CyStack

DATA SHEET

Quản lý chương trình săn lỗi nhận thưởng

Phát hiện lỗ hổng trước khi bị khai thác bởi kẻ tấn công

Bảo mật cộng đồng

Trong bối cảnh người dùng internet ngày càng áp đặt những tiêu chuẩn cao cho sản phẩm họ sử dụng, doanh nghiệp vô tình bị đẩy vào cuộc đua phát triển sản phẩm đủ nhanh, đủ tốt mà vẫn vận hành an toàn. Phần mềm được cập nhật càng thường xuyên thì càng có nhiều khả năng có lỗi bảo mật.

Giải pháp cho vấn đề này là các nhà phát triển phải nhanh hơn tin tặc trong việc tìm và sửa các lỗ hổng trong sản phẩm của họ. Một cách tiếp cận nâng cao ở đây là sử dụng bảo mật cộng đồng.

Về cơ bản, đây là phiên bản mở rộng của kiểm thử bảo mật truyền thống về mặt nhân lực. Thay vì làm việc với một nhóm gồm 2-5 chuyên gia kiểm thử bảo mật, giờ đây các công ty có một cộng đồng chuyên gia nghiên cứu bảo mật gồm hàng nghìn người sẽ giúp họ tìm ra các vấn đề bảo mật.

Một số ưu điểm của bảo mật cộng đồng so với các phương pháp bảo mật truyền thống:

- Phạm vi bao phủ rộng hơn: Bảo mật cộng đồng cho phép các doanh nghiệp tương tác với một số lượng lớn các chuyên gia bảo mật có kỹ năng và chuyên môn đa dạng, giúp xác định các lỗ hổng mà các nhóm bảo mật nội bộ có thể đã bỏ qua. Các phương pháp bảo mật truyền thống thường dựa vào một nhóm nhỏ hơn gồm các chuyên gia bảo mật nội bộ.
- Góc nhìn mới: Bảo mật cộng đồng mang đến một góc nhìn mới về các vấn đề bảo mật, vì các chuyên gia bảo mật từ bên ngoài tổ chức có thể xác định các lỗ hổng và vector tấn công mà các nhóm nội bộ đã bỏ qua.
- Phát hiện và phản hồi nhanh hơn: Bảo mật cộng đồng giúp doanh nghiệp nhanh chóng phát hiện và phản hồi các lỗ hổng bảo mật vì các chuyên gia bảo mật có thể xác định và báo cáo các lỗ hổng một cách kịp thời.
- Hiệu quả về chi phí: Bảo mật cộng đồng là giải pháp thay thế tiết kiệm chi phí cho các phương pháp bảo mật truyền thống, cho phép các doanh nghiệp tiếp cận với một nhóm lớn các chuyên gia bảo mật với chi phí chỉ bằng một phần nhỏ so với việc thuê một nhóm bảo mật toàn thời gian.
- Danh tiếng tích cực: Bằng cách khởi chạy một chương trình bảo mật cộng đồng, các doanh nghiệp thể hiện cam kết của mình đối với bảo mật, giúp xây dựng lòng tin và nâng cao danh tiếng của họ.

Trường hợp sử dụng

- Bảo mật ứng dụng web
- Bảo mật ứng dụng di động
- Bảo mật Internet Vạn Vật (IoT)
- Bảo mật mạng và hạ tầng
- Kiểm tra tuân thủ và các quy định
- Bảo mật ứng dụng bên thứ ba
- Bảo mật chuỗi cung ứng
- Ứng cứu sự cố

Giải pháp của CyStack

WhiteHub, nền tảng bảo mật cộng đồng đầu tiên và lớn nhất do CyStack phát triển tại Việt Nam nhằm giải quyết triệt để các vấn đề nêu trên. WhiteHub giúp các doanh nghiệp khởi chạy chương trình săn lỗi nhận thưởng của riêng họ để tìm ra các lỗ hổng một cách hiệu quả.

Chương trình săn lỗi nhận thưởng là một loại hình bảo mật cộng đồng nhằm khuyến khích các cá nhân hoặc nhóm, được gọi là "hacker mũ trắng", xác định và báo cáo các lỗ hổng bảo mật trong phần mềm hoặc hệ thống của công ty. Các công ty trao thưởng bằng tiền, quà tặng hoặc sự công nhận, cho những hacker mũ trắng phát hiện và báo cáo các lỗ hổng này.

Mục đích của chương trình săn lỗi nhận thưởng là xác định và giải quyết các lỗ hổng bảo mật một cách kịp thời và hiệu quả, đồng thời cung cấp một môi trường an toàn và bảo mật cho các hacker mũ trắng để báo cáo các lỗ hổng, giúp các doanh nghiệp cải thiện tình trạng bảo mật, giảm nguy cơ bị tấn công mạng và lộ lọt dữ liệu. Các chương trình săn lỗi nhận thưởng có thể được sử dụng để kiểm tra tính bảo mật của nhiều hệ thống và ứng dụng, bao gồm ứng dụng web, ứng dụng dành cho thiết bị di động và thiết bị IoT.

