina
Pacífico Sur
Atlántico Sur
Océano Antártico
Océano Índico
Finlandia
Suecia
Polonia
Alemania
Ucrania
Rusia
Kazajistán
Mongolia
China
Turquía
Irak
Irán
Afganistán
Pakistán
India
Tailandia
Australia
Nueva Zelanda
Argelia
Libia
Egipto
Mali
Níger
Chad
Sudán
Nigeria
Etiopía
Kenia
Angola
Namibia
Botsuana
Madagascar
Monaco
Andorra
ANDORRA
BARSAV
SeaMeWe-4
Med Cable
Madrid
PORTUGAL
Lisbon
SPAIN
WACS [2012]
Europe India Gatway
GLO-1
FLAG Europe-Asia
Tata TGN-Western Europe
SeaMeWe-3
ACE [2012]
Algeria-Spain
Atlas Offshore
ALPAL-2
GIBRALTAR
Algiers
Production + Design
Nick Browning, Markus Kriselya, Larry Larson, Alan Mauldin

Internet es la obra de **ingeniería** más grande que ha construido nunca

Pero las **cosas** no son buenas ni malas, dependen de cómo las usa el ser humano

Por otro lado… Nunca hemos invertido tanto en **ciberseguridad**…

Pero… **Todo va a peor**.

¿Por qué?

1

TODO SOFTWARE CONTIENE BUGS

- La impaciencia genera más bugs de los deseados.
- Algunos de ellos son vulnerabilidades explotables.
- Muchos no se detectan (zero-day exploits).
- Parcheo infinito de sistemas y aplicaciones.
- Se necesita detección y respuesta en tiempo real.

2

TODO VA A SER SMART

- Smart: ordenadores en todas partes y más software.
- Multitud de nuevos dispositivos diseñados SIN seguridad, la facilidad de uso por delante.
- La seguridad está reñida muchas veces con la funcionalidad y el negocio.

3 TODO VA MUY RÁPIDO

- En 15 años ha cambiado el mundo. ¿Cómo será en 2034 todo?
- Coches autónomos, compartición de todo, sensorización, drones, todo en la nube, más redes sociales… Yo qué sé!
- La velocidad es enemiga de la seguridad: la tecnología va por capas…
- Rapidez acelera el efecto “bug”, la calidad del software es peor.

4

CIBERCRIMEN Y GOBIERNOS

- El lado oscuro del ser humano en marcha.
- agencias de inteligencia y los gobiernos entran en juego
- Guerra comercial entre diferentes países
- Armas cibernéticas
- IA en el lado atacante

5

RIESGOS CATASTRÓFICOS

- Desaparece el perímetro. ¿Qué y cómo tenemos que protegernos?
- Todo conectado: Coche, hogar, etc. y sensorizado -> Efectos inmediatos – Impacto enorme.
- EQUIFAX (150M), Collection #1 (773M direcciones correo únicas y 21M passwords)
- https://haveibeenpwned.com/
- Estado de la ciberseguridad en https://securitycenter.sonicwall.com

AGENDA

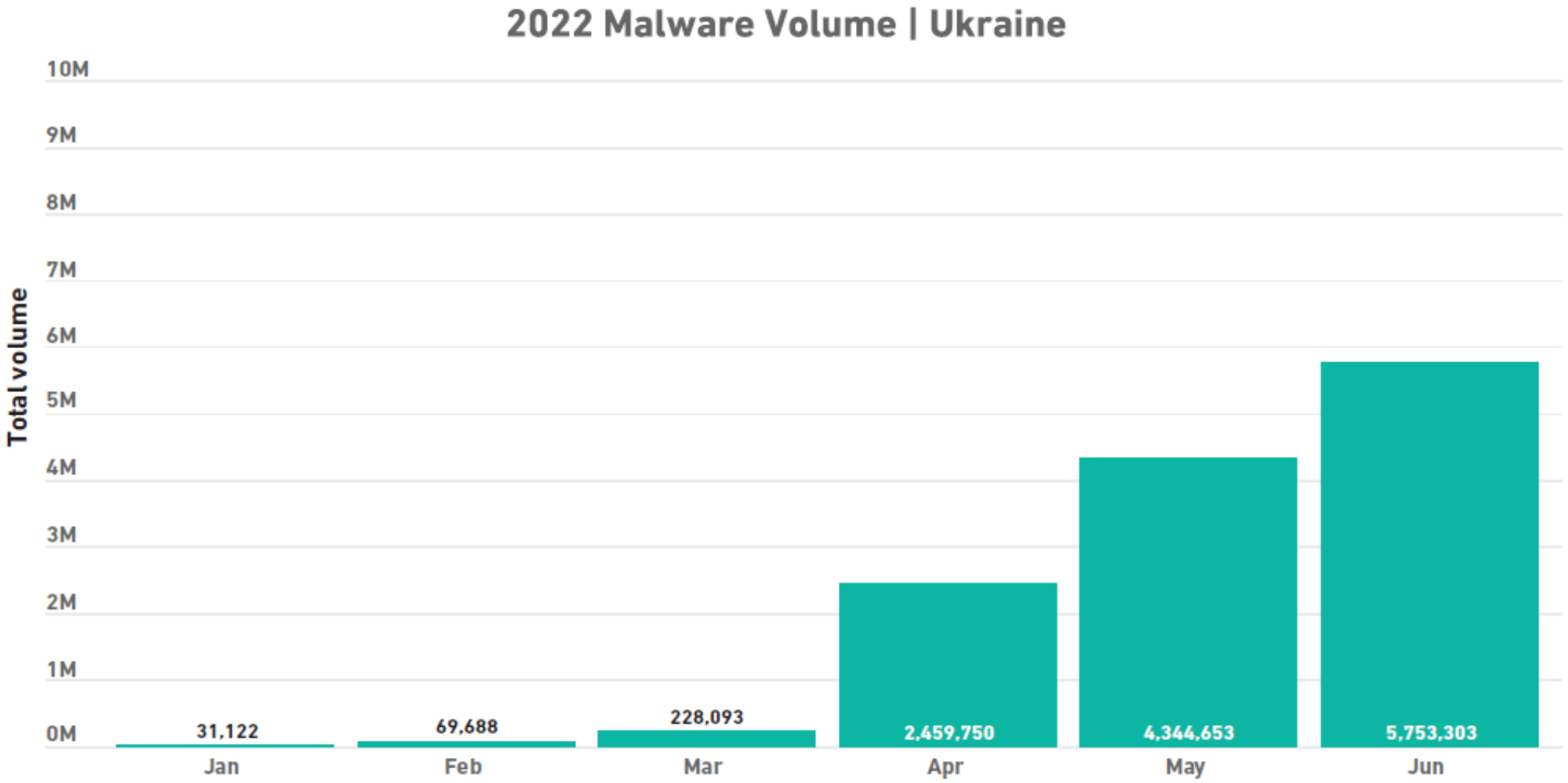
Nuevos retos de ciberseguridad

23th octubre. Barcelona

1. Introducción a la Ciberseguridad
2. Estado de la ciberseguridad: tendencias
3. NIS2: Responsabilidad de los consejeros
4. Nuevas amenazas en el horizonte
5. Preguntas y respuestas

Durante los últimos 12 meses, el 57% de todas las organizaciones de 100 a 5.000 usuarios sufrieron uno o más ciberataques — y cada ataque costó de media unos $5,34 millones

Y EN UCRANIA… X200. CIBERGUERRA!



