DevSecOps Day EMEA Unlock 2024

Software Supply Chain As a Platform

Gal Marder, EVP of Strategy

@ JFrog

DEVELOPER-AUTOMATED SOFTWARE DELIVERY

> By 2026 **80%** of **Engineering Organizations Applications** will establish **platform teams** as internal providers of reusable services, components and tools for **application delivery.**
>
> Gartner

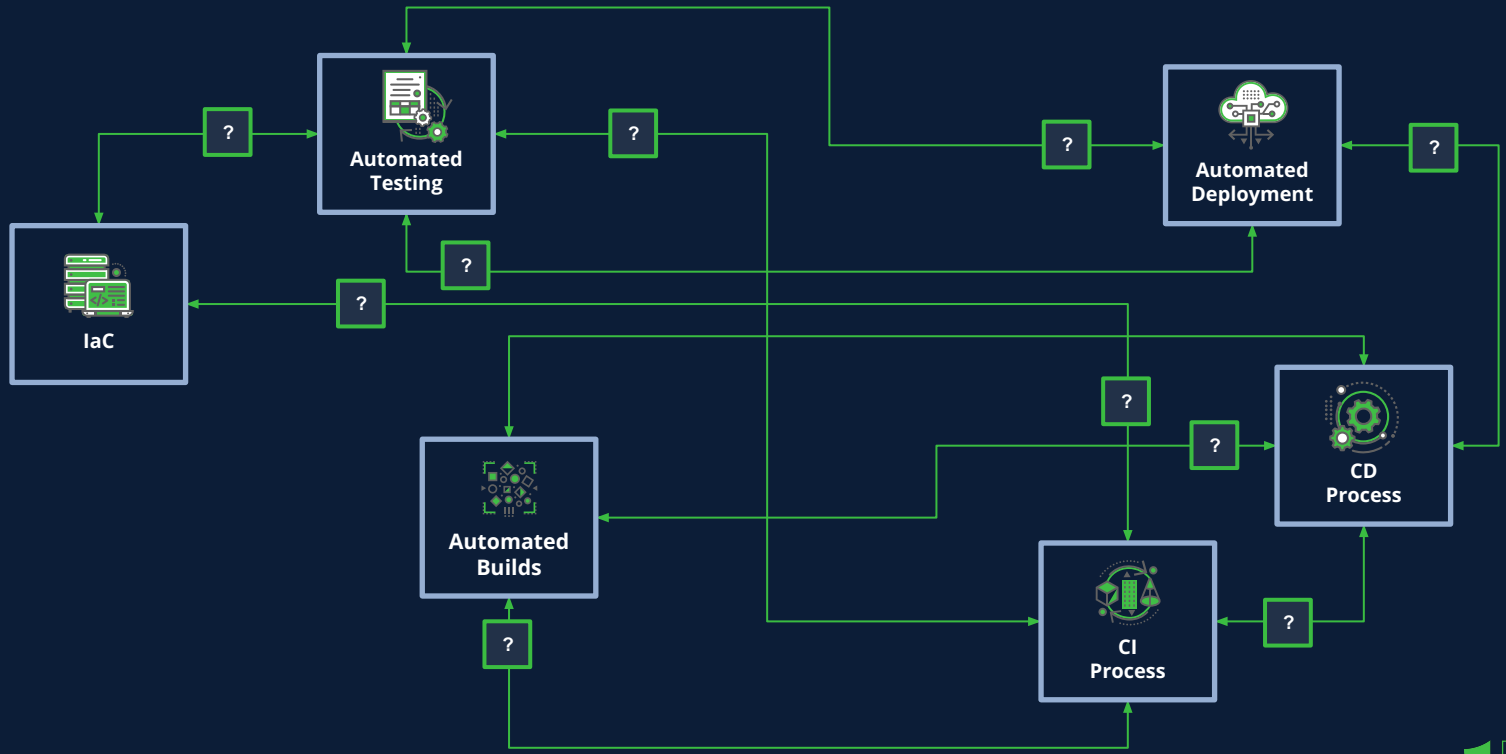
THE SOFTWARE SUPPLY CHAIN
is a **CRITICAL FOUNDATION to** create **TRUSTED** application delivery.

