déjà vu SECURITY

Advisory Services

SecureDevOps

IS SECURITY THE BOTTLENECK?

Digital transformation is the use of digital technology in solving traditional problems where transformation occurs by means of digital innovation, resulting in new solutions. By its nature, it causes constant disruption to new and existing business models, products, services, or experiences enabled by data and technology across the enterprise. The ensuing continuous demand for new capabilities at faster speeds and bigger scales is pushing the limits of traditional development models.

Progress in the age of digital transformation has seen DevOps become the preferred development methodology of market leaders who are constantly adapting to meet fluctuating customer demands. DevOps includes continuous deployment with quick development of new capabilities and constant collaboration. The goal of DevOps is to shorten the systems development life cycle while delivering features, fixes, and updates frequently in close alignment with business objectives.

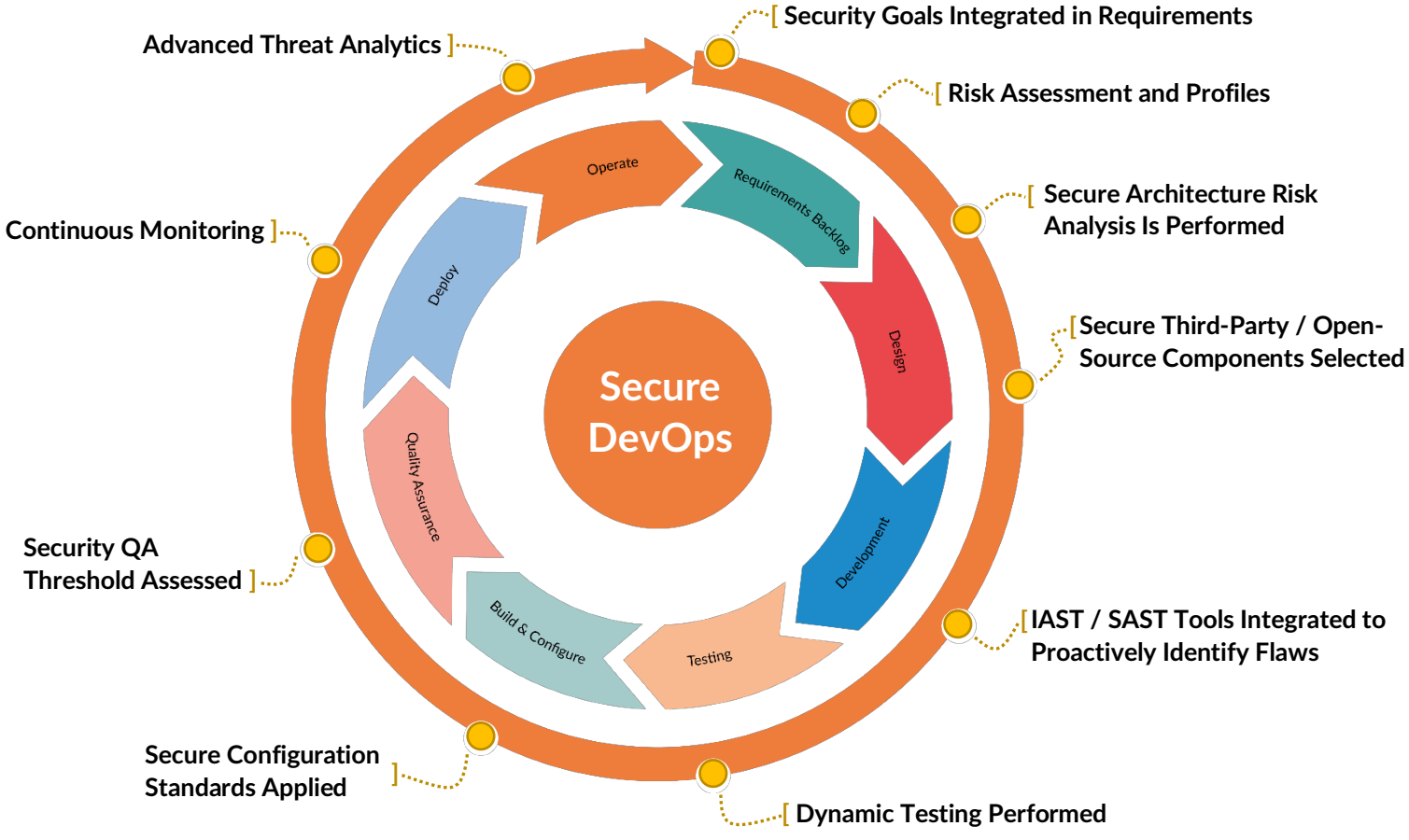
Industry issues/trends

Digital transformation increases the risk of threats due to software security flaws introduced on account of faster development and adoption time frames. Attackers exploit these weaknesses to gain access to an organization's data and intellectual property. An attack at the software layer can not only damage a corporation's brand and reputation, but also cause heavy financial damages, reduce competitive advantage, and create legal/regulatory noncompliance.

