CyStack

DATA SHEET

DevSecOps

Đảm bảo sản phẩm an toàn trong suốt quy trình phát triển phần mềm

Phát triển phần mềm với nguyên tắc an toàn từ khâu thiết kế

DevSecOps là phương pháp tích hợp bảo mật vào vòng đời phát triển của phần mềm. Mục tiêu của DevSecOps là tạo ra một văn hóa lập trình, trong đó bảo mật là một phần không thể thiếu của quy trình phát triển phần mềm chứ không phải là một chức năng riêng biệt hoặc được thực hiện sau đó.

DevSecOps là dạng mở rộng của phương pháp DevOps, kết hợp phát triển, bảo mật và vận hành trong quá trình phát triển phần mềm. Ba thuật ngữ thể hiện trách nhiệm riêng biệt của các đội ngũ kĩ thuật trong suốt quá trình phát triển:

- **Phát triển** liên quan đến việc lập kế hoạch, viết code, xây dựng và kiểm thử ứng dụng.
- **Bảo mật** là sự kết hợp các biện pháp bảo mật sớm hơn trong vòng đời phát triển phần mềm, bao gồm việc các lập trình viên đảm bảo rằng mã nguồn an toàn và không có lỗ hổng, trong khi các chuyên gia bảo mật kiểm thử phần mềm để phát hiện bất kỳ lỗ hổng bảo mật tiềm ẩn nào trước khi phát hành.
- **Vận hành** đề cập đến nhóm chịu trách nhiệm triển khai, giám sát và giải quyết mọi vấn đề phát sinh với phần mềm.

Trong môi trường DevSecOps, các biện pháp bảo mật được tự động hóa và tích hợp vào quy trình phát triển phần mềm ngay từ đầu, thay vì được thêm vào cuối cùng. Điều này có nghĩa là tính bảo mật được "xây dựng" từ trong mã nguồn, đồng thời quá trình kiểm tra và giám sát bảo mật diễn ra tự động và liên tục.

Bằng cách tích hợp bảo mật vào quy trình DevOps, DevSecOps có thể cải thiện tính an toàn của các ứng dụng, phần mềm, giảm nguy cơ tồn tại lỗ hổng và vi phạm bảo mật, đồng thời tăng tốc độ và tính hiệu quả của việc phát triển và triển khai phần mềm.

Lợi ích của khách hàng

- Nhận biết lỗ hổng phần mềm sớm
- Liên tục nhận phản hồi và cải thiện
- Thời gian tiếp cận thị trường nhanh hơn
- Xây dựng văn hóa nhận thức về bảo mật
- Tiết kiệm chi phí

Giải pháp của CyStack

Hiểu tầm quan trọng của việc tích hợp bảo mật vào quy trình phát triển phần mềm, biết rằng có thể khó áp dụng bảo mật trong vòng đời phát triển, nhưng CyStack đã triển khai thành công cả phương pháp DevOps và DevSecOps. CyStack giúp khách hàng của mình đạt được mức độ bảo mật và hiệu quả tương tự trong quá trình phát triển phần mềm của họ bằng cách cung cấp các dịch vụ DevSecOps.

Kinh nghiệm trong việc xây dựng phần mềm bằng các phương pháp DevOps và DevSecOps cho phép CyStack tạo ra văn hóa cộng tác và chia sẻ trách nhiệm về bảo mật giữa các đội ngũ phát triển, bảo mật và vận hành. Khách hàng được hưởng nhiều quyền lợi từ chuyên môn và kiến thức của CyStack bằng việc áp dụng cách tiếp cận tương tự, từ đó cải thiện tính an toàn cho các ứng dụng và giảm nguy cơ vi phạm bảo mật.

