Telefónica Tech

Microsoft Sentinel

Deployment Accelerator, Support & Managed Detection and Response (MDR)

Agenda

01

Why Microsoft Sentinel?

02

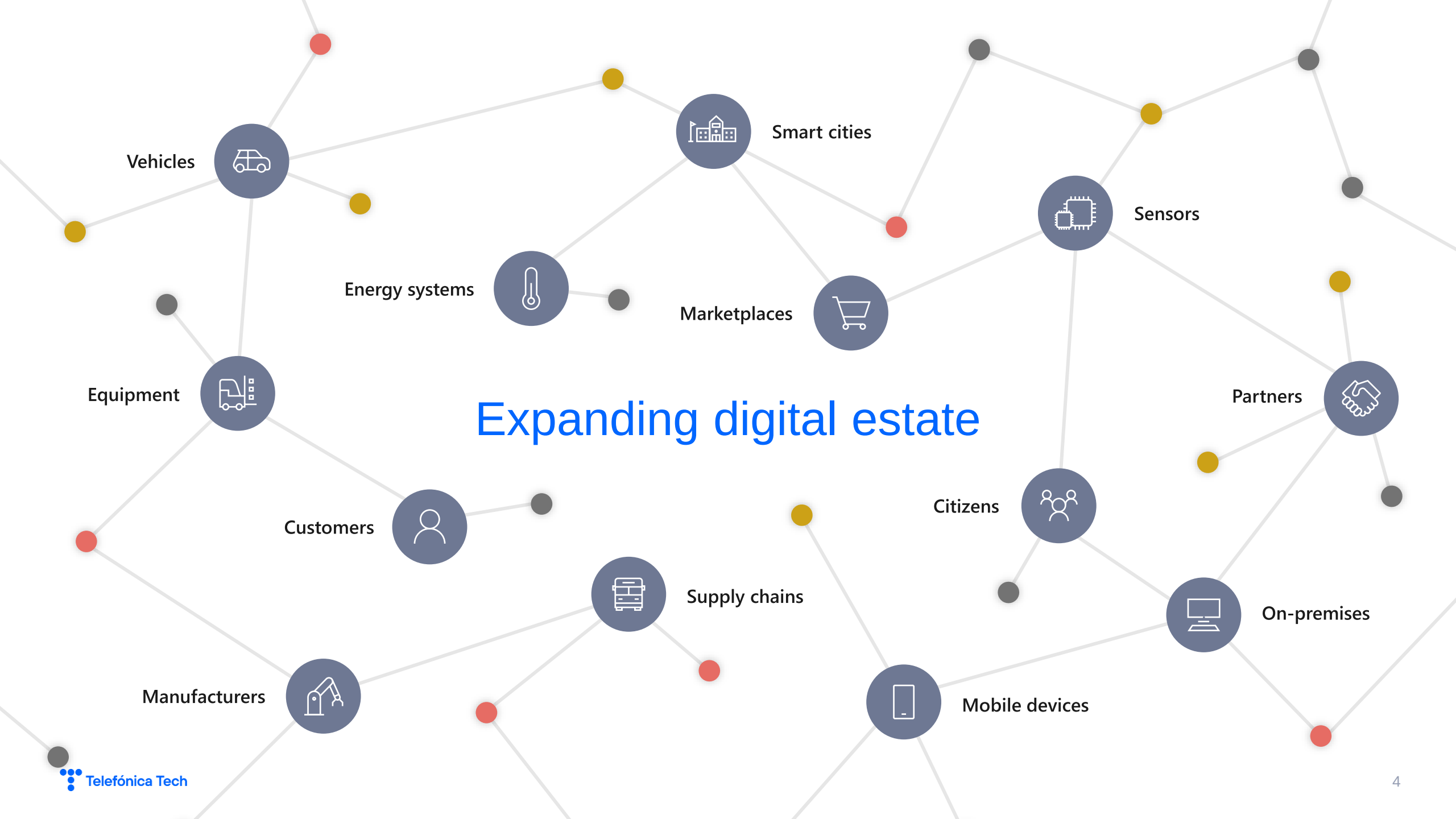
How can we help?

