A Systems Approach to Software Supply Chain Security and Continuous ATO

Mark Hurter, Solution Architect

29-August, 2022

Agenda

- The AO Dilemma
- Demonstrable Competencies
- Continuous ATO: A New Hope
- Three Layers of Compensating Control
- Q&A
- Closing

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Continuous Authorization To Operate (cATO)

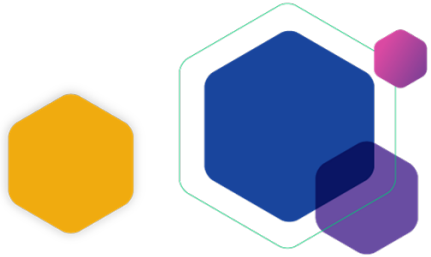
The Risk Management Framework (RMF) establishes the continuous management of system cybersecurity risk. Current RMF implementation focuses on obtaining system

"Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached."

cATO represents a challenging but necessary enhancement of our cyber risk approach in order to accelerate innovation while outpacing expanding cybersecurity threats. In order to achieve cATO, the Authorizing Official (AO) must be able to demonstrate three main competencies: On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of an approved DevSecOps reference design.


Deploy
Wait
THE ATO
imgflip.com
JAKE-CLARK.TUMBLR

The AO Dilemma



- How do I assess in real time whether or not the application is secure and compliant?
- Based on my risk posture can I assert that I am compliant?
- Do I have the evidence that underpins my assertions?

cATO Demonstrable Capabilities

- The adoption and use of an approved DevSecOps reference design

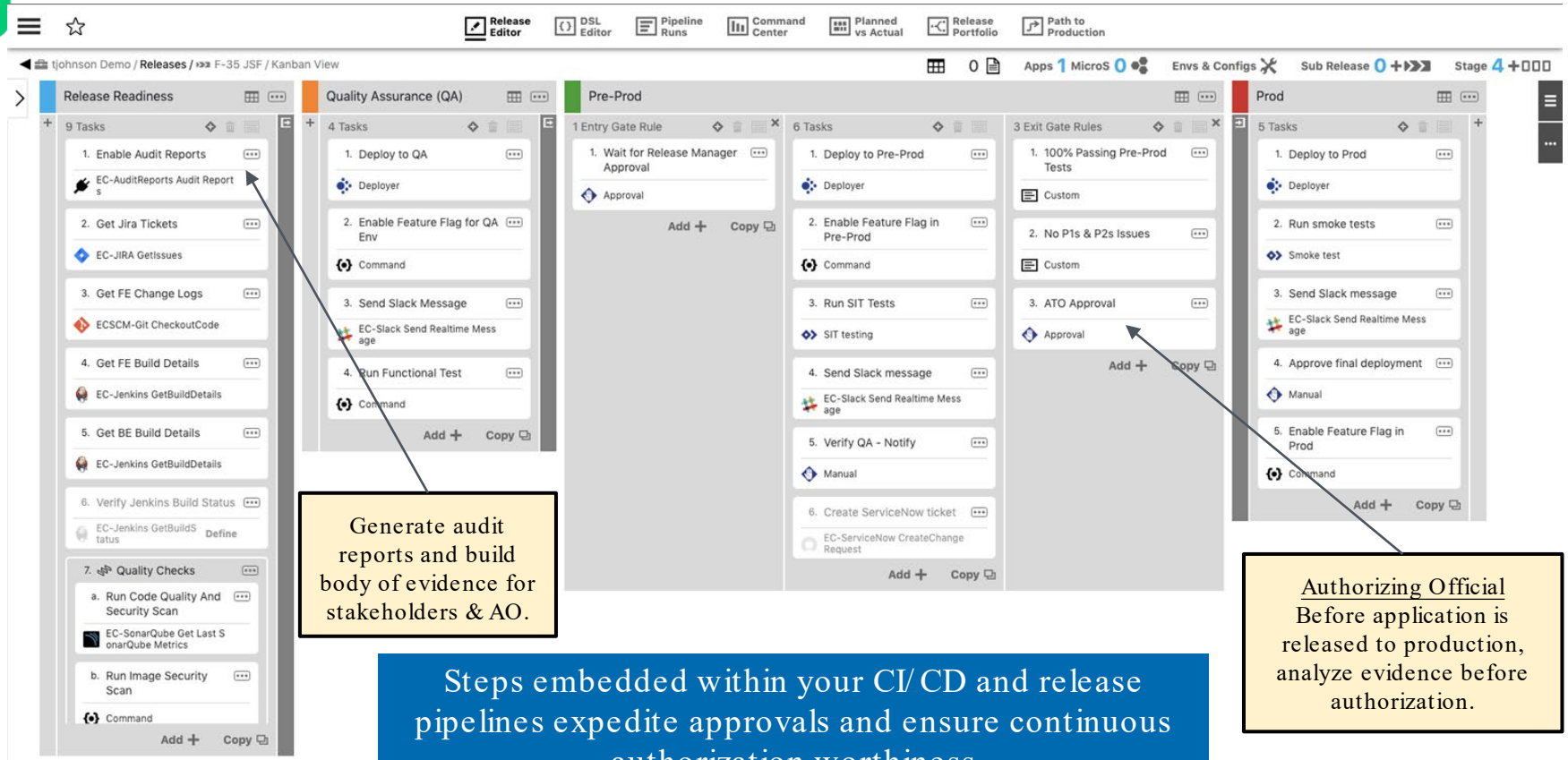
- On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls;

