

## Sự cần thiết của dịch vụ bảo mật ứng dụng toàn diện

Với tốc độ thay đổi chóng mặt đến từ thị trường và yêu cầu từ khách hàng, quy trình về quản lý cơ sở hạ tầng và phát triển phần mềm thường xuyên phải đổi mới để đáp ứng được nhu cầu thực tế. Việc tối đa hóa chuyển giao các tác vụ tự động để tiết kiệm thời gian phát triển và phát hành sản phẩm được ưu tiên hàng đầu.

Các xu thế và mô hình mới dần được áp dụng rộng rãi, đi theo đó là rủi ro về việc gia tăng các nguy cơ về an toàn bảo mật nếu các bước trong quá trình không được áp dụng đúng cách và không được kiểm duyệt bởi đội ngũ chuyên gia ATTT.

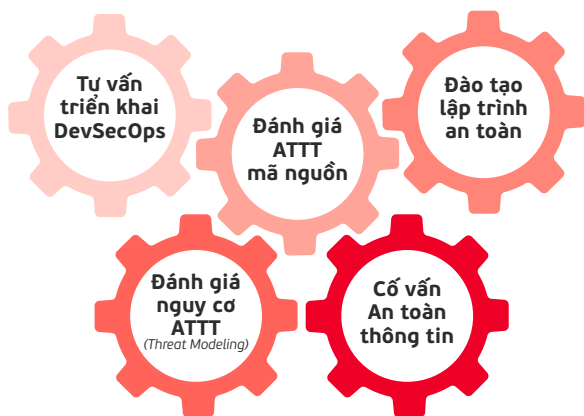
Việc tăng tốc độ phát hành các phiên bản mới của sản phẩm khiến chất lượng kiểm duyệt ATTT trở nên khó kiểm soát hơn rất nhiều, bài toán về việc cân đối giữa nhu cầu thương mại và đảm bảo ATTT trở nên khó giải quyết, và các biện pháp đánh giá ATTT ứng dụng truyền thống dần không theo kịp tốc độ phát hành sản phẩm.

Tuy nhiên thực tế đã cho thấy, hậu quả của việc các sản phẩm công nghệ thông tin khi gặp các sự cố về ATTT là rất lớn. Nó không chỉ tác động trực tiếp tới công ty cung cấp phần mềm mà còn gây ảnh hưởng nghiêm trọng tới khách hàng. Vì vậy việc đảm bảo ATTT cho sản phẩm công nghệ thông tin cần phải luôn được chú trọng.

## Dịch vụ bảo mật ứng dụng toàn diện

Dịch vụ Application Security do Viettel Security cung cấp hướng tới mục tiêu hoàn thiện chu trình phát triển phần mềm của một tổ chức về mặt mô hình, công cụ, phương thức thực hiện và nhận thức về ATTT của đội ngũ lập trình viên.

**Để đạt được mục tiêu này, các dịch vụ cung cấp bao gồm:**



## Những điểm chính của dịch vụ



### TỰ VẤN TRIỂN KHAI DEVSECOPS

Nếu hiểu khái niệm DevOps là sự kết hợp giữa nhiều triết lý văn hóa, biện pháp thực hành và công cụ giúp tăng khả năng phân phối ứng dụng và dịch vụ của một tổ chức ở tốc độ cao, phát triển và cải tiến sản phẩm ở nhịp độ nhanh hơn các tổ chức sử dụng quy trình quản lý cơ sở hạ tầng và phát triển phần mềm truyền thống, thì khái niệm DevSecOps cũng tương tự. DevSecOps giúp việc kiểm định ATTT bắt kịp với tốc độ phát hành phần mềm bằng cách tối đa hóa việc tích hợp công cụ tự động vào vòng đời phát triển phần mềm, tối ưu công cụ và quy trình, đồng thời đào tạo nhận thức nhằm thay đổi về văn hóa và tư duy cho đội ngũ phát triển về mặt ATTT.



### ĐÁNH GIÁ AN TOÀN THÔNG TIN MÃ NGUỒN

Thay đổi lớn nhất về mặt đánh giá ATTT mã nguồn so với phương pháp truyền thống là việc tích hợp thêm công cụ rà quét mã nguồn tự động vào vòng đời phát triển phần mềm. Điểm mạnh của việc sử dụng công cụ so với việc thực hiện thủ công chính là tính linh hoạt và tối ưu về mặt thời gian. Thay vì phải có nguồn lực về con người thì một công cụ có thể hoạt động 24/7 và đưa ra kết quả rà quét bất cứ khi nào một bản cập nhật mới được phát hành. Điều này giúp giảm thiểu rủi ro đáng kể về mặt ATTT cho sản phẩm mỗi khi phát hành bản cập nhật mới.



### ĐÀO TẠO LẬP TRÌNH AN TOÀN

Nhân tố con người luôn đóng vai trò quyết định trong quá trình phát triển phần mềm. Nhận thức về ATTT của đội ngũ phát triển trực tiếp phản ánh tình trạng ATTT của sản phẩm. Bên cạnh đó, thực trạng về việc liên tục thay đổi nhân sự của đội ngũ lập trình viên trong các tổ chức cũng là một yếu tố gây tác động lớn tới tình trạng ATTT của sản phẩm đó. Bài toán đặt ra là cần có một chương trình đào tạo linh hoạt, tối ưu về mặt thời gian nhưng vẫn đảm bảo cung cấp đủ nhận thức về các lỗ hổng có thể mắc phải khi lập trình. Dịch vụ Đào tạo lập trình an toàn do Viettel Security cung cấp chính là giải pháp để giải quyết vấn đề này.

## Những điểm chính của dịch vụ



### THREAT MODELING

Nếu như mục đích của việc đánh giá ATTT mã nguồn là việc chỉ ra danh sách lỗ hổng của một ứng dụng thì mục đích của việc đánh giá nguy cơ ATTT (Threat Modeling) là chỉ ra danh sách các nguy cơ về ATTT của cả một hệ thống. Điểm mạnh của phương pháp này là có thể thực hiện ngay tại bước đầu tiên trong vòng đời phát triển phần mềm – bước thiết kế. Việc sớm nhìn nhận được các nguy cơ và đưa ra phương án khắc phục ngay tại bước chưa bắt đầu bất kỳ dòng code nào giúp cho nỗ lực thay đổi hay cập nhật tại các bước sau được giảm đi đáng kể, giúp tiết kiệm cả về thời gian, nhân lực và chi phí. Ngay cả trong trường hợp hệ thống đã được xây dựng thì việc thực hiện Threat Modeling cũng giúp liệt kê sớm các nguy cơ về ATTT mà hệ thống có thể gặp phải, giúp áp dụng sớm các biện pháp ngăn chặn các cuộc tấn công có thể xảy ra trong tương lai.



### CỐ VẤN AN TOÀN THÔNG TIN

Đội ngũ cố vấn ATTT do Viettel Security đảm nhiệm đóng vai trò:

- Hỗ trợ đội ngũ phát triển trong quá trình xây dựng sản phẩm về mặt ATTT
- Hỗ trợ khắc phục lỗi ATTT được chỉ ra tại dịch vụ Đánh giá ATTT mã nguồn và Threat Modeling
- Tối ưu công cụ SAST theo nhu cầu thực tế của từng sản phẩm
- Định nghĩa các tiêu chuẩn ATTT cần áp dụng cho ứng dụng, hệ thống