HP Software EMEA Performance Tour 2013

Zurich, Switzerland September 18

Integrating Application Security into Application Lifecycle Management

Migchiel de Jong / September 18, 2013

1

Somebody builds bad software

2

IT deploys the bad software

3

We are breached or pay to have someone tell us our code is bad

4

$ $ $

We convince and pay the developer to fix it

Agenda

- Why be Concerned with Application Security?
- Most Common Application Security Program Approach Mistakes
- Characteristics of a Successful Application Security Program
- The technology perspective

Why be concerned with Application Security ?

Building Effective Application Security Programs

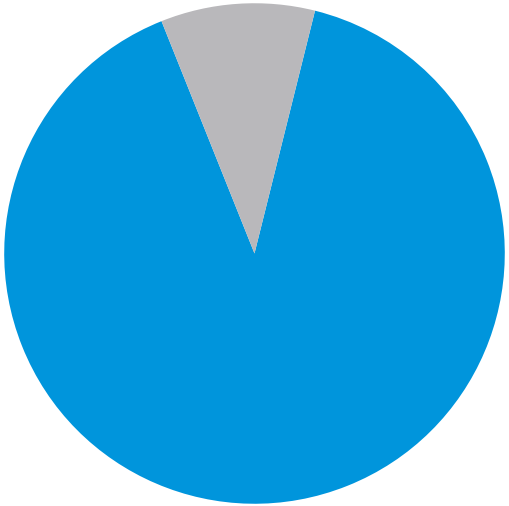
Why be Concerned with Application Security?

The End of the Corporate Network

- The Corporate Network as we know it will not exist in 10 years.
  - *Silicon Valley*
- The move to Cloud and Mobile Computing will greatly reduce the effectiveness of traditional perimeter security controls.
- But just how effective are these controls today?

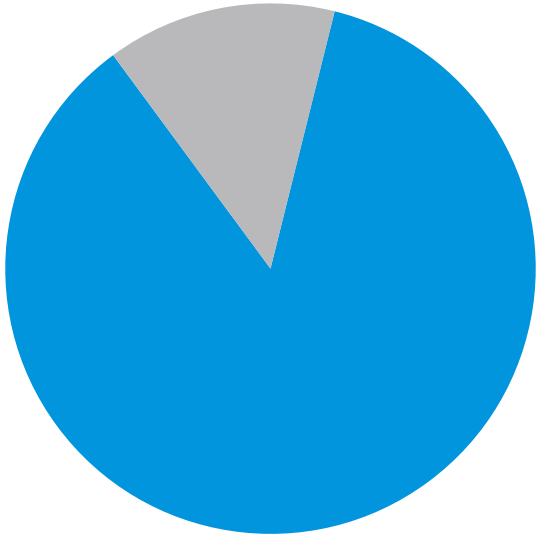
Why be Concerned with Application Security?

- In a recent survey of 583 U.S companies conducted by Ponemon Research on behalf of Juniper Networks, 90% of the respondents said their organizations' computers had been breached at least once by hackers over the past 12 months.
  - *[source: Computerworld, June 22, 2011]*



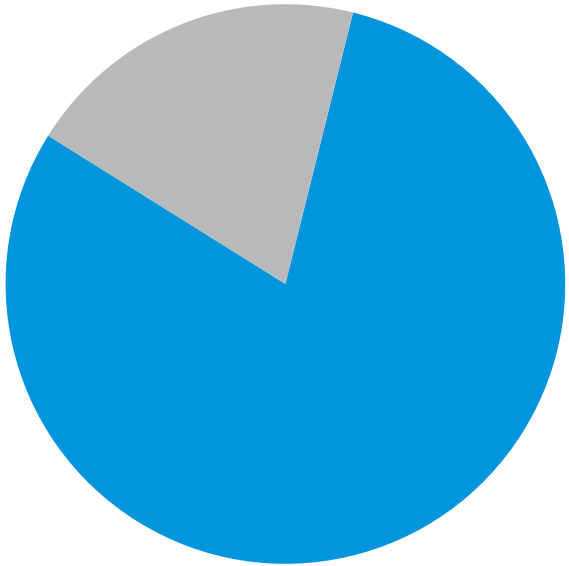
Why be Concerned with Application Security?

- From scans of over 31,000 sites, over 85% showed a vulnerability that could give hackers the ability to read, modify and transmit sensitive data.
  - [Web Application Security Consortium].



Why be Concerned with Application Security?

- “80% of Malicious Attacks happen at the application layer”.
  - [Gartner]



Most Common Application Security Program Approach Mistakes

Most Common Application Security Program Approach Mistakes

I have yet to see any problem,
however complicated, which,
when you look at it in the right way,
did not become still more complicated.

– Poul Anderson

Failed or ineffective application security programs almost always have one or more of the following characteristics:

- The view that application security is a “security” problem , and hence must be dealt with by the security team.
- The view that testing or “assessment” can and will resolve the problem.
- The view that “tools” and technology are the answer to solve the problem.
- The view that application security is an “all or nothing” endeavor.

Characteristics of a Successful Application Security Program

People seem to want to treat computer security like it's rocket science or black magic.

In fact, computer security is nothing but attention to detail and good design.

It's certainly possible to turn a computer security problem into a rocket-science or brain surgery class problem, but if you've done that it's almost a certain indication that you've already started down the wrong path.

[source: Marcus Ranum]

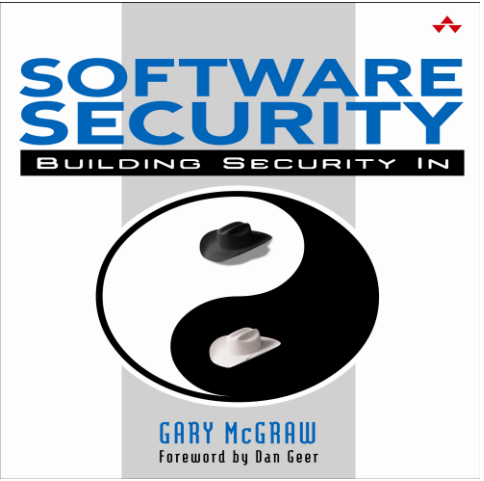
Successful application security programs:

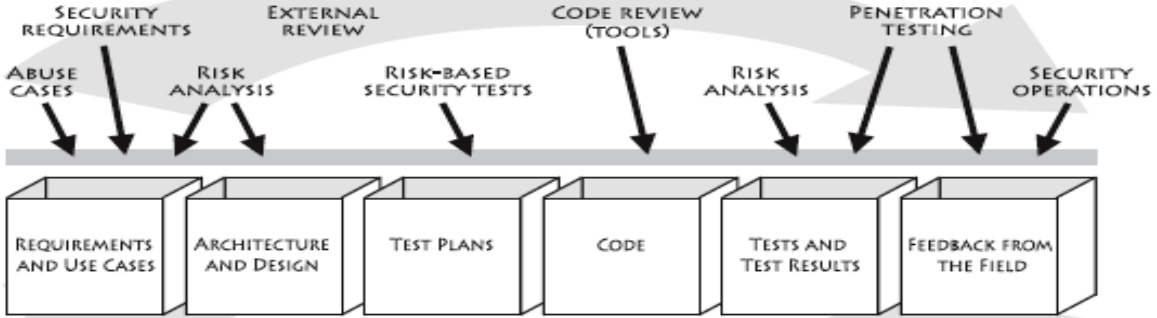
- Recognize that application security, like all security, is a business problem.

