Smart Contract Audit for

Our Clients

Tezos

BINANCE SMART CHAIN

1inch EXCHANGE

STARKWARE

METAMASK

tenderly

Why Sayfer

100+ Global Clients	**$1.1B+** Secured by Audits
ZERO Client's Hacked	Money Back Guarantee on Security Audits*
54 Years of Combined Experience	We Work with Any Budget

Sayfer - Who are we

Sayfer is a leading Web3 cybersecurity company based in Israel. We specialize in working with Web3 SaaS companies and startups, providing high-quality cyber security services and making sure our clients' applications are secure.

By employing highly skilled security researchers who are passionate about hacking, and with the combination of our unique *business cybersecurity risk model* we are able to understand our clients' significant potential security breaches and make sure these are protected.

In our smart contract audits, we follow the latest and extensive Smart Contract Security Verification Standard (SCSVSv2), which is accepted by all major regulations such as SOC2, ISO27001, HIPPA, and many more. The standard is also embraced by tech industry leaders such as the Ethereum Foundation and much more Web3 businesses.

At your service at any time,
Sayfer Company.

The Team

The most important aspect of a quality penetration test is the team. This is why we share with our clients the team members who will conduct the research in every project.

Or D., CTO - With over 15 years of experience in R&D and cyber security industry, Or will lead the project and make sure every aspect of the platform is tested.

One of his more interesting findings (which we can publicly disclose) was the famous Badreveal exploit, which affected 10% of all NFT projects. The vulnerability enables attackers to know what is the rarest NFT before the reveal of the project. This allows an attacker an uneven advantage amongst investors to buy the rarest and most expensive piece.

Avigdor Sason Cohen, Web3 Senior Security Researcher - Avigdor is a dedicated security researcher at Sayfer. With a fervent passion for cybersecurity and blockchain, his primary mission is to fortify web3 protocols, making them accessible and secure for broader adoption.

Drawing upon his engineering background, Avigdor thrives when faced with intricate systems and challenges, taking pleasure in deconstructing and resolving them.

In his 5 years of experience, Avigdor has already made a substantial mark, conducting dozen of audits as part of his esteemed work at Sayfer. Furthermore, he has delved deep into multiple distinct long-lasting research projects on DeFi security, a testament to his commitment and expertise in the field.

Not just limited to the technical realm, Avigdor's academic accomplishments are commendable. He holds a BSC in Mathematical and Physical Engineering. Taking his passion a notch higher, he pursued a MSC in Cybersecurity from the renowned ESILV Paris engineering school.

Roman Böhringer, Lead Researcher - Roman is a security researcher and developer with 6 years of blockchain experience. Since joining the blockchain space, he has done over 100 audits as part of his work here at Sayfer and his previous jobs. He works on Solidity (various chains/ecosystems), Rust (CosmWasm, NEAR, and desktop apps), JavaScript/TypeScript (mobile/desktop apps & NEAR), Dart (mobile apps), and Vyper (various chains) projects. Notable clients include Etherisc, Violet Protocol, Nym, FreshCut, SKALE, and Reserve Protocol.
Roman is also a renowned bug bounty hunter who has not only participated in Code4Areana auditing competitions and has also achieved top positions in several of them. Specifically, he has secured the first rank in Rigor (1/132), Party DAO (rank 1/110), Foundation (rank 1/108), and Yieldy (rank 1/99).

Roman has a BsC in Computer Science and a MsC in Data Science with a minor in financial mathematics from ETH Zürich.

Description of service

The service provided is a smart contract audit following the SCSVS guidelines

As part of the research, Sayfer's technical team will look for, investigate and alert on technical, organizational, and logical hazards that could harm one of the customer's contracts. The team will then write a detailed report specifying the security risks we found and best practices that will improve the contract security posture.

