CyStack

DATA SHEET

DevSecOps

Securing your software development from start to finish

Develop software based on secure-by-design concepts

DevSecOps is a software development approach that integrates security practices into the Software development lifecycle (SDLC). The goal of DevSecOps is to create a culture where security is an integral part of the software development process rather than an afterthought or a separate function.

DevSecOps is an expansion of the DevOps methodology, which combines development, security, and operations in software development. The three terms represent distinct responsibilities of software teams throughout the development process:

- **Development** involves the planning, coding, building, and testing of the application.
- **Security** means incorporating security measures earlier in the software development lifecycle. This can involve developers ensuring that the code is secure and free from vulnerabilities, while security practitioners test the software to detect any potential security flaws before it is released.
- **Operations** refers to the team responsible for deploying, monitoring, and addressing any issues that arise with the software.

In a DevSecOps environment, security is automated and integrated into the software development process from the beginning, rather than being added on at the end. This means that security is built into the code, and security testing and monitoring are automated and continuous.

By integrating security into the DevOps process, DevSecOps aims to improve the security of software applications, reduce the risk of security vulnerabilities and breaches, and increase the speed and efficiency of software development and deployment.

Customer Benefits

- Catch software vulnerabilities early
- Continuous feedback and improvement
- Faster time to market
- Build a security-aware culture
- Cost savings

How CyStack Helps

At CyStack, we understand the importance of integrating security into the software development process. We know that it can be challenging to apply security in the SDLC, but we have successfully implemented both DevOps and DevSecOps methodologies. We can help our customers achieve the same level of security and efficiency in their software development by offering DevSecOps services.

Our experience in building software using DevOps and DevSecOps methodologies has enabled us to create a culture of collaboration and shared responsibility for security across development, security, and operations teams. Our customers can benefit from our expertise and knowledge by adopting a similar approach, which will improve the security of their software applications and reduce the risk of security breaches.

There are many benefits to adopting DevSecOps practices in software development including:

- **Catch software vulnerabilities early**
  The DevSecOps approach involves conducting security checks at each stage instead of waiting until the software is completed. By detecting security issues at earlier stages, software teams can reduce the cost and time of fixing vulnerabilities, which results in minimal disruption and greater security for users after the application is produced.
- **Continuous feedback and improvement**
  DevSecOps practices involve regular security assessments and vulnerability scanning, which provide continuous feedback on the security of software applications. This allows developers to identify and address security issues more quickly, leading to continuous improvement in the security of the software.
- **Faster time to market**
  DevSecOps automates many security tasks and integrates security testing and monitoring into the development process, resulting in faster software development and deployment. This allows companies to bring products to market more quickly and stay ahead of their competitors.
- **Build a security-aware culture**
  DevSecOps encourages the dev team to become more proactive in spotting potential security issues in the code, modules, or other technologies used to build the application. This approach creates a shared understanding of software security and promotes best practices for secure development.
- **Cost savings**
  DevSecOps practices can reduce the cost of security testing and remediation by integrating security into the development process. This can help companies save money on security-related expenses while also reducing the risk of costly security breaches.

How does DevSecOps work?

