
CALFIRE
RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.
NAVIGATING THE FUTURE OF
FEDRAMP & CLOUD SECURITY

COALFIRE RAMPCON

06.09 — 06.10.2025 • WASHINGTON D.C.

Automating FedRAMP CI/CD

MICHAEL SCRIBELLITO | SR. TECHNICAL MANAGER | COALFIRE
NIKOLAS THEISS | SENIOR CONSULTANT | COALFIRE



Architecting CI/CD for FedRAMP can feel like Reinventing the Wheel





Common Mistakes

Major Challenges

Automation Framework

Common Mistakes



Common Mistakes & Misconceptions



Point & Shoot

Breaks the principle of a strict authorization boundary and isolated environments



Lift & Shift

Most CI/CD tools are not FedRAMP authorized & processes will not align 1:1



2x

Twice the code, overhead & cost

What's at Stake?



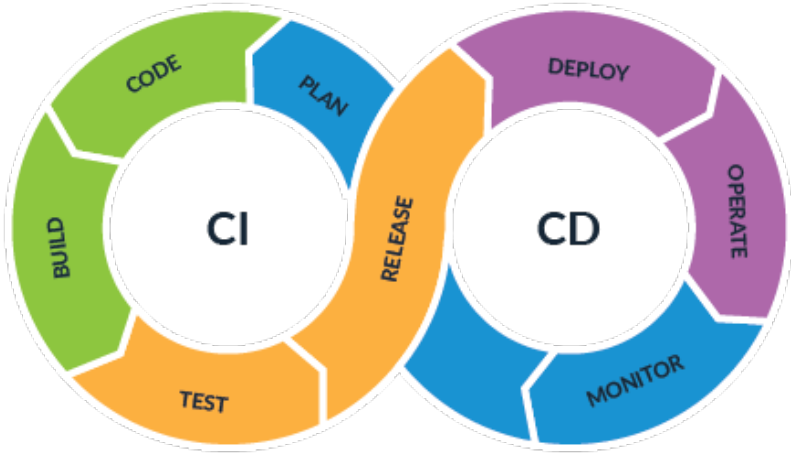


Release Velocity

Developer Experience

Automating FedRAMP CI/CD

- 4 Challenges to FedRAMP CI/CD Automation
- FedRAMP CI/CD Framework



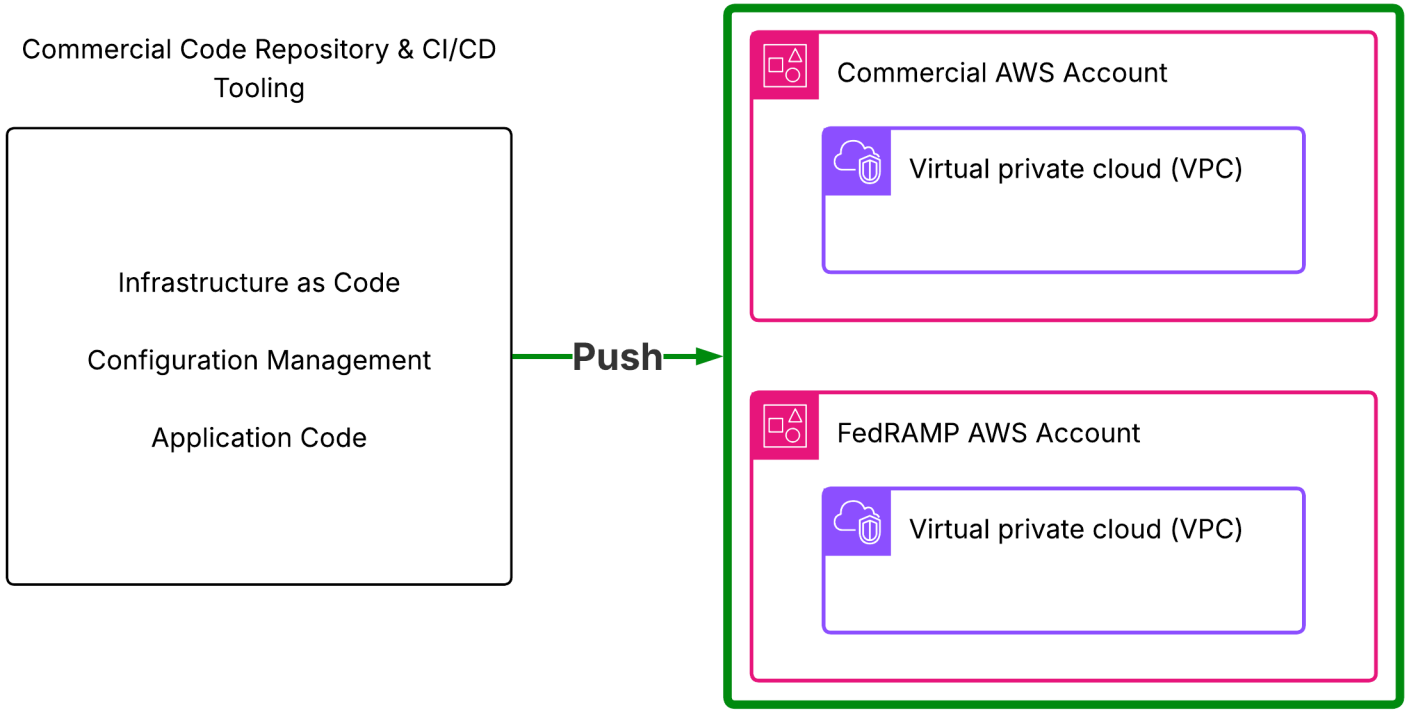
Major Challenges



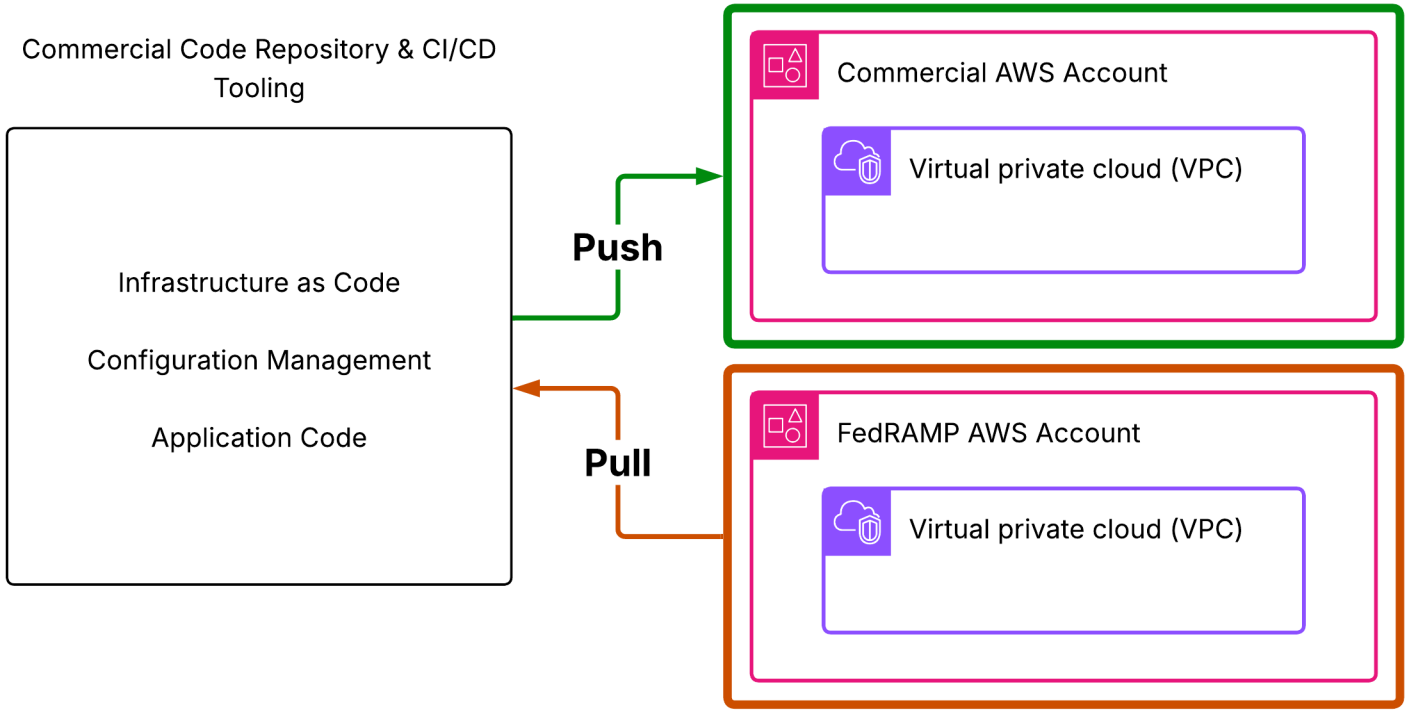
CSP Specific Challenges

- **Parity**
  - Alignment of commercial staff, processes & tools to FedRAMP
- **Speed**
  - Time to market
- **Codebase**
  - Forking of Infrastructure as Code (IaC) and application code to support disparate environments
- **Continuous Deployment vs Continuous Delivery**