Quyền lợi khách hàng

WhiteHub là một nền tảng săn lỗi nhận thưởng cho phép các doanh nghiệp quản lý và điều phối các chương trình săn lỗi nhận thưởng của họ, đồng thời cung cấp thị trường cho các hacker mũ trắng để tìm và báo cáo các lỗ hổng:

- **Quy trình công việc có thể tùy chỉnh**: WhiteHub cho phép các doanh nghiệp tùy chỉnh các biểu mẫu gửi lỗ hổng và quy trình công việc của họ, cho phép họ xác định các quy trình của riêng mình để xử lý các báo cáo lỗ hổng.
- **Bảng điều khiển tập trung**: WhiteHub cung cấp bảng điều khiển tập trung để quản lý và theo dõi các báo cáo về lỗ hổng, bao gồm khả năng phân công nhiệm vụ, đặt mức độ ưu tiên và theo dõi tiến trình.
- **Kênh liên lạc an toàn**: WhiteHub bao gồm một hệ thống liên lạc tích hợp để cộng tác dễ dàng và an toàn giữa các doanh nghiệp và hacker mũ trắng.
- **Hệ thống phần thưởng**: WhiteHub có một hệ thống phần thưởng sẵn có để công nhận và khuyến khích những đóng góp có giá trị từ các hacker mũ trắng.
- **Kết nối với cộng đồng tin tặc có đạo đức toàn cầu**: WhiteHub cho phép các doanh nghiệp tìm kiếm và tương tác với các chuyên gia bảo mật từ khắp nơi trên thế giới một cách nhanh chóng và dễ dàng.
- **Tích hợp với các công cụ hiện có**: WhiteHub tích hợp với các công cụ và nền tảng bảo mật hiện có, cho phép các doanh nghiệp dễ dàng tích hợp nền tảng này vào cơ sở hạ tầng bảo mật hiện có.
- **Báo cáo và phân tích**: WhiteHub cung cấp báo cáo và phân tích toàn diện, cung cấp cho các doanh nghiệp thông tin chuyên sâu chi tiết về hiệu quả của chương trình săn lỗi nhận thưởng của họ.

Cách thức hoạt động

Một chương trình săn lỗi nhận thưởng tại WhiteHub thường hoạt động như sau:

1. **Phạm vi và quy định**
   CyStack cùng với khách hàng định nghĩa phạm vi của chương trình săn lỗi nhận thưởng, hay làm rõ các hệ thống hoặc phần mềm được phép kiểm thử, cùng với các loại lỗ hổng hợp lệ được trao thưởng. Quy định của chương trình cũng được cần được thiết lập, bao gồm các mức trao thưởng, quy trình gửi báo cáo và khoảng thời gian nhận phần thưởng.
2. **Khởi chạy chương trình**
   CyStack khởi chạy chương trình săn lỗi nhận thưởng trên WhiteHub, công bố với cộng đồng và đưa ra thông tin chi tiết về phạm vi của chương trình.
3. **Kiểm thử**
   Hacker mũ trắng, cũng có thể gọi là chuyên gia săn lỗi, thuộc cộng đồng WhiteHub tìm kiếm các lỗ hổng trong các hệ thống và phần mềm được yêu cầu. Các hacker mũ trắng sử dụng đa dạng các kỹ thuật và công cụ để phát hiện các lỗ hổng, bao gồm kiểm thử thủ công, rà quét tự động và kiểm thử xâm nhập.
4. **Báo cáo**
   Khi chuyên gia săn lỗi tìm thấy một lỗ hổng, họ báo cáo lỗ hổng này trên WhiteHub và cung cấp thông tin chi tiết về lỗ hổng, bao gồm các bước tái tạo lỗ hổng và các tác động hoặc rủi ro xảy ra khi khai thác lỗ hổng đó.
5. **Xét duyệt**
   CyStack sẽ duyệt lỗ hổng được báo cáo để quyết định đó có thực sự là một vấn đề bảo mật, và vấn đề này có đạt đủ điều kiện nhận thưởng.
6. **Trao thưởng**
   Nếu lỗ hổng được báo cáo là đúng và hợp lệ, chuyên gia săn lỗi sẽ nhận khoản trả thưởng theo bảng định mức trao thưởng đã được thiết lập cho chương trình. Giá trị của phần thưởng có thể khác nhau, quyết định bởi mức độ nghiêm trọng của lỗ hổng, tác động của lỗ hổng lên công ty và khách hàng của công ty đó, cũng như mức độ phức tạp để phát hiện ra lỗ hổng.
7. **Khắc phục lỗ hổng**
   Khách hàng theo đó khắc phục lỗ hổng và có thể trao đổi trực tiếp với chuyên gia săn lỗi để làm rõ thêm thông tin cũng như yêu cầu trợ giúp để xác nhận bản vá lỗi hoạt động hiệu quả.
8. **Công khai các phát hiện**
   Sau khi lỗ hổng đã được khắc phục, khách hàng có thể công bố công khai lỗ hổng và vinh danh chuyên gia săn lỗi vì sự đóng góp của họ đã giúp hệ thống của doanh nghiệp trở nên bảo mật hơn.

