



# Scaling Your DevSecOps with Compliance: From Bottleneck to Business Enabler

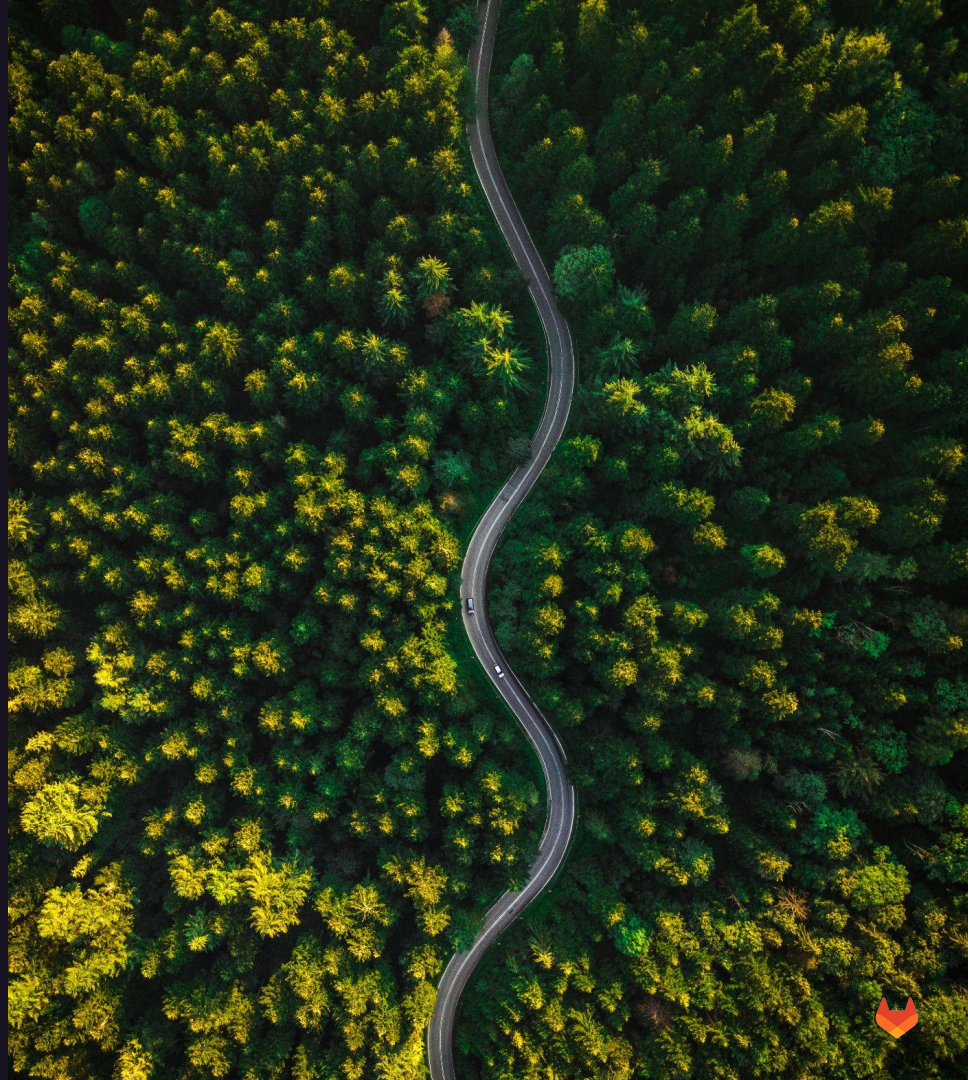
# Tomasz Skora

Staff Solutions Architect, ANZ

GitLab



# Introduction



# The challenges we hear today



## Developer Productivity



## Unified Governance and Compliance



## Operational Efficiency

### Challenges

How do we reduce the compliance burden on developers and embed it into workflows?

How do we consistently enforce security & compliance policies across teams and environments?

How do we scale security efforts with limited personnel and increasing demands?

### Side effects

Developers bypass security steps.  
Compliance seen as a blocker

Inconsistent security  
Increased complexity & conflicting rules  
Audit and reporting gaps

Backlogs in risk review  
Over-reliance on manual work  
Burnout in Compliance & Sec teams

Compliance Fatigue

Governance Fragmentation

Security Resource Constraints

# Market & customer expectations are changing more rapidly than ever

Development teams must increase their **velocity** and **security** to match.



