Quality and Software Assurance

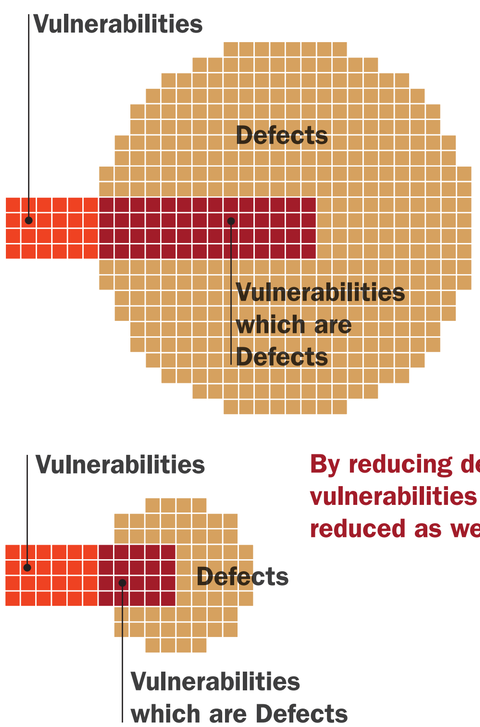
Vulnerabilities are Defects

Literature Review: Vulnerabilities are 1-5% of defects Analysis of defects for five versions of Microsoft windows operating systems and two versions of Red Hat Linux systems) (Alhazmi, et.al., 2007)

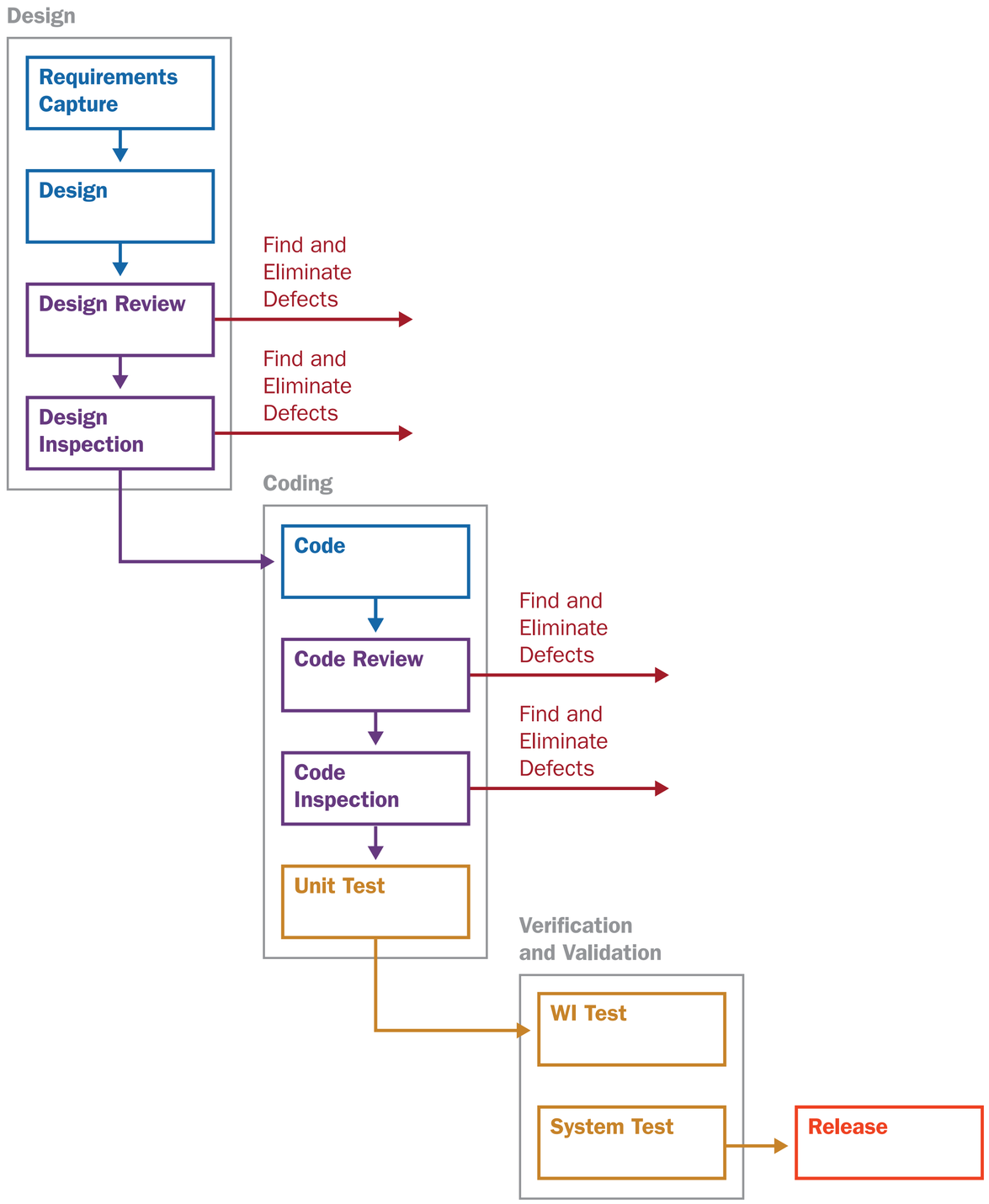
Win 95 (14.5 MLOC) and Win 98 (18 MLOC) vulnerabilities are 1.00% and 0.84% respectively of identified defects

Red Hat Linux 6.2 (1.8 MLOC) and 7.1 (6.4 MLOC) vulnerabilities are 5.63% and 4.34% respectively of identified defects. Tom Longstaff asserted that vulnerabilities might represent 5% of total defects (http://research.microsoft.com/en-us/um/redmond/events/swsecinstitute/slides/longstaff.pdf)

Ross Anderson: “it's reasonable to expect a 35,000,000 line program like Windows 2000 to have 1,000,000 bugs, only 1% of them are security-critical.” (Anderson, 2001) Experiment: Evaluating an open source product to test predictions



Workflow for Quality and Software Assurance

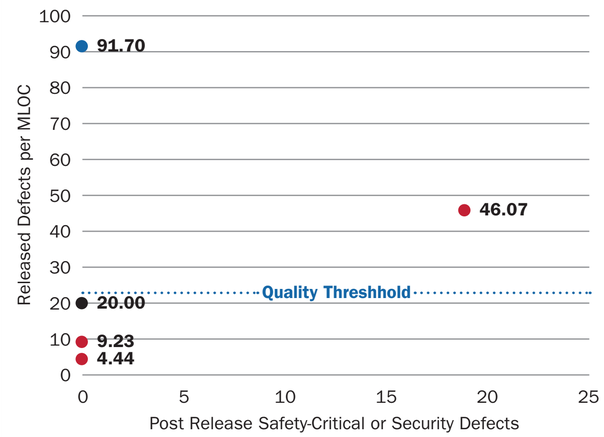


Can Predictions of Quality Inform Security Risk Predictions?

The SEI has quality data for over 100 Team Software Process (TSP) development projects used to predict operational quality.

Data from five projects with low defect density in system testing reported very low or zero safety critical and security defects in production use.

HYPOTHESIS: A sufficiently low level of defects measured in test and production will reasonably predict very low risk of escaped safety critical or security vulnerabilities



Contact: Carol Woody cwoody@cert.org