BRIGHTSIDE

Helping organizations prevent AI-powered cyber attacks before they happen

BRIGHTSIDE

Incredible AI engineers, years of experience in ML
Backed by advisory board of cybersecurity and privacy experts

Team

Andrey Suzdaltsev
Co-Founder & CEO

Deloitte. analytics institute

Ex-Deloitte Analytics Institute

Ex-CTO @ Luxury watch company

9 years in Machine Learning

Andrey Lazarev
Co-Founder & COO

BCG BOSTON CONSULTING GROUP

Ex-BCG

5+ years in business operations

Sergey Lavrikov
CTO / Chief of ML

soveren

kaspersky

Ex-Soveren (Lead ML)

Ex-Aitu-DALA (Head of ML)

Ex-Kaspersky (Lead Data Scientist)

10 years in Machine Learning

18 years in Software engineering

3 Full-stack engineers

2 Marketing specialists

2 UX designers

Advisors & Investors

Rand Hindi

Founder @ Zama.ai

Serial entrepreneur

Deep tech investor

Mike Podlas

14+ years in product management

Founder @ Undatify – EU Data Privacy startup

Alex Kosik

3X Entrepreneur

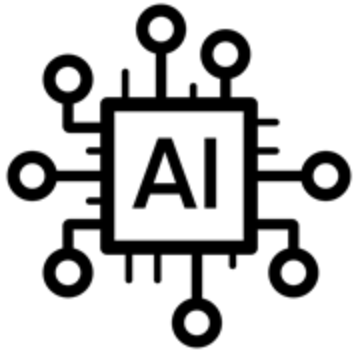
Operations Expert

Investor

BRIGHTSIDE

Since the launch of ChatGPT, the number of targeted cyberattacks skyrocketed by 1,265%

Large Language Model



+

Personal Data

=

Targeted fraud

Hello Name - Alex Peterson,

Given your position of Position - QA engineer at Job - Alibaba Group I wanted to invite you to the conference in Location - New York on Interest - Testing.

Please register with the following link: Phishing link

Best regards,

John Conrad

BRIGHTSIDE

Most companies still rely on outdated security awareness courses, which are not effective against AI-powered attacks

Classic trainings – outdated, ineffective

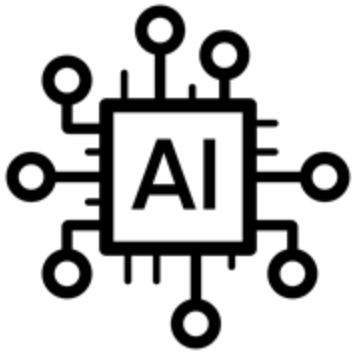
Engagement – extremely low

Approach – memorizing, hope

BRIGHTSIDE

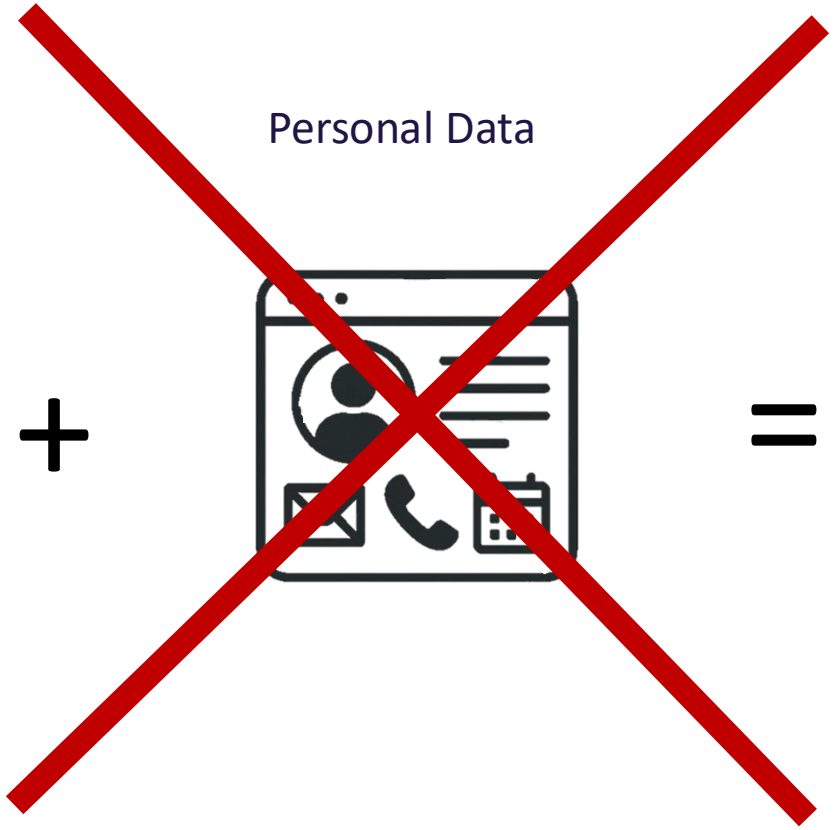
We can’t stop hackers from using AI – but we *can* stop them from accessing personal data to generate fraud

