MURILO MACHADO

MLOps | Platform Engineer | DevSecOps | QA

DETAILS

ADDRESS
Zaandam, Noord-Holland
Netherlands

PHONE
+31 645276112

EMAIL
murilo.paula.machado@gmail.com

LINKS

GitHub

LinkedIn

LANGUAGES

English

Portuguese

Dutch

SKILLS

NVIDIA DGX

vLLM

Ollama

Open WebUI

PROFILE

With 15+ years of IT experience, my career has evolved from Software Development, QA, and Pentesting to scaling my own physical IT training school into a successful consultancy. After selling my stake in the business to pursue new technical endeavors in the Netherlands, I specialized in Platform Engineering and Cybersecurity (DevSecOps, AppSec) before transitioning into AI Infrastructure and MLOps. Today, I architect secure on-premise GPU clusters (DGX), deploy LLM hosting solutions (vLLM, Open WebUI), and build open-source synthetic data pipelines (distilabel, trafilatura, firecrawl and others), leveraging my deep foundation in cloud-native infrastructure and secure SDLC to deliver production-ready AI environments. Recently, I secured a FULL WBSO granted from the Netherlands Enterprise Agency (RVO) for 3000h in AI R&D;

EXPERIENCE

Senior AI Platform & MLOps Engineer, spriteCloud
Amsterdam

Sept 2024 — Present

- Architected a secure hybrid AI infrastructure combining on-premise DGX Blackwell (Arm/128GB VRAM) for high-performance inference (vLLM, Qdrant) as a secure DMZ zone and Hetzner cloud for management (Open WebUI), bridged via a NetBird WireGuard mesh.
- Enforced Zero Trust network boundaries across the hybrid environment by integrating Google Workspace SSO as the central Identity Provider (IdP), ensuring unified, secure authentication for all internal LLM services.
- Led performance benchmarking of vLLM vs. Ollama on DGX hardware to optimize PagedAttention parameters, successfully balancing GPU memory allocation between concurrent user inference and model training workloads.
- Engineered automated CI/CD pipelines using GitHub Actions, seamlessly integrating SAST/SCA security scanning and dynamic secret management for secure production deployments.
- Successfully secured a FULL WBSO grant from the Netherlands Enterprise Agency (RVO) for 3,000 R&D hours.
- Developed and open-sourced "Topic-Lode", a production-grade

Synthetic Data Generation

LLM-as-a-Judge

distilabel

trafilatura

Firecrawl Self-hosted

Hugging Face Datasets

Parquet

MinHash Deduplication

PII Sanitization

ISO27001 Analysis and Evidence Collection

Threat Modeling (STRIDE, Attack Trees, DFDs, Trust Boundaries)

Zero-Trust Networking

NetBird

WireGuard VPN

SSO (SAML/OIDC)

Burp Suite

Secure SDLC

SAST

DAST

SCA

Secret Scanning

Dynamic Secret Management

Semgrep

Checkmarx

SonarQube

TFSec

Trivy

AWS (API Gateway, Fargate, CloudWatch)

Azure (DevOps, KeyVault, Artifact and Release Pipelines)

GCP

Hetzner

synthetic data pipeline utilizing *distilabel* for hierarchical breadth/depth knowledge mining and agentic tool-use generation, enforcing dataset integrity via automated PII sanitization, MinHash deduplication, and LLM-as-a-judge validation.
- Co-authored the "Expert Model Training Pipeline" (EMTP), creating a robust workflow using Firecrawl and DuckDuckGo to scrape, sanitize, and convert web content into high-quality Markdown QA datasets.

Security Researcher & Penetration Tester (Internal Projects), spriteCloud   Amsterdam

Mar 2021 — Present

- Conducted sporadic black-box and gray-box penetration tests for high-compliance clients in Government, Fintech, and Retail, utilizing Caido, Burp Suite, Naabu, DeepHat AI and more necessary tooling for modern vulnerability scanning;
- Follow PTES Standard;
- Discovered and remediated a critical Account Takeover (ATO) vulnerability for a global beverage e-commerce platform; Identified and patched a Privilege Escalation vector within a major educational institution's portal.
- Executed advanced enumeration to map attack surfaces across WooCommerce, Supabase, PHP, and JavaScript environments;
- Developed custom Python scripts to automate specific exploit chains and validate findings using local AI, moving beyond automated scanner results;
- Hosted and maintained DefectDojo instance on Hetzner VPS;
- Prepared reports, write-ups, and meetings to present findings, steps to reproduce, mitigation and fixing alternatives;

