#AI4SWE

AI Powered Software Engineering

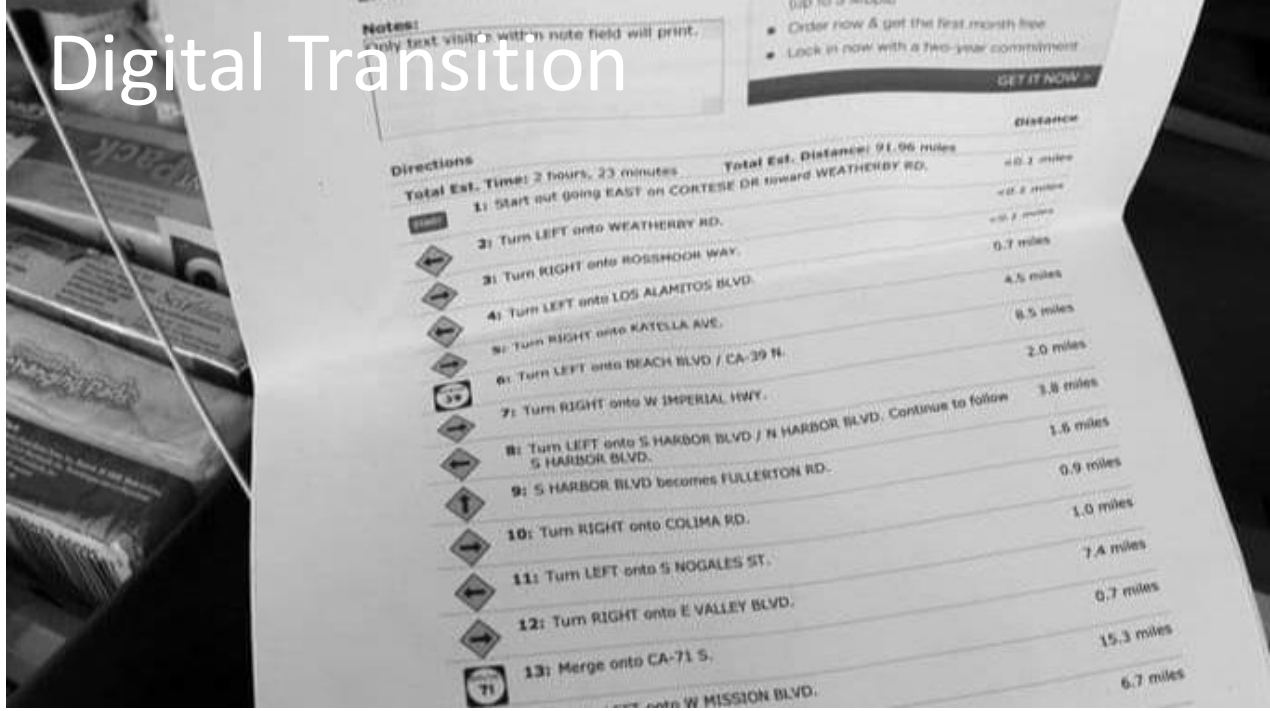
Unlocking Innovation

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

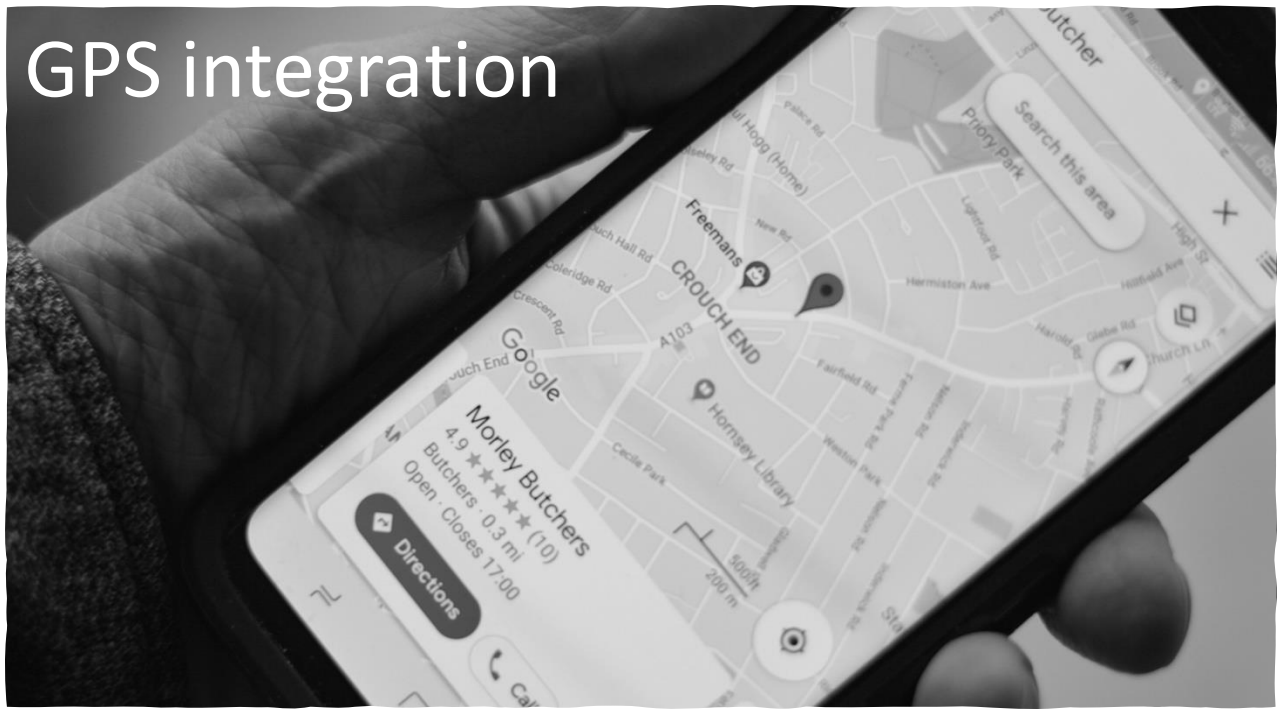
Trac Bannon

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

The Early Days


Digital Transition
Directions
Total Est. Time: 2 hours, 23 minutes
Total Est. Distance: 91.96 miles
1: Start out going EAST on CORTESE DR toward WEATHERBY RD.
3: Turn LEFT onto WEATHERBY RD.
3: Turn RIGHT onto ROSSMOOR WAY.
4: Turn LEFT onto LOS ALAMITOS BLVD.
5: Turn RIGHT onto KATELLA AVE.
6: Turn LEFT onto BEACH BLVD / CA-39 N.
7: Turn RIGHT onto W IMPERIAL HWY.
8: Turn LEFT onto S HARBOR BLVD / N HARBOR BLVD. Continue to follow S HARBOR BLVD.
9: S HARBOR BLVD becomes FULLERTON RD.
10: Turn RIGHT onto COLIMA RD.
11: Turn LEFT onto S NOGALES ST.
12: Turn RIGHT onto E VALLEY BLVD.
13: Merge onto CA-71 S.
Distance
0.7 miles
4.5 miles
8.5 miles
2.0 miles
3.8 miles
1.6 miles
0.9 miles
1.0 miles
7.4 miles
0.7 miles
15.3 miles
6.7 miles

