SECURE CODE

WARRIOR

How to spend $3.6M on one coding mistake and other fun stuff you can do with $3.6M

Matias Madou Ph.D., Secure Code Warrior

Matias Madou, Ph.D.

CTO and Co-Founder

- Ph.D. in Computer Engineering from Ghent University
- Over 15 years hands-on software security experience
- Led multiple application security research projects for HPE Fortify which have led to commercial products
- Instructor for advanced application security training courses
- Speaker at global conferences including RSA Conference, Black Hat, DefCon, BSIMM, OWASP AppSec and BruCon

What we believe…

… that developers can become the first line of defense against cyber attacks.

What can coding mistakes lead to?

INTRODUCTION

Coding failure costs money

Ariane 5 rocket

- $7 billion
- 10 years of work

Technical:

- Velocity: 64-bit float
- Convert to 16-bit int
- Overflow
- Error handling suppressed (performance)

Coding failure brand damage

C-Level people get fired

What's in the name?

APPSEC

Code Sample: Ariana 5 rocket

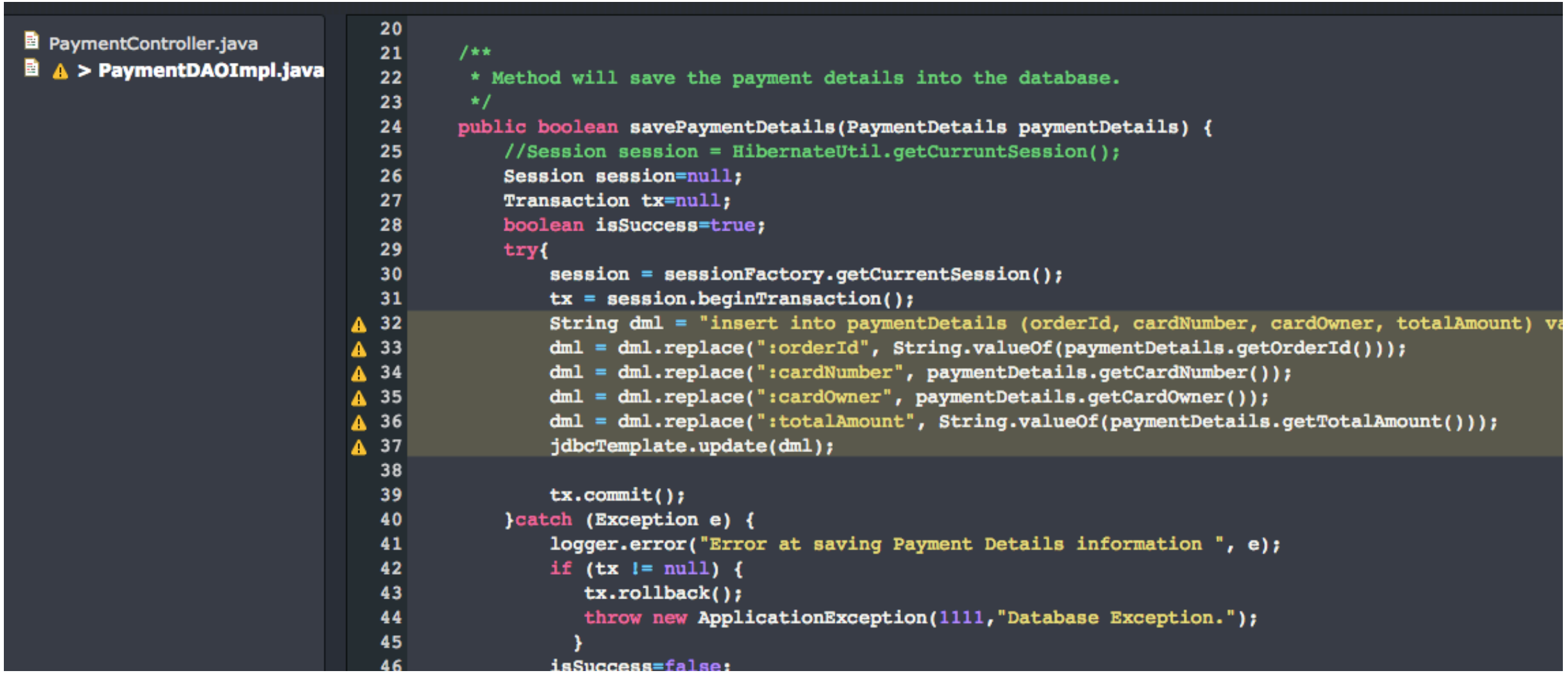
Why visibility matters—the Ariane 5 crash

- Velocity was represented as a 64-bit float
- A conversion into a 16-bit signed integer caused an overflow
- The current velocity of Ariane 5 was too high to be represented as a 16-bit integer
- Error handling was suppressed for performance reasons

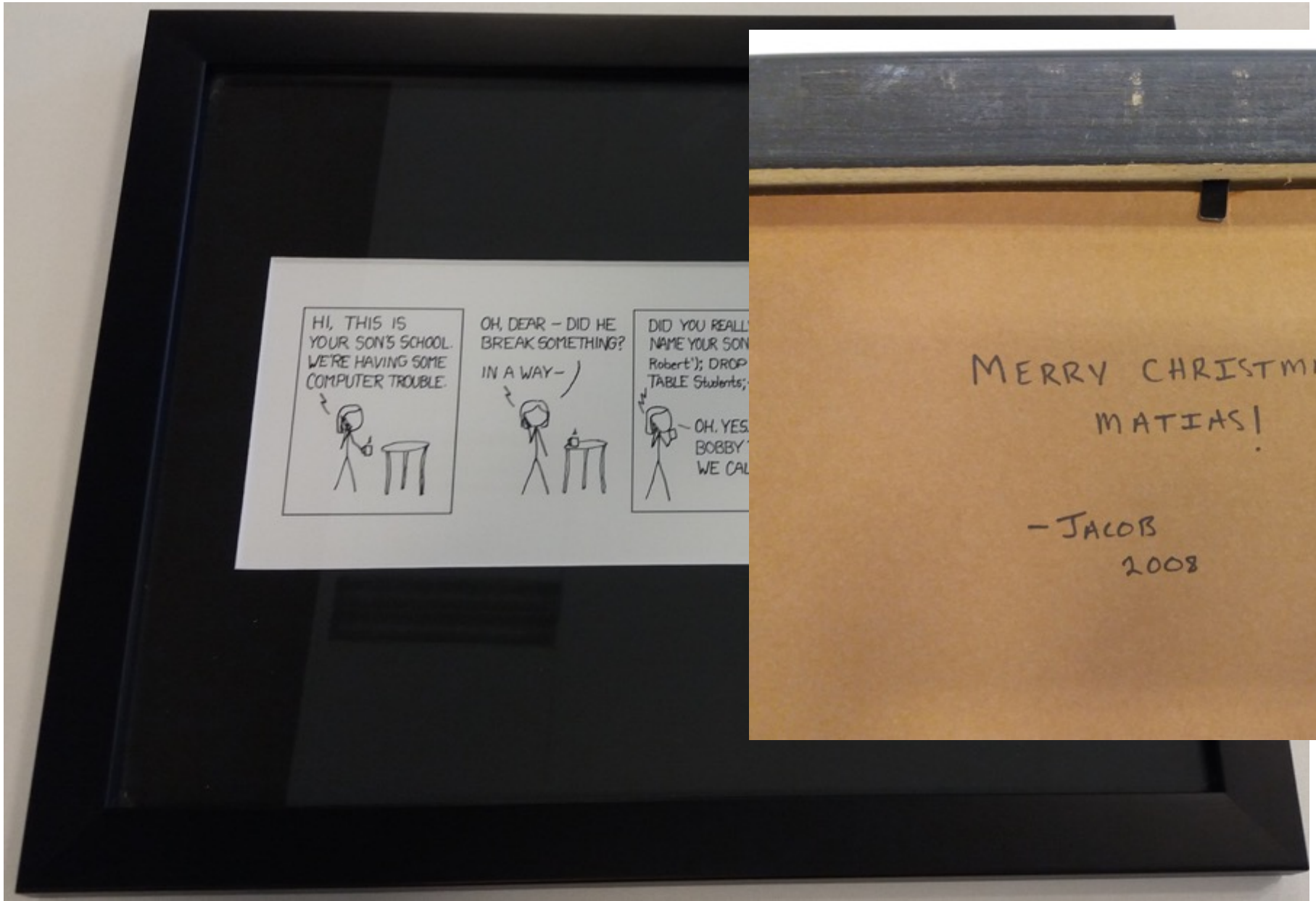
*Source: http://moscova.inria.fr/~levy/talks/10enslongo/enslongo.pdf

```
-- Vertical velocity bias as measured by sensor
L_M_BV_32 :=
   TBD.T_ENTIER_32S ((1.0/C_M_LSB_BV) *
   G_M_INFO_DERIVE(T_ALG.E_BV));
-- Check, if measured vertical velocity bias ban be
-- converted to a 16 bit int. If so, then convert
if L_M_BV_32 > 32767 then
   P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
elsif L_M_BV_32 < -32768 then
   P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
else
   P_M_DERIVE(T_ALG.E_BV) :=
            UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M_BV_32));
end if;
-- Horizontal velocity bias as measured by sensor
-- is converted to a 16 bit  int without checking
P_M_DERIVE(T_ALG.E_BH) :=
   UC_16S_EN_16NS (TDB.T_ENTIER_16S ((1.0/C_M_LSB_BH) *
   G_M_INFO_DERIVE(T_ALG.E_BH)));
```

