Find and fix software security problems… wait, do not make security mistakes in the first place!

SENSEI SECURITY

Faster time to secure code

- Founded in 2016 to create the next generation of solutions to expertly guide developers in writing secure code.

Thought leadership

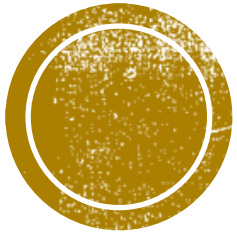
Experts

Built successful products

WHO ARE YOU?

What is your interest in this talk?

- Audience — Students, developers, security
  - Developer? — Is Security annoying?
  - Security? — Are developers annoying?
  - Students? — Security Courses?



“SECURITY”

What are software security problems?

SECURITY

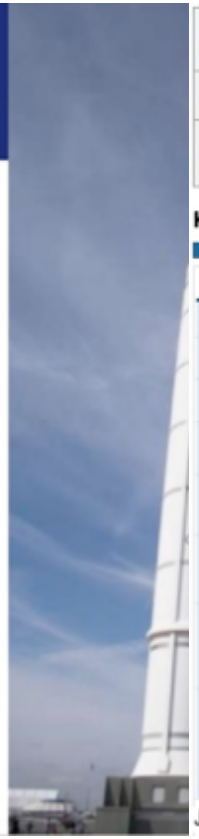
What's in the name?

DEVELOPERS INTRODUCE BUGS

Most expensive bugs?

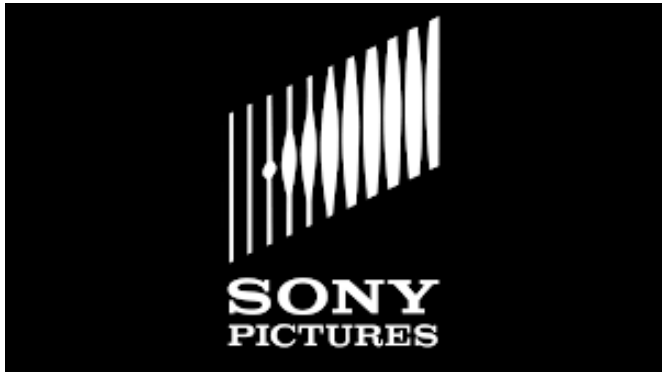
The Ariane 5

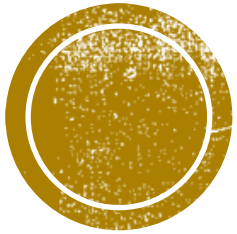
- $7B development
- $500M rocket & cargo
- Software Based on the Ariane 4



SOFTWARE SECURITY PROBLEMS

Tell me some application security stories! (SQL injection)





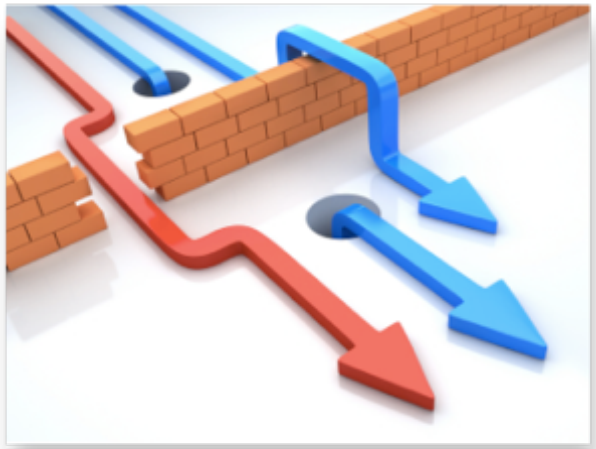
FIND PROBLEMS

Today's view on Application Security: All about finding problems

PEOPLE AND TOOLS

SAST, DAST, IAST, RASP, …

DAST (Penetration testing solutions and the like)



