PORQUÉ SE NECESITA UNA NUEVA CIBERSEGURIDAD

Sergio Martínez
Country Manager Iberia
Sonicwall

SONICWALL

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…

Università di Pisa

Joint Strike Fighter — JSF F-35 — Lethal Survivable Supportable Affordable

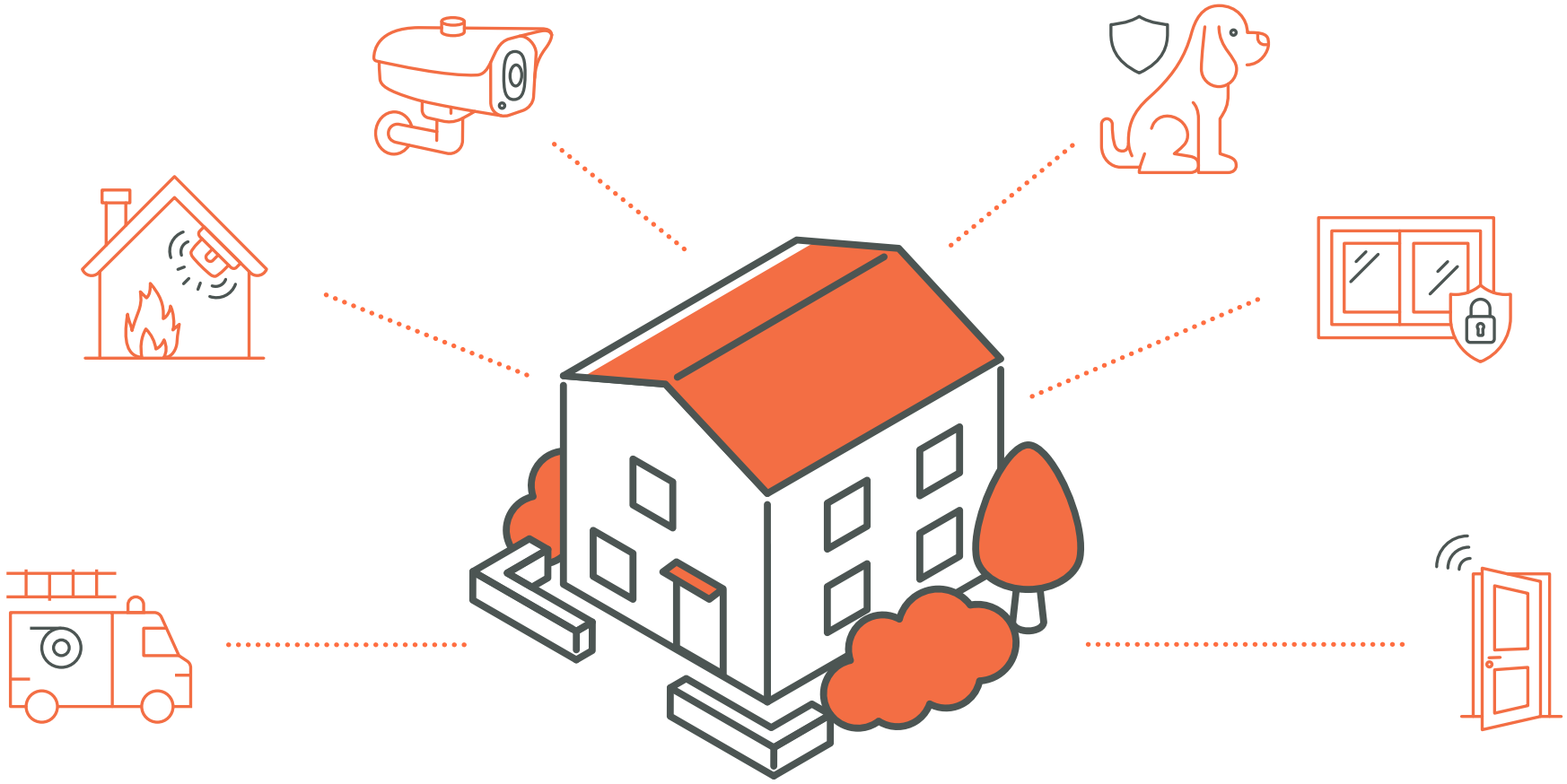
HIGHER EDU
Docenas de Universidades
500,000+ estudiantes