Challenge 1 – Government Clouds: Assumption



Government Clouds: Reality

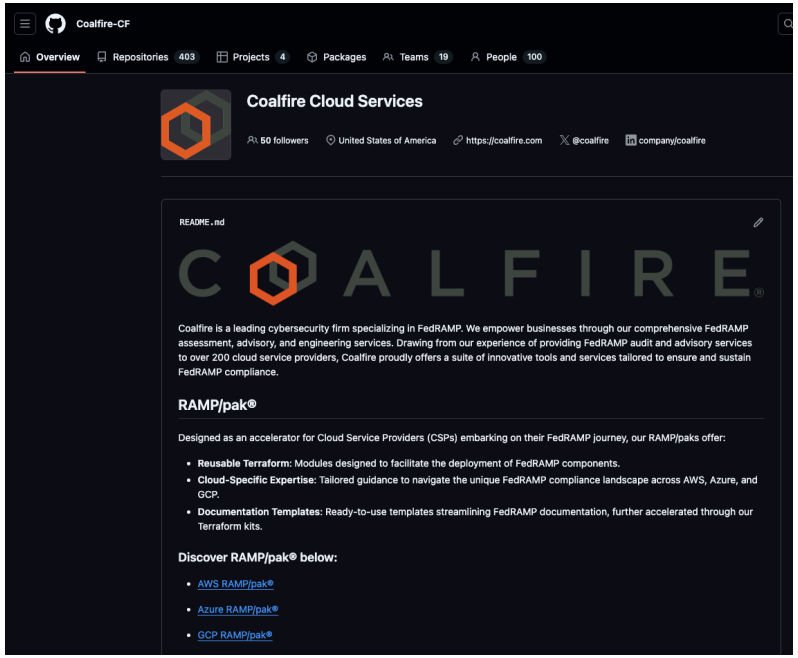


Government Clouds: Reality

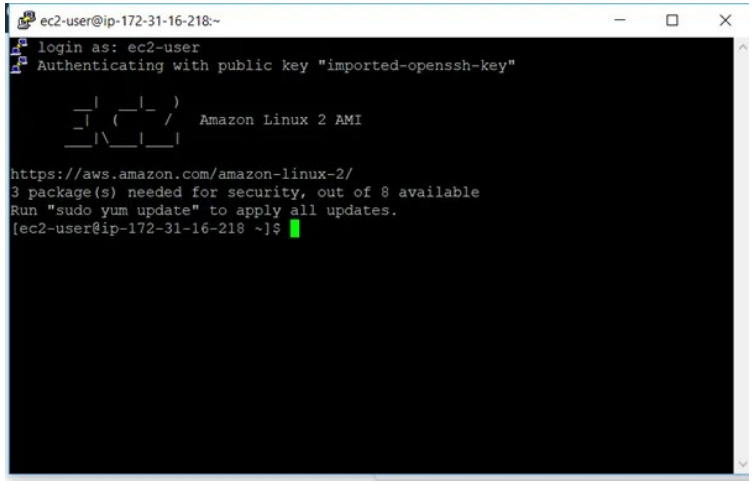
- **AWS GovCloud is a physically isolated partition**
  - ARNs, VPCs & IAM cannot cross boundaries
- **Plan for code changes and re-architecting efforts**
  - Hardcoded configuration
  - Service availability
  - Feature limitations

