SECURING YOUR DIGITAL WORLD ON THE HIGHEST LEVEL

<Continuous Online Security/>

zerocopter

THE TOOLSET

<The toolset that adds powerful security capabilities to your software delivery process/>

1. Researcher Programs

2. Coordinated Vulnerability Disclosure (CVD)

3. Automated Scanning

Extra Dedicated Hacker Time

THE TOOLSET

1. Researcher Programs

Your team of ethical researchers

<Leverage the skills of our pool of elite ethical hackers to search for unknown vulnerabilities in your applications./>

Many companies are unable to hire, train and retain a team of world-class security experts, with each team member having a unique set of security skills. With a Researcher Program, we offer the possibility to have a selected group of the best ethical hackers search for unknown vulnerabilities on your website or application. All ethical hackers in our platform are screened and tested, so you can be sure we only work with the best and the most reliable hackers in the world.

A Researcher Program is based on no cure, no pay. You decide the budget beforehand, and researchers will only be rewarded if they report a valid vulnerability. Zerocopter's triage team of security experts checks if the reported vulnerabilities are valid and if the reports are complete. During a Researcher Program, you can communicate with the researchers, and with Zerocopter's triage team, about the reports.

Once you solve a reported vulnerability, the researcher will be rewarded: the reward will be subtracted from your budget. An overview of the minimal rewards can be found at 0copter.com/rewards. A Researcher Program ends when the indicated time has expired or once the budget has been spent. You can always extend a Researcher Program or start a new one.

How the Program works:
We help you to use our platform in a way that fits you best. We assist in selecting services, setting up programs, defining scopes and selecting ethical hackers that match your scope best.

- Together, we decide the scope of the Researcher Program;
- You specify the budget of the Researcher Program;
- Together, we determine the start date and length of the Program;
- We assemble the best team of ethical hackers to match your scope.

2. Coordinated Vulnerability Disclosure (CVD)

A ready-to-use reporting infrastructure

<Give users the opportunity to report vulnerabilities discovered in your systems without the need to set up your secure infrastructure./>

A Coordinated Vulnerability Disclosure policy is important for anyone who accidentally runs into a vulnerability on your online environments and wants to report this to you. Implementing a Coordinated Vulnerability Disclosure policy makes you, for example, promise not to take any legal action against your visitor (and maybe even reward them), but only if your visitors follow your rules.

Include the Coordinated Vulnerability Disclosure policy in your applications to enable users and ethical hackers to report vulnerabilities. Our triage team of security experts will review all reports, so your team only deals with full reports on relevant vulnerabilities. The accepted vulnerability reports are presented in our dashboard, you and your team will receive an email if a report has been added or edited. You can decide to reward the person responsible for sharing a vulnerability, and we will take care of the payment!

MONITOR SECURITY

3. Automated Scanning

Regularly check for missing patches, outdated software or other known vulnerabilities

<Utilize world-class vulnerability scanners to monitor the security of your applications./>

Use automated scanners to regularly check your website for SQL injections, cross-site scripting vulnerabilities (XSS), missing security patches, and hundreds of other potential security issues lurking in your app.

Choose your scope by simply adding URLs you wish to scan and schedule the scanner. Scanner reports are scored by severity, parsed into a readable format and immediately made visible on your dashboard. Zerocopter's scanners are updated daily to scan for the latest vulnerabilities.

WHY USE ZEROCOPTER

<Leverage the skills of the world's most knowledgeable ethical hackers to secure your applications/>

WHY ZEROCOPTER

1 **Continuous online security**
We offer true continuous online security. Instead of having your online environments tested one or two times a year, we offer the possibility for a continuous check on vulnerabilities.

2 **Quality**
We select the best ethical hackers in the world to improve your online security. Running a Researcher Program in our platform means that multiple (10, 15, 25, 50, etc.) ethical hackers will search for vulnerabilities within your online environments. It doesn't get any better!

3 **Flexibility**
You decide what services you want to use and when you want to use them. This makes it easy to match your online security policy to e.g. your development cycles or release policy.

4 **Managed service**
We help you to use our platform in a way that fits you best. We assist in selecting services, setting up programs, defining scopes and selecting ethical hackers that match your scope best.

5 **Speed**
Using our platform, you can set up and start a Researcher Program within the hour. This might come in handy when marketing just decided to release a website without notifying you ;)

6 **Triage**
All reports (submitted by ethical hackers) in our platform are being triaged by a selected team of security experts. They make sure you only have to deal with full reports on valid vulnerabilities.

