VinCSS
Trusted Cybersecurity Pioneer

RED TEAMING

MÔ TẢ

Red team là dịch vụ mô phỏng các cuộc tấn công tinh vi có chủ đích (APT) nhằm vào các tổ chức và doanh nghiệp nhằm phát hiện và xử lý sớm các hướng tấn công khả thi có thể bị lợi dụng khai thác, cũng như đánh giá tính hiệu quả của các biện pháp phòng vệ mạng hiện có dưới góc nhìn của kẻ xấu.

Dịch vụ Red team khi được cung cấp dưới hình thức liên tục (Continuous Red teaming) có thể giúp các tổ chức doanh nghiệp phát hiện và cảnh báo sớm các mối đe doạ thường bị bỏ sót từ các biện pháp và quy trình phòng vệ, hoặc các mối đe doạ an ninh bảo mật phi kỹ thuật.

Trusted Cybersecurity Pioneer

CHỨC NĂNG

MÔ PHỎNG TẤN CÔNG TINH VI CÓ CHỦ ĐÍCH

Dịch vụ Red team có thể mô phỏng kỹ chiến thuật (TTPs) của các nhóm APT hoặc mô phỏng một cuộc tấn công tinh vi có chủ đích nhằm giúp các doanh nghiệp kiểm tra thực nghiệm, cũng như có được một cái nhìn thực tế về cách mà các lỗ hổng an ninh bảo mật bị lợi dụng để nhằm vào hoạt động sản xuất kinh doanh của doanh nghiệp.

SĂN TÌM MỐI NGUY CHỦ ĐỘNG

Dịch vụ Red team khi được cung cấp dưới hình thức liên tục (Continuous Red teaming), sẽ giúp các tổ chức doanh nghiệp chủ động săn tìm để từ đó phát hiện sớm các nguy cơ an ninh bảo mật từ bên ngoài có thể bị lợi dụng để nhằm vào tổ chức doanh nghiệp. Hoặc phát hiện và khắc phục sớm các chuỗi điểm yếu an ninh bảo mật từ bên trong có thể bị kẻ xấu lợi dụng để đạt được mục tiêu, mở rộng phạm vi ảnh hưởng sau khi đã thâm nhập được vào nội bộ.

THEO DÕI VÀ CẢNH BÁO DỮ LIỆU BỊ RÒ RỈ

Dưới sự trợ giúp của hệ thống theo dõi thông tin về dữ liệu bị rò rỉ trên Internet - Data Leak Intelligence, dịch vụ Red team chủ động theo dõi và cảnh báo khi phát hiện dữ liệu liên quan đến doanh nghiệp bị rò rỉ hoặc bị kẻ xấu rao bán trên Internet.

ĐÁNH GIÁ KHẢ NĂNG PHÒNG VỆ MẠNG

Dịch vụ Red team có thể được sử dụng để đánh giá khả năng phòng vệ mạng, an ninh vật lý tại một văn phòng, trụ sở, cơ sở, nhà máy. Tổ chức doanh nghiệp cũng có thể sử dụng dịch vụ Red team để thực hiện các cuộc thực nghiệm, mô phỏng nhằm phối hợp với Blue team trong việc đánh giá tính hiệu quả, cải thiện chất lượng cho các giải pháp phòng vệ mạng (Purple Teaming).

VinCSS
Trusted Cybersecurity Pioneer

QUY TRÌNH

01

XÁC ĐỊNH MỤC TIÊU

VinCSS sẽ thảo luận cùng khách hàng để xác định được mục tiêu cụ thể mà khách hàng muốn đạt được từ dịch vụ. Ví dụ, kiểm tra khả năng kẻ xấu có thể thâm nhập từ bên ngoài Internet vào mạng nội bộ và chứng minh khả năng kẻ xấu có thể tiếp cận được dữ liệu tài chính.

02

THỐNG NHẤT PHƯƠNG PHÁP VÀ THỜI GIAN THỰC HIỆN

Sau khi thống nhất được mục tiêu, VinCSS tư vấn cho khách hàng các phương pháp nên được thực hiện để đạt được mục tiêu, thời gian thực hiện. Ví dụ, nên triển khai các biện pháp nghiệp vụ nào, công cụ sử dụng ra sao, kỹ chiến thuật được lựa chọn là gì. Nên triển khai Continuous Red teaming hay Red team Campaign, campaign kéo dài bao lâu.

03

XÁC ĐỊNH QUY TẮC THỰC HIỆN:

VinCSS thảo luận cùng khách hàng để xác định các quy tắc cần tuân thủ trong quá trình thực hiện dịch vụ. Ví dụ, các biện pháp nghiệp vụ không được thực hiện hoặc cơ chế phối hợp giữa VinCSS và khách hàng trong thời gian diễn ra dịch vụ.

04

THỰC HIỆN

VinCSS sẽ tiến hành các hoạt động theo timeline đã cam kết.

