RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

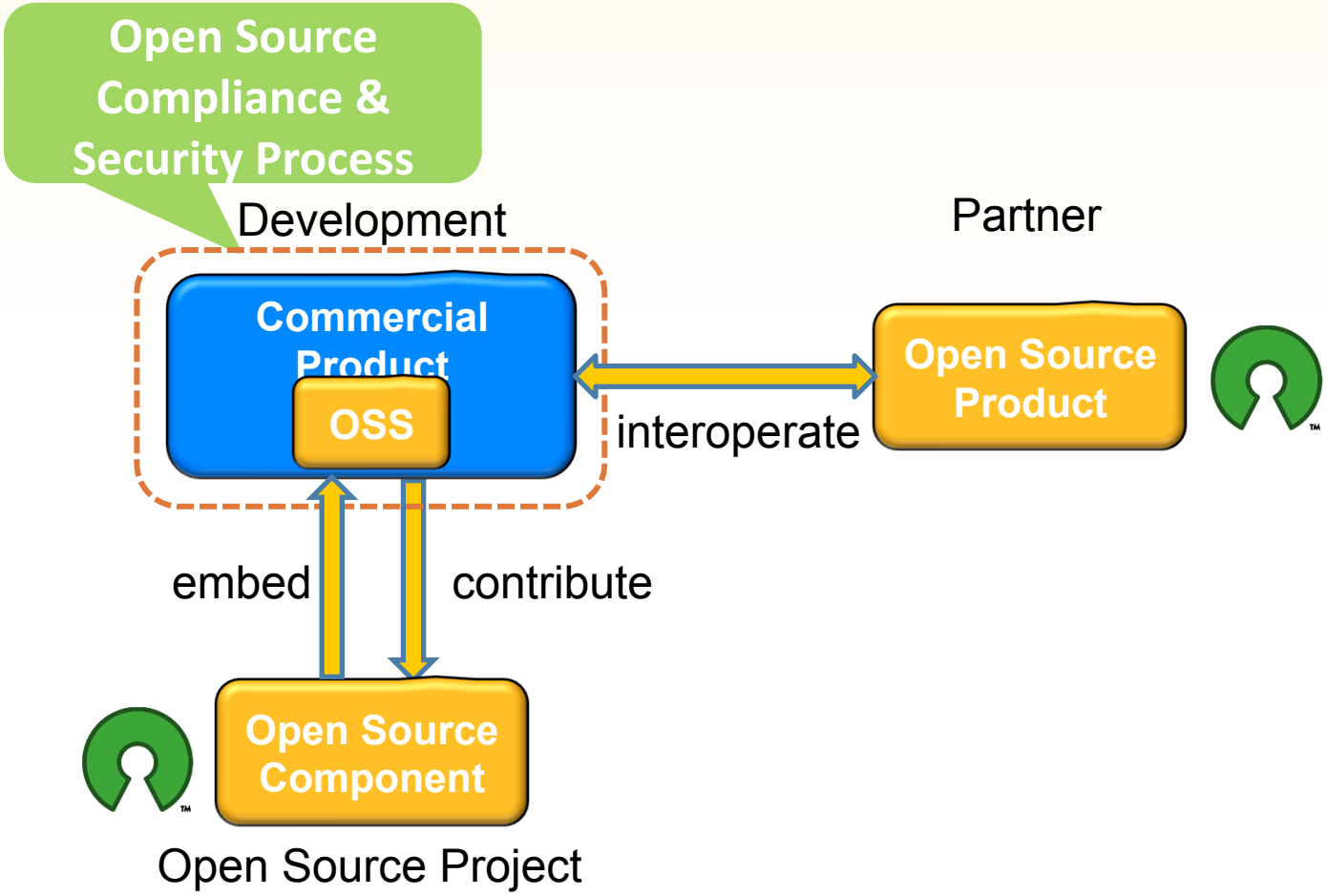
Open Source Security Nightmares And Silver Bullets

Dr. Gunter Bitz, MBA, CISSP, CPSSE
SAP China / Quality Governance and Production

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

- Open Source Usage in Commercial Software
- Legal Risks with Using Open Source
- Security Risks in Open Source Software
- Silver Bullets:
  - Shield Open Source components
  - Integration of Security and Compliance in Software Development Lifecycle
  - Open Source Approval Workflow
  - Security Test Methods
  - Security Response Process for OSS

