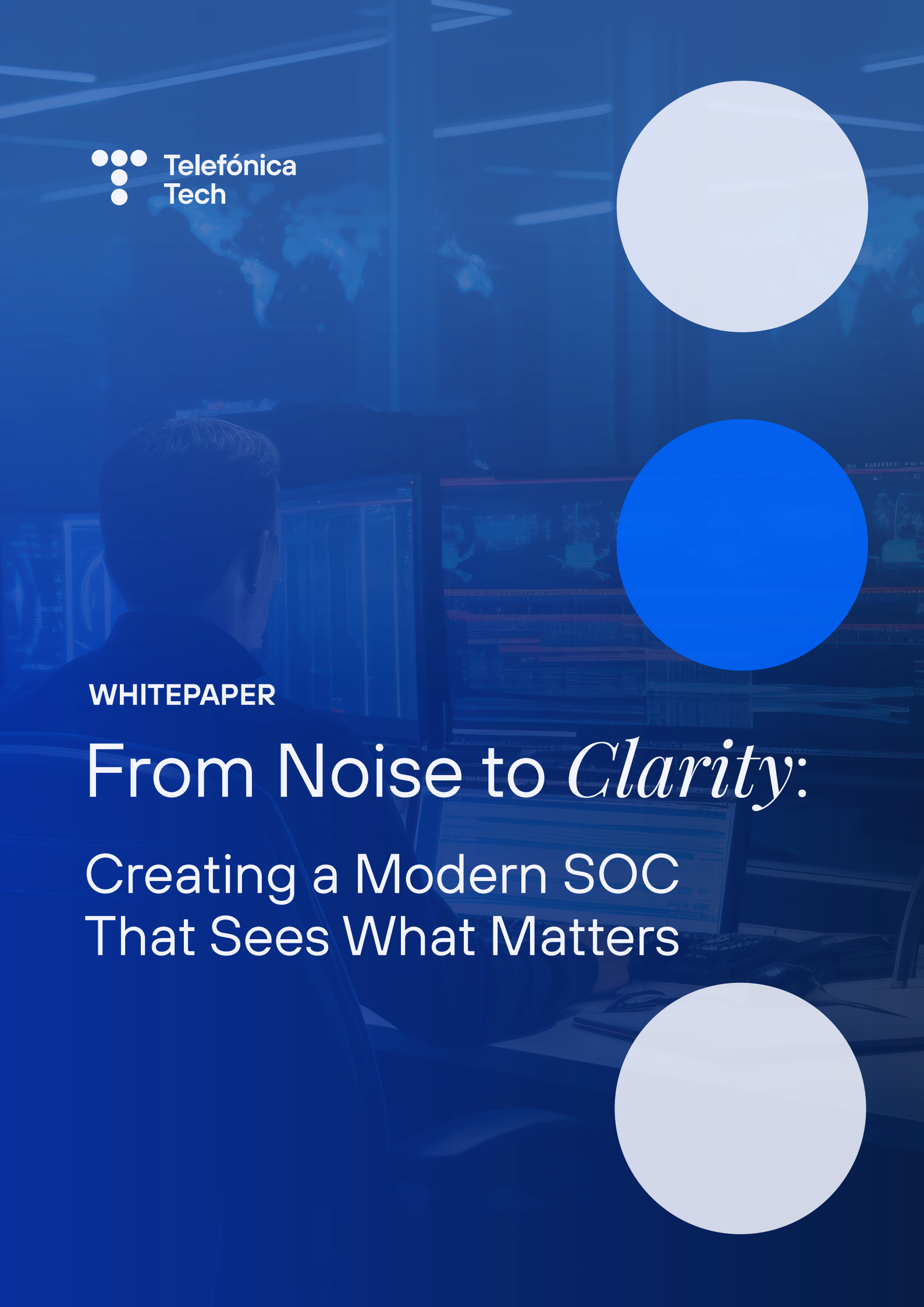


Telefónica Tech

WHITEPAPER

From Noise to *Clarity*:

Creating a Modern SOC That Sees What Matters

EXECUTIVE SUMMARY

Security leaders today face a paradox: overwhelmed by endless alerts yet blind to the most critical threats. Traditional Security Operations Centres (SOCs) drown teams in false positives, siloed data, and manual processes, leaving true risks hidden in plain sight.

