Alexandru Cochirleanu

Secure AI Automation & Cybersecurity Architect

AI Systems Architect | Methodology Architect | Prompt Engineer | Information Security Advisor | Senior Penetration Tester

Bucharest, Romania | International & online engagements	**https://www.linkedin.com/in/alexcochirleanu/**
	mindsteep.com | coevolve.ro | academianlp.org

20+ years in IT and security	**10+** years in penetration testing	**6** methodologies and AI agents	**6+** industries served

Executive Profile

Alexandru Cochirleanu is a cybersecurity and secure AI automation specialist with more than two decades of experience across IT administration, information security, ISO 27001 audit, penetration testing, GDPR/DPO advisory, security operations and enterprise-grade AI implementation. His professional work connects adversarial security thinking, technical assessment, governance, LLM orchestration, RAG systems and AI-enabled development methodologies.

He has held senior cybersecurity roles across online gaming, telecom, retail, oil and gas, IT outsourcing and technology environments, delivering web application penetration testing, vulnerability assessment, infrastructure security review, compliance preparation, remediation reporting and technical security advisory. His background includes hands-on work with OWASP methodology, Kali Linux, Metasploit, Burp Suite Pro, vulnerability scanners, SIEM implementation and security-awareness programmes.

Since 2024, his work has expanded into the architecture and implementation of AI-enabled profiling, leadership development, sales development and adaptive coaching systems within the MindSteep and CoEvolve ecosystem. He contributes as Methodology Architect and AI Implementation Lead to commercially usable MVP products and functional AI agents that combine assessment logic, scoring, development methodology, prompt engineering, AI orchestration and human-AI collaboration.

Authority Platform

- Cybersecurity assessment, penetration testing, vulnerability validation and remediation advisory
- Enterprise AI agents, LLM orchestration, RAG systems, prompt engineering and AI FinOps
- AI security, guardrails, prompt-injection resilience and controlled tool/API interaction

- Methodology architecture for profiling, leadership, transformation, coaching and sales development
- Information security governance, ISO 27001, PCI-DSS readiness, GDPR technical assessment and DPO support
- Human-vulnerability resilience, cybersecurity awareness and human-AI collaboration systems

Professional Leadership Experience

GLI Bulletproof Europe | 2019-Present

Senior Penetration Tester

- Delivers web application penetration testing using OWASP methodology, OWASP Top 10 and OWASP Testing Guide 4.1.
- Conducts vulnerability assessment and validation through manual testing and practical attack techniques.
- Creates jurisdictional-specific assessment reports, presents discovered issues to customers and provides remediation methods.
- Reviews and validates penetration testing reports prepared by colleagues.
- Performs web and infrastructure security assessments using open-source and commercial security tools.

MindSteep Consulting & Training / CoEvolve Research Ecosystem | 2024-Present

CTO / Methodology Architect & AI Implementation Lead

- Contributes to AI-enabled profiling, transformation analysis, leadership development and coaching methodologies researched through Asociația CoEvolve.
- Implements functional AI agents and MVP/commercial products based on assessment, scoring and development frameworks.
- Architects prompt systems, conversational flows and controlled AI interactions for human-development and business-use cases.
- Works within an intellectual-property framework held by Alexandru Cochirleanu, Ovidiu Panea, Monica Panea and MindSteep Consulting & Training.

Penetration Testing Freelancer and Security Consultant | 2016-Present

Security Consultant

- Provides web application penetration testing, vulnerability assessment, reporting and customer-facing remediation explanations.
- Advises on secure implementation of new systems and infrastructure.
- Provides GDPR consultancy, IT gap analysis in the GDPR context and DPO support for several companies.

T-Mobile Czech Republic | 2018-2019

Senior Penetration Tester

- Performed web application penetration testing and vulnerability validation using OWASP methodology.
- Presented findings and remediation methods to customers and reviewed colleagues' penetration testing reports.

- Replicated adversarial vantage points for external and internal information systems, identifying high-risk vulnerabilities and attack vectors.

Startech Team | 2018

Security Operations Center Manager

- Managed a team of security practitioners and experts.
- Developed SIEM capability and security concepts including log management, firewall centralised management, antivirus management and update management.
- Supported ISO 27001 compliance audit and maintenance of company certification.

Earlier Security, Audit & IT Infrastructure Roles

Mega Image, Ahold Delhaize Group | 2016
Information Security Officer. PCI-DSS and ISO 27001 preparation, internal audits, web application penetration testing, compliance and technical audit, policy review, vulnerability management and information-security awareness.

Safetech Innovations | 2015
Web Application Penetration Tester. Customer penetration testing, OWASP-based assessment, vulnerability scanning, third-party ISO 27001 audit support, firewall and IDS/IPS log review and incident reporting.

OMV Petrom | 2013-2015
Information Security Officer. Internal ISO 27001 audit, PCI-DSS preparation, third-party audit, penetration-test coordination, vulnerability scans, policy review and employee awareness campaigns.

