[ARTICLE]
Christèle Jacq-Arnoult
Marketing & Communications Manager

****

The adoption of application security today does not yet enjoy the same level of maturity as "traditional" cyber.

Why Code Mining is an interesting asset to bridge the Gap

Digital transformation is still accelerating and with it the needs in application and human resources are constantly increasing. Consequently, CISOs and experts are confronted with an unprecedented complexity of information systems in a particularly tense cyber context.

The "bunkering" of infrastructures often prevails on applications security management. Yet, **applications - which are omnipresent in information systems - offer an entry point** that is now widely exploited by hackers. Numerous examples are showing that it's impacting organizations of all sizes every day, from SMEs to large corporations.

So how can we concretely optimize the response to this complexity by strengthening application security?

The validation of the security of an application often requires a PENTEST performed by an expert. This is an opportunity for the CISO to obtain an external view of the security status of the organization's applications. He is then able to establish a **SECURE CODING** action plan to correct the vulnerabilities in the source code.

This implies mobilizing the development teams who play a key role in the organization's cybersecurity. Raising awareness and increasing the skills of the teams becomes unavoidable. It is therefore necessary to give developers the means to be both informed and proactive actors of secure coding.

Code mining is a very interesting asset

Okay, but what is it exactly?

It's a deeptech approach that relies on advanced algorithms and allows an **exhaustive mapping** of the application's properties. Thus, the advanced contextualization obtained with Code Mining enables the **Developer** to easily access an **interactive and educational diagnosis straight from the source code** of the application he is working on. This helps him to understand the root causes of the alert and to quickly increase his skills in a "Learn-as-you-do" mode.

Does this concern other actors than developers?

Code Mining also gives the **Security Champion** the means **to fine tune** his approach by proceeding to a symptoms' correlation. Not only he discovers an application more quickly but also, since he can access to the mapping of all the source code, **he can see more things, run precise queries, and identify complex vulnerabilities** that are longer and more difficult to detect manually.

The **CISO**, as the true conductor of the organization's IS security, decides **a seamless integration of Code Mining technology into a DevSecOps process** and optimizes the **remediation of critical source code vulnerabilities before they generate an open breach**. It is a great mean for him to also have the vulnerabilities coming from the outsourced code fixed before integration into internal source code.

It provides a real advantage in consolidating application security by promoting team synergy, increasing the Developer's skills, and empowering the Security Champions.

It is also a good way **to reinforce the confidence** of both customers and organization's entities, such as sales, marketing, or HR departments for example.

The sooner, the better

In conclusion, exploiting the power of innovation resources - such as Code Mining - in an **upfront security by design approach** within a DevSecOps context is a great idea to stand for. This will accelerate the active adoption of application security management as a complement to the "traditional" means which are in place.

This double approach will **strengthen forerunners' position** and that's why all the cybersecurity stakeholders must take up the subject without delay.

Do not hesitate to get in touch for more information

contact@yagaan.com