Large Language Model



+

Personal Data



=

Targeted fraud

Hello Name - Alex Peterson,

Given your position of Position - QA engineer at Job - Alibaba Group I wanted to invite you to the conference in Location - New York on Interest - Testing.

Please register with the following link: Phishing link

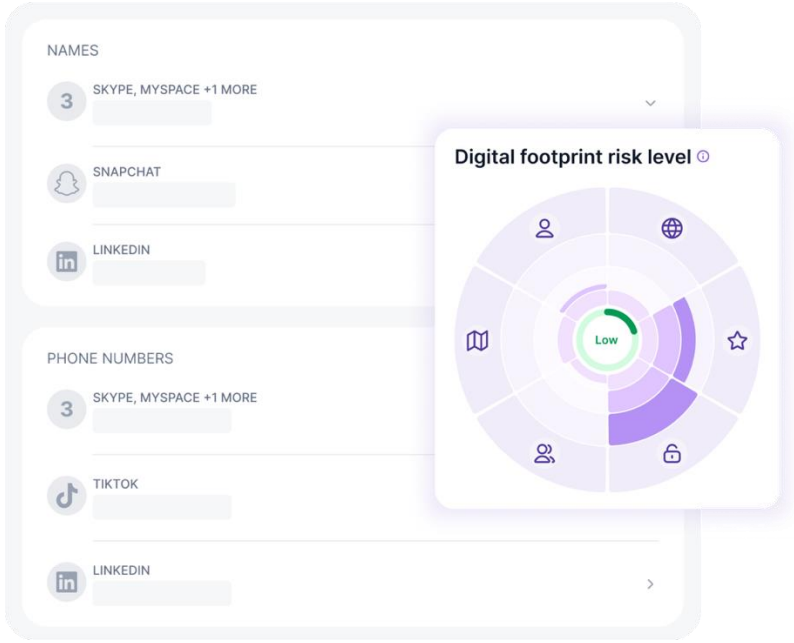
Best regards,

John Conrad

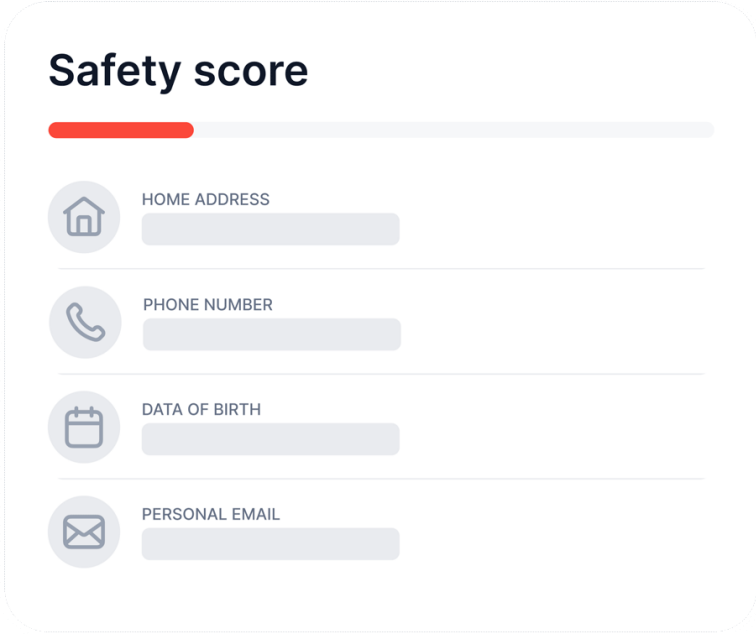
BRIGHTSIDE

AI agent finds and proactively removes vulnerable data from the Web reducing company attack surface

