




Security & Compliance


Beyond Scans: The Road to Continuous Compliance
with GitLab





Dominique Top

Solutions Architect, GitLab


 @gitlab_dlectronique


 dtop@gitlab.com

 @devopsdomi


 scan QR to add me→



 Originally from The Netherlands

 Currently based in London, UK

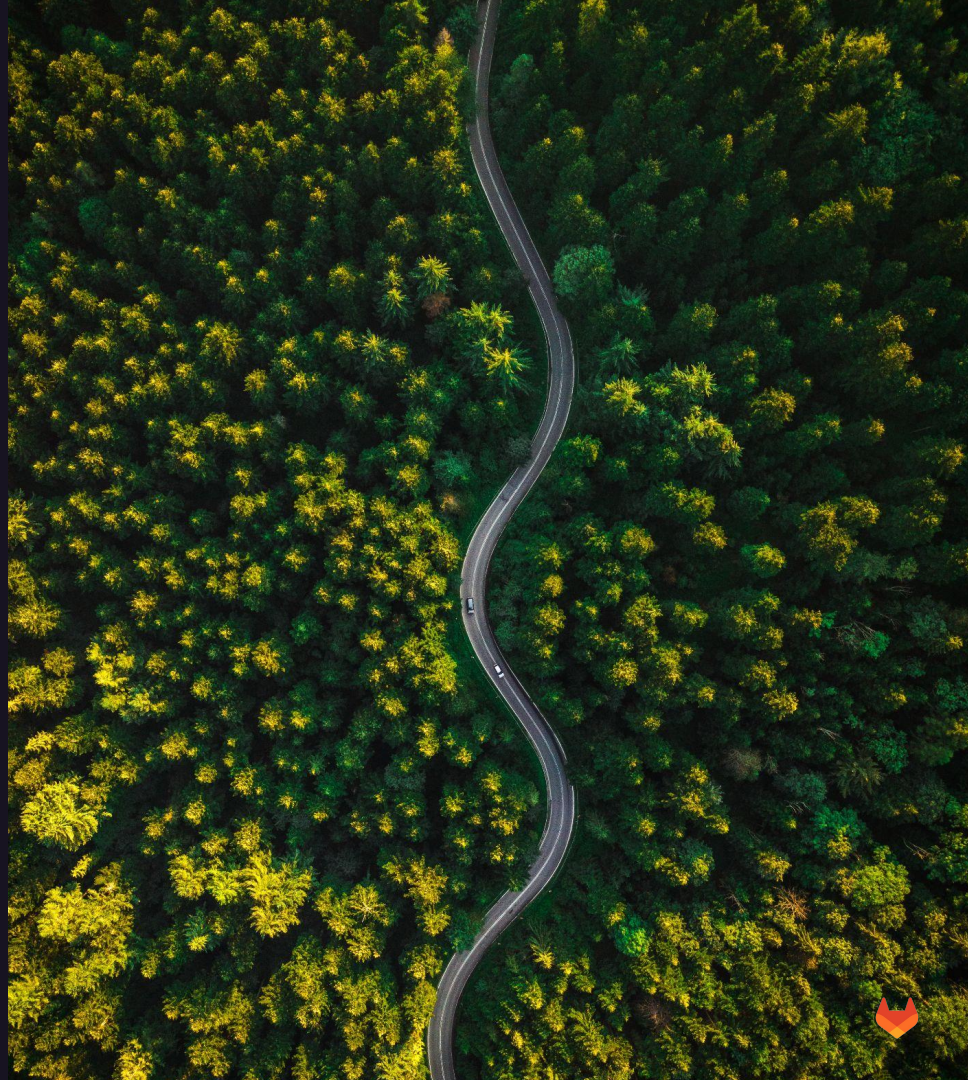
 Degree in Vocals & Sound Engineering

 Techno DJ - D'lectronique



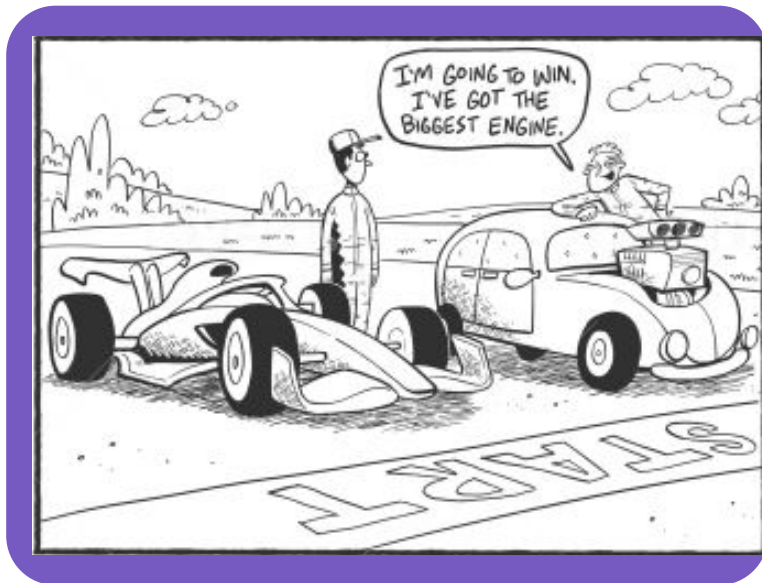
Agenda

- ✓ Introduction
- ✓ Why is compliance so hard to achieve?
- ✓ The Road to Continuous Compliance
- ✓ Questions