03

Commercials

Why Microsoft Sentinel

01



Expanding digital estate

Security operations challenges

76% report increasing security data*

Sophistication of threats

IT deployment and maintenance

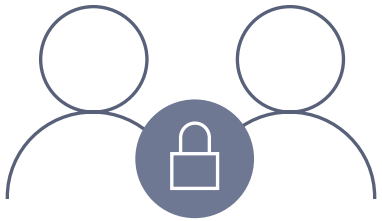
44% of alerts are never investigated*

Too many disconnected products

3.5M unfilled security jobs in 2021**

Lack of automation

*ESG: Security Analytics and Operations: Industry Trends in the Era of Cloud Computing 2019
**CSO Magazine



Security
Operations Team

+

Cloud + Artificial Intelligence

Microsoft Sentinel

Optimise security operations with cloud-native SIEM & SOAR powered by AI & automation

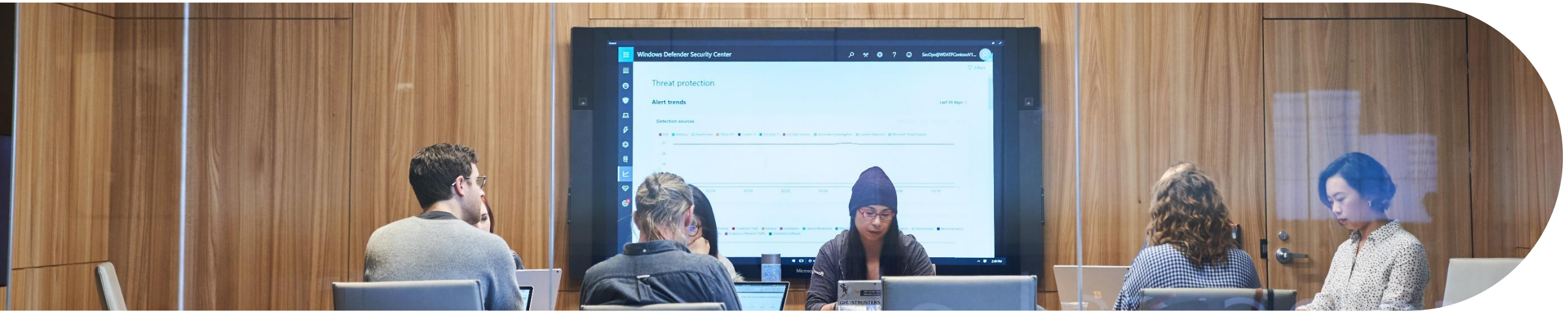
Harness the scale of the cloud

Detect evolving threats

Expedite incident response

Get ahead of attackers

An empowered SecOps team:



48%
less expensive compared to legacy SIEMs

79%
decrease in false positives over three years

67%
decrease in time to deployment with pre-built SIEM content and out-of-the box functionality

56%
reduction in management effort for infrastructure and SIEM

80%
reduction in investigation labor effort

201%
ROI over 3 years

Forrester Consulting, Total Economic Impact™ of Microsoft Sentinel, 2020

Microsoft Sentinel—a Leader in the Forrester Wave™: Security Analytics Platform

"**Microsoft roars into the security analytics market…**
The vendor's entry into the security analytics space captivated security buyers. Microsoft's bold move to allow the ingestion of Microsoft Azure and Microsoft Office 365 activity logs into Sentinel at no cost makes the solution attractive to enterprises invested in Azure and Microsoft 365."

