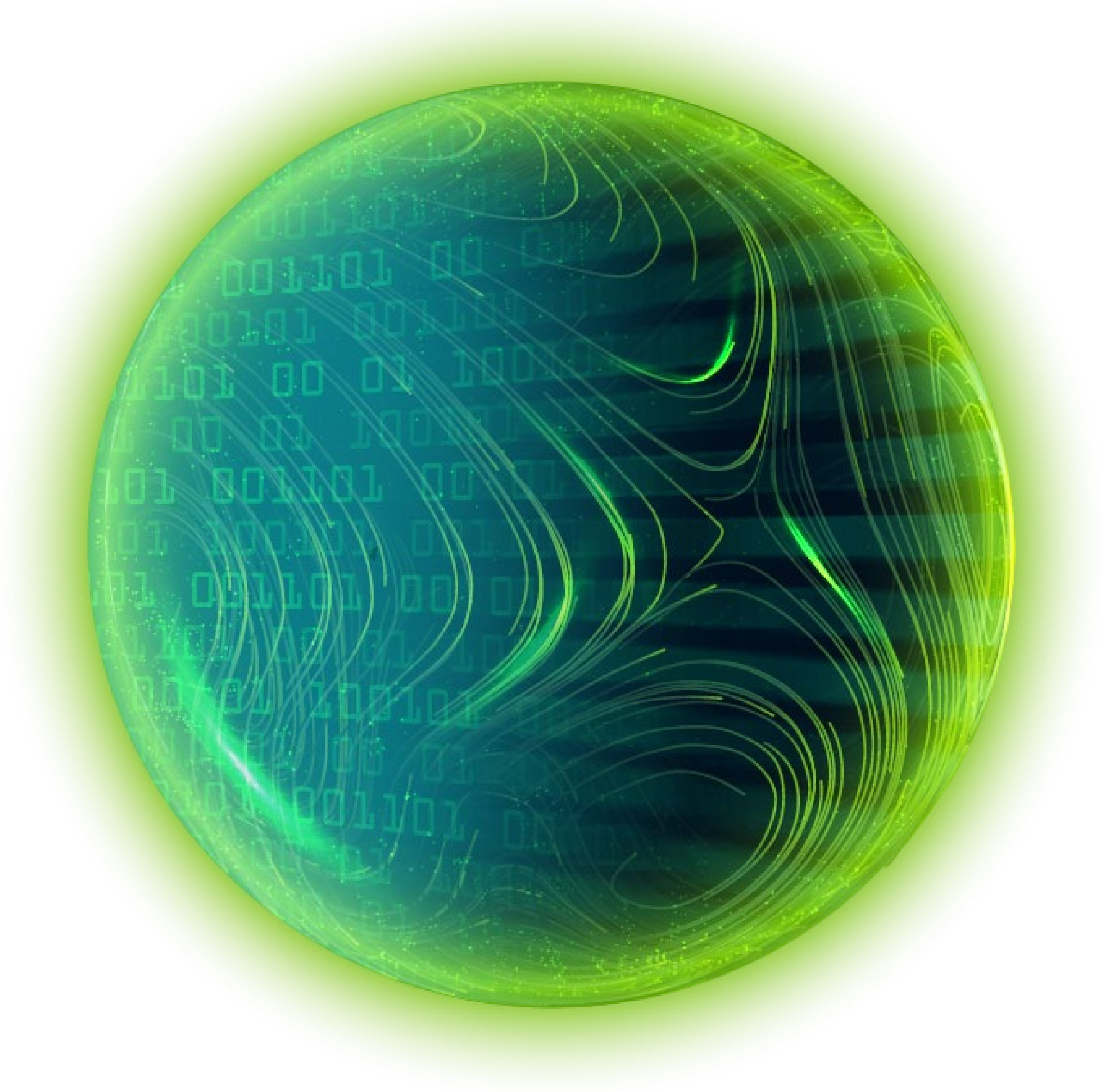
Deloitte.



Implementing DevSecOps

A cloud deployment perspective

Table of contents

[DevSecOps] adoption is not merely a checkbox for compliance; it is a strategic imperative for organizational success in today's digital landscape that Deloitte can help actualize.

