PeopleCert

DevOps Institute
A member of the PeopleCert Group

DEVOPS DAYS 2023 CAIRO

## DevOpsDays Cairo Conference 2023 Program

### "AI for DevOps Transformation"

**Location:** Creativa in Giza
**Date:** 27 September, 2023
**Time:** 5:00 pm to 10:30 pm

**Ad Satour**
Senior Solutions Architect

### "The Impact of AI on DevSecOps"

**Keynote: Abdelahad Satour - PeopleCert**

05:30 pm 06:00 pm

https://devopsdays.org/events/2023-cairo

www.ad-satour.com/do2023


## Abdelahad SATOUR

hello@ad-satour.com


Sr. Solutions Architect
x 54 IT Certifications

DevOps Institute Ambassador
PeopleCert Ambassdor
DeepLearning.AI Event Ambassador

ad-satour.com
satour.medium.com
github.com/asatour
linkedin.com/in/adsatour

- CEO/CTO for 13 years and as Solution Architect.
- Founded 4 companies: 2 startups and 2 digital services companies.
- Managed more than 30 projects and 20 consulting missions. With teams of different sizes.
- Delivered over 80 technical trainings and 12 seminars.

# Agenda

From debunking myths to exploring buzzy topics and diving deeper

01
**Myths vs. Reality**

02
**DevSecOps Pipeline**

03
**AI Dimensions**

04
**Buzzy Topics Unveiled**

05
**AI-DevSecOps**

06
**Diving Deeper**

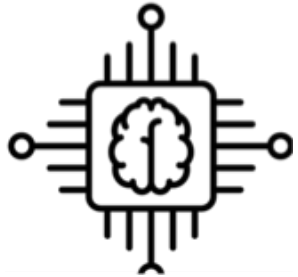
# 1. Myths vs. Reality

A Deep Dive into Contemporary Topics

# 1. Myths vs. Reality

A Deep Dive into Contemporary Topics

- **AI Can Replace Human Security Experts**:
  - **Myth**: AI tools and algorithms can handle all security needs, making human experts obsolete.
  - **Reality**: While AI can enhance and streamline many processes, human intuition, judgment, and expertise remain essential. AI should be seen as augmenting human capabilities, not replacing them.
- **AI Guarantees Flawless Security**:
  - **Myth**: Once AI is integrated into DevSecOps, systems become impervious to breaches.
  - **Reality**: No system can guarantee 100% security. AI can strengthen defenses and detection, but vulnerabilities and potential breaches will always be a concern.
- **DevSecOps With AI Is Too Complex For Most Teams**:
  - **Myth**: Implementing AI into DevSecOps requires a massive team of AI experts and is not feasible for most organizations.
  - **Reality**: Many off-the-shelf tools and cloud solutions (from AWS, Azure, GCP) make it simpler for DevSecOps teams to integrate AI capabilities without needing deep AI expertise.
- **AI Will Slow Down the DevSecOps Process**:
  - **Myth**: Incorporating AI will add overhead, slowing down the CI/CD pipeline.
  - **Reality**: When properly integrated, AI can automate and streamline numerous processes, potentially speeding up the DevSecOps lifecycle.



# 1. Myths vs. Reality

A Deep Dive into Contemporary Topics

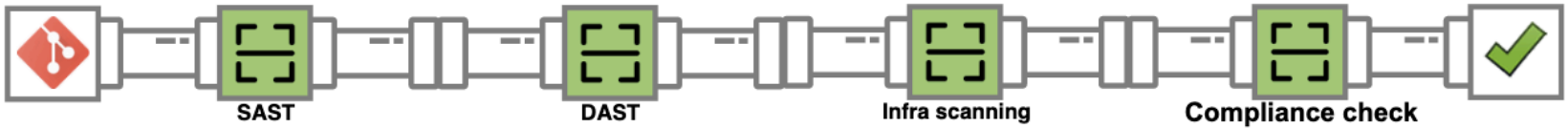
- **Data Privacy Isn't a Concern With AI in DevSecOps**:
  - **Myth**: AI tools that analyze code or infrastructure for vulnerabilities don't pose a data privacy risk.
  - **Reality**: AI tools often require access to vast amounts of data. Ensuring this data is handled securely and in compliance with privacy regulations is crucial.
- **AI Integration is a One-Time Task**:
  - **Myth**: Once you integrate AI into your DevSecOps processes, you're done.
  - **Reality**: AI models and tools require continuous training and updating to address new threats and vulnerabilities. Integration is an ongoing effort.
- **Only Large Organizations Benefit from AI in DevSecOps**:
  - **Myth**: Small and medium-sized businesses won't see the benefits of integrating AI with DevSecOps.
  - **Reality**: Even smaller teams can benefit from enhanced automation, threat detection, and other AI-driven capabilities.
- **Every DevSecOps Tool Needs AI**:
  - **Myth**: To stay competitive, every tool and process in the DevSecOps pipeline should incorporate AI.
  - **Reality**: While AI can provide significant benefits in many areas, not every process or tool will benefit from AI integration. It's essential to evaluate the real needs and potential benefits critically.