Challenge 2 – Access Controls

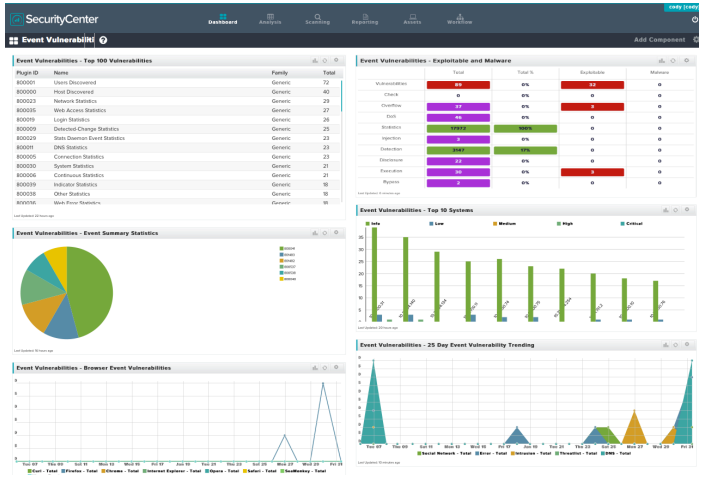
Code



Systems

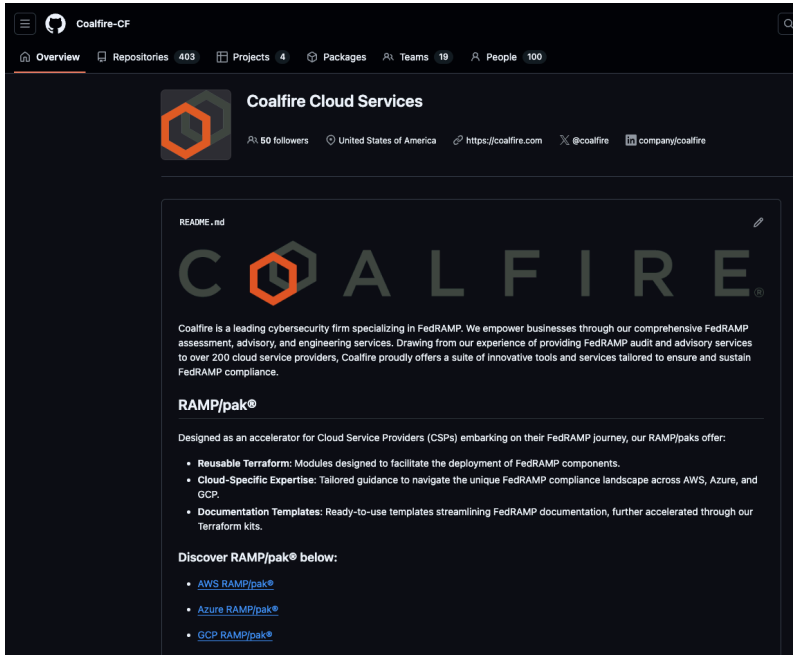


Web Consoles

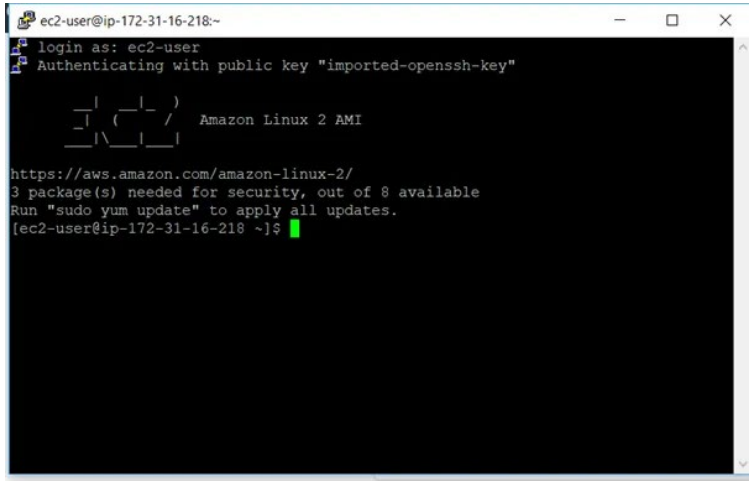


Gray Areas

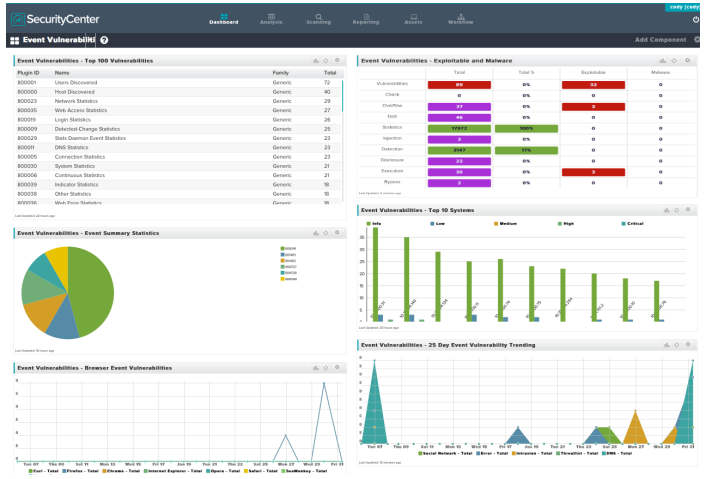
Code



Systems



Web Consoles



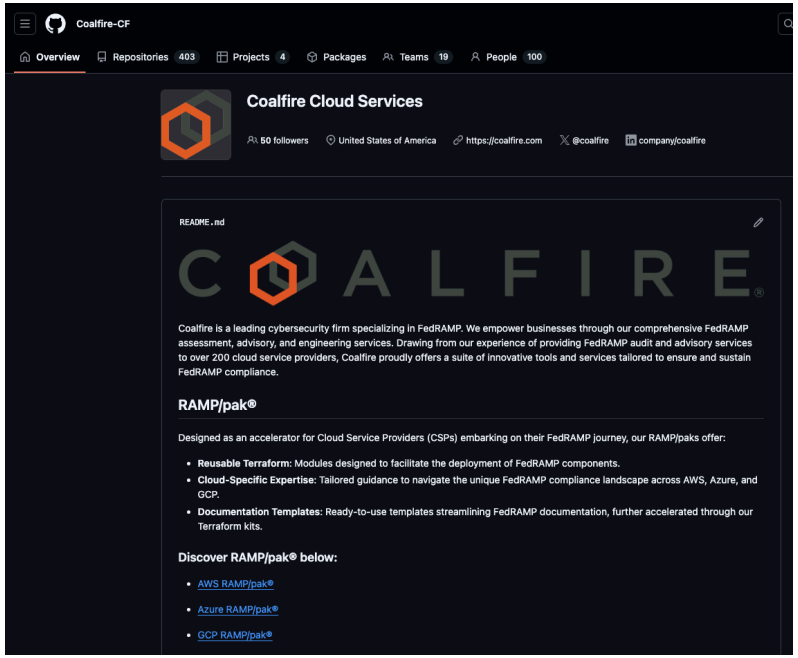
FedRAMP Boundary

Gray Areas

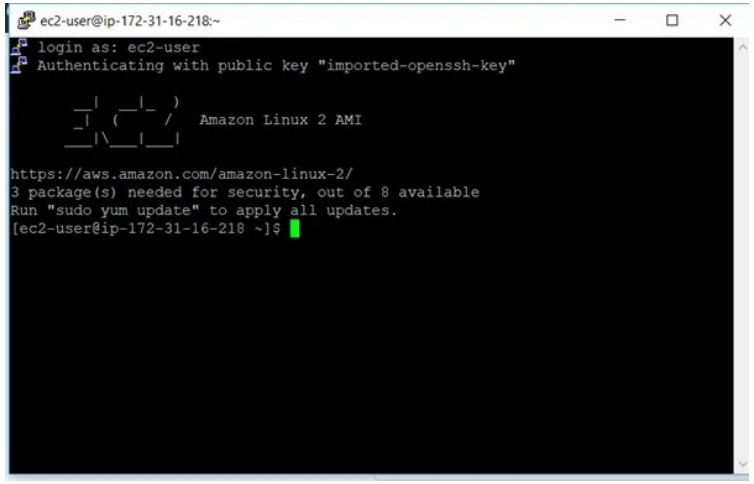
- **Who can view it?**
  - FedRAMP users are subject to guardrails
- **How is it accessed?**
  - Systems containing sensitive metadata must reside within the FedRAMP boundary
- **Sensitive metadata**
  - Configuration data (hostnames, IPs, patching level, etc.)
  - Scan data & security documentation
  - Incident response data & tickets with specific system details