Special GPS Units
tomtom
The GPS signal was lost
15 sec ago

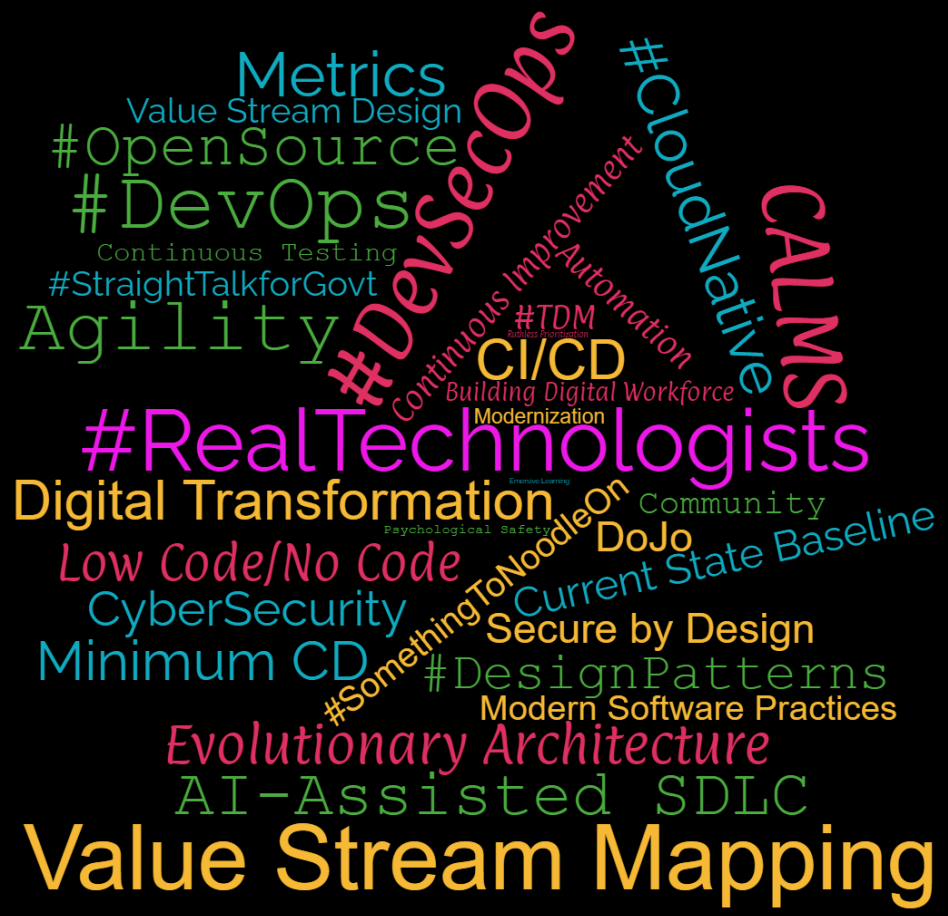

GPS integration
Search this area
Freemans
CROUCH END
Google
Morley Butchers
4.9 ★★★★★ (10)
Butchers · 0.3 mi
Open · Closes 17:00
Directions
Hornsey Library
Priory Park

AI & Software Engineering

Digital Transition: **This is where we are today.**

Who Am I? Tracy "Trac" Bannon

/trās/



vsm consortium
Influencer

AMBASSADOR
DevOps Institute
ADVANCING THE HUMANS OF DEVOPS

IEEE
SENIOR MEMBER

MITRE

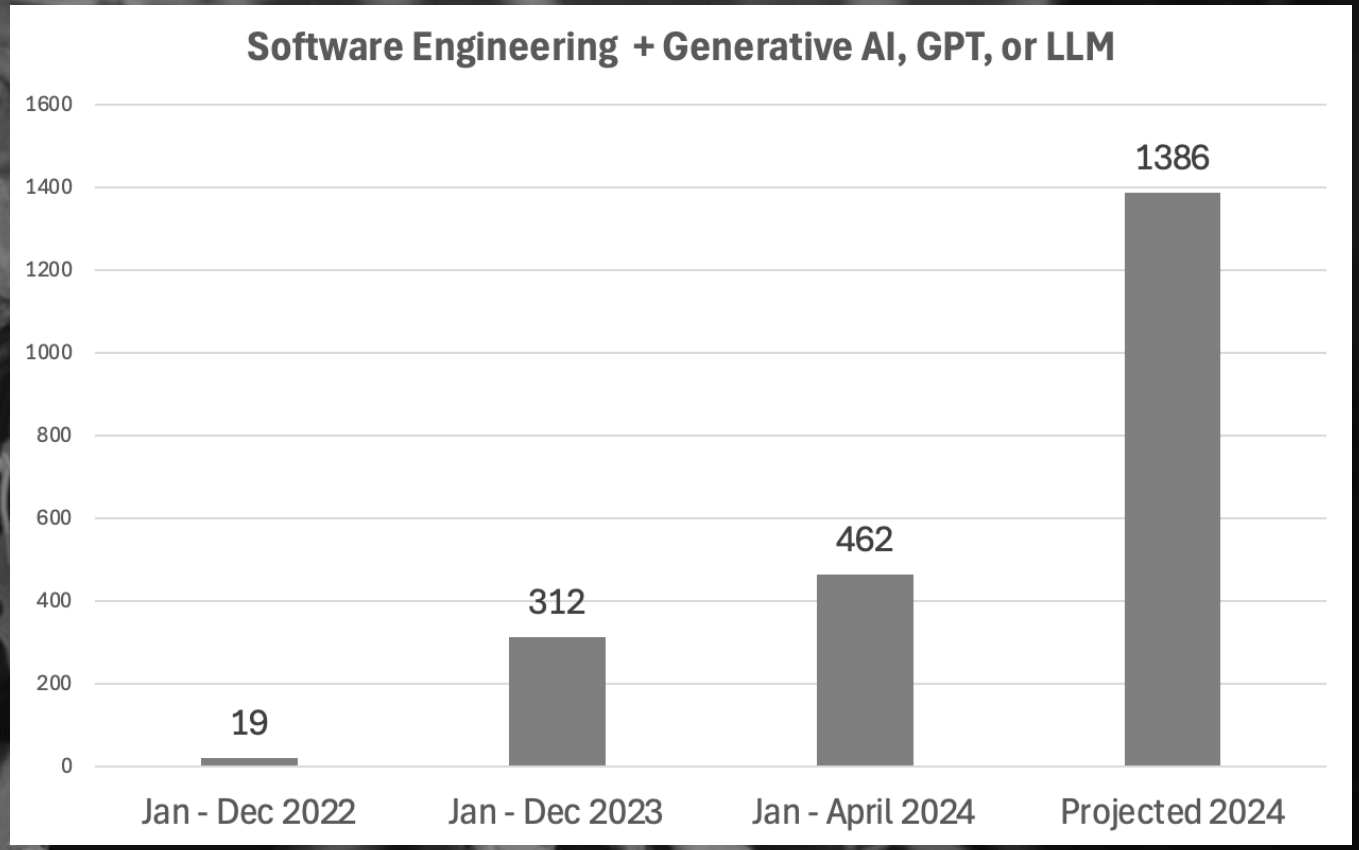
Software architect | researcher | engineer

