swisscom

Thanks to Swisscom

www.swisscom.com
@Swisscom_de

S-SDLC – Ready for Clouds?

Robert Schneider

robert.schneider@owasp.org

Robert Schneider

swisscom ICT Security Officer @Swisscom IT Services

robert.schneider@owasp.org

@schattenbaum_ch

www.schattenbaum.ch

www.owasp.ch

Table of Contents

1. Introduction
2. Phases
   - Purpose
   - Possible candidates
   - Pitfalls
3. Wrap up
4. Questions & Open discussion

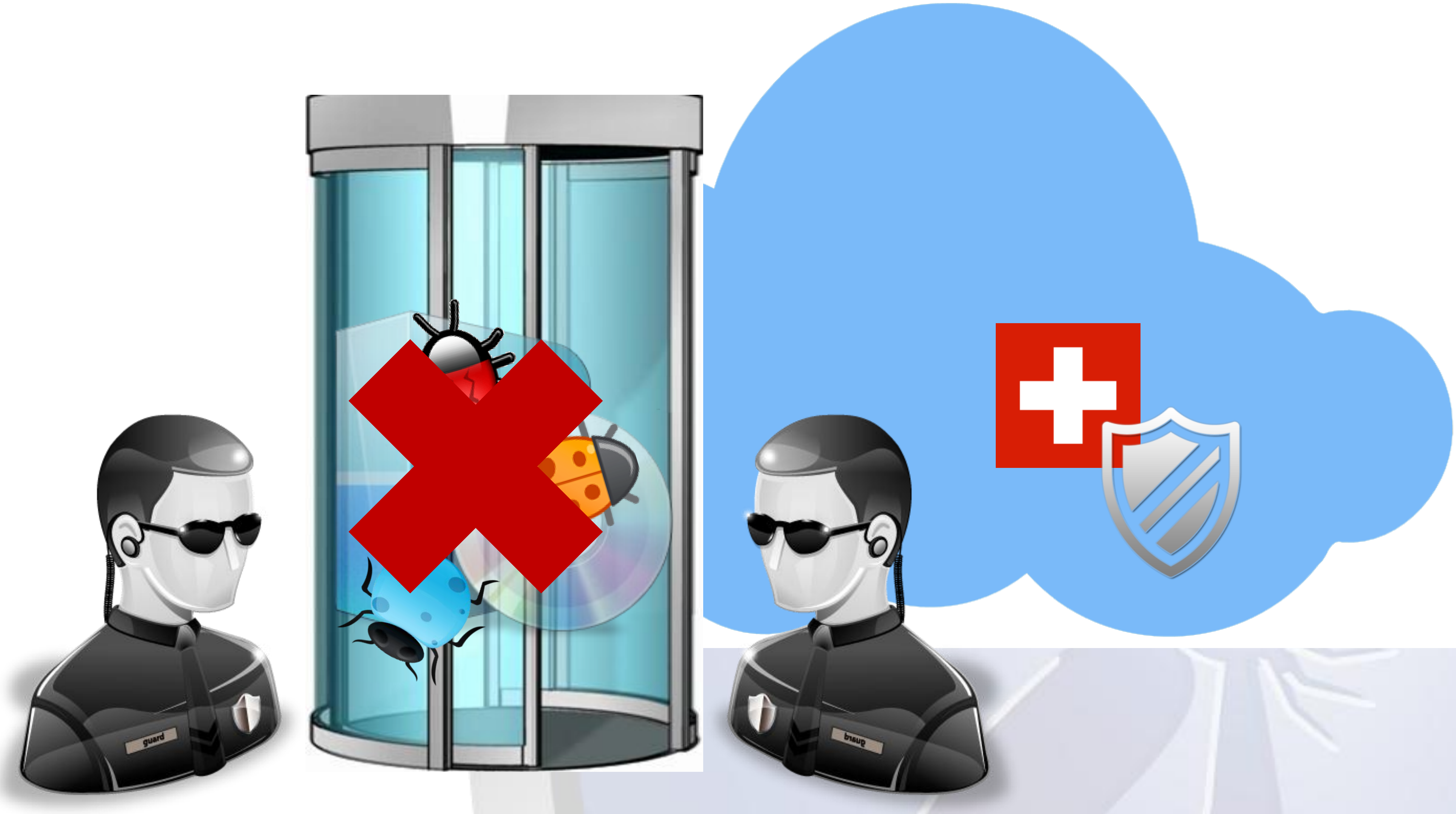
Disclaimer

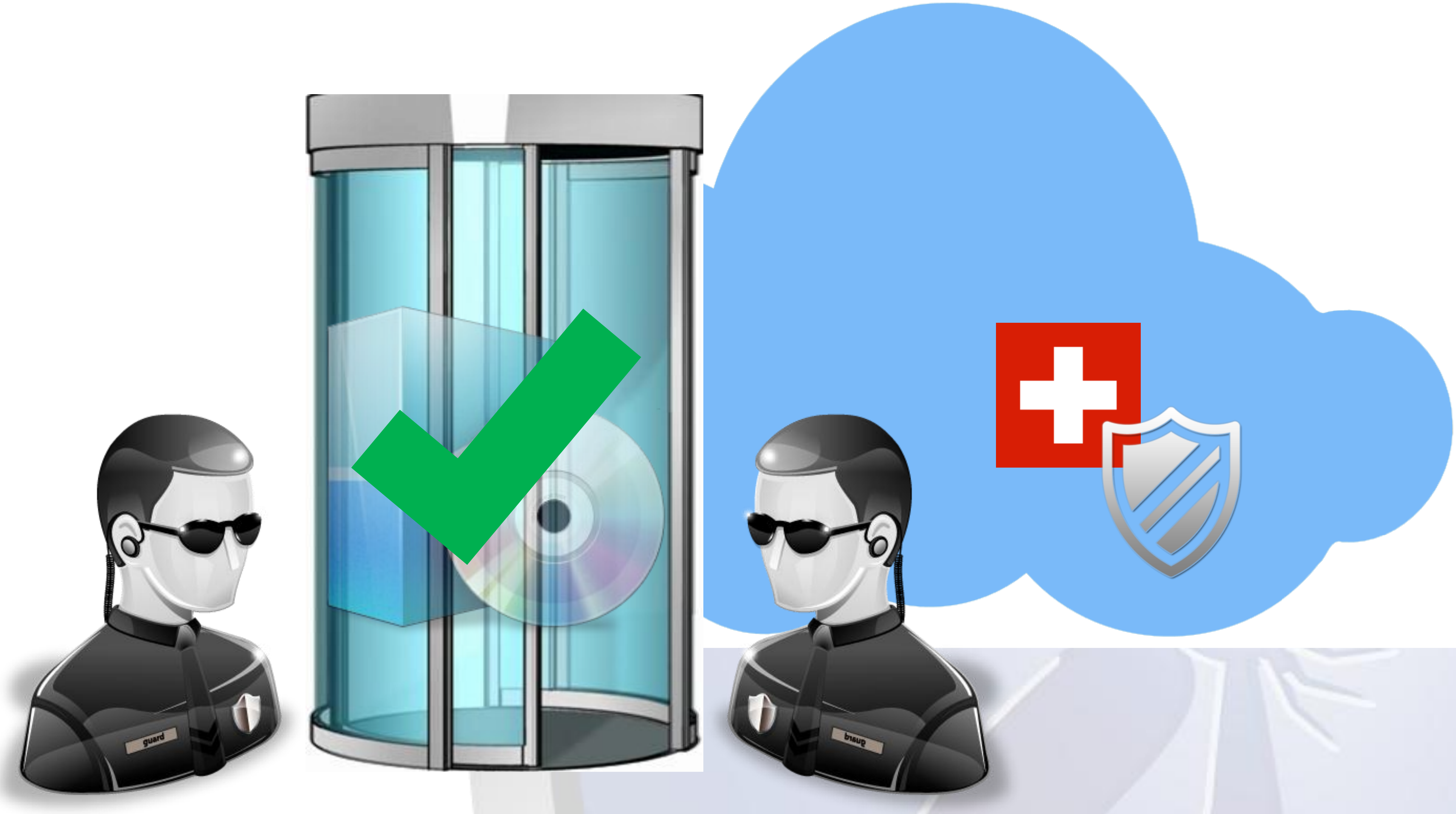
