Software Supply Chain
As a Platform
Gal Marder, EVP of Strategy
@JFrog
BY 2026, 80% of Engineering Organizations Applications will establish platform teams as internal providers of reusable services, components and tools for application delivery. Gartner

THE SOFTWARE SUPPLY CHAIN is a CRITICAL FOUNDATION to create TRUSTED application delivery.

HOW?
SOFTWARE DELIVERY HISTORY:
ISLANDS OF AUTOMATION
RELEASE-FIRST: NEED FOR CONTROL
INJECTING CONTROLS ALONG THE ASSEMBLY LINE TO GUARANTEE TRUST

[✔] Security
[✔] Licensing
[✔] Compliance
[✔] Quality
THE SUPPLY CHAIN OF YOUR SOFT DRINK

source: https://www.selectscience.net/editorial-articles/behind-the-scenes-at-coca-cola-the-key-to-high-quality-drinks-and-happy-consumers/?artID=53213
THE MOVE TO RELEASE-FIRST APPROACH

SOURCE ENVIRONMENT

TRUST

? QUALITY

INTEGRITY

? 

CHECK

VISIBILITY?

TARGET ENVIRONMENT

VISIBILITY?
THE MOVE TO RELEASE-FIRST APPROACH

1. ANALYZE
2. VALIDATE
3. SIGN

SOURCE ENVIRONMENT

QUALITY CHECK

TARGET ENVIRONMENT
THE MOVE TO RELEASE-FIRST APPROACH

1. Analyze
   - Scan Dependencies
   - Scan Dependencies SAST
   - Scan Release with Dependencies

2. Validate
   - Validate Dependencies
   - Validate Release
   - Validate Promotion

3. Sign (Evidence SBOM)
   - Record Admittance
   - Tag a Release
   - Create Release Bundle
   - Record Promotion Evidence
   - Record Distribution Evidence
   - Record Deployment Evidence
   - Report Runtime Metadata

Curate
Create
Package
Promote
Distribute
Deploy
Run

CODE
BINARIES
RELEASE-FIRST LIFECYCLE MANAGEMENT
THE ROAD TO TRUSTED RELEASES

DEV
- Curation Record
- Pipeline SBOM (signed pipeline)
- License Compliance Records
- Promotion Records
- Deployment Approvals
- Build SBOM (buildInfo)
- Vulnerability Scanning Results
- Distribution Records

RUNTIME

Release Bundle
RELEASE-FIRST SECURITY-INJECTED PLATFORM
QUALITY CONTROL vs QUALITY ASSURANCE

Package Curation
Blocking unwanted software components from entering your SSC
RELEASE-FIRST SECURITY-INJECTED PLATFORM

CODE
- CURATE
- CREATE
- PACKAGE
- PROMOTE
- DISTRIBUTE
- DEPLOY
- RUN

BINARIES
- CURATE
- SAST
- XRAY + ADVANCED SECURITY

- Inject MALICIOUS PACKAGES
- Discover 0-DAYS
- Exploit CVEs
- Steal SECRETS
- Abuse MISCONFIGS
- Tamper BINARIES
- Attack PRODUCTION
“LEFTER” THAN LEFT: SECURING THE DESKTOP

SEAMLESS INTEGRATION WITH JFROG AS THE ORGANIZATION’S SINGLE SOURCE OF TRUTH

The JFrog PLATFORM

- JFrog CLI
- Artifactory-based RESOLUTION
- SDKs & tools
- IDE integration
- Package managers CONFIG
- IDE plugins
- CURATION of OSS libraries
- SECURITY scanning

SEAMLESS INTEGRATION WITH JFROG AS THE ORGANIZATION’S SINGLE SOURCE OF TRUTH
CONTROLLING THE DEVELOPMENT ENVIRONMENT
RELEASE-FIRST SECURITY-INJECTED PLATFORM

**CODE**
- CURATE
  - Inject MALICIOUS PACKAGES
- CREATE
- PACKAGE
- PROMOTE
- DISTRIBUTE

**BINARIES**
- DEPLOY
- RUN
  - Attack PRODUCTION
  - Tamper BINARIES
  - Abuse MISCONFIGS
  - Steal SECRETS
  - Exploit CVEs
  - Discover 0-DAYS

**CURATE** | **SAST** | XRAY + ADVANCED SECURITY | **STAY TUNED...**
DEVOPS  DEVSECOPS  MLOPS
of new software applications will contain **ML Models or services** as enterprises utilize the massive amounts of data available to the business.

Gartner, “A Mandate for MLOps, ModelOps, and DevOps Coordination,” Van Baker, Nov. 22, 2022
Transition – Maybe Board Slide
MLOPS BRIDGING THE AUTOMATION GAP

DataOps
- Collect data
  Spark, Snowflake, Kafka, etc.
- Transform it
- Store and version
  Feature sets & other metadata

ModelOps
- Experiments to train the model
  May need GPUs
- Validate & fine-tune
- Package model for runtime
- Store and version model

RuntimeOps
- Distribute model
- Deploy model in runtime
- Serve the model
- Monitor & extract performance data

DevOps Automation
JFrog Platform Integration
MLOPS THE MODEL++

MODEL FILES ARE BINARIES MANAGED HOLISTICALLY WITH OTHER BINARIES
TRUSTED, SECURE ML MODELS
BRINGING DEVOPS & DEVSECOPS SOFTWARE SUPPLY CHAIN PROCESSES TO MLOPS
MLOPS IN THE JFROG PLATFORM

Smart model registry with integrated security

- Model versioning
- Model sharing
- Model++ release bundling
- Model traceability
- Remote model hosting
- Model vulnerability scanning
- Model license scanning
END TO END

SECURE SSC PLATFORM