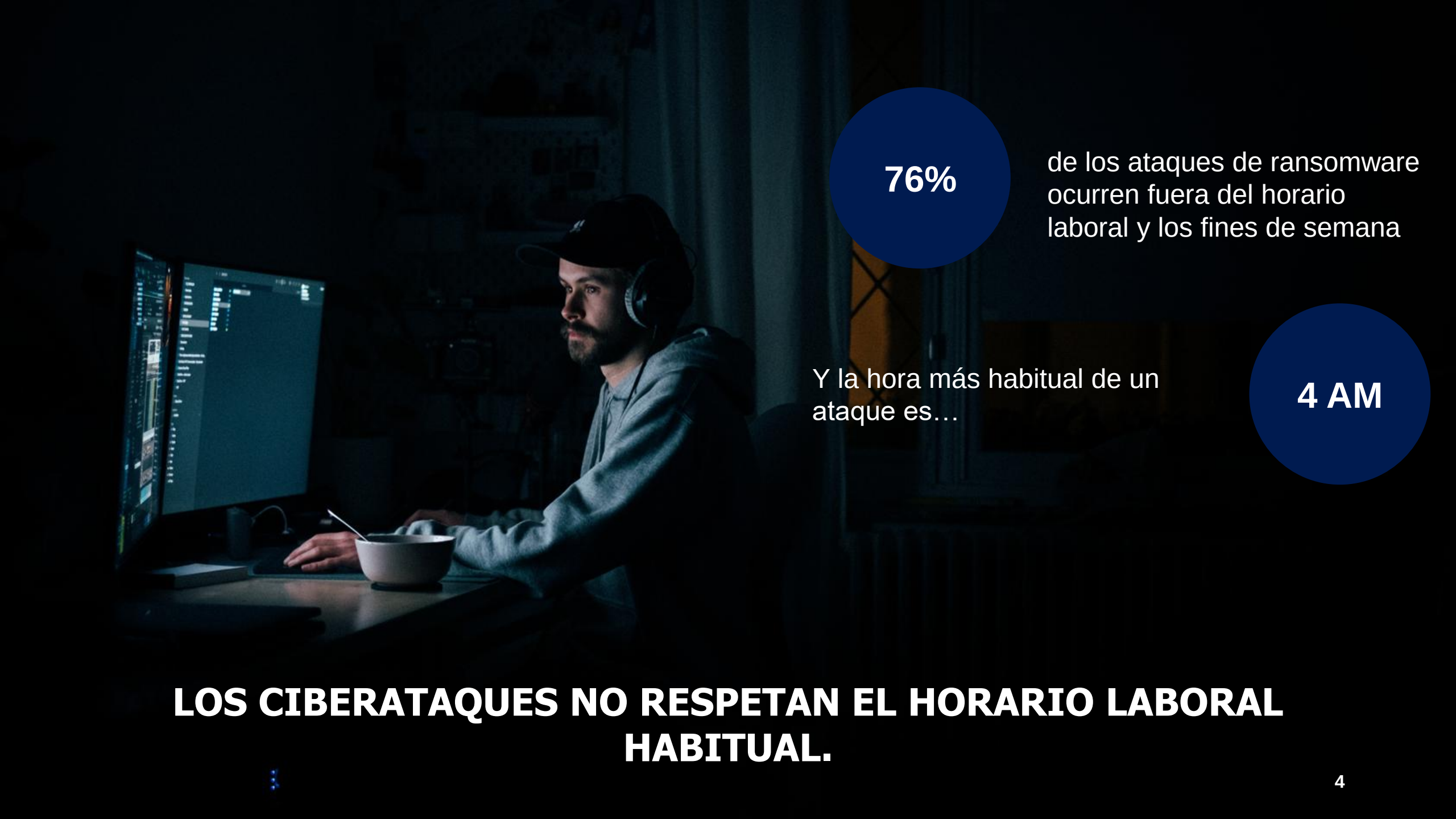
GOVERNMENT
10+ Ministerios defensa
1M+ tropas

K-12
Cientos de colegios
2M+ estudiantes

RETAIL
100+ Marcas
200,000 Tiendas

PREVENCIÓN – DETECCIÓN – RESPUESTA





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.

PROBLEMAS CON...

Tiempo de respuesta

Las alertas a gestionar se producen en horas intempestivas, proporcionando un tiempo valioso a los atacantes ante la falta de respuesta en tiempo.

Fatiga de alertas

Muchas alertas son falsos positivos.

El constante flujo de alertas puede enmascarar las de carácter crítico

Faltan expertos

Los MSPs ayudan a los clientes en todos los servicios de IT, hasta la instalación de impresoras

Es difícil para ellos captar y retener talent de Ciberseguridad para poder gestionar correctamente estas alertas.

SONICWALL®

INFRAESTRUCTURA NO MONITORIZADA: UN RIESGO EVITABLE

60%

De los incidentes se deben a una **mala configuración**

48

Hours

Tiempo medio para **explotar** una brecha

120

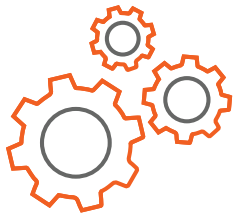
Days

Tiempo medio en **parchear**

90%

De todas las brechas se deben a un error **humano**

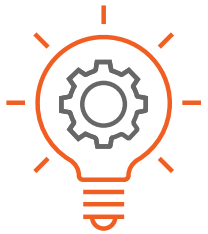
EL CAMPO DE BATALLA ESTÁ CAMBIANDO



Las redes son más **complejas**

Las amenazas crecen en volumen y **sofisticación**

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



Hay que estar preparado para responder 24x7x365

#KnowTheThreats

GET THE LATEST CYBER INTELLIGENCE

Download the mid-year update to the **2025 SonicWall Cyber Threat Report** to gain exclusive insight into cybercrime's shifting frontlines and how changing behaviors may impact your organization.