ArchAITecture Research Collaborative

- Focusing on human/machine teaming and trust
- Diverse thought leaders
- Merging scholars and industry
- Data at scale
- Not-for-profit

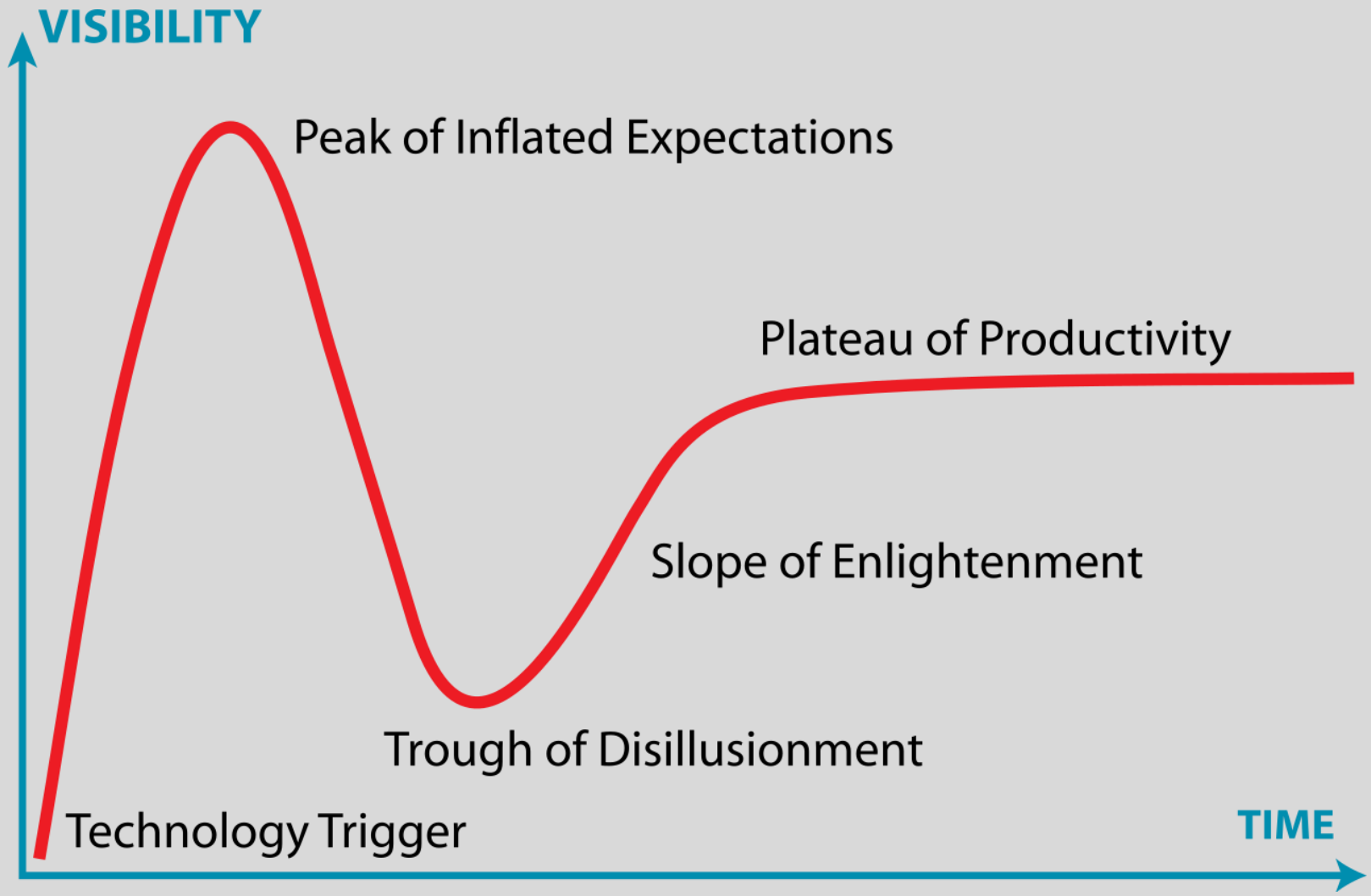
Quick Retrospective

- January 2023 - ChatGPT users hits 100M
- Chronic FOMO
- 2024 - Publishing surges
- Peer-reviewed research lags