Typical SQL Injection sample



Frame


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALL
NAME YOUR SON
Robert'); DROP
TABLE Students;
OH, YES.
BOBBY
WE CAL

MERRY CHRISTMAS
MATIAS!
–JACOB
2008

Why is this not resolved yet?

Security knows about issues in code

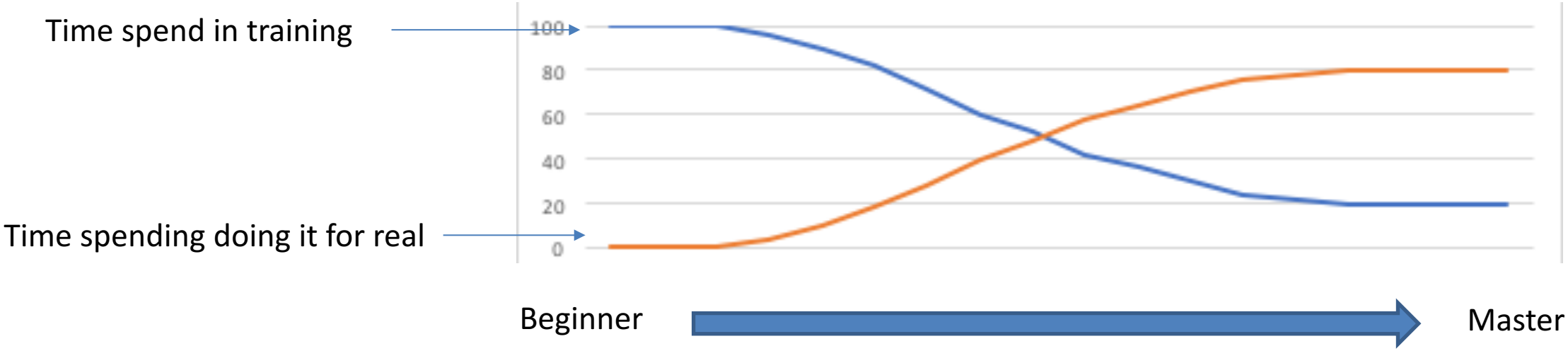
1) Fix known security issues → Scale of AppSec team?

→ Ton of overhead!

2) Do not introduce new issues → 700+ categories of problems!

∞ Never ending story…

Flying a plane: simulator vs flying for real



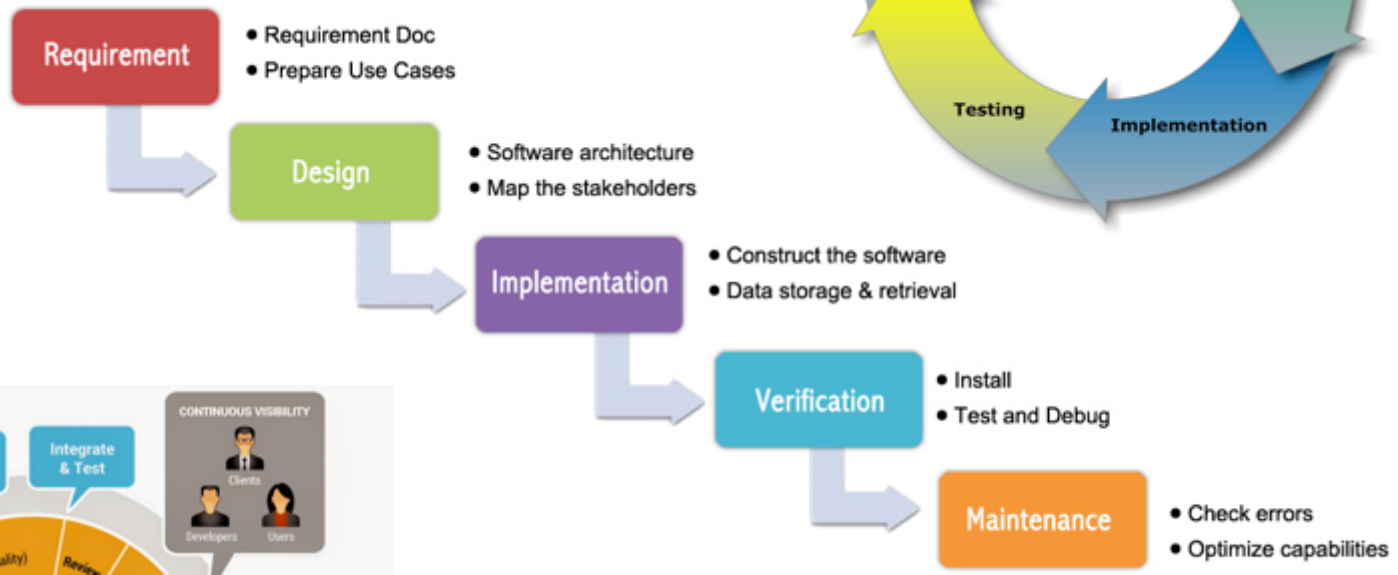
Software Development Lifecycle

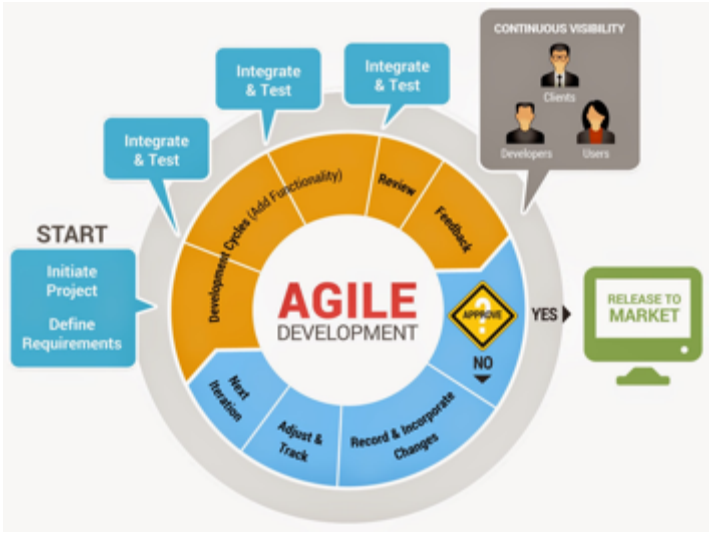
WHERE DO MISTAKES HAPPEN

Software development lifecycle

Waterfall, agile, …

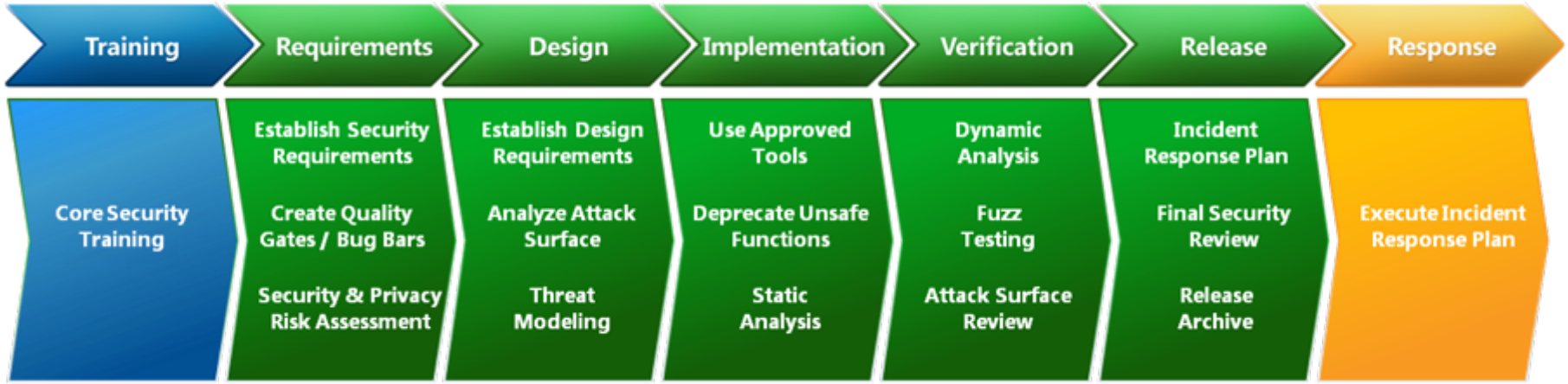
1. Security, where?
2. Developer view?

