

TOP SECRET

Mission objective

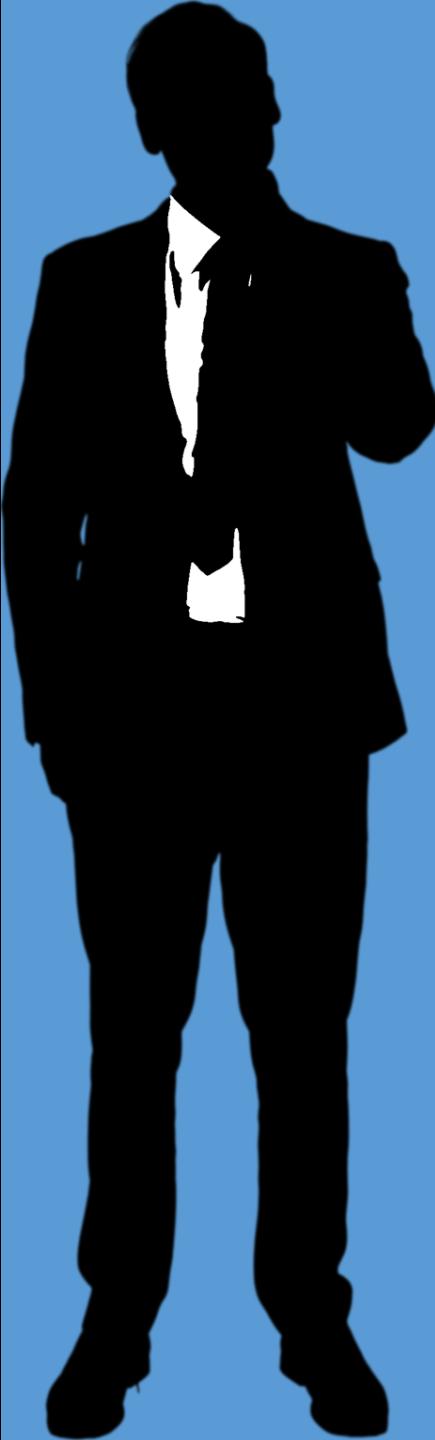
Design process of software development that minimizes risk of being hacked

Start time

NOW

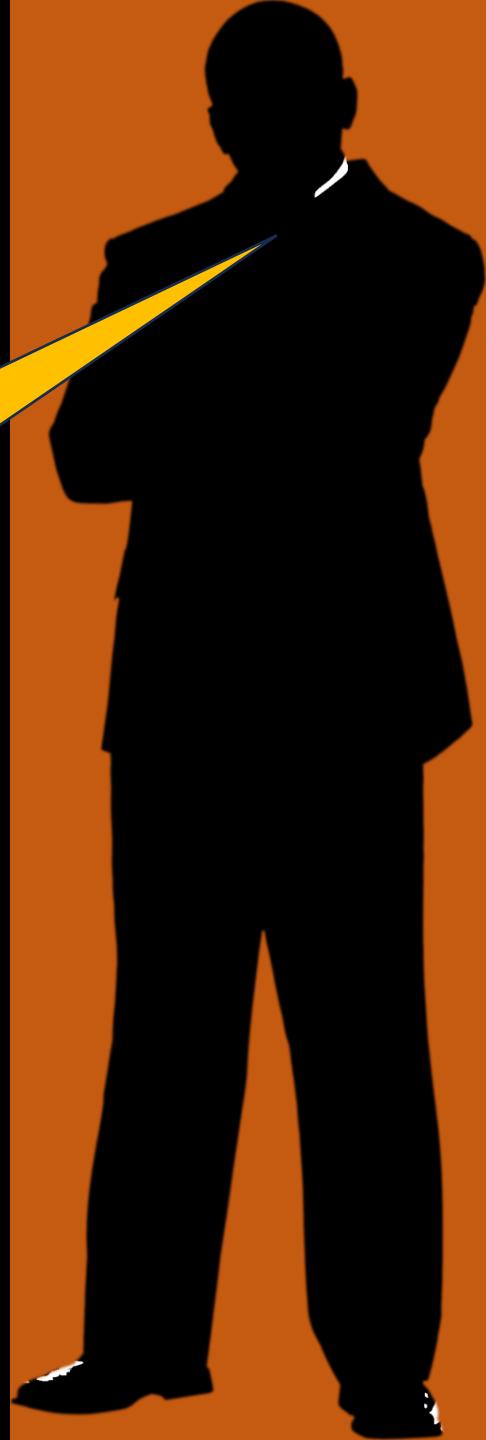
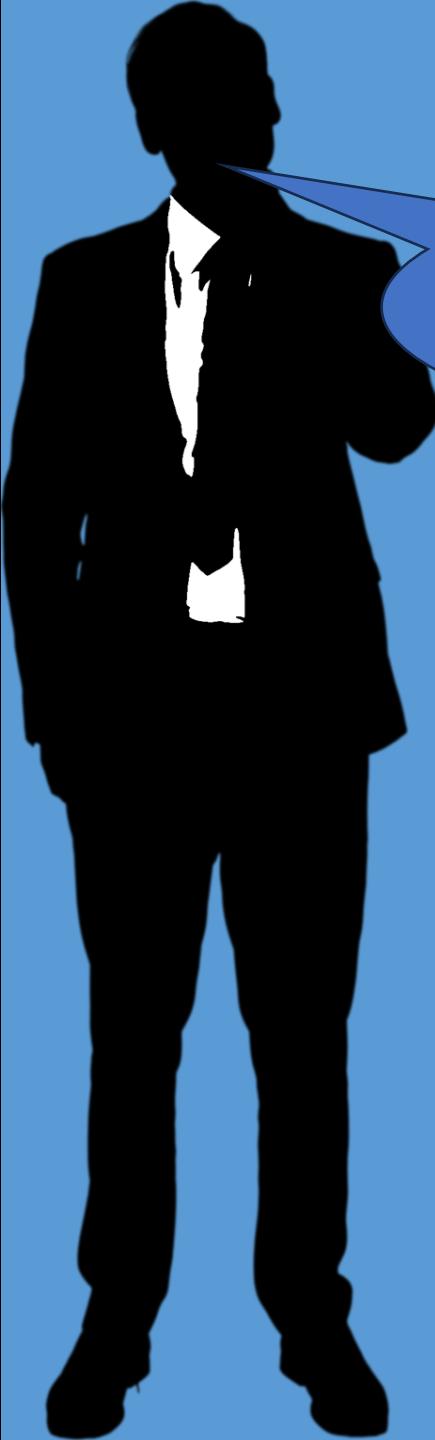
Agents

Devel & Secar



S
E
C
A
R

D
E
V
E
L



So another 0
day problem...

Yes... thankfully
it's already fixed!

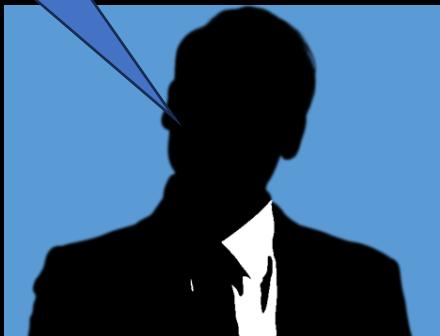
0 day problem





Nope. Don't like that.

At all





What vulnerability
scanner was used?

A scanner...

S.A.S.T.

S.A.S.T.

t
a
t
i
c

S.A.S.T.

t p
a l
t i
i c
c a
t t
i a
n o

S.A.S.T.

t p e
a p c
t l u
i i r
c c i
a a t
t t y
i i
o o

S.A.S.T.

t p e e
a p c s
t l u t
i i r i
c c i n
c a t g
a t y
i i g
n i n

S.A.S.T.

S.A.T. • S.C.A. D.A.S.T.

t a t i c
a p l i c a t i o n
e c u r i t y
e s t i n g

sonarQube



snyk.io/advisor

Find the best package for your next project.

Search and compare over 1 million open source packages.

npm ✓ react, angular, vue, moment, passport, mocha

PyPI

Go

Docker

Search packages

nodemon v2.0.7

Simple monitor script for use during development of a node.js app.

NPM README GitHub Website MIT Latest version published 2 months ago

npm install nodemon

Explore Similar Packages

webpack 100 / 100 > pm2 97 / 100 > forever 66 / 100 >

Package Health Score

90 / 100

POPULARITY	KEY ECOSYSTEM PROJECT
MAINTENANCE	SUSTAINABLE
SECURITY	NO KNOWN SECURITY ISSUES
COMMUNITY	ACTIVE

Make sure the open source you're using is safe to use [SECURE MY PROJECT](#)

Popularity

KEY ECOSYSTEM PROJECT

WEEKLY DOWNLOADS (3,610,952)

DEPENDENTS 24.28K GITHUB STARS 22.06K FORKS 1.44K CONTRIBUTORS 140

Maintenance

SUSTAINABLE

COMMIT FREQUENCY

OPEN ISSUES 26 MERGED PR 269 OPEN PR 3 LAST COMMIT 18 hours ago

snyk.io/advisor

Find the best package for your next project.

Search and compare over 1 million open source packages.

npm ✓ Search packages 

- npm ✓ react, angular, vue, moment, passport, mocha
- PyPI
- Go
- Docker

nodemon v2.0.7
Simple monitor script for use during development of a node.js app.
[NPM](#) [README](#) [GitHub](#) [Website](#) [MIT](#) [Latest version published 2 months ago](#)

npm install nodemon

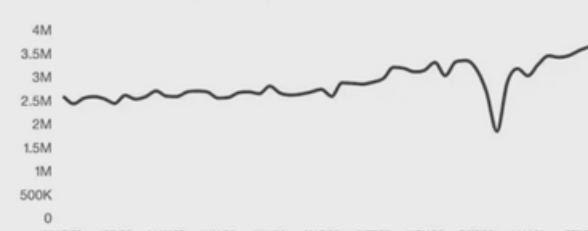
Explore Similar Packages

webpack 100 / 100 > pm2 97 / 100 > forever 66 / 100 >

Package Health Score
90 / 100

POPULARITY	KEY ECOSYSTEM PROJECT
MAINTENANCE	SUSTAINABLE
SECURITY	NO KNOWN SECURITY ISSUES
COMMUNITY	ACTIVE

Make sure the open source you're using is safe to use [SECURE MY PROJECT](#)

Popularity KEY ECOSYSTEM PROJECT
WEEKLY DOWNLOADS (3,610,952)


Month	Downloads (approx.)
MAR 20	2.5M
APR 20	2.6M
MAY 20	2.7M
JUN 20	2.8M
JUL 20	2.9M
AUG 20	3.0M
OCT 20	3.1M
NOV 20	3.2M
DEC 20	3.3M
JAN 21	3.4M
FEB 21	3.5M

Maintenance SUSTAINABLE
COMMIT FREQUENCY


Month	Commits
MAR 20	4
APR 20	4
MAY 20	2
JUN 20	2
JUL 20	0
AUG 20	0
SEP 20	1
OCT 20	5
NOV 20	1
DEC 20	1
JAN 21	8
FEB 21	1
MAR 21	4

DEPENDENTS 24.28K GITHUB STARS 22.06K FORKS 1.44K CONTRIBUTORS 140
OPEN ISSUES 26 MERGED PR 269 OPEN PR 3 LAST COMMIT 18 hours ago

snyk.io/advisor

Find the best package for your next project.

Search and compare over 1 million open source packages.

npm Search packages

npm ✓ node, react, angular, vue, moment, passport, mocha

PyPI

Go

Docker

nodemon v2.0.7
Simple monitor script for use during development of a node.js app.
[NPM](#) [README](#) [GitHub](#) [Website](#) [MIT](#) [Latest version published 2 months ago](#)
`npm install nodemon`

Explore Similar Packages

webpack 100 / 100 > pm2 97 / 100 > forever 66 / 100 >

Package Health Score
90 / 100

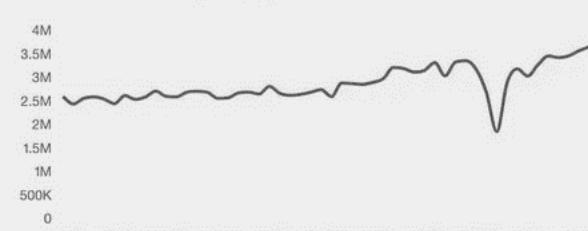
POPULARITY [KEY ECOSYSTEM PROJECT](#)

MAINTENANCE [SUSTAINABLE](#)

SECURITY [NO KNOWN SECURITY ISSUES](#)

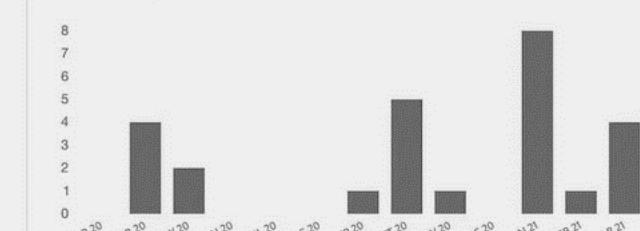
COMMUNITY [ACTIVE](#)

Make sure the open source you're using is safe to use [SECURE MY PROJECT](#)

Popularity [KEY ECOSYSTEM PROJECT](#)
WEEKLY DOWNLOADS (3,610,952)


Month	Downloads (approx.)
MAR 20	2.5M
APR 20	2.6M
MAY 20	2.7M
JUN 20	2.8M
JUL 20	2.9M
AUG 20	2.8M
OCT 20	3.0M
NOV 20	3.1M
DEC 20	3.2M
JAN 21	3.3M
FEB 21	3.4M

DEPENDENTS 24.28K GITHUB STARS 22.06K FORKS 1.44K CONTRIBUTORS 140

Maintenance [SUSTAINABLE](#)
COMMIT FREQUENCY


Month	Commits
MAR 20	0
APR 20	4
MAY 20	2
JUN 20	0
JUL 20	0
AUG 20	0
SEP 20	0
OCT 20	5
NOV 20	1
DEC 20	0
JAN 21	7
FEB 21	1
MAR 21	4

OPEN ISSUES 26 MERGED PR 269 OPEN PR 3 LAST COMMIT 18 hours ago

snyk.io/advisor

Find the best package for your next project.

Search and compare over 1 million open source packages.

npm Search packages

npm ✓ node, react, angular, vue, moment, passport, mocha

PyPI

Go

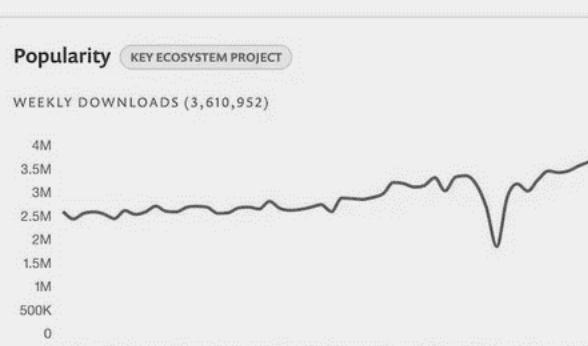
Docker

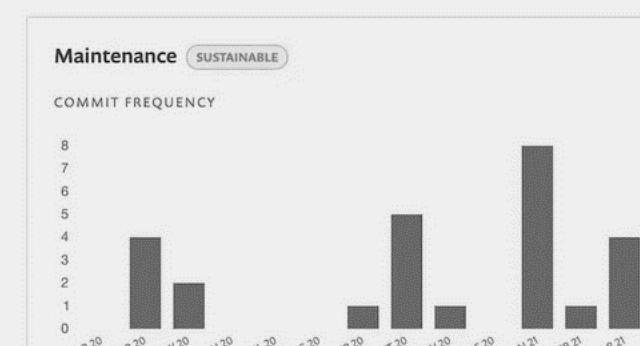
nodemon v2.0.7
Simple monitor script for use during development of a node.js app.
[NPM](#) [README](#) [GitHub](#) [Website](#) [MIT](#) [Latest version published 2 months ago](#)

`npm install nodemon`

Explore Similar Packages
[webpack](#) 100 / 100 > [pm2](#) 97 / 100 > [forever](#) 66 / 100 >

Make sure the open source you're using is safe to use [SECURE MY PROJECT](#)

Popularity KEY ECOSYSTEM PROJECT
WEEKLY DOWNLOADS (3,610,952)

DEPENDENTS 24.28K GITHUB STARS 22.06K FORKS 1.44K CONTRIBUTORS 140

Maintenance SUSTAINABLE
COMMIT FREQUENCY

OPEN ISSUES 26 MERGED PR 269 OPEN PR 3 LAST COMMIT 18 hours ago

Package Health Score
90 / 100

POPULARITY KEY ECOSYSTEM PROJECT
MAINTENANCE SUSTAINABLE
SECURITY NO KNOWN SECURITY ISSUES
COMMUNITY ACTIVE

snyk.io/advisor

Find the best package for your next project.

