



Reimagining modern DevSecOps

Traditional security often happens late in software development, risking costly delays and vulnerabilities. Development, security, and operations (DevSecOps) integrates security into each stage of development, enhancing visibility, collaboration, and operational efficiency.

Machine learning security operations (MLSecOps) is the next step in the evolution of DevSecOps specifically tailored to meet the different challenges of developing, deploying, and maintaining ML models. Unlike traditional approaches that focus primarily on code, MLSecOps encompasses the ML life cycle—including data, model artifacts, and the interactions between models, users, and systems.

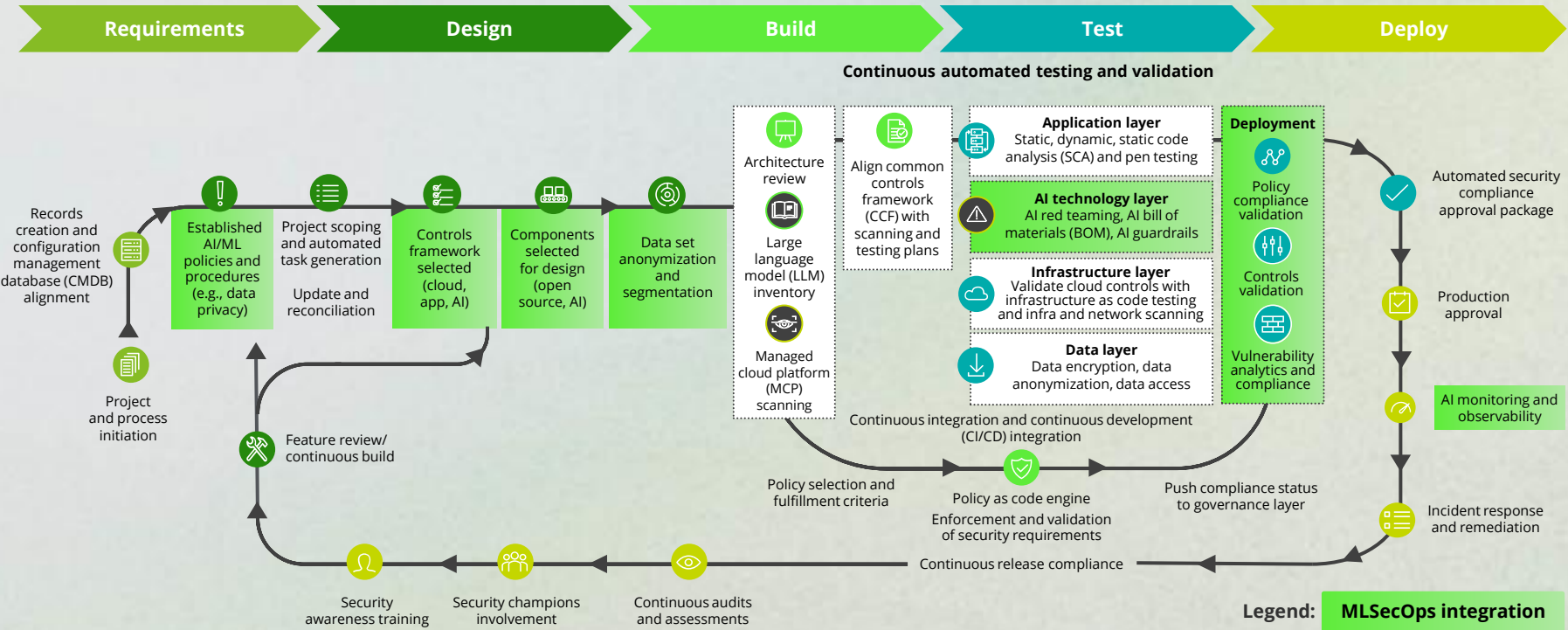
As artificial intelligence (AI) and ML become central to business operations, MLSecOps adapts and expands DevSecOps principles to help ensure security, risk management, and governance are embedded throughout the ML process. This approach delivers benefits such as accelerated AI innovation through secure experimentation and deployment; trustworthy and responsible AI promoting fairness, compliance, and reliability; and stakeholder confidence earned through proactive risk management and ethical AI practices.

AI can introduce new threats to applications

Targets	Application	Model	Infrastructure	Data
Threats	Intellectual property theft Unintended system interaction Model theft	Model bias attack Prompt self-replication Intellectual property (IP) infringement Model denial of service (DoS)	Misconfiguration Integration issues Malware distribution	Data poisoning Data loss or compromise (personally identifiable information, sensitive data) Information manipulation

MLSecOps integrates into DevSecOps to secure these threats

A blueprint for an AI-powered future: This model illustrates a strategic approach to evolving MLSecOps processes, aligning governance, secure MLOps, and automated compliance across design, development, deployment, and monitoring. Integrating AI-driven security and continuous risk management can empower organizations to proactively defend against emerging threats, including intellectual property theft, model bias attacks, and data poisoning.



