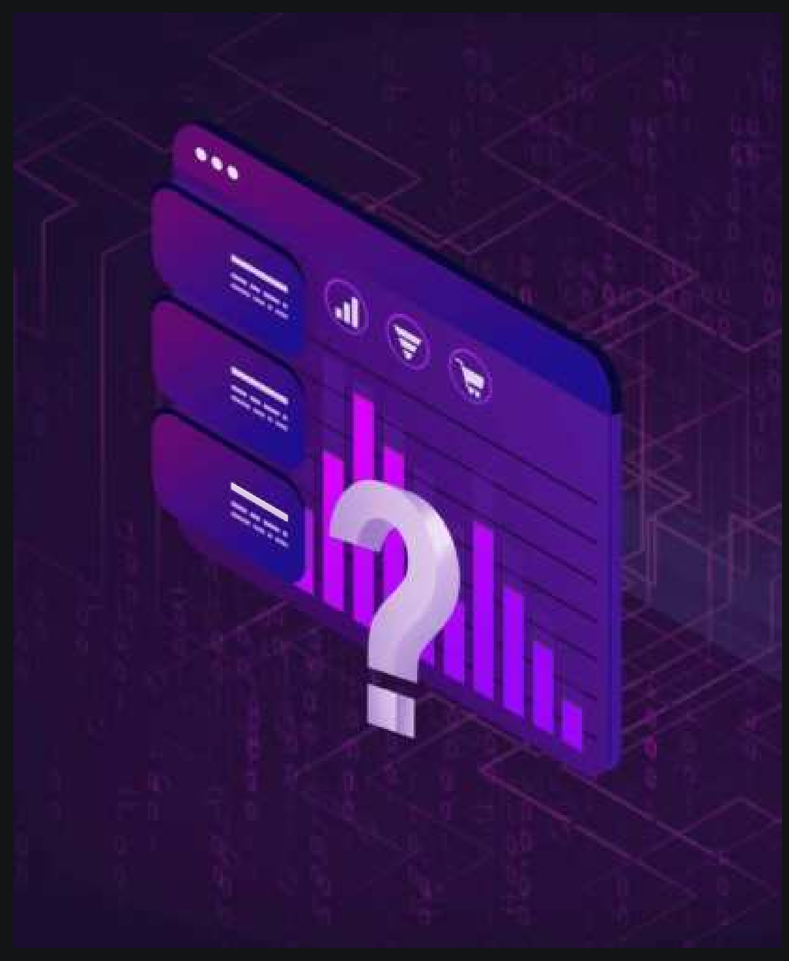
SAYFER LITEPAPER

A New Approach for Web3 Projects' Security

Table of Contents

The Problem



Web3 hacks are on the rise. Every few days, another major project gets hacked. At best, the only security measure Web3 projects perform is an audit of their contracts. This security measure eventually leaves many other aspects of the business vulnerable to attacks. We've often seen this in hacks like the $120M BadgerDao hack, $650M Ronin Bridge hack, and Pretty much every CEX that lost its private keys.

This old approach contains many lousy security practices that will increase the chance of getting acked.

These problems include:

1. Single Point of Failure
2. Lack of Security Layers
3. One Time Testing

We believe that for projects to gain mass adoption from "mainstream" users, they have to be much more stable in their cybersecurity. Today, most of the crypto market are early adopters, but that is changing, and the new type of clients will not accept such risk.

SINGLE POINT OF FAILURE

When creating complex projects and protocols, you want to ensure that even if one component of your system is compromised, you won't lose all of your funds. This approach is more easy said than done.

Sometimes it is easy to know where the points of failure are, but it is tough to find a way to mitigate the risk.

Imagine you developed a token contract. Analyzing the risks is straightforward with simple questions such as – "How can you not lose all of your investors' money if the contract gets hacked?" "How will you know if something bad happens?" "Which component of your system is the weakest?

It is tough to find the not-so-obvious point of failure.

Here's another example, you have a very secure contract, but your new employee's phone got stolen. This phone is connected to a GitHub account that can commit and push new code. How will this be prevented or blocked?

Without proper monitoring tools, a backdoor can be inserted into your contract without you even knowing about it.

LACK OF SECURITY LAYERS

The only way to create a secured project is by having multiple security layers. It was very much in place before the computer era and is relevant in today's Web3 project and protocol architectures more than ever.

Security is not a binary outcome; it is layers. You can not lock the door and leave the window open. Different projects have different needs and different levels of risk. If your risk is high, you should mitigate it with more security layers.

Though the theory sounds nice, what does it mean when implemented?

