Marco **Lancini**

PRINCIPAL SECURITY ENGINEER

London, UK

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

Summary

I am a Principal Security Engineer with experience building security functions at Fortune500, pre-IPO companies, and exponential growth startups. Currently, I own efforts to secure GitLab's SaaS cloud infrastructure and container technologies.

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 blog about cloud security and technical leadership, and I'm writing The CloudSec Engineer, a book on how to enter, establish yourself, and thrive in the cloud security industry as an individual contributor.

I am a member of the AWS Community Builders program, part of the committee tasked with creating the Certified Kubernetes Security Specialist (CKS) Certification, and a mentor in the Lead the Future program, a non-profit that helps young Italian talents pursue a career in the STEM field.

Languages and Technologies

Languages	Python, Go, Bash
Technologies	• *Cloud Providers*: AWS, GCP, Azure. • *Containerization*: Docker, Kubernetes. • *Infrastructure as Code*: Terraform, Ansible, HashiStack.
Other	• Cloud networking architecture, cloud operations, security, automation and orchestration. • Security requirements in the cloud aligned with PCI, GDPR, ISO27K, Cloud Security Alliance (CSA). • Security issues associated with containers, Kubernetes, distributed systems, and large-scale web applications. • Software Architecture, Secure Software Development, Project Management.

Work Experience

Principal Security Engineer — April 2022 - now

GITLAB — *Remote*

- Acted as Tech Lead for the whole Security Department. Examples include initiatives like shifting the Security Department's mindset from reactive to proactive, and liaising with other departments (e.g., Product and Infra) to start producing Architecture Decision Records that allow for Security to be looped in early enough to provide meaningful and timely advice.
- Led cross-department projects like the "Ransomware Protections for Backups" initiative, with direct interest from the CTO and senior leadership, to protect the production data and its backups from the threat of ransomware.
- Instilled the culture needed to enable a high-performing team; examples of this were following an Agile/Kanban process to define work intake and visualize/limit work in progress, having quarterly retrospectives, and having psychological safety as the base for a blameless culture.
- Focused on hiring and growth:
  - Defined and formalized the Technical Interview process for the InfraSec and Security Logging teams, and delivered 40 technical interviews.
  - Onboarded multiple ICs concurrently and coached them to improve their project management, communication, and technical writing skills and adapt them to a remote work setting.
  - Coached and helped other members being promoted to Staff Security Engineers.

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

GitLab — *Remote*

- Bootstrapped GitLab's Infrastructure Security team, which owns efforts to secure GitLab's SaaS cloud infrastructure and container technologies. In particular:
  - Instituted the team's roadmap and defined processes for providing counterpart support to other departments.
  - Created the first iteration of technical resources for the team. This included Terraform configuration for the team's technical resources, GitLab CI/CD pipelines, Kubernetes workloads, Docker images, etc. These resources continue to be used regularly by the Infrastructure Security Team and other teams throughout the organization.
  - To support growing the team, defined an interview process and created a new team member onboarding plan. The onboarding plan included a checklist and supporting documentation to ensure new members would be able to get up to speed quickly.
  - Instilled a culture focused on transparency and information sharing; examples of this are the use of design documents during the definition of software designs, architectural decision records, and risk registries.
- Guided the design of GitLab Dedicated , a new single-tenant SaaS offering with a focus on data residency, isolation, and private networking to meet complex compliance needs.
- Led the team's projects, which included the rollout of Falco and OSQuery to provide security visibility over Gitlab's production fleet running on GKE and GCE, and Cartography to manage the multi-cloud inventory of resources.
- Provided expert knowledge needed to support other teams' operations. Examples are the delivery of multiple Production Readiness Reviews (performed to identify the security and reliability needs of a new service), and support to the Incident Response team during security incidents.

Lead Cloud Security Engineer — **Oct 2020 - March 2021**

Thought Machine — *London, UK*

- As Tech Lead, provided security expertise ranging from architecting high-level designs impacting the whole company, to implementing security controls which helped achieve PCI DSS, ISO 27001, and SOC 2.
- Designed and led a team of engineers implementing an ad-hoc Cloud IAM framework, which overhauled and matured the way the 300+ engineers authenticated and got authorised to access cloud environments, agnostically from the underlying cloud provider.
- Designed and worked with multiple teams (like operations and SREs) to rollout a comprehensive monitoring & alerting solution, able to collect logs from both cloud environments and Kubernetes clusters, as well as ensuring it is in line with industry standards.
- Collaborated with infrastructure teams to rollout and mature security controls required to properly secure the multiple Kafka clusters used by the core banking platform, without impacting performance.