# 2. DevSecOps Pipeline

Building a Responsive DevSecOps Model

# 2. DevSecOps Pipeline

## Building a Responsive DevSecOps Model




**SAST**
- Static Application Security Test

**DAST**
- Dynamic Application Security Test

**IaC**
- Infrastructure scanning

**CaC**
- Compliance check and SaC

The AppSec Pipeline project is a place to gather together information, techniques and tools to create your own AppSec Pipeline.

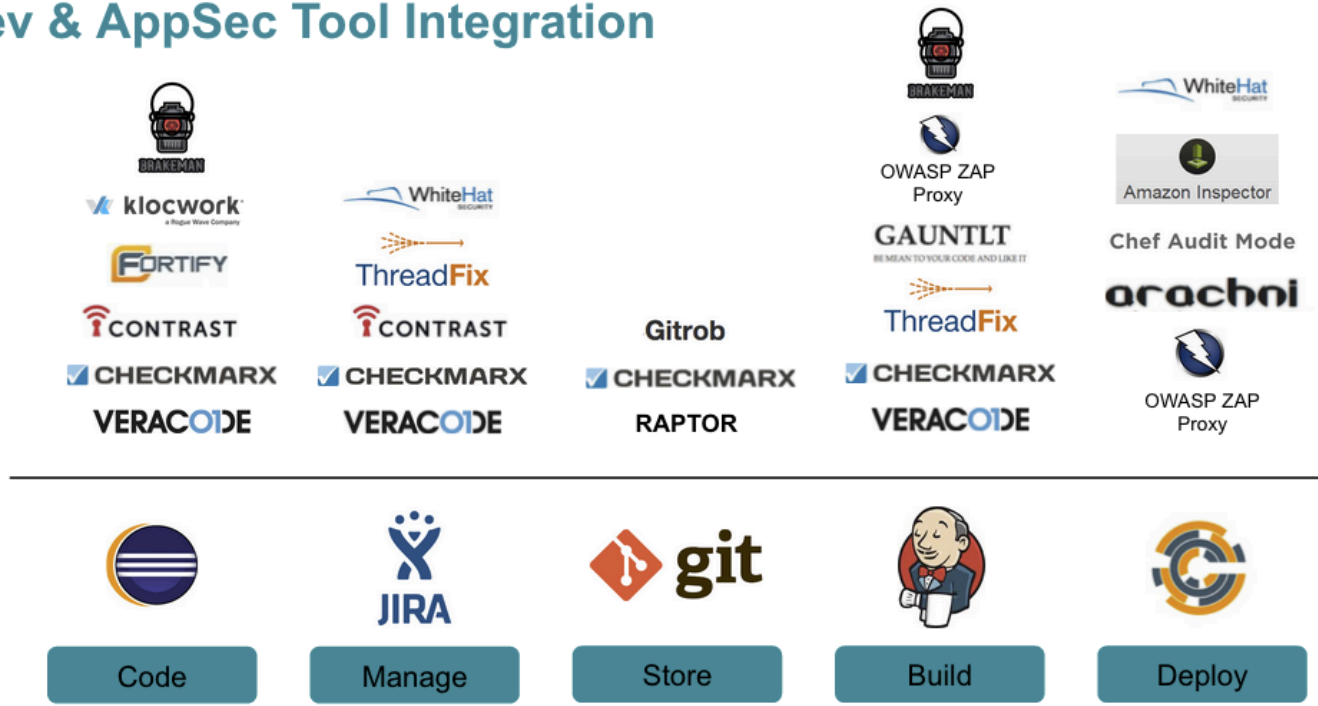
**AppSec Pipeline Toolbox**

https://www.appsecpipeline.org

# 2. DevSecOps Pipeline

Building a Responsive DevSecOps Model

## Dev & AppSec Tool Integration



# 2. DevSecOps Pipeline

## Leading DevSecOps Pipeline Tools and Solutions


### Leading DevSecOps Pipelines

- Deloitte
- Aqua
- GSA Tech Guide
- PS&C Group
- ServiceNow
- CloudBees
- Sonatype
- …

