DevSecOps для современных приложений
Подходы и процессы

Михаил Кадер, инженер

mkader@cisco.com
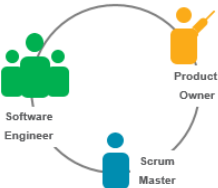
2 июня 2021

Cisco IT Transformation Journey

"We Develop, We Secure & We Operate"

Software Engineer

Product Owner

Scrum Master

Architecture Led: Services Orientated
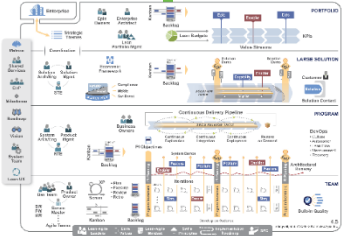
Scaled Agile Maturity

2007

2017

2019

Pervasive Agile Mindset

DevSecOps

DevSecOps

"Empowered development team takes full ownership of how their application behaves in production including security"

DevSecOps is all about to get development teams to make certain mindset shifts and adopt security practices into their daily activities which requires healthy collaboration and mutual trust between development and security teams.

Some fundamental thoughts

"Mindset & Cultural Shift "

- How well you actually know what you are talking about ? (Credibility)

- How often and quickly do you do what you say ? (Reliability)

- How much you show that you care about someone else's interests ? (Empathy)

- How apparent it is that your words and actions are in your own interest ? (Self-interest)

- How much trust you have with each other ? (Trust)

DevSecOps via Trust & Empowerment

trust = (credibility + reliability + empathy) / self-interest
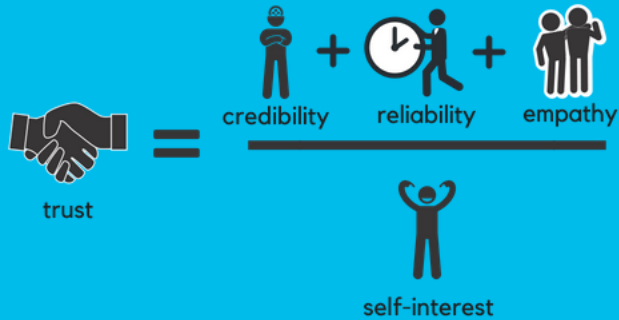
DSO Core Team Formation

Workshops with IT Service Owners and commitments

Consolidation of models, Enabling or facilitating capabilities, filling gaps
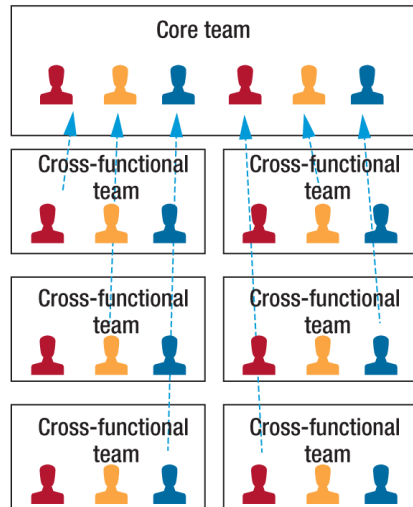
Transformation & Measurement

The DevSecOps Core team act as enabler and advisors, to make sure the development team has all the information necessary to make empowered decisions while trusting them for decision towards "the right thing" and help baking security via automated enabled security tools and process to their SDLC with the speed of business.

