Microsoft Sentinel Accelerator

Telefónica Tech combine our extensive experience as a Microsoft Azure Expert MSP, with established cyber security and SOC services, to provide a flexible portfolio of services for Microsoft Sentinel.

We ensure that you can rapidly provision a Sentinel environment to our best practice standard – in hours, not weeks.

Our Microsoft Sentinel support services then help you to maximise your investment in Sentinel – from simple support, through to a fully managed detection and response service.

Deploy a Microsoft Sentinel Platform to best practice standards in hours, not weeks:

- Solution Design – standardised definition of analytics rules and governance against Microsoft and Telefónica Tech's best practice
- Accelerated Deployment – rapid provisioning of your environment using orchestrated automation
- Optional enrolment into Telefonica Tech essentials support or full MDR services

Delivered by Telefónica Tech's team of global cyber security and cloud experts.

Background

Organisations are aware of the increase in cyber risk and the importance of having a strong IT security capability. Being able to rapidly identify and respond to potential threats is critical, and is the main reason we have seen the huge surge in demand for SIEM and SOAR products, as well as advanced managed security services from MSSPs.

Microsoft's Sentinel platform has become the prevalent SIEM & SOAR technology for enterprise IT

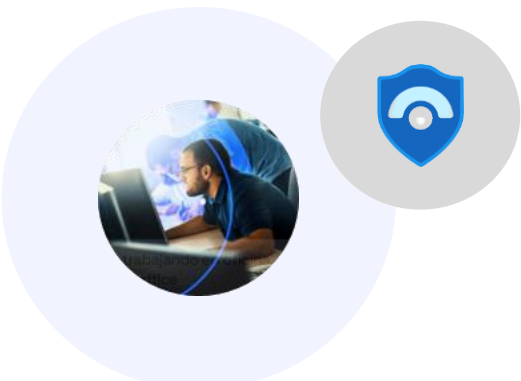
- More than just a SIEM platform – Sentinel also provides SOAR functionality to allow your organisation to respond to security threats in real-time and through automation.
- Comprehensive threat intelligence through Microsoft's and Telefónica Techs combined threat research
- Seamless integration with the common platforms – Sentinel integrates with Windows, M365, Defender, Azure and many other vendors' technology
- Free log source consumption - for many Microsoft services such as M365 and Defender for Endpoint, the costs for analysing logs are free, reducing the overall SIEM TCO.
- Commercially competitive vs similar services - if deployed and managed correctly.

The Challenges in Deploying Microsoft Sentinel?

- Not having the available skills – Microsoft Sentinel deployments require a broad set of skills, including security, infrastructure, and cloud.

  Lacking these skills can lead to;

- Expensive and extensive deployments – projects taking months to deploy and see value
- Inconsistent and poor quality deployments – like any cloud (or IT service), poor configuration often results in a poor quality service. For any SIEM platform, it is critical that the 'right' alerts are picked up and responded to.



What is Telefónica Tech's 'Microsoft Sentinel Accelerator'?

The Microsoft Sentinel Accelerator is a unique service package, combining Telefónica Tech's advanced automation and leading Microsoft Azure and IT security professional services capabilities.

The service helps clients rapidly deploy Microsoft Sentinel to Microsoft and Telefónica Tech's combined best practice standard.

How do we deliver the service?

	Consultancy	Automated Deployment
Kick Off		
Solution overview & pre-requisites	✓	
Confirmation of requirements, scope & deliverables	✓	
Deployment approach, timings and scheduling	✓	
Design		
Provision of standard product design elements - Sentinel Configuration - Analytics Rules & Data Collection	✓	
Provision of standard product design elements - Governance, including Access Control, Deployment and Management, Naming Conventions & Consumption Costs	✓	
Deployment		
Creation of Azure DevOps Project, Service Connection and IaC, Rules, and Wiki Repositories		✓
Deployment of Azure resources - Including Automation Account, Log Analytics, Sentinel, Azure Policy		✓
Azure Resource Monitoring - Deploy User Assigned Identities to facilitate Azure Resource sentinel Coverage		✓
Enable monitoring - Deploy Defender for Cloud, configure diagnostics, M365 monitoring config		✓
Create Sentinel Analytics rules from templates		✓
Connect on premises Windows Servers (using Arc)	✓	
Connect on premises Security Appliances and Linux servers	✓	
Testing		
Operationally test and provide 'End of Test' report	✓	✓
Solution Handover		
Remote handover session – walkthrough core components, log source onboarding processes, alert tuning processes.		✓

Who is it for?

Our Microsoft Sentinel Accelerator can be used whether you're looking to deploy Microsoft Sentinel and manage it yourselves. Or, if you're looking to deploy Microsoft Sentinel and have it managed by Telefónica Tech, either as part of our Essentials support service, or with a full Managed Detection and Response service.

How is it Charged?

We pass the benefits of our advanced automation on to you, and have created a fixed price engagement, inclusive of our automated delivery and professional services.

£5,000.00*

*monthly Azure charges will be based on consumption.

Why partner with Telefónica Tech UK&I?

Telefónica Tech UK&I has focused on helping customers meet their business goals with the best technology answers since the mid 1990s. By carefully listening and understanding their needs, we make the complex, simple. Our complete IT solution includes robust consultancy, innovative design, best-practice deployment, plus management & support from our government accredited UK and Ireland Data Centres.