CASE STUDY

Could a game be the way to a developer's heart when it came to security compliance?

How a Tier-1 Financial Institution created a

Revolutionary Security Certification Experience

With millions of customers, a rich history as a trusted global financial institution, and a commitment to innovation and keeping pace with digital transformation, this tier-1 banking client utilized Secure Code Warrior as part of a truly unique education experience within their organization.

They created an in-house technology education initiative, aimed at supporting thousands of employees to learn practical, cutting-edge skills in a number of disciplines, including machine learning and cybersecurity.

The financial services industry is currently in a period of rapid, radical transformation, in which many companies are changing their service offerings to align with the fast-paced development of emerging technologies. In essence, they are becoming fully-fledged tech companies with a finance focus. Our client's approach has not only allowed them to keep up with this trend, but also achieve better (and smarter) outcomes than most. They have invested enormously in their own people to stay up-to-date with such vital, rising fields, and as a result, they are at the forefront of FinTech innovation and expertise.

To successfully execute this program, our client and the wider team saw a need to ensure their developers were fully versed in secure coding, with a high level of cybersecurity awareness. The Security Awareness Manager sought to engage the team positively, getting them excited about security from the very beginning.

The Challenge

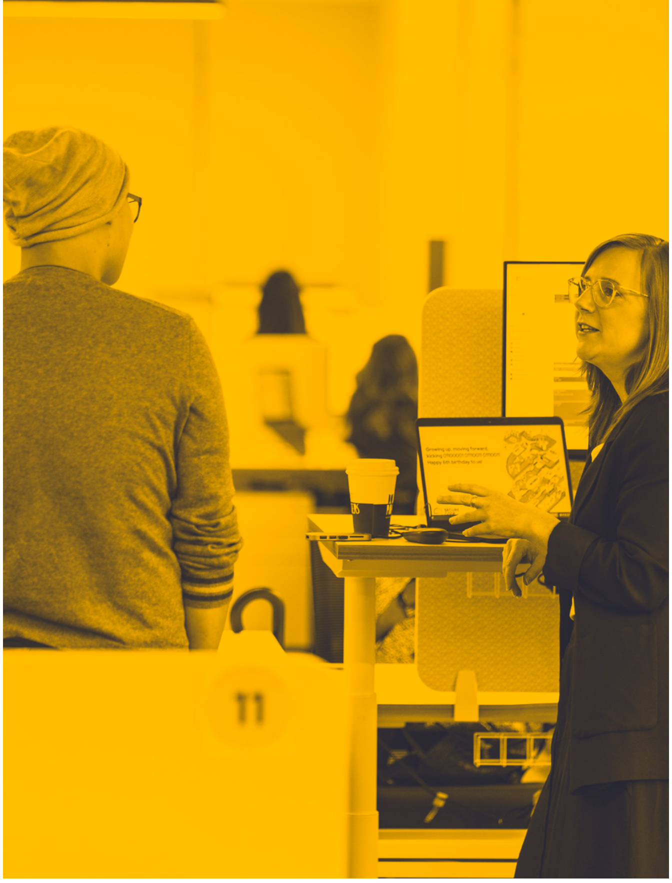
Our client's Security Awareness Manager has a long tenure in the security industry, giving him a front-row seat to the explosive growth of online application adoption by companies large and small, as well as the rapid increase in digital-focused teams. He has seen first-hand the inevitable siloing of expertise that can follow such hyper-expansion, and ultimately, this has been an issue for many security and development teams: "In the early stages of online adoption, developers did think about security and apply it to their software builds. However, in an increasingly siloed environment, one team will work on, say, an operating system which will then be sent to a security team for analysis, and it will often come back with a bunch of red marks and notes on how to fix it. It is inevitably secured, but the findings and knowledge disappear into a black hole, only to happen over and over again," he said.

He referenced the "people challenge" when speaking of the security issues he sees frequently in his role:

"Software engineers are paid to build features, and security can be seen as a huge impediment to agile development. They are busy with their own priorities, and often view the security aspect as someone else's job. On the most extreme end of the scale, some take the view of 'Well, nothing has happened yet. Why are we so worried about securing this software, and why is it interrupting my development lifecycle?' In a world of increasing digitization, this attitude has to change. Rather than being looked at as a nuisance, we need to drive home the importance of sharing responsibility for software security".

With the growing dependence on development to power our digital lives, he saw the writing on the wall: as a society, we are sitting ducks for hackers on an increasingly unfair playing field for the good guys. Developers needed to take security seriously, develop a keen interest and become the first line of defense in his organization (and, indeed, that of any serious tech company).

So, he set about turning traditional training on its head.



The Implementation

The Security Awareness Manager drove our client's overall philosophy of setting a new standard in software quality. Specifically, the notion that the level of security inherent in a piece of software is an indication of its overall quality and product viability. As it stands today, security is not closely tied to measures of quality in most instances, and certainly not in the same way as overall UI, speed and serviceability are considered when assessing software.

