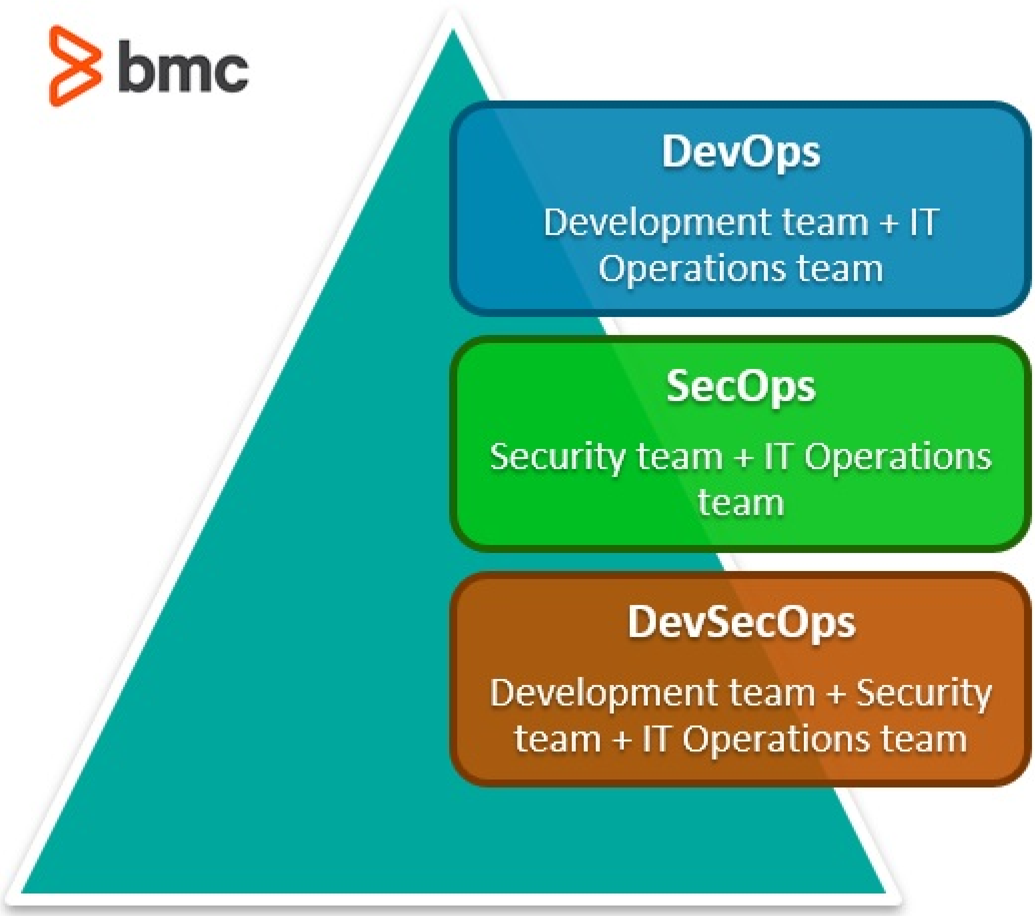
SECOPS VS DEVSECOPS: WHAT'S THE DIFFERENCE?

With a variety of philosophies and methodologies adopted in the tech world, figuring out what each one encompasses can be confusing. If you focus closer on an entire culture shift, such as DevOps, even that type of approach comes with as many different definitions as there are developers. Going further into DevOps are ideologies like SecOps and DevSecOps, leaving even the most experienced team members at times scratching their heads.

Worry no more. We have put together a complete guide to define the differences between SecOps and DevSecOps as well as how they might benefit your organization.


bmc
DevOps
Development team + IT Operations team
SecOps
Security team + IT Operations team
DevSecOps
Development team + Security team + IT Operations team

What is DevOps?