Introduction

Cloud technology is now a necessity for enterprise IT, especially in the federal sector. As government reliance on the cloud grows, robust security practices are critical to balance risks and benefits. The vision of inherently secure cloud infrastructure has not fully materialized, leaving IT teams with greater complexity to manage.

DevSecOps-integrating security throughout development, deployment, and operations-is one of the most effective ways to secure cloud environments. By embedding security early and continuously, DevSecOps proactively identifies and mitigates vulnerabilities, reducing risk and fostering a culture of shared responsibility.

Deloitte advocates for a holistic DevSecOps approach that incorporates secure culture, practices, and tools to drive visibility, collaboration, and agility across four main areas:

- **Security in Development**: Establish governance, security baselines, reusable artifacts including application code blocks and reference architectures, and automated CI/CD scanning and testing.
- **Security in Deployment**: Implement secure Everything as Code (XaC) for infrastructure, configuration, and policy, and automate system build and hardening.
- **Security in Operations**: Integrate security policies with enterprise capabilities like Identity and Access Management (IdAM), Security Information and Event Management (SIEM), and Security Operations Center (CSOC).
- **Security as Part of Training**: Launch agency-wide security awareness programs to foster a security-aware culture, recognizing that security is only as strong as the people implementing it.

Deloitte’s approach extends beyond technology, requiring a transformative shift in development culture to prioritize security. This prevents security from being seen as a hindrance or mere compliance checkbox. This document reviews the key elements of robust DevSecOps, highlights areas of application, and introduces Deloitte’s methodology for secure cloud environments.

DevSecOps

Integrating security as a core element throughout the software development lifecycle is fundamental to the practice of DevSecOps. This starts with a commitment from leadership to require security to be embedded from the start and to hold teams accountable for adhering to those security requirements and policies. At the same time, organizations should empower all personnel to understand and implement DevSecOps through training and associated process maturation.

Strategic, timely, and consistent implementation of security within DevSecOps pipelines can help reduce team workload and avoids unnecessary automation, ensuring security measures are thoughtfully integrated. Security is achieved without slowing down development or hindering mission outcomes. Additionally, DevSecOps enables emerging and changing requirements, such as those for Secure Software Supply Chain and continuous Authority to Operate (cATO). This is increasingly important as different flavors of artificial intelligence (AI), like generative and agentic AI, enable faster development and testing while providing agility to adjust to frequent changes.

Key elements for a robust DevSecOps environment

- **Shifting Security Left:** Embed security from the outset across development, deployment, and operations, making it proactive rather than an afterthought.
- **Cultural Change:** Build a culture where security is integral to mission success and understood by all personnel.
- **Strategic Automation:** Automate security processes early and often to ease burdens across teams.
- **Integrate AI:** Leverage AI to increase both speed of development and security throughout the lifecycle.

With a security-first culture, early consideration in policies and procedures, and strategic automation, organizations can effectively implement DevSecOps practices. These concepts extend beyond software development, which can benefit the entire enterprise.

Potential DevSecOps application areas

- **Development:** Integrate security measures at the coding stage to identify and address vulnerabilities early, while optimizing performance and increasing reliability.
- **Deployment:** Adhere to security protocols during the deployment phase for a consistent, secure launch.
- **Operations:** Implement continuous monitoring and regular updates to maintain a strong security posture.
- **Training:** Conduct regular training to keep teams informed on evolving security threats and mitigation best practices.

Development, Deployment, and Operations operate in a feedback loop, enabling the lessons learned from one stage are applied to the others, enhancing the overall security posture.