HOW?

Gartner, "What Is Platform Engineering?", Lori Perri, Oct. 5, 2022


DEVOPS
DEVSECOPS
MLOPS

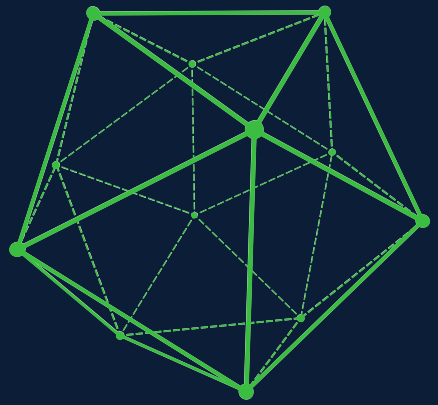
SOFTWARE DELIVERY HISTORY:
ISLANDS OF AUTOMATION




RELEASE
Automated Testing
Automated Deployment
IaC
Automated Builds
CD Process
CI Process
?

RELEASE-FIRST: NEED FOR CONTROL

INJECTING CONTROLS ALONG THE ASSEMBLY LINE TO GUARANTEE **TRUST**



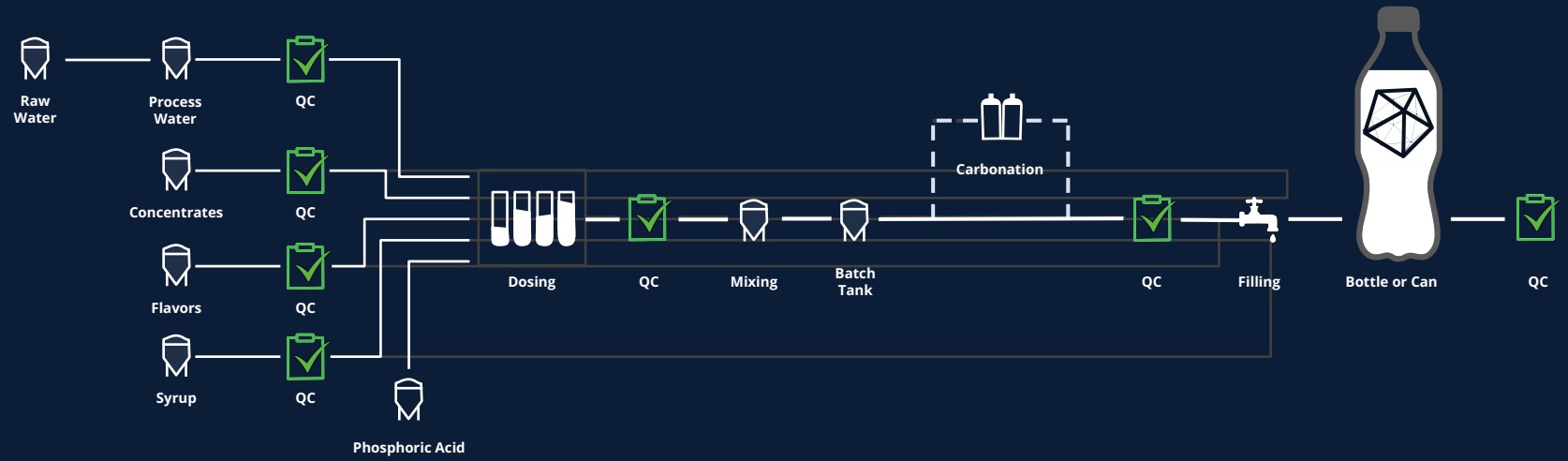
[✓] Security

[✓] Licensing

[✓] Compliance

[✓] Quality

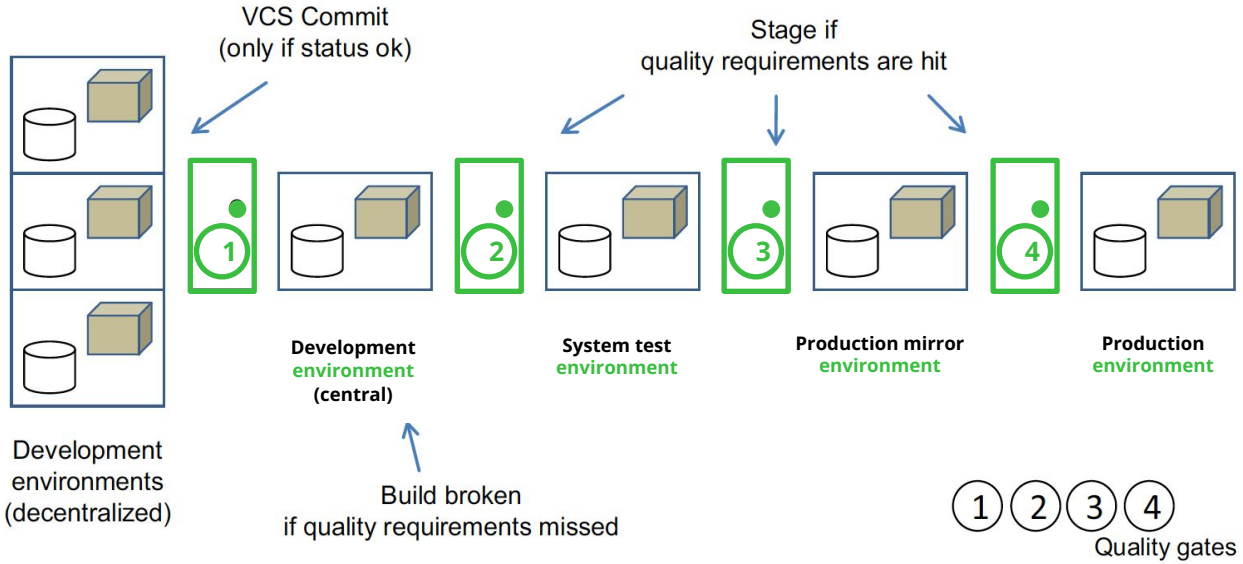
THE SUPPLY CHAIN OF YOUR SOFT DRINK



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

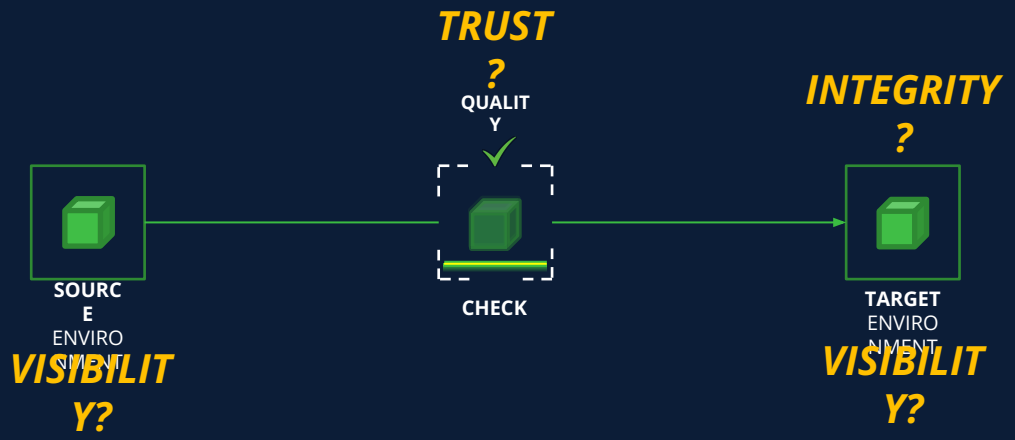
SOFTWARE QUALITY GATES

(Agile ALM - 2011)