Projects should have many components, and each component should be able to face compromises without risking the entire project's integrity. Each component should be monitored, and when abnormal behavior is detected, the people in charge of the project should be informed, and based on predefined policies, transactions should be blocked.

ONE TIME TESTING

When building a complex project you need to take into account that the project is a living evergrowing creature. However, the nature of audits is to occur once every few months. Yet, during that time of the year, projects can not risk being less secure. The projects need an ongoing security process.

REAL-LIFE EXAMPLE:

A perfect example of this problem is the Wormhole bridge exploit. Eight hours after a commit with a deprecated function was deployed to the blockchain, $300M was stolen. This case would have been prevented with the proper CI/CD tools that would block the commit in addition to other ongoing security measures that can detect vulnerabilities on the go and not only on the audit-day. This problem is so common even projects that have just done an audit a few days ago tend to add a "last feature" after the audit, which can cause harm.

The Solution

A 360° cyber approach. Projects and protocols aren’t just contracts. They are complex systems that require complex solutions.

By being a native Web3 cybersecurity company, Sayfer can understand the architecture of your platform, the structure of your business, and the budget and development hours you can afford to allocate to a project. We will provide a tailor-made complete cybersecurity roadmap for you.

After you implement all our findings, which will resemble ongoing support rather than a one-time shot, the security of your project will grow at the same pace that your project grows.

This way, security will not be a soft spot that will harm your growth in the future. We will follow these steps to ensure your business’s 360° cyber security protection:

ACTIVE & PASSIVE ASSESSMENT

HISTORICAL HACKS ANALYSIS

BUILD A SECURITY ROADMAP

IMPLEMENTATION GUIDANCE

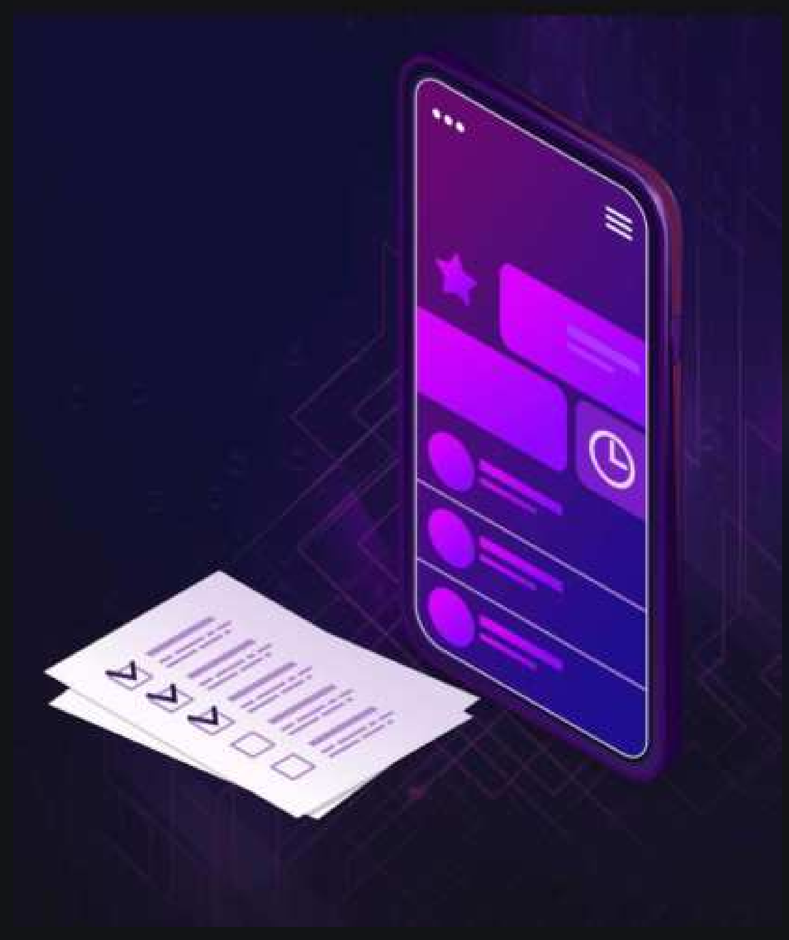
First Step: Conduct Passive & Active Assessment