Peer code review

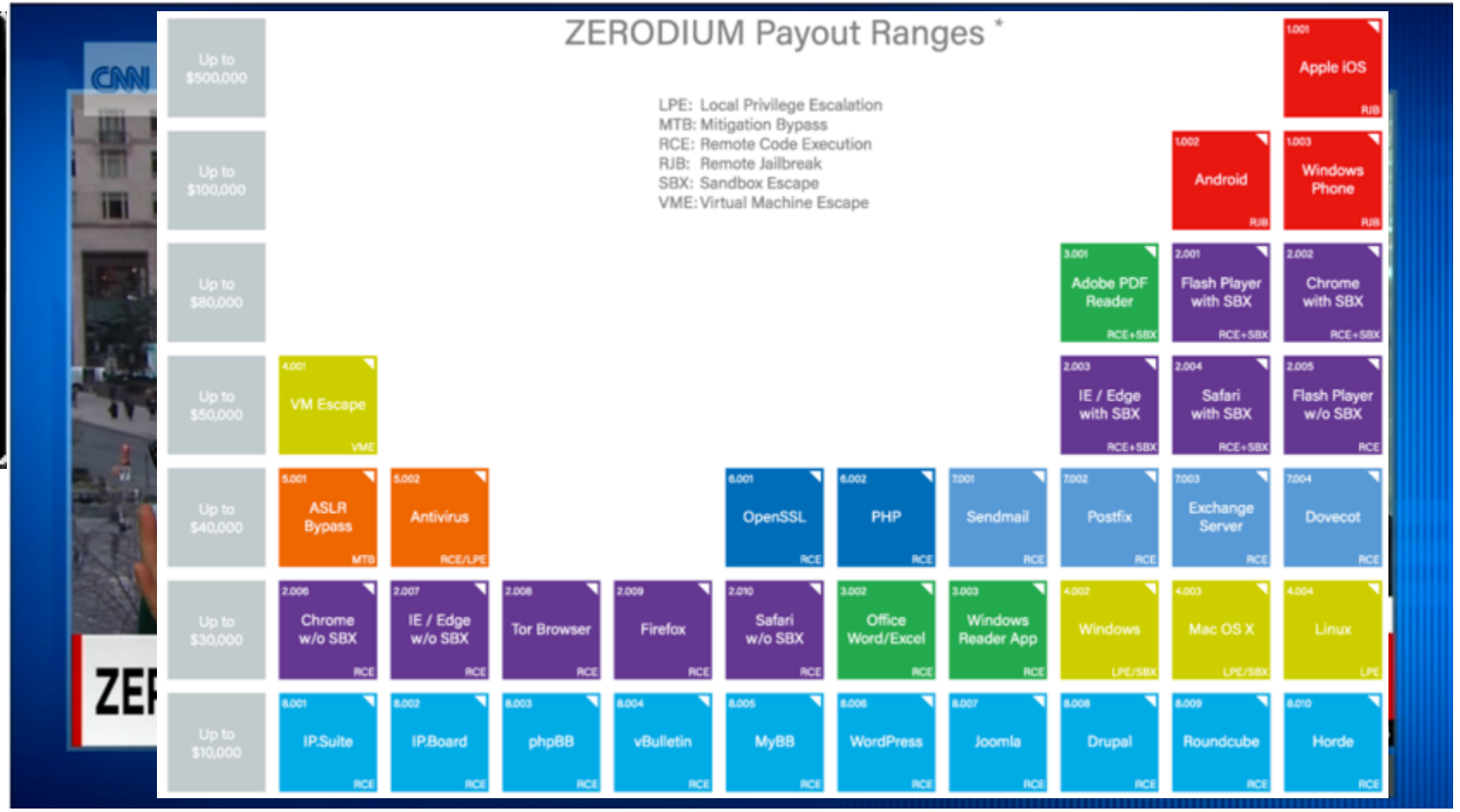
Static Analysis (SAST)

WHITE-HAT HACKERS

Knock knock, who's there?

BLACK-HAT HACKERS

No longer underground

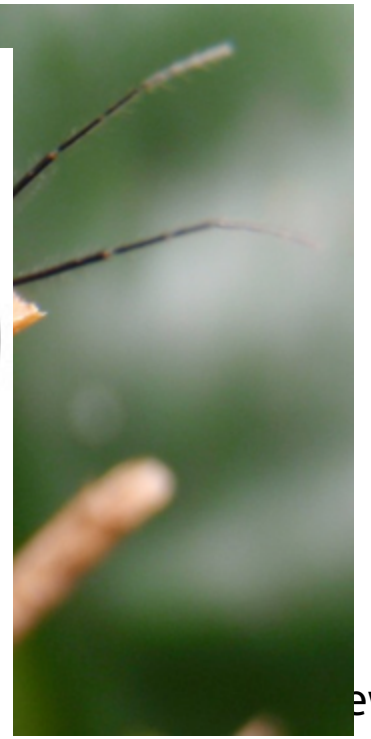


SECURITY IS AWARE OF PROBLEMS

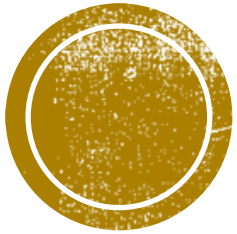
Probably more than 1 problem

Get

Penetration testing solutions



ews



FOUND THEM. NOW FIX THEM!

Developers vs. Security

WHERE IS THAT PROBLEM?