Senior Platform Engineer, Nationale Nederlanden via spriteCloud   The Hague

Jan 2024 — Sept 2024

- Integrated advanced security scanning tools (Semgrep, SonarQube) and SIEM observability (Splunk) into enterprise environments, resulting in a measurable reduction in security events and accelerated incident response times;
- Led comprehensive security assessments across multiple cross-functional engineering squads, facilitating mitigation planning and providing hands-on architectural support to successfully resolve security gaps;
- Spearheaded enterprise threat modeling using the STRIDE methodology, architecting and documenting comprehensive Data Flow Diagrams (DFDs), Attack Trees, and Trust Boundaries to expose and mitigate systemic risks;
- Streamlined and standardized fragmented CI/CD workflows within Azure DevOps, significantly reducing deployment lead times and increasing release reliability for development teams;

Engineering Manager, spriteCloud   Amsterdam

Jan 2023 — Jan 2024

- Directed enterprise technology strategy and served as the primary technical authority in executive stakeholder discussions, bridging the gap between business objectives and engineering execution;

Kubernetes

Helm

ArgoCD

GitOps

Terraform

Pulumi

Bicep

Docker

Containers

Nginx

GitHub Actions

GitLabCI

Jenkins

Azure Pipelines

CircleCI

TravisCI

BitRise

Bamboo

Cypress

Appium

JMeter

K6

Gatling

Playwright

Puppeteer

Protractor

Selenium

XCUITest

Espresso

BDD/Cucumber

BlazeMeter

BrowserStack

SauceLabs

- Led technical consulting engagements for major enterprise clients, translating complex requirements into actionable Cloud, QA, and DevSecOps infrastructure roadmaps.;
- Scaled and mentored distributed engineering teams, overseeing the full talent lifecycle including hiring, performance management, and 1:1s to cultivate a culture of engineering excellence.;
- Spearheaded internal innovation projects and cross-organizational mentorship programs, laying the strategic groundwork for modern platform and AI infrastructure initiatives;

Senior DevSecOps Engineer - Team Phoenix, Ahold Delhaize via spriteCloud
Zaandam

Sept 2021 — Feb 2023

- Engineered and enforced automated security gates within enterprise CI/CD pipelines,

Checkmarx (SAST), TFSec (IaC), Trivy, and Clair to proactively catch vulnerabilities pre-deployment.;

- Spearheaded DevSecOps Maturity Model (DSMM) assessments across multiple engineering squads,

identifying critical security gaps and driving the enterprise-wide adoption of secure coding practices;

- Led technical Proof of Concepts (POCs) and Proof of Value (POVs) to architect the team's security stack,

driving decisions on enterprise-grade infrastructure and scanning tools;

- Leveraged Firebase Test Lab to provision robust, scalable device testing environments, enabling rapid

feedback loops for the development teams.

Test Transformation Consultant, Ahold Delhaize via spriteCloud
Zaandam

Apr 2021 — Sept 2021

- Prepared assignments and interviewed QA candidates;
- Designed and implemented automated mobile release pipelines utilizing BitRise, Jenkins, and Azure DevOps to streamline cross-platform application delivery;
- Engineered the integration of cross-platform Flutter automation scripts directly into the deployment pipelines;
- Leveraged Firebase Test Lab to provision robust, scalable device testing environments, enabling rapid feedback loops for the development teams.

Quality Assurance Automation Engineer, Ahold Delhaize via spriteCloud
Zaandam

Jan 2020 — Apr 2020

- Define the QA Strategy;
- Introduced FrontEnd and Mobile automation in Chama;
- Introduced automated contract tests for the APIs;
- Trained QA's with Cypress and Git;
- Delivered performance tests using Gattling and k6;
- Delivered mobile, frontend, backend, and API automation;

Taurus

HP LoadRunner

Python

JavaScript

Node.js

Bash/Shell

Ruby

Go

Caido

Naabu

DefectDojo

DeepHat LLM

- Created and maintained pipeline/workflow in BitRise for mobile automation tests with Appium;
- Created and maintained build and release pipelines for automation in Azure DevOps;
- Developed a solution to test ETL Migrations and ensure data consistency after migration;

Quality Assurance Automation Engineer, Chama The App
Amsterdam

Jan 2019 — Dec 2019

- Define the QA Strategy;
- Introduced FrontEnd and Mobile automation in Chama;
- Introduced automated contract tests for the APIs;
- Trained QA's with Cypress and Git;
- Delivered performance tests using Gattling and k6;
- Delivered mobile, frontend, backend, and API automation;
- Increased the coverage by 318% for the API scenarios;
- Created and maintained pipeline/workflow in BitRise for mobile automation tests with Appium;
- Created and maintained build and release pipelines for automation in Azure DevOps;
- Developed a solution to test ETL Migrations and ensure data consistency after migration;