DOWNLOAD THE REPORT

SonicWall.com/ThreatReport

SONICWALL

INFORME ANUAL DE CIBERSEGURIDAD

1.1m+
Global Sensors

215+
Countries & Territories

24x7x365
Monitoring

<24hrs
Threat Response

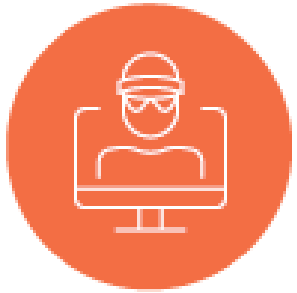
140k+
Malware Samples Collected Daily

28m+
Malware Attacks Blocked Daily

SONICWALL

LAS AMENAZAS CRECEN

RANSOMWARE



El Ransomware se intensifica en Norteamérica (+8%) y explota en LATAM

▲259%

$850,700

Coste medio del rescate de un ataque de Ransomware: En 2024 el pago medio del rescate alcanzó los $850.000, con un total de pérdidas relacionadas de $4.91M, incluido los costes de no servicio y de recuperación.

LAS AMENAZAS CRECEN

MALWARE

▲8%

Los ataques de malware subieron un 8% YoY, incluyendo un pico de un 92% en mayo.

IoT AND ENCRYPTED

Los ataques de IoT (+124%) y de amenazas encriptadas (+93%) continúan creciendo globalmente.

▲124%

¿DÓNDE ESTÁ LA MAYORÍA DE LAS AMENAZAS?

SECURITY OPERATION CENTER (SOC)

85%

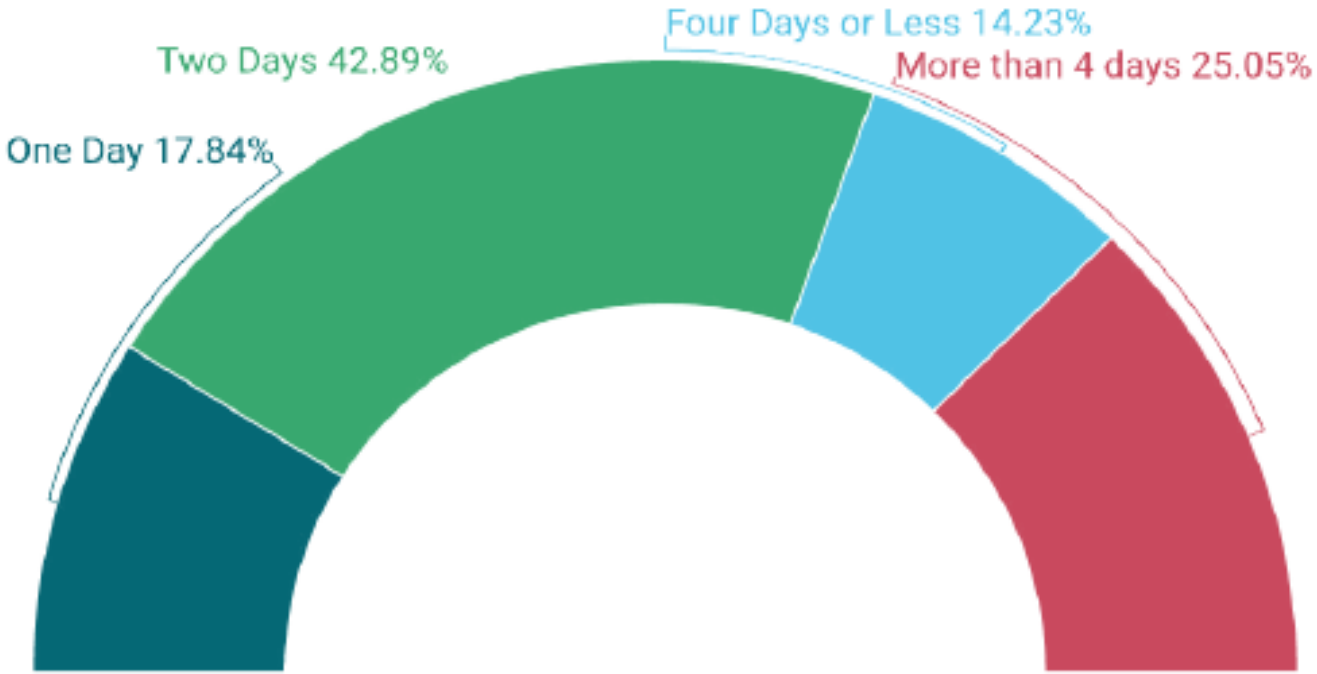
Un 85% de las alertas en nuestro SOC están relaciones con robos de identidad, Cloud y credenciales comprometidos

