University of Maryland

Project Management Symposium

NEXT SESSION

Applying AI to DevSecOps Processes to Optimize Project Execution and Delivery

Andrew Boyle & Jason Baker

Distinguished Digital & Cyber Technologist, Booz Allen Hamilton
Chief Technologist & IT Program Manager

PROJECT MANAGEMENT
CENTER FOR EXCELLENCE
A.J. CLARK SCHOOL OF ENGINEERING
Civil & Environmental Engineering Department

This session will be recorded.

Project Management Symposium

AI-Enabled DevSecOps

Andy Boyle and Jason Baker

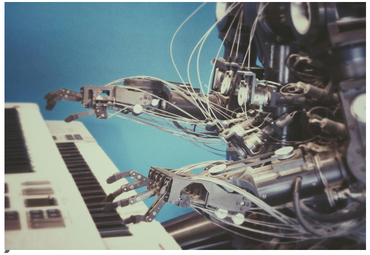
PROJECT MANAGEMENT
CENTER FOR EXCELLENCE
A.J. CLARK SCHOOL OF ENGINEERING
Civil & Environmental Engineering Department

Speaker bio: Andy Boyle

- Distinguished Digital and Cyber Technologist
- Leads projects developing analytic capabilities for Government and commercial clients
- DevSecOps industry expert
- 30+ years of technical PM experience
- University of Maryland College Park Alumni!

Speaker bio: Jason Baker

- Chief Technologist, IT Program Manager
- Experienced Geospatial Data Scientist with 15+ years in federal service
- Served on NGA AI working groups to guide agency adoption of AI/ML capabilities
- UC, Berkeley - M.S. Data Science

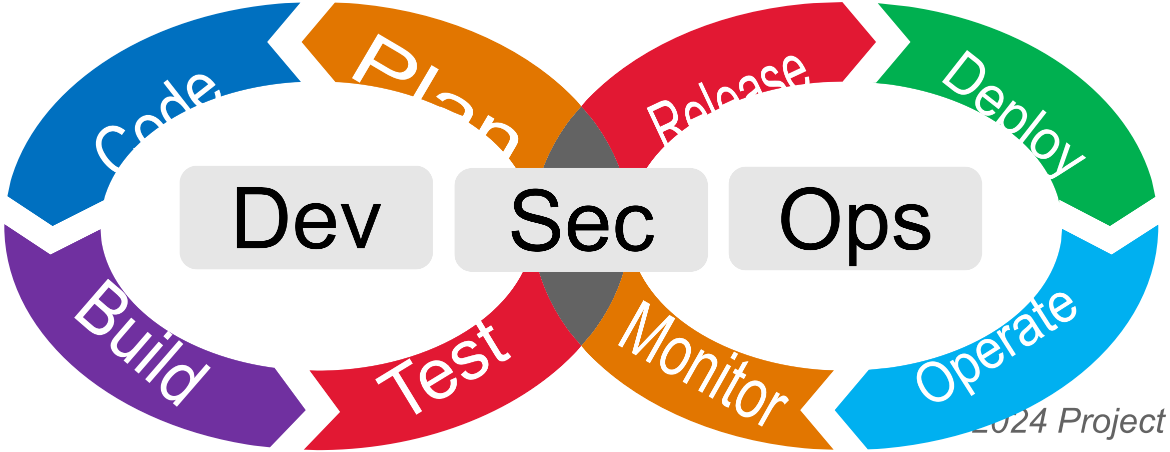


What is AI?

- Field of study (not one specific product or app revolving around making machines that can operate similarly to human intelligence
- Taking large amounts of data and using it to make future predictions
- Comprised of numerous sub-fields
  - Ex: Machine learning, natural language processing, computer vision

What is DevSecOps?

