Building a Robust Application Security Model For **Free**

Pradeep Chhabra
- CISSP, CISA, CISM, CRISC
pradeep.chhabra@owasp.org

OWASP Delaware Chapter
July, 2014

The OWASP Foundation
http://www.owasp.org

Agenda

- Recent Events
- Verizon 2014 Data Breach Investigations Report
- Current Practice – Reactive / Just a Band-aid
- Proactive Approach – Enable Development Teams (Waterfall)
- Proactive Approach – Build Security Controls (Waterfall)
- What is Agile?
- Proactive Approach – Enable Development Teams (Agile)
- Proactive Approach – Build Security Controls (Agile)
- What to do with vulnerabilities besides fixing them?
- Questions

Recent Events

Increasing Impact and Risk

Security Breaches	Hackers infiltrated gaining access to credit card and other personal data of 2.9 million customers * *October, 2013*	70-110 million customer s effected. "Target had the Chance to Stop Breach", Senators Say. Data Breach Hurts Profit at Target. 46% drop in profit * *December, 2013*	Potentially exposed payment card information from transactions at 77 of 85 stores between July and October , 2013 ** *January, 2014*	More than 400,000 Yahoo Inc user names and passwords were stolen and published on the Web ** *January, 2014*

* NY Times, ** Reuters

OWASP

Why? Verizon 2014 Data Breach Investigation Report *

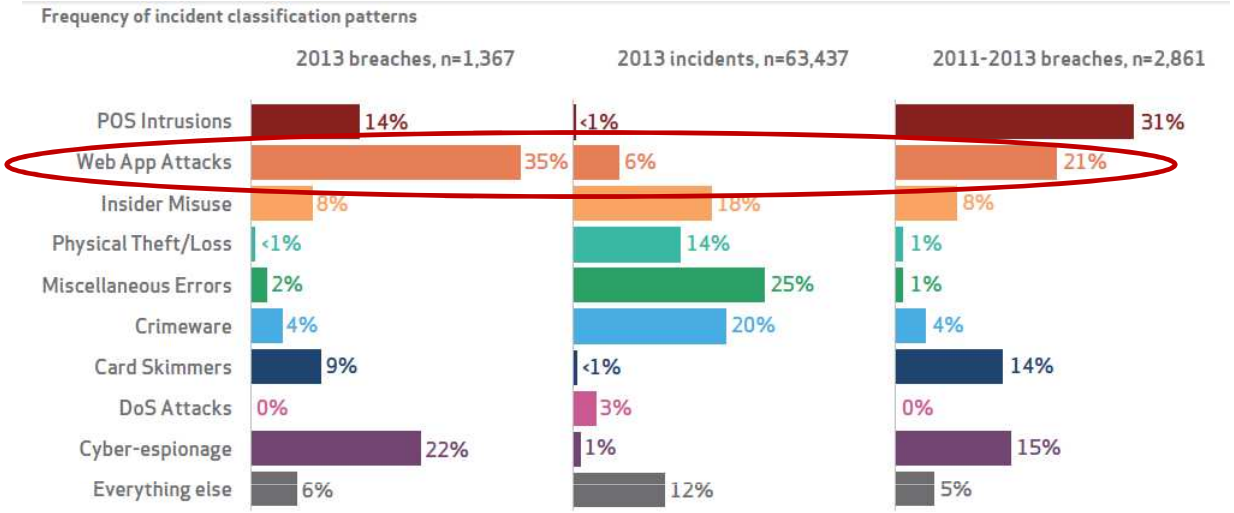


Figure 17.
Number of selected incident classification patterns over time

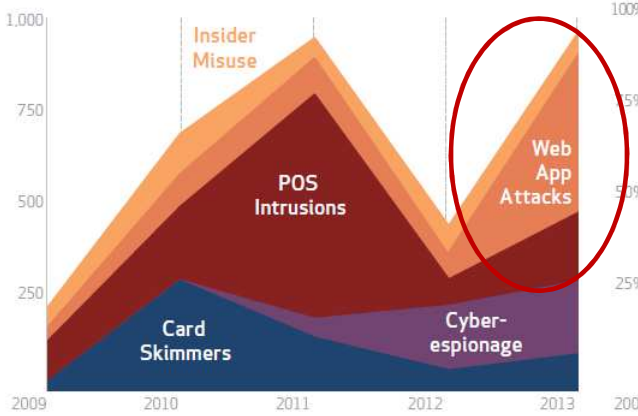
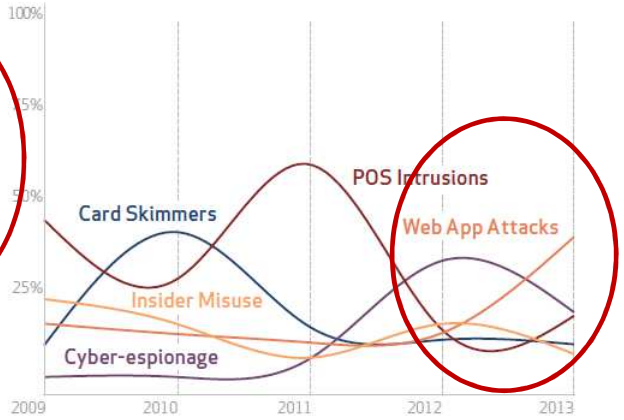
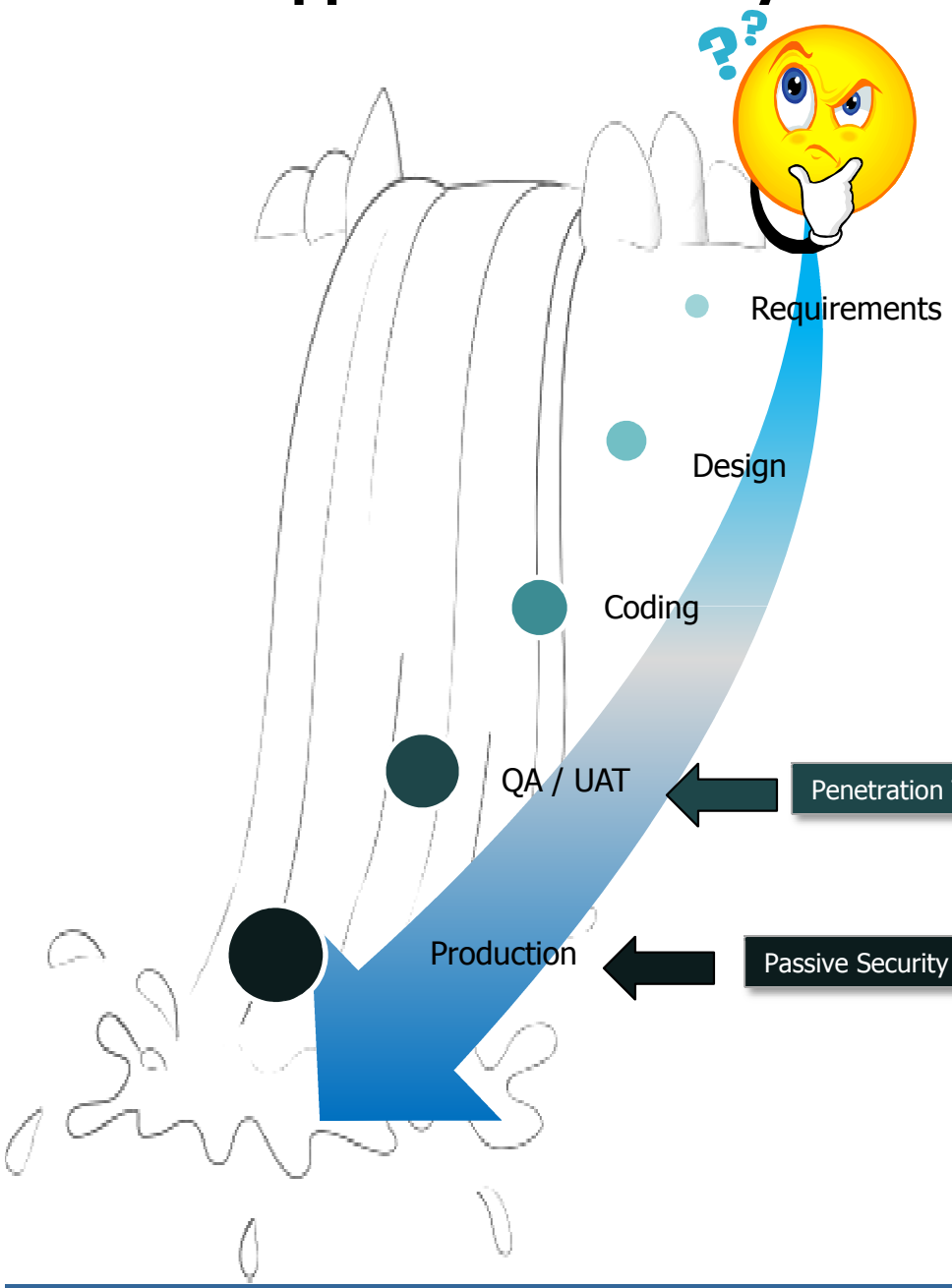


