Telefónica Tech

CASE STUDY

Protecting a leading UK Charity with a Fully Managed SIEM

telefonicatech.uk

Telefónica Tech

CASE STUDY

Improved Visibility of Security

As part of a UK charity's continuous efforts to improve their cyber security, they sought the assistance of Telefónica Tech to deploy a Security Information and Event Management (SIEM) solution. With our expert assistance and Sentinel Accelerator, they swiftly established a SIEM solution, gaining improved oversight of their entire IT setup.

THE CHALLENGE – RAPID SIEM DEPLOYMENT

Telefónica Tech's Sentinel Accelerator provided the charity with a fast and effective SIEM solution. As their trusted Microsoft Cloud Solution provider, Telefónica Tech used their deep understanding of the charity's existing IT to deliver a powerful cloud-based security suite.

MANAGED SIEM

COST EFFECTIVE

IMPROVED VISIBILITY

T: 0845 605 2100 | info@telefonicatech.co.uk | telefonicatech.uk

THE SOLUTION - GREATER THREAT PROTECTION WITH SENTINEL

Typically, setting up a SIEM system can take anywhere from 3 to 6 weeks. But with our in-house Sentinel Accelerator solution, our skilled team was able to install a SIEM exceptionally quickly. This was made possible by our seamless API connection to the customer's environment. Throughout the deployment, we meticulously ensured there were no conflicts or problems. After rigorous testing and validation, we successfully completed the installation. Our meticulous preparation, which involved thorough requirement checks and our deep understanding of the charity's Azure environment, paid off as we executed a seamless rollout. Subsequently, in a show-and-tell meeting, we demonstrated the flow of incoming logs and the swift creation of instances in response to issues identified within those logs.

"Telefónica Tech's SIEM solution has provided the charity with much greater visibility across our entire infrastructure. The Telefónica Tech team guided us with their knowledge and expertise, ensuring a seamless and efficient implementation.

CTO, Leading UK Charity

THE RESULTS - A BIRD'S EYE VIEW OF ACTIVITY

The charity's IT team now monitors their IT system with automatic threat alerts from Sentinel. They work closely with Telefónica Tech experts through our Managed Service, which is cost-effective and lets their IT team focus on other tasks.

To keep an organisation secure, it's vital to prevent unauthorised access due to compromised usernames and passwords. Monitoring login and authentication is crucial. For the charity, Microsoft Sentinel is ideal for reducing risks associated with M365 and hybrid identity using Azure AD and Windows Server AD.

Sentinel detects threats to specific entities and provides detailed information about who, what, where, when, and how. By ingesting logs from active sources, Sentinel acts as the charity's eyes and ears, providing a comprehensive view of all activity.

Compared to other solutions, Sentinel enables quick incident resolution. This helps the charity's team focus on developing even more advanced security.

SOLUTION OVERVIEW

A fully managed SIEM deployed using Sentinel Accelerator and protected by Telefónica Tech's Managed Service

- Enable security monitoring and response cost-effectively
- Oversight of security events across the entire network