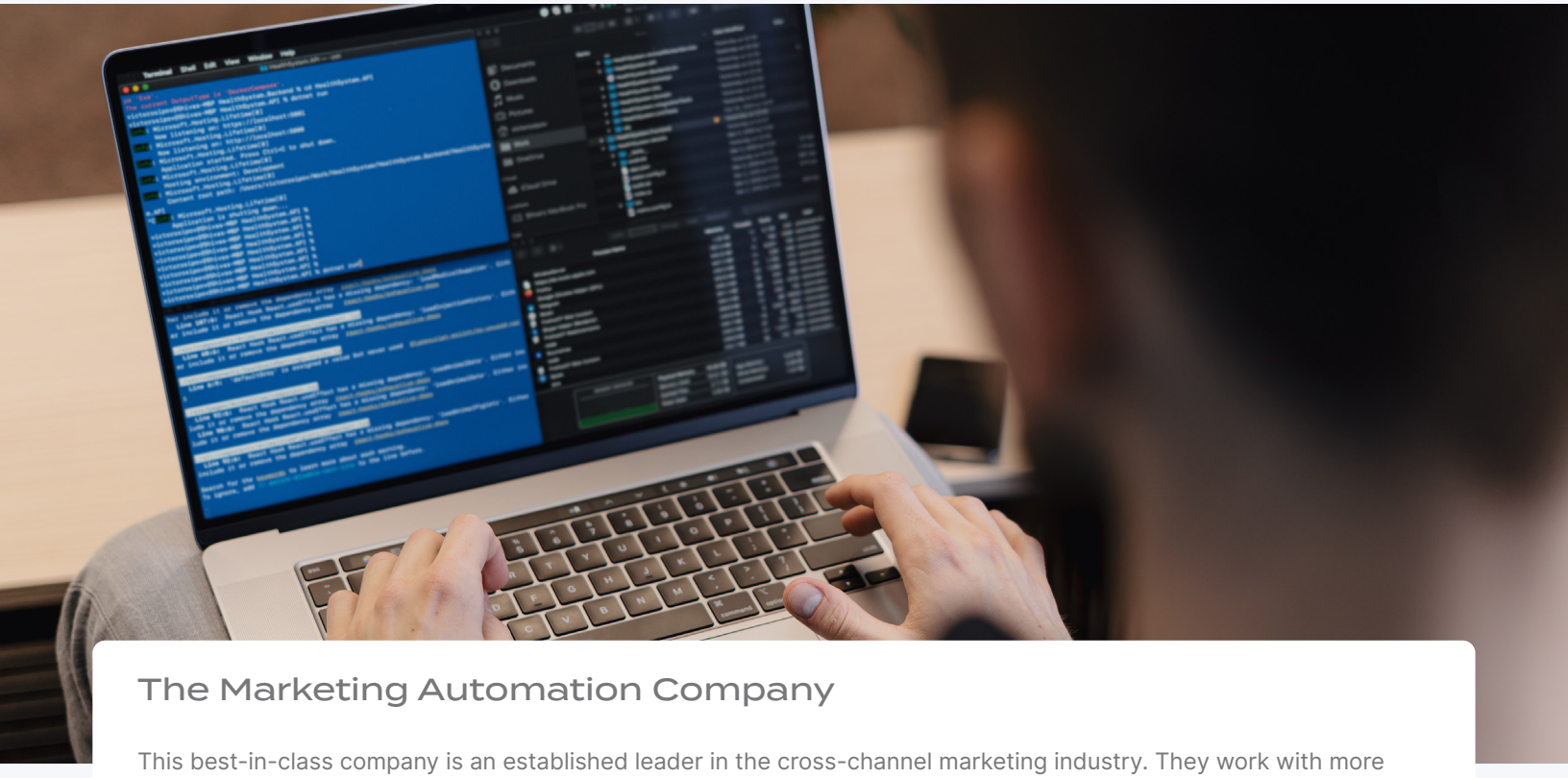
Security Journey Case Study

A Leading Marketing Automation Company Takes Secure Coding Best Practice To Another Level

Take a Page From This Company's Secure Code Training Playbook

Learn how a world-class marketing automation company, integrated Security Journey into its secure coding culture. They epitomized secure coding training best practices by taking a holistic approach to developing their annual program. By taking advantage of the offensive and defensive training, their developers upped their coding skills, making their platform safer for their thousands of satisfied clients.



The Marketing Automation Company

This best-in-class company is an established leader in the cross-channel marketing industry. They work with more than 1,000 retailers and brands, providing leading-edge SMS, email, identity resolution, and behavioral marketing solutions. The company embraces the importance of secure applications which protect their customers' data.

