Applying AI to the SDLC: New Ideas and Gotchas!

Leveraging AI Models to Improve Software Creation

Trac Bannon
Senior Principal
Software Architect & Digital Transformation Advisor
MITRE Advanced Software Innovation Center

October 2023

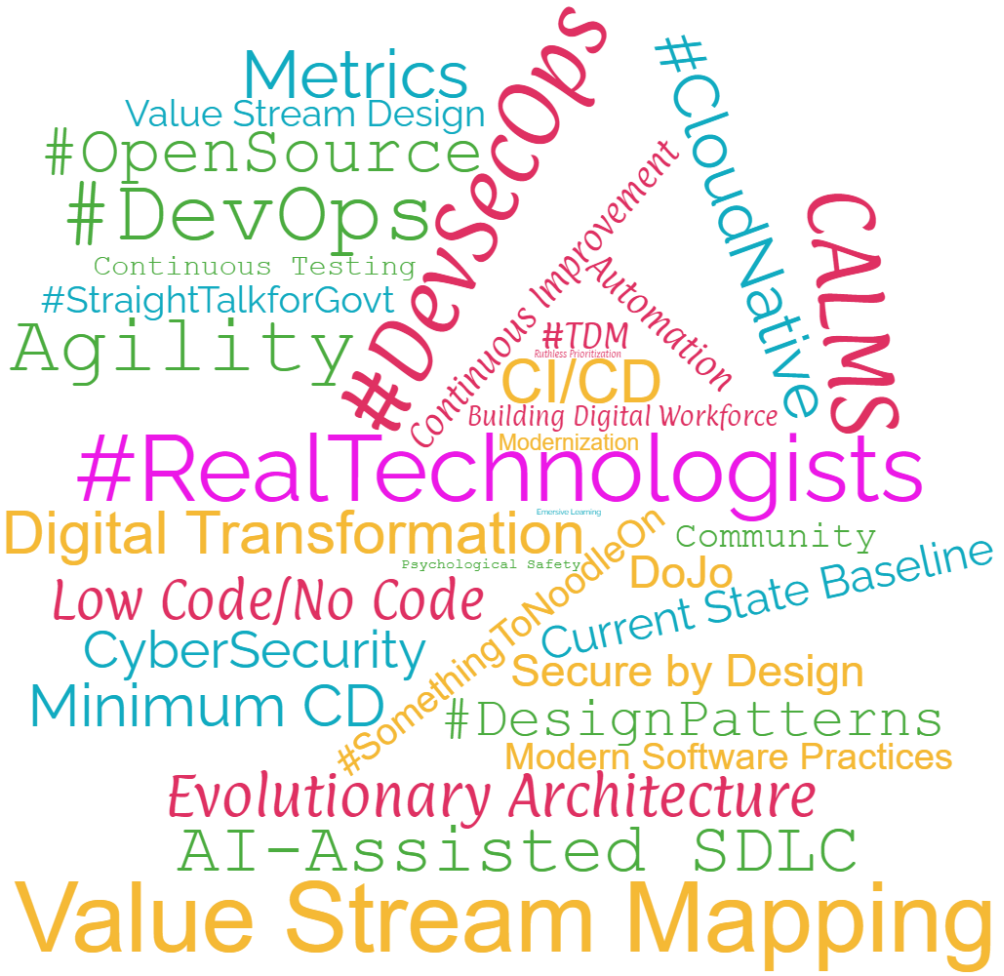
Tracy L. Bannon

"Trac"

Software architect | engineer | mentor | community leader

Who Am I?

/trās/



vsm consortium Influencer

AMBASSADOR DevOps Institute ADVANCING THE HUMANS OF DEVOPS

IEEE SENIOR MEMBER

MITRE

Based on an illustration by Nicholas Konrad / The New Yorker

Applying AI, ML, and GAI:

The question is not if but how

MITRE

All Software Ecosystems Benefit from AI/ML/GAI

LowCode/NoCode

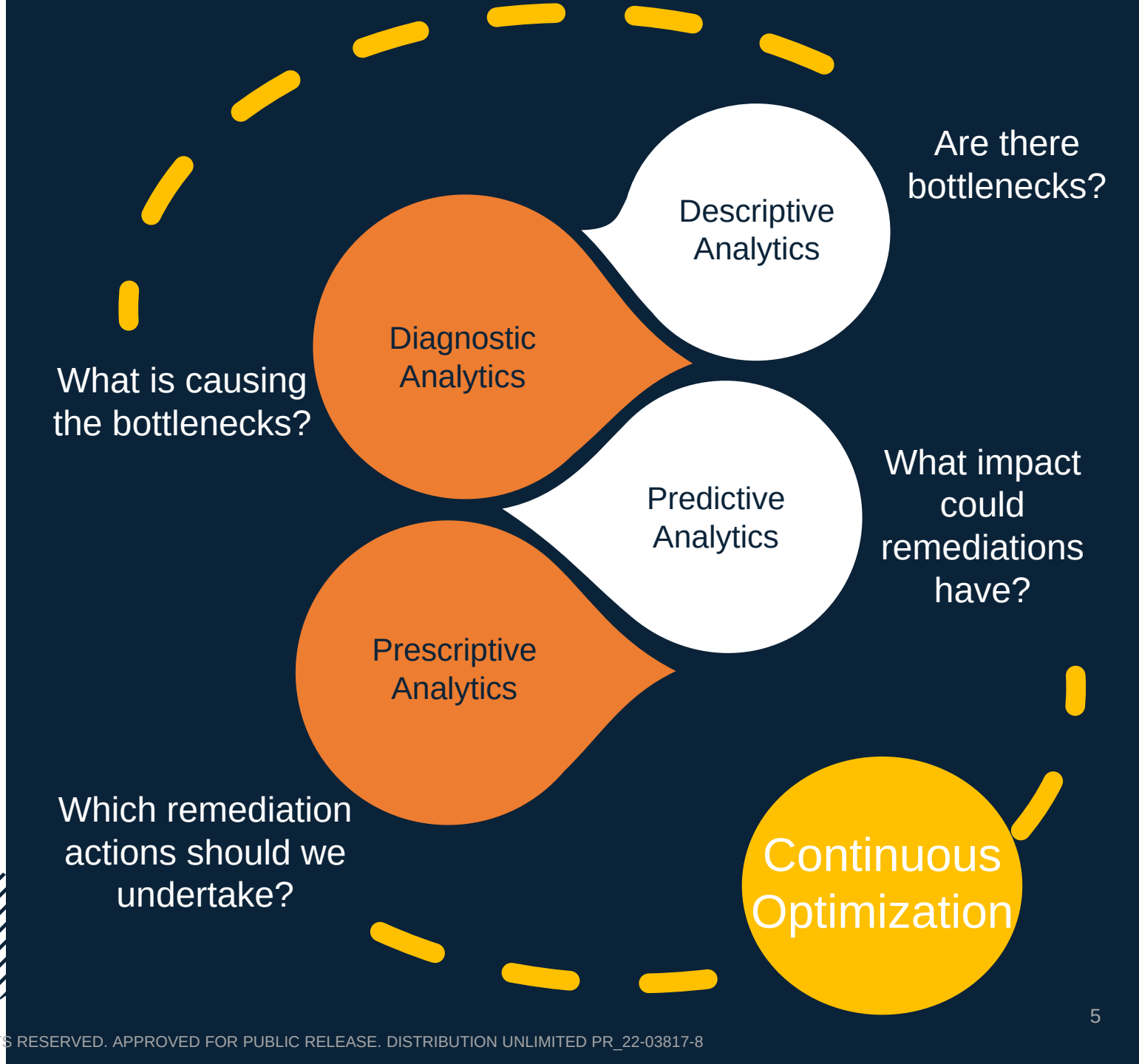
- Faster adoption into the LC/NC platforms
- Purpose of the platforms are to simplify and accelerate
- Equipping non-IT personas
- Leveraging AI *before* the recent GPT surge
- Suggests users are more likely to adopt new tech

