ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

Giai đoạn 1: Thiết kế & Lập kế hoạch

- [ ] **Hoàn tất mô hình hóa mối đe dọa cho tính năng/sản phẩm mới**

  Xác định phương thức tấn công tiềm ẩn, ranh giới tin cậy, luồng dữ liệu nhạy cảm và tình huống lạm dụng trước khi bắt đầu quá trình phát triển.

- [ ] **Ghi lại phương thức tấn công**

  Ghi lại cách kẻ tấn công có thể lạm dụng API, giao diện người dùng, tích hợp từ bên thứ ba hoặc điểm truy cập đặc quyền.

- [ ] **Xác định ranh giới tin cậy**

  Định rõ nơi dữ liệu di chuyển giữa các hệ thống, dịch vụ, người dùng và các bên bên ngoài để hiểu rõ nguy cơ bảo mật.

- [ ] **Ưu tiên và gán người sở hữu cho rủi ro bảo mật**

  Phân loại rủi ro theo mức độ nghiêm trọng và bảo đảm mỗi rủi ro đều có người sở hữu chịu trách nhiệm giảm thiểu.

- [ ] **Định rõ công cụ phát triển được phê duyệt**

  Duy trì danh sách các công cụ phát triển, CI/CD, AI và cộng tác được phê duyệt, đáp ứng yêu cầu bảo mật của công ty.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

- [ ] **Đánh giá và phê duyệt trợ lý lập trình AI**

  Đánh giá quyền riêng tư dữ liệu, quyền sở hữu code, sự tuân thủ và rủi ro bảo mật của các công cụ AI trước khi triển khai ứng dụng.

- [ ] **Sao lưu bằng tài liệu các yêu cầu về quyền riêng tư dữ liệu**

  Xác định cách thức thu thập, lưu trữ, xử lý và giữ lại dữ liệu nhạy cảm, dữ liệu khách hàng và dữ liệu được quản lý theo quy định.

- [ ] **Xác định yêu cầu xác thực**

  Định rõ cơ chế xác thực như SSO, MFA và OAuth hoặc các tiêu chuẩn về mật khẩu.

- [ ] **Ghi lại yêu cầu ủy quyền**

  Xác định rõ ràng vai trò người dùng, quyền truy cập và ranh giới đặc quyền.

- [ ] **Định rõ tiêu chuẩn mã hóa**

  Thiết lập các phương thức mã hóa được phê duyệt cho dữ liệu đang truyền cũng như dữ liệu tĩnh.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

Giai đoạn 2: Phát triển

- [ ] **Đào tạo về tiêu chuẩn lập trình an toàn cho lập trình viên**

  Đảm bảo nhóm kỹ thuật hiểu rõ quy tắc lập trình an toàn cùng với các dạng lỗ hổng bảo mật phổ biến.

- [ ] **Đánh giá top 10 rủi ro theo chuẩn OWASP**

  Xác nhận nhóm hiểu rõ các rủi ro bảo mật ứng dụng web phổ biến nhất và chiến lược giảm thiểu rủi ro.

- [ ] **Thực thi peer code review (đánh giá mã ngang hàng) bắt buộc**

  Bắt buộc đánh giá độc lập trước khi bất kỳ code nào được hợp nhất vào các nhánh production.

- [ ] **Đánh giá code tạo bởi AI bằng người thật**

  Đảm bảo kỹ sư rà soát code được AI hỗ trợ viết để phát hiện vấn đề bảo mật, lỗi logic và rủi ro tuân thủ.

- [ ] **Tích hợp công cụ SCA vào pipeline CI**

  Tự động quét các phụ thuộc từ bên thứ ba để tìm kiếm lỗ hổng đã biết.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

- [ ] **Giám sát thư viện (depedencies) của bên thứ 3**

  Liên tục theo dõi cập nhật bảo mật và thông tin công bố lỗ hổng gây ảnh hưởng đến phụ thuộc của phần mềm.

- [ ] **Ưu tiên cập nhật phụ thuộc quan trọng**

  Xác định thỏa thuận mức độ dịch vụ (Service Level Agreement) cho việc cập nhật thư viện và framework rủi ro cao.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

Giai đoạn 3: Thử nghiệm & Xác minh

- [ ] **Tích hợp SAST vào luồng CI**

  Tự động phân tích mã nguồn và phát hiện lỗ hổng trước khi triển khai.

- [ ] **Tích hợp DAST vào môi trường thử nghiệm**

  Liên tục thử nghiệm ứng dụng đang chạy để tìm kiếm lỗ hổng có thể bị lạm dụng.

- [ ] **Đưa quét bảo mật vào quy trình phát hành**

  Đưa xác thực bảo mật trở thành yêu cầu phát hành bắt buộc.