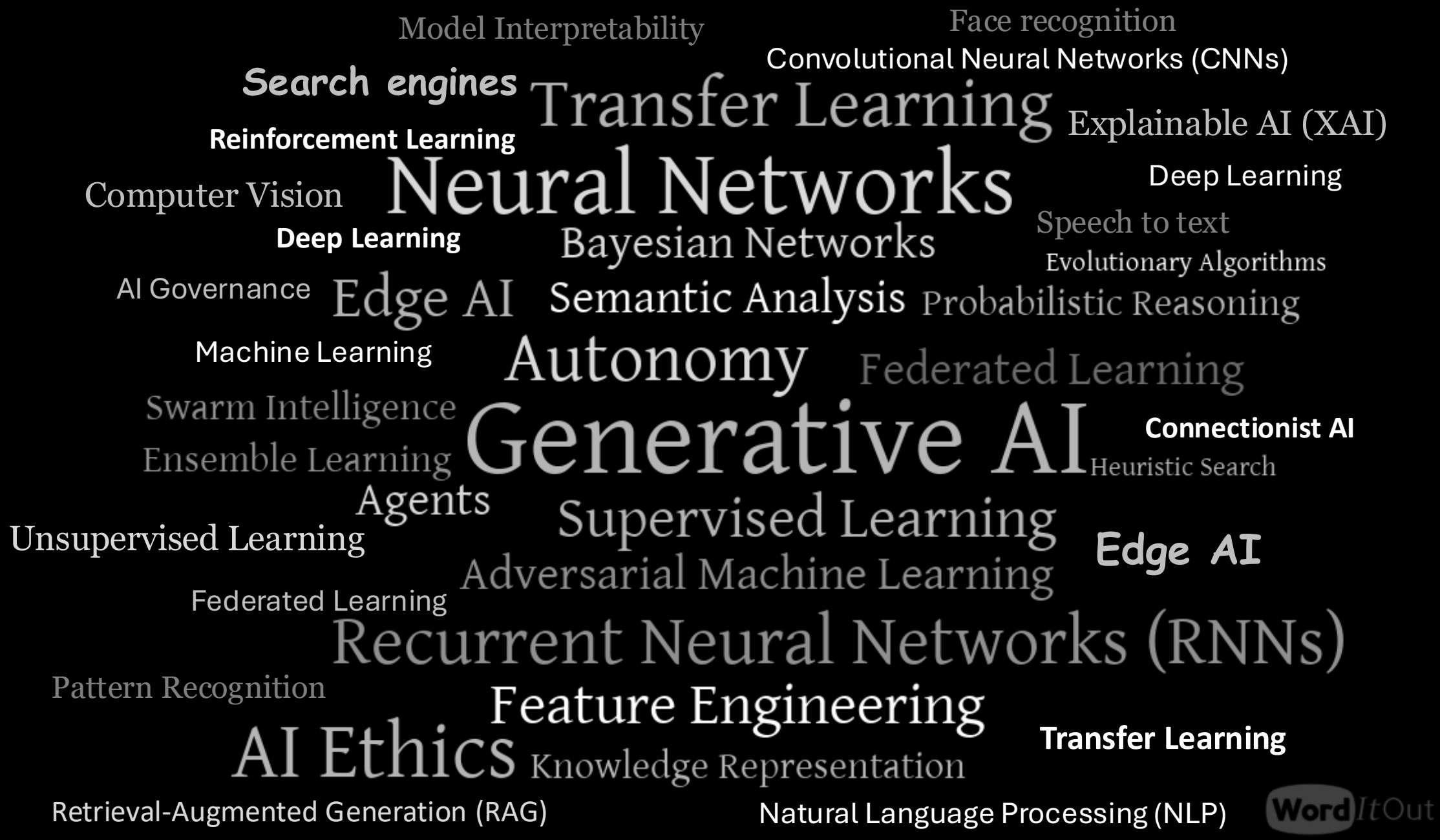


Don’t get swept away by the hype

AI in SwEngineering… where are we now?