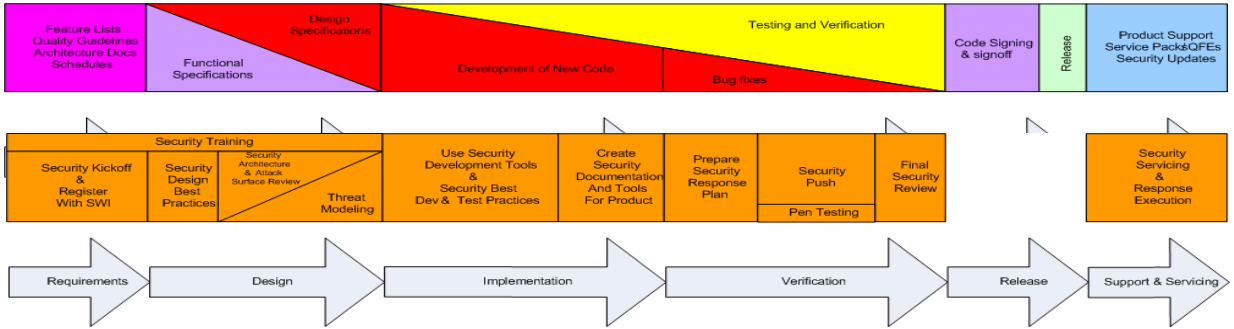
- Have clearly defined Goals and Objectives that are understood and accepted throughout the organization

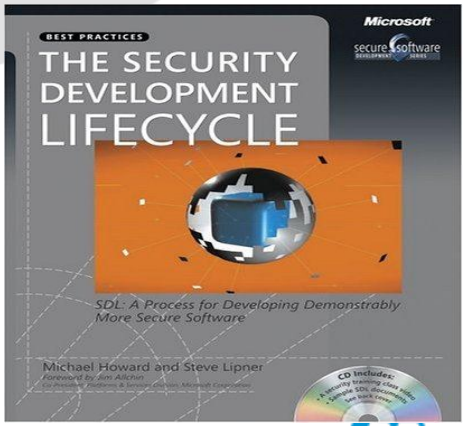
- Have a well defined Approach that includes:
  - The Capability to clearly define application security from a business risk perspective
  - The Capability to create secure code
  - The Capability to validate security requirements are being met
  - The Capability manage security defects in production

