DevSecOps: Moving Security Left in Contemporary Development Practices In the ever-evolving world of software development, security is no longer a box that gets ticked off at the end of the development lifecycle as a minor consideration.Top Strategies to Overcome Hurdles Here are some strategies organizations can adopt to implement DevSecOps successfully: Automate where you need to: Leverage tooling that has automation around code scanning, vulnerability detection, and compliance checks.Risk-based approaches: Focus on vulnerabilities that depend on the risk and likelihood rather than the noise of false positives Monitor and Optimize Performance: Regularly assess and tune security tools to reduce their effect on build times Embed Security mindset: Nurture a culture of shared, collective responsibility towards security, making it an integral part of software development.However, weighing up the challenges, the organizations that do in fact manage to embed security into their CI/CD pipelines derive numerous benefits in the shape of minimized risk, improved compliance and shorter delivery times.The emergence of DevSecOps, a methodology that embeds security practices within DevOps workflows, has transformed how application security is managed by organizations.Likewise, security teams do not always understand DevOps principles, so there is a skills gap in place that prevents collaboration from occurring.Cultural Resistance DevSecOps is a cultural change that encourages collaboration between developers, operations, and security teams.By building up Training: Equip your teams with the skills they need through regular training sessions and workshops, and encourage interaction between developers and security professionals.Skill Gaps The idea of securing CI/CD pipelines is that devs need to learn a bit of how security works, but that is often outside a their expertise.However, by overcoming these challenges with careful planning and cooperation, teams can make that security is more a facilitator to innovation than an inhibitor.]Especially in organizations where traditional silos have become entrenched practices, breaking down silos and mutualizing responsibility for security can be a difficult task.Set them up to run incrementally, on the new code changes.