CyStack

DATA SHEET

Managed Security Service

Đối tác bảo mật tin cậy cho doanh nghiệp

Thách thức bảo mật

Trong thời đại kỹ thuật số hiện nay, các doanh nghiệp phải đối mặt với ngày càng nhiều các rủi ro an ninh mạng, khiến việc bảo vệ hạ tầng mạng và dữ liệu trở nên vô cùng khó khăn. Những thách thức bảo mật thường bao gồm:

- **Thiếu hụt chuyên gia an ninh mạng**: Khi nhu cầu về chuyên môn bảo mật liên tục tăng, nhiều doanh nghiệp gặp khó khăn trong việc tìm kiếm và giữ chân các chuyên gia an ninh mạng có năng lực để đáp ứng các nhu cầu bảo mật của doanh nghiệp.
- **Bắt kịp các mối đe dọa mới nhất**: Các mối đe dọa an toàn thông tin mới liên tục xuất hiện, gây khó khăn cho các doanh nghiệp để bắt kịp xu hướng tấn công mới nhất cũng như các phương pháp tốt nhất để ngăn ngừa và phòng chống các cuộc tấn công.
- **Quản lý nhiều giải pháp bảo mật**: Doanh nghiệp thường phải quản lý nhiều giải pháp bảo mật như tường lửa, hệ thống phát hiện xâm nhập, phần mềm diệt virus, có thể khiến doanh nghiệp mất rất nhiều thời gian và gặp nhiều khó khăn.
- **Tuân thủ các quy định của ngành**: Nhiều lĩnh vực có các quy định và tiêu chuẩn cụ thể mà doanh nghiệp phải đáp ứng như HIPAA hoặc PCI DSS. Việc tuân thủ các quy định và tiêu chuẩn này là một thách thức với các doanh nghiệp, thậm chí các doanh nghiệp có nguy cơ chịu phạt khi không đáp ứng các yêu cầu tuân thủ.
- **Ngân sách hạn chế**: Các doanh nghiệp vừa và nhỏ thường có ngân sách hạn chế, gây khó khăn cho việc đầu tư vào các giải pháp bảo mật và nhân sự cần thiết.

Các dịch vụ quản lý bảo mật có thể giúp doanh nghiệp vượt qua những thách thức nói trên. Bằng cách giao phó nhiệm vụ đảm bảo an toàn thông tin cho nhà cung cấp dịch vụ bảo mật (MSSP), doanh nghiệp được tiếp cận một nhóm chuyên gia luôn theo sát và cập nhật liên tục các mối đe dọa mới nhất, cũng như các phương pháp phòng chống lỗ hổng bảo mật tốt nhất. MSSP cũng giúp doanh nghiệp quản lý cùng lúc nhiều giải pháp bảo mật, đảm bảo tuân thủ các tiêu chuẩn và quy định của ngành, đồng thời cung cấp báo cáo thường xuyên, định kỳ về tình trạng bảo mật của khách hàng. Ngoài ra, MSSP có hỗ trợ đào tạo cho nhân viên của doanh nghiệp về cách nhận biết và ứng phó với các mối đe dọa. Hơn nữa, khi giao nhiệm vụ bảo mật cho MSSP, các doanh nghiệp có thể tiết kiệm tài nguyên và giảm nguy cơ xảy ra các sự cố bảo mật tốn kém.

Lợi ích của khách hàng

- Cải thiện tình hình bảo mật tổng thể bằng cách sử dụng đánh giá toàn diện và liên tục về các rủi ro, lỗ hổng bảo mật và biện pháp kiểm soát
- Giảm chi phí liên quan đến an ninh bằng cách loại bỏ nhu cầu thuê và duy trì đội an ninh nội bộ
- Đơn giản hóa các hoạt động bảo mật, ứng phó hiệu quả hơn với các mối đe dọa và sự cố bảo mật tiềm ẩn
- Tiếp cận với nhóm chuyên gia bảo mật có kiến thức và chuyên môn cao để giữ an toàn cho hệ thống
- Yên tâm khi biết rằng bảo mật của hệ thống được các chuyên gia bảo mật giàu kinh nghiệm và năng lực

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 và được ghi danh trên Hall of Fame của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Sea Group, Alibaba, v.v.