Software **released 2x+ faster** in 2025 by most of companies

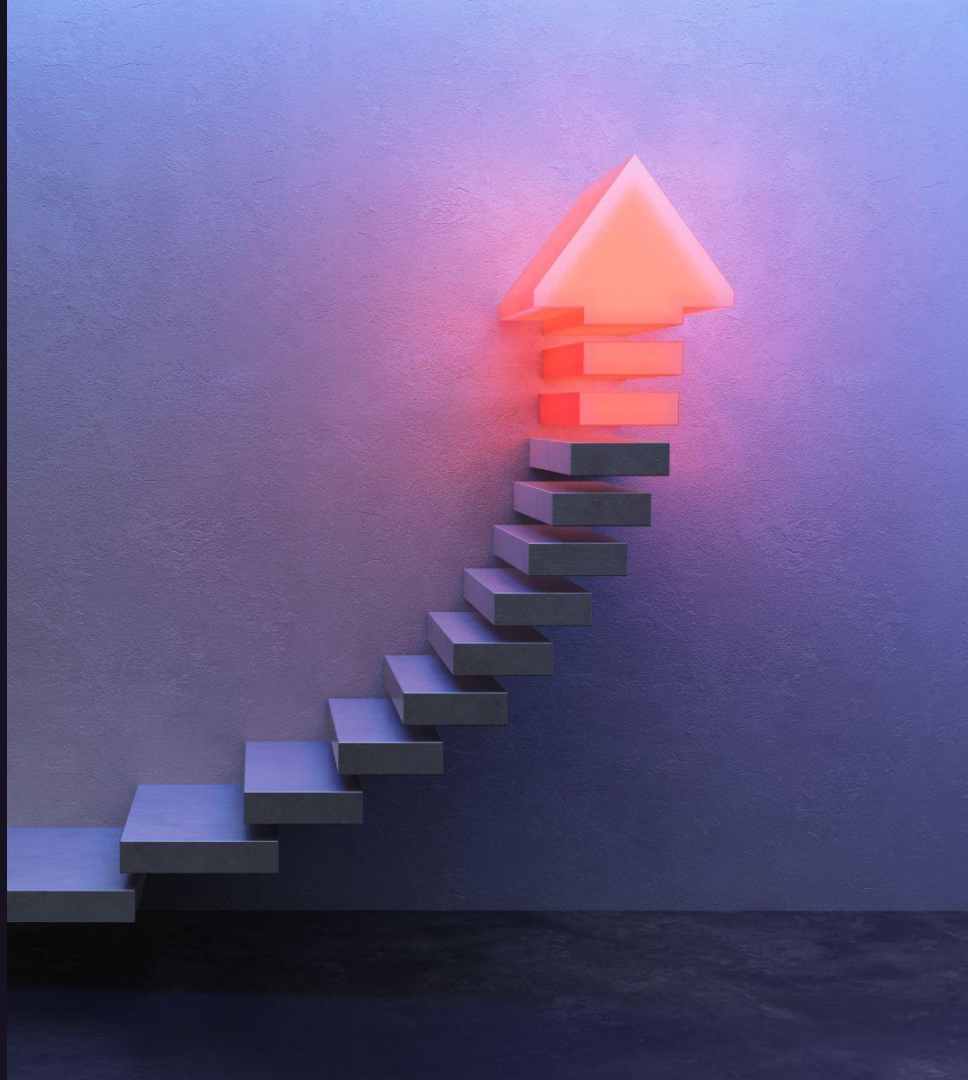


**>25% of code** worked on is from open source libraries by majority of developers

Source: GitLab 2025 DevSecOps Report







© 2025 GitLab Inc.





# The tools are more advanced than ever, yet breaches and attacks are increasing. Why?

## Recent security breaches and attacks:

-  500M customer records breached with unauthorized cloud database access
-  10B passwords leaked
-  Unpatched software and 3rd party dependencies
-  Content update failure put airlines and banks on halt



# Tool chain sprawl makes security practices harder to enable

- ✗ 100s of tools
- ✗ Multiple data models
- ✗ Complexity & risk
- ✗ Lack of transparency
- ✗ Misaligned data models



# AI can be a double edged sword



AI will offer **significant advantages** in terms of time and cost efficiencies when leveraged by security teams