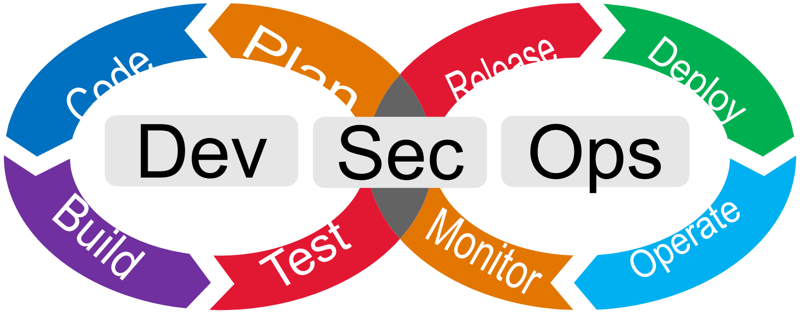
- Development + Security + Operations
- An approach to building software
- Security is integrated throughout the entire process



Why implement DevSecOps?

- Address Security Issues early
- Continuous Security Improvement
- Enable a collaborative approach

- Agility & Speed
- Risk Mitigation
- Automation



Quiz: Approximately what percentage of teams are using AI in DevSecOps?

A: 0%

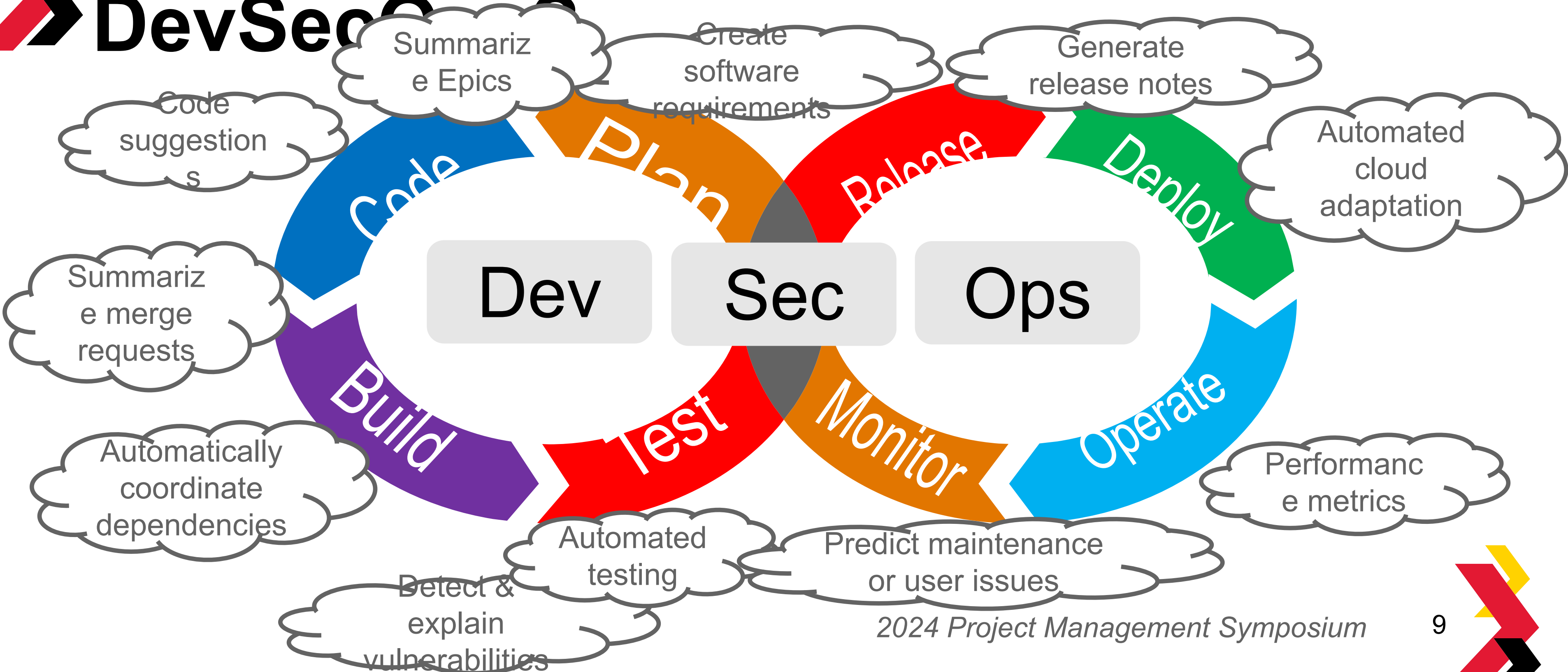
[✓ B: 25%]

C: 50%

D: 75%

According to a GitLab study, approximately 23% of teams currently use AI in DevSecOps. (GitLab)

Where can AI be applied to DevSecOps?



