Future SOC de Telefónica Tech: una ciber-resiliencia dinámica potenciada por la automatización e IA

DAVID MARTIN LINDSTRÖM

Global Product Marketing Head Network Security & MSS

KATTERINE NODARSE MORALES

Global Product Manager

2025

FUTURE SOC

Agenda

1. Contexto actual de Ciberseguridad
2. Estrategia de plataformización
3. SOC del Futuro de Telefónica Tech
4. Alianza Telefónica Tech y Palo Alto

El contexto actual de la ciberseguridad

ENTORNO TECNOLÓGICO

Entornos híbridos, Cloud, IA, trabajo en remoto, SCR, etc, más difíciles de proteger. Falta de visibilidad, mayor superficie de ataque o tráfico de datos más complejo.

AUMENTO DEL VOLUMEN DE DATOS

Más fuentes con más eventos que derivan en más alertas de seguridad.

ATAQUES MÁS SOFISTICADOS Y RÁPIDOS

Los ciberatacantes se aprovechan también de la tecnología: GenAI, Automatización. (legacy + emergentes).

FALTA DE PROFESIONALES

Analistas de seguridad EDR /SIEM, Threat Hunting, Arquitectos SIEM ...

SITUACIÓN GEOPOLÍTICA

Guerra, situación EEUU, ataques promocionados por estados, etc.

NUEVAS NORMATIVAS

NIS2, DORA

Un ecosistema cada vez más híbrido, más complejo y difícil de proteger

+90%

de los SOCs siguen dependiendo de procesos manuales

Fuente: Incident Response 2024 (Unit 42)

+333 millones

de eventos de ciberseguridad fueron detectados en el segundo trimestre de 2024

Fuente: Informe sobre el Estado de la Seguridad 2024 H2 (Telefónica Tech)

45%

de los casos, los atacantes exfiltran datos en menos de un día

Fuente: Informe Incident Response 2024 de Unit 42

FUTURE SOC

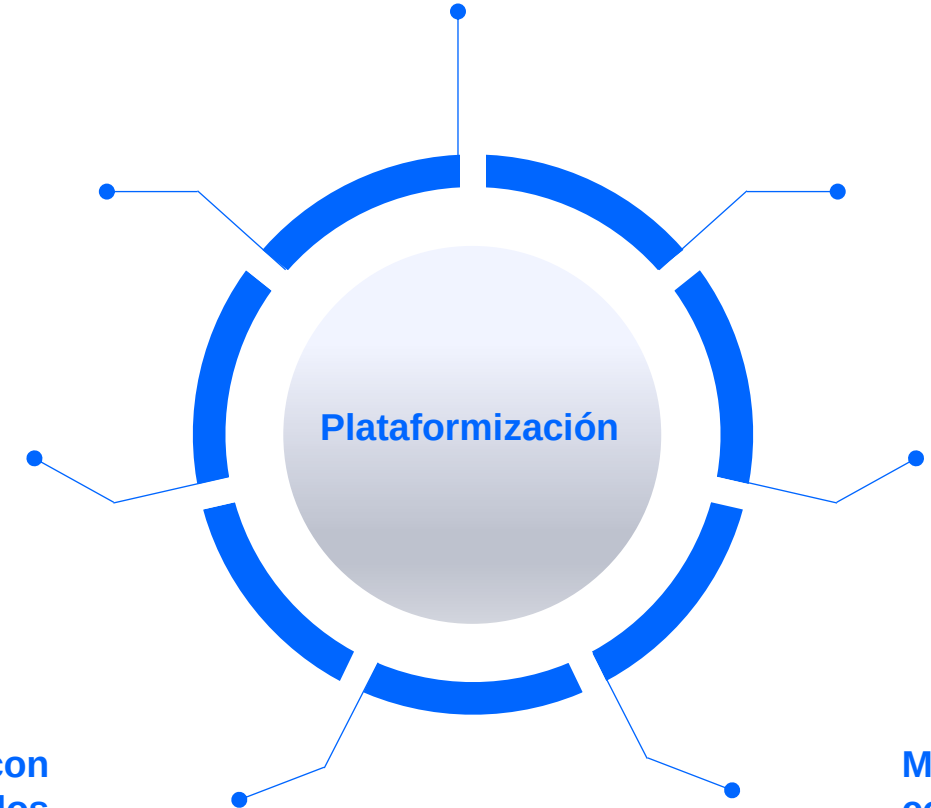
Desafíos actuales en los SOCs

- Múltiples equipos con herramientas operadas en silos que no se comunican entre sí.
- No hay visión transversal de los incidentes.
- Mantenimiento de sistemas y plataformas.
- Fatiga de alertas: Urgente vs Importante vs Alerta vs Incidente
- Falta de visibilidad y mayor superficie de ataque.
- Tiempos de detección y respuesta altos (MTTD , MTTD).