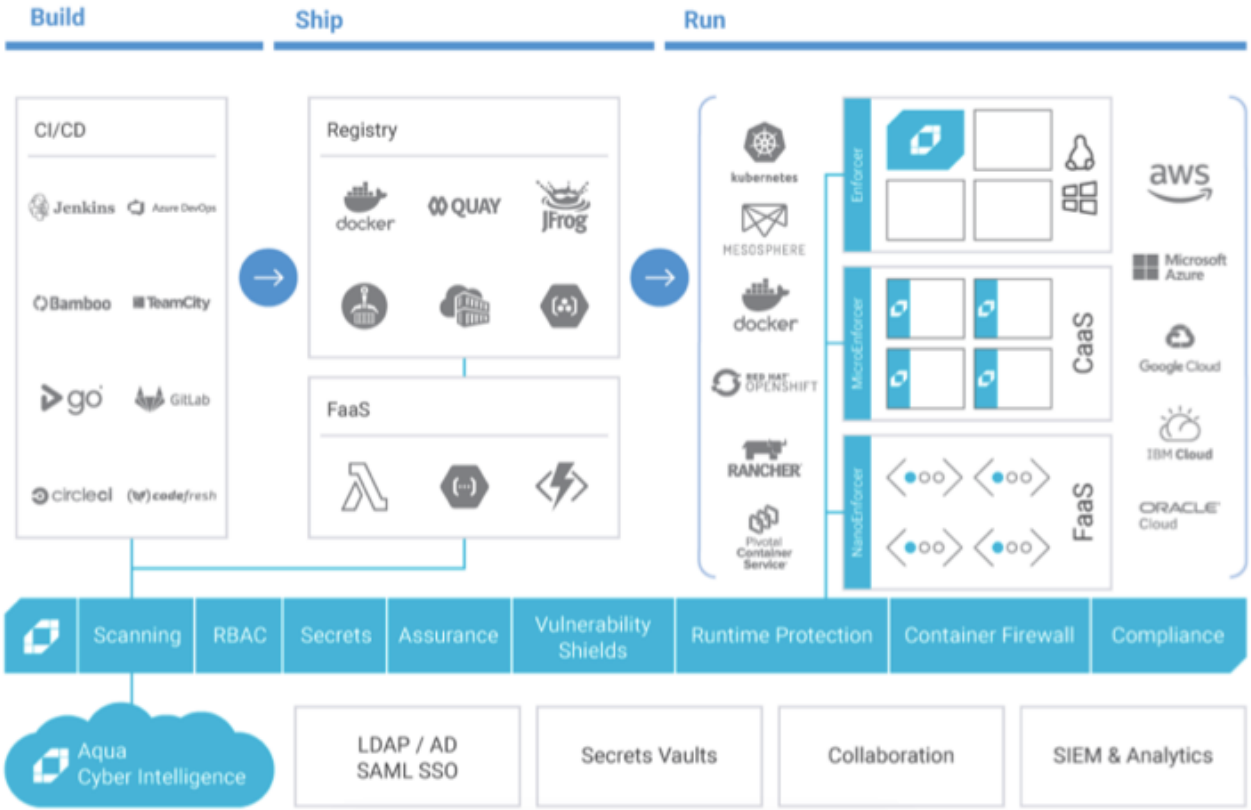
# 2. DevSecOps Pipeline

Leading DevSecOps Pipeline Tools and Solutions: Sonatype: DevSecOps Reference Architectures

| | Integration Points and Degree of Automation | | | | |
|---|---|---|---|---|---|
| DevSecOpsTooling | Design | Development (IDE) | Repository Manager | CI/CD | Post-Deployment |
| Open source governance | ● | ● | ● | ● | ● |
| Open source software analysis | ● | ● | ● | ● | n/a |
| Static Application Security Testing (SAST) | ● | ● | ● | ● | n/a |
| Dynamic Application Security Testing (DAST) | ● | n/a | n/a | n/a | ◔ |
| Interactive Application Security Testing (IAST) | ● | n/a | n/a | ● | n/a |
| Mobile Application Security Testing (MAST) | ◐ | n/a | ◐ | ◐ | n/a |
| Run-time Application Self Protection (RASP) | n/a | n/a | n/a | ◐ | ● |
| Container and Infrastructure Security | ◐ | n/a | ● | ● | ● |