The Challenge

Many of the company's developers hadn't had much exposure to the offensive side of secure coding. The company knew they needed a training solution that offered offensive and defensive lessons to equip their developers with the skills to go after vulnerabilities by teaching them to think like hackers. After exploring their options, the company came to Security Journey because they met the company's extensive list of requirements.

The Must-Haves

"We didn't find anything else on the market that taught both offense and defense that was worthwhile. The other solutions' offensive content seemed trivial. We stopped looking at any other products after we found Security Journey."

The Director of Information Security, knew exactly what the organization needed. The developer training products they used previously were all missing the mark and lacked an extensive content library. With the previous training solutions the definition of interactive content was either watching a video, or copying and pasting code then submitting it. He knew firsthand that it was important the developers enjoyed the process, and at their core developers love problem solving. He knew enabling them to write code in an application sandbox would keep them engaged, committed to completing the lessons, and ultimately help them learn and retain secure coding skills.

The company was looking for a truly hands-on training approach that offered enough relevant content to plan and schedule a 12-month training plan that wouldn't be redundant or boring.

Their training requirements were:

- Offensive and defensive training
- Engaging hands-on approach
- Extensive training library with digestible lessons
- Capture-the-flag (CTF) events

Offensive AND defensive training

High priority on the company's list of requirements was offensive and defensive training. They believed teaching developers how exploits are executed and how to prevent them would be more effective and memorable than simply teaching them how to fix vulnerabilities. In turn, their secure coding knowledge would significantly improve.

A true Hands-on approach

It was important to the company that their developers combined theory and practice. Security Journey's sandbox environment provided the hands-on approach they had been searching for. Most of the other solutions they had tried claimed to be hands-on. But, the reality was they offered video-based or copy-paste lessons, which wasn't what they were in the market for. The company appreciated that our claim of hands-on literally meant their developers had to write secure code. Because the lessons are so interactive, their developers remained interested and focused on completing their training.

Strong digestible lessons for a continuous program

The company wanted the lessons to be brief and focused to make the best use of developer time but still enable them to learn multiple topics each month. Equally important, they were looking for a product with an extensive content library. One that would offer their developers comprehensive training without repeating lessons.

The ability to run a CTF event

"Security Journey made it easy to set up and run the hackathon. Our customer success manager helped tremendously and gave us a roadmap that matched the hacking challenge to the lessons that the developers had already completed."

The company wanted to create a custom CTF (Capture the Flag) event. With the help of their Security Journey Customer Success Manager, a custom training plan was developed that taught concepts included in a hacking challenge mid-year. They wanted to set up their developers for success which is an excellent testament to their overall approach to their training plan. As a result, the CTF was a massive success, with developers completing several more challenges than anticipated. The team will be repeating the CTF each year, during which they will repeat some challenges but also raise the bar by introducing more advanced challenges.

Best Practice Training Program

Due to the amount of experience the marketing automation company's leaders have in development, they know what it takes to run a successful, secure coding program. They applied learning science principles to create their developers' training schedules for 2021 and move into 2022, understanding the importance of repetition in building long-term memory. They wanted their developers not just to know the 'how' in secure code, but the 'why' was equally important.

"Early on in the training program developers questioned why they needed to learn offensive techniques which opened up the conversation amongst their peers and with our security team. I was happy to explain the importance of understanding how hackers exploit code and how it improves skills in finding and fixing vulnerabilities"

Another page in their best-practice playbook was time. The Director of Information Security was mindful of the hour per month his team had available to dedicate to secure coding training which meant bite-sized yet robust lessons were imperative. Because Security Journey lessons only take between 20-30 minutes to complete, his team could get through at least two, if not three, in that hour timeframe.

Every month is a different theme with two to three lessons, again being respectful of their developers' limited spare time. However, during their first year using our platform, the developers were so engrossed they worked ahead of schedule. Many completed the lessons far before the due date.

Next year the company will be covering many of the same topics to reinforce the training already completed and will add newly released lessons as well.

The Outcome

“Your content is worthwhile, and we see that you’ve already added to it since we started. We have no reason to look anywhere else.”

Initially, a secure coding program was a hard sell, and some developers were concerned that their progress or scores would impact their growth within the organization. However, the leaders recognized how important it was to communicate the main objective of the training: improve security knowledge. They made sure to alleviate their developers’ fears, which led to a successful training program.

One of their most enthusiastic developers had the following comments about the training:

Lesson:	Rating:
Command Injection	10/10

“I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT!
I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT!
I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT!
I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT!
I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT! I LOVE IT!”

Because the content teaches practical skills, the company’s developers not only become absorbed in the program, but also learn new tactics to apply to their applications. By replicating last year’s lessons for the current year, the company’s holistic approach to repetition means those developers will retain the information long-term. For future sessions, the marketing automation company is considering integrating their SAST and DAST tools to create adaptive training that will focus specifically on vulnerabilities within their organization.