Có nhiều lợi ích khi áp dụng các phương pháp DevSecOps trong phát triển phần mềm, bao gồm:

- **Nhận biết lỗ hổng phần mềm sớm**
  Phương pháp DevSecOps sẽ tiến hành kiểm tra bảo mật ở từng giai đoạn thay vì đợi cho đến khi phần mềm hoàn tất. Bằng cách phát hiện các vấn đề bảo mật sớm hơn, đội ngũ phát triển có thể giảm chi phí và thời gian khắc phục các lỗ hổng, giúp giảm thiểu sự gián đoạn và tăng cường tính bảo mật cho người dùng.
- **Liên tục phản hồi và cải thiện**
  Phương pháp DevSecOps đánh giá bảo mật thường xuyên bằng cách quét lỗ hổng, cung cấp phản hồi liên tục về bảo mật của các ứng dụng. Điều này cho phép các nhà phát triển xác định và giải quyết vấn đề bảo mật nhanh hơn, dẫn đến cải thiện liên tục về an ninh của phần mềm.
- **Thời gian tiếp cận thị trường nhanh hơn**
  DevSecOps tự động hóa nhiều tác vụ bảo mật, đồng thời tích hợp kiểm tra và giám sát bảo mật vào quy trình phát triển, giúp triển khai phần mềm nhanh hơn. Điều này cho phép các công ty đưa sản phẩm ra thị trường nhanh hơn và đi trước các đối thủ cạnh tranh.
- **Xây dựng văn hóa nhận thức về bảo mật**
  DevSecOps khuyến khích lập trình viên chủ động hơn trong việc phát hiện các vấn đề bảo mật tiềm ẩn trong mã nguồn, mô-đun hoặc các công nghệ khác được sử dụng. Cách tiếp cận này tạo ra sự hiểu biết chung về bảo mật và thúc đẩy các phương pháp tốt nhất để phát triển bảo mật.
- **Tiết kiệm chi phí**
  Các phương pháp DevSecOps có thể giảm chi phí kiểm tra và khắc phục bảo mật bằng cách tích hợp bảo mật vào quy trình phát triển. Điều này có thể giúp các công ty tiết kiệm tiền cho các chi phí liên quan đến bảo mật.

Quy trình DevSecOps

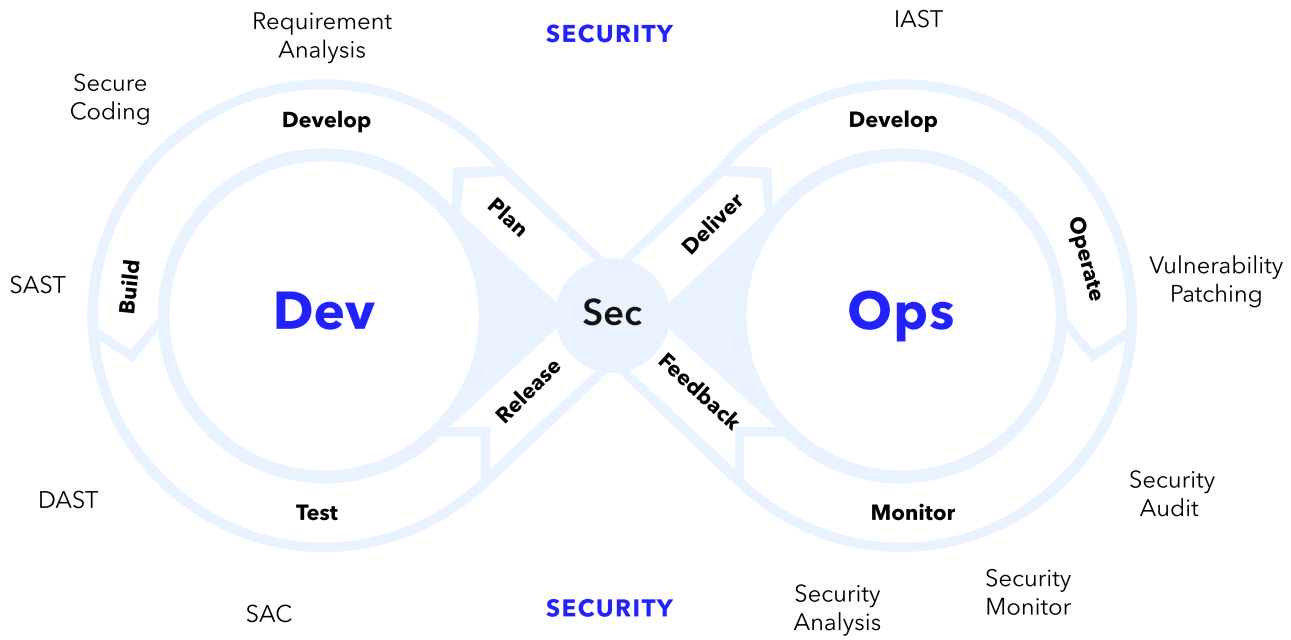
Để triển khai DevSecOps, trước tiên, đội ngũ phát triển phần mềm cần triển khai DevOps và luồng CI/CD.

