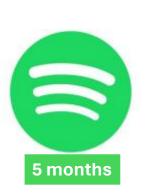


Dr. Leila Taghizadeh

Global Head of Cyber Risk Management & CISO IberoLatAm @Allianz

https://www.linkedin.com/in/leilataghizadeh/

# Time took to reach 1 million users











# Enterprise Applications & use cases for Gen-Al

generative AI

Generating forecasts for complex scenarios

Analyzing massive volumes of complex and unstructured data

Aggregating key metrics across production systems

Automating creation of text, charts, and graphs for reports

Analyzing operational concerns, such as inventory and staffing

**Optimizing pricing strategies** 

Auto-generating and adapting contracts, purchase orders, and invoices

> Understanding user preferences, behaviors, and contextual cues

Automating and personalizing customer service

> Learning from previous and unresolved support tickets

> > Providing intelligent scripts for agent interactions

Developing personalized marketing

Increasing precision and effectiveness of ad targeting

Detecting security threats and account takeover attempts

Analyzing communications for phishing attempts and social engineering

Source: MIT Technology Review Insights, based on data from 'The Rise of Generative AI', 'The Great Unlock' Large Model Survey by Emerj AI Research conducted in January–March 2023.

#### Automation vs AI vs Generative AI

#### **Automation**



**Definition:** the process of using technology to perform repetitive tasks without human intervention.

**Application:** to streamline workflows, reduce errors, and increase efficiency.

**Example:** An automated email that sends predefined replies based on keywords in incoming messages

#### Artificial Intelligent

**Definition:** creating systems or software that can perform tasks that typically require human intelligence.

**Composition:** machine learning, natural language processing, & computer vision.

**Example:** A recommendation algorithm that suggests personalized content based on a user's browsing history.

#### **Generative AI**

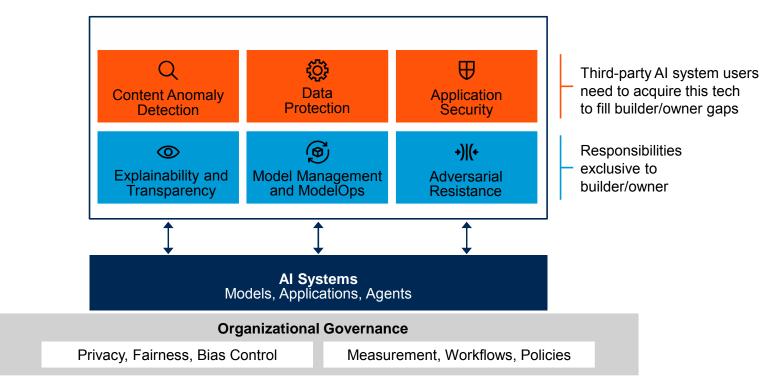
ģ

**Definition:** beyond traditional AI by creating new content rather than just analyzing existing data.

**Output:** novel outputs, such as text, images, or music.

**Example:** A language model that generates creative stories or poems based on a given prompt.

### AI Technology Component



Source: Gartner - The Executive Guide to Al Trust, Risk and Security Management

# Key Risks Introduced by Generative Al

1010 10110 101 101 0100110 10 1010 10 111011

> 1010 10110 10 101 0100110 1 1010 10 11101

1010 10110 10 101 0100110 10 1010 10 11101

### **Enhanced Social Engineering**

- Hyper-personalized phishing
- Natural language generation
- Emotional manipulation
- Evasion tactics
- Automated reconnaissance
- Diversification in attack Methods

https://www.forbes.com/sites/forbestechcouncil/2023/05/26/how-ai-is-changing-social-engineering-forever/?sh=56f762a4321b