IBM Systems & Technology Group | 2013
IT Security Specialist. Implementation of IBM ITCS104 security standard, user awareness, access safeguards, virus-protection monitoring, KCO reviews and ITCS104-related security audits.

Class IT Outsourcing | 2010-2012
ISO 27001 IT Audit | CISO. Internal and external IT audit, security reporting to top management, ISO 27001 documentation, security policies, vulnerability management, penetration testing, patch management and incident management.

ClassIT Outsourcing | 2009-2010
Project Manager | Security Officer. Security policies for new customers, update management, antivirus, backups, vulnerability assessment, employee training and infrastructure improvement.

S.C. Brenntag S.R.L. | 2007-2009
Senior IT System Administrator. Active Directory, firewall, web filtering, shared resources, WSUS, backup supervision, patching and country-branch support.

S.C. MaxiNet S.R.L. | 2003-2007
IT System Administrator. Technical support, hardware and software maintenance, IT infrastructure updates and security-policy application.

Selected Strategic & Technical Domains

- OWASP-based web application penetration testing and customer-facing remediation reporting
- External and internal vulnerability assessment across enterprise infrastructure and internet-facing systems

- ISO 27001, PCI-DSS and GDPR-related technical security assessment and compliance preparation
- SIEM implementation, log-management concepts and security operations coordination
- Human-risk, security awareness and AI-enabled cybersecurity resilience

AI Systems, RAG & Multi-Agent Automation

Alexandru's AI work focuses on secure enterprise automation, multi-agent orchestration, retrieval-augmented generation, prompt engineering, AI cost optimisation and controlled LLM interaction with internal systems. The profile below reflects directly declared AI work and should be supported, when required, by project documentation, demos, technical briefs or client-approved descriptions.

Senior AI Specialist Profile

Senior AI specialist with deep expertise in designing and implementing autonomous agents and enterprise RAG systems. Experienced in orchestrating leading language models across OpenAI, Anthropic Claude and Google Gemini environments, with emphasis on secure API interaction, FinOps, scalable business-process automation and guarded enterprise deployment.

Declared AI Implementation Results

- Designed and implemented a multi-agent architecture using CrewAI and LangGraph for technical-support and sales workflows, reducing response time by 70%.
- Orchestrated Claude 3.5 Sonnet and GPT-4o through advanced function-calling techniques, enabling agents to interact securely with internal APIs and SQL databases.
- Implemented prompt caching and dynamic model-routing strategies, including Gemini Flash for simpler tasks, reducing monthly OpenAI/Anthropic API costs by 42%.
- Developed an advanced RAG system with metadata filtering and Cohere reranking, increasing AI answer accuracy from 65% to 94% and reducing hallucinations on internal enterprise documents.
- Created, tested and versioned more than 150 complex system prompts in Google AI Studio and OpenAI Playground for content generation and financial analysis.
- Used LangSmith for performance monitoring, prompt A/B testing, output-quality evaluation and latency reduction by 30%.

AI Tech Stack

LLMs & APIs	OpenAI GPT-4o, Assistants API; Anthropic Claude 3.5 Sonnet; XML tag optimisation; Google Gemini 1.5/2.0 Pro/Flash; Vertex AI
Agent Orchestration	CrewAI, LangGraph, LangChain, Microsoft AutoGen
Prompt Engineering	Chain-of-Thought, Tree of Thoughts, few-shot learning, dynamic context caching, function calling and tool use
Vector Databases & RAG	Pinecone, ChromaDB, PGVector, hybrid search, metadata filtering, Cohere reranking
Languages & Tooling	Python, Asyncio, FastAPI, TypeScript, JSON Schema, Git, Docker, CI/CD
AI Security & Monitoring	NVIDIA NeMo Guardrails, LangSmith, Promptflow, LlamaGuard, prompt-injection and jailbreaking defence

Methodology Architecture, Profiling & Human-AI Development

Within MindSteep Consulting & Training and the CoEvolve research ecosystem, Alexandru contributes as Methodology Architect and AI Implementation Lead to a portfolio of AI-enabled profiling, evaluation, coaching and development systems. The related intellectual property is held by Alexandru Cochirleanu, Ovidiu Panea, Monica Panea and MindSteep Consulting & Training, with research developed through Asociația CoEvolve.

Co-Authored / Co-Developed Methodology Areas

MindSteep Profiling. Mindset patterns, internal drivers, motivations, interests, attitudes and values.

Leadership Profiling. Leadership potential and performance across approximately 100 leadership competencies.

Transformation Analysis. Wants, needs, challenges and transformation priorities forming the basis of a focused coaching plan.

Cybersecurity Awareness and Human-Vulnerability Resilience. Human-risk, behaviour, awareness and resilience patterns connected to security posture and social-engineering exposure.

Human-AI Collaboration, Prompt Engineering and Adaptive Coaching. Human-AI working models, prompt systems and AI-assisted development flows for coaching and professional learning.

AI Agent Portfolio

The Frontline Management Agent | 2024-2026

Evaluation, scoring and development methodology implemented as a functional AI agent; MVP internal system and commercial product.

