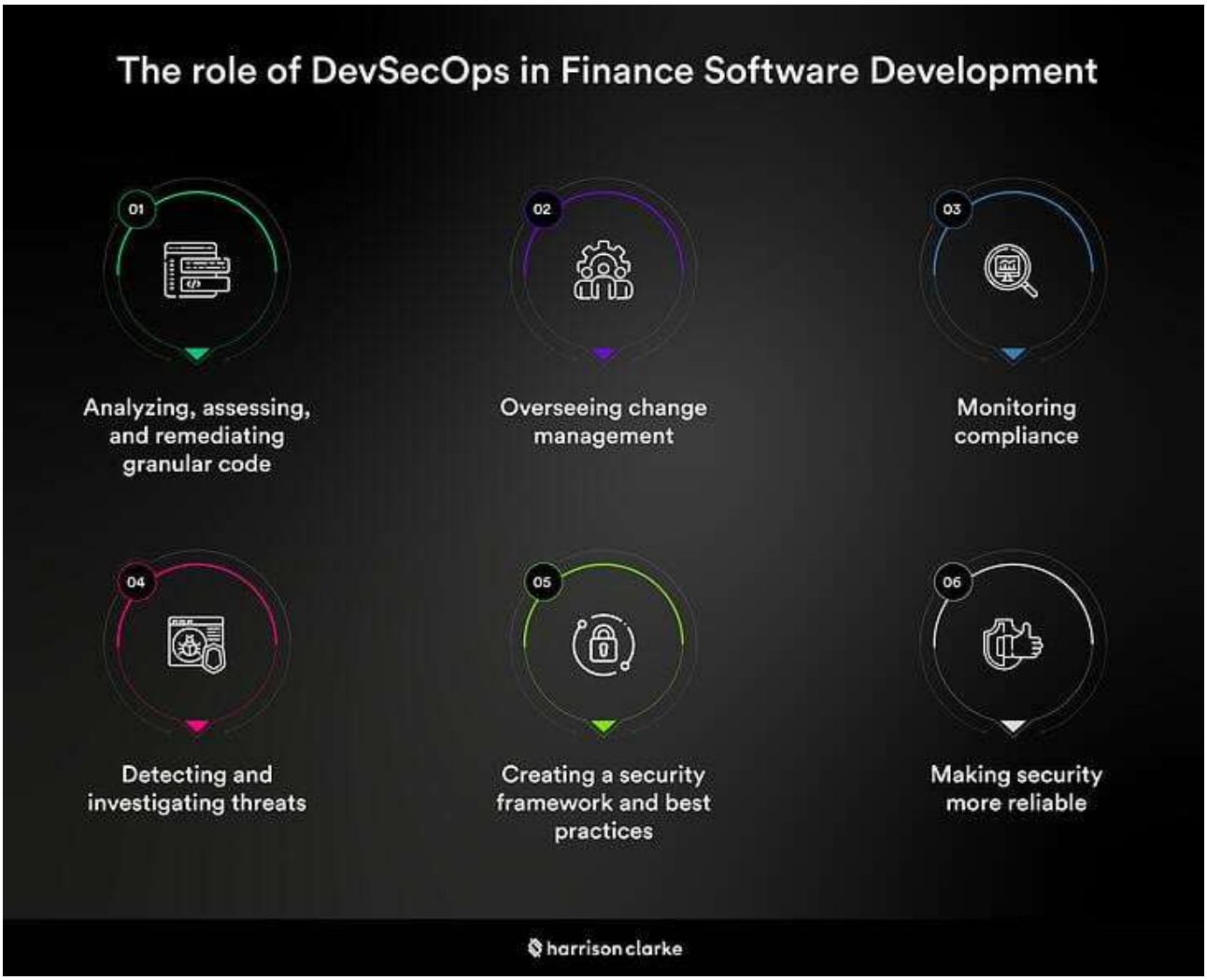
GETTING DEVSECOPS RIGHT

IN FINANCIAL SERVICES

Banks, finance organizations, and insurance companies face increasing pressure to improve their cyber security and increase the speed at which new software is released. They appear to be in conflict at a first impression. DevSecOps, however, provides a mechanism for financial services businesses to achieve these seemingly conflicting goals at the same time.

Development, security, and operations teams collaborate and automate their activities across the SDLC (software development lifecycle), resulting in frequent and secure releases of the software that supports digital business, including mobile apps, web service APIs, and IoT networks.



Challenges in the Financial Sector

The speed and security of software pipelines are top priorities for firms of all kinds, but those in the financial services sector face issues that are either unique or even more pronounced. A popular target for online criminals Financial institutions is a prominent target for cybercriminals because of the vast amounts of personal and financial data they store and process. Breaching a financial institution can provide hackers access to a wealth of private information, including personal and business financial records. As a result, these institutions are always under attack from all sides and with all tactics, even the most advanced and cutting-edge.

There is no way to predict when or how an institute will be the victim of a DDoS (distributed denial of service) attack, a ransomware attack, a phishing campaign, a zero-day vulnerability exploit, or an APT (advanced persistent threat).

Regulators have imposed a Heavy Burden

As one of the world's most heavily regulated businesses, financial services are subject to various industry mandates and government regulations. As you can imagine, this is an enormous strain on DevOps teams who must guarantee that the software they deliver to employees, customers, and partners conforms to an increasing number of complicated and often perplexing requirements in all the nations and areas where their organizations conduct business. If you don't follow the rules, you could face fines, legal liability, a damaged reputation and lost revenue.

A Digital world that is extremely Constrictive

The financial services industry's IT infrastructure is characterized by severe restrictions that impede agility more than any other, including air-gapped systems, increased access control, minimal cross-team collaboration, slow change management and approvals, rigorous auditing and governance, and limited flexibility for developers.

