



3rd Party Application Analysis: Best Practices and Lessons Learned

Chris Wysopal
Founder and CTO
Veracode

Agenda

- ❑ About Veracode
- ❑ Need for 3rd Party Analysis
- ❑ Terminology
- ❑ Sample Size/Success Rates
- ❑ Challenges
- ❑ Best Practices
- ❑ Lessons Learned
- ❑ Government Requests
- ❑ The Future of 3rd Party Analysis

About VERACODE

- ✓ Perform automated application security assessments
- ✓ Operate in a SaaS model
- ✓ Assessment techniques include
 - ✓ Static binary analysis
 - ✓ Dynamic analysis
 - ✓ Manual analysis
- ✓ More information available at www.veracode.com

Need for 3rd Party Analysis

Question:

Who would release a product riddled with security problems simply to make money?

Answer:

Pretty much every vendor out there.

- Andrew Hay, Senior Security Analyst



Need for 3rd Party Analysis

“33% of Veracode assessed applications are identified as created by a 3rd Party”

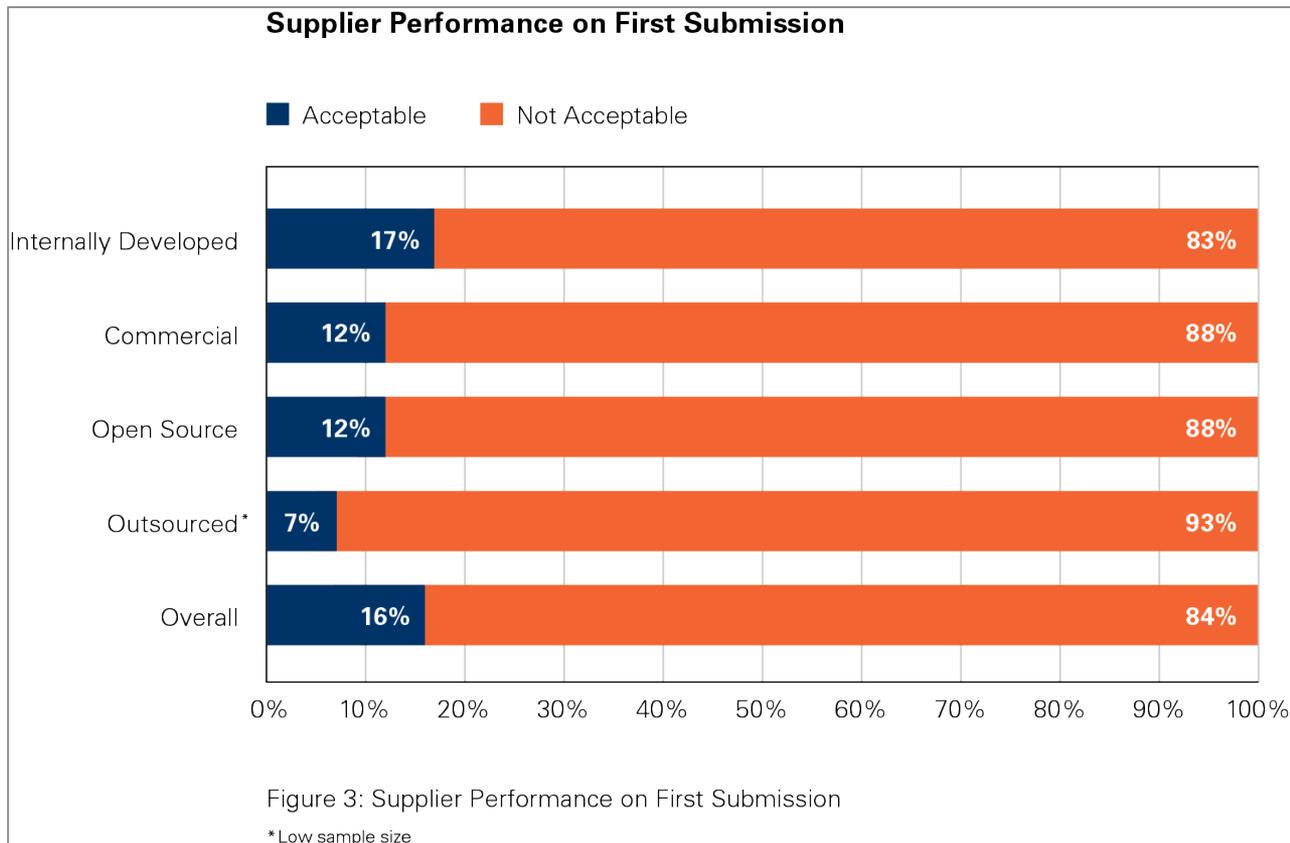
- Veracode State of Software Security Volume 4*