A race car with a **big engine**,
but without **brakes** or functioning
steering will put you on a **stretcher**..



Great **scanners** without **governance**
will put you on the front page of
Svenska Dagbladet..



Why is compliance so hard to achieve?



Francis Ofungwu

Global Field CISO
GitLab

Governance challenges faced by our customers:

**Lack of
SDLC-Wide
Risk
Management**

**Extended
Incident
Management
Lifecycle**

**Reduced
Developer
Productivity**

**Vulnerability
Management
Tool Sprawl**

**Difficulties
Enforcing
Policy at Scale**

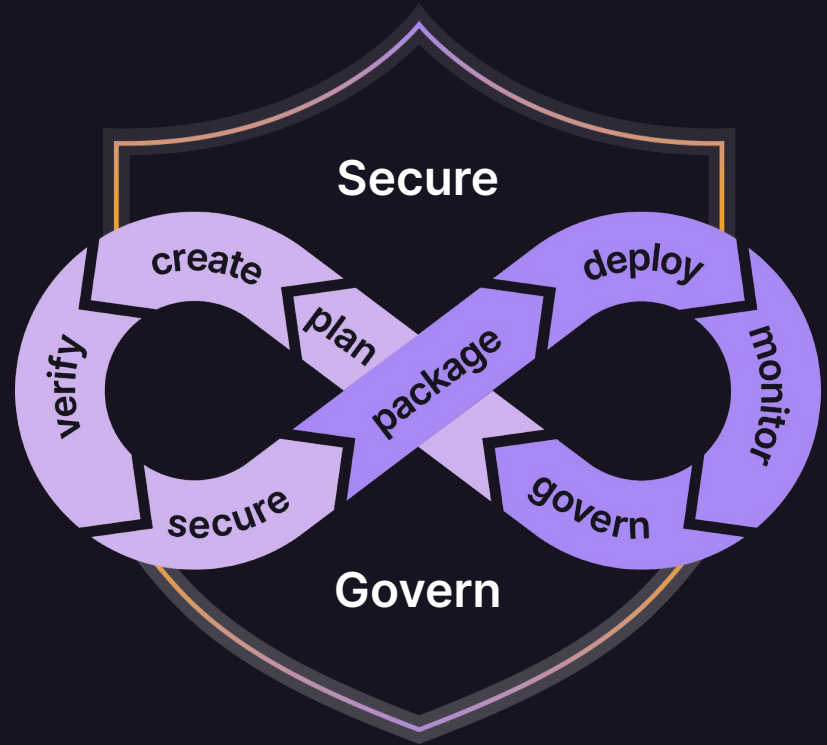


Single Platform for DevSecOps

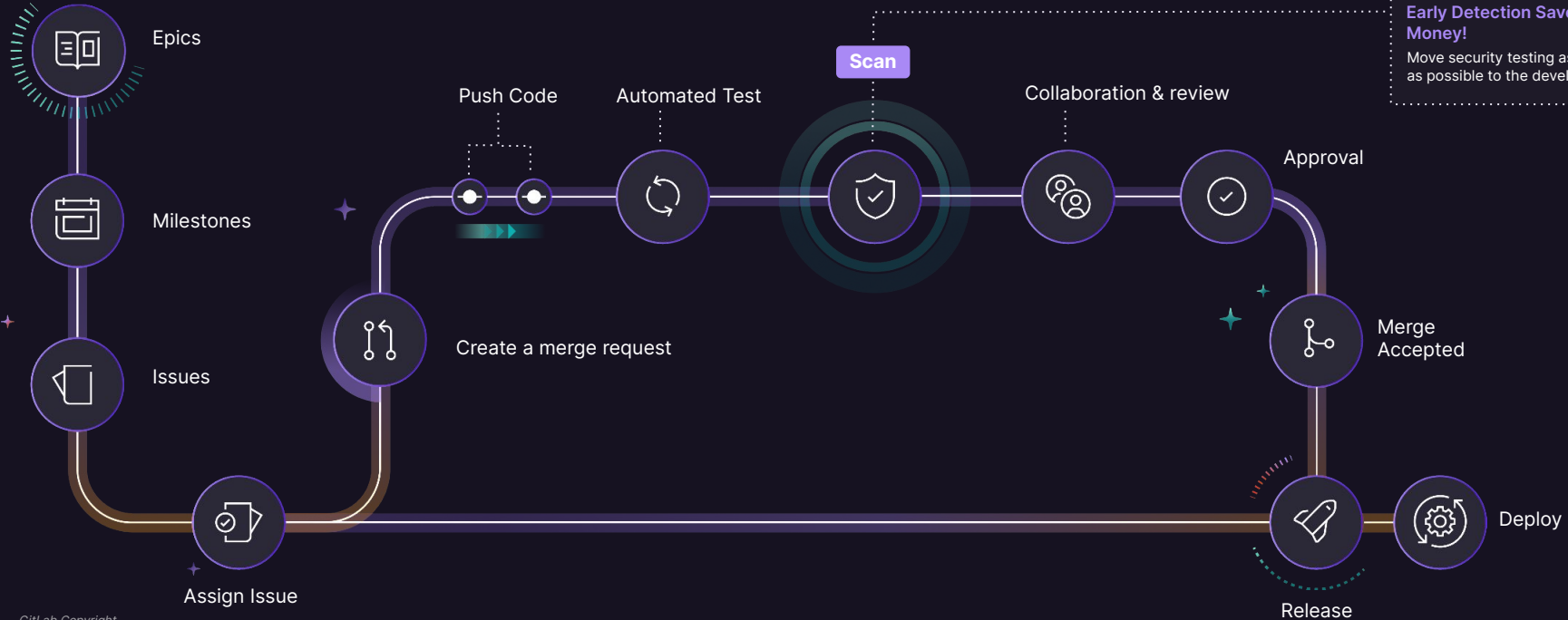
GitLab is the leading DevSecOps platform that empowers your teams to balance speed and security by automating software delivery and securing your end-to-end software supply chain.

GitLab is a single platform that enables organisations to:

- ✓ Identify vulnerable software