- [ ] **Chặn triển khai khi có phát hiện rủi ro cao**

  Chặn triển khai production khi các lỗ hổng nghiêm trọng chưa được giải quyết.

- [ ] **Hoàn tất pentest (kiểm tra xâm nhập) cho hệ thống quan trọng**

  Mô phỏng các cuộc tấn công thực tế nhắm vào ứng dụng và dịch vụ rủi ro cao.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

- [ ] **Thử nghiệm cơ chế xác thực**

  Xác nhận luồng đăng nhập, điều khiển MFA, quản lý phiên làm việc (session) và chính sách mật khẩu.

- [ ] **Phê duyệt logic ủy quyền**

  Đảm bảo người dùng không thể truy cập tài nguyên hoặc hành động vượt quá quyền được cấp.

- [ ] **Nhận phê chuẩn bảo mật**

  Yêu cầu phải nhận sự phê duyệt chính thức từ các bên bảo mật liên quan trước khi phát hành.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

Giai đoạn 4: Triển khai & Vận hành

- [ ] **Giới hạn truy cập vào quy trình**

  Chỉ cho phép người được ủy quyền truy cập quy trình CI/CD thông qua nguyên tắc đặc quyền tối thiểu (Least Privilege Principle)

- [ ] **Quản lý chắc chắn thông tin mật**

  Lưu trữ thông tin xác thực, khóa (key) và token trên các nền tảng quản lý bí mật được phê duyệt.

- [ ] **Xác nhận Sản phẩm đầu ra (build artifact)**

  Xác minh tính toàn vẹn, xác thực và khả năng truy xuất nguồn gốc của các gói triển khai (deployment package).

- [ ] **Bắt buộc xác thực đa yếu tố cho truy cập production**

  Yêu cầu xác thực đa yếu tố cho mọi truy cập đặc quyền vào hệ thống production.

- [ ] **Áp dụng mô hình đặc quyền tối thiểu**

  Chỉ cấp quyền tối thiểu cần thiết để thực hiện chức năng kinh doanh.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

- [ ] **Hoàn tất gia cố hạ tầng**

  Vô hiệu hóa dịch vụ không cần thiết, đóng các cổng không được dùng và áp dụng cấu hình bảo mật.

- [ ] **Kích hoạt ghi nhật ký bảo mật**

  Ghi lại các sự kiện liên quan đến bảo mật khắp mọi ứng dụng, hạ tầng và hệ thống quản lý danh tính.

- [ ] **Giám sát sự kiện quan trọng**

  Thiết lập giám sát và cảnh báo đối với hành động khả nghi và sự cố bảo mật.

- [ ] **Ghi thành tài liệu quy trình liên lạc ứng phó sự cố**

  Duy trì lộ trình nâng cao vấn đề hiện đại cùng với mô hình sở hữu ứng phó sự cố.

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

Kiểm tra lần cuối trước khi phát hành (release)

- [ ] **Không còn lỗ hổng quan trọng**

  Xác minh mọi phát hiện nghiêm trọng đã được khắc phục hoặc chính thức chấp nhận thông qua quản trị rủi ro.

- [ ] **Hoàn tất kiểm tra bảo mật**

  Thực hiện đánh giá bảo mật lần cuối đối với kiến trúc, code, hạ tầng và cấu hình.

- [ ] **Phê duyệt kiểm tra xâm nhập (pentest)**

  Xác nhận rằng kết quả đã được xem xét và hoạt động khắc phục đã hoàn tất.

- [ ] **Giám sát vận hành**

  Đảm bảo nhật ký, cảnh báo, bảng điều khiển và quy trình phản hồi đang hoạt động đúng.

- [ ] **Ghi thành tài liệu kế hoạch khôi phục**

  Xác định quy trình hoàn tác các bản phát hành một cách an toàn nếu xảy ra sự cố vận hành hoặc bảo mật.

- [ ] **Nhận phê chuẩn từ cấp cao nhất**

  Xác minh các bên liên quan trong công ty chấp nhận rủi ro an ninh vận hành cũng như còn lại.

- [ ] **Nhận phê chuẩn từ chủ sở hữu bảo mật**

ekino.

Checklist quy trình phát triển phần mềm an toàn

Khuôn khổ đánh giá bảo mật từ thiết kế đến triển khai

Đối tượng: CTO, Quản lý kỹ thuật, Trưởng nhóm bảo mật

Mục tiêu: Thẩm định rằng biện pháp kiểm soát an ninh được áp dụng xuyên suốt quy trình

Đánh giá nhanh

Điểm số

Trạng thái	Điểm
Hoàn thành	1
Chưa hoàn thành	0

Tổng điểm: ___ / 48

Kết quả	Mức độ sẵn sàng bảo mật
0 - 24	Rủi ro cao
25 - 36	Cơ bản
37 - 44	Được quản lý
45 - 48	Bảo mật cao