Security Compass

Achieving Continuous Compliance in DevOps Programs

DevSecOps Days 2021 – Los Angeles

Arun Prabhakar

DevSecOps Consultant

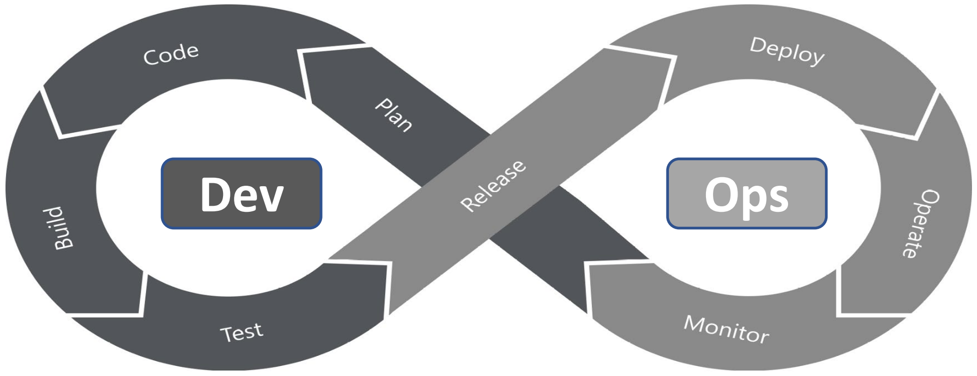
Definitions and Objectives

- Security and Compliance
- Compliance goals
- Continuous Compliance
- Compliance as Code
- Accomplishing Continuous Compliance
  1. How to implement the security concepts
  2. How to organize the security teams

Fit Security in DevOps

Security in the Pipeline

- Authentication as Code
- Privacy as Code
- Security Policy as Code
- Process as Code
- Codifying the Security Best Practices



Security of the Pipeline

- Security of code repository
- Security of orchestration platforms
- Security of third-party integration and automation tools
- Setting secure configuration, logging of Cloud services

Security for the Pipeline

- Architecture Security
- Threat Modeling
- Risk Management
- Periodic Security Audits
- Infrastructure Assessments
- Composition Analysis

Security beyond the Pipeline

- Planning & Management
- Budgeting & Resourcing
- Evangelism & Training
- Culture & Process

Accomplishing Objectives –

How to implement the security concepts

Codifying Security in DevOps

All **Security principles**, **tools**, defensive mechanisms and the verification logic should be codified

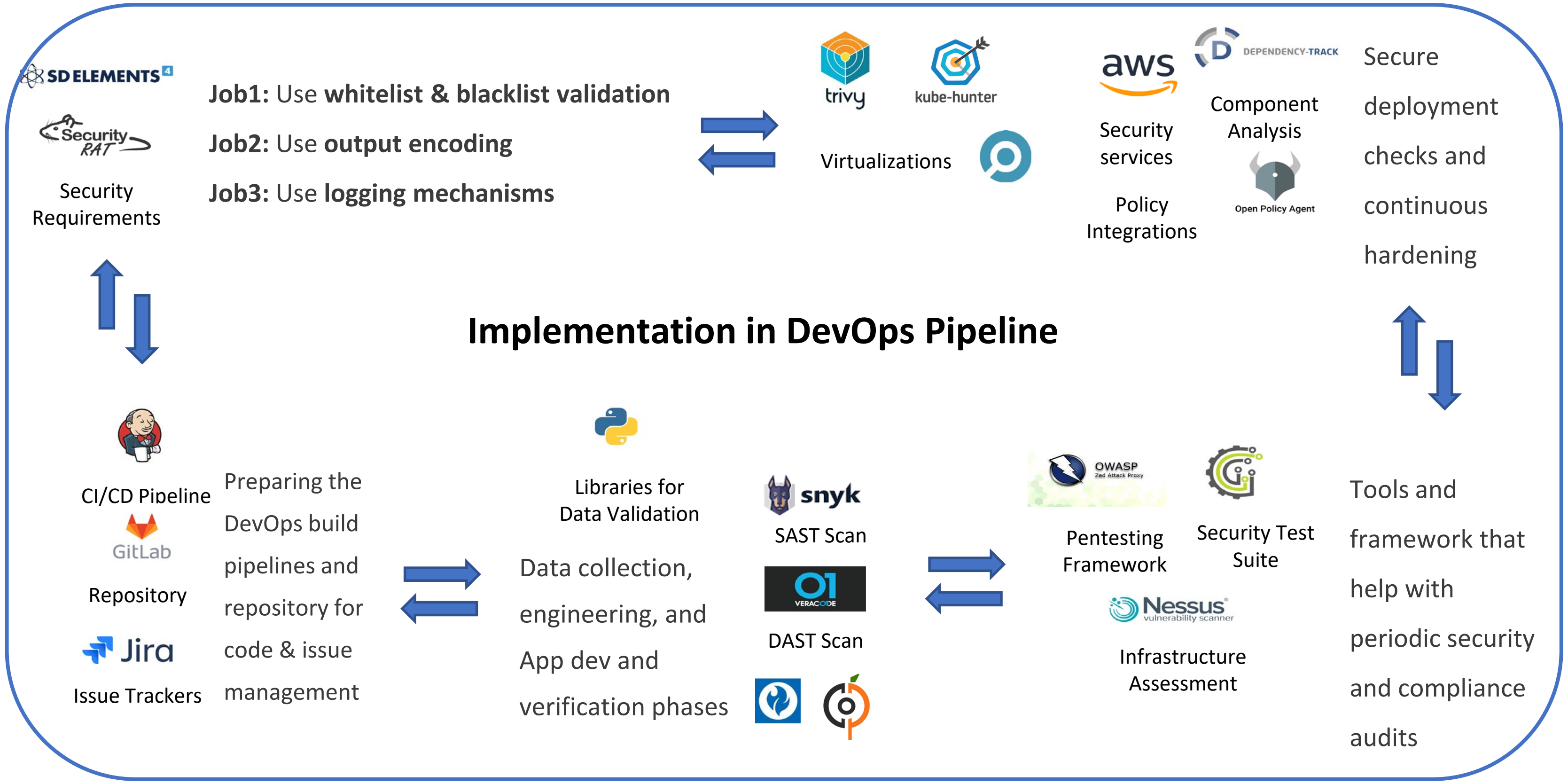
Every phase of the product development program need to be secure & codified

