

Moving from Product Lessons Learned to Benchmarking

Software Assurance (SwA) Forum
Software Supply Chain Risk Management
11 March 2010

VERACODE

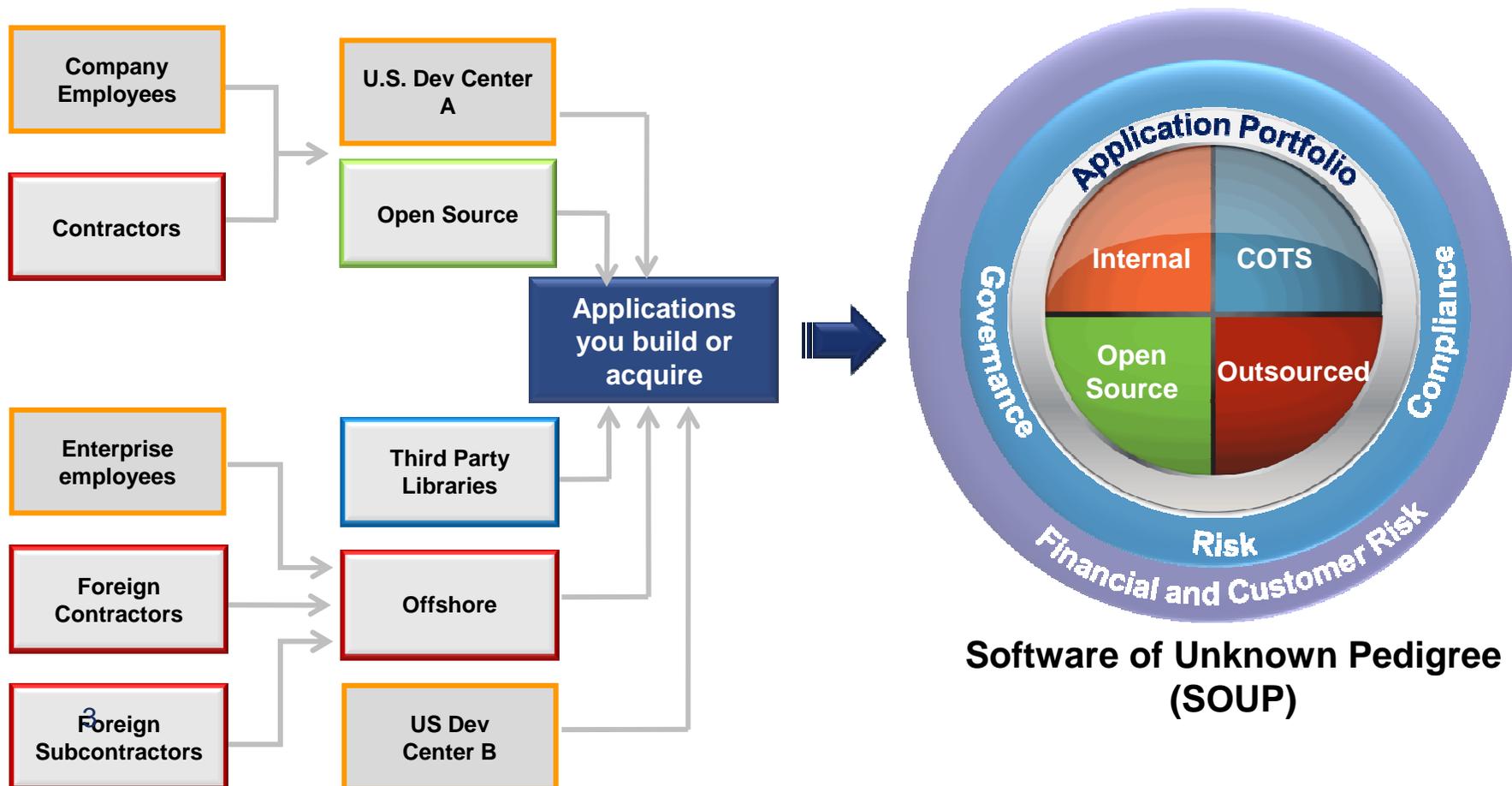
Chris Wysopal
CTO and Founder
cwysopal@veracode.com

Agenda

- **The vulnerability supply chain**
- **Static analysis for 3rd party code**
- **Acceptance testing process**
 - Scan
 - Remediate and/or mitigate
 - 3rd party validation
 - Publish report to purchaser

Vulnerability Supply Chain

- Enterprise application portfolio comprised of software derived from multiple heterogeneous sources
- Need to secure third-party libraries, components and open source code that makes it way into the compiled code during the SDLC