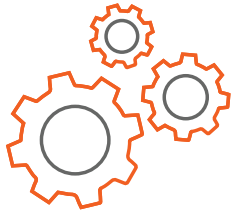
SONICWALL

CAMBIO DE PARADIGMA

Modelo “Bastión” a uno más parecido a un “Aeropuerto”

SONICWALL

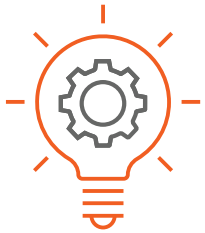
EL CAMPO DE BATALLA ESTÁ CAMBIANDO



Las redes son más **complejas**

Las amenazas crecen en volumen y **sofisticación**

Los empleados están distribuidos y **fuera del perímetro**



Los Partners **evolucionan** para proteger major a sus clientes

INFORME ANUAL DE CIBERSEGURIDAD

1.1m+
Global Sensors

215+
Countries & Territories

24x7x365
Monitoring

<24hrs
Threat Response

140k+
Malware Samples Collected Daily

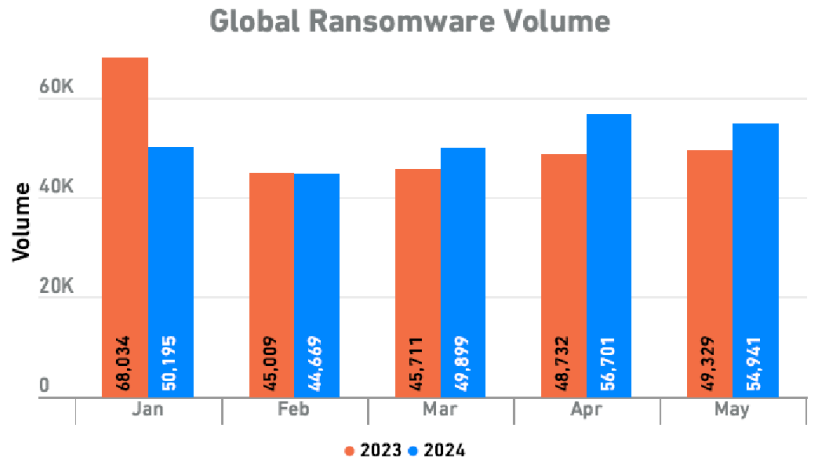
28m+
Malware Attacks Blocked Daily

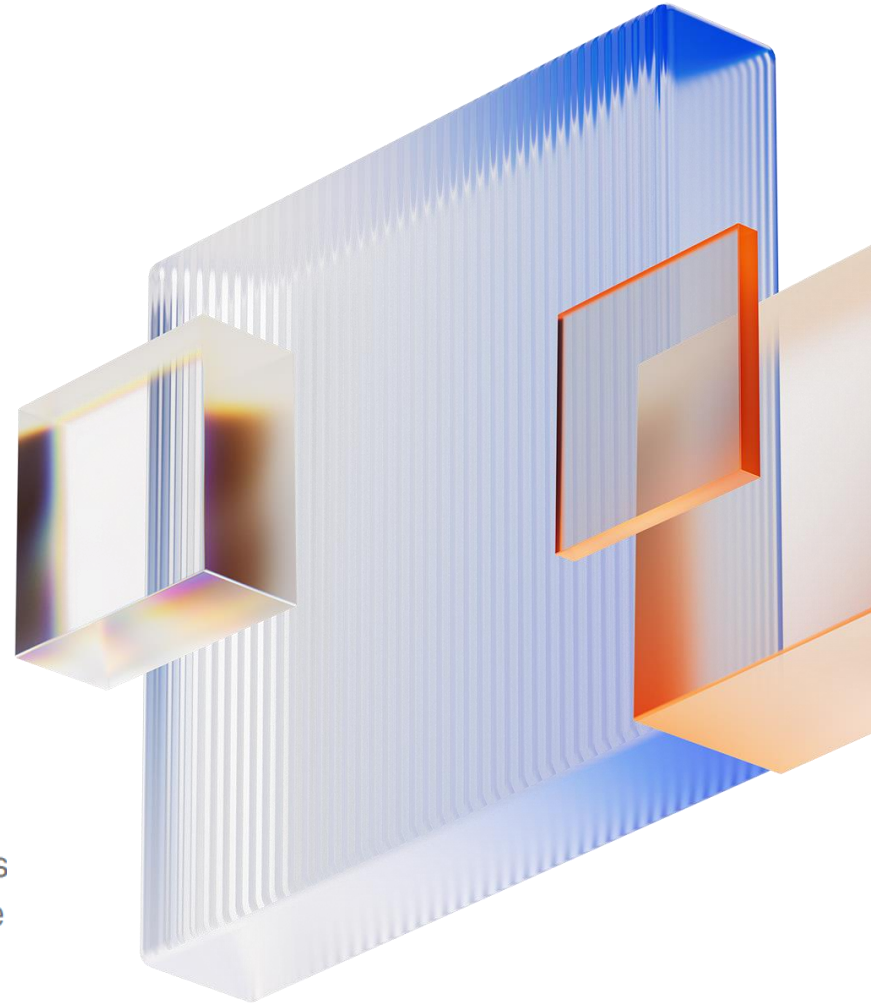
SONICWALL

LAS AMENAZAS CRECEN

RANSOMWARE

El ransomware va en aumento en las Américas (NOAM: 15 %, LATAM: 51 %). EMEA, sin embargo, está arrastrando las cifras globales a la baja, con un -49 % que sugiere que las medidas de ciberseguridad mejoradas y las intervenciones de las autoridades están teniendo un impacto positivo.





MALWARE

▲30 % El malware mostró una tendencia al alza desde marzo hasta mayo, con un enorme aumento del 92 % solo en mayo.

15 % El 15 % de todos los ataques de malware están utilizando el empaquetado de software como TTP MITRE.

LAS AMENAZAS CRECEN

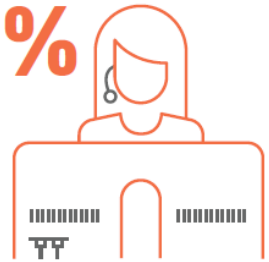
MALWARE DE IoT

Los dispositivos de IoT atacados han pasado un promedio de 52,8 horas bajo ataque.

▲107 %

SOC

83%



El ochenta y tres por ciento de las alertas recibidas por los clientes de nuestros servicios gestionados están relacionadas con aplicaciones en la nube y credenciales comprometidas.

AMENAZAS CIFRADAS

11001X
10XX11
001XX1
100X11
110X10

▲92 %

Las amenazas cifradas han ascendido un 92 %, lo cual pone de relieve la creciente sofisticación de los cibercriminales, así como el hecho de que siguen utilizando transferencias cifradas con TLS para entregar malware y otras amenazas a través de la red.