Custom Development

- Improving quality
- Repetitive tasks
- Being applied to complete value stream

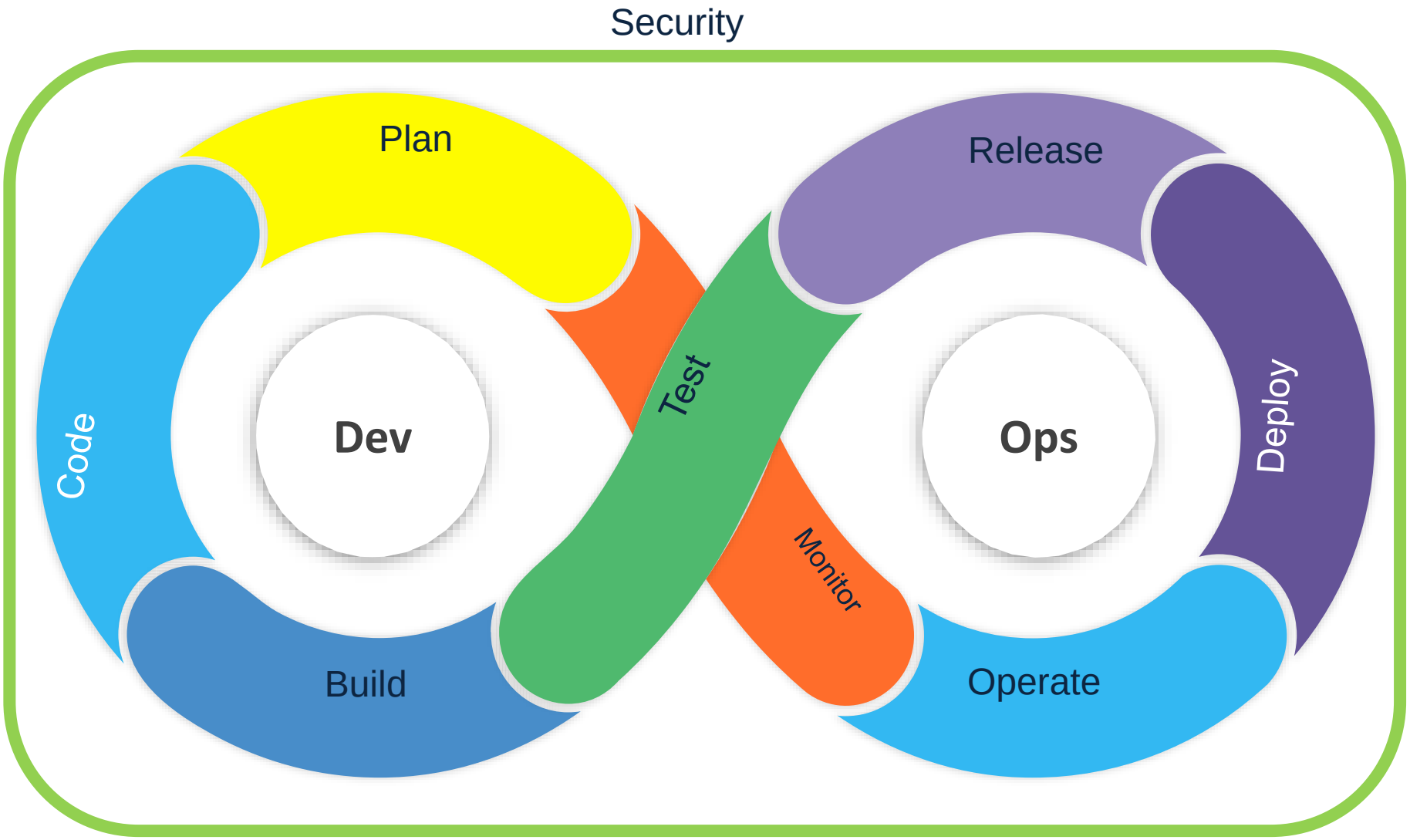
MITRE

AI-Infused Value Stream



MITRE

Where can AI be used with Dev*Sec*Op?



[10] *DevOps Infinity Loop Inspired by SlideEgg*

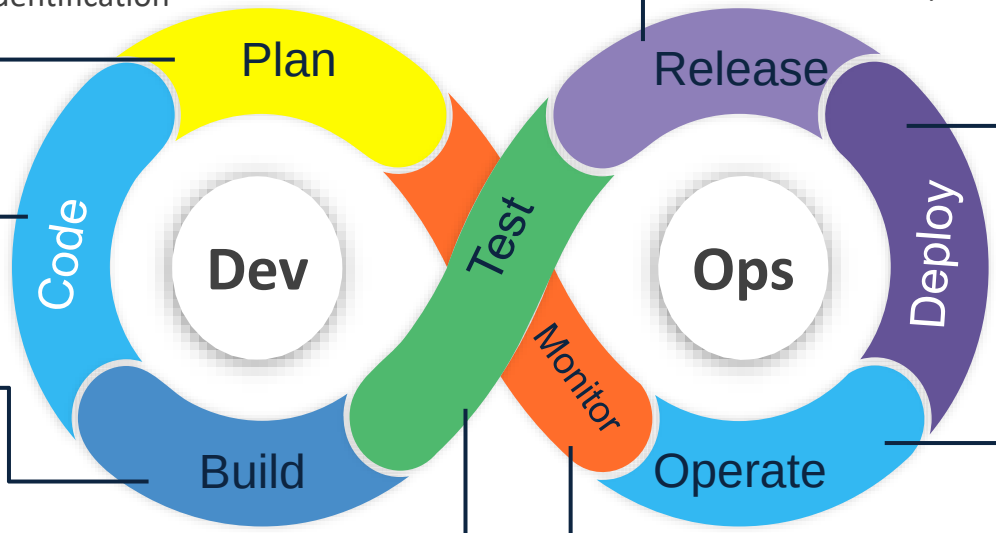
Infusing AI across the Dev*Sec*Ops Continuum

