CyStack

DATA SHEET

Kiểm thử bảo mật đám mây

Đánh giá và củng cố bảo mật cho cơ sở hạ tầng đám mây chuyên nghiệp

Tổng quan

Kiểm thử bảo mật đám mây là thực hiện kiểm tra toàn diện các hệ thống và cơ sở hạ tầng đám mây của một doanh nghiệp để xác định các lỗ hổng tiềm ẩn và các vấn đề tuân thủ bảo mật. Quá trình kiểm thử bảo mật đám mây thường bao gồm cả kiểm thử tự động và thủ công, cũng như đánh giá các chính sách và quy trình tuân thủ của doanh nghiệp. Mục tiêu của kiểm thử bảo mật đám mây là đảm bảo các hệ thống đám mây của doanh nghiệp được bảo mật và tuân thủ các tiêu chuẩn và quy định của ngành.

Giải pháp của CyStack

Đội ngũ kiểm thử bảo mật của CyStack bao gồm những chuyên gia tài năng giàu kinh nghiệm, thành thạo các phương pháp kiểm thử bám sát mục tiêu và tối ưu nhất. Họ là những chuyên gia có nền tảng vững chắc về phát triển phần mềm và nghiên cứu an ninh mạng, giúp đội ngũ CyStack đánh giá toàn diện nhất các rủi ro bảo mật trong sản phẩm số của doanh nghiệp. Các chuyên gia tại CyStack cũng thường xuyên tham gia các hội nghị an ninh mạng lớn trên thế giới với vai trò diễn giả hàng năm, đồng thời họ là những chuyên gia săn lỗi phần mềm với nhiều thành tích phát hiện ra các lỗ hổng bảo mật nghiêm trọng trong sản phẩm của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Sea Group, Alibaba, etc.

Các chuyên gia tại CyStack có thể thực hiện đánh giá cơ sở hạ tầng đám mây của doanh nghiệp, bao gồm máy chủ, mạng và kho lưu trữ, cũng như kiến trúc của hệ thống và cách cấu hình để xác định bất kỳ lỗ hổng hoặc cấu hình sai nào có thể bị tin tặc khai thác. Đội ngũ CyStack cũng sẽ đánh giá các cài đặt và cấu hình bảo mật của các ứng dụng và hệ thống đám mây của doanh nghiệp để đảm bảo chúng được thiết đặt đúng, bao gồm kiểm tra cơ chế mã hóa, kiểm soát truy cập và bảo mật mạng.

Lợi ích của khách hàng

- Tăng cường bảo mật cho các hệ thống và cơ sở hạ tầng đám mây
- Đảm bảo tuân thủ các tiêu chuẩn và quy định của ngành
- Hiểu và quản lý rủi ro bảo mật hiệu quả hơn
- Xây dựng mô hình quản trị tốt hơn và đưa ra chiến thuật quản lý rủi ro mạnh mẽ hơn
- Có chứng thực của bên thứ ba độc lập về tình trạng bảo mật hệ thống và hạ tầng đám mây

Phương pháp luận

Kiểm thử bảo mật đám mây tiêu biểu bao gồm:

- **Đánh giá kiến trúc và cơ sở hạ tầng đám mây**: Đội ngũ chuyên gia của CyStack sẽ xem xét cơ sở hạ tầng đám mây của doanh nghiệp bao gồm máy chủ, mạng và kho lưu trữ, cũng như kiến trúc của hệ thống và cách chúng được thiết lập.
- **Đánh giá cấu hình bảo mật**: CyStack xem xét các cài đặt và cấu hình bảo mật của các ứng dụng và hệ thống đám mây của doanh nghiệp, tìm kiếm bất kỳ cấu hình sai hoặc lỗ hổng nào có thể bị khai thác. Việc này bao gồm kiểm tra cơ chế mã hóa, kiểm soát truy cập và bảo mật mạng.
- **Đánh giá chính sách và quy trình**: CyStack xem xét các chính sách và quy trình của doanh nghiệp liên quan đến bảo mật đám mây, bao gồm kế hoạch ứng phó sự cố, kế hoạch khắc phục sau sự cố và kiểm soát truy cập, ngoài ra, xác định bất kỳ lỗ hổng hoặc sự không nhất quán nào trong các chính sách và thủ tục và đưa ra các khuyến nghị để cải thiện.
- **Đánh giá tuân thủ**: CyStack kiểm tra cơ sở hạ tầng và hệ thống đám mây của doanh nghiệp đảm bảo tuân thủ các tiêu chuẩn và quy định của ngành như ISO27001, HIPAA, PCI-DSS và SOC 2.
- **Kiểm thử bảo mật**: CyStack thực hiện kiểm thử bảo mật để mô phỏng các kịch bản tấn công trong thực tế và xác định các lỗ hổng cho phép kẻ tấn công có quyền truy cập trái phép vào dữ liệu hay hệ thống đám mây của doanh nghiệp.
- **Hướng dẫn khắc phục**: Khi các lỗ hổng và vấn đề tuân thủ đã được xác định, CyStack cung cấp hướng dẫn chi tiết và đề xuất khắc phục, bao gồm các khuyến nghị bảo mật cập nhất để bảo mật hệ thống và cơ sở hạ tầng đám mây.
- **Báo cáo**: CyStack cung cấp báo cáo chi tiết về các phát hiện, bao gồm bản tóm tắt các lỗ hổng và vấn đề tuân thủ đã xác định, cùng với các đề xuất khắc phục.

