

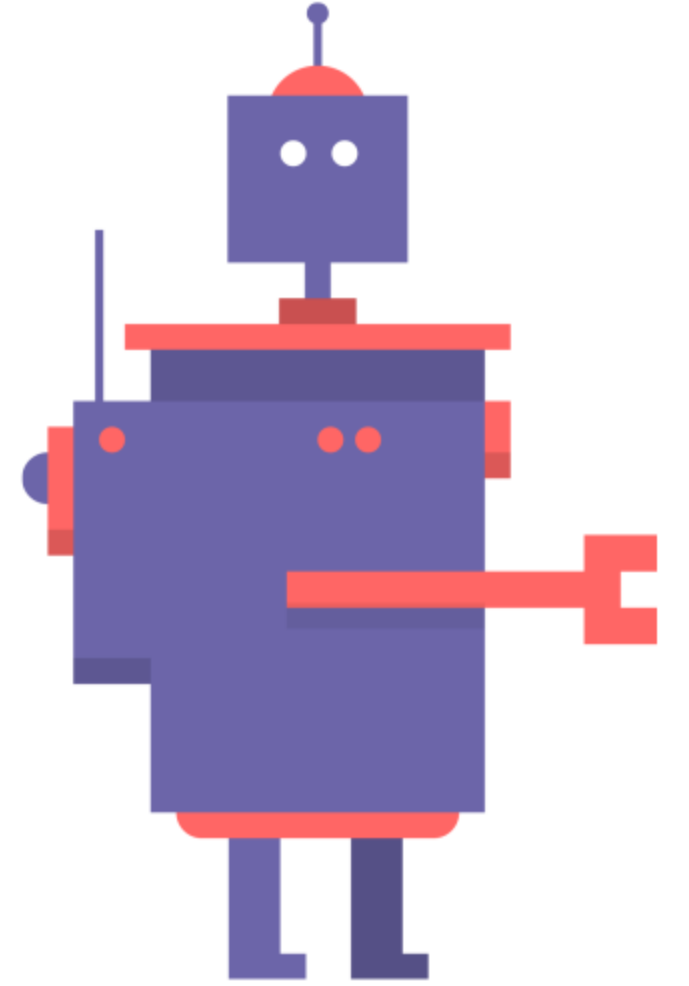
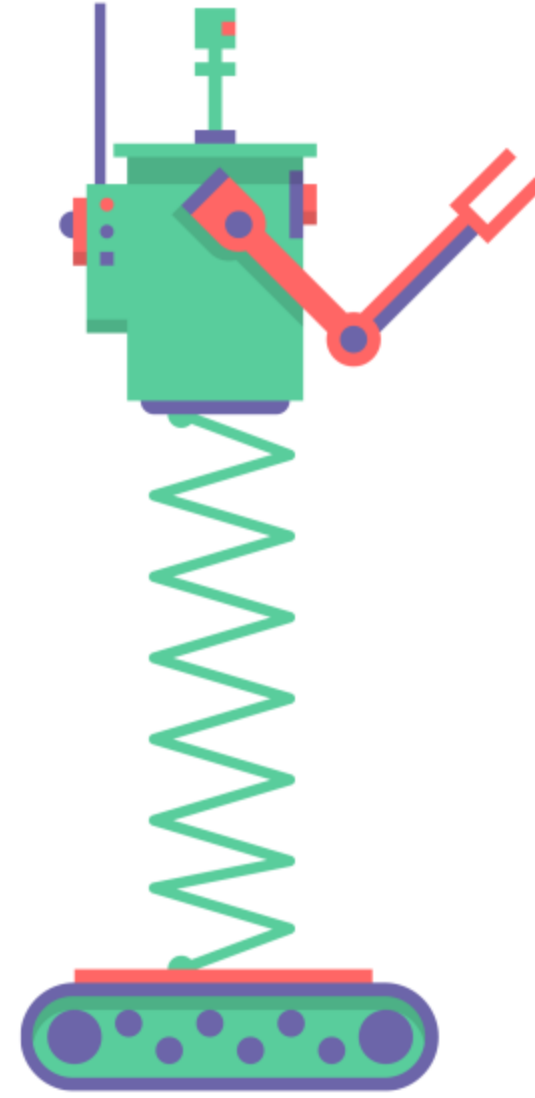
