Cydrill: Ensuring Proactive Security with Effective Coding Practices

Follow Cydrill on :

Ernő Jeges, MD & CTO

Over the years, cyber incidents have been ranked as one of the top global business risks. Despite being the most common threat, cyber incidents are the least understood risks for businesses. Businesses often spend hefty amounts handling the consequences through tools such as anti-virus, intrusion detection, and more, making security an afterthought. However, the root cause of these security incidents is vulnerabilities caused by software bugs. Studies suggest that more than 90 percent of hacks can be traced back to a previously known programming error in the code of a software. While coding, programmers may not necessarily know about the vulnerabilities or risks the apps are being exposed to. Even if they do, they may lack up-to-date skills and the practice to handle them or to respond correctly. As they continuously work under pressure, they are also single-handedly focused on the functionality, forgetting that the code they produce may also be open to certain vulnerabilities. It is predicted that out of the 26 Mn professional developers globally, only one percent is trained professionally on secure coding practices. The relevant skills and knowledge on secure software development not only help resolve cyber security issues but also preempt it. This much-needed shift in the developer's mindset fits well into the shift left approach.

Focusing on preventative cyber security, Cydrill, a

> *“While others provide pain killers for this problem of cyber security, we provide vaccines”*

Cydrill then offers insights into basic hacking techniques to identify potential dangers that can arise from the code. As remediation, the company focuses on educating developers with best practices to avoid mistakes and apply protection techniques.

Cydrill also presents real-life case studies with deep technical narratives to present the consequences of potentially risky codes. “We do not teach developers how to write code –rather guide them on how not to code. It is the preparedness toward secure coding among all developers that really counts, which is what we aim to increase,” says Laszlo Drajko, Co-founder of Cydrill.

Cydrill also fulfils clients' requirements of scalability of training for all teams and up-skilling. The company offers a blended learning journey where selected people, such as security champions, can receive classic instructor-led training with a chance to dive deeper into selected topics while training the rest of the team via e-learning subscriptions in a scalable manner. For up-skilling, the company offers continuous drills and lab practices with certifications and live score ratings to measure readiness. “With the continuous update of the material and the lab drills, we are always aligned to the latest trends and developments both on the light and on the dark side,” says Robert Budafoki, Co-founder of the company. What is more, Cydrill's training is unique from an educational technology view as its lab framework is presented in an environment that is the same as in which developers work daily. “We enable developers to learn in their natural habitat,” says Jeges.

security company, is dedicated to helping software engineers learn cyber security best practices to develop secure apps and software. Cydrill focuses on training corporate software developers as well as architects and testers on secure coding practices. “While others provide pain killers for this problem of cyber security, we provide vaccines,” says Ernő Jeges, MD and CTO of Cydrill.

Cydrill uses a four-step approach to educate developers. At first, the company assists the developers in identifying the problem with the current coding practices.

He draws attention to cyber security from a game theory point of view, which clearly is not a zero-sum game. Rather than beating the enemy, the goal is to stay in the game, which in a corporate context is to “stay on the market”. Cydrill is continuously refining its services and expanding its curriculum to update the content as required per new trends empowering clients to be proactive in security to avoid threats and stay in the market.