Figure 18.
Percent of selected incident classification patterns over time



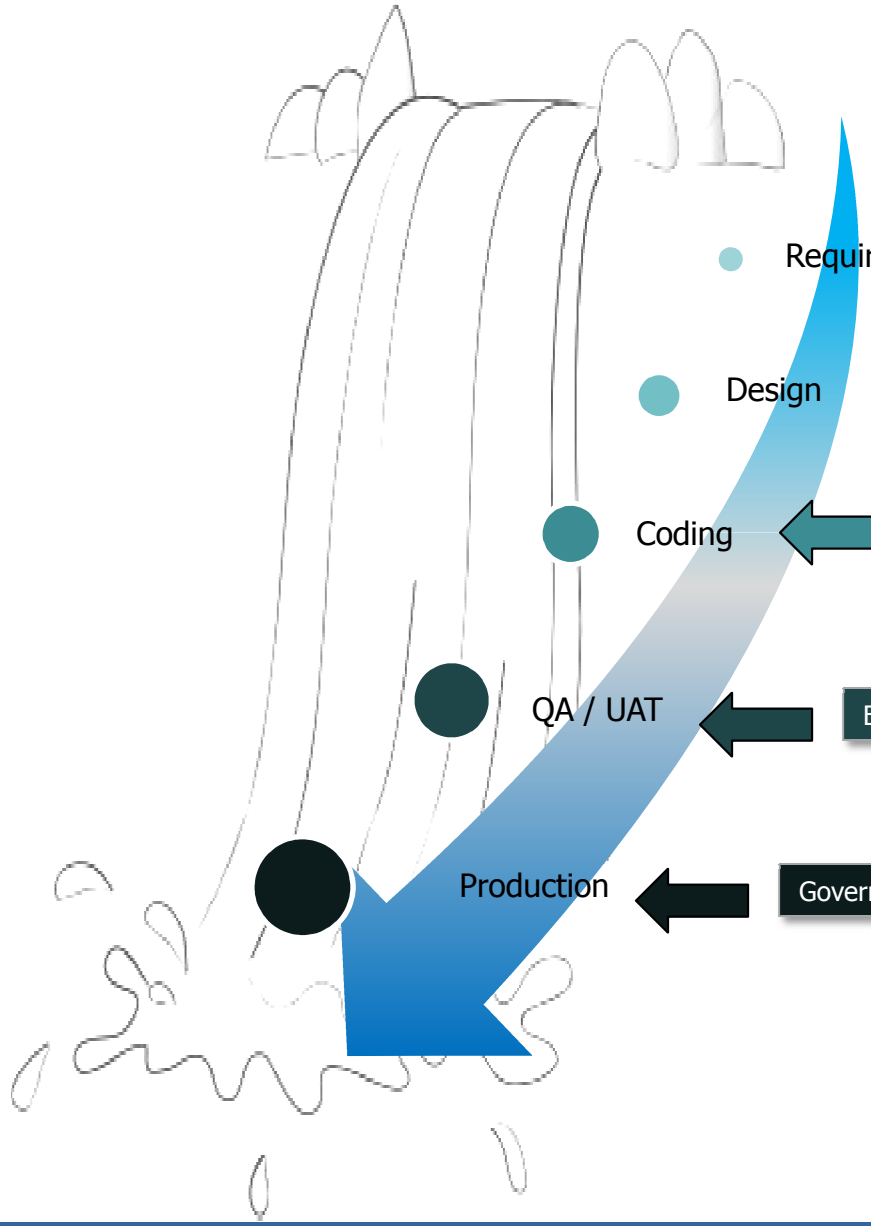
* Source: Verizon 2014 Data Breach Investigations Report