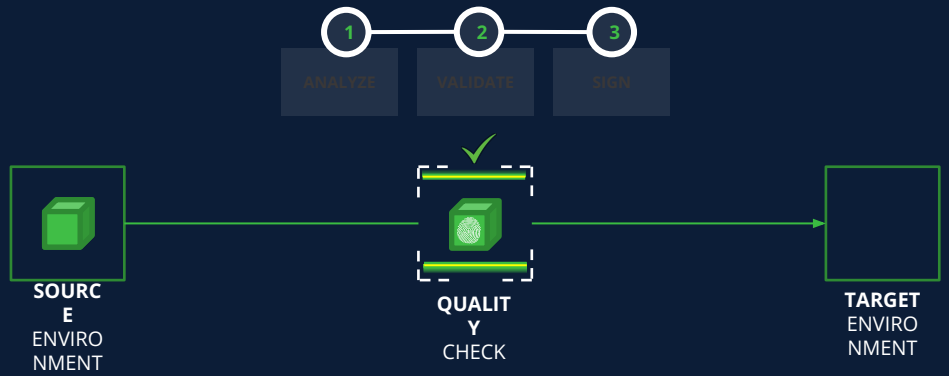


SOURCE: Michael Huettermann, Agile ALM book

THE MOVE TO RELEASE-FIRST APPROACH



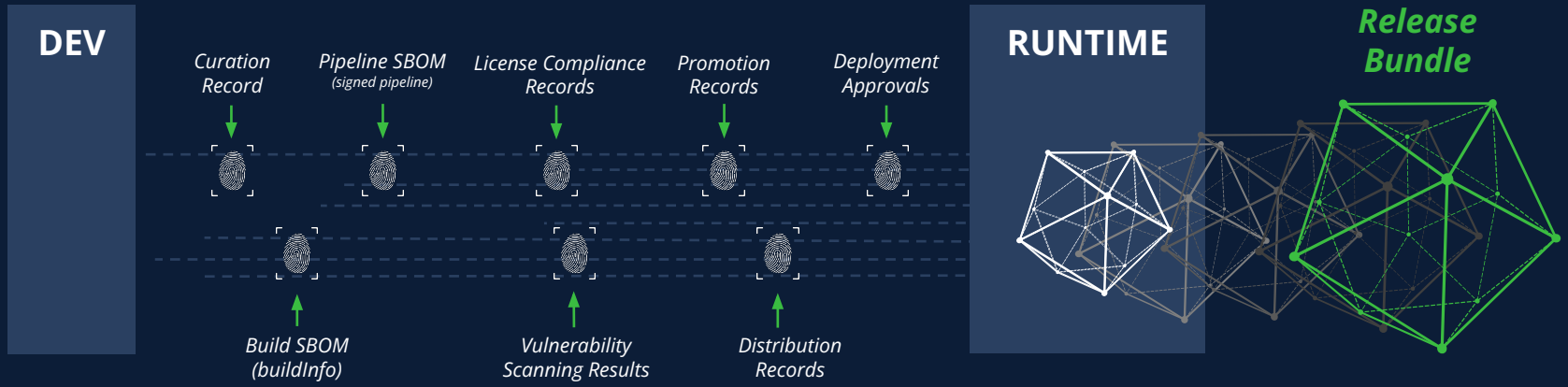
THE MOVE TO RELEASE-FIRST APPROACH



THE MOVE TO RELEASE-FIRST APPROACH

