Software Sustainment

Ms. Jennifer Zbozny

25 May 2017
Ensuring Sustainable Readiness

Everything has software

Everything is connected

Exponential Software Growth in Army Systems

The Human Factor on the Security and Quality of Software Impacts Cyber Readiness

18.5 Million Software Developers
  • 11.5 Million Professional
  • 7 Million Hobbyists

IDC - 2014 Worldwide software developer and ICT-Skilled Worker Estimates

Bad Actors State, Non-State, and Insiders In Our Software Supply Chain

Embedded Security Vulnerabilities
Electronic IAVA Patching

Providing the Army the ability to push software security patches over the network with automatic compliance tracking.

- **Current Status**
  - Successfully executed electronic patching proof of concept in high bandwidth environment
  - Electronic patching available on 6 tactical Programs of Record
  - Expanding to additional systems as aggressively as possible
  - Implemented at Fort Bragg, JBLM, Fort Hood, Germany (66th MI)

- **EXORD**
  - Co-authored by CECOM and ASA(ALT)
  - Socialized with PEOs
  - Socializing with ASCCs, ARCYBER, FORSCOM, HQDA
  - Expecting Army G-3 EXORD publication

- **Microsoft System Center Configuration Manager (SCCM) Test**
  - Testing low bandwidth tactical environment
  - Simulating multiple network tolerances
Software Assurance leverages COTS and GOTS tools to find cyber and quality code defects BEFORE testing or fielding.

- Source code from developers
- Raw findings from suite of tools
- Human analysis of findings
- Actionable reports for developers and executives
- Code DX correlation framework

Mapping of findings to requirements from DISA Application Security and Development STIG

- DISA STIG
- CAT I
- STIG ID
- CAT II
- STIG ID
- CAT III
- STIG ID

Repository of data to show trends of security posture

- STIG ID
- STIG ID
- STIG ID

- CAT I
- CAT II
- CAT III

Graph showing trends over revisions (Rev1, Rev2, Rev3, Rev4):
Software assurance performance will become a gate for transitioning software to sustainment.

**DoDI 5000.02** Change 2, February 2017, “Operation of the Defense Acquisition System” requires acquisition programs to:

- Include software assurance in contract requirements
- Use automated software vulnerability detection and analysis tools
- Ensure risk-based remediation of software vulnerabilities
- Verify software assurance through continued use of tools and testing

As required by section 933 of P.L. 112-239 (NDAA 2013)

**DA PAM 25-2-x** “Software Assurance” to be published in June will provide implementing guidance.
C4ISR Partnering

CECOM is partnering with the PEO/PMs to proactively ensure sustainment is part of program acquisition strategies.

CECOM Acquisition Life Cycle Cell (ALCC) – The LCMC entry and coordination point for material requirements and acquisition forums, document reviews, acquisition policy and related processes to ensure sustainment strategies enable cost effective and robust support.

SEC ALCC Focus:
- Software Architecture
- Technical Data Rights
- COTS/GOTS Strategy
- Use of Software Assurance
- Contracting Strategies
Q&A Discussion