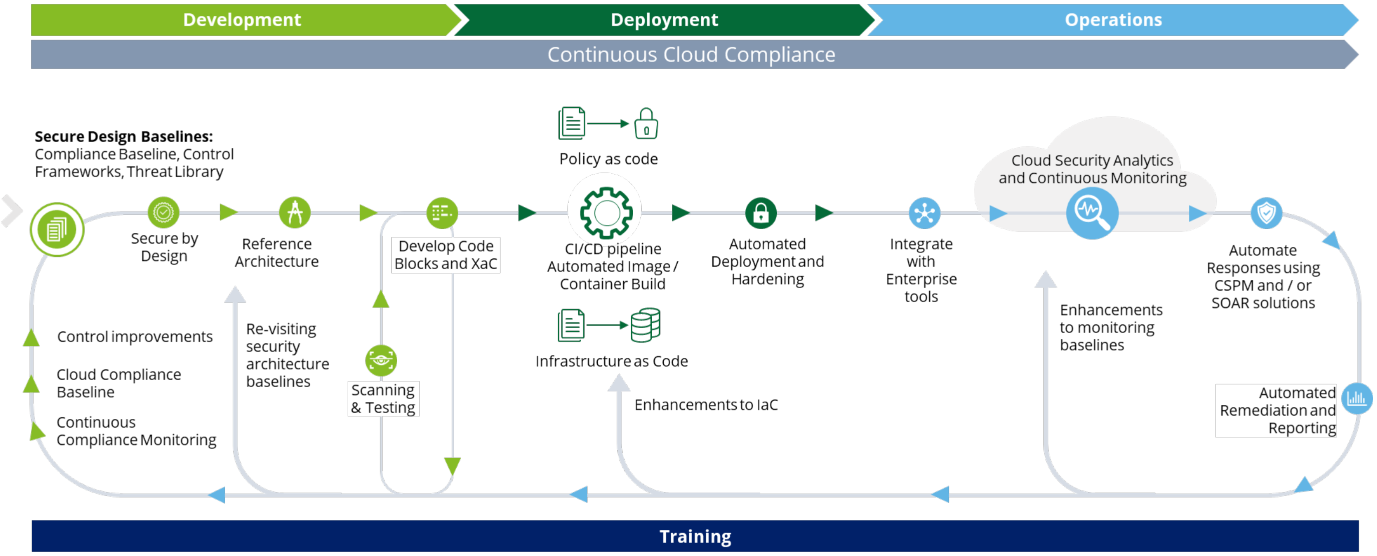

Development
Deployment
Operations
Continuous Cloud Compliance
Secure Design Baselines: Compliance Baseline, Control Frameworks, Threat Library
Secure by Design
Reference Architecture
Develop Code Blocks and XaC
Policy as code
CI/CD pipeline Automated Image / Container Build
Infrastructure as Code
Automated Deployment and Hardening
Integrate with Enterprise tools
Cloud Security Analytics and Continuous Monitoring
Automate Responses using CSPM and / or SOAR solutions
Control improvements
Cloud Compliance Baseline
Continuous Compliance Monitoring
Re-visiting security architecture baselines
Scanning & Testing
Enhancements to IaC
Enhancements to monitoring baselines
Automated Remediation and Reporting
Training

Figure 1: Diagram of Development, Deployment, and Operations feedback loop

Deloitte's approach to DevSecOps in cloud environments emphasizes the smooth integration of security into every stage of the software development and deployment lifecycle. This method enables the delivery of secure and efficient cloud solutions tailored to organizational needs, so that security is continuously improved and adapted to meet evolving challenges.

A Deloitte Approach

Deloitte's DevSecOps (DSO) methodology in cloud environments leverages the "everything as code" (XaC) paradigm-where infrastructure, services, and storage are defined by code-to deliver continuous compliance and security. By integrating DSO, Deloitte helps organizations achieve secure, efficient cloud operations across four key areas: Development, Deployment, Operations, and Training.

Security in development

Deloitte establishes security baselines aligned with industry best practices and compliance standards, enabling developers to build secure code and infrastructure from the start. Security gates are integrated into Agile sprints and reviews, supported by Deloitte accelerators like the Secure Cloud Composer (SCC) Generator and SCC Code Checker.

- **Secure Cloud Composer (SCC) Generator:** SCC Generator simplifies the process of building compliant cloud environments by leveraging automation and Generative Artificial Intelligence (GenAI) in an easy-to-use natural language chatbot, reducing the time developers need to spend building and securing cloud infrastructure.
- **Secure Cloud Composer (SCC) Code Checker:** Leverages AI to review and auto-correct XaC based on common or custom compliance frameworks reducing the risk of vulnerabilities reaching deployment.

