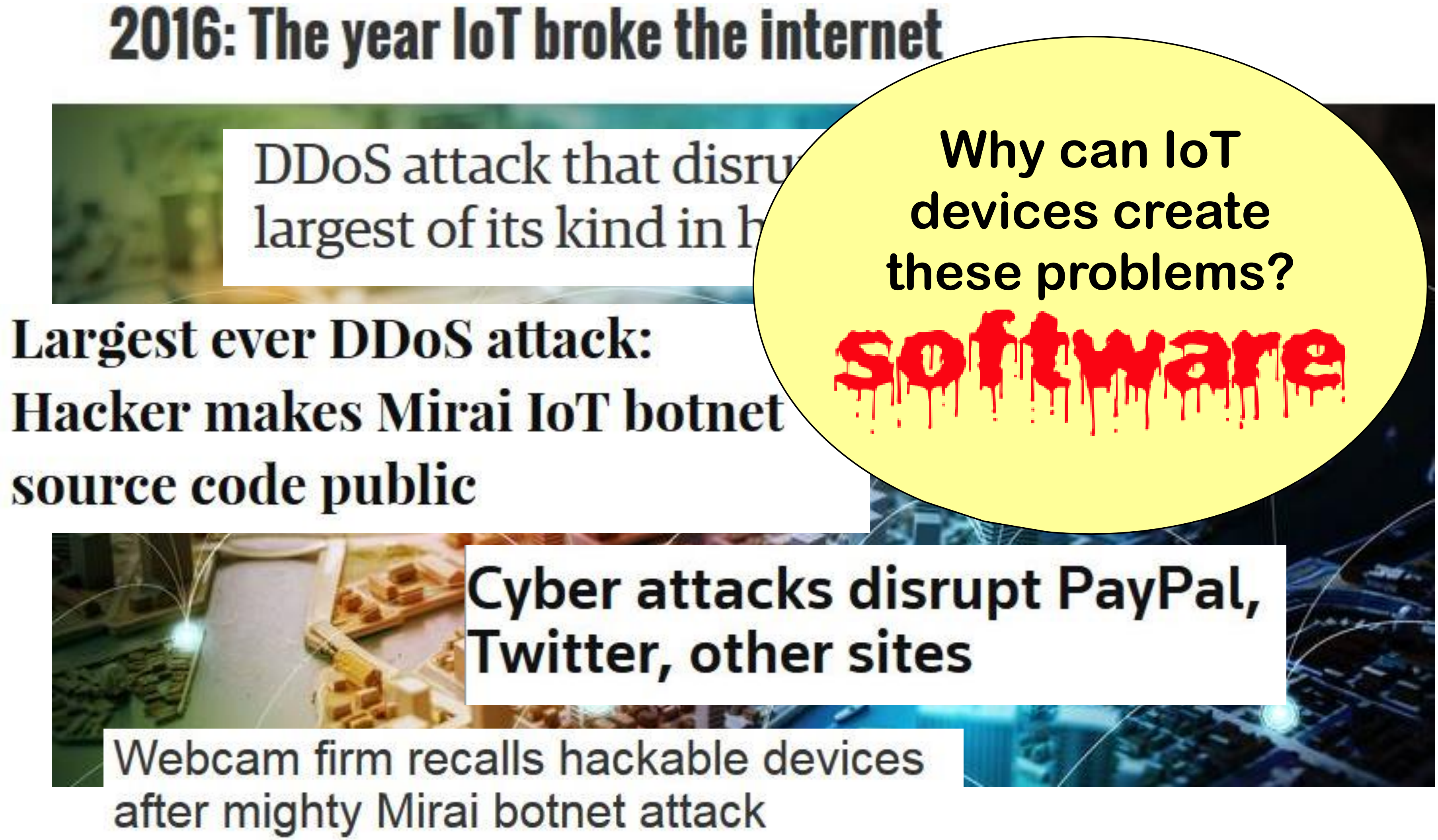
Security in the Software Development Lifecycle

Erik Poll

Digital Security group

Radboud University Nijmegen

Depressing security news…



2016: The year IoT broke the internet

DDoS attack that disru
largest of its kind in h

Largest ever DDoS attack:
Hacker makes Mirai IoT botnet
source code public

Cyber attacks disrupt PayPal,
Twitter, other sites

Webcam firm recalls hackable devices
after mighty Mirai botnet attack

Why can IoT
devices create
these problems?