Cloud Security Engineer — **Aug 2019 - Oct 2020**

Thought Machine — *London, UK*

- Joined as the first cloud security hire, and grew the team to 6 engineers (with a mix of both security and backend engineers).
- Defined and led the cloud security strategy, aligned with CSA CCM and prioritised consistently with the company's product: a SaaS banking platform built on top of Kubernetes, distributed micro-services, and supporting the 3 major cloud providers (AWS, GCP, and Azure).
- Designed and built Detective and Responsive controls in AWS/GCP and Kubernetes, to enforce the security baseline at scale for hundreds of accounts. Collaboratively worked with developers and DevOps engineers to implement and integrate such controls in the main CI/CD pipeline.
- Built automation to provide asset inventory and actively audit the infrastructure for security misconfigurations (whether at the Cloud provider or Kubernetes level).

Senior Security Engineer — **Feb 2018 - Aug 2019**

Mastercard — *London, UK*

- Built and led Mastercard's Offensive Security Program, managing budget and long-term strategy (like headcount and business requirements) while building the team's technical capabilities:
  - Bootstrapped the red teaming charter.
  - Matured the network penetration testing service to deliver 6 times the number of assessments compared to the same timeframe in previous years.
- Provided domain expertise for Mastercard's migration of their 63 globally distributed data centres to the Cloud, by ensuring the security and robustness of the new architecture, and the integration of containerization technologies (i.e., Docker and Kubernetes) within the main CI/CD pipeline. While doing so, I worked with multiple teams within the business to coordinate and provide security guidance on the rollout of the new deployments.
- Managed a fully remote team, spanning USA/EU/APAC, and grew it to 7 engineers. Coached and mentored 2 junior team members who got promoted to senior engineers.
- Defined processes/methodologies/best practices, as well as created custom tooling and infrastructure, required to support the scaling of the team and to assist junior team members in their own career progression.

Security Consultant
2015 – 2018

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

- Delivered more than 90 security assessments covering mobile, infrastructure, web and desktop application security testing, as well as code reviews.
- Led a multi-million-dollar project to secure the flagship applications (supporting over 24 million customers) of one of the biggest UK banks, acting as domain expert and lead of a team of 8 security engineers.
- Drove research initiatives for the UK mobile practice of MWR, coordinating directly with the Head of Global Research to provide guidance and support to other consultants within the company. Increased the submission/acceptance rate to international security conferences by 30%.
- Created Needle , an iOS Security Testing Framework, and developed the ”Offensive iOS Exploitation” training, which I delivered at international security conferences.
- Collaborated with OWASP to create the ”Mobile Testing Guide”, to provide a standardised process for security professionals to follow when assessing mobile solutions.
- Supported internal processes such as mentorship, recruiting, team building, and quality assurance.

Security Researcher and Consultant
2013 – 2015

CEFRIEL *Milan, Italy*

- Engaged in consulting projects for both public and private companies (in sectors like banking, assurance, logistics, energy, and telecommunications), ranging from providing support for Security Governance and Information Security Management, to more technical engagements like the delivery of Vulnerability Assessments & Penetration Tests and the design and development of ad-hoc tools (in areas like fraud management, automatic testing, crawling and information retrieval).
- Performed research on new attack vectors, aiming to highlight new trends of attacks and threats contextualized to the reality of corporate clients (e.g., mobile malware, cryptocurrencies threats, HCE payments, etc.).
- Created and delivered training courses focused on topics such as enterprise security and penetration testing techniques.

Certifications

2023	**AWS Certified Security - Specialty (AWS SCS)**, Amazon AWS
2021	**GCP Professional Cloud Security Engineer**, Google Cloud
2021	**GCP Associate Cloud Engineer**, Google Cloud
2020	**Certified Kubernetes Security Specialist (CKS)**, CNCF
2020	**Microsoft Certified: Azure Fundamentals**, Microsoft
2020	**HashiCorp Certified: Terraform Associate**, HashiCorp
2020	**HashiCorp Certified: Vault Associate**, HashiCorp
2019	**Certified Cloud Security Professional (CCSP)**, (ISC)2
2019	**Certified Information Systems Security Professional (CISSP)**, (ISC)2
2018	**AWS Certified Solutions Architect - Associate (AWS CSA)**, Amazon AWS
2015	**CREST Registered Penetration Tester (CRT)**, CREST
2014	**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*

Projects and Community

Writing

Technical Blog

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

CloudSecList

- I curate 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

- I curate CloudSecDocs.com , a website collecting (~200 pages) and sharing my technical notes and knowledge on cloud-native technologies, security, technical leadership, and engineering culture.