It is a common mistake to assume that traditional security controls can still be used in this new iterative environment since defects are fixed at a faster rate. While secure development principles still apply, and automated checkpoints do need to be built into each phase, the integration points and methodology need to be changed to adapt to the faster phases and account for the operation's changes.

DevOps and the Security Challenge

DevOps refers to the combination of development and operations with a focus on cross-departmental integration and automation. The idea of DevOps spawned from the popularity of Agile, but placed greater emphasis on the cultural shifts necessary to sustain faster releases and drive toward a shared goal.



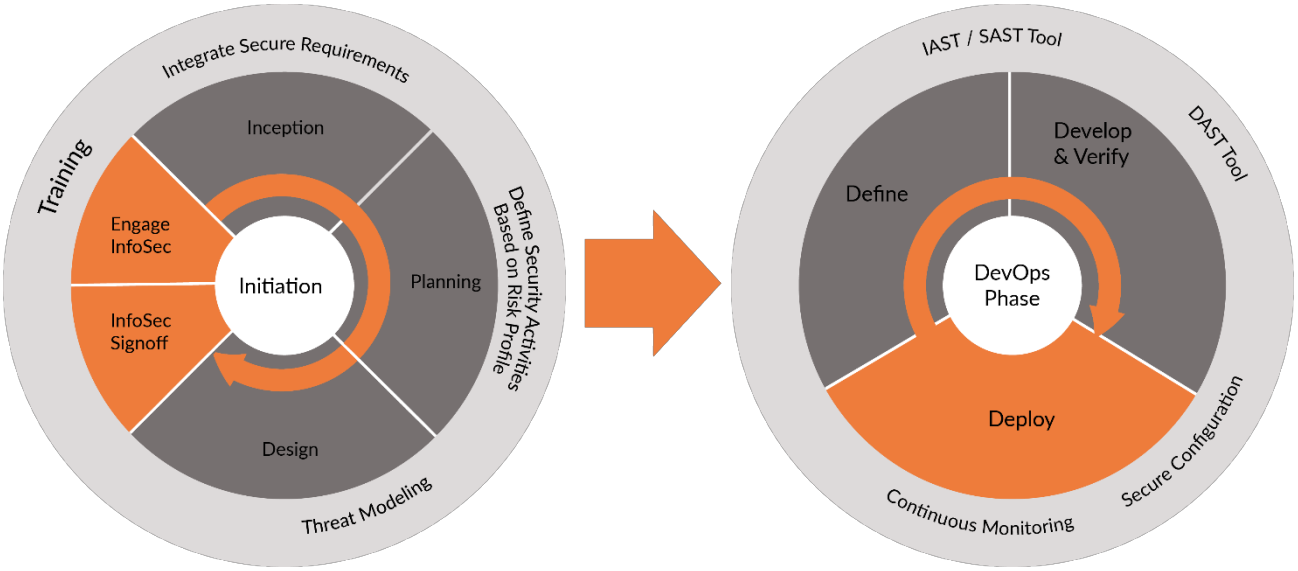
Security practices need to adapt to the business drivers making these methodologies popular, such as the need to increase speed to market, enhance overall product quality, and address issues in a timely manner. Security must adapt to the requirements that enable the business drivers, such as short iterations, narrow focus, and an ability to quickly accommodate changing demands.

Integrating Security into DevOps

The top changes used by successful organizations to incorporate security into DevOps and overcome the characteristic challenges were identified and are described below:

- Integrate Security Champions: Security team members need to be an integral part of the DevOps team through a champion/maven model deployment. Structurally, this helps build one cohesive development, operation, and security team, with one overarching objective to achieve business needs. The Security Champion is responsible for iterative threat modeling during the design process, using templates for driving architectural design patterns. The Information Security (InfoSec) team needs to set the standards the application team needs to meet on a periodic basis.
- Risk-based approach: A risk-based approach to integrating security in the DevOps life cycle must be adopted.