Search and compare over 1 million open source packages.

npm

Search packages

npm react, angular, vue, moment, passport, mocha

PyPI

Go

Docker

nodemon v2.0.7

Simple monitor script for use during development of a node.js app.

NPM README GitHub Website MIT Latest version published 2 months ago

npm install nodemon

Explore Similar Packages

webpack 100 / 100 > pm2 97 / 100 > forever 66 / 100 >

Package Health Score **90 / 100**

POPULARITY KEY ECOSYSTEM PROJECT

MAINTENANCE SUSTAINABLE

SECURITY NO KNOWN SECURITY ISSUES

COMMUNITY ACTIVE

Make sure the open source you're using is safe to use

SECURE MY PROJECT

Popularity KEY ECOSYSTEM PROJECT

WEEKLY DOWNLOADS (3,610,952)

DEPENDENTS 24.28K GITHUB STARS 22.06K FORKS 1.44K CONTRIBUTORS 140

Maintenance SUSTAINABLE

COMMIT FREQUENCY

OPEN ISSUES 26 MERGED PR 269 OPEN PR 3 LAST COMMIT 18 hours ago

snyk.io/advisor

Find the best package for your next project.

Search and compare over 1 million open source packages.

npm ✓ react, angular, vue, moment, passport, mocha

PyPI

Go

Docker

Search packages

nodemon v2.0.7

Simple monitor script for use during development of a node.js app.

NPM README GitHub Website MIT Latest version published 2 months ago

npm install nodemon

Explore Similar Packages

webpack 100 / 100 > pm2 97 / 100 > forever 66 / 100 >

Package Health Score

90 / 100

POPULARITY	KEY ECOSYSTEM PROJECT
MAINTENANCE	SUSTAINABLE
SECURITY	NO KNOWN SECURITY ISSUES
COMMUNITY	ACTIVE

Make sure the open source you're using is safe to use [SECURE MY PROJECT](#)

Popularity

KEY ECOSYSTEM PROJECT

WEEKLY DOWNLOADS (3,610,952)

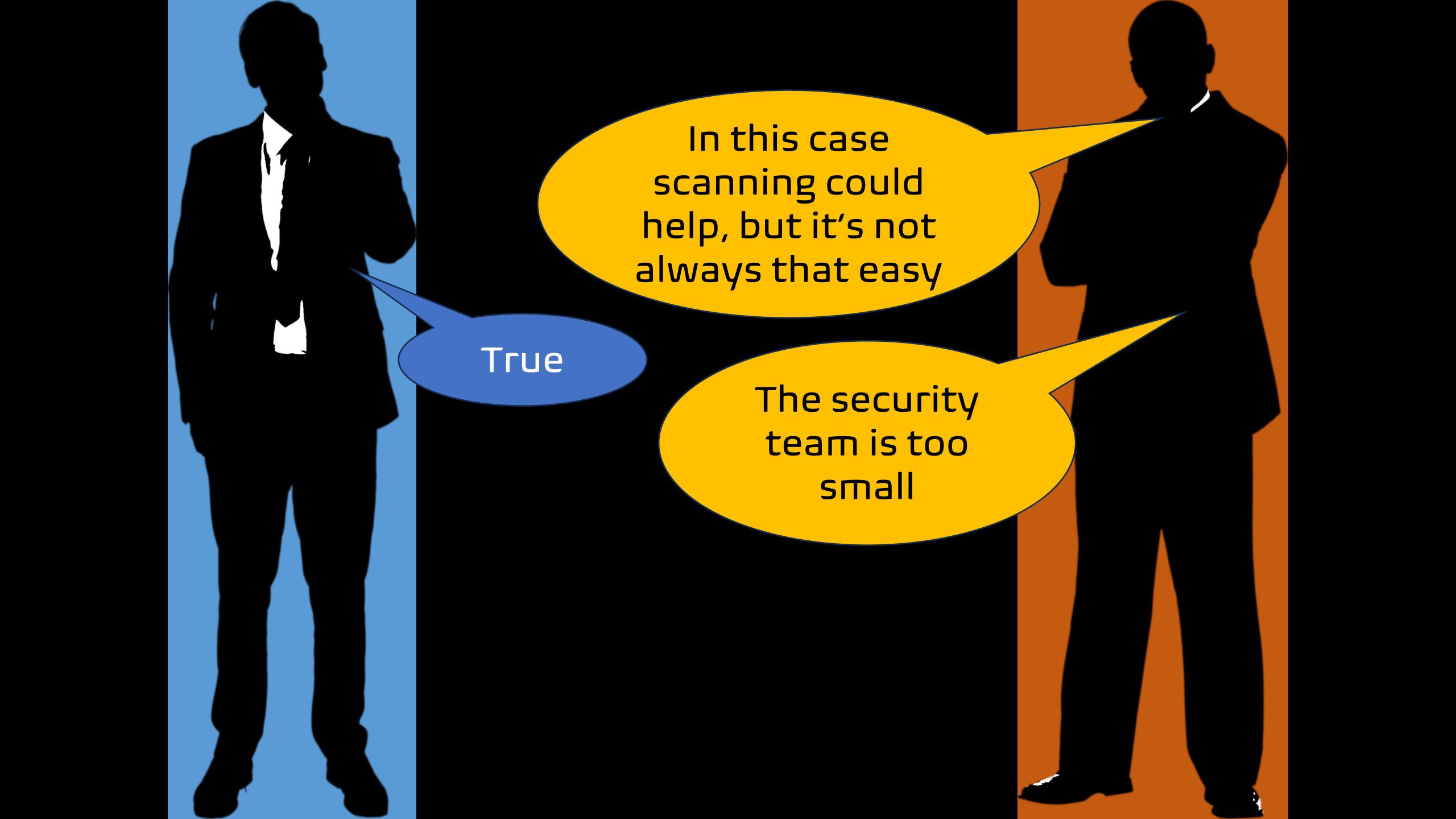
DEPENDENTS 24.28K GITHUB STARS 22.06K FORKS 1.44K CONTRIBUTORS 140

Maintenance

SUSTAINABLE

COMMIT FREQUENCY

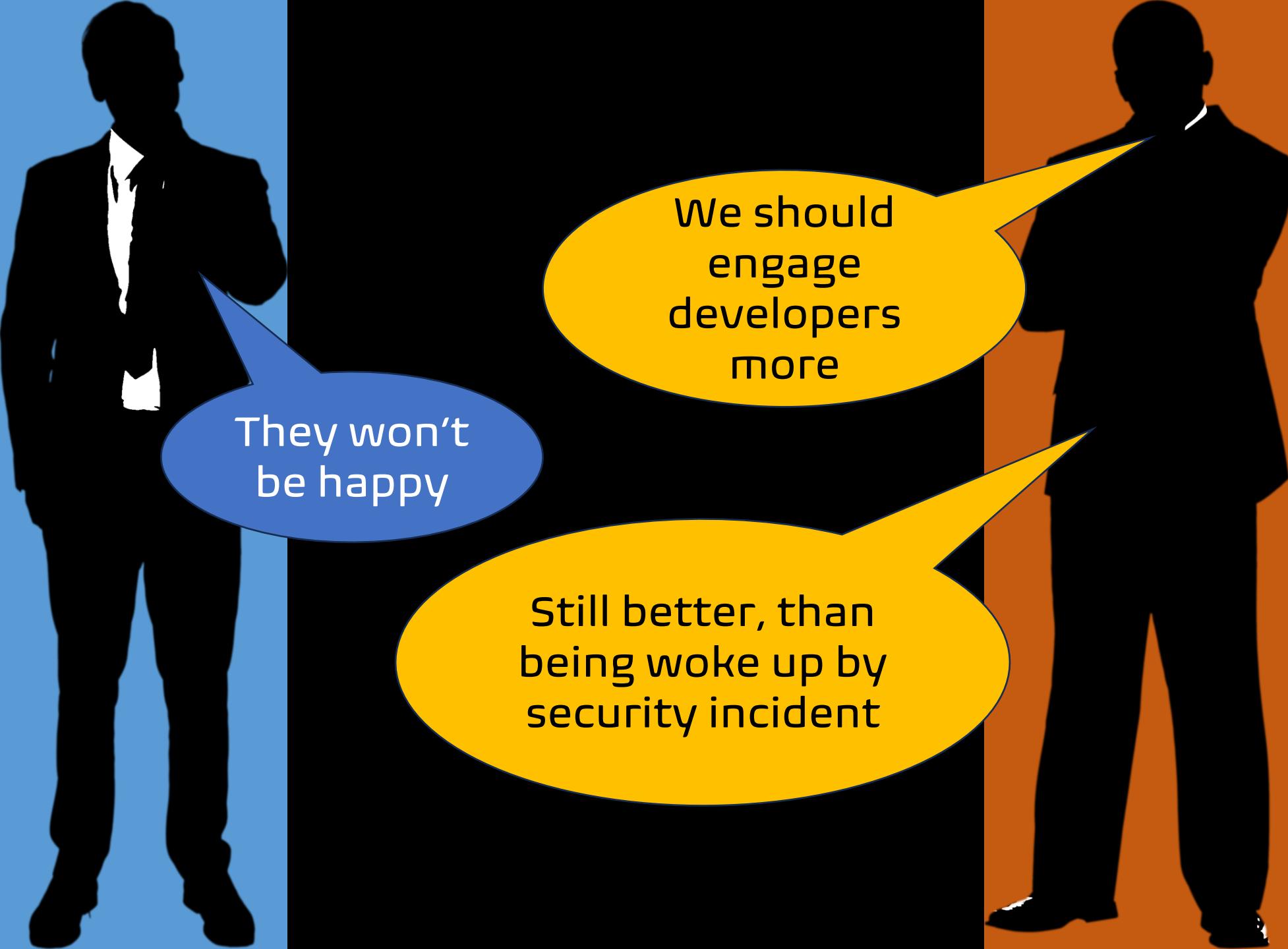
OPEN ISSUES 26 MERGED PR 269 OPEN PR 3 LAST COMMIT 18 hours ago

A graphic featuring two black silhouettes of men in suits. The man on the left stands against a blue vertical background. The man on the right stands against an orange vertical background. They are facing each other. Two yellow speech bubbles with black outlines are positioned between them. The top bubble contains the text "In this case scanning could help, but it's not always that easy". The bottom bubble contains the text "The security team is too small".

