PROTECTING THE ITALIAN AUTOMOTIVE AFTERMARKET SERVICE PROVIDERS



UNIT PLUS

HWG Sababa

AKITO
IT FOR CHOICE

Unit Plus

It is a part of Unit Holding an innovative company with 160 employees working daily with different customers

Solid experience in the automotive aftermarket sector

It offers innovative, high-performance and measurable over time solutions

Akito

It is a System Integrator specialising in Security and Cyber Security

It offers innovative technologies and services, with the added value of specific professional skills

It operates throughout the country, for public and private sector companies

"The most valuable asset we hold in our hands is data. The mere possibility that data can be compromised, destroyed or made unreachable to us is something we cannot and do not even want to imagine."

Christian Olivier,
IT Manager of Unit Plus

UNIT PLUS

HWG Sababa

AKITO IT FOR CHOICE

Today's vehicles are increasingly connected and able to interact with each other and the outside world. The size of the global market for connected cars was estimated at $24 billion in 2021 and is expected to reach $57,6 billion by 2026.
But while connectivity provides a better driving experience, it also introduces potential vulnerabilities and entry points that hackers could exploit, making the attack surface extremely large.

In light of this scenario, the automotive industry has developed guidelines - such as UNECE R155-156 - aimed at integrating cybersecurity throughout the entire vehicle lifecycle, from design to testing, production and scrapping.

This is the context for the protagonist of this story, **Unit Plus**, a company that deals daily with some of the key-players in the automotive supply chain, being focused on providing services for the specific needs of Car Fleets, OEMs and many others actors in the automotive aftermarket.

Ensuring secure data management as the top priority

Unit Plus' business is based on a broad portfolio, ranging from **Business Intelligence** - aimed at converting millions of data into indispensable information for decision-making and forecasting - to **Information Technology** - intended for designing highly customised hardware and software networks and infrastructures. Therefore, technology and data are two fundamental pillars of the company's activity.

"Over time, our customers began to question how their data was being managed and to what extent the services and products we provide them with were secure,"

commented Christian Olivier,
IT Manager of Unit Plus

"This is why we turned to Akito - our trusted cybersecurity partner of many years - and searched the market together for a solution that could ensure our internal infrastructure with the level of security the clients wanted. Our goal was to find a 24x7 experienced guardian who could keep threats away from our systems."

During the decision-making process, several alternatives were considered by Unit Plus and Akito's experts. Given the need for a structured team that could monitor its heterogeneous infrastructure, detect anomalies, contain and respond to cyber-attacks, the choice fell on HWG Sababa and its SOC service. With a five-year agreement, the SOC - precisely because of its complexity and importance - is the only security process that the company decided to outsource.



Despite the varied infrastructure of Unit Plus - consisting of servers, switchboards, firewalls, platforms, and more - the onboarding process was quite smooth. The most complex part of this phase was precisely the inventory, which was essential to enable the SOC analysts to access the information of individual nodes and properly activate the monitoring probes.
Once the onboarding was finished, the actual monitoring began, aimed at nipping in the bud any attack attempt.

SOC service in detail

HWG Sababa offers SOC service including levels 1, 2 and 3, and meeting the security needs of IT and OT environments leveraging advanced technologies - such as SIEM, SOAR, Threat Intelligence - and tailored solutions for different industries and sectors.

Providing round-the-clock monitoring, detection, analysis, and response to security incidents and threats, the SOC is composed of 70 certified cybersecurity analysts, representing the real added value of the service.

The internal organisation of the SOC is 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 has been running since 2021 with no incidents occurring so far, but a constantly high level of attention.

“We all know that it is no longer a question of whether an attack will happen but when. My goal is precisely to postpone this moment and, at the same time, have the necessary tools to respond in case we are taken by surprise”, commented **Christian Olivier.**

"The ongoing monitoring has certainly increased our security level and ensures a proactive response to attacks attempts. The feedback is positive, we are very pleased with this collaboration”.

Moreover, on a monthly basis, Unit Plus is receiving reports with corrective actions to be implemented in order to reduce the risk from threats or vulnerabilities.

“The monthly report is definitely what I appreciate the most and I also consider it very useful as it allows us to keep an eye on critical tools and systems." concluded Christian.

HWG Sababa

AKITO
IT FOR CHOICE

UNIT
PLUS

Follow us on:

HWG Sababa
www.hwgsababa.com

Akito
www.akito.it