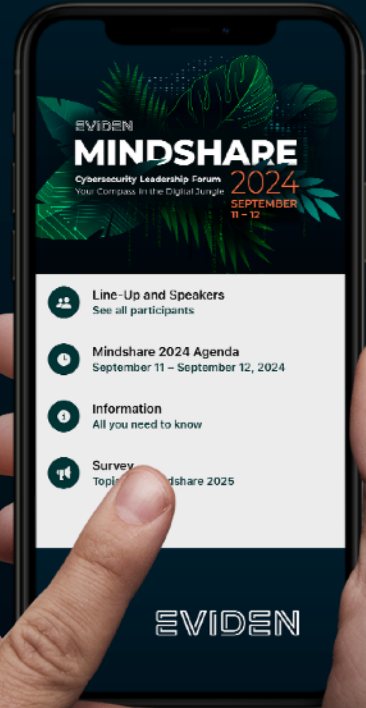


# MINDSHARE 2024 AGENDA



SCAN NOW !



# GenAI for IAM

How can Generative AI help Identity & Access Management?

**David Leporini**

Director of IAM Cybersecurity Products & General Manager of Evidian



## We are Evidian

Software vendor of Identity and Access Management solutions

- Access Management
- Identity Governance
- On premise, As a Service, Managed Services



### Global references

Europe, Japan, North America, MEA

**+900 clients**



R&D in Europe

**+5 millions** professional users

### Technological partnerships and interoperability



# GenAI

## Quick introduction

- In essence, GenAI can generate data from a large set of data learned preliminarily during a learning phase. In response to a question called prompt, new data is generated, i.e., predicted and not just copied, based on the pretrained Large Language Model (LLM) with billions of parameters inside
- It aims at facilitating, simplifying, and expanding the usage of sophisticated applications and processes
- It is penetrating the operations of many, if not all, business domains – of course, one natural candidate of such applications is Identity and Access Management (IAM)
- Typical day-to-day interactions an IAM practitioner would perform, to be more productive in the administration of the identity and access governance, by simplifying, shortening and de-risking the interactions with IAM tools
  - Asking questions: “Please explain me why user X can’t access the same business applications as user Y, even though they have the same job position in the same business unit.”
  - Requesting actions: “Please assign the newly hired user Y the same permissions as user Z”



## When using GenAI

### When Generative AI Is and Is Not Effective

Use-case family	Generative models' current usefulness	Example use cases
Prediction/forecasting	Low	Risk prediction, customer churn prediction, sales/demand forecasting
Decision intelligence	Low	Decision support, augmentation, automation
Segmentation/classification	Medium	Clustering, customer segmentation, object classification
Recommendation systems	Medium	Recommendation engine, personalized advice, next best action
Content generation	High	Text generation, image and video generation, synthetic data
Conversational user interfaces	High	Virtual assistant, chatbot, digital worker

# How can Generative AI help IAM?

- Getting the best from the product(s) documentation and the customer care expertise, especially when the searched information is shared among several rich sources, supplementing existing support means such as knowledge databases and consulting experts
- Auto-configuring an IAM deployment, by automatically generating approval workflows that are often tailored to specific customers, helping setting up the initial instantiation of the policy model, managing the role lifecycle and entitlement assignments to end-users, co-programming rules for decision management systems...
- Simplifying IAM administration by helping extract advanced analytical insights and interact with the Identity Fabric APIs, to act on the security policy lifecycle. This is probably the use case where we expect the biggest breakthrough, benefiting IAM practitioners in the short-term



# How do we build a GenAI-based IAM?

- A conversational app as a simplified user interface to interact with the LLM using natural language
- Prompt engineering, to enrich the question asked with additional contextual information or focus the question on the appropriate scope
- A VectorStore database to optimize the efficiency of frequent requests made by the LLM to the IAM data sources
- An orchestration tool to chain multiple inputs to the LLM, outputs from the LLM, combined with API requests and responses to an IAM Identity Fabric and rich sources of information
- An LLM to execute the prompt requests with the closed target of serving demands related to the IAM topic only, with safety checks on inputs and outputs
- IAM agents to securely retrieve data from the IAM policy database and the data lake, as well as to act on IAM policy data, using the Identity Fabric APIs



# How can we mitigate specific risks?

- Same key principles as for protecting business applications must be applied to GenAI techniques: strong multifactor authentication to access GenAI, fine-grained dynamic authorization to enforce the least privilege principle for all accesses to the underlying Identity Fabric API, exhaustive audit of inputs and outputs, active monitoring of the audit trail...
- Risks related to LLMs, chatbots and AI technologies with AI-specific criteria such as explainability, bias, information leakage, and more recently hallucinations, where the LLM predicts an output recommendation that is pure inappropriate invention
- GenAI must be constrained to process questions and deliver answers only within the strict scope of IAM when interoperating with the IAM Identity Fabric, by applying dedicated consistency-checking rules to challenge the outputs delivered by the LLM and avoid hallucinations
- A rule-based decision management safety tool can be linked with the approval workflow in place to add a preliminary human approval from the security officer before applying changes suggested by the GenAI tool





# GenAI in action

Integrated with Evidian IDaaS NextGen









List of authentication methods












Please select an authentication method

 **PASSWORD AUTHENTICATION**  
Use your login and password.

 **EVIDIAN AUTHENTICATOR PUSH AUTHENTICATION**  
Use your phone and Evidian Authenticator.

  
MORE

[ACTIVATE MY ACCOUNT OR RESET MY PASSWORD WITH 4 EYES VALIDATION](#)

[MOBILE PHONE ENROLLMENT PROCESS](#)

[FORGOTTEN PASSWORD?](#)

[LOST IDENTIFIER](#)

# A new era for the IAM user experience

- GenAI will definitely and deeply impact the user experience when interacting with IAM tools in a natural, non-tedious and very powerful manner
- GenAI for IAM is just a step away from becoming a reality in production
- Well-known security approaches will minimize risks frequently associated with GenAI technology



# Questions?

**David Leporini**

Director of IAM Cybersecurity Products & General Manager of Evidian



# TAKE A MINUTE AND GIVE US FEEDBACK ...



**RATE  
NOW!**