During the project, the following contracts will be tested:

Contract Name	SHA256
AccountOnboard.sol	f11a242cf0e912bbd37175deccb19f1ca405542cc7e0c1ff594109b1d52ece8f
GCOTI.sol	5d79bd3d7cfb664349e7a1899f28f69ad89549bb171724a987fde5a0d8989541

These smart contracts are in the following repository:
https://github.com/coti-io/coti-infra-contracts/blob/main/contracts

Additional Services

In addition to the above, we think there are multiple other areas where the security of your organization can be increased by investing more in other areas:

Website Penetration Test

Our experienced penetration testers simulate real-world attacks to uncover vulnerabilities in your websites, networks, and systems before malicious hackers do. Using manual and automated techniques, we attempt to bypass security controls to identify flaws that could lead to a breach. We thoroughly test web apps, endpoints, cloud infrastructure, and more to find weaknesses. After documenting all findings, we provide clear remediation advice to strengthen defenses. Our goal is to help you continuously improve security through comprehensive penetration testing tailored to your environment. Regular testing is key for proactively managing risk.

Marketing & PR Package

Building Trust in Web3

The Web3 world depends on community and trust. We want to earn users' trust by being transparent about how we keep them secure.

Strengthening Security

After Sayfer submits the final report and the fixes are fixed, we will ping you in our chat and share a short form that will allow us to share useful insights on the product or service you have and about the company.

Sharing Our Security Efforts

With your OK, we will write an article talking about the steps we take together to better safeguard your product and company. This will show users some of the behind-the-scenes work to build trust.

Getting the Word Out

We commit to getting your story on 7 popular crypto sites seen by over 200,000 people. Sites include Benzinga, CoinMarketCap, Crypto Daily, and more. We'll promote it on our social channels too for more visibility.

See Past Examples

Check out one media coverage we recently secured for Bolide Finance on CoinMarketCap

key Management Audit

We offer a key management audit to assess your key handling practices and help you determine the most suitable products.
We will focus on your specific needs and provide tailored recommendations to enhance your security measures.

We will check the hardware wallet setup, multi-sig wallet configurations, seed phrase storage and the risk of losing access or stolen wallets, factoring in all of these we can come up with a plan so you can understand the risks and mitigations that need to be applied.

Though this is a high-level audit, we believe it has the potential to deliver significant value to your organization.

Pricing and Payment Terms

The full payment for the services in this price proposal will be in USD excluded from VAT and divided as such:

1. **Smart Contract Audit** - 2K USD

Payment will be made before we start working.

We accept crypto payment as well, via USDC on Ethereum mainnet

Bank account information for transfers:
Company: D.D SAYFER INFORMATION SECURITY LTD
Bank: HaPoalim
Account: 635907
Branch: 722
IBAN: IL020127220000000635907

Project Schedule

The project will start on an agreed-upon date after the following price proposal is signed. Subsequently, the project will follow the following phases:

1. One week before the agreed-upon starting date of the project, we will schedule a kickoff meeting. The meeting will provide us with knowledge about the platform with a live demo. The meeting will also include a short business risk analysis.
2. We will work for 2-4 weeks on the project from the agreed-upon starting date.
1. We will then open a DM communication channel like slack to ensure you'll be updated in real-time on all important information.
3. Then we will share with the client a full detailed report with all the vulnerabilities we found, including an explanation of all the adjustments that need to be done to eliminate or mitigate the found vulnerabilities.
4. At this point, we enter the revision phase where the client's developers will fix the security findings, and we will make sure these are fixed correctly. This step usually takes one to two revisions. The time for each revision mostly depends on the client.
   We will be available to answer any questions before, during, and after the tests are done.

After finishing the revision phase, your system will have a competent level of security and receive the following **Sayfer Badge** (Available in several design options to suit your design materials).

General Terms

1. To the extent that Sayfer has received payment, IP rights developed by Sayfer for the customer in the performance of the service will be owned by the customer.

2. The customer and Sayfer are independent contractors and this proposal does not create an employment relationship between the customer and Sayfer

3. The service and any report or advice are provided “AS-IS” without warranty of any kind. The customer understands and agrees that there is no guarantee that every vulnerability and possible security issue in the platform will be identified during the service, i.e. the service does nor guarantee the nonexistence of any further findings of security issues. Sayfer does not assume any responsibility or liability in relation to the platform.

4. The customer guarantees that the performance of the service does not violate any laws or rights of third parties and that it has obtained the necessary rights and permissions to permit Sayfer to perform the service.

   If there will be a need to deviate from said guidelines, Sayfer will provide notice to the customer prior to such deviation.

Company Tax/Bn/ID Number	Client Signature	registered company name