Gray Areas

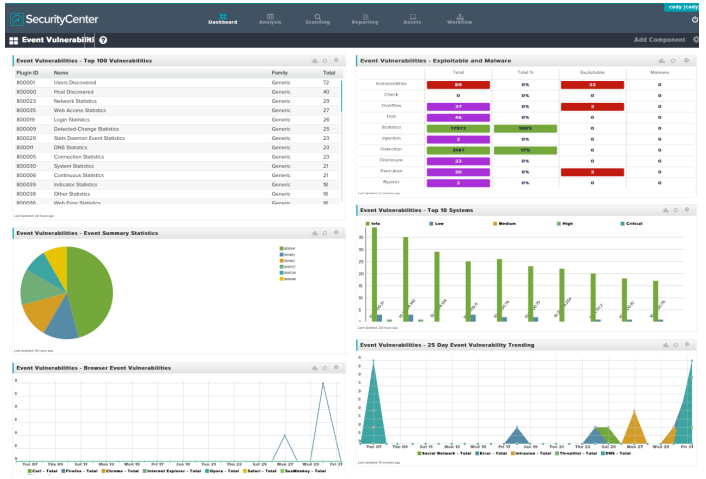
Code



Systems

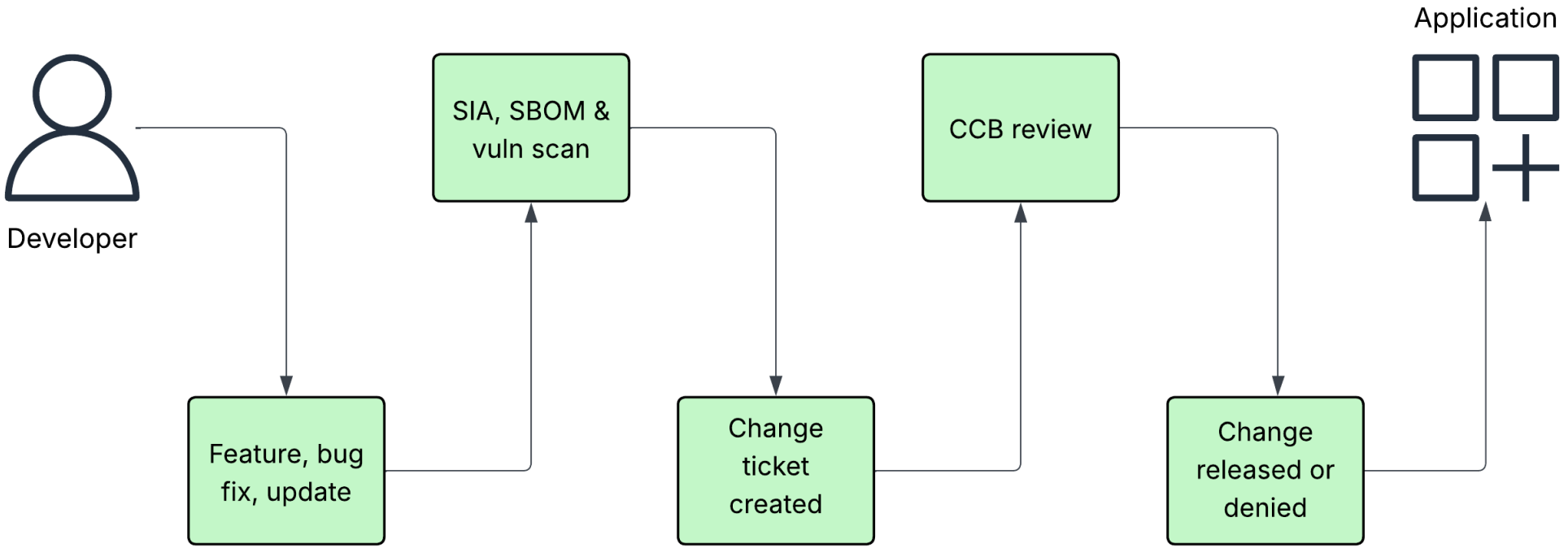


Web Consoles

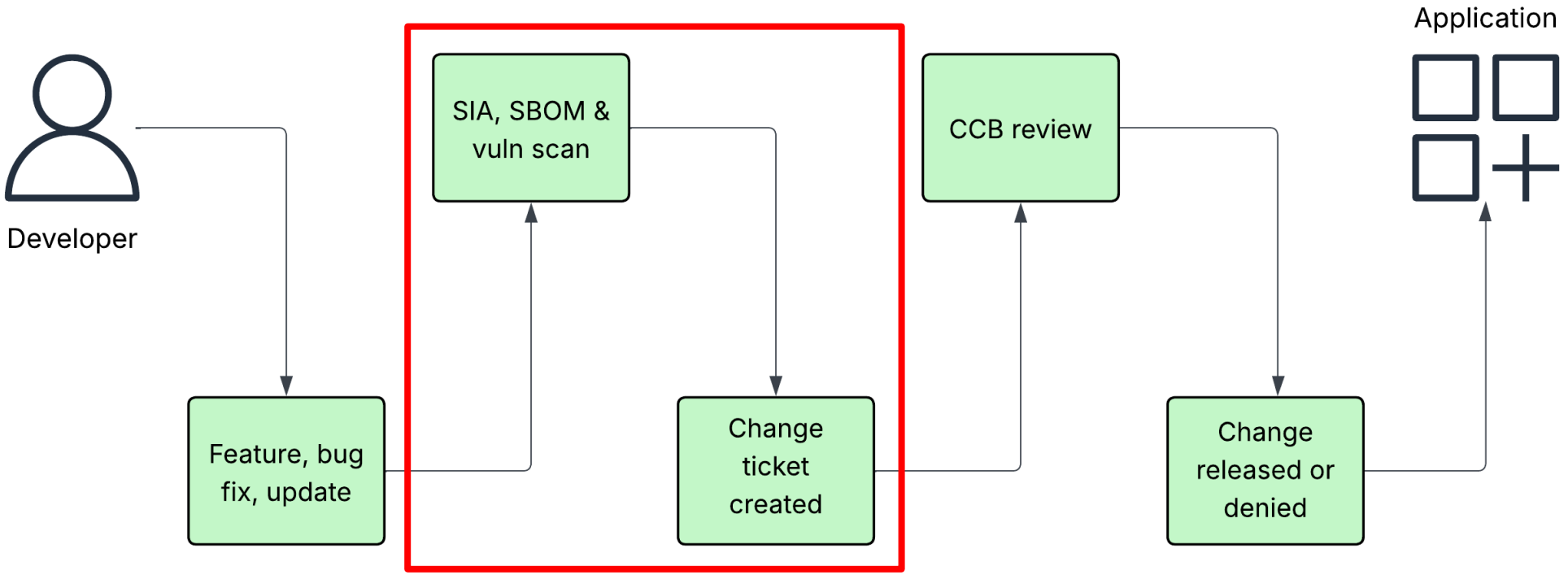


FedRAMP Boundary

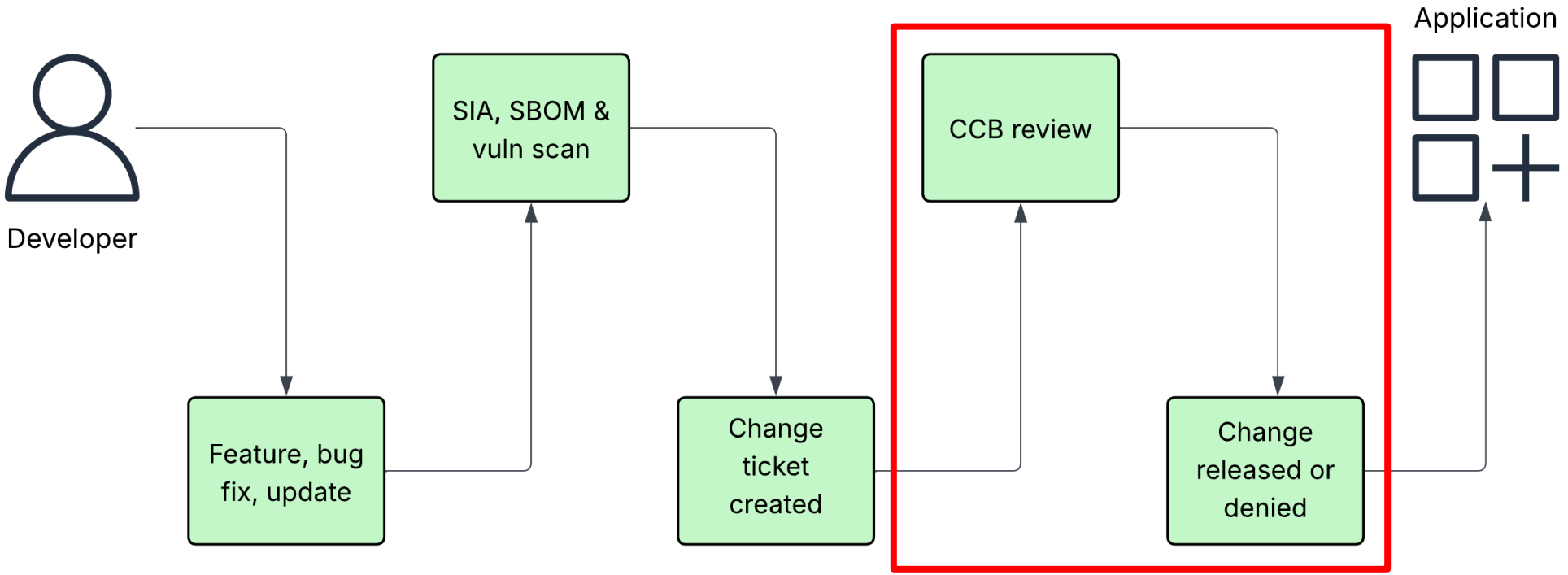
Challenge 3 – Change Management



Developer Experience Friction



Release Velocity Friction



Challenge 4 – Limited Tooling

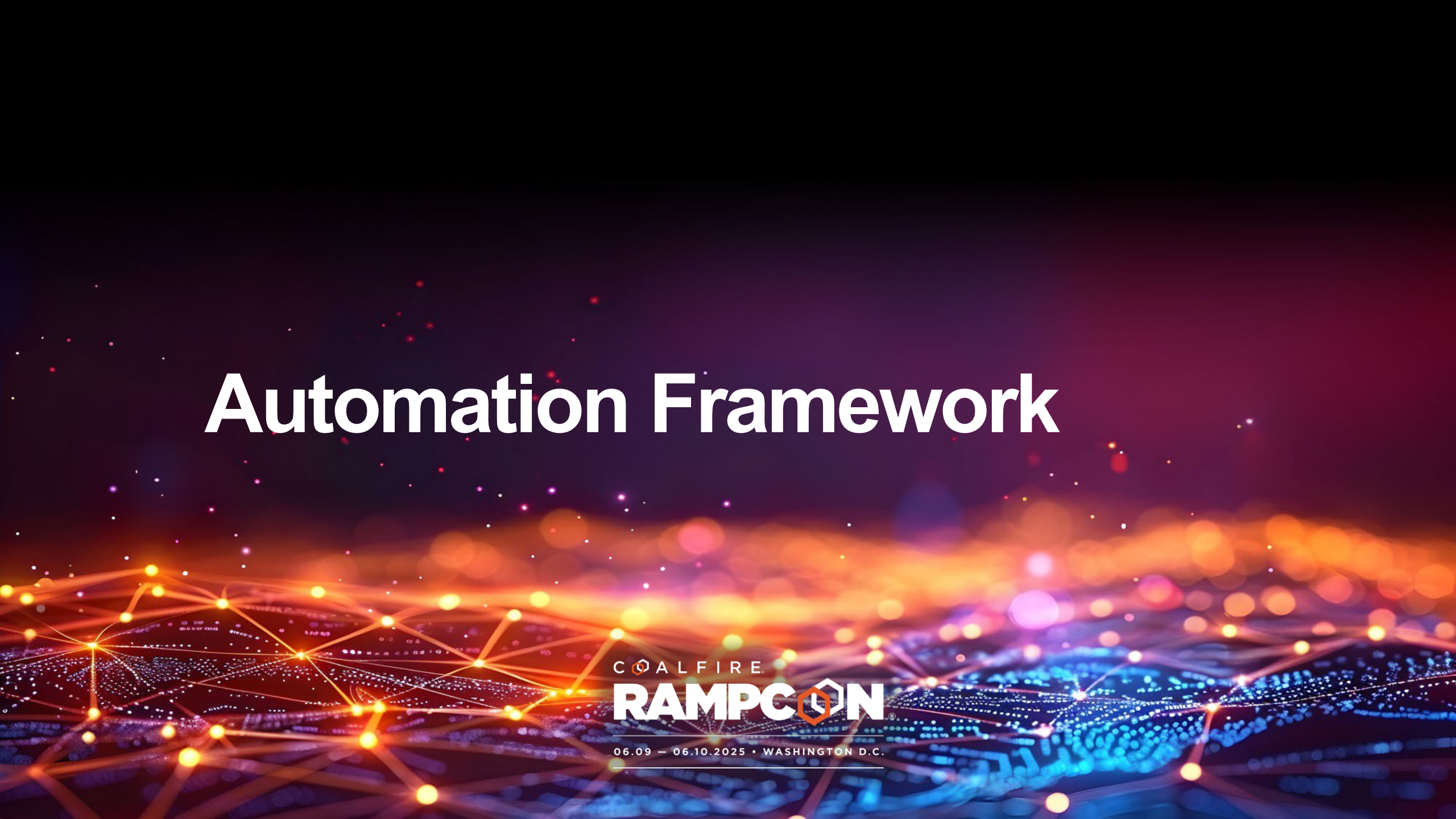
FedRAMP Authorized or Self-Hosted	FIPS-Validated Cryptographic Modules	Functionality