DevOps là một văn hóa phát triển phần mềm, trong đó kết hợp các đội ngũ phát triển và vận hành bằng cách tự động hóa để thúc đẩy việc hợp tác và giao tiếp. Từ đó giúp cho việc phát triển phần mềm nhanh hơn trong khi vẫn duy trì tính linh hoạt.

CI/CD là một phương pháp phát triển phần mềm hiện đại khác, bao gồm các bước xây dựng và kiểm thử tự động để cung cấp những thay đổi nhỏ cho ứng dụng một cách đáng tin cậy và hiệu quả. Các nhà phát triển sử dụng công cụ CI/CD để phát hành các phiên bản mới của ứng dụng và phản hồi nhanh chóng đối với những sự cố bất ngờ.

DevSecOps đưa bảo mật vào DevOps bằng cách tích hợp các đánh giá bảo mật trong suốt quy trình CI/CD, khiến bảo mật trở thành trách nhiệm chung giữa tất cả các thành viên trong đội ngũ xây dựng phần mềm. Đội ngũ phát triển cộng tác với đội bảo mật trước khi viết mã nguồn và đội ngũ vận hành tiếp tục theo dõi phần mềm để tìm các vấn đề bảo mật sau khi triển khai. Kết quả là, các công ty có thể cung cấp phần mềm một cách nhanh hơn, an toàn nhanh hơn.

So với DevOps, vốn tập trung vào việc đưa ứng dụng ra thị trường nhanh nhất có thể, DevSecOps biến việc kiểm tra bảo mật thành một phần của chính quy trình phát triển ứng dụng. Các kĩ sư bảo mật và nhà phát triển hợp tác để bảo vệ người dùng khỏi các lỗ hổng phần mềm. Các kỹ sư bảo mật kiểm tra các điểm yếu, các nhà phát triển thiết kế mã nguồn để ngăn chặn các lỗ hổng và kiểm tra tất cả các thay đổi để ngăn chặn truy cập trái phép của bên thứ ba.



Các phương pháp DevSecOps tốt nhất

Các phương pháp DevSecOps tốt nhất cần tích hợp được các biện pháp kiểm soát bảo mật vào quy trình phát triển, phân phối và vận hành một cách tự nhiên.

Shift left

"Shift left" là một khái niệm quan trọng của DevSecOps, chính là việc di chuyển các biện pháp kiểm soát và thực hành bảo mật từ các giai đoạn sau chuyển giao sang giai đoạn đầu của quy trình phát triển. Bằng cách tích hợp bảo mật vào quy trình phát triển ngay từ đầu, các doanh nghiệp sử dụng DevSecOps có thể xác định và giải quyết sớm nhiều rủi ro và mối đe dọa bảo mật. Điều này đòi hỏi sự tham gia của các kiến trúc sư hạ tầng và kỹ sư an ninh mạng như một phần của đội ngũ phát triển, những người đảm bảo rằng mọi thành phần và cấu hình đều được vá và log lại một cách an toàn. "Shift left" đảm bảo rằng bảo mật không phải là vấn đề được cân nhắc kỹ lưỡng mà là yếu tố quan trọng cần cân nhắc ngay từ đầu trong quá trình phát triển, cho phép thực hiện các biện pháp bảo mật ngày càng hiệu quả hơn.