"Security must become a non-negotiable requirement for high software quality," he said. "It correlates with reliability, which is a huge concern for most corporations, especially those with a rapidly transforming, digitizing business model."

With the costs of fixing vulnerabilities in committed code up to thirty times more expensive than if it was written securely from the beginning, it has become a key objective to "bake" a viable security culture into his development teams. After all, there are certain vulnerabilities that scanning tools won't detect, and the most efficient solution to combat them is a security-conscious development team.

The Security Awareness Manager detailed his experience with other forms of training, many of which are still commonly used to "win over" and prepare developers to tackle growing security concerns: "When developers are left to learn about security through a tonne of theory-based work, or worse: infrequent 'tick the box and move on' compliance training, there simply isn't enough hands-on learning or time spent to make a lasting impact. I was determined to change this by applying a more effective solution," he said.

The benefits of high engagement

Under the advice of a savvy Security Awareness Manager and his team, our client implemented a bespoke certification program, of which the Secure Code Warrior platform is an integral part.

Their investigation into a more effective, engaging developer training solution led them to become an early adopter of gamification, maximizing its potency and potential with their own structured, full-scale curriculum.

"It was vital that we made high-engagement training part of the culture, and kept students coming back to further their learning. The system is a deliberate approach to build knowledge, skills, and a sense of value towards security, ultimately resulting in them working with real source code that they use every day," he said.

Ensuring the solution was holistic, covering both industry-standard security best practice and internal guidelines, our client was able to mobilize training rapidly, positively impacting software security within the organization.

METRICS

Time spent training:

5000+ hours

Challenges Completed:

46,000

Number of Security-Aware Developers:

300 and growing

** Statistics accurate as at October 2019.*

The Result

Our client's certification program is a successful, constantly-evolving training format that is perfect for such forward-thinking initiatives as their in-house tech education facilities. The in-depth course, rolled out in such a fun, interactive and incentivized way, ensures that all students have the best chance of knowledge retention, as well as the support to truly develop a security-first culture and mindset. While gamification certainly makes learning palatable, the core practicality of the program remained: to give developers the skills required to identify and thwart high-risk vulnerabilities in their applications.

It is important to note that the training was not mandatory, instead requiring an element of motivation on the part of the developer. While this was undoubtedly supported by offering incentives and rewards, adoption of the program by the wider team was a result of swelling team support and approval of the process.

In addition to vital competency continuing to be developed, the program also helps bridge relationship gaps between development and AppSec teams, getting them on the same page, speaking the same language and forming mutual interest.

A far cry from a compliance check-box, this program has become foundational in the ongoing support of valued staff and their career, providing measurable upskilling in one of the most high-growth industries on the planet: cybersecurity. It is training programs such as this that will become the benchmark in improving software security from the start.

FAST FACTS

- ✓ There has been an unprecedented response from students who have completed the certification and expressed an interest in becoming instructors. This ground-up evangelism is a powerful factor in spreading word-of-mouth support, uptake and overall security awareness.
- ✓ Our client is in the process of rolling the program out to more than 2500 developers within their organization, with over 90% already active in the system.
- ✓ They use this training to assist staff in overall career development, ensuring they are armed with the knowledge required to utilize their skills in an ever-changing technology space.

Tips for success

Take the time to explain the benefits of training, intended roll-out and projected outcomes to key stakeholders, participants and team leaders. If they are included from the beginning, it may be easier to get support in vital areas as the program grows.

It's a marathon, not a sprint: any training programs should grow and adapt to the changing needs of the industry and organization. It doesn't have to be set in stone from day one.

Make it fun! Training doesn't have to be boring, and a gamified platform like Secure Code Warrior is the perfect opportunity to turn such an important task into a memorable event. You will be rewarded with high engagement when you go the extra mile to include prizes, certificates, and even a theme - the possibilities are endless.

ABOUT SECURE CODE WARRIOR

Secure Code Warrior is the developer-chosen solution for growing powerful secure coding skills. By making security a positive and engaging experience, our human-led approach uncovers the secure developer inside every coder, helping development teams ship quality code faster.

Through inspiring a global community of security-conscious developers to embrace a preventative secure coding approach, our mission is to pioneer a people-first solution to security upskilling, stamping out poor coding patterns for good.

bsi. ISO/IEC 27001 Information Security Management

FM716415

ISO Certification

Secure Code Warrior holds an ISO27001 certificate for information security management. This BSI-issued certification reflects our commitment to deliver excellence within the development and operations of a SaaS platform, created to improve secure software development competencies among software engineers. It is granted only after intensive inspection of how a company manages and protects its customer data, and confirms our uncompromising approach to security and privacy for our clients.

securecodewarrior.com

info@securecodewarrior.com