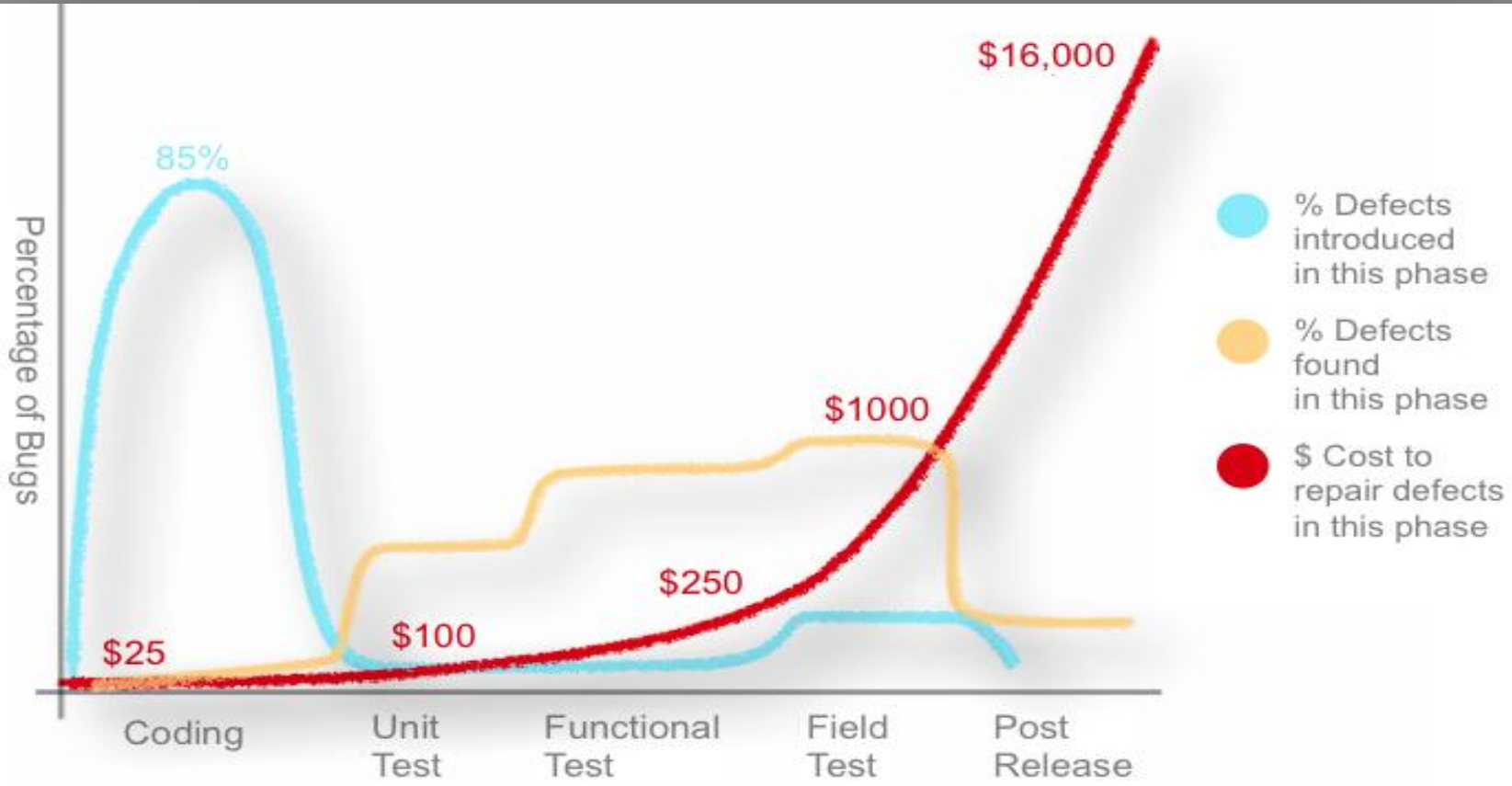
Security in the Development Lifecycle



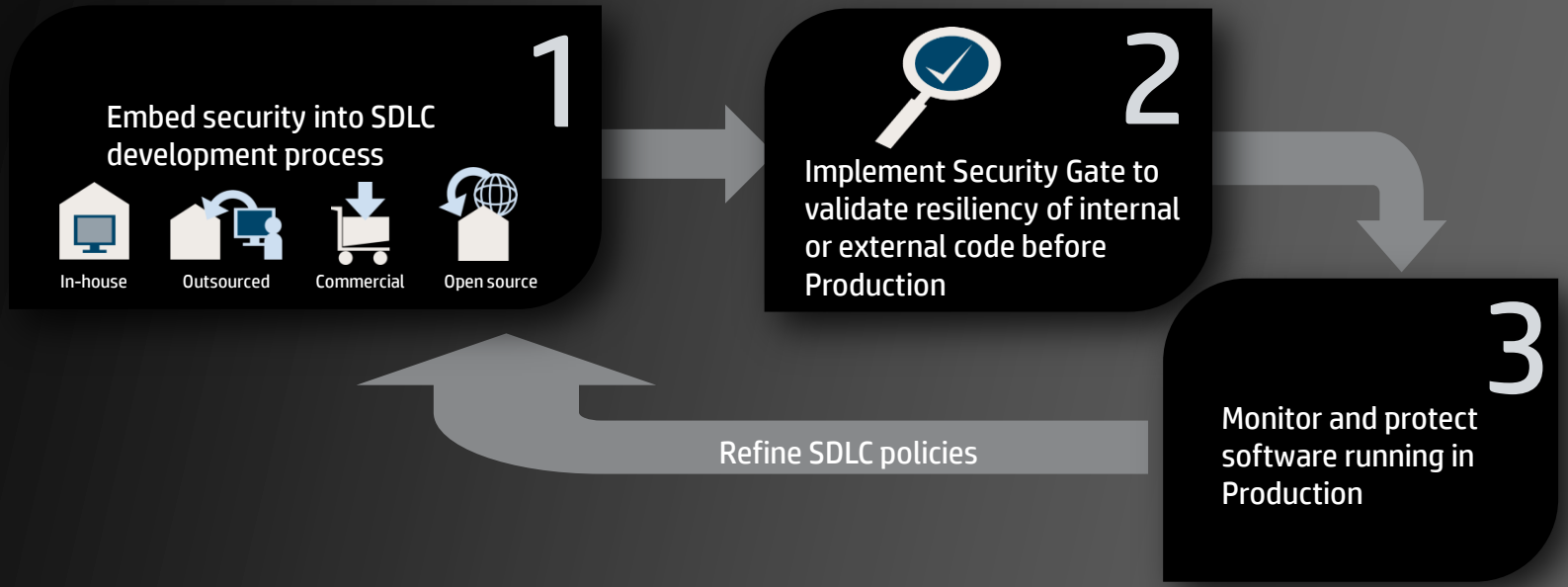








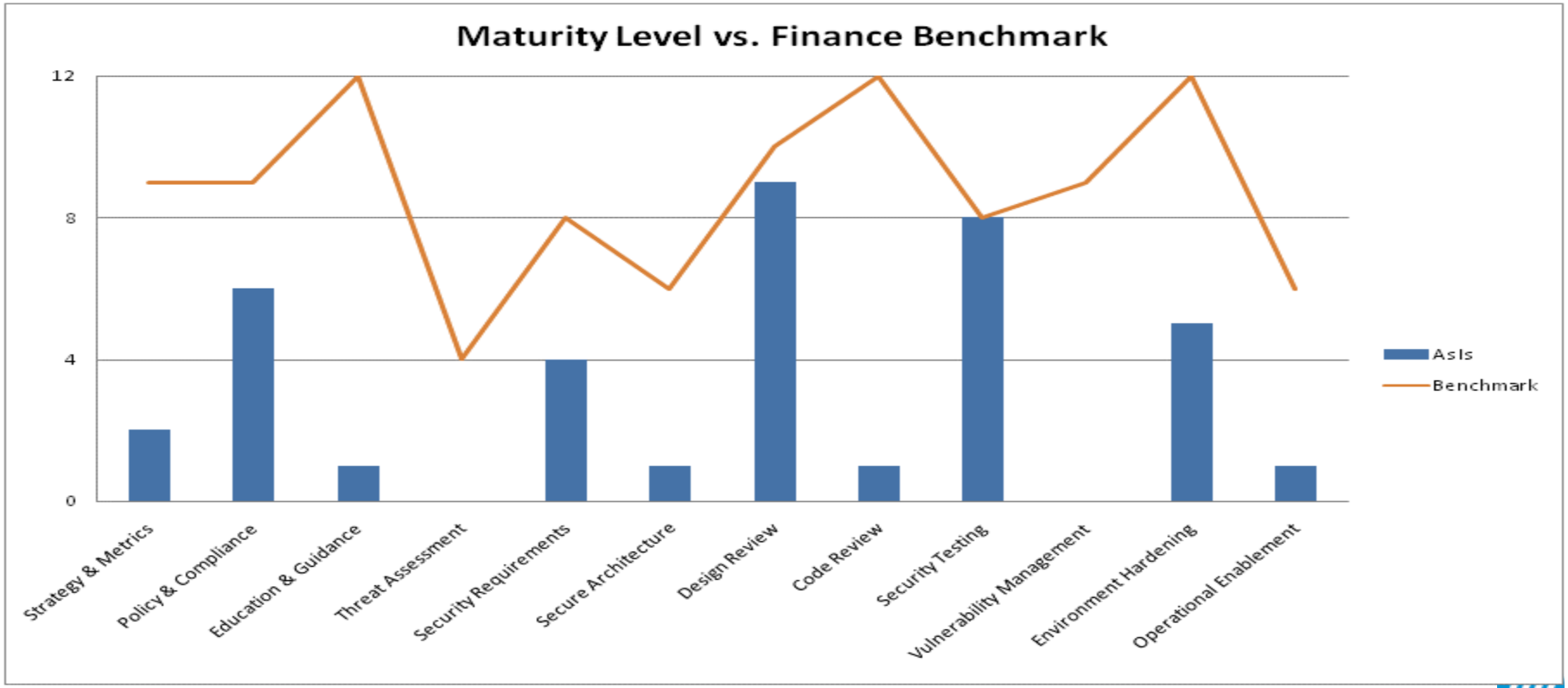
Source: Applied Software Measurement, Capers Jones, 1996