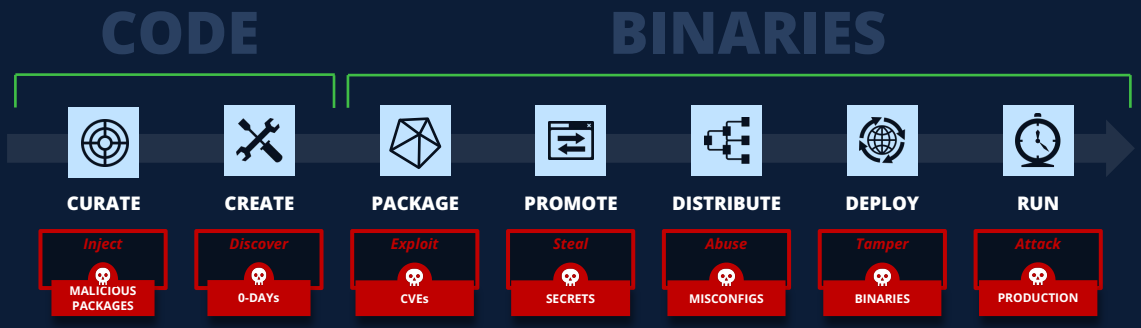
RELEASE-FIRST LIFECYCLE MANAGEMENT

THE ROAD TO TRUSTED RELEASES

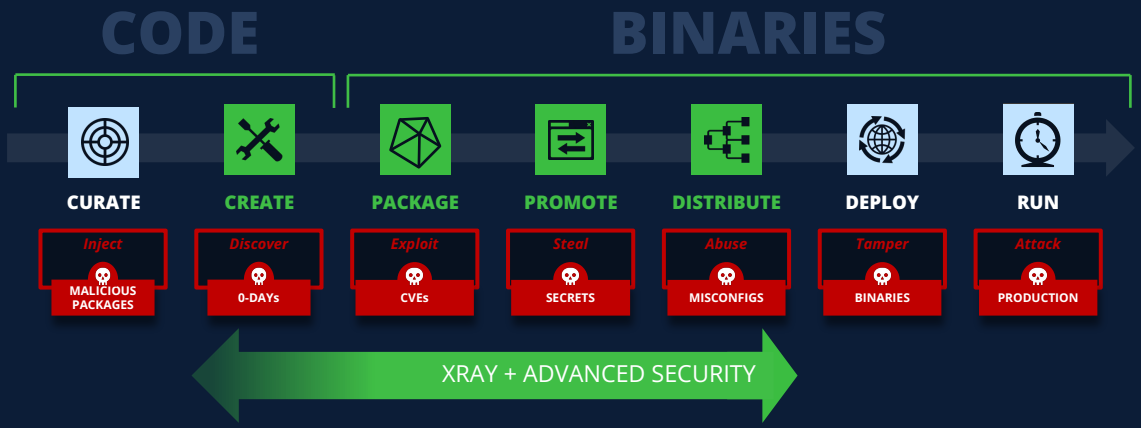



DEVOPS
DEVSECOPS
MLOPS

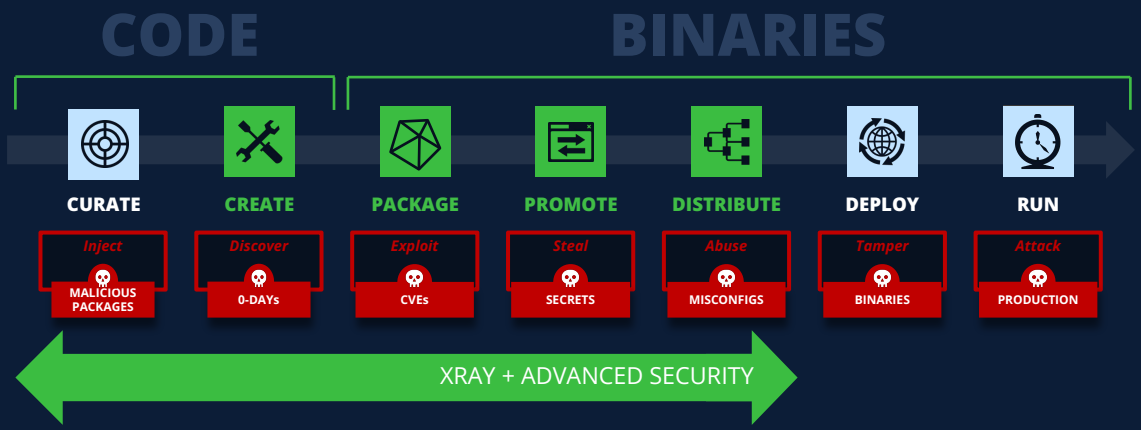
RELEASE-FIRST SECURITY-INJECTED PLATFORM