True

In this case
scanning could
help, but it's not
always that easy

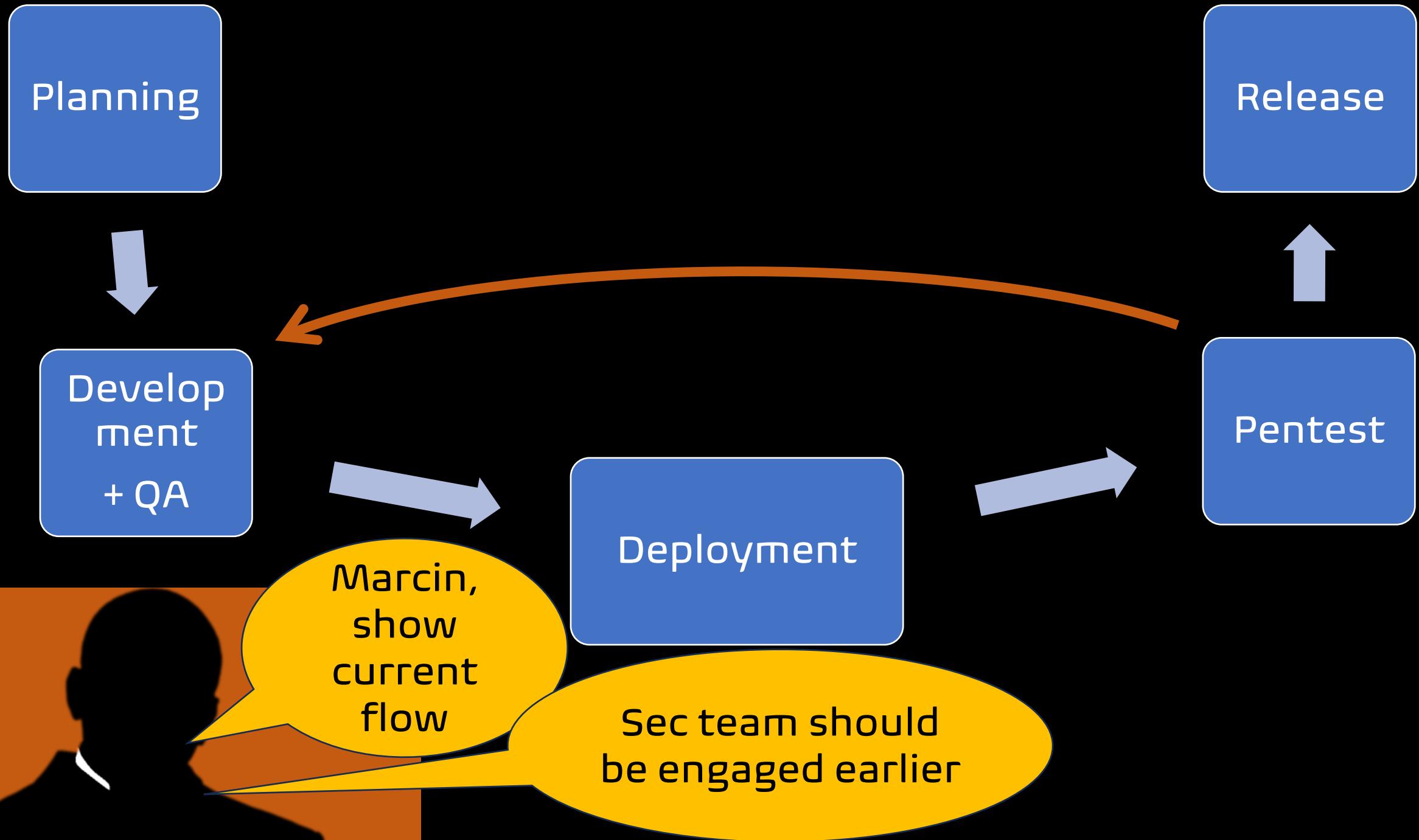
The security
team is too
small

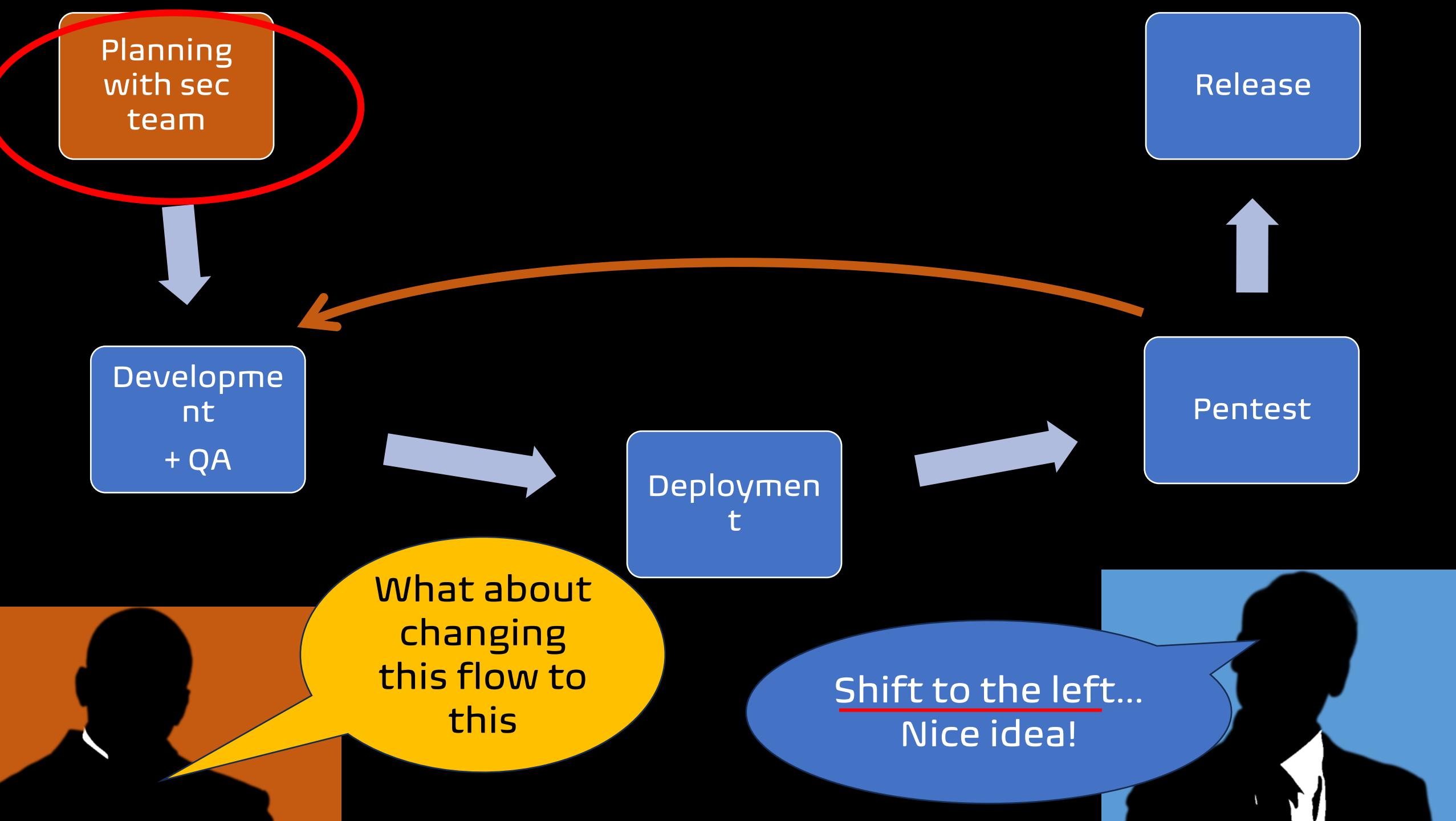


They won't
be happy

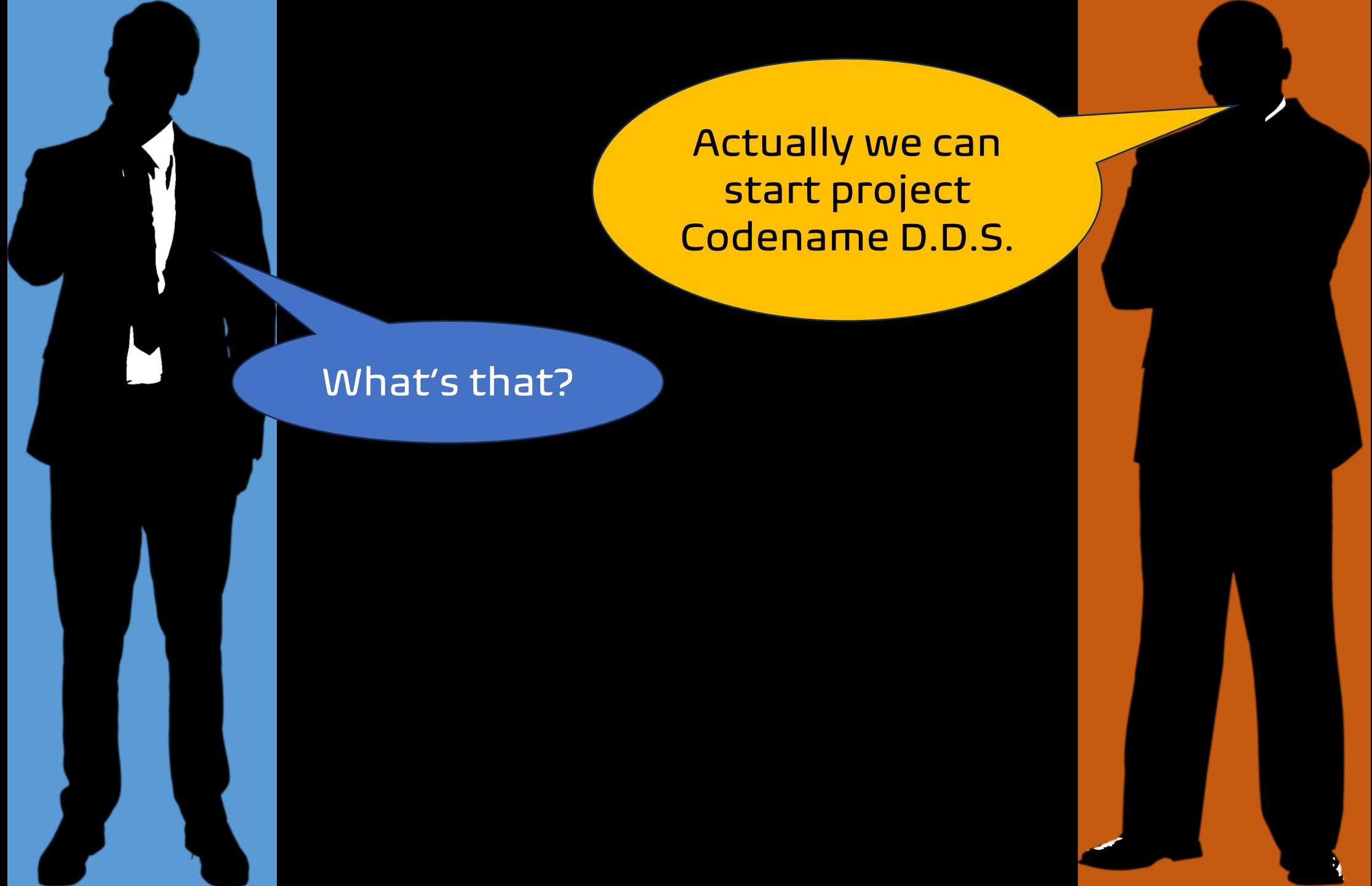
Still better, than
being woke up by
security incident

We should
engage
developers
more









Actually we can
start project
Codename D.D.S.

What's that?

DEVELOPER

DRIVEN

SECURITY

DDS

Developers take
responsibility for
security

Threat modelling

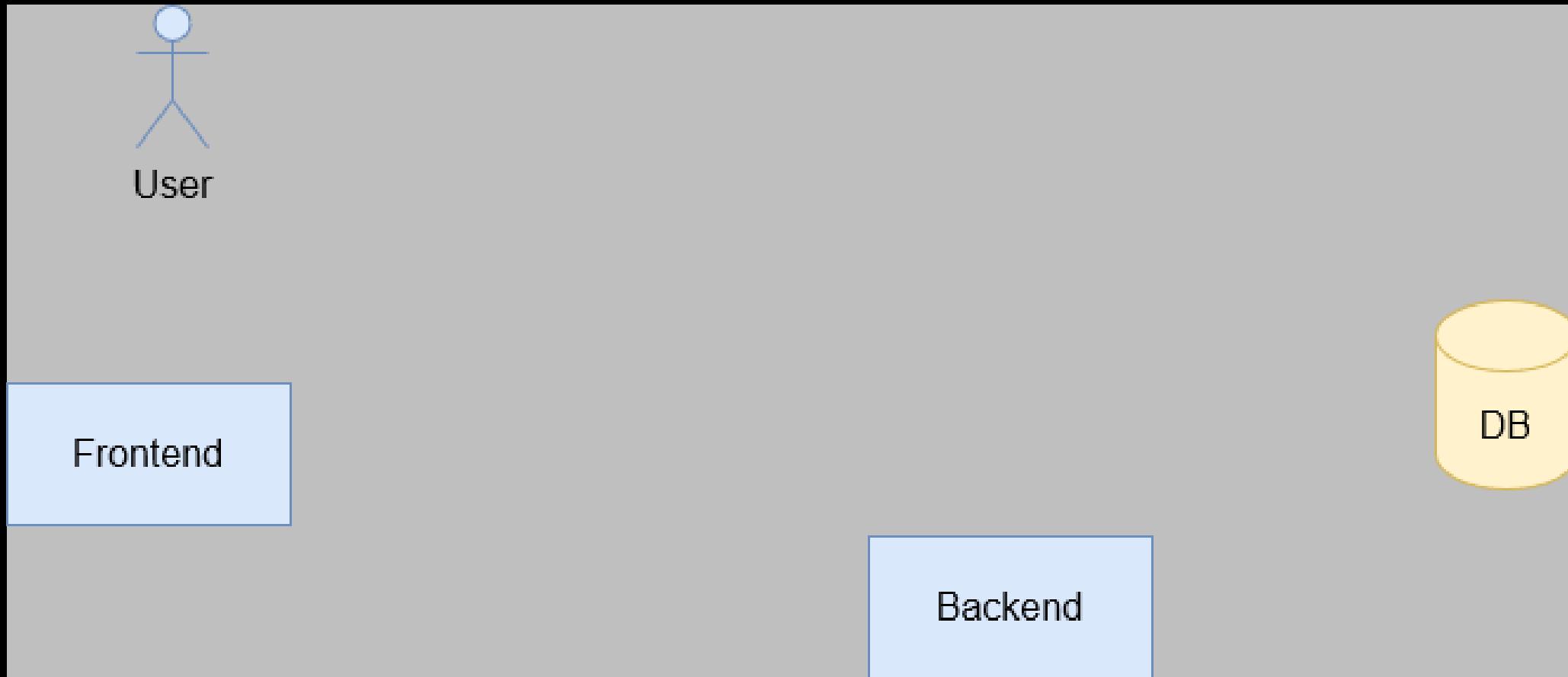
- Structurizes discussion
- Identifies security requirements
- Pinpoints security threats and potential vulnerabilities
- Quantifies threat and vulnerability criticality
- Prioritizes remediation methods

Blog application

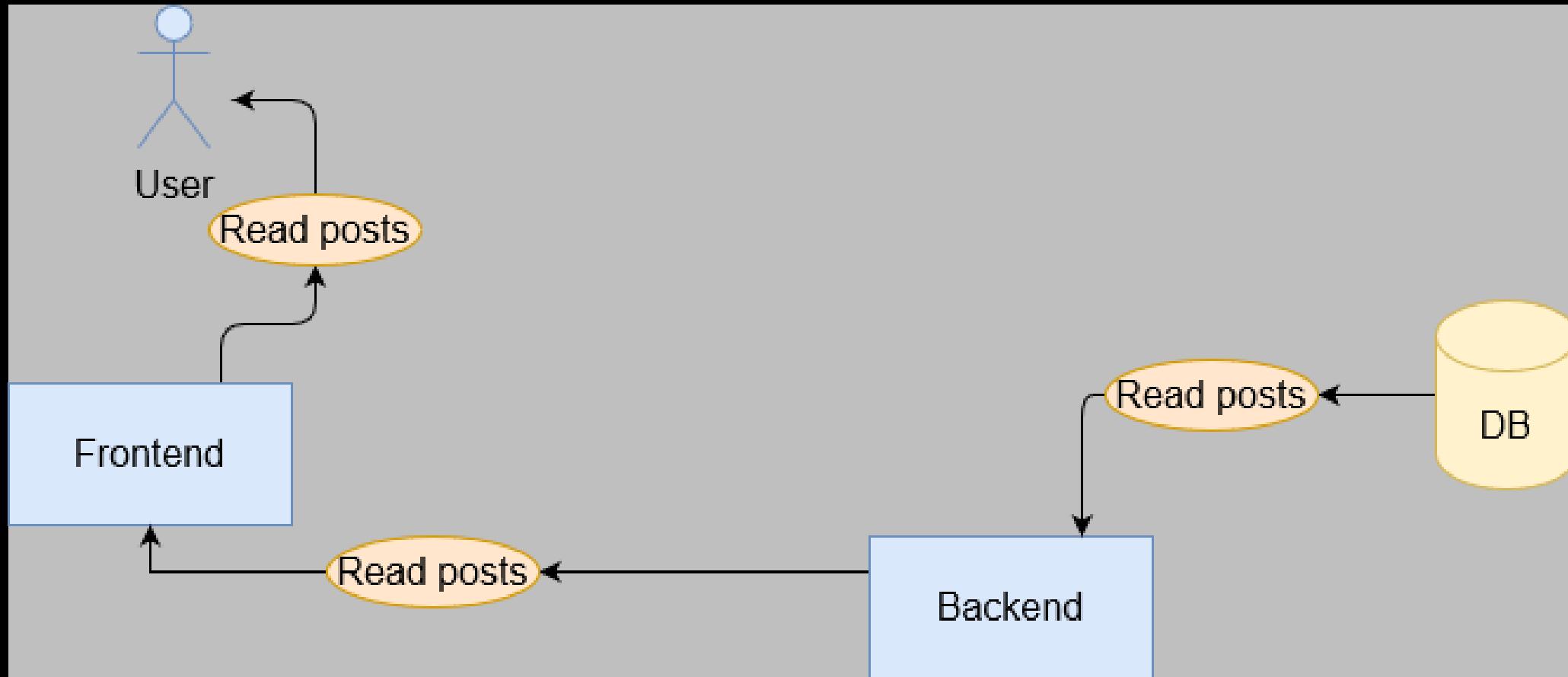
- Add post
- Read posts
- Login mechanism (for adding posts)