software

software is no. 1 root cause of trouble

Devices be hacked because they contain software

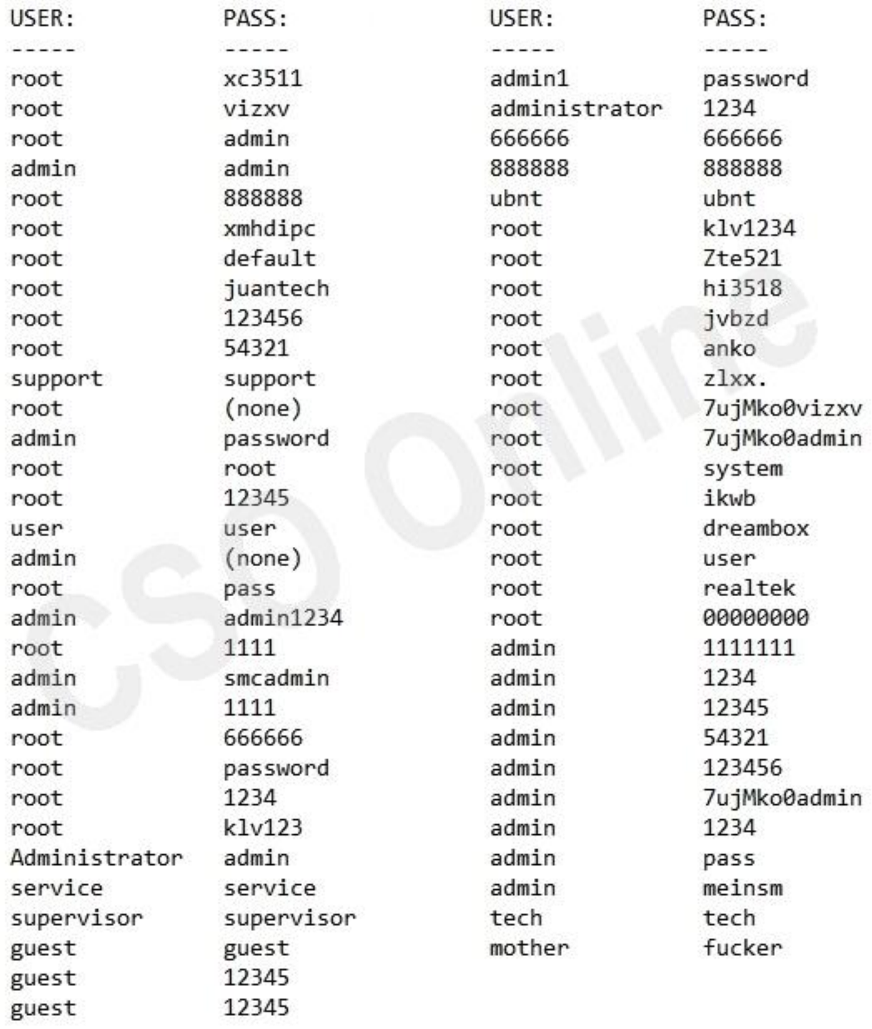
Making devices *programmable* is the start of all trouble:

- insecure software allows IoT devices to be 'hacked'
- malware then allows these devices to start DoS-ing
- software allows the attack to be *automated* & *scaled*

As is often the case, the damage is an externality,
ie. the polluter does *not* pay…