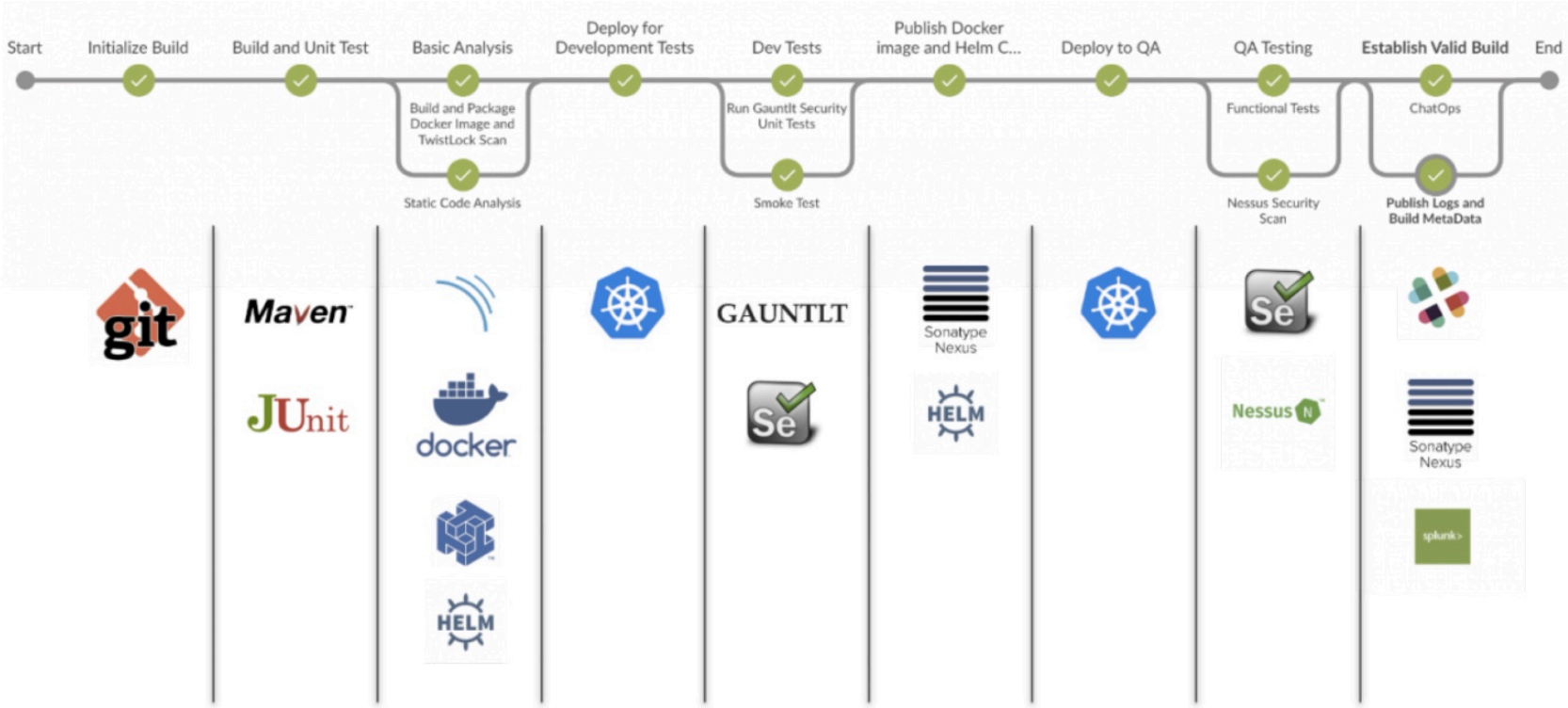
# 2. DevSecOps Pipeline

Leading DevSecOps Pipeline Tools and Solutions: Aqua : A DevSecOps Guide by Aqua



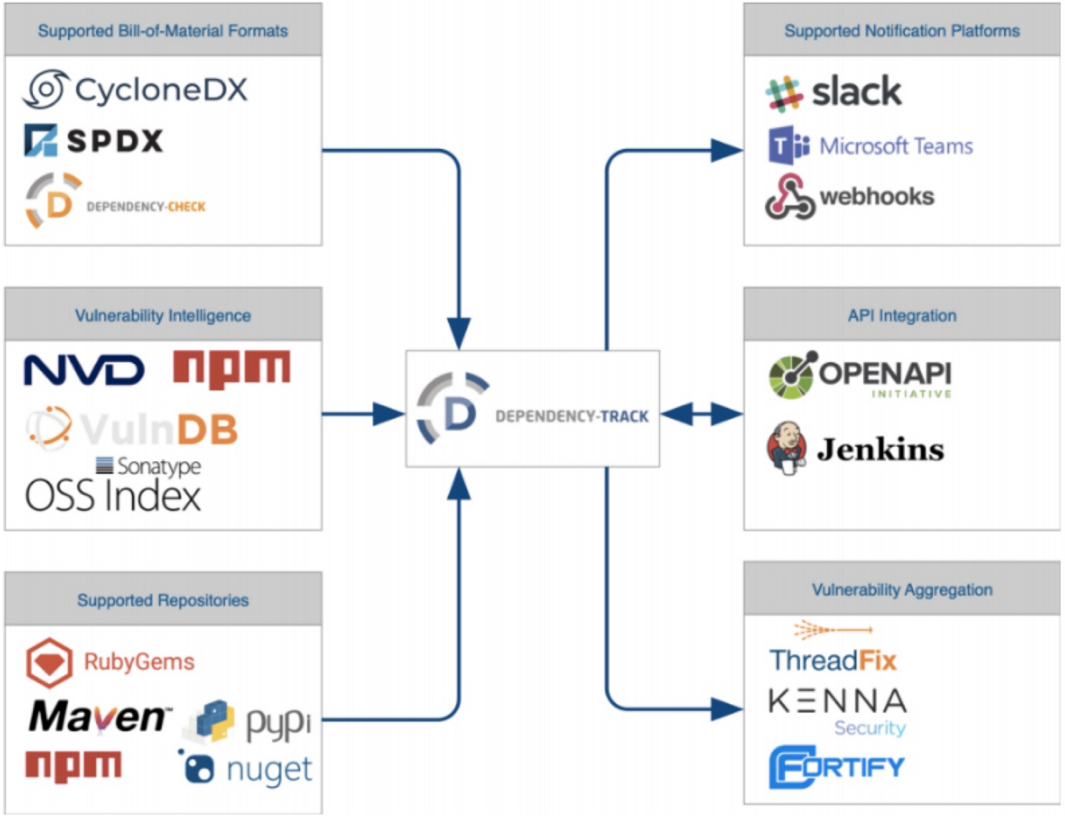
# 2. DevSecOps Pipeline

Leading DevSecOps Pipeline Tools and Solutions: DevSecOps according to Ben Chicoski and CloudBees



# 2. DevSecOps Pipeline

Leading DevSecOps Pipeline Tools and Solutions: DevSecOps according to Steve Springett and ServiceNow



# 3. AI Dimensions

5 Pillars or the ways we categorize and characterize AI

# 3. AI Dimensions

Pillars or the ways we categorize and characterize AI

1. Based on Capabilities
2. Based on Functionality
3. Based on Learning
4. By Approach
5. Applications in Different Fields

# 3. AI Dimensions

Pillars or the ways we categorize and characterize AI

## 1. Based on Capabilities:

a) **Narrow or Weak AI**: Specializes in one task. Examples include chatbots or image recognition systems.

b) **General or Strong AI**: Systems that can perform any intellectual task that a human being can. This is still theoretical and has not yet been achieved.

c) **Superintelligent AI**: AI that surpasses the smartest human brains in practically every field, including creativity, general wisdom, and social intelligence.

# 3. AI Dimensions

Pillars or the ways we categorize and characterize AI

## 2. Based on Functionality:

a) **Reactive Machines**: These AIs respond to specific inputs with specific outputs, without using past data as a reference. For example, IBM's Deep Blue.