Overview: Open Source Usage in Commercial Software



Legal Risks with Using Open Source

- Open Source Software (OSS) with Different License Agreements
  - Permissive: Apache, BSD, MIT
  - Copyleft / Viral: GPL, LGPL
- Obligations of Copyleft agreements
  - Publish source code of modifications and derivative work
  - Same license terms apply to any derivative work
- Remediation
  - Comply to agreements
  - Remove infringing code
- Lawsuits for neglecting the agreements: Busy Box

Westinghouse to pay US$ 90,000 in damages for violating GPL terms

RSA CONFERENCE CHINA 2012

TECHNOLOGY LAB / INFORMATION TECHNOLOGY

BusyBox takes out bankrupt opponent in GPL lawsuit

A software developer has convinced a court that an electronics manufacturer …

by **John Timmer** - Aug 6 2010, 2:25am -800

23

The person behind a set of GPL-licensed Unix utilities called BusyBox has been engaged in a lawsuit against a dozen consumer electronics companies, accusing them of violating his copyright. The companies allegedly have been distributing hardware (including HDTVs) that includes BusyBox, but then licensing it to consumers under GPL-incompatible terms.

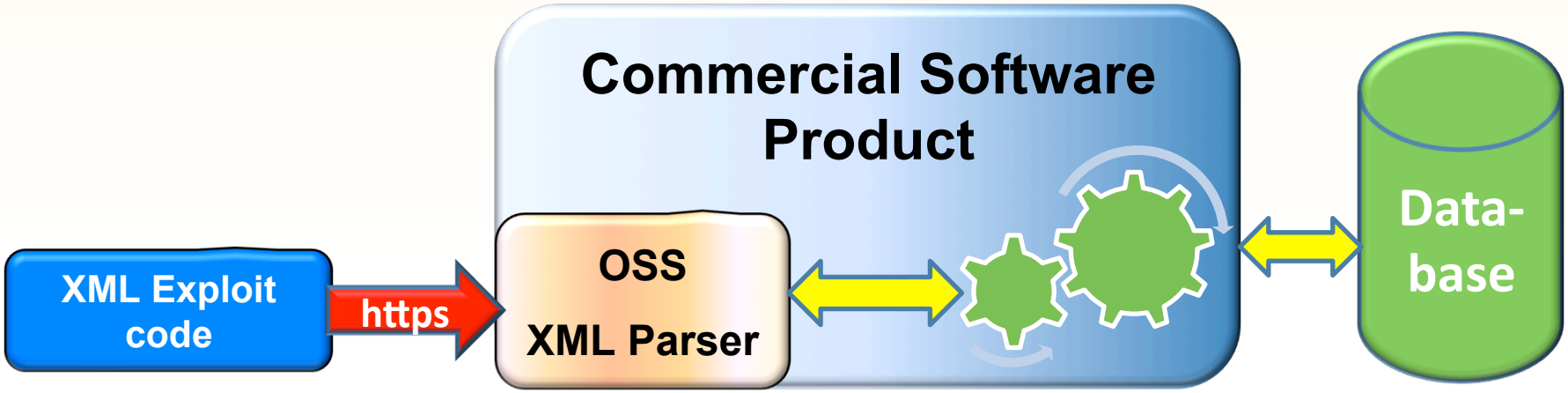
In late July, the judge in the case issued a summary judgement against one of the defendants, Westinghouse Digital Electronics, which stopped participating in the case when it entered bankruptcy protection. The ruling isn't a sweeping victory for the GPL, but it does show that the GPL is compatible with the standards for summary judgement.

Source: http://arstechnica.com/information-technology/2010/08/court-rules-gpl-part-of-a-well-pleaded-case/