Nuevo enfoque para enfrentarse a estos desafíos: La Plataformización como epicentro

Integración de soluciones de terceros no incluidas en la plataforma.

Visión integral para un análisis conjunto



Inteligencia de amenazas

Punto de contacto único y oferta más competitiva

Automatización e IA.

SOC especialista de esta tecnología, con recursos certificados

Mejor respuesta a incidentes. Visión completa de seguridad

Future SOC

NextDefense

La propuesta de Future SOC de Telefónica Tech maximiza el valor de la estrategia de plataformización de Palo Alto Networks.

Añade un conjunto de nuevas capacidades y servicios junto con una metodología enfocada en la mejora continua de la postura de seguridad del cliente

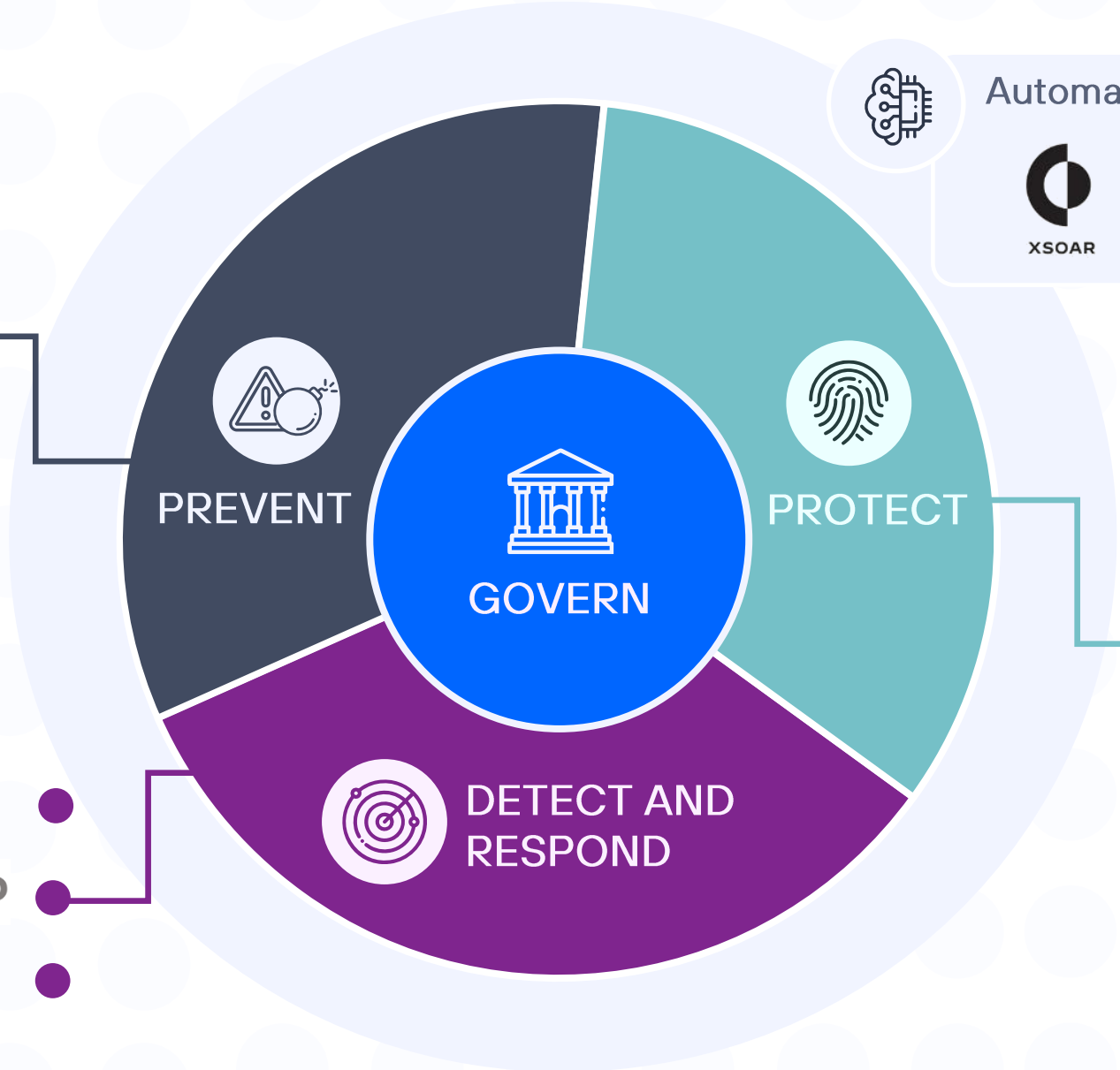
Adopción de IA y automatización para minimizar los procesos manuales, agilizar la respuesta a amenazas y disminuir el tiempo de detección y respuesta.