- ✓ Mitigate Security Risks
- ✓ Leverage Policies for Compliance
- ✓ Increased visibility across entire software development lifecycle
- ✓ Provide system wide governance








Shift Security Left in the Development Workflow



The Road To Continuous Compliance with GitLab

Leverage the single platform approach to:

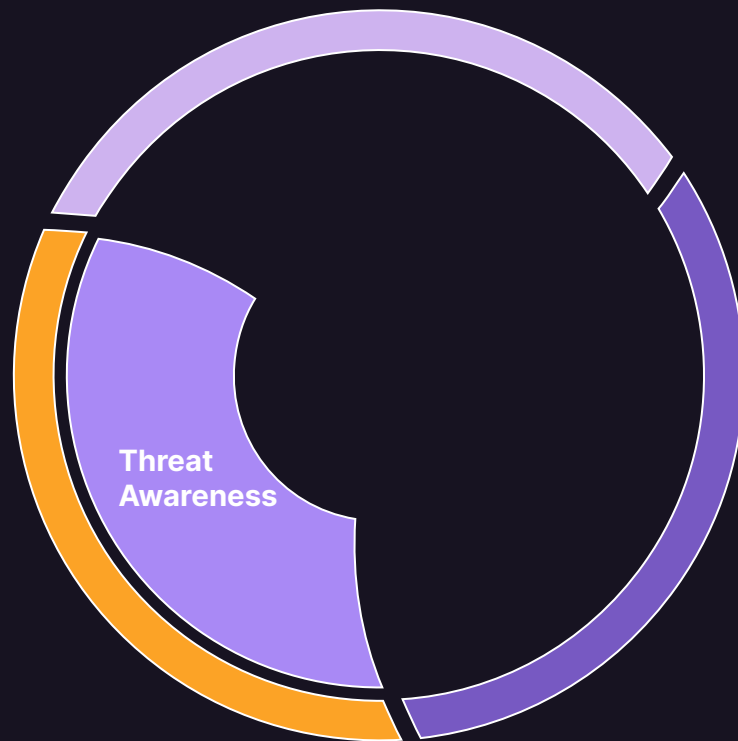
-  Highlight threat vectors
-  Secure the software supply chain
-  Adhere to compliance requirements
-  Have visibility across entire software development lifecycle
-  Enable system wide governance



The Road To Continuous Compliance with GitLab

Threat Awareness

- ✓ Wide Range of Threats
- ✓ Scan & Detect Vulnerabilities
- ✓ Leverage AI and emerging technologies safely



Wide Range of Threats



Compromised Source Control

Identity and Access Management is one of the biggest attack vectors

Hackers take over repositories, impersonate users, and modify downstreams processes