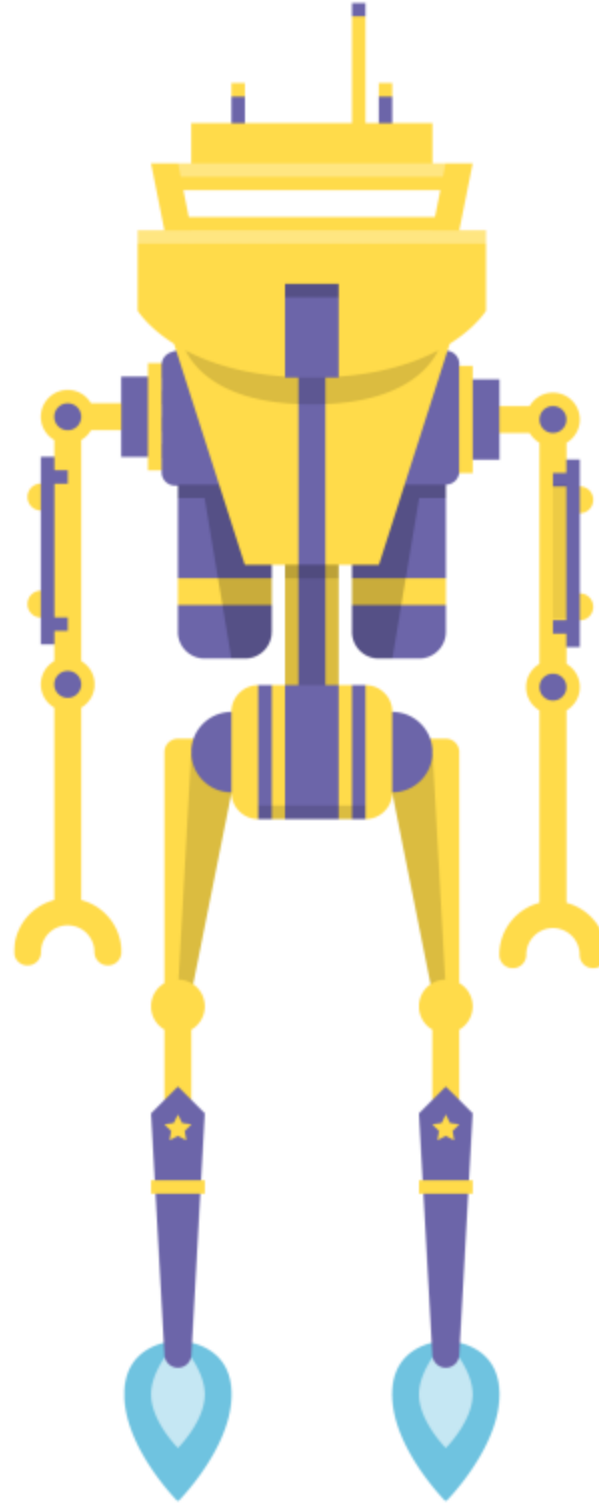
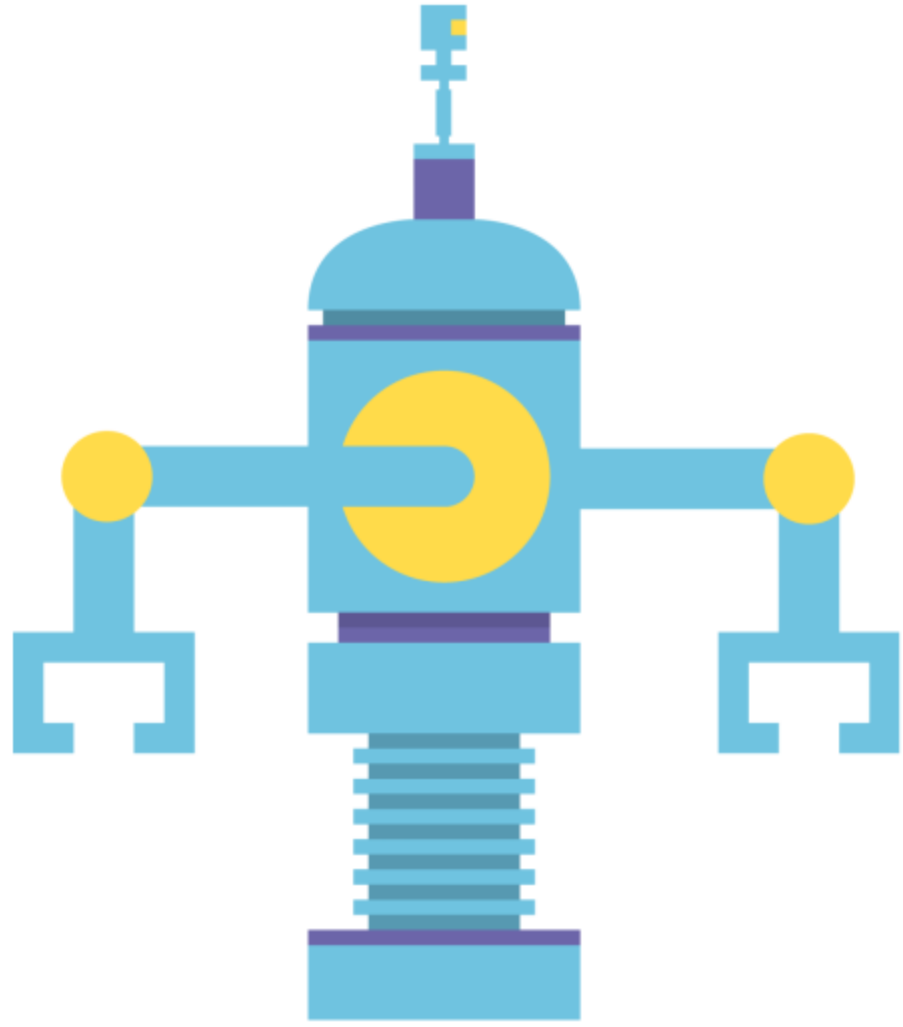
**Y**andex