Actualizaciones continuas de playbooks adaptadas a cada industria y basadas en las mejores prácticas.

El ”Future SOC” aborda la evolución continua de la ciberseguridad del cliente y su modelo operativo

¿Cómo integra el *NextDefense* SOC el 100% de la tecnología de Palo Alto Networks?

Future SOC



Automation and AI

XSOAR

Precision AI®

CORTEX XPANSE

STRATA

PRISMA SASE
BY PALO ALTO NETWORKS

PRISMA ACCESS

PRISMA SD-WAN

CORTEX XDR
BY PALO ALTO NETWORKS

CORTEX® CLOUD
BY PALO ALTO NETWORKS

CORTEX XSIAM

FUTURE SOC

Acompañamiento del cliente en todo el ciclo de vida para una postura de seguridad adaptativa

NextDefense SOC

Adaptación continua del proceso D&R al contexto del cliente (riesgo, económico, personas, criticidad, etc.)

Beneficios para el cliente

- Ampliación y mejora de la cobertura de detección en términos de eficacia y eficiencia.
- Repuesta automática mejorada, potenciada por la plataformizacíon
- Mejora de KPI´s fundamentales como MTTD y MTTR.
- Mejora en eficiencia del proceso de D&R.

Telefónica Tech

NextDefense

El primer SOC que soporta el 100% de la tecnología de Palo Alto Networks

paloalto NETWORKS

Para aumentar la calidad de seguridad y aumentar la protección de nuestras organizaciones, Telefónica Tech cuenta con un SOC que integra toda la plataforma convergente de Palo Alto Networks

LIDERAZGO EN SEGURIDAD

- La tecnología líder en ciber-seguridad junto al líder de los servicios profesionales y gestionados
- Pioneros en automatización

COVERTURA COMPLETA ANTE AMENAZAS

- La red, los end-points, los usuarios, los datos, la identidad, la nube, etc.
- La unión de la mejor inteligencia sobre adversarios y amenazas, en tiempo real

TRANSVERSALIDAD. ELIMINACIÓN DE SILOS

- Plataforma SOC unificada
- Eliminación de redundancias y ángulos muertos (técnicos y operativos)
- Visión holística de la seguridad

MEJORA CONTINUA DE LA CALIDAD

- Evolución de la cobertura y extensión de la detección y respuesta a todos los escenarios
- Procesos de mejora continua integrados en toda la plataforma y servicios

NUEVOS MODELOS OPERATIVOS

- Por módulos o como SOC completo
- Modelo as a Service
- SLAs vs FTEs

paloalto NETWORKS | Cybersecurity Partner of Choice

THE STATE OF CYBER SECURITY IN TELEFÓNICA TECH

Customers choose us for our experience, reliability and continuous innovation

A global Managed Security Service Provider with a complete portfolio of cyber security capabilities

Experience, reliability and continuous innovation

Industry recognition

Gartner · FORRESTER · IDC Analyze the Future · GlobalData. · AVASANT

Customer Recognition

Santander · ALDI · MELIÃ HOTELS INTERNATIONAL · BBVA · INDITEX · ferrovial · Navantia · ARLANXEO · ie UNIVERSITY · BOSCH Invented for life · viesgo

Technical scale

350k Tickets managed per year

500k Alerts managed per year

15k Managed security devices

600 Security migrations per year

120k Digital customer notifications

6k Customer security reports

>10k Fraudulent sites closed per year

114 Cyber intel sources integrated

20mi IoCs evaluated and rotating in our intel

15 Years
Years of cyber security practice in Telefonica

+1,700 corporates
Cyber security customers at **global** level

+5,5k experts
Cyber security professionals at **global** level

>50 technologies
Cyber security technologies managed by our SOCs

Palo Alto Networks is a **strategic partner** of Telefónica Tech, and the relationship has evolved into a **cornerstone** of market positioning for both companies.

Telefonica Tech has de **maximum partnership level** DIAMOND Innovator at a **global scale**, supported on a **global partnership agreement** and accredited by **2 top PANW company level certifications: ASC and CPSP**.