Unintentional vulnerabilities such as flaws in logic or committed secrets can create issues



Risky Open Source Dependencies

Unvalidated open-source code can jeopardize quality and security

Threats from direct and nesting dependencies

Can come from accidental flaws or through malicious code



Compromised Build Pipeline

Attackers can inject malicious code into the build process and distribute code downstream

Security threats possible within Runners, Build Tools, or the Pipeline Orchestrator

CI/CD pipelines have access to range of environments and credentials creating a dangerous attack surface



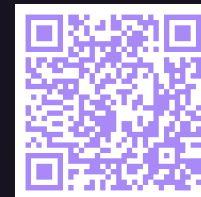
Insecure Web Applications

Attackers can exploit weaknesses in production or runtime environments

Injection attacks can manipulate an application

Security misconfiguration and authentication failures can all be used to manipulate an application

Security was the **#1 Investment Priority** for companies. Scan QR to download our **Annual DevSecOps Survey** →



Identify Vulnerable Software

Scan and detect threats during Development, and in Production

SAST

Scan application source code and binaries

Dependency Scanning

Analyze external dependencies

Secret Detection

Looks for hard-coded creds in commits

API Security

Analyze APIs for runtime vulnerabilities

License Compliance

Detect in-use licenses, and enforce policies

DAST

Analyze web applications for runtime threats

IaC Scanning

Scan infrastructure files for insecure practices

Container Scanning

Scan for known security vulnerabilities

Fuzz Testing

Use malformed data

Bring your own Tool

Integrate existing scanners

Devs: can we use GitLab Scanners?
Sec: we have scanners at home
The scanners at home:



AI is central to GitLab's DevSecOps platform

Throughout the Software Delivery Lifecycle

Improve DevSecOps workflow efficiency by **10x** by applying AI assisted workflows to all teams involved in delivering software value



Privacy-First, Enterprise-Grade

Lead with a privacy-first approach allowing enterprises and regulated organizations to adopt AI assisted workflows

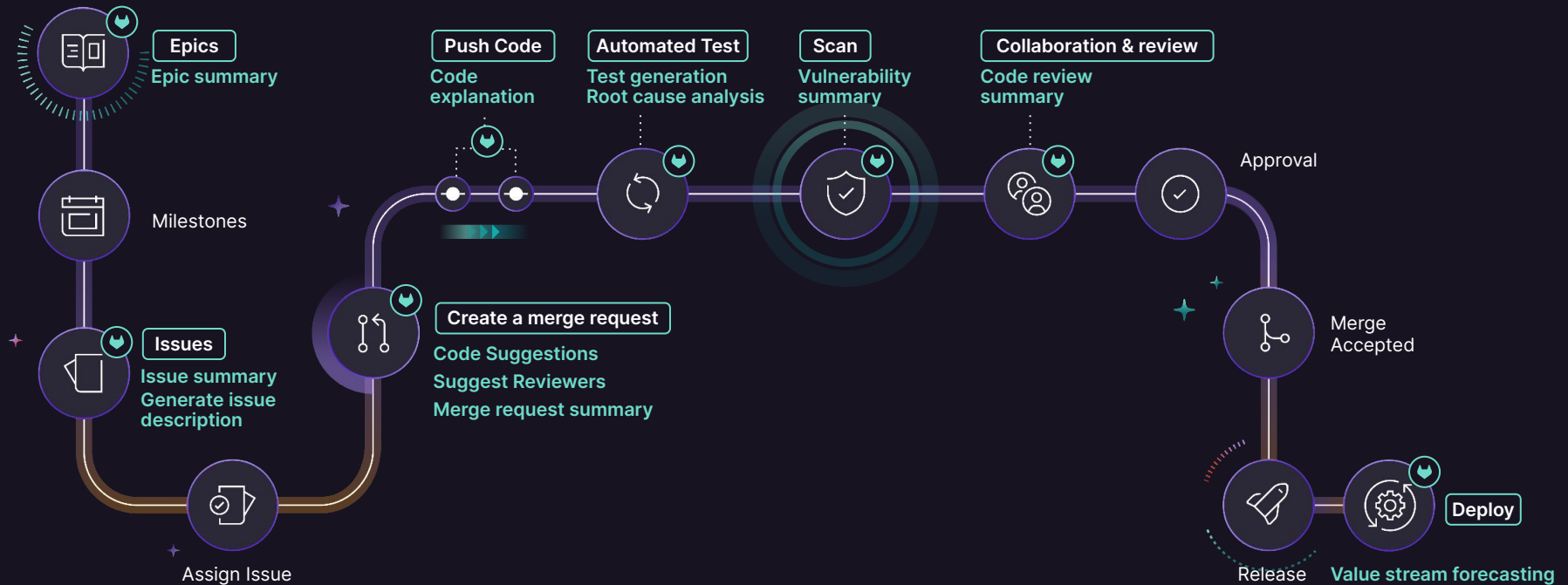


Single Application

Leverage the benefits of GitLab's single application to deliver more software faster, enabling executive visibility across value streams and preventing context switching