Cisco IT Transformation towards DevSecOps

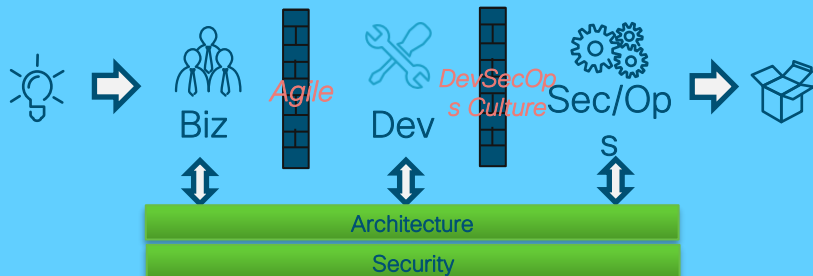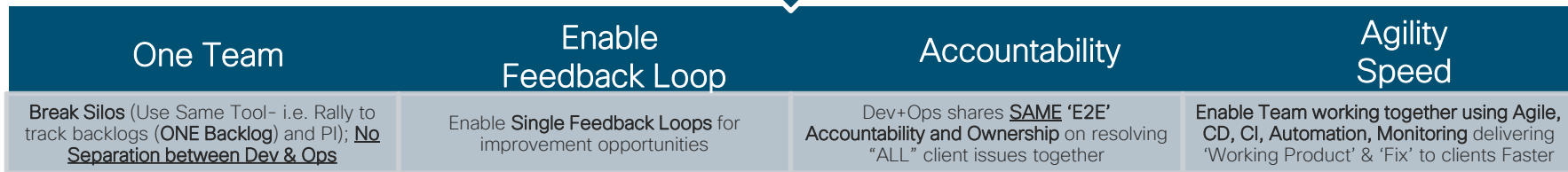*"DevSecOps is cultural movement that furthers the movement of Agile and DevOps into Security"*

DevSecOps

DevSecOps mantra:
Start small & Build; Measure; Learn

Leadership & management commitment
to drive transformation is required

One Team	Enable Feedback Loop	Accountability	Agility Speed
Break Silos (Use Same Tool- i.e. Rally to track backlogs (**ONE Backlog**) and PI); <u>No Separation between Dev & Ops</u>	Enable **Single Feedback Loops** for improvement opportunities	Dev+Ops shares <u>SAME</u> 'E2E' **Accountability and Ownership** on resolving "ALL" client issues together	Enable Team working together using Agile, CD, CI, Automation, Monitoring delivering 'Working Product' & 'Fix' to clients Faster

Biz

Agile

Dev

DevSecOps Culture

Sec/Ops

Architecture

Security

Outcome
- ✓ Security
- ✓ Break Down Silos
- ✓ Faster time to Release Product
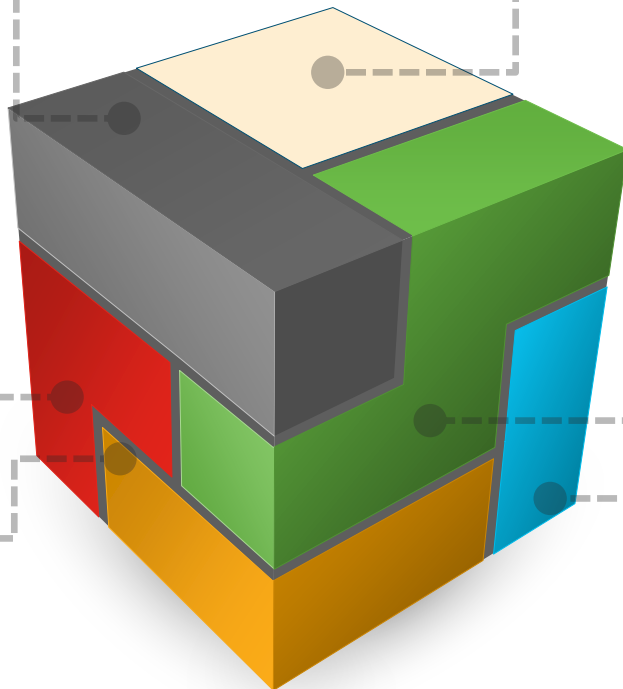- ✓ Improved Quality
- ✓ Operational stability
- ✓ Experience

