

# EA and Generative AI: Ideas and Gotchas!

Leveraging AI Models in the Enterprise

**Trac Bannon**

Senior Principal

Software Architect & Digital Transformation Advisor

**MITRE** Advanced Software Innovation Center

September 2023

# Tracy L. Bannon

"Trac"

Software architect | engineer | mentor | community leader

## Who Am I?



/trās/

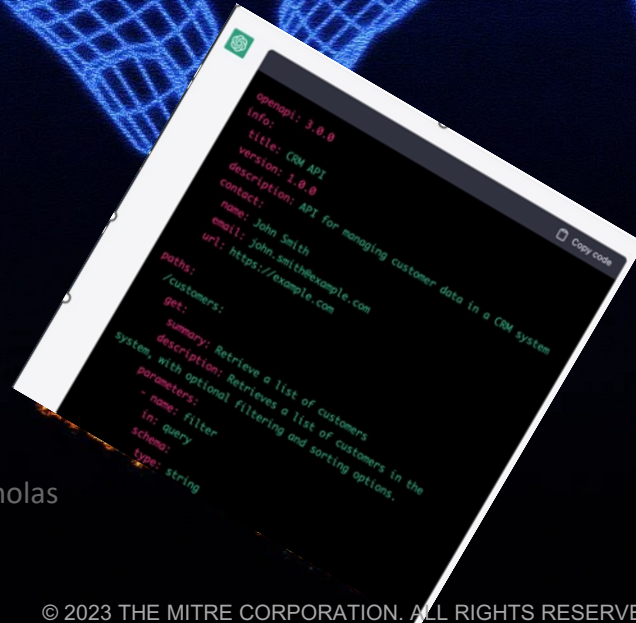
A word cloud of technology and DevOps-related terms. The most prominent terms include:

- #DevSecOps** (large, red, diagonal)
- #RealTechnologists** (large, purple, horizontal)
- Value Stream Mapping** (large, orange, at the bottom)
- Evolutionary Architecture** (large, red, horizontal)
- AI-Assisted SDLC** (large, green, horizontal)
- Agility** (large, green, horizontal)
- #OpenSource** (large, green, horizontal)
- #DevOps** (large, green, horizontal)
- Metrics** (large, blue, horizontal)
- Continuous Testing** (medium, blue, horizontal)
- #StraightTalkforGovt** (medium, blue, horizontal)
- Value Stream Design** (medium, blue, horizontal)
- Continuous Improvement** (medium, red, diagonal)
- Automation** (medium, red, diagonal)
- #CloudNative** (medium, blue, diagonal)
- CALMS** (medium, red, diagonal)
- CI/CD** (medium, yellow, horizontal)
- Building Digital Workforce** (medium, yellow, horizontal)
- Modernization** (medium, yellow, horizontal)
- Digital Transformation** (medium, orange, horizontal)
- Community** (medium, green, horizontal)
- DoJo** (medium, orange, horizontal)
- Current State Baseline** (medium, blue, horizontal)
- Secure by Design** (medium, orange, horizontal)
- #DesignPatterns** (medium, green, horizontal)
- Modern Software Practices** (medium, orange, horizontal)
- Psychological Safety** (medium, green, horizontal)
- SomethingToNoodleOn** (medium, orange, diagonal)
- Minimum CD** (medium, blue, horizontal)
- CyberSecurity** (medium, blue, horizontal)
- Low Code/No Code** (medium, red, horizontal)