Specific uses of AI

- Developer uses Google Bard to write code
- PM uses ChatGPT to create system update messages
- Software lead uses Userdoc to create software requirements
- Developer uses Microsoft Security Copilot to run security checks while coding
- Manager uses GitLab Duo chat to explain chunk of

The benefits of AI are real

- Enhanced security
- Increased quality
- Decreased costs
- Actionable metrics
- Proactive system monitoring
- Lower risk
- Increased productivity
- Lower time

Quiz: What is the worldwide AI market size expected to reach this year?

A: $50B

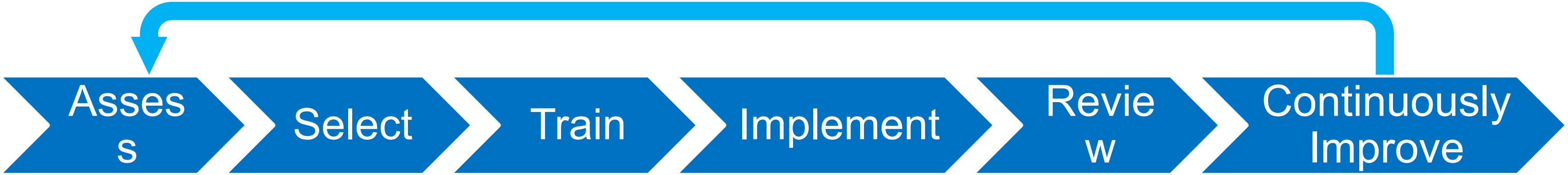
B: $100B

C: $200B

[✓ D: $300B]

The AI market size is expected to reach $305B this year, a $65B increase from last year. (Statista)

Follow AI-enabled DevSecOps processes



Asses s

Select

Train

Implement

Revie w

Continuously Improve

- **Assess** your current DevSecOps process
- **Select** the proper AI tool(s) to use
- Ensure all team members have proper AI **training**
- **Implement** AI into your DevSecOps process
- **Review** and **continuously improve** your use of AI