- Ability to conduct active cyber defense in order to respond to cyber threats in real time

Continuous ATO: A New Hope

- Requirements
  - Continuous == in-process/ad hoc, on New, and on Change
  - Highly automated
  - Holistic
  - Prioritize fixes
  - Includes compensating controls

Layer 1: The Modeled Reference Design



Generate audit reports and build body of evidence for stakeholders & AO.

Authorizing Official
Before application is released to production, analyze evidence before authorization.

Steps embedded within your CI/CD and release pipelines expedite approvals and ensure continuous authorization worthiness

Common Digital Assets

Code

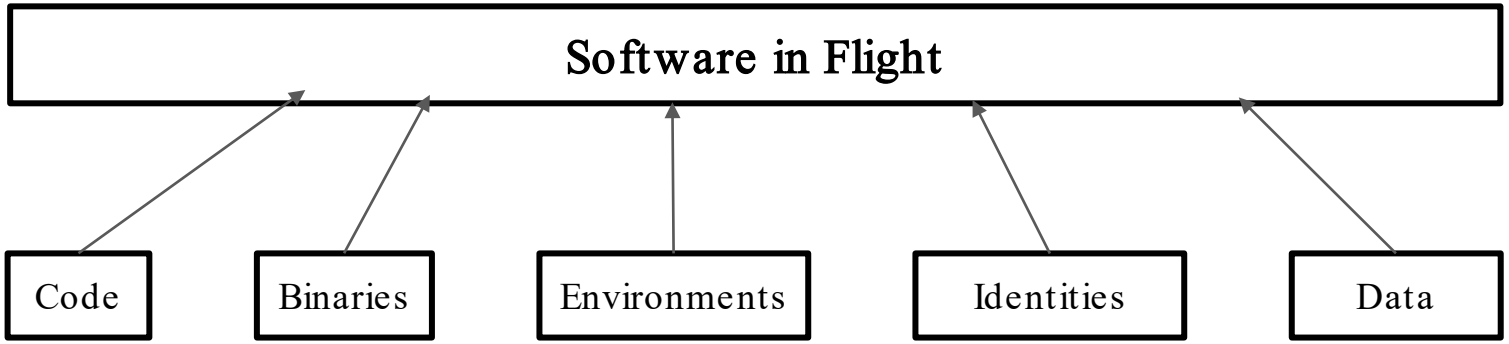
Binaries

Environments

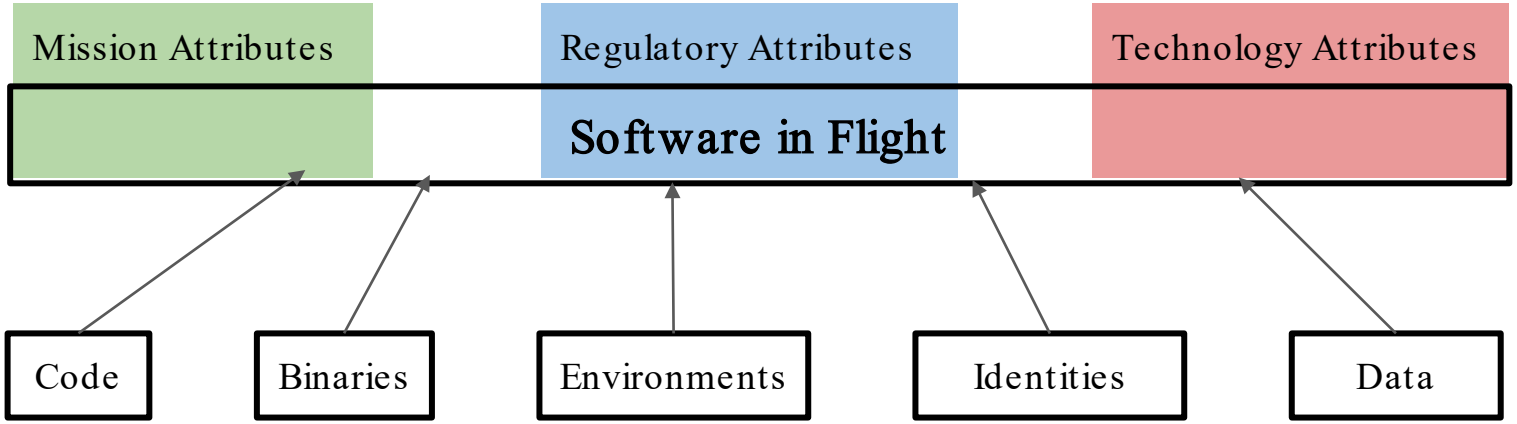
Identities

Data

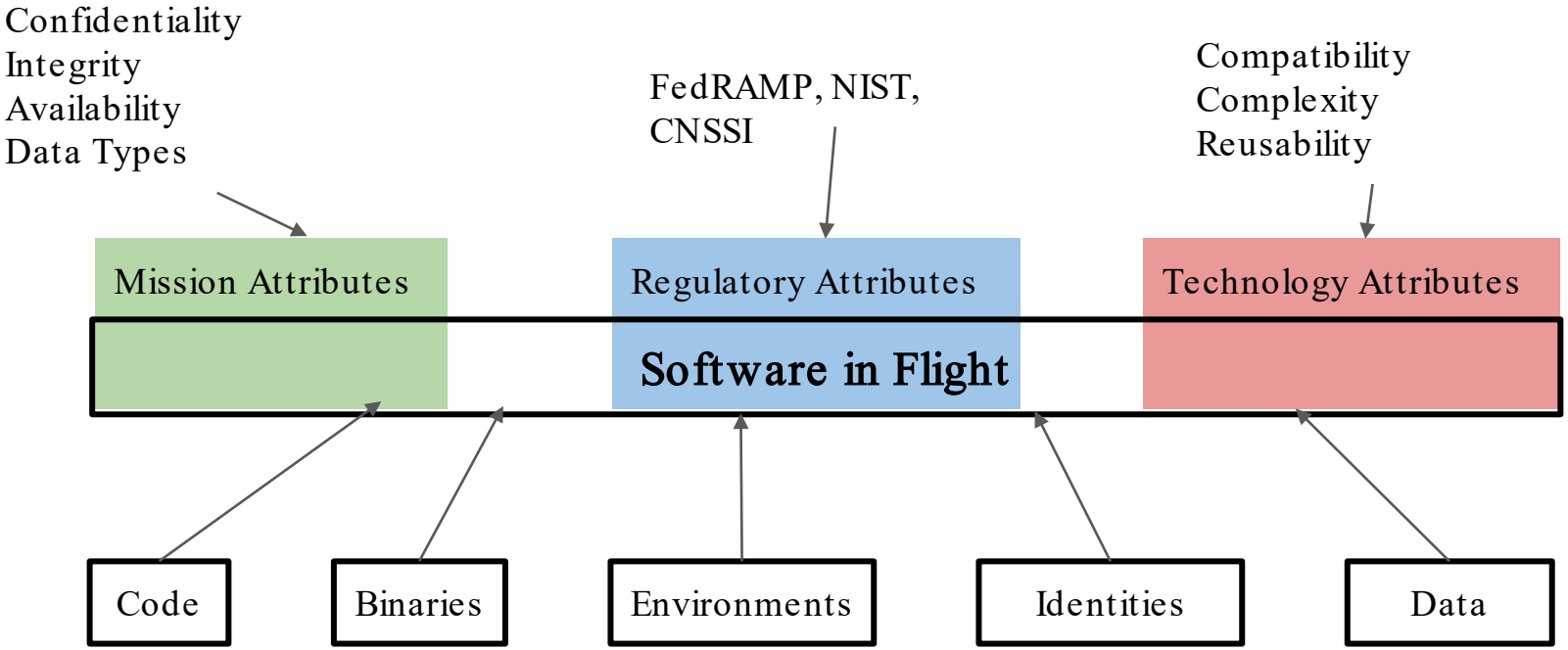
Define the Application



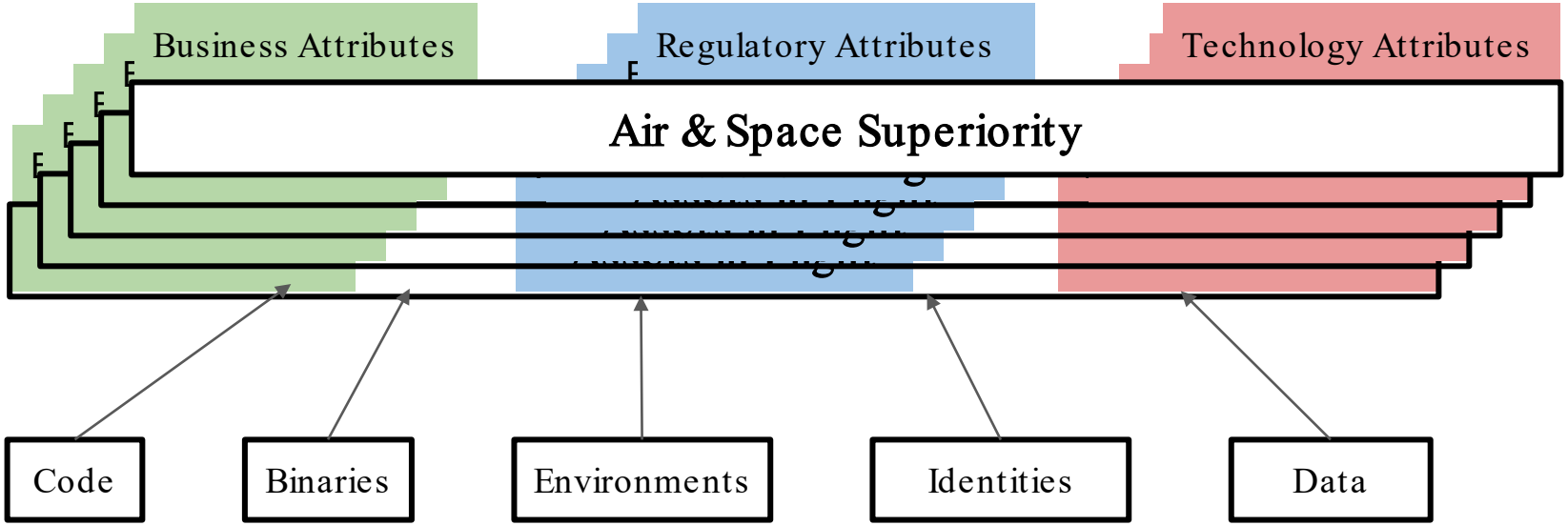
Model Risk Profile then Select Controls



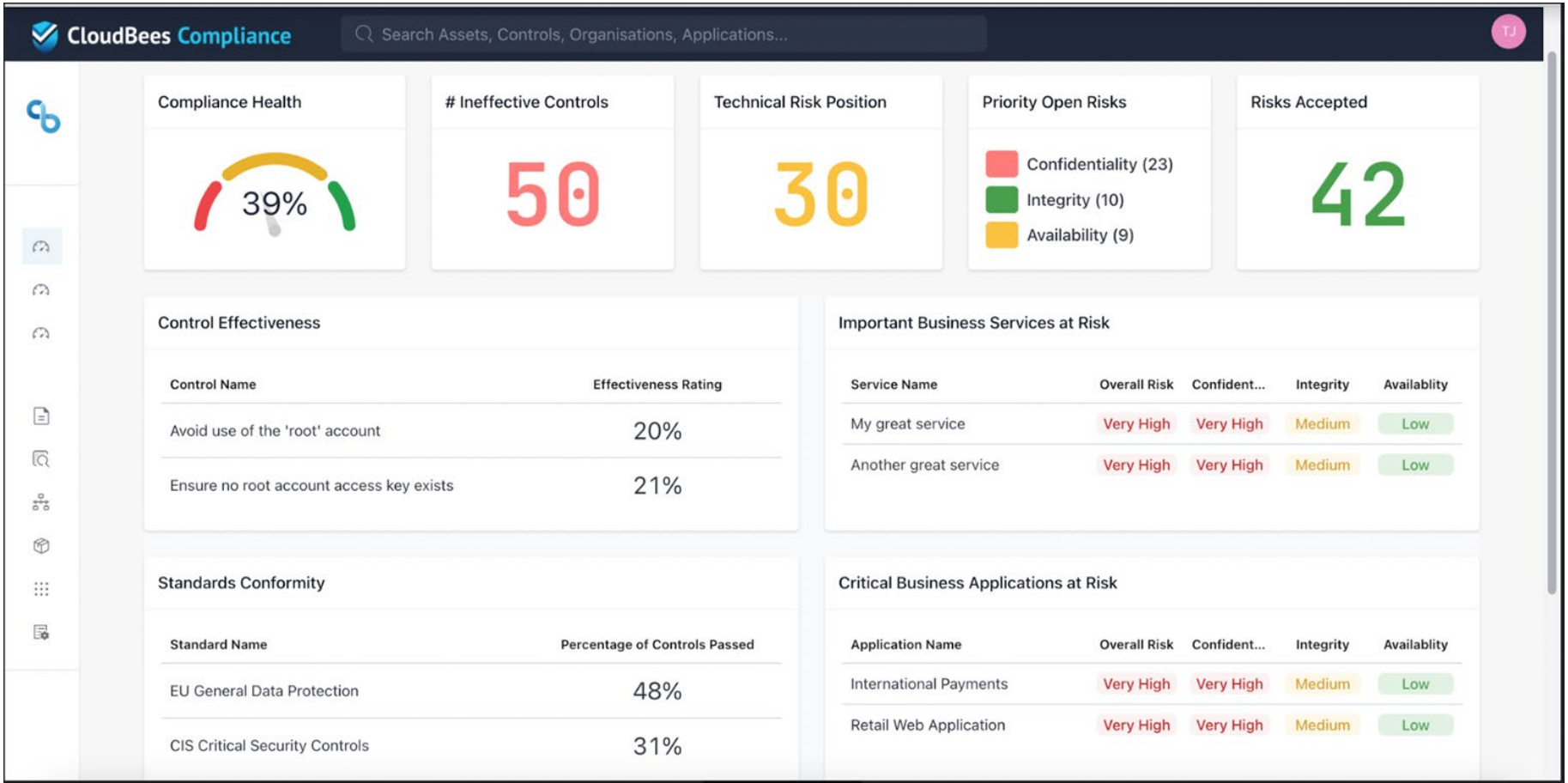
Model Risk Profile then Select Controls



