Software Assurance Metrics

TASC Insight Applied

Steve Winterfeld
DCG CTO and TASC Cyber Tech Dir
Sept 2012

TASC
INSIGHT APPLIED

© 2012 TASC, Inc.

Define what we looking for

- DoD says Software Assurance is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software
- NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project says software assurance is "the planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures to help achieve:
  - Trustworthiness - No exploitable vulnerabilities exist, either of malicious or unintentional origin, and
  - Predictable Execution - Justifiable confidence that software, when executed, functions as intended."

What should metrics do?

- Support a decision (real time)
- There should be benchmarking and artifacts (Quantified vs Qualified)
- Determine if security is both efficient and effective
- Measure (behavior, infrastructure) = Dashboard / Scorecard
- Need to understand intent – value delivery / process improvement / decision support = meaningful
- Link Cybersecurity to business value propositions (ROI)

At the end of the day metrics should be Specific, Measurable, Attainable, Repeatable, and Time-dependent (SMART)

Auditing

- Audits are the regular, structured evaluation of an enterprise's cyber systems, software, and processes.
- The audit process represents the measurement step in a continuous Cybersecurity improvement program.
- Cyber audits are often subset of other accounting requirements or based on compliance standards.
- Today most cyber audits are manual and labor intensive, the trend needs to move to real time auditing via automation.
- This is the tool that will detect insider threats and the threat that has gotten inside.

Programs

- NIST: Software Assurance Metrics and Tool Evaluation (SAMATE)
  - NIST Special Publication 500-268 v1.1
  - NIST Special publication 500-270
- NIST: Security Content Automation Protocol (SCAP)
- DHS: Build Security In
- DHS: Software Assurance Curriculum Project
- MITRE (making security measurable):
  - Common Weakness Scoring System (CWSS™)
  - Common Weakness Risk Analysis Framework (CWRAF™)
  - Common Weakness Enumeration (CWE™) List
  - Requirements and Recommendations for CWE Compatibility and CWE Effectiveness
  - Common Vulnerabilities and Exposures (CVE®) List

Best practices (tactical)

- CWE/SANS 25 most common problems
- Open Web Application Security Project (OWASP) top 10
- Tools for static program analysis ([edit] Multi-language / Language-specific / Methodologies) [HP and IBM]
- Testing (security vs performance)
- Bug count – bounties
- Scorecards

Gartner: Dynamic application security testing (DAST) report says the by 2016, 40% of enterprises will make proof of independent security testing a precondition for using any type of cloud service.

Metrics

- Metrics are the key to enable decisions on how to best protect, react and invest for Cybersecurity. There has been a lot of work done, but there is no clear set of industry standard cyber metrics today. There are three basic categories of metrics to consider:
  - **Technical:** Based on tactical statistics.
  - **Security:** Cost-based analysis on benefits from implementing new technology or policies. Goals must be set to track performance are established.
  - **Risk Posture:** Analysis on impact of cyber exploits to enterprise and operations.

Next steps

- Differentiate between auditing and metrics
- Develop metrics that drive decisions around risk posture
  - Understand what decisions are made at each level
    - Development
      - Coders
      - Program managers
      - Leadership
    - Customers
      - Users
      - Acquisition staff
      - Senior Leaders

TASC

INSIGHT APPLIED