- here the polluters are devices manufacturers & owners

The bad news: the usual mistakes again ☹

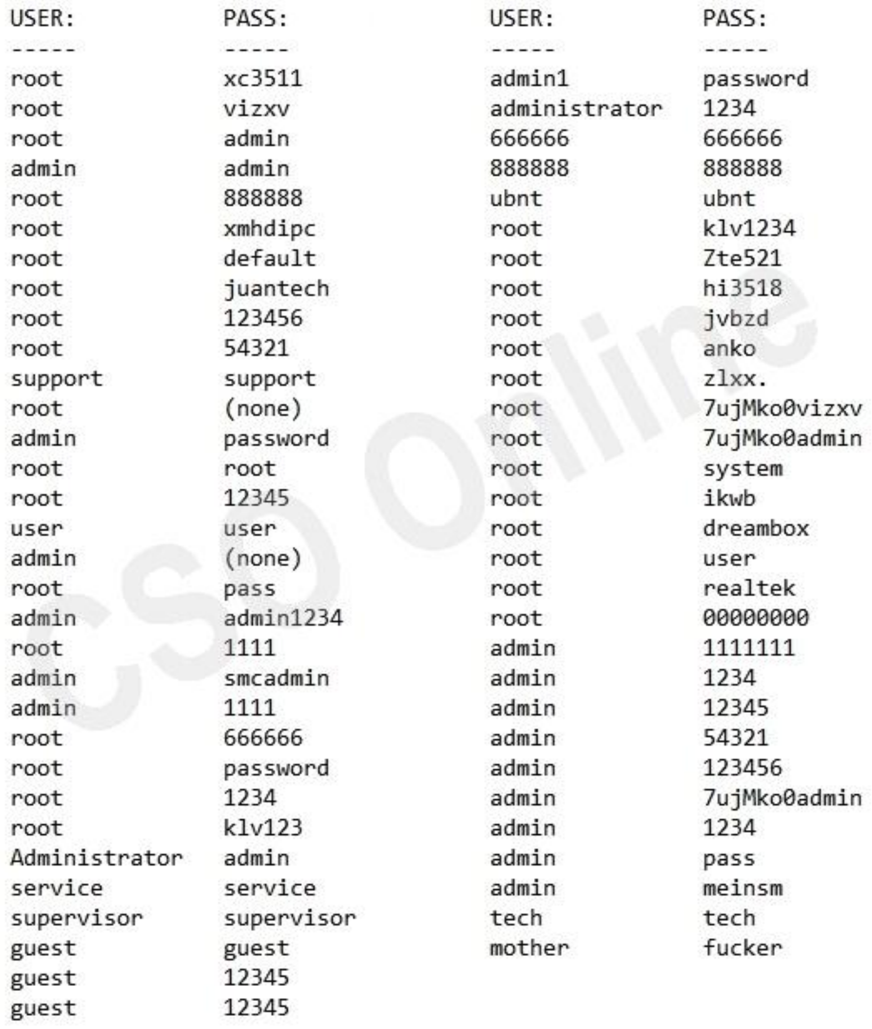


USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

The defaults passwords exploited by Mirai

The good news?

The good news: the usual mistakes again ☺



```
USER:          PASS:               USER:          PASS:
-----          -----               -----          -----
root           xc3511              admin1         password
root           vizxv               administrator  1234
root           admin               666666         666666
admin          admin               888888         888888
root           888888              ubnt           ubnt
root           xmhdipc             root           klv1234
root           default             root           Zte521
root           juantech            root           hi3518
root           123456              root           jvbzd
root           54321               root           anko
support        support             root           zlxx.
root           (none)              root           7ujMko0vizxv
admin          password            root           7ujMko0admin
root           root                root           system
root           12345               root           ikwb
user           user                root           dreambox
admin          (none)              root           user
root           pass                root           realtek
admin          admin1234           root           00000000
root           1111                admin          1111111
admin          smcadmin            admin          1234
admin          1111                admin          12345
root           666666              admin          54321
root           password            admin          123456
root           1234                admin          7ujMko0admin
root           klv123              admin          1234
Administrator  admin               admin          pass
service        service             admin          meinsm
supervisor     supervisor          tech           tech
guest          guest               mother         fucker
guest          12345
guest          12345
```