Small Subset of Industry Best-In-Class Tools

Recently Authorized CSOs

- **FedRAMP Moderate SaaS ticketing and CI/CD!**
  - 03/14/2025 – Atlassian Government Cloud
  - 05/15/2025 – GitLab Dedicated for Government
- **Reduced overhead and management of self-hosted tooling**

Automation Framework



Foundational Pillars



Compliance “Shift Left”

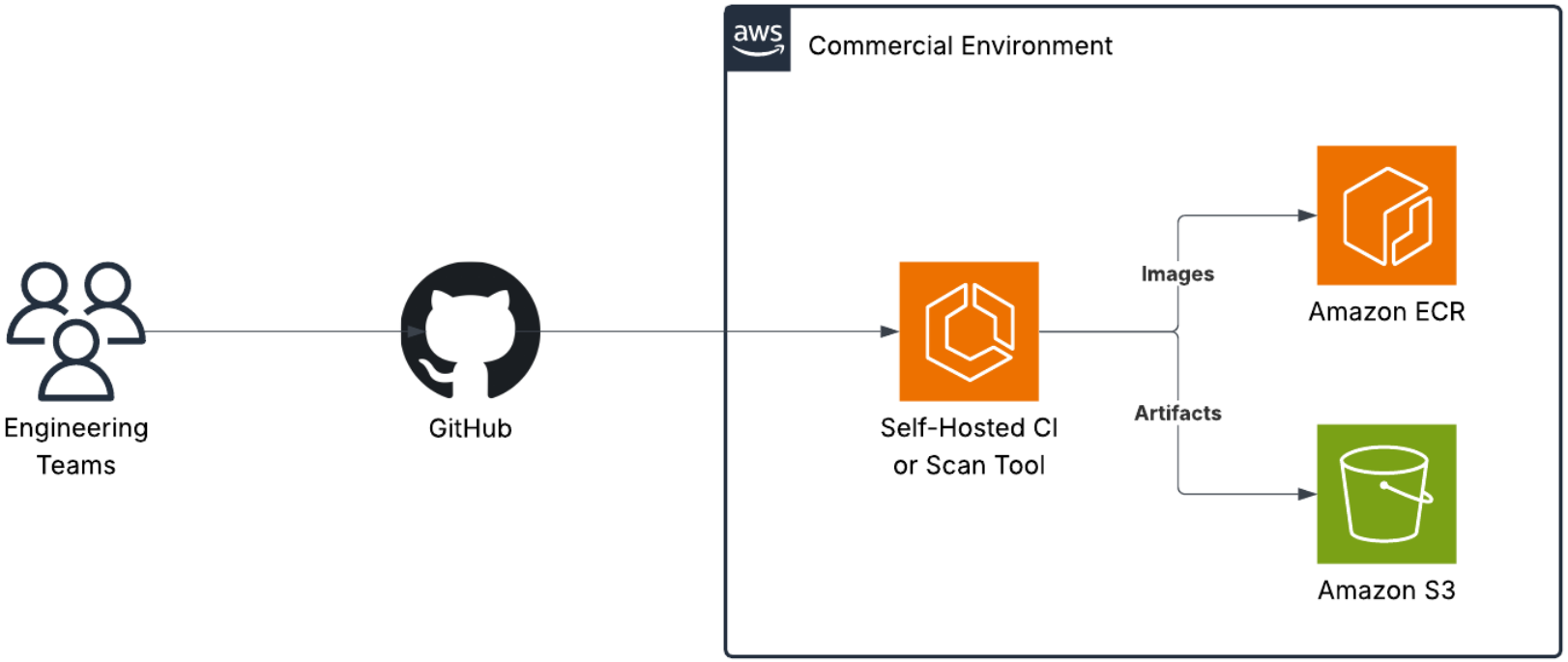


FedRAMP as a Consumer



Optimize Change Control with Automation

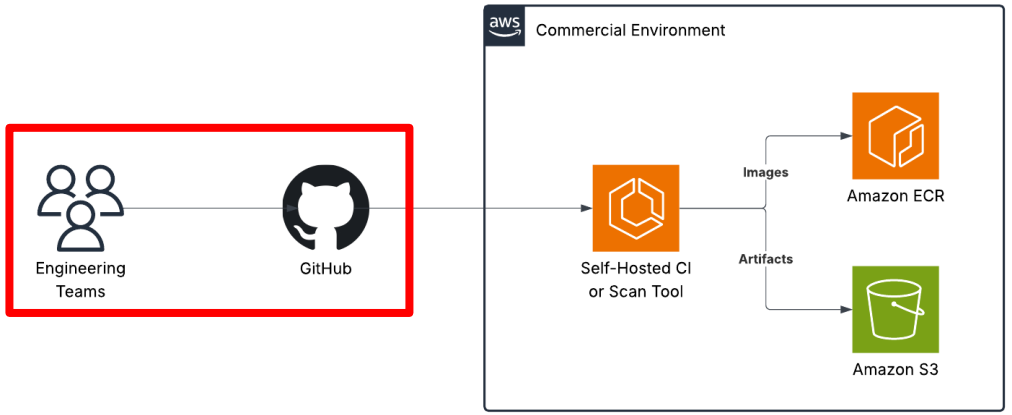
Shifting Compliance Left



Shifting Compliance Left

Compliant IaC

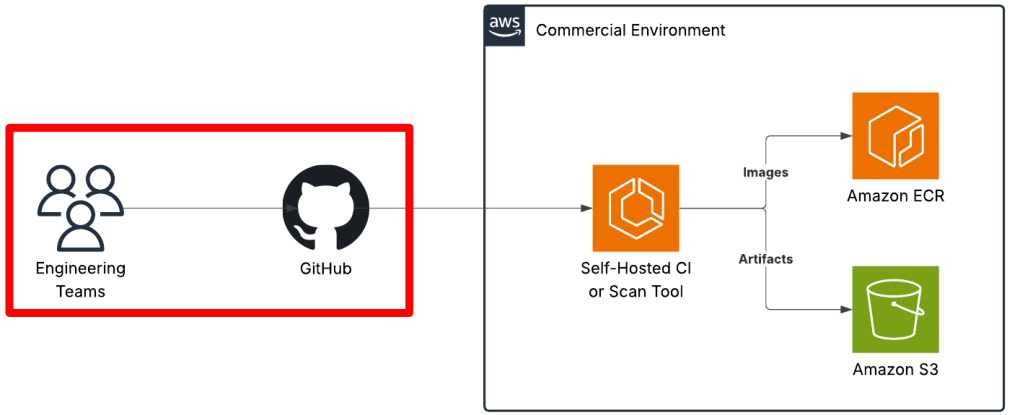
1. Utilize centralized module repository with ”building block” reusability in mind
2. Bake security best practices and compliance requirements into modules
3. Integrate vulnerability and compliance scans into pipelines
4. Re-audit usage and feedback cycle