DevSecOps Cisco IT Focus Areas

Leadership Support in People/Workforce Culture Transformation

Enable Automation Everywhere- Automated Testing, Deployment

Agile Methodology

Use DevOps Tools, Continuous Delivery(CD) & Continuous Integration(CI) Toolset- Docker, Git, Jenkins, Puppet etc…

Enable Security in Architecture, Code, and Operations

Enable E2E Monitoring- AppD, Splunk etc

How we are driving Security in DevSecOps

Automate Security (Security as Code)

Define Built-In Security

Agile Security (Hackathons)

Driving Security in DevSecOps
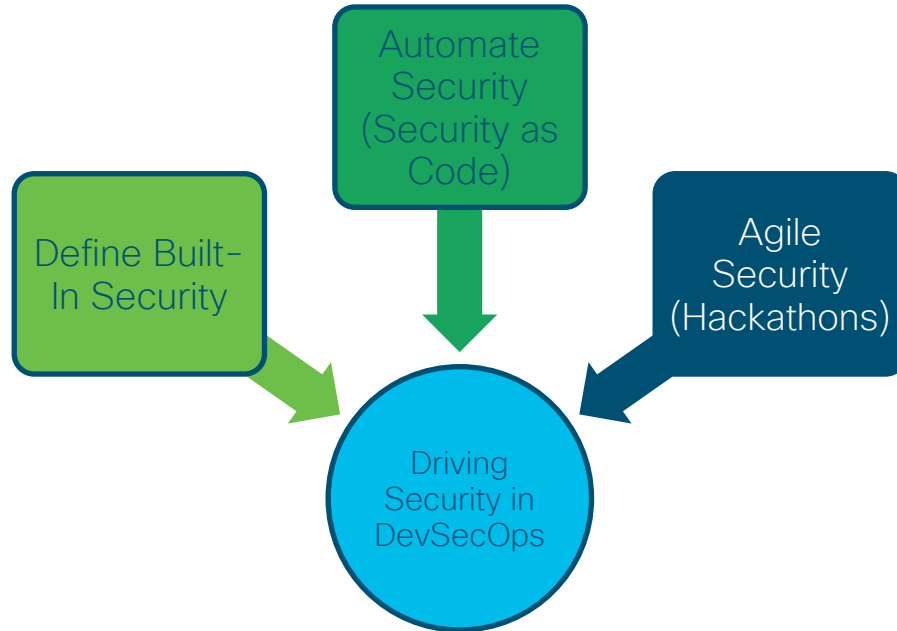
Continuous Security Buddy

Why Security is different in DevSecOps

"Security in DevSecOps is all about built-in security instead of standalone function as a perimeter around data and apps"

