Ricardo Nahuel Prieto

AI SECURITY ENGINEER

CONTACT

San Carlos de Bariloche, Argentina
Open to Relocation & Remote
philocyber.com
linkedin.com/in/richieprieto

CORE EXPERTISE

AI & GenAI Security
LLM Threat Modeling, Multi-Agent Systems, MCP Security, RAG Pipeline Security, OWASP Top 10 for LLMs / Agentic Applications / MCPs & Skills, NIST AI RMF, MITRE ATLAS

Application Security
Web App & API Pentesting, SAST/DAST/SCA, CI/CD Security, Vulnerability Triage, Code Review

Security Management
Security Champions Programs, Cross-functional Collaboration, Technical Training, Risk Assessment

TOOLS & FRAMEWORKS

MITRE ATT&CK, MITRE ATLAS, OWASP ASVS, ISO 27001, NIST CSF, Burp Suite, HackerOne, Qualys, Nessus, Python, SQL

CERTIFICATIONS

Certified AI Security Professional (CAISP)
Practical DevSecOps

Trusted AI Safety Expert (TAISE)
Cloud Security Alliance

HTB Certified Bug Bounty Hunter (cBBH)
Hack The Box & HackerOne

eWPT / eJPT
eLearnSecurity

CCSK
Cloud Security Alliance

C-AI/MLPen
Certified AI/ML Pentester

HTB Certified Offensive AI Expert (COAE)
Hack The Box · In Progress

LANGUAGES

Spanish — Native
English — Professional

EDUCATION

M.S. Information Security
University of Buenos Aires (UBA)
Expected Dec 2026

Diploma Computer Security
National Tech University (UTN)
Completed 2020

PROFESSIONAL SUMMARY

AI Security Engineer and Senior AppSec leader with 7+ years securing enterprise-grade applications, AI/ML systems, and complex infrastructures. Currently leading organization-wide AI Security programs — threat modeling LLM pipelines, securing multi-agent systems and MCP implementations, and establishing AI Security Baselines aligned with OWASP LLM Top 10, NIST AI RMF, and MITRE ATLAS.

Specialized at the intersection of offensive security and AI/GenAI security, with hands-on red team and blue team experience spanning Fortune 500 companies, international pentesting consultancy, and global cybersecurity community leadership.

PROFESSIONAL EXPERIENCE

Senior AI Security Engineer
Jul 2026 – Present
CookUnity
Remote, USA

- Hired to build and lead the AI Security practice from the ground up, securing GenAI-powered products across the platform
- Own end-to-end threat modeling for LLM pipelines, agentic systems, and MCP integrations, aligned with OWASP Top 10 for LLMs, NIST AI RMF, and MITRE ATLAS
- Partner with engineering and data teams to embed AI security guardrails and secure-by-design practices across the SDLC

itti
Jun 2025 – Jul 2026
Remote, Argentina

Senior AI Security Engineer
Oct 2025 – Jul 2026

Led the organization's end-to-end AI Security function and served as the focal point for all AI Security matters within Cybersecurity, securing GenAI-powered products and internal AI tooling.

- Threat modeled Generative AI applications end-to-end: mapped attack surfaces across LLM pipelines, prompt injection vectors, data leakage risks
- Established org-wide AI Security Baseline aligned with OWASP Top 10 for LLMs, NIST AI RMF, and MITRE ATLAS
- Defined guardrails and trust boundaries for multi-agent systems and MCP implementations
- Conducted security reviews of AI platform configurations including Kore.ai and AWS Bedrock

Senior Application Security Engineer
Jun 2025 – Oct 2025

- Program Owner of Security Champions program — designed security culture initiative embedding threat-aware practices org-wide
- Served as AppSec focal point for org's AI security strategy, initiating groundwork for GenAI threat modeling
- Integrated SAST, DAST, and SCA tools into CI/CD pipelines to shift security left

Cybersecurity Tutor
Feb 2025 – Present
TripleTen
Remote, USA

- Delivered specialized offensive security mentorship to 50+ students through live sessions
- Reduced student time-to-competency by 35% through customized 1-on-1 learning paths
- Achieved 4.9/5 instructor rating based on student feedback

Co-Founder & Ambassador
May 2024 – Present
Hack The Box (HTB)
Argentina & New Zealand

- Founded HTB's New Zealand meetup and later joined the Argentina chapter as an organizer, helping grow the communities to 200+ practitioners
- Negotiated partnerships with 8 institutions to secure 100% free event spaces, reducing costs by $12,000 annually
- Led cross-regional team coordination managing 12 volunteer organizers, increasing member retention by 45%

Senior Penetration Tester & Security Consultant
Jun 2023 – Dec 2024
Bastion Security Group
Wellington, New Zealand