“Up to 70% of internally developed code originates outside of the development team”

- Veracode State of Software Security Volume 4*

* Veracode State of Software Security Report Volume 4 is available here : <https://info.veracode.com/state-of-software-security-report-volume4.html>

Need for 3rd Party Analysis



Source: Veracode State of Software Security Report Vol. 4

Terminology

- ❖ **Enterprise** – Purchaser of the software requesting analysis
- ❖ **Vendor** – Producer and IP owner of software being analyzed
 - ISV
 - COTS
 - GOTS
 - Open Source Software
- ❖ **3rd Party Analysis (Dual Meaning)**
 - 3rd Party Supplier – The creator of purchased software (aka Vendor)
 - 3rd Party Analyzer - Independent party performing analysis (Veracode, pen testers, auditors, etc)

The Data

- Request from 62 separate enterprises across 470 distinct vendors
- 1,396 static scans completed
- 336 dynamic scans completed
- 81% overall success rate
- ~92% success rate when enterprises follow best practices

Challenges

❖ Enterprise

- Vendor Outreach/B2B Relationship
- Timelines/Remediation Expectations
- Product Specifics (Version, scope, etc)

Challenges

❖ **Vendor**

○ IP Protection

○ Timelines

Challenges

❖ Analysis Team

- Technologically Capable
- Cooperative Enterprise and Vendors

Best Practices



Best Practices

❖ Guiding Principles

- Enterprises Have All The Leverage
- Basic Project Management Goes A Long Way

❖ Best Practices

- Policy Definition
- B2B Interactions
- Vendor Education
- Results Communication



Best Practices

❖ Policy Definition

- Define Business Goals
- Set Analysis Expectations
- Determine Exception Process

❖ B2B Interactions

- Initial contact from Enterprise to Vendor
- Enterprise Introduction of Analysis Team