Current Application Security Practice – Reactive / Just a Band-Aid



- **Fixing symptoms not the root cause**
- **No clear guidance causing frustration among developers**
- **Finding vulnerabilities is as good as the usage of scanner.**
- **Different class of vulnerabilities are entirely missed.**
- **Remediation becomes expensive**
- **Very little security training**
- **Difficult to enforce compliance**

Proactive Approach – Enable Development Teams



Emerging Threats / Best Practices

Improve Standards & Policies

Requirements — Provide Security Requirements to Developers

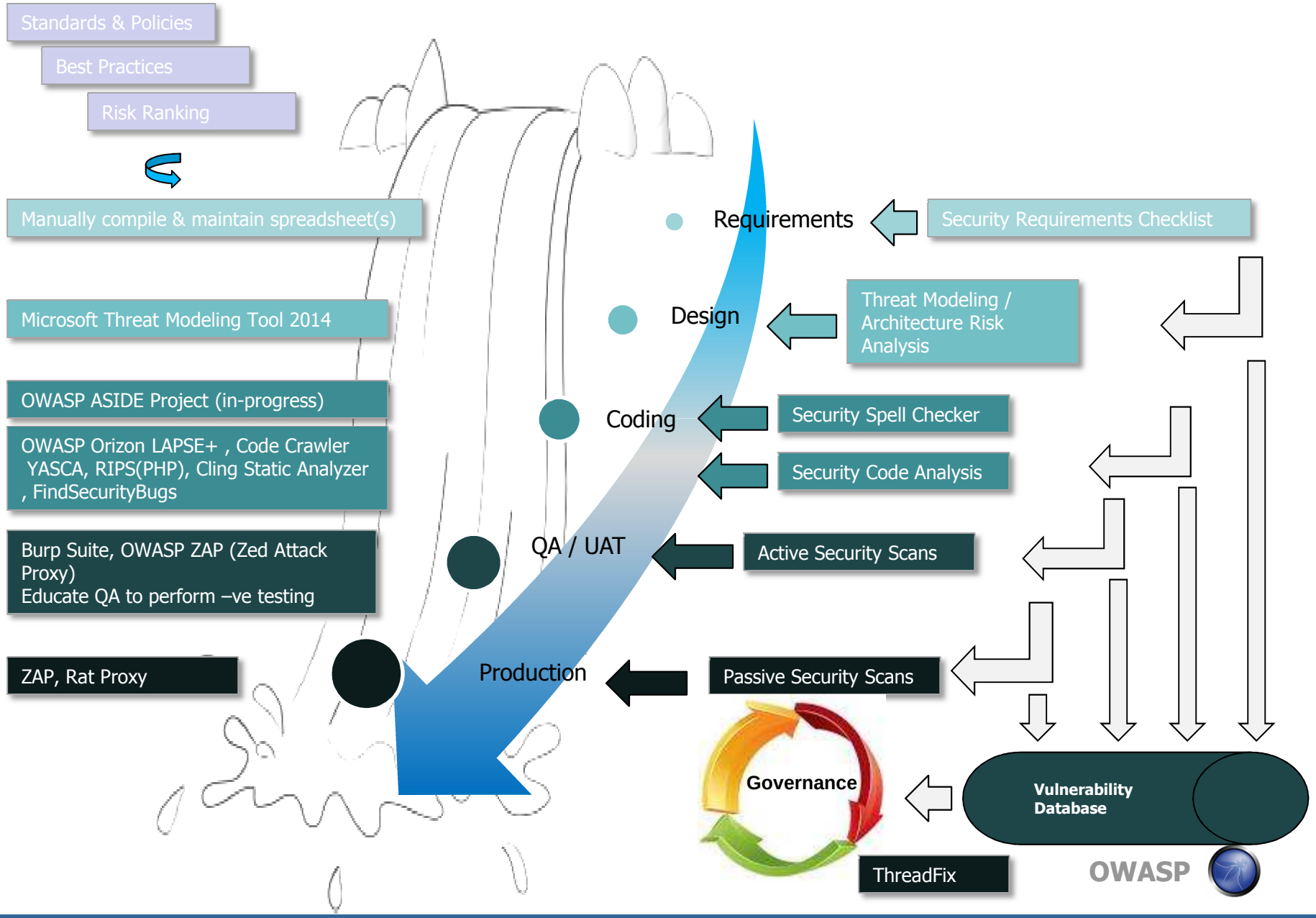
Design — Create & Maintain Security Design Patterns