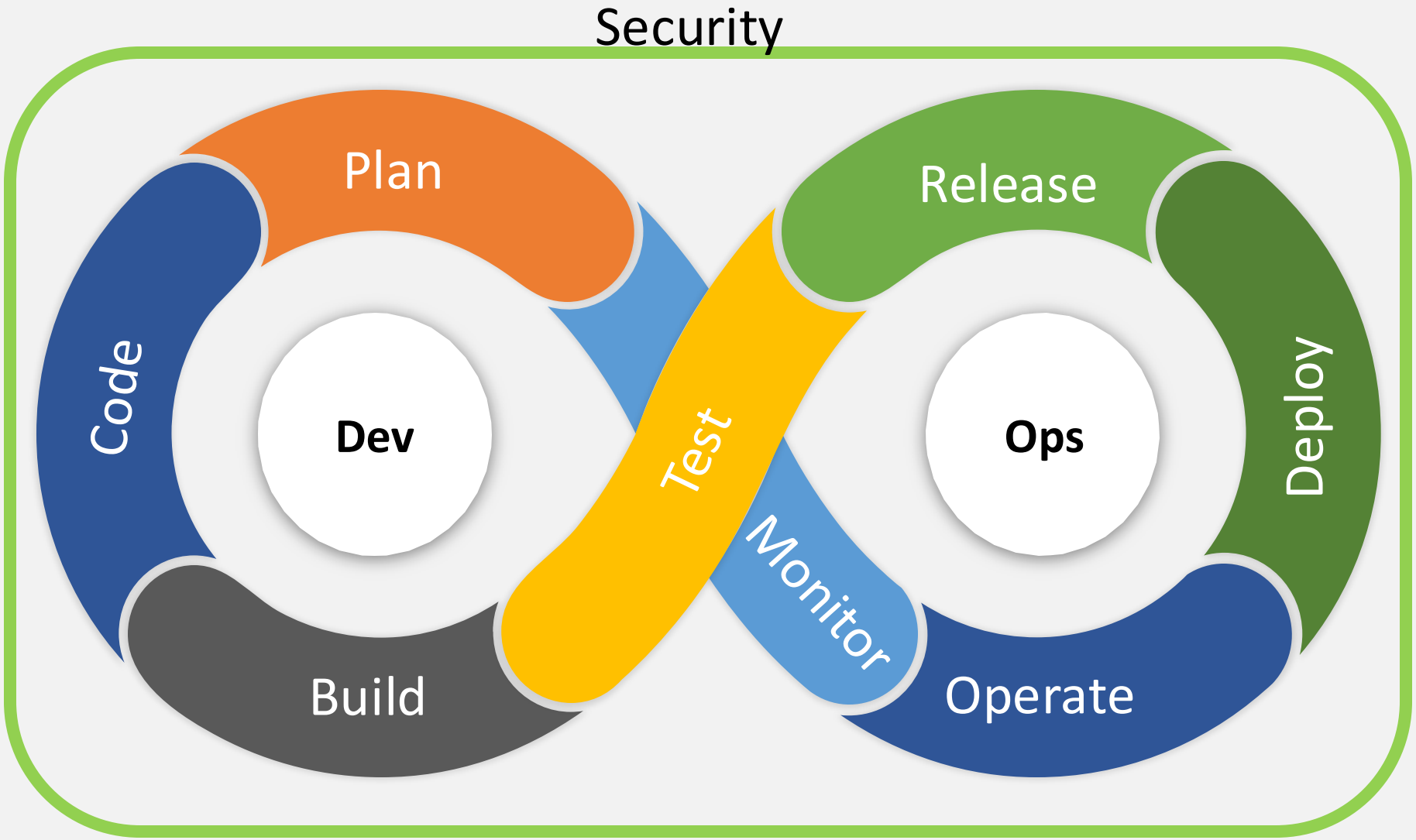


Internal Developer Portals
Machine Customers
GitOps
Prompt Engineering
Homomorphic Encryption
AI TRiSM
Federated Machine Learning
Reinforcement Learning
Artificial General Intelligence
Digital Immune System
Autonomous Agents
AI-Augmented Software Engineering
Superapps
Cloud-Native
WebAssembly
Generative AI
AI Supercomputing
6G
Multiagent Systems
Disinformation Security
Cybersecurity
Mesh Architecture
Digital Twin of a Customer
Spatial Computing
Humanoid Working Robots
Large Action Models
2 – 5 years to reach productivity plateau
EXPECTATIONS
As of August 2024
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
TIME



© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

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



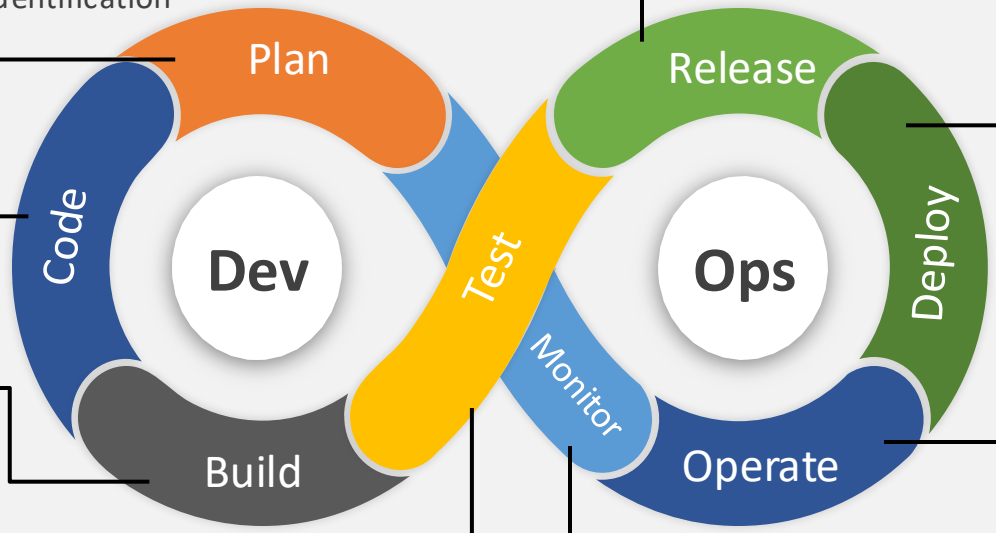
Infusing AI across the Dev*Sec*Ops Continuum

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
- ML Anomaly Detection
- GAI Deployment Scenario Simulations



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
- Intelligent Test Execution

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

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

GAI Usage Patterns

Content Generation

Complex auto-complete as well as new content creation is typically leveraged for generating test cases, code, documentation, and deployment scripts.

Automated Reasoning

Analyzing patterns, suggesting alternatives about code quality, identifying security vulnerabilities, optimizing deployment strategies, and ensuring compliance with standards.

Treat GAI like a young apprentice...

Always pay close attention!!

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

Does Generative AI contradict DevSecOps principles?

Where are people using GAI today?

- Searching for answers
- Documentation
- Requirements Analysis
- Debugging
- Code Completion
- Test Case Augmentation

Sources: 2023 & 2024 StackOverflow Developer Survey
TechStrong/Tricentis: AI-Augmented DevOps Report

Unveiling the Human Side of AI in Software Engineering

Practice-wide survey to get to ground truth

Human-Machine Collaboration

Trust Optimization

Skill Evolution & Team Communication

Personal Impact & Future Outlook

Take the Survey

Most challenging, time consuming, or painful tasks^

Challenge	%
Collaborating with cross-functional teams	50%
Managing technical debt	
Continuous integration/continuous deployment (CI/CD) pipeline setup	
Documentation (code, systems, APIs, etc.)	
Maintaining legacy code	
Maintaining security compliance	
[…]	
Code reviews	
Writing New Code	3%

Take the Survey

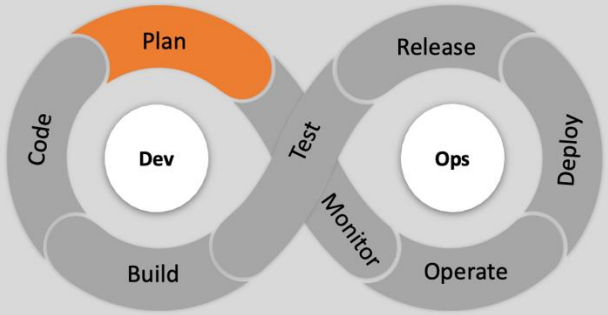
40+ different challenges have been identified so far!

^This data will be more insightful when correlated with role and experience

Are we addressing the pain points?

AI-Augmented

^ Requirements Analysis



Use Case:

- Requirements generation via text analysis
- Analyze user transcripts
- Include crowdsourced survey

Considerations:

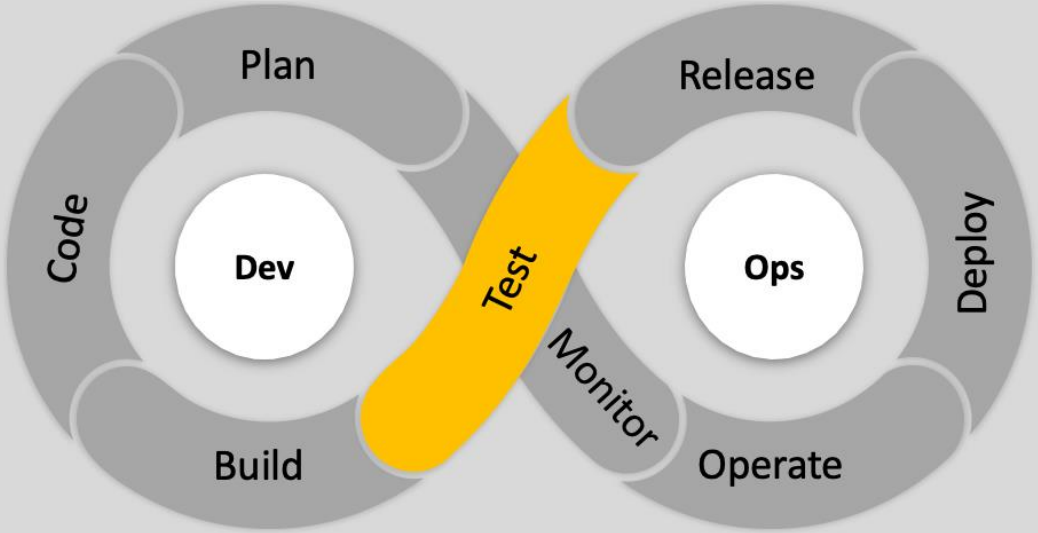
- Version control GPT prompts ++
- Diverse Datasets
- QA = rigorous testing + humans in the loop

