Security Operations Center (SOC)

[SEC]

Improves and monitors the company's cyber security posture, proactively protecting it from cyber risks

Main benefits

Safeguarding business continuity, confidentiality and reputation

S2E's SOC is the right service for evolving a company's cyber security from a reactive to a proactive approach. Through the synergy of specialized skills, processes and specific technologies, we monitor, identify and address cyber threats within the company, ensuring a structured governance of the company's infrastructure aimed at increased security, prevention and reactive response to safeguard business continuity.

Scope

The SOC service is suitable for medium and large-sized companies that provide answers to modern and evolving needs of their customers, involving an increase in the complexity and variety of their IT infrastructure, regardless of the sector in which the company operates.
The need to process sensitive data, as well as participation in high-risk markets, requires the company to equip itself with an appropriate tool to safeguard corporate information, while also complying with growing regulatory requirements.

Challenges facing companies

The digitization of the company exposes its assets to multiple cyber risks whose structured governance requires specific skills that are difficult to find on the market.
Companies live with a sense of uncertainty caused by the lack of knowledge of their vulnerabilities and the inability to predict the timing, modalities and effects of a cyber attack.
While companies are aware of the risks to which they are constantly exposed, it is difficult to justify investments in security in the eyes of investors.

The advantages offered

The SOC enables the early identification of risks, threats and vulnerabilities, reducing risk exposure and enabling timely responses to incidents. It safeguards business continuity and mitigates reputational risks due to data leaks and cyber attacks. The CISO acquires skills and resources to fulfill its role as a guarantor of corporate information security.

S2E: approach and proposed methodology

S2E's SOC is tailored to the client's IT structures, as well as its current processes and technologies. Through our team of experts, we design a structured synergetic monitoring and response process that provides for different levels of identification and analysis of detected security alerts, involving both analysts in the alert triage phase and digital forensics experts for complex incidents, with the aim of analyzing, evaluating and classifying the alerts generated by the IT infrastructure in a centralized manner, qualifying their relevance and criticality. This allows the customer to gain visibility into anomalous activities in a timely manner, correlating their causalities to identify vulnerabilities in the IT infrastructure.
Thanks to S2E's SOC, the customer gains the ability to prevent cyber attacks through vulnerability analysis, and to respond promptly to ongoing threats thanks to the real-time identification of the incident and the precise knowledge of which resources have been compromised, isolating the perimeter and circumscribing the impact surface.

Future development benefits

The main advantages of S2E's SOC are:

1. Reduction and mitigation of risks to business continuity.
2. Safeguarding corporate assets from simple and numerous attacks.
3. Reduction of the impact surface on complex and structured attacks.
4. Visibility of alerts, incidents and security events that previously went unnoticed.
5. Centralized, real-time monitoring of the entire corporate infrastructure.
6. Generation of corporate risk awareness and its dissemination throughout the company.

A SOC designed around the customer's uniqueness makes it possible to provide a security solution tailored to the company's specific needs and threats, increasing data protection and reducing the risk of breaches.

Offer model

S2E's SOC is a tailor-made managed service. Through an initial assessment aimed at understanding the resources involved in the perimeter, and their governance and functional aspects, we propose an ad-hoc solution for the implementation of the service, which guarantees both the safeguarding of the target resources, and compliance with service and intervention levels appropriate to the importance and criticality of the resources we protect.
Subsequent to the implementation phase, we manage the SOC implemented with a dedicated and continuously supported team, so that the company is safeguarded without the need for intervention by the organizational structures, which are only involved in case of need and incident escalation.
The service is provided on an annual fee basis.