Signs of a Failed DevSecOps Strategy Which None Should Ignore

DevOps, when combined with a robust security strategy, is what becomes DevSecOps. While DevOps is all about swift production and delivery, DevSecOps is all that DevOps is with security ingrained at its core. While this practice is not new, rigid security practices hamper productivity and developer experience. This impediment paved the way for the emergence of DevSecOps.

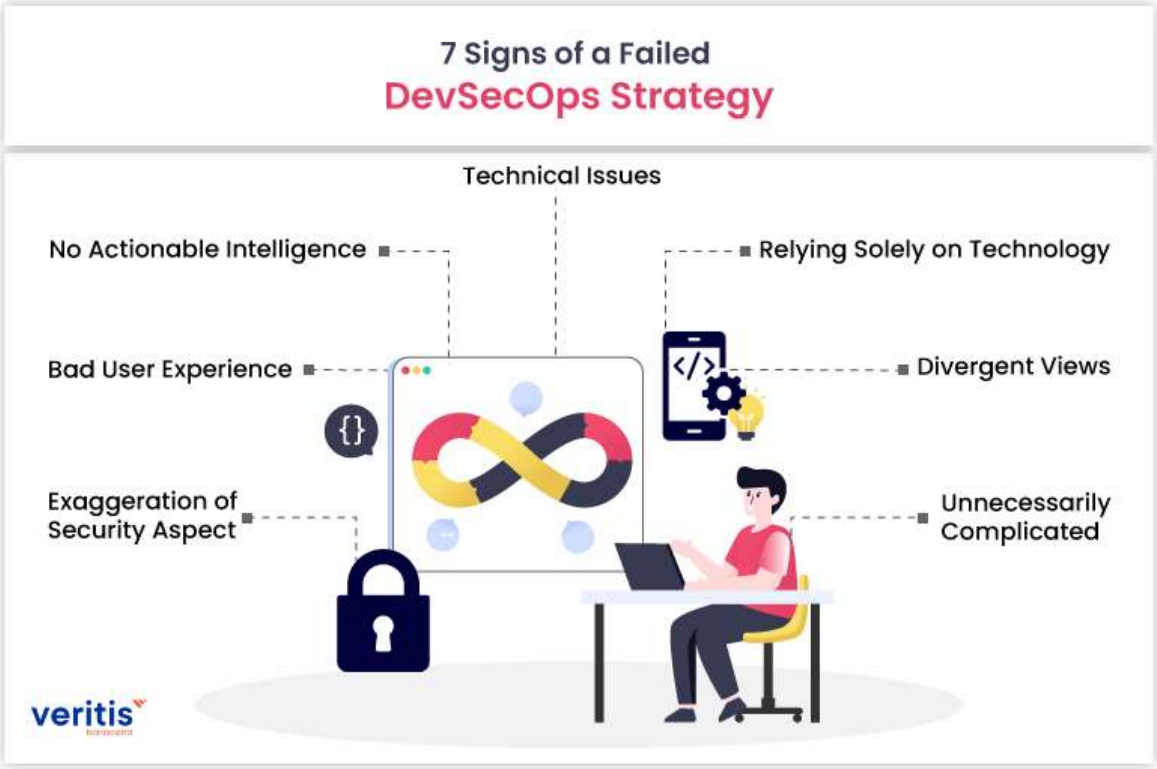
While most companies embraced **DevSecOps**, there is a significant risk of a potential failure as companies, without proper understanding, jump on the bandwagon to be a part of the next big thing. This approach will stunt productivity and incur unwanted expenses, which may lead to organization-wide ramifications.

But when does one realize that they have messed up with the implementation of DevSecOps? That is what this blog post seeks to address. Here, we shall outpoint what symptoms of a failed **DevSecOps strategy** are. Let's dig in.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

7 Signs of a Failed DevSecOps Strategy



1) Exaggeration of Security Aspect

Often organizations love to exaggerate what they possess. Although security is ingrained in every organization at some level, some like to indulge in unwarranted exaggeration by showcasing some minuscule security aspects. While the motivational reasons for this exaggeration are various, this would only result in cluelessness across the company.