Best Practices

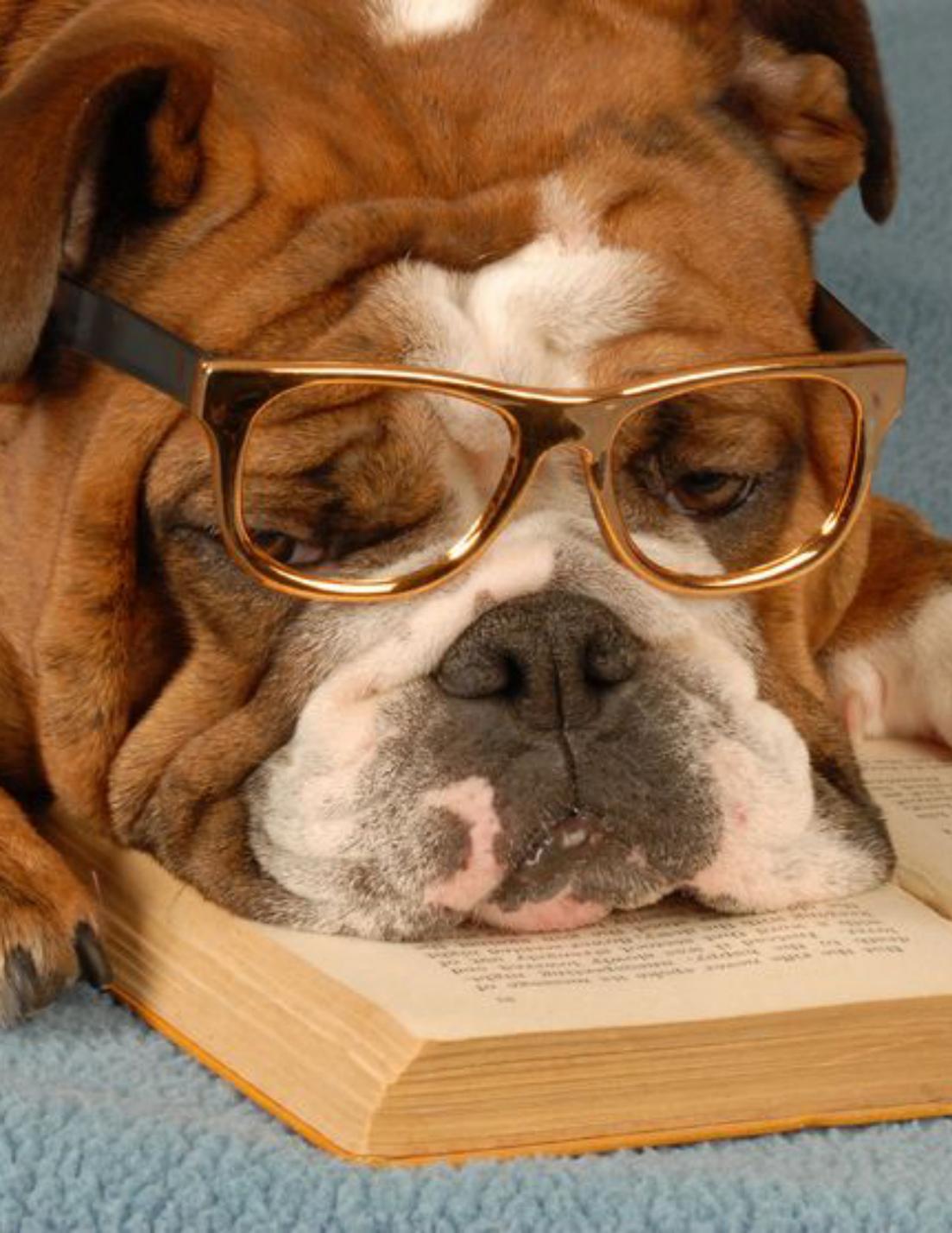
❖ Vendor Education

- 3 Way Kickoff Call is Critical
- Process Transparency/Documentation Increases Productivity
- Aim for Verbal Vendor Commitment to Enterprise