# Other risks...



**Sophisticated Phishing Attacks** 



AI-powered Malware



Data Privacy



**Deepfakes and Misinformation** 



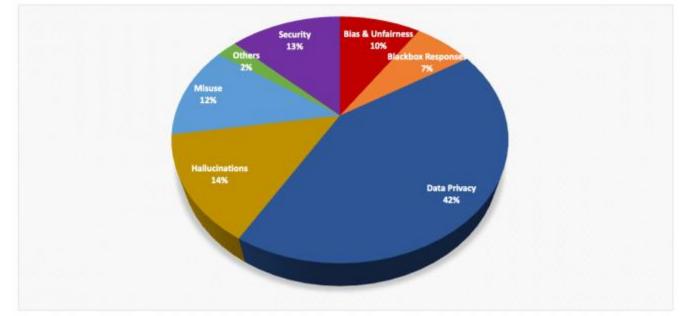
Automated Hacking Tools



**Ethical Dilemmas** 

### Survey from the IT leaders

#### Poll: Which Risks of GenAl Are You Most Worried About?



Source: Gartner IT Executives Webinar Poll (August 2023), n = 713 799579

#### Other opinions....



# Key Opportunities Presented by Generative AI

## **Transforming Opportunities**



**AI-Enhanced Threat Detection** 



**Enhanced Incidence Response** 



Automation of Security Tasks



**Predictive Capabilities** 

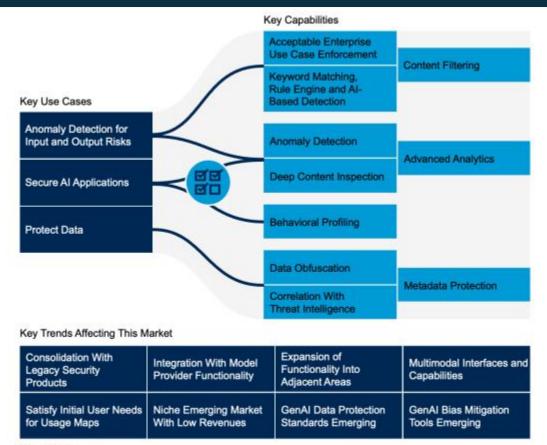


**Advanced Simulation & Training** 



**Customized Security Solutions** 

### When (not) to use AI



Source: Gartner

799579\_C

# When (not) to use AI

Al technique suitability 📕 Low (L) 📒 Medium (M) 📕 High (H)

Use-case families	Common Al techniques					
	Generative models	Nongenerative machine learning	Optimization	Simulation	Rules/ heuristics	Graphs
Prediction/ forecasting	L	н	L	. н	м	L
Planning	L	L	н	м	м	н
Decision intelligence	L	м	H	н	н	м
Autonomous systems	L	м	н	м	м	L.
Segmentation/ classification	м	н	L	L.	H	н
Recommendation systems	м	н	м		м	н
Perception	м	н	L	£	L.	L.
Intelligent automation	м	н	L		н	м
Anomaly detection/ monitoring	м	н	L	м	м	н
Content generation	н	L	L		L	L
Conversational user interfaces	н	н			м	н
Knowledge discovery	н	м		4	м	н

Source: Gartner B06238\_C

Navigating the Future with Generative AI in Cybersecurity



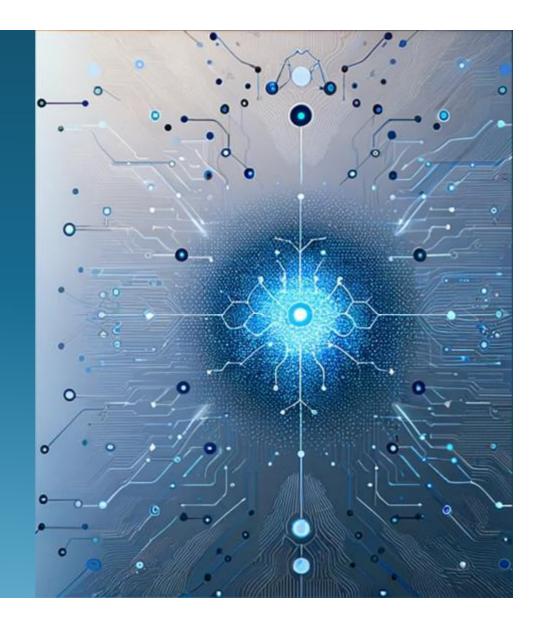
Adoption



Regulation & Oversight



Continuous Learning



## Learning Opportunities – Free Courses

- 1. Google AI Courses offers 5 different courses to learn generative AI from the ground up. <u>https://lnkd.in/eW5k4DVz</u>
- 2. Microsoft AI Course offers an AI course that covers the basics and then more. https://lnkd.in/eKJ9qmEQ
- 3. Harvard University is offering a full 7-week course to explore the concepts and algorithms of AI. https://lnkd.in/g4Sbb3nQ
- 4. Prompt Engineering for ChatGPT by Vanderbilt University offers beginners a starting point to writing better prompts. https://lnkd.in/d-rCb-AM
- 5. ChatGPT Prompt Engineering for Devs in collab with DeepLearning is offering this course taught by Isa Fulford and Andrew Ng. <u>https://lnkd.in/gtGc5Znp</u>
- 6. LLMOps offered by Google Cloud in collab with DeepLearning taught by Erwin Huizenga. https://lnkd.in/gMXDr7MJ
- 7. Big Data, Artificial Intelligence, and Ethics by the University of California Davis covers big data and introduces IBM's Watson. <a href="https://lnkd.in/gVEf3Dvm">https://lnkd.in/gVEf3Dvm</a>
- 8. An introductory course on prompt engineering that goes beyond the basics. <u>https://lnkd.in/g2P9U\_Bs</u>