# Artificial Intelligence and the Enterprise



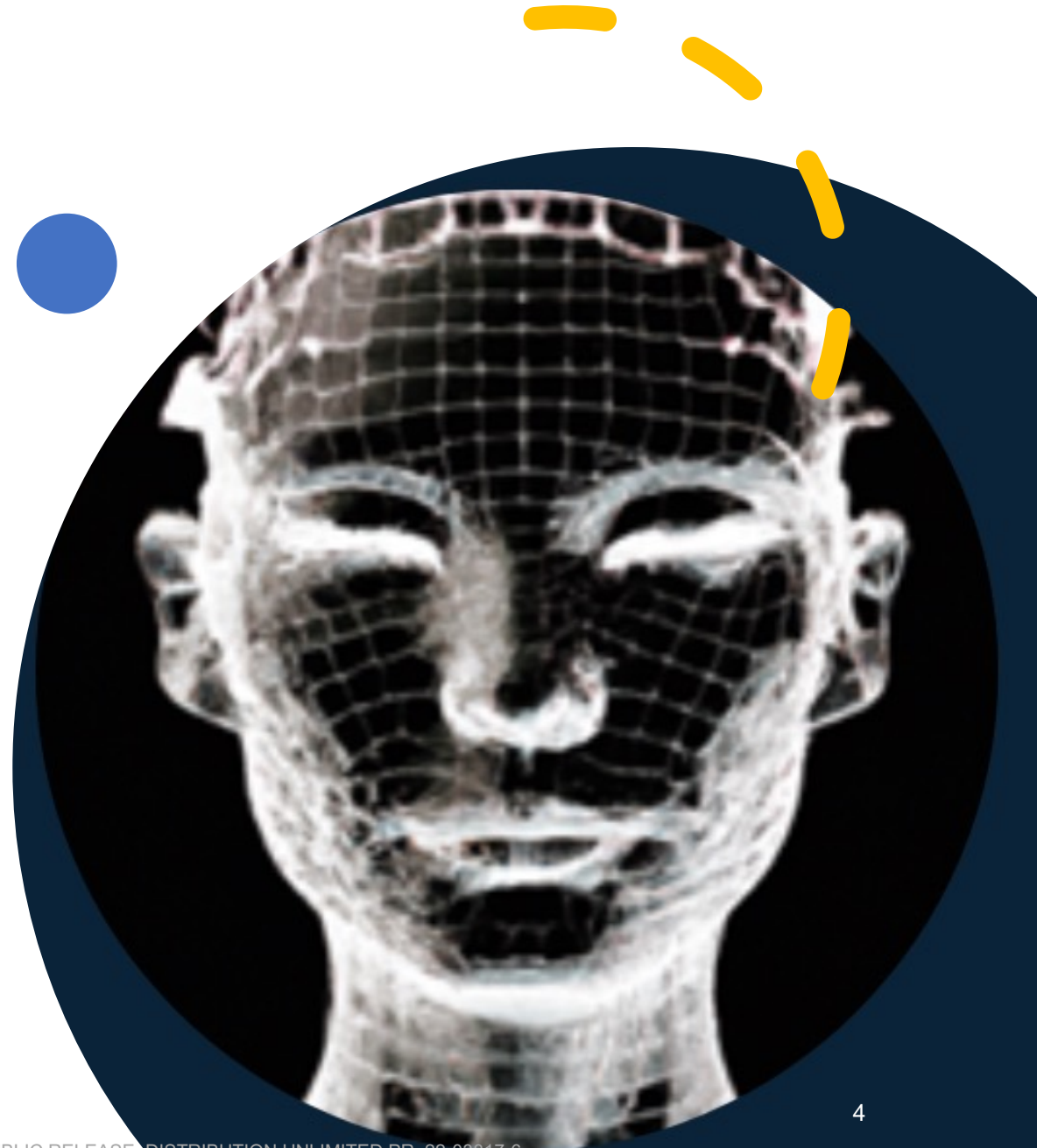
Based on an illustration by Nicholas  
Konrad / The New Yorker

**MITRE**



# Some definitions to help our conversation

- **Generative AI** is a category of AI algorithms that focus on generating new content, data, or patterns after being trained on existing information.
- Generative AI includes text, images, video, or even music (tool names)
- **Large language models (LLMs)** are a subset of Generative AI trained on vast amount of text data
- LLMs calculates probability distribution over sequences of words and scores the likelihood of word sequences
- Parameters in LLMs help the model to understand relationships in the text, which helps them to predict the likelihood of word sequences
- By sampling over the probability distribution, the models can write text mimicking human-like language understanding
- **AI-assisted** development often refers to using LLMs to improving developer productivity





# Show of Hands

---

Who is using Generative AI in their enterprise?

---

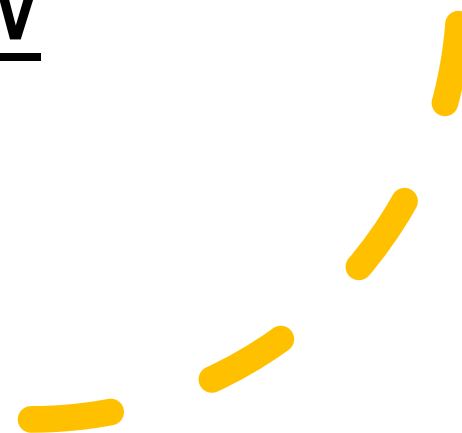
How is Generative AI being used?