Your entire software development and deployment workflow powered by GitLab^{Duo}



AI-assisted capabilities for everyone involved in the software development lifecycle



Developer Teams



Security & Operations



For Everyone

Available features

Code Suggestions

AI paired programming

Suggested Reviewers

Better code reviews

Summarize MR Changes

Drive alignment and action

Summarize My MR Review

Get your point across

Help with Git Commands

Natural language CLI assistant

Explain This Vulnerability

Remediate security issues

Generate Tests in MRs

Automate repetitive tasks

Explain This Code

Uplevel and understand

Resolve this Vulnerability

Recommendations to fix vulnerable code

Issue Comment Summaries

Understand and take action

GitLab Chat

Get help fast

Value Stream Forecasting

Predict the future



Coming soon

Experimental

Beta

General Availability

AI-assisted capabilities for everyone involved in the software development lifecycle



Developer
Teams



Security &
Operations



For
Everyone

Available features

Code Suggestions

AI paired programming

Suggested Reviewers

Better code reviews

Summarize MR Changes

Drive alignment and action

Summarize My MR Review

Get your point across

Help with Git Commands

Natural language CLI assistant

Explain This Vulnerability

Remediate security issues

Generate Tests in MRs

Automate repetitive tasks

Explain This Code

Uplevel and understand

Resolve this Vulnerability

*Recommendations to fix