Văn hóa: Giao tiếp, con người, công nghệ và quy trình

Để triển khai DevSecOps, cần phải thay đổi văn hóa, bắt đầu bằng việc các lãnh đạo cấp cao giải thích tầm quan trọng và lợi ích của việc áp dụng các phương pháp bảo mật cho đội ngũ DevOps. Yếu tố giao tiếp này rất quan trọng để thúc đẩy thay đổi văn hóa của toàn bộ tổ chức trong khi thành phần con người là yếu tố quan trọng nhất. Với DevSecOps, các lập trình viên phần mềm và đội ngũ vận hành hợp tác chặt chẽ với các chuyên gia bảo mật để cải thiện tính bảo mật trong suốt quá trình phát triển.

Khía cạnh công nghệ của DevSecOps rất quan trọng để thực hiện CI/CD và kiểm tra bảo mật tự động trong quá trình phát triển. Cuối cùng, quy trình DevSecOps nhấn mạnh tầm quan trọng của việc tích hợp bảo mật vào mọi giai đoạn của vòng đời phát triển phần mềm. Điều này đòi hỏi một sự thay đổi trong tư duy và sự thay đổi trong các quy trình phát triển truyền thống.

Đào tạo bảo mật

Để đảm bảo rằng mọi người trong doanh nghiệp hiểu tình hình bảo mật của công ty và tuân theo các tiêu chuẩn giống nhau, điều quan trọng là phải đào tạo tất cả các bên liên quan về những nguyên tắc bảo mật. Trong đó bao gồm các kỹ sư phát triển, nhóm vận hành và nhóm kiểm thử. Mọi người nên hiểu các nguyên tắc cơ bản về bảo mật ứng dụng, như top 10 OWASP và kiểm thử bảo mật. Các lập trình viên nên có kiến thức về các mô hình hóa mối đe dọa, kiểm thử cơ bản, đo lường rủi ro, bề mặt tấn công và triển khai kiểm soát bảo mật. Việc tuân thủ các biện pháp kiểm soát bảo mật yêu cầu sự kết hợp giữa kỹ thuật và tính kỷ luật, đồng thời cần cả sự liên kết chặt chẽ giữa các đội ngũ kỹ thuật.

Khả năng truy xuất, khả năng kiểm thử và khả năng hiển thị

Kết hợp khả năng truy xuất, khả năng kiểm thử và khả năng hiển thị trong quy trình DevSecOps có thể tạo ra một môi trường an toàn hơn cùng hiểu biết sâu sắc hơn. Khả năng truy xuất liên quan đến việc theo dõi cấu hình trong suốt chu kỳ phát triển và đảm bảo tuân thủ, giảm tần suất lỗi và duy trì mã nguồn. Khả năng kiểm thử rất quan trọng đối với việc tuân thủ các biện pháp kiểm soát bảo mật, yêu cầu thủ tục và kỹ thuật được lập thành văn bản rõ ràng mà tất cả các thành viên trong nhóm đều phải tuân thủ. Khả năng hiển thị rất quan trọng đối với việc quản lý nói chung và môi trường DevSecOps nói riêng, cho phép hệ thống giám sát có thể đo lường hoạt động, gửi cảnh báo, nâng cao nhận thức về các tấn công mạng, đồng thời cung cấp trách nhiệm giải trình trong suốt vòng đời của dự án.