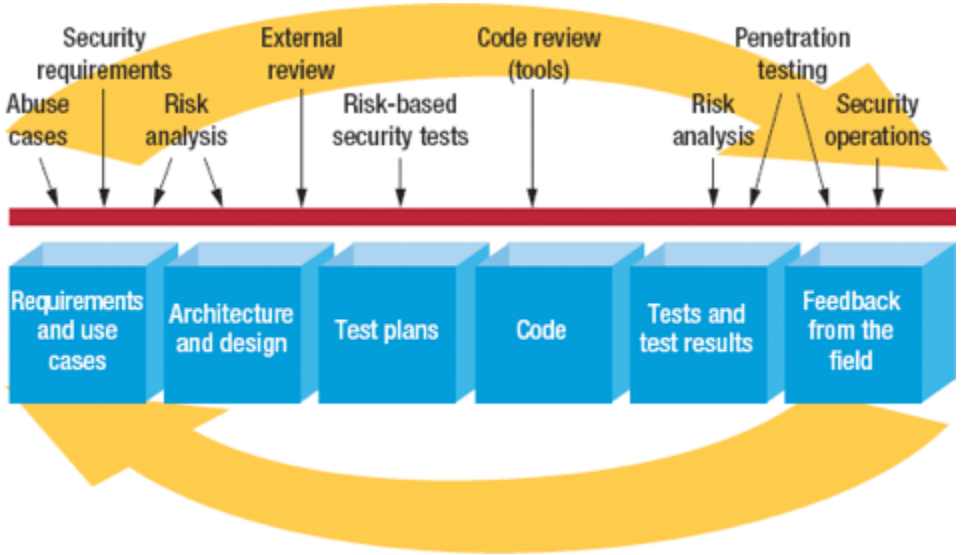




Secure Software Development Lifecycle

Microsoft SSDLC





Cigital Touchpoints

How does a developer look at this?

Developer → Write → Repository → Build → Deploy → Production

How does a developer look at this?

Developers can do something

No idea what's happening over there

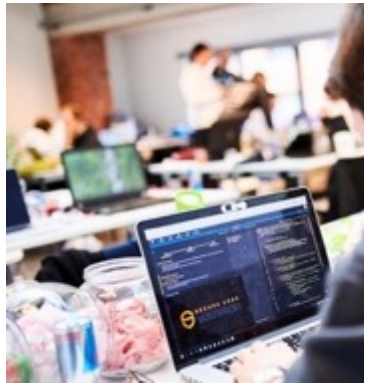
Developer → Write → Repository → Build → Deploy → Production

SECURITY…

How does

Developers can do

Developer



Production

How does a developer look at this?

Developers can do something

No idea what's happening over there

Developer → Write → Repository → Build → Deploy → Production

SECURITY…

Developer: total control
Security: no control

Developer: no control
Security: can access it…

How does a developer look at this?

