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
  - Developer? Is Security annoying?
  - Security? Are developers annoying?
  - Students? Security Courses?

Students, developers, 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)
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

Penetration testing solutions

Getting hacked

Peer code reviews
FOUND THEM.
NOW FIX THEM!
WHERE IS THAT PROBLEM?

Fix it!
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)
WHO’S HELPING THE DEVELOPER OUT?

Lonely person...

Finding problems (security)

Bug Tracking Systems

FORTIFY
An HP Company

klocwork

AppScan
IBM Rational

VERACODE

Sensei Security

Bugzilla

JIRA

ThreadFix
NOW STOP MAKING NEW PROBLEMS, PLEASE.
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 develop features, not to learn about security!

Calendar

- Build features
- Fix bugs, security training, …
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

WANTED
Bug Bounty Program
Patched or Alive
Cash Reward
$50 to $500

Fortify
An HP Company

WHITE HAT  GRAY HAT  BLACK HAT

klocwork

AppScan
IBM Rational

VERACODE

Bugzilla

× JIRA

ThreadFix

Sensei Security
HELP THE DEVELOPER

A software security person next to every developer?

Your AppSec team
Talent shortage in security

40% of IT Security positions vacant in 2014

Private sector shortfall of 1.5 million in 2020 in IT Security

From 1.99 to 1.95 to 1.4 to 1.33 SSG members/100 developers.
BENEFITS FINDING PROBLEMS EARLY

Cost to fix vulnerabilities

Research by Aspect Security
Moving towards fixing the root cause
ADVANTAGES

Be as close as possible to developers

- Faster development
- Less security bugs
- Pro-active and positive
- On the job training
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!

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
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