EL TIEMPO ES CRUCIAL: LAS PRIMERAS 48 HORAS

Time of Threat Actor Exploitation

How fast hackers leverage exploit code

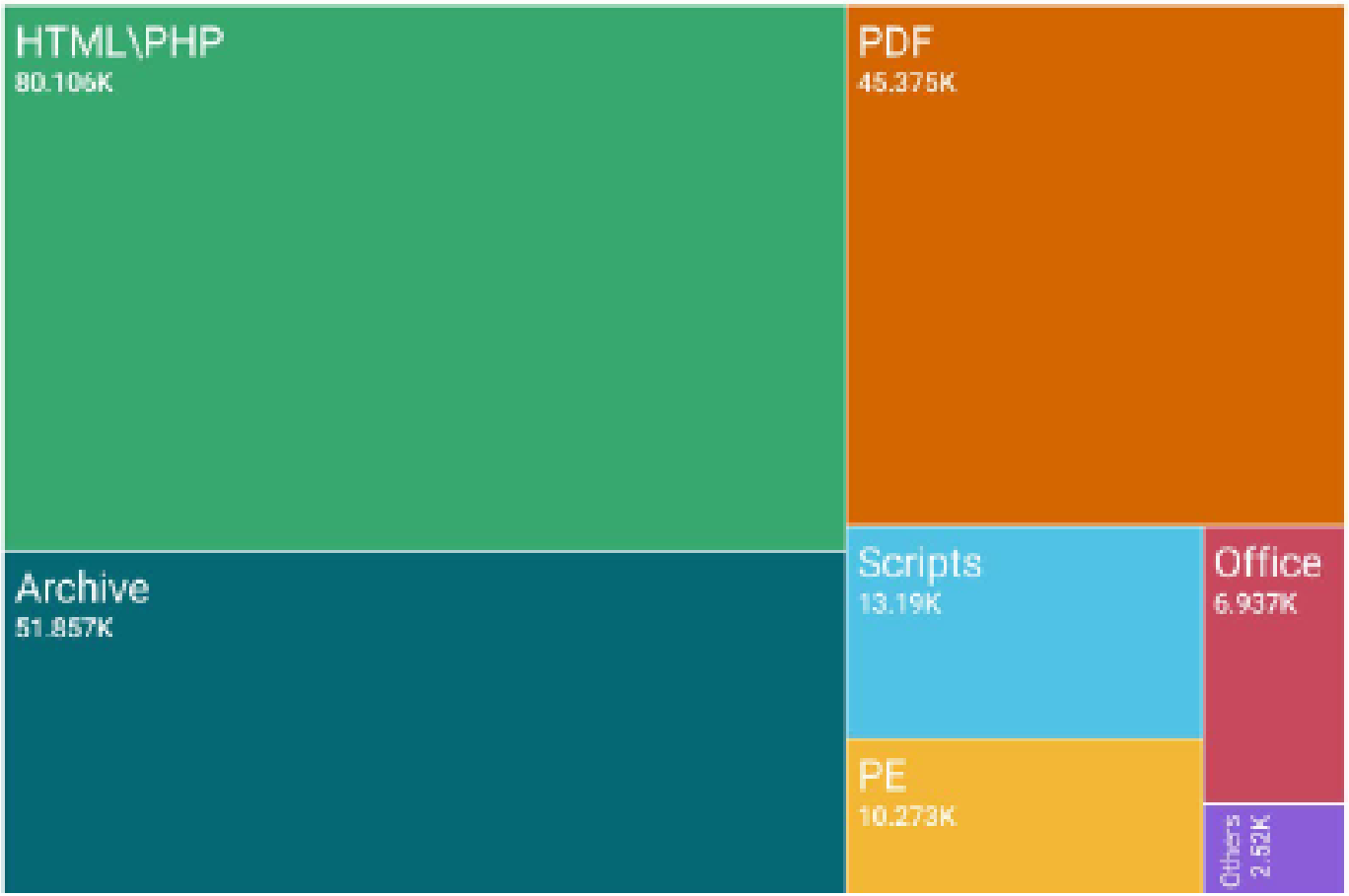
60%



LA LETALIDAD DE LO COTIDIANO

Tipos de fichero usados en ataques maliciosos

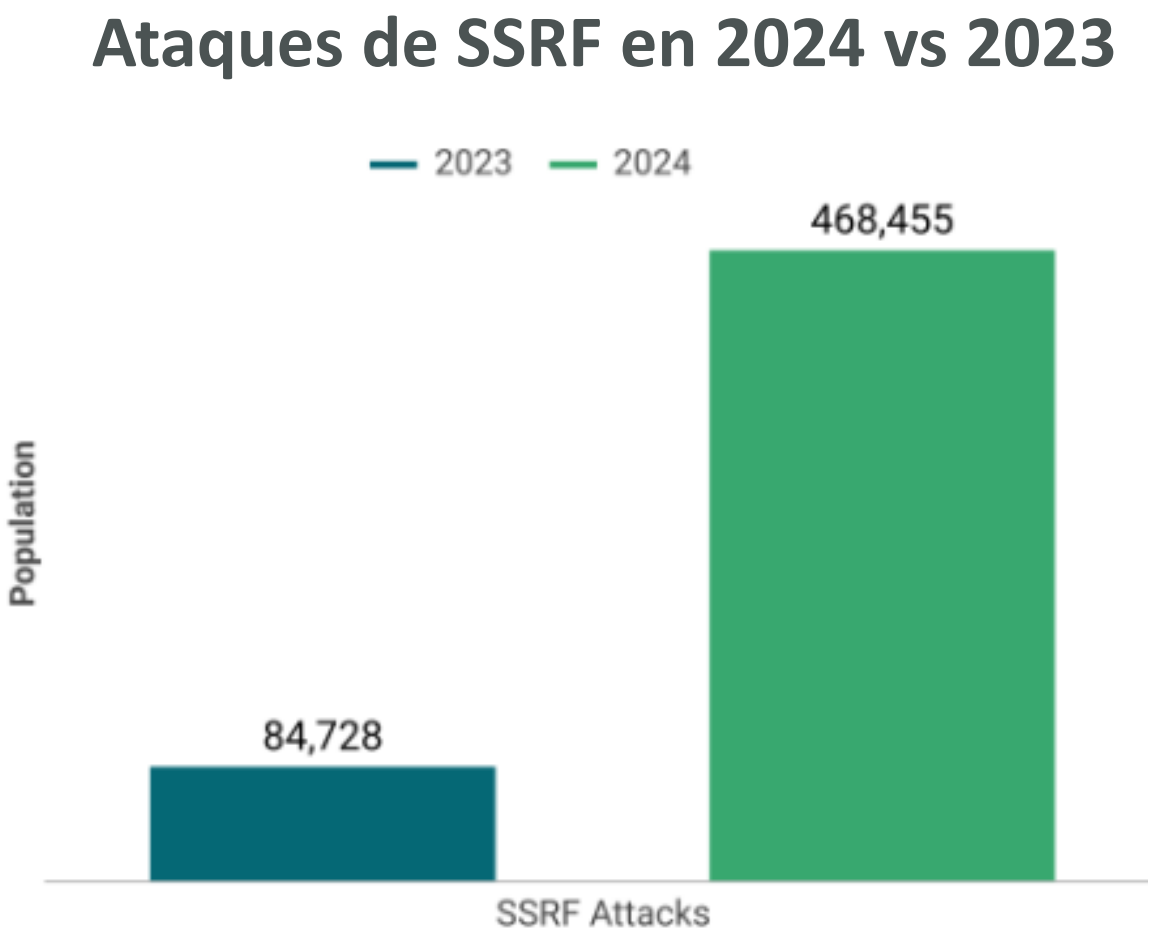
Esquema de los ficheros usados a diario por las amenazas



SONICWALL

IA: FACILITA LOS ATAQUES E INCREMENTA SU COMPLEJIDAD

Viejas amenazas revitalizadas por la IA



SSRF: Server Side Request Forgery

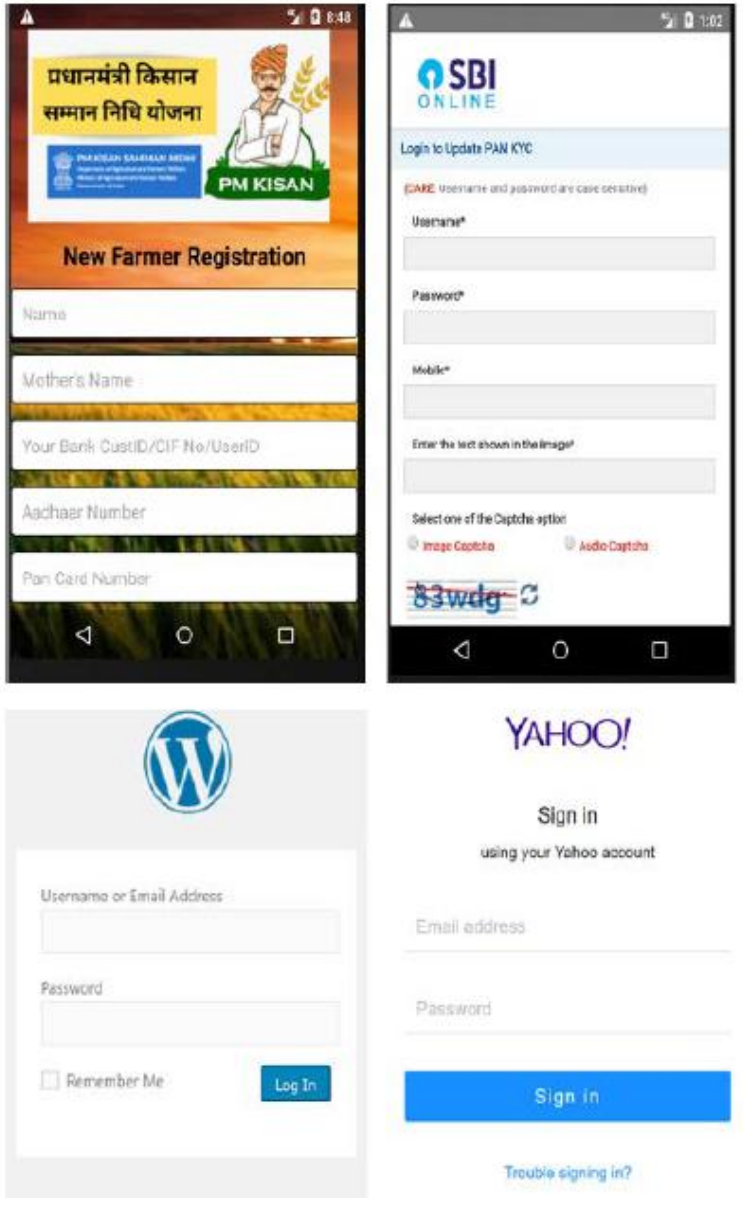
La introducción de las herramientas potenciadas por **IA generativa**, ha reducido las barreras de entrada. Algunos de los ataques que ha potenciado son:

- **Localización de sistemas no parcheados** o anticuados: Los escaners basados en IA identifican los sistemas “legacy” con vulnerabilidades no parcheadas, incluso en redes complejas.
- **Automatización de encadenamiento de Exploits**. La IA diseña procesos de encadenamiento SSRF con vulnerabilidades para el escalado de privilegios y movimientos laterales.
- **Evasión de detección**. La IA proporciona técnicas de ofuscación para evadir la detección, haciendo más efectivos los ataques.