Tính năng chính

- Đảm bảo hạ tầng đám mây an toàn
- Đánh giá toàn diện hạ tầng đám mây về các cấu hình, kiến trúc, chính sách và quy trình
- Quản lý, theo dõi, đánh giá mức độ ưu tiên và khắc phục những phát hiện trong nền tảng quản lý lỗ hổng của CyStack
- Nhận các khuyến nghị phù hợp để tăng cường bảo mật hệ thống
- Giảm thiểu các rủi ro và nâng cao hiệu quả vận hành

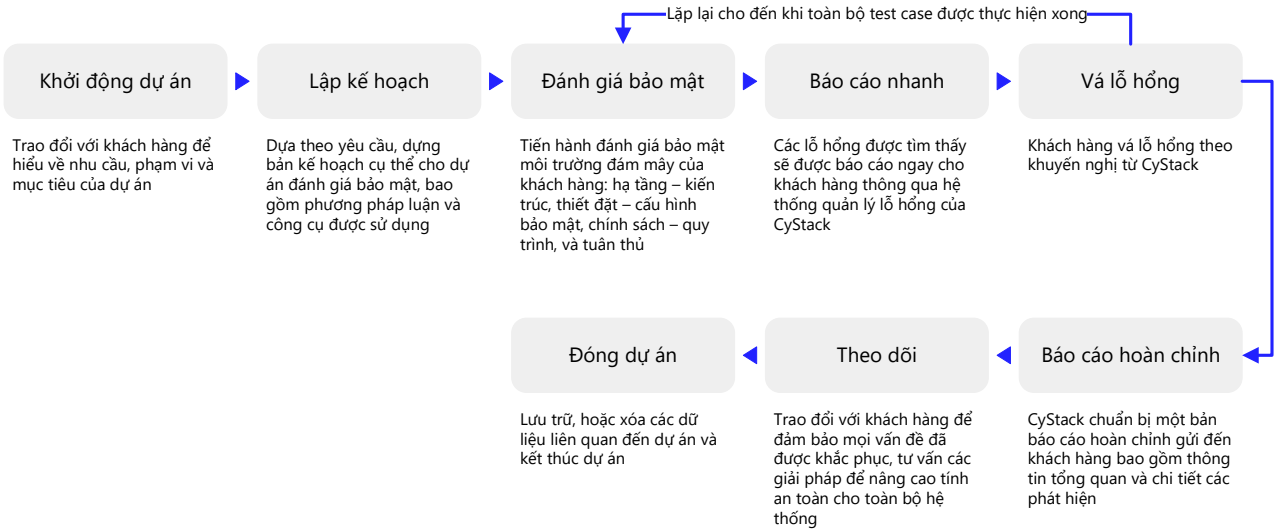
Các tiêu chuẩn

Các hướng dẫn và tiêu chuẩn quốc tế mà CyStack sử dụng làm khuôn khổ để tiến hành kiểm thử bảo mật đám mây:

- **ISO/IEC 27001:2013**: Tiêu chuẩn quốc tế này cung cấp khuôn khổ cho hệ thống quản lý an ninh thông tin (ISMS), bao gồm các hướng dẫn về quản lý rủi ro, quản lý sự cố và quản lý tính liên tục của doanh nghiệp, có thể áp dụng cho các hệ thống và cơ sở hạ tầng đám mây.
- **SOC 2**: Tiêu chuẩn này do Viện Kế toán Công chứng Hoa Kỳ (AICPA) phát triển và dành cho các tổ chức dịch vụ như nhà cung cấp dịch vụ đám mây. SOC 2 tập trung vào các hoạt động kiểm soát của các nhà cung cấp dịch vụ liên quan đến bảo mật, tính khả dụng, tính toàn vẹn của quá trình xử lý, tính bảo mật và quyền riêng tư.
- **PCI DSS**: Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) là một bộ tiêu chuẩn bảo mật được tạo để bảo vệ dữ liệu của chủ thẻ thanh toán, được áp dụng cho bất kỳ tổ chức nào lưu trữ, xử lý hoặc truyền dữ liệu về chủ thẻ. Cần đảm bảo cơ sở hạ tầng đám mây được sử dụng để lưu trữ, xử lý hoặc truyền dữ liệu chủ thẻ tuân thủ PCI.
- **NIST SP 800-53**: Ấn phẩm đặc biệt 800-53 (SP 800-53) của Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ (NIST) cung cấp các hướng dẫn về bảo mật hệ thống thông tin liên bang, bao gồm các họ kiểm soát như đánh giá và ủy quyền bảo mật, quản lý bảo mật và ứng phó sự cố. Tiêu chuẩn này có thể được áp dụng cho các hệ thống và cơ sở hạ tầng đám mây, cũng như các hệ thống tại chỗ.
- **CSA CCM**: Ma trận kiểm soát đám mây (CCM) là một khung chuẩn do Liên minh an ninh điện toán đám mây (CSA) phát triển nhằm cung cấp các hướng dẫn về bảo mật đám mây, bao gồm các lĩnh vực kiểm soát như quản trị an ninh, quản lý rủi ro và quản lý sự cố.
- **HIPAA**: Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA) là luật yêu cầu các tổ chức bảo vệ quyền riêng tư và bảo mật thông tin sức khỏe cá nhân của người dùng. Vì vậy, bất kỳ tổ chức nào lưu trữ, xử lý hoặc truyền tải thông tin sức khỏe được bảo vệ (PHI) đều phải tuân thủ HIPAA.

CyStack cũng đối chiếu các nguyên tắc bảo mật từ các nhà cung cấp đám mây lớn như AWS, GCP và Azure cũng như từ Cloud Security Alliance trong quá trình kiểm thử bảo mật đám mây.

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