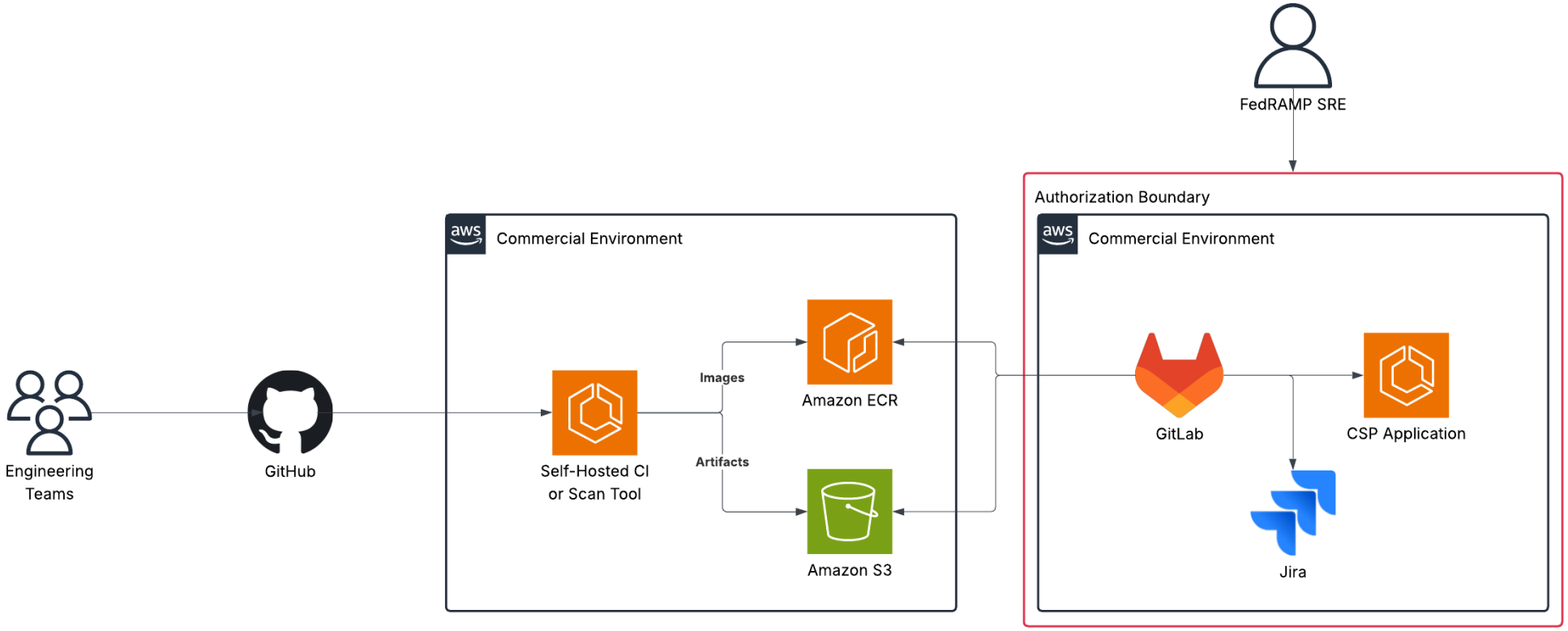
Shifting Compliance Left

Compliant Applications

1. Utilize feature flags to control FedRAMP app features
2. Integrate vulnerability and compliance scans into pipelines
3. Automate FedRAMP artifact creation

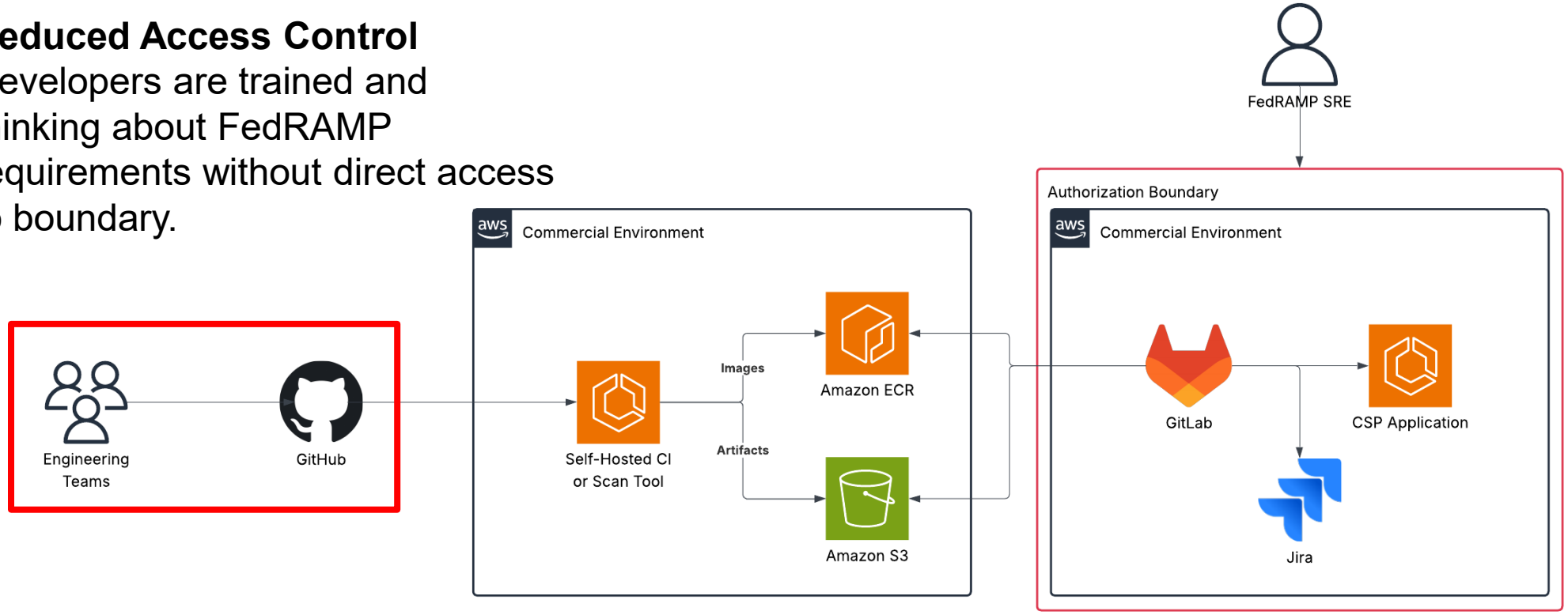


FedRAMP as a Consumer



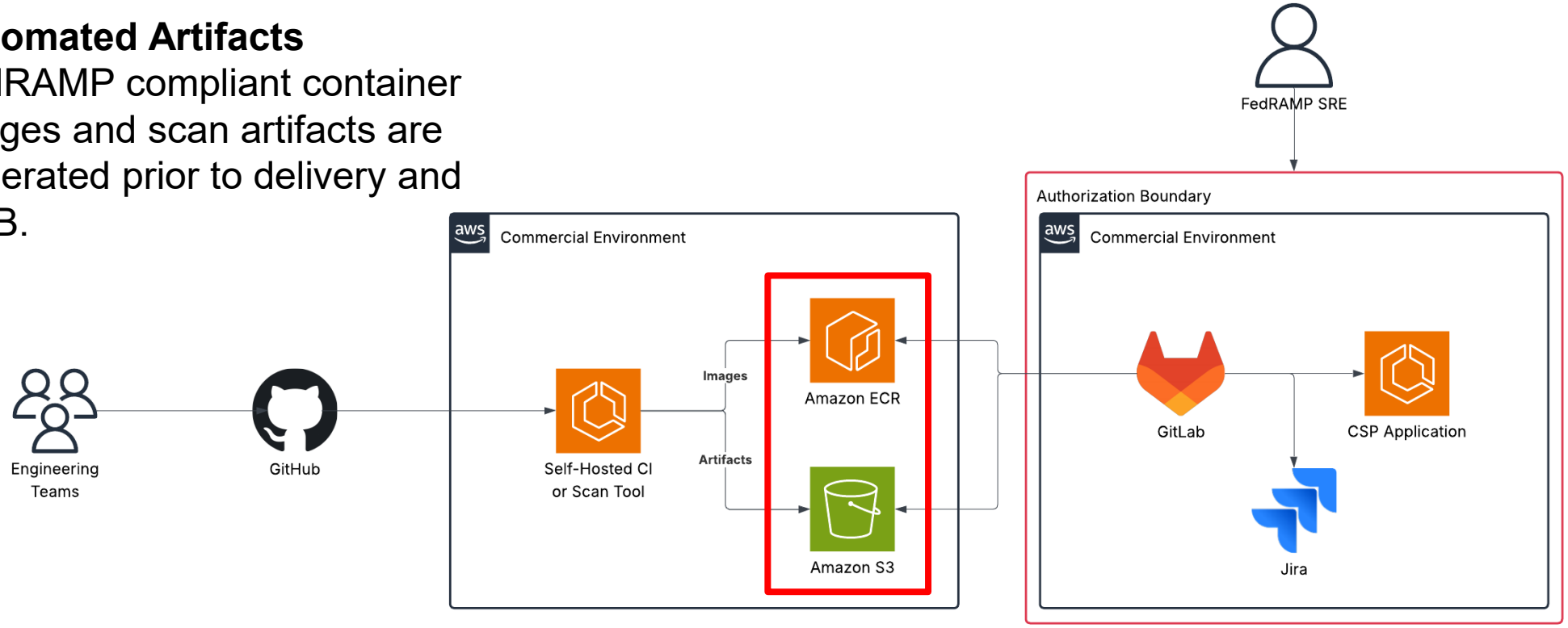
FedRAMP as a Consumer

Reduced Access Control
Developers are trained and thinking about FedRAMP requirements without direct access to boundary.