Là đơn vị cung cấp dịch vụ bảo mật hàng đầu tại Việt Nam, CyStack giúp doanh nghiệp bảo vệ mạng và dữ liệu bằng cách cung cấp hàng loạt dịch vụ được thiết kế đặc biệt để giảm thiểu rủi ro an toàn thông tin. Các giải pháp của CyStack tập trung vào kiểm tra bảo mật, củng cố, giám sát, đào tạo và ứng phó với các mối đe dọa. Mục tiêu của CyStack là giúp các doanh nghiệp đảm bảo an ninh cho toàn bộ hệ thống của họ, trong khi họ chỉ cần tập trung vào phát triển sản phẩm và hoạt động kinh doanh của mình.

Tính năng chính

- Quản lý lỗ hổng bảo mật
- Dịch vụ siết chặt bảo mật
- Giám sát bảo mật
- Đào tạo bảo mật
- Ứng cứu sự cố
- Nền tảng bảo mật tích hợp

Phương pháp luận

CyStack, với tư cách là Nhà cung cấp dịch vụ bảo mật (MSSP), đưa ra đa dạng các dịch vụ có thể tùy chỉnh để đáp ứng nhu cầu cụ thể của từng khách hàng. Khách hàng được linh hoạt lựa chọn các dịch vụ phù hợp nhất với nhu cầu và ngân sách của doanh nghiệp, là sự kết hợp bất kỳ của các dịch vụ sau:

Dịch vụ	Giải pháp chính
Quản lý lỗ hổng bảo mật	Đánh giá lỗ hổng bảo mật + Kiểm thử xâm nhập + Quản lý chương trình săn lỗi nhận thưởng
Dịch vụ siết chặt bảo mật	Đánh giá cấu hình + Kiểm soát truy cập + Cập nhật phần mềm
Giám sát bảo mật	Nhật ký sự kiện + Phát hiện mối đe dọa + Phát hiện bất thường
Quản lý chương trình săn lỗi nhận thưởng	Nền tảng săn lỗi nhận thưởng WhiteHub

Quản lý lỗ hổng bảo mật

Quản lý lỗ hổng bảo mật là quá trình xác định, sắp xếp mức độ ưu tiên và xử lý các lỗ hổng bảo mật trong các hệ thống và hạ tầng mạng của khách hàng. Mục tiêu của quản lý lỗ hổng là giảm thiểu rủi ro do vi phạm bảo mật bằng cách chủ động phát hiện và xử lý các điểm yếu tiềm tàng trước khi kẻ tấn công tiến hành khai thác. Quản lý lỗ hổng bảo mật hiệu quả giúp các tổ chức ngăn ngừa các vụ vi phạm bảo mật và bảo vệ thông tin nhạy cảm, cũng như hệ thống và hạ tầng của họ. Đây là quy trình quan trọng trong một chiến lược bảo mật tổng thể và cần được thực hiện thường xuyên để ngăn ngừa các mối nguy tiềm tàng mới.

Các dịch vụ nằm trong giải pháp Quản lý lỗ hổng bảo mật của CyStack bao gồm:

- **Đánh giá lỗ hổng bảo mật**: Để đơn giản hóa và tự động thực hiện Đánh giá lỗ hổng bảo mật, CyStack phát triển CyStack Web Security (CWS), là công cụ rà quét và giám sát lỗ hổng cho các ứng dụng web. CWS giúp các tổ chức rà quét các tên miền phụ và địa chỉ IP trong mạng nội bộ, cũng như phát hiện các lỗ hổng bằng kỹ thuật fuzzing và cơ sở dữ liệu về lỗ hổng bảo mật riêng của CyStack. Với CWS, các lỗ hổng bảo mật mới được giám sát liên tục và cảnh bảo tự động ngay khi phát hiện. CWS cũng cung cấp một nền tảng để quản lý, theo dõi, sắp xếp mức độ ưu tiên và đề xuất cách xử lý cho các phát hiện. Hơn nữa, các tổ chức có thể tích hợp CWS với các công cụ CI/CD và các công cụ quản lý hiệu suất khác. Tham khảo thông tin chi tiết tại đây.

