Marco **Lancini**

Director of Security · CISO

Hampshire, UK

marco@marcolancini.it | marcolancini.it | marcolancini | marco-lancini | @lancinimarco

Summary

I am a Director of Security and Certified Chief Information Security Officer (C|CISO) with 13 years of experience building security functions from the ground up at Fortune 500 companies, pre-IPO startups, and high-growth organizations. I specialize in establishing security programs that enable business growth, securing multi-million-dollar deals through compliance initiatives (HIPAA, SOC2, PCI DSS), and building cross-functional teams that position security as a strategic partner across engineering, product, legal, and go-to-market functions.

I write about security strategy, technical leadership, and cloud security. I am the author of The CloudSec Engineer, a book on how to enter, establish yourself, and thrive in the Cloud Security industry.

I curate CloudSecList, a newsletter that keeps thousands of security professionals informed about current happenings and news related to the security of cloud-native technologies, and CloudSecDocs, a website collecting and sharing my technical notes and knowledge on cloud-native technologies, security, technical leadership, and engineering culture.

I served on the committee that created the Certified Kubernetes Security Specialist (CKS) certification, worked as a maintainer of Cartography (a CNCF-incubated security tool), and presented research at top-tier security conferences including Black Hat, KubeCon, and OWASP AppSec. I mentor young professionals through the Lead the Future program, a non-profit helping Italian talents pursue STEM careers.

Work Experience

Director of Security — August 2024 - now

Lakera — *Remote*

- Hired as the first Security hire to **build and lead the Security Department** end-to-end, reporting directly to the CTO. Built and grew the team while owning strategy, roadmap, and **seven-figure annual budget** across all Security verticals.
- Established foundational Security processes from scratch:
  - Built the Security roadmap and technical risk registry with prioritized remediation plans aligned to business objectives.
  - Established quarterly review cadence and decision logs to enable transparency and drive a proactive Security culture.
  - Implemented internal communication strategies that foster psychological safety.
  - Advised C-suite on security strategy, risk posture, and investment priorities, translating technical risks into business impact for executive decision-making.
- Built **cross-functional** collaboration spanning Engineering, Product, Legal, Sales, Marketing, and HR teams, positioning Security as a strategic partner across the organization.
- Drove product Security maturity and vulnerability management:
  - Deployed a logging infrastructure organization-wide with automated alerting, enabling continuous monitoring and threat detection.
  - Established incident response capability with coordinated response procedures and post-incident analysis to strengthen organizational resilience.
  - Defined and implemented vulnerability management procedures, Security disclosure policies, and tooling integrations to track and remediate issues against SLAs.
  - Integrated Security into SDLC by working with Engineering teams to implement secure development practices, shifting Security left in the development lifecycle.
- Led enterprise-wide identity and access management transformation, deploying Okta with hardware-based MFA (YubiKeys) across all critical systems through phased rollout and change management.
- Achieved compliance milestones that directly enabled **market expansion** and positioned Security as a **go-to-market enabler**:
  - Led company-wide HIPAA and GDPR compliance initiatives, closing all administrative, technical, and physical safeguard gaps to unlock healthcare vertical opportunities.
  - Delivered exception-free SOC2 Type II audit through evidence collection, control implementation, and cross-functional coordination.
  - Established third-party risk management program, implementing vendor security assessment processes, due diligence procedures, and ongoing monitoring to protect supply chain security.
  - Directly supported deal closures with enterprise customers by responding to Security questionnaires and providing security domain expertise that accelerated sales cycles.