Các công cụ DevSecOps phổ biến

Đội ngũ DevSecOps sử dụng nhiều công cụ khác nhau để phát hiện và báo cáo các lỗi bảo mật trong quá trình phát triển phần mềm:

- **Kiểm thử bảo mật tĩnh (SAST)**: Quét mã nguồn để tìm lỗ hổng.
- **Phân tích thành phần phần mềm (SCA)**: Kiểm tra một hệ thống mã nguồn không xác định và ghi lại các thành phần nguồn mở được sử dụng kèm theo lỗ hổng và các thông tin khác.
- **Kiểm thử bảo mật ứng dụng tương tác (IAST)**: Sử dụng trình giám sát bảo mật trong ứng dụng để đánh giá các lỗ hổng tiềm ẩn trong môi trường thật.
- **Kiểm thử bảo mật động (DAST)**: Mô phỏng các cuộc tấn công vào ứng dụng từ bên ngoài và xác định các lỗ hổng bằng cách tương tác với ứng dụng giống như kẻ tấn công.

Phương pháp luận

Dịch vụ CyStack DevSecOps được tiến hành theo các bước sau:

1. **Đánh giá trạng thái hiện tại**: Đánh giá các quy trình, công cụ và tình trạng bảo mật cũng như phát triển phần mềm hiện tại của khách hàng.
2. **Phát triển chiến lược DevSecOps**: Phát triển chiến lược DevSecOps tùy chỉnh dựa trên nhu cầu và mục tiêu của khách hàng. Chiến lược này nên bao gồm việc lựa chọn các công cụ và quy trình phù hợp để triển khai các biện pháp kiểm soát bảo mật trong suốt vòng đời phát triển phần mềm.
3. **Sắp xếp đội ngũ phát triển và bảo mật**: Đảm bảo rằng các đội ngũ bảo mật và phát triển được liên kết và làm việc cùng nhau ngay từ đầu quá trình phát triển. Điều này bao gồm việc kết hợp các yêu cầu bảo mật vào từng giai đoạn của chu kỳ phát triển.
4. **Thực hiện kiểm soát bảo mật**: Thực hiện kiểm soát bảo mật bằng cách sử dụng các công cụ kiểm tra bảo mật tự động như SAST, DAST, IAST và SCA để phát hiện và khắc phục các lỗ hổng trong suốt vòng đời phát triển.
5. **Giám sát và duy trì bảo mật**: Thiết lập giám sát và duy trì liên tục các quy trình và kiểm soát bảo mật, bao gồm đánh giá thường xuyên và phát triển liên tục các biện pháp bảo mật.
6. **Đào tạo và giáo dục nhân sự**: Đào tạo và giáo dục nhân viên về các nguyên tắc DevSecOps, các phương pháp tốt nhất về bảo mật cũng như các công cụ để đảm bảo mọi người trong doanh nghiệp nhận thức được vai trò và trách nhiệm của họ trong việc duy trì quy trình phát triển an toàn.
7. **Đo lường và báo cáo tiến độ**: Đo lường và báo cáo tiến độ cho khách hàng một cách thường xuyên, bao gồm số liệu về các lỗ hổng được phát hiện và cách khắc phục, tình hình tuân thủ các yêu cầu bảo mật và tình trạng bảo mật tổng thể.

Quy trình làm việc với khách hàng

Về CyStack

CyStack là một công ty đổi mới sáng tạo trong lĩnh vực an ninh mạng tại Việt Nam, chúng tôi tiên phong xây dựng các sản phẩm bảo mật thế hệ mới cho cả doanh nghiệp và cá nhân. Các giải pháp của CyStack tập trung vào bảo vệ dữ liệu, phòng chống tấn công mạng và quản lý lỗ hổng bảo mật.

Để biết thêm chi tiết, liên lạc tới hotline **(+84) 247 109 9656** hoặc gửi mail tới **contact@cystack.net** để trao đổi cùng các chuyên gia bảo mật tại CyStack.
cystack.net