Establishing a security baseline

Security baselines set minimum controls for all applications, following standards like FedRAMP, NIST 800-53, and ARC-AMPE, among others. They determine what security controls need to be met to achieve an authority to operate (ATO). Obtaining the ATO is often the hardest and longest part of development for Federal agencies, and it can be difficult for developers to know where to start. We facilitate this process through our RMF.AI accelerator, which provides guidance and acceleration by leveraging AI to determine system categorization and tailor controls. This allows developers to understand security requirements early in the development process, speeding up the time to deploy capabilities to support the mission.

Security by assembly

Developers should focus on development without having to navigate complex security requirements for their applications. We leverage GenAI to build modules of secure code based on leading design practices, then thoroughly test and correct the code so it can be trusted for reuse. We validate the code again through automated testing in CI/CD pipelines, with checkpoints at each development stage to meet standards and minimize potential risks. This approach allows developers to assemble known-good code instead of starting from scratch, creating a flywheel that speeds up development and embeds compliance and security without additional effort from developers.

Integration of automated security scanning and testing

To prevent security from being a bottleneck in development, it is important to automate security scanning and testing. Deloitte's Alliances including Palo Alto, Wiz, and CrowdStrike, provide a wide-ranging and rapidly maturing capability set that not only provides scanning and testing but also the ability to track code through deployment to the cloud. These tools can be integrated into CI/CD pipelines, automating the detection and remediation of vulnerabilities before deploying to production. Integration of these tools can be simple, but they cannot be deployed in a "set it and forget it" manner. We apply our experience to enhance tools and pipelines to meet and validate security baselines, enabling early detection and remediation of vulnerabilities and reducing threat exposure before deployment, all without slowing down development.

Security in deployment

The tools and artifacts generated during development accelerate deployment into secure landing zones where we validate security and functionality including integration with enterprise solutions such as Identity and Credential Access Management (ICAM) and Security Incident and Event Management (SIEM) tools. This is an important step in that it adds the context of an operational environment that may impact what, if any, additional security controls an application may need.

Runtime security tools: Implementing a data lake

Through development and deployment, many tools and processes generate data that provide context into the application. Instead of switching between tools to understand progress or how security is being met, a data lake provides a centralized location to store all the data and query against it. At the same time, it may not be cost-effective to send all data to one place or cloud, so the data lake should be extendable and federated, utilizing APIs to support data calls. Deloitte's Cyber Analytics Engine (CAE) is a cloud-native data lake that streamlines data ingest and indexing so it can be easily queried. CAE also supports integration with SIEM and ITSM tools, as well as AI/ML/LLM capabilities. This is especially helpful in the DSO process, as at any point in the development and deployment lifecycle, you can query the data and generate dynamic dashboards to get a better understanding of the overall security posture. This also enables real-time visibility into what security controls are being met and how they are being met, further accelerating the ATO process.

Security in operations

An application deployed to a testing or pre-production environment is different from an application that is live with active users, depending on the functionality and security of the application. Security should be transparent to users, while security operations should maintain that security with a feedback loop to developers on risks and security gaps. Our approach leverages much of an enterprise's existing tools: SIEM, vulnerability management, CNAPP, etc., which is enhanced by the use of a data lake like CAE, mentioned in the previous section. Additionally, security operations benefit from automation and increasingly the incorporation of AI / GenAI / agentic AI.

Security automation strategy

It is common to focus on a Security Orchestration and Automated Response (SOAR) tool to handle security but as tools increasingly incorporate automation capabilities, it is important to establish a strategy that unifies how each tool will be used to accomplish a specific action or response. For instance, if the SIEM triggers an alert for a cloud misconfiguration, the alert could be sent to a CNAPP or the cloud provider to trigger an auto-remediation, while integration with an ITSM product like ServiceNow could capture the activity for tracking. Deloitte brings our experience in security automation with customizable SOAR playbooks and automation strategies, including an understanding of how to integrate the different tools together. Additionally, we bring AI-enabled capabilities to inform decisions about the behavioral security baseline of the enterprise. This serves to accelerate detection and remediation of vulnerabilities and risks, while also supporting continuous enforcement of security controls, which can enable continuous ATOs.

