kod szkolenia: GH-600 / ENG DL 1d

Developing in Agentic AI Systems

The training covers key issues related to developing, deploying, and managing agentic AI systems within GitHub-based software development workflows.

Training recipients

The training is designed for:

- Architects who design and oversee the implementation of AI-driven development systems and need to integrate agentic AI into enterprise software development workflows.
- Platform Engineers and DevOps Engineers who manage development infrastructure, automation pipelines, and CI/CD workflows, and want to incorporate AI agents into their operational practices.
- Application Developers who build and maintain software applications and seek to leverage AI agents to enhance productivity and code quality.
- Product Managers who oversee software development processes and need to understand how AI agents can be integrated into product development lifecycles.
- Security Engineers responsible for ensuring compliance, security, and governance in AI-enhanced development environments.
- Those preparing for GitHub Agentic AI Developer Certification.

Benefits

- Practical skills in agentic AI development – You'll gain hands-on experience integrating AI agents into real-world software development workflows using GitHub as the control plane.
- Advanced agent architecture design – You'll learn to separate planning, reasoning, and execution in agent systems, improving reliability and control in production environments.
- Multi-agent system orchestration – You'll master coordinating multiple AI agents using GitHub workflows, enabling you to build complex, scalable AI-driven development systems.
- Production-ready governance and security – You'll implement robust governance frameworks using

GitHub-native controls, human-in-the-loop approvals, and least-privilege access to ensure safe and compliant AI operations.

- Memory and state management expertise – You'll learn to persist agent progress across environments and manage context drift, ensuring continuity in long-running agent workflows.
- Tool integration and MCP implementation – You'll configure agent tools, permissions, and Model Context Protocol (MCP) servers to enable agents to interact effectively with development environments.
- Evaluation and optimization capabilities – You'll develop skills in defining success signals, analyzing agent failures, and continuously improving agent behavior in production systems.

Training program

1. Foundations of Agentic AI in GitHub
   - Introduction
   - Define agentic AI in the SDLC
   - Explain the agent lifecycle – plan, act, evaluate
   - Describe GitHub as the system of record and control plane
   - Identify responsibilities, risks, anti-patterns, and traceability needs
   - Apply the contributor model to agent-generated work
2. Designing Agent Architecture and SDLC Integration
   - Introduction
   - Map agent responsibilities to the SDLC
   - Define inputs, outputs, and success criteria
   - Separate planning, reasoning, and execution
   - Examples of implementing PR governance with templates, checks, CODEOWNERS, rules, and environment gates
   - Build reliable workflows – outputs, contexts, triggers, and cross-job handoffs
   - Control and operate agents – observability, tools, MCP, secrets, hooks, and reliability
3. Tooling, MCP, and Agent Execution Environments
   - Introduction
   - How agents interact with GitHub APIs and workflows
   - Model Context Protocol (MCP) servers, registries, and allow lists
   - Execution context and boundaries
   - Agent execution limits and protections
4. Multi-Agent systems and orchestration
   - Introduction
   - Define multi-agent responsibilities in the SDLC
   - Orchestrate agents using GitHub workflows
   - Isolate execution – branches, workflows, permissions, and concurrency

- Detect and resolve conflicts using GitHub-native arbitration
- Make the system observable – attribution, evidence, and handoffs
- Operate reliably at scale – diagnose failures and recover safely

5. Memory, State, and Evaluation
   - Introduction
   - Implement agent memory strategies
   - Persist agent state and manage context drift
   - Ensure continuity of agent memory and state across tools and environments
   - Define evaluation signals and enforce quality gates
   - Analyze agent failures and improve behavior
6. Governance, guardrails, and operations
   - Introduction
   - Define risk-based autonomy and action boundaries
   - Enforce governance with GitHub controls
   - Design human-in-the-loop workflows
   - Control agent capabilities using least privilege
   - Make actions observable, traceable, and auditable
   - Maintain governance and operational reliability

Expected preparation of the participant

- The participant must have a GitHub account.
- Basic understanding of AI fundamentals
- Basic understanding of repositories, branches, and pull requests
- General knowledge of CI and CD concepts

To increase the comfort of work and training’s effectiveness we suggest using an additional monitor. The lack of additional monitor does not exclude participation in the training, however, it significantly influences the comfort of work during classes.
You can find information and requirements of participation in Distance Learning trainings at: https://www.altkomakademia.pl/en/how-it-works/about-courses/

Training Includes

- manual in electronic form available on the platform: https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Czas trwania

1 dni / 7 godzin

Language

- Training: English
- Materials: English