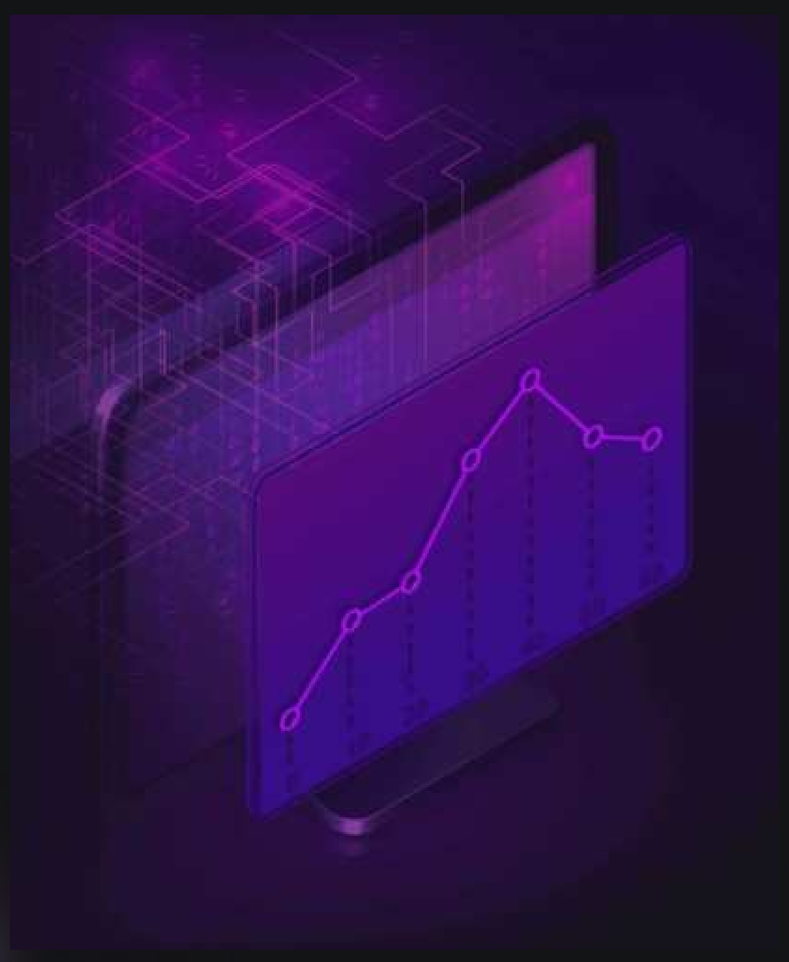
During the first phase of our process to make your project secure, we will perform a full assessment of your business cyber security posture. This part is very important because we need to know your starting point in order to build a correct security roadmap tailored for you.

First, we will use the passive approach. We will talk to you and understand your project. In this first approach, you will tell us as many details as possible about your applications, architecture, employees, potential known security vulnerabilities, and the risks you pose to your system.

Once we have gotten the details in the passive approach, we will then proceed to the active approach. We will “test” your claims by trying to hack into your system. The process will be done either by security audit to the contracts, a standard penetration test to test the web or mobile application security, or a red-team style penetration test to find novel breaches to your system.

After performing both types of assessments, we will have a high understanding of your current business cybersecurity posture and its potential risks.





Second Step: Conduct Historical Hacks Analysis

Hackers are not different from any other human being. They see what their colleagues are doing, and if it works, they will try to do the same.

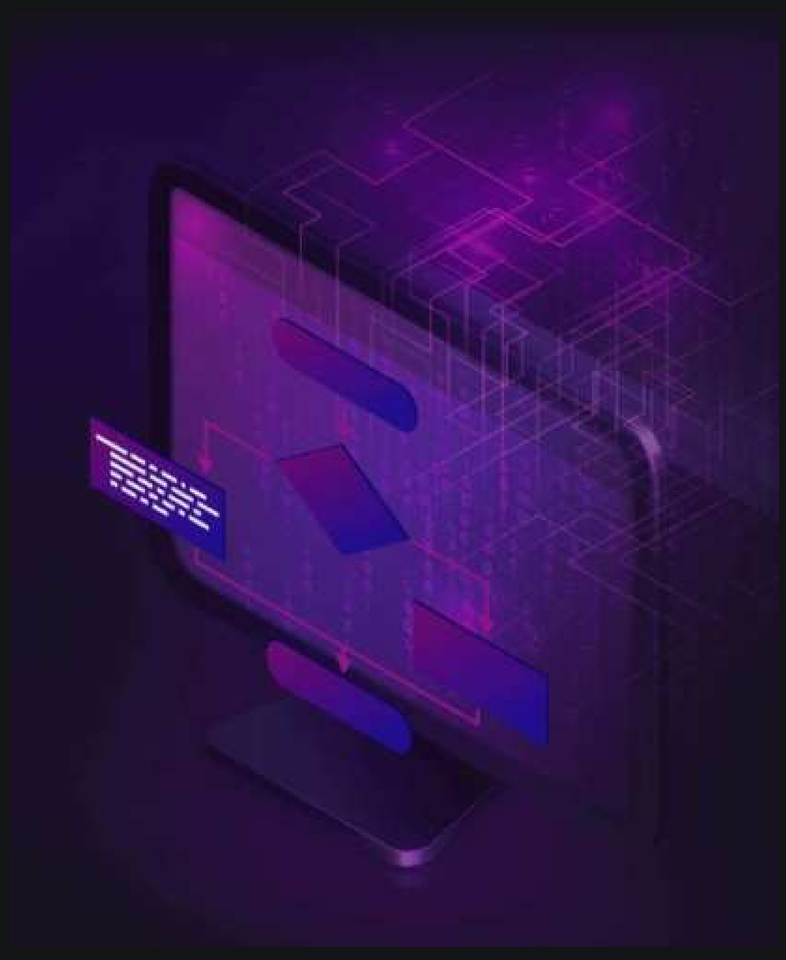
So to predict where the next attack on your system will come from, we will need to understand the current standard practices in the hacker community.