- **The Forrester Wave™: Security Analytics Platforms, Q4 2020 report**

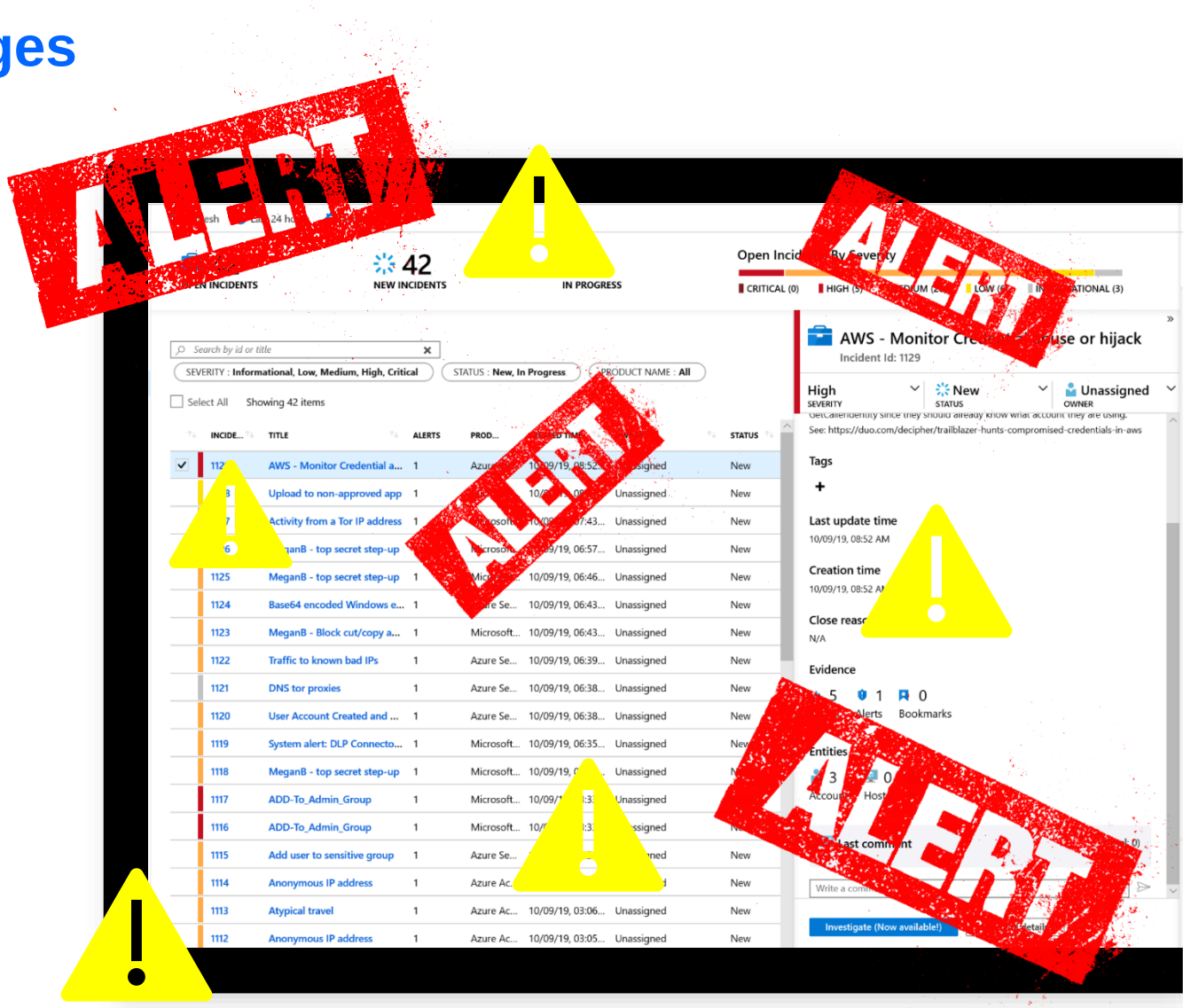
How can we help?

02

Common Microsoft Sentinel Challenges

Lack of the required hybrid skillset (Cloud, Infrastructure, & Security) resulting in:

- Expensive and extensive deployments
- Inconsistent and poor quality deployments
- No optimisation and highs rates of false positives
- Inability to analyse and respond quickly
- Inability to provide 24x7 security operations capability



How can Telefonica Tech support me with Microsoft Sentinel?

Project

Rapidly deploy a best practice Sentinel environment using Telefónica Tech's **Microsoft Sentinel Accelerator**

Deployed in CSP

Infra Support

We provide world class support for your Sentinel environment free of charge with our **Essentials Support Service**

How can Telefonica Tech support me with Microsoft Sentinel?