Yandex Security

Security in developer's life.  
Knowledge is power

```
$ whoami
```

- › Product security team lead in [Yandex](#)
- › [OWASP Russia](#) chapter leader
- › `(yandex|google)://oxdef`





Automation is security's  
answer to the agile  
development problem



But...



Just writing secure code  
is better

# Problems and questions

- › How to avoid questions about typical vulnerabilities?
- › How to make developers aware about security processes and controls?
- › How to make developers read security guides?
- › How to measure the result?
- › How to use these metrics in other security activities?



# Security in developer's life

- › Interview
- › The first day at work
- › The first lines of code
- › The first security audit
- › The first security issues in the code

# Interview

- › Learn about your new developers from the interview
- › If you use hire platform then add security related questions to it
- › After the interview is completed you can automatically gather and analyze answers via API

# The first day at work

- › “Welcome” meeting and small introduction talk about security processes
- › Internal staff portal with API
- › Use this API for monitoring new developers
- › Automatically send them “Welcome” letter

# How to write secure code at Yandex

Alexander, welcome to our team!

Here at Yandex we make beautiful, functional, fast AND secure services!

Security team had prepared security guides for you:

<https://internal-portal/security/guides/>.

Please, find some time to read them as soon as possible.

If you have any questions feel free to contact us.

--

Product Security Team

<https://internal-portal/security/>



# Internal security portal

- › Security guides
- › Quick links to security self-checking services
- › AskSecurity contact form
- › Latest posts from internal security blog
- › Current projects



# Structure

- › Separate guides for web, Android, iOS and C/C++ developers
- › From common topics and practices to typical issues and specific cases
- › Use cards as a format for publishing complex issues
- › Developers don't want to read "long read" articles
- › Content should be easily searchable based upon factors such as platform, programming language, framework, typical words, etc.
- › Integrated self-assessment quiz and feedback form