All requirements, mandated by regulations, **policies** MUST be completely codified

Security is a process, and every **process step** must be codified

Implementation of Continuous Compliance

Business Mandate	Applicable Regulation	Data Validation Requirement	Description	Controls Identified
Software Product has a mandate to adhere to regulations on **data protection**	Follow **GDPR regulations** to adhere to all the data protection regulations	Article 25 / Recital 78 is one of the req identified by the **Security team** for the Project	There must be Data protection by design and by default. Obligation to meet appropriate technical and organizational measures	**Data Validation** on all forms of internal and external user Input



Implementation in DevOps Pipeline

Security Requirements

Job1: Use **whitelist & blacklist validation**

Job2: Use **output encoding**

Job3: Use **logging mechanisms**

Virtualizations

Security services

Component Analysis

Policy Integrations

Secure deployment checks and continuous hardening

CI/CD Pipeline

Repository

Issue Trackers

Preparing the DevOps build pipelines and repository for code & issue management

Libraries for Data Validation

Data collection, engineering, and App dev and verification phases

SAST Scan

DAST Scan

Pentesting Framework

Security Test Suite

Infrastructure Assessment

Tools and framework that help with periodic security and compliance audits

Accomplishing Objectives –

How to organize the security teams

Security Champions

White Teamer

Who are they? : A functional role, strategizing events to foster better collaboration among all security teams.

Champion Responsibilities :

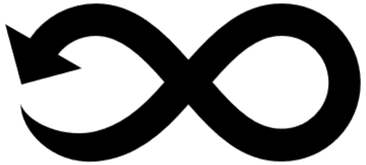
- Auditing the programs
- Planning the complete process steps
- Coordinating among all the teams
- Taking accountability of actions

Purple Teamer

Who are they? : A technical role, act as bridge-builders primarily between the defensive and offensive teams.

Champion Responsibilities :

- Performing Due diligence
- Defining validation strategy
- Planning the Security tests
- Determining Cost-benefit tradeoff



Achieving Continuous Compliance

- ✓ Continuous Governance
- ✓ Process Automation
- ✓ Knowledge Management
- ✓ Continuous Management
- ✓ Continuous Collaboration

- ✓ Continuous Monitoring
- ✓ Continuous Training
- ✓ Continuous Verification
- ✓ Continuous Reviews
- ✓ Continuous Reporting

Best Practices and Next Steps

- Continuous Everything will lead to Continuous Compliance
- Perform Threat Models well ahead
- Monitor your security Architecture
- Getting trained in Secure Coding
- Test Driven Security
- Automate Everything
- Learning to speak the same Language
- Knowledge management
- Involve a Security Champion

Thank You

Arun Prabhakar

https://www.linkedin.com/in/arun-prabhakar/

https://arunp14sec.medium.com/

Interested in

- Collaboration
- Research
- Learning
- Projects