Introduction to agentic AI

Artificial intelligence has come a long way from rule-based systems that simply follow instructions. Now, with agentic AI, we're entering the era where AI actively makes decisions, learns from its environment and takes action without human intervention.

Traditional AI relies on predefined rules or passive responses – it responds to a specific set of inputs. Generative AI takes the next step, going beyond the predictive capabilities of traditional AI with the ability to create new content based on its training data. Agentic AI is a big leap forward in the development of AI, adding the capability to operate with a level of autonomy. It can assess situations, adjust strategies, and pursue objectives in dynamic environments, all while refining its own approach over time. Agentic AI is once again significantly changing the way that humans interact with AI. This evolution is fueling breakthroughs across industries, from automating complex workflows to enabling more intelligent robotics.

As AI continues to advance, the shift toward agentic systems raises both exciting possibilities and new challenges. Understanding what sets agentic AI apart is key to grasping where the next wave of AI innovation is headed.

Generative AI (GenAI)

Flow: Input → Model → Result

GenAI systems (like large language models) generate text or code in response to prompts. They're stateless and lack agency—output is entirely driven by the input, with no goal persistence or task planning.

AI Agents

Flow: Goal → Agent → Tools → Output

Agents are task-oriented systems that invoke tools (e.g., APIs, web search, code execution) to complete a specified goal. They exhibit some autonomy but are often tightly scoped and remain prompt-dependent. Most agents rely on a single execution loop and lack persistent memory or dynamic planning.

Agentic AI

Flow: Objective → Sub-Agents → Tools + Memory → Output

Agentic AI systems are designed for autonomous, multi-step operations. They decompose objectives into subtasks, coordinate sub-agents, use external and internal tools, and leverage short- and long-term memory. These systems exhibit planning, adaptability, and initiative, allowing for long-horizon task execution with minimal human input.

The integration of agentic AI in cybersecurity leverages various **advanced AI techniques, prominently including machine learning (ML)** and natural language processing (NLP). Machine learning forms the analytical backbone, allowing agentic

systems to learn from vast datasets and identify complex patterns that signify malicious activity.

Within ML, various techniques are employed, including:

- supervised learning for classifying known threats (e.g., identifying malware based on labeled datasets)
- unsupervised learning for **detecting anomalies** (e.g., flagging unusual network behavior without predefined rules)
- reinforcement learning for optimizing response strategies (e.g., an agent learning the most effective way to contain a breach through trial and error in a simulated environment)

These ML models enable the agentic AI to continuously refine its understanding of normal versus malicious behavior, adapting to new attack vectors and evolving threat tactics.

Natural language processing (NLP) is key to enabling agentic AI to comprehend and interact with human-generated data, which is abundant in cybersecurity. By leveraging NLP, these AI systems can process unstructured text from sources like threat intelligence reports, security forums, phishing emails, and incident response notes. This allows them to extract vital information, detect emerging attack patterns, and understand the intentions behind suspicious communications.

For instance, agentic AI can use NLP to interpret a newly released vulnerability report, automatically identify which systems in an organization are at risk, and even trigger a patching procedure. Likewise, it can assess the wording of an email to detect potential phishing attempts, regardless of the sender or embedded links. By combining advanced machine learning for pattern recognition with NLP's contextual insights, agentic AI can efficiently analyze and act on varied cybersecurity data, enhancing its effectiveness in complex security operations.