autorabit

EBOOK

7 Ways Banks Can Improve Their Salesforce DevSecOps Pipeline

Maintaining Security While Increasing Velocity

INTRODUCTION

The financial industry has a lot to gain from optimizing their Salesforce DevSecOps processes. Stronger and more frequent releases help banks to better address the needs of their customers. New applications and updates can improve customer experience either through offering new services or providing helpful tools to team members.

DevOps has helped to accomplish these goals in the past. The emergence of DevSecOps involves many of the same processes with the addition of keeping an eye toward data security throughout the entire pipeline.

Data security is incredibly important to banks and other financial services companies. Certain precautions and protections are required through government regulations as well as customer demands.

So how can businesses in the financial industry provide the security and services their customers need, maintain high quality levels in these services, while also retaining a profitable ROI?

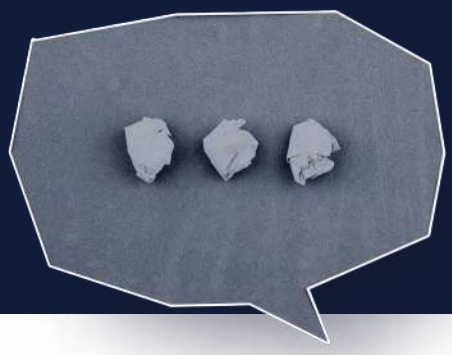
An optimized and streamlined DevSecOps platform provides the tools banks need to accomplish these goals.

Here are 7 things banks can do to improve their DevSecOps pipeline:

1. Facilitate Constant Communication Between Teams
2. Focus On Security Throughout the Pipeline
3. Utilize Automation
4. Sustain High Quality Code From the Start
5. Stress Adherence to Best Practices
6. Maintain Contemporary Data Backups + Recovery Capabilities
7. Monitor Successes and Opportunities for Improvement

01

Facilitate Constant Communication Between Teams



A successful and beneficial DevSecOps strategy is going to involve the efforts of team members across various departments. The levels of success for your Salesforce development projects will depend on how well these teams are able to work with each other.

Failures in communication will create problems. This can lead to broken deployments, compromised security measures, or poor performance by the completed product.

Banks provide a service that has a huge impact on the lives of their customers. Failures in these areas are simply not an option. And the first step toward accomplishing your goals is to ensure these lines of communication are open.

FIRST STEPS

Clearly describe every team member's role and what is expected of them. Make sure they know the surrounding structure to their role, so they know who to contact when they have a question or need help.

A clear hierarchy within your Salesforce DevSecOps pipeline decreases the chance that a team member won't have a clear direction when something comes up. Telling your team to communicate is important, but it simply won't happen if they don't know who they are supposed to be communicating with.

You must also give your team members a means of communicating with each other. The days of working on your particular task, handing it off to the next phase, and forgetting all about it are a thing of the past. DevSecOps requires the efforts of multiple departments throughout the various phases of the process. Utilize communication tools to make it easier for team members to interact.

02

Focus on Security Throughout the Pipeline

> *One of the best release management solutions out there in the market. Highly recommend it."*
>
> STELLA WAGNER

Banks are among the most highly targeted industries by cybercriminals. The majority of crime is motivated by money, and financial institutions have a large amount of sensitive information relating to finances.

The stability of basic coding structures might not seem like a security issue, but it is. In fact, every step of the DevSecOps pipeline will impact the overall security strategy and effectiveness of a given update or application.

A dedicated security team can run tests and diagnostics to verify the stability of a development project. And those efforts can be supported by communicating the importance of security measures to team members throughout the entire process.

FIRST STEPS

You'll often hear the phrase "shift left" in relation to shifting to a DevSecOps strategy. This refers to integrating security measures into every step of the pipeline. Previously, security checks wouldn't happen until the very end of the process (the right side of the development timeline). Shifting these concerns left means you are including security considerations in the early stages as well—such as planning and design.

Automation can be used to bolster these security efforts. Static Code Analysis—for example—inspects every line of code as it is written. Any potential bugs or errors are spotted, alerting the developer to their mistake. This allows them to fix the error before it can create a data security vulnerability.

Other tools such as Continuous Integration and Continuous Delivery can automate security checks as well. Utilizing these tools and making data security a priority will keep your end users safe and contribute to regulatory compliance.

03

Utilize Automation

Manual processes are an unavoidable aspect of a Salesforce DevSecOps pipeline. However, there are a variety of tools that are emerging and being perfected to assist with these processes.

Your team members are an integral aspect of your DevSecOps pipeline. However, even the most highly skilled team members are capable of making costly mistakes. There are aspects of the development process that can become repetitive. This is an environment likely to contribute to errors.

Code overwrites, unstable coding structures, or incomplete testing can create problems that impact interconnected areas of the project. And if they're not caught right away, these problems can compound themselves and become quite costly.

FIRST STEPS

Various financial institutions will have unique needs. The first thing you must do to optimize your Salesforce DevSecOps platform is to analyze your current capabilities, and set goals for how you would like to grow. Instituting automated processes is not likely to be done all at once.

So what are your priorities? What areas do you feel can be improved?

The answers to these questions will point you toward the automated processes that will best help your financial institution see quick results. Take this information and research the available options. However, keep in mind that your DevSecOps efforts will continue to progress, so utilizing a complete DevSecOps platform like AutoRABIT will make integrating these features much easier as your efforts become more mature.