❖ Results Communication

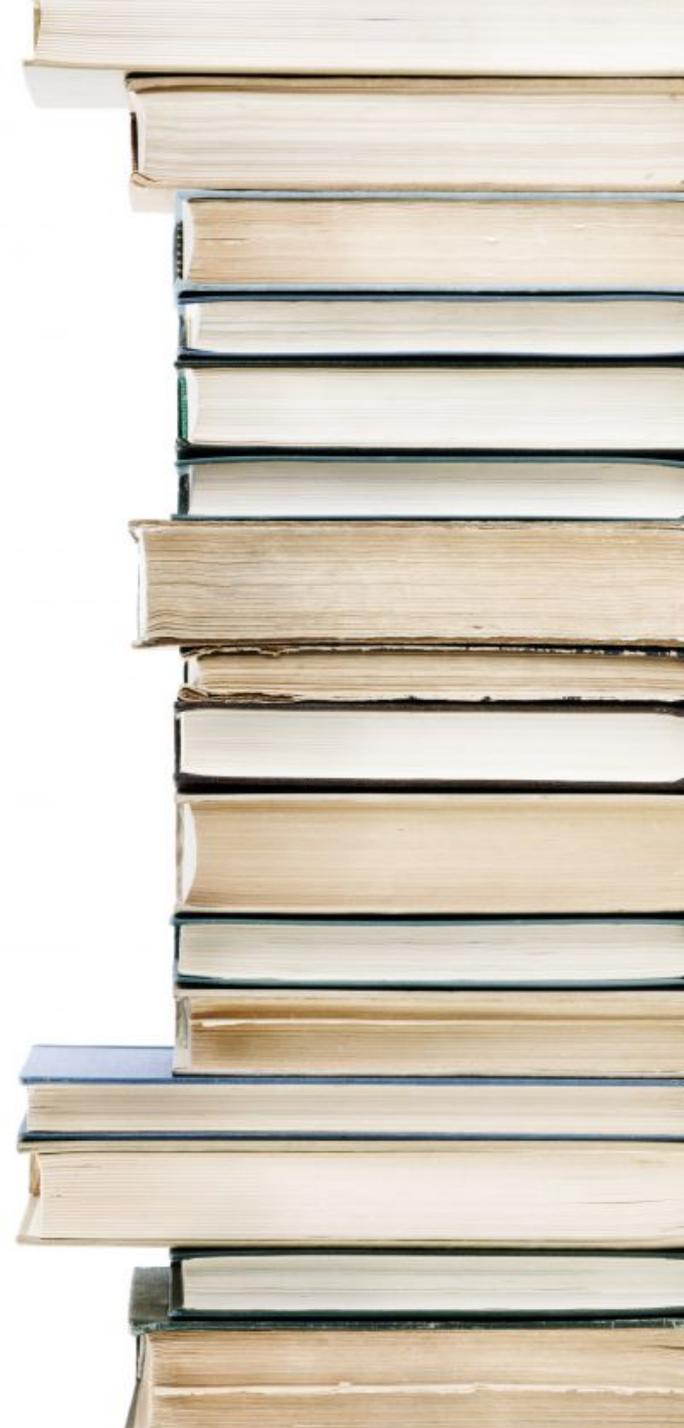
- Vendor Participation Hinges on Protecting IP
- Limit Disclosure of Details to Enterprise
- Full Result Sets to Vendor Team
- Provide Vendor Ability to Review, Learn and Comment





Lessons Learned

Government Requests



Limited Government Requests

- ❖ Numerous Discussions w/
Government Agencies
- ❖ < 5 Government Agencies
Analyzing Externally Developed
Software
- ❖ Limited Internal Drive
- ❖ Inconsistent Vendor Response



Limited Government Requests

❖ Why?

- Strict Contractual Requirements
- Expectations Not Proactively Set
- Limited Government Leverage
Cooperation After Contract is Signed



Limited Government Requests

❖ What To Do?

- Set Expectations During Evaluations
- Contractually Require Security Testing
- Determine Specific Security Policies and Requirements Vendors Must Meet