05

BÁO CÁO KẾT QUẢ

Đối với hình thức chiến dịch đơn lẻ, VinCSS sẽ gửi báo cáo kết quả chi tiết, các kịch bản giúp tái hiện lại vấn đề (nếu cần) sau khi kết thúc chiến dịch. Đối với hình thức Continuous Red teaming, VinCSS báo cáo các mối nguy bảo mật ngay khi phát hiện và thực nghiệm thành công, đồng thời báo cáo tiến độ công việc định kỳ.

06

XÁC MINH TÌNH TRẠNG KHẮC PHỤC

VinCSS đồng hành cùng khách hàng trong việc tư vấn khắc phục và xác minh tình trạng khắc phục các điểm yếu bảo mật đã được báo cáo cho đến khi các điểm yếu đã được khắc phục. Báo cáo xác nhận sau khắc phục.

KẾT QUẢ

Từ các báo cáo Red team, tổ chức doanh nghiệp sẽ nhìn thấy một cách chân thực nhất các vấn đề bảo mật nào đang hiện hữu đối với môi trường của mình.

Đặc biệt, các vấn đề đó được liên kết và xâu chuỗi để khai thác như thế nào, liệu kẻ xấu có thành công đạt được mục tiêu để tạo ra những ảnh hưởng thực sự to lớn cho tổ chức doanh nghiệp hay không.

Ngoài ra, báo cáo Red team cũng sẽ tư vấn cho các tổ chức doanh nghiệp phương án khắc phục các vấn đề bảo mật và những điểm yếu cần quan tâm xử lý để giảm thiểu nguy cơ trở thành nạn nhân của một cuộc tấn công tinh vi nhắm mục tiêu.

Trusted Cybersecurity Pioneer

LỢI ÍCH

GIẢM THIỂU CÁC HƯỚNG TẤN CÔNG

Thực tế có thể bị lợi dụng để gây ra ảnh hưởng thực sự đối với hoạt động kinh doanh của tổ chức doanh nghiệp.

CHỦ ĐỘNG PHÁT HIỆN VÀ GIẢM THIỂU CÁC VẤN ĐỀ AN NINH BẢO MẬT

Đặc biệt là các vấn đề bảo mật tiềm tàng nhưng có thể tạo thành một chuỗi khai thác trong thực tế, hoặc các vấn đề mới phát sinh trong quá trình vận hành liên tục của tổ chức doanh nghiệp.

KIỂM TRA SỰ HIỆU QUẢ CỦA CÁC GIẢI PHÁP PHÒNG VỆ

Cũng như giảm thiểu tối đa các vấn đề bị bỏ sót từ các biện pháp an ninh bảo mật khác.

ĐIỂM MẠNH

ĐỘI NGŨ NHÂN SỰ GIÀU KINH NGHIỆM

VinCSS có một đội ngũ Red team giàu kinh nghiệm từng đạt nhiều chứng chỉ an ninh bảo mật uy tín trong ngành như chứng chỉ SANS, Offensive Security. Đội ngũ Red team của VinCSS được rèn luyện liên tục qua nhiều môi trường trong một Tập đoàn đa ngành nghề hàng đầu trong nước như Automotive, Y tế, Bán lẻ, Bất động sản, Sản xuất thiết bị di động, Công nghệ, Giáo dục.

PHƯƠNG ÁN KỸ THUẬT ĐA DẠNG

Các chiến dịch Red team của VinCSS thường được tổ chức với các bộ kỹ chiến thuật đa dạng, không giới hạn phương pháp. Từ mô phỏng Phishing, Vishing, Wireless Testing, Physical Testing. Phương pháp kỹ thuật sẽ được lựa chọn và đề xuất phù hợp theo từng bài toán của khách hàng.

MINH BẠCH

Mọi hoạt động Red team của VinCSS được giám sát chặt chẽ bởi VinSOC, khách hàng có thể theo dõi hoặc kiểm tra hoạt động và dữ liệu của đội ngũ Red team bất kỳ khi nào có nhu cầu.

HỖ TRỢ TỐI ĐA TRONG QUÁ TRÌNH KHẮC PHỤC SAU BÁO CÁO

VinCSS theo sát để đồng hành cùng khách hàng trong quá trình khắc phục các vấn đề bảo mật đã được phát hiện, tư vấn và giúp khách hàng xác minh tình trạng khắc phục cho đến khi mọi vấn đề đã báo cáo đều được khắc phục.

VinCSS
Trusted Cybersecurity Pioneer

THANK YOU!

VINCSS INTERNET SECURITY SERVICES JSC

• Floor 20A, Vincom Center Dong Khoi Building, No 45A Ly Tu Trong Street, Ben Nghe Ward, Dist. 1, HCMC, Vietnam.

• Email: sales@vincss.net • Website: www.vincss.net