Step 1: data flow diagram

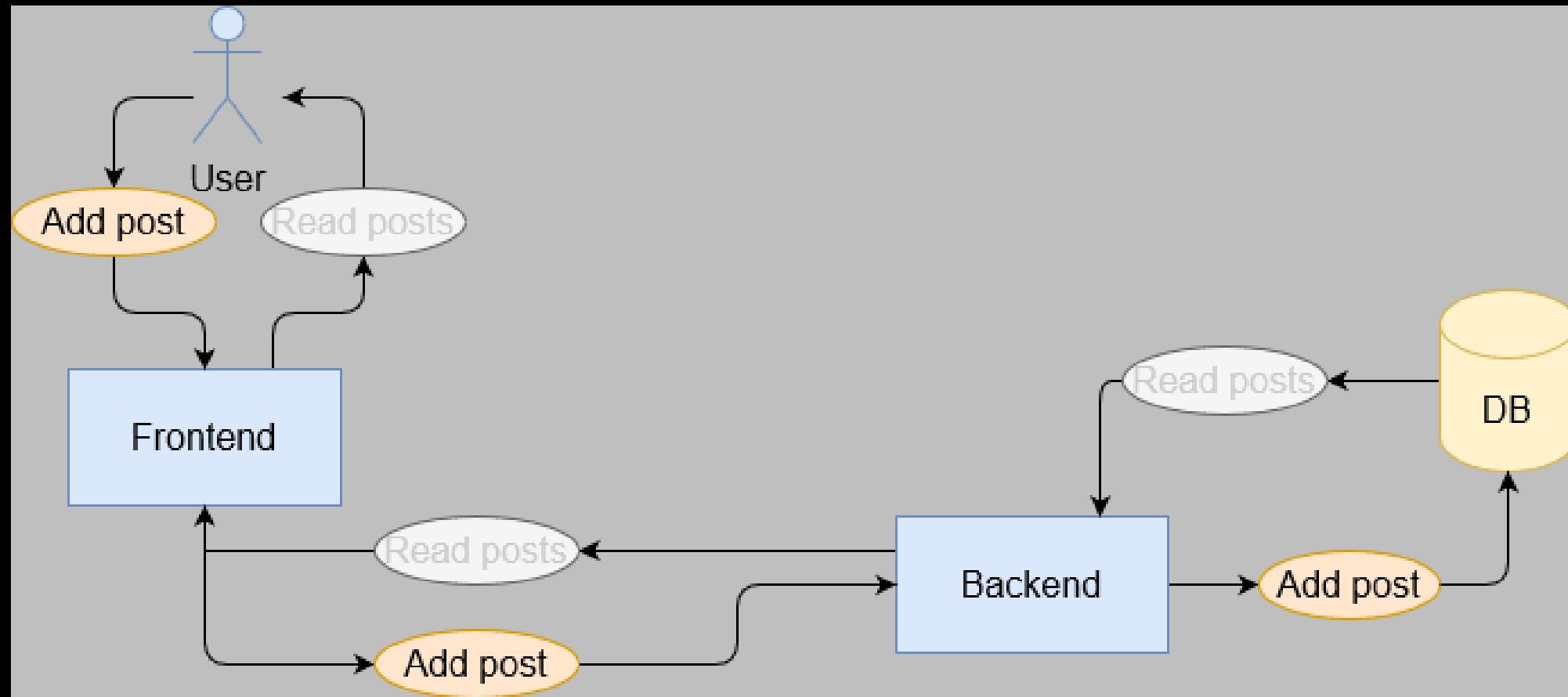
Blog application



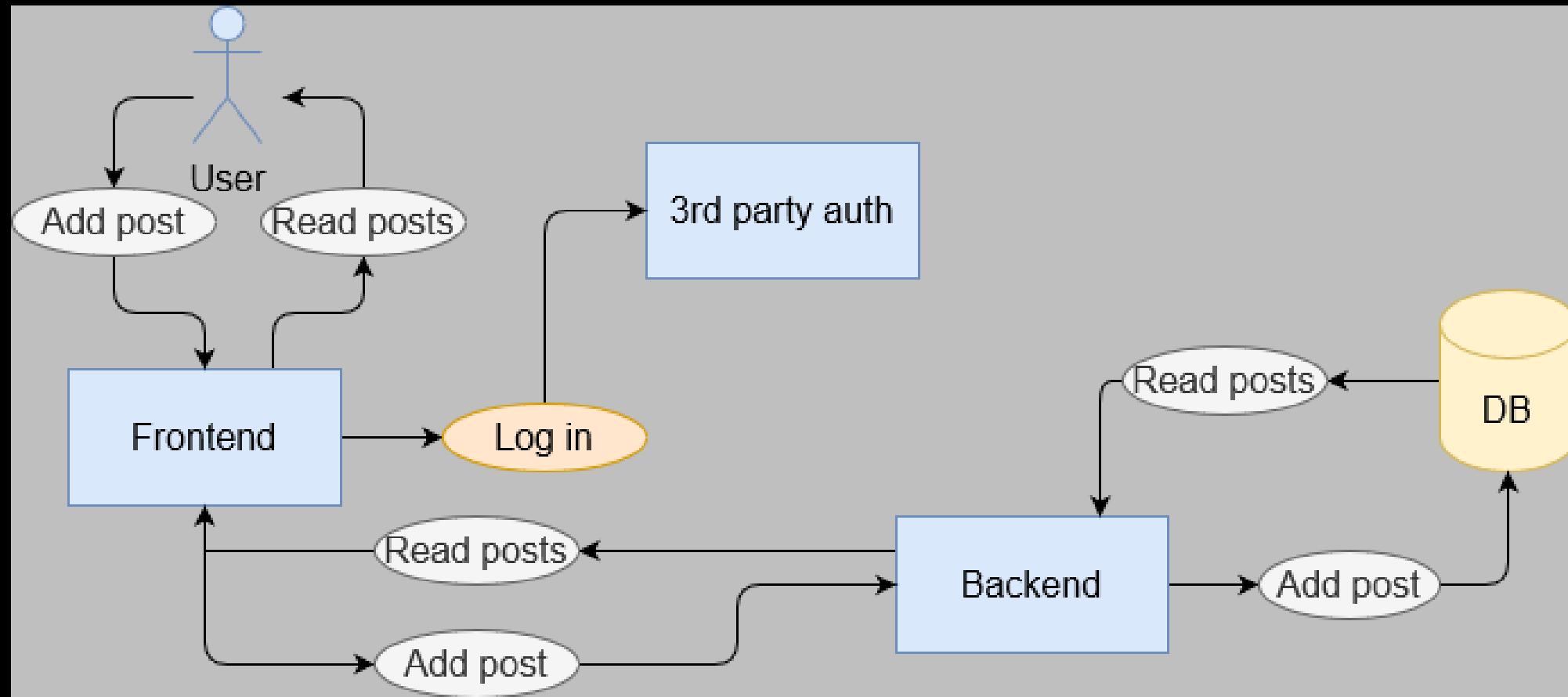
Blog application



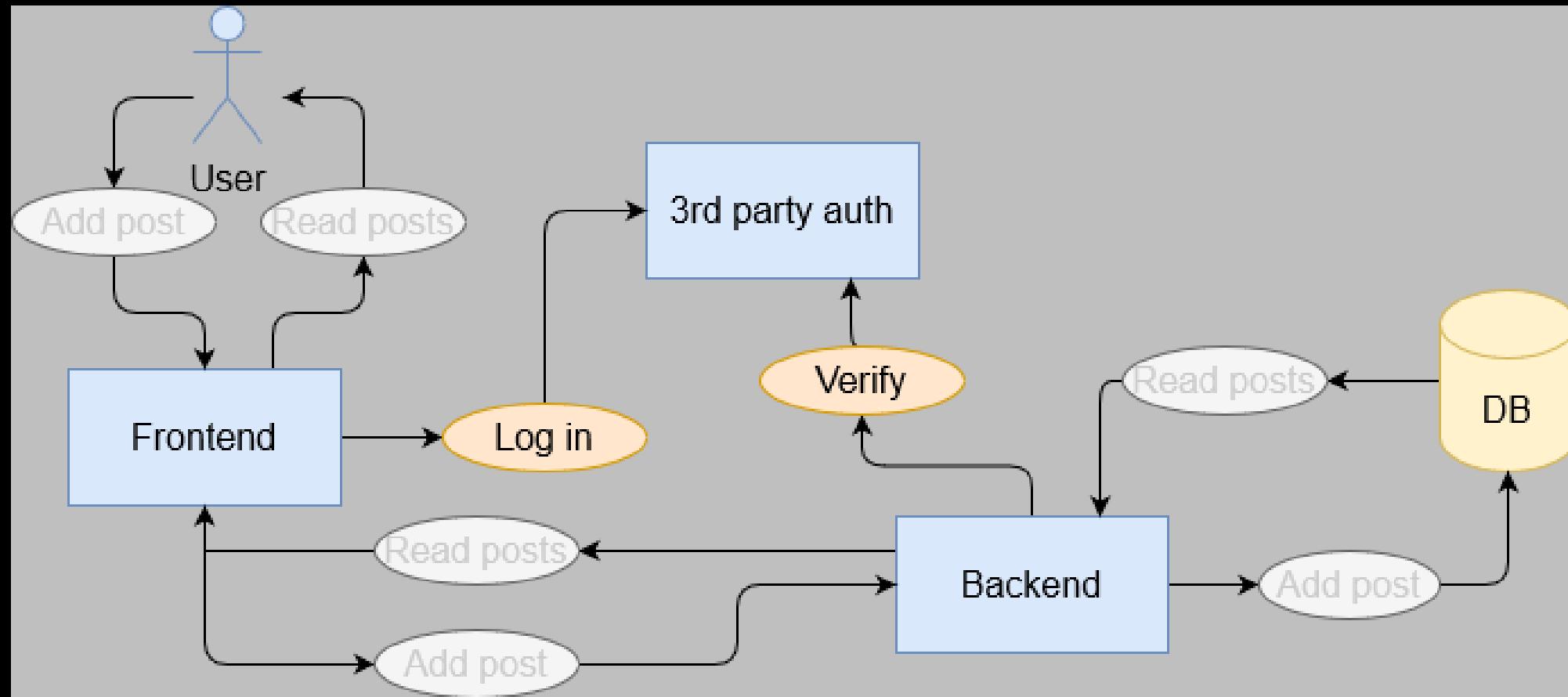
Blog application



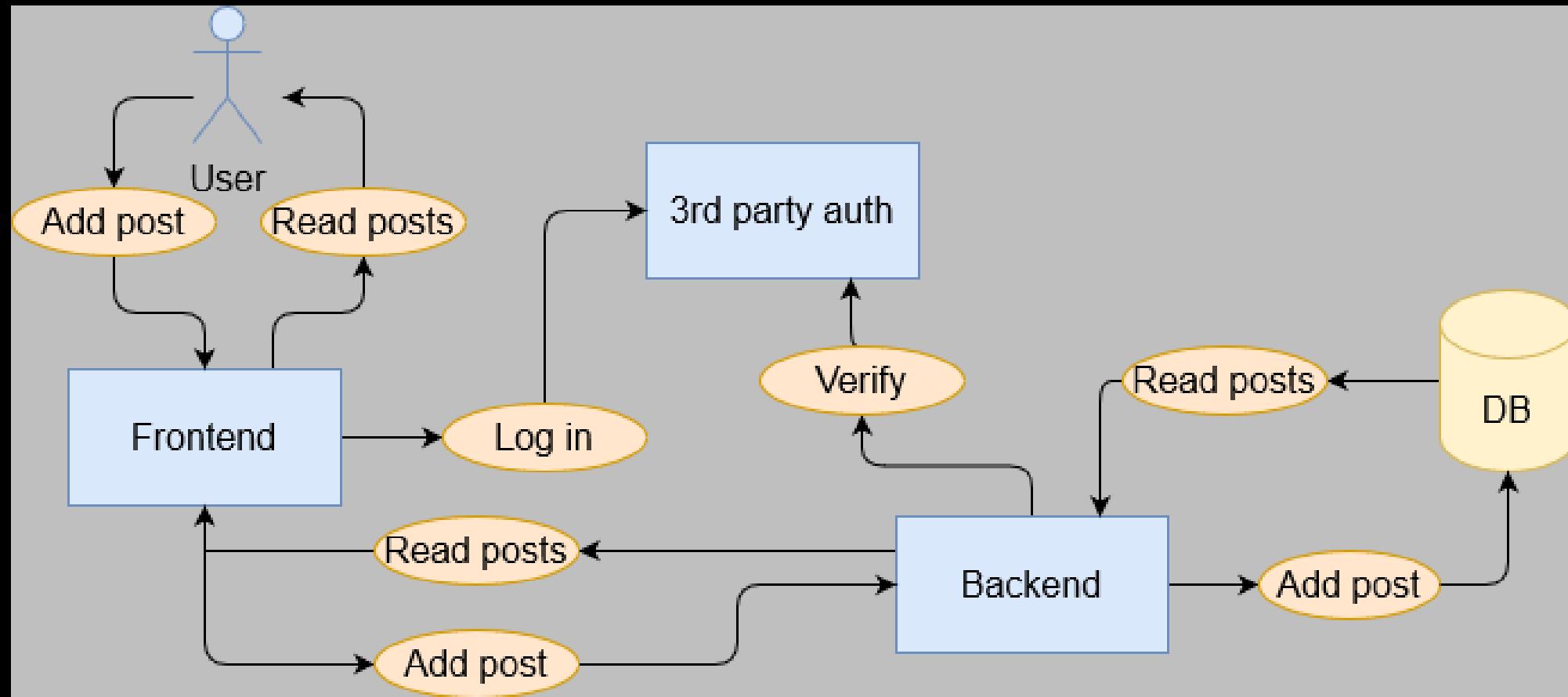
Blog application



Blog application



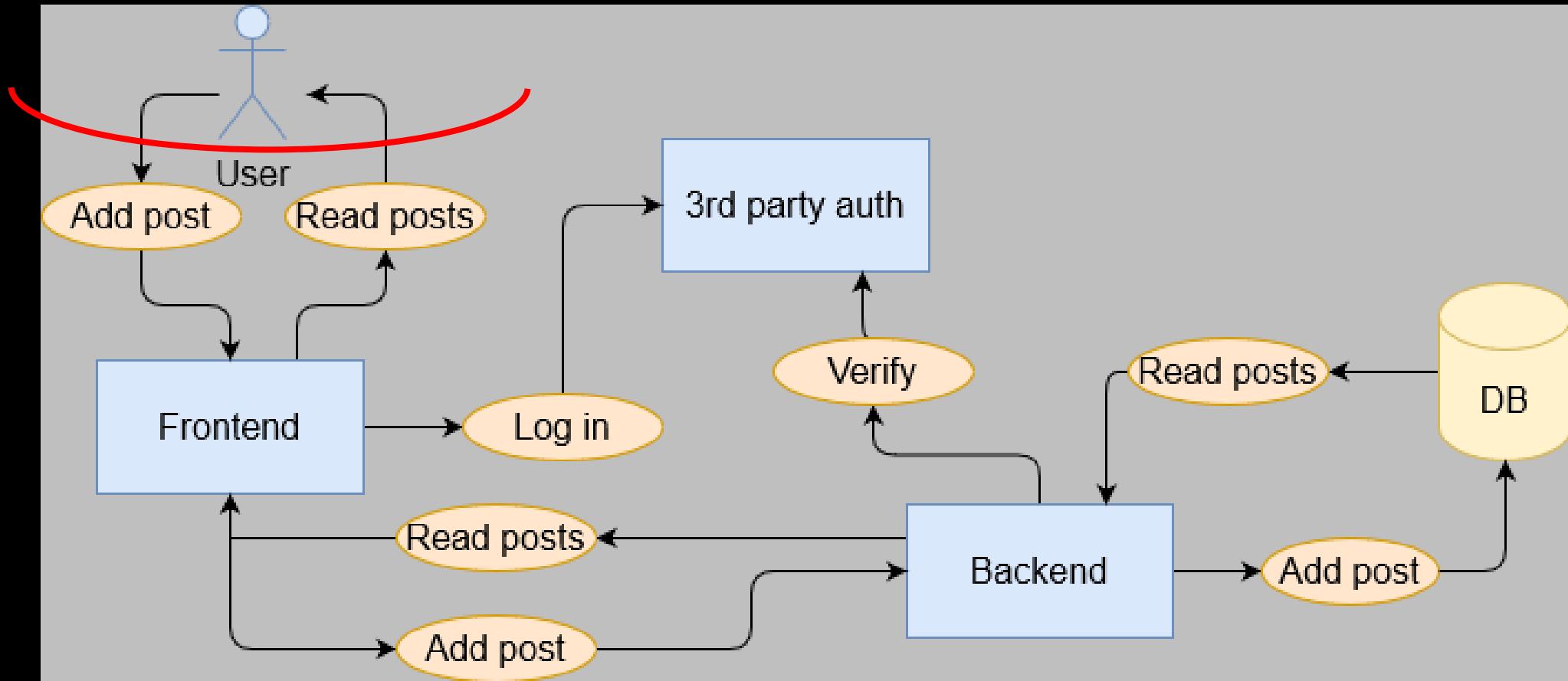
Blog application



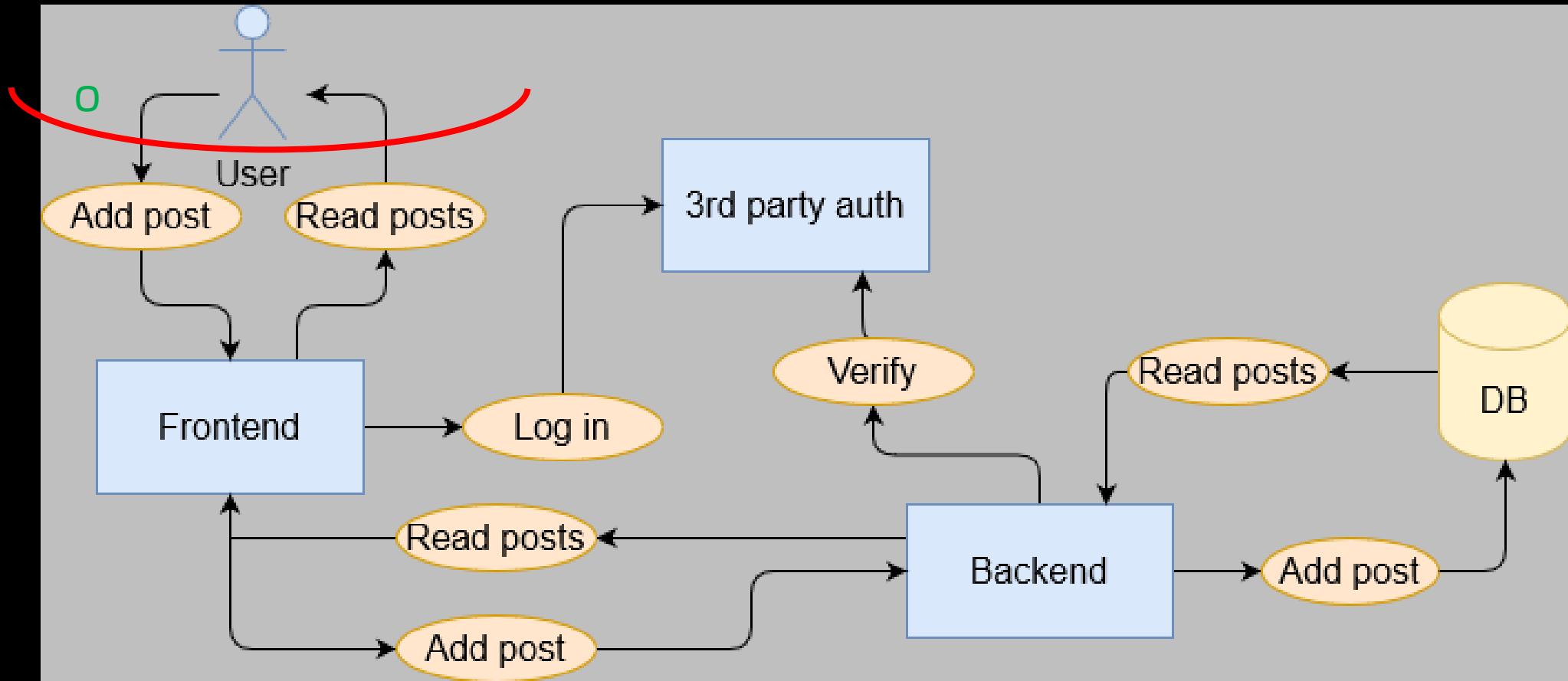
Step 1: data flow diagram

Step 2: trust zones

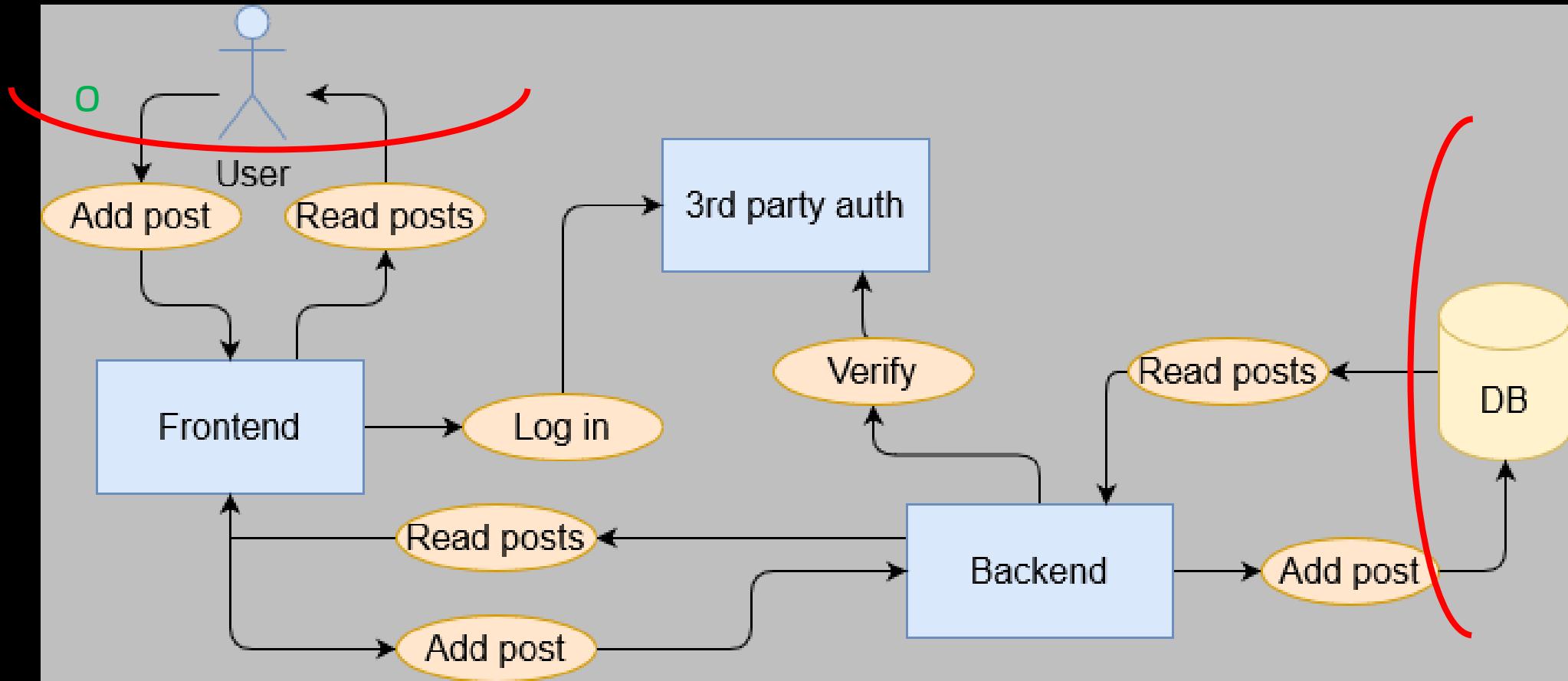
Trust zones