Connect to accelerate

Contact our leaders to dive deeper into the blueprint and reimagine what’s possible for your organization.



Mark Nicholson
Principal
Cyber AI
GTM Leader
Deloitte & Touche LLP
manicholson@deloitte.com



Naresh Persaud
Principal
AI Transformation Leader
Deloitte & Touche LLP
napersaud@deloitte.com

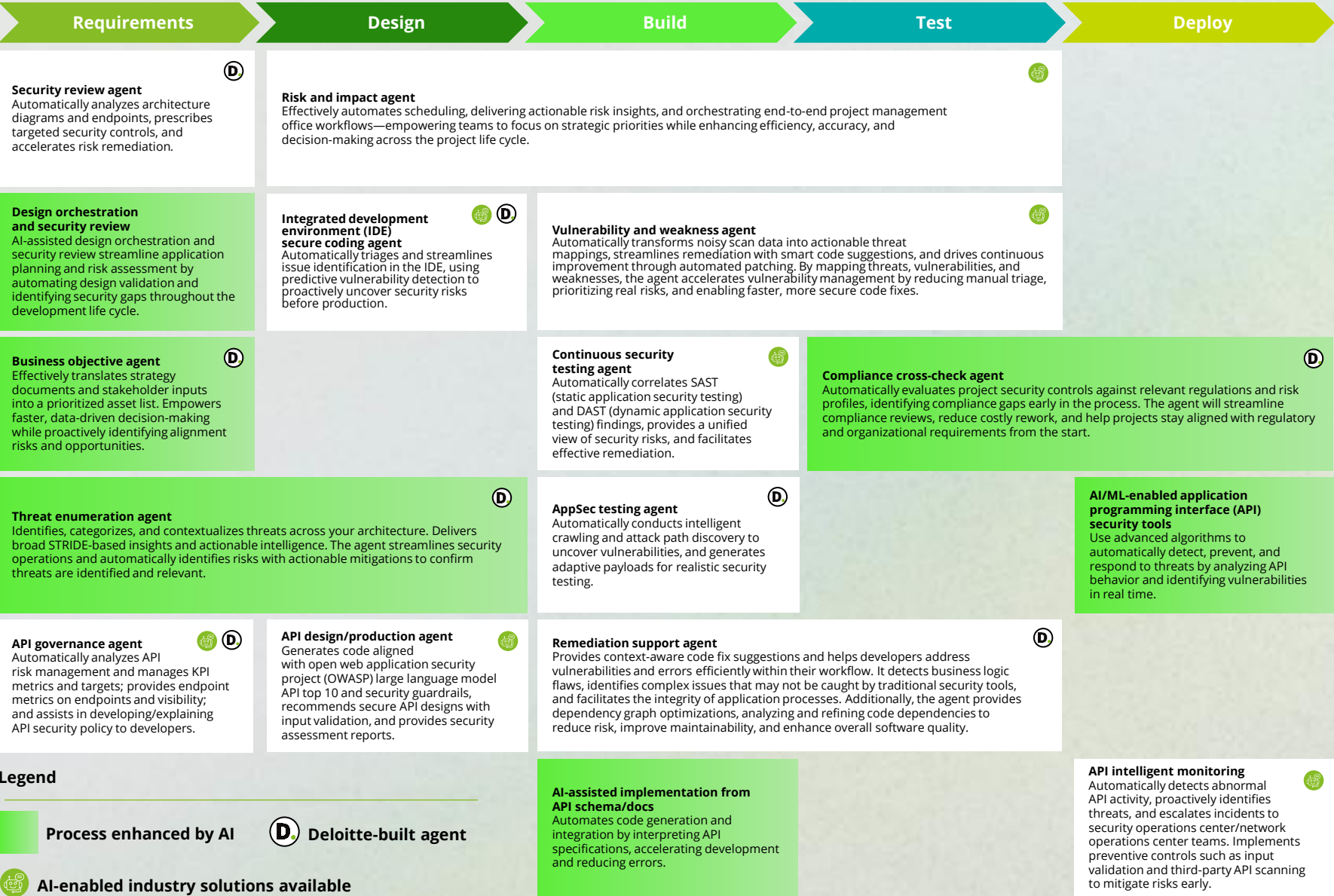


Faris Naffaa
Senior Manager
Secure by Design Leader
Deloitte & Touche LLP
fnaffaa@deloitte.com



Steve Ruzzini
Senior Manager
Cyber AI GTM
Activation Lead
Deloitte & Touche LLP
sruzzini@deloitte.com

How AI can uplift DevSecOps



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Copyright © 2025 Deloitte Development LLC. All rights reserved.