Các gói dịch vụ

WhiteHub cung cấp 2 gói cho khách hàng: Chương trình công lỗ hổng bảo mật và săn lỗi nhận thưởng được quản lý. Bảng dưới đây mô tả sự khác biệt của các gói dịch vụ:

	Chương trình công bố lỗ hổng bảo mật	**Chương trình quản lý săn lỗi nhận thưởng**
Phù hợp với	Doanh nghiệp có nhân sự bảo mật, có thể tự quản lý chương trình săn lỗi nhận thưởng	Doanh nghiệp không có nhân sự bảo mật hoặc có nhưng không muốn chi thêm nhân lực cho việc hạy chương trình săn lỗi nhận thưởng
Lỗ hổng được xử lý bởi Đối tượng thảo luận với người báo cáo và xác minh báo cáo	Khách hàng	Đội ngũ WhiteHub
Tên miền có thương hiệu Chương trình được truy cập qua miền/miền phụ của máy khách, không phải miền WhiteHub	Không	Có
Số lượng chương trình Số lượng chương trình tối đa mà khách hàng có thể khởi chạy	Tối đa 2	Tối đa 4
Chương trình hiển thị với Đối tượng có thể xem và tham gia chương trình	Mọi người	Mọi người, hoặc chỉ các chuyên gia nghiên cứu được mời
Chính sách chương trình được xây dựng bởi Đối tượng và cách chính sách chương trình được xây dựng	Khách hàng, dựa trên chính sách cơ bản	Khách hàng, với sự tư vấn từ đội ngũ WhiteHub
Được quảng bá qua Các kênh được sử dụng để quảng bá chương trình	Các kênh miễn phí (mạng xã hội, nhóm chat, v.v.)	Cả kênh miễn phí và trả phí (quảng cáo, báo chí, v.v.)
Đánh giá trước Đội ngũ WhiteHub thực hiện kiểm thử bảo mật trước khi khởi chạy chương trình	Không	Đánh giá lỗ hổng và kiểm thử bảo mật
Kênh hỗ trợ Kênh nhận hỗ trợ từ đội ngũ WhiteHub	Ticket, chat	Ticket, chat, điện thoại và hỗ trợ ưu tiên
Các chuyên gia nghiên cứu được lựa chọn dựa trên Quy tắc lựa chọn chuyên gia nghiên cứu bảo mật cho chương trình	Không có tiêu chí cụ thể	Kỹ năng, điểm danh tiếng, chứng chỉ, NDA
Chuyên gia xử lý lỗi Các quy tắc để chỉ định một chuyên gia xử lý phát hiện mới	Xác định trước	Xác định trước, ngẫu nhiên hoặc vòng tròn

Quy trình làm việc với khách hàng

Tư vấn ban đầu	Thiết lập chương trình	Vận hành chương trình	Báo cáo và phân tích	Hỗ trợ liên tục
Khách hàng và đội ngũ của WhiteHub sẽ có một cuộc tư vấn ban đầu để thảo luận về các mục tiêu bảo mật của khách hàng, phạm vi của chương trình và các loại lỗ hổng sẽ nằm trong phạm vi.	Đội ngũ của WhiteHub sẽ làm việc với khách hàng để thiết lập chương trình, bao gồm việc tạo biểu mẫu gửi tùy chỉnh và quy trình làm việc, thiết lập hệ thống phần thưởng và thiết lập cấu hình phạm vi của chương trình.	Sau khi chương trình được thiết lập, WhiteHub sẽ khởi chạy chương trình và mời các chuyên gia nghiên cứu bảo mật tham gia thông qua các chiến dịch quảng cáo, sau đó chúng tôi chờ và xử lý báo cáo.	WhiteHub cung cấp báo cáo và phân tích toàn diện, đem lại cho các tổ chức thông tin chuyên sâu, chi tiết về hiệu quả của chương trình săn lỗi nhận tiền thưởng.	WhiteHub cung cấp hướng dẫn và hỗ trợ liên tục để đảm bảo chương trình săn lỗi nhận tiền thưởng hoạt động trơn tru.

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