Integration of security in devOps - a bigger picture

The global paradox

Software is the king and developers are the kingmakers. This statement indicates the growing demand for software, as the current business transformation requires interaction with computers or computer-assisted objects. This omnipresent computing has the potential to uptrend the incentives for misuse, thereby increasing the risk portfolio especially towards software. In the thick of things lies agile software development, a methodology rapidly adopted by organizations developing software. Being responsive to change, and delivering software at speed is the main essence of agile methodology. Security both as a process and as a technology requires intense planning and detailed analysis in order to arrive at the desired result. Even some of the best practices and frameworks encourage security testers to adopt manual intrusive approach for the best outcome. This brings us to the global paradox - whether to deliver software at high velocity, which propelled the need for competitiveness in the current marketplace, or focus on imperative security challenge to deliver secure software, perceived to have negative influence on the velocity.

Defining new approach

We should understand that the state of security today is similar to the state of operations back when DevOps was at its nascent phase.
The velocity of change does create a major challenge and requires a new way of thinking about security. To ensure seamless alignment to agile methodology and integration with DevOps, a change in approach is required in the following aspects:

Security is always viewed as a technology problem, rather than taking the holistic approach in tackling the business challenges.

Current security processes suit Waterfall model rather than agile, which requires more collaboration with the developers to work faster and more iteratively.

Security is always push not a pull, as the development team does not proactively engage the security team.

Experienced security practitioners can only use and interpret results from the security tools.

Adaptation of manual approach to identify vulnerabilities in the application, which requires significant amount of time and effort.

Focus is always on finding not fixing, it is great to identify security issues upfront, but need to find ways to handle an issue if discovered later in the lifecycle or in production.

Security effectiveness is measured on mere identification of vulnerabilities rather than overall enablement to deliver secure software.

DevSecOps framework

Approach security as a journey, not a destination - this means developing a progressive security program. The program should not only focus on the technical aspects but also create the right framework that fits the business objective of the organization. To create such a framework, it is important to understand the eco-system governing the organization in terms of people, process, and technology. The below section enumerates best practices to adopt for building an effective and robust DevSecOps framework encompassing the golden triad:

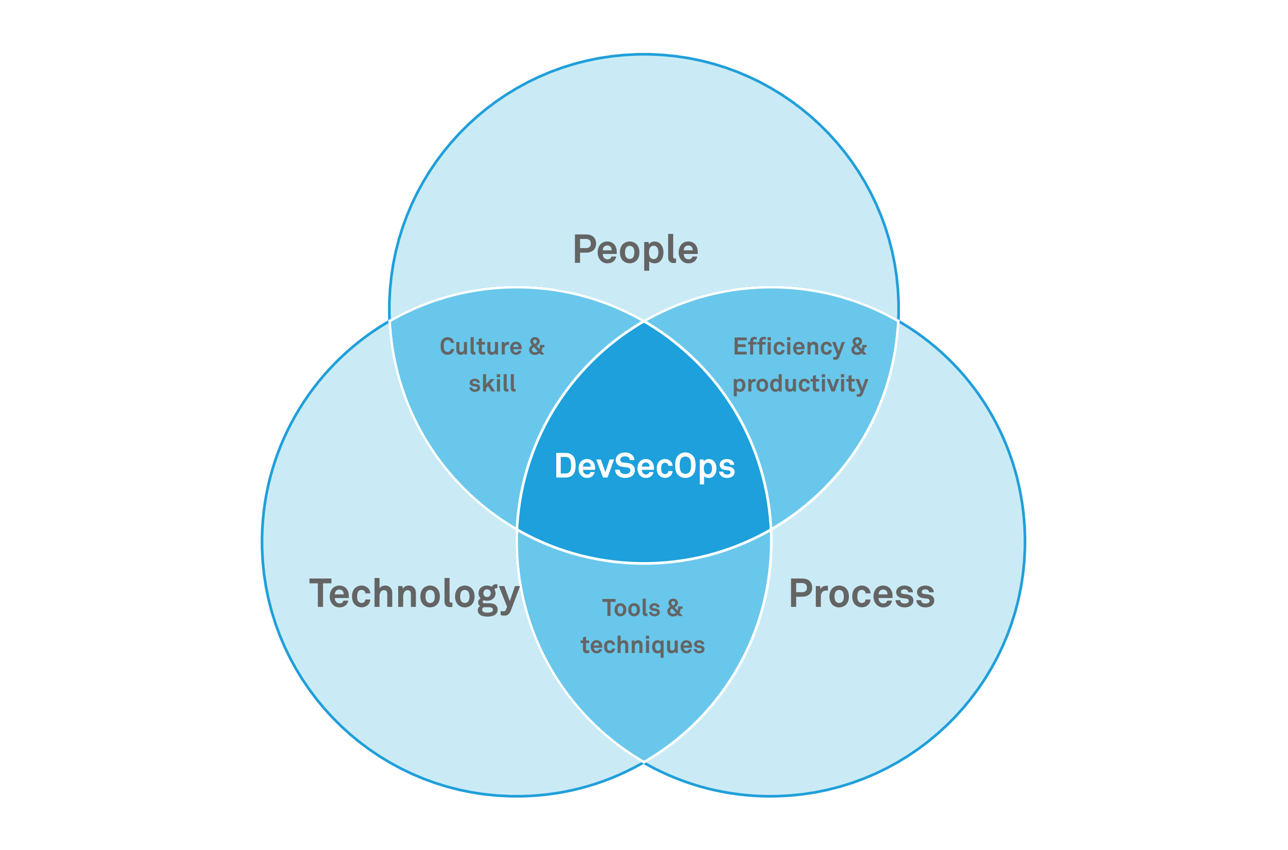

Fig. 1: Framework

People

The get-go for any successful implementation of a program are people – they are the starting point. The idea is to create a common goal among development, security, and operations by building the right culture and developing the required skillset to achieve the collective objective.

- **Break the silos and build collaborative working style** among development, security and operations by establishing common goals to achieve.
- **Shift from being exclusive to inclusive** by integrating security teams to work along with development and operations.
- **Security is about partnership not ownership,** actively engage DevOps teams in decision-making and always look to contribute to the solution instead of just highlighting issues.
- **Embrace a transparent and blameless approach** while engaging with developers which will not only help them to understand the issue and but also incrementally spread that knowledge.
- **Establish a platform for security outreach** to proactively engage with DevOps teams and discuss about latest security trends, present innovative ideas, and obtain feedback to enhance the value of security in DevOps.
- **Focus on delivering training and awareness session** to empower developers by educating the about secure design / coding, security tools, and the reasoning for adoption of a security processes in the DevOps pipeline.

Process

Organizations have to create acceptable and repeatable process to facilitate secure development and deployment without comprising the objective of faster delivery.

- **Shifting security to left** enables developers to understand threat landscape and develop an appropriate mitigation strategy early in the development lifecycle.
- **Striking the right balance between finding and fixing,** helps to reduce the cost by fixing the change faster and safer, at the same time detecting issues early.
- **Establishing process to improve tool performance** by building the policies to look only for the applicable set of bugs / vulnerabilities.
- **Checking for compliance using metadata** by identifying requirements and integrating them with the tools set to evaluate the percentage of compliance.
- **Adopting risk-based approach for building gated checks** will help developers to prioritize the remediation strategy by addressing the appropriate / applicable vulnerability to ensure faster and secure delivery of software.
- **Building practical and effective metrics** that not only indicates the density of the bugs / vulnerabilities but burn down rate and reoccurrence of such defects in the software.

Technology

DevSecOps provides a new spin to technology driving more automation and innovation. There is a demand to both create new and extend the existing tool sets to cater not only to the security professional but also the developers.

- **Leveraging automation throughout the pipeline** quickens the testing duration, reporting, and synchronous integration with DevOps tools.
- **Deploying the right tool sets** that support automation platform to achieve continuous integration and delivery of software.
- **Adaption of security tools to DevOps model** is key ingredient to establish security as an enabler in the DevOp world. For example, SAST tools tends to perform intrusive scans that take long time to complete which is not desirable in continuous integration/delivery environment. To adapt, most SAST tools introduced a feature called incremental scans which only scans for code that are changed allowing scans to complete faster.
- **Securing DevOps technologies** such as containers, serverless, and cloud each of which offers new functionality that in turn generates specific security requirements.

Conclusion

DevSecOps as a practice is getting increasing popular as organizations look to tackle ever-evolving challenges in security. Imparting the agile mindset in security is challenging as it conflicts the well-known and agreed methodical approach. However, the transformation is dependent on how people, process, and technology can be brought together to achieve overall business objectives in this new paradigm. This calls for defining a new philosophy towards security thereby bringing an inclusive culture and building the right set of process and technology. In this era of digital transformation, security should be an influencing factor along with agility, availability, and scalability.

About the author

Sriram Krishnan
Practice head, Cybersecurity & Risk Services,
Wipro Ltd.

Sriram Krishnan is currently the Practice Head for Security Assurance Services within Wipro's Cybersecurity and Risk Services (CRS) division. He has over 13 years of experience in strategizing, leading, and implementing cyber security initiatives in organizations across product development, banking and big 4 consulting. He has worked and managed projects relating to Secure SDLC, threat modelling, secure coding, and penetration testing, and has advised on security best practices for global clients in telecom, technology, banking and financial services, and public sector. Sriram holds a Master's degree in Computer Application from Anna University and has completed the Chief Information Security Officer (CISO) Executive Education Program from the Carnegie Mellon University.

He can be reached at **sriram.07@wipro.com**

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**