57 Leadership Skills Agent | 2024-2026

Leadership competency evaluation and development methodology implemented as a functional AI agent; MVP internal system and commercial product.

Effective Sales Agent | 2024-2026

Sales evaluation, development and coaching methodology implemented as a functional AI agent; MVP internal system and commercial product.

Programme Portfolio Areas

- Leadership, frontline management, sales capability and professional-development assessment
- Transformation analysis, adaptive coaching plans and human-performance development
- Cybersecurity awareness, human-vulnerability resilience and social-engineering risk reduction
- Human-AI collaboration, prompt engineering, AI-enabled coaching and professional learning

Cybersecurity, Penetration Testing & Security Governance

Alexandru's cybersecurity authority is grounded in a career that moved from system administration and IT infrastructure into ISO 27001 audit, information security governance, penetration testing, security operations and GDPR/DPO consultancy. This gives his AI work a distinctive security-informed foundation: automation is treated not only as a productivity layer, but as a system requiring controlled access, adversarial testing, monitoring and risk-aware deployment.

Core Cybersecurity Capabilities

- Web application penetration testing using OWASP Top 10 and OWASP Testing Guide methodology
- Manual vulnerability validation, attack-vector identification and exploitation-oriented assessment
- Infrastructure security assessment using vulnerability scanners, web application scanners, intercepting proxies, enumeration tools and exploitation frameworks
- Customer-facing reports with discovered issues, technical risk explanation and remediation methods
- Review and validation of penetration-testing reports produced by other consultants
- ISO 27001, PCI-DSS and GDPR/DPO-related security assessment, audit preparation and technical gap analysis
- Security-awareness programmes, human-vulnerability resilience and responsible AI/security education

Security Tooling & Technical Environments

Nessus, Qualys, Nexpose, OpenVAS, Burp Suite Pro, Netsparker, Acunetix, W3AF, OWASP ZAP, Websploit, Metasploit, Cobalt, Dradis, Maltego CaseFile, PlexTrac, Kali Linux, Nikto2, Wireshark, Nmap, SQLMap, Hydra, John the Ripper, Hashcat, testssl, wfuzz, curl, Fortigate, Blue Coat, Windows Server, Active Directory, WSUS, Linux distributions, Apache, IIS, FTP/SFTP and mail-server environments.

Education, Certifications & Professional Development

Bachelor in Orthodox Theology
Orthodox Theological Institute, Pastoral Section, University of Bucharest | 2003-2007

Theological Seminary
Bucharest | 1998-2003

Courses, Certifications & Training

- CEH v.11 Certification (ECC5087124639) | 2022
- DPO Certification | 2019, Bucharest
- GDPR Training | 2018, Bucharest
- CISSP Bootcamp, New Horizons | 2014, Bucharest
- Transition from ISO 27001:2005 to ISO 27001:2013, Rina Simtex | 2013, Bucharest
- Microsoft Sales Specialist for Medium Organizations | 2011, Bucharest
- Training of external auditors for Information Security Management System by ISO 2700:2006 and ISO 19001:2003 standards | 2011, Bucharest
- CISSP Review Seminar | May 2010, Bucharest
- ISACA Member; CISA Training | 2010, Bucharest
- Administration of Linux Servers | 2009, Bucharest
- Lotus Notes Training | 2008, Bucharest
- Networking Training, Genesys Computers | 2004, Bucharest

Languages

Romanian - Native | English - Advanced | French - Medium reading/writing, beginner spoken

Specialist Capabilities

Cybersecurity. Penetration testing, vulnerability assessment, web and infrastructure security, OWASP, SIEM concepts, incident reporting, remediation advisory, ISO 27001, PCI-DSS and GDPR technical security review.

AI Engineering. LLM orchestration, agent frameworks, RAG architecture, vector databases, prompt engineering, function calling, model routing, prompt caching, AI monitoring and evaluation.

Governance & Human Risk. Information-security policy, audit readiness, awareness programmes, human-vulnerability resilience, DPO support and cybersecurity behaviour design.

Technology Foundation. Python, TypeScript, FastAPI, Docker, CI/CD, Linux, Windows Server, Active Directory, networking protocols, firewalls, VPN, web servers and enterprise IT operations.

Evidence & Attribution Note

The career chronology, education, certifications and cybersecurity responsibilities are drawn from Alexandru Cochirleanu's supplied CV. AI implementation results, MindSteep/CoEvolve methodology roles, co-author attribution and product status are based on direct information supplied for this Master Authority CV. Client names and project details should be disclosed only where permission exists.

Personal Information

Base: Bucharest, Romania | Available for projects across Romania, international travel and online delivery

Professional Positioning

Alexandru Cochirleanu works at the intersection of cybersecurity, penetration testing, information security governance, enterprise AI implementation, prompt engineering, RAG systems, human-risk resilience and AI-enabled professional development. His professional portfolio is designed for corporate cybersecurity engagements, secure AI automation, AI agent implementation, methodology licensing, commercial AI products, conference contribution and strategic partnerships.