Personal safety portal for each employee to view and manage their data exposure, radically boosting employee engagement



Eliminate employee data risks with proactive data removal from data brokers, online services and more



BRIGHTSIDE

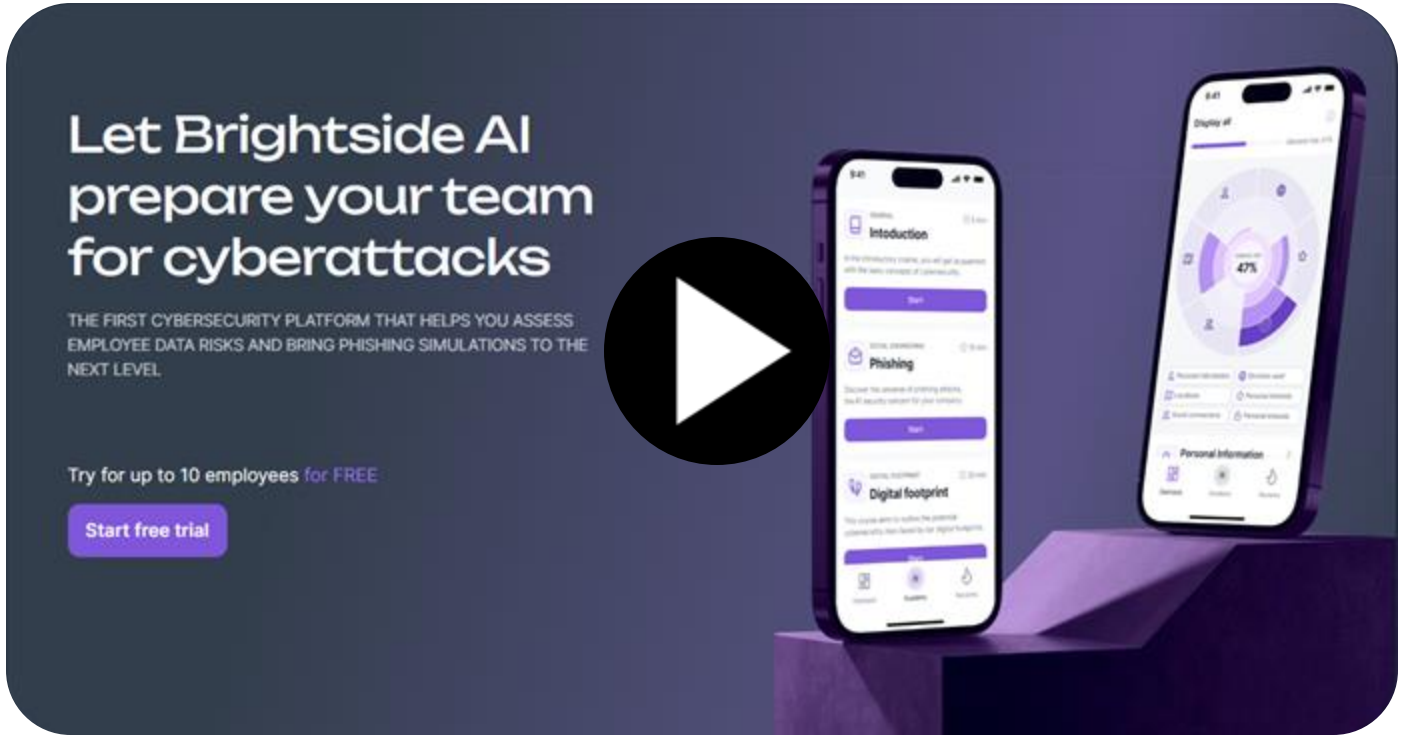
With remaining public data, we run realistic AI attack simulations mimicking real hackers and preparing teams for latest threats