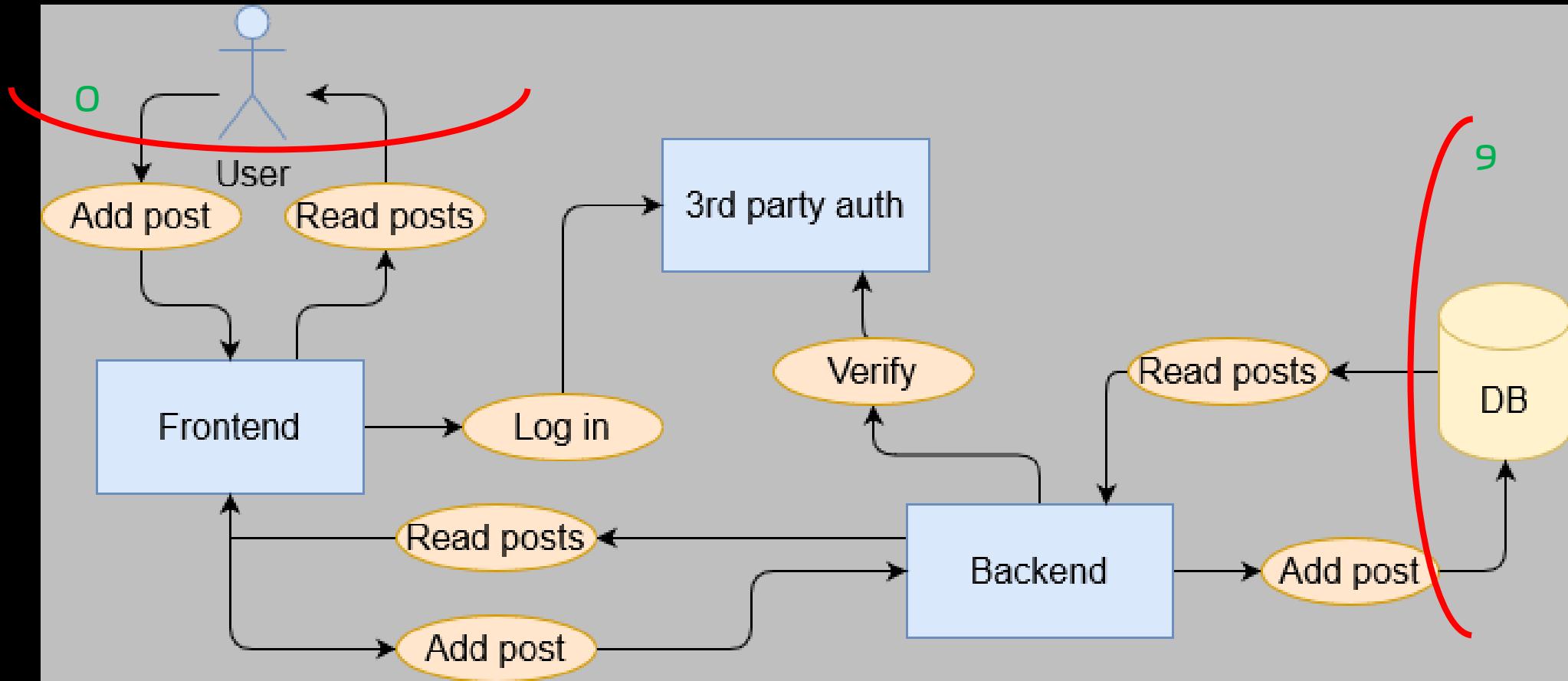
Trust zones



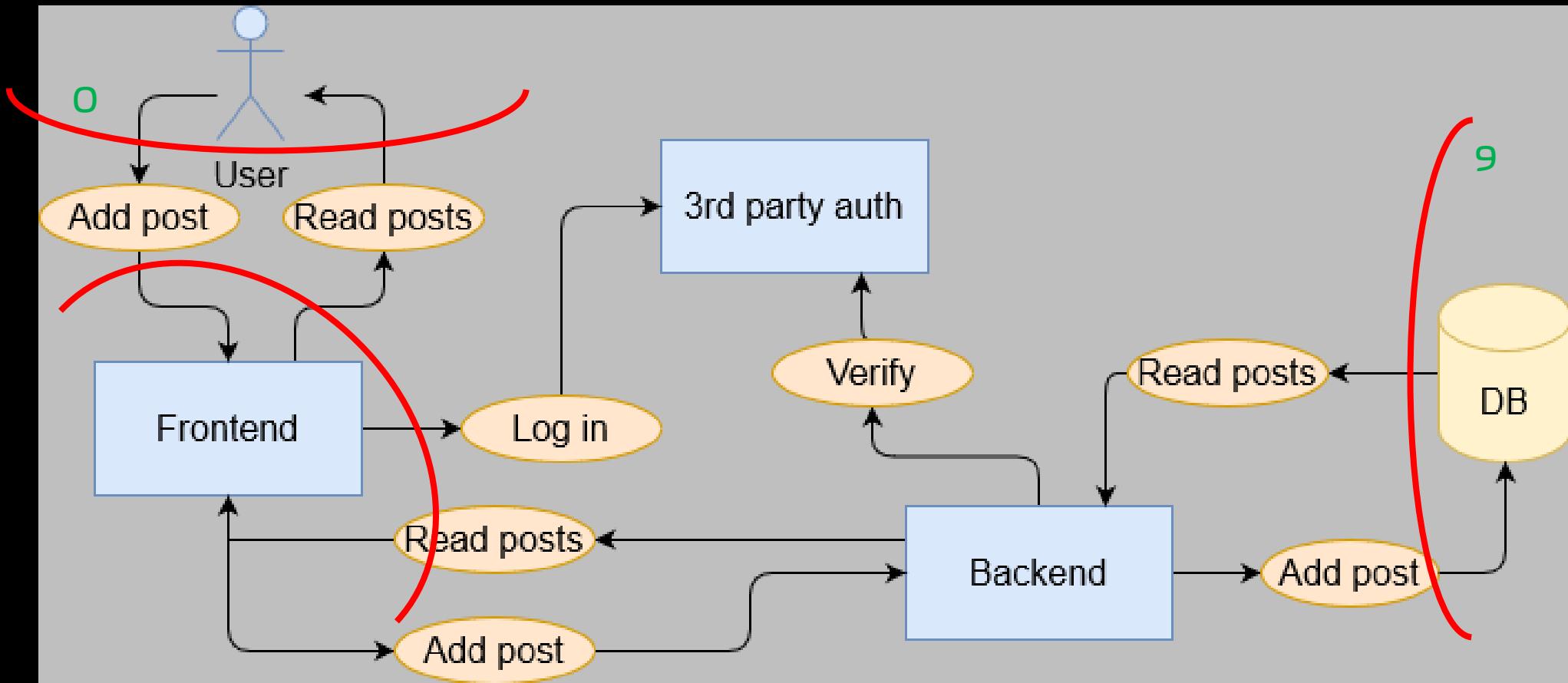
Trust zones



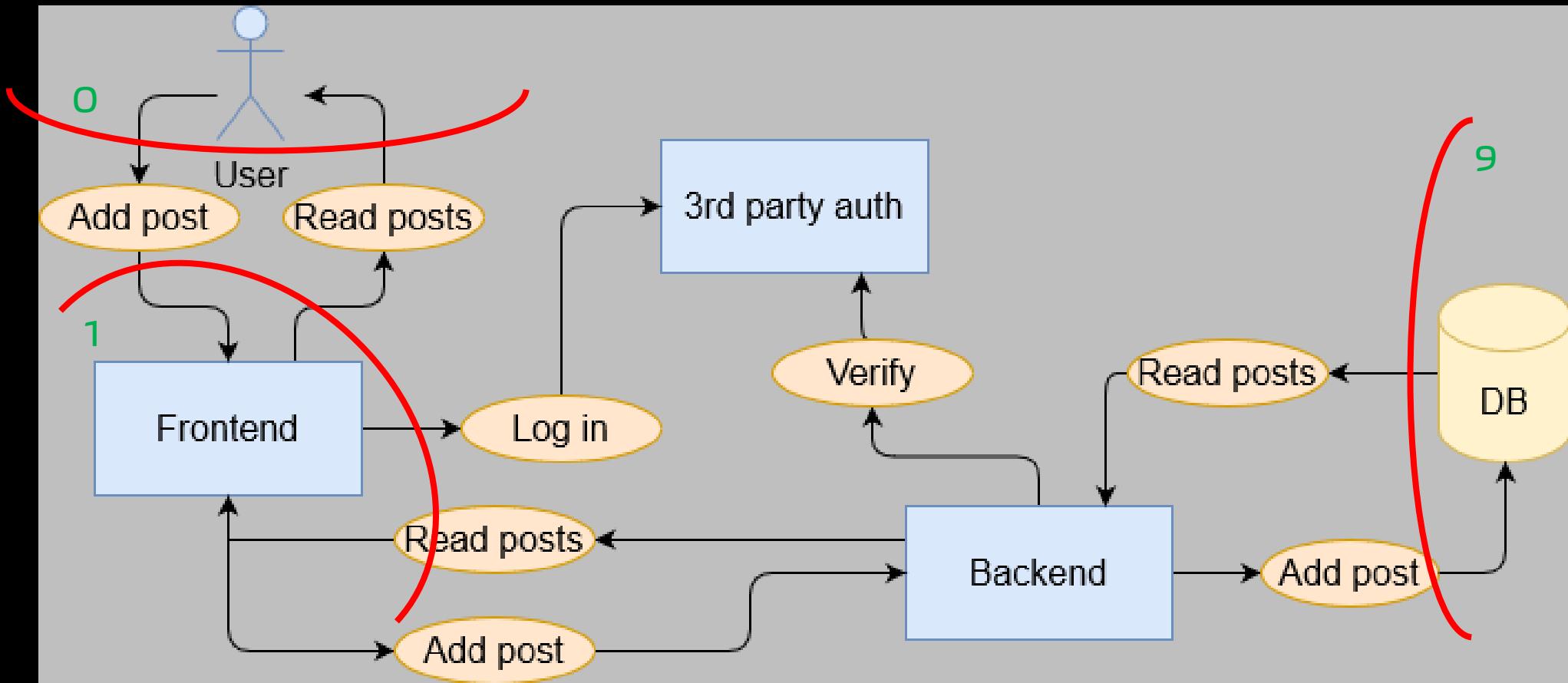
Trust zones



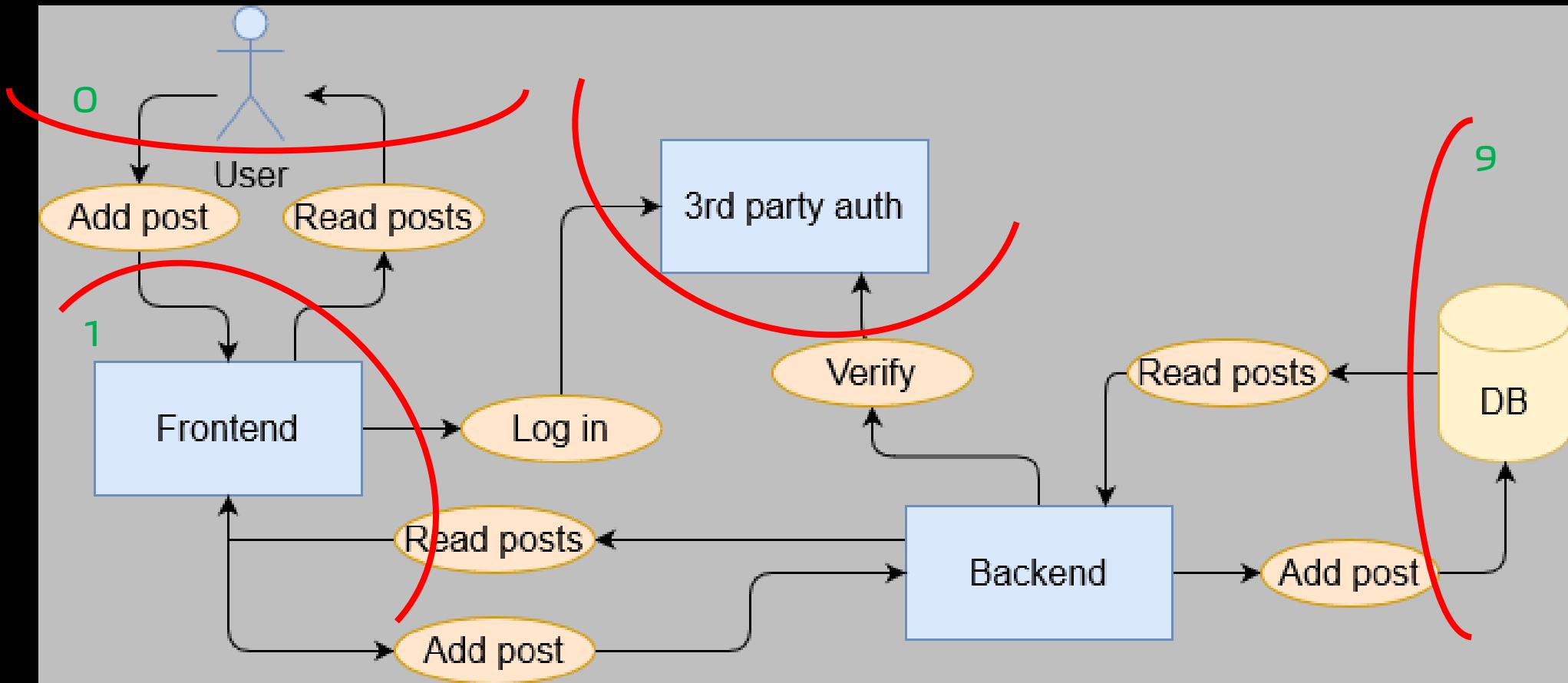
Trust zones



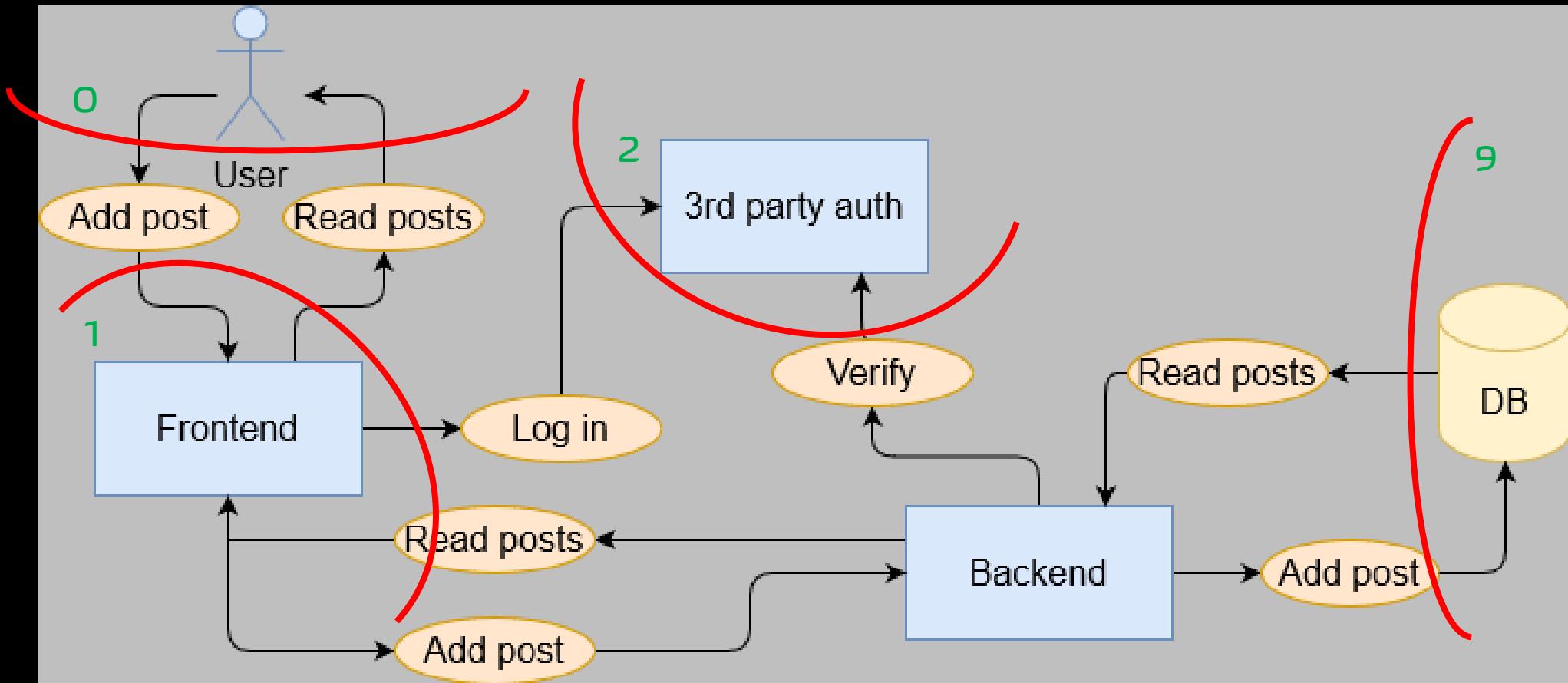
Trust zones



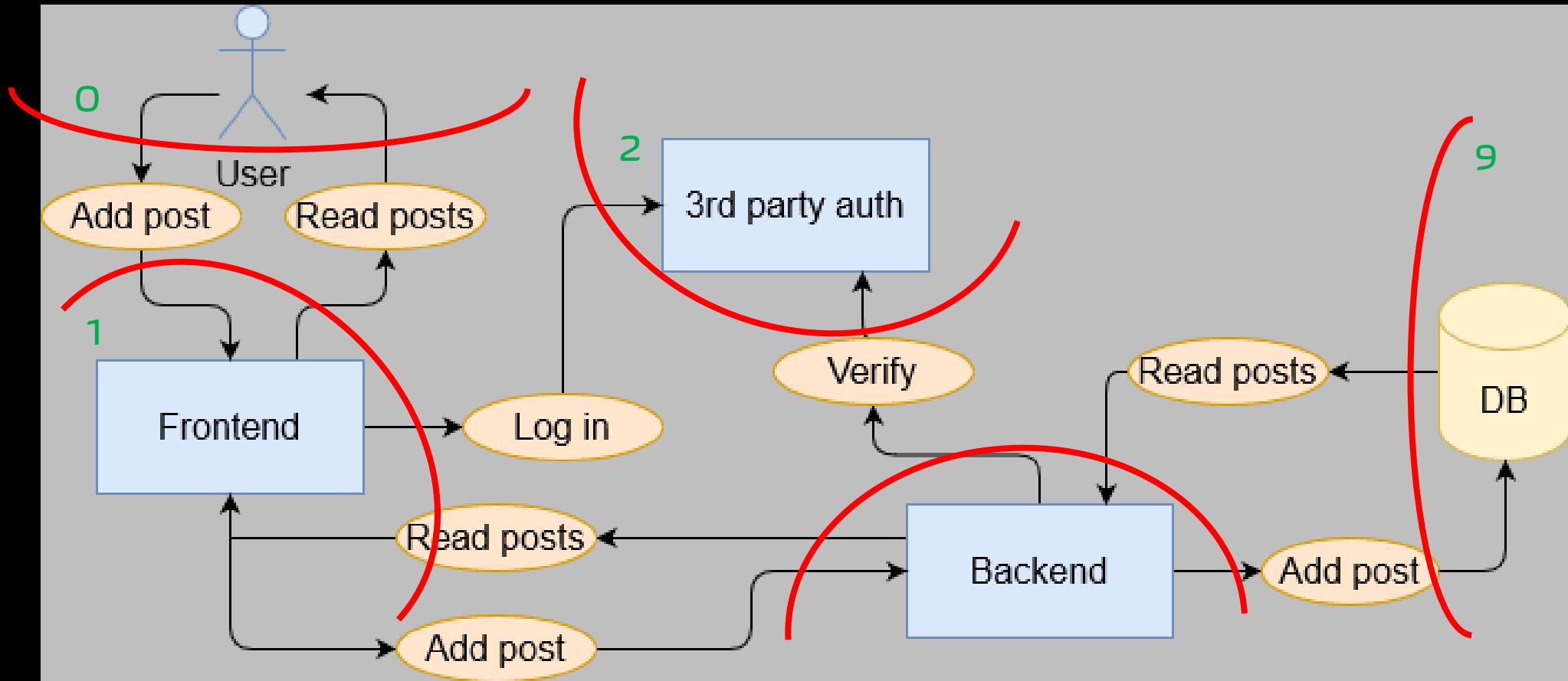
Trust zones



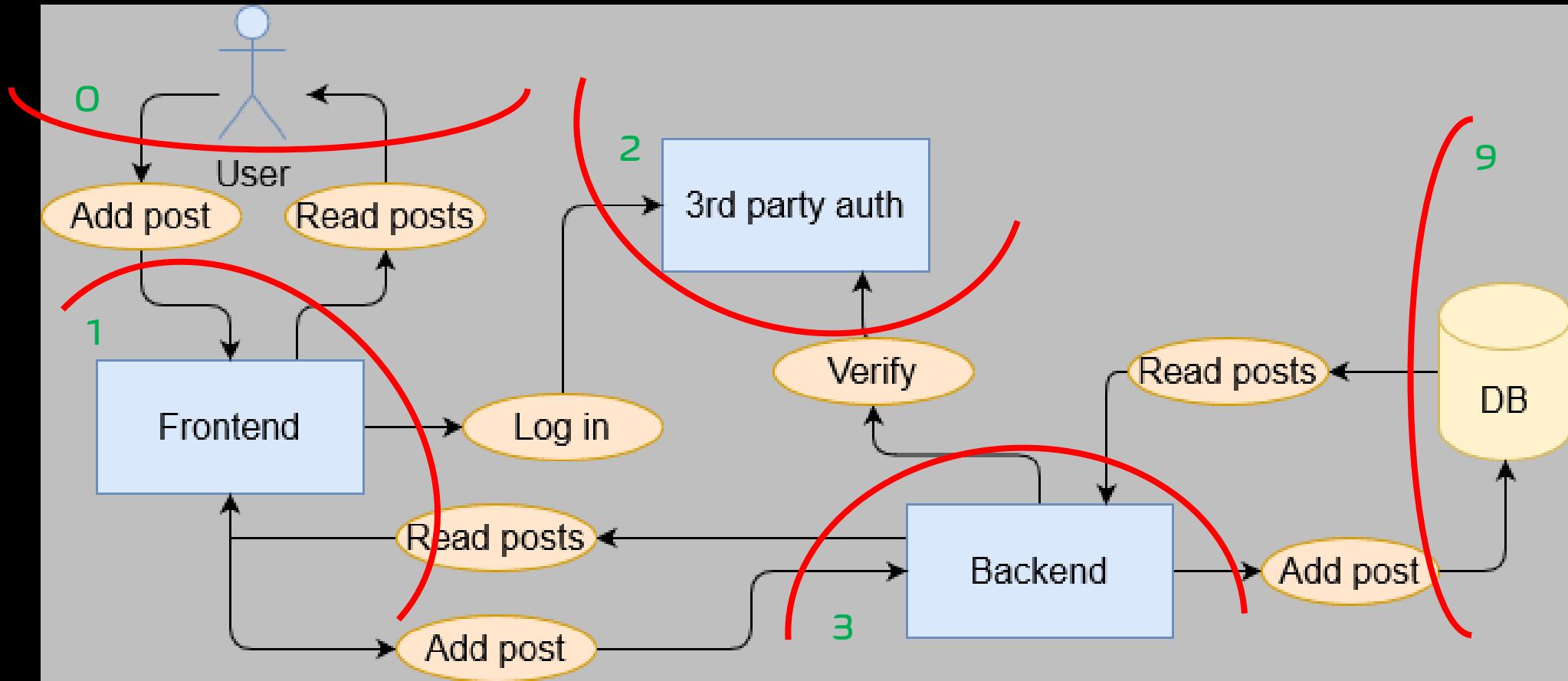
Trust zones



Trust zones



Trust zones



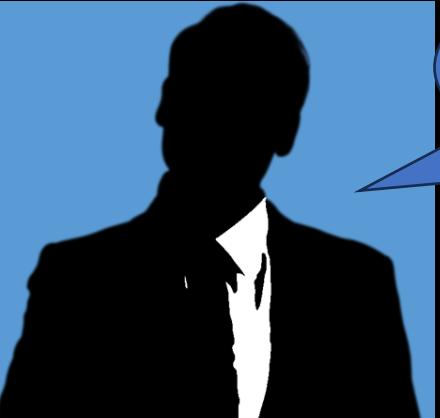
Step 1: data flow diagram

Step 2: trust zones

Step 3: risks