- **Kiểm thử xâm nhập**: Kiểm thử xâm nhập là sự mô phỏng lại cuộc tấn công an ninh mạng vào một hệ thống, mạng lưới máy tính hoặc ứng dụng web để phát hiện các lỗ hổng bảo mật có thể bị khai thác. Kiểm thử xâm nhập được thực hiện bởi các chuyên gia bảo mật, sử dụng đa dạng các loại công cụ và kỹ thuật để đánh giá tính bảo mật của môi trường mục tiêu, từ đó, tìm ra những điểm yếu có thể bị tấn công. Tham khảo thông tin chi tiết tại đây.
- **Quản lý chương trình săn lỗi nhận thưởng**: Chương trình săn lỗi nhận thưởng là một hình thức bảo mật cộng đồng nhằm trao thưởng cho các cá nhân hoặc đội nhóm, hay còn gọi là hacker mũ trắng, có phát hiện và gửi báo cáo về các lỗ hổng bảo mật trong một phần mềm hoặc hệ thống của doanh nghiệp. Các doanh nghiệp đưa ra các mức thưởng, có thể bằng tiền, quà lưu niệm hoặc các hình thức ghi danh, tạo động lực cho các hacker mũ trắng tìm kiếm và báo lại những lỗ hổng bảo mật đã tìm được. CyStack cung cấp cho các tổ chức WhiteHub, là nền tảng bảo mật cộng đồng lớn nhất tại Việt Nam. Tham khảo thông tin chi tiết tại đây.

Dịch vụ siết chặt bảo mật

Dịch vụ siết chặt bảo mật là quá trình bảo mật hệ thống và mạng lưới doanh nghiệp bằng cách triển khai các biện pháp và điều chỉnh tối ưu nhất về bảo mật, nâng cao khả năng chống chịu trước các cuộc tấn công. Mục tiêu của việc siết chặt bảo mật là để cải thiện tình trạng bảo mật chung của một hệ thống hoặc mạng lưới, giảm thiểu rủi ro bị tấn công thực sự, và nâng cao tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin nhạy cảm và các tài nguyên. Siết chặt bảo mật là một quá trình yêu cầu sự đánh giá và điều chỉnh liên tục để ngăn ngừa các mối nguy mới không ngừng biến đổi.

Dịch vụ siết chặt bảo mật của CyStack bao gồm:

- **Đánh giá cấu hình**: Đánh giá các thiết đặt bảo mật và cấu hình của các hệ thống và ứng dụng trong tổ chức, phát hiện các cấu hình sai hoặc các lỗ hổng có thể khai thác.
- **Kiểm soát truy cập**: Đánh giá sự hiệu quả trong các quy trình kiểm soát truy cập của tổ chức như cơ chế xác thực và phân quyền, đồng thời phát hiện các điểm yếu tiềm tàng trong các quy trình kiểm soát truy cập..
- **Cập nhật phần mềm**: Cập nhật và cài đặt bản vá các phần mềm ứng dụng và phần mềm hệ thống để khắc phục các lỗi và lỗ hổng bảo mật.

CyStack tư vấn và đưa ra quyết định cùng với khách hàng cho các Dịch vụ siết chặt bảo mật được thiết kế riêng, dựa trên cấu trúc hạ tầng, công nghệ và những yêu cầu cụ thể khác. CyStack cũng có những dịch vụ khác liên quan đến Dịch vụ siết chặt bảo mật, bao gồm Kiểm thử mạng nội bộ, Kiểm thử bảo mật đám mây và DevSecOps.

Giám sát bảo mật

Giám sát bảo mật là quá trình liên tục giám sát các mạng lưới và hệ thống để phát hiện những bất thường, mối đe dọa và sự cố bảo mật tiềm ẩn. Mục tiêu hàng đầu của giám sát bảo mật là phát hiện và xử lý sự cố bảo mật kịp thời trước khi chúng gây hại nghiêm trọng, nhằm hạn chế thấp nhất các tác động có thể và ngăn ngừa tối đa thiệt hại gây ra bởi một vụ vi phạm bảo mật. Giám sát bảo mật thường sử dụng các công nghệ bảo mật như tường lửa, hệ thống phát hiện và ngăn ngừa xâm nhập (IDS/IPS), hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) cùng phần mềm antivirus. Giải pháp này cũng cần có sự giám sát thủ công và phân tích trực tiếp từ các chuyên gia bảo mật.

Các dịch vụ Giám sát bảo mật của CyStack bao gồm:

- **Nhật ký sự kiện**: Ghi chép và lưu trữ thông tin chi tiết về các sự kiện xảy ra trên một hệ thống hoặc mạng lưới, nhằm giám sát và phân tích hoạt động liên quan đến tính bảo mật.
- **Phát hiện mối đe dọa**: Phát hiện và phân tích các mối đe dọa và các cuộc tấn công bảo mật vào các hệ thống và mạng lưới của một tổ chức bằng cách sử dụng các công cụ và kỹ thuật giám sát bảo mật, kết hợp việc phân tích thủ công bởi các chuyên gia bảo mật.
- **Phát hiện bất thường**: Phát hiện và cảnh báo các sai lệch so với hành vi thông thường và dự kiến trong một hệ thống và mạng lưới, bao gồm nhận diện các hoạt động đăng nhập bất thường, lưu lượng mạng trái dự kiến hoặc các dấu hiệu truy cập tài liệu bất thường.

