Omar Passos — CV (English)

Oct 2, 2026 · @Omar Passos

Curitiba, Brazil · Open to remote work omar.ctba@gmail.com · +55 41 99968-1251 · linkedin.com/in/omarpassos · omar-passos.vercel.app

Summary

I've spent 15+ years in tech, more than 12 of them living and breathing security, working my way up from analyst to CISO at places like TOTVS, Copel, DNIT, and a few scale-ups along the way. What I'm really good at is building a security function from scratch and taking it from "we don't really have one" to genuinely mature: ISO 27001/ISMS, running a SOC (SIEM, EDR, the whole alert-triage grind), incident response, risk-based vulnerability management with real follow-through on actually fixing things, risk assessments, audits, LGPD (Brazil's privacy law), and third-party risk.

I lean on frameworks like ISO/IEC 27001, NIST CSF, CIS Controls, and PPSI 2.0, and I've got solid hands-on experience with networking, firewalls, IDS/IPS, and security architecture across AWS, Azure, and GCP. I'm comfortable leading technical teams, working closely with IT to keep things compliant, and, maybe most importantly, turning threats and compliance headaches into priorities and numbers that actually make sense to a C-level exec or a board.

On the side, I founded zynTRIQ, a platform for Attack Surface Management and GRC that puts a real dollar figure on risk (FAIR methodology). I've also worked at an international company and get by comfortably in conversational English.

Skills

- **Monitoring & SIEM:** SIEM (ELK), monitoring dashboards, security event analysis, alert triage
- **Detection & Response:** EDR/XDR, SOAR, incident response, DFIR, digital forensics, Threat Intelligence, playbooks
- **Vulnerability Management:** vulnerability assessments, risk-based vulnerability management (RBVM), Attack Surface Management, pentesting, Purple Team, SLA-driven remediation, FAIR

- **Networks & Security Architecture:** firewalls (Fortigate, PFSense), IDS/IPS (Snort, Suricata), VPN, hardening
- **Frameworks & Compliance:** ISO/IEC 27001 (ISMS), NIST CSF, CIS Controls, PPSI 2.0, LGPD, PCI-DSS, internal and external audits
- **Risk & Governance:** risk analysis, third-party risk management, security policies, awareness programs
- **Data Protection:** DLP, data classification, tokenization, masking
- **Cloud & Automation:** AWS, Azure, GCP; Python, Go, Ruby
- **Investigation:** OSINT, corporate intelligence, due diligence, evidence analysis

Languages

- **Portuguese:** native
- **English:** conversational, intermediate level

Work Experience

Founder & Head of Cyber Security — zynTRIQ

São Paulo, SP · 07/2023 – Present (run on the side, alongside my 2023–2025 roles)

- Came up with the idea for zynTRIQ and I'm leading its development, it's a platform for Attack Surface Management, Vulnerability Intelligence, and GRC that ties exposure, vulnerabilities, and financial risk together (FAIR methodology).
- Built ISO/IEC 27001, NIST CSF, CIS Controls, and PPSI 2.0 right into the platform, mapping vulnerability and exposure findings to real controls and compliance requirements.
- Cut average triage time for findings by roughly 60% through automation (Python, Go, Ruby) and more standardized processes.
- Knocked the critical vulnerability backlog down by about 45% with RBVM and tighter SLA governance on fixes.
- Designed data protection controls (discovery, classification, tokenization, masking, DLP) hooked into SIEM (ELK) and response pipelines, including cloud exfiltration detection.
- Set the security roadmap and policies, aligned with ISO/IEC 27001, NIST CSF, LGPD, PCI-DSS, CIS Controls, and PPSI 2.0.

Cyber Defense Center Coordinator — Task TI

Curitiba, PR · 12/2024 – 07/2025

- Set the strategy and operating model for the SOC, picking and rolling out IVM, IDR, ASM, DFIR, MDR, and OSINT tools.
- Ran monitoring and analysis of security events through SIEM and EDR, including alert triage and escalation.
- Led investigation and response to security incidents, from containment through recovery, keeping business stakeholders in the loop the whole way.
- Wrote the incident response playbooks and docs, standardizing how the SOC ran.
- Led a team of security specialists, handling resourcing, performance, and delivery.
- Kept things compliant through ongoing audits and security assessments.

Information Security Architect — Copel

Curitiba, PR · 07/2024 – 10/2024

- Designed and rolled out security architecture for a large-scale corporate environment, with ongoing risk analysis and assessment.
- Implemented, monitored, and validated security controls, and ran awareness initiatives for employees.

Information Security Specialist — meutudo.

Fortaleza, CE (remote) · 12/2022 – 05/2024

- Built the fintech's security program from the ground up: security policy, ISMS (ISO/IEC 27001), RBVM, and third-party risk management.
- Ran vulnerability assessments and coordinated fixes with IT and dev teams.
- Rolled out application security monitoring with SIEM (ELK) dashboards and network controls (PFSense firewall, Snort/Suricata IDS/IPS).
- Worked on pentesting and Purple Team exercises, and led the security awareness program (talks, handbooks, videos, gamification).

CISO — Exago Innovation

Portugal (remote) · 01/2022 – 11/2022

- Owned information security for the company end to end, rolling out a security and compliance program covering RBVM, ISMS, and third-party risk management.

- Led application security initiatives, human-factor risk management, and built out a cybersecurity culture.

Senior Information Security Analyst — TOTVS

Curitiba, PR · 12/2020 – 01/2022

- Contributed to the information security policy and the RBVM/ISMS program at one of Brazil's biggest software companies.
- Ran penetration tests and Purple Team exercises, validating perimeter and detection controls.
- Built SIEM (ELK) dashboards for security event monitoring and ran awareness campaigns with gamification.

Security Analyst / Pentester — Rentcars.com

Curitiba, PR · 12/2019 – 08/2020

- Worked on pentesting, vulnerability management, incident investigation, and getting LGPD compliance rolling.

Security Consultant, Pentester & Bug Bounty — Independent

Remote · 08/2018 – 12/2019

- Ran penetration tests, did reverse engineering, and handled DDoS attack response.

Network Security Analyst — DNIT

Brazil · 06/2014 – 06/2018

- Managed Fortigate firewalls and VPNs, and monitored security events through SIEM.
- Worked on digital forensics and DDoS attack analysis.

IT & Projects Coordinator — Levier Tecnologia

Brazil · 07/2008 – 11/2012

- Coordinated infrastructure, data, and systems development, including work with neural networks.

Education

- **Business Administration**, focus on Foreign Trade — PUC-PR, 1998–2004

Certifications

- **CISM** — Certified Information Security Manager, ISACA
- **SANS FOR508** — Advanced Computer Forensics & Incident Response, SANS Institute, 2012
- **EXIN PDPE** — Privacy & Data Protection Essentials (LGPD), EXIN, 2020
- **ISO/IEC 27001 Foundation Essentials** — PMG Academy, 2020

Other Courses I've Taken

- CIS Controls — ENAP, 2024
- CS50 — Introduction to Computer Science, Harvard / Fundação Estudar, 2023
- CRISC — Cybrary, 2019
- CEH v10 — CIP Cyber, 2019
- OSCP — Kali Linux
- CompTIA Network+ — Cybrary
- LGPD — ENAP, 2019
- Cloud Computing Fundamentals — SOFTEX, 2019