Risks

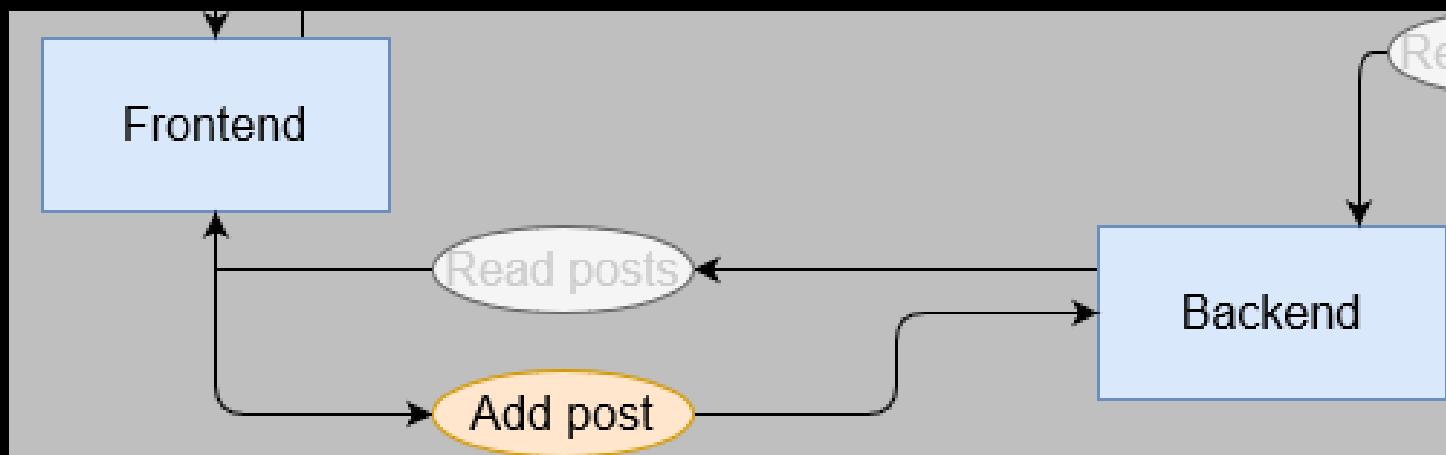
Defined for every process that goes
between zones with **different levels**

A black silhouette of a person's head and shoulders, facing right, positioned next to a blue speech bubble.

OWASP may be
helpful here

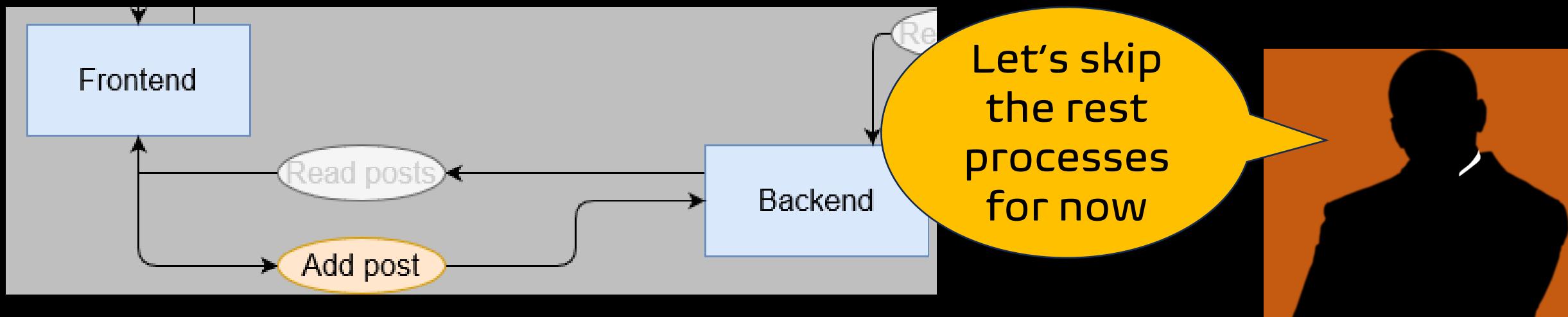
Risks

1. XXE attack
2. Overflow
3. Unauth addition of post
4. Malicious input files
5. Man in the middle



Risks

1. XXE attack
2. Overflow
3. Unauth addition of post
4. Malicious input files
5. Man in the middle