A new AI role is needed in DevSecOps

Experience Assurance

Security Compliance

Software Developer

AI Architect

Automation Architect

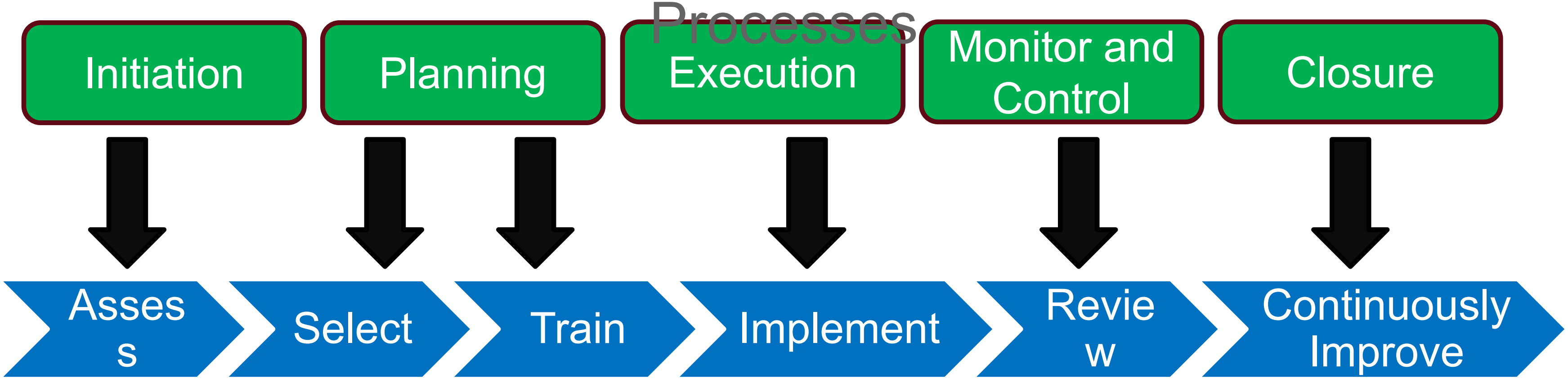
DevSecOps Engineer

Release Manager

Source: FinOps Personas by FinOps Foundation

PMs can drive the injection of AI into DevSecOps

PM Processes



Initiation

Planning

Execution

Monitor and Control

Closure

Asses
s

Select

Train

Implement

Revie
w

Continuously Improve

Processes to enable AI-powered DevSecOps

Quiz: What percentage of IT spending is expected to be allocated to AI by 2025?

A: 20%

B: 30%

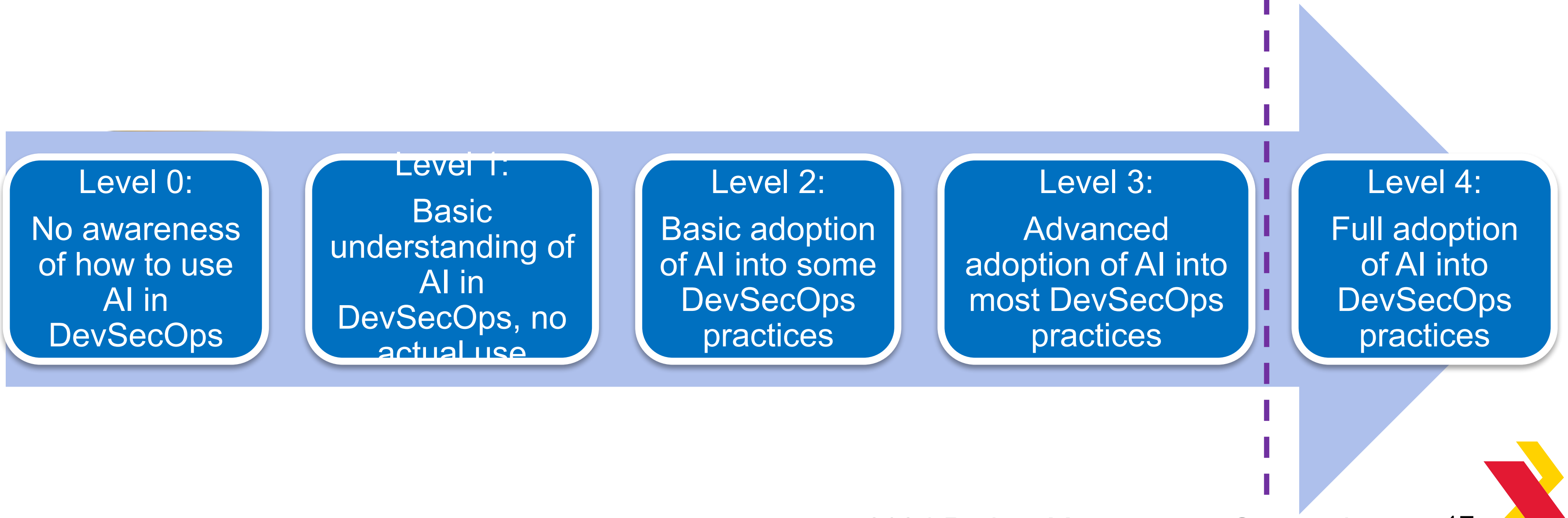
[✓ C: 40%]

D: 50%

IDC projects that corporations will devote 40% of their IT budget to AI-related tech by 2025. (IDC)

AI-enabled DevSecOps maturity levels

‘Eureka’ moment! Value greatly increases while costs taper off.