Many organisations hesitate to change, fearing disruption and complexity. While many existing SOCs still serve a vital purpose, without modernisation they may struggle to keep pace with today's evolving threat landscape and growing compliance demands. Telefónica Tech's guide provides a practical, proven framework to help you advance your SOC with clarity, flexibility and measurable outcomes.

Discover how top organisations adopting modern SIEM solutions like Microsoft Sentinel achieved:

50%
reduction in alert volumes

44%
cost savings compared to on-premises SIEMs

35%
lower risk of data breaches

Up to
234%
return on investment (ROI)

40%
improvement in analyst productivity

50%
faster incident response times

This was achieved by following a modular, maturity-aligned approach tailored to evolving business needs.

Too Much Noise. Not Enough Insight.

Modernise your SOC to see clearly, act faster, and defend smarter.

INDEX

01

THE CASE FOR SOC MODERNISATION

The cyber security landscape is evolving rapidly. IT, OT, hybrid and multi-cloud environments converge, while remote work remains permanent. Attackers leverage AI, nation-state resources, and ransomware tactics to breach defences. Meanwhile, boards, regulators, and insurers demand SOCs be demonstrably effective, resilient, and cost-efficient.

Traditional SIEMs and SOCs, often built on siloed, reactive systems, fail to meet these demands. They produce noise, drain resources, and leave critical threats undiscovered. Yet many organisations are understandably wary of change, fearing disruption or complexity.

Partnering with a managed security services provider like Telefónica Tech can mitigate these risks, offering a scalable, safe, and strategic path to SOC modernisation.

02

WHAT A MODERN SOC LOOKS LIKE

A modern SOC is a strategic function, not just dashboards. It delivers continuous visibility, adaptive defence, and trusted outcomes across environments.

Key attributes:

- Unified visibility across cloud, on-premises, endpoints, identity, and borderless environments including IoT, BYOD, and third-party access.
- AI and automation for triage, enrichment, and response at machine speed
- Modular architecture adapting as business and threats evolve
- Integrated threat intelligence prioritising critical risks
- Governance and compliance built into every workflow

Outcomes to aim for:

- Reduced Mean Time to Detect (MTTD) and Respond (MTTR)
- Fewer false positives and reduced analyst burnout
- Improved regulatory reporting and audit readiness
- Increased cost-efficiency through smarter resource use and automation
- Greater confidence from stakeholders and regulators

03

CHOOSING THE RIGHT MODERNISATION PATH

SOC modernisation is a continuum, and not a one-size fits all project. Align your approach to your current capabilities and ambitions.

Considerations:

- Are you targeting 24/7 response or enhanced triage?
- Do you have internal security engineering capacity?
- How important is cost predictability and tool control?

Deployment models:

- In-house: Full control, high resource demands
- Co-managed: Shared responsibility with expert oversight
- Fully managed: SLA-based, scalable with minimal internal lift

Moving to a modern SIEM like Microsoft Sentinel typically reduces data breach risk by **35%** compared to traditional on-premises solutions.

04

THE HIDDEN PITFALLS OF SOC PROJECTS

Most SOC projects fail not due to tools, but poor planning:

- Tech-first decisions without defined outcomes
- Rigid licensing leading to lock-in or underuse
- Alert fatigue due to noise and poor workflows
- Misalignment between security, IT ops, and risk teams
- Unclear risk ownership and lack of accountability for resolution

05

PLANNING FOR EVOLUTION, NOT JUST IMPLEMENTATION

Your SOC isn't defined by what you deploy today, but how it evolves.

Planning principles:

- Design for scalability, not just quick wins
- Prioritise people and processes before tools
- Build governance checkpoints and continuous improvement loops

06

FROM NOISE TO INSIGHT: MAKING YOUR SOC OPERATIONAL

Deploying platforms is only step one. Real value lies in operationalising, turning alerts into actionable insights.