Code
- Architectural Design
- GAI based pair programming
- Code & Unit Testing Generation
- In IDE Secure Code Vulnerability Solution
- ML assisted code review selection
- AI Assisted Code Review
- AI Enabled collaboration
- Suggestive Refactoring

Plan
- Natural Language Requirements Gathering
- NLP Requirements Analysis for inconsistency and ambiguity
- GAI Epic and User Story Generation
- Effort Estimation using Neural Networks
- GAI-assisted Threat Model Policy Identification

Release
- Compliance Validation
- Reinforced Learning-based models generate deployment scripts
- AI Enabled Failure Analysis
- Release Risk/Success Prediction
- AI Driven CI/CD workflow automation

Deploy
Dynamic Environment Provisioning and Deployment Optimization
Realtime Rollback
AI-assisted Log Aggregation



Security
Is infused into all actions and activities

AIOps engines provide correlation and predictive monitoring

Build
- Aggregated Merge Request Impact Analysis
- GAI-based identification of security vulnerabilities
- ML algorithm optimized build times
- AI-Assisted Security Vulnerability Detection
- Software Composition Analysis

Test
- Natural Language Test Case Generation
- Test Data Generation
- AI Enabled test effectiveness predictions
- E2E Functional Test Execution
- Intelligent Failure/Self Healing Testing
- NLP based API based contract definition

Monitor
- Event Correlation
- False Alarm Filtering
- Self-Healing Techniques
- Root Cause Analysis
- Observe system performance
- Usability Patterns
- Monitoring

Operate
- Deterministic AI based ticketing and support allocation
- AI Based Self Healing Decision
- LLM Integration for Virtual Assistance
- GAI/GPT powered Knowledge Bases

MITRE

Augmented Planning

- Requirements Generation
- User Story Creation

Key Considerations

- **Data Integrity and Diversity**: Use diverse datasets from a broad spectrum or perspective and scenarios
- **Quality Assurance**: Human oversight needed to ensure that the generated user stories are relevant and meet the needs of the stakeholders

Assisted Coding

- Code Completion & Generation
- User Personalization

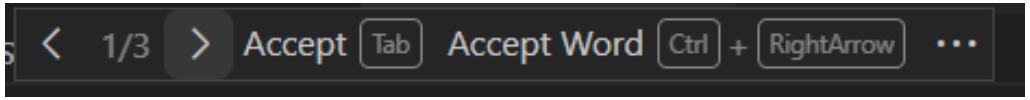
Key Considerations

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

Code Generation via GAI

Platform: CoPilot – Alternative Solution Generation Feature

Generating Code




```
def max_sum_slice(xs):
    """Return the maximum sum of a slice of xs."""
    max_sum = 0
    for i in range(len(xs)):
        for j in range(i, len(xs)):
            this_sum = 0
            for k in range(i, j + 1):
                this_sum += xs[k]
            if this_sum > max_sum:
                max_sum = this_sum
    return max_sum
```

Ideas and Gotchas:

- Start the code yourself and be as explicit as possible
- Defects abound - if you are new in career and can't easily identify defects, you will waste time
- Limited context: doesn't make use of functions defined in the code elsewhere
- Users accepted on average 26% of all completions shown by GitHub Copilot
- GitHub recommends precautions "to ensure its suitability":
  - Rigorous testing
  - IP scanning
  - Checking for security vulnerabilities

Infused Testing

- Automated Test Data Management
- Optimized Test Strategy

According to **Stack Overflow's 2023 Developer Survey**, 55.17% of respondents are interested in using AI for software testing, but only 2.85% say they have a high degree of trust in AI tools.