Developers can do something

No idea what's happening over there

Developer → Write → Repository → Build → Deploy → Production

SECURITY…

Training

In IDE help

SAST

IAST

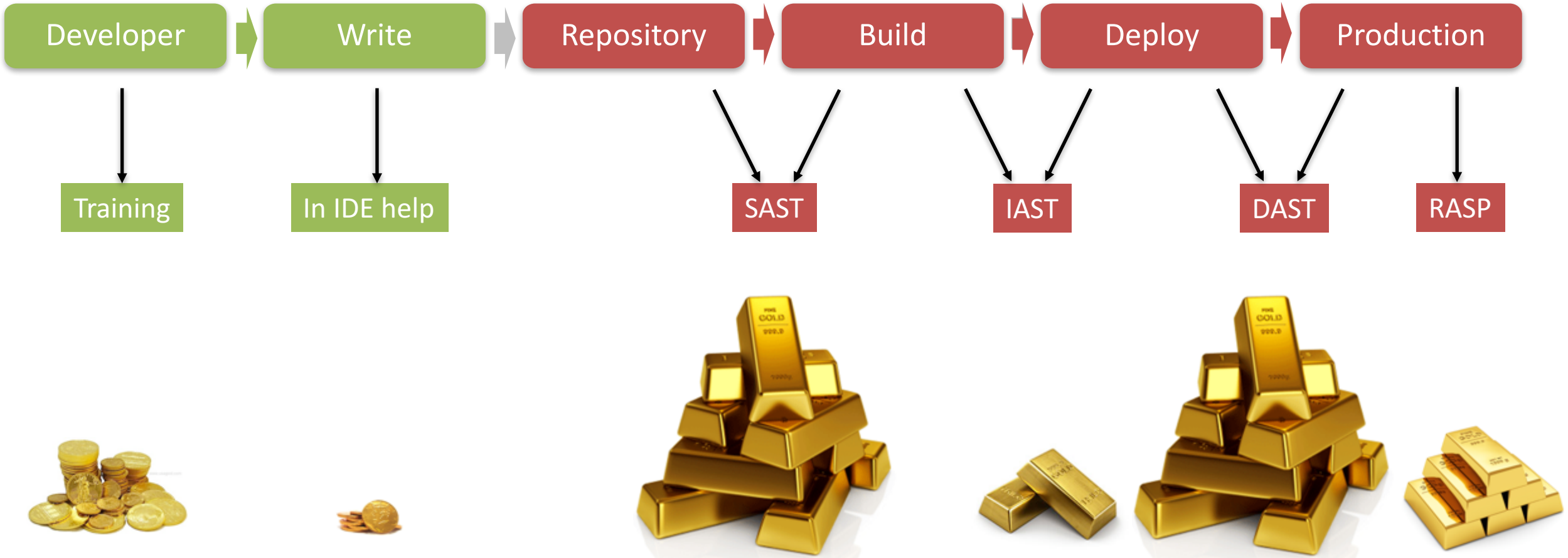
DAST

RASP

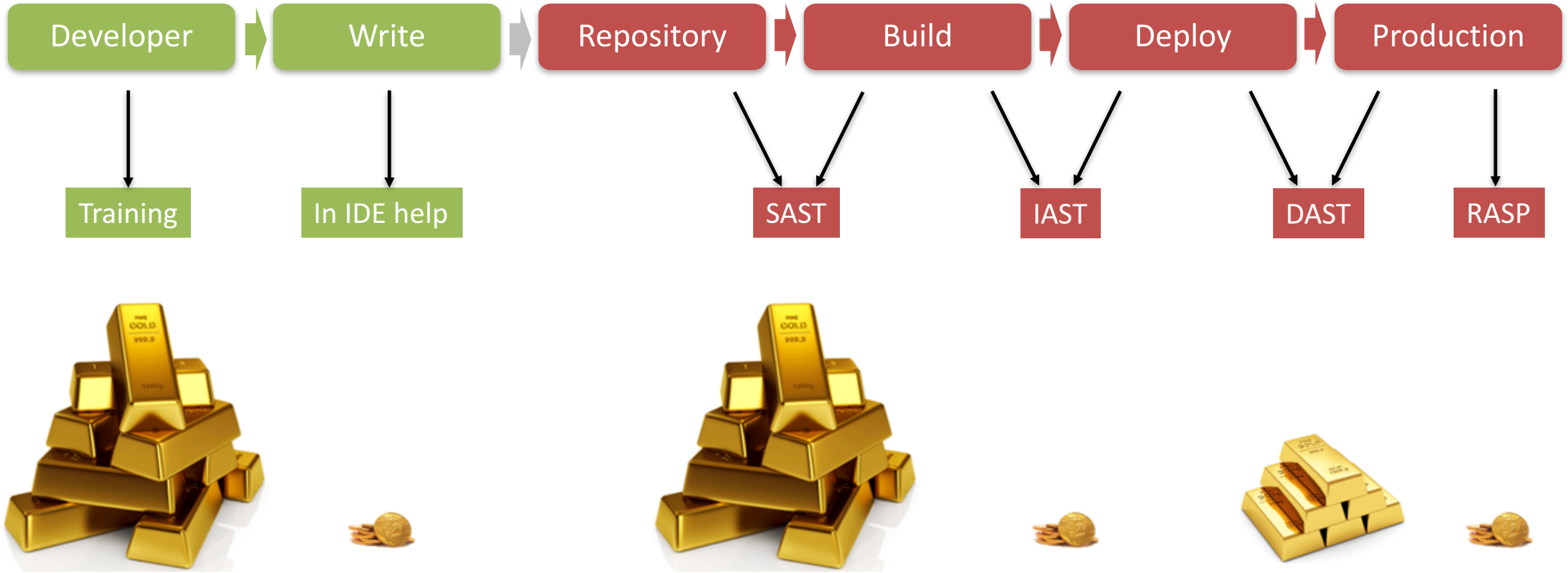
Solutions in place. Results

WHERE DO WE SPEND THE MONEY

How do companies spend their money?

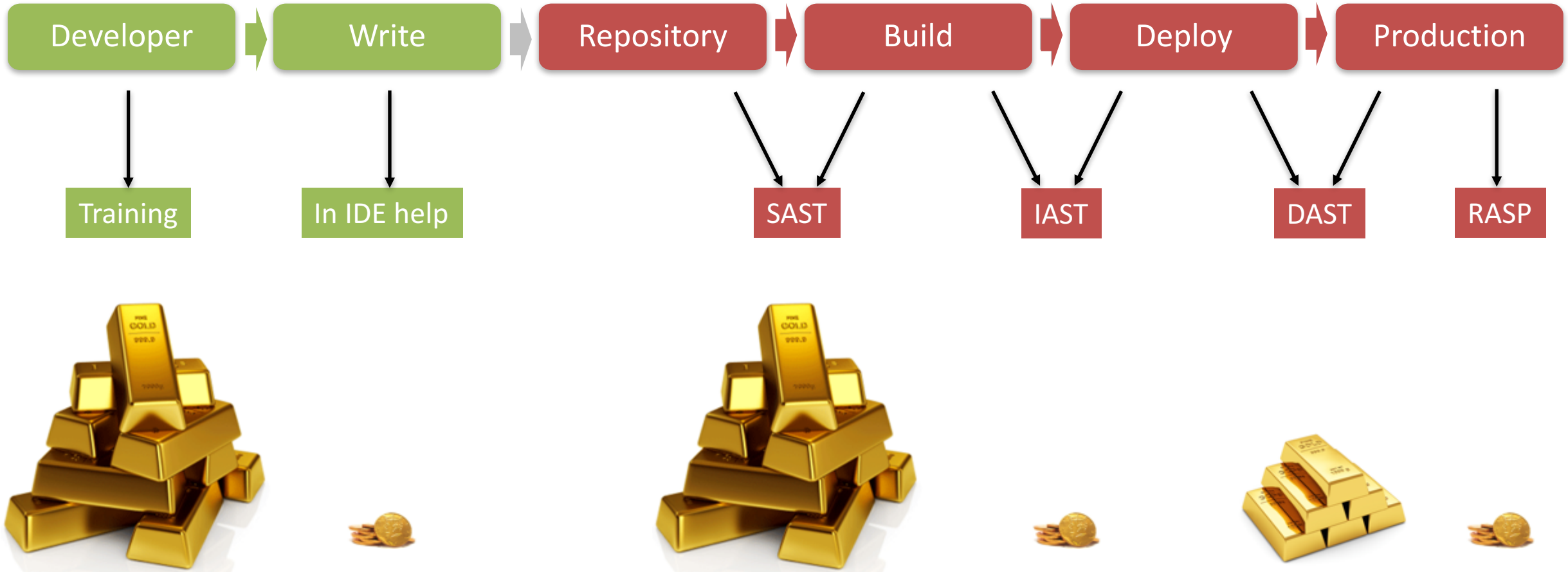


How do companies spend their money?



How do companies spend their money?

How do we spend the AppSec budget in the most optimal way? Nobody knows.

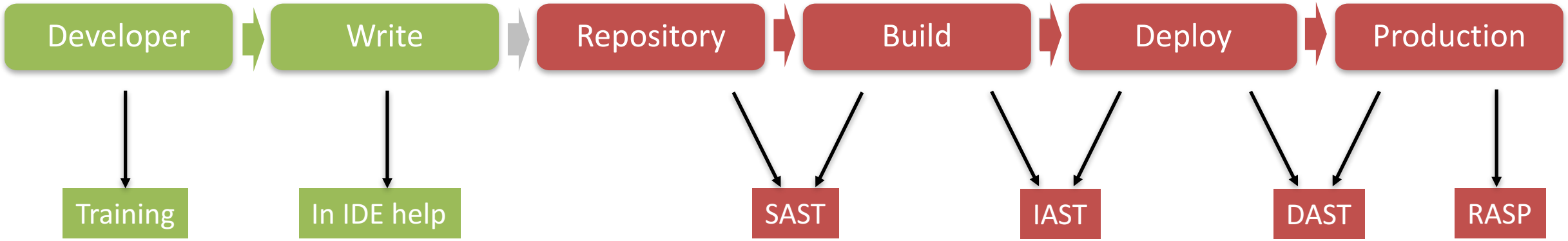


What we see in the field? Is there a pattern?

ACTUAL SPENDING

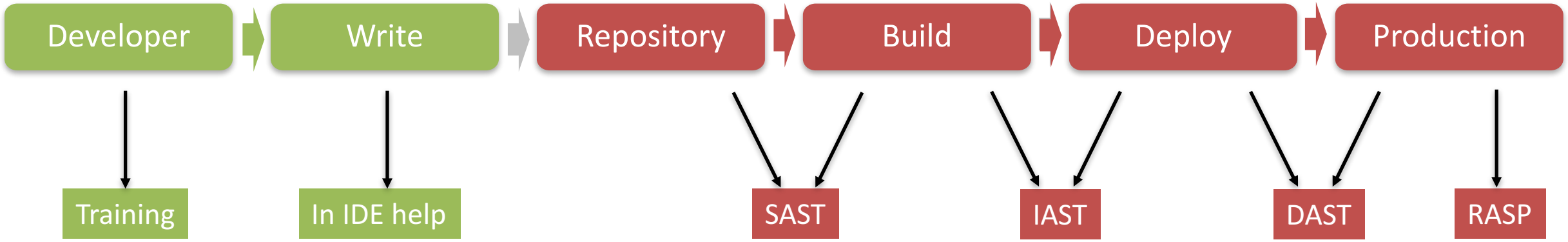
What type of company is this?

"All is good"-company Or, we are not hacked company … yet



What type of company is this?

"Ow s***, we need to do something" - company

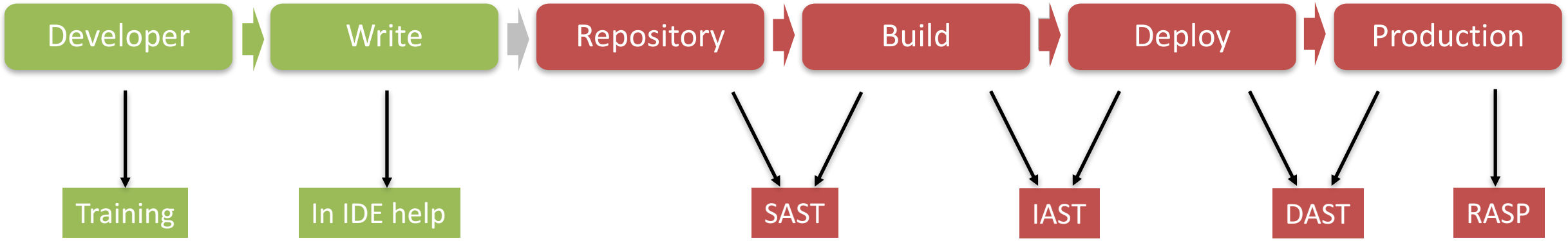


Ow s***, we need to do "pen-testing" and hackers and the like

What type of company is this?

Company maturing over time…

but it's very reactive and baseless.