vulnerable code*

Issue Comment Summaries

Understand and take action

GitLab Chat

Get help fast

Value Stream Forecasting

Predict the future

Coming soon

Experimental

Beta

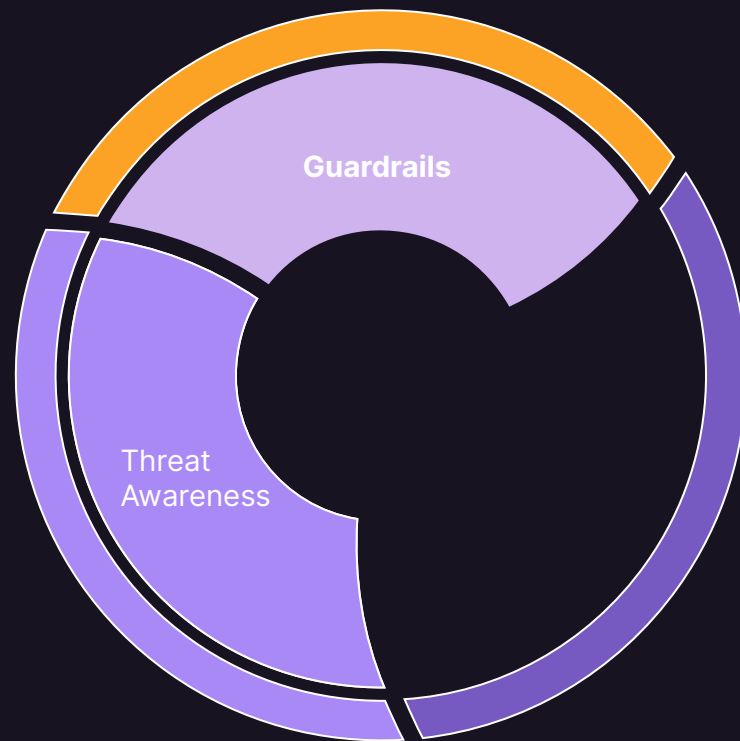
General Availability



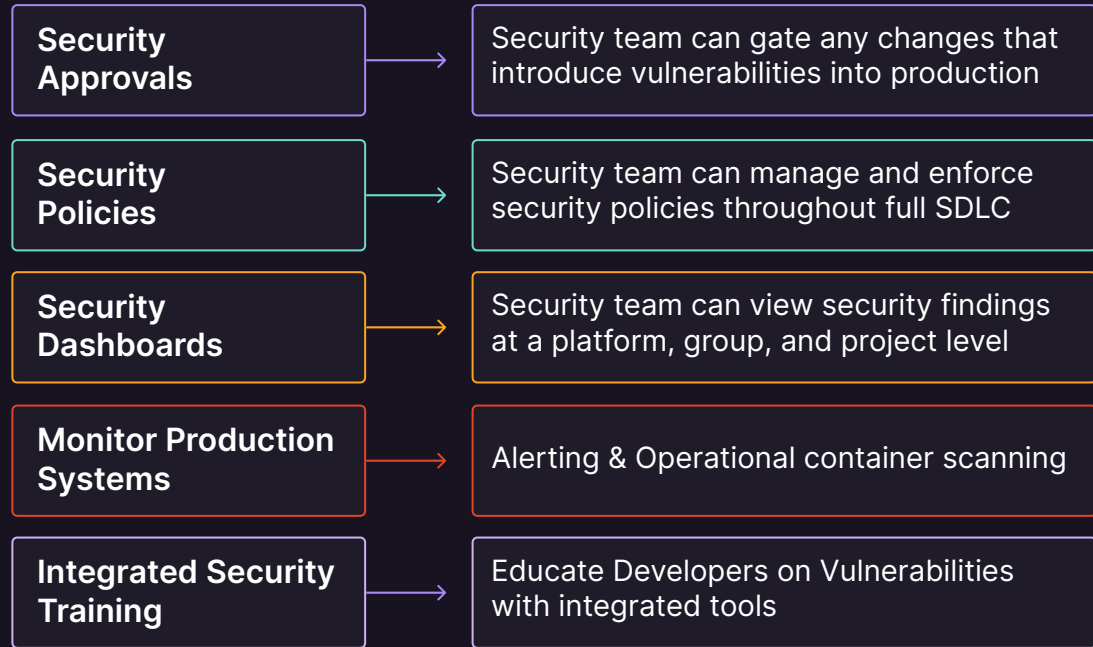
The Road To Continuous Compliance with GitLab

Guardrails

- ✓ Risk Mitigation Capabilities
- ✓ Policy management
- ✓ Actionable CI pipeline output
- ✓ Streamline the Review and Approval Process



Broad Set of Security Risk Mitigation Capabilities





Policy Management

Defining and enforcing rules and policies

Granular User Roles & Permissions

Define user roles and permission levels that make sense for your organization

Separation of Duties

Requires multiple actors to complete a task to increase protection from error as well as prevent malicious activity

Access Control

Limit access with two-factor authentication and expiration tokens

Compliance Policies

Define and enforce compliance framework policies for specific projects, groups, and users

Credentials Inventory

Keep track of all the credentials that can be used to access a GitLab self-managed instance

Protected Branches

Control unauthorized modifications to specific branches (including creating, pushing, and deleting a branch) without adequate permissions or approvals

MR Approval Rules

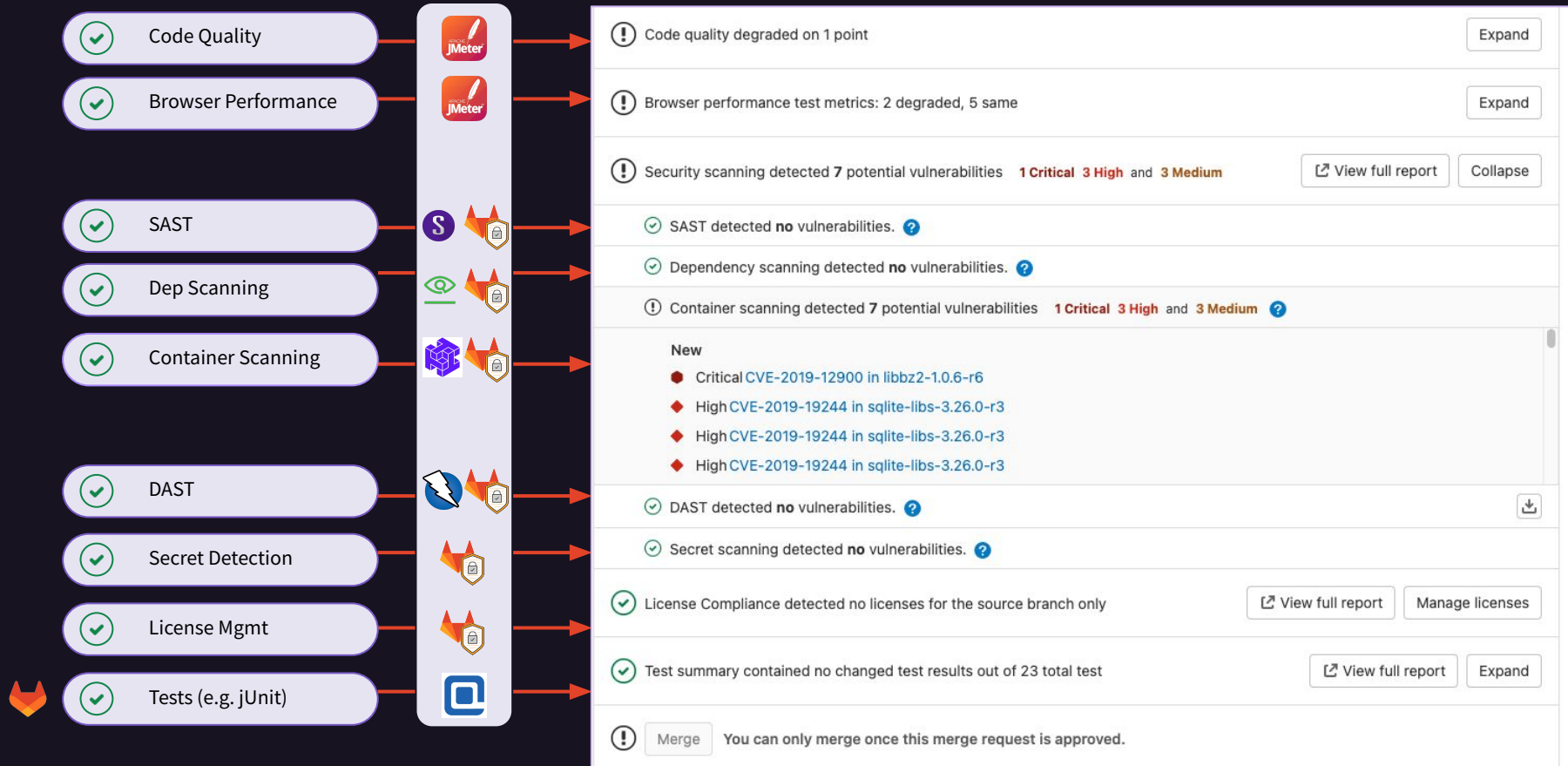
Define how many approvals a merge request must have before it can be merged and who can approve