Key Considerations

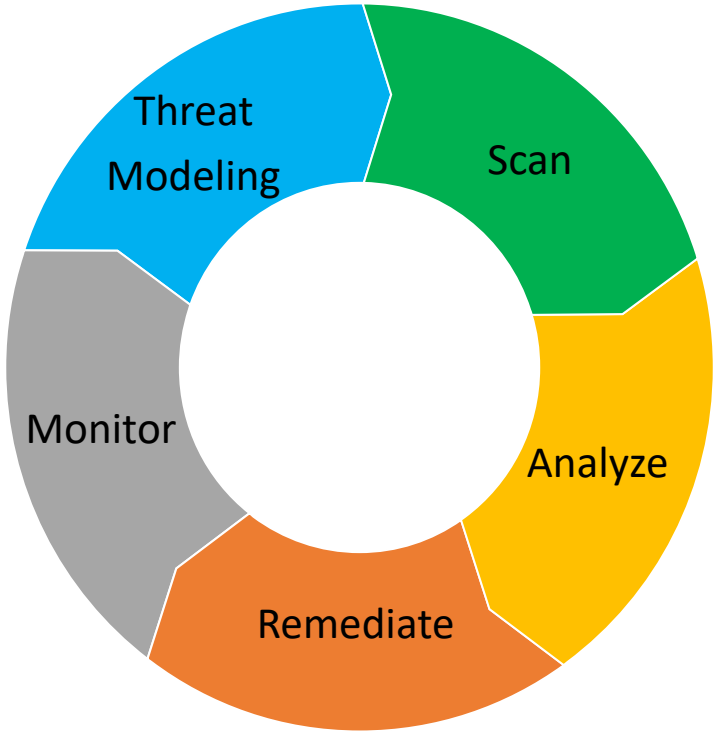
- **Data Privacy & Integrity**: Protect sensitive information; evaluate synthetic data for instances of real-world mimicking

- **Balance & Adaptability**: Manual human testing brings intuition and unpredictability; AI models should be adaptable to changing software landscape

MITRE

Improved Cybersecurity

- Threat Modeling and Threat Hunting
- Security Protocols
- AI-based Vulnerability Checking



Key Considerations

- **Data Privacy**: Ensure that AI models are trained on anonymized data

- **Human Oversight**: Maintain human supervision for crucial security decisions

Augmented Release Management

- Release Risk/Success Prediction
- Dynamic Environment Provisioning and Deployment Optimization

Key Considerations

- **Data Quality and Completeness**: Consistency, quality, diversity and volume of data are cornerstone to release success predictive analysis

- **Deployment Strategy Alignment:** Align application architecture to the deployment strategy

MITRE

Augmented IT Service Desk

Start with anything repetitive then expand

- AI Based Self Healing decisions
- Deterministic ticketing and support allocation

Key Considerations

- **Decision Trustworthiness**: Careful validation and testing of the model must be rigorous
- **Feedback Integration**: Humans must provide feedback on AI-driven tickets to refine model accuracy

Supplemented 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

The Future of AI Infused DevOps

Start with anything repetitive then expand

- AI is just now being incorporated and experimented with
- Continuous testing is current the most impacted
- AIOps is on the rise enhancing observability and ConMon
- Shift Left Security needs humans in the loop
- Release Anomaly prediction is improving rapidly

MITRE

Questions to ask your AI providers

- How do you ensure the security and privacy of data used by the AI models?
- What measures have been taken to prevent the AI model from generating malicious or vulnerable code?
- How do you manage and control access to the generative AI models and their generated outputs?
- How do you handle model updates, and what steps are taken to evaluate and maintain the security of the AI models over time?
- Is it possible to extend the model's capabilities to address our unique requirements or use cases?
- How does the tool handle edge cases or unexpected inputs?
- Are there any hidden costs or usage limitations we should be aware of?
- What are the pricing options and licensing terms?

MITRE

Other things to keep in mind

- Prompt engineering as a discipline
- Human-Machine teaming
- Software team performance
- Trust and reliability in software outcomes when driven by AI-assisted or AI-generated software
- 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 providers to ask model quality and security questions
- Ask your platform vendor about their AI roadmap
- Pulse your organization to see if and how 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 | alt: 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 - 1

[1]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

[2]https://spectrum.ieee.org/ai-code-generation-language-models

[3]https://www.codecademy.com/resources/blog/programming-languages-created-by-women/

[4]https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

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

[6]https://advisory-marketing.us.kpmg.com/speed/pov-generativeai.html

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

[8]https://www.linkedin.com/pulse/using-ai-establish-continuous-value-stream-mapping-devops-ahmed/

[9]https://academy.broadcom.com/blog/valueops/using-ai-to-establish-continuous-value-stream-mapping

[10]www.slideegg.com

[11]https://www.forbes.com/sites/janakirammsv/2022/03/14/5-ai-tools-that-can-generate-code-to-help-programmers/?sh=570b83ff5ee0