Principal Security Engineer — April 2022 - August 2024

GitLab — *Remote*

- Promoted to Principal Security Engineer, the first in GitLab Security organization history. Provided **technical leadership across 4 Security sub-departments** (80 professionals), securing GitLab's SaaS platform serving 30 million users.
- Led department-wide strategic initiatives with **regular executive reporting** to CTO and C-suite:
  - Drove cultural transformation to shift Security Department from a reactive to a proactive approach, introducing Architecture Decision Records to embed security early in engineering processes.
  - Led cross-organizational initiative to redefine infrastructure production access management, addressing top company risks involving Security, Infrastructure, and IT teams.
  - Led ransomware protection initiative with direct CTO and board visibility, designing multi-phase approach to protect production data and backups, providing executive briefings on threat landscape and risk mitigation strategies.
- Established department-wide mentoring and development programs, formalized learning hours and 1:1 coaching across InfraSec, AppSec, Red Team, Field Security, and Compliance teams.
- Drove hiring and team development: defined technical interview processes, delivered 40 interviews, onboarded multiple engineers, and coached team members promoted to Staff Security Engineer level.

Staff Cloud Security Engineer (acting Engineering Manager) — April 2021 - April 2022

GitLab — *Remote*

- **Bootstrapped GitLab's Infrastructure Security team from zero**, serving as acting Engineering Manager. Established team roadmap, defined processes for cross-department support, and built technical foundation and automation infrastructure used department-wide.
- Built and scaled the team as sole tenured IC: defined interview processes, onboarded 3 engineers concurrently, and established team culture focused on transparency, design documents, architectural decision records, and risk registries.
- Provided security architecture guidance for GitLab Dedicated , a new single-tenant SaaS offering with focus on data residency, isolation, and private networking for complex compliance requirements.
- Led security monitoring initiatives that provided visibility across GitLab's production infrastructure, enabling detection of misconfigurations and security threats at scale.

Lead Cloud Security Engineer — Aug 2019 - March 2021

Thought Machine — *London, UK*

- Joined as the **first Cloud Security hire** and built the team from scratch, growing it to 6 engineers. **Promoted to Lead** within 14 months, managing the team while providing technical leadership across Security, Infrastructure, and Engineering organizations.
- Defined and led cloud security strategy aligned with CSA CCM for a multi-cloud SaaS banking platform built on top of Kubernetes, distributed micro-services, and supporting the 3 major cloud providers (AWS, GCP, and Azure).
- Led cross-organizational initiatives involving Security, IT, DevEx, Cloud, and Engineering teams:
  - Designed and led implementation of a Cloud IAM framework that overhauled authentication and authorization for 300+ engineers across cloud providers.
  - Architected comprehensive security logging and monitoring solution for cloud environments and Kubernetes clusters aligned with industry standards.
  - Coordinated SaaS threat modeling effort across application, cloud, and corporate security teams.
- Drove security controls and architecture that enabled PCI DSS, ISO 27001, and SOC 2 compliance, implementing detective and responsive controls at scale across hundreds of cloud accounts and Kubernetes clusters.

Senior Security Engineer — Feb 2018 - Aug 2019

Mastercard — *London, UK*

- **Built and led Mastercard's Offensive Security Program**, managing **multi-million-dollar budget**, strategy, and headcount. Established red teaming charter and matured penetration testing capabilities, scaling delivery 6x year-over-year.
- Grew and managed fully remote team from 3 to 7 engineers across USA, EU, and APAC regions. Established processes, methodologies, and tooling to enable team scaling and career development, coaching 2 engineers to senior promotions.
- Provided security architecture guidance for Mastercard's cloud transformation of 63 globally distributed data centers, advising on containerization (Docker/Kubernetes) and CI/CD pipeline security across multiple business units.

Security Consultant — 2015 – 2018

MWR InfoSecurity (now F-Secure) — *London, UK*

- Led multi-million-dollar project to secure flagship mobile applications (24 million customers) for major UK bank, managing team of 8 security engineers and providing domain expertise.
- Drove research initiatives for UK mobile security practice, coordinating with Head of Global Research to mentor consultants and increase international conference submission/acceptance rate by 30%.
- Created Needle , an iOS Security Testing Framework, and collaborated with OWASP on Mobile Testing Guide, establishing industry-standard mobile security assessment methodologies.

