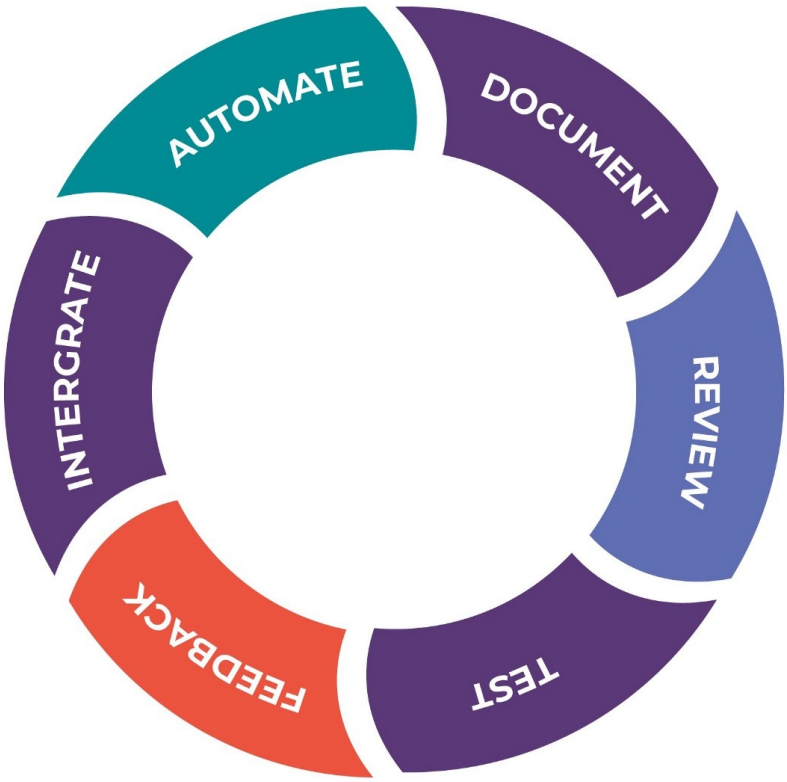
Fearless

DevSecOps: It's more than security

Fearless Sep 14 · 3 min read

A guest post from Fearless' Director of Engineering TJ Famodu:



DevSecOps, like many engineering terms, is thrown around a lot because it is very trendy in tech right now. Unfortunately, most people don't understand what DevSecOps means and what it truly does.

To start, DevSecOps is not a role or specific job on a team, it's a cultural mentality that the entire team must adopt for it to be successful. There is no saying, "There is a DevSecOps person on this project so we are doing DevSecOps."

Let's rewind to when DevOps was first introduced. DevOps initially included security in the same way DevSecOps is discussed today. But the industry's initial implementation of

DevOps focused mainly on breaking down the silos between development and operations. The broader industry defines DevOps as sharing the responsibility of development and operations across the team.

DevSecOps is about sharing the responsibility of development, ***security***, and operations across the team.

The importance of cross-functional teams

In a true DevSecOps culture, engineers carry and wear multiple hats. Besides software and infrastructure development and other traditional responsibilities seen in DevOps, they are also responsible for the security of the product.

This means ensuring vulnerability testing is being done and making sure static analysis scans are happening at the team level, instead of engaging with a separate security team to handle these responsibilities.

Unfortunately, my experience has shown that unless a team has experienced security people or there is a mandate to prioritize security, then it gets ignored until it is too late or something negative happens.

"The only thing more dangerous than a developer is a developer conspiring with security. The two working together gives us means, motive, and opportunity." –The Phoenix Project

Implementing DevSecOps shifts security left. What that means is shifting security toward the developer and prioritizing security at the beginning of development and not at the end or middle.

Compliance is a part of security, not a replacement for it

What I often hear when someone is talking about the security process and measures in a project, is that they are actually talking about compliance.

Security and compliance are very different things. Compliance is a component of security, it is not an interchangeable term for it.

"Compliance is not optional. It's the law. My job is to keep them out of orange jumpsuits…" - The Phoenix Project

At its most basic level, compliance focuses on regulatory or third party requirements. Compliance is critical but it can't be the end of a team's security discussion or process. Being too dependent on compliance often leads teams to view security as a one-off activity. If they've gone through the Authority to Operate (ATO) process then a team could fall into the trap of thinking they are fine moving forward security-wise and don't need to do anything else to maintain security.

Security, on the other hand, refers to tools, processes and systems used to protect a product's data and technology. Security is not a onetime checklist to complete, but requires continual maintenance. By adopting CI/CD and shifting security left to the teams, we can develop a culture of shared security ownership.

Team and organization adoption

Changing how your team works and adopting a DevSecOps mindset can be a very rocky transition. Think back to when your team transitioned to DevOps, that was probably difficult too. Changing the way people work requires a culture change and a mind shift.

You'll never have an entire organization sign on for change unless they see one team taking the first step and having success. I challenge you to be that first team in your organization.

To move an entire organization to DevSecOps at once there needs to be intense buy-in at the top. I prefer the team-by-team model because when it works successfully that team becomes a model for other teams to replicate.

Fearless has written before about how changing tech is easy, it's changing culture that's hard. Acknowledging difficulties and holding space for team members to have open dialogue will go a long way in successfully transitioning to DevSecOps.

DevOps | Devsecops | Devsecops Solutions | Devsecops Services | Devops Practice