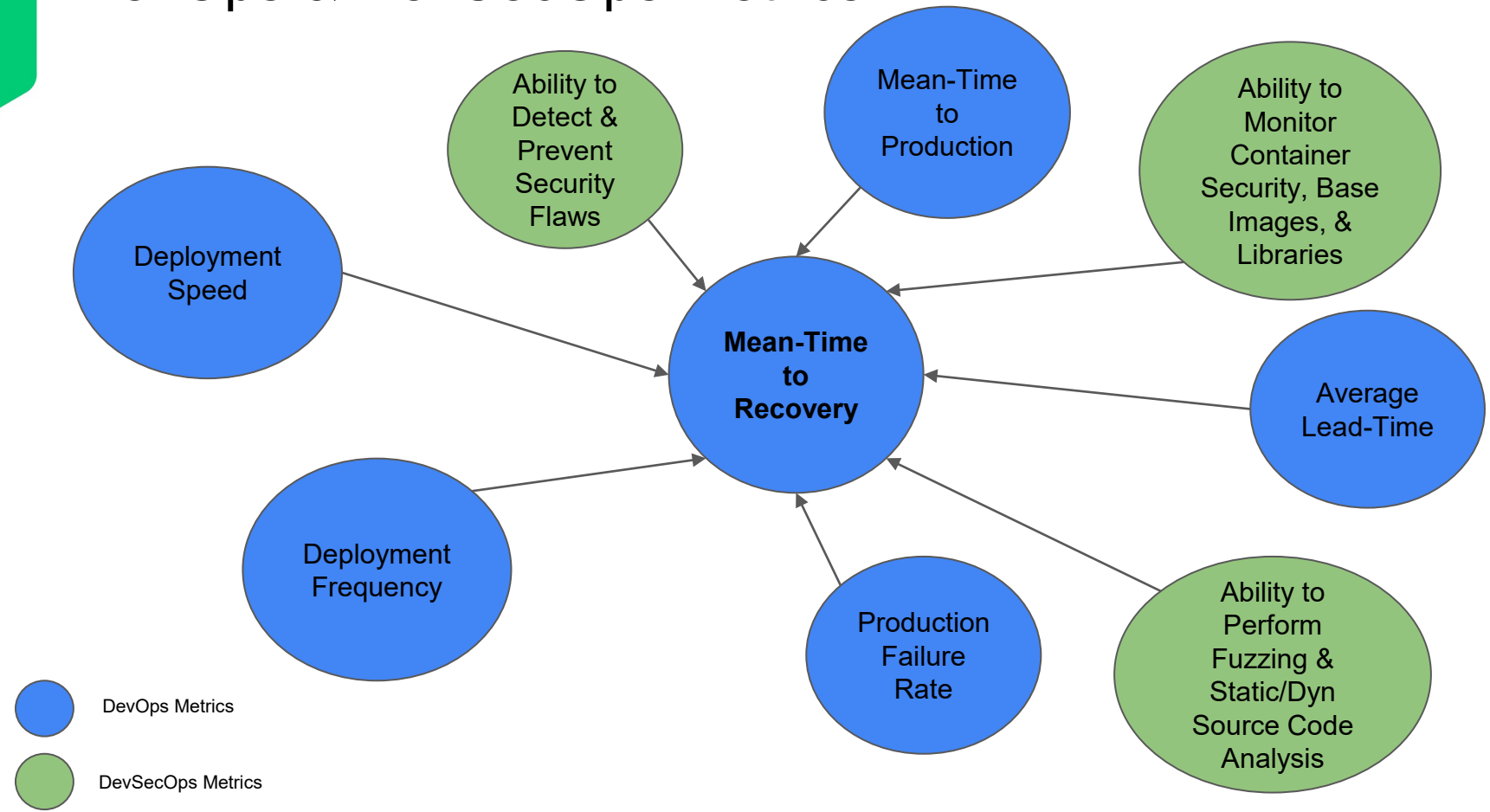
Assemble Applications into Critical Services



Layer 2: On-Going Visibility



DevOps & DevSecOps Metrics



Layer Three: Compensating Controls

Mean Time to Mitigate

- Feature flag as kill switch
  - Everyone has to follow the same build method
  - Kill features, not the experience
