Winston Mascarenhas

winstonmascarenhas@gmail.com | (+49) 15256546875 | Stuttgart, Germany | LinkedIn | Portfolio

Professional Summary

Information Risk Management & cloud security **enthusiast** who builds secure, automated platforms. At Brillio: **70% faster releases** and **93.9% uptime** via CI/CD, GitOps, and real-time observability. Strengths: risk-based incident response, vulnerability management, and cross-team delivery to tight SLAs.

Work Experience

Senior Engineer, Digital Infrastructure – Brillio

October 2022 to October 2024 | Bengaluru, India

- • Reduced MTTR by 35% (from 20 to 13 minutes) and sustained 100% SLA on P1 incidents, clearing 100% backlog monthly; managed 450+ tickets/month with >95% escalation resolution.
  • Strengthened security posture by enforcing MFA, least-privilege IAM, TLS/mTLS, and segmentation; cut auth escalations by 42%, recorded zero unauthorized access incidents, and reduced MFA-related tickets by 18.
  • Built 14 Freshworks automations and 6 integrations, auto-routing 32% of tickets and cutting first-response time by 27%, saving 2.5 minutes per ticket on assignments.
  • Authored 9 L2 runbooks (phishing, MFA reset, access reviews), adopted team-wide and referenced in QA and audit preparations.
  • Automated security workflows using PowerShell and Microsoft Intune, reducing manual effort by 35% and improving device compliance from 81% to 93%.
  • Enhanced communication via calls, Microsoft Teams, and email, boosting CSAT to 97.3% and reducing resolution time by 12%.
  • Recognized as Best Employee of the Month, youngest achiever, and top-ranked for client feedback; praised by ITBP and directors for fast, high-quality resolutions.

Education

Master of Science in Computer and Systems Engineering

Technische Universität Ilmenau | Stuttgart, Germany

- Advanced Database Systems| Control Engineering| Software and Systems Engineering| Security in Embedded systems| Cloud Computing| Security Engineering| Software Safety| Advanced Mobile Communication
- Researched Ladon, a parallel multi-BFT design with DAG sequencer; achieved ~4× throughput and ~40% latency reduction with near-linear scaling.

Bachelor of Computer Application

St. Joseph's College (Autonomous) | Bengaluru, India | Graduated: 2022-10-22

Volunteering & Leadership

Volunteer – AERO INDIA 2021

2021-02-03 to 2021-02-05

- Volunteered at Aero India 2021 as Medical Department Incharge, coordinating hospital operations and facilitating liaison between Commando Air Force Hospital and Hindustan Aeronautics Limited India, ensuring strict confidentiality and emergency response readiness.

Cultural Representative – National Service Scheme

2021 to 2022

- Served as Cultural Representative (2021-2022), participating in social service events, workshops, and cultural programs with hosting responsibilities.

President – National Service Scheme

2020 to 2021

- Led **250 volunteers** to deliver **50+ drives** (blood donation, clean-ups, vaccination support), reaching **~5,000 people**.
- Introduced and enforced **event SOPs** (first aid, crowd/access control) with **minimal-PII sign-ups** and drills—**zero major incidents**.
- Coordinated approvals with university/municipality; maintained **risk register** and **after-action reviews** for continuous improvement.
- Ran rosters, logistics, and comms via **Sheets/Forms, WhatsApp, Email** using **RACI** and checklists for on-time delivery.

President – Eco- Club at St. Joseph's Pre university College

2018 to 2019

- In 2018-2019, I served as President for Eco- Club at St. Joseph's Pre university College, I was involved in leading and coordinating efforts to promote environmental awareness, sustainability, and eco-friendly practices within the college community.

Certifications

AWS Certified Solutions Architect – Associate (SAA-C03) - Amazon Web Services Training and Certification • September 2023

Skills

English C1, German A2
Programming Languages: Python, Java, C, C++, JavaScript, Bash, Rust
Databases: MySQL, MongoDB, PostgreSQL
Tools: Git, Kubernetes, Linux, Unix, Postman, GitHub
Specialisations: Active Directory, Distributed Systems, Cloud Computing
Interpersonal Skills: Dynamic team-player, Meticulous & Autonomous work ethics, Problem-Solving, Open-Minded Communication, Curious learner, Reliable

Projects

Custom CI/CD CLI for GitHub workflows

2025-08 to 2025-09

- Built a robust, containerised CI/CD system from scratch to automate build, test, and deployment project-specific workflows using YAML configs. Orchestrated microservices with Kubernetes and integrated version control, RabbitMQ, MongoDB, and MinIO-boosting deployment speed and release reliability by 30%, with 70%+ test coverage.

HISSEC – ABAC-Based Access Control for Hospital Information System

2025-06 to 2025-07

- Selected ABAC (ABAC variant) as core paradigm, incorporating GDPR-style principles, rust and ward-level data isolation. Designed attribute resolution strategy reducing rule complexity by 40% and enabling faster policy updates. Modeled user/admin state transitions as deterministic automaton to prevent privilege escalation; authored formal policies ensuring auditability.

Elastic ML Inference Serving

2025-05 to 2025-07

- Built a secure, autoscaling inference prototype (CPU-only ResNet-18) handling bursts ~150 **requests/sec (RPS)** with **p95 (95th-percentile) ≈ 280 ms** and **<1% errors** in lab benchmarks; **−35% downtime** in fault-injection drills.
- Security by design: HTTPS/TLS, API tokens, rate limits, secrets hygiene, **PII-free** logging.
- Ops: Prometheus/Alertmanager/Grafana, ELK/Loki, GitHub Actions; **MTTD ≈ 2 min**, canary rollback **<3 min**, **MTTR ≈ 6 min**; health checks, graceful restarts, autoscaling on CPU & queue depth.

AES Implementation

2024-11-20 to 2024-12-04

- Developed AES encryption/decryption module compliant with NIST FIPS-197, implementing core rounds and ECB/CBC modes.
- Validated against official NIST test vectors with 100% correctness; applied secure key handling practices.
- Benchmarked runtime and memory usage using Python profiling tools, demonstrating secure and efficient implementation.

Weaponization of IOT- The rise of Microbots

2020-05 to 2020-10

- Conducted 6-8 weeks of academic research reviewing 35-45 sources; applied STRIDE and MITRE ATT&CK frameworks.
- Identified critical IoT risks including insecure boot, unsigned firmware, weak credentials, and poor segmentation enabling lateral movement.
- Proposed mitigations such as secure boot, signed firmware, identity-first access, OTA hardening, and Zero Trust micro-segmentation.