> *"AutoRABIT has helped us add a lot of automation to our software development lifecycle. I highly recommend it!"*
>
> FOREST COOK

04

Sustain High Quality Code From the Start

> *Fantastic tool to implement CI/CD concept in Salesforce. The best part is end-to-end automated process for building, packaging, and test execution for Salesforce applications."*
>
> JASVINDER SINGH

Redundant work is a drain on your team members as well as your bottom line. Banks offer an essential service to their customers, but they're still businesses. And just like any other business, banks need to reduce overhead costs to maximize their returns.

Low quality code will create errors and bugs that will need to be addressed. This creates redundant work for your team members that takes them away from projects that will propel your institution higher in the financial industry.

And any low quality code that isn't caught before deployment will negatively impact the user's experience. Maintaining high quality code from the very beginning is the best way to produce the best products possible at the lowest cost.

FIRST STEPS

The quality of code throughout your Salesforce DevSecOps pipeline starts with your developers themselves. Finding and nurturing the most talented team members possible will yield benefits for a long time.

Static Code Analysis is a great tool that helps even the most talented developers to improve the quality of code they create. This essential tool monitors every line of code in real time for any potential errors. These errors become more costly to fix the later they are found in the pipeline, so the ability to spot them early saves your operation a lot of time and money.

Test your coding structures as they are merged with the main repository. Every line of defense should be used to ensure stability of the coding structure.

05

Stress Adherence to Best Practices

A successful DevSecOps pipeline depends on a combination of factors. You can have the most well-defined processes, top of the line tools, and open communication, but your pipeline won't be successful if the team members aren't performing their tasks correctly.

A series of best practices can be put in place to direct the efforts of your team. This includes tasks and habits specific to their roles, as well as general practices relating to how they interact with your Salesforce environment.

Failing to adhere to these practices can open the system up to hackers and runs the risk of accidentally triggering a data loss event.

FIRST STEPS

Analyze the ways in which your team members interact with your Salesforce environment. How are they accessing their accounts? Are they paying attention to how they use their computers? A simple mistake such as walking away from a computer without locking the screen can create an opportunity for disaster.

Here are some examples of potential best practices your bank can employ:

1. Use Secure Passwords
2. Enable Two Factor Authentication
3. Update User Permissions
4. Run Frequent System Audits
5. Be Aware of Phishing Attempts
6. Track Login History

These are only a few examples of practices that will support both data security as well as productivity within your DevSecOps pipeline.

06

Maintain Contemporary Data Backups + Recovery Capabilities

Data loss events can never be completely guarded against. Even if a series of best practices are instituted and followed, there are still vulnerabilities that can be exploited by cybercriminals.

But not all data loss events are due to malicious acts. Accidents by well-meaning team members can also compromise or altogether delete important system information.

Government regulations are put in place to dictate how these circumstances are protected against and addressed should they occur. The financial industry handles a lot of personally identifiable information that is subjected to these regulations.

FIRST STEPS

A discontinuation of service can be catastrophic for a bank. Customers can experience drastic consequences when they don't have access to their personal accounts. And if that information becomes compromised, they can have even greater issues.

Backing up your system data helps to have a reliable repository of information to fall back on should a massive data loss event occur. This helps you return to operations much faster than if this backup didn't exist.

These backups should be automated so you are assured to have a recent snapshot of your Salesforce DevSecOps environment.

You must also have the ability to restore this information, which is a different service from the backup itself. Retrieving the data from the backup repository and reinstituting it into your system will help you regain operations so you can continue providing essential services to your customers.

> *"It's one of the best release management solutions in the market! It has added useable value to our Salesforce experience."*
>
> GABBY KOONCE

07

Monitor Successes and Opportunities for Improvement

Every Salesforce DevSecOps project is going to pose its own series of challenges. This will require a slight tweaking of the development plan. These variances provide an opportunity to try new things and learn from their successes and failures.

Optimizing your Salesforce development pipeline involves continually updating your processes, methods, and standards. The insight gained from analyzing current and past projects can be used to inform alterations to methods or teachable moments for team members.

FIRST STEPS

Reporting capabilities provide repeatable and easy to understand metrics relating to your Salesforce DevSecOps pipeline.

Where are the most errors occurring? Are there any bottlenecks in the pipeline? Which team members are excelling in completing their tasks?

The answers to these questions will direct your efforts so you can magnify the successes and learn from underperforming areas of your pipeline.

Speak with team members to get their feedback and insights on the current DevSecOps framework. This valuable insight can be compiled and analyzed to alter and potentially optimize the processes used to develop your Salesforce projects.

> *"We have been using AutoRABIT since 2015, and it has transformed the way we deliver Salesforce applications."*
>
> DANIEL MUCHUMARRI

CONCLUSION

The process of optimizing a Salesforce DevSecOps pipeline is going to be different for everybody. However, those in the banking industry will need to include data security measures throughout every step of the process. Government regulations require this, but it's also your responsibility to protect your customers. There are various automated tools that will speed the development process along while also maintaining quality levels. These considerations are essential to providing the important services your customers expect.

An optimized and streamlined DevSecOps pipeline will position your company at the forefront of your industry. The market rewards those who are first to offer innovative products and services. And a streamlined development program is the best way to quickly and sufficiently address emerging customer needs.

ABOUT

autorabit

AutoRABIT is a Continuous Integration and Delivery suite for SaaS platforms. We automate and accelerate the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides automated Metadata Deployment, Version Controlling, Advanced Data Loading, Orgs and Sandbox management, Test Automation, and Reporting. Our services complement and extend Salesforce DX. AutoRABIT Vault—our backup and recovery solution—streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery and endpoint data protection on Cloud.

VISIT US TODAY TO LEARN MORE

www.autorabit.com