Payatu

DevSecOps Datasheet

OVERVIEW OF THE SERVICE

For organizations that follow a rapid product development model, where new features are released on a daily or weekly basis, the adoption of DevSecOps is becoming increasingly important. With the traditional waterfall development model, security was typically addressed towards the end of the development cycle, which often led to delays and additional costs.

In contrast, DevSecOps encourages a shift-left approach to security, where security is integrated into every stage of development, from planning and design to deployment and operations.

Security vulnerabilities are always attributed to significant losses when it comes to businesses and organizations.

With DevSecOps, the security team is involved from the very beginning of the development process. They work closely with the development team to identify potential security issues and suggest ways to address them.

Payatu is a leader in offering DevSecOps strategies and services to clients who want to identify and address security issues earlier in their development process, to reduce the likelihood of vulnerabilities in their final product.

KEY ATTRIBUTES

Payatu's objective is to assess the current posture of the client's CI/CD pipeline to help in improving overall level of security of the systems and what sets this service provider apart is -

A combination of realistic and abstract approach

Having substantial experience and understanding of DevOps approaches paired with security expertise helps Payatu Bandits to define a process and roadmap specific to the client.

End-to-end defining of the scope

It is important for Payatu to address all types of potential gaps in the client's DevOps process, which is why its scope covers everything ranging from code analysis, DAST, IaC, to SCA, VA, logging and monitoring.

Ultramodern tech integrations

Payatu strives to offer a widen coverage, by integrating different internal, external, and modern third-party tools and software.

Active collaboration throughout the project

Passive contributions and one way participation are shortcomings that can make any DevSecOps produce little to no results. With Payatu, clients get a partner that walks hand in hand with them, every step of the way, to build a robust DevSecOps pipeline.

The Payatu Extra Mile

Payatu goes an extra mile by offering guidance to the in-house security team of the client on getting the compliance of the systems with the mandated standards, and a lot more.

Payatu

KEY BENEFITS

Payatu's goal is to help its clients create a culture of collaboration between development, security, and operations teams, with a shared responsibility for building secure and reliable software.

01 Security Testing to Build Secure Software

Security testing can help clients in identifying security problems in the software before deployment. Payatu tests the CI/CD pipelines of the clients to identify gaps so that the clients can build a more secure pipeline and software.

02 Understanding Client's Pain Points to Design Custom Solutions

Every organization comes with a different set of requirements and pain points, which means each company has different security needs. Payatu offers tailored DevSecOps approaches to cater to each client's unique needs and provide a more effective and efficient solution.

03 High-level DevSecOps Expertise to Achieve Desired Security Posture

Payatu Bandits are experts in the said field and can help clients understand the best practices for integrating security into their software development process and recommend specific tools and techniques to achieve their security goals.

04 Build Brand Confidence for Users

Clients can make security their value proposition in the competitive digital market by establishing trust within their users/clients by offering security as their brands proposition.

05 Improved Software Security for Better Brand Reputation

By integrating security into the software development lifecycle, organizations can reduce the likelihood of security breaches and improve their overall brand reputation.

06 High-Quality Offerings

9 out of 10 industry leaders have made it a point to recommend Payatu's services to other pioneers because of the experiences they had while availing the DevSecOps offering. This has been made possible because of the best-in-class hires who have proved their mettle by going beyond their scope of work, even before they're hired.

Top Customers

butn®

Payatu

ENGAGEMENT MODELS

You choose what works best for you!

Payatu offers different engagement models to let the client decide what floats their boat when they avail themselves of the web application security assessment service. They can choose from

01

Expert Guidance

Under this model, clients will be guided by Payatu's DevSecOps' experts on what's missing in their CI/CD pipeline and how they can fix these gaps, in order to achieve a stronger security posture.

Hours allotted per week = 10-20 hours

02

Deep Involvement

Pipeline Conversion

Clients that have a DevOps pipeline and want to convert it to a robust DevSecOps pipeline will be assisted by dedicated Payatu experts throughout the entire conversion process.

Hours allotted per week, with dedicated personnel = 40-80 hour

Pipeline Development

Payatu helps its clients set up an entire DevSecOps pipeline from scratch under this model. They are assigned dedicated DevSecOps experts who will create the entire pipeline from start to finish.

Hours allotted per week, with dedicated personnel = 40-80 hours

The depth of involvement will be decided according to levels of comprehensiveness

Level	Tools Integration	Time Estimation (Approximately)	Deliverables
1	SAST	1-2 week	Tool Deployment + Configuration + Optimization
2	SAST, DAST	2-4 weeks	
3	SAST, DAST, IaC, SCA	4-6 weeks	