Level 0: No awareness of how to use AI in DevSecOps

Level 1: Basic understanding of AI in DevSecOps, no actual use

Level 2: Basic adoption of AI into some DevSecOps practices

Level 3: Advanced adoption of AI into most DevSecOps practices

Level 4: Full adoption of AI into DevSecOps practices

There is value in AI-enabled DevSecOps

- Results from a company-wide experiment[1]
  - 24% app delivery acceleration ⬆
  - 45% less time spent on security scanning ⬇
  - 18% decrease of incidents in production ⬇
  - 32% decrease of false-positive vulnerabilities ⬇
- 23% of teams currently use AI in DevSecOps[2]
  - Over 90% plan to in the future

Sources: (1) Schwenger
(2) GitLab

Case study

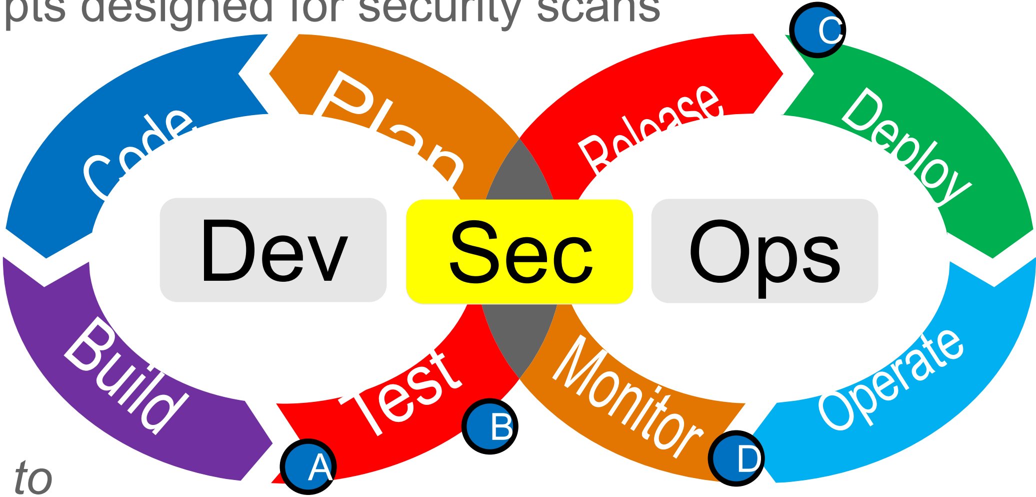
- Financial services company has DevSecOps troubles
  - Problems with custom scripts designed for security scans

A Identify false positives in security scans

B Analyze and prioritize security issues

C Issues are auto-delivered into Jira

D Create dashboards to report effectiveness of Dev teams



*Result: Significantly more **secure** DevSecOps cycle, allowing developers to efficiently **identify and fix security issues***

Source: Maverix

Best practices for organizational adoptions of AI-enabled DevSecOps

- Mandate training
- Follow policies and procedures
- Ease developer fears of losing jobs to AI
- Mitigate organizational concerns about AI
- Test, secure, govern
- Maintain control of data
- Start slow – You can always ramp up
- Start now – Don’t wait

Quiz: Among teams who use AI in DevSecOps, what is the top AI use case?

A: Bots to test code

[✓ B: Code checks (not testing)]

C: Summarizing epics

D: Suggesting merge requests

Using AI to check code (separate from testing it) is the current top use case of AI in DevSecOps. (GitLab)

Lessons learned from a PM perspective

Security first

Private data should stay private

Be aware of copyright

Don't ignore the human element

Watch out for biased datasets

Seek out expertise

Summary

- AI can be **integrated throughout** the DevSecOps cycle
- AI can **accelerate delivery**, make applications more **secure**, and increase developer **productivity**
- PMs can be the **driving force** behind getting AI implemented on their teams, but it can be wise to yield to an **expert** when it comes to specific uses

Questions?

