DevSecOps - An Ideal Use Case For Applying AI

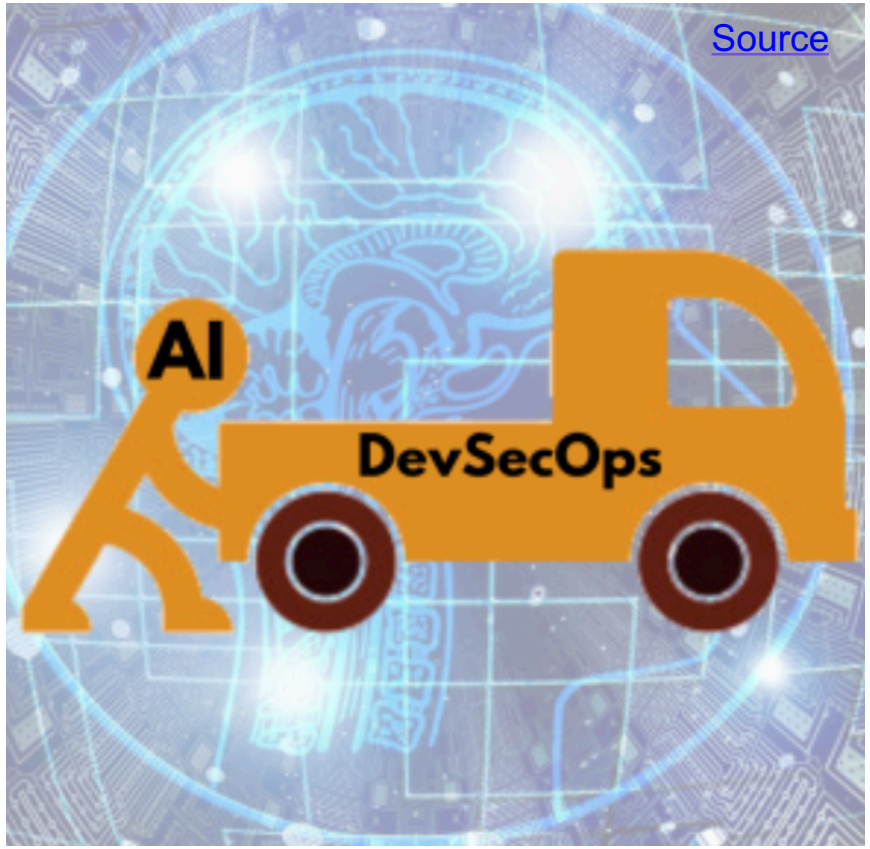
DEVOPS WORLD by CloudBees

DevSecOps Transformation

Maria N. Schwenger ,
AVP, Head of App Sec and Data Protection

Agenda

- Business drivers for AI in DevSecOps
- Technological use cases for AI in DevSecOps
- Our experiment and our results
- “Food for thoughts” for DevSecOps leaders and professionals



Acknowledgements and Disclaimers

- **No Affiliation** - All references to vendor's products, programs, or services in this presentation are made with no affiliation to any of the vendors or companies.
- **No Advisory** - The sessions and materials have been prepared by the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS-IS without warranty of any kind, express or implied. The speakers or their employer shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations
- **Examples/results shared** - All examples described are presented as illustrations of how companies have used certain products and the results they may have achieved. The actual results, such as environmental costs and performance characteristics may vary. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

About the Speaker

Maria N. Schwenger

Enterprise IT Security AVP -
Head of Cyber Security AppSec & Data Protection
American Family Insurance
mschweng@amfam.com | www.amfam.com

AMERICAN FAMILY INSURANCE®
Insure carefully, dream fearlessly.

1) **DevSecOps Expert** – proven success in building DevSecOps organizations from scratch

2) **Cloud Practitioner** (building frameworks and platforms - APIs/microservices, Cloud Native, managing complex SaaS offerings, migrating data and on-prem solutions to cloud, etc.).