Security Risks in Open Source Software

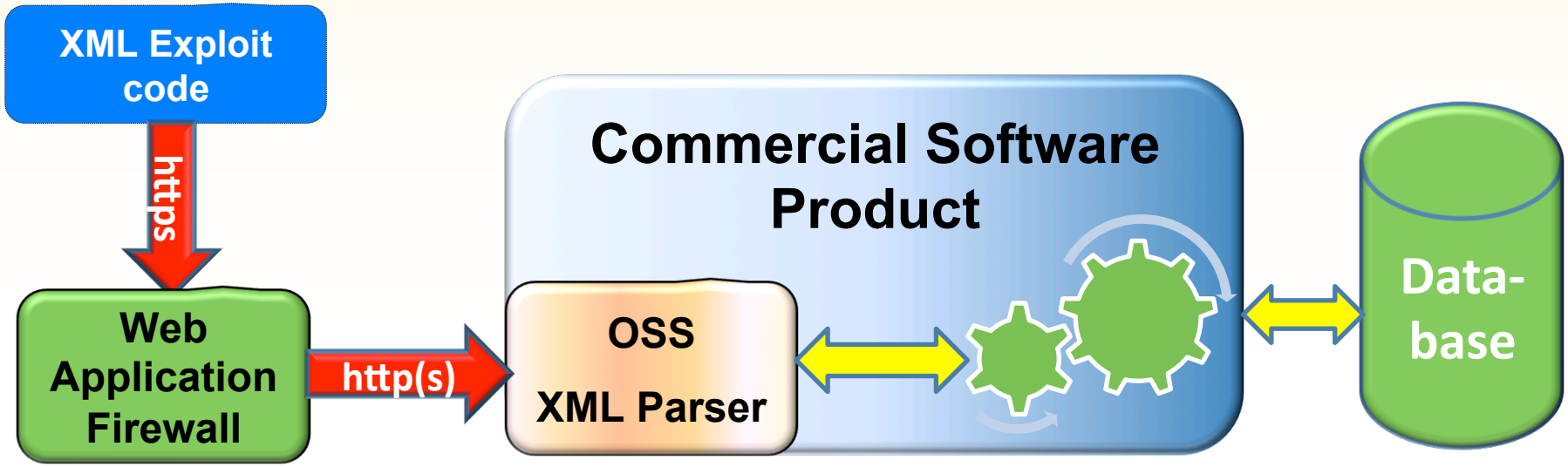
- Is Open Source Software more or less secure?
- Depends on a number of factors:
  - Strong or weak governance regarding code changes?
  - Project team actively testing for security?
  - Usage of 3rd party black-box or white-box testing tools
  - Security Response Process established?
  - Size of the active developer community
  - Project team still active // No updates published for long time
  - Size of the user community (who can report bugs)

Whom to blame ?



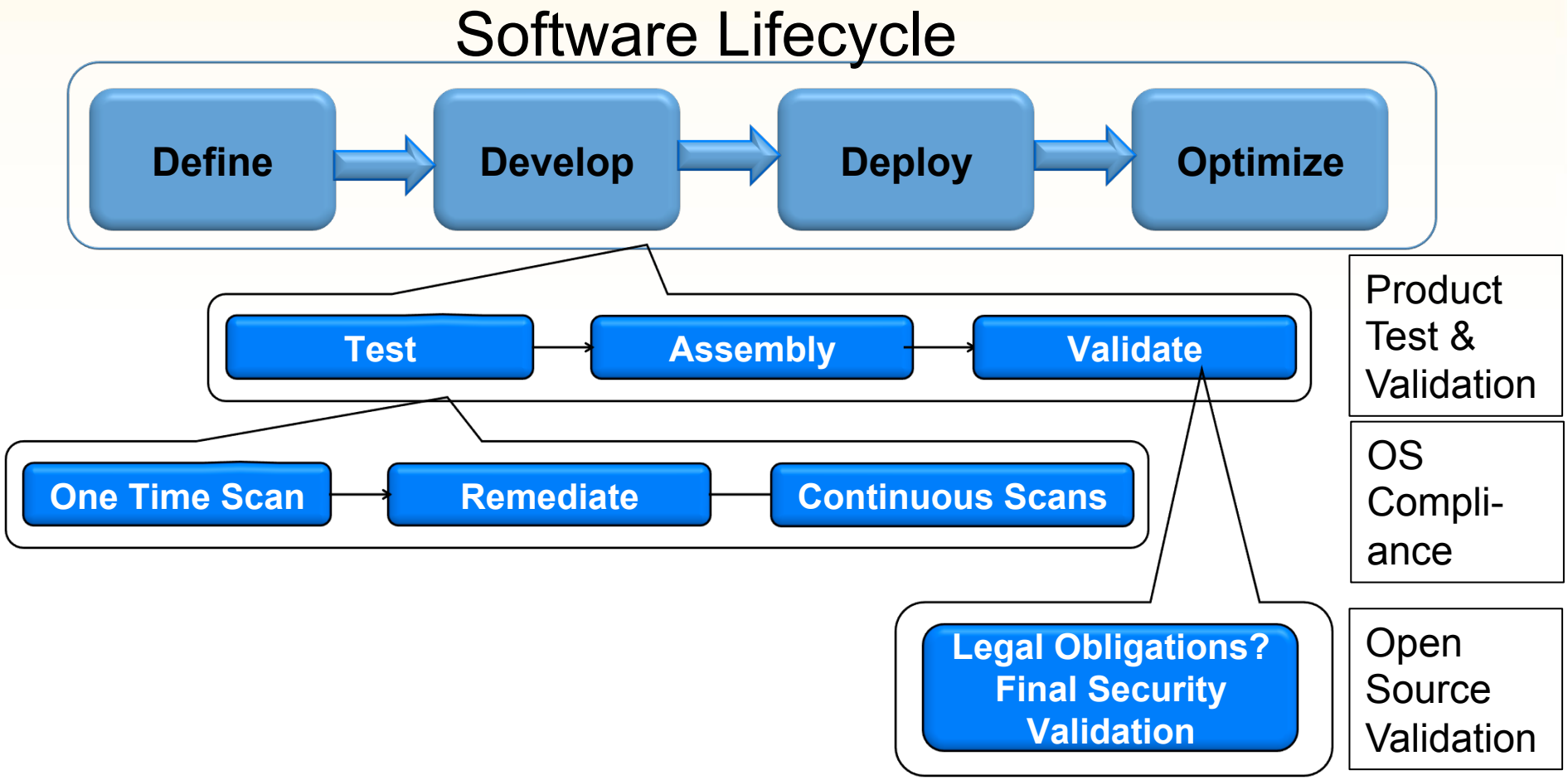
- Open Source Software Developer does not assume responsibility for Security
- “Problem” will stick with vendor of Commercial Software Product