- Automated roll back to known good state
  - Rehearsed and integral to the system
  - When a bigger hammer is required

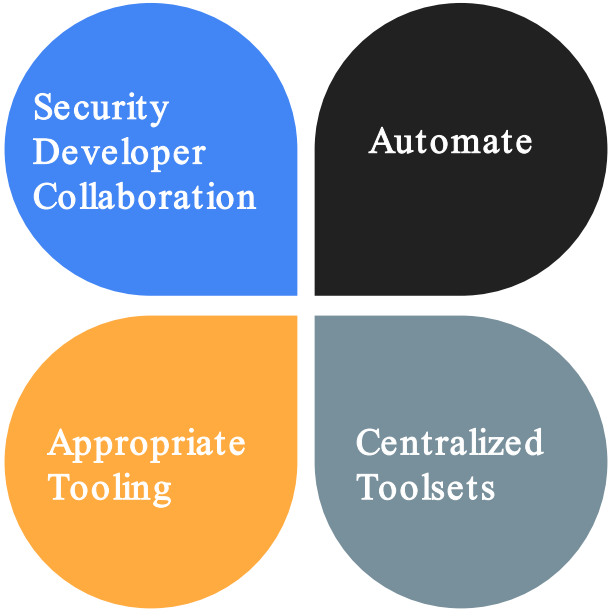
Keys to a Secure Software Supply Chain

Security/Dev Collab

- Security Defines Stds
- Improve Developer Experience
- Increase Velocity
- Improve Risk Posture