Build Security In more than bolt it on

Rely on empowered development Teams more than security specialists
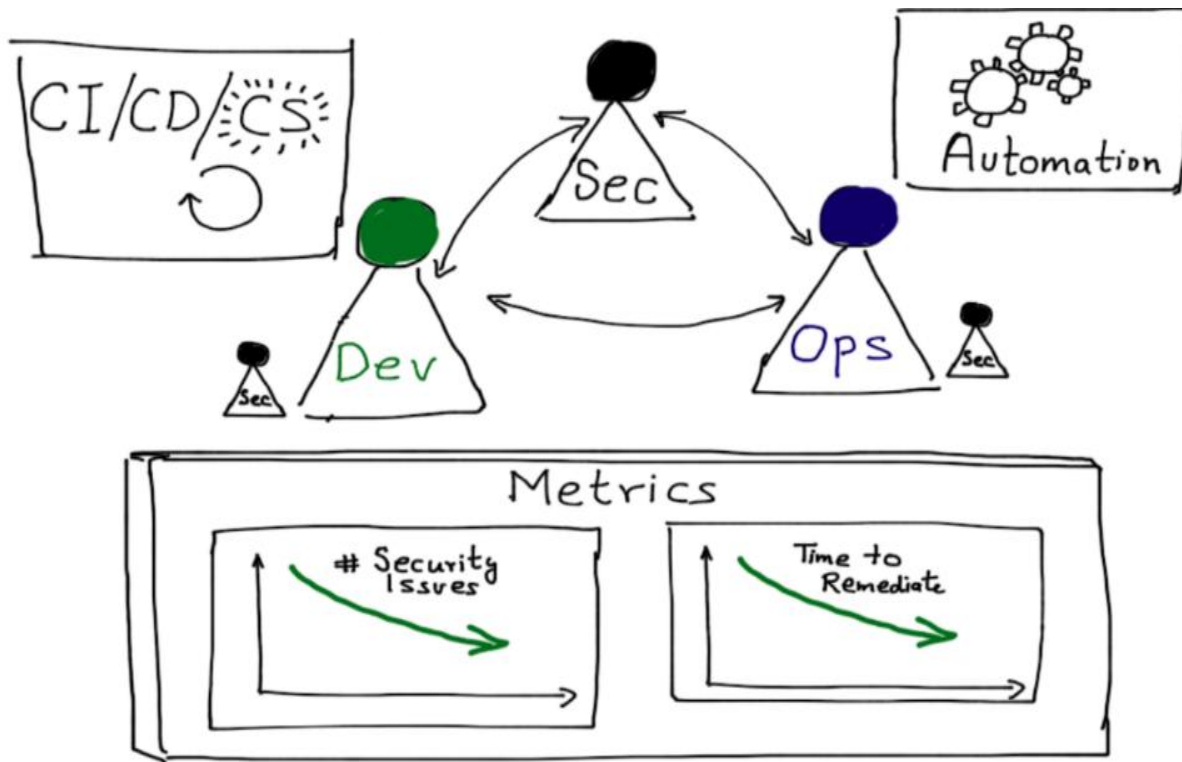
Implement Features securely more than security features

Rely on continuous learning more than end-of-phase gates

Build on culture change more than policy enforcement

Security in DevSecOps

DevSecOps: Embed Security

Security in DevSecOps

- Security bridges Dev & Ops
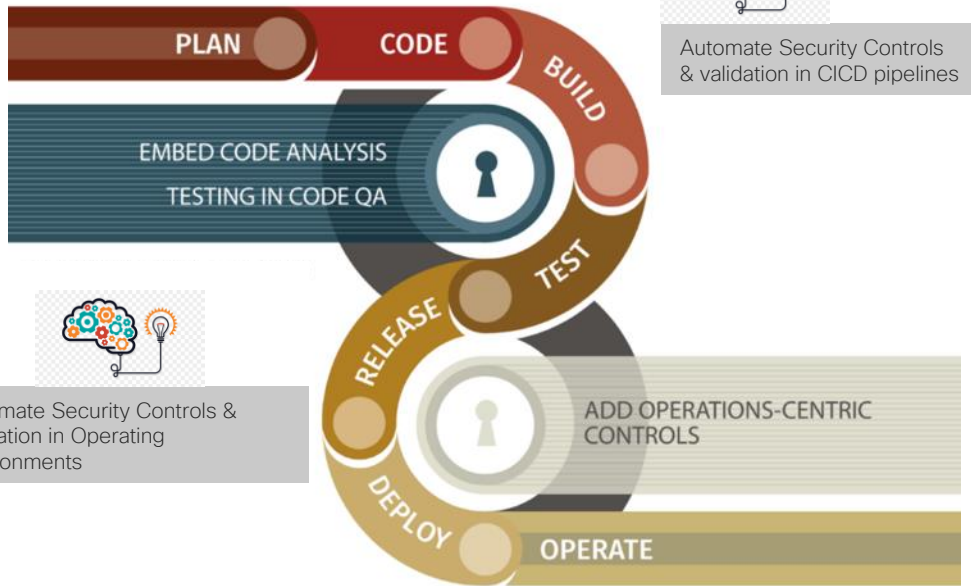- Automation in Scale
- Promotes Self-Service
- Trust & Verify
- Value Add Real Time Metrics