Planning principles:

- Alert correlation and triage workflows
- Automated playbooks for common threats
- Integrating threat intelligence and compliance
- Metrics: dwell time, incident impact, threat reduction

Implementing automated playbooks typically sees a **40%** drop in alert volume and **20%** faster threat resolution.

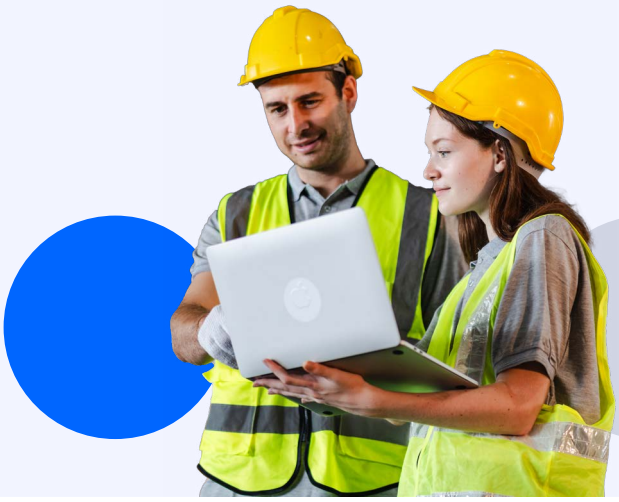
CASE STUDY

Sentinel-First Professional Services Deployment for a UK Utility Provider

Telefónica Tech partnered with a major UK utility provider to deploy a Microsoft Sentinel and SOAR solution across their converged IT and OT environments. This professional services engagement delivered:

- Seamless integration within the customer's own Microsoft subscription, ensuring IP ownership and compliance
- A dedicated virtual SOC team with Level 1-3 analysts and architects embedded onsite
- AI-driven automation to accelerate threat detection and response
- Service Integration and Management (SIAM) governance ensuring operational continuity
- UK-based service delivery meeting stringent regulatory requirements

This deployment demonstrates how modern SOC evolution requires tailored professional services and expert operationalisation, not just technology adoption.



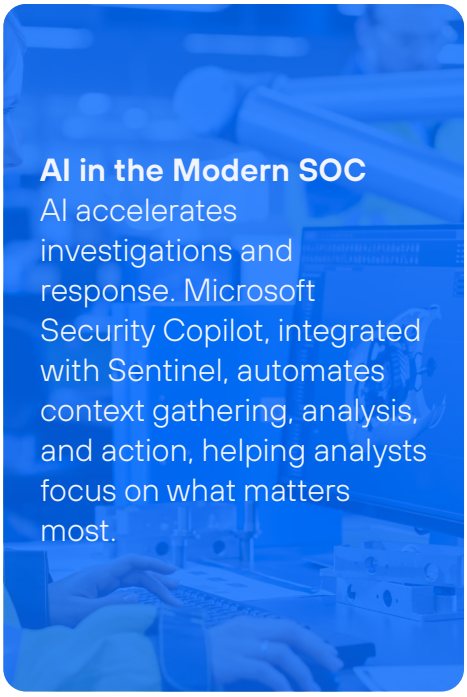
07

MICROSOFT SENTINEL SPOTLIGHT: A MODERN, SCALABLE SOC SOLUTION

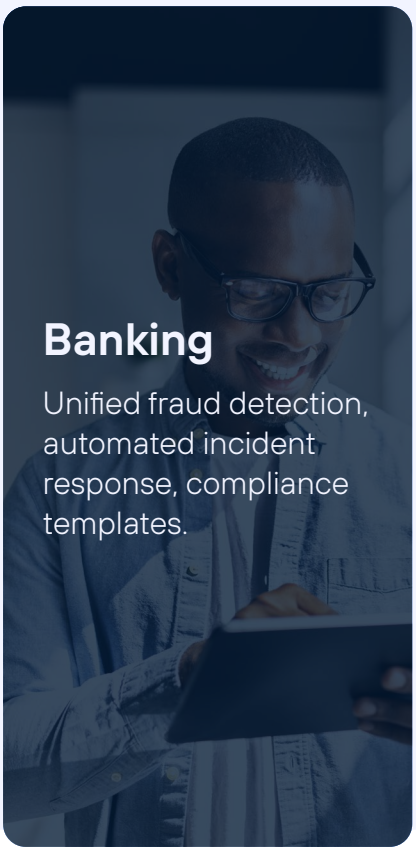
Microsoft Sentinel is a cloud-native SIEM and SOAR platform unifying threat intelligence, incident management, and automation for efficient, strategic security operations.