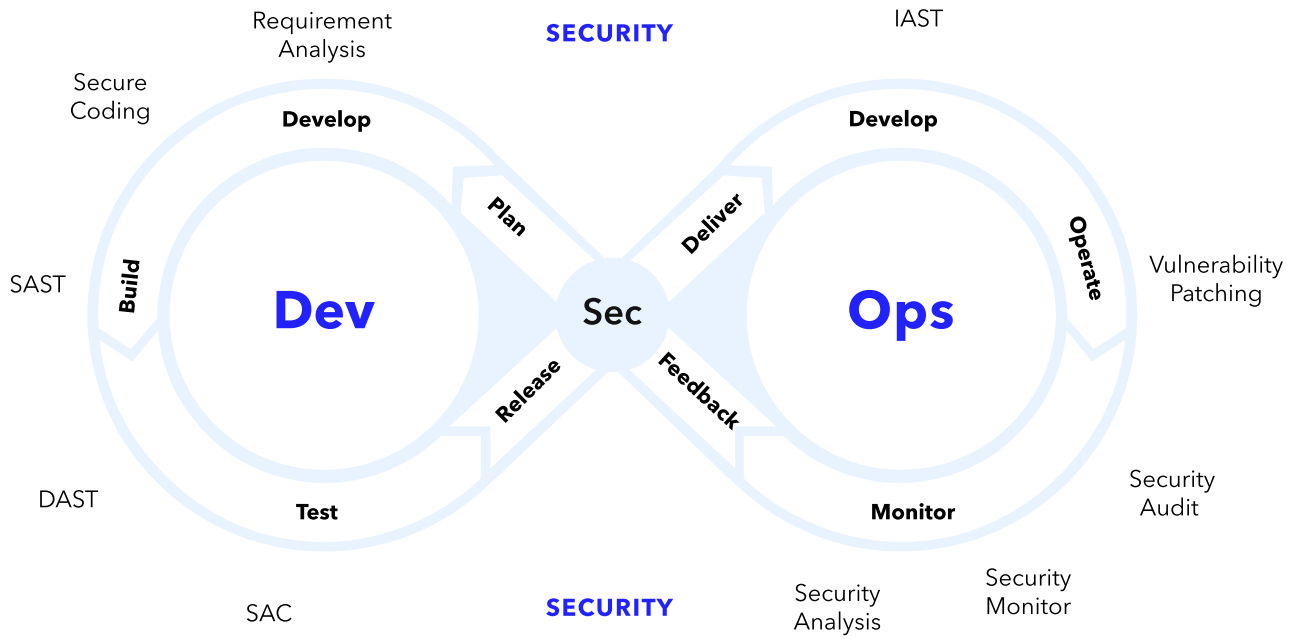
To implement DevSecOps, software teams need to implement DevOps and continuous integration first.

DevOps is a software development culture that brings together development and operations teams using tools and automation to promote collaboration and communication. This results in quicker software development while maintaining flexibility for changes.

Continuous integration and continuous delivery (CI/CD) is another modern software development practice that uses automated build-and-test steps to reliably and efficiently deliver small changes to the application. Developers use CI/CD tools to release new versions of an application and respond quickly to issues after users have access to the application.

DevSecOps brings security into the DevOps practice by integrating security assessments throughout the CI/CD process. It makes security a shared responsibility among all team members who are involved in building the software. The development team collaborates with the security team before writing any code, and operations teams continue to monitor the software for security issues after deployment. As a result, companies can deliver secure software faster and ensure compliance.

Compared to DevOps, which focuses on getting an application to market as fast as possible, DevSecOps makes security testing part of the application development process itself. Security teams and developers collaborate to protect users from software vulnerabilities. Security engineers check weaknesses, developers design the code to prevent vulnerabilities, and testers test all changes to prevent unauthorized third-party access.



Best practices for DevSecOps

The best practices for DevSecOps involve integrating security controls into the development, delivery, and operational processes in a natural way.

Shift left

The concept of "Shift left" is an important aspect of DevSecOps. It involves moving security practices and controls from the later stages of the delivery process to the beginning of the development process. By integrating security into the development process from the start, organizations using DevSecOps can identify and address security risks and threats early on. This requires the involvement of cybersecurity architects and engineers as part of the development team, who ensure that every component and configuration item is securely patched and documented. "Shift left" ensures that security is not an afterthought but a key consideration from the very beginning of the development process, allowing for more efficient and effective security practices.

Culture: Communication, people, technology, and process

To implement DevSecOps, a cultural shift is necessary, and it starts with senior leaders explaining the importance and benefits of adopting security practices to the DevOps team. This communication element is vital for promoting cultural change throughout the organization while the people component leads to a transformation involving software teams. With DevSecOps, software developers and operations teams work closely with security experts to improve security throughout the development process.

The technology aspect of DevSecOps is crucial for performing CI/CD and automated security testing during development. Finally, a DevSecOps process emphasizes the importance of integrating security into every stage of the software development lifecycle. This requires a change in mindset and a shift in traditional development processes.

Security education

To ensure that everyone in the organization understands the company's security posture and follows the same standards, it is important to educate all involved parties on security principles. This includes development engineers, operations teams, and compliance teams. Basic principles of application security, such as the OWASP top 10 and security testing, should be understood by everyone. Developers should have knowledge of threat models, compliance checks, risk measurement, exposure, and security control implementation. Compliance with security controls requires a combination of engineering and compliance, and an alliance between teams can help ensure that these controls are met.