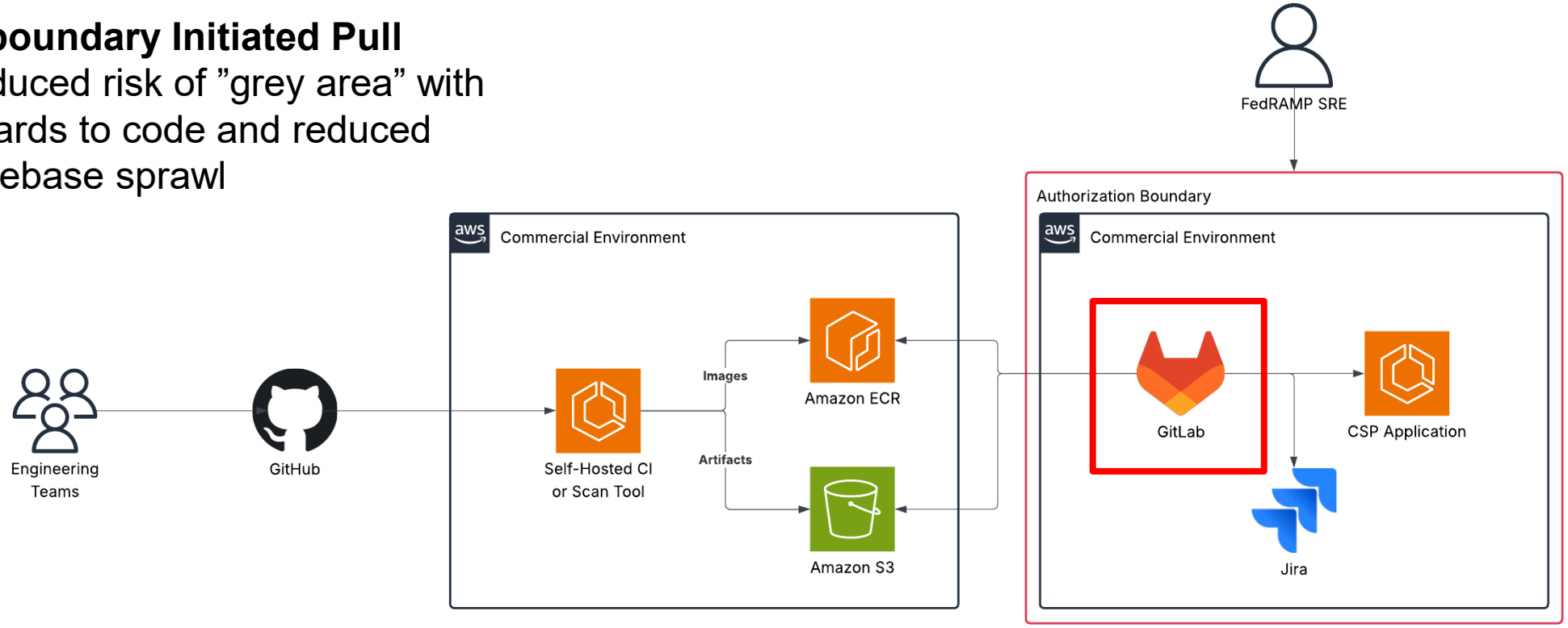
FedRAMP as a Consumer

Automated Artifacts
FedRAMP compliant container images and scan artifacts are generated prior to delivery and CCB.



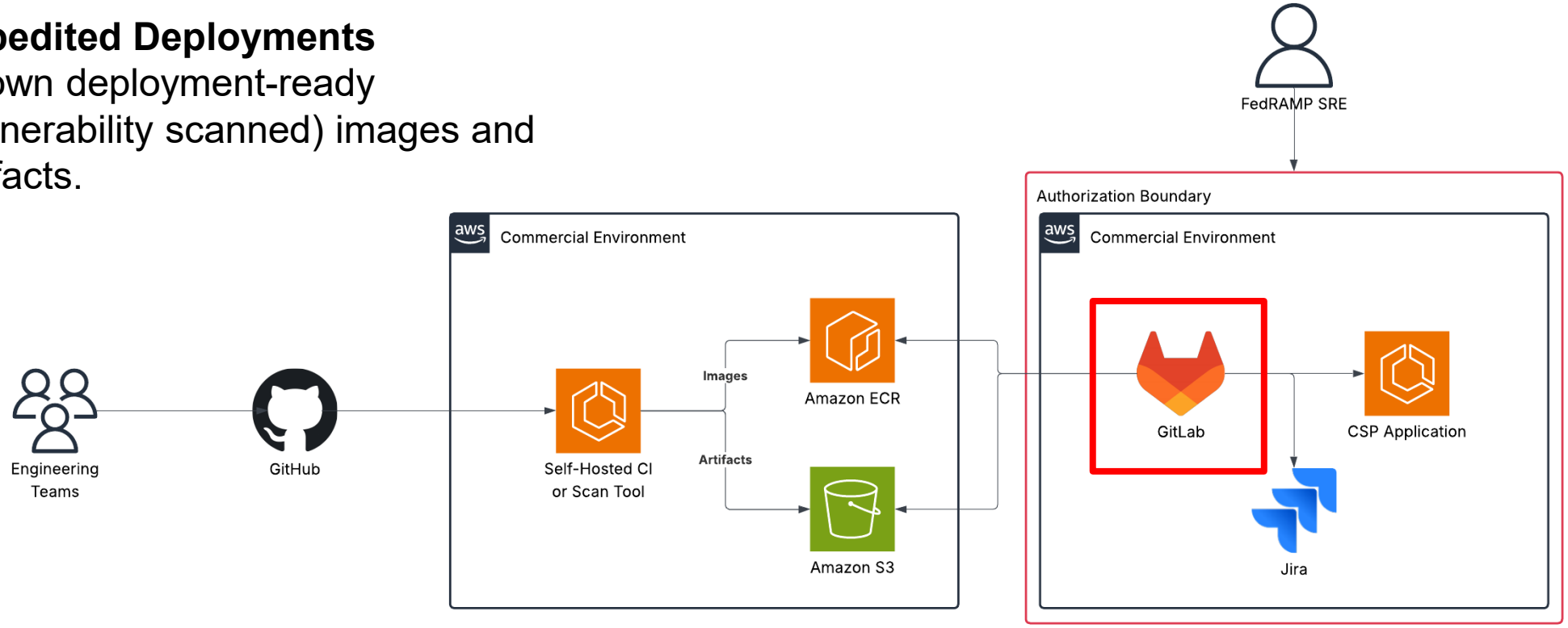
FedRAMP as a Consumer

In-boundary Initiated Pull
Reduced risk of ”grey area” with regards to code and reduced codebase sprawl