7 **Improve the skills of your developers**
You can choose to add your developers to our platform and let them communicate with our ethical hackers about reported vulnerabilities. This helps developers understand the way hackers look at their code and improves their development skills drastically!

MONTHLY SUBSCRIPTION PLANS

<Three types of monthly subscription to match the services you need for your online security policy/>

Prices are based on the number of projects (e.g. website or mobile app), triage response time and your SLA requirements. View **0copter.com/pricing** for pricing details

About Zerocopter projects
As stated in our subscription plans, we limit the number of projects per plan. Since you can add an unlimited number of members to a single project, you can consider a project as a team. All members will be notified about (and will be able to work with) reported vulnerabilities within the project. We recommend working with multiple projects if you have multiple teams working on different 'scopes'.

Zerocopter security reports
We offer management reports per project containing all vulnerabilities reported in a designated time, current statuses of those vulnerabilities, statistics including financial data, and a management summary explaining your current status of online security, in a way you can easily share it with the rest of your company. You are charged € 1.500,- per report.

STARTER	PROFESSIONAL	ENTERPRISE
Monthly fee **€ 1.000**	Monthly fee **€ 2.500**	Monthly fee **€ 5.000**
Includes **Up to 3 websites or mobile apps**	Includes **Up to 10 websites or mobile apps**	Includes **Up to 25 websites or mobile apps**
Triage Response Time **Within 3 Business Days**	Triage Response Time **Within 3 Business Days**	Triage response time **Within 1 Business Day**
Client Support **App Support (during business hours CET)**	Client Support **App & Services Support (during business hours CET)**	Client Support **App & Services Support (during business hours CET)**
		24/7 support **+ €2.000 per month**

More than 25 projects? Anything is possible. See the next page.

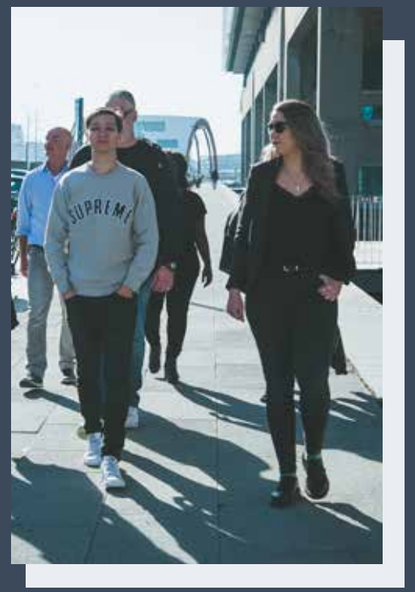
* Prices are based on annual billing. Monthly fees exclude payments to Researchers within Researcher Programs or Coordinated Vulnerability Disclosure, payment fees within Coordinated Vulnerability Disclosure and handling fees within Researcher Programs.
** During business days and business hours, CET.

DEDICATED HACKER TIME

We research **your unique project** for a fixed price

In need of a security check done by quality researchers? Want to steer the focus of the research? For unique projects as yours, we have a code.

With our 10.4 – Dedicated Hacker Time, we acknowledge your specific needs and start you up fast. We appoint a project leader and settle on a fixed price for the amount of work that needs to be done, and in a couple of days, we have four Researchers (or more) on the job. They research what you need researched and deliver you a detailed report of their findings.



<Code 10.4 – Dedicated Hacker Time/>

You do not have to worry about Researchers focussing on matters that are of less interest for you at that moment. Additional advantages our 10.4 offers are:

- **Quality**
  Zerocopter Researchers/White Hats that have undergone a rigorous vetting
- **Custom arrangements**
  Even checking what is nót broken is on the table!
- **A fixed price**
  No matter the number of vulnerabilities we find
- **Quick start**
  Dedicated Hacker Time can be set up and started in one (1!) workday
- **Live action**
  Follow everything we do live –and take immediate action– through our platform
- **Direct communication**
  Quick and direct communication through Slack

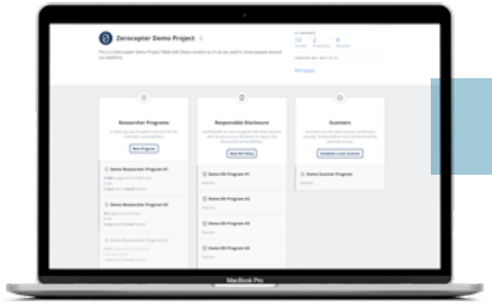
Receive a detailed report

Based on the scope of the project, we deliver a detailed report of our findings to you. This key-information provides you with the opportunity to improve your security measures further.

