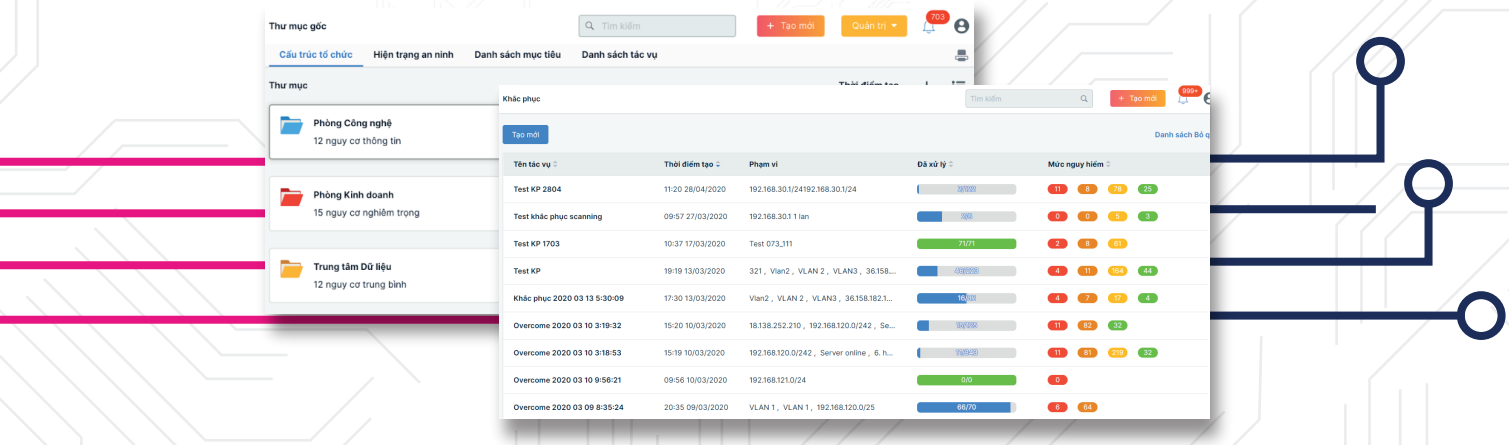
SecurityBox

GIẢI PHÁP QUẢN TRỊ NGUY CƠ AN NINH MẠNG NỘI BỘ



4NETWORK

SECURITYBOX 4NETWORK LÀ GIẢI PHÁP QUẢN TRỊ NGUY CƠ AN NINH TOÀN DIỆN CHO HỆ THỐNG MẠNG NỘI BỘ.

SecurityBox 4Network thực hiện rà quét, phát hiện và vẽ ra bức tranh toàn cảnh về tình trạng an ninh, số lượng điểm yếu, lỗ hổng của toàn hệ thống. Điều này cho phép quản trị viên nắm được thực trạng chi tiết an ninh của hệ thống, từ đó dễ dàng khoanh vùng và thực hiện các biện pháp xử lý, khắc phục để đảm bảo an toàn cho hệ thống.

SecurityBox 4Network là giải pháp duy nhất hiện nay có khả năng cung cấp công nghệ tạo, quản lý và hướng dẫn khắc phục mọi nguy cơ an ninh của hệ thống. Công nghệ này thiết kế một quy trình xử lý nguy cơ thông minh, cho phép khách hàng và đối tác dễ dàng khắc phục điểm yếu và lỗ hổng đã được cảnh báo và phát hiện.

NĂNG LỰC RÀ QUÉT VÀ PHÁT HIỆN NGUY CƠ AN NINH CỦA SECURITYBOX 4NETWORK:

Tiêu chí	Thông số
Số lượng mã nhận diện lỗ hổng/điểm yếu an ninh	> 120.000
Số lượng script để phát hiện lỗ hổng đặc thù hoặc thực hiện kiểm thử xâm nhập tự động.	> 1.000
Số lượng mã nhận diện cập nhật hàng tháng	> 500
Số lượng kiểu thiết bị được hỗ trợ (Máy tính, máy in...)	> 1.000

