Security Awareness Management Program

[SAC]

Equip your company with the best defense against cyber threats: knowledgeable and trained staff

Main benefits

Improve safety posture with a profiled and managed training course

Company security depends to a large extent on the ability of staff to recognize and avoid potentially dangerous behavior, which may be done lightly, with little awareness, or by mistake: according to the 2023 Verizon DBIR (Data Breach Investigations Report), the in 74 percent of security incidents involve the human factor in various ways.

Realizing the need and difficulty of disseminating training and awareness among corporate employees on cyber threats, from the most widespread to the most elaborate, Security Awareness Management Program (SAMP) is the managed service that devises a security training program tailored to the company's risk profile.

Scope

The service is aimed at companies that need to improve awareness of cybersecurity threats to all business users.

The service is aimed at both small and medium-sized companies, providing qualified support for corporate training, as well as large companies that, despite having the dedicated figures, often have difficulty coordinating different functions in the company that engaged in different priority projects

Challenges facing companies

Tailoring safety training based on the different risk profile that different company figures are exposed to requires skilled and expert knowledge.

Companies also face the difficulty in monitoring and measuring the improvement in safety posture due to training, making the investment difficult to justify in the eyes of corporate management.

The advantages offered

The ICT function gets a comprehensive, managed and organized plan on corporate training, with clear and shared goals. Human resources respond to a concrete need of the company, without the burden of additional operational activities, getting a fully managed service. Corporate users have a stimulating training plan based on modern learning modes (e.g., gamification), adapted to the individual risk profile consistent with time management by often busy corporate profiles.

S2E: approach and proposed methodology

Security Awareness Management Program - SAMP is a fully managed service that aims to design a customized training plan based on both the company's risk profile and that of the business figures involved. The training plan is designed by qualified professionals capable of selecting quality content, deliverable in complete flexibility through specialized online training platforms, such as CyberGuru and KnowBe4, available from any type of device, even in multilingual.
The training plan is crafted to include specific milestones, measured through specific actions organized fully managed. (such as e-mail phishing campaigns).
After an initial phase of business risk assessment and design of the training plan, the performance of the service is monitored and measured with constant frequency, providing analytical KPIs that allow on the one hand the measurement of ROSI (Return On Security Investment), and on the other hand the identification of areas of risk with greater criticality accompanied by corrective actions.

Future development benefits

The main benefits of Security Awareness Management Program are:

1. Measurability of the improvement of information security culture in the company.
2. Prevention of risk from the main vehicle of security threats: people.
3. Improved learning propensity through a stimulating format that is easy to fit into busy agendas.
4. Improved sensitivity to signs that may be the prelude to a cyber attack, making people the company's best defense.
5. Minimal involvement of already highly engaged business functions.

Offer model

Security Awareness Management Program is delivered as a managed service, with a pricing model based on the amount of users included in the corporate training plan.

Each service bundle includes:

- Context analysis
- Design
- Tenant setup
- Customization
- Directory synchronization
- User grouping and profiling
- Phish Alert Button Integration
- Targeted content
- Communications and support
- 4 phishing campaigns
- Analysis of results
- Metrics and KPIs definition
- Reporting
- 4 online workshops