Coding — Maintain & Enforce Secure Coding Practices

QA / UAT — Educate QA to perform Negative Testing

Production — Governance – Enforce your policy

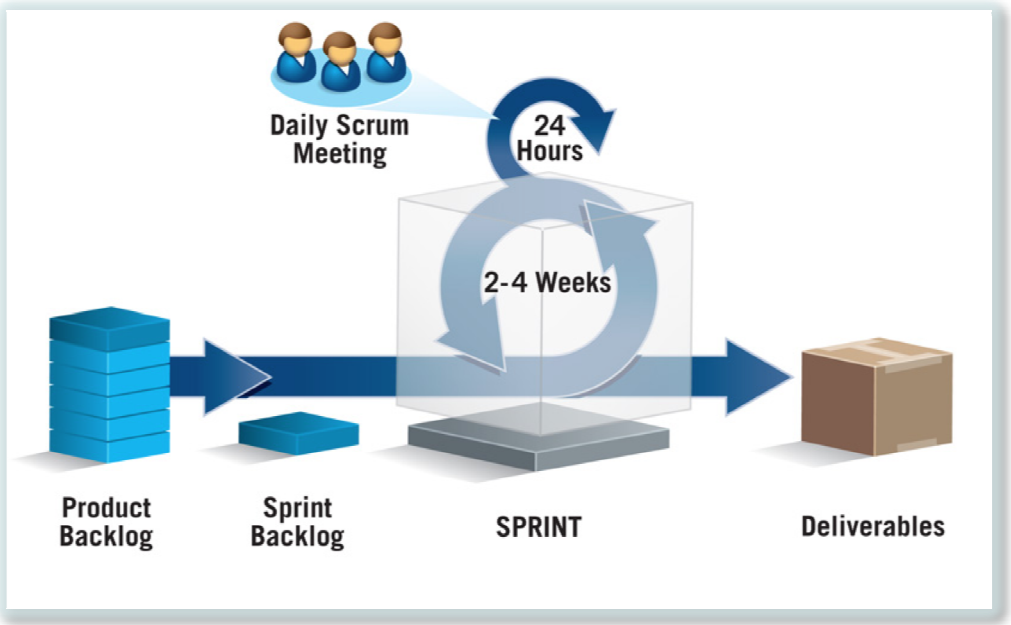
Proactive Approach – Build Security Controls in Each SDLC Phase



What is Agile?