The defaults passwords exploited by Mirai

The *bad* news

people keep making the same mistakes

The *good* news

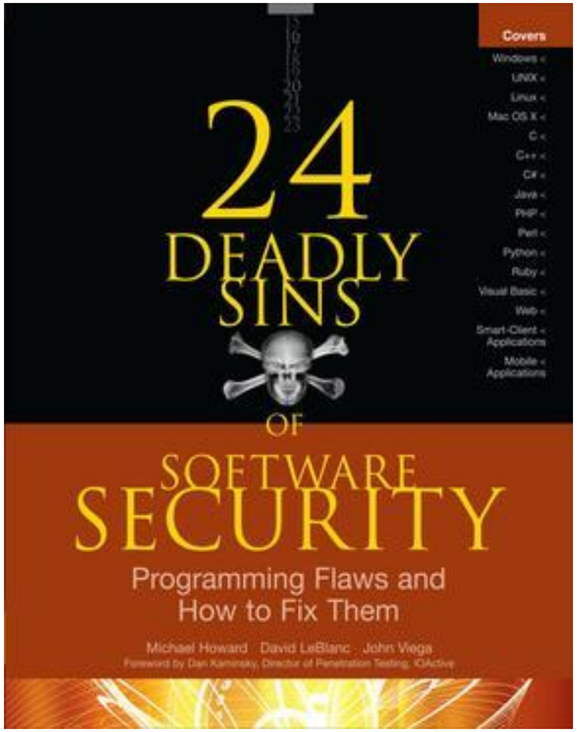
people keep making the same mistakes

...... so we can do something about it!

“Elk voordeel hep z'n nadeel” [Johan Cruijff]

Standard flaws, and ways to prevent them

OWASP
The Open Web Application Security Project
OWASP Top 10 - 2013
The Ten Most Critical Web Application Security Risks
release
Creative Commons (CC) Attribution Share-Alike
Free version at https://www.owasp.org

