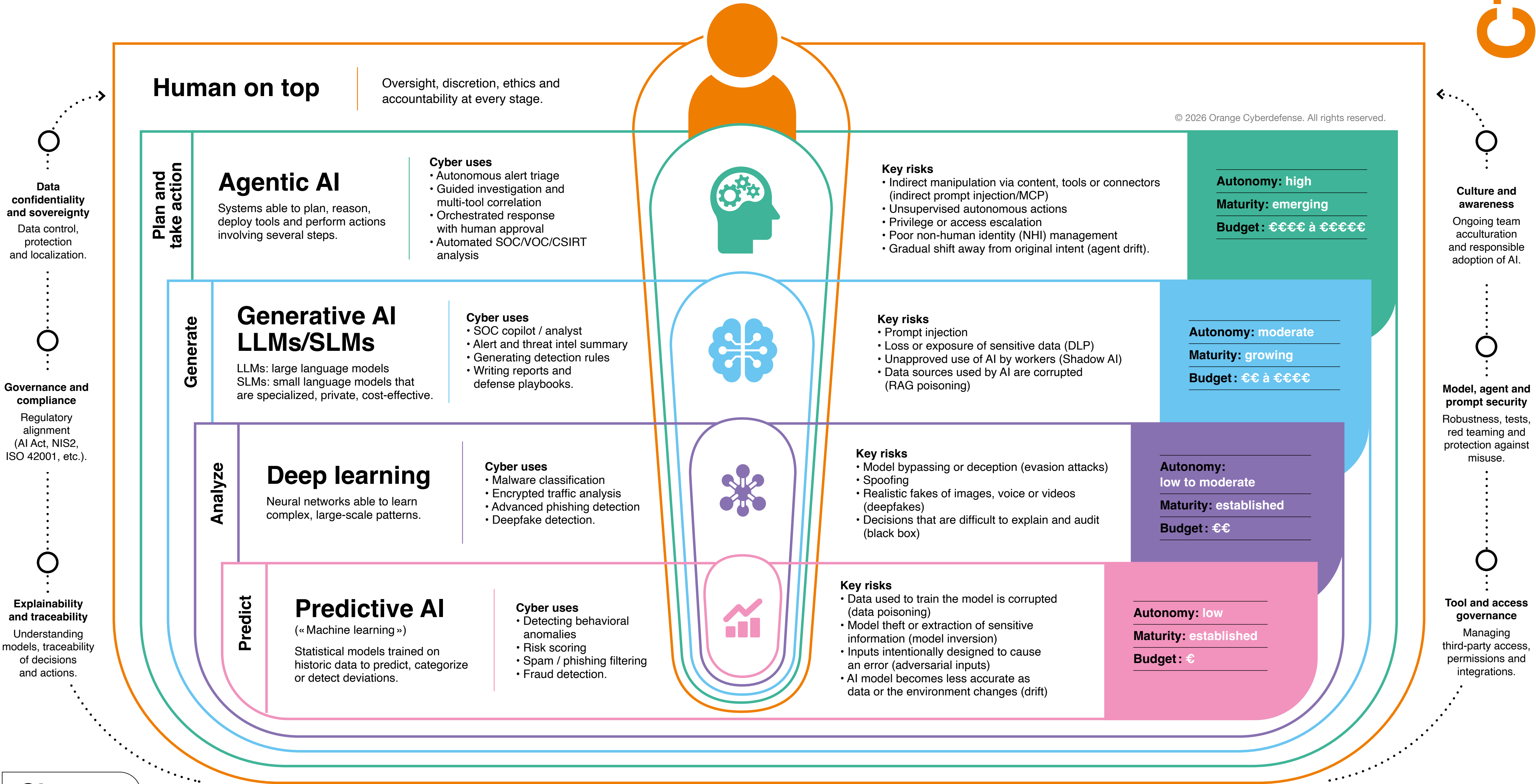




Glossary

- MCP:** Model Context Protocol, protocol allowing an AI tool or agent to connect to internal or external tools and data sources.
- NHI:** Non-Human Identity, digital identity used by an application, service or AI agent.
- DLP:** Data Loss Prevention, tools aiming to prevent the loss of sensitive data.
- Shadow AI:** use of AI tools beyond the parameters approved by the organization.
- RAG:** Retrieval-Augmented Generation, method allowing an AI tool to consult knowledge bases before responding.
- Drift:** decline in model accuracy as the data or environment changes.
- LLM:** Large Language Model, able to understand and generate text.
- SLM:** Small Language Model, specialized and generally easier to deploy.
- SOC/VOC:** Security and Vulnerability Operations Centers.
- CSIRT:** Computer Security Incident Response Teams.