LEVEL OF PARTNERSHIP

- Diamond

MSSP INNOVATOR & PRISMA MSSP

SOLUTIONS

- Managed Security services
- New Generation Firewall services (NGFW)
- Endpoint Protection services
- Secure internet access services
- Security Service Edge services (SSE)
- Cloud Posture Management & Workload Services
- Detection & Response Services
- XSOAR Automation Services

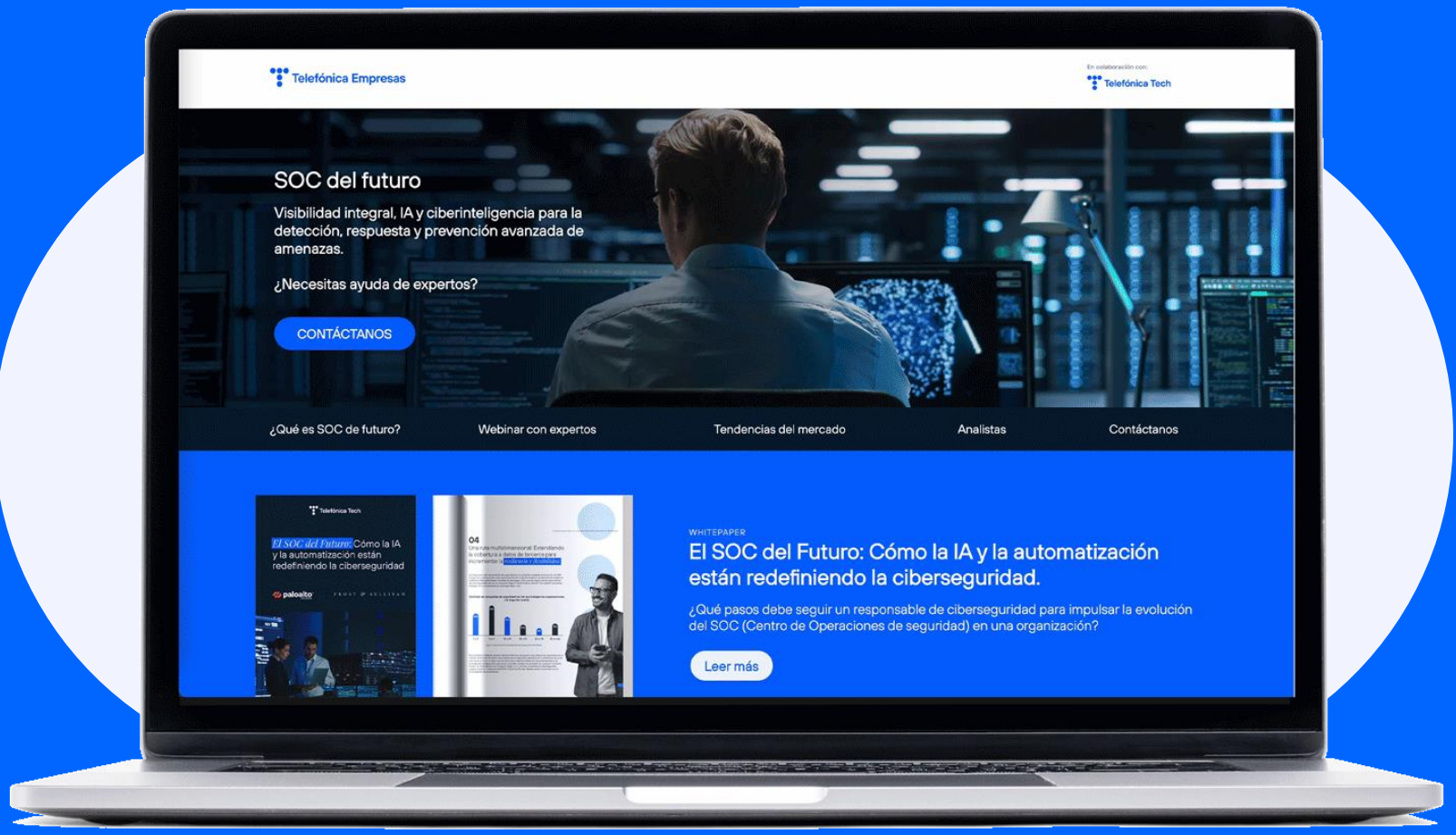
RELATED

- **Partner of the Year 2024**

6 SPECIALIZATIONS

- Authorized Support Center (ASC)
- Certified Professional Services Provider Partner (CPSP)
- Prisma NextWave SASE Specialization
- Prisma NextWave Cloud Specialization
- Cortex Nextwave XDR&SOAR Specialization
- Hardware Firewall
- MSSP Innovator
- Prisma MSSP

+300
certifications



Escanea el QR y accede a la web


Telefónica Tech