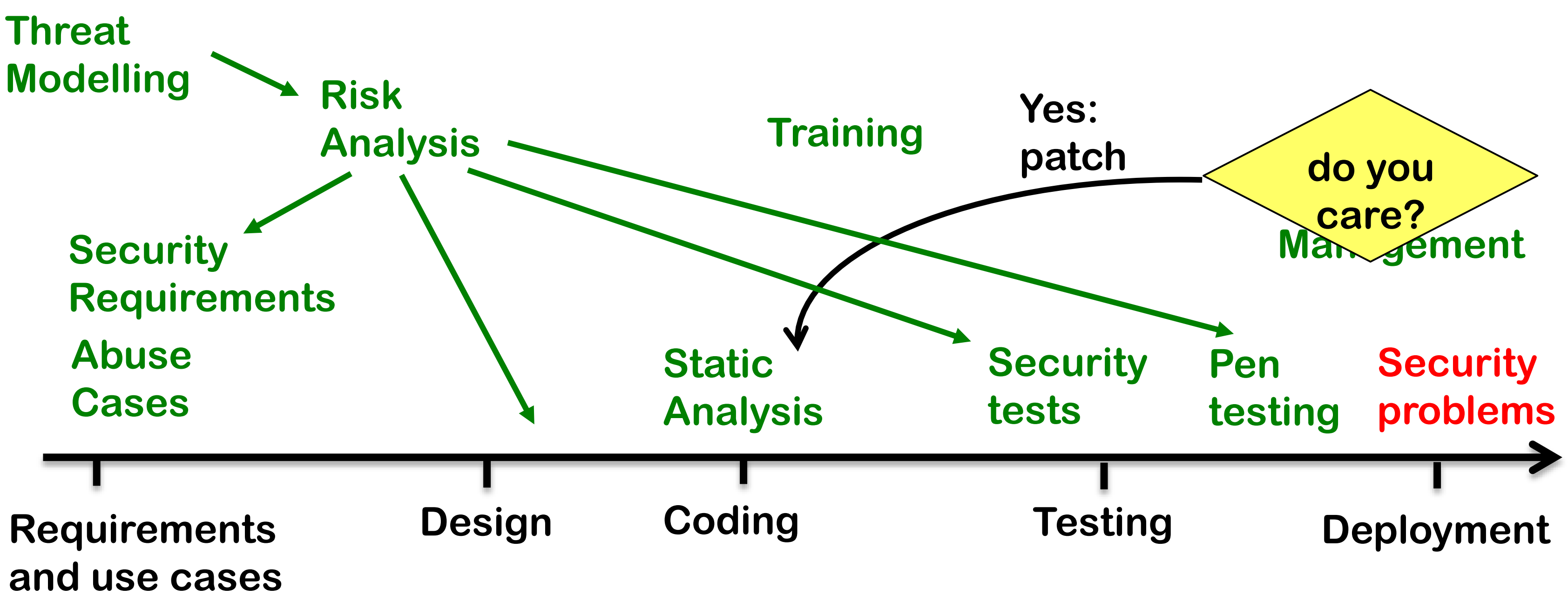


Security in Software Development Lifecycle

Security by Design

Privacy by Design

Evolution of Security Measures



Software Development Life Cycle

OpenSAMM best security practices

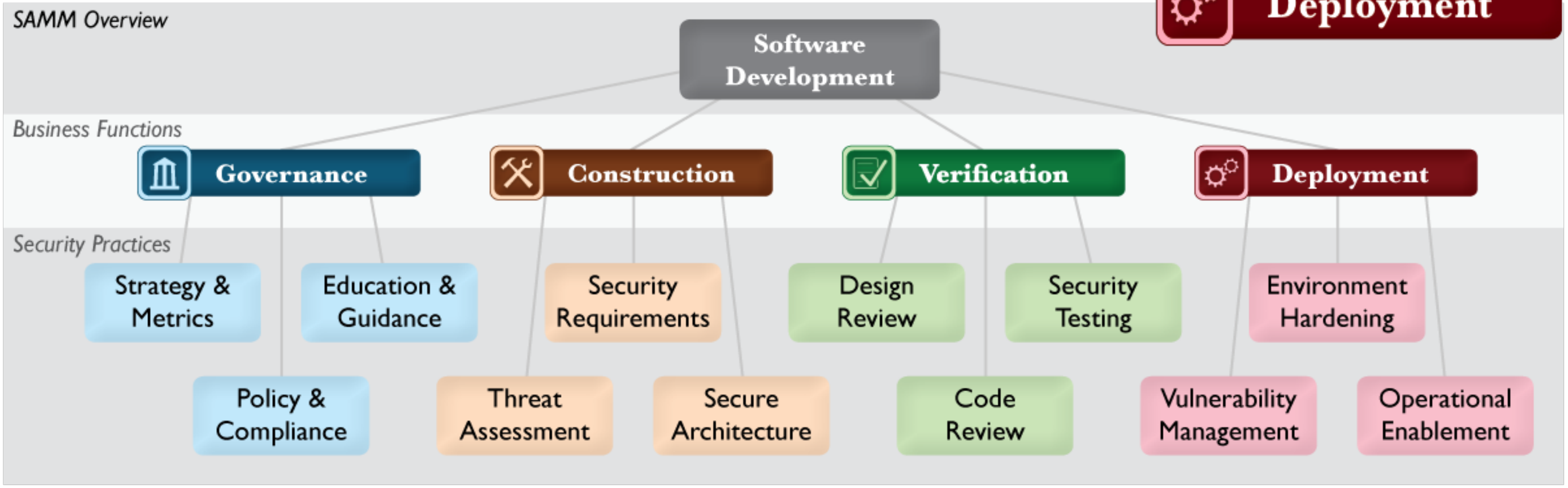
OpenSAMM

Governance

Construction

Verification

Deployment



SAMM Overview

Software Development

Business Functions

Governance — Construction — Verification — Deployment

Security Practices

Governance: Strategy & Metrics, Education & Guidance, Policy & Compliance

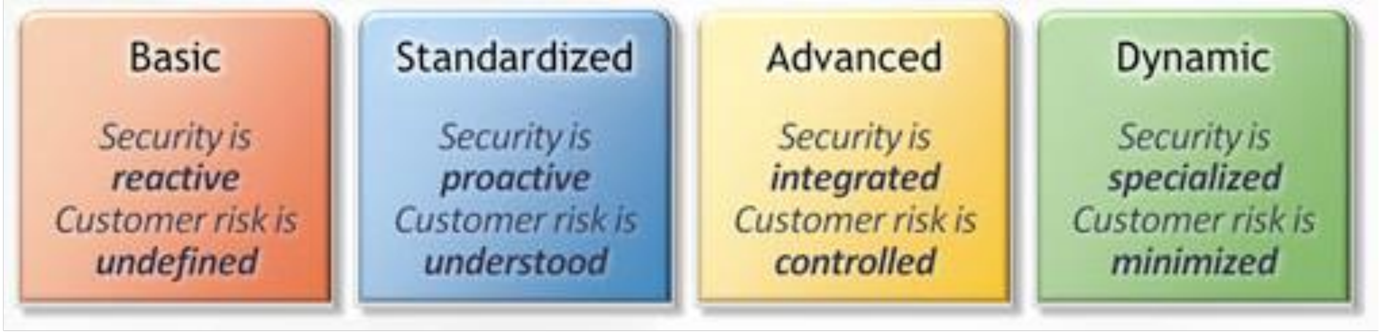
Construction: Security Requirements, Threat Assessment, Secure Architecture