Software Developer Engineer In Test, QWIC
Amsterdam

Jan 2018 — Dec 2018

- Responsible for research tools, create it if needed, and cover the technicals questions;
- Ministered Dojo's classes for test automation web, performance, and load tests;
- I taught classes for newcomers in SCRUM;
- Integrated automation tests with Apex from SalesForce;
- Maintained EC2 with performance and stress tests;
- Maintained the automation jobs for every delivery;

Head of Quality Assurance & Scrum Master, Gupy
São Paulo

Apr 2016 — Jan 2018

- Head of QA responsible for study and implement new technologies, develop solutions based on squads and product necessities;
- Define the style guide used for all squads, and apply the code review for new implementations on the main Automated Test Framework;
- Responsible to implant and implement the QA area and spread the Quality mindset;
- Responsible to create the CI/CD process with Jenkins and Docker;

Co-founder & Instructor, VilasBoasIT
São Paulo

Oct 2016 — Apr 2017

- Co-founded a QA training and consultancy business; managed implementations for enterprise clients (Anheuser-Busch InBev, CVC,

ViaVarejo, Hummingbird) and established QA departments and best practices.

- Designed and delivered courses on mobile and web test automation and mentored junior engineers.

- Built automation frameworks for Web (Selenium/Capybara), API (Rest-Client), and Mobile (Calabash) and developed the open-source pretest Ruby gem to onboard newcomers.

- Implemented Continuous Integration pipelines with GitLabCI, AWS, and Azure.

Quality Assurance Automation Engineer, Anheuser-Bush InBev   São Paulo

Jan 2016 — Oct 2016

- QA Engineer responsible for study and implement new technologies, develop solutions based on squads and product necessities;
- Define the style guide used for all squads, and apply the code review for new implementations on the main Automated Test Framework;
- Create a custom report for all Automation segmentations (API/Web/Mobile), providing data for KPI from each squad environment;
- Manage the Xamarin Test Cloud to execute Calabash-iOS/Calabash-Android tests;
- Create Performance Scripts with Scala Language and Gatling;

Quality Assurance Coordinator, NetShoes   São Paulo

Jan 2015 — Jan 2016

- Responsible for minister Dojo's classes for test automation mobile and web;
- Elaboration of test plans, test cases, scenarios, test evidence, and defects report;
- Requirements, artifacts, and system functional specification analysis;
- Execution of manual, integration, regression, functional, exploratory tests, and test automation at Front

End, BackEnd, and mobile iOS and Android;

- Scripts creation and performance tests execution with JMeter and BlazeMeter;
- Test automation with Ruby, Cucumber, Calabash, Capybara, Watir, NodeJS, Supertest, and SuperAgent;
- Test automation with JMeter, Gattling, and Tsung to gather performance and scalability metrics;
- Jobs creation and maintenance at Jenkins and Travis for Continuous Integration;
- Test coverage maintenance with Istanbul and Simplecov;

OPEN SOURCE PROJECTS

aigate (AI Security Sandbox)

Developed an OS-level sandbox in Go for AI coding agents (Claude Code, Cursor, Copilot). Engineered kernel-enforced file, process, and network isolation utilizing Linux mount namespaces, POSIX ACLs, and cgroups v2 to ensure GDPR/ISO compliance and prevent unauthorized system access during AI-assisted development.

SpecHammer (Kubernetes Testing)

Created a Go-based validation framework for Kubernetes Kustomize and Helm manifests. Engineered a testing engine that evaluates infrastructure-as-code against custom YAML assertions to enforce security, performance, and compliance standards pre-deployment.

yankrun (Templating Engine)

Engineered a CLI scaffolding tool for secure repository cloning and dynamic template value replacement, featuring customizable delimiters, size-based parsing limits, and built-in transformation functions.

structlint (CI/CD Linter)

Built a Go-based CLI tool integrated into CI/CD pipelines to validate and enforce strict directory structures and file naming conventions, ensuring project consistency and creating reliable context boundaries for AI tooling.

ParseCraft & pb (CLI Utilities)

Developed a cross-format parser (JSON, YAML, Markdown) leveraging gojq for advanced data querying, alongside a cross-platform (Linux/macOS/Windows) clipboard CLI utility for terminal piping integrated with X11/Wayland.

EDUCATION

Certified Ethical Hacker, EC-Council

Ruby on Rails Bootcamp, Campus Code

Ethical Hacking Post Exploitation, GoHacking

C# Development, Impacta

BPMN, Training

Babok 2.0, Training

ITIL V3 foundations, Training

UML, Impacta

ABAP SAP Academy, Training

WebApp Security Training, Zolder

Automated pentest with Python, Python University