SOAR

I. Khái niệm

+ SOAR (security orchestration, automation and respond) là một tập hợp các chương trình phần mềm tương thích cho phép tổ chức thu thập dữ liệu về các mối đe dọa an ninh mạng và ứng phó sự cố với các sự kiện bảo mật mà không cần hoặc có rất ít sự trợ giúp của con người.

+ Có 3 thành phần chính: Điều phối bảo mật (security orchestration), tự động hóa bảo mật (security automation), phản hồi bảo mật (security respond)

\* Security orchestration:

+ Điều phối bảo mật kết nối và tích hợp các công cụ bên trong và bên ngoài khác nhau thông qua tích hợp sẵn hoặc tùy chỉnh và giao diện lập trình ứng dụng

+ Các hệ thống được kết nối: vulnerability scanners, endpoint protection product, user and entity behavior analytics, firewalls, IDS/IPS, SIEM, endpoint security software, nguồn cấp dữ liệu thông tin về mối đe dọa bên ngoài và các nguồn của bên thứ ba khác.

=> Thu thập đươc nhiều dữ liệu => Nâng cao phát hiện threats >< Cảnh báo sinh ra nhiều hơn, phải phân tích nhiều hơn

\* Security automation:

+ Được cung cấp bởi dữ liệu và cảnh báo được thu thập từ việc điều phối bảo mật, nhập và phân tích dữ liệu, đồng thời tạo các quy trình tự động, lặp lại để thay thế các quy trình thủ công

+ Các nhiệm vụ được các nhà phân tích thực hiện trước đây, chẳng hạn như quét lỗ hổng, phân tích nhật ký, khả năng kiểm tra và kiểm tra vé, có thể được chuẩn hóa và thực thi tự động bởi nền tảng SOAR = sử dụng AI và machine learning để giải mã và điều chỉnh thông tin chi tiết từ các nhà phân tích.

+  tự động hóa SOAR có thể ưu tiên các mối đe dọa, đưa ra khuyến nghị và tự động hóa các phản hồi trong tương lai,

+ tự động hóa có thể nâng cao các mối đe dọa nếu cần sự can thiệp của con người

+ Quan trọng: Playbook – được tạo sẵn hoặc tùy chỉnh là các hành động tự động được xác định trước

\* Security respond:

+ Cung cấp một cái nhìn duy nhất cho các nhà phân tích trong việc lập kế hoạch, quản lý, giám sát và báo cáo các hành động được thực hiện sau khi phát hiện ra mối đe dọa.

+ Chế độ xem duy nhất này cho phép cộng tác và chia sẻ thông tin về mối đe dọa giữa các nhóm bảo mật, mạng và hệ thống. Nó cũng bao gồm các hoạt động ứng phó sau sự cố, chẳng hạn như quản lý và báo cáo trường hợp.

II. Cách hoạt động:

1. Thu thập dữ liệu:

+ SOAR tích hợp với các công cụ bảo mật để thu thập dữ liệu từ các nguồn khác nhau như logs hệ thống, cảnh báo từ SIEM, dữ liệu threat intelligence và các nguồn khác

1. Phân tích dữ liệu:

+ SOAR phân tích và chuẩn hóa dữ liệu, sau đó sử dụng các thuật toán hoặc quy tắc để xác định các mối đe dọa tiềm tàng

1. Kích hoạt kịch bản:

+ Dựa trên sự phân tích, SOAR kích hoạt các kịch bản bảo mật (playbooks) để ứng phó với mối đe dọa. Playbooks có thể bao gồm việc điều tra chi tiết, thực hiện hành động cách ly, hoặc thông báo cho đội ngũ bảo mật

1. Phản ứng và xử lý sự cố:

+ SOAR tiến hành thực hiện các hành động cần thiết để xử lý sự cố, bao gồm cách ly hệ thống bị ảnh hưởng, chặn lưu lượng mạng, hoặc gửi cảnh báo chi tiết đến nhóm bảo mật để điều tra sâu hơn

1. Báo cáo và theo dõi:

+ Sau khi sự cố được xử lý, SOAR tạo ra các báo cáo chi tiết về quá trình phản ứng và kết quả cuối cùng. Các báo cáo này giúp tổ chức theo dõi và cải thiện quy trình bảo mật.