First things first, it is necessary to understand the idea of DevOps before you can move on to comparing the other two. Although its definition greatly varies, at its core DevOps is the combination of tools, practices, and philosophies that increases an organization's ability to deliver services and applications at a high velocity.

In the past, IT Operations (ITOps) would have to manually build infrastructure, causing days or even weeks to go by before code could be tested and deployed. With DevOps, this entire process is automated. By integrating the development and ITOps teams, DevOps enhances and streamlines the current software development process, allowing apps to be developed and deployed at a much quicker rate.

Free Download ›

Benefits of adopting DevOps include:

- Improved collaboration
- Faster to market with innovations
- Enhanced problem solving
- More time to innovate
- Increased ROI

What is SecOps?

SecOps is a methodology that aims to automate security tasks by combining security teams and ITOps teams together. By automating these mission critical tasks, security no longer starts once the security team gets a hold of the app—often an afterthought; rather, security is injected into the entire lifecycle of a product.

Similar to DevOps, SecOps is a philosophy that encourages greater levels of collaboration among designers, programmers, and those responsible for security. This team is able to consider security threats during the entire development cycle and how these threats could affect both the software and the users that might encounter them.

The biggest difference between SecOps and other types of programming philosophies, such as DevOps or Agile, is that SecOps is focused on ensuring every member of the development cycle team is aware of and responsible for security. Engineers might report code injection attempts or sales reps may notice and pass along suspicious emails. This methodology aims to prevent risks before they are even an issue.

A major benefit of SecOps is that it allows security teams to scale, distributing responsibilities to other personnel and helping to "bake in" security mitigation at every turn. The security team will no longer be siloed, but instead will be collaborating quite closely with most team members, especially those heavily involved in development.

Other benefits of SecOps for enterprises include:

- Improved productivity
- Enhanced resource usage
- Increased return-on-investment
- Fewer app disruptions
- Fewer cloud security threats
- More efficient auditing processes

What is DevSecOps?

In a nutshell, DevSecOps is the integration of both DevOps and SecOps. Like DevOps in the sense that it also seeks to enhance results through collaboration and communication, DevSecOps is another type of philosophy that promotes building security into applications during the development process.

With DevSecOps, developers run tests during coding, then run additional security tests in order to pass it on to deployment and production. If they fail at any point, the code is sent back to the developer to fix before it even reaches the production stage. Utilizing this process, there is a much lower risk of the software being deployed with security flaws attached.

Implementing DevSecOps greatly increases security measures by finding any vulnerabilities early in the development cycle. It also ensures that there is an automated way for code to be reviewed and to promote secure design patterns and principles among developers. This teaches developers to consider security as they are writing code, which in turn increases value and reduces costs.

Improved automation throughout the software delivery pipeline reduces the amount of downtime and attacks while also eliminating mistakes. Other advantages of DevSecOps include:

- Stronger collaboration and communication among teams
- Greater agility and speed for security teams
- Early awareness and mitigation of vulnerabilities in code
- Improved ability for rapid changes
- Enhanced opportunities for quality assurance testing

SecOps or DevSecOps: Which to choose?

At the end of the day, both SecOps and DevSecOps are highly similar philosophies. The key difference: SecOps focuses more on the integration of the security and operations teams while DevSecOps brings the development team to support security and ITOps teams as well.

The most important understanding to take away from all these terms and definitions is the agile nature and collaborative component they all share. By breaking down silos and incorporating automation and agility, responsibilities are shared, communication is enhanced, and security is infused. Given the increasing risks for organizations in 2020, incorporating security into any type of process is key, and automating this process ensures maximum benefit and safety.

Additional resources

For more on this topic, explore the BMC DevOps Blog and the BMC Security & Compliance Blog or check out these articles:

- Is DevOps Dead?
- State of DevOps 2020: A Report Roundup
- How to Maximize SecOps Potential
- What is DevSecOps? DevSecOps Explained
- DevOps Guide, with 30+ articles on DevOps practices, culture, and recommendations