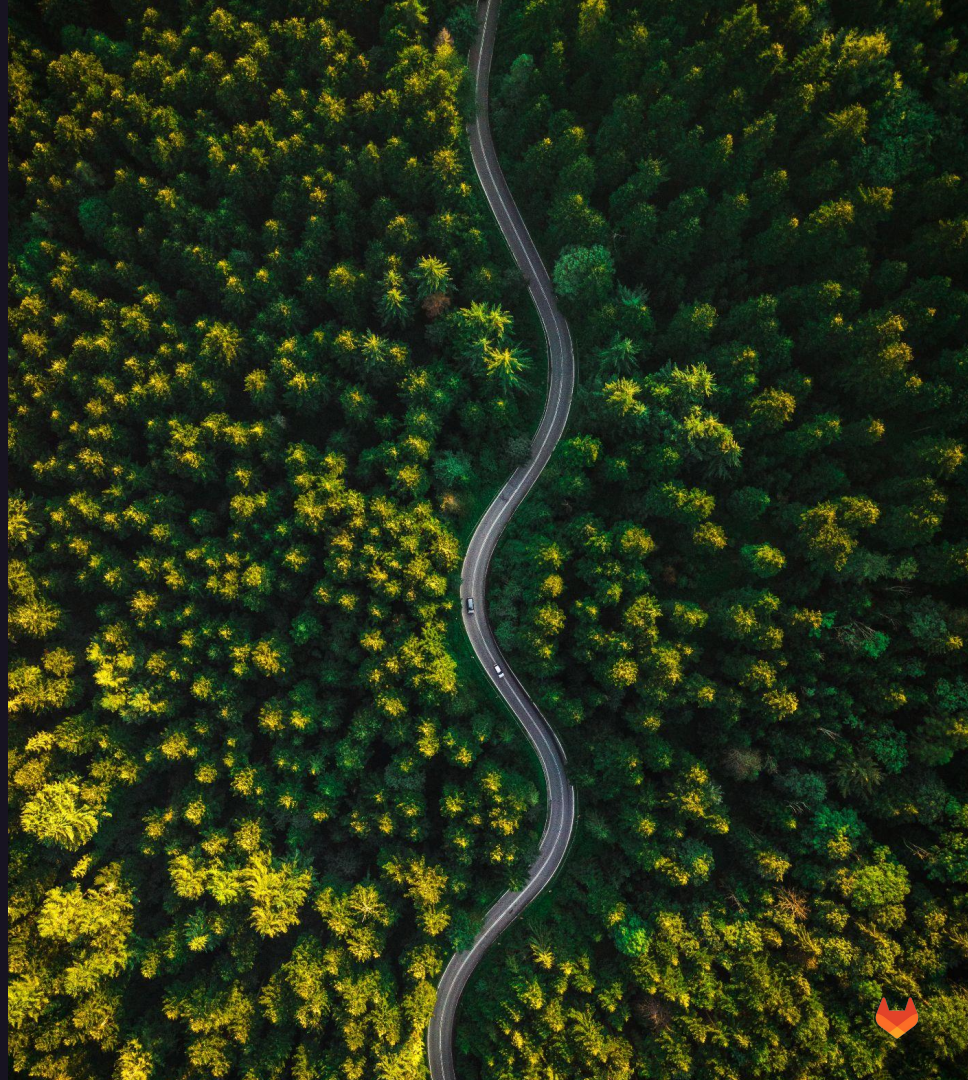


AI poses **additional risks** and threats to businesses



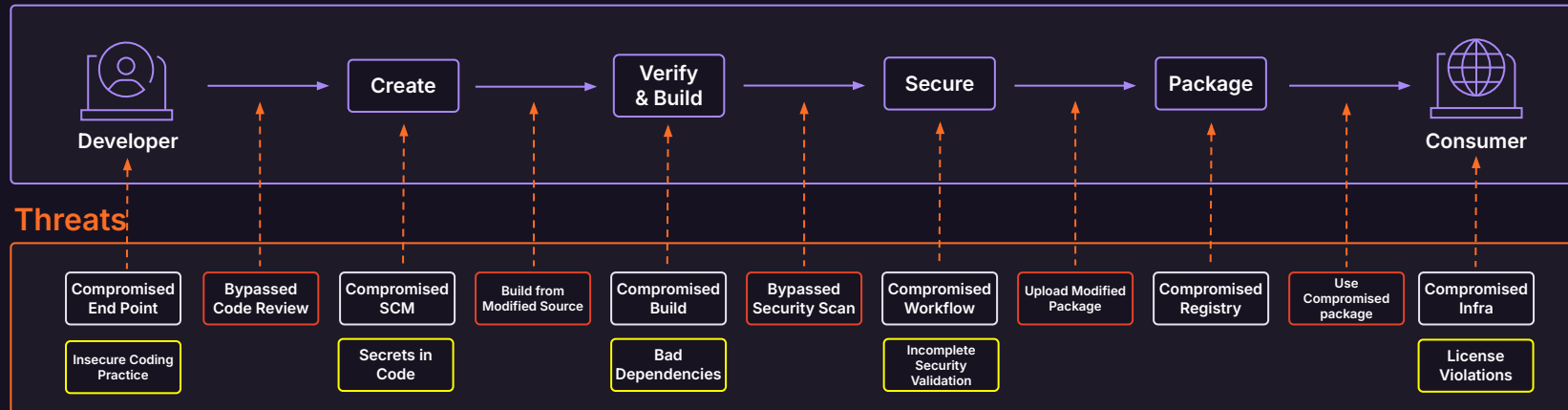


# What is Slowing Down Value Delivery



# The security complexity of value delivery is increasing

## Software Development Lifecycle



## Threats Categories



# What is slowing down value delivery

## Developer Workflow Pain Points

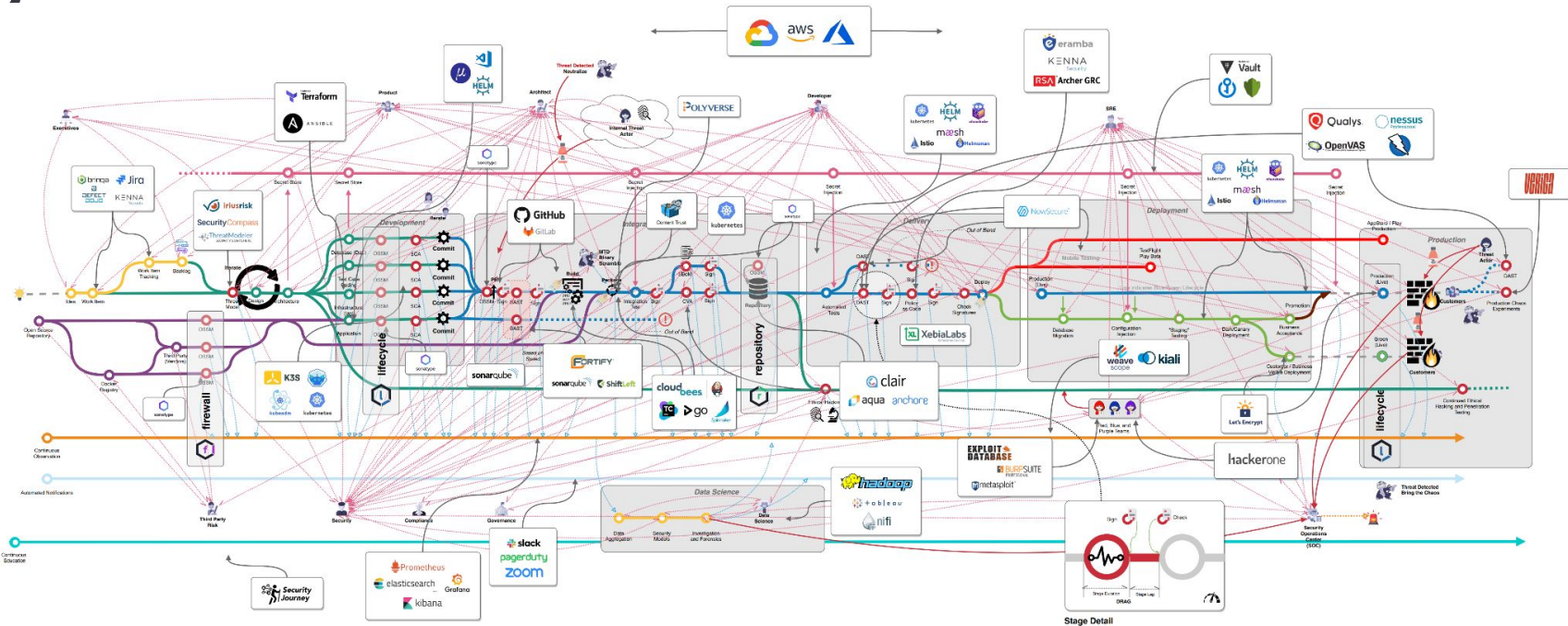


# What is slowing down value delivery

## Developer Workflow Pain Points



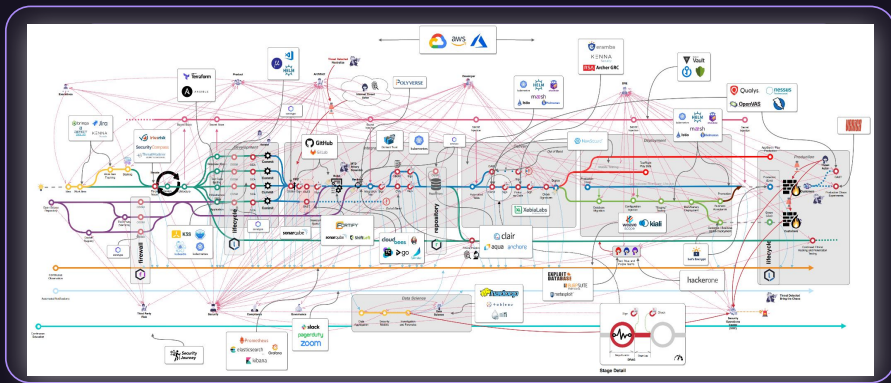
# More and more shortcuts... but how can we ensure visibility, compliance, and governance?