Improve cybersecurity with hyper realistic AI phishing tests and deepfake simulations

Close security knowledge gaps with relatable and interactive chat-bot courses

BRIGHTSIDE

Quick video demo showcasing Brightside's capabilities



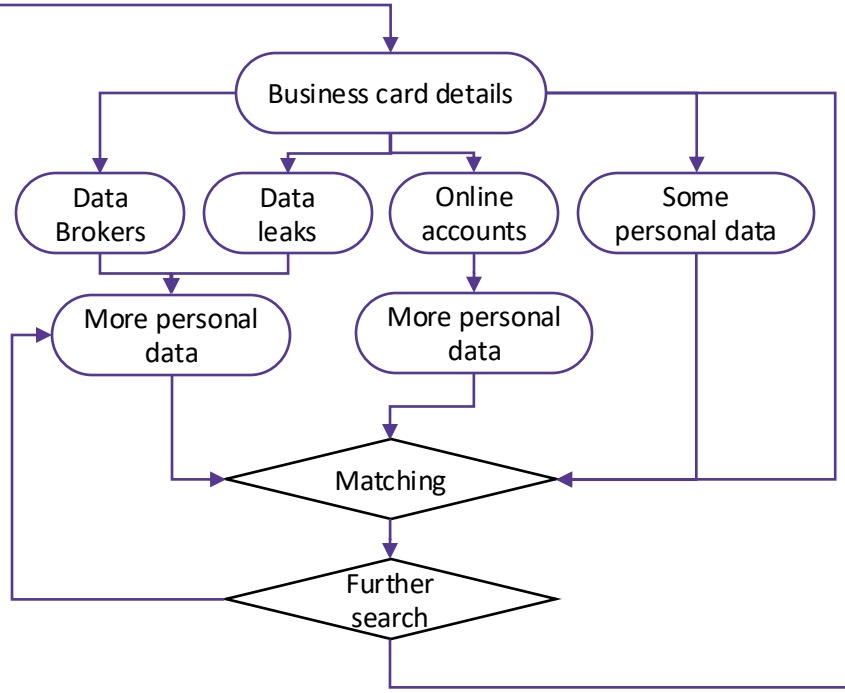
Brightside AI in action

Fully automated OSINT enables quick, accurate and scalable data search – AI private investigator for the whole team, not just C-level executives

Input – business card details

AI search and matching
(the Secret Sauce – over simplified)