Developers and customer work together throughout

Open to changes throughout life cycles, as prioritized by customers

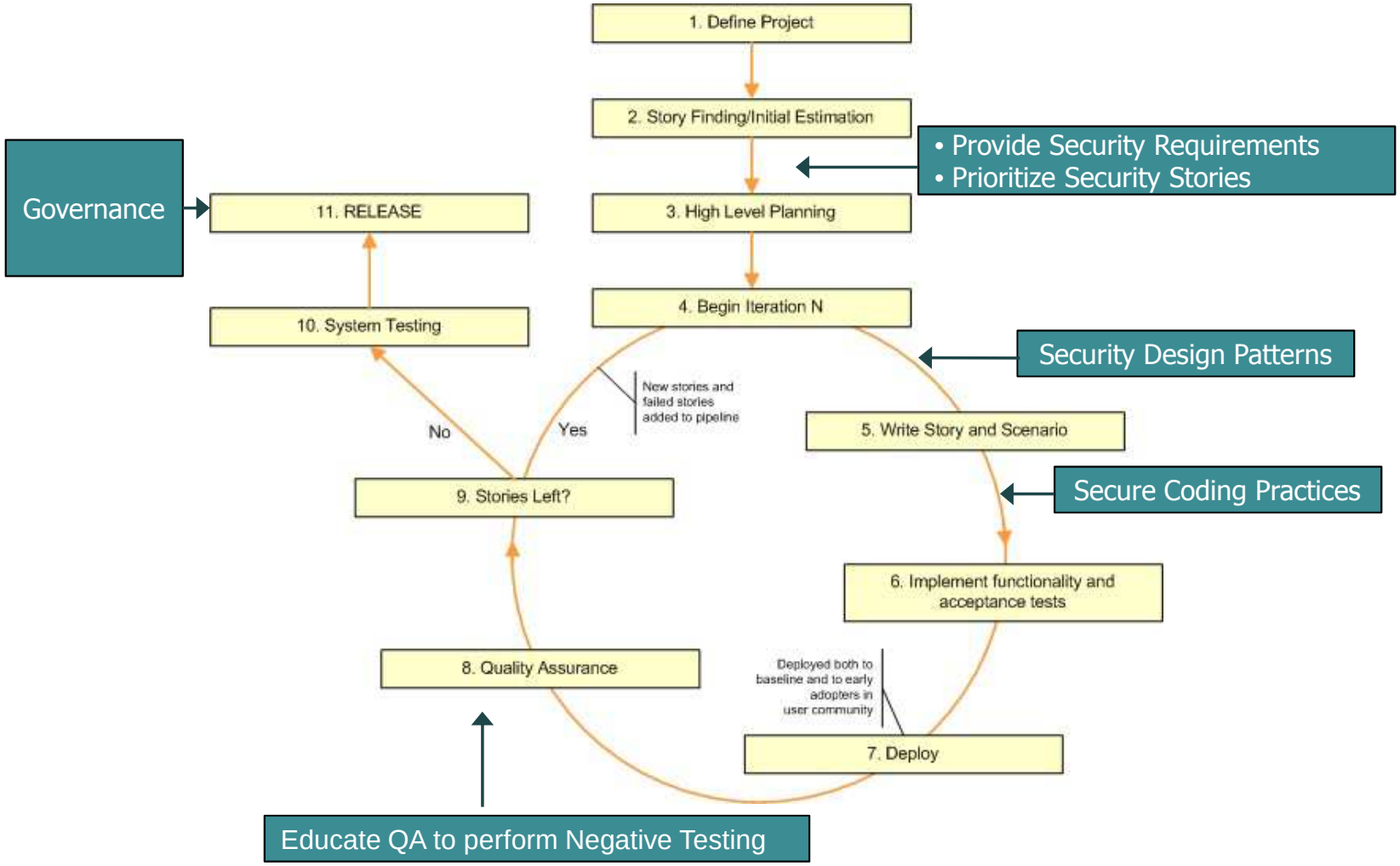


Continuous delivery of business value

Focus on small, deliverable, vertical chunks of work – releasing value earlier in the process

