GOTHAM DIGITAL SCIENCE

Application Security – Often Overlooked Resources and Practices

Justin Clarke
Director – Gotham Digital Science
OWASP London President / Global Connections Committee

Introduction

- Gotham Digital Science (GDS)
  - Information security consulting firm that works with clients to help identify, prevent and manage security risks
  - Offices in New York and London, serving largely financial services clientele
- Justin Clarke
  - Author, Speaker, Security Consultant, Co-Founder of GDS
  - Former E&Y Advanced Security Centers (New York & Houston)

Overview

- OWASP application security resources and projects you may not be aware of
- Possibly overlooked application security practices

Why this talk?

- There are many useful resources provided by OWASP, however OWASP is not good at informing potential users

- There are many practices for assuring application security, but there are other practices used in other industries and parts of the world that may be worth consideration

What is OWASP?

- *The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license*

- An unordered collection of variously useful and non-useful information and resources, with no clear version or quality control

OWASP Resources

- OWASP AntiSamy Java Project
- OWASP AntiSamy .NET Project
- OWASP Enterprise Security API (ESAPI) Project
- OWASP JBroFuzz Project
- OWASP Live CD Project
- OWASP WebScarab Project
- OWASP WebGoat Project
- OWASP Development Guide
- OWASP .NET Project
- OWASP Ruby on Rails Security Guide V2
- OWASP Application Security Verification Standard Project
- OWASP Code Review Guide
- OWASP Testing Guide
- OWASP Top Ten Project
- OWASP AppSec FAQ Project
- OWASP Legal Project
- OWASP Source Code Review for OWASP-Projects

OWASP Resources (cont)

- OWASP CSRFGuard Project
- OWASP Encoding Project
- OWASP OpenSign Server Project
- OWASP OpenPGP Extensions for HTTP - Enigform and mod openpgp
- OWASP Access Control Rules Tester Project
- OWASP Code Crawler
- OWASP DirBuster Project
- OWASP LAPSE Project
- OWASP Orizon Project
- OWASP Pantera Web Assessment Studio Project
- OWASP Report Generator
- OWASP Site Generator
- OWASP Skavenger Project
- OWASP SQLiX Project
- OWASP Sqlibench Project
- OWASP Tiger
- OWASP WeBekci Project
- OWASP Live CD Education Project
- OWASP Teachable Static Analysis Workbench Project
- OWASP AppSensor Project
- OWASP Backend Security Project
- OWASP Securing WebGoat using ModSecurity Project
- OWASP Tools Project
- OWASP CLASP Project
- OWASP Education Project
- OWASP Internationalization Project
- OWASP Spanish Project

Etc etc etc

OWASP Guides

- OWASP Development Guide
  - a massive document covering all aspects of web application and web service security
- OWASP Code Review Guide
  - a project to capture best practices for reviewing code
- OWASP Testing Guide
  - a project focused on application security testing procedures and checklists