3) Building **AI frameworks and platforms**

4) **Data Governance Leader** - skilled in working with very large databases/data stores (relational and NoSQL) and leading adoption of data stores on Cloud

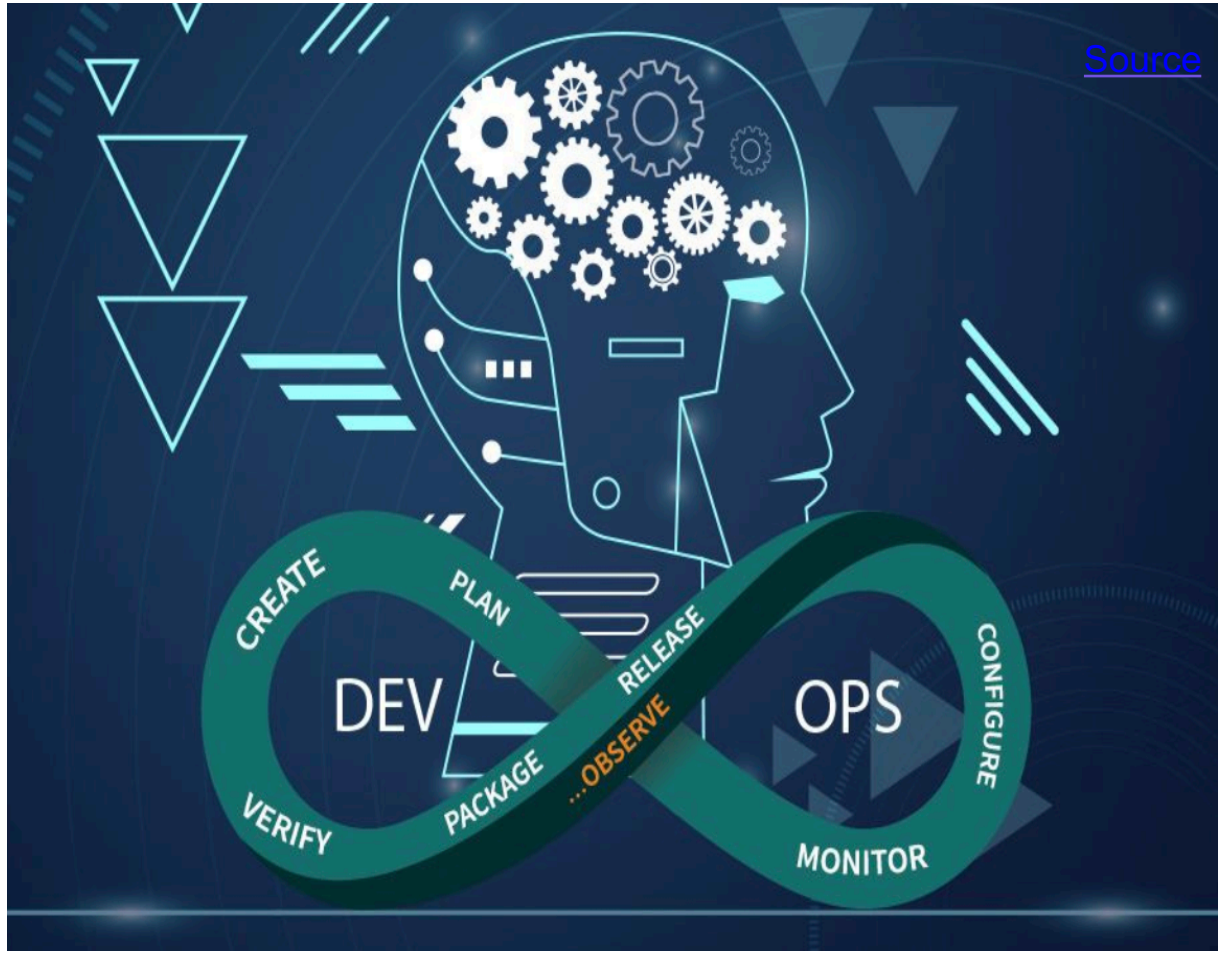
My Company

- Based in Madison, Wisconsin, and founded in 1927, American Family Insurance group is the nation's 13th-largest property/casualty insurance group, ranking No. 254 on the Fortune 500 list
- The group sells American Family-brand products, primarily through exclusive agency owners in 19 states
- The American Family Insurance group also include CONNECT, powered by American Family Insurance, The General, Homesite, and Main Street America