PCI Compliance sticker

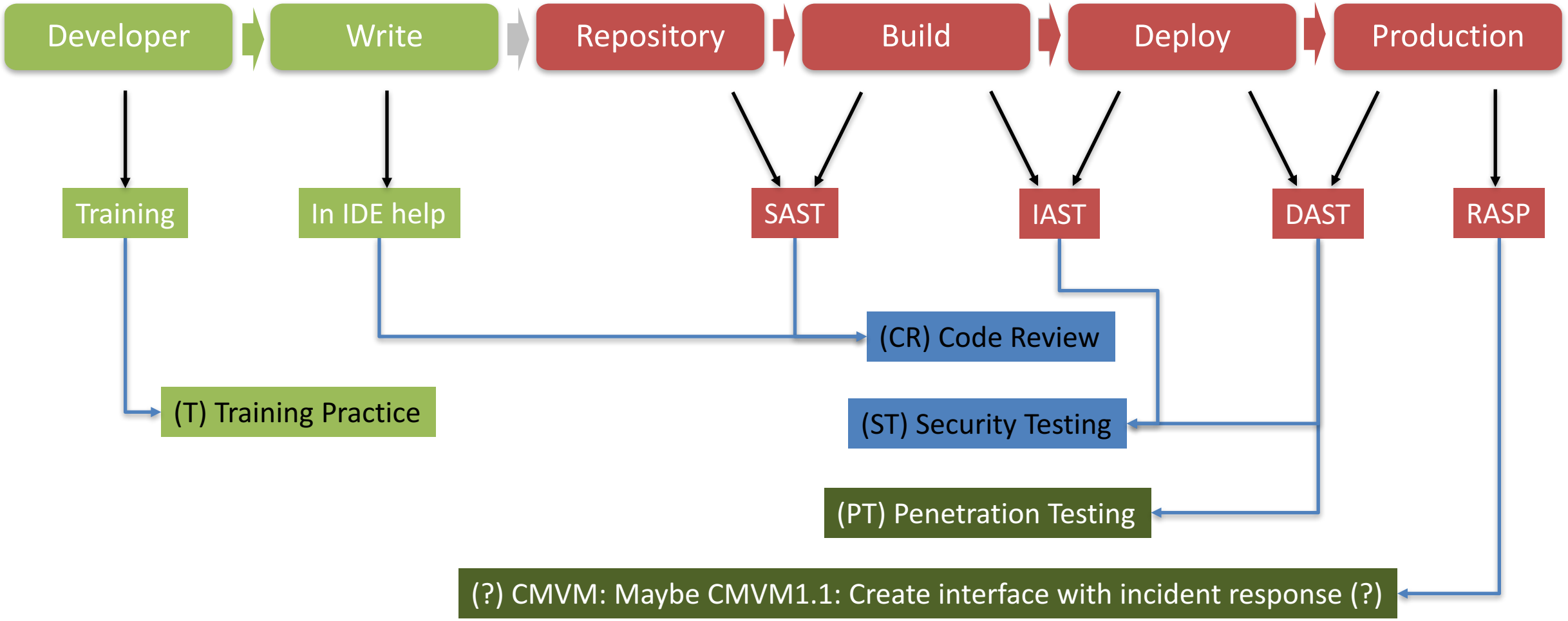
Good sales people, lot of traction

Gartner says it's the latest good stuff

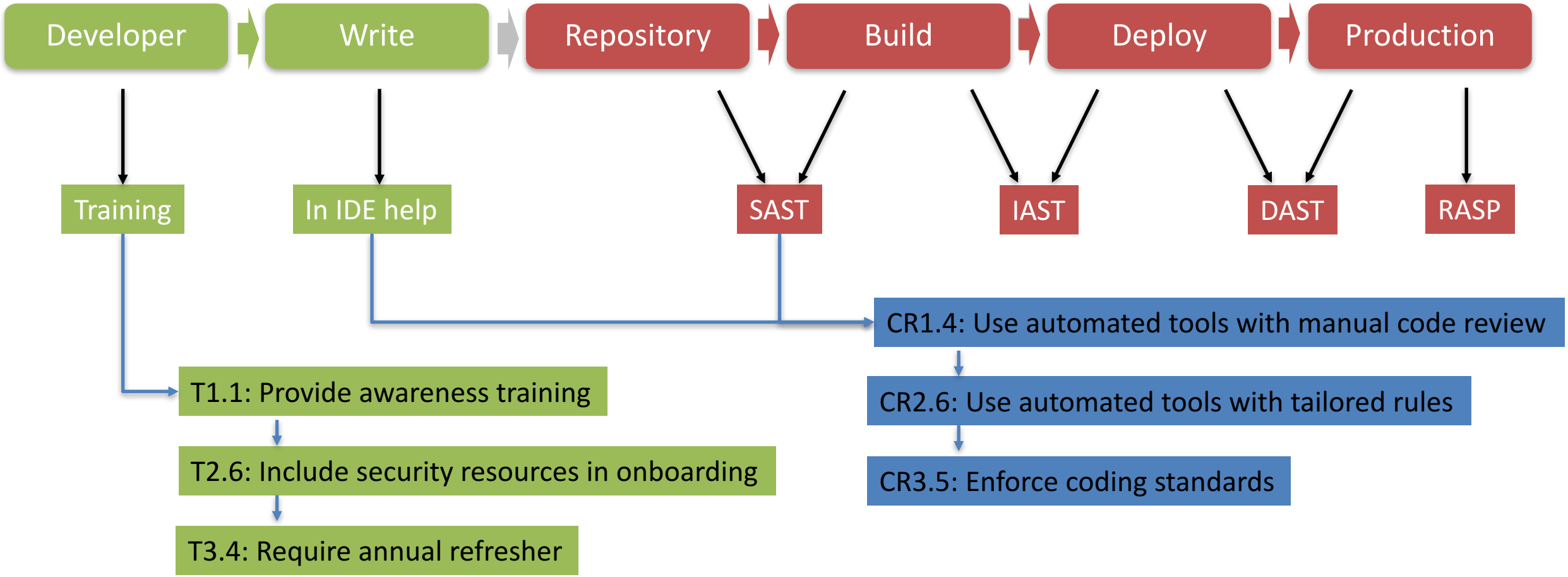
Pros and cons on the technology

WHERE DO WE HAVE TO SPEND?

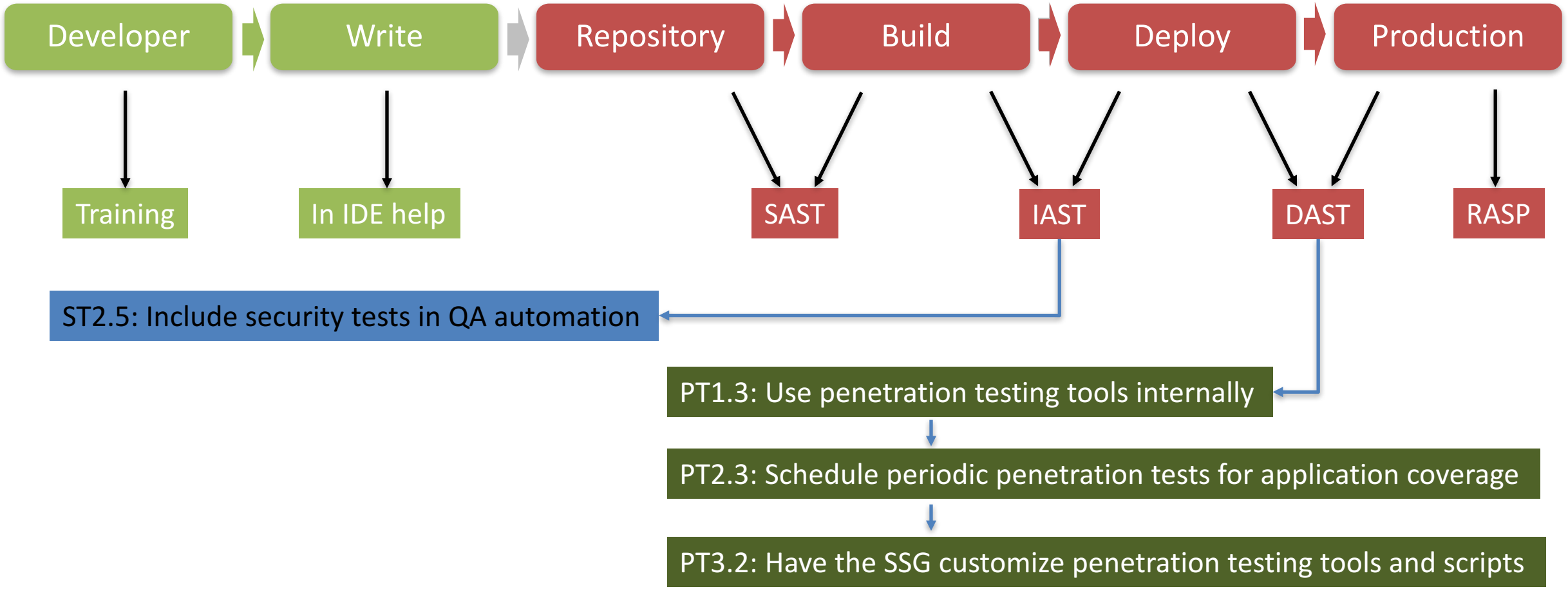
What does the BSIMM say?