RTDMI™

526

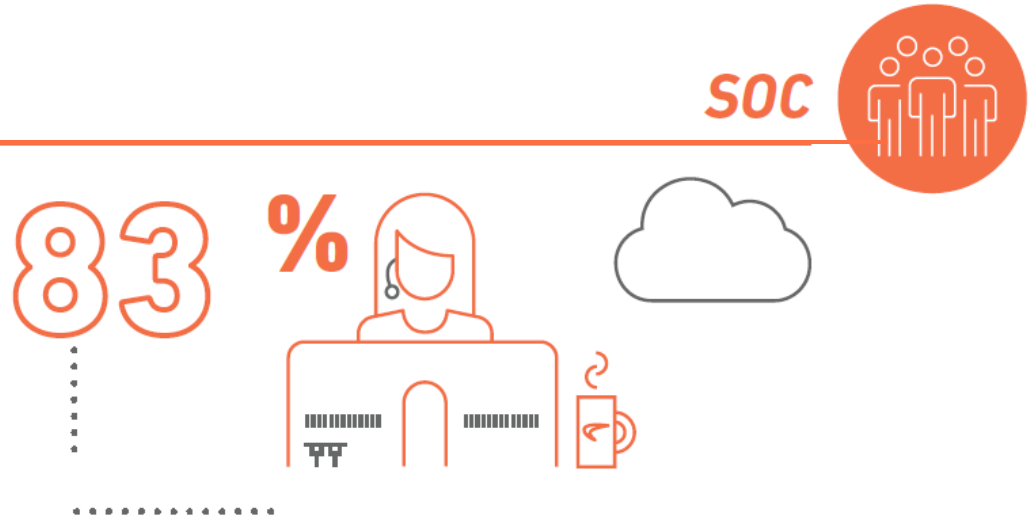
— NUEVAS VARIANTES —

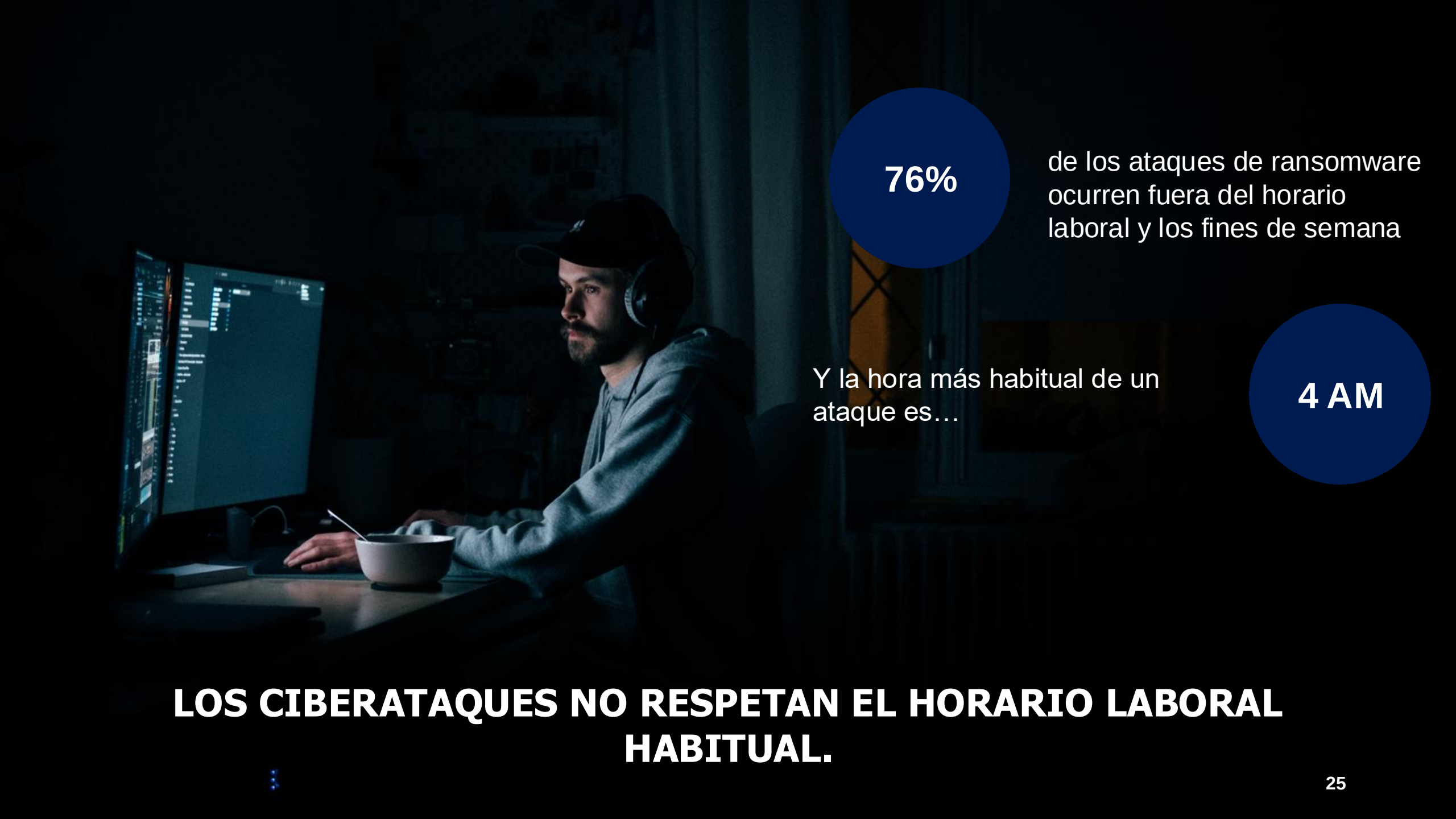
AL DÍA

SonicWall Capture Advanced Threat Protection (ATP) con Inspección de memoria profunda en tiempo real (RTDMI ™) ha registrado 78.923 nuevas variantes.

¿DÓNDE ESTÁ LA MAYORÍA DE LAS AMENAZAS?

El ochenta y tres por ciento de las alertas recibidas por los clientes de nuestros servicios gestionados están relacionadas con aplicaciones en la nube y credenciales comprometidas.





76%

de los ataques de ransomware ocurren fuera del horario laboral y los fines de semana