CONNECT POWERED BY AMERICAN FAMILY INSURANCE | THE GENERAL INSURANCE | Homesite | THE MAIN STREET AMERICA GROUP

Problem Statement

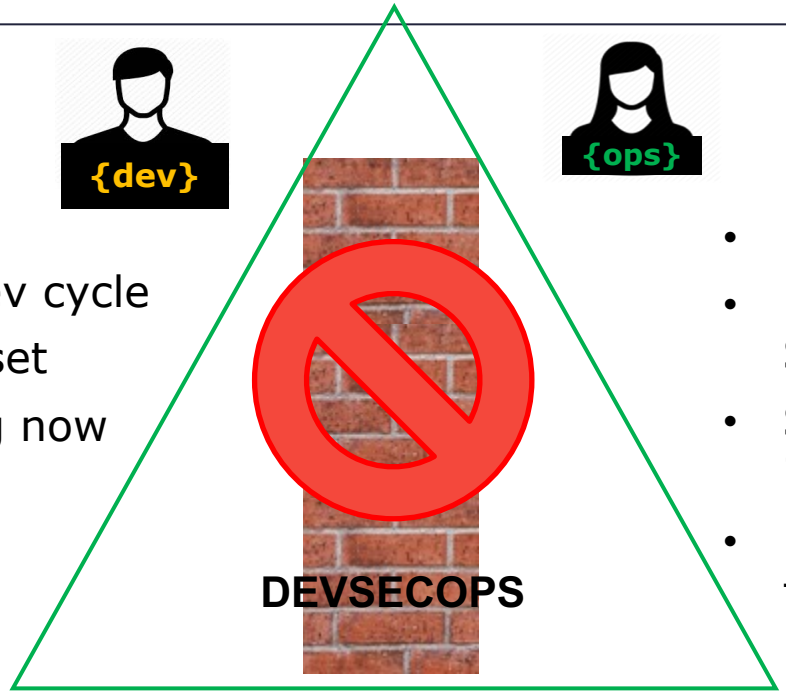
- Can AI drive the future of DevOps?
- What is the value of AI powered DevOps for agile software delivery?
- What are the best use cases to apply AI in DevOps?
- Can AI expand the human capabilities in the DevSecOps process?



The Main Actors – DevSecOps Collaboration with Agile

Developers (Agility)

- CI/CD adoption & standardization
- Tools consolidation throughout Dev cycle
- Single cloud and "on-prem" mindset
- Infrastructure automation starting now
- Real time metrics for DevOps
- Consolidated test framework



Operations (Stability)

- No hard handoffs between Dev & Ops
- Dev and Ops equality responsible for SLOs
- Starting to work on advanced infrastructure automation
- Baked-in security practices in Ops - tools, metrics and processes

All about process optimization and automation

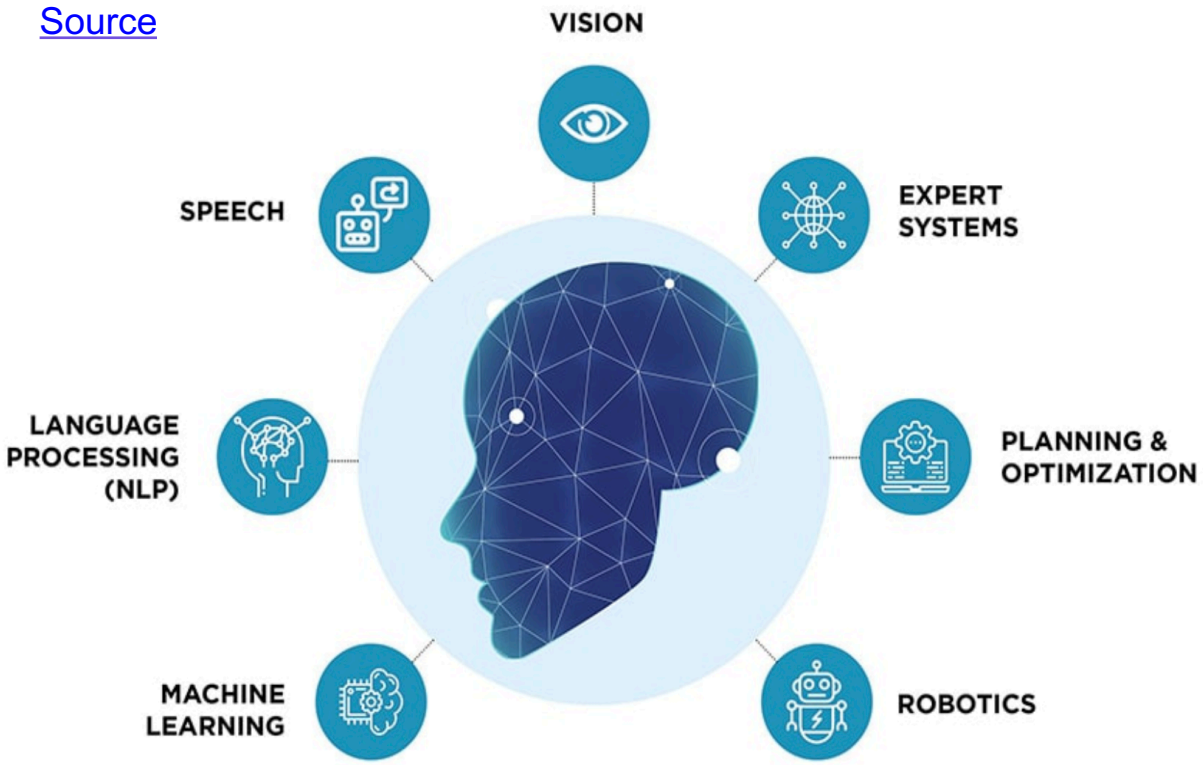
- "Shift Security left" within the DevOps cycle
- Secure engineering & risk awareness
- Security is part of unified test framework