AI / GenAI / Agentic AI

The area of AI / GenAI / agentic AI is rapidly evolving and maturing, and while organizations may be hesitant to adopt these technologies, shrinking budgets and increasing requirements are accelerating the need for adoption. Deloitte's experience and strategic relationships, including those with Anthropic, Nvidia, and Palantir, enable us to be at the forefront of incorporating AI into enterprises. This is especially applicable in DSO, as we can now use data to identify security issues, but also to rapidly generate, test, and implement fixes. For instance, based on security data, user data, and overall performance data, we can identify that a minor security issue is causing performance issues with an application. We can then use AI agents to generate the code fix, perform testing, and implement the fix with no impact on operations or users. This is just one example, and Deloitte can bring our experience and knowledge, including an entire practice around Trustworthy and Ethical AI, to incorporate AI solutions that can enhance DSO for your organization.

DevSecOps training

More than technology, it is important to incorporate DSO into processes and train people, as adopting DSO can be a cultural shift in how an organization currently operates. Training in a comprehensive DevSecOps approach allows organizations to incorporate their people into the process. Deloitte offers specialized training programs that begin with a thorough review of existing training initiatives to identify knowledge gaps or areas for improvement. This sets the stage for updates to Standard Operating Procedures (SOPs) and the development of new guidelines, providing clear directives for integrating security into all areas of work. With these guidelines in place, professionals can conduct engaging and interactive training sessions emphasizing the security gains provided by a well-established DevSecOps practice. The process culminates in the creation of Centers of Excellence (CoEs), promoting ongoing learning, knowledge sharing, and collaboration. This continuous learning fosters a robust security culture within the organization and contributes to the overall security of the DevSecOps pipeline.

Review current training programs:

The first step in enhancing security training involves working with the organization to review current training programs surrounding development and operations. This process identifies gaps in knowledge or skills and reports on areas needing improvement or further focus. Organizations can use this information to create new training initiatives and improve existing ones.

Update or develop new SOPs and requirements guidelines

Once the organization understands the current training landscape, it can update existing SOPs and requirements guidelines or develop new ones as needed. These documents serve as the backbone of the training program by providing clear instructions and guidelines for developers and operators on how to incorporate security into all aspects of their work.

Perform training:

With updated SOPs and guidelines in place, the next step is to conduct training sessions. These trainings can take various forms, such as instructor-led live and virtual sessions, on-demand video training, workshops, and seminars, among others. The focus of these training sessions should be on DevSecOps and the importance of incorporating security into all aspects of development and operations. Trainers should design these sessions for engagement and interaction, encouraging participants to apply the knowledge in their roles.

Develop centers of excellence:

The final step in enhancing security training is the development of CoEs. These CoEs serve as hubs for promoting secure development and operations within the organization. They provide a platform for ongoing learning, knowledge sharing, and collaboration, which helps build a strong security culture within the organization.

Through these CoEs, team members can stay abreast of the latest security trends and threats, learn about leading practices, and continually improve their skills, contributing to the overall security of the organization's DevSecOps pipeline.

Conclusion

As cloud adoption and virtualization expand, organizations face increasing security challenges targeting these new environments. DevSecOps helps address these risks by integrating security throughout development, deployment, operations, and training, fostering a security-focused culture.

Deloitte has championed DevSecOps since its inception, developing experience and practical applications by leveraging the key innovations of cloud computing. Our approach emphasizes intentional adoption in four key areas:

- **Development**: Establish security baselines and build secure XaC using tools like Deloitte's SCC Generator and Code Checker to accelerate secure development and ATOs.
- **Deployment**: Integrate runtime security tools and a data lake to drive better security insights.
- **Operations**: Leverage automation and AI capabilities to optimize security.
- **Training**: Strengthen security culture by updating training programs, developing new guidelines, conducting DSO-focused sessions, and establishing Centers of Excellence.

By leveraging Deloitte's experience and tools, organizations can effectively mitigate risks, protect assets, and meet regulatory requirements. DSO adoption can not only enhances compliance but it can also build shared accountability and strengthen the overall security posture, making security a strategic imperative for success in today's digital landscape.

Meet the team

Mason Evans
Managing Director Deloitte & Touche LLP

masevans@deloitte.com

Dean Lee
Specialist Leader Deloitte & Touche LLP

deanlee@deloitte.com

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document 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 adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

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.

MAKING AN IMPACT THAT MATTERS since 1845