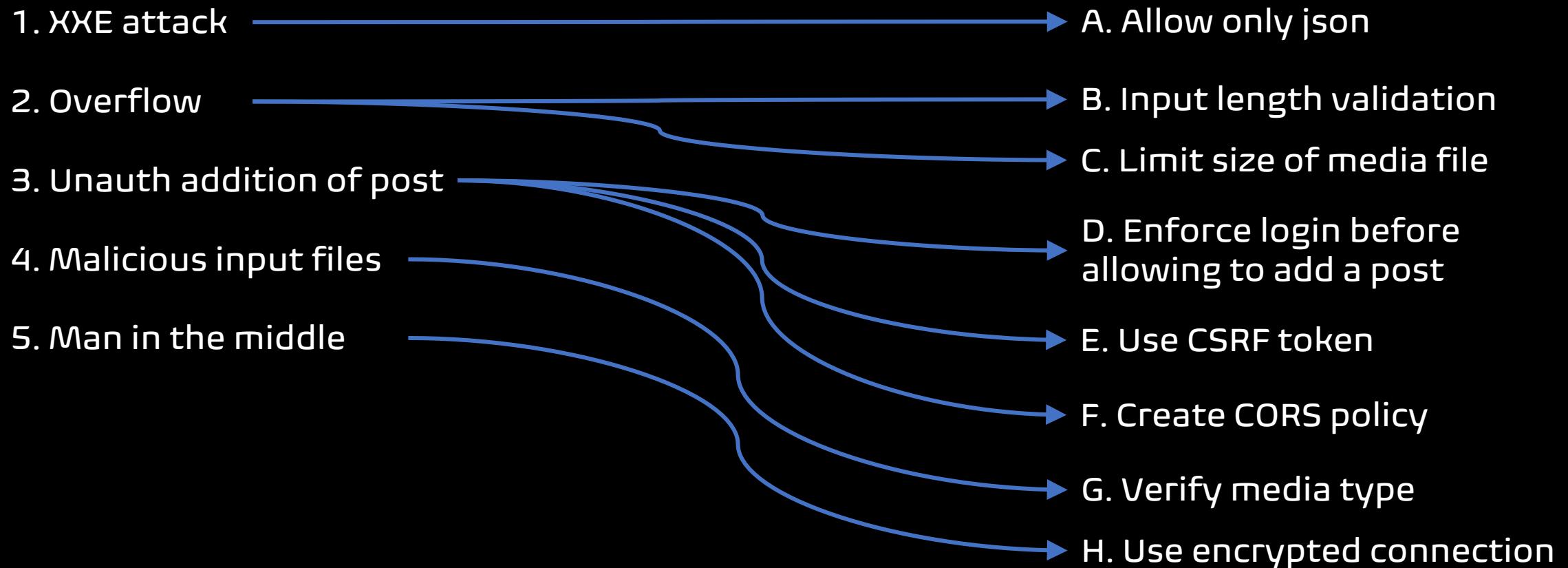
Step 1. data flow diagram

Step 2. trust zones

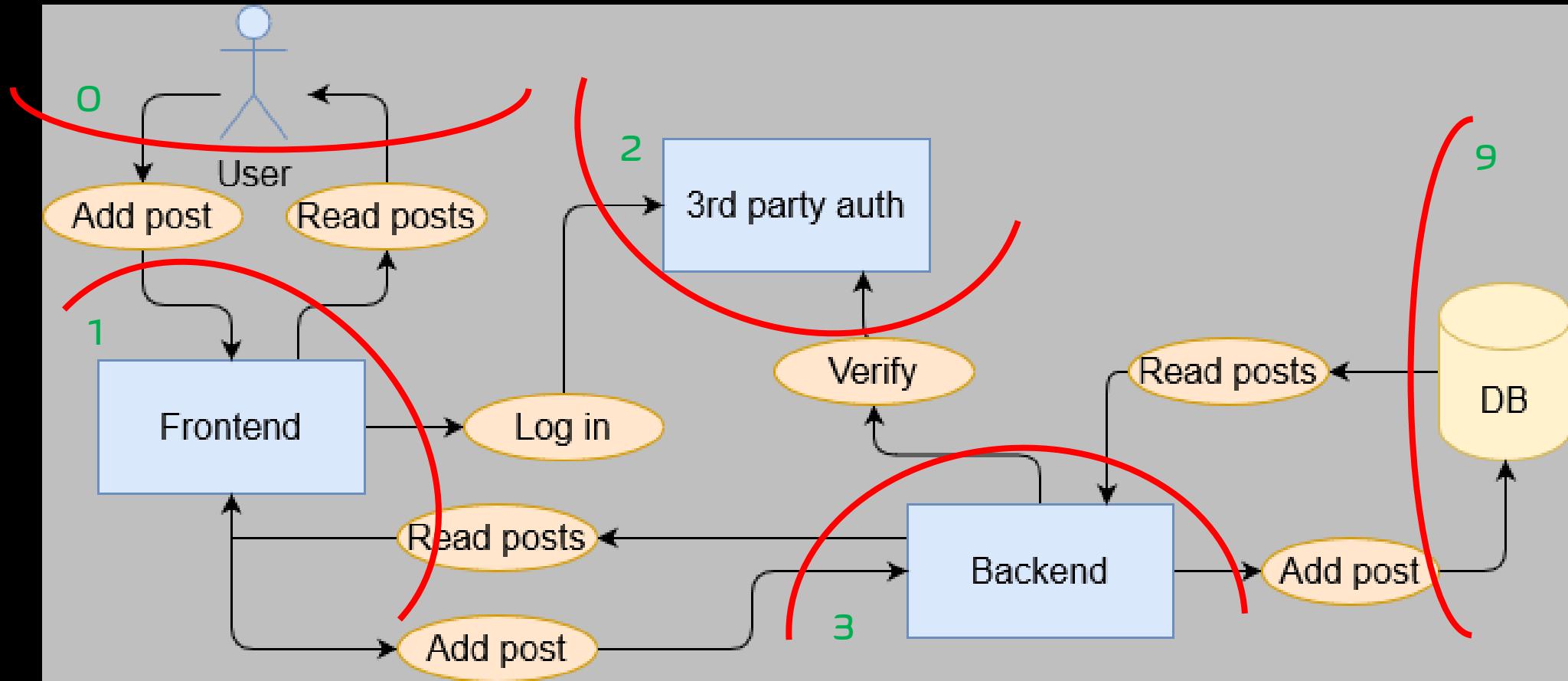
Step 3. risks

Step 4. remediations

Remediations



Repeat 8 times



Step 1. data flow diagram

Step 2. trust zones

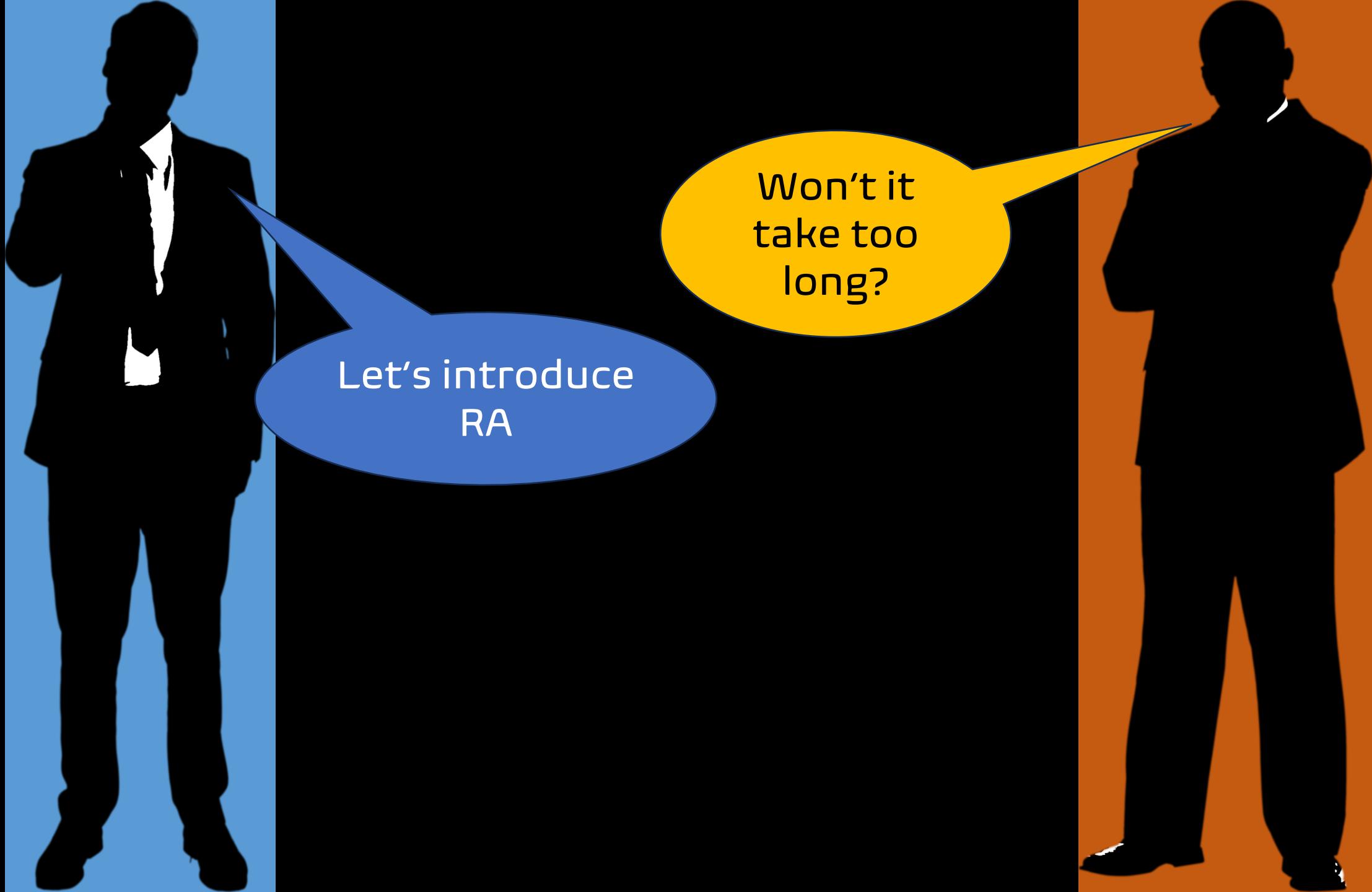
Step 3. risks

Step 4. remediations

Step 5. matrix

Vulnerabilities matrix

Risk	Criticality	Probability	Score
Overflow	3	7	10
Unauth access	9	6	15
Malicious js	5	9	14



Let's introduce
RA

Won't it
take too
long?