Silver Bullet 1:
Shield Open Source components

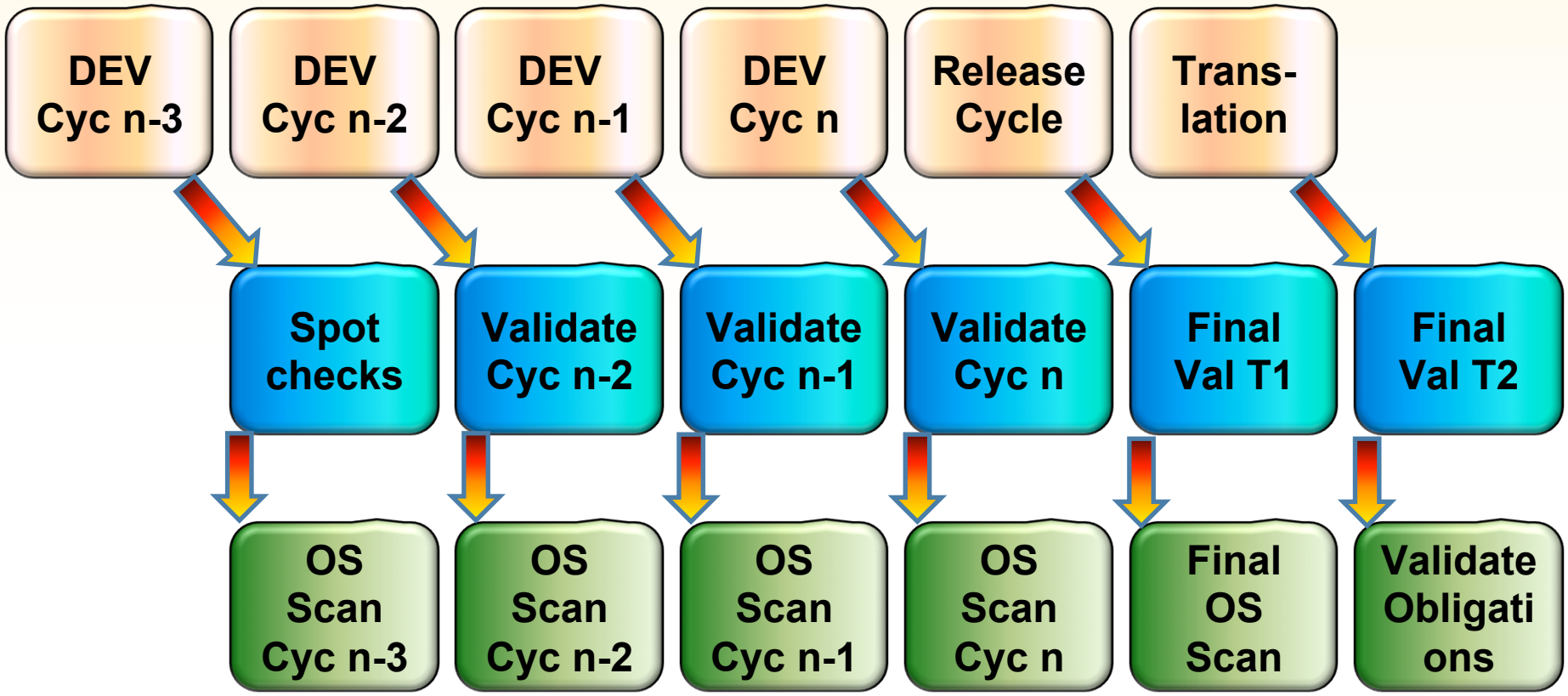


- Scenario with additional Web Application Firewall to block malicious requests