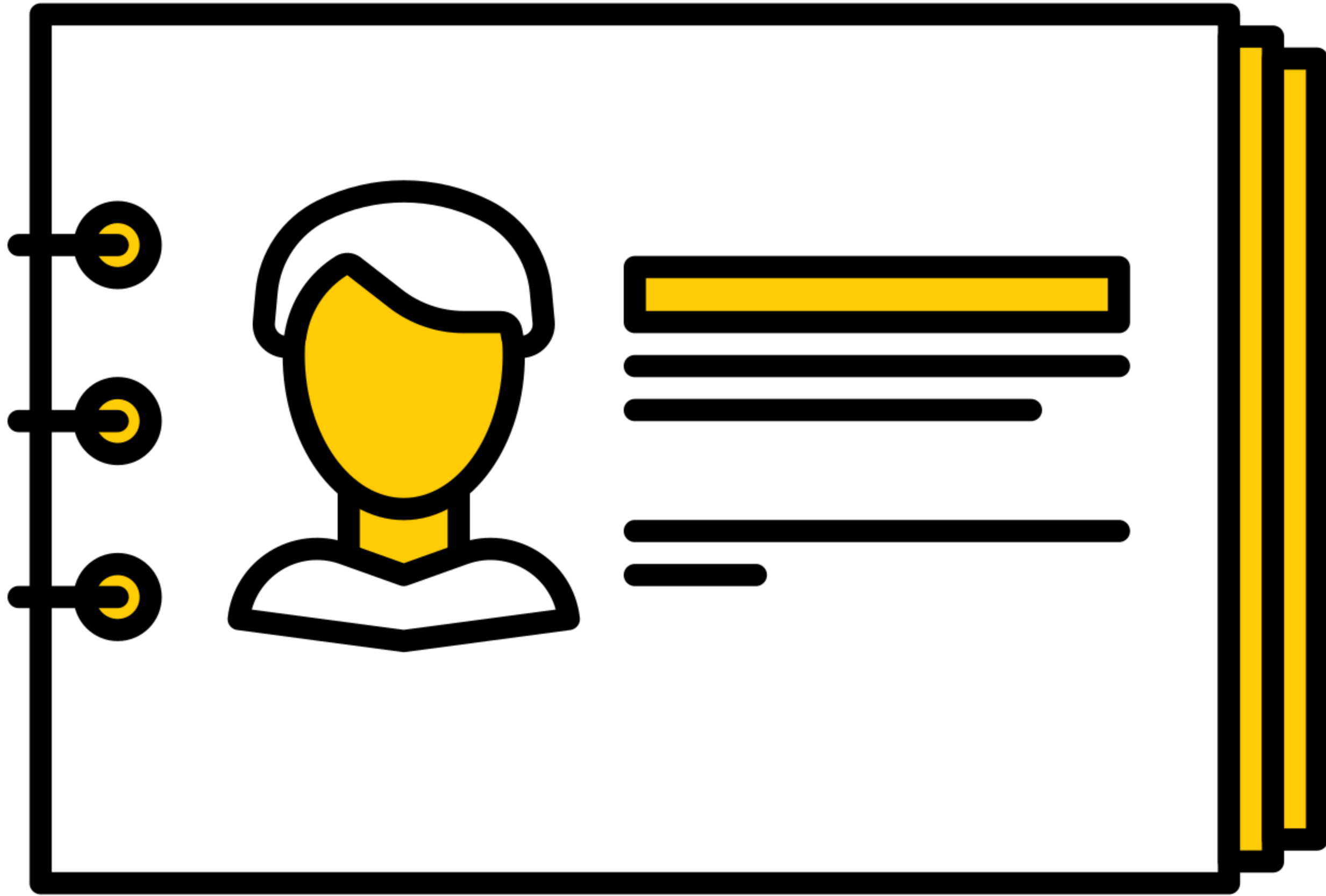
# Content

- › High-level best practices: authentication/authorization, input validation, output encoding, error handling, etc.
- › Security team internal processes, services and controls
- › OWASP Top 10 typical threads and mitigations
- › Specific internal topics