THE ZEROCOPTER PLATFORM

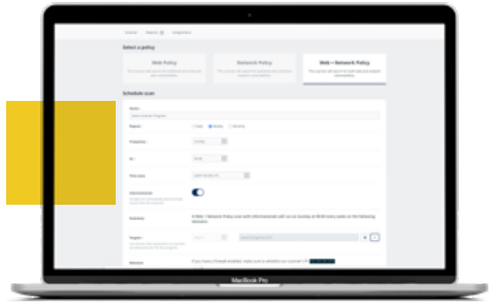
<A sneak peek of your platform for digital security/>

Schedule a demo on **0copter.com/demo**



Get started

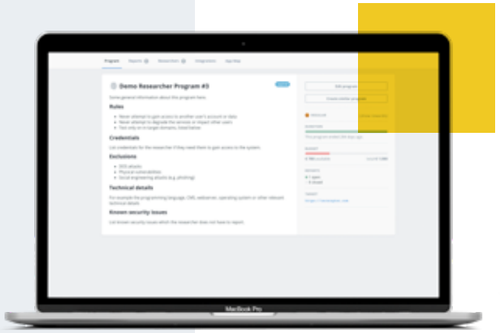
Get started with continuous online security by creating your first Zerocopter project! Add your colleagues as members and immediately start using our services.



Automated Scanning

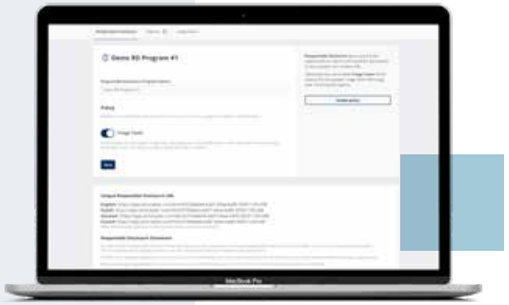
Create a scanner schedule to regularly check your online environments on known security issues like missing patches, insecure libraries or invalid certificates.

THE ZEROCOPTER PLATFORM



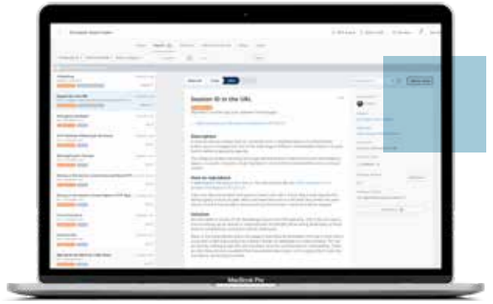
Researcher Programs

Start a Researcher Program and have the best ethical hackers check your online environments on unknown vulnerabilities. By determining your budget, your scope, the duration of the program and the number of researchers, you are in control, and we assist you all the way! Bug Bounties is a comprehensive way to have your scope tested, based on a no-cure-no-pay model.



Coordinated Vulnerability Disclosure (CVD)

Setup a Coordinated Vulnerability Disclosure policy, so anyone can report a vulnerability on your online environments. Our triage team will check all incoming reports, so your team will only work with valid and full vulnerability reports.



Focus on fixing

Once a new vulnerability report has been filed, start working on it right away! Our team, and of course the researchers, are available to assist you. Invite your consultants on single reports and chat with your team members. You focus on fixing the vulnerabilities, and we deal with the rest!

ABOUT ZEROCOPTER

<Zerocopter was founded with the ambition to bring continuous online security to the world/>

ABOUT ZEROCOPTER

Zerocopter enables you to confidently leverage the skills of the world's most knowledgeable ethical hackers to secure your applications.

Working as ethical hackers and security researchers over the past decade, we learned that online security became a Wild West for companies. Trying to get control of risk levels by assigning security teams, hiring security companies at scheduled intervals and licensing multiple expensive solutions, but eventually, ending up with a security flow that is not insightful and with reports scattered all over the place. Online security isn't just about implementing smart technology, it is also about including the right people, gathering insider intelligence and the ability to align all these processes towards one goal. Instant access to the best security expertise and tools is essential for organizations to be able to keep up with rapid developments on 'the other side'.

Edwin van Andel CEO

zerocopter.com

zerocopter.com | info@zerocopter.com | +31 20 261 67 43