The Challenges of Software Assurance and Supply Chain Risk Management

Carol Woody, PhD

Software Engineering Institute, Carnegie Mellon University

Software supply chain risk has increased exponentially since 2009 and will continue to do so given the current environment.

Identified Criteria	Project	Product	Protection	Policy
Long-Term Support	🟥 Forked Project			🟥 No Security Policy
Dependencies	🟥 74 Abandoned Dependencies	🟥 No Update Tools		
Security		🟥 4 Unfixed Critical Vulnerabilities	🟥 Workflow with Excessive Permissions	
Integrity		🟥 No Fuzz Testing	🟥 30 Unreviewed Change Sets	
Malicious Actors	🟥 Commit ID Known Malicious			
Suitability				🟥 12 Restrictive Licenses

🟥 Red Flag

Realm of Observable Facts of OSS Projects and Products

- **Review data available**
- **Identify useful criteria**
- **Extract key data**
- **Map to acceptable criteria**
- **Evaluate red flags**
- **Identify appropriate mitigations**
- **Confirm supportability**

Measure and baseline what you have, especially open source.

Assess how you are vulnerable and identify an improvement path.

Integrate measurement and monitoring throughout the lifecycle.

THE TWENTY-FOURTH ANNUAL
HIGH CONFIDENCE SOFTWARE AND SYSTEMS CONFERENCE
MAY 6 - 8, 2024 | http://cps-hcss.org