DevSecOps: Security Implementation as Code

Continuous Security Buddy (CSB)

PLAN   CODE   BUILD

EMBED CODE ANALYSIS
TESTING IN CODE QA

TEST

RELEASE

Automate Security Controls & validation in CICD pipelines

Automate Security Controls & validation in Operating environments

ADD OPERATIONS-CENTRIC CONTROLS

DEPLOY   OPERATE

CSB: Pipeline Edition

- Third Party Lib
- PSB Validation and Reporting
- Static Scan
- Web and API Scanning
- Hardening Checks
- Credentials Management

CSB Pipeline

CSB: Platform Edition

- IAM
- logging & Monitoring
- Network
- Compute
- Storage

CSB Platform

Continuous Security Buddy (CSB) Platform edition

IAM

Audit Checks to ensure MFA, SSO, Access Key Rotation and Root login usage, no non-cisco identities, Password Policy

CSIRT monitor the IaaS infra, CIS Benchmark controls,

logging & Monitoring

Network

Bastion Host Check, Wide open security groups, External Surface

CSB Platform

Qualys Scan external facing hosts Hardened AMIs

Compute

Storage

Misconfigured Storage Policies, Missing tags/labels, Untrusted images, Misconfigured Encryption Policies

CSB Pipeline Edition

CSB Pipeline

Third Party Lib

Automate integration with Corona/Blackduck tools to identify and register in IP Central.