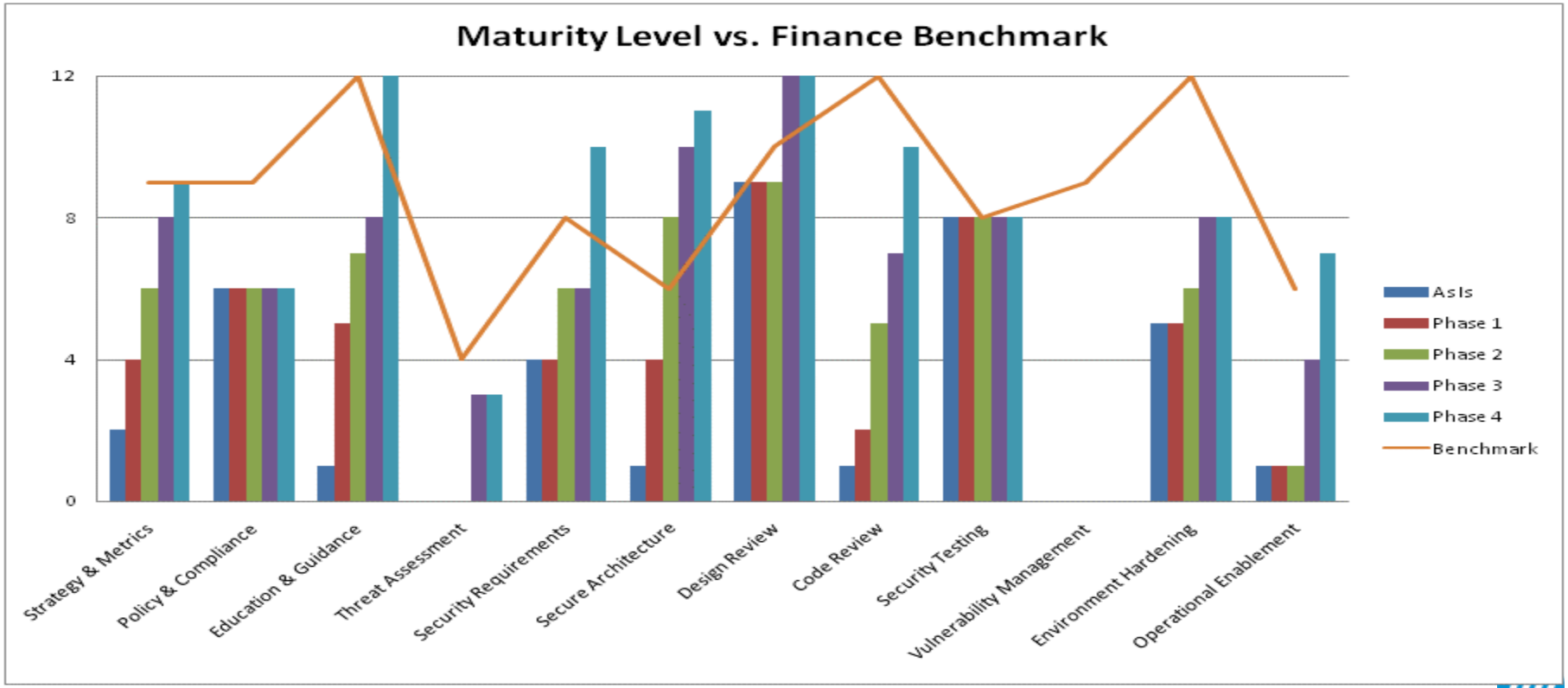
This is Software Security Assurance


Education & Guidance
Standards & Compliance
Strategic Planning
Alignment & Governance
Threat Modeling
Security Requirements
Defensive Design
Requirements & Design
Architecture Review
Code Review
Security Testing
Verification & Assessment
Vulnerability Management
Infrastructure Hardening
Operational Enablement
Deployment & Operations

SSA Benchmark



SSA Roadmap



SSA Best Practice Approach

- Quickly find and remediation of critical vulnerabilities
  - Don't "forget to fix" or "boil the ocean"

- Prevent introduction of new vulnerabilities
  - Integrate into existing SDLC with minimal process changes
  - Provide flexibility to integrate with new SDL as it rolls-out

- Provide support for the developers
  - Training in the context of their own code base
  - Mentoring as required

- Monitor and control
  - Automate gathering of vulnerability statistics and publish
  - Enforcement via security gate

