# Nicolas V.

Security Engineer | AppSec, SSDLC, Vulnerability Management & Cloud | PCI-DSS, SOC 2, CRA
LinkedIn | GitHub | nclv.pages.dev | Paris, hybrid or remote

## PROFILE

Security engineer with a software development and penetration testing background, now on the defensive side: SSDLC, vulnerability management, hardening of cloud and CI/CD, and compliance (PCI-DSS, SOC 2, CRA) for payment platforms. Uses an attacker's view to prioritise what matters and works with development and platform teams to get it fixed.

## EXPERIENCE

**Security Engineer**, Ingenico — Sep 2025 - present

- **Vulnerability management:** built the programme from scratch: risk-based prioritisation (CVSS, EPSS, KEV, SSVC), OpenVEX to remove false positives, Jira workflow with SLAs and reporting, and automated retests (one replayable test per vulnerability, run in every environment)
- **Product security:** led architecture reviews, threat models and penetration tests across the cloud platform, payment terminals, PKI/HSM and e-signature products: 500+ vulnerabilities documented, each with a proof of concept (from the source code or tested on a real environment), a severity rating and a proposed fix
- **SSDLC:** embedded security in the SDLC with development and platform teams (1,300+ developers): threat modeling, code review, SAST/DAST/SCA in CI, SBOMs and signing (SLSA). Ran the secret scanning initiative across all teams in China and on the cloud platform
- **Cloud, CI/CD and IAM:** audited the software factory and cloud platform: CI/CD, Vault, Okta, Terraform and AWS (IAM, SCPs, network exposure), Kubernetes, Keycloak-based authentication (BFF) and OAuth/SAML federation with customers' external identity providers; real attack paths demonstrated
- **Standards and compliance:** wrote the security standards (cryptography, supply chain, containers, Kubernetes, secrets, CI/CD, LLM agents) and the technical requirements and evidence for PCI-DSS, SOC 2 and CRA; evaluated the security tools (Wiz, SonarQube, Burp Suite), deployed Burp Suite DAST and piloted the other rollouts (usage, users, least privilege)
- **Mentoring:** lead the security ambassadors network (weekly sessions) and filter external pentest reports so that teams only receive validated findings; selected the developer training platform (SecureFlag)
- **AI:** built AI-assisted vulnerability research and CVE triage, with an automated validator on the model's output

**Offensive Security Consultant and Software Engineer**, Calypt/Lexfo — Feb 2022 - Aug 2025

- Penetration tests, red team, phishing and source code audits: web, internal, cloud (200+ hosts, 1600+ domains)
- Configuration audits and hardening: Linux, Windows, Okta, GitHub, GitLab, Kubernetes, AWS, GCP, Microsoft 365
- Built internal tools used daily: pentest report converter, BloodHound and AADInternals forks

**Freelance Software Engineer**, Adrenalyse — 2021

- Trading application in Go (event sourcing, gRPC, PostgreSQL), deployed on GCP

## EDUCATION

Diplôme d'Ingénieur (MSc. in Engineering), Grenoble-INP ENSIMAG — 2019-2022

Master of Science in Cybersecurity, Grenoble-INP UGA — 2021-2022

## KEY SKILLS

- Application security: threat modeling, code review, pentest
- SSDLC and DevSecOps (SAST, DAST, SCA, secrets)
- Vulnerability management and risk-based prioritisation
- Software supply chain security (SBOM, SLSA, signing)
- Cloud, Kubernetes and CI/CD security (AWS)
- IAM and federation (OAuth, SAML, Keycloak)
- Applied cryptography
- Compliance: PCI-DSS, SOC 2, CRA
- Mentoring and security awareness

## TOOLS

**Security**
Burp Suite, SonarQube, Wiz
Trivy, Grype, cosign, TruffleHog

**Cloud and infrastructure**
AWS, GCP, Kubernetes, Terraform
GitLab CI, Docker, Vault

**Programming**
Python, Go, Kotlin/Java, TypeScript
C, Bash, PowerShell

## LANGUAGES

**French**
Native proficiency

**English**
Professional working proficiency (C1), TOEIC 950/990

## INTERESTS

Reading, music (guitar, piano), archery, judo, snowboarding, climbing.