



AI AND AUTOMATION

Agentic AI: Opportunity and Attack Surface

DURATION

1 day

AUDIENCE

Board, Managers

LANGUAGE

Polish or English

FORMAT

On site or online

AI agents act on their own, which changes both the upside and the attack surface. This training shows how to prepare an organisation for the agentic era: trust architecture, control over agent actions, new risk vectors. Builds on my talk at Commerzbank Connect Tech.

WHAT WE COVER

- From chatbots to agents: what changes when AI acts instead of answering
- Where agents pay off first: realistic use cases in operations, service and back office
- Trust architecture: permissions, boundaries and human checkpoints for autonomous systems
- The new attack surface: prompt injection, data exfiltration and agents as insider risk
- Controls that work: logging, limits and kill switches without killing the benefit
- A readiness roadmap: what to pilot, what to postpone and what to decide now

YOU LEAVE WITH

- A readiness assessment for your organisation: where agents fit and where they do not yet
- A control checklist for any agent pilot, from permissions to monitoring
- A decision framework for the board: pace, guardrails and ownership

WHO IT IS FOR

Board members, senior managers, and leaders of IT, security and operations who will own agent deployments. Also works as a joint session for business and IT leadership.



BOOK THIS TRAINING

Write to michal.krauze@krauzeadvisory.com with the subject "Training: Agentic AI: Opportunity and Attack Surface". Add preferred dates and group size. Closed programs are tailored to your organisation.