- Continuous Improvement

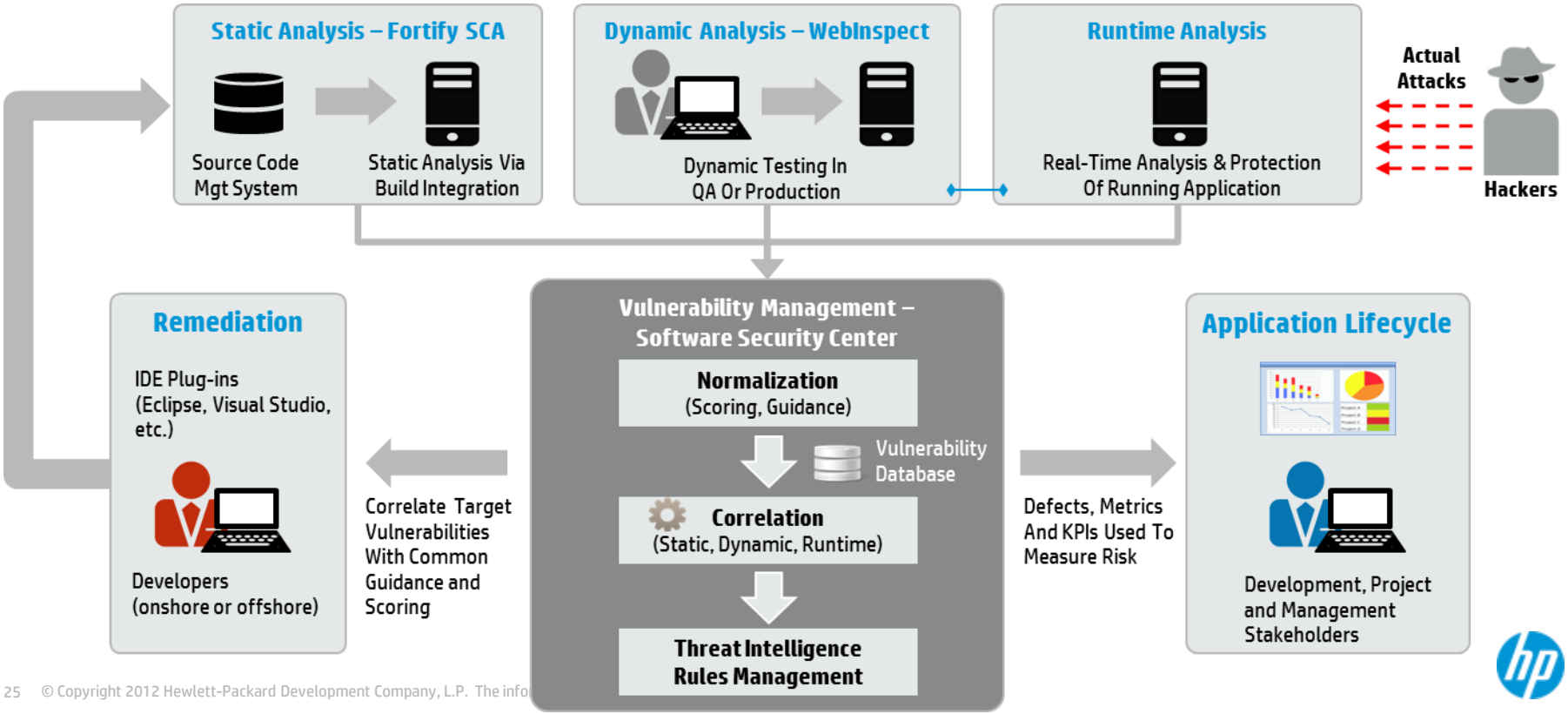
The Technology Perspective

Solution Components

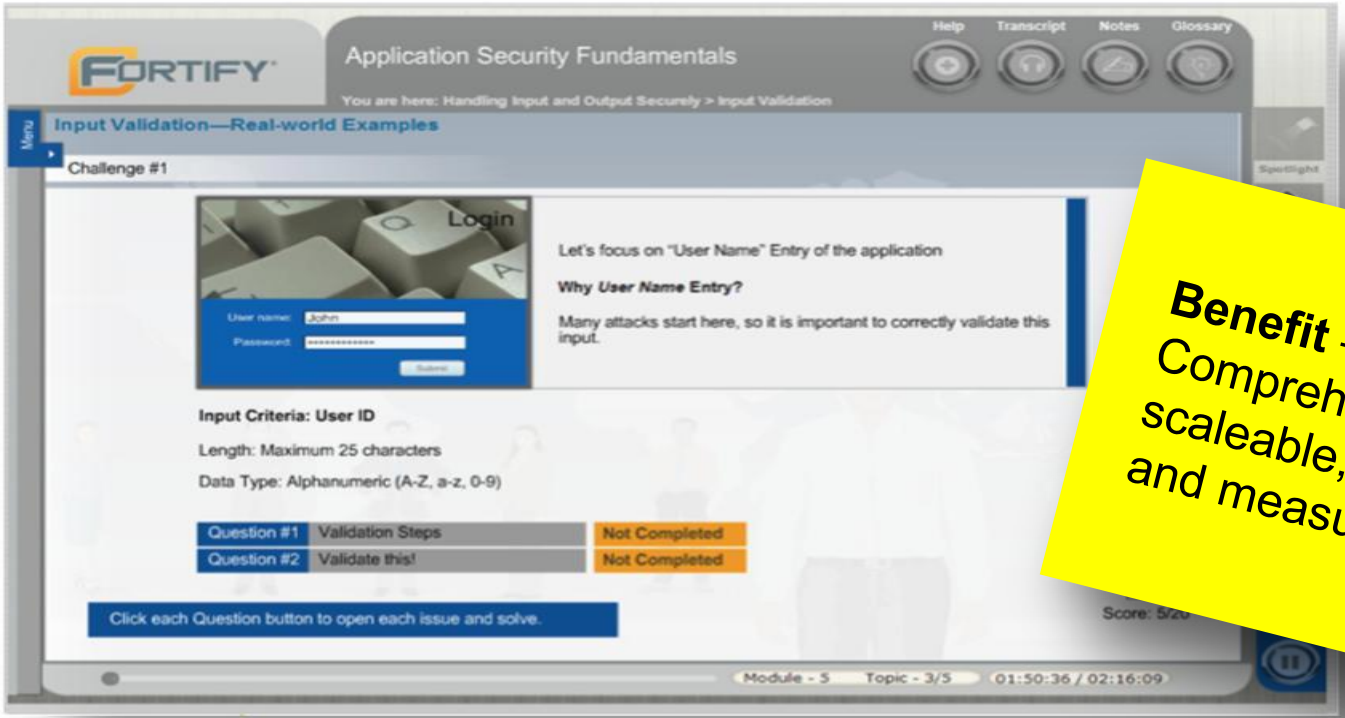
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Runtime Application Security Testing (RAST)
- Hybrid Analysis (combining SAST and DAST through RAST)
- FOD (SAST and DAST in the cloud)