# Value Delivery - Out of Control

## Security and Compliance Pain Points



Security and  
Compliance  
Point-of-View

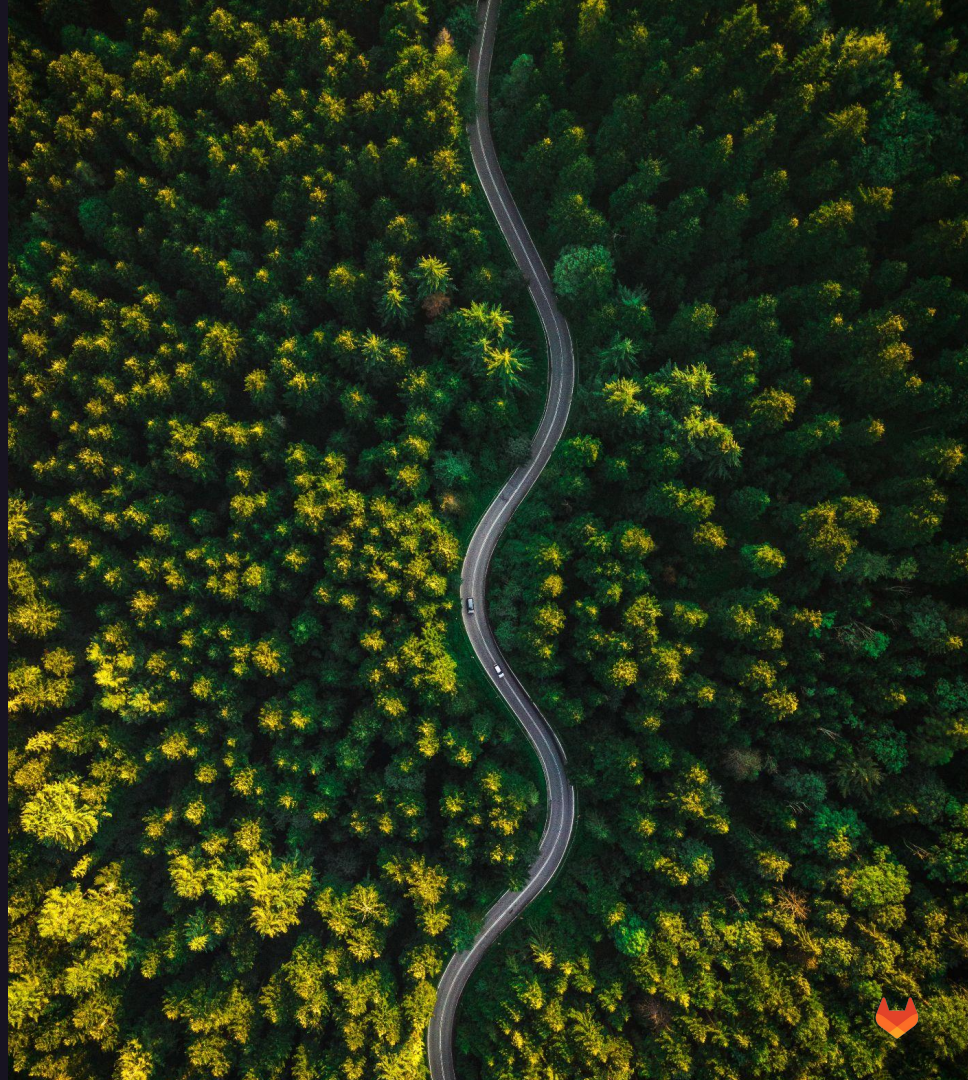
How  
???

How do we generate and track SBOMs across all services and releases?  
How do we assess and manage risk from open source and third parties?  
How do we detect and fix vulnerabilities without slowing delivery?  
How do we ensure all teams follow the same compliance policies?  
How do we collect evidence continuously without burdening teams?  
How do we detect violations early enough to prevent non-compliance?