RELEASE-FIRST SECURITY-INJECTED PLATFORM



SHIFTING SECURITY LEFT

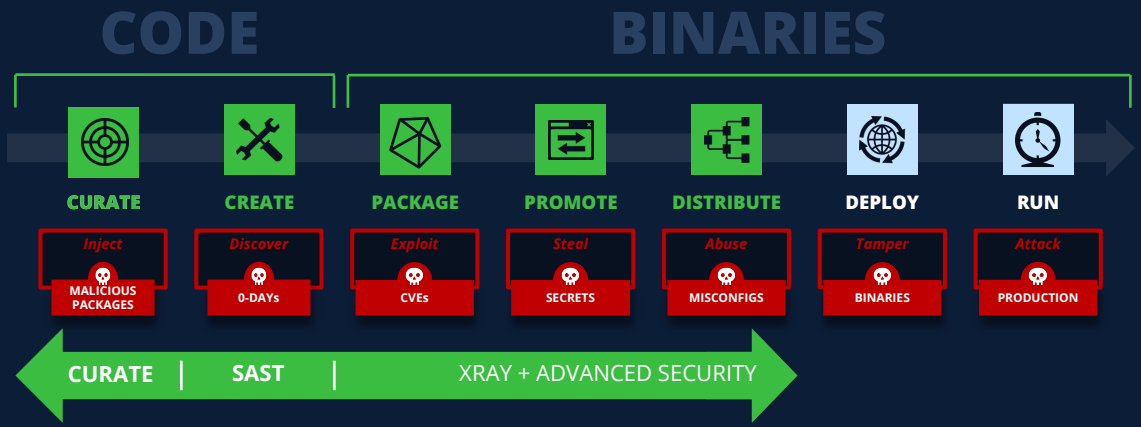


QUALITY CONTROL vs QUALITY ASSURANCE

Package Curation

Blocking unwanted software components from entering your SSC

RELEASE-FIRST SECURITY-INJECTED PLATFORM



“LEFTER” THAN LEFT: SECURING THE DESKTOP

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

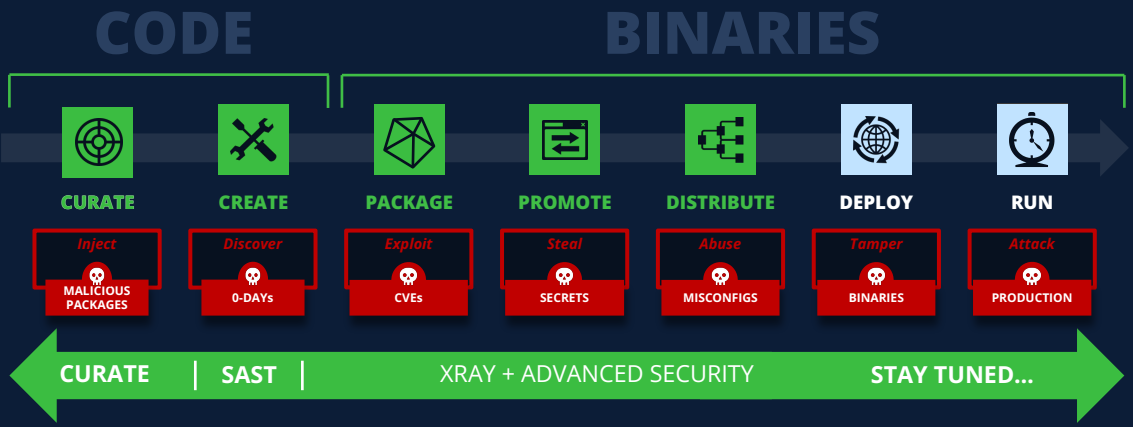
CONTROLLING THE DEVELOPMENT ENVIRONMENT

DEMO

JFrog

DevSecOps Day EMEA Unlock 2024

RELEASE-FIRST SECURITY-INJECTED PLATFORM




DEVOPS
DEVSECOPS
MLOPS

BY 2027

over **90%** *of* ***new software applications*** *will contain* ***ML Models or services*** *as enterprises utilize the massive amounts of data available to the business.*