HP Fortify – Software Security Assurance

On-Premise and On-Demand

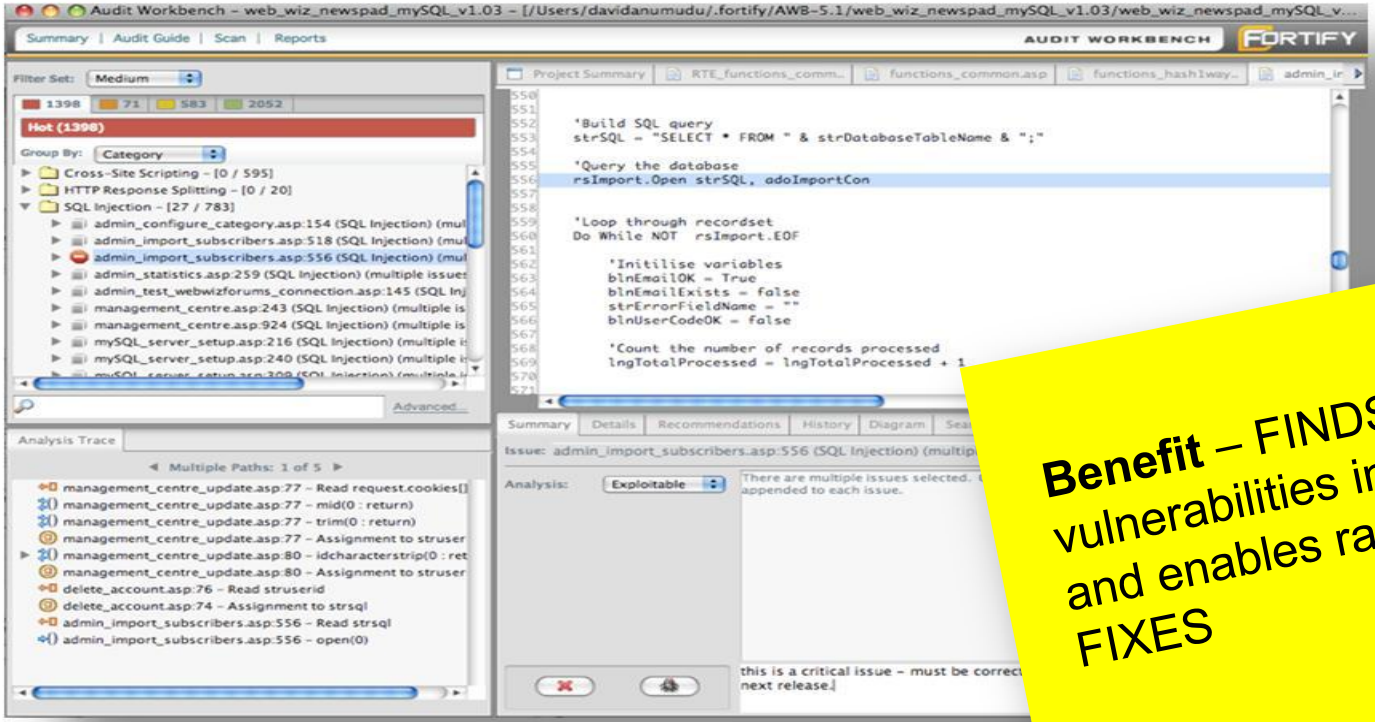


Fortify eLearning – Cloud Based Education



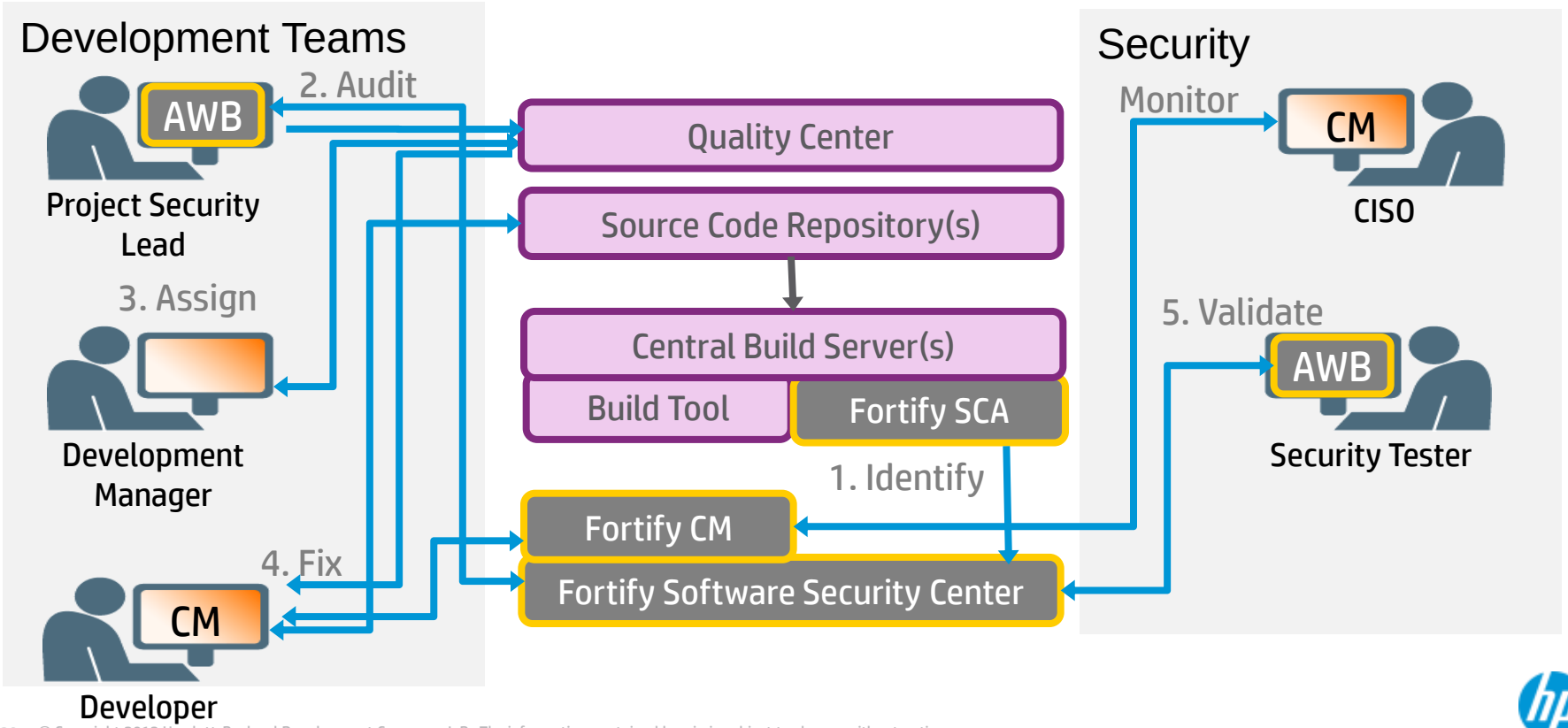
Benefit – Comprehensive, scaleable, repeatable and measureable