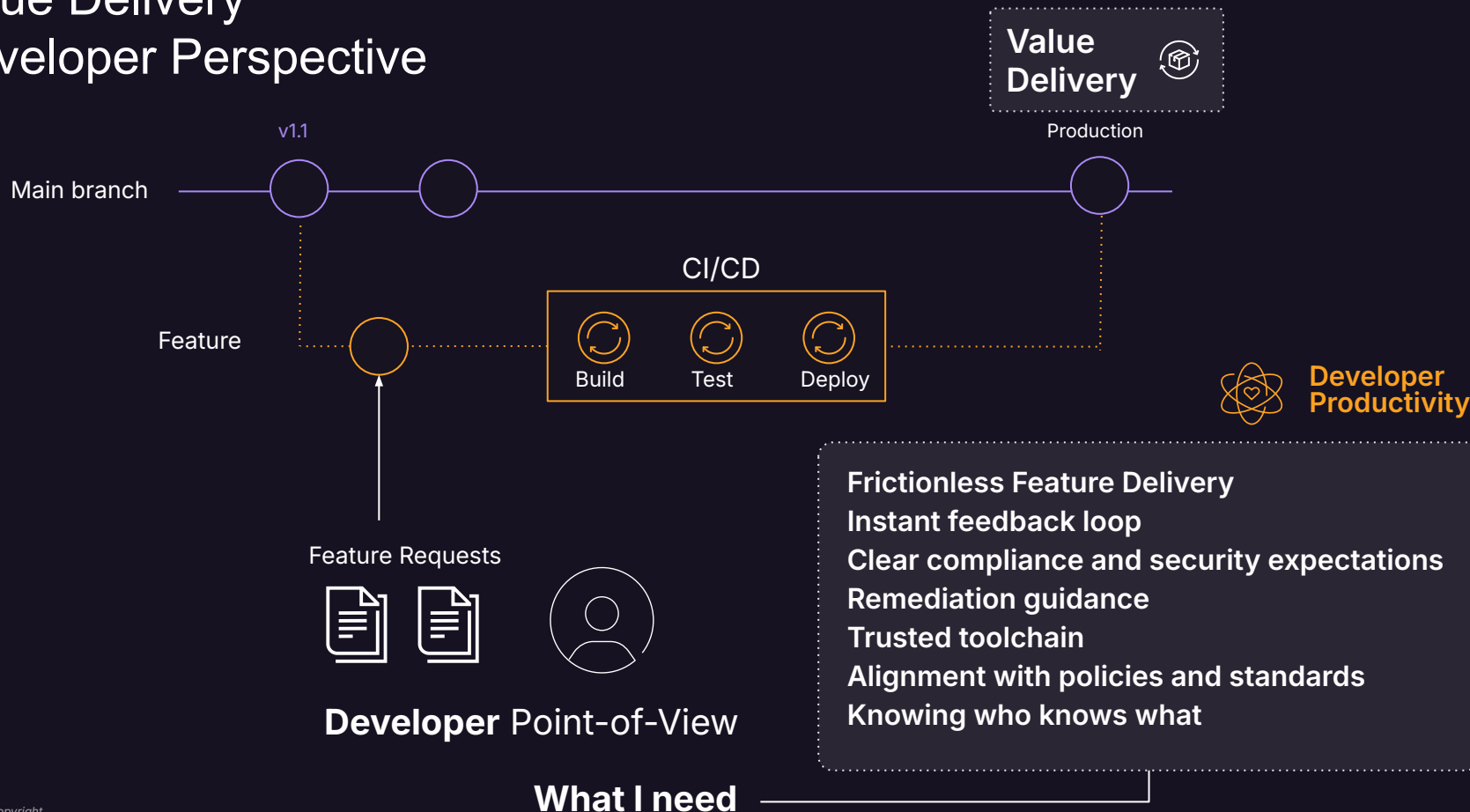




# Accelerate Value Delivery Through Unified Security & Compliance with GitLab

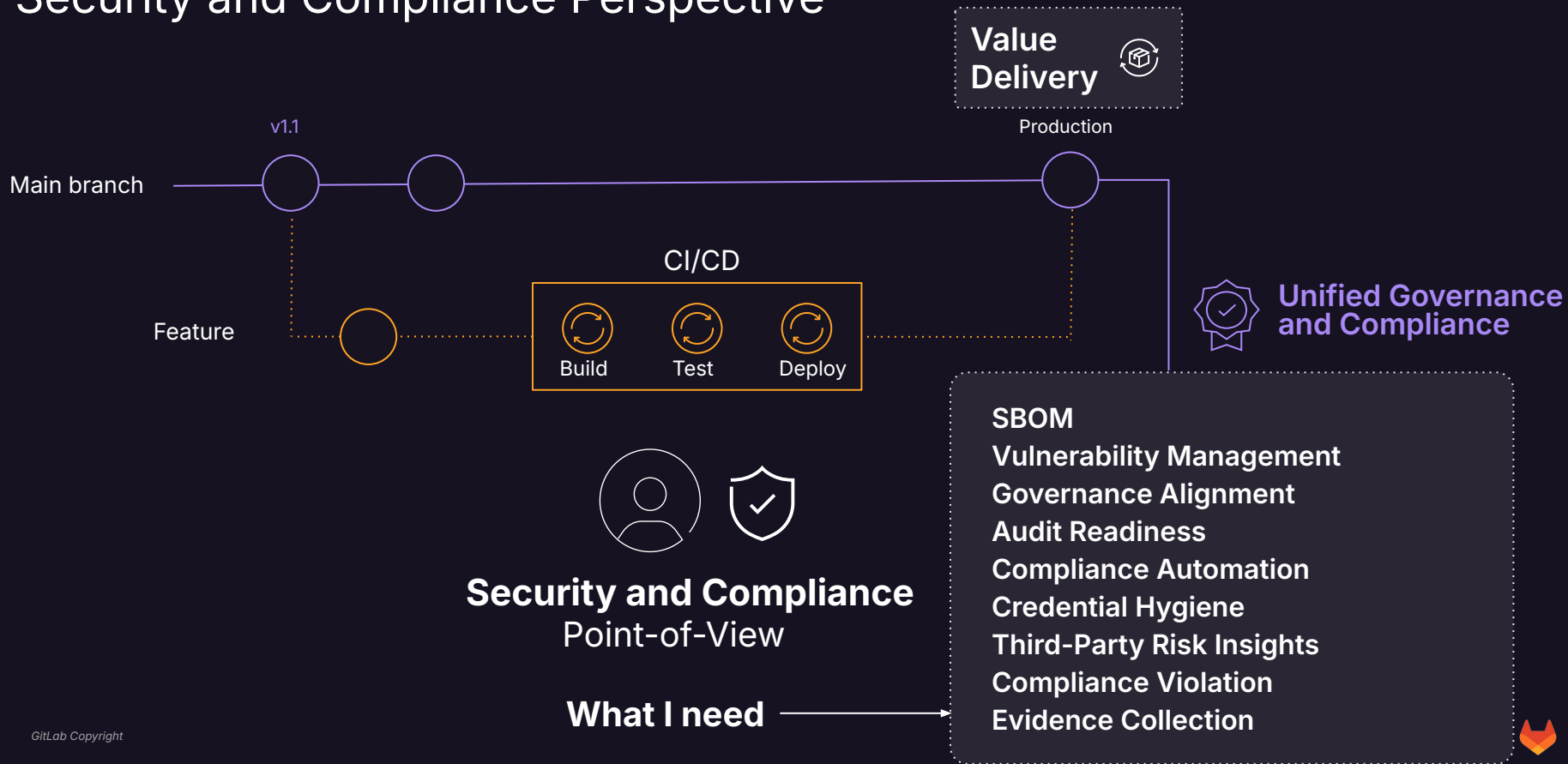


# Value Delivery Developer Perspective

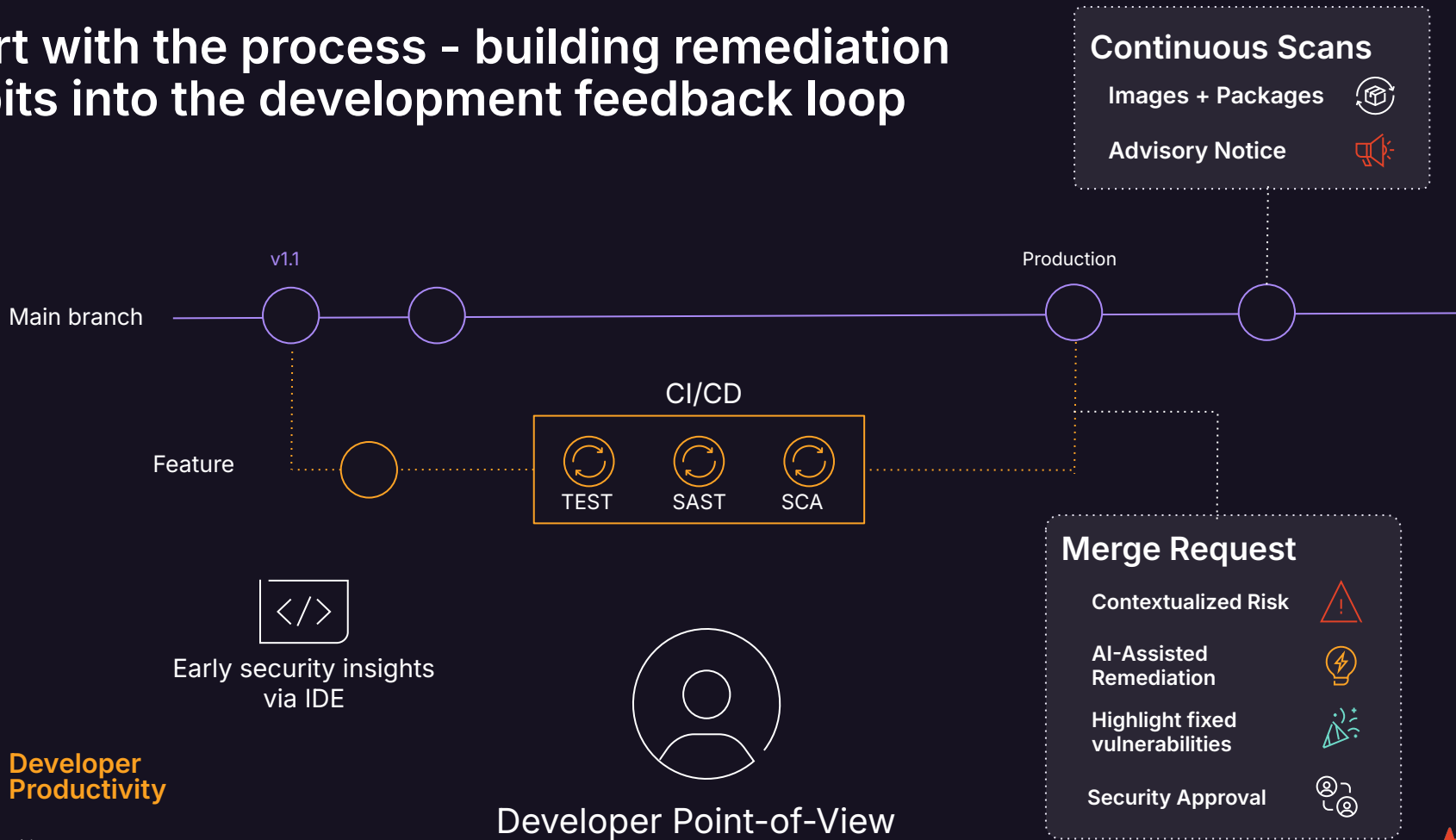


# Value Delivery

## Security and Compliance Perspective



# Start with the process - building remediation habits into the development feedback loop



# Security & Compliance by Design



## Policy Enforcement

What severity threshold should be allowed into production?

What applications or repositories are not scanned?

