Telefónica Tech

Microsoft Sentinel

Cyber

telefonicatech.uk

Service Overview

Monitoring and correlation of security events with 24x7 alert management, providing a solid foundation in security threat detection through our global use case catalogue, SOAR and threat intelligence platform. Our managed Microsoft Sentinel solution is the core for a Security Operations Centre (SOC). This service enables continuous 24/7 threat monitoring and detection across your organisation.

This service aims to expand detection and response capabilities through continuous monitoring and correlation of events, logs and alerts in the customer's IT environment. This provides visibility of the security status, as well as support to security teams in case of any threat detected. Providing a service with high levels of automation in the detection of security anomalies and cyber threats.

End-to-end Management – Our teams are responsible for the delivery, configuration, deployment, and installation of SIEM solutions, providing close guidance and support to the customer's IT teams throughout the process.

Proactive Threat Hunting – Our most experienced analysts leverage the latest information on TTPs, vulnerabilities, and IoCs to identify overlooked threats.

24/7 monitoring and detection – Including triage, analysis and elimination of false positives, as well as remote escalation of any confirmed threat under orchestrated procedures.

Detection & Customisation – Extensive correlation and aggregation catalogue with a customised implementation adapted to the customer's assets and processes, supported by experts maintaining an up-to-date environment with customised information.

Benefits:

Adopt next-generation SIEM technology from Microsoft, delivering intelligent security analytics across the enterprise.

Expand security capacity over on-premise, cloud and hybrid environments, obtaining a global monitoring vision and reducing security risks.

Increase detection capabilities and response times efficiently and continuously through teams of 24/7 expert analysts and enriched intelligence.

Full integration with in-house SOAR automation, ticketing, threat intelligence and customer portal capabilities.

Our Deliverables:

- End-to-end Management
- Proactive Threat Hunting
- 24/7 monitoring and detection
- Detection & Customisation

Why Telefónica Tech?

1. Our Propel method gets you from idea to working solution fast. This lets you unlock value quickly from your modernisation initiatives.
2. We have deep expertise across the full app stack with proven customised solutions that speed your modernisation.
3. We help you adopt change with less risk and disruption, using modular delivery that keeps compliance and quality high.

We focus on high-value apps and features that deliver clear business impact.

Additional Services to Elevate Your Business

Cyber Threat Intelligence (CTI).
Helps organisations understand digital risks, providing a strategic advantage for better identification and anticipation against threats.

- Prevention increases the number of prevented intrusions and the number and impact of patched vulnerabilities.
- Detection increases the number of detections and positive alerts, also reducing false positives, while reducing the time spent on each alert.
- Response reduces the mean time to detection (MTTD), facilitating the discovery of a greater number of incidents and the mean time to remediation (MTTR).

Multi-Cloud
Deliver workload freedom by deploying your workloads across multiple cloud providers seamlessly.

Cloud Managed Services
Expert management and support for your cloud environment.

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