This talk is not going to be about

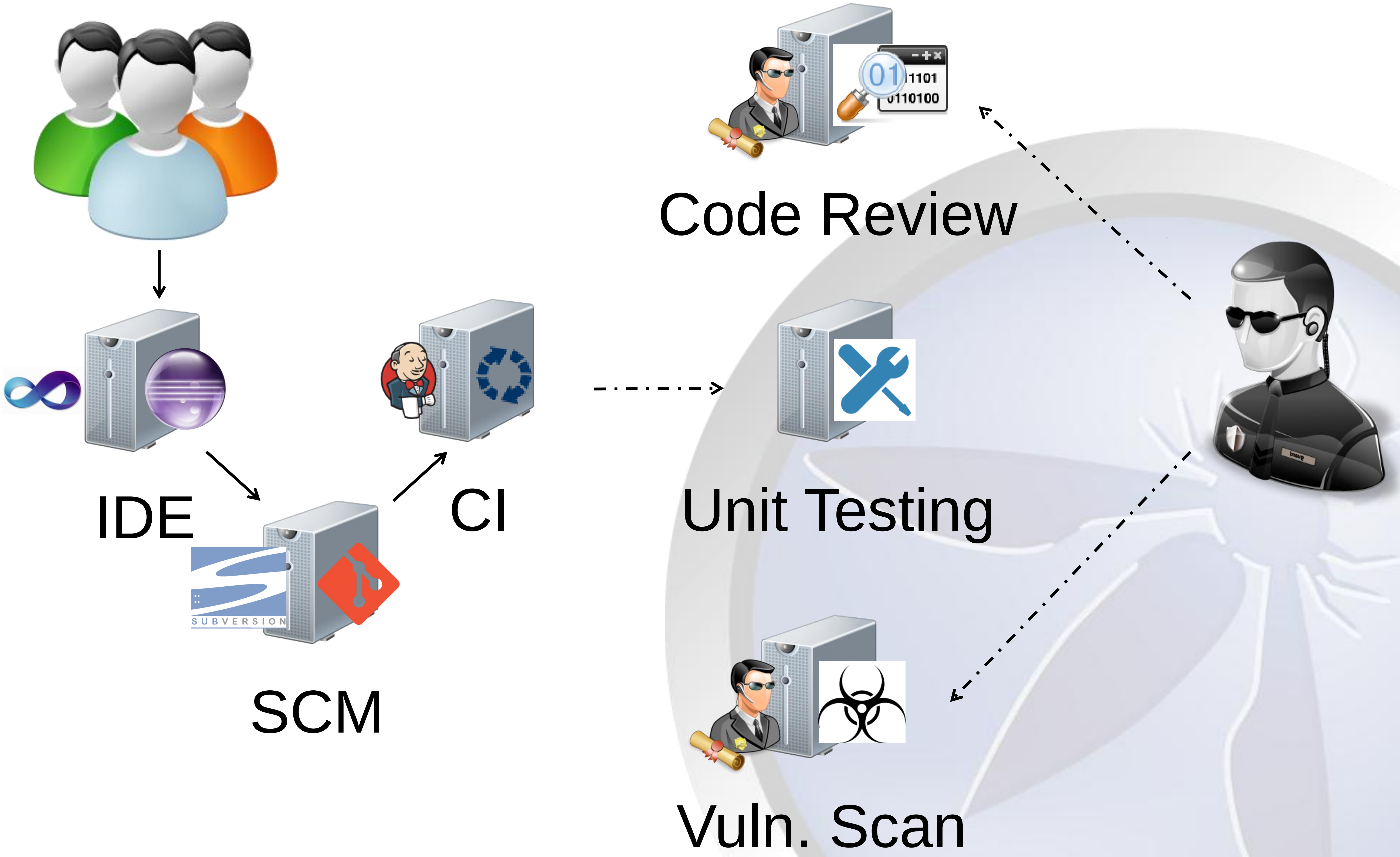
- SDLC basics (Waterfall, Agile SW Development, Sprints, …)
- Checks for malicious behaviour (additional features to assure this)

Introduction

What are we building?