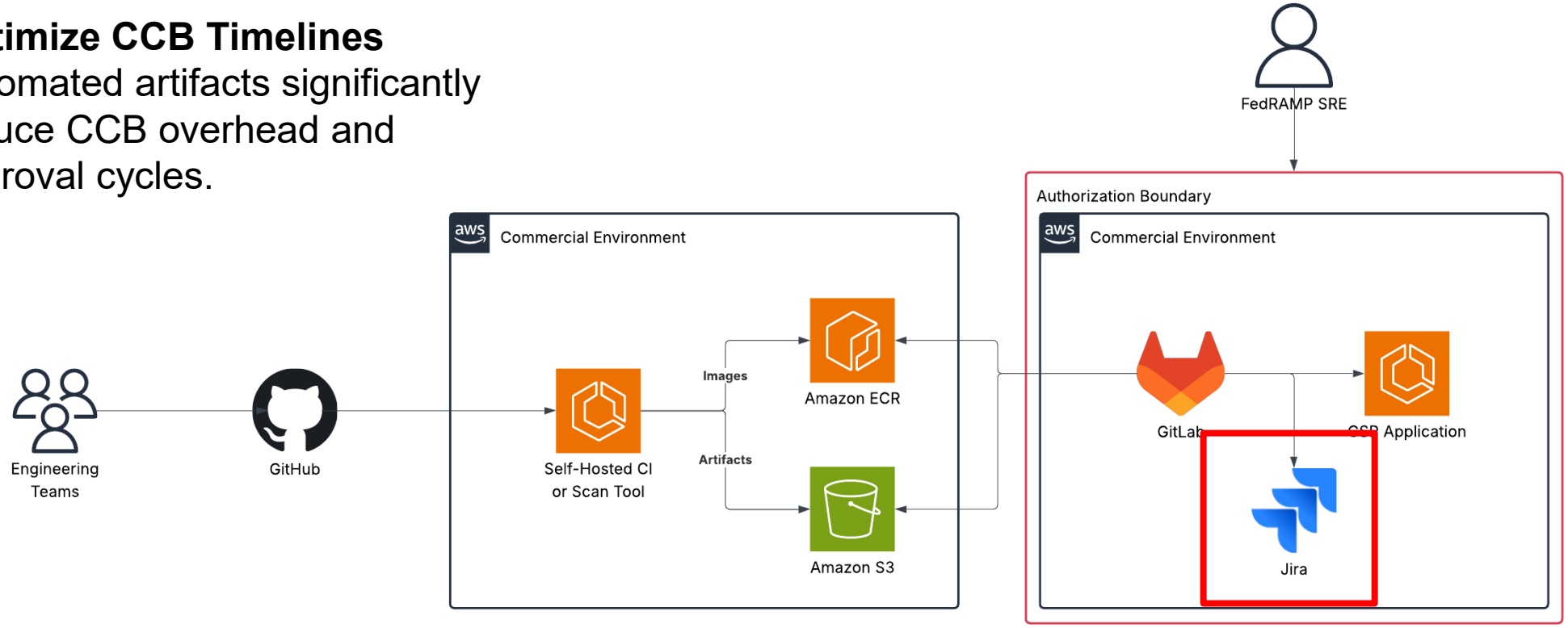
Optimize Change Control with Automation

Expedited Deployments
Known deployment-ready (vulnerability scanned) images and artifacts.



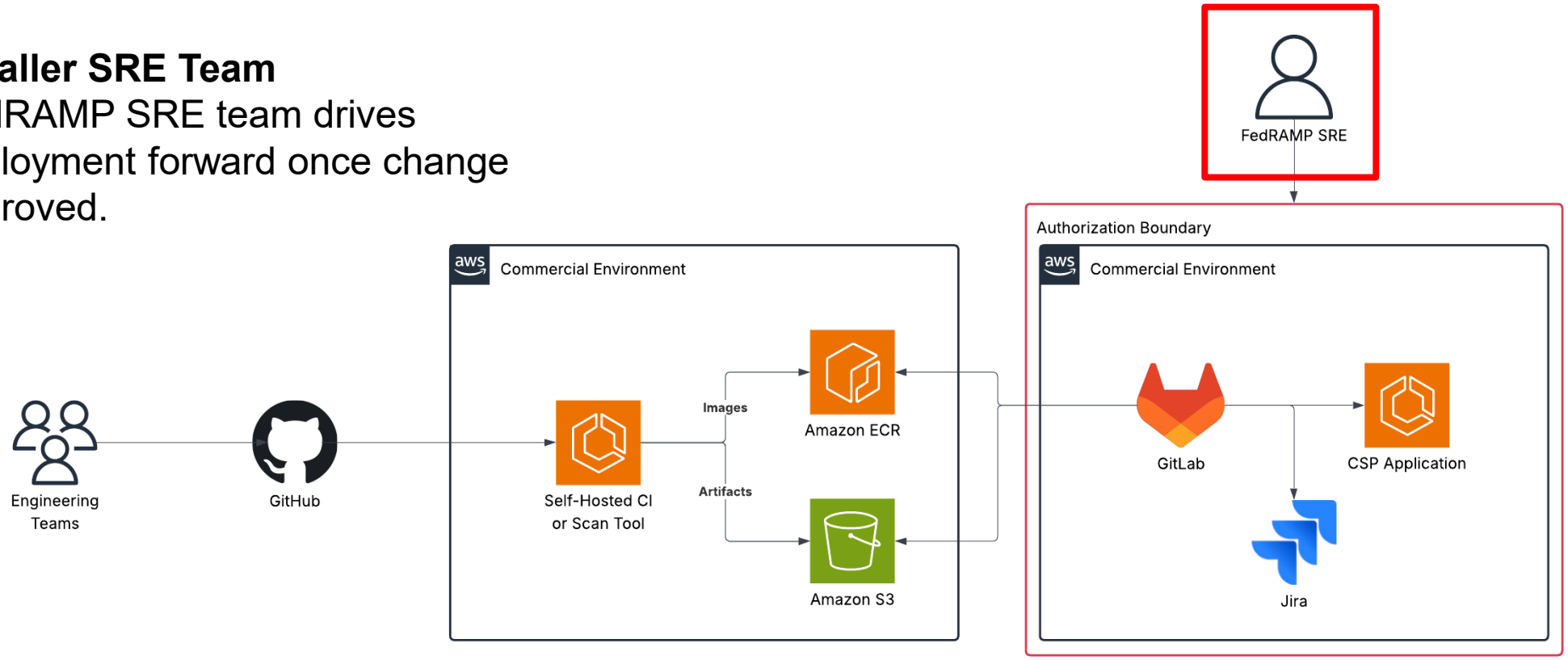
Optimize Change Control with Automation

Optimize CCB Timelines
Automated artifacts significantly reduce CCB overhead and approval cycles.



Optimize Change Control with Automation

Smaller SRE Team
FedRAMP SRE team drives deployment forward once change approved.



Foundational Pillars



Shift Compliance Left

Embed FedRAMP compliance in existing developmental practices reduces new systems and overhead while shortening development cycles.



FedRAMP as a Consumer

Making FedRAMP a consumer rather than standalone reduces the need for new tools and shortens deployment timelines by reducing systems in scope of audit.



Optimize Change Control with Automation

Change control can be expedited with automation and artifacts, saving hours to days.

Conclusion



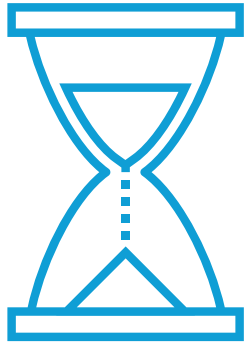
Automating FedRAMP CI/CD



CI/CD is achievable in FedRAMP with minor adjustment to staff, processes & tooling



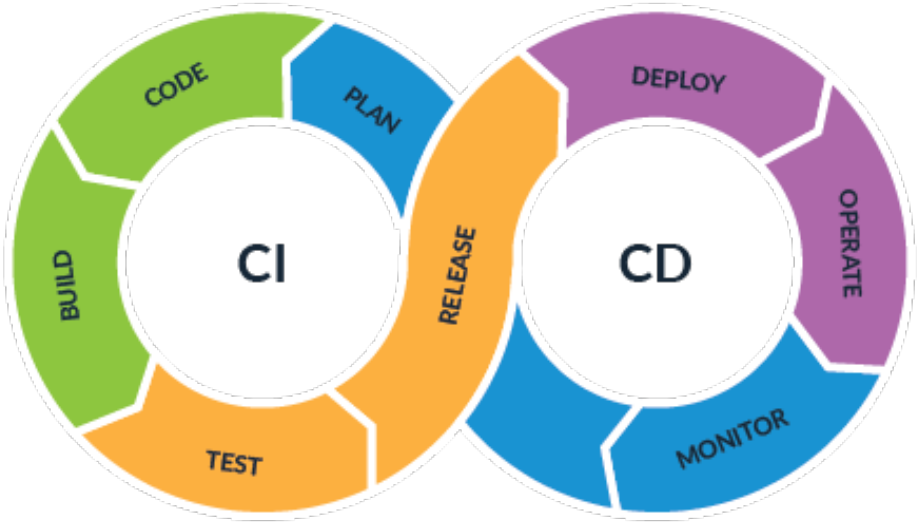
Commercial application code SDLC can remain untouched allowing for development outside of boundary



Move with similar velocity as commercial while achieving FedRAMP compliance

Automating FedRAMP CI/CD

Build
Shift compliance left into commercial SDLC. Remediate vulnerabilities outside of boundary.



Deploy
Automated deployment allows for small FedRAMP SRE team. Portable code allows development to occur outside of boundary.

Release
Automate compliance artifact creation. Continue to iterate on friction points.