Verification: Design Review, Security Testing, Code Review

Deployment: Environment Hardening, Vulnerability Management, Operational Enablement

Microsoft's SDL (Security Development Lifecycle)

4 maturity levels



Basic

Security is *reactive*
Customer risk is *undefined*

Standardized

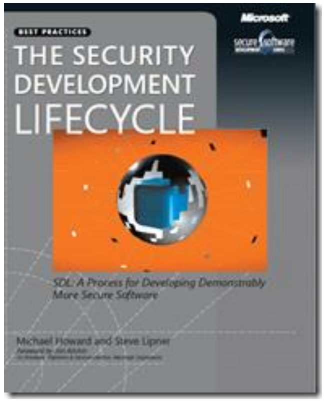
Security is *proactive*
Customer risk is *understood*

Advanced

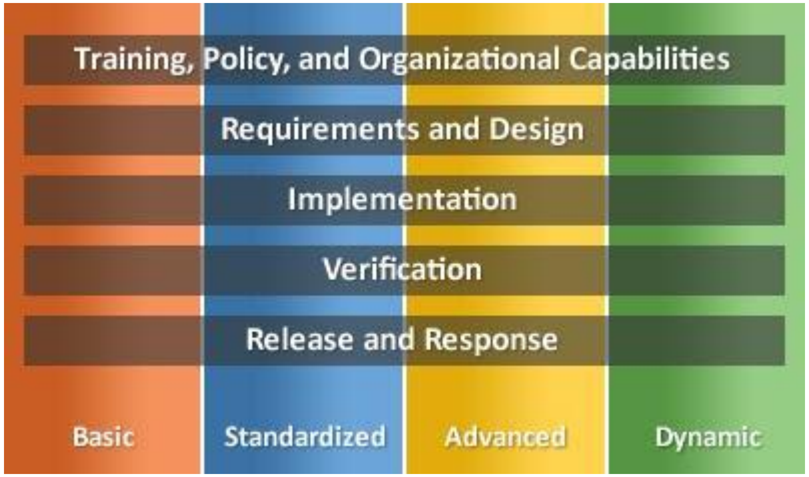
Security is *integrated*
Customer risk is *controlled*

Dynamic

Security is *specialized*
Customer risk is *minimized*


BEST PRACTICES
Microsoft
secure software
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner

5 capability areas



Training, Policy, and Organizational Capabilities

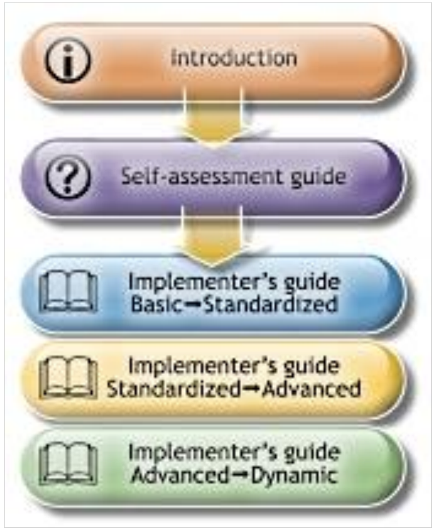
Requirements and Design

Implementation

Verification

Release and Response

Basic | Standardized | Advanced | Dynamic



Introduction

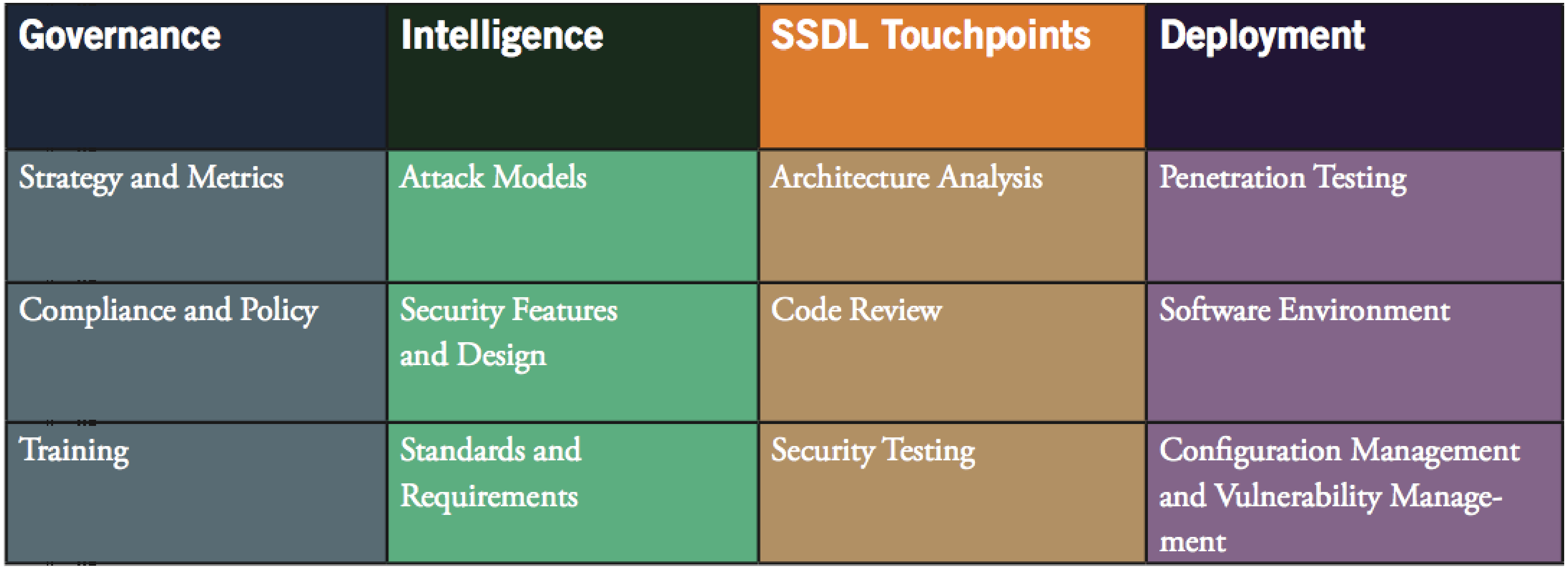
Self-assessment guide

Implementer's guide Basic→Standardized

Implementer's guide Standardized→Advanced

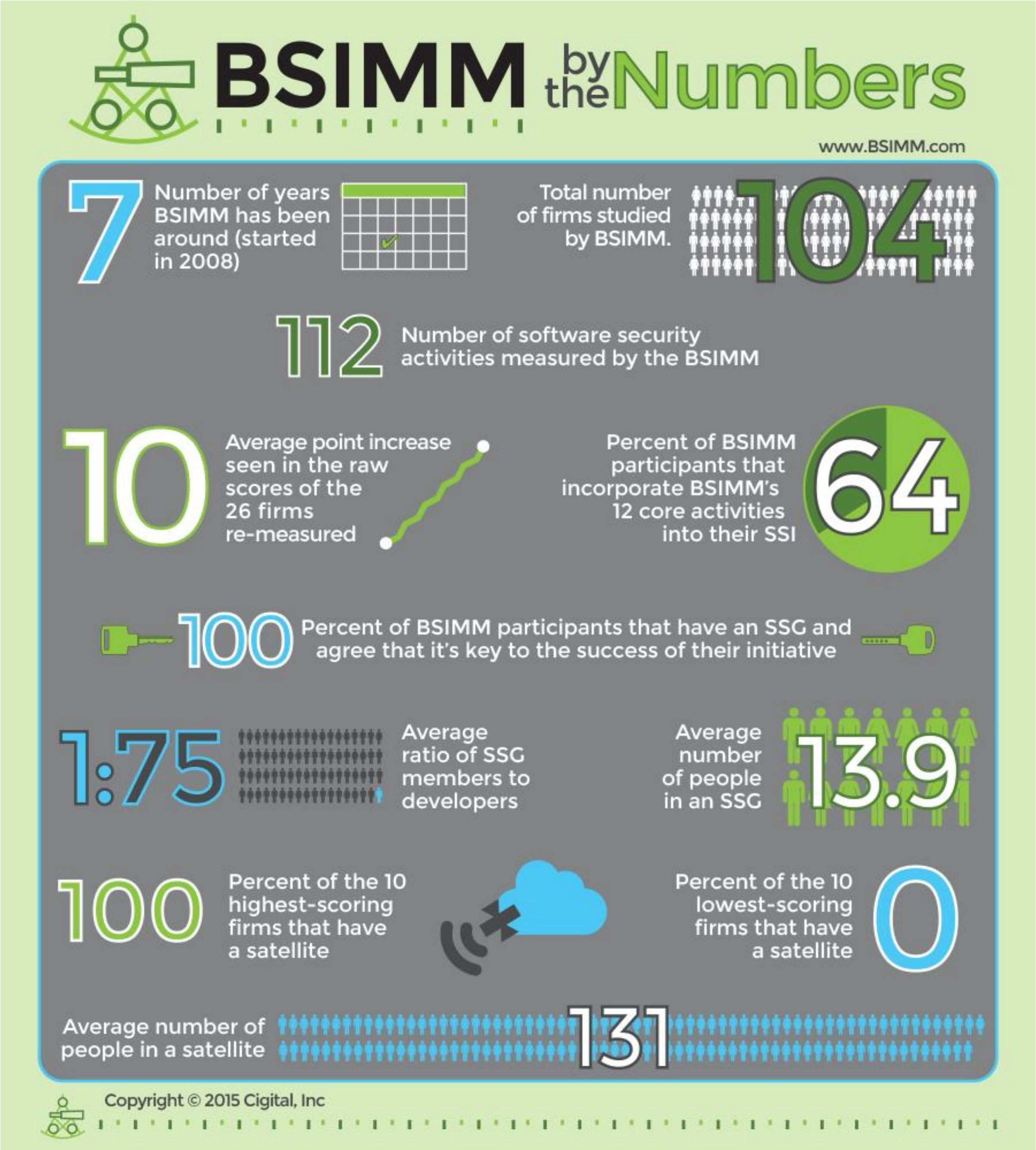
Implementer's guide Advanced→Dynamic

BSIMM (Building Security In Maturity Model)



Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

Not *pre*scriptive, but *de*scriptive, based on data on software security practices in various companies



BSIMM by the Numbers

www.BSIMM.com

7 Number of years BSIMM has been around (started in 2008)

Total number of firms studied by BSIMM. **104**

112 Number of software security activities measured by the BSIMM

10 Average point increase seen in the raw scores of the 26 firms re-measured

