opsek

Audit Report

Operational Security Audit

OPERATIONAL SECURITY AUDIT / PUBLIC VERSION

PREPARED FOR

3F

PREPARED BY

Opsek

About this report

This is the public version of the Operational Security (OpSec) audit report prepared by Opsek for 3F. It describes each step of the audit, the work completed and the value of that work for the company.

The detailed findings, the configuration changes and the recommendations are in a separate confidential report delivered to 3F.

Some risk remains after any audit. Section 1.9 explains what this means for the company.

Summary

1. Audit steps 3

1.1 Threat modeling 3
1.2 OSINT research 3
1.3 One-to-one OpSec sessions 3
1.4 Security awareness training 4
1.5 Company infrastructure and OpSec calls 4
1.6 Multisig audit and signer training 5
1.7 Tabletop exercises 5
1.8 Reporting and follow-up 6
1.9 Residual risk 6

2. Audit timeline 7

3. Conclusion 8

4. Sign off 9

1. Audit steps

Most attacks on Web3 companies start with a phishing message, a stolen account or a compromised device. The audit covered the company's tools, its processes and its people, in the steps described below.

1.1 Threat modeling

Opsek built a threat model of the company. Opsek studied the company's structure, its operations and its assets to understand what an attacker would target. Together with the leadership team, the auditors listed the assets that matter most, such as treasury funds, production systems, customer data and public accounts. The analysis then identified who would want to attack them and which methods those attackers use against comparable companies. The result was a written threat model specific to the company. It set the priorities for the rest of the audit and showed which accounts, people and processes needed the most attention.

1.2 OSINT research

Opsek collected open-source intelligence (OSINT) about the company and its team members. OSINT is information that anyone can find on the internet without special access. It includes exposed email addresses and phone numbers, credentials leaked in past data breaches, public social media activity and details that link personal accounts to the company. Attackers run this same research before a phishing or impersonation campaign, so Opsek ran it first. Each team member received a private report listing what Opsek found about them, with clear steps to remove or reduce it. Individual reports stayed between Opsek and the team members concerned.

1.3 One-to-one OpSec sessions

Team members took part in private one-to-one sessions of up to three hours, starting with the people who hold the most sensitive access. Each session went through the person's devices and accounts in detail. Professional and personal accounts were both in scope, because attackers often reach a company through an employee's personal email or phone. The sessions covered hardware security keys and phishing-resistant authentication, email accounts, password managers, account recovery options, and the configuration of laptops and phones. The auditor and the team member applied the changes together during the session, so each team member left with the work done. Participants also received Opsek's public resources, including the YubiKey cheatsheet, the SafeCheck tool and the device hardening toolkit.

1.4 Security awareness training

The whole team attended live training sessions. The sessions presented the attack methods currently used against Web3 companies and illustrated them with real cases. Topics included phishing and fake login pages, impersonation on messaging apps, fake job offers, malware delivered through files and links, and physical threats. For each attack, the trainers explained how it works, what the warning signs are and what to do when something looks wrong. The team also agreed on a simple rule. Anyone who has a doubt reports it immediately through a known channel, without fear of blame. After the sessions, team members can keep practicing with chooseyourownthreat.opsek.io, an interactive security story by Opsek based on real attacks.

1.5 Company infrastructure and OpSec calls

Working calls with the administrators of each platform covered the company's shared tools and accounts. The first step mapped the attack surface, which included domains, email, collaboration tools, code repositories, the password manager and public accounts. Opsek then reviewed each platform against its hardening standards and applied the changes with the administrators during the calls. The same principles applied to every platform. Owner and administrator roles were limited to the people who strictly needed them. Phishing-resistant authentication replaced weak sign-in and recovery methods. Each person can now only reach the resources their role requires.

- **Google Workspace**

The workspace holds the company's email, documents and user identities. The review covered the number and protection of the most privileged accounts, the authentication and password policies, account recovery, approval requirements for sensitive administrative actions, and the security alerts available to administrators. Many other tools rely on this workspace for sign-in, so its security sets the baseline for the rest of the company.

- **Slack and messaging tools**

The review covered how the team signs in to its messaging tools and who administers them. Where a tool cannot use hardware security keys directly, the review checked whether sign-in can go through the company's main identity provider, so that the tool inherits the same phishing-resistant protection as the company's email accounts.

- **GitHub**

The GitHub organization hosts the company's source code. The work covered owner accounts, team and repository permissions, protection of the main branches, review requirements before a change reaches production, and the built-in features that detect vulnerable dependencies and leaked secrets.

- **Domains and DNS**

This part of the audit covered the configuration of the company's domains, DNS and email authentication records. These settings protect against domain hijacking, forged emails sent in the company's name and interception of traffic to the company's websites.

- **Password manager**

Opsek reviewed the configuration of the company password manager, its owner accounts and its authentication settings. A vault-by-vault review checked that each team member can only reach the credentials their role requires.

- **Social media accounts**

Public accounts are a frequent target for impersonation and scams. The audit covered the company's public accounts, who has access to them and how that access is protected. Where the platform allows it, delegated access is preferred to shared credentials, so that if an attacker compromises one person, they get limited permissions and the company keeps ownership of the account.

1.6 Multisig audit and signer training

The audit covered every in-scope multisig and the team's signing practices. In-scope multisigs included treasury, operational treasury, protocol upgrades, protocol ownership and position management Safes. Each Safe's configuration was reviewed directly from on-chain state across every network where it is deployed: owners and threshold, signer composition, nested owner Safes, delegated proposers, enabled modules and guards, fallback handler, and Safe version. The audit assessed risk isolation, including whether high-impact powers such as upgrades and treasury custody are separated from routine operations, whether signers overlap across Safes, and which on-chain controls limit the impact of a compromised Safe, such as timelocks, delay modules, guards, and role or spending limits. A signer questionnaire and targeted interviews covered how transactions are proposed, verified, signed, and recorded, how keys are stored, and how the team would respond in an emergency. The engagement included one supervised live transaction, from proposal through execution, and concluded with a gap analysis outlining the risks behind each finding, prioritized recommendations, and support for remediation.