Traceability, auditability, and visibility

Incorporating traceability, auditability, and visibility in a DevSecOps process can lead to a more secure environment and deeper insight. Traceability involves tracking configuration items throughout the development cycle and ensuring compliance, reducing bugs, and maintaining code. Auditability is crucial for compliance with security controls and requires well-documented technical, procedural, and administrative security controls that all team members adhere to. Visibility is important for management and a DevSecOps environment, allowing for a monitoring system that can measure the operation, send alerts, increase awareness of changes and cyberattacks, and provide accountability throughout the project lifecycle.

Common DevSecOps tools

DevSecOps teams utilize various tools to detect and report security flaws during software development:

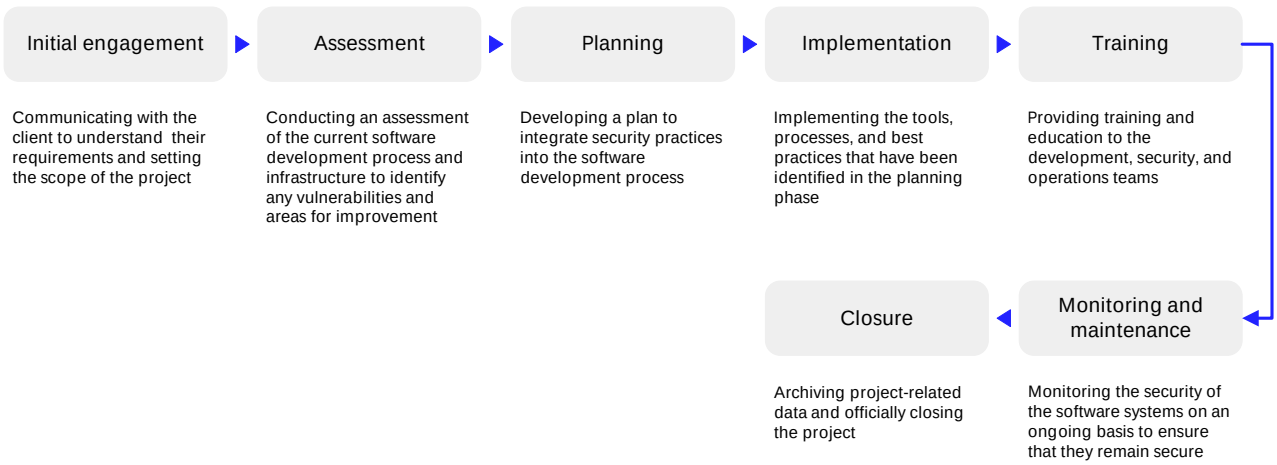
- **Static application security testing (SAST)**: Scan source code for vulnerabilities.
- **Software composition analysis (SCA)**: Inspect an unknown codebase and document the open-source components used, their vulnerabilities, and other information.
- **Interactive application security testing (IAST)**: Utilize security monitors within the application to assess potential vulnerabilities in the production environment.
- **Dynamic application security testing (DAST)**: Simulate attacks on applications from outside the network and identify vulnerabilities by interacting with the application just as an attacker would.

Methodology

CyStack DevSecOps service methodology includes the following steps:

1. **Assess the current state**: Evaluate the customer's current software development and delivery processes, tools, and security posture.
2. **Develop a DevSecOps strategy**: Develop a customized DevSecOps strategy based on the customer's needs and goals. This strategy should include selecting appropriate tools and processes to implement security controls throughout the software development life cycle.
3. **Align security and development teams**: Ensure that the security and development teams are aligned and working together from the beginning of the development process. This includes incorporating security requirements into the product backlog and ensuring security is included in each stage of the development cycle.
4. **Implement security controls**: Implement security controls using automated security testing tools such as SAST, DAST, IAST, and SCA to detect and remediate vulnerabilities throughout the development life cycle.
5. **Monitor and maintain security**: Establish ongoing monitoring and maintenance of security controls and processes, including regular assessments and continuous improvement of security practices.
6. **Train and educate personnel**: Train and educate personnel on DevSecOps principles, security best practices, and tools to ensure everyone in the organization is aware of their roles and responsibilities in maintaining a secure development process.
7. **Measure and report progress**: Measure and report progress to the customer regularly, including metrics on vulnerabilities detected and remediated, compliance with security requirements, and overall security posture.

Flow To Work With Clients



About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net