b) **Limited Memory**: Uses historical data to make decisions. Most machine learning, including deep learning applications, falls into this category.

c) **Theory of Mind**: This is a hypothetical AI stage where the machine can attribute beliefs, desires, intentions, etc., to something or someone. It understands entities and emotions.

d) **Self-aware AI**: AI that has its own consciousness and emotions, which is still a speculative idea.

# 3. AI Dimensions

Pillars or the ways we categorize and characterize AI

### 3. Based on Learning:

a) **Supervised Learning**: Algorithms are trained on labeled data.

b) **Unsupervised Learning**: Algorithms are trained on unlabeled data.

c) **Semi-supervised Learning**: Uses both labeled and unlabeled data.

d) **Reinforcement Learning**: The model learns by interacting with an environment and receiving feedback in the form of rewards or penalties.

# 3. AI Dimensions

Pillars or the ways we categorize and characterize AI

**4. By Approach:**

a) **Symbolic**: Based on symbols and rules to solve problems.

b) **Connectionist (Neural Networks)**: Uses neural networks, especially deep learning, to process information.

c) **Evolutionary**: Uses algorithms that mimic the process of natural selection.

d) **Bayesian**: Uses probability and statistics to make predictions.

e) **Analogizers**: Uses analogies to recognize patterns (e.g., Support Vector Machines).