Before doing TM,
let's put a
questionnaire

Risk Assessment



Secar can You
help with
questions?

It's not like
this...

So it's your
idea, but I've
got to do the
job...

Let's work it out
together

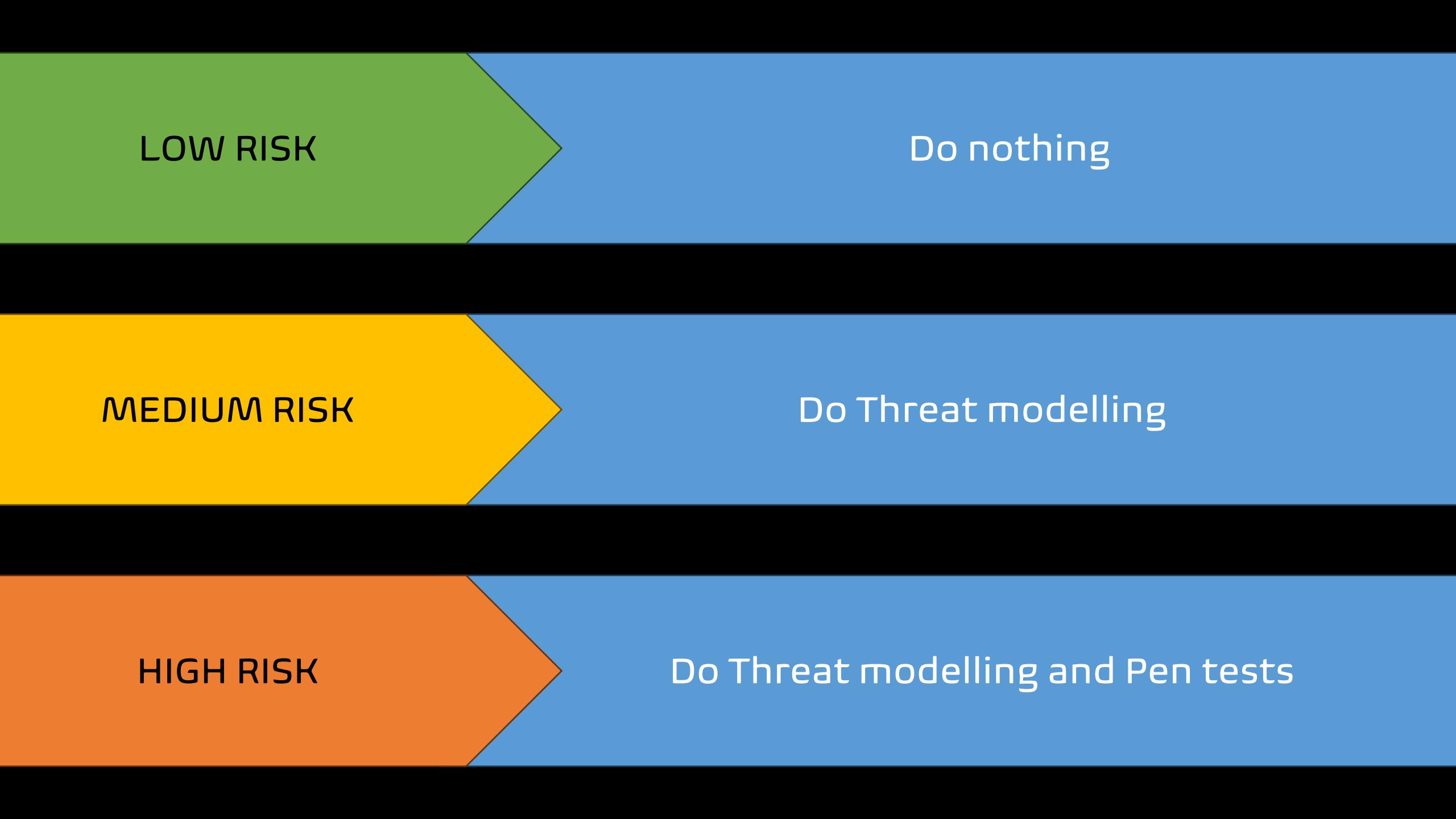
Q1: Does it touch customer data?

Q2: Does it expose new public endpoint?

Q3: Is new service introduced?

Q4: Does it change auth mechanism?

Q5: Is new 3rd party api used?



LOW RISK

Do nothing

MEDIUM RISK

Do Threat modelling

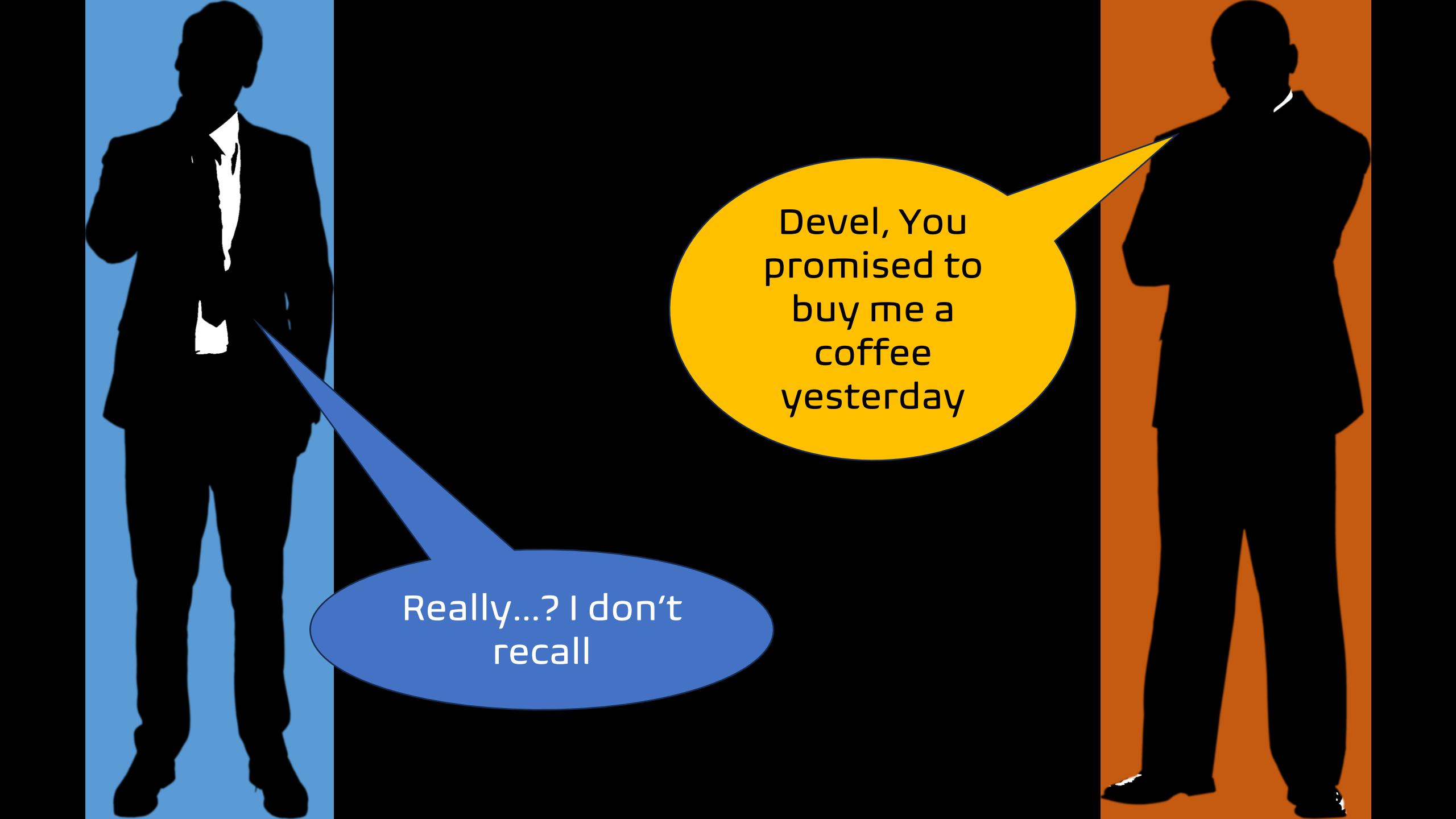
HIGH RISK

Do Threat modelling and Pen tests

Answers to RA questions and remediations in TM are

Promises





A black silhouette of a man in a suit stands on the left against a blue background. A yellow speech bubble originates from his mouth. A black silhouette of another man in a suit stands on the right against an orange background. A blue speech bubble originates from his mouth. The blue and orange areas overlap in the center where the two men are facing each other.

Devel, You
promised to
buy me a
coffee
yesterday

Really...? I don't
recall

Security Validation

Comment to RA answers and TM remediations with proof:

- Link to code line
- Link to generated report
- Screenshot
- Logs



I think it's
about
time to
sum up

... and for
a
promised
coffee

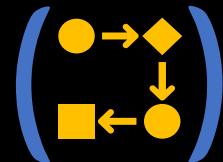
Planning dev (+ sec)



RA



TM



Coding + QA



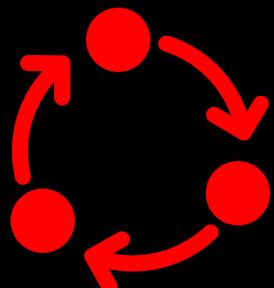
SAST/SAT



Validation



Pentest



Cons



More work on
developers side

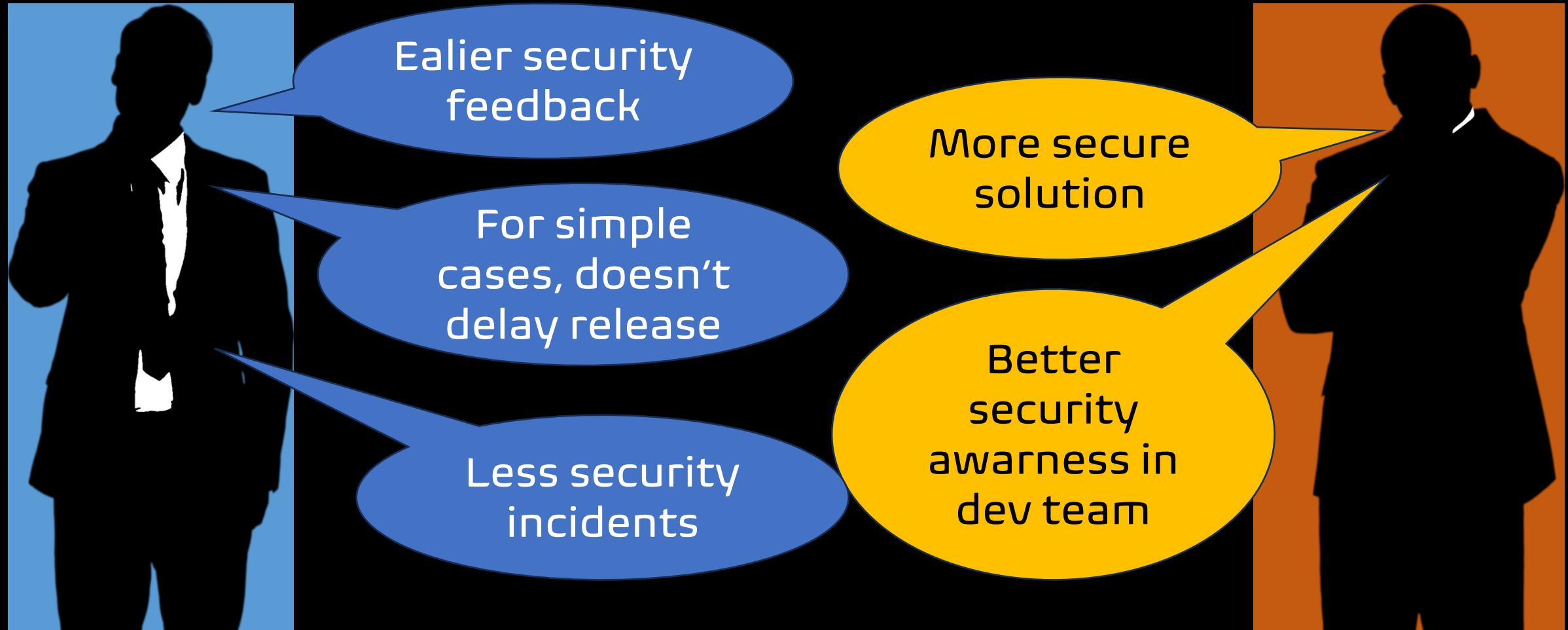
Requires
training

Delays
release

Vulnerable to
human errors



Pros

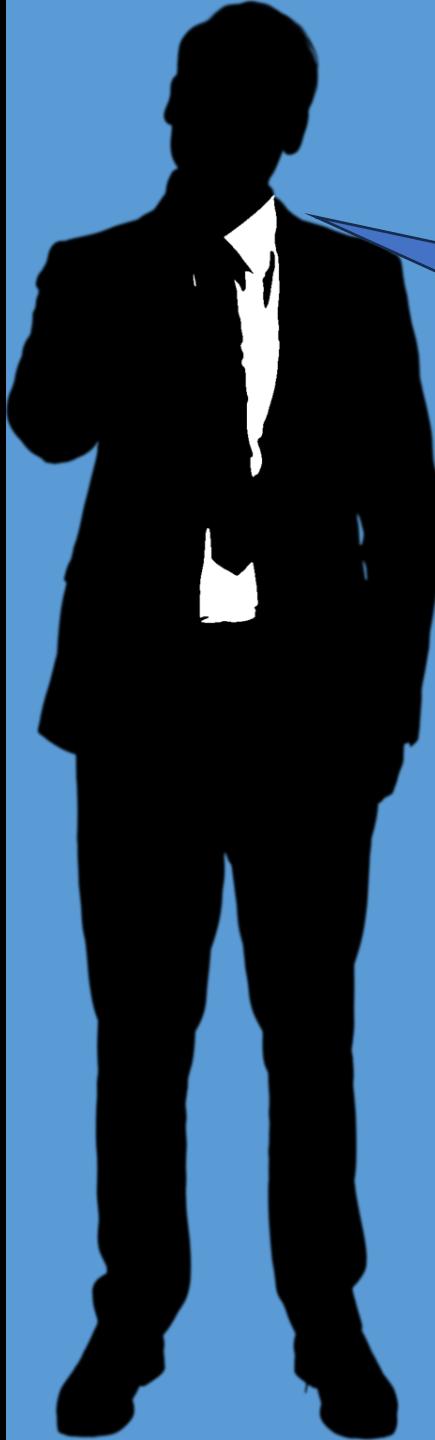




I guess this is
enough as 1st
draft

Definitelly

You can go
back to your
talk Marcin



Nevertheless,
have a good
day, bye!

Bye!