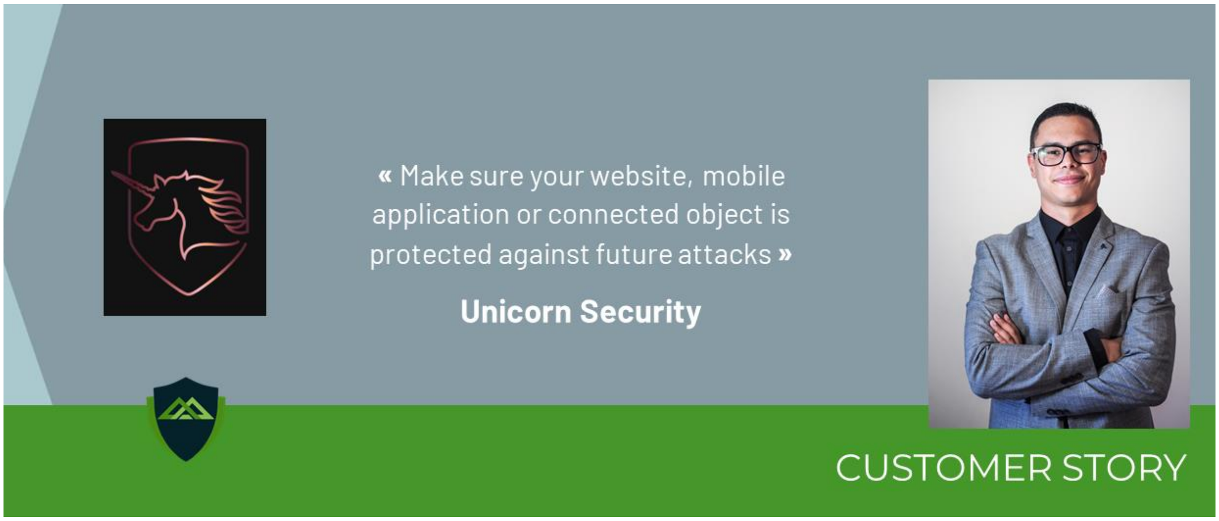
« Make sure your website, mobile application or connected object is protected against future attacks »
Unicorn Security
CUSTOMER STORY

We asked Antoine Royer, co-founder of Unicorn Security, IT security expert and Yag-suite user to answer some questions about his use of our tool.

In what context do you use the Yag-suite?

We propose our customers a packaged offer which contains an audit part with a classic Pentest assessment, and we provide in addition a code review service by relying on the Yag-suite.

How does our tool help you?

The Yag-suite is very useful to us technically to enrich our Pentests and particularly to confirm or deny suspicions that we have concerning some security problems. Actually, it's important to know that when we audit an application, it is often difficult to see everything in a few days. By exploiting the results of the source code analysis, we can read the report generated by the Yag-suite and see where errors are located on the application side.

Could you give us an example?

For example, we sometimes see that we receive some weird packages, such as server-side errors, and we see that on the application side Yagaan's tool has detected something in the code, which is a conformance defect, an error case that is not handled.

It's very interesting to be able to confirm this and for the customer it's very valuable to be able to have it thus remediated.

How do you use the information provided by the Yag-suite?

We always look on the features of the target application in a generic way, but we obviously cannot go and inject manually on all the parameters, all the features. Yagaan's tool allows us to know, for example, that a function which creates a user has got a symptom of bad encryption, bad password storage, bad database entry, etc. and this allows us to have a more precise idea of the exploitability of a security problem.

In fact, when we start a Pentest, we go to places that are somewhat unused in the application. By causing errors and correlating with the Yagaan's tool report we can know if there are exploitable elements or if it is just a bug. It's very important to have this knowledge because it allows us to find out more critical issues and go further by checking where there is a symptom in the report provided by the Yagaan report. It's very useful for us but for the customer also, especially to enrich the "black box" view that a standard Pentest provides him.

« The information delivered by the Yag-suite allows us to select specific features beyond those that we test systematically and on which we can rely to further our investigations. »

In a "black box" approach, we communicate to our customer what we have done to reproduce the problem. The main thing generally is a http request or an interaction with the server.

However, in this case, as we do not have access to the source code it is not easy to identify which line of code or which file is responsible for causing the error and may be involved in a vulnerability.

The information provided by the YAG-suite makes it possible to be more relevant in the correction recommendations that can be proposed.

This is very valuable for the customer because it will allow him to optimize his time for the correction of a security problem.

> « We can tell our customer that we have managed to exploit this problem to the end, and the line of code that caused the problem is here »

Does the Yag-suite save you time?

The time saving is always difficult to quantify.

However, the YAG-suite allows us to go faster to clarify a doubt and see if a point is critical or not. As a result, I'd rather say that it enables us to see more. So, in terms of time savings, if we're talking about a specific task, let's say there's an injection point that's going to be detected during a black box phase, I would say that with the Yagaan tool, depending on the size of the source code, we can easily imagine that this saves up to half a day in the search for injection faults.

> « With the Yagaan tool, in the same amount of time I can produce a much more precise work, cover many more problems and this is very interesting for the customer too. »

I'd like to say that I had the opportunity to test several other tools. I no longer work with them as reports were not easy to exploit.

This is not the case with Yagaan. You can really feel the time spent by the development team on the reporting aspect and it is something which is very important to me.

> « I used to spend way too much time reading and understanding reports of other tools. Yagaan's reports are very intuitive and easy to understand. »

The interest with the Yag-suite is also the integration with the IDE. It allows you to quickly go back into the code structure and identify false positives where other tools provide a simple pdf. When we have 2 or 3 million lines of code with class names and file names that all look a little bit alike, being able to browse the source code and do custom searches changes everything!

Antoine Royer – Unicorn Security

After working for ANSSI and Amadeus, Antoine Royer co-founded Unicorn Security to help small and medium-sized businesses control their IT security.

Created in 2020, the company already works with several domestic companies but also with organizations established in various countries including the United States, Germany and South East Asia.

Want to learn more about how Yagaan can help you control the cyber risk carried by applications?

Get in touch with the team!