With the management plastering DevSecOps over its marketing material and employees not knowing what the humbug is all about, there would likely be discord between the management and production teams. The matters will only worsen if the company accepts any DevSecOps project with the production team not knowing how to proceed. “Too many times, I’ve seen organizations say that they do DevSecOps when in reality there is little security involved,” says Sean Wright, lead application security SME at Immersive Labs. “

“Just because you have a tool in your process doesn’t necessarily mean you are doing DevSecOps.”

The company can cauterize this ailment by educating the employees on what DevSecOps is all about and not jumping the gun.

Useful Link: 6 DevOps Technical Benefits To ‘Startup’ Firms

---

2) Bad User Experience

DevSecOps is all about making life easy for all. Be it developers, testers, or users. But, if the strategy is shoddy, all three of them will bear the brunt as the end-user will be saddled with a poor user experience. The developers will have to devise new routes to better the experience, and testers will hammer out the bugs. The delayed rollout will only leave the clients/users waiting.

3) No Actionable Intelligence

Security reviews are supposed to produce actionable information on which the production team can better the deliverables or the entire product. However, if the company is dragging its feet on security review meetings and if these delayed meetings elicit little to no action items or insights regarding the product’s future, there is a problem.

The organization must take the DevSecOps strategy much more seriously and imbibe the same sense into its employees.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

4) Technical Issues

DevSecOps initiative means not only cultural change but also technical change. After the due assessment, the company should not leave any gaping holes. Ignoring this aspect will invite breaches and data thefts. Instead of hastily executing the **DevSecOps implementation strategy**, one should take the time out to assess the company's readiness when it comes to DevSecOps culture.

Useful Link: What are the best DevSecOps practices for security and balance agility?

---

5) Relying Solely on Technology

DevSecOps is not just a production approach but a cultural change. A successful DevSecOps strategy will usher in how people interact with each other. Be it the way developers and testers interact with each other, or the way users interact with the end-product; ultimately, a successful strategy will bring a welcome tectonic shift.

New challenges arise when this shift comes in, and a company should rely on people and technology to solve the problems.

If one is of the impression that automation and the rest other innovations of recent times will overcome the challenges and impediments, then it is a blunder. The organization should never forget that security has been ingrained in DevSecOps to protect the data of the clientele. Ignoring the human aspect of this strategy will be the same as shooting oneself in the foot.

6) Divergent Views

The management needs to take the production team along with their views. Should there be discord, meetings and discussions would end in stalemates, resulting in divergent views that lead nowhere.

Should one of the parties decide to be bullish, it would only result in more disagreements. It is essential to convince one another about the benefits and pitfalls of the strategy. This would stunt the chances of DevSecOps failures.

Useful Link: **DevSecOps Solution to Cloud Security Challenge**

7) Unnecessarily Complicated

Solutions are meant to simplify, but the purpose would be defeated if the clientele is made to run pillar to post. The user experience and production experience must be simple and secure. Ultimately, the goal is to better the time to market and increase the reliability on an overall front. If the development process is overly complicated, then there is little to no doubt that the DevSecOps strategy has gone awry.

Conclusion

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

In the age where strategies are cropping everywhere, it is pertinent for companies to perceive the new, emerging approaches with a pinch of salt. Instead of shouldering the load alone, one can seek out the services of an experienced MSP such as Veritis. Based out in Texas, Veritis has doled out unique and cost-effective solutions for its clients, who range from Fortune 500 to emerging enterprises. Since its inception, we have strived to deliver customized and cost-effective solutions.

And in the process of delivering robust solutions, we ingrain security at every step to ensure that that data is protected. So, reach out to us, and we shall better the working culture of your organization.

Services