Fortify SCA – Early Lifecycle Security Testing

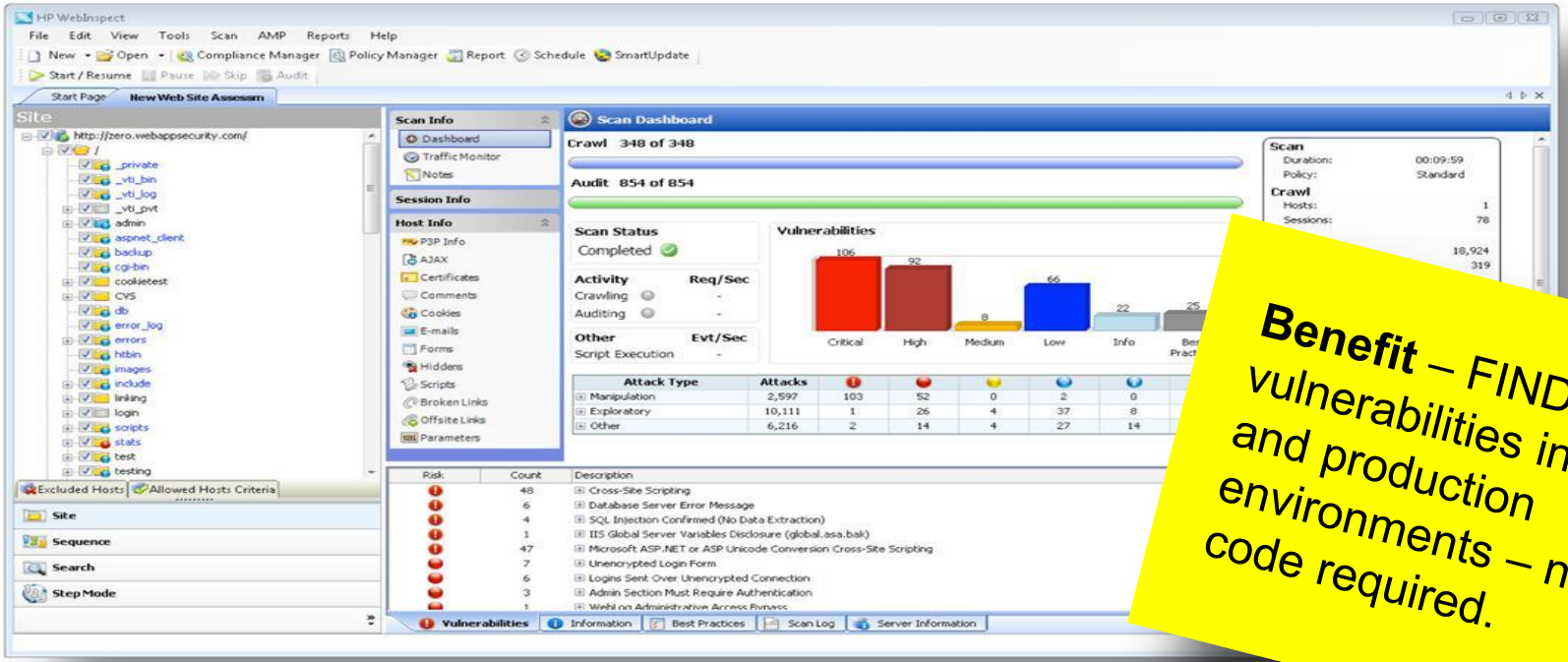


Benefit – FINDS vulnerabilities in code and enables rapid FIXES

Example Implementation – Source Code Analysis

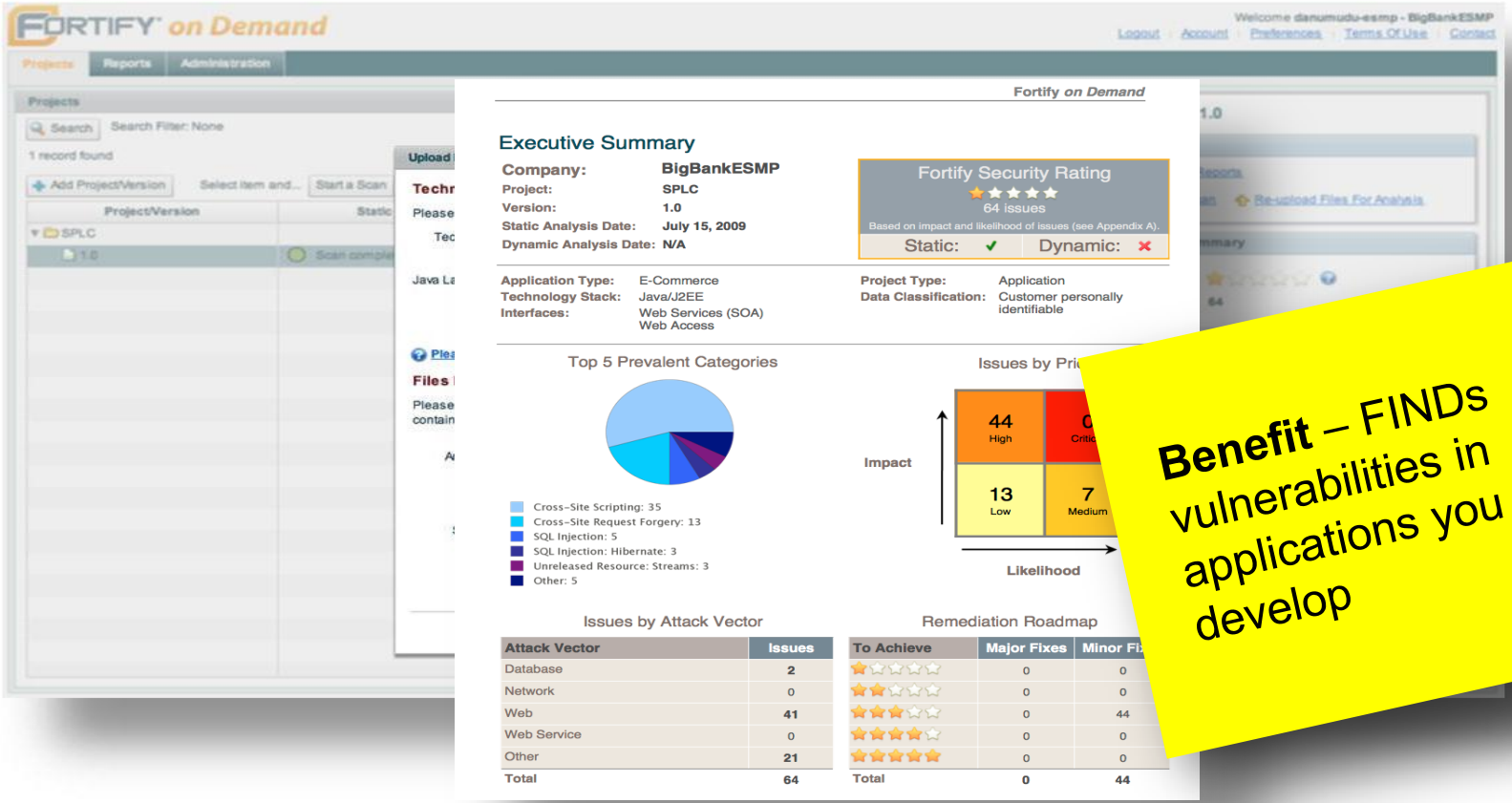


WebInspect – Late Lifecycle Security Testing



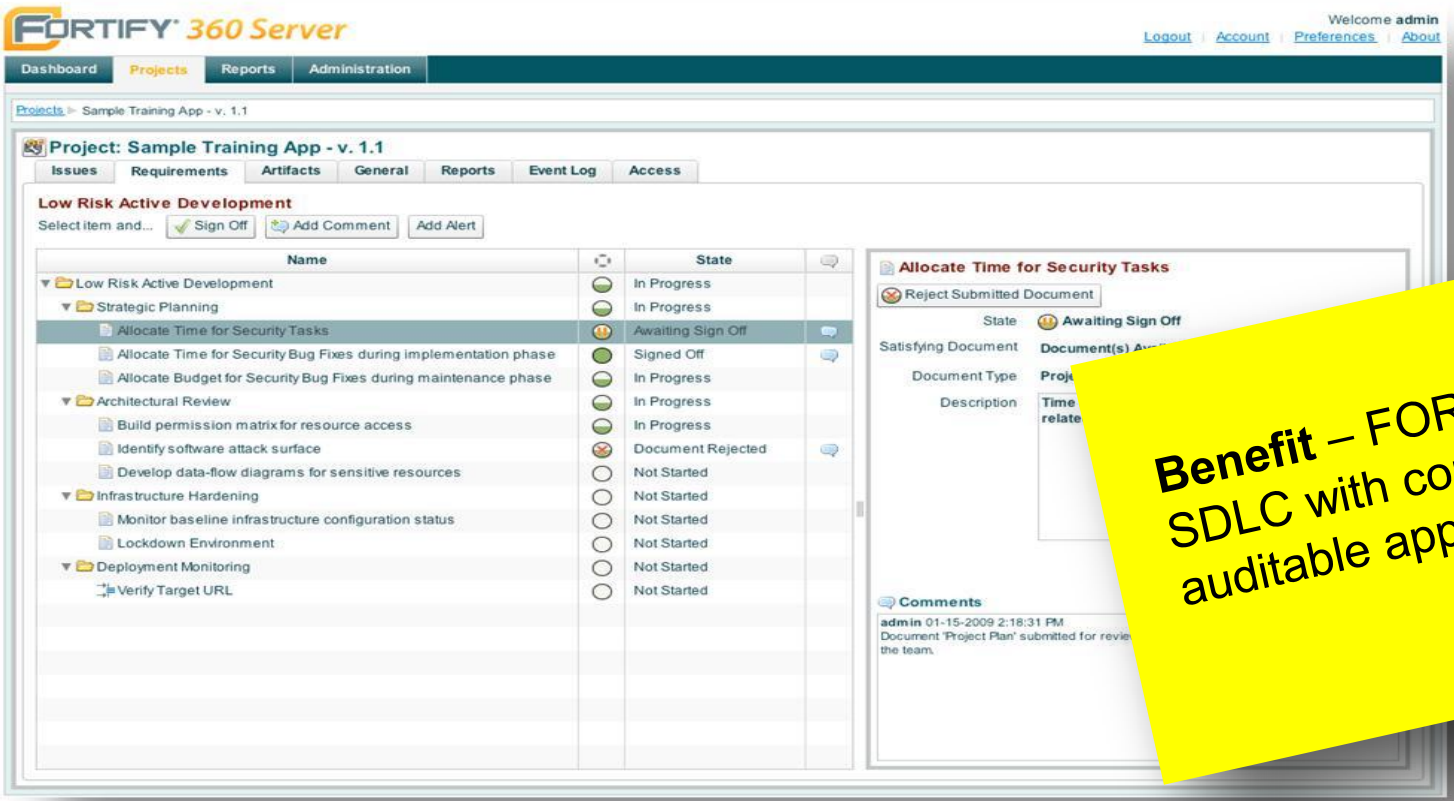
Benefit – FINDS vulnerabilities in QA and production environments – no code required.