- Can the Firewall filter all possible attack vectors?

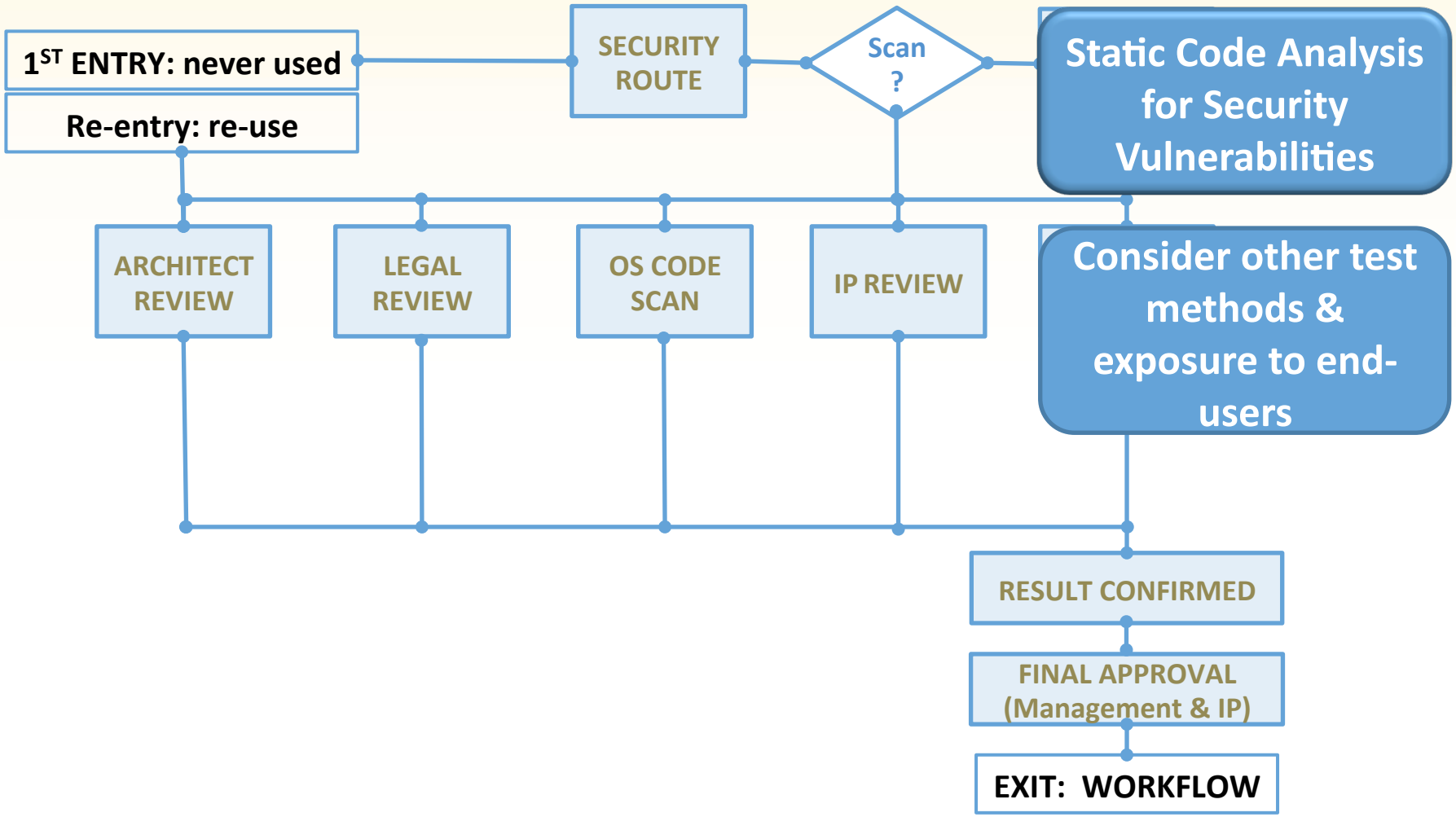
Silver Bullet 2: Integration of Security and Compliance in Development Lifecycle