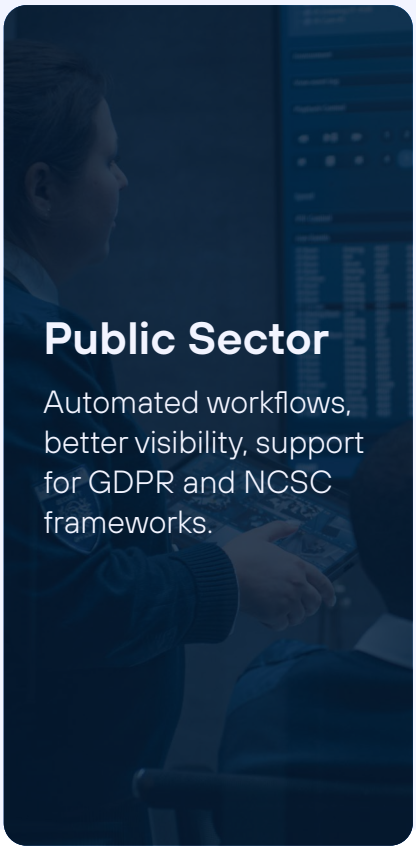
Benefits

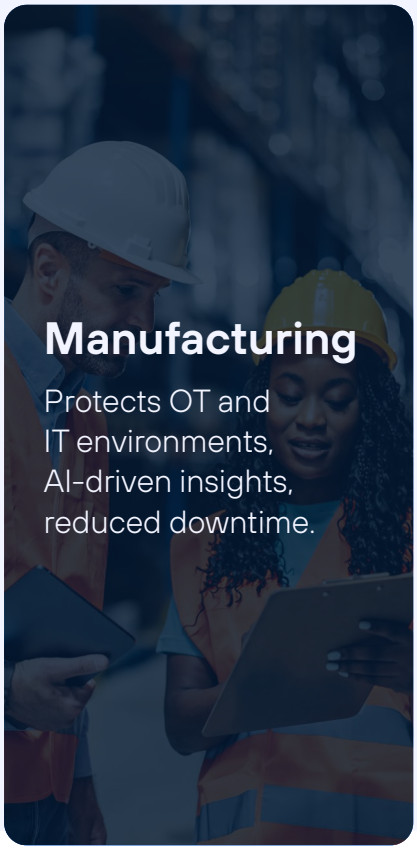
- Supports hybrid, multi-cloud, on-premises with 350+ connectors
- Up to 44% cost reduction, 35% lower breach risk, and 234% ROI potential
- Native SOAR automates triage and response
- Flexible and scalable for cloud-first organisations



Sentinel Sector Snapshots







08

TRADITIONAL SOC VS. MODERN SOC SOLUTION

Category	Tradtional SOC	Modern SOC (eg Microsoft Sentinel)
Visibility	Fragmented	Unified IT, OT, Hybrid, multi-cloud
Threat Detection	Manual, reactive	AI-powereed, proactive
Indicient Response	Slow, manual	Automated playbooks, rapid containment
Operational Overhead	High, duplicated efforts	Streamlined, automated
Scalability	Limited, rigid	Cloud-native, scalable
Skill Gaps & Efficiency	Analyst burnout, silos	Built-in AI guidance (Security Copilot)
Cost Effectiveness	High upfront and ongoing costs	Lower TCO, pay-as-you-go model