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

AI-Augmented

^ Testing Use Cases

- Increase test coverage
- Brainstorming
- Synthetic Test Data Augmentation

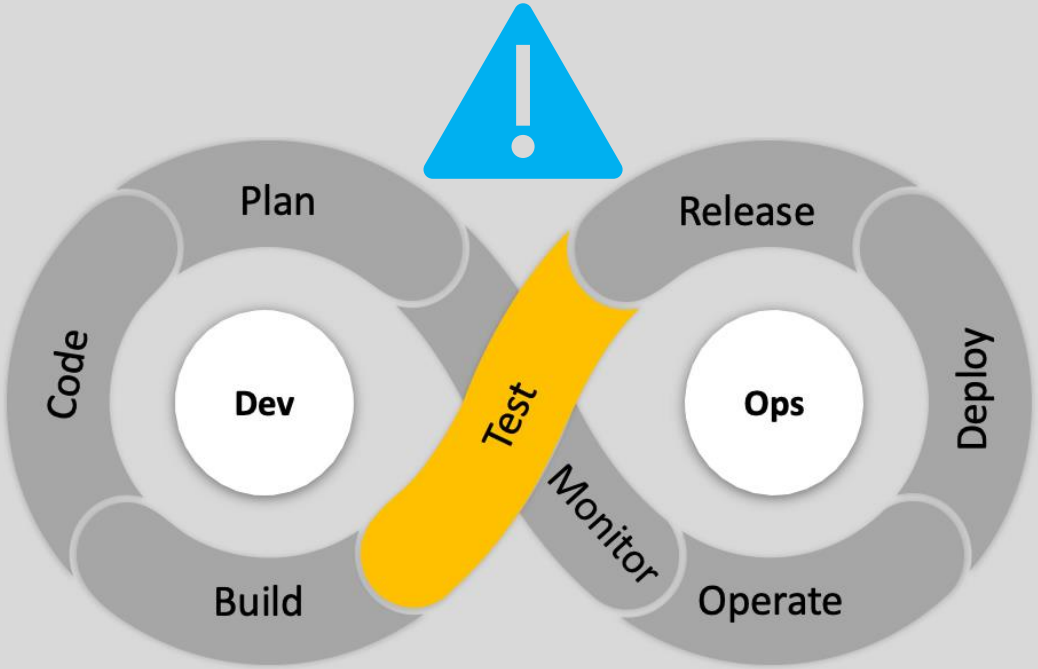


© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

AI-Augmented

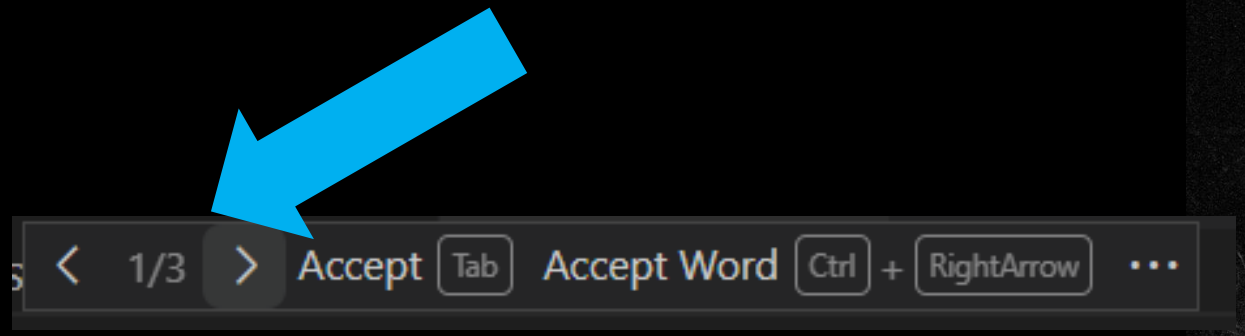
^ Testing Considerations

- Data Privacy & Integrity
- Beware of Irrelevant Tests
- Transparency and Explainability

