BlackBerry. Intelligent Security. Everywhere.

Evolving Secure Development Practices for Protecting Software Supply Chain

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

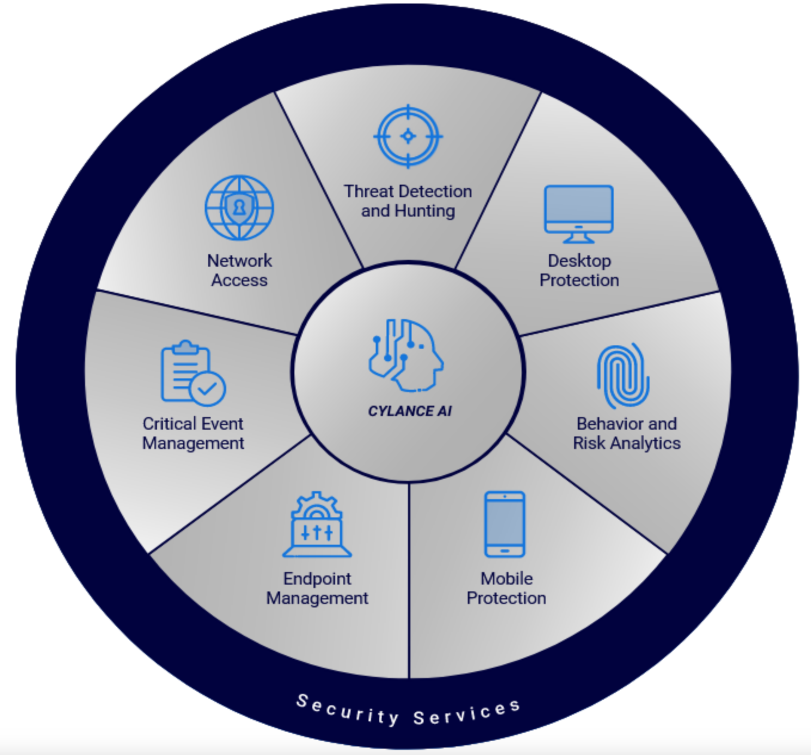
Takashi Suzuki, BlackBerry Standards,
tsuzuki@blackberry.com

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



Cylance Endpoint Cybersecurity

BlackBerry QNX & JARVIS

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)

black hat USA 2016

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

black hat USA 2018

– Security review for assessing software readiness

– ESF Software Supply Chain Working Panel (2021) Binary SCA for final package validation

SECURITY SUMMIT

– Securing software supply chain and SBOM

SECURING THE SOFTWARE SUPPLY CHAIN

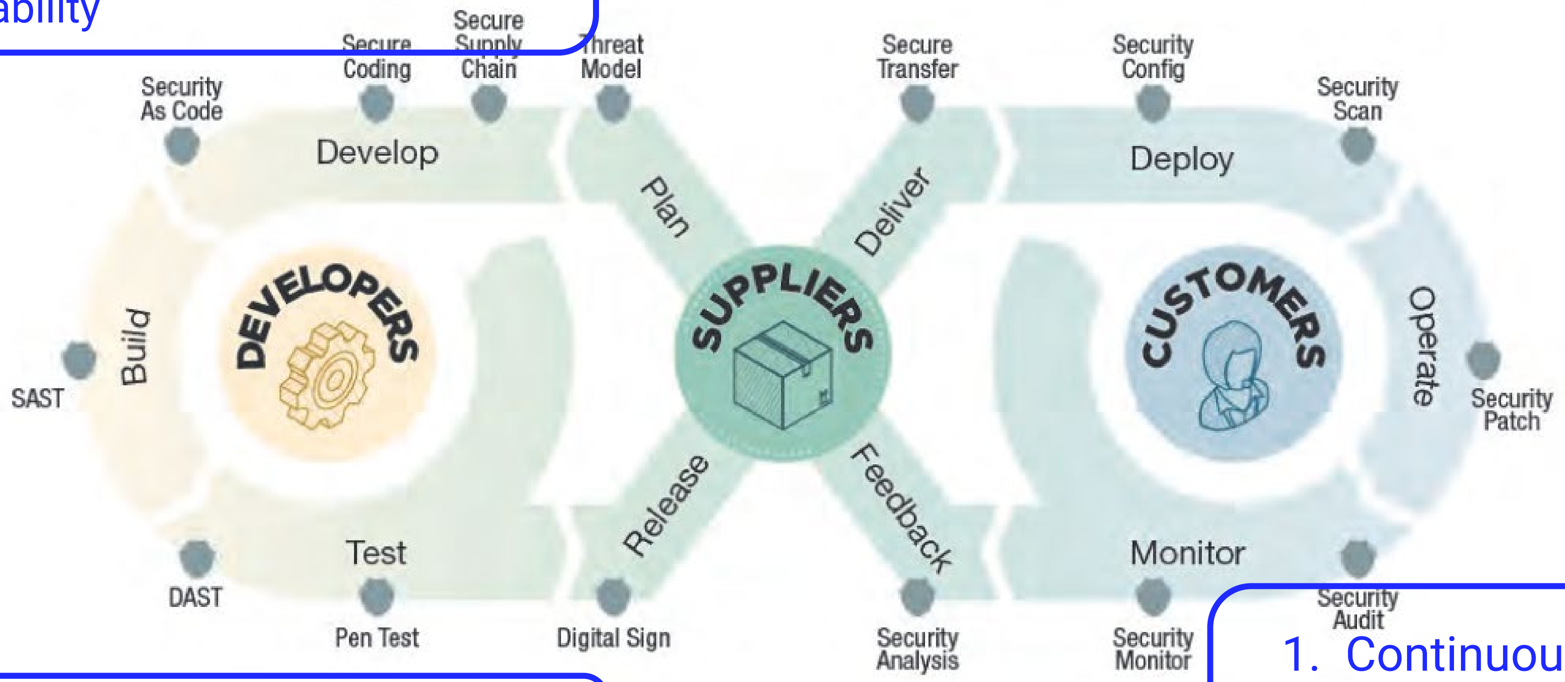
RECOMMENDED PRACTICES GUIDE FOR DEVELOPERS