guard


guard
guard



IDE

SCM

CI

Code Review

Unit Testing

Vuln. Scan

Introduction

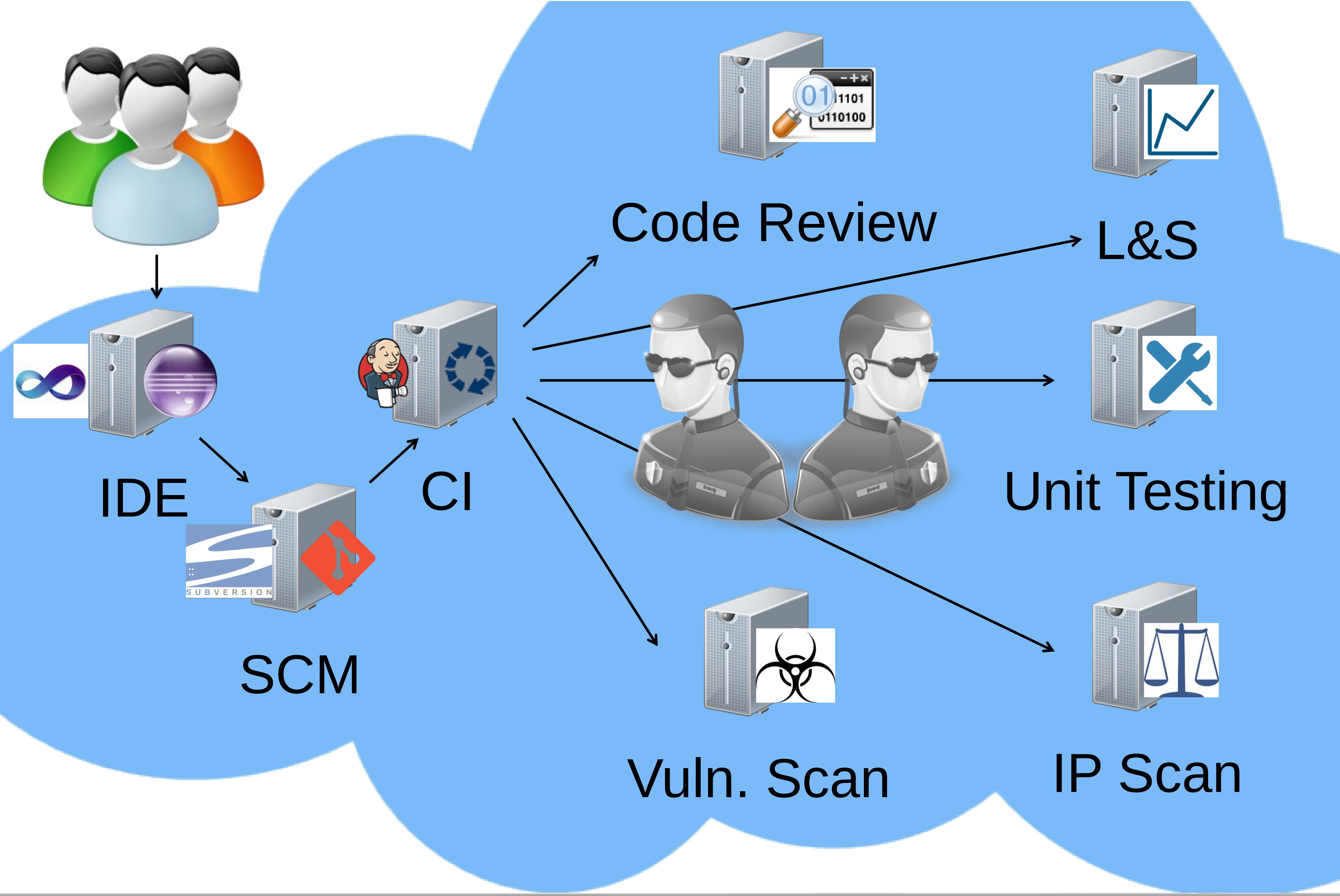
What do we have to keep in mind?

- Wide range of coding language support
- CI: Jenkins / Bamboo / …
- SCM: GIT / SVN /…
- Traceability (Logging)
- Multiuser & -tenant

Introduction

What do we want to achieve?