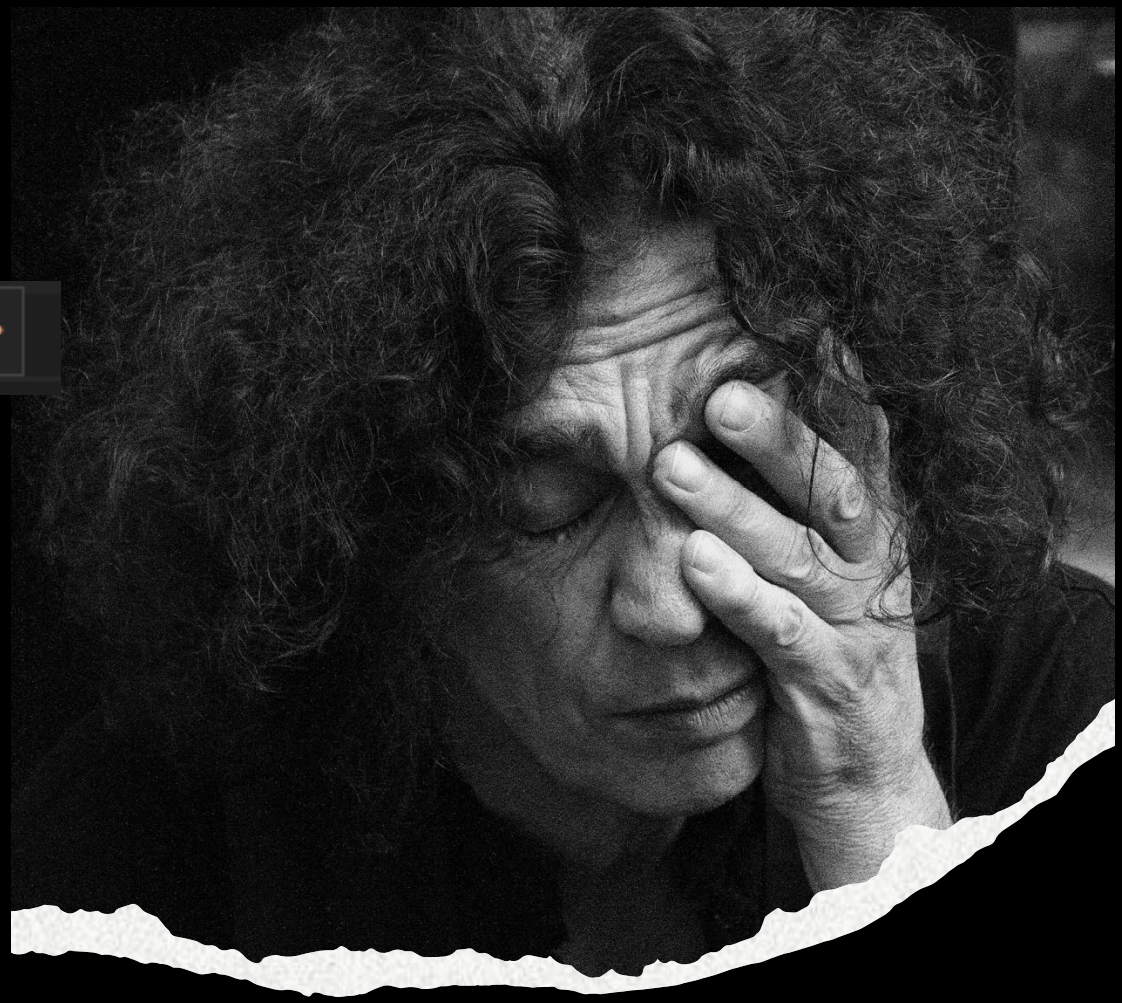


© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

In IDE Help




```python
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
```



© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

Don’t generate code and tests

- Lack of Independent Verification
- Bias and Blind Spots
- Overfitting

GAI can be unreliable.

Pay close attention!

Is your organization prepared?

Fix your SDLC first

- Address existing issues
- GAI can magnify existing problems

Gotchas to avoid

Adaptation to New Workflows

- Measurements and metrics will waiver
- Training is a must
- Humans resist change

What about productivity?

- Perceived productivity
- Team productivity *not* Individual productivity

The Importance of Context

- AI requires a massive corpus of data
- If you subscribe to a service, you must provide context
- Are you okay with sharing?

Keep Humans in the Loop!

Leading practices for today's AI-augmented SDLC

- Keep humans in the loop
- Everything in source control including prompts
- Secure your vulnerabilities
- Don't provide your private info/IP into public AI engines

Choose when and where to start

AI-Augmented

Designing Your ^ Software Engineering Tool Chain

Looking Ahead

The Evolving Role of Digital Platforms

- Making it hard for humans to make mistakes
- Codify leading practices
- ”Pro Code”
- The jumping off point for GAI-augmentation and future agentic capability

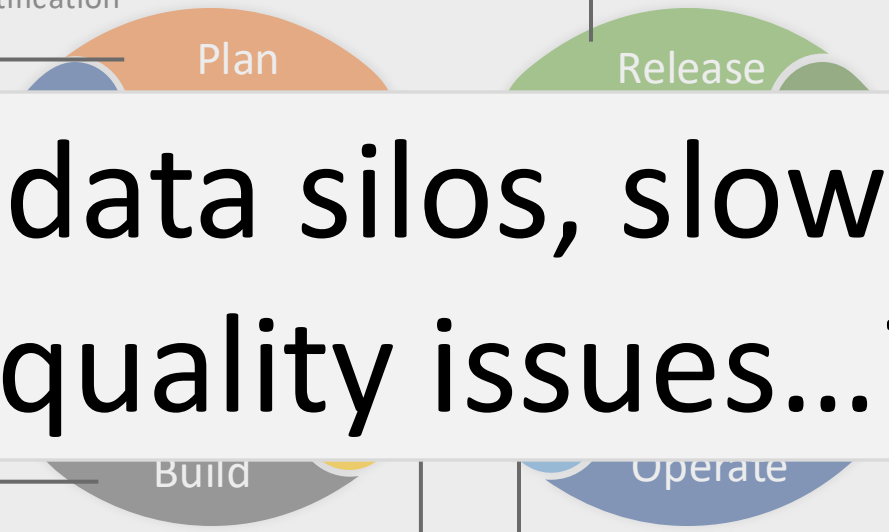
What does the SDLC look like over the next few years?

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 collabora
- Suggestive Refactori

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

- Dynamic Environment Provisioning and Deployment Optimization
- Realtime Rollback
- AI-assisted Log Aggregation
- ML Anomaly Detection
- GAI Deployment Scenario Simulations



Sec
Is in
acti

Build
- Aggregated Merge Rec 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
- Intelligent Test Execution

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

More data silos, slower flow, more quality issues…?

Jensen Huang
CEO@ NVIDIA

But what about this…

Is the future of coding dead?

When will AI-engineers join the team?

Scott Wu
CEO@ Cognition AI

AI/Human Teaming

Who will we optimize for? Humans? AI Agents?