**Complete Security Coverage**

Inheritance Applied

## Organization

### Business Unit

### Application

v1.1

### CI/CD

TEST

SAST

SCA



# Assess and prioritize risk across the organization

Organization → Group

Business Unit → Group

Application → Project

Developer



Security Pro

v1.1

Production



Triage



SBOM



Bring-your-own

## Insights

Severity trend

- Most at-risk apps
- Historical

## Vulnerability Reporting

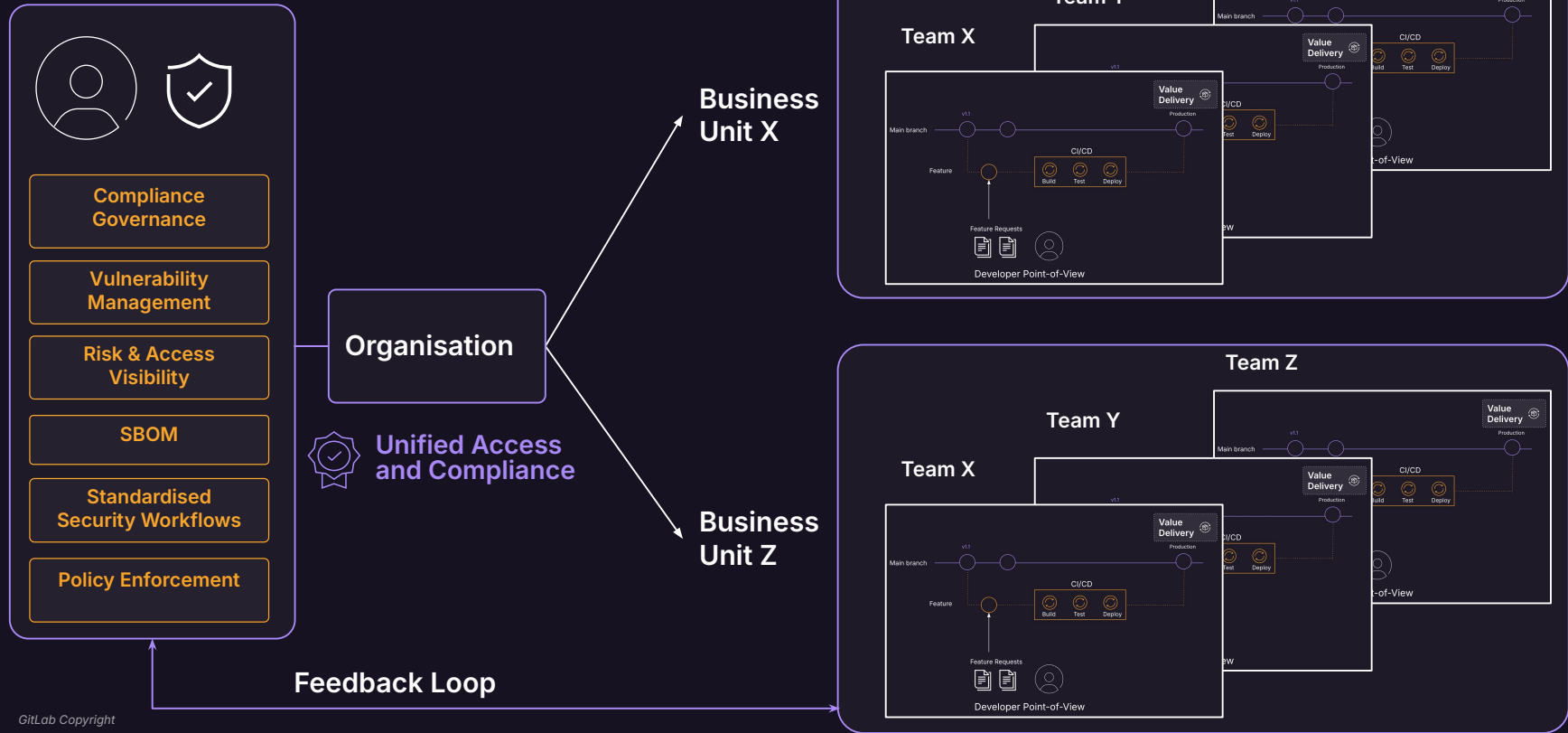
- Single report of all scans
- Export or API
- Point of introduction