Fix it!

Security group

Developers

HOW DO YOU GET THEM FIXED?

Install a process

How do you incentify developers to get things fixed.

Process in place?

SECURITY PROBLEMS IN SOFTWARE

Great, get me a stool

84%

Of breaches occur at the application layer

(Source: HP Research)

et
?

0

WHO'S HELPING THE DEVELOPER OUT?

Lonely person…

Finding problems (security)

FORTIFY
An HP Company

klocwork

AppScan
IBM. Rational.

VERACODE

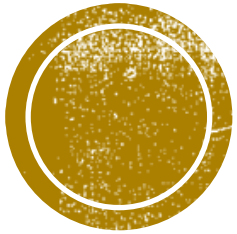
Bug Tracking Systems

Bugzilla

JIRA

Sensei Security

ThreadFix



NOW STOP MAKING NEW PROBLEMS, PLEASE.

Approaches

STOP CREATING NEW PROBLEMS

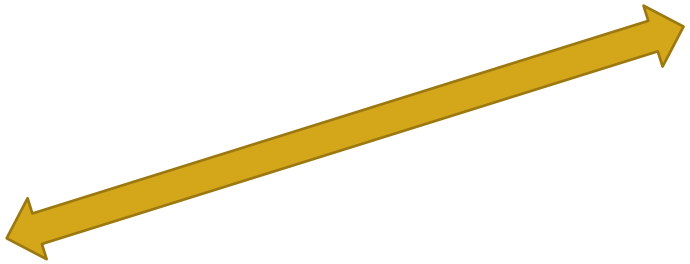
Developers keep on introducing problems.

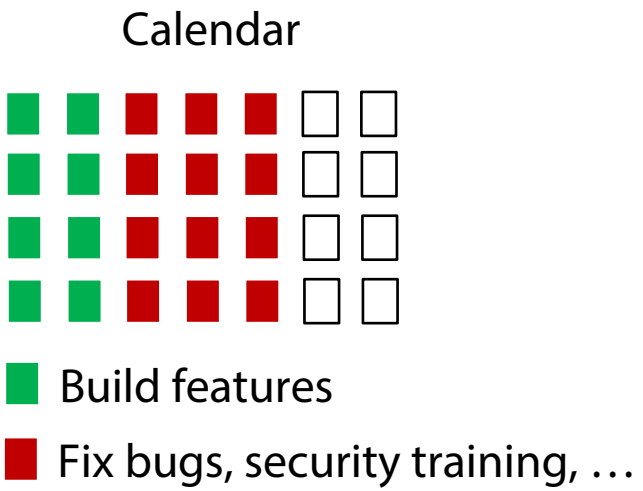
How do they not introduce more problems?

- There are 700 different categories of problems developers can make!
- Detection happens fairly late.

DEVELOPERS: FEATURES

Developers are paid to to develop features, not to learn about security!



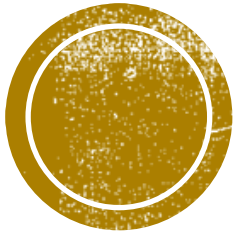


HOW DO WE FIX UNKNOWN ISSUES

How can we fix what we do not see?

When fixing all the known problems, is your code secure?

Fixing is not robust and consistent programming



ANY OTHER SOLUTIONS TO THIS PROBLEM?

REMEMBER...

Lonely developer, no help

Finding problems (security)