Output – actionable online safety report



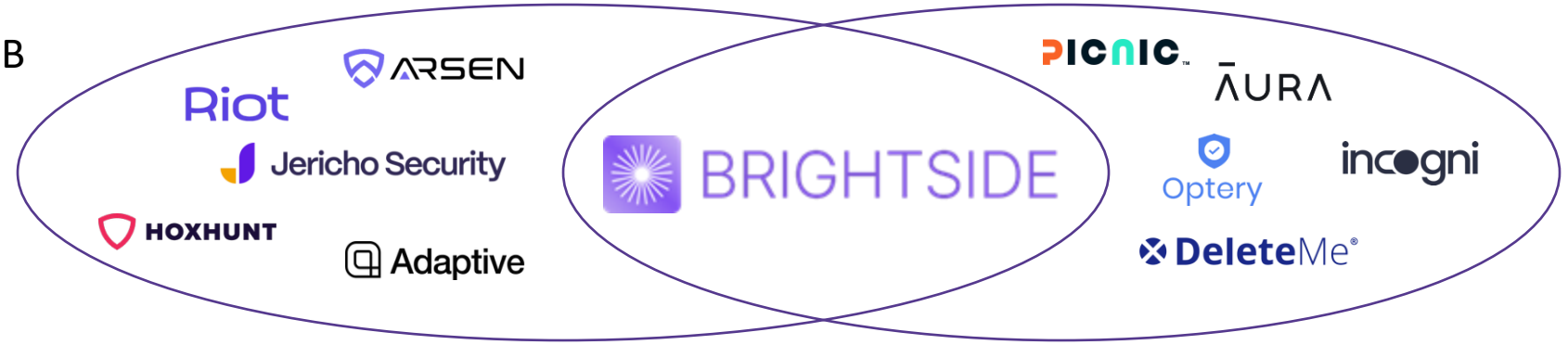
Complete online safety report

- Full and actionable online safety report with insights and immediate actions
- Covers all publicly visible data (both work and personal)
- Automatically re-scanned every month

BRIGHTSIDE

Current B2B security focuses on basic awareness, and B2C tools on data removal – Brightside AI improves on best of both worlds

New-gen B2B awareness



B2C data removal tools

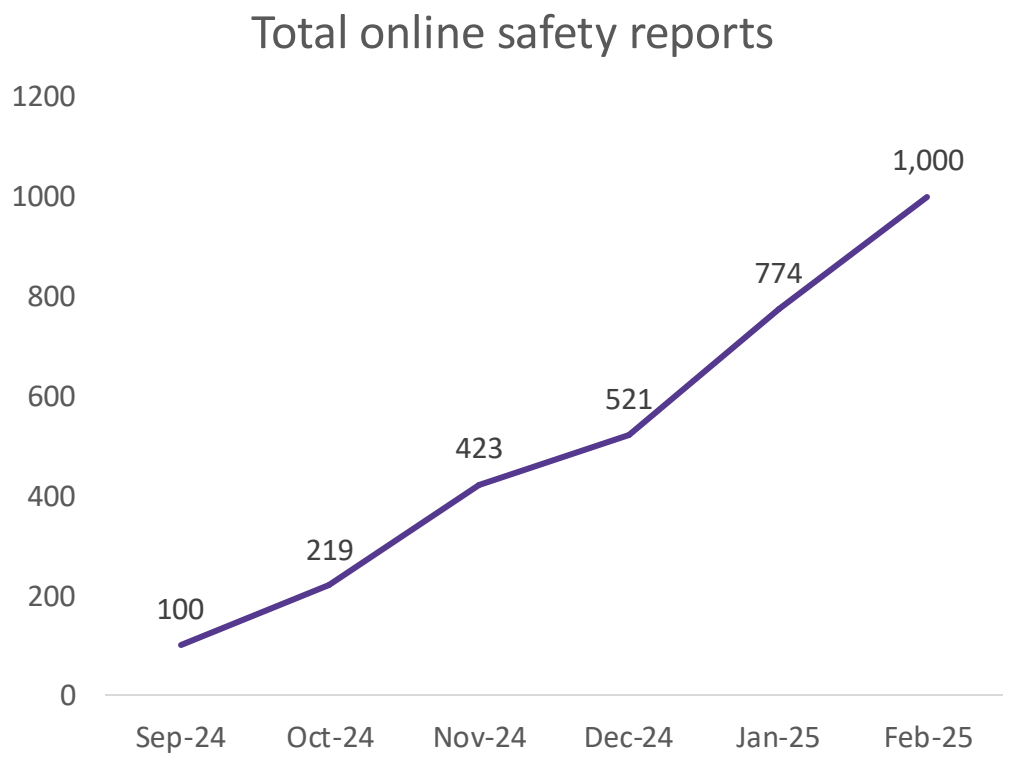
- Pain for the employees
- Fail to address actual attack surface (employee data online)
- Don’t show true risk profile of organization (only an estimate based on tests)
- Fail to do realistic simulations due to lack of employee actual data

+ Making sure employee data vulnerabilities ACTUALLY get removed from the Web (reduced attack surface -> less attacks)
+ Realistic tests with AI and employee details
+ Personal value to employees (individual online safety) -> unmatched engagement

- Cover only data brokers (not the full picture)
- Lack of security awareness tools, which is a MUST for business compliance
- Don’t provide an actual solution (removal of data at source), data brokers will just recollect all data again from public records