Automatic Rollup



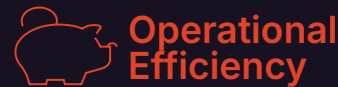


# Scale Compliance & DevSecOps in the organization

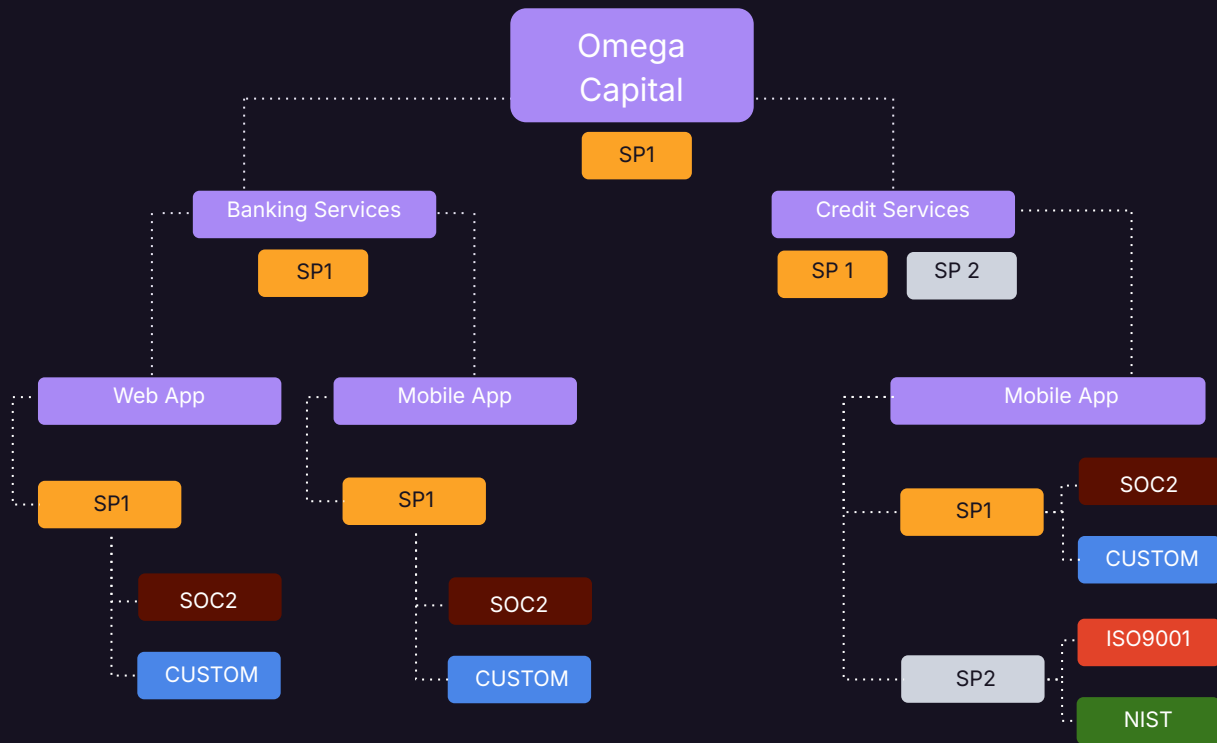
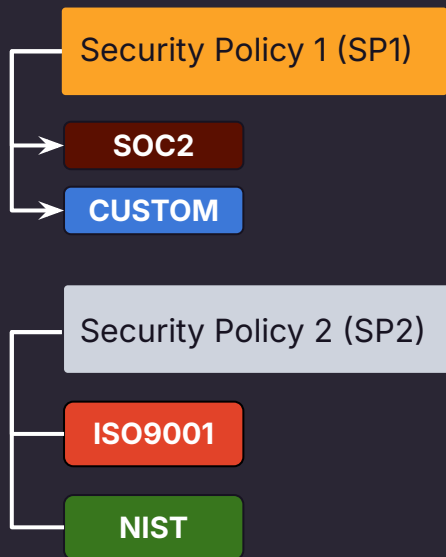


# Simplifying DevSecOps Governance

## Increase impact without increasing costs



### Security Policy Management



# Comprehensive security & compliance capabilities to accelerate value delivery

82% of highly regulated companies require specific security controls and compliance checks embedded into their DevOps operations.