Bug Tracking Systems

Developer has to fix

FORTIFY
An HP Company

klocwork

AppScan
IBM Rational

VERACODE

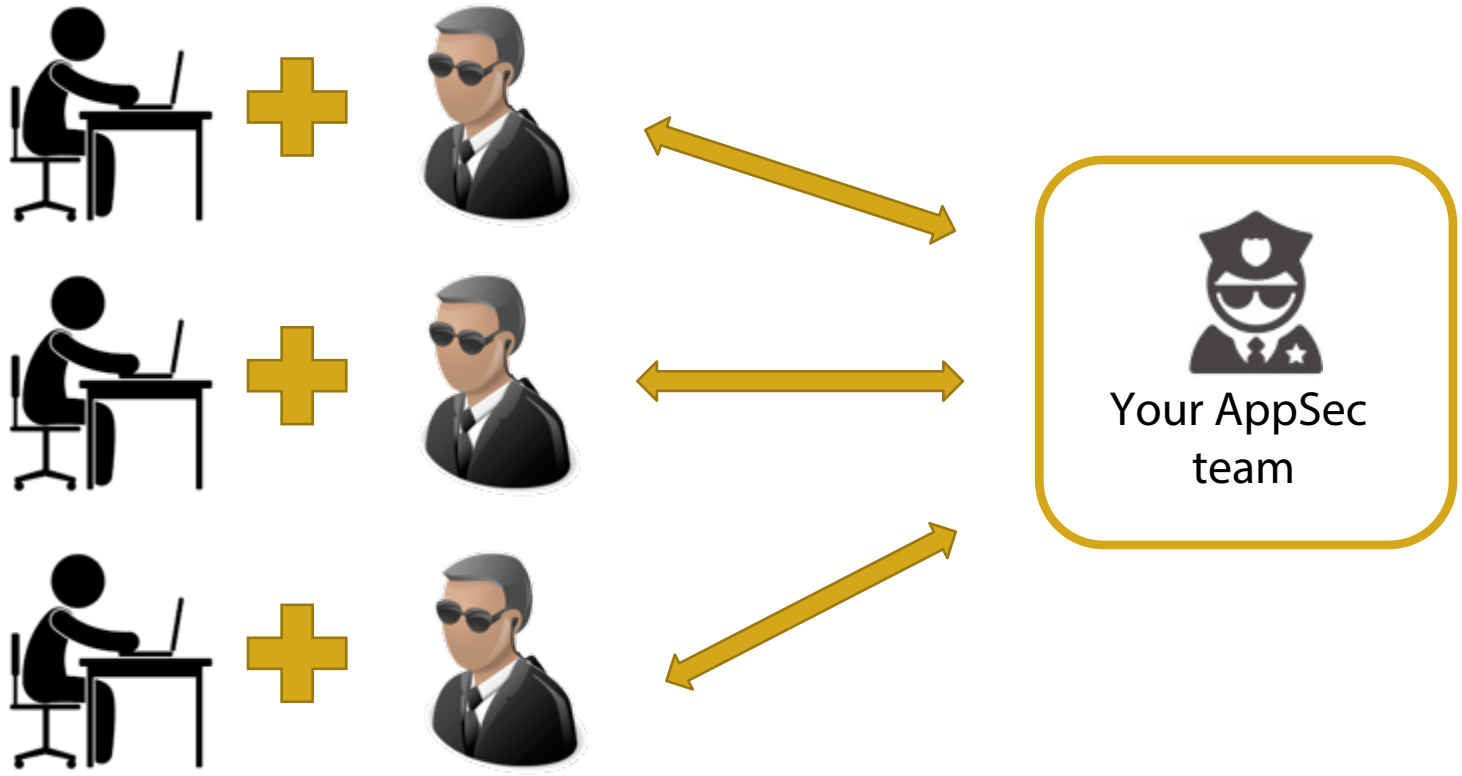
Bugzilla

JIRA

ThreadFix

HELP THE DEVELOPER

A software security person next to every developer?