Enduring Security Framework
August 2022

DevSecOps Practices addressing Operational Risks

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

4. Guardrails for deployment decisions



3. Test Plan & Execution

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

DevSecOps Figure: NSA CISA ODNI “Securing software supply chain – recommended practices guide for developer”

Today’s Challenges

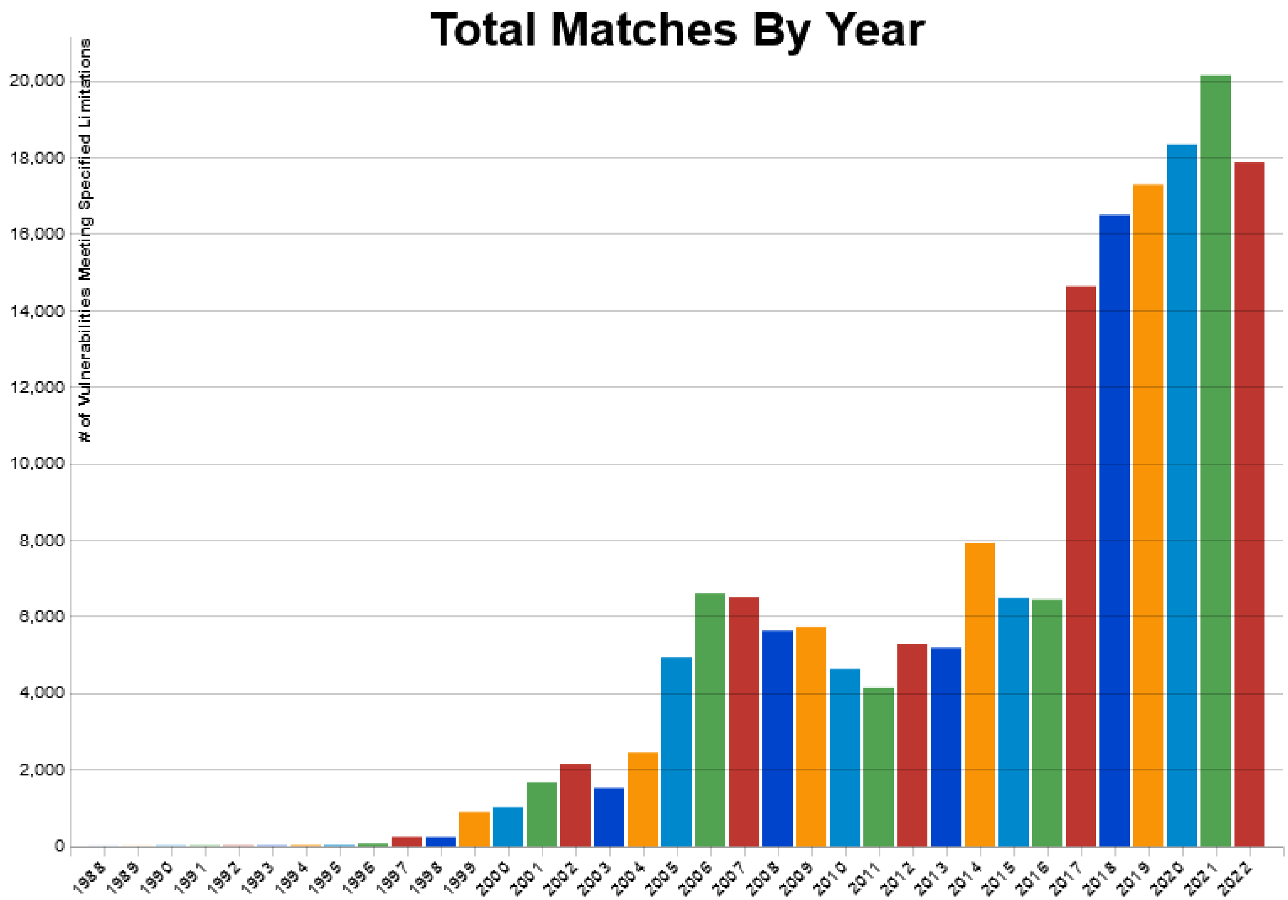
- Sharp rise of CVEs

- Scalable & accurate search for affected products

- Protection against evolving threat landscapes

Search Parameters:

- Results Type: Statistics
- Search Type: Search All
- CPE Name Search: false



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

BlackBerry® Intelligent Security. Everywhere.