Security scanning



Policy Enforcement



Controls and standards



Compliant workflow automation



Audit management



SBOM & Vulnerability and dependency management



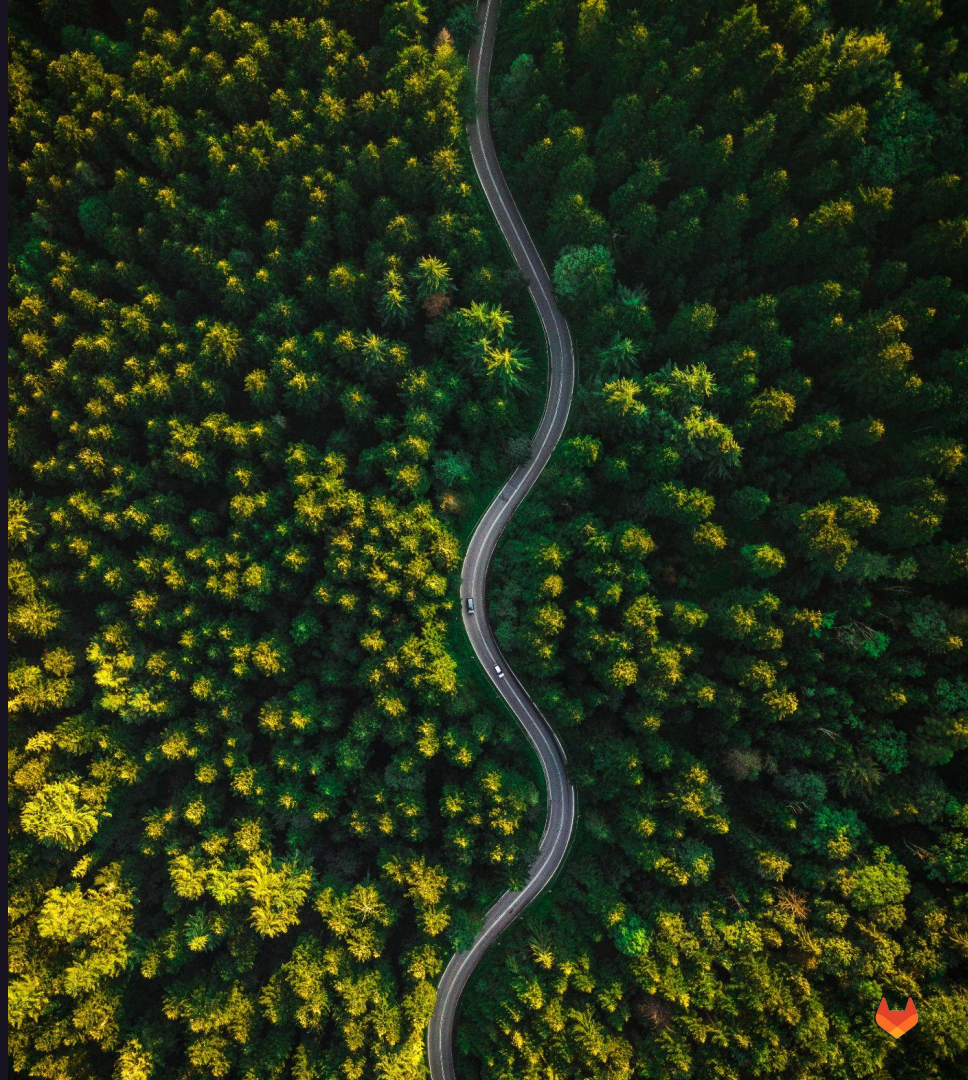


# Agent Platform

The DevSecOps orchestration platform  
for humans and AI agents to accelerate  
value delivery



GitLab Copyright



## The Problem

# The problem isn't code creation

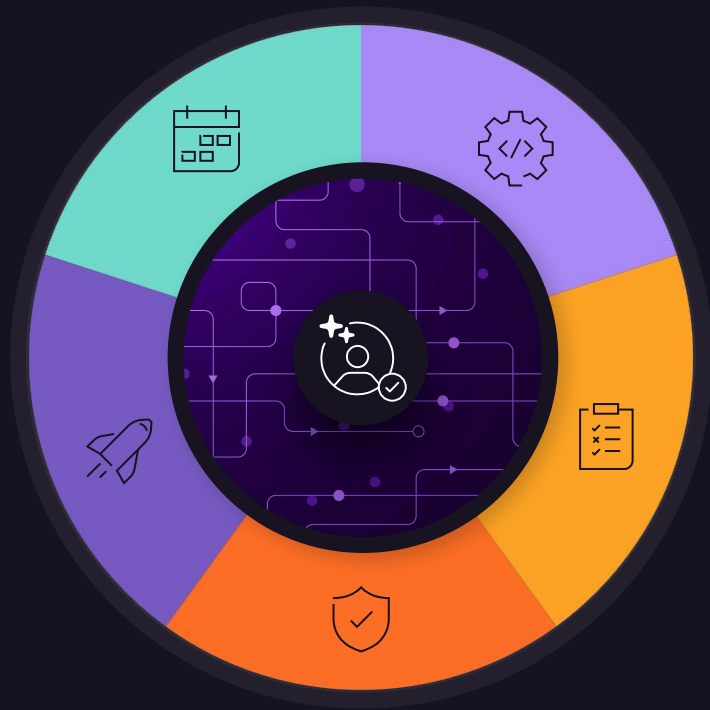
AI coding agents can boost the volume of code created however the overall efficiency is hindered by other software development steps that AI agents do not understand.



## The Solution

# AI agents need full project context

AI agents that have full context of the software project, from planning to coding, building to securing, and deploying to monitoring, can boost efficiency across the SDLC unlocking delivering secure software faster.





# GitLab Duo AI Agent Platform to Accelerate Value Delivery and Improve Compliance

GitLab Duo Agent Platform is a framework on top of our intelligent DevSecOps platform that extends GitLab Duo's control plane introducing extensibility and customization of agents unique to your software development processes.

## GitLab Intelligent DevSecOps Platform



Agent



Agent



Agent



Agent



Agent



Agent



GitLab Duo Agent Platform

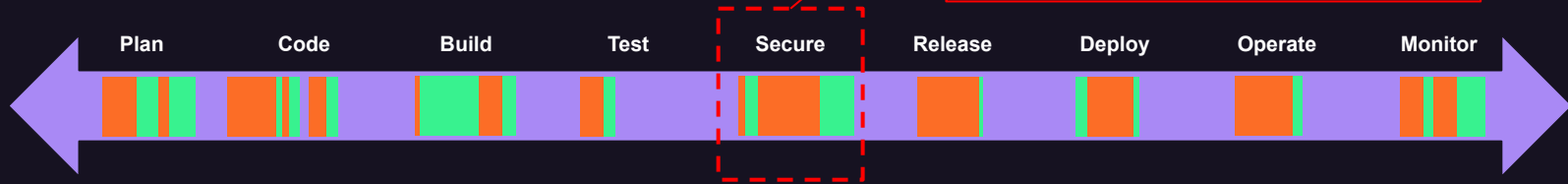


Unified Data Model



# Identify gaps through the Platform Context with Value Stream Management

## Current DevSecOps State



## Desired DevSecOps Future State



# How do you address these challenges in your DevSecOps Value Stream?

## Developer Risk Awareness

How do you give developers actionable risk insight & remediation guidance?

## Unified Compliance

How do you enforce consistent workflows and policies across all teams and environments?

## Operational Efficiency Under Pressure

How do you scale security and compliance with limited resources and increasing complexity?

# Thank you