Appropriate Tooling

- Low/No Code approach for security
- Consumable by different personas
- Enable rapid response and RT/NRT feedback



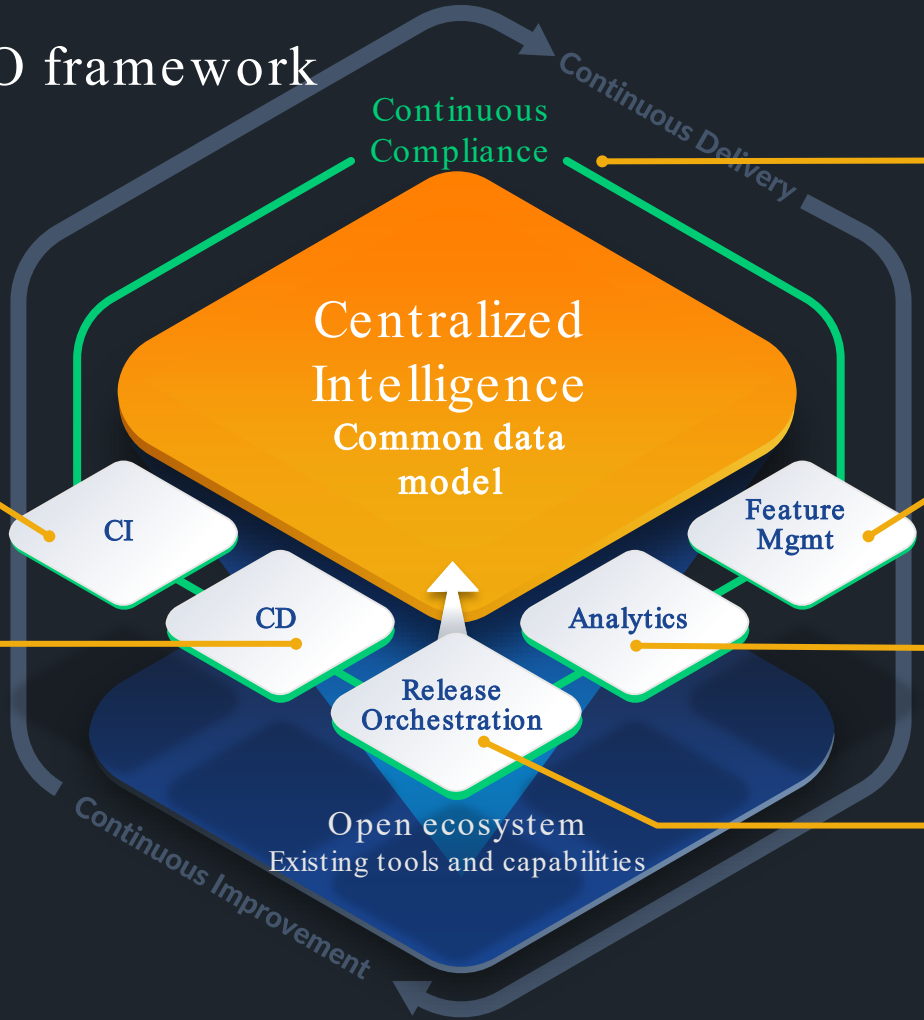
Automate Controls

- Continuously Assess
- Evidence as a service
- Control gates prevent non-compliant deployment

Centralized Toolsets

- Enterprise view
- Project view
- Persona-specific dashboards
- Centralized authoritative security/compliance/defect tracking to reduce noise