Full MDR Service

A fully managed SOC, with SIEM and SOAR powered by Microsoft Sentinel, using Telefónica Tech's **Managed Detection & Response (MDR) Service**

Project

Rapidly deploy a best practice Sentinel environment using Telefónica Tech's **Microsoft Sentinel Accelerator**

Deployed in CSP

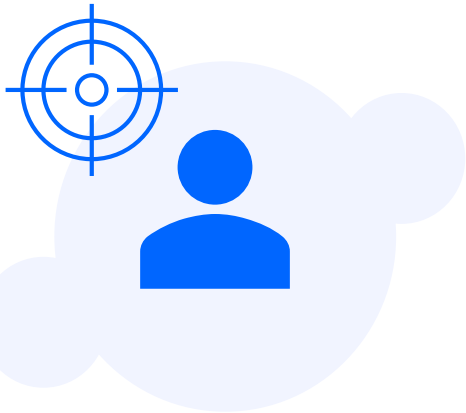
Infra Support

We provide world class support for your Sentinel environment free of charge with our **Essentials Support Service**

Which option is right for me?

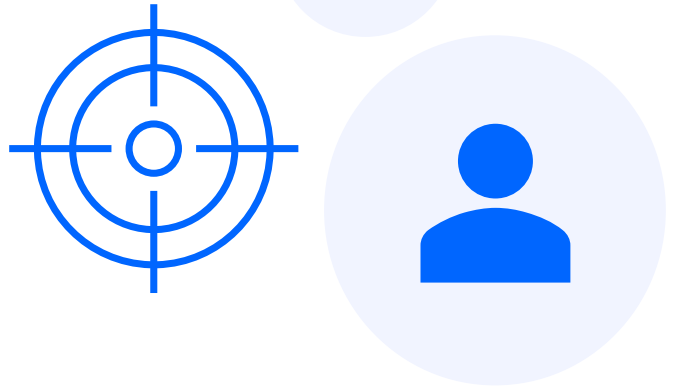
- I have a SOC & cloud skills.
- I want a rapid deployment of a best practice Microsoft Sentinel instance
- Deployed into CSP and uplifted to ‘Essentials Support’ unless otherwise specified

Choose our Sentinel Accelerator Service



- I have a SOC & cloud skills.
- I want to purchase Sentinel services from Telefónica Tech, and be able to ask advice / log support calls
- I want a rapid deployment of a best practice Microsoft Sentinel instance

