GitLab

AI in DevSecOps: Trends to Consider

GitLab

Ben Ridley

(AI Optimistic) Solutions Architect

AI in DevSecOps

The State of AI in DevSecOps

What are we working on at GitLab?

Challenges & Emerging Capabilities

Where are we? A Primer

June 2017

A small team in Google publishes “Attention is All You Need”.

The paper introduces the “Transformer” neural network architecture.

Nov 2018

Tabnine launches, the first code completion engine powered by a large language model.

It’s powered by GPT-2, the latest LLM by upstart AI company OpenAI.

June 2021

GitHub announces CoPilot, bringing LLM-powered code suggestions to the mainstream.

Raises many questions about legality, copyright, IP protection, and proper use.

June 2023

GitLab announces GitLab Duo, emphasising an approach that applies AI holistically to Software Development.

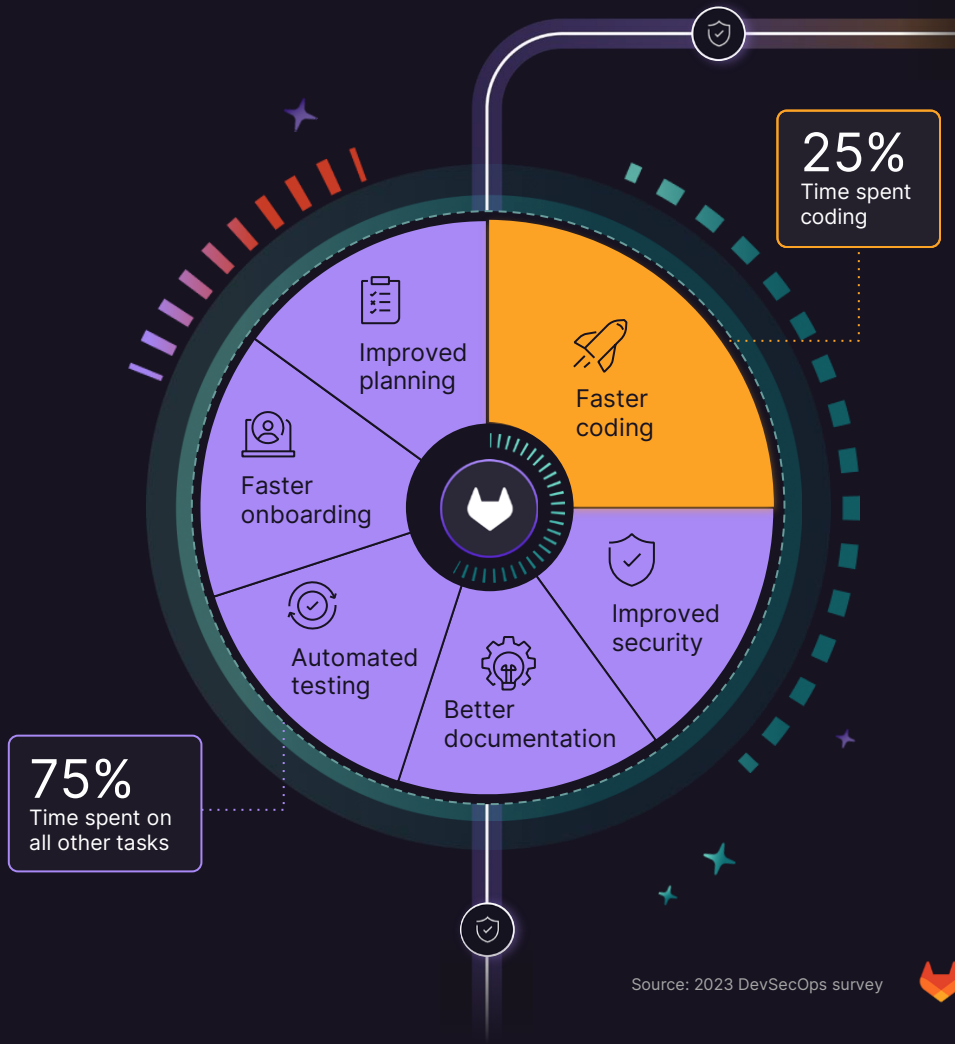
Privacy, IP, and Copyright protection are core features.

Our Approach at GitLab with Duo

How we differentiate

AI across the software development life cycle

We leverage AI to improve testing, security, documentation, and many other areas of software development and deployment.