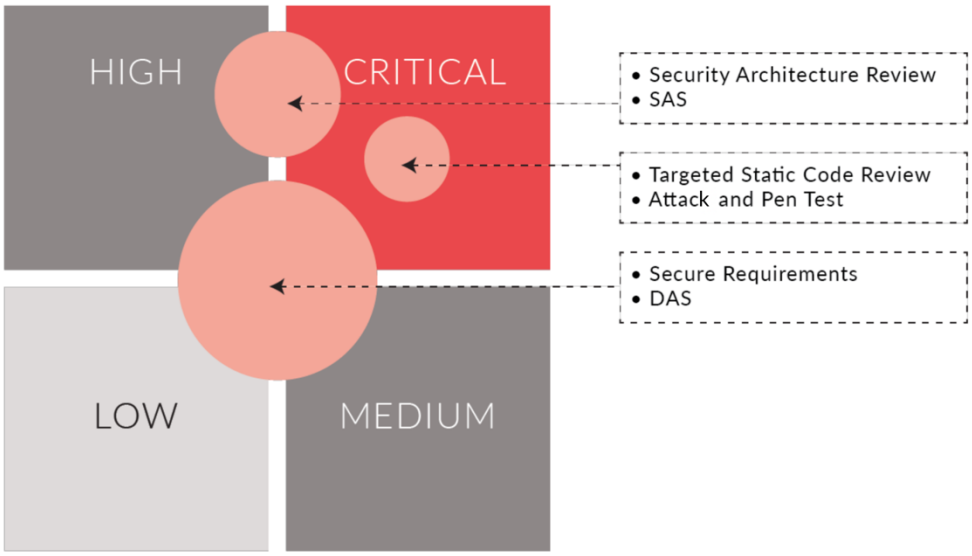
App Team and InfoSec Engagement



Periodic: Application Team and InfoSec Team collaboration

Every sprint: Application Team and InfoSec Team

- Organizations consistently apply a set of security activities to every release. These security activities must scale based on the risk profile of the user story and the associated epic. Defining these parameters is key to understanding the security activities that need to be integrated in the process.
- Automation: Traditional security activities do not fit the short iterative DevOps cycles. Security methodologies are not being built for DevOps. Organizations are trying to adapt existing security methodologies used in traditional software development life cycle (SDLC) models. Organizations need to leverage automation to integrate security into the DevOps cycle. A couple of ways to do that include:
    - Using Integrated Application Security Testing (IAST) instead of traditional static analysis during automated quality assurance (QA) testing to identify security bugs
    - Leveraging Runtime Application Self-Protection (RASP)-based technologies to help mitigate and monitor product level code



- Preapproved security patterns: Predefined nonfunctional security requirements need to be created and added to story cycles. Enterprise-approved libraries/functionalities must be available for core functionalities, such as authentication and system accounts management. Any deviation from the approved patterns is typically considered a defect that needs to be tracked to remediation. In addition, security testing results need to be tracked as part of a defect tracking system. Security vulnerabilities need to be considered bugs and added as criteria for automated checkpoints before release.
- Standardize infrastructure and operational controls: Environment and security controls must be consistent across all environments, including testing and production. Organizations need to have a security baseline for infrastructure that is consistent across environments and can be deployed in an automated manner (e.g. cloud-based deployment activities with scripts can be leveraged for automation and complemented with checks to ensure security baselines are met).
- Continuous monitoring: In addition to automation and baseline controls, activities to identify security defects must be performed on an ongoing basis. Continuous monitoring needs to include red team testing and fuzzing.
- Using cloud-based technologies allows teams to take advantage of Security Center detection capabilities built into the platform.

Benefits of This Model

The methods presented above have several key benefits:

Improving end-to-end security coverage by strategically planning, implementing, and deploying security processes	⟷	Positioning information security to support application teams operating in DevOps
Deploying faster to production, saving time without compromising security	⟷	Enabling development teams to independently execute security testing activities
Saving time and money by fixing security issues during the development process	⟷	Moving security and risk management to the left, allowing security teams to engage early

---

Deja's Advisory Services specialize in helping enterprise customers plan for a secure future, by providing strategies and pathways to navigate the intricate foundations of risk.

Shahnawaz Sabuwala
Principal Security Consultant

Akshay Aggarwal
Founder and Executive Chairman