Security (Awareness, Risk avoidance)

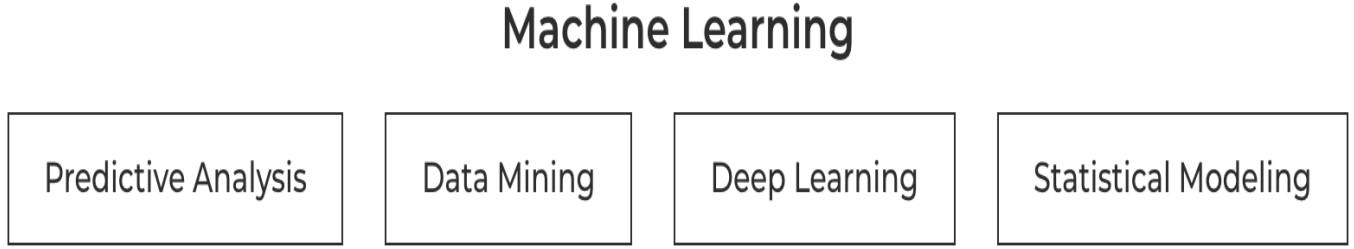
- Most MVPs include security & DevOps
- Going to Prod mandatory security scans
- Security monitoring for all environments

The Main Actors – Artificial & Machine Intelligence

Source



- **Artificial intelligence** - systems that allow computers to imitate human cognitive processes or perform tasks that used to be done by humans.
- **Machine intelligence** – a computer system enabled to learn proactively from inputs (rather than directed by linear programming) and after extracting various kinds of data (using machine learning and artificial intelligence) to establish its own processes and/or arrive at its own conclusions. (Source: Technopedia)



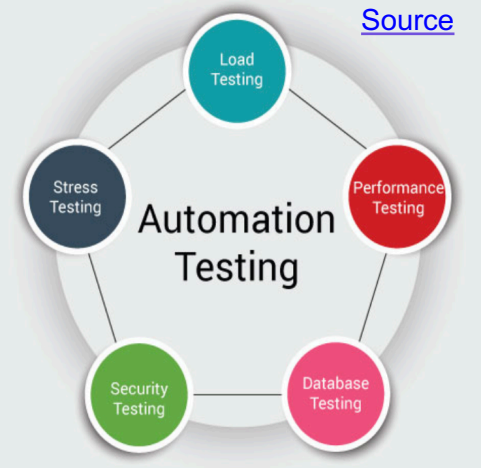
How AI and DevOps Are Interrelated?

DevSecOps Practices	AI Solution
Generating large amount of data (often in a short period of time)	AI is the best approach to analyze in depth large amounts of data collected in logs or by tools
DevSecOps rely on static workflows and passive orchestration	AI optimizes workflows and orchestration processes based on real time data
DevSecOps monitoring – looking for what “we already know” enabling reactive actions	AI helps searching for what we do not know and prepares us to be proactive rather than reactive
SecOps teams are looking for exceptions, issues, faults (out of normal)	AI can help analyze in depth the data and shows trends and forecasting
Rule-based automation in DevOps	Self-discovering and self-governing systems
Complex feedback loop based on heterogeneous sources and tools	Faster analysis of collected data and optimized feedback loop for correction/resolution in advance