Continuous ATO framework



Continuous Integration
Build and test at scale

Continuous Delivery
Self-service, scalable, repeatable paths to production

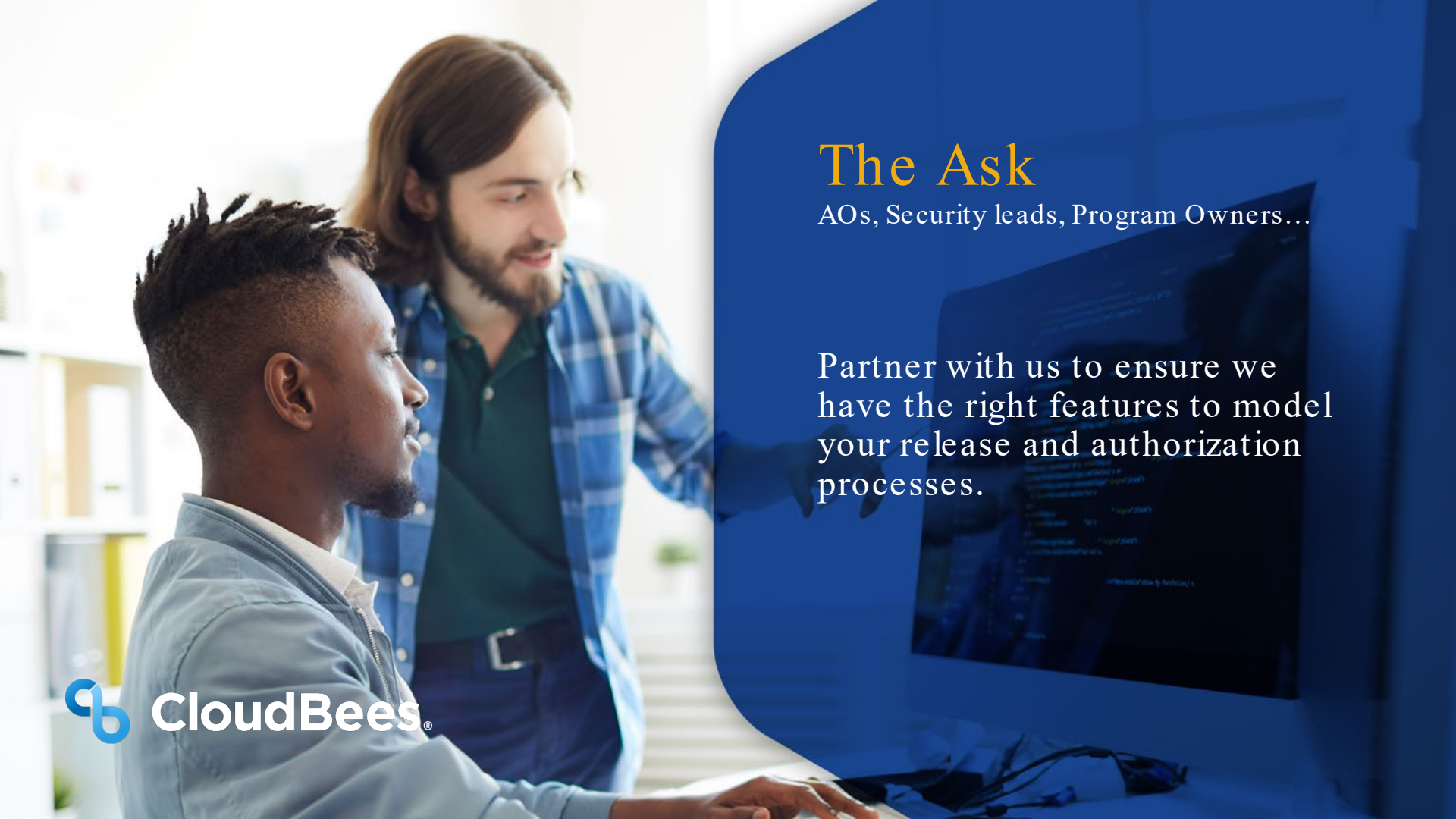
Continuous Compliance
Real-time code and infrastructure compliance verification

Progressive Delivery
Progressive roll-out and control of new features

Analytics
A single source for real-time measurement and contextual answers

Release Orchestration
Higher-order visibility, management, and intelligence

CloudBees.

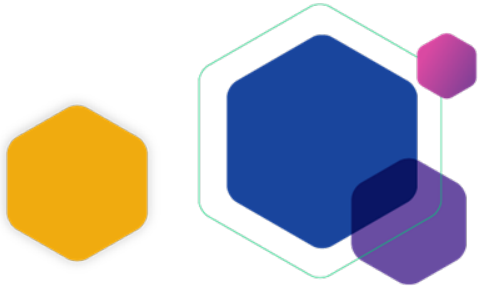


The Ask

AOs, Security leads, Program Owners…

Partner with us to ensure we have the right features to model your release and authorization processes.

CloudBees®



Q & A

CloudBees®


CloudBees®
https://www.cloudbees.com/federal