Dr. Jan Kalbantner

Bridging Technical Risk & Business Strategy

Email me | kalbantner.com | linkedin.com/in/jankalbantner

Professional Summary

Technical Leader with over a dozen years of experience bridging digital-native AI innovations with traditional enterprise needs in highly regulated industries (FSI, Automotive, Critical Infrastructure). Passionate about deploying reliable, interpretable and societally beneficial systems. Expert at leading pre-sales & post-sales technical teams, co-building Go-To-Market strategies and scoping complex enterprise AI and security architectures. Proven track record of navigating complex organizational structures to validate technical ROI, build C-suite consensus and drive commercial growth globally.

Core Competencies

- Secure AI & Cloud Architecture: Deep technical proficiency in AI security, cloud security, application security and bridging modern API integrations with stringent enterprise compliance standards.
- Pre-Sales Leadership & GTM Strategy: Co-building GTM strategies, managing technical pre-sales teams, and owning the technical execution of enterprise deals (including use case scoping, technical adoption workshops, and POC execution).
- Regulated Industry Expertise: Navigating complex technical and regulatory requirements (GDPR, ISO 27001, NIS2, TISAX, EBA) to build trust and drive AI transformation within large enterprises.
- Commercial & Financial Stewardship: Directing multi-million-euro budgets and securing over EUR 5 M in strategic contracts through expert business development and value-based solutioning.

Professional Experience

Senior Manager, Capgemini Invent

Stuttgart, Germany | Hybrid
September 2025 - Present

- Serves as a high-level strategic advisor to C-suite executives, architecting comprehensive cybersecurity transformations and resilient global strategies for DAX and MDAX organizations across diverse industries (retail, manufacturing, automobile, software).
- Accomplished technology adoption and scalable architectures for DAX organizations, as measured by securing multi-million-euro enterprise contracts, by acting as a cybersecurity leader to co-build Go-To-Market strategies, execute Proof of Concepts, and lead multidisciplinary technical advisory teams.
- Drives significant business development and commercial growth, securing multiple cybersecurity consulting contracts through expert stakeholder management and value-driven solutioning.
- Spearheads the strategic development of the cybersecurity service portfolio, defining market-leading offerings that address emerging threats and regulatory shifts.

Senior Manager Information Security, Porsche

Stuttgart, Germany | Hybrid
June 2024 - August 2025

- Orchestrated a comprehensive global security transformation that reduced enterprise-wide incidents by 30% through the strategic deployment of Zero Trust, DevSecOps, and cloud-native defense architectures.
- Steered a €1.7M strategic budget and cross-functional team to drive a 20% gain in operational efficiency by pioneering AI/ML, advanced cryptography, and OT security initiatives.
- Architected a global Information Security Service Delivery model that optimized incident response times by 50% while maintaining 99.99% availability for mission-critical international operations.
- Advanced corporate governance by aligning global security policies with TISAX, ISO 27001, and NIS2 standards, resulting in a 15% increase in measurable compliance maturity.

Domain Leader & Cyber Security Manager, KPMG Ignition Tokyo

Tokyo, Japan | Hybrid
September 2023 - May 2024

- Acted as a technical leader to elevate the organizational risk posture and ISO 27001:2022 compliance maturity by 25% across global operations.

- Enhanced operational resilience and incident resolution efficiency by 20% through the strategic design and implementation of automated security orchestration workflows.
- Engineered and integrated automated security orchestration workflows (SIEM/SOAR via Microsoft Sentinel), demonstrating deep technical proficiency with complex enterprise API integrations.
- Spearheaded the development and governance of inaugural corporate policies for Artificial Intelligence (AI), establishing foundational frameworks for safe and compliant enterprise AI use cases.

Cloud Architecture & Cyber Security Lead, Wechselgott

London, UK | Hybrid
October 2019 - August 2023

- Built and led the Cloud and Cybersecurity team in a fast-paced B2B startup environment, architecting and securing the foundational multi-cloud infrastructure (AWS, Azure, Kubernetes) from the ground up to ensure 99.9% reliability.
- Spearheaded B2B pre-sales initiatives, developing technical concepts and architectural solutions that translated complex product capabilities into compelling enterprise value propositions, directly contributing to a 50% year-over-year expansion of the global customer base.
- Bridged digital-native agility with enterprise compliance, directing a risk strategy that achieved 100% regulatory alignment (ISO 27001, NIST) to build technical trust and overcome procurement hurdles with highly regulated enterprise prospects.
- Institutionalized a "Secure-by-Design" engineering culture, acting as the technical champion to integrate DevSecOps orchestrations that reduced production vulnerabilities by 40%.