# 3. AI Dimensions

Pillars or the ways we categorize and characterize AI

**5. Applications in Different Fields:**

a) **Natural Language Processing (NLP)**: Understanding and generating human language.

b) **Computer Vision**: Enables machines to interpret and make decisions based on visual data.

c) **Robotics**: Building robots that can interact with their environment.

d) **Expert Systems**: Mimicking the decision-making abilities of a human expert.

# 4. Buzzy Topics Unveiled

Delving into Key Trends that Integrate AI with DevSecOps

# 4. Buzzy Topics Unveiled

## Delving into Key Trends: Integrating AI with DevSecOps

### AppSec

Application Security (often termed AppSec) involves securing software applications from threats. Tools like **OWASP Zap** and standards like **OWASP Top 10** guide professionals in this area.

### AiOps

It stands for Artificial Intelligence for IT Operations. Platforms like **Moogsoft** use AI to automate and enhance IT operations.

### LowCode/NoCode

Platforms like **OutSystems** (LowCode) and **Appy Pie** (NoCode) allow for application development with minimal coding, accelerating development

### GitOps

A Git-based workflow for continuous deployment. Tools like **ArgoCD** and **Flux** support GitOps practices.

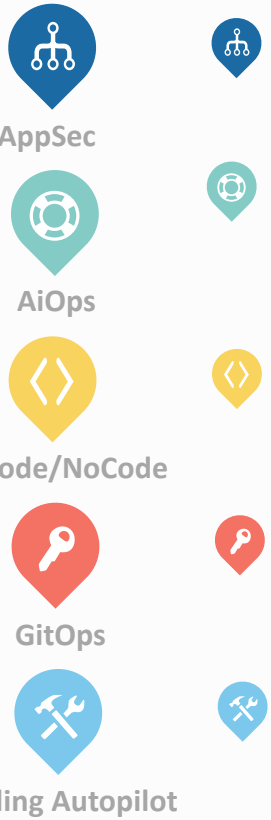
### Coding Autopilot

Autopilot coding uses AI to automate parts of software development. It provides real-time code suggestions and corrections based on developer intent..

# 4. Buzzy Topics Unveiled

## Delving into Key Trends: Integrating AI with DevSecOps Pipeline

*Train yourself by filling the DevSecOps Table with the trending concepts*




| | Integration Points and Degree of Automation | | | | |
|---|---|---|---|---|---|
| DevSecOpsTooling | Design | Development (IDE) | Repository Manager | CI/CD | Post-Deployment |
| Open source governance | ● | ● | ● | ● | ● |
| Open source software analysis | ● | ● | ● | ● | ● |
| Static Application Security Testing (SAST) | ● | ● | ● | ● | |
| Dynamic Application Security Testing (DAST) | ● | n/a | n/a | n/a | ◔ |
| Interactive Application Security Testing (IAST) | ● | n/a | n/a | ● | n/a |
| Mobile Application Security Testing (MAST) | ◐ | n/a | ◐ | ◐ | n/a |
| Run-time Application Self Protection (RASP) | n/a | n/a | n/a | ◐ | |
| Container and Infrastructure Security | ◐ | n/a | ● | ● | ● |

# 5. AI-DevSecOps

How AI Can Enhance and Streamline DevSecOps Processes

# 5. AI-DevSecOps

How AI Can Enhance and Streamline DevSecOps Processes

## 1. Infrastructure Monitoring

AI can monitor the health and behavior of individual containers or microservices.

## 2. Behavioral Analysis

AI can monitor user and network behavior to detect anomalies, potentially identifying breaches faster than traditional methods.

## 3. Adversarial Attacks

While AI brings many benefits, it's not a silver bullet. There's the potential for false positives, and AI models themselves can be targets for attacks. Plus, an over-reliance on AI might lead to complacency.

## 4. Predictive Analysis

AI can analyze past security breaches or vulnerabilities to predict and prevent future threats..

## 5. Continuous Learning

As more data is collected, AI models can continuously learn and adapt, enhancing security measures over time.

## 6. Integration with CI/CD

As code moves through a CI/CD pipeline, AI tools can automatically test the code, ensuring vulnerabilities are caught early.

## 7. Automated Threat Detection

Using AI to detect vulnerabilities in code automatically, reducing human errors and speeding up the detection process.