Y la hora más habitual de un ataque es…

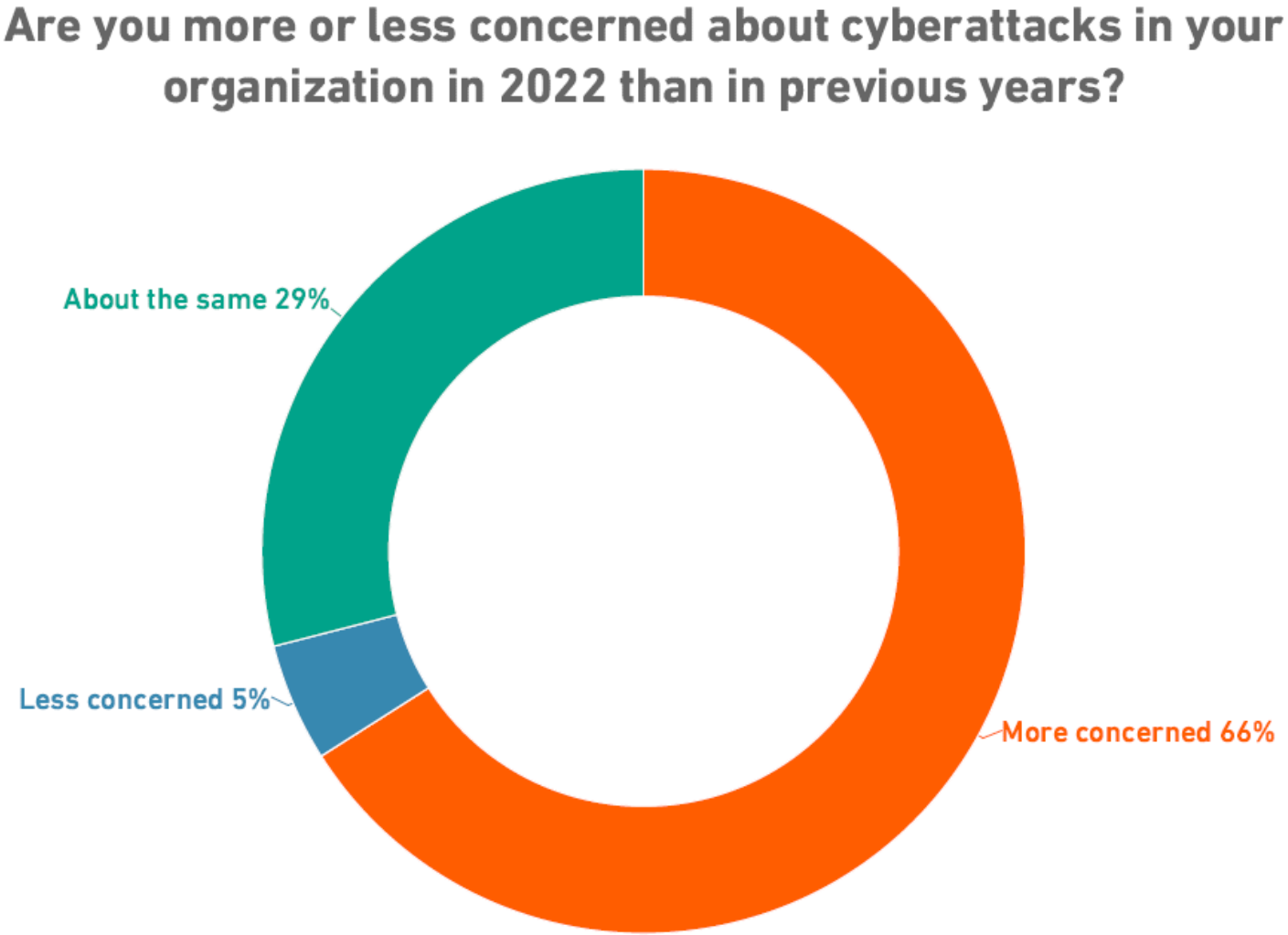
4 AM

LOS CIBERATAQUES NO RESPETAN EL HORARIO LABORAL HABITUAL.

TODO VA A PEOR… ¿QUÉ PIENSAN LOS CIOS?

66%

Todo va a peor… Y los CIOs así lo piensan…

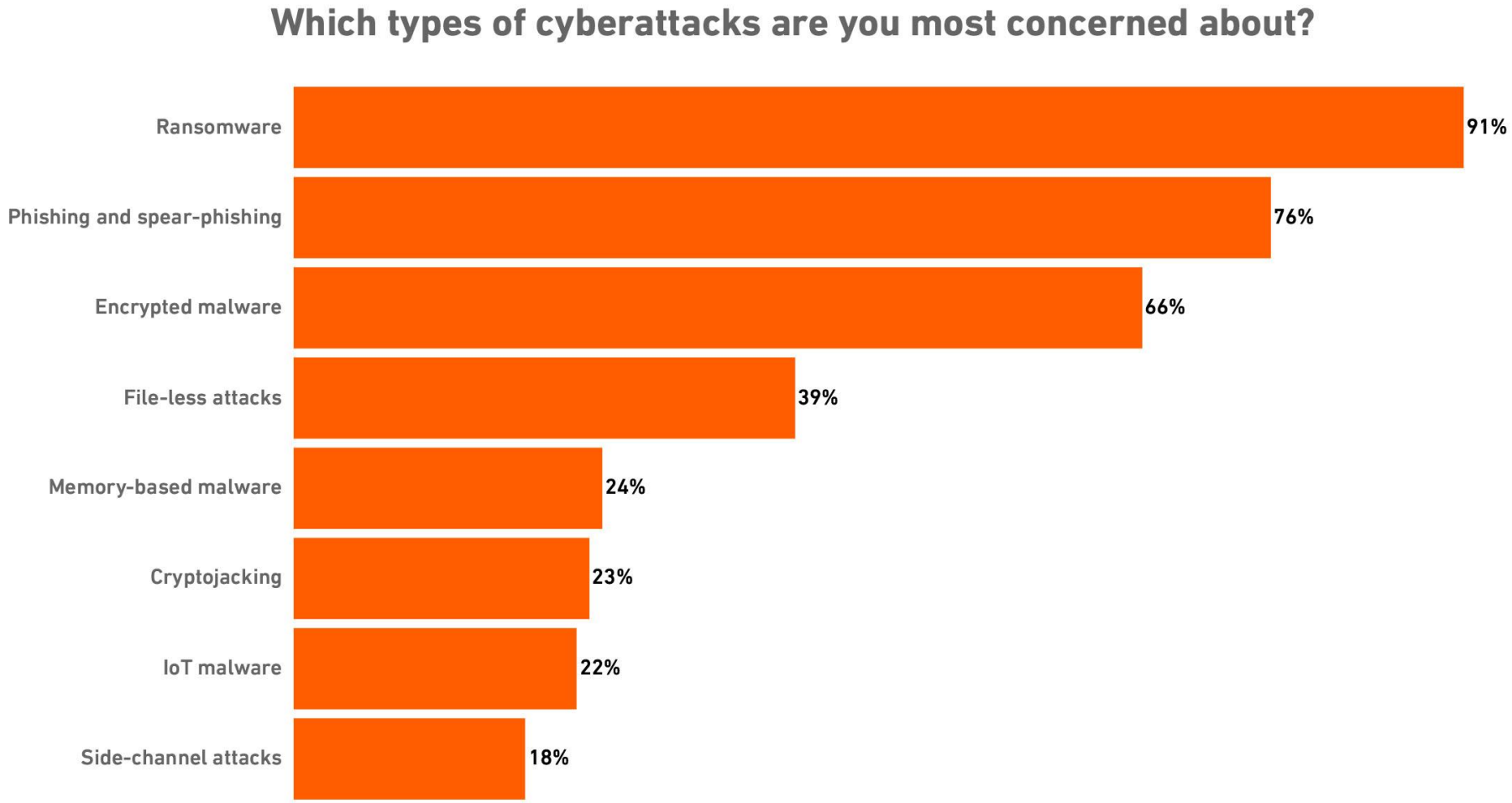


Source: 2022 SonicWall Threat Mindset Survey.

Y EL RANSOMWARE PREOCUPA A TODOS

91%

Despite a decline in overall volume in 2022, ransomware was chosen by **91%** of respondents as their top concern in 2022.



Caso: incidente en el Hospital Clínic de Barcelona

- 11:17, domingo, 5 de marzo de 2023. Ciberataque al HC, de tipo ransomware.
- El ciberataque afecta a los servicios de laboratorio, farmacia, urgencias, etc.
- Hay robo de información y piden un rescate de $4M. Si no se paga en 1 semana, publicaran los datos robados en los servidores.

1. ¿Qué daño y tipos se han producido?