Choose our Sentinel Accelerator + Essentials Support Service

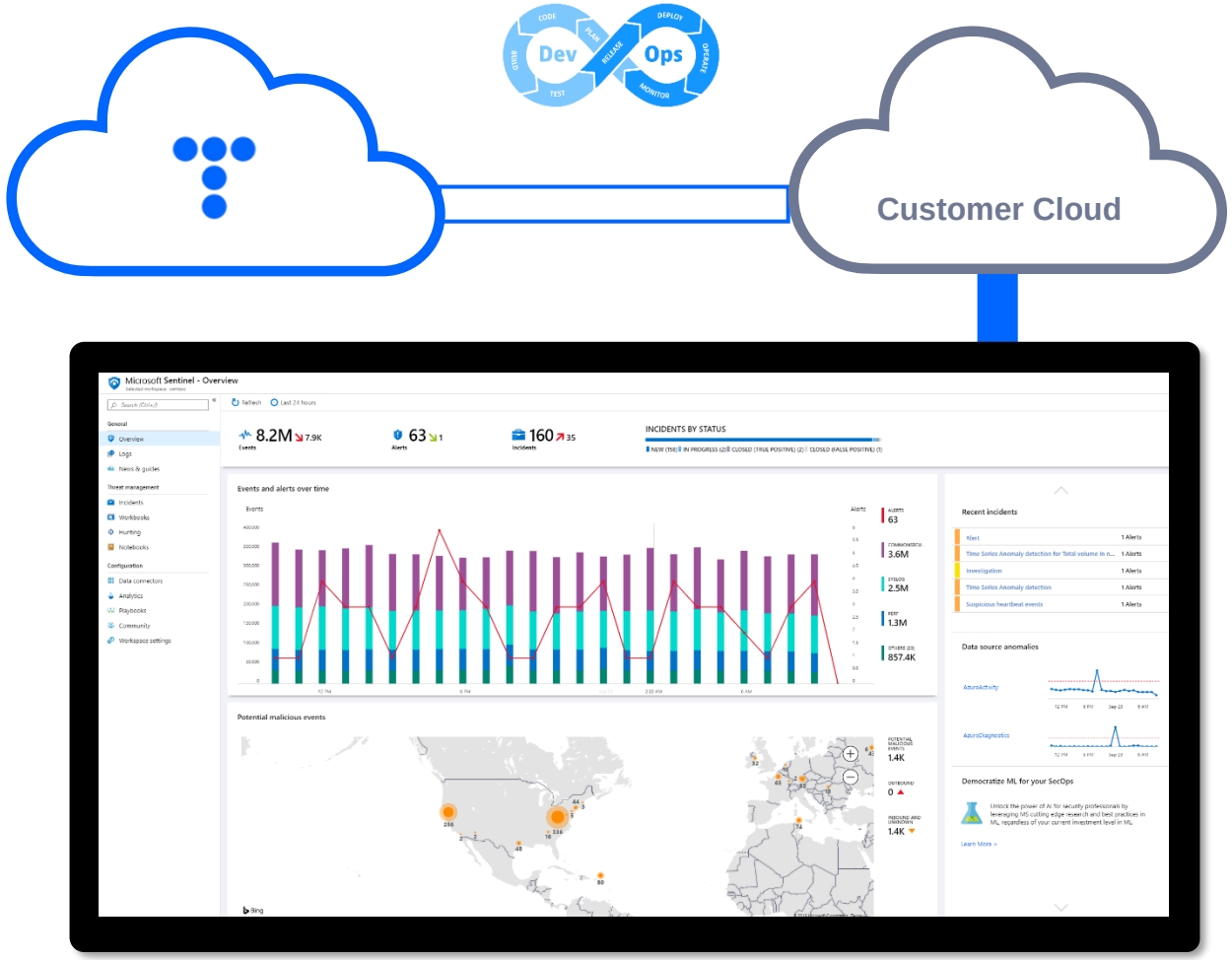


- I want a fully managed SIEM and SOC service
- I want Telefónica Tech to be responsible for detecting and responding to security events
- I want best practice for my Microsoft Sentinel instance and management of Azure and Sentinel

Choose our Managed Detection & Response Service

Microsoft Sentinel Accelerator

- Codified Best practice design – a best practice design of Microsoft Sentinel defined as code
- Deployed through our orchestrated automation – Deployed in hours, not weeks
- Flexible deployment – installed in your Azure subscription or in a subscription provided and supported by us
- Overseen by experts – The automated delivery model doesn't replace our people, it just means we work smarter.



What's included with the Sentinel Accelerator?

	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.		✓

Service/product features are subject to change, latest features can be found in the Service Description documentation

Essentials Support Service

- ***No charge*** – included when you purchase your Azure consumption from Telefonica Tech
- Deployed through our Sentinel Accelerator using orchestrated automation
- Deployment of standard threat hunting rules
- Support is on hand – Telefónica Tech are here to help with issues and escalations for both Azure and Microsoft Sentinel

	Essentials
Sentinel Deployment	Automated - using Telefónica Tech's IP
Azure and Sentinel Tenancy	Provided by Telefonica Tech
Azure Support and Management	Client Responsibility, with escalation and support provided by Telefónica Tech
Optimisation	Client Responsibility
Threat Hunting Rules	Microsoft Sentinel security standard analytics and correlation rules
SOC - Incident Detection	Client Responsibility
SOC - Incident Response	Client Responsibility
SOC - Incident Resolution	Client Responsibility

Managed detection and response (MDR)