What does the BSIMM say?

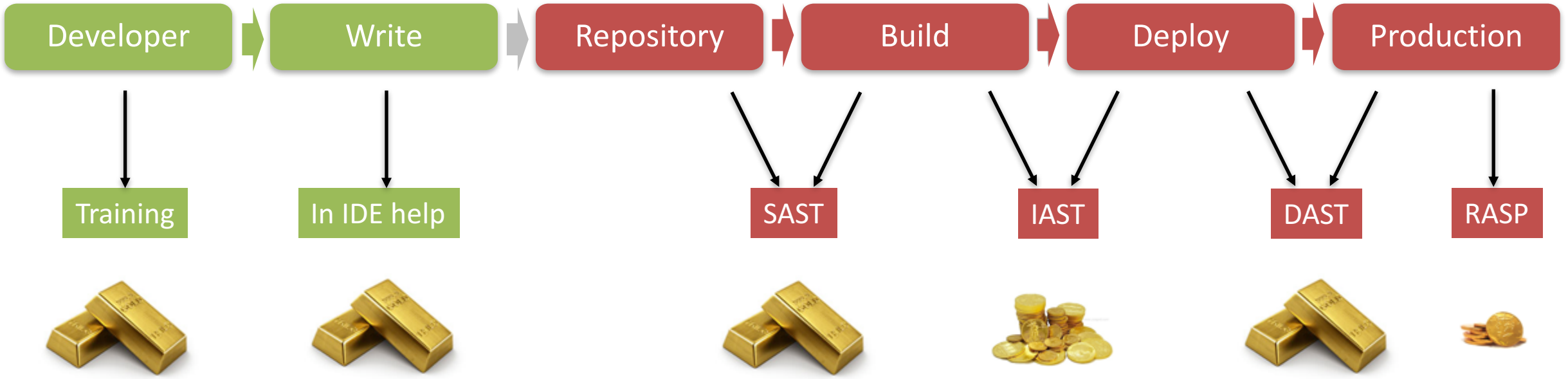


What does the BSIMM say?



End result: all solutions have their pros and cons

Cool … but we cannot call this progress



All this is saying: Yes, there is a valid case to spend money

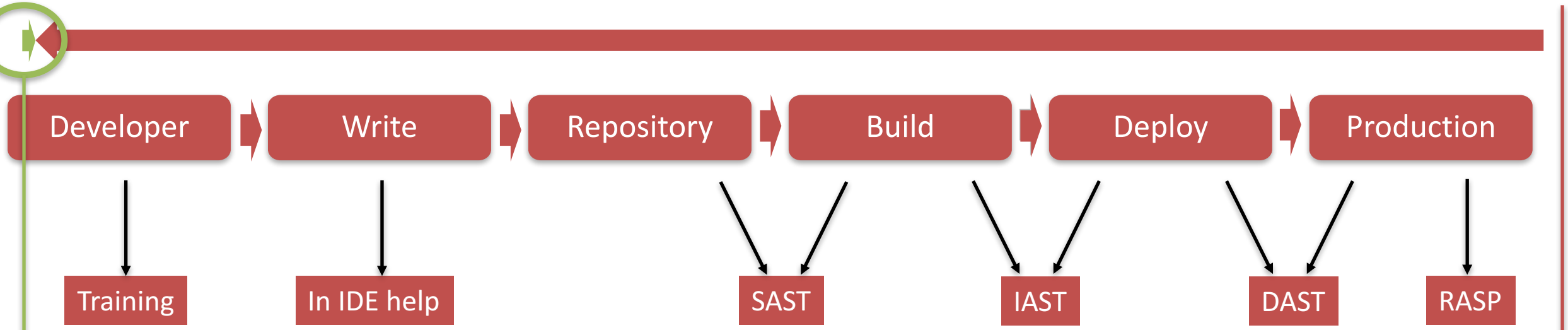
Finding problems vs. coding right

WHAT DO WE DO IN APPSEC?

What do we do?

Write Secure code: Coding guidelines

Find the bad stuff: talk about vulnerabilities

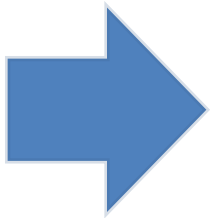


- OWASP Secure coding guidelines
- Android Secure development (JSSA)
- …

- SQL Injection
- OWASP Top 10
- …

AppSec approach today

```
“SELECT * FROM database WHERE
        param1 = ‘ ” + param1 + ” ’ and
        param2 = ‘ ” + param2 + ” ’ and
        param3 = ‘ ” + param3 + ” ’ and
        param4 = ‘ ” + param4 + “ ’;”
```



```
“SELECT * FROM database WHERE
        param1 = ? and
        param2 = ? and
        param3 = ???????????????? and
        param4 = ‘ ” + param4 + “ ’;”
```

Ask QA to find an exploit?

What's the difference?

Vulnerability	Write coding guideline
• SQL injection • Command injection • …	• Use parameterized queries • Command line execution is forbidden • …

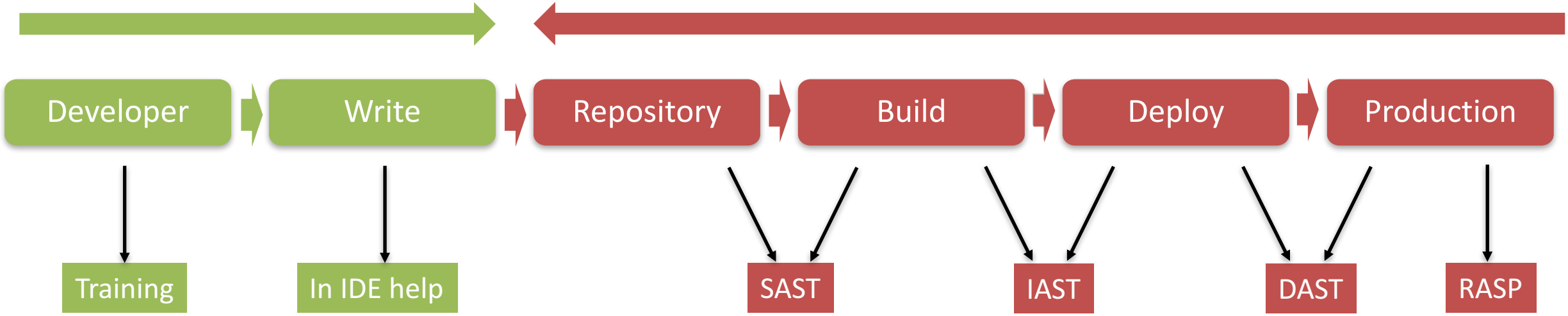
Badness-ometer

Courtesy of Gary McGraw, Cigital

Best ROI and value for money?