OWASP ESAPI

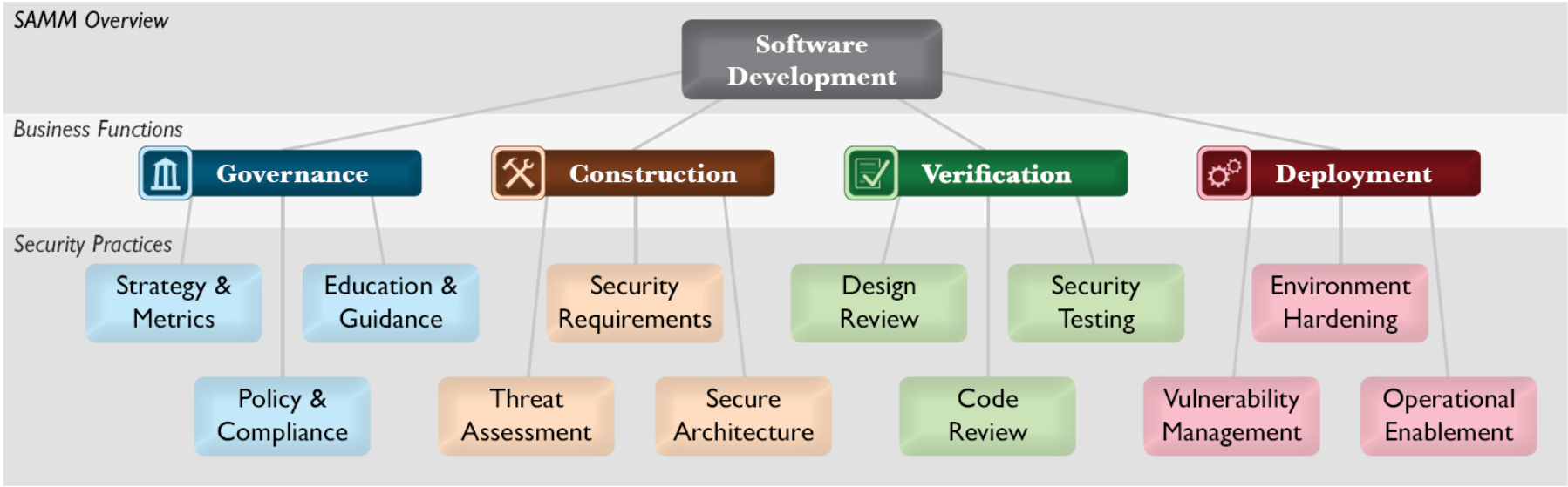
OWASP Top Ten Coverage

OWASP Top Ten	OWASP ESAPI
A1. Cross Site Scripting (XSS)	Validator, Encoder
A2. Injection Flaws	Encoder
A3. Malicious File Execution	HTTPUtilities (upload)
A4. Insecure Direct Object Reference	AccessReferenceMap
A5. Cross Site Request Forgery (CSRF)	User (csrftoken)
A6. Leakage and Improper Error Handling	EnterpriseSecurityException, HTTPUtils
A7. Broken Authentication and Sessions	Authenticator, User, HTTPUtils
A8. Insecure Cryptographic Storage	Encryptor
A9. Insecure Communications	HTTPUtilities (secure cookie, channel)
A10. Failure to Restrict URL Access	AccessController

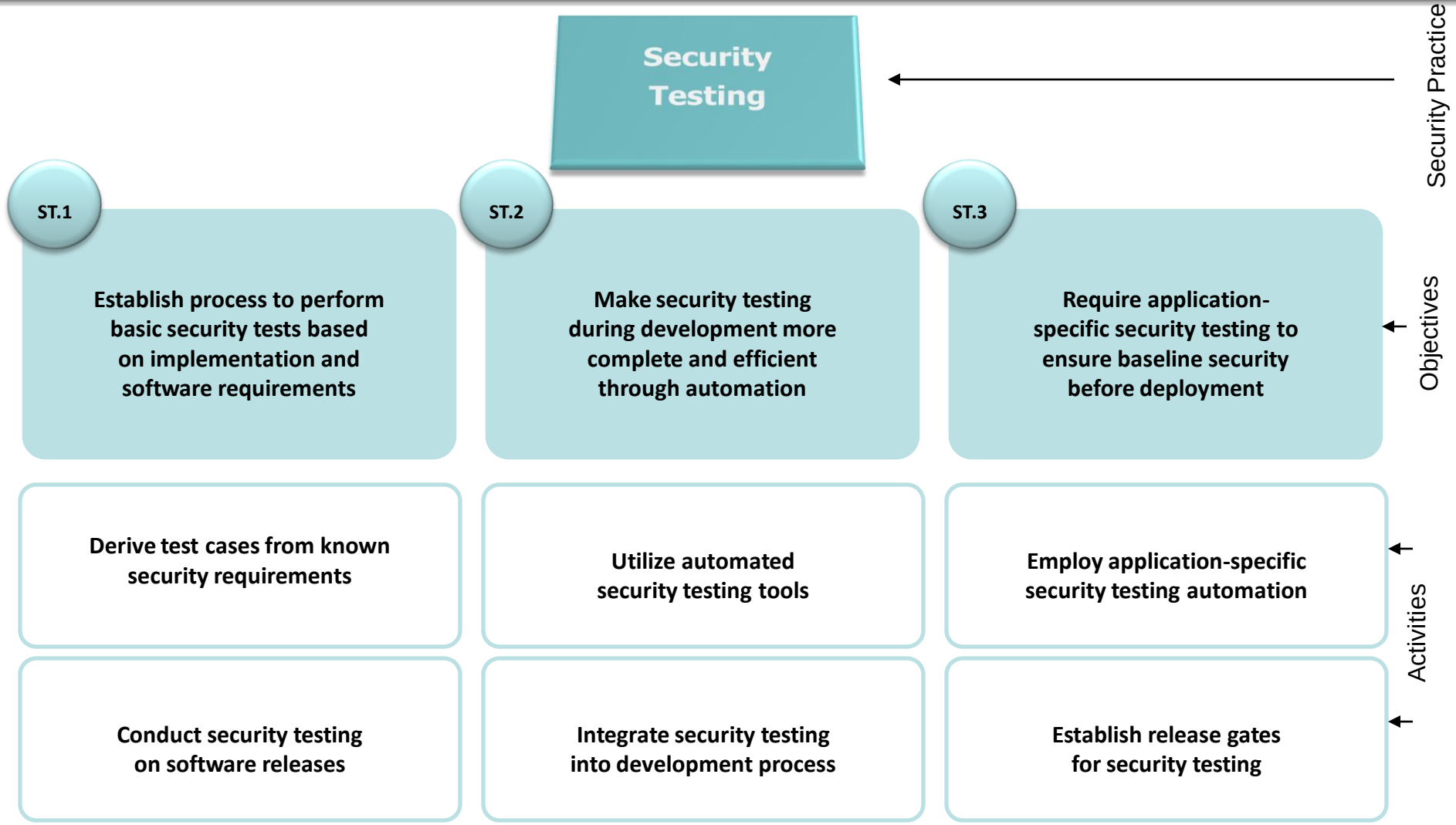
OpenSAMM

- Almost any organisation involved with software development must fulfill each of the Business Functions to some degree.