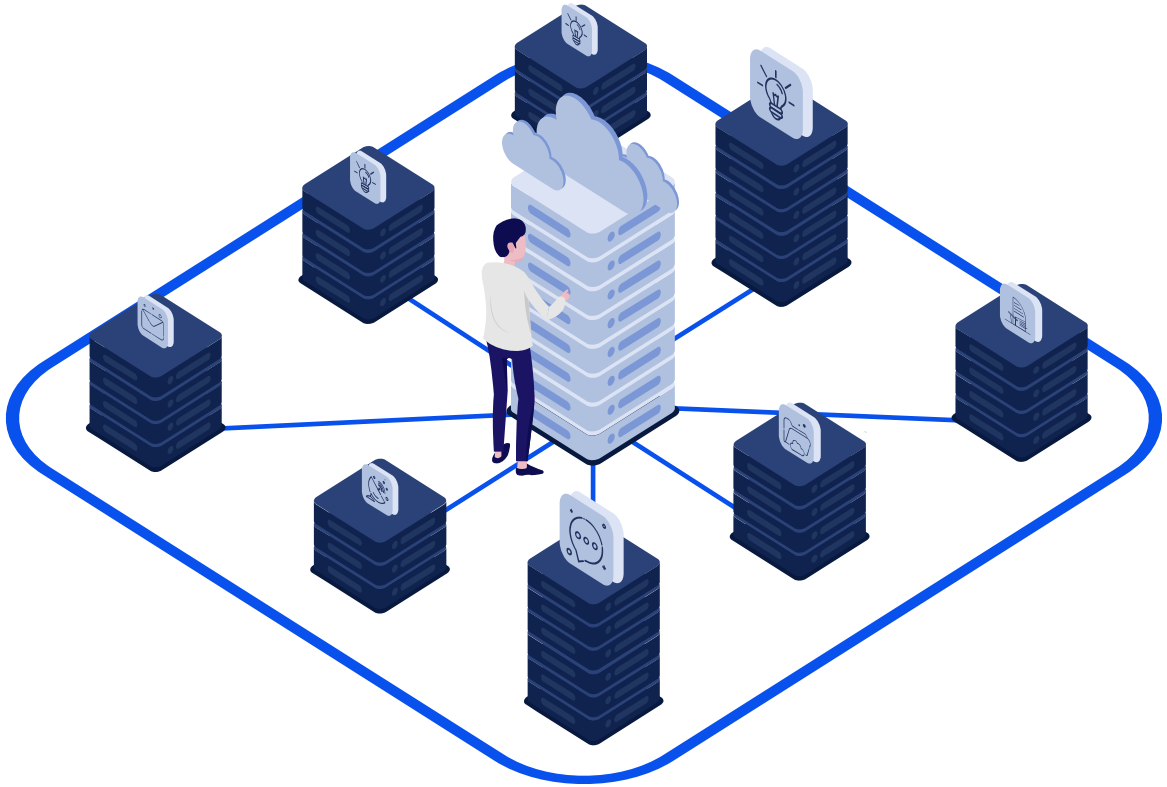
- A fully managed SOC, with SIEM and SOAR powered by Microsoft Sentinel
- Accelerated Deployment - as with Sentinel Accelerator
- Fully managed – Telefónica Tech is responsible for managing and optimising your Azure environment and Sentinel platform
- Managed Detection and Response – our 24x7 SOC detect and respond to all issues identified by Sentinel

	MDR
Sentinel Deployment	Automated - using Telefónica Tech's IP
Azure and Sentinel Tenancy	Provided by Telefónica Tech or another party
Azure Support and Management	Managed by Telefónica Tech
Optimisation	Managed by Telefónica Tech
Threat Hunting Rules	Access to Telefónica Tech's Custom Rulesets
SOC - Incident Detection	Managed by Telefónica Tech
SOC - Incident Response	Managed by Telefónica Tech
SOC - Incident Resolution	Client Responsibility (unless provided under additional contracted service with Telefónica Tech)

Managed Detection and Response Explained

“Minimise your risks without the upfront investment needed to build and operate your own SOC”

- Integration, management and review of traffic feeds
- Correlation management, SIEM and SOAR tuning
- Proactive and protective monitoring services
- Initial triage and analysis
- Vulnerability management
- Alerting and response
- Incident management
- Root cause analysis
- Continuous improvement
- Remediation escalation to onsite team



OUR SOLUTION

What is the goal of a Managed Detect and Response Service?

Speed of Detection

masses of tools and devices. f/ws, endpoint detection, email filtering, application access – vast amount of data. Need to make sense of it and act fast.

Capability

Requires skilled people across multiple disciplines to identify and tune, analyse, defend, investigate and report.

Visibility

Correlation/big picture. Without it, you may miss an attackers movements, not know how far they've gone. Detecting complex attacks without it is very difficult.

On-going Security Posture

Business and technology leaders are worried by what they can't see. Helps to give hour-by-hour security posture.

Speed of Response

Going to Google not the answer. Need to have experienced analysts, playbooks and a degree of automation and orchestration and need to react fast.

Collaborate

Cyber criminal community do it. Why wouldn't legitimate businesses?