# 6. Diving Deeper

AI-DevSecOps: A Thorough Investigation into Common Beliefs

# 6. Diving Deeper

## 6.1 Infrastructure Monitoring

### Business Case

**Snapchat** uses Google Cloud's monitoring tools to oversee their vast infrastructure, ensuring optimal performance.

### Impact

Improved user experience due to reduced buffering times, leading to higher subscription retention.

### Financial Benefits

Minimized potential costs of data breaches; improved efficiency reduced manual review hours.

### Trend

Increased adoption of LowCode and NoCode platforms for rapid application development.

### Project Size

**Big**, given the intricate infrastructure of major e-commerce platforms.

### Complexity

**Small:** Quicker troubleshooting of infrastructure issues.

**Medium**: Improved game uptime, leading to happier users.

**Big:** Increased in-game purchases due to a smoother gaming experience.

### Cloud Solutions

**AWS CloudWatch, Azure Monitor, GCP's Stackdriver.**



### Technical Aspects

- **Containers & Microservices:** Monitoring solutions like **Datadog**, **New Relic**, and **Sysdig** can be integrated with AI to monitor container health and behaviors more effectively.

### Containers & Microservices



# 6. Diving Deeper

## 6.2 Behavioral Analysis

### Business Case

**Samsung SDS** uses behavioral analysis on GCP to detect unusual activities in their cloud infrastructure.

### Impact

Prevention of potential IP theft, safeguarding business secrets.

### Financial Benefits

Minimized potential costs of data breaches; improved efficiency reduced manual review hours.

### Trend

Rise in UBA (User Behavior Analytics) tools integrated into SIEM platforms.

### Project Size

**Small to Medium**, as startups may not have vast networks but still value their intellectual property.

### Complexity

**Small:** Minimized downtime, ensuring smooth operations.

**Medium:** Retained customer trust by ensuring site availability during key periods.

**Big:** Preserved millions in revenue that could've been lost during the attack.

### Cloud Solutions

**AWS GuardDuty, Azure Advanced Threat Protection, GCP's Chronicle.**

Amazon GuardDuty

Advanced Threat Protection

Chronicle

### Technical Aspects

- **Network Traffic Monitoring: Darktrace** uses machine learning to detect unusual network behavior.
- **User Behavior Analytics (UBA) :** Tools like **Exabeam** and **Splunk UBA** employ machine learning to profile standard user behaviors and highlight anomalies.

### Network Traffic Monitoring

DARKTRACE

### User Behavior Analytics (UBA)

exabeam

# 6. Diving Deeper

## 6.3 Challenges - Adversarial Attacks & Model Transparency

### Business Case

**OpenAI** (while not strictly a business) is researching robustness against adversarial attacks and often utilizes cloud platforms for its experiments.

### Impact

Ensuring robust AI models prevents potential revenue loss due to manipulated models making incorrect decisions.

### Financial Benefits

Transparent decision-making ensured regulatory compliance.

### Trend

Emphasis on Explainable AI (XAI) in sectors like finance and healthcare.

### Project Size

**Big**, given the scale and complexity of ML models in large tech companies.

### Complexity

**Small:** Improved stakeholder understanding of AI decisions.

**Medium:** Reduced potential legal challenges by ensuring AI transparency.

**Big:** Ensured adherence to strict healthcare regulations, avoiding hefty fines.

### Cloud Solutions

All three providers offer AI services (like **AWS SageMaker**, **Azure Machine Learning**, **GCP's AI Platform**) which can be configured for robustness against adversarial attacks.

Amazon SageMaker | Google AI Platform | Azure Machine Learning

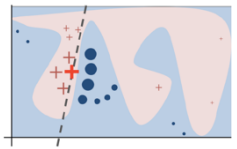
### Technical Aspects

- **Adversarial Attacks**: Adversarial machine learning is a rising field with many academic papers and research but lacks commercial tools. However, **IBM's Adversarial Robustness Toolbox** is one of the tools designed to help defend ML models against adversarial attacks.
- **Model Transparency: LIME (Local Interpretable Model-Agnostic Explanations)** and **SHAP (SHapley Additive exPlanations)** are methods/tools to explain the output of any ML model.

#### Adversarial Attacks

Adversarial Robustness Toolbox

#### Model Transparency



SHAP

# 6. Diving Deeper

## 6.4 Predictive Analysis

### Business Case

**GE Aviation** migrated to Azure and utilized its predictive analytics to anticipate equipment failures.


### Impact

By preemptively addressing issues, companies can avoid costly downtimes and deliver a consistent user experience, leading to sustained customer trust.

### Financial Benefits

Identified and patched three critical vulnerabilities before public disclosure.