- Security Practices that are the independent silos for improvement that map underneath the Business Functions of software development.



OpenSAMM (cont)



General Approach

DR 2

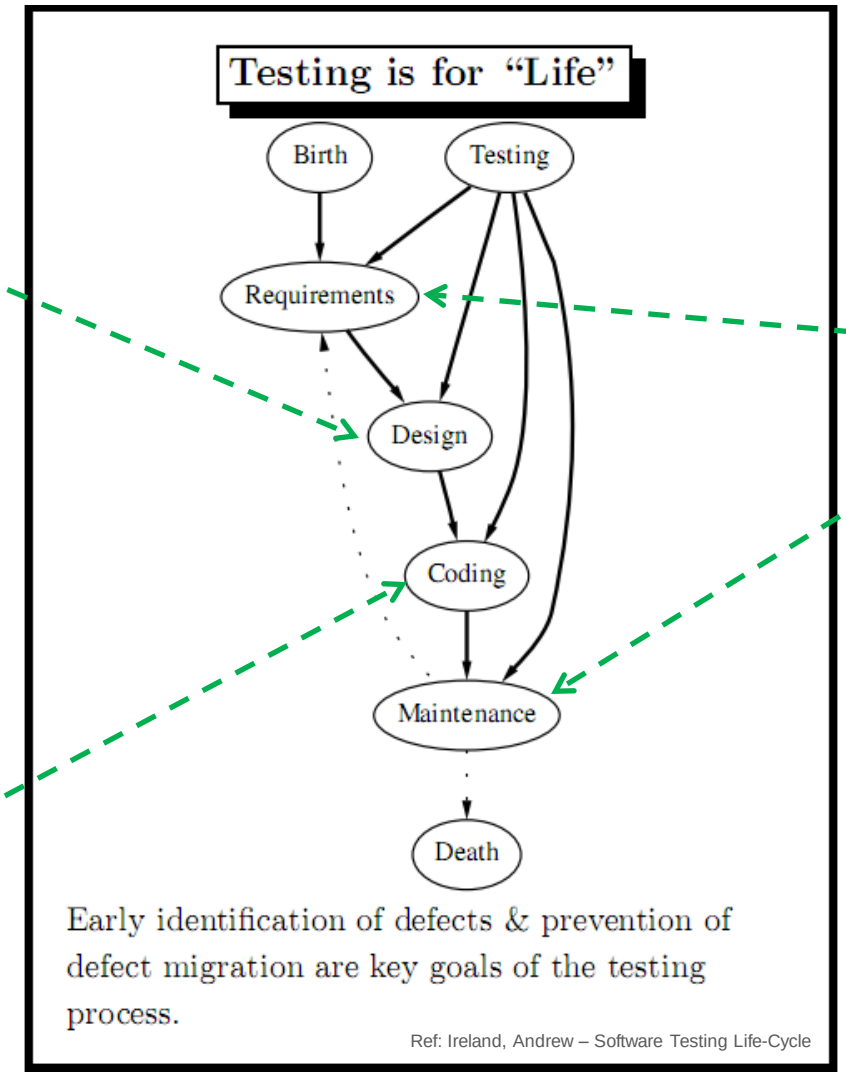
Offer assessment services to review software design against comprehensive best practices for security

A. Inspect for complete provision of security mechanisms
B. Deploy design review service for project teams

CR 2

Make code review during development more accurate and efficient through automation

A. Utilize automated code analysis tools
B. Integrate code analysis into development process



ST 1

Establish process to perform basic security tests based on implementation and software requirements

A. Derive test cases from known security requirements
B. Conduct penetration testing on software releases

Difference in Approach

- Based on empirical experience in US and UK across large scale enterprises
- Confirmation provided by BSIMM Europe survey
- Contrasting approaches Europe vs US, Financial Services vs other verticals

Automated Analysis

- Dynamic and static analysis automation
- Security testing in QA automation
- Coverage analysis

Issue Reporting Loops

- Operational issues fed back to development / shared with QA
- Bugs fed back into development process improvement
- Communication of attacker perspectives

Threat Modelling / Assessment

- Formal threat modelling vs project threat assessment
- Focus on how an architecture is attacked, and controlled

Contact

- OWASP – www.owasp.org
- Gotham Digital Science – www.gdssecurity.com

- Justin Clarke
  - justin@gdssecurity.com
  - justin.clarke@owasp.org

- Gotham Blog - http://www.gdssecurity.com/l/b