



Continued funding of SDLC MetriCon 8

Mahesh Saptarshi

Technical Director, Product Security Group

SDLC – Purpose

- Secure Design
- Secure implementation
- Security QA
- Secure deployment

.... So that when the application is deployed
It doesn't make the security worse

Software security – Challenges

- Funding and commitment
- Justifying funding priorities
- Differentiation – between product versions and between competing products
 - ROI/Cost Benefit
- Assurance/comparison of 3rd party components/products
 - External dependencies and 3rd Party software
 - OWASP top-N list candidate
 - Security assurance for integrated systems
- Third party verification

Software security – Attributes of the Metrics

- One metric will not work
 - Single metric hides important information
- Effort based metric is required
 - SDLC is a process
- Metrics should be strongly correlated to spending
 - Predictive results
- Qualitative metrics are OK
 - Ordering must be possible

Software security Metrics - Proposal

1. Results of tool based analysis
 - Static source code scanning tools
 - Vulnerability scanning tools
 - Pen-testing tools
2. SDLC activity priority list coverage
 - Person-hour spent on SDLC activities
 - SAFECODE/BSIMM/some such
3. Measure of Initial quality – lagging indicator
 - Vulnerabilities found in 1st year of product release
 - Including vulnerabilities in 3rd party components
 - Time to “first Service Pack”

Software security Metrics – Other options

- Ratio of outstanding issues to reported issues
- How long the product withstands attacks through tools or human effort
- Code coverage through the tools based analysis
- Number of entry points covered by tools
- Level of compliance for specific standards
- Mean time to first exploit
- Any other proxy metrics?



Thank you!

Mahesh Saptarshi

Mahesh_saptarshi@symantec.com

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.