NOTA: SSRF es la falsificación de peticiones en lado del servidor, el atacante lo manipula para realizar peticiones a recursos internos o externos.

Y LOS ATAQUES A SMARTPHONES, PARTICULARMENTE ANDROID…

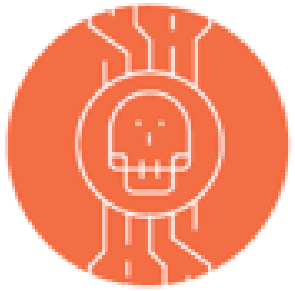
Aplicaciones ANDROID maliciosas: Explotan la confianza y los permisos para el Fraude Movil.



TRÁFICO ENCRIPTADO

72%

Del tráfico en internet (enero 2025) está cifrado (HTTPS)



549%

Ene 2024 contra Enero de 2025, el uso de las amenazas cifradas crece un 549%. El uso del tráfico TLS como túnel de entrada en las organizaciones se ha popularizado y el malware que lo utiliza crece exponencialmente.

HTTPS: Es una avenida para el cibercrimen

CAMBIO DE PARADIGMA

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

SONICWALL

¿NOS PODEMOS PERMITIR UN SOC?

VIGILANCIA EN TODA LA SUPERFICIE

SonicSentry Managed XDR

Alert Management · Threat Hunting · Threat Mitigation
Log Retention · Reporting

1 MDR for Endpoint

Protection and response for endpoints

CROWDSTRIKE

Capture Client

SentinelOne

Microsoft Defender

SOPHOS

2 MDR for Cloud

Protection and response for cloud apps and email

Cloud Email Security

Microsoft 365

Google Workspace

Cloud Threat Analytics

slack

Dropbox

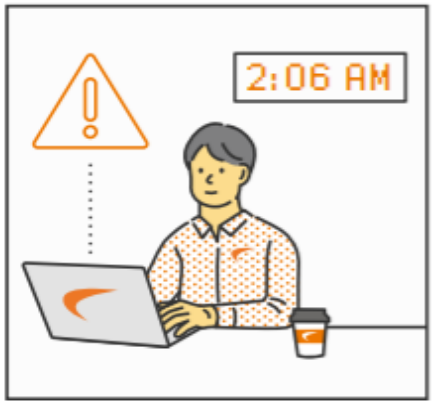
salesforce

3 MDR for Network

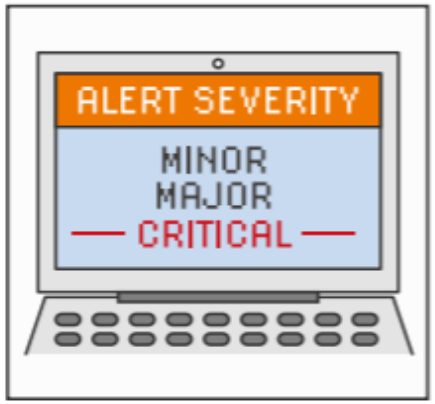
Protection and response at the perimeter

Any network device from any maker

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.

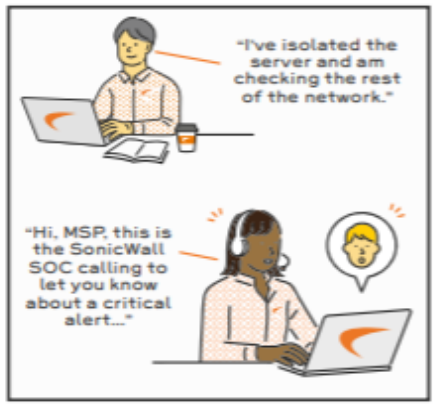


Alerts are classified as minor, major, or critical alerts. The SOC team sets rules and configurations that automatically classify alerts, and then the SOC analyst can upgrade or downgrade the alert as necessary.

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.

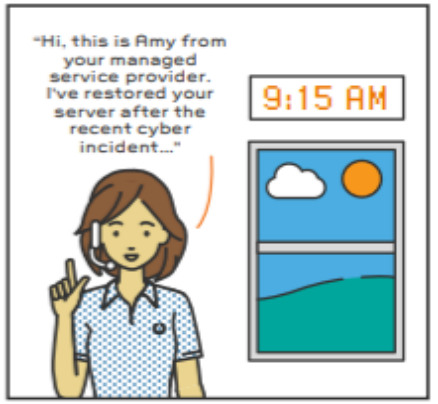
Major alerts are used when there is confidence of malicious activity on the endpoint. Often this activity was stopped by security tools, such as malware being quarantined automatically by a next-generation antivirus. The SOC will contact you by email with recommended follow-up, such as additional phishing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

MITIGATION VS. REMEDIATION

La respuesta inmediata es la diferencia

Mitigar

Nuestro SOC toma la iniciativa y aisla los dispositivos comprometidos, sea un endpoint, un servidor, etc.