MLOPS

Gartner

Gartner, "A Mandate for MLOps, Mode… …Ops Coordinati… …, Nov. 22,

JFrog

…s Day
…lock 2024

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

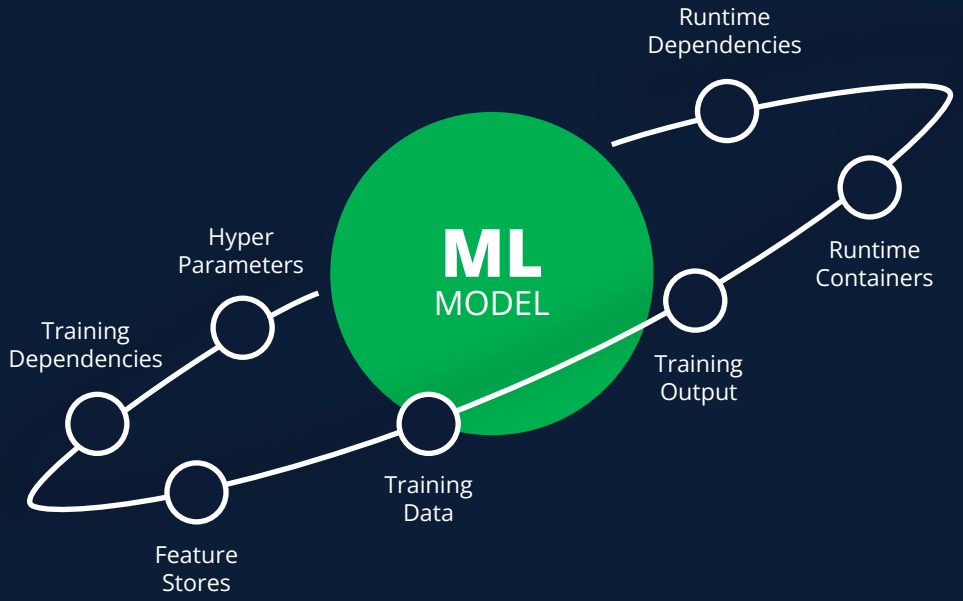
Deploy model in runtime

Serve the model

Monitor & extract
performance data

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

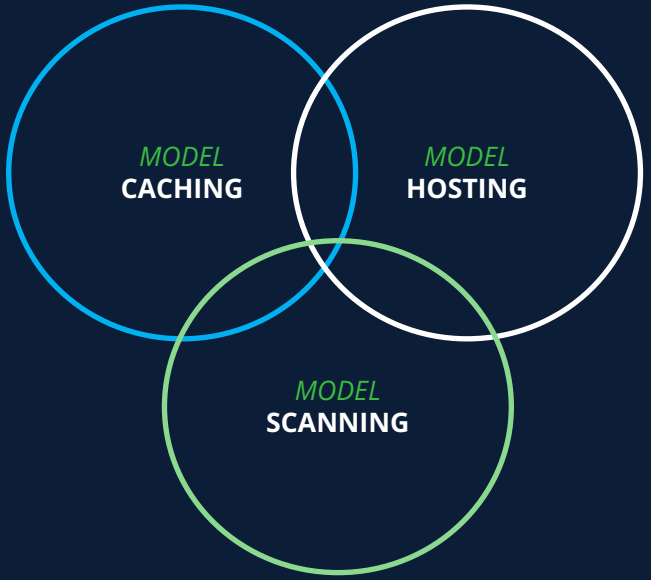
MLOPS IN THE JFROG PLATFORM

Smart model registry with integrated security

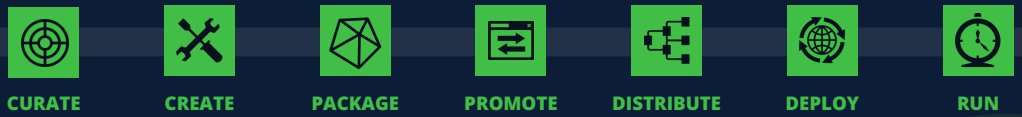
- Model versioning
- Model sharing
- Model++ release bundling
- Model traceability

- Remote model hosting

- Model vulnerability scanning
- Model license scanning



END TO END



SECURE SSC PLATFORM