Integration in case of Agile Software Development



Silver Bullet 3:
Open Source Approval Workflow



Silver Bullet 4: Security Test Methods

RSA CONFERENCE CHINA 2012

- Static Source Code Analysis "Code Scan"
  - High number of false positives
  - Results very difficult to interpret for Server Code (e.g. web server, application server)
- Code Review – practically impossible for large applications
- Fuzzing
  - Experts required to runs tests
  - Code coverage not always optimal
- Manual penetration testing
  - Very precise results
  - Code coverage depends on available budget
- Automated penetration testing
  - Precise results
  - Code coverage not always optimal

Stand alone or Integrated

Stand alone

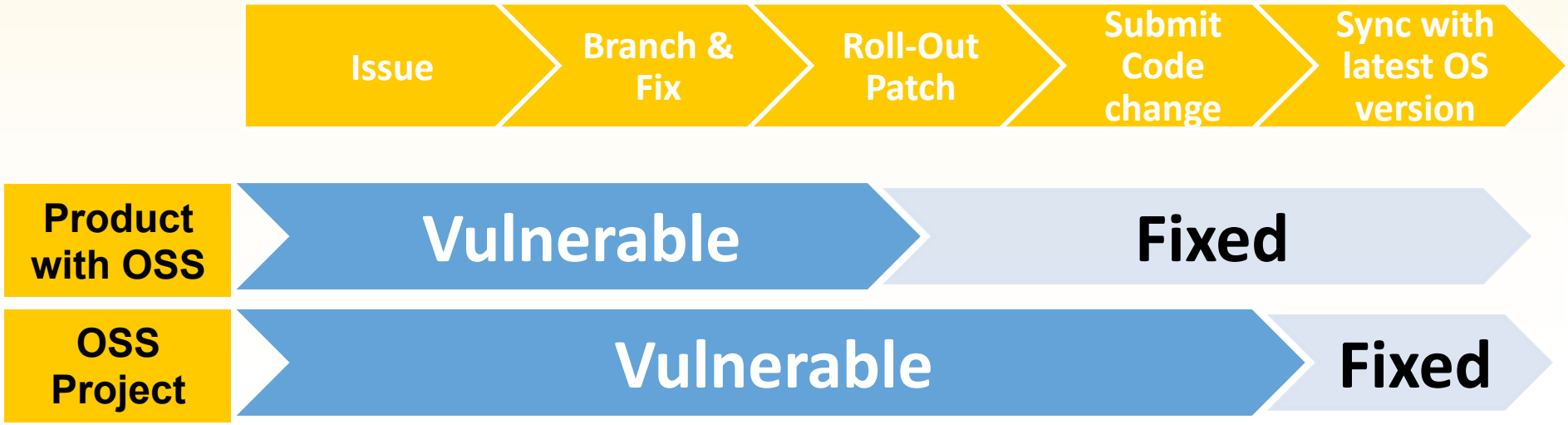
Integrated

Silver Bullet 5: Security Response Process for OSS

- Dedicated In-house owner for each Open Source Software Component
  - 1 owner for multiple product groups using same OSS component
  - Owner is responsible for maintenance of OSS component
  - Owner receives all requests for bug fixing
- Monitoring of public sources
  - Anything found here create a request for bug fixing
  - CVE / MITRE
  - SANS
  - CERT / CC
  - Security Focus (Bug Traq)
  - NVD – (US National Vulnerability Database)
  - Project website, and many more

Security Response Process for Open Source Software

RSA CONFERENCE CHINA 2012



- Security Issue is fixed first in commercial product code
  - Prevents liability issues with customers
- Submit code to Open Source Community to share knowledge
- Roll-in of patched Open Source Software component
  - Reduce effort in case the OSS component shall be upgraded in future

Summary

- Legal risks should be considered prior to using Open Source Software
- Security of Open Source Software depends largely on the maturity of the OS project team
  - No guarantee that it is better or worse than in-house developed
- Inbound Open Source Governance process required to control intake of Open Source Software
- Integration of Security Testing in Development Lifecycle is essential
  - Also works for agile software development process
- Security Response Process must as well cover Open Source Software

Thank You !

Gunter Bitz, SAP
gunter.bitz “at” sap.com

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012