Evolving Secure Development Practices for Protecting Software Supply Chain

2022-09-19 -- NIST DecSecOps Workshop – Industry Panel

Takashi Suzuki, BlackBerry Standards, tsuzuki@blackberry.com
Agenda

- BlackBerry, a software company
- Advocacy for product security
- DevSecOps practices addressing operation risks
- Today’s Challenges
- Use Cases for NCCoE Project
BlackBerry – a Software Company

• Providing technologies enabling the safety and security of devices & systems our customers rely on
• Diverse product portfolio, embracing & practicing DevSecOps approach, securing 500M endpoints
Our Advocacy – Product Security and Software Supply Chain Risks

“Most software today relies on one or more third-party components, yet organizations often have little or no visibility into and understanding of how these software components are developed, integrated, and deployed, as well as the practices used to ensure the components’ security.”

(NCCoE Project Description LL86-89)

– Supply chain risk of OSS and Vulnerability Assessment & Tracking System

– Security review for assessing software readiness


– Securing software supply chain and SBOM
DevSecOps Practices addressing Operational Risks

1. Continuous monitoring
   - Proactive vulnerability search
   - Detect & Respond

2. Impact analysis & Fix
   - Modular & loosely coupled design
   - Traceability

3. Test Plan & Execution

4. Guardrails for deployment decisions

DevSecOps Figure: NSA CISA ODNI "Securing software supply chain – recommended practices guide for developer"
Today’s Challenges

• Sharp rise of CVEs

• Scalable & accurate search for affected products

• Protection against evolving threat landscapes

SBOM Forum: “A Proposal to Operationalize Component Identification for Vulnerability Management”
Use Cases for NCCoE DevSecOps Project

• Securing source repositories and build environment
  – Application of ZTA principles
  – AI powered protection, detection and response tools

• Detecting & remediating known and potential vulnerability
  – Integration of proactive vulnerability management into DevOps
  – Contextualized output from the tools for risk based prioritization and readiness assessment

• SBOM generation & verification
  – Combining and verifying SBOMs
Thank you

© 2021 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.