We can’t put the genie back in the bottle

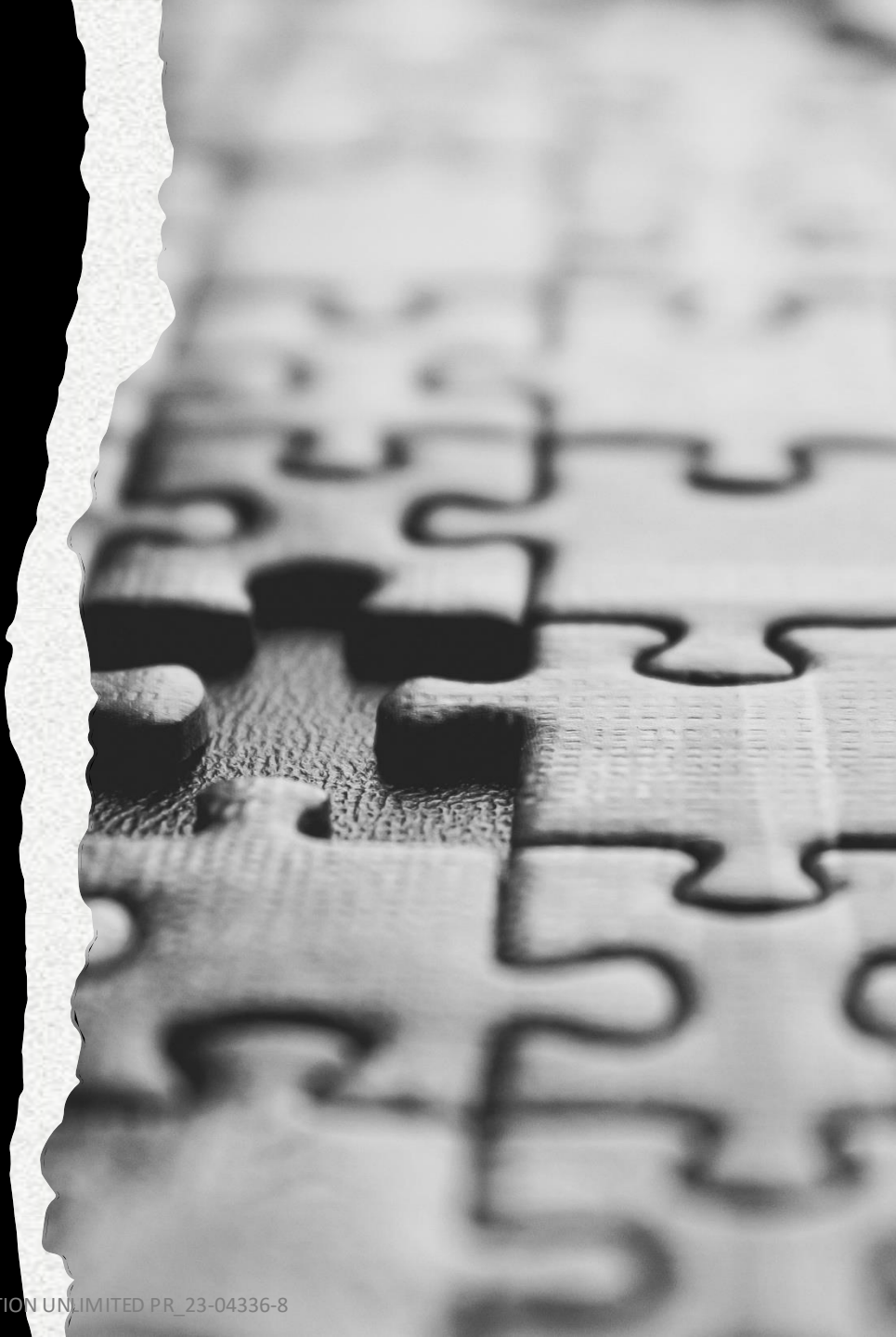
- Prompt engineering as a discipline
- Ethics of prompts
- Who owns the generated outcomes
- Human-Machine teaming
- Software team performance
- Trust and reliability in software outcomes

Call to Action – Your Next Steps

- Make Cybersecurity as your highest priority
- Enable research and discovery for GAI usage
- Establish on reasonable guardrails
- Ask your GAI providers about
  - model quality
  - security
  - roadmap

What I need from you...

- How do you think the SDLC will change?
- How is your organization preparing?
- What are you **personally** focusing on?
- Share your organization's story and lessons learned
- Share out new use cases and new tools



© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

What matters are the humans.

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

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

ADDO

ALL DAY DEVOPS

BY sonatype

OCTOBER 10, 2024

Image Attributions

Slide 2 –
Paper map photo by Jakob Owens on Unsplash
https://thevspotblog.com/2012/09/basic-emergency-supplies-for-car.html
GPS Unit photo by Brock Wegner on Unsplash
iPhone photo by henry perks on Unsplash → Validate

Slide 3- https://thevspotblog.com/2012/09/basic-emergency-supplies-for-car.html
Slide 6 – crowd surf photo by Karsten Winegeart on Unsplash
Slide 7 – Twister photo by Nikolas Noonan on Unsplash
Slide 8 -https://en.wikipedia.org/wiki/Gartner_hype_cycle#/media/File:Gartner_Hype_Cycle.svg
Slide 10 – 2024 Hype https://www.gartner.com/en/newsroom/press-releases/2024-08-21-gartner-2024-hype-cycle-for-emerging-technologies-highlights-developer-productivity-total-experience-ai-and-security
Slide 11 - DevOps Infinity Loop Inspired by SlideEgg
Slide 11 - DevOps Infinity Loop Inspired by SlideEgg
Slide 14 - Apprentice photo by Vance Osterhout on Unsplash
Slide 15 – One way sign photo by Brendan Church on Unsplash
Slide 16 –dipping Toes photo by Christopher Sardegna on Unsplash
Slide 17 – Team room photo by Arlington Research on Unsplash
Slide 23 – fatigue photo by brut carniollus on Unsplash
Slide 24 – Mirror Mirror photo by Milada Vigerova on Unsplash
Slide 25 – Apprentice photo by Vance Osterhout on Unsplash
Slide 27 – Beaver

- Slide 28 – Uh Oh photo by Ben White on Unsplash
- Slide 29 – Highway Interchange photo by John Lockwood on Unsplash
- Slide 30 – Crewing photo by Peter Pryharski on Unsplash
- Slide 31 – library emil-widlund-xrbbXIXAWY0 on Unsplash
- Slide 32 – Apprentice photo by Vance Osterhout on Unsplash
- Slide 34 – two paths diverge photo by Vladislav Babienko on Unsplash
- Slide 35 - photo by Emmanuel Boldo on Unsplash (tailor)
- Slide 35 - photo by Anthony Sebbo on Unsplash (off the rack)
- Slide 38 - Slide 16 - *DevOps Infinity Loop Inspired by SlideEgg*
- Slide 39 – Jensen Huang Image credit: Bloomberg via Getty Images
- Slide 39 – Scott Wu - Cognition AI
- Slide 47 – Generated with Getty's permission
- Slide 41 – Horse's end photo by Belinda Fewings on Unsplash
- Slide 42 – Runner photo by Nicolas Hoizey on Unsplash
- Slide 43 – Puzzle photo by Sigmund on Unsplash
- Slide 44– Apprentice photo by Vance Osterhout on Unsplash

MITRE

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-5

References

Academic Research, Industry Reports, Market Analysis

Given the extensive bibliography, the content has been moved to a separate file for readability and ease of use.

© 2024 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED PR_23-04336-8

MITRE