- As much automation as possible
- Developers are integrated in automated monitoring
- As few additional effort for developers as possible
- Early detection of software flaws



IDE

SCM

CI

Code Review

L&S

Unit Testing

Vuln. Scan

IP Scan

Introduction

This should help us to achieve

- A secure cloud

Phases

1. Intellectual Property Scan
2. Code Review
3. Vulnerability Scanning
4. Stress & Load Testing

INTELLECTUAL PROPERTY SCAN

IP Scan

Who is using Open Source Software (OSS)?

IP Scan

What OSS components do you use?

In which version?

IP Scan

Are you sure that you know them all?

Even snippets?

IP Scan

Has Security approved the use of them?

Legal as well?

IP Scan

Are you allowed to contribute your work?

If yes:

- What are you allowed to contribute back to the community?
- How are you allowed to do that?

IP Scan

Is one of the used components vulnerable to a CVE?

cve.mitre.org

Possible candidates

- Palamida
- Open Logic
- Black Duck

Ohloh

WWW.OHLOH.NET

Pitfalls

- Processes of different operation units do not merge as easy as you would like them to.
- You may need additional employees.
- Do you allow the tool to connect to the internet and transmit data?
- What do you do after you know your problems?

CODE REVIEW

Code Review

- Detect software flaws as early as possible
- Even some bad coding practices

Code Review

Long-term benefits

- Developers get to know what actually to look for and
- Know how to prevent these flaws from the beginning

Code Review

Time & budget saving

Possible candidates

- Sonatype
- HP Fortify
- Defensecode ThunderScan
- Checkmarx

See also www.owasp.org

Pitfalls

- Training needed
- False Positives & Negatives
- Developers do not see the tool as an improvement
- Management does not see the long-term benefits

WHAT ABOUT BINARIES?

Binaries?

Veracode

- Big players are using it
- Placed in the USA
- Your data does not stay at “home”

VERACODE

VULNERABILITY SCANNING

Vulnerability Scanning

Is the ready-to-deploy application still vulnerable?

Vulnerability Scanning

This phase is comparable to an automated Penetration test.

Vulnerability Scanning

Pre-deployment

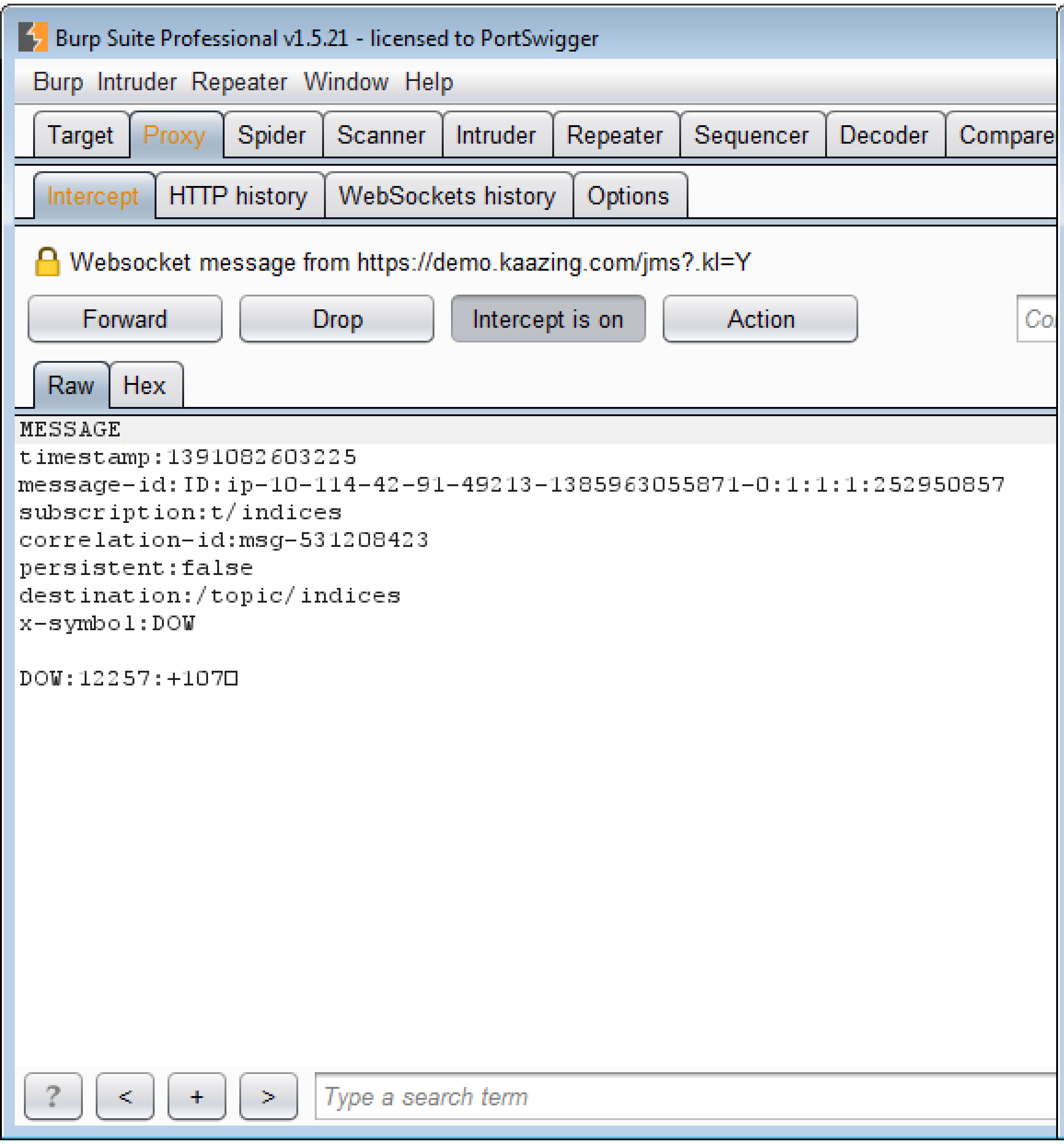
- Again checking for OWASP Top 10 and
- Even the flaws we have not been able to test for during phase 2