Security Researcher and Consultant **2013 – 2015**

CEFRIEL *Milan, Italy*

- Delivered security consulting across banking, logistics, energy, and telecommunications sectors, spanning governance and risk management to technical assessments (penetration testing, vulnerability assessments) and custom security tooling development.
- Conducted research on emerging attack vectors and security trends, providing strategic guidance to enterprise clients on evolving threat landscapes.

Certifications

Leadership & Management

Certified Chief Information Security Officer (C|CISO), EC-Council
Certified Information Systems Security Professional (CISSP), (ISC)2
Certified Cloud Security Professional (CCSP), (ISC)2

Technical Certifications

Certified Kubernetes Security Specialist (CKS), CNCF
AWS Certified Security - Specialty (AWS SCS), Amazon AWS
GCP Professional Cloud Security Engineer, Google Cloud
Offensive Security Certified Professional (OSCP), Offensive Security

Education

M.Sc. in Engineering of Computing Systems **2013**

Politecnico di Milano *Milan, Italy*

- University is the #1 ranked university for Computer Science and Engineering in Italy.
- Won the NATO CCDCOE Best Thesis Award, and the Clusit Thesis Award.

B.Sc. in Engineering of Computing Systems **2011**

Politecnico di Milano *Milan, Italy*

Community & Industry Contributions

Writing

The CloudSec Engineer

- Author of The CloudSec Engineer , a book on how to enter, establish yourself, and thrive in the Cloud Security industry as an individual contributor.

CloudSecList

- Curator of CloudSecList.com , a newsletter that keeps thousands of security professionals informed about current happenings and news related to the security of cloud-native technologies.

CloudSecDocs

- Curator of CloudSecDocs.com , a website collecting and sharing technical notes and knowledge on cloud-native technologies, security, technical leadership, and engineering culture.

Technical Blog

- I write a technical blog (marcolancini.it). Popular articles include collections like Applied AI for Security & Engineering , Cloud Security Strategies , Kubernetes Primer for Security Professionals , and Continuous Visibility into Ephemeral Cloud Environments

Industry Engagement

Lead the Future

- Mentor in the Lead the Future program, a non-profit that helps young Italian talents to pursue a career in the STEM field.

Publications & Conference Talks

- Presented at international security conferences including Black Hat (USA/EU), NATO's CYCON, KubeCon, OWASP AppSec, BSides, and DEEPSEC.
- Published research in top-tier security conferences including ACM CCS and ACSAC.
- Technical reviewer of Cloud Native DevOps with Kubernetes , 500 Lines or Less , and IEEE Journals (e.g., "*Transactions on Emerging Topics in Computing (TETCSI)*").

CNCF Security Technical Advisory Group (STAG)

- Member of the CNCF Security Technical Advisory Group (STAG) , which facilitates collaboration to discover and produce resources that enable secure access, policy control, and safety for operators, administrators, developers, and end-users across the cloud native ecosystem.
- Part of the CNCF committee that created the Certified Kubernetes Security Specialist (CKS) certification.
- Part of the Cloud Native Security Day Program Committee.

OWASP

- I've been involved for several years in the OWASP Project. Over the years I contributed to projects like the Web Application Top 10 and the Mobile Security Testing Guide .

Cloud Security Roadmap

- Released a framework to establish a cloud security program aimed at protecting a cloud native, service provider agnostic, container-based, offering, aligned with NIST and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).
- Created a micro-website with the roadmap template, and a companion blog post (On Establishing a Cloud Security Program) to explain the details.

Cartography

- Maintainer of Cartography , a Python tool that consolidates infrastructure assets and the relationships between them in a graph view powered by a Neo4j database. Actively helped define the long-term roadmap, contributed new features, and focused on improving its reliability and speed.
- Helped get Cartography incubated by the CNCF .
- Drove adoption in Kubernetes environments, producing articles (Mapping Moving Clouds , Tracking Moving Clouds , Automating Cartography Deployments on Kubernetes) and conference talks (Cartography: using graphs to improve and scale security decision-making).