



# How CM.com improved its security posture with a bug bounty program

BY ANNA HAMMOND · SEPTEMBER 12, 2022 · LAST UPDATED ON MARCH 6, 2025

CM.com's story began in 1999 with the sending of SMS messages to update nightclub and festival visitors. Today, it is a global leader in cloud software for conversational commerce. Sándor Incze is CISO at CM.com—a job that involves ensuring the cybersecurity for all of CM.com's platform offerings.

Having seen significant improvements in CM.com's security posture since implementing a bug bounty program, Intigriti sat down with Sándor to hear more about his approach to cybersecurity.

Intigriti interviews CM.com's CISO, Sándor Incze

## **Intigriti: Hi, Sándor! Can you start by giving us some background on your role at CM.com?**

**Sándor:** Absolutely. I've been working for CM.com now for almost 12 years, so you can probably tell how much I like the company by that alone. I started in my role as Chief Information Security Officer in 2019, and ever since, I've been working with my team to find the best ways to protect our large attack surface from bad actors, oversights, and everything else that goes with the cybersecurity game.

## **Intigriti: Before we move to cybersecurity, could you define “conversational commerce” for anyone who might be new to it?**

**Sándor:** Put simply, it's about businesses instantly communicating with customers through messaging apps and chatbots. The goal is to enhance customer experience through regular, personalized content and also to simplify commercial transactions.

Given the capabilities of today's mobile devices, that could be anything from easier payments during a mobile-guided gastronomy tour to finding the closest bathrooms at a music festival. It also has a lot of use cases in customer support and sales.

## **Intigriti: CM.com is a rapidly growing organization with many clients who trust you with their customer data. What type of security posture does such a wide range of assets and infrastructure require?**

**Sándor:** Well, in a lot of businesses, we talk about putting the customer first. In our case, that would include our customers' customers and their data. But when your product is a software platform, the best way to protect everyone is to ensure the security of your offering. You put your own security first, in other words.

We work really hard to maintain the highest levels of security for all our platform technology, and we keep our customers regularly updated on the status of our cybersecurity.

## **Intigriti: How does that play out in practice?**

**Sándor:** Take pentests as an example. The goal of our pentesting is to ensure that our attack surface is protected and our infrastructure is as robust as possible. At the same time, we have a lot of customers who ask specific questions about security and want to see pentest reports. Once we've done a pentest, we can provide them with reports to demonstrate our strong security posture. At the same time, for our security and for that of our clients, we wanted to add stronger continuous security testing. That's why we started our bug bounty programs.

## **Intigriti: What specific challenges did you see in using pentests that made you look beyond them for cybersecurity testing?**

**Sándor:** Well, a pentest will give you the result of a specific moment provided by the knowledge of that specific pentester or pentesting group. I believe that bug bounty programs add another layer of security in that they give you a continuous protected surface on your platform.

Also, you can hire pentesters, but not all pentesters are equal. Therefore, it's very hard to determine if the pentester you're hiring is good. With crowdsourced security, however, you have a much larger pool of expertise.

## **Intigriti: Can you explain how a bug bounty program overcomes these limitations of pentests?**

**Sándor:** The thing I like about the Intigriti platform and the bug bounty programs it provides is that it has a lot of security experts, and they each have their own specialty. As they work on our programs, they submit reports in an ongoing way. So, we still have the reports that show to the customer we do pentesting. In addition, now we have the Intigriti program findings for our own health. We know it makes us safer.

## **Intigriti: Why did you choose the Intigriti platform as CM.com's bug bounty program provider?**

**Sándor:** When we started researching bug bounty programs, Intigriti came to our attention because it was well known as Europe's leading provider. We read up and liked what the platform technology offered. Then, when we were looking deeper into bug bounty programs, we saw that one of the biggest time drains is triage—like assessing reports for validity, finding duplicates, etc. Intigriti offers triage as part of its core service, so that sealed it for us. We decided to give it a go.

## **Intigriti: How easy was it to get started with your bug bounty program?**

**Sándor:** So, we had created a strategy regarding how to keep CM.com safe, and bug bounty programs were going to be part of that. We started with an Intigriti community that was fairly small and in a closed, private community. When we got more confident, we opened up the scope and brought in more researchers. This was a great way to get started and learn how things work. And it was very easy to set up.

Intigriti is also a very transparent platform. That gave us confidence too. For example, every hacker has a unique and traceable ID, so we have up-to-date insights on who has been testing what as our bug bounty program progresses.

## **Intigriti: How have your customers reacted to the addition of bug bounty programs to CM.com's security posture?**

**Sándor:** Our customers expect us to do what needs to be done to keep their data and our data safe. A bug bounty program is the cherry on top of our security strategy, and our customers approve of it.

## **Intigriti: Has running a bug bounty program improved cybersecurity at CM.com?**

**Sándor:** Definitely! The reports that are generated by the Intigriti bug bounty hunters are top-notch and are very understandable for our developers to work with. They're well written and always valid because they've been through the Intigriti triage.

## **Intigriti: Were there any unforeseen benefits or issues with bug bounty programs?**

The vulnerability report quality from our programs is also very good, and our developers like working with them. The bug is explained, they see why it is a vulnerability, and they see how they can fix it. So, with Intigriti, on top of the immediate security improvements, the developers also learn and improve from the program.

## **Intigriti: Do bug bounty programs have a future at CM.com?**

**Sándor:** Intigriti is now part of the complete security program that we have here at CM.com. We've decided we will run a continuous bug bounty program and keep extending it with the new applications we add to our own platform. What's safe today may not be safe tomorrow, but at least we are trying to do our best, and we can show our customers that we are absolutely doing our best to keep our platform safe.

## **Intigriti: Would you recommend bug bounty programs to other CISOs?**

**Sándor:** Yes. For us at CM.com, a bug bounty program works very well because it seamlessly integrates with how we practice security. When we started, everybody was saying, "No, you don't need such a thing, they're not experienced enough." But, try it! See if it can work for you as it has for us.

## **Learn more**

Intrigued by what you have read? Want to know more about bug bounty programs? Get in touch to [request a demo](#) with a member of our team today.

---

## About Sándor



Sándor is the CISO of CM.com. He is responsible for developing and implementing CM.com's information security program, which includes procedures and policies designed to protect the platform's systems and assets from both internal and external threats.

**REQUEST A DEMO**

[intigriti.com/demo](https://intigriti.com/demo)

**VISIT THE WEBSITE**

[intigriti.com](https://intigriti.com)

**GET IN TOUCH**

[hello@intigriti.com](mailto:hello@intigriti.com)