---

Do you have a corporate AI strategy?



Applying Generative AI:  
the question is not if but how





# Three Areas for EA Focus



Start with anything  
repetitive then expand



SDLC and Testing



Cybersecurity



IT Operations



# Applying to the SDLC

- Faster adoption into the LC/NC platforms
- Code Generation and Testing
- Personalizing User Experience

## *Key Considerations*

- **Ethical AI:** Ensuring that the AI does not propagate existing biases in code
- **Quality Assurance:** Rigorous testing to ensure generated code meets quality standards



# Improving Cybersecurity

- Threat Modeling
- Security Protocols

## *Key Considerations*

- **Data Privacy:** Ensure that AI models are trained on anonymized data
- **Human Oversight:** Maintain human supervision for crucial security decisions

# IT Operations

- Automated Resource Allocation
- Predictive Maintenance

## *Key Considerations*

- **Cost:** Careful assessment of ROI for implementing AI-driven solutions
- **Scalability:** Solutions should be able to scale as the organization grows

# Adding AI to the Enterprise Strategy

---

# Parts of an AI Strategy

Organizations need to thoughtfully incorporate generative AI into the enterprise strategy

- Needs Assessment
- Pilot Programs
- Skill Development
- Governance
- Monitoring and Feedback Loop
- Thought Leadership



# Questions to ask your platform vendors

---

How does the platform ensure the security and privacy of data used by the generative AI models?

---

What measures have been taken to prevent the AI model from generating malicious or vulnerable code?

---

How does the platform manage and control access to the generative AI models and their generated outputs?

---

How does the vendor handle AI model updates, and what steps are taken to evaluate and maintain the security of the generative AI models over time?

# More questions to ask your vendors

---

What are the pricing options and licensing terms for using the generative AI features?

---

Are there any hidden costs or usage limitations we should be aware of?

---

How does the tool handle edge cases or unexpected inputs?

---

Are there any built-in fail-safes to prevent the generative AI from producing harmful or problematic code?

---

Can the generative AI model be fine-tuned or customized to our organization's specific coding standards and practices?

---

Is it possible to extend the model's capabilities to address our unique requirements or use cases?



# Other things we need to understand

- Prompt engineering as a discipline; turning human factors on its edge
- Human-Machine teaming
- Software team performance
- Trust and reliability in software outcomes when driven by AI-assisted or AI-generated software
- Automating decisions and software development workflows
- Ethics of prompts and who owns the data once created

**We can't put the genie back in the bottle; we need to discuss, research, and understand**



# Call to Action



## Your next steps:

- Connect with your vendors to ask model quality and security questions
- Ask your platform vendor about their AI roadmap
- Pulse your organization to see if and how generative models are being used
- Enable research and discovery or LLM usage with Cybersecurity as your highest priority
- Establish on reasonable guardrails

## What I need from you:

- Share your organization's story and lessons learned
- Continue to share out new use cases and new tools





Tracy L. Bannon

[tbannon@mitre.org](mailto:tbannon@mitre.org) | alt: [Trac@tracybannon.tech](mailto:Trac@tracybannon.tech)



<https://www.linkedin.com/in/tracylbannon>



@TracyBannon



<https://tracybannon.tech>

Disclaimer: The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

**MITRE**

**SOLVING PROBLEMS  
FOR A SAFER WORLD®**

# References

<sup>1</sup><https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023>

<sup>2</sup><https://spectrum.ieee.org/ai-code-generation-language-models>

<sup>3</sup><https://www.codecademy.com/resources/blog/programming-languages-created-by-women/>

<sup>4</sup><https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai>

<sup>5</sup><https://www.marktechpost.com/2022/08/25/researchers-develop-ticoder-framework-for-code-generation-using-user-feedback-with-90-4-consistency-to-user-intent/>

<sup>6</sup><https://advisory-marketing.us.kpmg.com/speed/pov-generativeai.html>

<sup>7</sup>[https://youtu.be/8Vat\\_jRt128](https://youtu.be/8Vat_jRt128) (Artificial Intelligence and Low Code/No Code - Leveraging AI models to improve software creation)