Fortify OnDemand – Security Testing Service



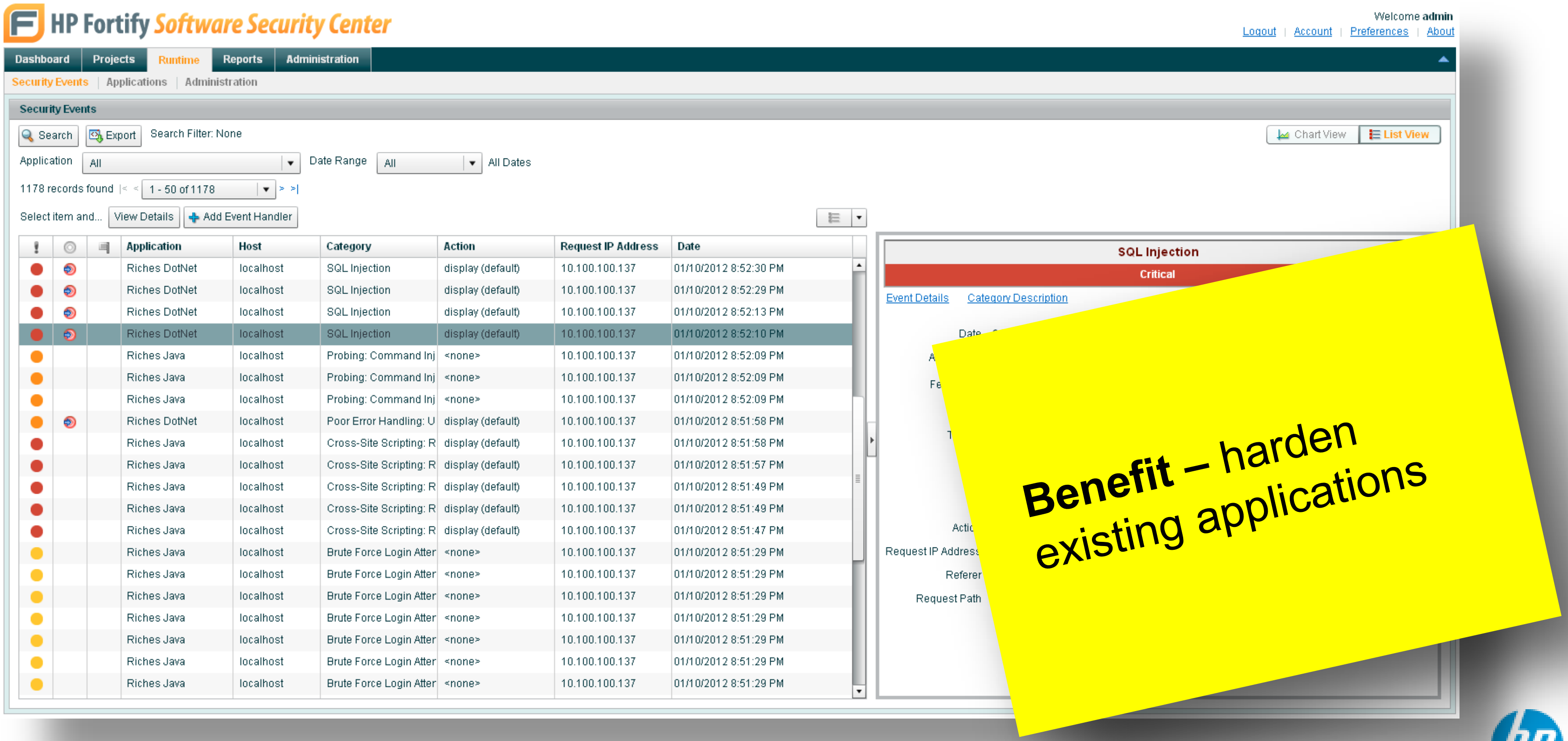
Benefit – FINDs vulnerabilities in applications you don't develop

Fortify Governance – SDLC Process Control

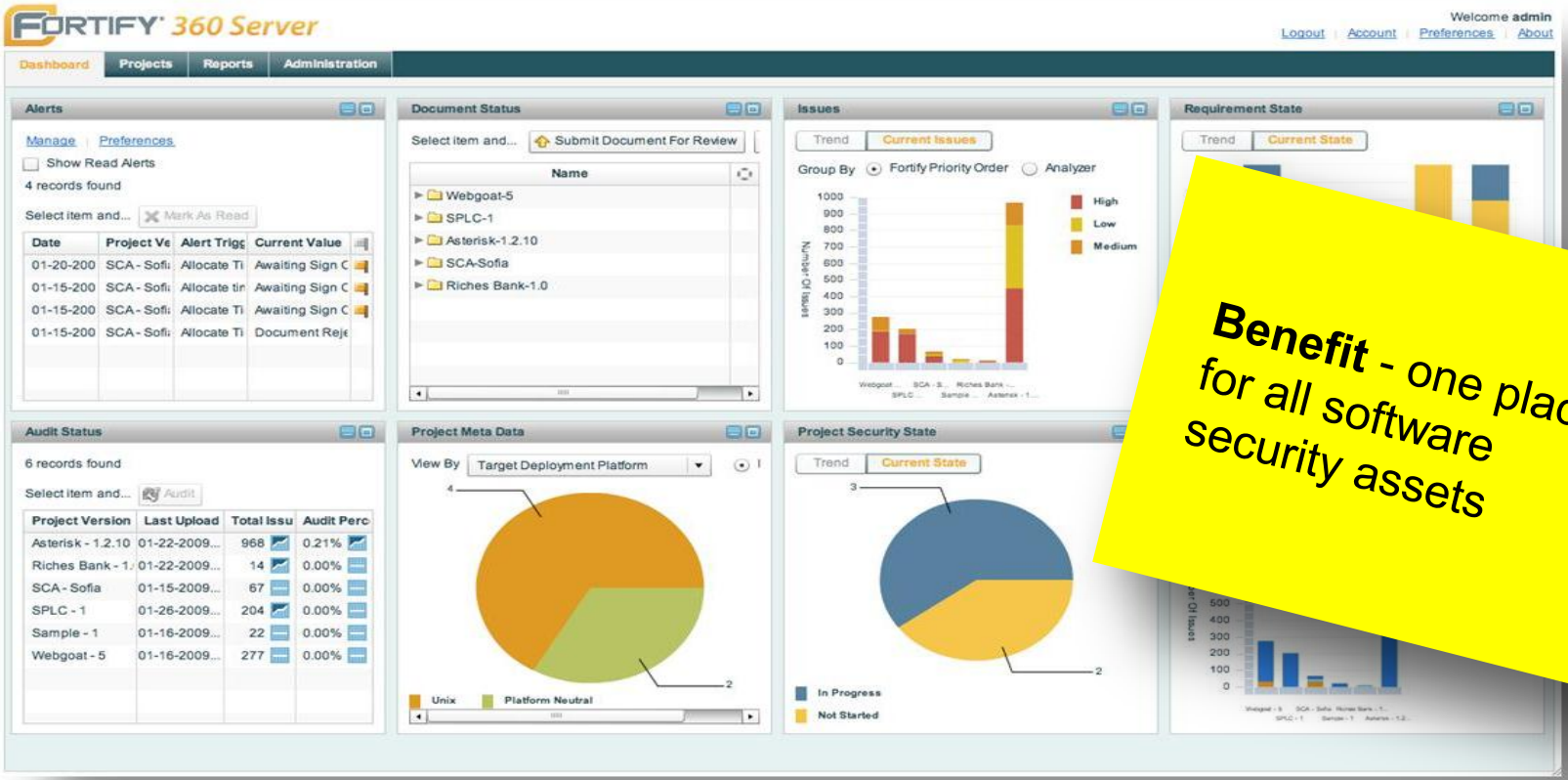


Benefit – FORTIFYs SDLC with consistent auditable approach

Fortify RTA – Application Deployment Protection



Fortify SSC- Management Dashboard



Benefit - one place for all software security assets

Thank you