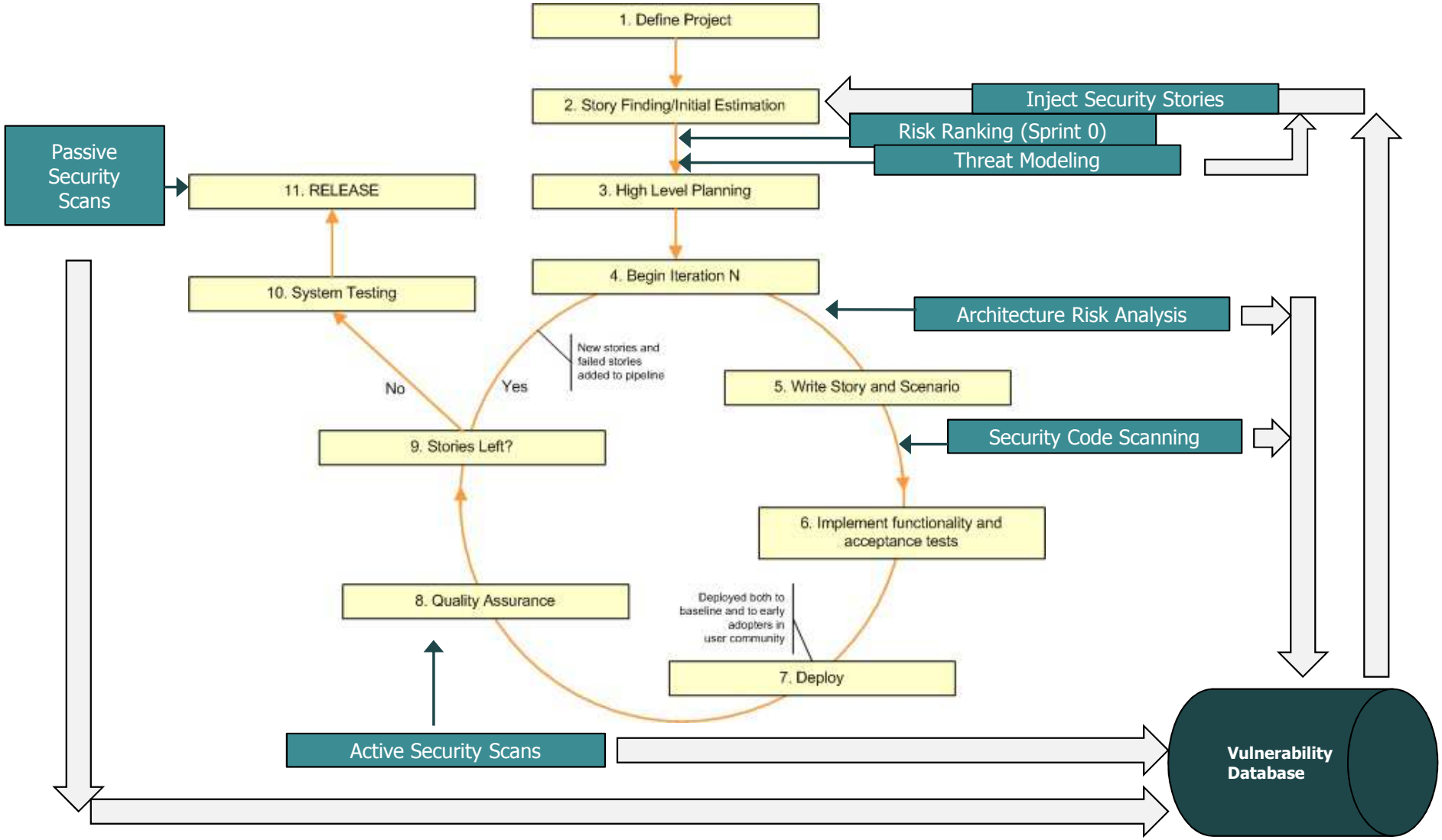
Automation of labor intensive and error prone activities, such as builds, regression, and deployments