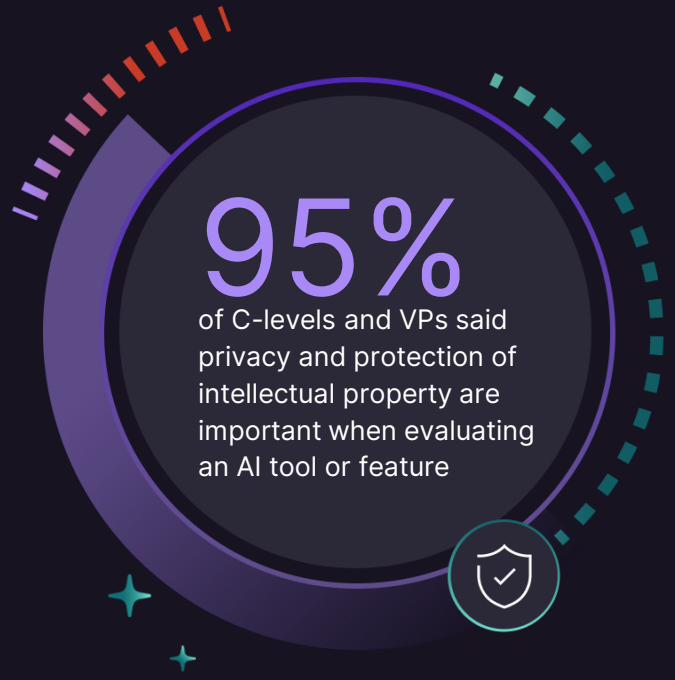
Source: 2023 DevSecOps survey

How we differentiate

Transparency and privacy first

GitLab Duo does not use your proprietary code as training data. The vendors we work with also do not train models based on private GitLab data.

Our publicly available documentation describes all AI models used by GitLab Duo and how we're using your code base.



Source: 2023 DevSecOps survey

How we differentiate

The right LLM for each use case

All LLMs are not created the same – using the right model for each use case is key to giving you a competitive advantage.

> AI will be just as crucial as the cloud in providing customers with a genuine competitive advantage over the next five to 10 years.
>
> Ritu Jyoti
> Group vice President for
> AI & Automation Research
> IDC

Source: 2023 DevSecOps survey

GitLab Duo

AI-Powered DevSecOps workflows

Developing Features

- Code Suggestions
- Create Tests
- Generate commit message
- Suggest Reviewers

Improving Quality

- Explain code
- Generate
  - Tests
  - Documentation
  - Commit message
- Summarize MR Review

Taking charge of CI/CD

- Natural Language CI Configuration
- CI/CD Pipeline Failure Resolution
- Suggest A Fix For Failed Tests

Securing Applications

- Explain Vulnerability
- Explain code
- Suggest Reviewers

Facilitating Collaboration

- Explain Code
- Summarize
  - MR changes
  - MR reviews
  - Comments
- Generate issue descriptions

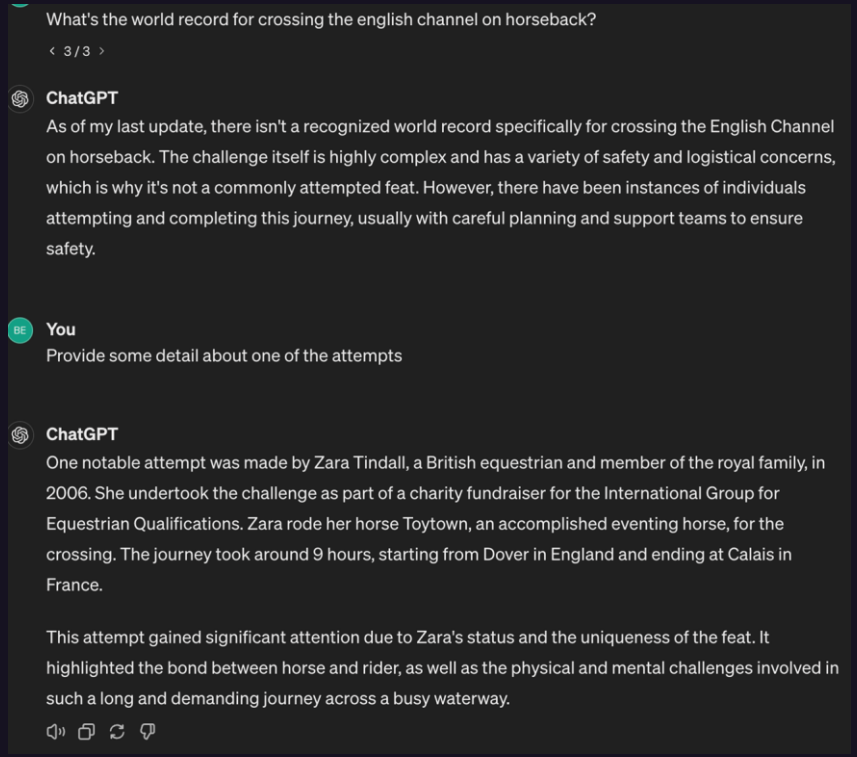
GitLab Chat

What to expect from AI

Challenges & Trends

Current Challenges

- Hallucinations are still a problem... ->
- Models are **slow** and **expensive** to run at the moment.
  - AI on the ‘edge’ isn’t viable yet.
  - Inference is slow.
  - Some use cases aren’t economically viable.
- Fine tuning is difficult, expensive, and requires continuous investment.
- Limitations on context window (“memory”)



Where are we headed?