2. ¿Responsabilidad de la dirección?

> Se han tenido que aplazar este lunes 150 cirugías no urgentes, entre 2.000 y 3.000 consultas externas y unas 400 extracciones de sangre

"No se va a pagar"

AGENDA

Nuevos retos de ciberseguridad

23th octubre. Barcelona

1. Introducción a la Ciberseguridad
2. Estado de la ciberseguridad: tendencias
3. NIS2: Responsabilidad de los consejeros
4. Nuevas amenazas en el horizonte
5. Preguntas y respuestas

NIS2 – ¿QUÉ ES?

Directiva UE – ampliación de la directiva NIS (2016)

NIS - **N**etwork and **I**nformation **S**ecurity

https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

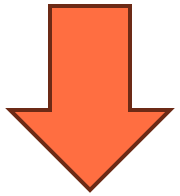
NIS2 es una normativa clave para fortalecer la resiliencia cibernética en Europa y garantizar que los sectores críticos estén mejor preparados para enfrentar las amenazas del mundo digital

NIS2 - OBJETIVO

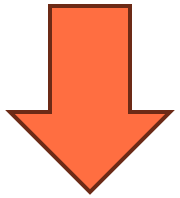
1. Ampliar el **alcance** de NIS (1)
2. Reforzar las **obligaciones de seguridad** implantando un sistema de **gestión de riesgos robusto**
3. Mejorar la **gestión de incidentes** (detección, notificación, respuesta)
4. Evaluar los riesgos de la **cadena de suministros**.
5. **Colaboración** entre Estados miembros
6. **Sanciones** más severas

NIS2 - ¿CUÁNDO SE APLICA?

Directiva NIS2 – Aprobada Noviembre 2022



21 meses para la transposición



17 Octubre 2024

(Implementación en España está pendiente a día de hoy……)

NIS2 – ¿A QUIÉN LE APLICA?

“Sectores Alta Criticidad":

Empresas con > 250 empleados o más
Una facturación de 50 millones de euros o un balance de 43 millones de euros.

"Otros sectores críticos":

Empresas > más de 50 empleados
Un volumen de negocios o balance anual de 10 millones de euros

RESUMEN DE LOS PASOS PARA CUMPLIR CON NIS2:

1. **Realizar evaluaciones de riesgos periódicas**.
2. **Implementar medidas de seguridad obligatorias**.
3. **Notificar los incidentes** de ciberseguridad dentro de los plazos.
4. **Asignar responsabilidades a nivel directivo** y asegurarse de la formación de personal.
5. **Realizar auditorías periódicas** para asegurar el cumplimiento.
6. **Cooperar con las autoridades y otras organizaciones** en la gestión de amenazas.
7. Desarrollar una **política de respuesta a incidentes** eficaz.
8. **Asegurar la seguridad en la cadena de suministro**.
9. Garantizar la **protección de datos y la mejora continua** de los sistemas de seguridad.

Cumplir con estos requisitos permitirá que las organizaciones se ajusten a la **NIS2** y puedan evitar sanciones y mejorar su ciberresiliencia.

SANCIONES Y RESPONSABILIDAD

1. Multas económicas

- hasta el **2% de los ingresos anuales globales** de una empresa, o hasta un máximo de **10 millones de euros**, lo que sea mayor. - GDPR.

2. Responsabilidades directivas: La alta dirección y el Consejo de administración deben establecer la ciberseguridad como una prioridad y son responsables de su aplicación o incumplimiento.

3. Medidas correctivas

4. Suspensión temporal de actividades (inhabilitación)

5. Evaluación periódica

6. Daños reputacionales

Las sanciones de la **NIS2** son más severas y están diseñadas para garantizar que las organizaciones **inviertan en ciberseguridad** y cumplan con las obligaciones legales

PREPÁRATE PARA CUMPLIR CON LA NORMA

¿Cómo hay que prepararse?

Be prepared

10 things organizations should consider for NIS2 compliance:

1. Determine if NIS2 applies to your organization.
2. Identify your critical assets.
3. Develop a risk management strategy.
4. Implement appropriate security measures.
5. Implement incident response procedures.
6. Conduct regular security testing.
7. Train employees.
8. Consider third-party risks.
9. Maintain documentation.
10. Comply with reporting requirements.

¿QUÉ HACER ANTE UN INCIDENTE?

QUÉ ES UN PLAN DIRECTOR DE CIBERSEGURIDAD

*"Documento estratégico que establece las directrices y acciones necesarias para **proteger** los **activos** digitales y la **información** sensible de una organización contra las **amenazas** cibernéticas"*

QUÉ DEBE INCLUIR UN PLAN DIRECTOR DE CIBERSEGURIDAD

1. Evaluación de riesgos
2. Política de ciberseguridad
3. Protección infraestructura
4. Gestión de incidentes
5. Continuidad del negocio
6. Formación del personal
7. Auditoría y revisión
8. Asignación de recursos
9. Plan de Implantación

SITUACIONES REALES QUE HAY QUE PREVEER…

- Un **virus informático** bloquea algunos de los laptops de los directivos
- Robo de **credenciales** de usuarios
- Se produce una **pérdida de datos sensibles** y no podemos recuperar la información porque la copia de seguridad está dañada
- **Timo del CEO**: suplantación y **estafa** monetaria a la compañía
- Nuestra **web de comercio** electrónico se bloquea por un ataque de denegación de servicio
- Se **estropea un servidor** o elemento de red y no podemos usar el correo electrónico o conectarnos a las aplicaciones de la empresa
- Nos **encriptan los servidores** y nos piden un rescate (ransomware)
- etc.

TIMO DEL CEO. CASO REAL. PROCESO:

- Robo de una cuenta de un usuario de la empresa
- Estudio del entorno durante meses
- Robo de cuentas de directivos o de usuarios privilegiados
- Mail fake o llamada al director financiero por parte del “supuesto CEO” para transferir unos fondos urgentemente
- La c/c es de un testaferro, desde dónde se transfiere a otra en un paraíso fiscal
- Y desaparición de cuentas y de pruebas.
- Otra modalidad es cambiar la c/c en facturar a pagar por parte de proveedores (“Man in the middle”)

CASO RANSOMWARE

Un viernes a las 12 de la noche nos llama el responsable de informática y nos dice que se ha bloqueado el acceso a los servidores de la empresa y que el cibercriminal que lo ha realizado pide un rescate de 10 bitcoins por la clave (1 bitcoin = 60.000 Eur aprox)

¿Qué le dices?

¿Pagas o no pagas?

¿Es legal pagar?