Write Secure code: Coding guidelines

Find the bad stuff: talk about vulnerabilities



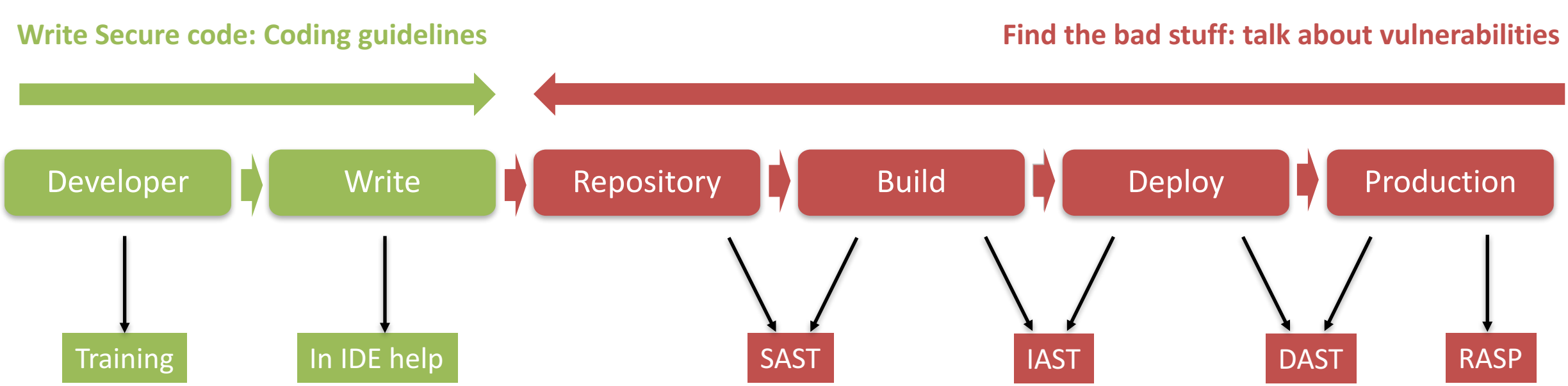
Prevention

Detection

Badness-ometer

Courtesy of Gary McGraw, Cigital

What type of company is this?



80% NOT introduced

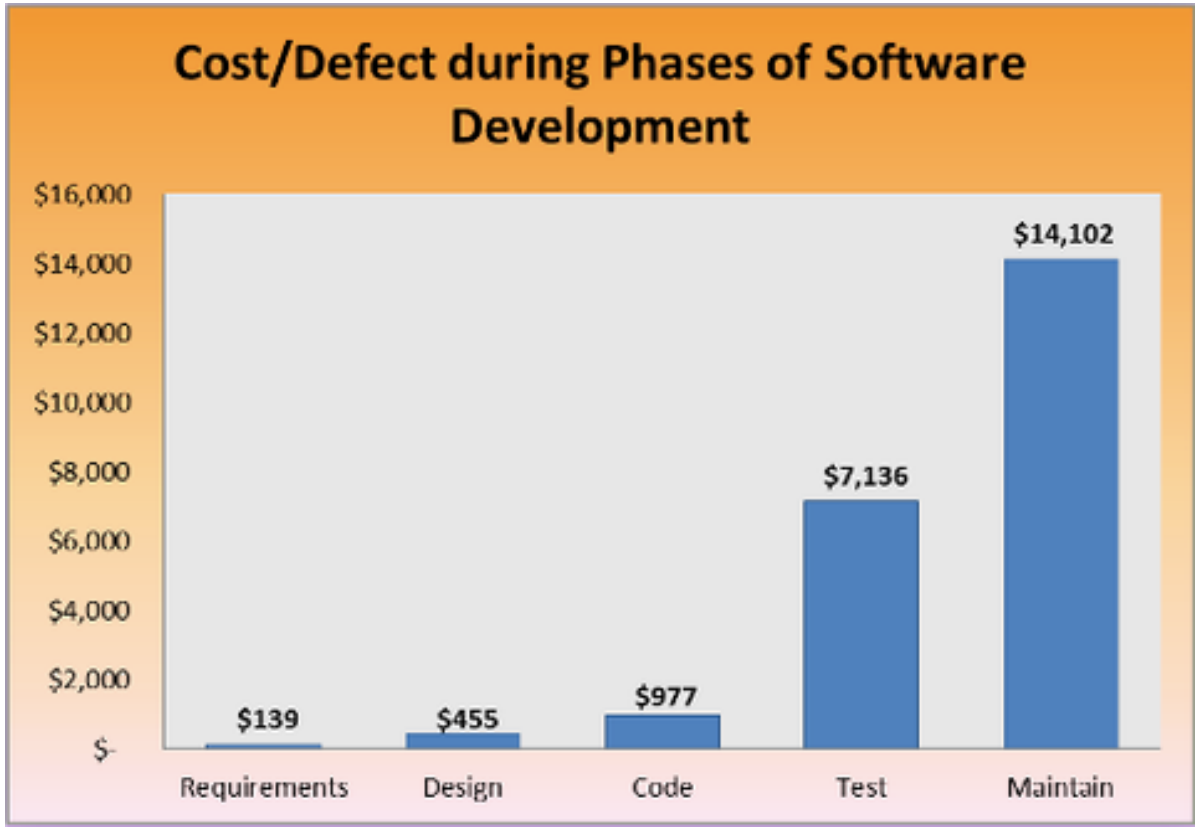
20% detected and fixed

Deeper dive

WHERE DO WE HAVE TO SPEND?

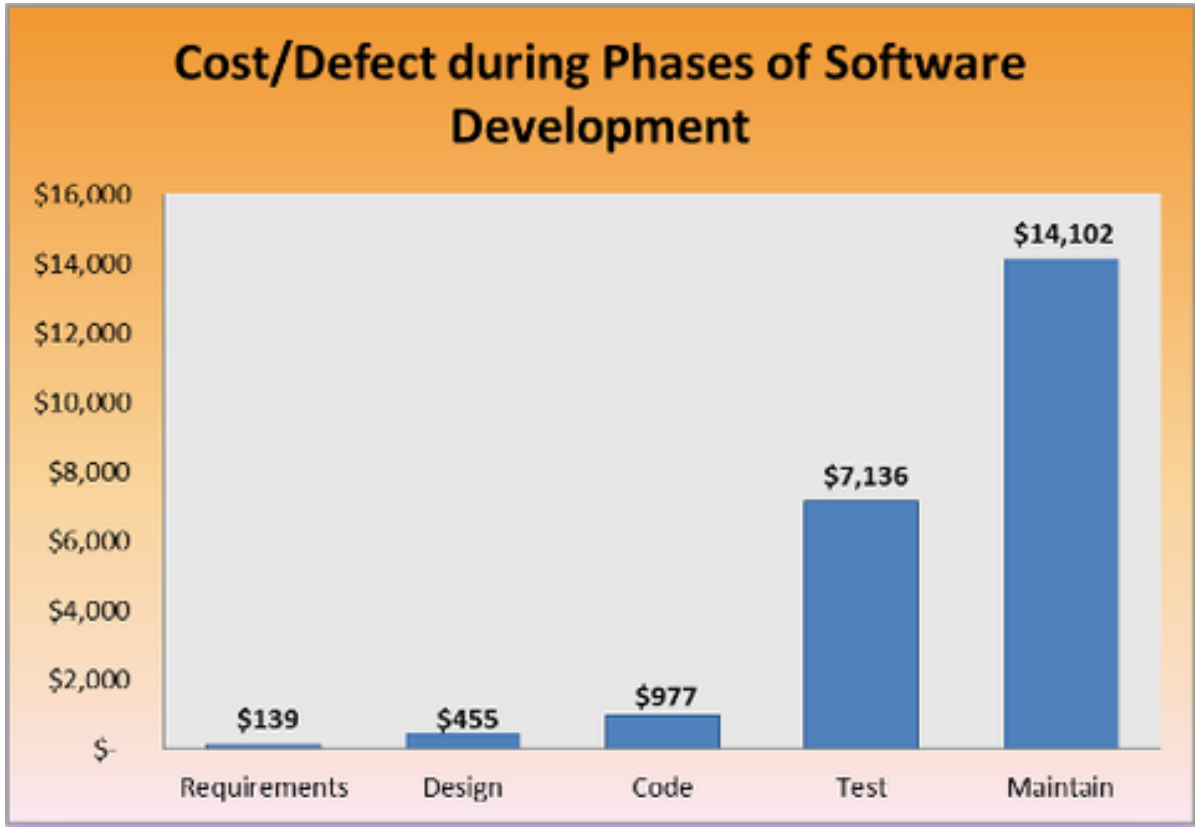
Let's throw numbers in there

General consensus: the earlier you find it, the less it costs to fix



Actual data from Jim Routh, Aetna

Should we care?



Actual data from Jim Routh, Aetna

3.6 million, average cost of a breach

		$ 3,600,000	
Requirements	$ 139	25,899	issues
Design	$ 455	7,912	issues
Code	$ 977	3,685	issues
Test	$ 7,136	504	issues
Maintain	$ 14,102	255	issues

You can fix more than 1 problem!