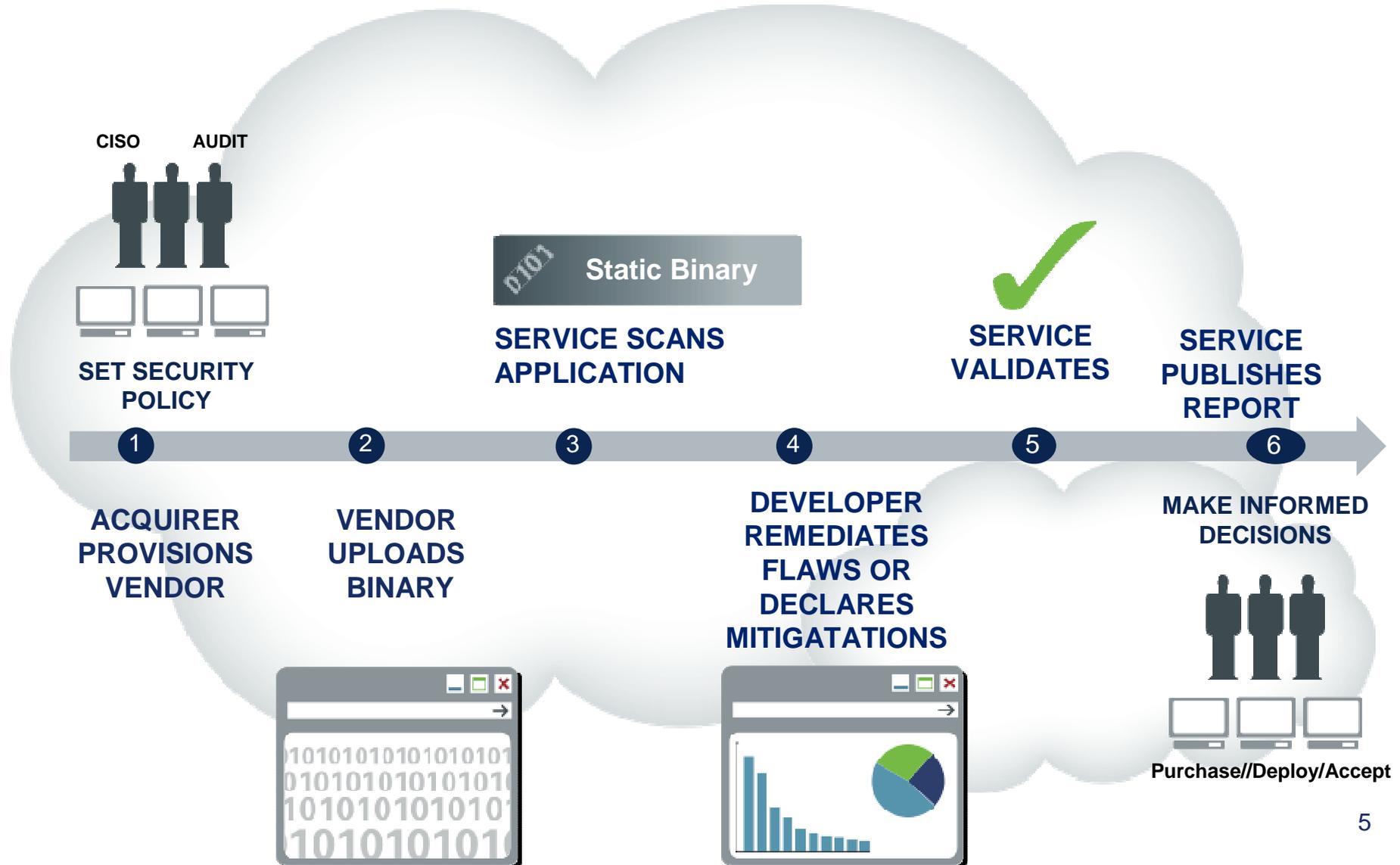
Static Analysis for 3rd party Software Assurance

Technology

- **Static binary modeling & analysis**
 - Binary modeling can analyze 100% of the final application
 - Includes analysis of libraries with inter-procedural flows
 - Both internal and external use cases (internal code; vendor code; mergers & acquisitions).

- **Vulnerability, backdoor and data exfiltration scans**
 - Scan for most commonly exploited vulnerabilities: buffer overflow, SQL Injection
 - Scan for backdoors such as hard-coded passwords, IPs
 - Map sensitive data and look for data exfiltration through network

3rd Party Acceptance Testing Service



Remediation & Declaring Mitigations

- **Static analysis has limitations for software security that must be overcome with manual process**
 - Static analysis has no visibility into environmental controls
 - Static analysis has false positives
- **Developer reviews output of static analysis and can either:**
 1. Remediate flaw
 2. Declare a mitigation: OS control, Network control, design control
 3. Claim a false positive
- **Testing service verifies**
- **Final report contains mitigation declaration**

Publish Report

- **Report contains only summary information, no detailed vulnerability information**
 - Counts of flaws by severity
 - Examples of highest categories of risk
- **Modules and versions scanned**
- **Declared mitigations**
- **Customer can make acceptance decision**
- **Vendors that have achieved an acceptable rating can display VerAfied mark.**



Example of VerAfied mark for SaaS



Honest financial guidance for everyone.

We find your money's potential and help you realize it.

Join and Get Ahead >

Navigation

- Home
- What We Do
- Give Hope
- Partner Prospects
- Who We Are
- Sitemap

Find Better Bank Products

- Earn Free Money
- Realistic Savings Ideas
- Local Information
- Keep an Eye on Your Bank

Make More with What You Have

- Save for College
- Buy a Home
- Save for Retirement
- Reduce Debt Safely
- Create a Financial Plan
- Automatically Track Your Goals
- Expert Guidance

Your Personal Money Manager

- Organization in Seconds
- Money Monitoring
- Avoid Bank Fees
- Create and Track a Budget
- Secure Your Money

Give Hope

- Community Partners



Link back to Veracode's website



HelloWallet

Company:	HelloWallet
Application Name:	HelloWallet.com
Assessment Technique(s):	Static Binary Analysis, Manual Application Penetration Testing
Assurance Level:	AL3 (Medium) Applications connected to the internet that process financial or private customer information
Issue Date:	03/02/2010
Application Description:	HelloWallet is a self-service website that helps users identify their financial goals while providing real-time comparisons of available checking, savings, and loan products. View Details



In its reviewed state, the [HelloWallet](#) application met or exceeded the security score outlined in the [Veracode Risk Adjusted Verification Methodology](#) for an application at the assurance level specified above. Veracode's risk adjusted verification methodology is based on respected industry standards including MITRE's [Common Weakness Enumeration \(CWE\)](#) for classification of software weaknesses and FIRST's [Common Vulnerability Scoring System \(CVSS\)](#) for severity and ease of exploitability and NIST's definitions of assurance levels.