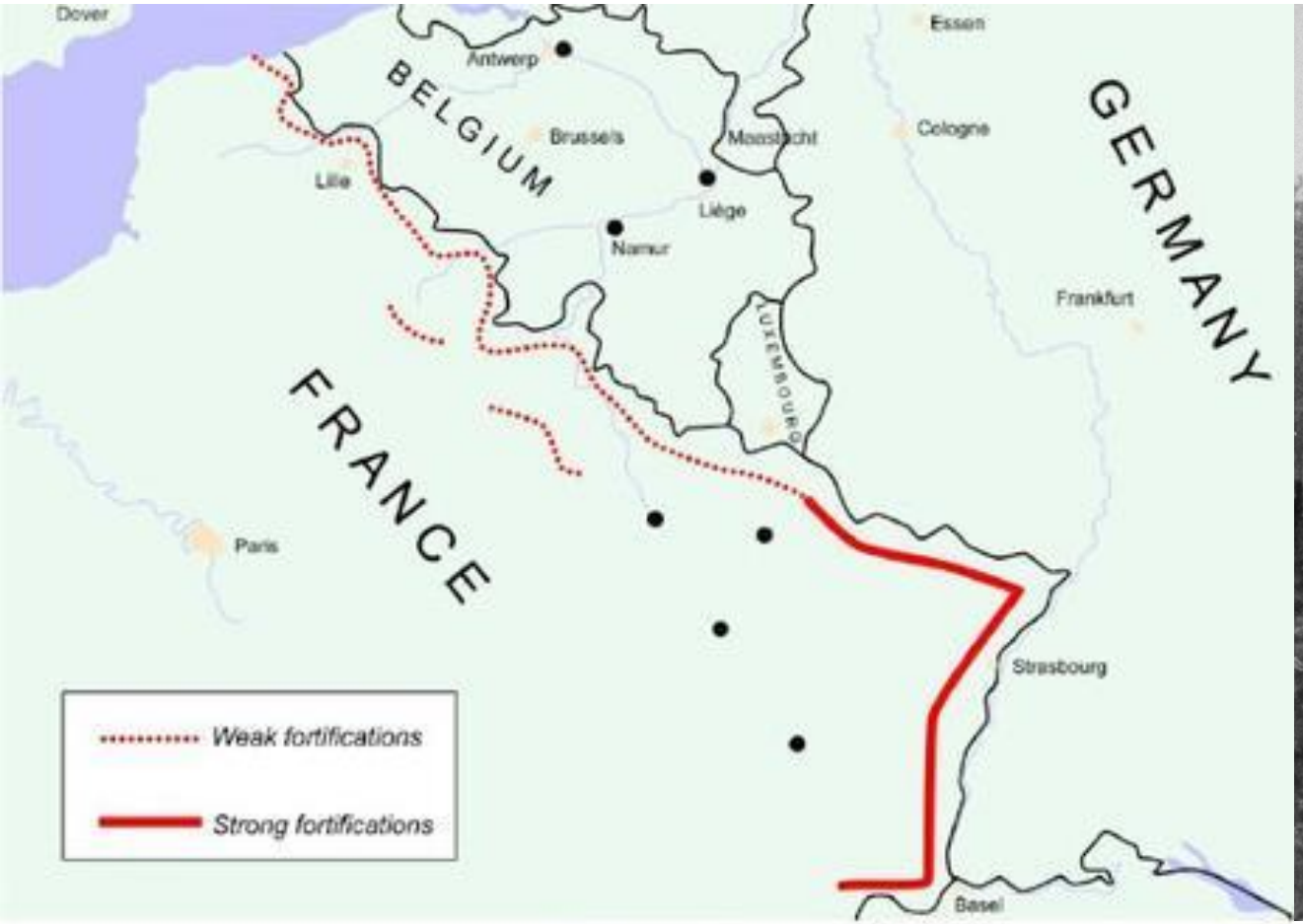
¿Qué pensáis que se debería hacer?

AGENDA

Nuevos retos de ciberseguridad
23th octubre. Barcelona

1. **Introducción a la Ciberseguridad**
2. **Estado de la ciberseguridad: tendencias**
3. **NIS2: Responsabilidad de los consejeros**
4. **Nuevas amenazas en el horizonte**
5. **Preguntas y respuestas**

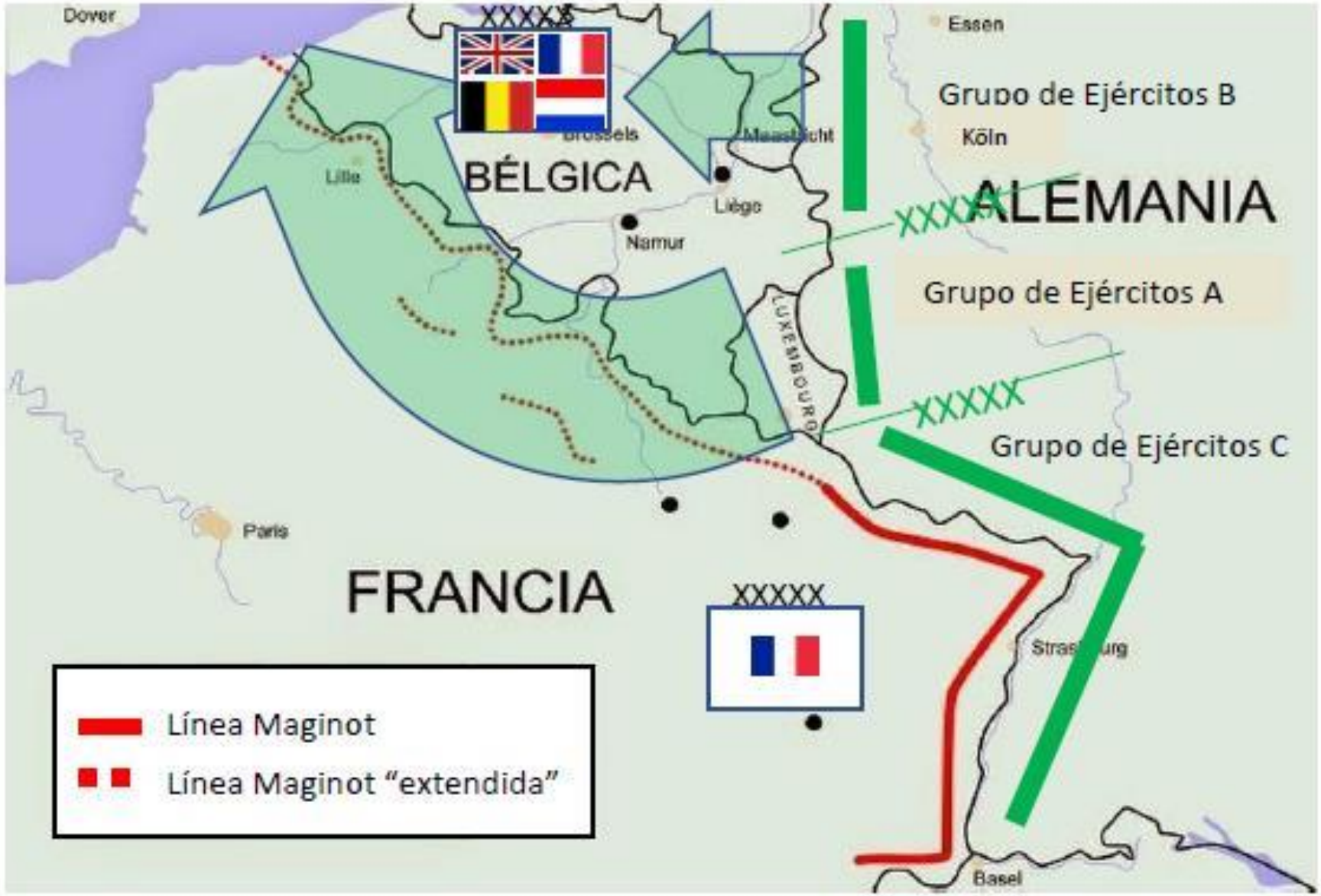
EJEMPLO: LINEA MAGINOT (1940)



Línea Maginot

¿Qué sucedió? El ataque a Francia en 1940 se realizó por Bélgica y Luxemburgo. Por la parte "débil", la no vigilada: Los bosques de las Ardenas.