Preparamos sugerencias para la plena remediación al partner, pero NO reconstruimos los dispositivos afectados.

Al igual que los bomberos, no reconstruimos la casa, nuestro SOC apaga el fuego, pero la reconstrucción es tarea del partner.

Remediar

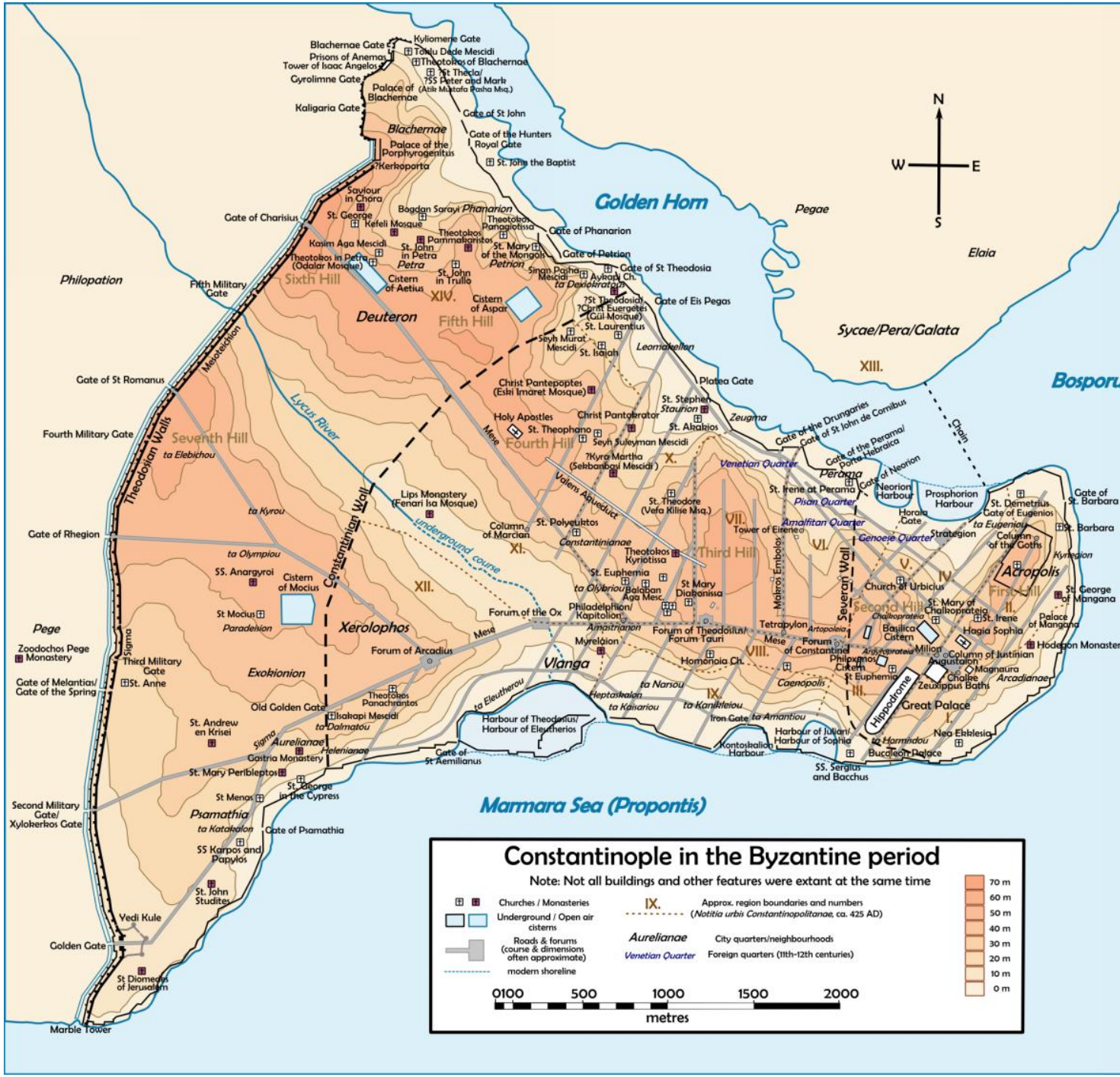
Después de que el ataque ha sido neutralizado, es el momento de que nuestro partner restaure los sistemas a un estado limpio de amenaza.

Nuestro SOC proporcionará sugerencias de remediación, pero será el partner el que la realice.