Chi tiết chức năng

Giải pháp giám sát tình trạng an ninh hệ thống

- Đánh giá hiện trạng an ninh toàn hệ thống hoặc của từng phòng ban/ tổ chức trong hệ thống theo tiêu chí An toàn/Nguy hiểm.
- Quản lý nguy cơ an ninh theo từng phòng ban, tổ chức.
- Phát hiện, cảnh báo thông tin lỗ hổng/điểm yếu trên toàn hệ thống.
- Phát hiện, cảnh báo thông tin lỗ hổng/điểm yếu cho từng phòng ban, tổ chức.
- Phát hiện, cảnh báo một số các bất thường xảy ra với hệ thống mạng như việc có sự biến động tăng/giảm về số lượng cổng/dịch vụ trên thiết bị; biến động về số lượng thiết bị tham gia vào hệ thống mạng.
- Phát hiện, cảnh báo tức thời các lỗ hổng/nguy cơ có khả năng khai thác thông qua Email/SMS/Slack.
- Tổng hợp và thống kê nguy cơ an ninh của hệ thống từng gặp phải theo thời gian.
- Giám sát các bất thường xảy ra với hệ thống trong ngày hoặc 7 ngày hoặc 30 ngày gần nhất. Đồng thời tổng hợp và thống kê các bất thường đã xảy ra với mục tiêu rà quét.
- Giám sát lịch sử đánh giá an ninh của hệ thống qua thời gian.
- Giám sát lịch sử kiểm tra trạng thái của từng thiết bị trong hệ thống qua thời gian.
- Thống kê lại toàn bộ lịch sử quá trình giám sát, đánh giá nguy cơ an ninh mạng.

Rà quét và phát hiện nguy cơ an ninh hệ thống

- Rà quét, phát hiện các thiết bị trong hệ thống mạng bao gồm máy chủ, máy tính, máy in, camera, các thiết bị IoT...
- Phát hiện các thông tin cơ bản trong mạng: thông tin cổng, dịch vụ, phiên bản tương ứng, thông tin hệ điều hành.
- Rà quét, phát hiện các lỗ hổng/điểm yếu hệ điều hành như Windows XP/7/8/10; Windows Server 2003/2008/2012/2016; OS X/Linux/Solaris; FreeBSD; Cisco; IBM ...
- Rà quét, phát hiện các lỗ hổng/điểm yếu phần mềm như Oracle, SQL Server, MySQL, DB2, Informix /DRDA, PostgreSQL, MongoDB ...
- Cơ chế học và dạy thiết bị thông minh để lọc bỏ dần các cảnh báo sai (false positive) trong thời gian đầu triển khai thiết bị.
- Thông tin chi tiết các lỗ hổng theo các chuẩn về lỗ hổng an ninh CVE, CPE và OVAL.
- Lỗ hổng điểm yếu hiện thị dưới 04 tiêu chí: Nguy cơ xâm nhập, mức an ninh Nghiêm trọng, mức an ninh Cao, mức an ninh Trung bình.
- Lập lịch rà quét an ninh định kì.

Tấn công kiểm thử

- Tấn công thử nghiệm với các lỗ hổng có khả năng tấn công khai thác.

Chi tiết chức năng

Khắc phục lỗ hổng/điểm yếu của hệ thống

- Đề xuất các biện pháp khắc phục tương ứng với các lỗ hổng, thiết bị và các thông tin đã thu thập được.
- Theo dõi số lượng lỗ hổng điểm yếu đã khắc phục, chưa khắc phục thông qua giao diện quản trị.
- Ghi dấu, theo dõi, giám sát quá trình khắc phục lỗ hổng điểm yếu. Hỗ trợ phương thức ghi chú trên từng lỗ hổng trong quá trình khắc phục.

Tự động hóa quy trình kiểm tra an ninh

- Toàn bộ việc kiểm tra an ninh được thực hiện tự động theo lịch đã đặt sẵn.
- Tùy chỉnh phương thức hoạt động theo kiến trúc mạng của doanh nghiệp.

Báo cáo

- Tạo báo cáo sau mỗi lần thực hiện rà quét (báo cáo cơ bản, báo cáo chi tiết).
- Tạo báo cáo hỗ trợ sửa lỗi tương ứng với từng mục tiêu đã thực hiện rà quét (báo cáo hỗ trợ sửa lỗi).
- Hỗ trợ báo cáo mọi lỗ hổng và nguy cơ được mô tả trong các chuẩn quốc tế OWASP, NIST, PTES, OSSTMM, ISSAF.
- Hỗ trợ báo cáo theo các mức độ khác nhau (báo cáo cơ bản, báo cáo chi tiết theo thiết bị, báo cáo chi tiết theo nguy cơ).
- Hỗ trợ báo cáo theo nhiều định dạng khác nhau như Word, Excel.

Phương thức vận hành

- Quản trị thông qua giao diện Website.
- Hỗ trợ tiếng Việt.
- Cấu hình mạng và các thông số cho thiết bị thông qua giao diện quản trị.