FIND SECURITY PEOPLE

Talent shortage in security

Ponem INSTI

FROS & SULLIV

BSI

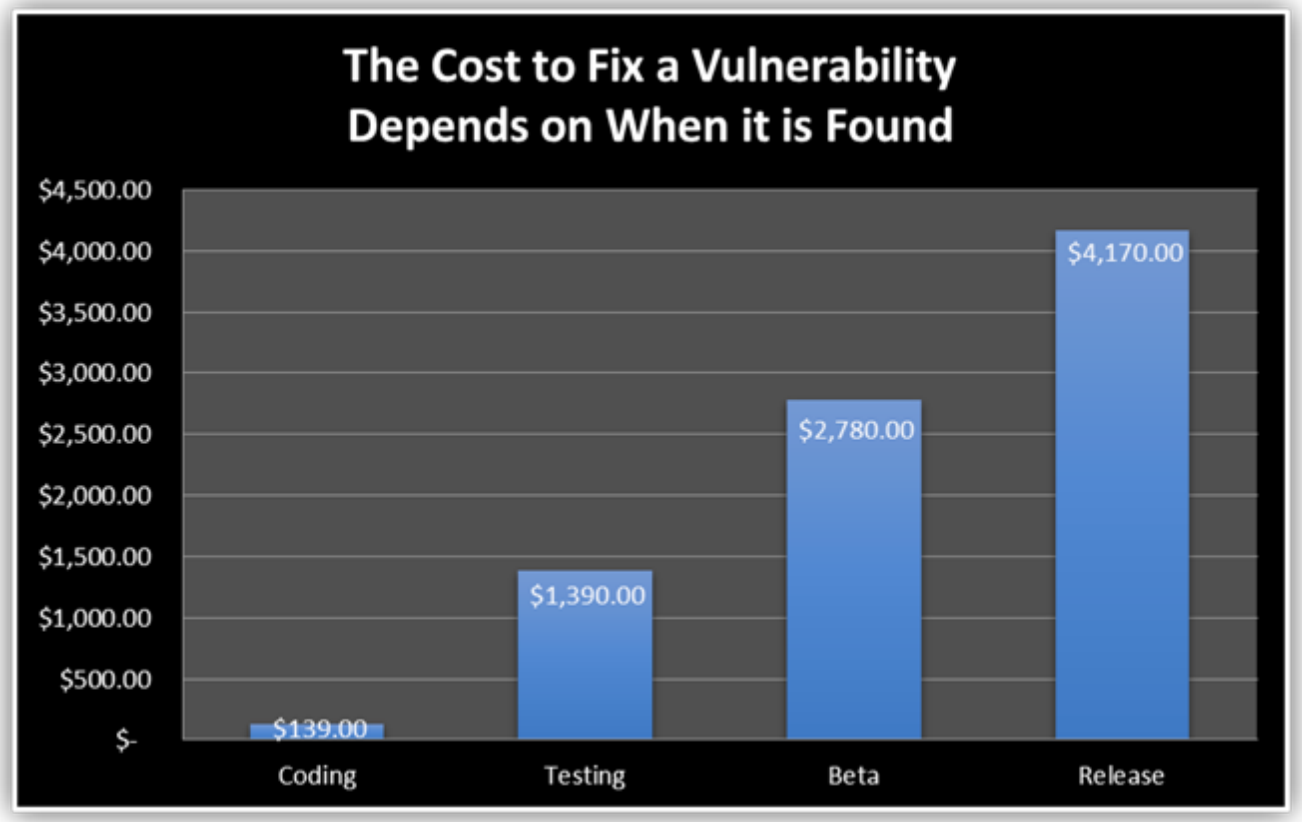
ant in 2014

in 2020 in IT Security

members/100 developers.

BENEFITS FINDING PROBLEMS EARLY

Cost to fix vulnerabilities



Research by Aspect Security

COMPLIANCE REASONS, STANDARDS

Moving towards fixing the root cause

PCI DSS requirements

NIST Special Publication 800-53

ISO/IEC 27034

ADVANTAGES

Be as close as possible to developers

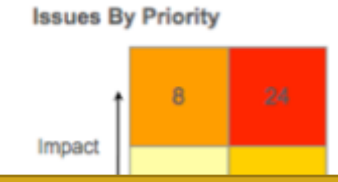
Faster development

Less security bugs

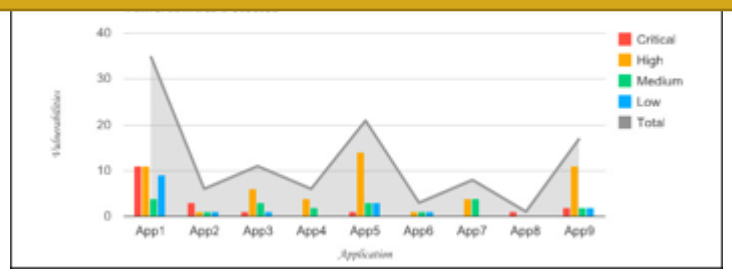
Pro-active and positive

On the job training

MEASURE SOFTWARE SECURITY



How about: How many problems got we fixed?
How many vulnerabilities did our developers avoid?



THANKS!

Matias Madou Ph.D.

@SenseiSecurity

https://www.linkedin.com/company/sensei-security

info@senseisecurity.com

@mmadou

https://www.linkedin.com/in/matiasmadou

mmadou@senseisecurity.com

PEOPLE INTERESTED?

We are looking for you!

SENSEI
security

Benefits:

- Work on cutting edge technology
- Work with cool people
- Want to work when you want (remote, on-site, day, night, whenever, wherever)

Come talk to me
or shoot me an e-mail!
jobs@senseisecurity.com
interns@senseisecurity.com

LOOK FOR FEEDBACK ON OUR PRODUCT

Is your organization serious about application security?

Your organization:

- Want to get software security right in a cost effective way
- Does not want to transform developers into security ninjas (otherwise, keep on training)
- Want to avoid juniors to introduce new problems
- Doesn't matter if you are using point and shoot software security solutions like static analysis solutions, penetration testing, …
- 50 Java developers.

Come talk to me or shoot me an e-mail!
mmadou@senseisecurity.com

QUESTIONS?

Matias Madou Ph.D.

@SenseiSecurity

https://www.linkedin.com/company/sensei-security

info@senseisecurity.com

@mmadou

https://www.linkedin.com/in/matiasmadou

mmadou@senseisecurity.com