EJEMPLO: LINEA MAGINOT (1940)



TRÁFICO ENCRIPTADO

74% **Del tráfico en internet (2023) está cifrado (HTTPS)**

▲300%

EL AUMENTO DE LAS AMENAZAS CIFRADAS LLEGA A LOS TRES DÍGITOS

Julio 2022 contra julio de 2023, tiene un incremento de un 300%. Es el mayor incremento visto nunca en los laboratorios de SonicWall. El uso del tráfico TLS como túnel de entrada en las organizaciones se ha popularizado y el malware que lo utiliza crece exponencialmente.

HTTPS: Una avenida para el cibercrimen

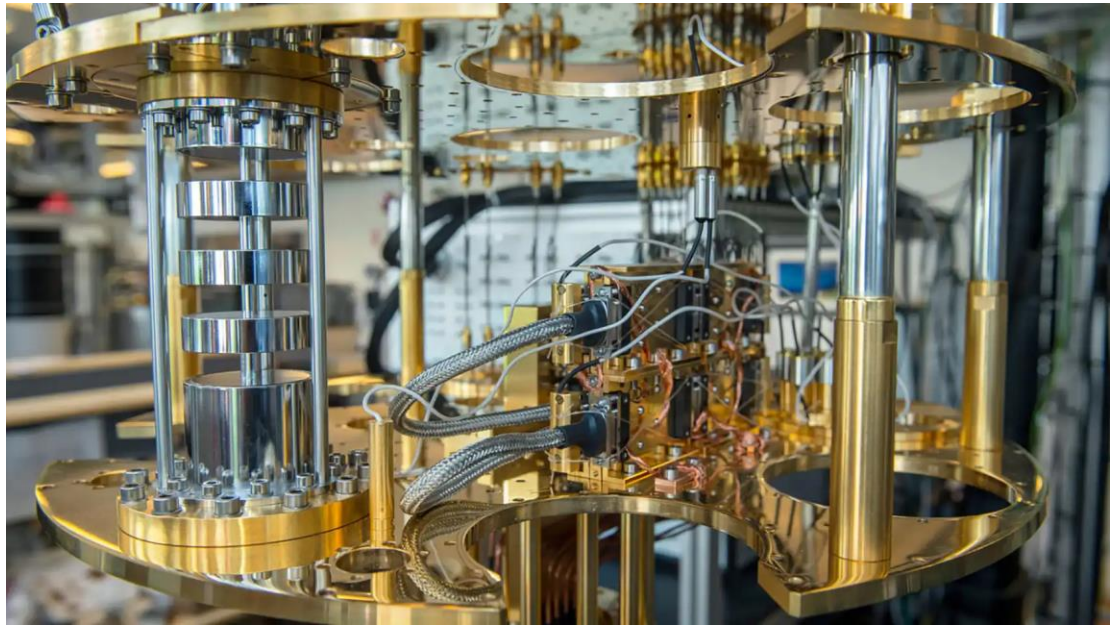
ES EL ETERNO DILEMA ENTRE…

¿Privacidad o Ciberseguridad?

¿Cuál es el importante…? Lo dejo a cada uno

OTRAS AMENAZAS:

- **Computación cuántica**: Lo que ahora es imposible de descifrar, lo será en segundos (o minutos)
- **Suplantaciones perfectas de identidad (IA)**: Muy difíciles de identificar
- **Falta de personal de ciberseguridad**: Cada vez más demandado y escaso
- **Aumento exponencial de la superficie de exposición**: Todo conectado.
- **Politización de internet**. Intento de control por los gobiernos.
- **Guerra cibernética**: APTs, etc.



Y EL MÁS IMPORTANTE: EL CIBERCRIMEN…

Su volumen ya es del tráfico de drogas, el de armas y el de seres humanos, todos juntos:

el 1.5% del PIB mundial según algunas estimaciones…

1 DEFENSA POR CAPAS

- Ataques cada vez más sofisticados
- Explosión del número de ataques
- Muchos de corte desconocido: Nunca ha habido tantas variantes desconocidas: 465K detectadas en 2022.
- Ransomware + focalizado
- No sabemos cómo ni cuándo nos van a atacar.
- La única solución: una defensa en profundidad, por capas, coordinada y **compartimentada**

VISIBILIDAD CENTRAL PARA DETECTAR Y RESPONDER

2

- La defensa por capas precisa de coordinación –> Un **SOC**.
- El uso de la IA es una ayuda también para la detección en tiempo real.
- Hay que estar preparado para responder y aislar partes de la red.
- Monitorización para evitar Account Takeovers (robo de identidades) -> Identificar usuarios: ¿Eres quien dices ser? Uso de Zero-Trust