Static Scan

Integrate CICD pipeline with source code static analysis tools

Hardening Checks

Perform OS and container hardening checks during build/deploy stages

Credentials Management

Integrate secure management of keys and service credentials in vault

Web and API Scanning

Perform Web and API scanning during build/deploy stages

PSB Validation and Reporting

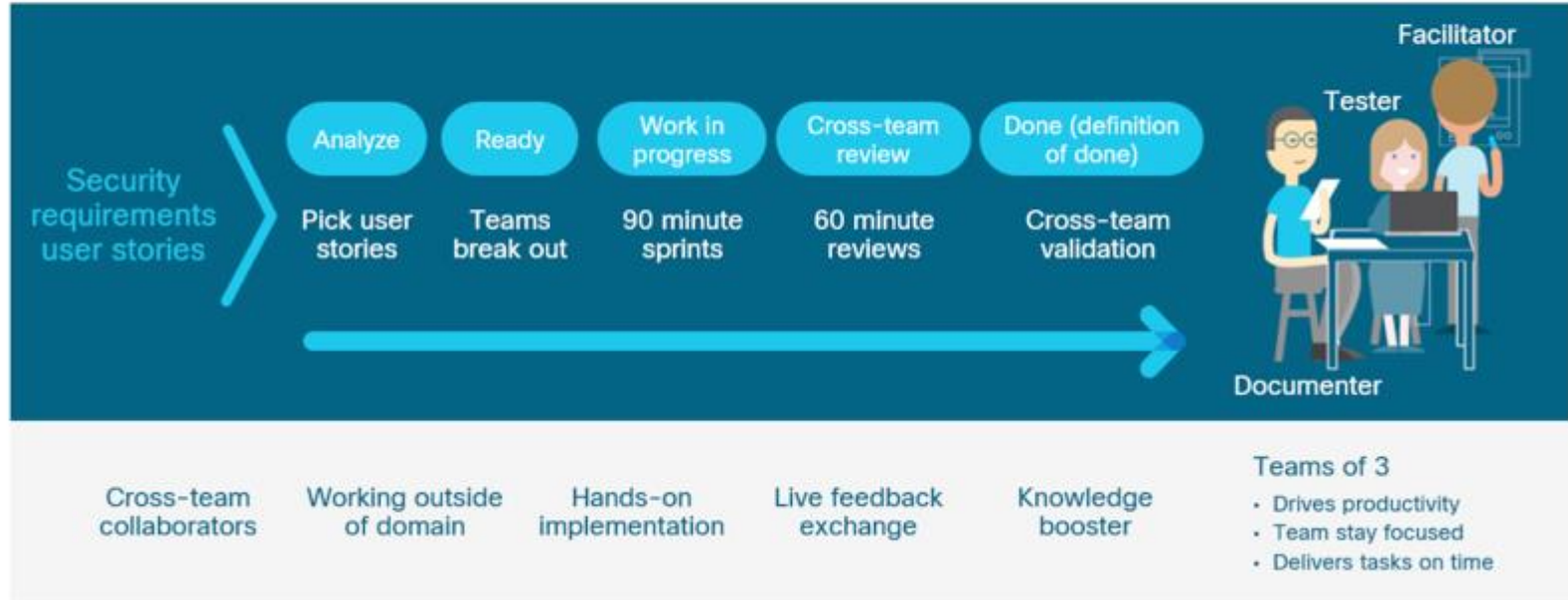Validate appropriate PSBs and integrates with backend reporting tools such as Jira/CDA/USM