### Trend

AI-driven threat intelligence platforms becoming mainstream.

### Project Size

**Big**, given the vast IT infrastructure of financial institutions.

### Complexity

**Small:** Fewer disruptions from unanticipated patches.

**Medium:** Enhanced customer trust, improved subscription retention.

**Big:** Prevention of large-scale data breaches, saving potentially millions.

### Cloud Solutions

**AWS Macie** (data security and data privacy), **Azure Security Center**, **GCP's Security Command Center.**



### Technical Aspects

- **Historical Data Utilization:** Threat intelligence platforms like **Recorded Future** use AI to analyze data and predict future threats.
- **Recommendation Systems: Dependabot** and **Snyk** automatically monitor dependencies for security vulnerabilities and provide fix recommendations.

#### Historical Data Utilization


#### Recommendation Systems

# 6. Diving Deeper

## 6.5 Model Training & Continuous Learning

### Business Case

**DigitalGlobe** uses GCP for machine learning, refining their satellite image categorization over time.


### Impact

Improved categorization allows quicker delivery to clients, leading to faster revenue recognition and higher customer satisfaction.

### Financial Benefits

20% increase in user engagement within six months.

### Trend

Growing emphasis on AiOps (AI for IT operations), especially in large-scale cloud operations.

### Project Size

**Small**, considering the specific niche and focus of most startups.

### Complexity

**Small:** Faster model training times.

**Medium:** Better personalized user experiences leading to increased usage.

**Big:** Significant uptick in ad revenue due to increased user engagement.

### Cloud Solutions

**AWS SageMaker, Azure Machine Learning, GCP's AI Platform.**




### Technical Aspects

- **Feedback Loop:** Continuous integration tools like **CircleCI** and **Travis CI** can be set up with AI-driven test suites to improve tests over time.
- **Transfer Learning:** Frameworks like **TensorFlow** and **PyTorch** support transfer learning, which can be utilized in security contexts.

#### Feedback Loop


#### Transfer Learning

# 6. Diving Deeper

## 6.6 Integration with CI/CD Pipelines

### Business Case

**King Games** (makers of **Candy Crush**) uses Azure DevOps for continuous integration, ensuring constant updates and feature releases.

### Impact

Faster feature releases mean quicker revenue generation from new content and sustained user engagement.

### Financial Benefits

Reduced post-deployment hotfixes by 70%.

### Trend

GitOps (a Git-based or source-centric approach to CI/CD) gaining traction.

### Project Size

**Medium**, as SaaS platforms require regular updates and feature rollouts.

### Complexity

**Small:** More stable software releases.

**Medium:** Significant reduction in post-launch debug time and manpower.

**Big:** Enhanced user experience, increased customer retention, and growth.

### Cloud Solutions

**AWS CodePipeline, Azure DevOps, GCP's Cloud Build.**

Azure DevOps

### Technical Aspects

- **Automated Security Testing: GitLab** and **Jenkins** integrate security testing into CI/CD pipelines. AI-driven tools can enhance these processes.
- **Dynamic Patching: Ksplice**(by Oracle) provides real-time updates without needing to reboot the system.

### Automated Security Testing

GitLab Jenkins

### Dynamic Patching

Ksplice

# 6. Diving Deeper

## 6.7 Automated Threat Detection

### Business Case

**Capital One's** adoption of cloud-native security tools to automate code reviews and detect threats.

### Impact

Faster time-to-market due to early detection, reducing potential costs of late-stage vulnerability management.

### Financial Benefits

Reduced vulnerabilities by 90% within a year. The platform reduced security review times by 60%, enabling faster releases.

### Trend

A growing emphasis on "Shift Left" to introduce security early in the development lifecycle

### Project Size

**Medium to Big**, given the continuous code updates in e-commerce platforms.

### Complexity

**Small**: Faster detection, saving weeks of potential debug time.

**Medium**: Reduced manpower costs due to reduced manual security checks.

**Big**: Multi-million-dollar savings by preventing potential breaches.

### Cloud Solutions

**AWS's CodeGuru, Azure's Security Center, and GCP's Cloud Security Scanner.**

### Technical Aspects

- **Static Analysis:** AI can be trained to perform static code analysis more effectively by learning from past vulnerabilities. Machine learning models can identify patterns or code structures often associated with security vulnerabilities.
- **Dynamic Analysis:** AI can observe running applications to identify unexpected behaviors, potential security threats, or data leaks.

### Static Analysis

### Dynamic Analysis

# Thanks for coming

Have a nice day!