NIST SP 800-53 Rev. 4

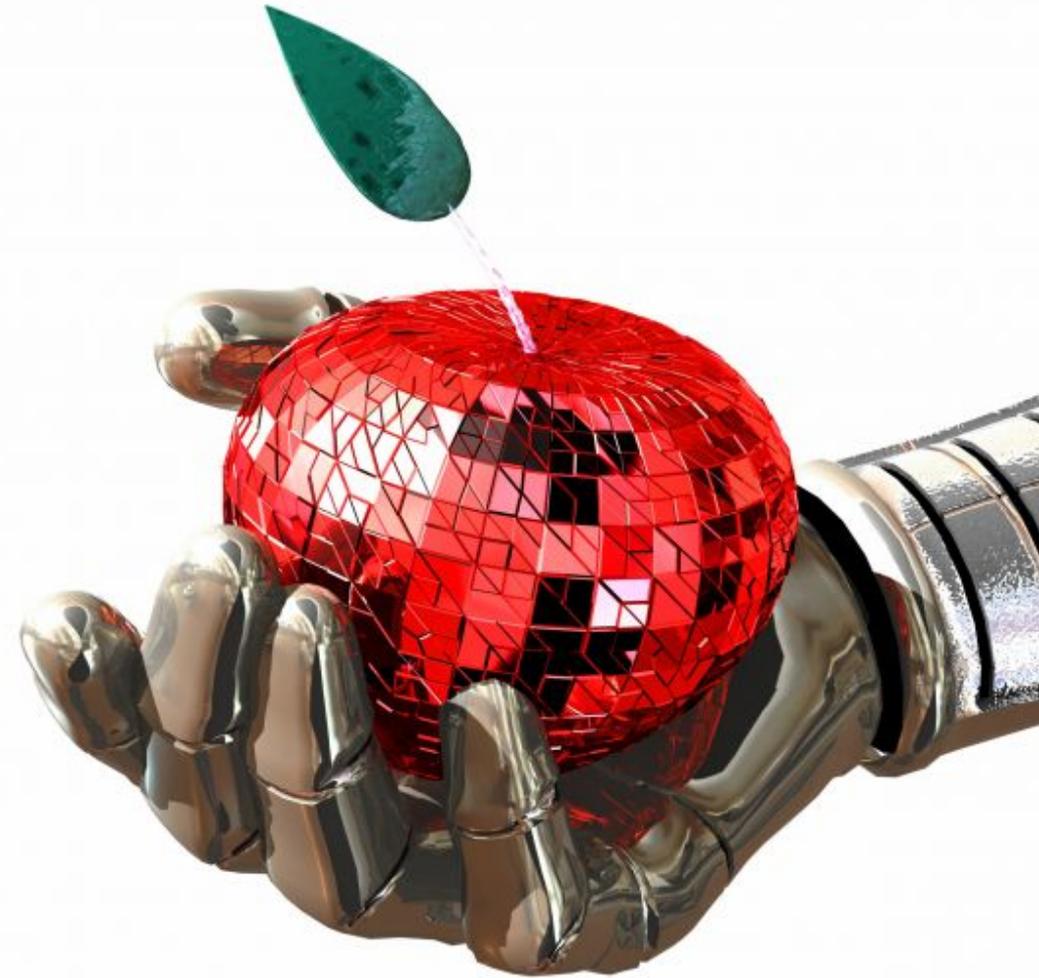
SA-12 Supply Chain Protection

[high]

The organization protects against supply chain threats by employing organization-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.

SA-12.7 Assessments Prior to Selection / Acceptance / Update

- ✓ The organization conducts assessments of [Assignment: organization-defined information systems, system components, information technology products, or information system services] prior to selection, acceptance, or update.
- ✓ Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malware, malicious processes, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by organizations.
- ✓ Prepare: Build security acceptance testing into acquisition process. Train staff or hire a service provider to perform this testing.



The Future of 3rd Party Analysis

The Future: Expectations

Past:

- ✓ Manual assessments
- ✓ Performed after deployment
- ✓ No contractual obligations

Present:

- ✓ Manual and automated assessments
- ✓ Performed during or after deployment
- ✓ Some contractual obligations, mostly handshake obligations

Future:

- ✓ Manual and automated assessments
- ✓ Analysis expected as part of SDLC
- ✓ Contractual requirements with documented expectations

The Future: Cost Coverage

Past:

- ✓ Enterprises pay for cost of manual analysis
- ✓ Focus on deployed, high risk applications

Present:

- ✓ Enterprises pay for cost of manual, static and dynamic analysis
- ✓ Focus on deployed/soon-to-be-deployed, high risk applications

Future:

- ✓ Enterprises expect testing to be part of SDLC
- ✓ Costs to be covered by software providers
- ✓ Focus on applications pre-purchase

The Future: Recommendations

Enterprises

- ✓ Determine internal policy
 - ✓ Flaws to be addressed
 - ✓ Acceptable testing procedures/providers
- ✓ Communicate policies with vendors
- ✓ Provide several analysis options

Vendors

- ✓ Understand current and future enterprise requirements
- ✓ Investigate available services, capabilities and cost structures
- ✓ BE PROACTIVE!

Need More Info?

❖ Veracode has a dedicated 3rd party team

3rdPartySupport@veracode.com

<http://www.veracode.com/3rdParty>



Questions?