- Delivered 40+ penetration testing engagements and security assessments/configuration reviews across web apps, APIs, cloud infrastructure, and networks
- Identified and documented 250+ vulnerabilities with actionable remediation strategies
- Primary technical point of contact for enterprise clients — maintained 95% client satisfaction rate
- Contributed to 15+ successful proposal wins valued at $500K+

Ricardo Nahuel Prieto

AI SECURITY ENGINEER

CONTACT

San Carlos de Bariloche, Argentina
Open to Relocation & Remote
philocyber.com
linkedin.com/in/richieprieto

CORE EXPERTISE

AI & GenAI Security
LLM Threat Modeling, Multi-Agent Systems, MCP Security, RAG Pipeline Security, OWASP Top 10 for LLMs / Agentic Applications / MCPs & Skills, NIST AI RMF, MITRE ATLAS

Application Security
Web App & API Pentesting, SAST/DAST/SCA, CI/CD Security, Vulnerability Triage, Code Review

Security Management
Security Champions Programs, Cross-functional Collaboration, Technical Training, Risk Assessment

TOOLS & FRAMEWORKS

MITRE ATT&CK, MITRE ATLAS, OWASP ASVS, ISO 27001, NIST CSF, Burp Suite, HackerOne, Qualys, Nessus, Python, SQL

CERTIFICATIONS

Certified AI Security Professional (CAISP)
Practical DevSecOps

Trusted AI Safety Expert (TAISE)
Cloud Security Alliance

HTB Certified Bug Bounty Hunter (cBBH)
Hack The Box & HackerOne

eWPT / eJPT
eLearnSecurity

CCSK
Cloud Security Alliance

C-AI/MLPen
Certified AI/ML Pentester

HTB Certified Offensive AI Expert (COAE)
Hack The Box · In Progress

LANGUAGES

Spanish — Native
English — Professional

EDUCATION

M.S. Information Security
University of Buenos Aires (UBA)
Expected Dec 2026

Diploma Computer Security
National Tech University (UTN)
Completed 2020

Cybersecurity Engineer
Sep 2022 – Apr 2023
Mercado Libre (MELI)
Buenos Aires, Argentina

- Led comprehensive vulnerability management program coordinating remediation across 15 development teams and 200+ applications
- Managed enterprise-scale vulnerability prioritization integrating HackerOne bug bounty and internal red team findings
- Automated security dependency scanning using Python and SQL, improving detection coverage by 40%
- Created security training for 100+ developers, reducing recurring vulnerability patterns by 25%

Cybersecurity Researcher
Dec 2020 – Sep 2022
Onapsis
Buenos Aires, Argentina

- Executed 30+ vulnerability assessments for top-tier North American clients
- Performed SAST/DAST code reviews identifying 150+ security flaws
- Delivered bilingual security reporting to C-level executives across Canada, Argentina, and US markets

Offensive Security Analyst
Dec 2019 – Dec 2020
Deloitte
Buenos Aires, Argentina

- Engineered security validation framework for enterprise SaaS platforms using Python automation
- Developed 15+ security modules preventing 200+ potential authorization vulnerabilities
- Delivered 20+ training sessions as internal subject matter expert

THOUGHT LEADERSHIP

Founder & Content Creator
philocyber.com
PhiloCyber
Active platform focused on AI/LLM security, RAG systems, and offensive security research.

- Published 25+ technical articles on AI/LLM security and penetration testing methodologies
- YouTube channel producing educational content on CVE breakdowns and security assessment techniques
- Established digital knowledge hub serving 2,000+ monthly visitors

ADDITIONAL INFORMATION

- **Conference Participation:** Active volunteer at Ekoparty Security Conference (2019, 2020, 2022) and CHcon Christchurch Security Conference (2023)
- **Community Service:** Volunteer at SPCA (canine department, animal shelter care)
- **Speaking Goal 2025:** Technical presentation on LLM security or AI threat modeling at a major security conference

KEY DIFFERENTIATORS

- **Unique expertise intersection:** offensive security + AI/ML security + security program management
- **Proven scale impact:** from individual assessments to enterprise vulnerability programs
- **International experience:** Argentina, New Zealand, remote US markets with bilingual capability
- **Community leadership:** built a 200+ member security community from zero across two countries
- **Continuous learning:** 7 active certifications (incl. AI-specific CAISP & TAISE), HTB COAE and Master's in progress, publishing technical content regularly

PROFESSIONAL REFERENCES

Available upon request. References include security leadership from: itti (AI Security & AppSec roles), TripleTen (Cybersecurity Education), Hack The Box (Community Leadership), Bastion Security Group (Pentesting Consultancy), Mercado Libre (Enterprise Security), Onapsis (Security Research), Deloitte (Offensive Security).