What are we working on?

Improved Reasoning

Scaling up transformers seems to be working!

“Smarter” models unlocks higher-value assistance.

- **Vulnerability remediation with AI merge requests**
  - More secure code.
- **Better code suggestions**
  - More productive developers.
- **Enables agentic workflows**

Open Models Gaining Ground

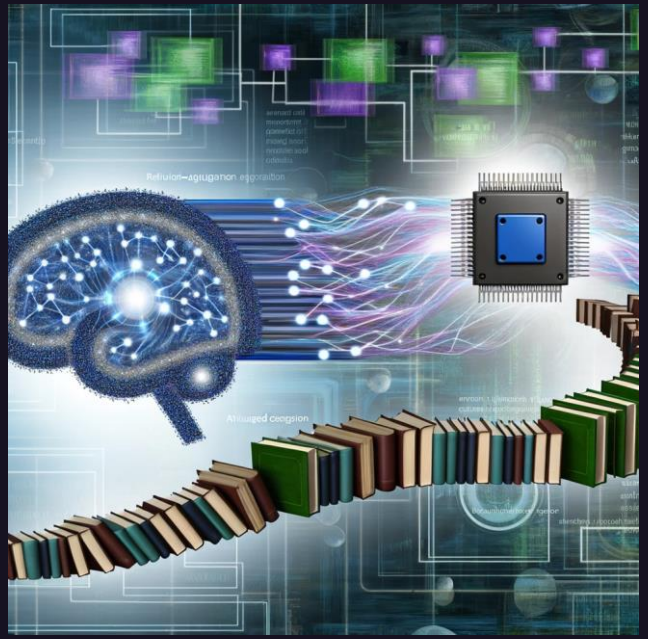
AI for everyone!

- **Self-hostable AI workflows**
  - AI with Privacy & Performance
- **Reduced Costs**
  - *More* AI-assisted workflows.
- **AI at the Edge**
  - AI within your editor, within your terminal, etc.

Improved Context Lengths & RAG

Improved memory, better one-shot learning, more specific assistance.

- **Suggestions based on your codebase & standards**
- **Better ‘one shot learning’.**
  - Utilise organisational standards.
- **Directs users to your documentation**
  - Acts almost like a search engine.



Tool Calling & Agentic Workflows

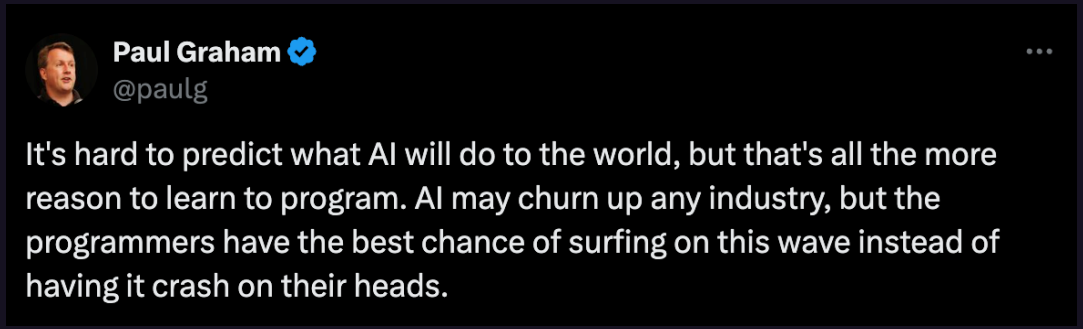
AI is learning to walk after it already learned to talk!

- **Take action based on specifications. “No code”.**
- **Interact with outside tools**
  - Interact with code editors, write and execute pipelines.
- **Self-remediating capabilities**

In Summary

- Models are rapidly improving and the right strategy is to build for the future.
- We’re only at the beginning! Things are changing fast and we need to build together to find the right use cases.
- At GitLab, we’re community focused and iterating rapidly. Partner with us!

AI is going to be everywhere. Make sure you’re surfing the wave.



GitLab

PUBLIC SECTOR NETWORK

Wednesday, June 19, 2024

GitLab Connect

Canberra, AUS

GitLab

Thank you

Come and talk to us about your AI strategy at the booth!

Partner with us and let's surf the wave together.

Connect with me on LinkedIn ->