09

HOW TELEFÓNICA TECH CAN SUPPORT YOUR JOURNEY

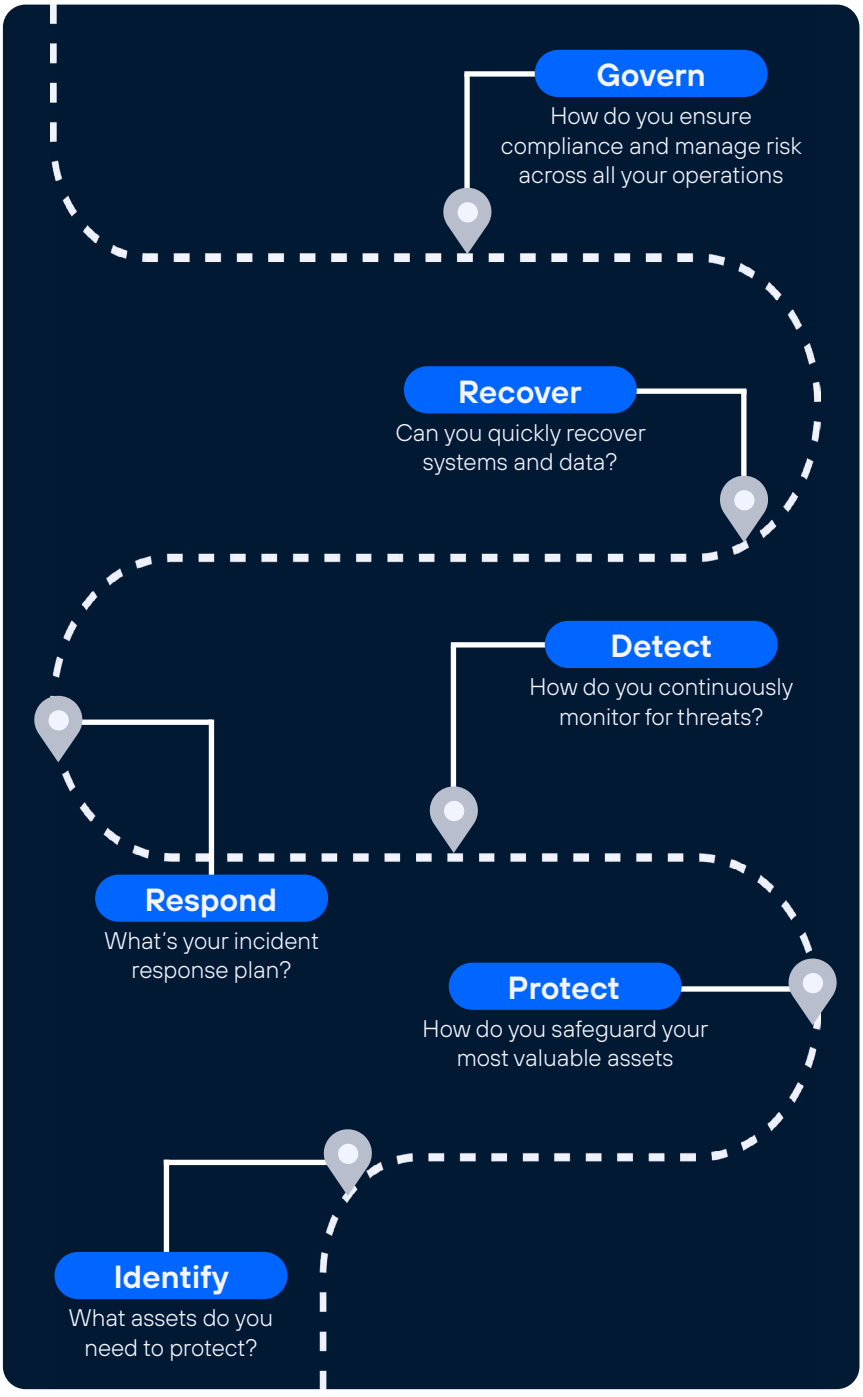
Telefónica Tech under our NextDefense managed security and support services guide organisations at every stage, from advisory to fully managed SOCs and beyond.

NextDefense

Cyber security isn't a destination but a **continuous journey**

We provide you with the insights to take the right action at the right time.

NextDefense is NIST-aligned.



NEXTDEFENSE: SIEM MANAGEMENT

Overview

NextDefense is Telefónica Tech UK's end-to-end security operations service designed to help organisations strengthen cyber resilience through expert-managed SIEM, SOAR, and advanced threat intelligence.