Comparing our Sentinel services

	Sentinel Accelerator	Essentials Support	Full MDR
Sentinel Deployment	Automated - using Telefónica Tech's IP	Automated - using Telefónica Tech's IP	Automated - using Telefónica Tech's IP
Azure and Sentinel Tenancy	Provided by Telefónica Tech (default) or another party	Provided by Telefónica Tech	Provided by Telefónica Tech (default) or another party
Azure Support and Management	Client Responsibility	Client Responsibility, with escalation and support provided by Telefónica Tech	Managed by Telefónica Tech
Optimisation	N/A	Client Responsibility	Managed by Telefónica Tech
Threat Hunting Rules	N/A	Microsoft Sentinel security standard analytics and correlation rules	Access to Telefonica Tech's Custom Rulesets
SOC - Incident Detection	Client Responsibility	Client Responsibility	Managed by Telefónica Tech
SOC - Incident Response	Client Responsibility	Client Responsibility	Managed by Telefónica Tech
SOC - Incident Resolution	Client Responsibility	Client Responsibility	Client Responsibility (unless provided under additional contracted service with Telefónica Tech)

Service/product features are subject to change, latest features can be found in the Service Description documentation

Commercials

03

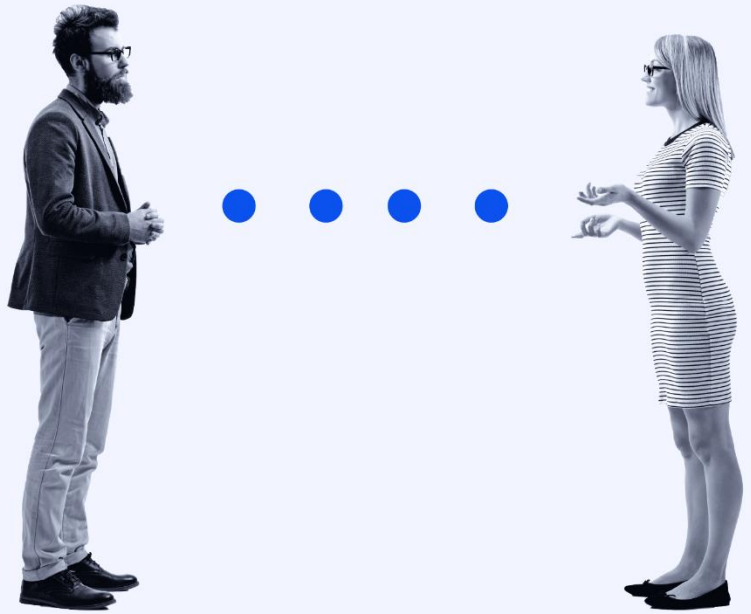
How are the services charged?

Our simple and competitive commercial model is split into three areas:

- **One time costs -** A fixed cost of **£5,000.00** for the accelerated deployment of Sentinel (included with the MDR service)

- **Microsoft Billing -** Charges are based on your log consumption and consumption of other services

- **Support and Management**
  - **Essentials Support** – No additional charge, included with your CSP billing
  - **Full MDR** – a monthly charge, calculated based on the number of log sources and users



Charging comparison

	Sentinel Accelerator	Essentials Support	Full MDR
One Time Deployment Charge?	One time, fixed cost - £5,000.00	One time, fixed cost - £5,000.00	Included in the MDR service charge
Recurring Charge	EA / CSP charges based on consumption	Included in EA / CSP charges	Monthly charge
How is it charged?	Fixed price deployment Microsoft billing is based on consumption	Fixed price deployment Microsoft billing is based on consumption Monthly service is included as part of your CSP consumption	Microsoft Billing is based on consumption Service charge based on assets in scope (per source and per user)
What commitment do I need to make?	One time charge and monthly charge in-line with your CSP consumption	One time charge and monthly charge in-line with your CSP consumption	12 months

Pricing is subject to change, latest pricing can be found in the Service Description documentation

Summary

A range of innovative and flexible offerings for deploying and managing Microsoft Sentinel

- Use our Sentinel Accelerator to deploy a best practise solution in hours, not weeks
- Use our Flexible support options:
  - Essentials Support for infrastructure support
  - Managed Detection and Response service for a fully managed SOC with SIEM and SOAR
- Delivered by a global team of cyber security and cloud experts


Telefónica Tech