ARDUINO AND HWG SABABA TRIUMPH OVER CYBERSECURITY CHALLENGES IN AUTOMATION



HWG Sababa

ARDUINO PRO

Arduino

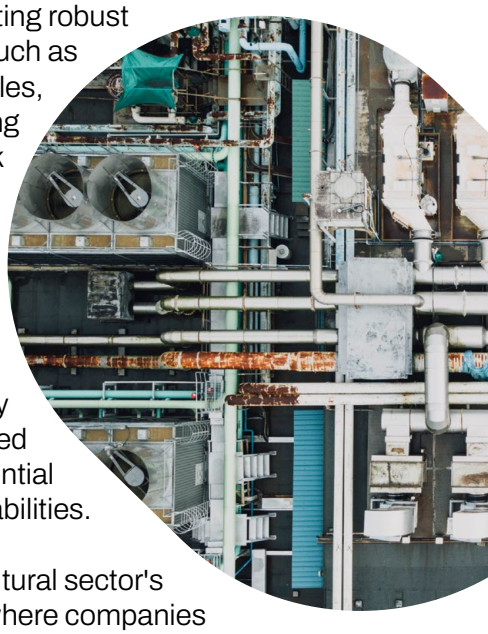
Founded in 2015 by Massimo Banzi, David Cuartielles, Tom Igoe and David Mellis, Arduino is a leading **open-source hardware and software company**

Its open and user-friendly nature has attracted a community of **30+ million users**, including engineers, developers, designers, students and makers

The Arduino ecosystem has been chosen for IoT, Industry 4.0, AI and ML projects on the edge in different sectors, including **industrial and building automation, smart agriculture** and many others

The increasing connectivity of industrial environments brings about undeniable advantages in terms of operational effectiveness and innovation, such as **real-time monitoring** and **predictive maintenance**. However, the growing necessity to connect processes and facilities to the cloud or the internet concurrently exposes such environments to escalating cybersecurity risks.

In response to this challenge, there is a heightened attention on developing and implementing robust cybersecurity measures, such as adopting security by design principles, regularly updating and patching systems, implementing network segmentation, and more. In parallel, when considering the overall cybersecurity strategy, it's essential to engage supply chain partners in the discussion. Collaborating with these stakeholders becomes essential to fortify the cybersecurity posture, recognising the shared responsibility in mitigating potential vulnerabilities.



As an example, consider the agricultural sector's growing embrace of Industry 4.0, where companies integrate smart systems to automate crucial functions like irrigation, greenhouse climate control, and farm management. Now, imagine a scenario where a farm invests in a seemingly secure system from a trusted supplier, only to discover potential cybersecurity vulnerabilities. What unfolds if this system becomes the target of a cyberattack? The implications could be extensive, impacting not just the efficiency of agricultural operations but also posing risks to data integrity, environmental sustainability, and overall farm security. In navigating such landscapes, ensuring the cybersecurity robustness of these systems becomes pivotal.

This is where we turn the spotlight on **Arduino** – a global leader in open-source hardware and software, with millions of developers worldwide.

HWG Sababa

ARDUINO PRO

Securing Tomorrow's Automation with HWG Sababa

As part of the go-to-market process for Opta , Arduino committed to actively verifying the security posture of its micro-PLC with IoT functionalities.



Opta allows professionals to scale up industrial and building automation projects by enabling a wide range of real-time control, monitoring and predictive maintenance applications

"As industries increasingly rely on our Opta to automate processes, the security and integrity of such devices are crucial for preventing vulnerabilities and safeguarding industrial operations. We've noticed a growing trend where companies are requesting us to showcase the security features of our micro-PLC. This goes beyond the standard inquiries about product stability and longevity, reflecting the evolving priorities in the industry"

commented Andrea Richetta, Head of Pro Customer Success at Arduino.

"Moreover, verifying the security posture of Opta is not just a technical necessity, but presents a distinct market advantage, positioning ourselves as a reliable and secure partner".

And what more effective approach than engaging in a Penetration Test activity to assess the *security resilience* of a system?

After a detailed analysis of proposals from various cybersecurity providers, HWG Sababa emerged as Arduino's preferred choice. The decisive factor was the exceptional focus on **understanding and addressing the specific needs of the customer**, avoiding the necessity for extensive explanations. Swiftly initiating discussions on potential procedures, tests and relevant aspects, HWG Sababa demonstrated not only a **comprehensive market understanding** but also **robust industry skills**, setting the stage for a collaborative and effective partnership.

Led by HWG Sababa's Offensive Team, the Penetration Test activity lasted one month.

A Closer Look at the HWG Sababa Penetration Test Service

Falling under the offensive security branch, HWG Sababa Penetration Test is a specialised service crafted to assess the security posture of the target system.

From Assessment to Exploitation. The journey begins with a detailed **vulnerability assessment**, revealing the weaknesses within the relevant environment, application or system. Our seasoned experts then assume the role of ethical hackers, stepping into the shoes of potential adversaries. Proactively, they verify the **exploitability of discovered flaws**, assessing to what extent these vulnerabilities can affect the level of security.

Customised Testing Modes and Comprehensive Reporting. The activity can be executed in three distinct modes, allowing organisations to tailor the level of privileges shared with the Penetration Tester. At the end of each activity, the Offensive Team delivers more than just insights: our comprehensive reports meticulously detail the vulnerabilities found and the methodologies employed in their exploitation. Furthermore, actionable recommendations are provided, empowering organisations to patch vulnerabilities effectively and fortify the security posture.

Diverse Security Horizons. HWG Sababa Penetration Test is a versatile service with a wide spectrum of applications – from examining Wi-Fi to scrutinising networks, from evaluating mobile to desktop applications, the activity seamlessly extends into the complexities of IoT and OT environments. Specifically, the OT Penetration Test emerges as a specialised service aimed at scrutinising various facets of the industrial ecosystem. This unique offering enables companies to identify vulnerabilities and assess the resilience of those systems that control and monitor physical processes in critical infrastructure such as manufacturing plants, power plants, and other industrial facilities. Among them, we find ICS, SCADA systems, PLCs and other components.

Results

After the Penetration Testing activity concluded and the final report was delivered, Arduino wasted no time in tackling the highlighted vulnerabilities.

“At the end of the activity, we provided the client with a technical report, outlining the steps taken, actions performed, and flaws discovered, accompanied by a strategic remediation plan”,

commented Raffaele Forte, Head of Adversary at HWG Sababa.

“Arduino adopted a proactive approach, further classifying and prioritising vulnerabilities according to their perceived importance. To begin with, the client focused on those technical areas where internal management and resolution were not only feasible, but also strategically imperative”.

“We were pleasantly impressed by the professionalism and competence demonstrated throughout the process. The report not only pointed out areas for improvement, but also proposed effective remediation strategies. This enabled us to promptly address concerns, classify risk levels, and strategically implement mitigating actions”,

explained Andrea Richetta, Head of Pro Customer Success at Arduino.

“We immediately initiated these activities and completed them within a few weeks”.

Expressing satisfaction with the collaborative venture with HWG Sababa, Arduino not only anticipates re-evaluating the same technology but also expressed a keen interest in extending this impactful activity to other products within their portfolio.

HWG Sababa

ARDUINO PRO

Follow us on:

www.hwgsababa.com