DETECTION & RESPONSE

SIEM Management

HOW CAN TELEFÓNICA TECH HELP?

Our managed SIEM solution enables continuous threat monitoring and detection across your organisation

The high number of IT assets and heterogeneous environments in organisations requires **advanced and efficient monitoring capabilities** that enable a joint and intelligent view of threats and regulatory compliance.

Detection requires expert knowledge and advanced technologies that guarantee **automation in the detection and response to any incident** thanks to the continuous monitoring of events and logs 24/7.

Telefónica Tech provides customers with the capacity **to have a large team of experts together with the latest SIEM technologies** to obtain an **effective layer of security** in the prevention, detection and response to threats and incidents.

WHO IS THIS SERVICE FOR?

Organisations that **need to implement or expand monitoring, detection and response capabilities** and comply with industry standards and regulations but want to reduce the financial burden of personnel recruitment costs and technology purchases.

Medium to large organisations with an established SecOps capability **looking to outsource heavy workload or 24/7 monitoring** to focus their security teams on strategic, high-value activities.

Organisations **looking to develop their own long-term ad-hoc event correlation and monitoring capabilities** and choose to grow and learn from a trusted partner with SIEM expertise.

OUR VALUE PROPOSITION

Our service

Telefónica Tech's SIEM Management service aims to expand detection and response capabilities through continuous monitoring and correlation of events, logs and alerts in the client's IT environment. It offers visibility of the state of security, as well as support for security teams in the event of any threat detected or the need for monitoring to evolve.

The objective is to provide a service with great automation in the detection of security anomalies and cyber threats, eliminating the need for a team and/or its own SIEM technology, obtaining orchestration and response capabilities "As-A-Service".

What does it allow you to do?

This service will allow you to:

- **Adopt next-generation SIEM technology** from the most relevant partners in the market.
- **Expand security capacity** over all technological environments (on-premise and cloud), 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.

Benefits

End-to-end management

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

Search for threats

Our most experienced analysts leverage the latest information on TTPs, vulnerabilities and IoCs to search for unnoticed 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 and 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.

Telefónica Tech's differential value

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

Cost savings and control with a flexible model based on multi-tenant or dedicated platform.

Partner with extensive global experience and real-time proprietary threat intelligence.

TEAMS & ACHIEVEMENTS

Our team

- **+150 SIEM expert analysts**.
- **+1.500** security certifications.
- **12** Security Operations Centres and 2 Global Digital Operations Centres.

Achievements

- **+600.000** tickets handled per year.
- **+4.000** million of security events monitored per day.
- **+19** million of IoCs stored in our threat intelligence platform.
- **+16.500** monitored devices per year.

BUSINESS MODEL

SIEM Management is a service based on the delegated management of the most relevant SIEM platforms on the market, adaptable for inclusion during any stage of the service (provision, integration or operation), under a **multi-client “As-a-Service” or dedicated model.**

Depending on the amount of data ingestion (GB/Day or EPS), event sources, use cases and number of dedicated analysts, the client can flexibly adjust its monitoring and analysis needs, obtaining **a 24/7 service with advanced detection capabilities.**

RELATED PARTNERS

RSA
Microsoft
splunk>
IBM

SERVICIOS RELACIONADOS

Digital Forensics & Incident Response

Cyber-incident and cyber-crisis response solution to minimise damage and speed operational recovery.

Managed Detection & Response

Comprehensive endpoint security monitoring through 24/7 detection, containment and rapid response to security breaches with continuous Proactive Hunting and expert cyber-crisis support, based on the leading EDR and XDR technologies.

Contact us to start the digital transformation of your organization.