# Quizzes and courses

- › To measure how well developers read the guides
- › Quiz should not take a lot of time
- › Quiz should not be boring!
- › Use FOSS, e.g. learning management system like [Moodle](#)
- › Other interesting services: [OWASP Security Knowledge Framework](#), [Hacksplaining](#), [Codebashing](#)



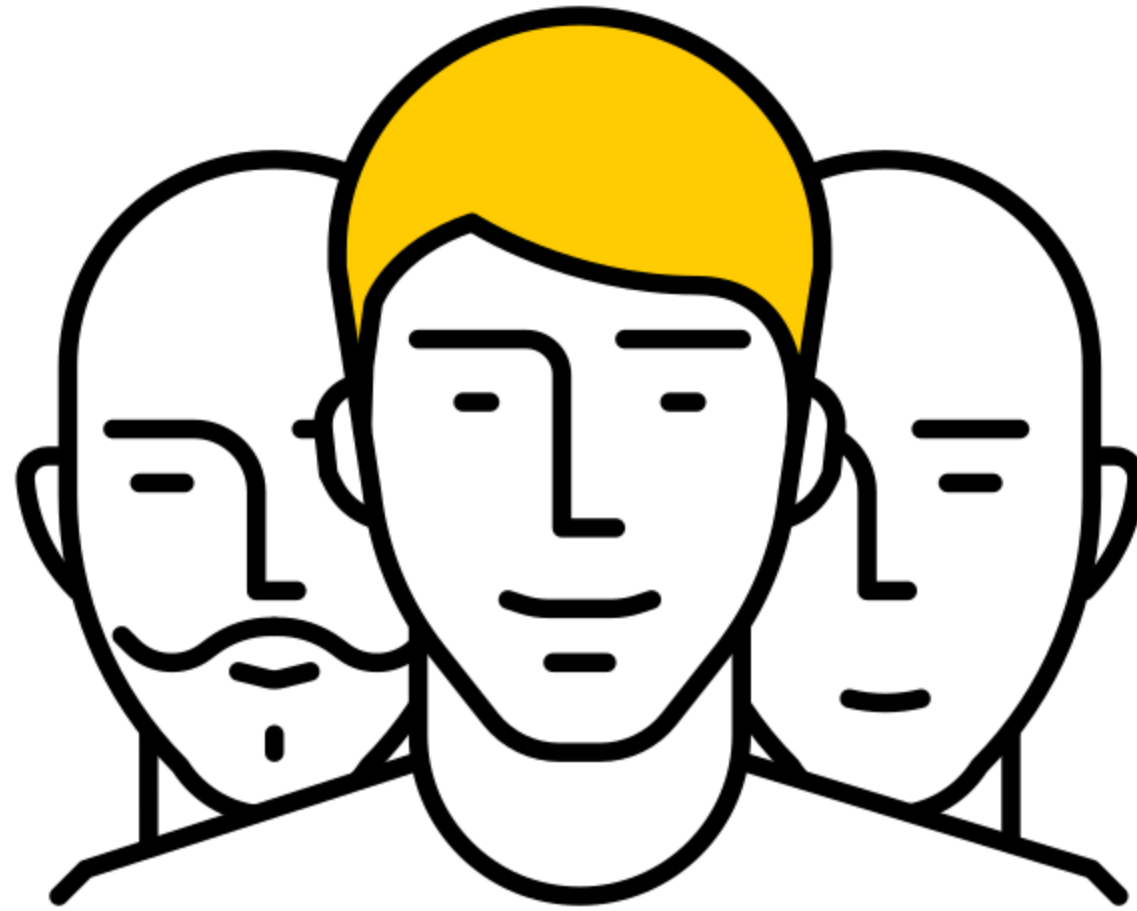
# Developer's profile


- › Badges for various security activities
- › Special flags, e.g. for reading our guides
- › Security “karma”
- › Use this information to make more accurate threat analysis of new releases

# Metrics

- › 60% developers briefed on security guides within the past year
- › No more questions about security issues
- › More followers in internal security blog

# Let developers be security champions





Application security  
should be closer to  
developers. From the  
first days and lines of  
code



Q&A

# Contacts

Taras Ivashchenko

Product security team



oxdef@yandex-team.ru



oxdef



@oxdef