Deloitte.

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.

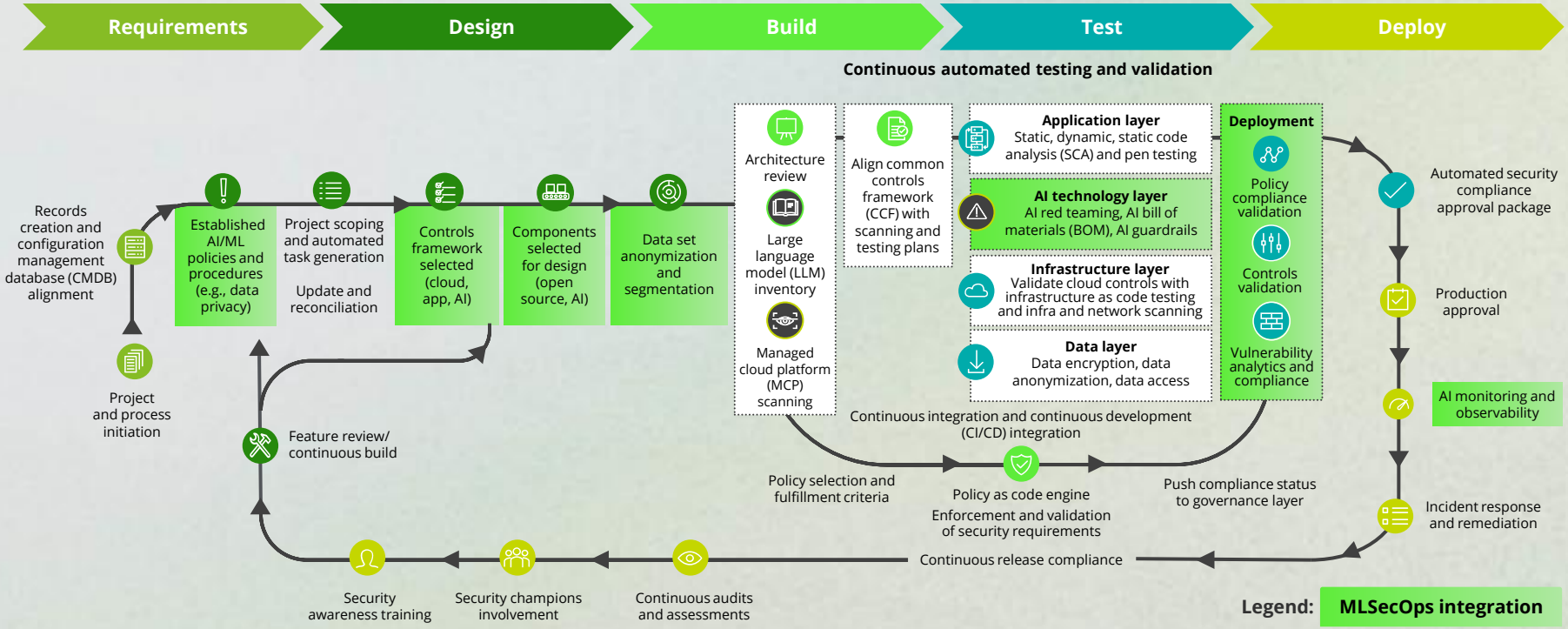
As artificial intelligence (AI) and ML become central to business operations, MLSecOps adapts and expands DevSecOps principles to help ensure security, risk management, and governance are embedded throughout the ML process. This approach delivers benefits such as accelerated AI innovation through secure 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

Requirements	Design	Build	Test	Deploy

Security review agent (D)
Automatically analyzes architecture diagrams and endpoints, prescribes targeted security controls, and accelerates risk remediation.

Risk and impact agent
Effectively automates scheduling, delivering actionable risk insights, and orchestrating end-to-end project management office workflows—empowering teams to focus on strategic priorities while enhancing efficiency, accuracy, and decision-making across the project life cycle.

Design orchestration and security review
AI-assisted design orchestration and security review streamline application planning and risk assessment by automating design validation and identifying security gaps throughout the development life cycle.

Integrated development environment (IDE) secure coding agent (D)
Automatically triages and streamlines issue identification in the IDE, using predictive vulnerability detection to proactively uncover security risks before production.

Vulnerability and weakness agent
Automatically transforms noisy scan data into actionable threat mappings, streamlines remediation with smart code suggestions, and drives continuous improvement through automated patching. By mapping threats, vulnerabilities, and weaknesses, the agent accelerates vulnerability management by reducing manual triage, prioritizing real risks, and enabling faster, more secure code fixes.

Business objective agent (D)
Effectively translates strategy documents and stakeholder inputs into a prioritized asset list. Empowers faster, data-driven decision-making while proactively identifying alignment risks and opportunities.

Continuous security testing agent
Automatically correlates SAST (static application security testing) and DAST (dynamic application security testing) findings, provides a unified view of security risks, and facilitates effective remediation.

Compliance cross-check agent (D)
Automatically evaluates project security controls against relevant regulations and risk profiles, identifying compliance gaps early in the process. The agent will streamline compliance reviews, reduce costly rework, and help projects stay aligned with regulatory and organizational requirements from the start.

Threat enumeration agent (D)
Identifies, categorizes, and contextualizes threats across your architecture. Delivers broad STRIDE-based insights and actionable intelligence. The agent streamlines security operations and automatically identifies risks with actionable mitigations to confirm threats are identified and relevant.

AppSec testing agent (D)
Automatically conducts intelligent crawling and attack path discovery to uncover vulnerabilities, and generates adaptive payloads for realistic security testing.

AI/ML-enabled application programming interface (API) security tools
Use advanced algorithms to automatically detect, prevent, and respond to threats by analyzing API behavior and identifying vulnerabilities in real time.

API governance agent (D)
Automatically analyzes API risk management and manages KPI metrics and targets; provides endpoint metrics on endpoints and visibility; and assists in developing/explaining API security policy to developers.

API design/production agent
Generates code aligned with open web application security project (OWASP) large language model API top 10 and security guardrails, recommends secure API designs with input validation, and provides security assessment reports.

Remediation support agent (D)
Provides context-aware code fix suggestions and helps developers address vulnerabilities and errors efficiently within their workflow. It detects business logic flaws, identifies complex issues that may not be caught by traditional security tools, and facilitates the integrity of application processes. Additionally, the agent provides dependency graph optimizations, analyzing and refining code dependencies to reduce risk, improve maintainability, and enhance overall software quality.

AI-assisted implementation from API schema/docs
Automates code generation and integration by interpreting API specifications, accelerating development and reducing errors.

API intelligent monitoring
Automatically detects abnormal API activity, proactively identifies threats, and escalates incidents to security operations center/network operations center teams. Implements preventive controls such as input validation and third-party API scanning to mitigate risks early.

Legend

Process enhanced by AI

(D) Deloitte-built agent

AI-enabled industry solutions available