Andy Boyle

Distinguished Digital and Cyber Technologist

Booz Allen Hamilton

boyle_andrew@bah.com

linkedin.co[illegible]yle-b74299

Jason Baker

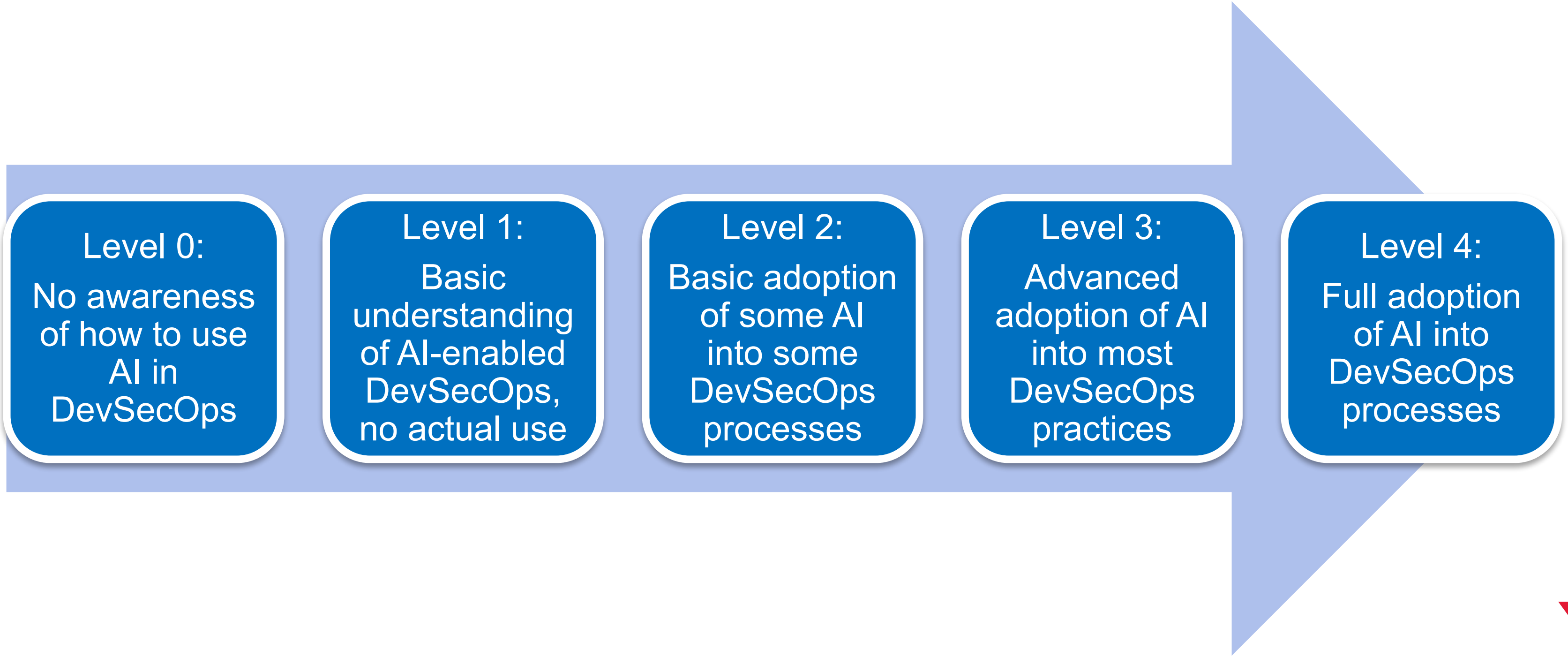
Chief Technologist, IT Program Manager

Booz Allen Hamilton

baker_jason3@bah.com

linkedin.com/in/jason-baker-8b640b3

AI-enabled DevSecOps maturity levels



Level 0: No awareness of how to use AI in DevSecOps

Level 1: Basic understanding of AI-enabled DevSecOps, no actual use

Level 2: Basic adoption of some AI into some DevSecOps processes

Level 3: Advanced adoption of AI into most DevSecOps practices

Level 4: Full adoption of AI into DevSecOps processes

Case study

- Booz Allen – GAMECHANG

GAMECHANGER
Evidence-Based Policy; Data-Driven Decisions

  - NLP and AI tool to navigate policy documents
  - 40,000 documents, 9,000 users, 140,000 queries
  - AI use case: Automated testing and data ingestion
  - AI use case: Model evaluation framework
  - AI use case: Collection of user data for continuous improvement

Evaluate Session