Possible candidates

- WhiteHat Security Sentinel
- Quotium Seeker
- HP WebInspect
- Defensecode Web Security Scanner
- Cenzic Hailstorm
- Burp Suite Pro
- Acunetix

WebSockets

Burp Suite Pro (v1.5.21)

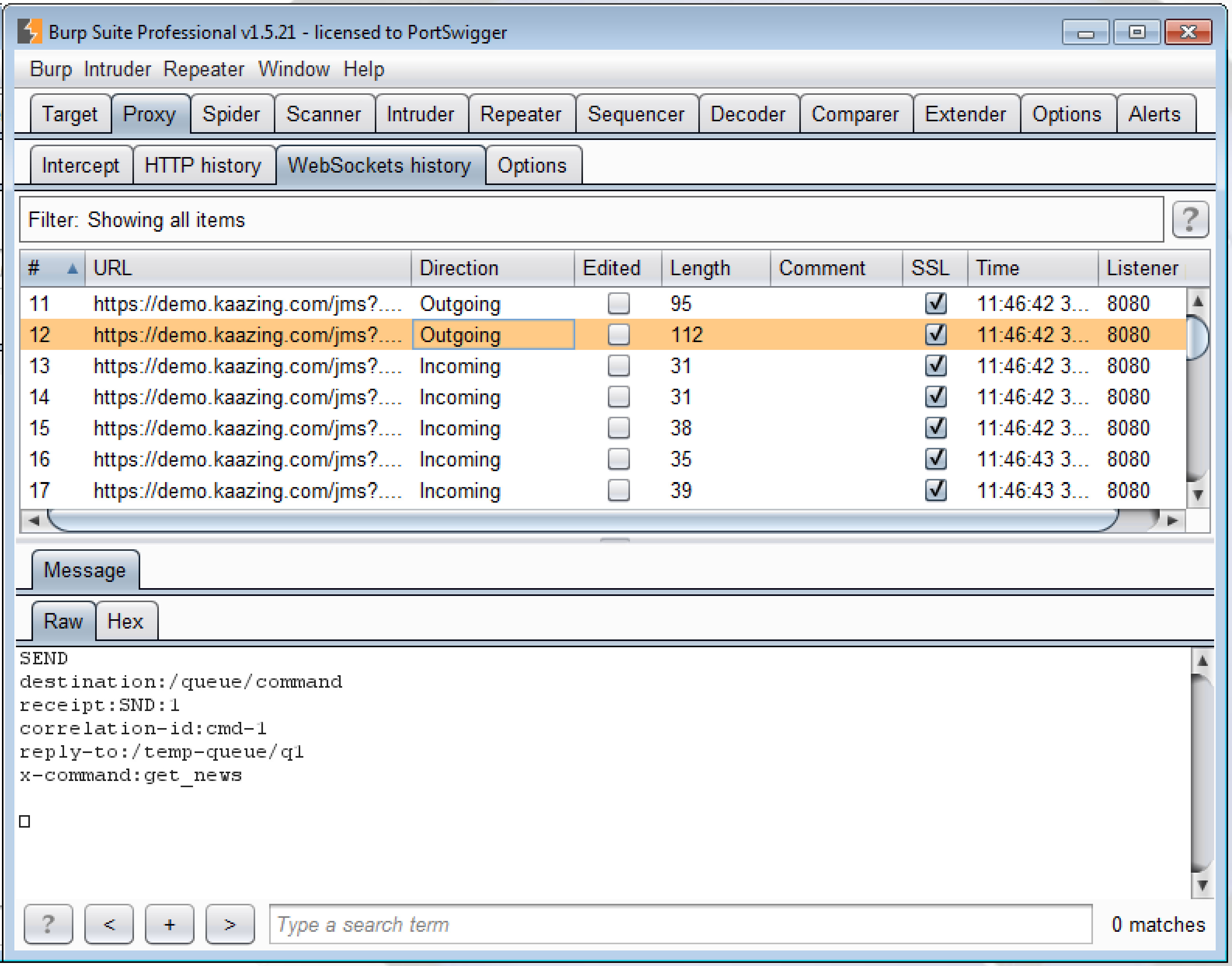


Burp Suite Professional v1.5.21 - licensed to PortSwigger
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compare
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Co
Raw Hex
?
<
+
>
Type a search term

Websocket message from https://demo.kaazing.com/jms?.kl=Y

```
MESSAGE
timestamp:1391082603225
message-id:ID:ip-10-114-42-91-49213-1385963055871-0:1:1:1:252950857
subscription:t/indices
correlation-id:msg-531208423
persistent:false
destination:/topic/indices
x-symbol:DOW

DOW:12257:+107□
```



Burp Suite Professional v1.5.21 - licensed to PortSwigger
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
?
Message
Raw Hex
?
<
+
>
Type a search term
0 matches

Filter: Showing all items

# ▲	URL	Direction	Edited	Length	Comment	SSL	Time	Listener
11	https://demo.kaazing.com/jms?....	Outgoing	□	95		☑	11:46:42 3...	8080
12	https://demo.kaazing.com/jms?....	Outgoing	□	112		☑	11:46:42 3...	8080
13	https://demo.kaazing.com/jms?....	Incoming	□	31		☑	11:46:42 3...	8080
14	https://demo.kaazing.com/jms?....	Incoming	□	31		☑	11:46:42 3...	8080
15	https://demo.kaazing.com/jms?....	Incoming	□	38		☑	11:46:42 3...	8080
16	https://demo.kaazing.com/jms?....	Incoming	□	35		☑	11:46:43 3...	8080
17	https://demo.kaazing.com/jms?....	Incoming	□	39		☑	11:46:43 3...	8080

```
SEND
destination:/queue/command
receipt:SND:1
correlation-id:cmd-1
reply-to:/temp-queue/q1
x-command:get_news

□
```