BRIGHTSIDE

We've already secured people 1,000 times and counting



10x growth in 6 months

Clients in:

US EU CH

BRIGHTSIDE

Teams love our approach due to its personalization, effectiveness and employee engagement

"It's like a personal security assistant for each team member.
We finally manage our human risk at scale not just simple courses and trainings"

- CISO, 20,000+ employees

"I can finally do something about the AI fraud my team keeps receiving"

- CISO, 150+ employees

"No one told me there was so much info about me that could be exploited for an attack.
I just had to get it for all my team"

- CISO, 250+ employees

BRIGHTSIDE

Current contracts value – 100k USD, current pipeline value – 680k USD

Current contracts

ZAMA

MSC CRUISES

INNOVAUD
THE PERFECT SETTING TO INNOVATE

+ 3 more

Current pipeline

logitech

QOQA

REPOWER
Unsere Energie für Sie.

+ 4 more

Lead generation

1,100 – monthly B2B interest volume

BRIGHTSIDE

One exposed employee can cost millions.
Subscription model ensures continuous security, not one-time training

Real-time employee online safety + preparation for latest threats

Flexible pricing ensuring best value for everyone from C-level management to regular team members…

…and even their families reducing hacking risks from all angles

$60-180/year

Individual employee protection

$325/year

Family protection reducing hacking risks from all angles

BRIGHTSIDE

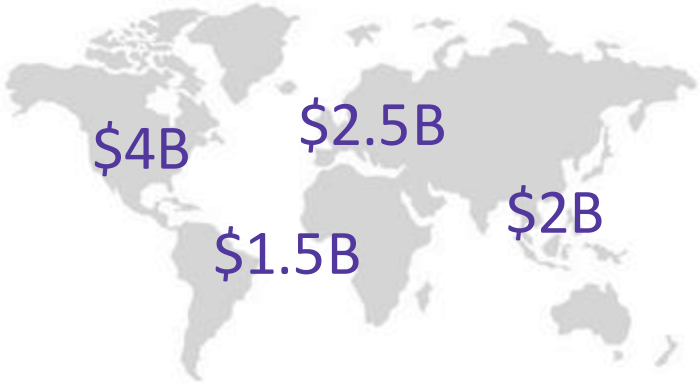
The industry shift is happening now. Investing in people, not firewalls is a new norm with $10B+ in global annual cyber awareness expenditure by 2027

Change drivers:

- Classic security trainings are outdated and ineffective
- AI-powered scams are nearly undetectable
- Employee engagement in traditional cybersecurity is low

Global TAM

$10B+



USA SAM

$2B+

Focusing on:

- Manufacturing
- Healthcare
- Finance & Insurance
- IT
- Business services

BRIGHTSIDE

Securing the US market is crucial for rapid growth and achieving $100M in ARR by 2030

Step 1:

Direct founder-led sales

In progress

Securing key large customers with founder sales model

Done

Striking partnerships with cyber influencers for brand positioning

Step 2:

Expert-2-expert channel

In progress

Onboarding CISO experts as ambassadors, establishing trusted brand

Done

Enabling ambassadors with value-driven product demo

Step 3:

Distributors and integrators

Done

First partnership with large security distribution firm in the US

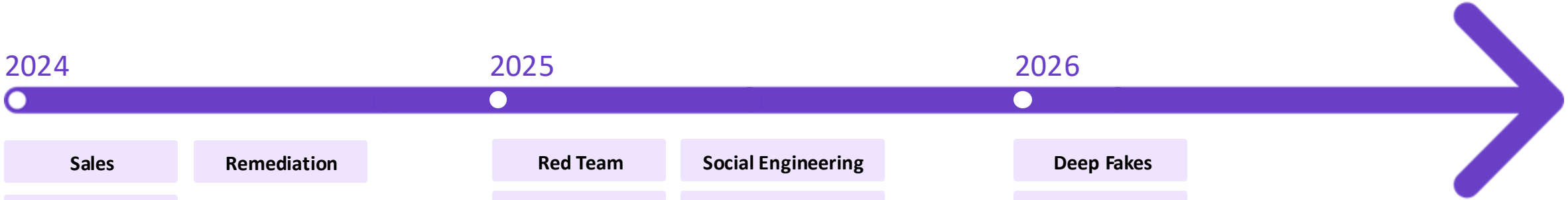
In progress

Extending partnerships with MSSPs for wider client coverage

In progress

Preparing a scalable sales playbook for easy sale and integration by partners

The roadmap supports our ambitions to reach EUR 100M ARR with 20k+ clients in the portfolio