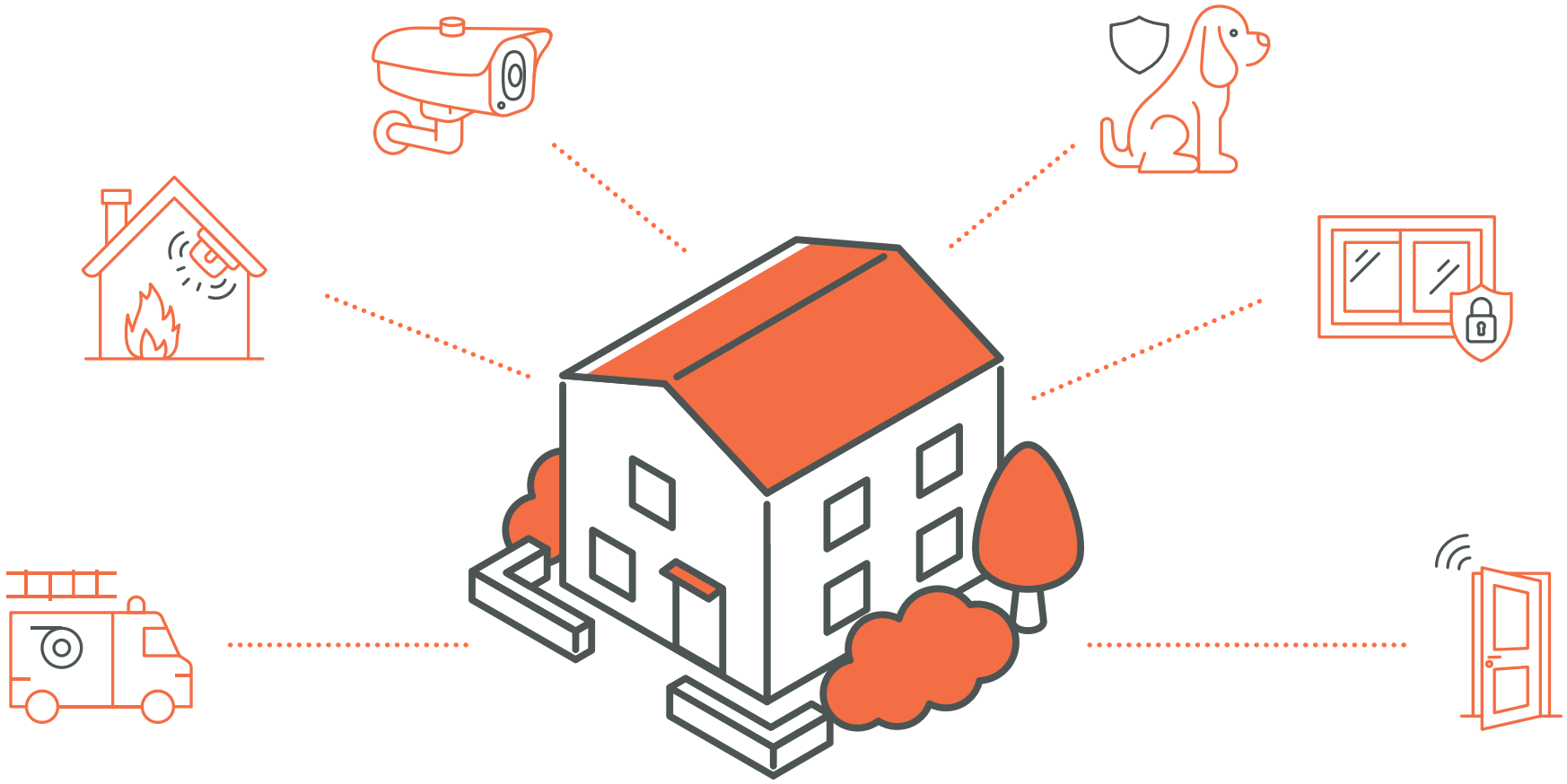
3 DETECTAR LO DESCONOCIDO

Uso de **Inteligencia artificial** para la detección
Miles de variantes de malware con y sin fichero (465K en 2022)
Más del 70% tráfico encriptado
El uso de sandbox Avanzado, con multiples estrategias, es fundamental

4 ACCESO REMOTO SEGURO

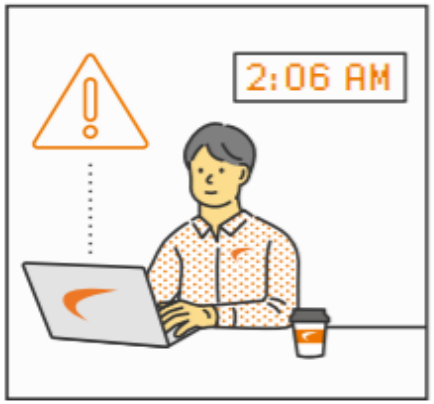
- Doble autenticación (2FA):
  - Algo que sabes, algo que tienes, algo que eres
- Centralizar el tráfico para inspeccionarlo
- Controlar el tráfico de los dispositivos remotos
- Zero trust – Mínimo privilegio – Desconfianza máxima.
- Endpoint control: ¿Es de confianza?
- Acceso compartimentado

PREVENCIÓN – DETECCIÓN – RESPUESTA

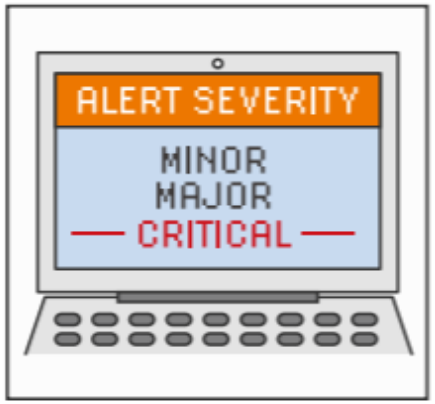


QUE ÉS UN SOC (SECURITY OPERATING CENTER)

SOC EN ACCION: CICLO DE VIDA DE UN INCIDENTE



SonicWall's Security Operations Center monitors for alerts and abnormal behavior 24 hours a day to protect our MSP partners and their clients from cyber threats. When alerts come in from security tools, a SOC analyst investigates.

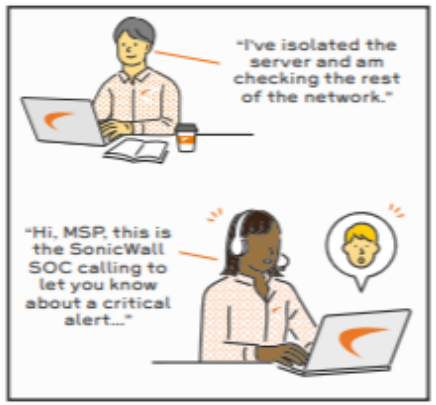


Alerts are classified as minor, major, or critical alerts. The SOC team sets rules and configurations that automatically classify alerts, and then the SOC analyst can upgrade or downgrade the alert as necessary.

Minor alerts are used for abnormal activities on endpoints, such as files being quarantined in unusual folders. They have a high likelihood of false positives. The SOC will contact you by email if further investigation is recommended.

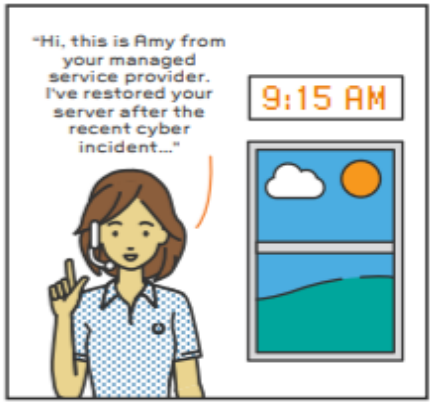
Major alerts are used when there is confidence of malicious activity on the endpoint. Often this activity was stopped by security tools, such as malware being quarantined automatically by a next-generation antivirus. The SOC will contact you by email with recommended follow-up, such as additional phishing training for end users.

When there is high confidence of a breach or compromise actively occurring, that's a critical alert. The SOC team jumps in to quickly minimize the damage and keep the compromise from spreading further across your network.



During a critical alert, the SOC team will call the emergency phone number you provided every 15 minutes for the first hour, then every hour after that if you don't answer. However, they won't wait for you to answer to begin defending you; they will immediately take whatever actions are necessary to stop the attack and protect the rest of your environment, typically by isolating endpoints.

The SOC analyst will create a report to document what happened, the scope of the incident, and any other areas of impact. The SOC will also make recommendations for your next steps.



Once the active threat is removed, you can work with your customer to repair their network, restore any isolated endpoints to a known-good state, and follow through on any other remediation needs.

SONICWALL


SONICWALL®
Never alone.
Relentless security.

WE ARE SONICWALL

Never alone. Relentless security.

Fundada en 1991, Headquarters en Milpitas (California), 1700+ empleados, https://www.sonicwall.com

SonicWall defiende a centenares de miles de empresas en todo el mundo

3.5 millones
Firewalls instalados

1.1 millones
Sensores activos

~30%
Market share de PYMES en NOAM

17,000+
Partners en +215 países y territorios

Porque somos un aliado del canal:

ZENXEON TECHNOLOGIES

Logically

InterVision

En retail…

ACE The helpful place.

Chick-fil-A

En universidades e incluso en un F-35…

In Supremæ Dignitatis 1343 Università di Pisa

Joint Strike Fighter JSF F-35 Lethal Survivable Supportable Affordable

HIGHER EDU	GOVERNMENT	K-12	RETAIL
Docenas de Universidades	**10+** Ministerios defensa	**Cientos** de colegios	**100+** Marcas
500,000+ estudiantes	**1M+** tropas	**2M+** estudiantes	**200,000** Tiendas