LEVELLING UP SECURITY MONITORING FOR AN IT SERVICE PROVIDER

HWG Sababa

AKITO
IT FOR CHOICE

Selda

Case study

Selda Informatica

It is a consortium company established in 1983; members are Fasi and Previndai[1]

The company implements and manages the various components of the automated IT systems of the Consortium members, but also of external customers

The main areas of activity are social security, health, insurance, education and trade unions

AKITO

Founded in 2016

Italian system integrator specialising in security and cybersecurity

Targets SMBs, central and local PA, entities and organisations across the country

"People always think that security incidents are something that can only happen to others, as long as they do not affect an industry or company close to them. This is what often causes a change in the approach to cybersecurity, but sometimes it can be too late"

Domenico Vitulli, Head of Systems, Networks and Technological Infrastructure of Selda Informatica

[1] Fasi (Fondo Assistenza Sanitaria Integrativa), Previndai (Fondo di Previdenza a Capitalizzazione per i Dirigenti di Aziende Industriali)

In recent years, cybercrime has become an increasingly prevalent threat to businesses of all sizes, to the extent that the global cost resulting from this phenomenon is expected to rise from $8.44 trillion in 2022 to $23.84 trillion by 2027. To reach these figures, cybercriminals illegally access systems, steal data, and either sell it or hold it for ransom, by leveraging different methods, such as phishing scams and malware attacks.

Therefore, the protection of data and digital infrastructure is no longer an option. Especially if you are a company that deals with health and social security data of customers on a daily basis.

This is where **Selda Informatica** - a consortium company established in 1983 and counting 30+ employees - comes in. In addition to the IT management services for its constituent funds, Selda also serves external customers gravitating in the management world within the social security, health, insurance, training and trade union sectors.

Strengthening Your Data Fortress

Cybersecurity has always been a major concern for Selda Informatica, so much so that they started considering security monitoring back in the late 90s. For this very reason, when they realised that their in-house security skills were no longer enough to monitor the entire corporate perimeter - made even more extended by the pandemic - they turned to their trusted security partner, **Akito**, with whom they have been working for over 6 years.

"Unlike what has happened to many companies, it was not the pandemic that changed our approach to security. For us, it has always been a key issue for the business, precisely because we handle sensitive data every day."

commented Domenico Vitulli, Head of Systems, Networks and Technological Infrastructure of Selda Informatica

"In Selda, we tend to do everything in-house, rarely relying on third parties. However, when we realised how complex the monitoring was becoming and at the same time how much the attack surface was expanding, we decided to outsource this process. Together with Akito we started to evaluate SOC."

Several suppliers had been considered in the scouting phase, and despite HWG Sababa young age and smaller size at the time, the choice fell on its SOC service. The great flexibility and solid technical expertise demonstrated at an early stage of the proposal were two decisive elements for Selda Informatica.

Getting to the heart of the project

Despite the increasingly tense geopolitical situation and the resulting internal pressures to speed up the activation of the service, the onboarding phase went quickly and smoothly, within a context of transparent cooperation between HWG Sababa, Selda Informatica and Akito. Given the need for a promptly start-up of the project, the first phase consisted of monitoring the most critical elements - such as Active Directory and firewalls - as well as launching the Threat Intelligence activities.

"At the beginning of March 2022, we held our first technical meeting in person. It was something we really appreciated, because we had the opportunity to visit the SOC and to meet our partners, which I believe is crucial to then work well remotely."

commented Roberto Vasari, Systems Architect of Selda Informatica

"At the beginning of May, we officially launched the service. It was a partial deployment, starting with monitoring the most critical systems and gradually adding the remaining ones."

SOC service in detail

Providing a comprehensive and coordinated approach to security management, the Security Operation Center is responsible for monitoring, detecting, analysing, and responding to security incidents and threats that may occur within an organisation's IT and OT environments.

Leveraging advanced technologies - such as SIEM, SOAR and Threat Intelligence - HWG Sababa SOC analysts identify security events, investigate and assess their severity, and take appropriate action to prevent or mitigate potential security incidents, thus monitoring customers' digital environments 24/7.

Composed of 70+ cybersecurity experts, SOC is organised as follows:

- **Security Manager**
  The main interlocutor for the customer, having a complete view and the responsibility for the state of service. This profile is involved during the incident management and review meetings phases.

- **Proactive Detection Team (levels 1 and 2).**
  A team of security analysts who identify threats addressed to the IT infrastructure by continuously monitoring the alert queue, triaging security alerts, performing deep-dive incident analysis.
  The team handles security incidents, determining if a critical system or data set has been impacted, caring for the remediation and providing support for new analytic methods for detecting threats.

- **Competence Center (level 3).**

Having in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications,it acts as an incident “hunter”. Being deeply involved in developing, tuning and implementing threat detection analytics, the Competence Center helps to resolve the most complicated security cases.

Reporting is another key component of the service. Automatic reporting from the tools can be available daily, while HWG Sababa analysts also provide the following:

- **Weekly report:**

detailed description of weekly alerts and custom reports requested

- **Monthly report:**

monthly service overview, that also includes a section on executive members

- **Annual report:**

annual service overview

Results

The project started in March 2022, with HWG Sababa analysts always being ready to detect and counter cyberattacks.

“Through the monitoring systems, we detected anomalous activity on some clients, but this behavior did not result in an incident because the antivirus nipped any malicious action in the bud. We involved HWG Sababa analysts in this episode and appreciated the speed with which they analyzed the problem and provided instructions for securing the clients that had been compromised.”

commented Domenico Vitulli,

“The SOC monitored all events to confirm that the compromise attempt had failed and that no others had occurred afterwards.”

As part of the service, Selda Informatica also receives daily, weekly and monthly reports, the latter of which are intended to provide an overview of the activities, checking how many tickets are opened, how many events are generated, whether any log sources need to be fixed in terms of SIEM, and more.

“There is a continual service improvement, also considering the new emerging threats.”

commented Roberto Vasari,

“The availability and flexibility of HWG Sababa granted us a service tailored to our needs, and this promptness on their side was a confirmation of what we had understood already in the scouting phase: precisely because of its size, HWG Sababa is able to provide special attention and care to its customers, unlike big players in the market that are often too rigid.”

HWG Sababa

AKITO
IT FOR CHOICE

Selda

Follow us on:

www.hwgsababa.com