2024

Sales | **Remediation** | **Personalization**

- Subscription release
- AI private investigator 2.0 (deeper and better data search)

2025

Red Team | **Social Engineering** | **Defense** | **Multi-step attacks**

- SMS/chats (SMSishing) and phone (Vishing) simulations
- Complex phishing exercises (multiple messages per attack)
- Email inbox phishing reporting and detection system
- Multi-language support
- 1-click tools to remove data from the Internet

2026

Deep Fakes | **Defense**

- Deep fake video calls simulations
- Personalized phishing detection across all devices

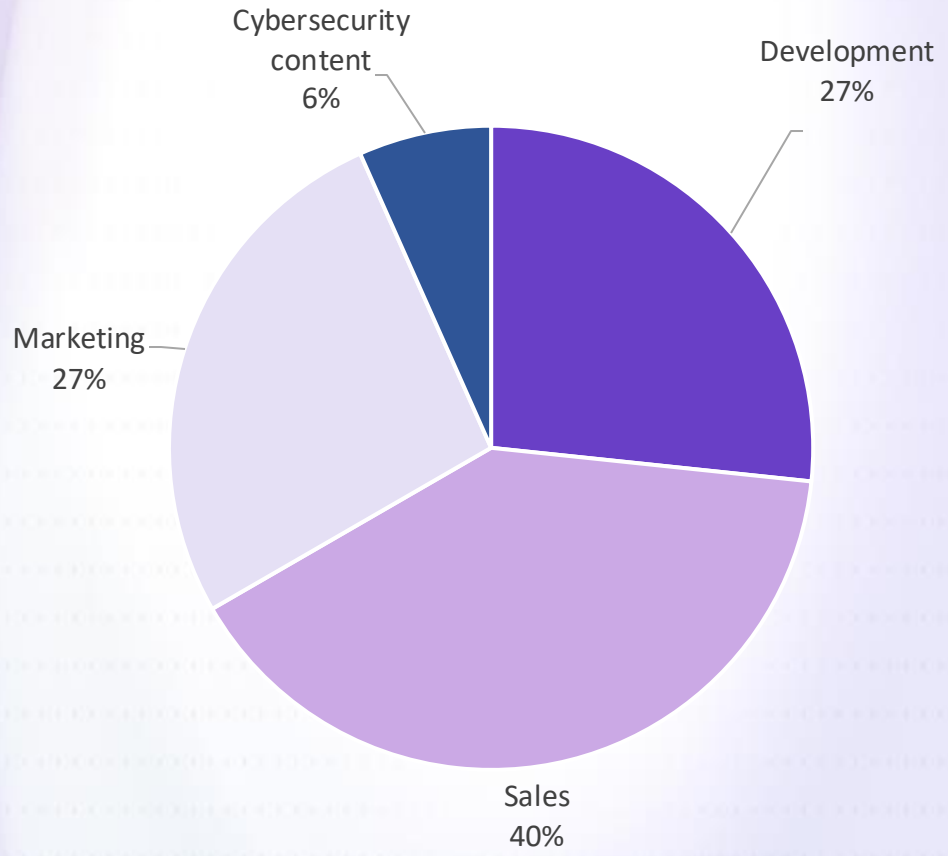
BRIGHTSIDE

Investment opportunity **$3M**

To scale the US customer base and develop state-of-the-art AI cybersecurity tools

Protecting millions of employees across the world

Use of funds



Scan to receive personal data assessment

Access code: **USVC**

www.brside.com/demo

BRIGHTSIDE

Want to participate in a round?

Andrey S. - CEO

as@brside.com

Andrey L. - COO

al@brside.com

www.brside.com