Percent of BSIMM participants that incorporate BSIMM's 12 core activities into their SSI **64**

100 Percent of BSIMM participants that have an SSG and agree that it's key to the success of their initiative

1:75 Average ratio of SSG members to developers

Average number of people in an SSG **13.9**

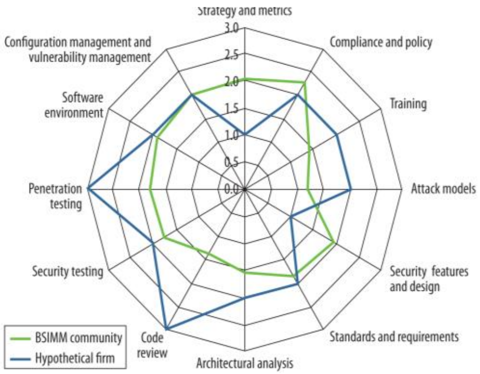
100 Percent of the 10 highest-scoring firms that have a satellite

Percent of the 10 lowest-scoring firms that have a satellite **0**

Average number of people in a satellite **131**

Remaining problems... for you

Lots of info about security is software development lifecycle available, so only remaining questions



1. How well are you doing, in any of these metrics?

2. How do you get commitment and resources to improve this?

3. How do you check/show (cost)effectiveness, and decide how much resources are needed?

PS you know there is an OWASP Netherlands chapter?