The signer training was a hands-on session focused on two essential checks before signing: intent (confirming the right transaction) and tampering (confirming the transaction has not been altered). Real-world case studies, such as the Bybit theft of February 2025, where a compromised Safe interface led signers to approve a malicious transaction, demonstrated the importance of these checks. More complex attack scenarios were also demonstrated and tested on a live Safe: hidden delegatecalls, malicious calls buried in MultiSend batches, unauthorized module activation, gas-refund parameters redirecting funds, address-poisoning lookalikes, and hash mismatches between the Safe interface and hardware wallets. Signers practiced independently verifying each transaction using a transaction decoder and comparing the results against their hardware wallet display.

3F applied the recommendations from the multisig audit, and the signers completed the hands-on training.

1.7 Tabletop exercises

The team took part in tabletop exercises. A tabletop exercise is a guided simulation of an incident. Participants talked through their response step by step while the facilitators introduced new events that changed the situation. The scenarios came from the threat model and could include a compromised

account, a DNS or email outage, a signer who becomes unreachable, or a physical threat against a team member. The exercises showed how the team communicates under pressure, who makes decisions and which steps were missing. Each gap became an action item or a playbook for the team to complete after the audit.

1.8 Reporting and follow-up

At the end of the audit, Opsek delivered a confidential report to the company. It contains the detailed findings, the changes applied during the audit and the remaining recommendations in order of priority. Opsek presented the report to the leadership team and answered the team's questions. That report stays with the company. After delivery, Opsek remains available to answer questions and to help the team with the remaining action items.

1.9 Residual risk

No audit removes all risk. Attackers change their methods, companies adopt new tools, and people join and leave teams. The work described in this report reduces the likelihood of a successful attack. It cannot guarantee that no incident will happen. The audit prepared the team, its processes and its tools as far as possible to limit the damage and contain an incident if one occurs. This report reflects the company's situation on the dates listed in the timeline. Opsek recommends that the team stays informed about new threats, onboards new members to the same security standards and repeats these exercises at least once a year. The Opsek blog publishes security alerts and analysis of recent incidents that can help the team stay up to date.

2. Audit timeline

The audit ran from April 2026 to 8 September 2026. The table below lists each step, when it took place and who took part.

Date	Audit step	Participants
16 May 2026	Audit introduction	Whole team
April to August 2026	OSINT interviews	Whole team (individual meetings)
April to June 2026	One-to-one OpSec sessions	Whole team (individual meetings)
9 July 2026	Security awareness training 1/3	Whole team
13 July 2026	Tailored security training for HR	HR
15 July 2026	Physical security training for founders	Founders
16 July 2026	Threat modeling	Leadership team
17 July 2026	Security awareness training 2/3	Whole team
24 July 2026	Tailored security training for developers	Developers
30 July 2026	Company infrastructure: Social media	Social media administrators, Opsek
7 August 2026	Security awareness training 3/3	Whole team
10 August 2026	Tailored security training for signers	Signers
18 August 2026	Company infrastructure: GitHub	Administrators, Opsek
26 August 2026	Company infrastructure: Google Workspace	Administrators, Opsek
26 August 2026	Company infrastructure: Password manager	Administrators, Opsek
26 August 2026	Company infrastructure: DNS security	Administrators, Opsek
8 September 2026	Tabletop exercise	Leadership team, Opsek
Async	Company infrastructure: Slack	Administrators, Opsek
Async	Multisig audit 1/2	Signer
Async	Multisig audit 2/2	Signer

3. Conclusion

Opsek conducted a full OpSec audit of 3F. Over the course of the engagement, 3F implemented the priority controls Opsek recommended. It deployed an EDR solution on its devices, which mitigated the main critical severity gap identified in the audit, and issued hardware security keys to all personnel. Opsek audited the whole multisig setup and 3F applied the recommendations. Combined with the signer training, this puts the team in a strong position on multisig security. Following the audit, 3F also acted on two other key recommendations. First, it carried out a full penetration test of its cloud infrastructure using the grey box methodology we recommended, which simulates lateral and vertical movement within the environment while also uncovering other vulnerabilities. All discovered issues have been fixed. Second, it implemented KYC and background checks, carried out by trusted companies, for every current team member and for all new hires from now on.

> No critical gaps remain open from this engagement. Residual risk sits in sustaining these controls over time. To strengthen its security posture further, we recommend that 3F add protection against supply chain attacks such as malicious packages and browser extensions, repeat the cloud penetration test after one year and then on a recurring schedule, keep strengthening its security function and multisig governance as the team grows, and standardize onboarding so new joiners reach the same OpSec baseline as the current team, including a hardware security key from day one.

4. Sign off

Opsek confirms that it performed the audit steps described in this report for 3F during the period stated in the audit timeline.

Name	Louis Marquenet
Title	Head of Research and Audits, Opsek
Date	16/11/2026
Signature	

opsek

This is the public version of the audit report.

RESOURCES

- YubiKey cheat sheet: how to set up and use hardware security keys.
- SafeCheck: where to enable security keys, remove phone numbers and prepare a backup plan.
- Device hardening toolkit: hardening scripts and factory reset guides for Linux, macOS and Windows.
- chooseyourownthreat.opsek.io: an interactive security story based on real attacks.
- Opsek blog: security alerts and incident analysis.

CONTACT

opsek.io
team@opsek.io
linktr.ee/opsek.io