We will do that by performing analysis for any project that has a similar structure and features to yours.

A practical example of such behavior is the centralized exchange hack, which almost always involves the loss of the exchange’s private keys. This tells us that we must implement reliable custodian services with strict policies.

Some Petri dishes for social engineering and advanced phishing attacks include NFT projects, Discord communities, and Twitter accounts. In other attacks, the art is copied and published in a different marketplace depending on the NFT art type and popularity. By understanding these, we will take the educational approach alongside detection tools for the malicious links in the Discord communities and detection tools to find stolen art and notify the marketplaces.

There are many more examples of this, and every project has its own nuances. This is why we must understand the current behavior of the hackers per client.



Third Step: Build a Cybersecurity Roadmap

After gaining all of the above information about your project, such as valuable assets and their risk potential, the market, and the potential security risks your system poses, we are ready to build a security roadmap for you.

What Cybersecurity Roadmap Entails

It is hard for a project to transition from a non-secure to a fully-secure state. You can’t simply do it by adding two tasks to your project management platform and forgetting all about it.

There will be many tasks. Some are more urgent than others, some are blocked by development tasks, some are complex, and you have no idea how to even start them. No worries, this is why we are here.

By building a roadmap for the upcoming months, you will have the opportunity to implement cybersecurity without delaying your main development project’s roadmap.

Steps Involved In Cybersecurity Roadmap

Based on our initial assessment work, each roadmap will be different and tailor-made for the specific project. Though the roadmap will be different, the goal is always the same, which is to map all valuable assets and their corresponding attack vectors and then protect them from several angles, in multiple layers, in runtime, and to make sure we eliminate the single point of failure at the development phase, the lack of security layers and the one-time testing problems.

Most projects have similarities and typical steps to achieve 360° cyber protections. These common steps include

1. Fixing known vulnerabilities - during our assessment, we will find major security vulnerabilities, so the first step is to fix these and make sure hackers can’t exploit them.
2. Mapping assets and their attack vectors
3. Implement Security Layers to protect these attack vectors
   a. 3rd party products
   b. Inhouse developed modules
4. Implement a secure software development process
5. Security architecture modification
6. Develop secure business processes
7. Educate employees about potential risks

Fourth Step: Implementation Guidance

As mentioned above, cybersecurity is not a one-time show - this is a live process like any other development process of a crypto project.

We will provide as much guidance as needed to implement our roadmap correctly. We will escort you every step of the way. This implementation guidance includes:

- We are helping you to implement 3rd party tools and write their policies.
- Consult and provide our knowledge when you design new modules that are directly affecting security or indirectly affecting the security of your project.
- Performing modifications to the roadmap to align with shifting business requirements and help find and eliminate new security breaches.
- Helping you in case of an incident, if something did happen, we would be with you to help you understand what happened, what got lost, and what we can do about it.

The Solution

Summary

Web3 security is hard, and almost any project is a victim of some sort of cyber security attack.

Using our unique approach to a 360° cyber protection we will take your project to the highest possible level of cyber security standards and make sure the bad guys won’t hack you.

To do so, we will first actively and passively find the security assets and breaches of your system. We also analyze historical hacks for projects similar to yours to better know what the common hacks are in the market.

We will then build with you a security roadmap that will add additional layers of security, prevent a single point of failure in your system and integrate an ongoing security testing scheme to make sure your system stays secure even after we are done.

After the security roadmap blueprint has been completed, we will stay by your side to help you correctly implement our findings to make sure that everything is at the highest level of security.

Get in touch

Find out more

https://sayfer.io/

Phone

+972-559139416

Location

Tel Aviv, Israel

Email

info@sayfer.io