Penetration testing: Consulting services

The numbers:

10D @ $$/day	Xxxx	$20,000
Issues found	Yyyy	10
Developer cost(fix)	Zzzz	No time
COST	Pretty big number	Waste of money
⬇	⬇	
COST/issue	Still a big number	

Penetration testing: Consulting services

The numbers:

10D @ $$/day	Xxxx	$20,000
Issues found	Yyyy	10
Developer cost(fix)	Zzzz	$2,000
COST	Pretty big number	$40,000
COST/issue	Still a big number	$4,000

Fill in your own numbers! This is an example. Do the exercise internally.

Penetration testing: Consulting services

The numbers:

10D @ $$/day	Xxxx	$20,000
Issues found	Yyyy	10
Developer cost(fix)	Zzzz	$2,000
COST	Pretty big number	$40,000
COST/issue	Still a big number	$4,000

Bear in mind that these are real issues !

Likability of an adversary exploiting these is high

SAST Solution

The numbers:

Cost of SAST solution	Xxxx
Issues found	Yyyy
Developer cost(fix)	Zzzz
COST	Pretty big number
COST/issue	Looks better than Pen testing

Bear in mind that these are theoretical problems

SECURE CODE WARRIOR

The numbers:

Cost of training

??

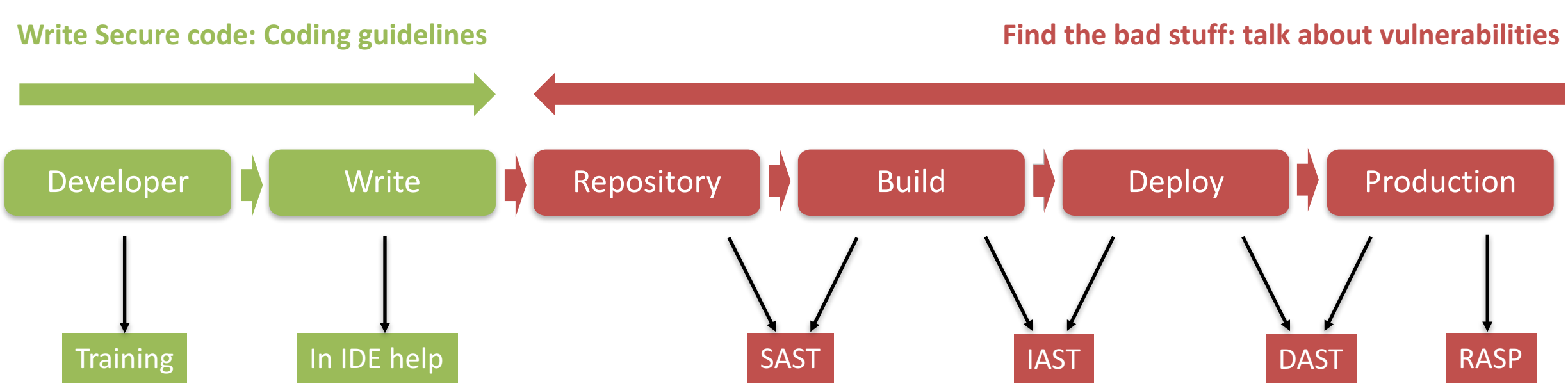
??

COST

COST/issue

Effect of training on coding: Less mistakes introduced + issues fixed

Conclusion on where to spend money



1. Measure! Security is measurable
2. Calculate ROI
3. Optimize your budget

➡ Developer introduces $45.18/day on security problems in the code

Solution 1: Get rid of all developers

Write Secure code: Coding guidelines

Find the bad stuff: talk about vulnerabilities

Developer

Training

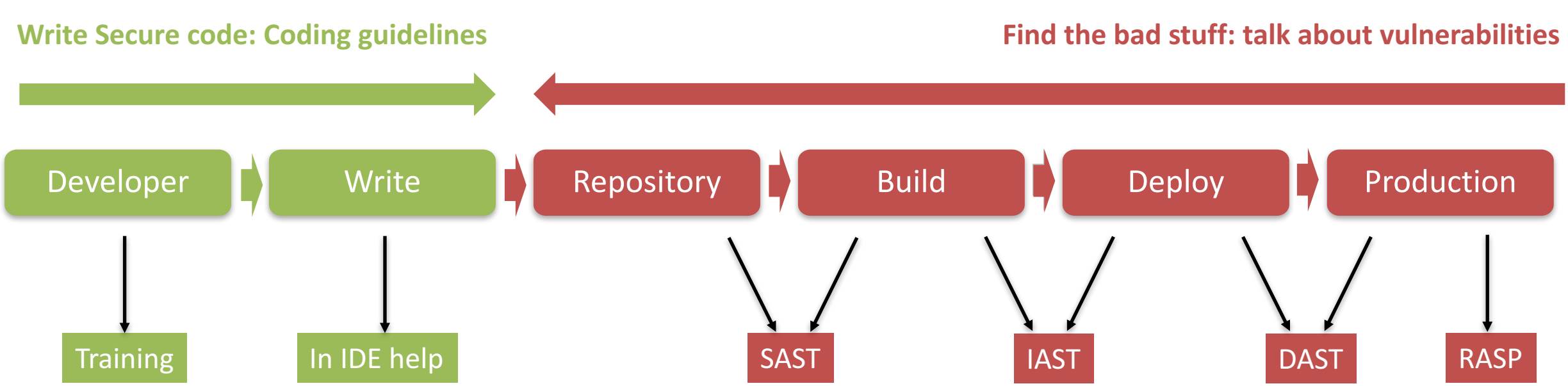
Production

RASP

1. Measure
2. Calculate
3. Optimize

Developer introduces $45.18/day on security problems in the code

Solution 2: Do the numbers and optimize budget



1. Measure! Security is measurable
2. Calculate ROI
3. Optimize your budget

Bring down this number!

Developer introduces ~~$45.18~~/day on security problems in the code

Try it out yourself

TOURNAMENT

Join the Tournament: Play and win

ACCOUNT & TOURNAMENT REGISTRATION

1. GO TO: **https://portal.securecodewarrior.com/#/register**

2. CLICK ‘REGISTER’, FILL IN YOUR EMAIL AND USE THE FOLLOWING TOKEN KEY:
   947 273 385 338

3. **Click on the Tournaments Tab, and then Click BENELUX2017**

THE TOURNAMENT WILL GO LIVE AT 10.30AM and stop at 4:00PM

Follow us on Twitter and be in with a chance to win some more cool prizes @Seccodewarrior #securecodewarrior

SECURE CODE WARRIOR

JOIN THE TOURNAMENT
WIN AWESOME PRIZES

ARE YOU A SECURE CODE WARRIOR?

Join Secure Code Warrior's live tournament to prove your web application security knowledge of the OWASP Top 10 or if you simply want to learn more about secure coding.

Players will be presented with a series of vulnerable code challenges that will ask them to identify the problem, locate the insecure code, and fix the vulnerability. Select from various software languages to complete the tournament, including: Java EE, Java Spring, C# MVC, C# WebForms, Ruby on Rails, Python Django, Scala Play, Java Struts & Node.JS.

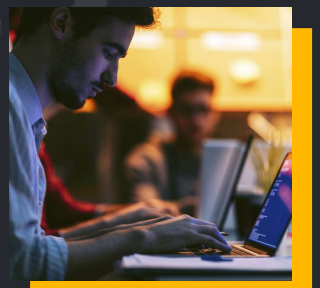
Watch as you climb to the top of the leaderboard and be crowned the 'Secure Code Warrior.' Prizes will be provided to the top three winners.

Instructions:

1. Visit https://portal.securecodewarrior.com/#register
2. Enter invitation token: 947 273 385 338
3. Update your details and go to the Tournaments tab and enter join code: BENELUX2017
4. Follow us on social media and use hashtag #securecodewarrior for a chance to win extra prizes

Connect with us:

- @seccodewarrior
- facebook.com/securecodewarrior
- linkedin.com/company/secure-code-warrior
- securecodewarrior.com



Matias Madou, Ph.D.

CTO and Co-Founder

Secure Code Warrior

+32 495 25 49 78

mmadou@securecodewarrior.com

@mmadou

www.linkedin.com/in/matiasmadou/

SECURE CODE WARRIOR

Follow us on social media and use the hashtag #securecodewarrior for a chance to win prizes!

APPLICATIONSECURITYINSIGHTS.SECURECODEWARRIOR.COM

SECURECODEWARRIOR.COM

@SECCODEWARRIOR

LINKEDIN.COM/COMPANY/SECURE-CODE-WARRIOR

FACEBOOK.COM/SECURECODEWARRIOR/