Scan Execution Policies

Enforce security scans to be run on a specified schedule, or whenever a project pipeline runs



Actionable Pipeline Output



Streamlining the Approval Process

Coverage-Check: Approval required if test coverage declines.

License-Check / Vulnerability-Check: Security is called in only if there is an attempt to merge a vulnerability of high, critical, or unknown severity. Or for denied licenses.

Utilize **CODEOWNERS** file to automatically require approval for a file or path within an application.

External Checks: These status check provide developers and reviewers with the approval status of external change management solution to accelerate cycle time for change requests.

Requires 4 more approvals from Coverage-Check, License-Check, and Vulnerability-Check.

▼ Collapse

Approvers	Approvals
✓ Any eligible user ?	Optional
Coverage-Check	0 of 1
License-Check ?	0 of 1
Vulnerability-Check ?	0 of 2

Approve additionally Merge request approved. Approved by

▼ Collapse

Approvers	Approvals
Code Owners	
✓ /api/	1 of 1
✓ /docs/	Optional

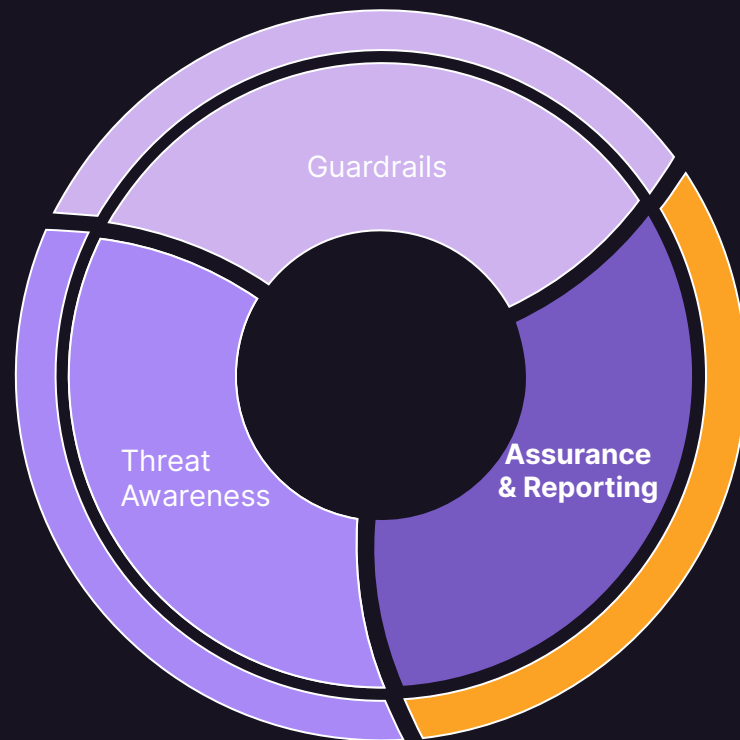
⚠ Status checks 2 pending
When this merge request is updated, a call is sent to the following APIs to confirm their status. [Learn more.](#) Collapse

- ⏸ Manual check, <https://manual.validator.com/validate>
- ⏸ Compliance check, <https://compliance.validator.com/validate>
- ✓ Custom validator, <http://custom.validator.com/validate>

The Road To Continuous Compliance with GitLab

Assurance & Reporting

- ✓ Automating Compliance Framework Workflows
- ✓ Audit Management
- ✓ Vulnerability Report
- ✓ Software Bill of Materials (SBOM)





Automating Compliance Framework Workflows

Workflow automation tools to enforce compliance by framework

Compliance Framework Project Templates

Create projects that map to specific audit protocols such as HIPAA to help maintain an audit trail and manage compliance programs

Compliance Framework Project Labels

Easily apply common compliance settings to a project with a label

Compliance Automation

Webhooks for automating integrations with external systems, like compliance management systems (e.g. Drata or Vanta).