Proactive Approach – Enable Development Teams



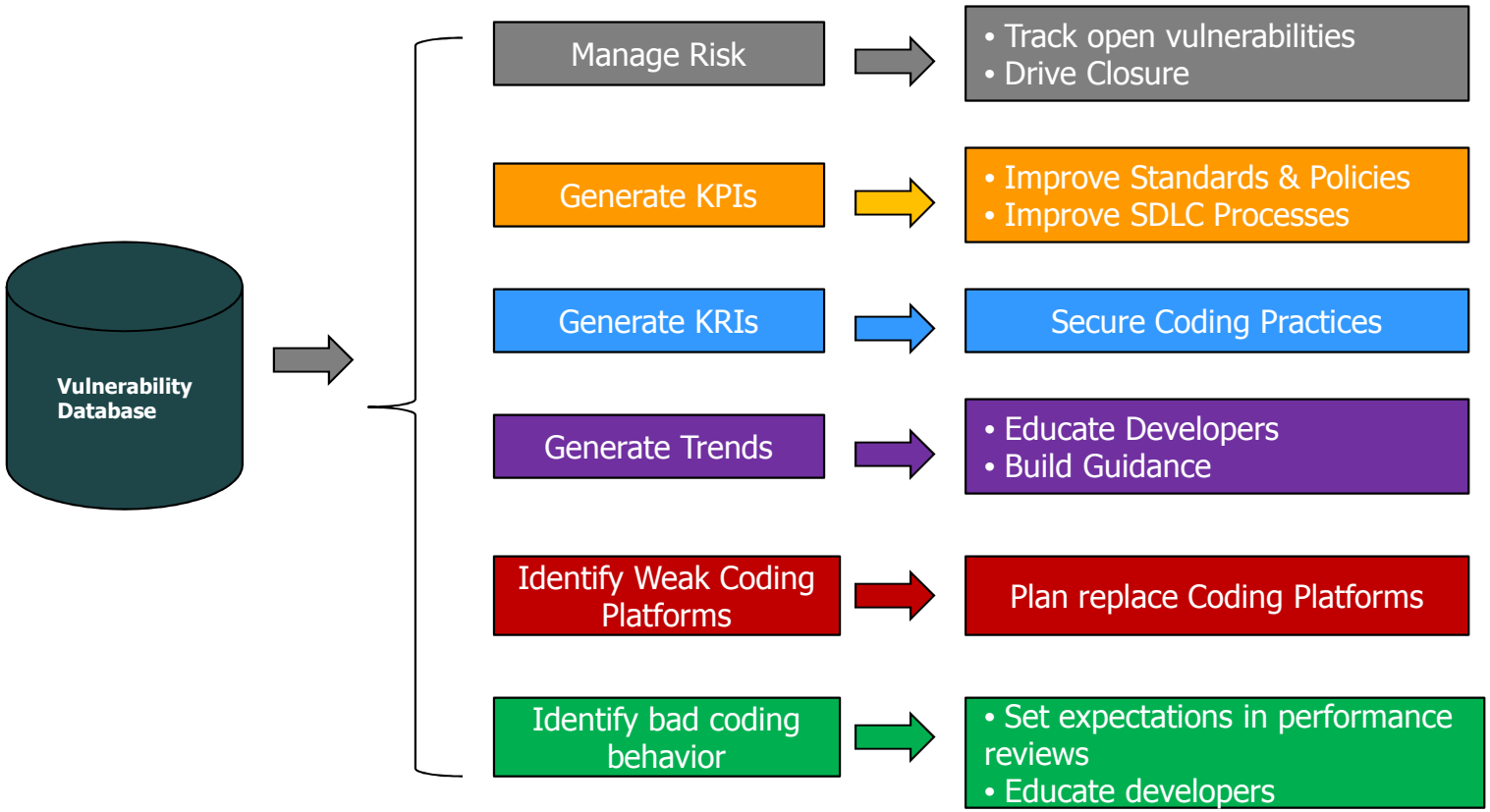
Source: Agile diagram is from https://www.owasp.org/images/b/b8/AppSecEU08-Agile_and_Secure.ppt

Proactive Approach – Build Security Controls



Source: Agile diagram is from https://www.owasp.org/images/b/b8/AppSecEU08-Agile_and_Secure.ppt

What to do with vulnerabilities besides fixing them?



… Potential use is endless …

Appendix – URLs for the free tools

Microsoft Threat Modeling Tool 2014 – http://www.microsoft.com/en-us/download/details.aspx?id=42518

OWASP Orizon Project (Java,PHP,C & JSP) - https://www.owasp.org/index.php/Category:OWASP_Orizon_Project

OWASP LAPSE+ (Java) - https://www.owasp.org/index.php/OWASP_LAPSE_Project

OWASP Code Crawler (.NET, Java) - https://www.owasp.org/index.php/Category:OWASP_Code_Crawler

YASCA - http://www.scovetta.com/yasca.html

RIPS(PHP) - http://sourceforge.net/projects/rips-scanner/

Clang Static Analyzer (C, Objective-C) - http://clang-analyzer.llvm.org/

FindSecurityBugs (Java, Groovy, Scala) - http://h3xstream.github.io/find-sec-bugs/

OWASP ASIDE Project (in-progress) - https://www.owasp.org/index.php/OWASP_ASIDE_Project

Burp Suite - http://portswigger.net/burp/

OWASP ZAP (Zed Attack Proxy) - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Threadfix (Software Vulnerability Aggregation and Management System) - https://github.com/denimgroup/threadfix

Note: You can find more tools at–
http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html

https://www.owasp.org/index.php/Static_Code_Analysis

Questions ?