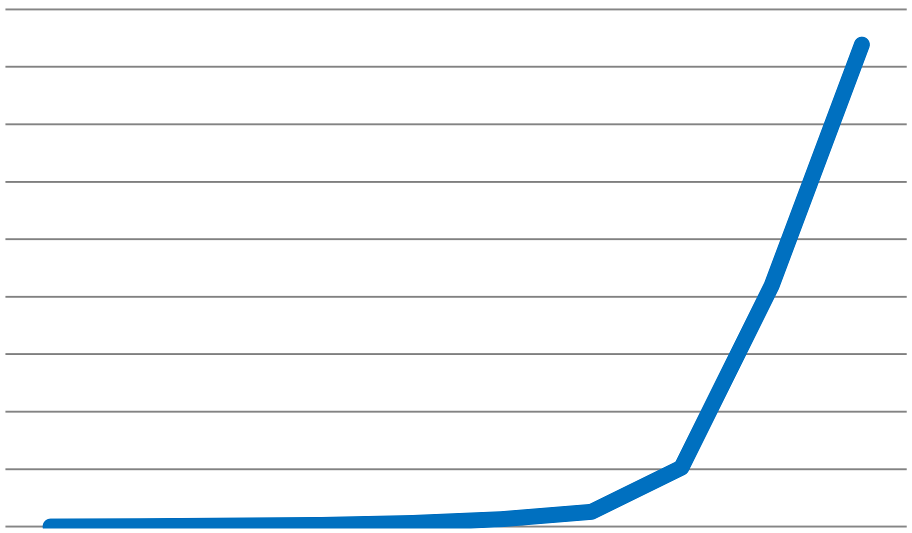
Pitfalls

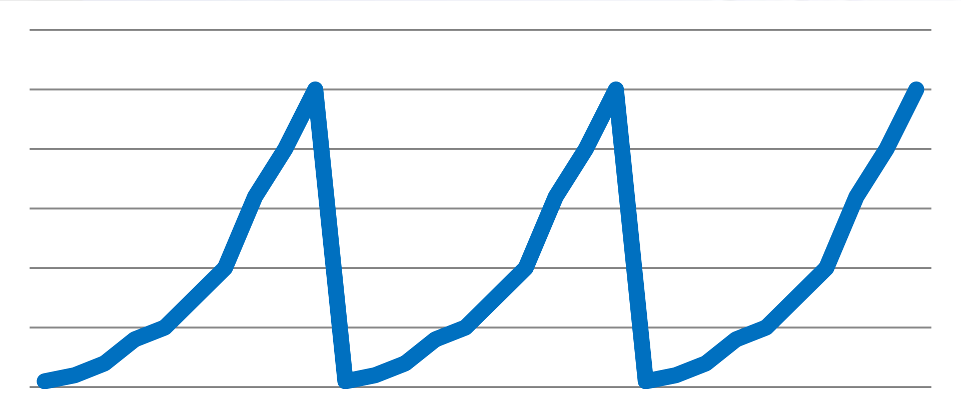
- Training needed
- False Positives & Negatives
- “Automated” deployment of applications needed (Sandbox?)
- Fixing times

STRESS & LOAD TESTING

S & L Testing

How does it scale?





- Will the software "ruin" us when we start using it in the cloud?

Possible candidates

- Proxy Sniffer
- OpenSTA
- Loadrunner
- JMeter

Pitfalls

- Automation probably impossible due to the need of user scripts.
- You may miss an important use case and therefore get an inaccurate feedback.
- Testing environment
- Testing data

WRAP UP

Wrap up

- To be ready for clouds you do not need something completely new according to the S-SDLC.
- However, you have to be aware that your software may not get accepted on every cloud as easy as you might think.

Wrap up

- In a first step, try to find the one phase that improves your S-SDLC the most.

1. Intellectual Property Scan
2. Code Review
3. Vulnerability Scanning
4. Stress & Load Testing

Wrap up

Intellectual Property Scan Benefits

- Know what OSS you are using and
- Know their Licenses

Wrap up

Code Review Benefits

- Detect software flaws as early as possible
- Even some bad coding practices

Wrap up

Vulnerability Scanning Benefits

- Know if the ready-to-deploy application is still vulnerable

Wrap up

Stress & Load Testing Benefits

- Know how the application scales

Recommendation

Dev. & Sec. → Code Review

Legal → IP Scan

Security → Vulnerability Scanning

Operation → Stress & Load Testing

Wrap up

- Try to help and not to annoy by adapting the S-SDLC.
- **You need feedback for improvements!**

QUESTIONS & OPEN DISCUSSION

Keep up to date!

JOIN THE LIST

FOLLOW US ON twitter

Join us on Facebook

Want to support OWASP?

Become member, annual donation of:

- $50 Individual
- $5000 Corporate

enables the support of OWASP projects, mailing lists, conferences, podcasts, grants and global strategic focus