Lead IT Consultant, K13 Solutions (Self-Employed)

Heidelberg, Germany | Remote
May 2015 - June 2020

- Owned the end-to-end technical sales cycle as an independent consultant, successfully driving engagements from initial outbound prospecting and pre-sales scoping through to the final technical execution and delivery of the project.
- Acted as the lead Cloud and Solutions Architect to design and supervise 5 major enterprise software development projects (web and mobile applications using TypeScript, C#, .NET), ensuring tight alignment with customer business needs.
- Served as a trusted technical advisor in the highly regulated financial as well as manufacturing sectors, conducting over 50 security audits to ensure 100% compliance with stringent EBA guidelines, BSI 200 and ISO 27001 standards.

IT Application Consultant, Bürkert Fluid Control Systems

Ingelfingen, Germany | On-Site
June 2013 - September 2017

- Led internal stakeholder management and enterprise change management initiatives, bridging the gap between technical development teams and non-technical business units to drive successful digital transformation within a traditional manufacturing environment.
- Designed and implemented Target Operating Models (TOM) to optimize internal software development lifecycles, establishing scalable frameworks and repeatable processes that fostered cross-functional collaboration.
- Directed internal full-stack software development projects (JavaScript, Java, PHP), ensuring that technical architectures and applications were tightly aligned with evolving business needs, operational workflows, and overarching organizational goals.

Education

Executive MBA (EMBA) in Business and IT (Ongoing)

Technical University Munich (TUM), Germany

- Focus: "Leadership & Cooperation"

Doctor of Philosophy (PhD) in Information Security

Royal Holloway University of London, United Kingdom

- Focus: Applied Cybersecurity and Data Privacy, Critical Infrastructure

Master of Science (MSc) in Information Security

Royal Holloway University of London, United Kingdom

- Focus: Cybersecurity, Applied Information Security, Research

Advanced Postgraduate Coursework: AI & Big Data

University of Heidelberg, Germany

- Completed specialized Master's level modules in Artificial Intelligence and Big Data as part of the Applied Computer Science MSc program to deepen technical expertise in frontier technologies.

Bachelor of Science in Applied Computer Science

DHBW Mosbach, Germany

- Focus: Software engineering, Applied Technologies

Technical Skills

- Applied AI & LLM Expertise: Prompt Engineering, LLM Evaluation, Enterprise AI Deployments, API Integrations, Production LLM Use Cases, AI System Architecture, Natural Language Processing (NLP), Deep Learning, Model Benchmarking, Conversational Applications.
- AI Safety & Governance: AI Security, Steerable & Interpretable AI, AI Corporate Policies, Trustworthy AI Systems, AI Risk Management.
- AI Ecosystems & Models: Claude (Enterprise, Code, API), Google Vertex AI / Gemini, OpenAI, Kimi, Mistral.
- Cloud Platforms: AWS, Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud
- Security Expertise: Identity Access Management (IAM), Privileged Access Management (PAM), Microsoft Defender for Cloud, AWS GuardDuty, Zero Trust
- Tools: Kubernetes, Docker, Terraform, Pulumi, Microsoft Azure Blueprints
- Security Tools: SAST/DAST (Snyk, SonarQube, SonarCloud), SIEM/SOAR (QRadar, Sentinel, Splunk, Chronicle), Palo Alto (NGFW, CASB, DLP, Prisma Cloud), Trellix, CyberArk, Tenable, Nessus, Aqua Security
- Standards & Regulations: ISO 270XX, ISO 4200X GDPR, OWASP Top 10, BSI 200-1/2/3/4, NIST 800-53 Rev. 5, EBA, DORA, NIS2, TISAX, CRA