Technical Books

- Technical reviewer of Cloud Native Devops with Kubernetes , 500 Lines or Less , and of some IEEE Journals (e.g., ”*Transactions on Emerging Topics in Computing (TETCSI)*”).

Projects

Lead the Future — 2022 – now

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

Cloud Security Roadmap — 2021 – now

- 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.

CloudSecGPT — 2023

- CloudSecGPT is a custom-built generative AI model that specializes in cloud security. This model is pre-loaded with an extensive knowledge base, encompassing a broad spectrum of subjects within the cloud security domain. It includes comprehensive data and insights from industry-leading resources, and it incorporates the entire content of CloudSecDocs.com .

CNCF Security Technical Advisory Group (STAG) — 2020 – 2023

- I am a 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.
- I have been part of the CNCF committee tasked with creating the Certified Kubernetes Security Specialist (CKS) certification.
- I have been part of the Cloud Native Security Day EU 2021 Program Committee.

Cartography — 2019 – 2023

- I am a maintainer of Cartography , a Python tool that consolidates infrastructure assets and the relationships between them in a graph view powered by a Neo4j database.
- As part of my involvement, I’m actively helping define the long-term roadmap for Cartography, as well as contributing new features and focusing on improving its reliability and speed.
- I’m also driving its adoption in Kubernetes environments, producing articles (Mapping Moving Clouds: How to stay on top of your ephemeral environments with Cartography , Tracking Moving Clouds: How to continuously track cloud assets with Cartography , Automating Cartography Deployments on Kubernetes), and conference talks (Cartography: using graphs to improve and scale security decision-making).

k8s-lab-plz: A modular Kubernetes Lab — 2020 – 2021

- I am the creator and maintainer of k8s-lab-plz , a modular Kubernetes lab which provides an easy and streamlined way to deploy a test cluster with support for different components.
- Supports both minikube and baremetal installations.

GoScan: An interactive network scanner — 2018 – 2019

- GoScan is an interactive network scanner client, featuring auto-completion, which provides abstraction and automation over `nmap`.
- Although it started as a small side-project I developed in order to learn Golang, GoScan can now be used to perform host discovery, port scanning, and service enumeration not only in situations where being stealthy is not a priority and time is limited (e.g., CTFs, OSCP, exams, etc.), but also during professional engagements.

Needle: The iOS Security Testing Framework — 2016 – 2018

- Needle is an iOS Security Testing Framework, released at Black Hat USA 2016. It is an open source modular framework which aims to streamline the entire process of conducting security assessments of iOS applications, and acts as a central point from which to do so. Needle is intended to be useful not only for security professionals, but also for developers looking to secure their code.
- Needle has been presented at and used by workshops in various international conferences like Black Hat USA/EU, OWASP AppSec and DEEPSEC.
- It was included by ToolsWatch in the shortlist for the Top Security Tools of 2016 , and it is featured in the OWASP Mobile Testing Guide . It reached #3 on Netsec, the first page of Hacker News, and it has been trending on Github.

OWASP **2013 – 2018**

- 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 .

Conference Talks

Cartography: using graphs to improve and scale security decision-making **2020**
Cloud Native Security Day North America 2020 *Virtual*

Needle v1.0.0: new native agent and CI integration **2017**
Black Hat Arsenal USA *Las Vegas, USA*

Offensive iOS Exploitation **2016**
DEEPSEC *Vienna, Austria*

Needle **2016**
Black Hat Arsenal EU *London, UK*

Needle: Finding Issues within iOS Applications **2016**
OWASP AppSec USA *Washington DC, USA*

Needle **2016**
Black Hat Arsenal USA *Las Vegas, USA*

Enhancing Mobile Malware: an Android RAT Case Study **2014**
BSides Vienna *Vienna, Austria*

Social Authentication: Vulnerabilities, Mitigations, and Redesign **2014**
DEEPSEC *Vienna, Austria*

Social Authentication: Vulnerabilities, Mitigations, and Redesign **2014**
International Conference on Cyber Conflict (CyCon) by NATO CCDCOE *Tallinn, Estonia*

Publications

In Depth Security (Proceedings of the DeepSec Conferences) **2016**
DEEPSEC *Vienna, Austria*

Social Authentication: Vulnerabilities, Mitigations, and Redesign **2014**
Proc. of the DeepSec Conferences - Magdeburger Journal zur Sicherheitsforschung *Vienna, Austria*

Faces in the Distorting Mirror: Revisiting Photo-based Social Authentication **2014**
Proc. of the 21st ACM Conference on Computer and Communications Security (CCS) *Scottsdale, Arizona, USA*

All your face are belong to us: Breaking Facebook's Social Authentication **2012**
Proc. Annual Computer Security Applications Conference (ACSAC) *Orlando, Florida, USA*