IT infrastructures in this sector tend to be complicated, big and heterogeneous ranging from on-premises data centres to current hybrid cloud deployments that use microservice architecture and containers. In addition, they must be able to handle a wide range of devices, including smartphones, ATMs, and point of sale terminals.

Due to disruptions brought about by New Technologies

When it comes to keeping up with technological innovation in their field, financial sector organizations are constantly under pressure to stay ahead of the curve. Recently, "fintech" advancements include Robo-advice and digital-only financial institutions, cryptocurrencies, blockchain and artificial intelligence-based services. Financial services organizations must regularly release updated software to maintain their digital offerings. Because of the risk of deploying software that has vulnerabilities, misconfigurations, or other security and compliance holes, many firms have generally avoided this speed of change.

DevSecOps protects & accelerates your SDLC

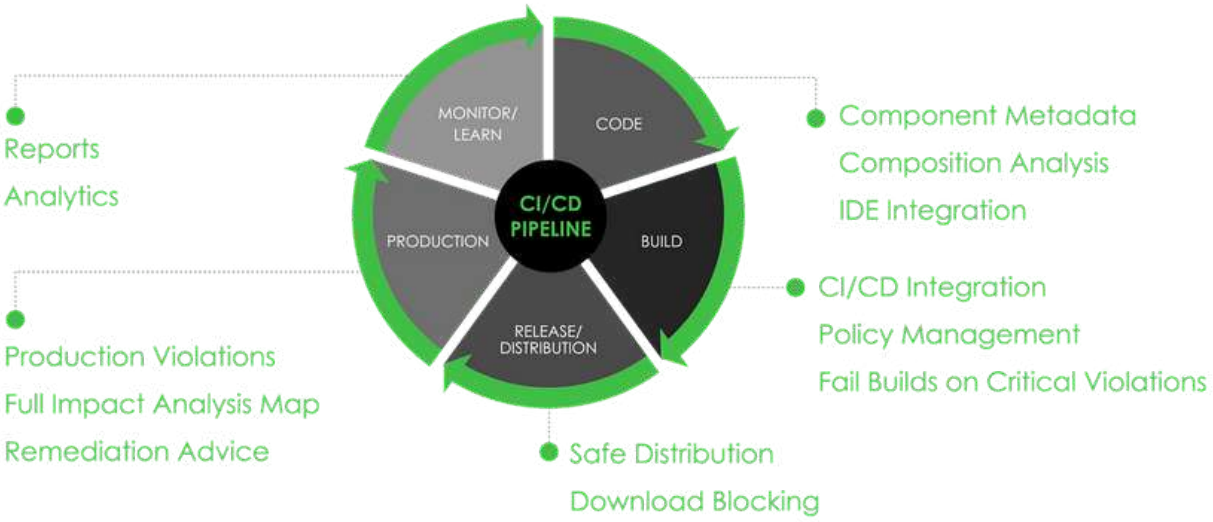
So, how do you go about dealing with these issues? How do you keep up with the pace of innovation while ensuring the security of your software? There should be an emphasis on making sure your SDLC processes are not just elegant but safe. DevSecOps makes that achievable, regardless of whether your IT environment is on-premises, on the cloud, or both. As a result of DevSecOps adoption, financial service organizations can:

- Set the stage for a culture of open communication, cooperation and shared accountability among all teams and stakeholders involved in the software development lifecycle (SDLC), including development, operations, security, and QA/testing.
- Automation and native integration of checks into every step of the SDLC from design to deployment is essential to ensure that faults are spotted early and frequently rectified, allowing for a more agile approach to software development.
- Suppose a software binary is determined to possess a significant vulnerability or compliance issue. In that case, you may immediately remedy the problem by tracing and granularly managing their software binaries throughout the SDLC.
- Every artefact generated by their SDLC should be authenticated to ensure that the builds created by a pipeline don't contain artefacts that have been tampered with.

A rise in Client Expectations

Customers' demands for a better digital experience from their financial institutions are only increasing. Banking, stock trading, payment processing and retirement account management are just some of the many digital services that consumers are looking for the ease of accessing on their smartphones, laptops and tablets. Digital transactions must be secure, and customers expect these service offerings to become more personalized, feature-rich, speedy and constantly available.

Changing financial service providers is now much easier for customers thanks to digitization, making it even more critical for these organizations to maintain and improve their digital customer experience.



Conclusion

In this booklet, we've outlined why financial services organizations need to use DevSecOps. DevSecOps aids businesses in securing their SDLC effectively while also allowing them to deliver software faster.

Financial service firms can reap the following DevSecOps benefits:

- End-to-end protection of the SDLC
- Accelerating the release of the software
- Dev, Ops, and security teams will see an increase in productivity.
- An increase in communication and cooperation between teams
- A rise in the standard of digital services in terms of their performance, dependability, and creativity
- A rise in the number of customers and revenue, as well as Increased revenue, Better customer retention, Lower costs & Enhanced customer experience

Want to learn more about how to successfully adopt DevSecOps in Financial Services?

ISmile Technologies DevSecOps Managed Services has all the features and functionalities to help you set up and manage an end-toend DevOps pipeline that releases secure and compliant software quickly and frequently.

Talk to an Expert Now!

About ISmile Technologies

ISmile Technologies is a proud automation-enabled intelligent cloud solution and managed IT services provider, and it is your multi-cloud technology advisor & key implementation partner.

We operate globally and leverage disruptive technologies alongside deep expertise to deliver business-specific cloud solutions. We maximize impact at an unparalleled value and securely accelerate business agility while infusing competitive excellence.

https://www.ismiletechnologies.com

sales@ISmileTechnologies.com

501 S Weber Rd Unit 108, Bolingbrook, IL 60490