Programming Languages

- Backend: C#, Python, R
- Frontend: JavaScript, TypeScript
- Mobile Development: Kotlin, Java, Swift
- Scripting and Query Languages: PowerShell, SQL, KQL (Kusto Query Language)
- Frameworks and Libraries: .NET, Tensorflow, PyTorch, Scikit-Learn, Keras, CNTK, Apache Spark, Pandas

Certifications

- University of Maryland (UMD), Fundamentals of Technology Sales - 2026 - Link
- Anthropic, Claude 101 - Link
- Anthropic, AI Fluency: Framework and Foundations - 2026 - Link
- Anthropic, Introduction to Model Context Protocol - 2026 - Link

- Google, AI Professional Certificate - 2026 - Link
- IBM, ETL and Data Pipelines with Shell, Airflow and Kafka - 2025 - Link
- Technical University Munich (TUM), EMBA, Leadership and Cooperation - 2025 - On Request
- Offensive Security, Certified Professional (OSCP) Course – 2024 - On Request
- Rochester Institute of Technology (RITx), Computer Forensics - 2024 - Link
- IBM, Generative AI for Cybersecurity Certificate – 2024 - Link
- IBM, Penetration Testing and Incident Response Certificate - 2024 - Link
- IBM, DevOps and Software Engineering Certificate - 2023 - Link
- IBM, Applied DevOps Engineering Certificate - 2023 - Link
- Microsoft, Cybersecurity Analyst – 2023 - On Request
- Google, Cybersecurity Certificate – 2023 - Link
- IBM, Security Analyst Fundamentals Certificate - 2023 - Link
- IBM, Cybersecurity Analyst Certificate - 2023 - Link
- Google, Project Management Certificate - Scrum/agile project management - 2022 - Link
- TÜV SÜD, DSGVO / GDPR Specialist Certificate – 2021 - On Request
- Certified Information Systems Security Professional (CISSP) Course - On Request
- Certified Information Security Manager (CISM) Course - On Request
- More certificates can be found here: https://www.credly.com/users/jan-kalbantner

Publications

- Kalbantner (2024) *Security and Privacy Issues of Distributed, Complex P2P Smart Grid Marketplace Systems.* PhD thesis. Available at: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/63153877/main.pdf.
- Kalbantner et al. (2024) *ZKP Enabled Identity and Reputation Verification in P2P Marketplaces.* Available at: https://ieeexplore.ieee.org/abstract/document/10664332.
- Shepherd, Kalbantner, Semal, Markantonakis (2023) *A Side-Channel Analysis of Sensor Multiplexing for Covert Channels and Application Profiling on Mobile Devices.* Available at: https://ieeexplore.ieee.org/abstract/document/10278225.
- Kalbantner et al. (2021) *A DLT-based Smart Contract Architecture for Atomic and Scalable Trading.* Available at: https://arxiv.org/abs/2105.02937.
- Kalbantner et al. (2021) *P2PEdge: A Decentralized, Scalable P2P Architecture for Energy Trading in Real-Time.* Available at: https://www.mdpi.com/1996-1073/14/3/606.
- Semal, Markantonakis, Akram, Kalbantner (2020) *A study on microarchitectural covert channel vulnerabilities in infrastructure-as-a-service.* Available at: https://link.springer.com/chapter/10.1007/978-3-030-61638-0_20.
- Semal, Markantonakis, Mayes, Kalbantner (2020) *One covert channel to rule them all: A practical approach to data exfiltration in the cloud.* Available at: https://ieeexplore.ieee.org/abstract/document/9343152.
- Semal, Markantonakis, Akram, Kalbantner (2020) *Leaky Controller: Cross-VM Memory Controller Covert Channel on Multi-Core Systems.* Available at: https://link.springer.

com/chapter/10.1007/978-3-030-58201-2_1.

- Kalbantner (2020) *Rowhammer – from DRAM faults to escalating privileges.* Available at: https://www.computerweekly.com/ehandbook/Royal-Holloway-Rowhammer-from-DRAM-faults-to-escalating-privileges.
- Kalbantner (2018) *Software-based Microarchitectural Fault Attack.* MSc thesis. Available at: https://www.royalholloway.ac.uk/media/14911/techreport-kalbantnerj.pdf.
- Also available on: Google Scholar

Languages

- German (Fluent)
- English (Fluent)
- French (Basic)
- Japanese (Basic)