Tham khảo thông tin chi tiết tại đây.

Quản lý chương trình săn lỗi nhận thưởng

Khi người dùng Internet ngày càng đòi hỏi sản phẩm công nghệ phải đáp ứng các tiêu chuẩn bảo mật, các doanh nghiệp vô tình vướng vào cuộc đua phát triển sản phẩm đủ nhanh và đủ tốt, mà cũng phải thật an toàn trong quá trình vận hành. Phần mềm cần liên tục cập nhật, kéo theo việc các lỗi bảo mật dễ dàng xảy ra hơn.

Giải pháp cho vấn đề này là các nhà phát triển phải phát hiện và khắc phục lỗ hổng trong các sản phẩm của họ nhanh hơn tin tặc. Áp dụng bảo mật cộng đồng chính là một phương pháp tiếp cận hiệu quả. Về cơ bản, đây là phiên bản mở rộng về mặt nhân sự so với phương pháp kiểm thử bảo mật truyền thống. Thay vì một nhóm chỉ gồm 2-5 kiểm thử viên, các công ty nay có một cộng đồng chuyên gia quy mô lên tới hàng nghìn người, hỗ trợ họ tìm kiếm và phát hiện các vấn đề bảo mật.

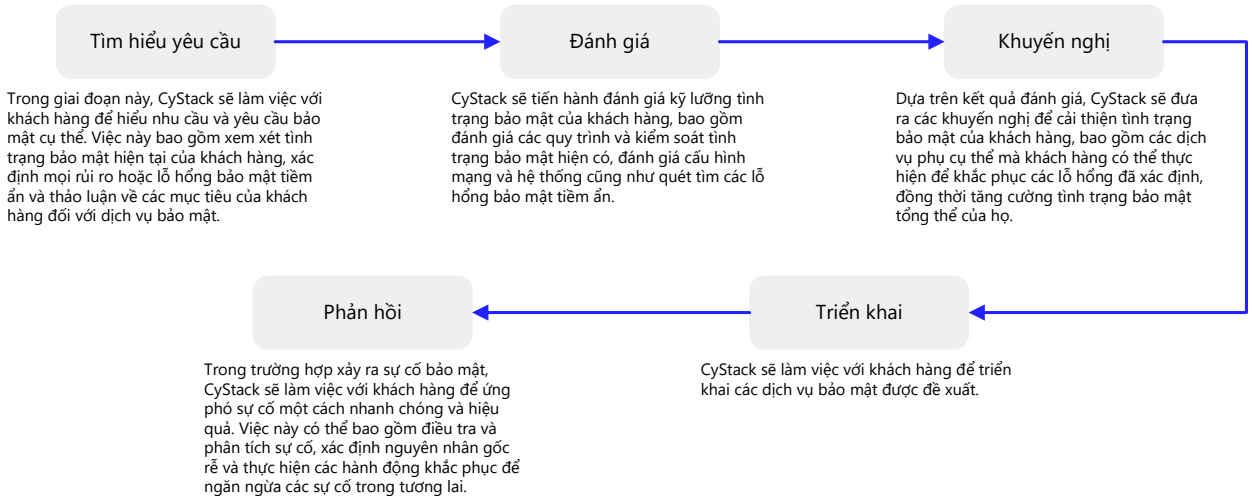
CyStack hỗ trợ các doanh nghiệp khởi chạy và quản lý các chương trình săn lỗi nhận thưởng trên WhiteHub, nền tảng bảo mật cộng đồng và lớn nhất Việt Nam, phát triển bởi chính CyStack.

Chương trình săn lỗi nhận thưởng nhằm xác định và xử lý các lỗ hổng bảo mật kịp thời và hiệu quả, đồng thời cung cấp một môi trường an toàn và bảo mật cho các hacker mũ trắng báo cáo về lỗ hổng bảo mật, giúp các tổ chức nâng cao tình trạng bảo mật cũng như giảm thiểu rủi ro của các cuộc tấn công mạng và lộ lọt dữ liệu.

Tham khảo thông tin chi tiết tại đây.

Quy trình làm việc với khách hàng

Quy trình làm việc với khách hàng trong dịch vụ bảo mật được quản lý thường bao gồm các bước sau:



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