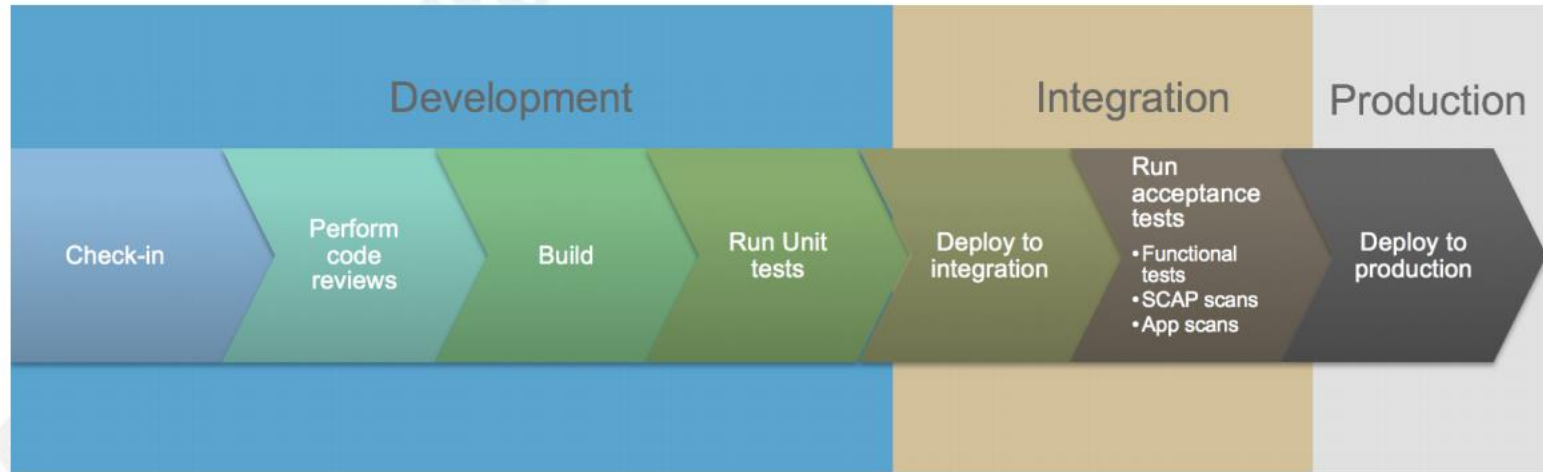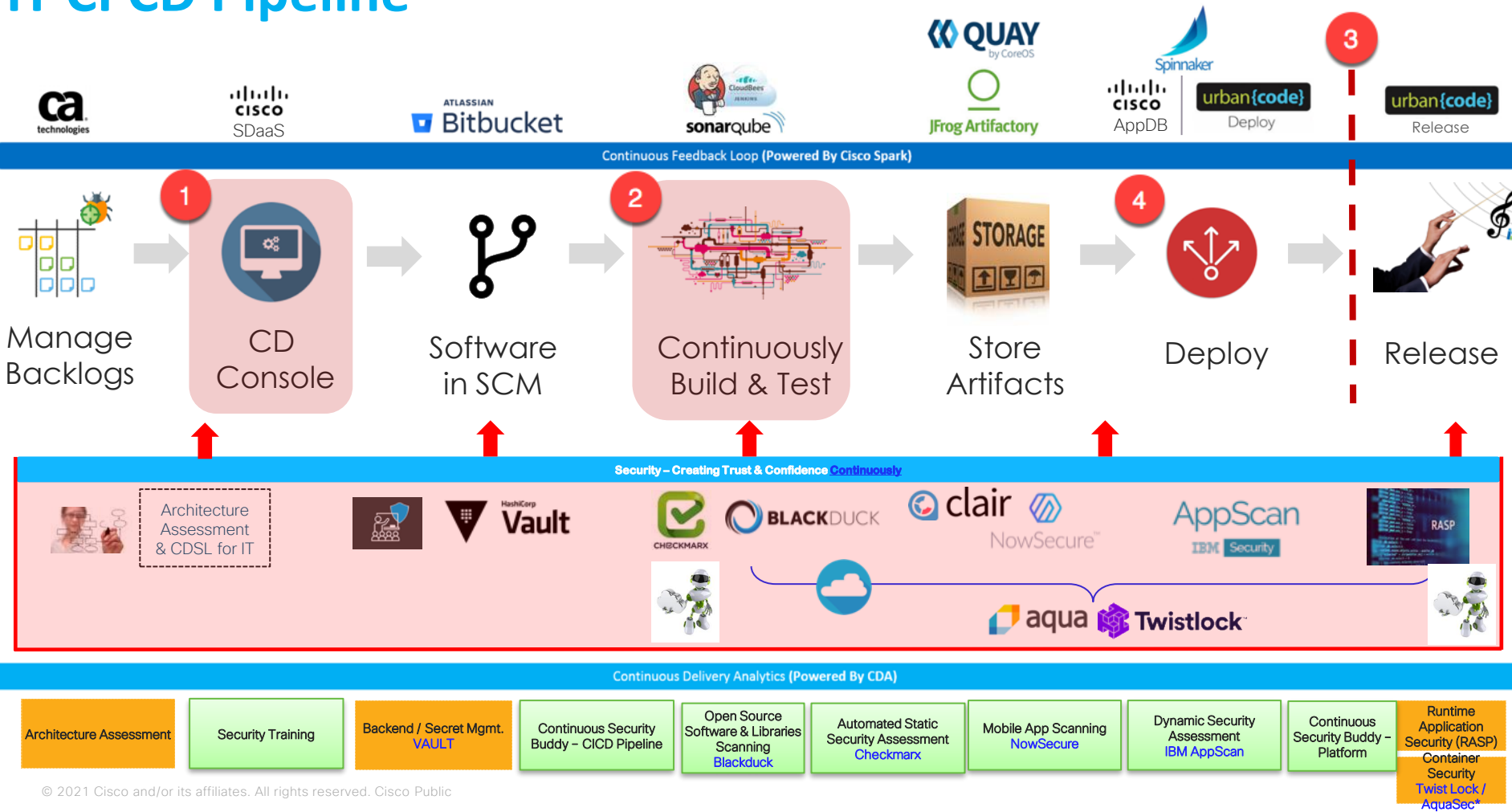
Agile Hackathons (Security)

Agile Hackathon: Testing real use cases

Security Testing and Continuous Deployment

IT CI CD Pipeline

DevSecOps Business Outcome

Operational Excellence
significant reduction in production cases

Velocity
Increased business value delivered
Velocity

Experience
Reduction in
Change Lead time
Mean Time To Resolution

DevSecOps

Security
Baked in Security
USM Score

Вопросы?