We combine cloud-native capabilities including Microsoft Sentinel with UK-based specialist teams to provide continuous monitoring, rapid incident response, and proactive threat hunting. All are tailored to your unique IT and operational technology environments.

Our Services includes:

24/7 UK-based SOC Monitoring & Incident Response
Certified analysts deliver real-time threat detection and swift, effective responses.

Seamless Microsoft Sentinel & SOAR Deployment
Customised implementation and orchestration automate incident workflows, enhancing efficiency and control.

Proprietary Cyber Threat Intelligence
Telefónica Tech's unique threat feeds and AI-driven analytics augment Sentinel's capabilities for better risk mitigation.

Flexible Delivery Models
From co-managed to fully managed services, adapted to your scale and operational needs.

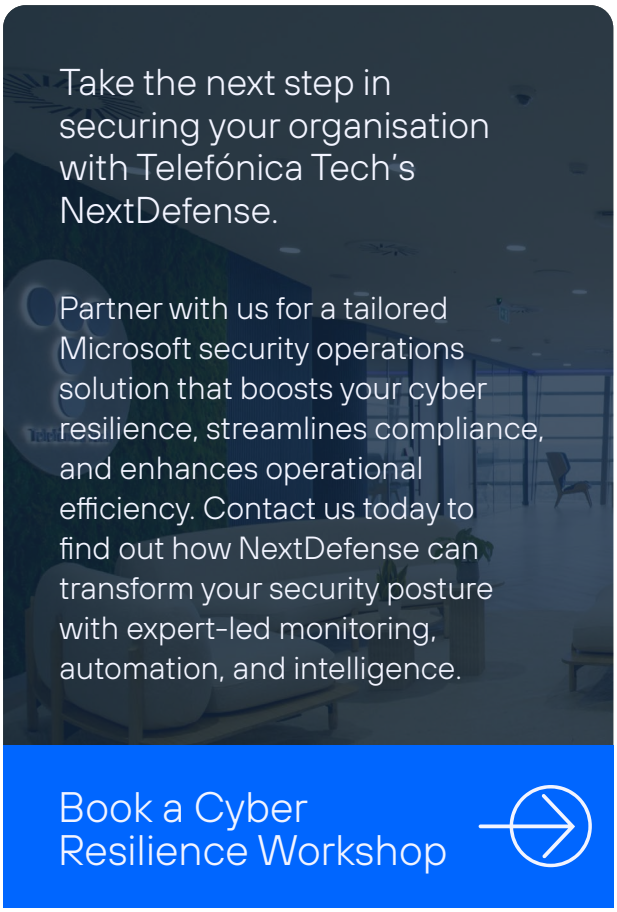
Governance & Compliance Support
Aligns with UK and global standards, easing audit and regulatory requirements.

Strategic Professional Services
Expert consultancy and deployment for complex environments, critical infrastructure, and OT/IT convergence.

WHY TELEFÓNICA TECH UK?

- Microsoft Azure Expert MSP with proven expertise across cloud-native security tools and Sentinel-first architectures.
- Deep experience securing UK critical infrastructure by integrating corporate IT and OT environments.
- Synergies with TELCO-grade network intelligence and global collaboration for enhanced threat context.
- Cost-efficient solutions that optimise analyst workloads and improve operational visibility.

Source: Commissioned study by Forrester Consulting, "The Total Economic Impact™ of Microsoft Azure Sentinel," November 2020. Results based on composite organisations.



Take the next step in securing your organisation with Telefónica Tech's NextDefense.

Partner with us for a tailored Microsoft security operations solution that boosts your cyber resilience, streamlines compliance, and enhances operational efficiency. Contact us today to find out how NextDefense can transform your security posture with expert-led monitoring, automation, and intelligence.

Book a Cyber Resilience Workshop

Leading the Way in *Digital Transformation* for our Customers

Telefónica Tech unlocks the power of integrated technology, bringing together a unique combination of the best people, with the best tech and the best platforms, supported by a dynamic partner ecosystem to make a real difference to every business, every day.

T: 0333 188 7868 | info@telefonicatech.uk | telefonicatech.uk