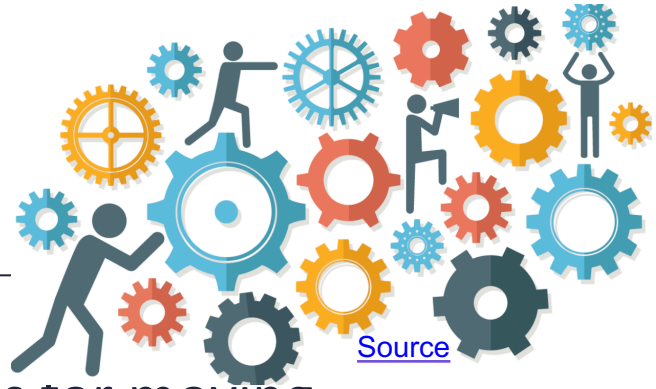
Most Common Use Cases

Automated software testing

- Defect identification
  - Finding potential issues before we kick the testing
  - Automated management of issues found in the testing process in ream time
  - Automated resolution of issues discovered in build, deployment, and testing
  - Automated documentation and easy auditing of issues
- Effective managing of QC and security testing bringing better development awareness, collaboration, and effectiveness
- Managing consistent configurations across all environments
- Simulated user-level test cases driven by AI



Most Common Use Cases


Source

Process optimization:

- Fine tuning of the Change Management processes and procedures for moving applications from Dev to Test to Prod environments leveraging historical data
- “Smart” management of code freeze and un-freeze
- Optimizing the Development cycle and providing proper planning based on data from delivery history of previous projects
- Alert Management – Prioritizing response/time and assigning alerts to proper teams based on factors such as past behavior, source of the alerts, and volume
- Automated compliance checks across applications/integrations, vendors, and environments

Most Common Use Cases

Automation of routine tasks within the CI/CD workflows:

- Capturing information on build failure/success and generating and assigning automated alerts to all stakeholders; Orchestrating complex pipelines
- Automated classification and root cause analysis of build/deployment data
- Using predictive analytics to flag potential areas of concern for future builds
- Assignment of bug fixes and issues to the proper people, based on build/commit/deploy data (even from previous projects)
- Embedding security testing within the DevOps cycle
- Optimize and secure “Infrastructure as code” concepts (repeatability/security)

Most Common Use Cases

Improved Collaboration

- Facilitate a continues feedback loops by proactively identifying potential and real issues early on and making recommendations to address timely
- Facilitate more effective collaboration between the Dev, Sec, and Ops teams
- Automatic posting of issues and tagging proper people in various collaboration tools (e.g., Slack)
- Data correlation across platform and tools by analyzing data streams from various heterogeneous systems and tools to find correlations and create a holistic view of new deployments, production issues, or application's health
- Personality awareness for team building and interactions

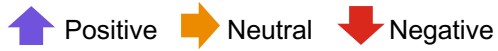
But, the biggest impact is in using AI/ML to automate software testing, defect identification, and integration.

Our Experiment - Starting Points

- AI can play a crucial role in accelerating DevOps efficiency
  - AI is changing how DevSecOps teams work (develop, deliver, deploy and test applications) for improved performance, security, and operations
- Start looking on a new way at the traditional DevSecOps metrics & tasks
  - Increase the efficiencies across the development, testing, security, and operational life cycles
- Create New DevSecOps metrics & tasks based on the AI/ML capabilities
  - Innovate and explore new ways to improve the productivity

Our Experiment – Results

Color Legend:



- Accelerated application delivery by up to 24%
- Improved maintenance times – unchanged
- Decreased number of alerts handled by developers with 57%
- Decreased number of incidents in production up to18%
- Decreased the time for running automated security scans by 45%
- Decreased the number of False-positive vulnerabilities by 32%
- Improved Promoting to Staging environment by 62%

How Can You Do It?

Source

- Keep investing in strong DevSecOps infrastructure
- Identify your DevSecOps targets to improve
- Start with simple tasks to gain experience and prove initial value
- Make sure you have the ML expertise you need
- Check out the Open Source Community to lower the entry barrier
  - e.g., Fabric for Deep Learning (FfDL) and Model Asset eXchange (MAX)
- Watch which vendors provides AI in DevSecOps tools “out of the box”

THANK YOU!