Compliance Pipelines

Define compliance jobs that should be run in every pipeline to ensure security scans are run, artifacts are created and stored, or any other steps required by your organization





Audit Management

Prepare for audits and better understand the root cause of issues with easy access to audit data

Audit events

Track important events such as changes to user permission levels, who added a new user, or who removed a user

Streaming audit events

Consolidate your audit logs in a tool of your choice

Audit reports

Respond to auditors by generating comprehensive reports such as instance, group, and project events, impersonation data, sign-in, and user events

Compliance report

Get a high-level view of compliance violations and the reasons and severity of violations in merge requests



Vulnerability Report

Easily see a complete list of detected vulnerabilities and take action in-context

Group and Project Level Visibility:

1. Latest pipeline run
2. Vulnerabilities by criticality
3. Detailed Vulnerability Reporting
4. Known Remediation Path
5. Export for Compliance

GitLab Menu

GitLab.org > GitLab > Vulnerability Report

Vulnerability Report

+ Submit vulnerability 5 Export

The Vulnerability Report shows results of successful scans on your project's default branch, manually added vulnerability records, and vulnerabilities found from scanning operational environments. [Learn more.](#)

Development vulnerabilities 10092 Operational vulnerabilities 0

Last updated 2 hours ago #540491990 1

Critical 2603 **High** 138 **Medium** 5923 **Low** 272 **Info** 749 **Unknown** 407

Status: Needs triage +1 more Severity: All severities Tool: All tools Activity: All activity

Status	Severity	Description	Identifier	Tool	Activity
2022-05-16	Critical	Google (GCP) Service-account detected; please remove and revoke it if this is a leak. app/models/integrations/prometheus.rb:80	Gitleaks rule ID Google (GCP) Service-account	Secret Detection 4	
2022-05-13	Critical	Password in URL detected; please remove and revoke it if this is a leak. ee/spec/models/project_spec.rb:1756	Gitleaks rule ID Password in URL	Secret Detection	
2022-05-	Critical	Password in URL detected; please remove and revoke	Gitleaks rule ID Pass	Secret	



Software Bill of Materials

A “**Software Bill of Materials**” (SBOM) has emerged as a key building block in software security and software supply chain risk management.

A SBOM is a nested inventory, a list of ingredients that make up software components.

– Software Bill of
Materials | CISA

What

Open Source and third party code adoption is driving the need to know exactly what is in our software

When

Current inertia began in 2017, but the term has been around since 2010

Where

Log4j highlighted the reuse of infected containers long after initial discovery

Why

- Vendor software can be a black box with no visibility to internal vulnerabilities
- Globally, various governments are legislating the requirement to have secure SDLC

How

SBOM provides a standard approach to understanding what is in software and why





Software Bill of Materials (SBOM)

Generation

- ✓ GitLab Dependency Scanning runs in the pipeline and creates a CycloneDX SBOM for source code dependencies.
- ✓ GitLab Container Scanning runs in the pipeline and creates a CycloneDX SBOM for operating system dependencies.
- ✓ 3rd party CycloneDX generators can also be used.
- ⚙️ Support for SPDX SBOMs.

Ingestion

- ✓ Any CycloneDX SBOM produced by the pipeline is ingested into GitLab automatically and stored in our database.
- 🕒 Support for ingesting SPDX SBOMs.

Continuous Analysis

- ✓ Dependencies are continuously analyzed for licenses.
- ⚙️ Dependencies are continuously analyzed for vulnerabilities.

Merge & Distribute

- ✓ Viewing the SBOM in the GitLab UI in the Dependency List.
- ✓ A combined/merged JSON file including license and vulnerability data can be downloaded from GitLab.
- ✓ Support for accessing a combined/merged CycloneDX SBOM through a CI/CD pipeline.
- 🕒 Support for downloading a combined/merged CycloneDX or SPDX file through the UI.

Key: ✓ Available now

⚙️ In progress

🕒 On the roadmap



The Road To Continuous Compliance with GitLab

Achieving Governance by

- ✓ Manage vulnerabilities, dependencies, policies
- ✓ Identify Risks
- ✓ Respond to risks with appropriate management tools
- ✓ Use Policies to automate compliance



Questions?

Tack!
Thank you!