Collaborative Penetration Test Case Study

Secarma worked closely with a well-known management software provider to test the strength of their flagship application's cybersecurity posture. Our experts carried out a collaborative penetration test – working with the company's in-house development team to remediate and mitigate risks as they were identified.

Our consultative and collaborative approach to penetration testing not only improved the organisation's overall security posture to an exceptionally high degree, but also resulted in a better understanding of secure coding, allowing the team to work within tight deadlines.

About the Organisation

The organisation's application simplifies, co-ordinates, and integrates large-scale storage and supply chain management. It empowers users to log in and efficiently track and administer workflow activities from one centralised location; allowing users to view and control relevant project data from anywhere, securely, using a web browser. As a leading software provider, this company is well recognised for their efficiency, know-how, and adherence to best practice.

Trust is Everything

Security can make all the difference when the work you do is integral to businesses and individuals up and down the country and beyond, so there's a lot resting on this business's platform being secure. In a heavily regulated industry – and when you're dealing with huge customers who have their own cybersecurity demands – trust is everything, so maintaining robust security is one of this organisation's top priorities.

With their customers uploading massive amounts of data to their platform on a daily basis, it's of the highest importance that the entire process is protected. No doubt, when data is uploaded via their customers' corporate devices, there'll be security in place. However, this business wanted to ensure cybersecurity was tackled, not just from a tick box exercise, but to achieve an exceptional level of security assurance – leaving no stone unturned, so to speak. The organisation chose to work with Secarma, due to their trust in our ability, our expertise, and our consultative approach.

What We Did

Our experts were given access to the company's application within a testing environment, along with source code to assess and analyse, in order to identify any security vulnerabilities present.

Traditionally, a dev team may not be thrilled at the idea of a penetration test, as they are often left in the dark during testing, and remediation advice can often be somewhat lacking. If a long list of vulnerabilities is discovered, this can lead to large technical rewrites – meaning deadlines for 'Go Lives' are often missed.

Secarma takes a different approach to testing: we actively encourage an open dialogue between our client's development or security teams and our consultants, both throughout engagements and into remediation. This communication could be in the form of daily stand-ups with the development team, or our consultants might be added as a guest to a code repository such as GitHub, where we can add vulnerabilities to code and assign remediation to specific developers. In this case, we had a dedicated channel set up to communicate issues directly with the lead developer as we found them. This dynamic style of testing allowed the developer to mitigate the risk, then our testers could confirm the fix; all during the test window.

"During the test, Secarma's testers were able to share with us what was going on, give us a chance to fix issues, and then take another look. For instance, if they told us on day one that XYZ isn't working or isn't secure, we were able to patch it overnight. We could then say, well, actually we've got another release ready for you to look at. So it wasn't just basic testing.

This was great from our point of view, because it means when Secarma created the output report, they can say we found this issue and then it was remediated during testing. It's far easier if that goes in the report, as it's a much better message to give to our customers and takes a lot of pressure off for us." **– The Organisation's Chief Technical Officer**

Client Feedback

Needless to say, the company's representatives were very pleased with the thorough documentation of issues that our testers found. This included what the issues were, how we found them, what we did to produce a problem, and how it could be used to exploit. They also appreciated that when any of our messaging seemed unclear, our testers were more than happy to jump on a call and explain everything, going as far as to set up a demonstration when necessary. Our testers went above and beyond to ensure the business got as much out of the engagement as possible, this was found to be *"really, really helpful"* by their CTO.

When discussing the corporate benefits to this approach, he said:

"From a business point of view, the main benefit is that we've avoided having to do a retest, saving us time and funds. If we hadn't embraced this approach, we would be doing all of the rework at the end of the engagement, following the report.

Security is taken seriously by our customers, and without being able to correct issues revealed during the pentest, this could result in our clients wanting a retest. The monetary cost of a retest isn't the biggest issue, but the cost of us delaying for two to three months *with all the back-and-forth communication between us and our clients, all the revenue, potential customer loss – that is a big issue."*

It wasn't just the work we did and our approach that impressed the CTO's team, they were also pleased with the communication skills of our testers and their willingness to collaborate, and had this to say:

"We appreciated that the report wasn't patronising at all, as well as their diplomatic approach, and how well they communicated with us."

We created a 'team within a team' environment, where both our testers and our client's development team were working together to achieve a common goal: allowing their customers to rest easy, knowing their data is safe.

How Secarma Can Benefit Your Business

Working with us means you have the knowledge of our testers at your disposal, who work to develop your cybersecurity posture, help you code more securely, and fortify your business against threats.

By investing in cyber security and penetration testing, you get the benefit of a new pair of eyes that examine your organisation's security from a potential threat's perspective. We offer flexible cybersecurity sessions: anything from one-off pen tests, to collaborating with your security team on a long-term basis – building that familiarity and rapport, as well as working towards the continuous development of your security standing.

Our skilled security consultants use a wide range of ethical hacking methodologies and are constantly undergoing training to keep on top of the latest techniques. This means they're able to hit the ground running – finding vulnerabilities, recognising linked issues, and working out issues from the ground up as an extension of your security team.

Find out more about our collaborative approach to penetration testing by getting in touch with a member of our dedicated team, or heading to our penetration testing page.