Esto pone al partner como responsable del proceso de remediación y restauración de los servicios del **cliente final, que es el suyo.**

1 DEFENSA POR CAPAS

- Ataques cada vez más sofisticados y focalizados
- Explosión del número de ataques inteligentes
- Ransomware muy focalizado
- No sabemos cómo ni cuándo vamos a ser atacados
- La única solución: una defensa en profundidad, por capas, monitorizada, coordinada y **compartimentada**



VISIBILIDAD CENTRAL PARA DETECTAR Y RESPONDER

2

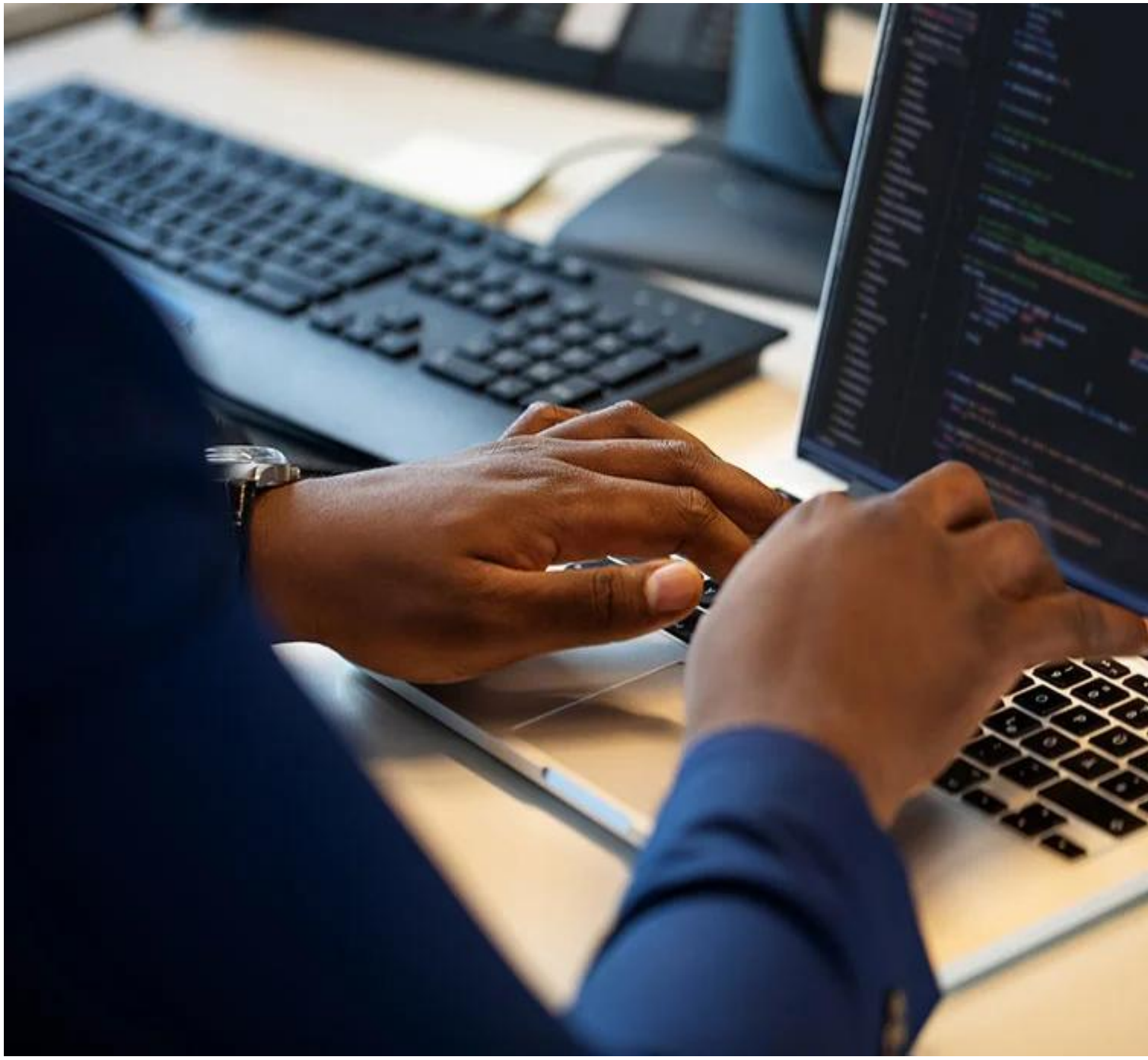
- La defensa por capas precisa de coordinación –> Un **SOC**.
- El uso de la IA es una ayuda también para la detección en tiempo real.
- Hay que estar preparado para responder y aislar partes de la red.
- Monitorización para evitar Account Takeovers (robo de identidades) -> Identificar usuarios: ¿Eres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

3 DETECTAR LO DESCONOCIDO

- Uso de Inteligencia artificial para la detección desde hace décadas
- 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 Y MODERNO

- Doble autenticación (2FA):
  - Algo que sabes, algo que tienes, algo que eres
- Servicios de VPN modernos -> Cloud Secure Edge
- Zero trust – Mínimo privilegio – Desconfianza máxima.
- Endpoint control: ¿Es de confianza?
- Acceso compartimentado



5 TCO Y COSTES DISRUPTIVOS

- Inspección de Gigabit a coste razonable
- Licenciamiento: solo nodo active de HA.
- Tecnología probada durante años en PYMES con IA y tecnología punta.
- Somos un aliado del canal: empujamos el negocio MSP

Sergio Martínez
Country Manager Spain & Portugal
@smartinezh
smartinez@sonicwall.com