Datasheet

Viettel Kill-chain & Anomaly
(VCS - KIAN)

viettel security

Sự cần thiết của giải pháp

Trong giai đoạn chuyển dịch tới kỷ nguyên công nghệ 4.0, việc bảo vệ & chống lại tác nhân nguy hiểm từ phần mềm độc hại, mối nguy từ bên trong, đến hành vi tấn công mang tính chủ đích từ bên ngoài bởi nhóm hacker ngày càng trở nên phức tạp. Phương thức khai thác, che giấu hành vi của tác nhân này ngày càng tinh vi & khó phát hiện hơn, khiến cho giải pháp truyền thống nhanh chóng trở nên thiếu hiệu quả, không đủ khả năng đáp ứng nhu cầu của Trung tâm giám sát & vận hành (S.O.C). Để giải quyết vấn đề này, tổ chức cần một giải pháp nâng cao dựa trên công nghệ hiện đại như học máy, phân tích hành vi, xử lý dữ liệu lớn.

Các tính năng chính

Phân tích và học tự động hành vi, thói quen của người dùng thực thể trong hệ thống mạng của tổ chức

VCS - KIAN thực hiện xây dựng và cập nhập hồ sơ của đối tượng theo một tập hành vi nghiệp vụ đã được hệ thống định nghĩa trước, sau đó sử dụng thông tin hành vi của đối tượng đã được mô hình hóa cho các quá trình phân tích, xử lý dữ liệu đầu vào từ nguồn gửi dữ liệu. Từng đối tượng người dùng & thực thể sẽ được người quản trị giám sát thông qua giao diện, cho phép cả hành động điều chỉnh ngưỡng cảnh báo rủi ro trên từng đối tượng. VCS-KIAN hỗ trợ xác định những người dùng/ thực thể hoặc hành vi mới xuất hiện trong hệ thống mạng.

Phát hiện và cảnh báo theo thời gian thực

VCS-KIAN cung cấp Engine xử lý dữ liệu với hiệu năng và khả năng chịu tải cao, cho phép phân tích sự kiện theo thời gian thực đối với dữ liệu nhật ký thu thập được từ nguồn dữ liệu, dựa trên tập kịch bản phát hiện bất thường đã được định nghĩa & thiết lập, hành vi đã được mô hình hóa của đối tượng & mức độ rủi ro của đối tượng. Từ đó đưa ra cảnh báo thời gian thực về dấu hiệu, nguy cơ, sự cố, cuộc tấn công & hành vi gây mất an toàn thông tin khác dựa trên kết quả thực thi tập kịch bản phát hiện bất thường; hoặc về đối tượng trong hệ thống được giám sát có điểm rủi ro vượt ngưỡng đã được thiết lập. Cảnh báo xuất hiện tự động thông qua hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo.

Kết hợp hướng đi rule-based truyền thông với học máy & phân tích hành vi

VCS - KIAN cung cấp nhiều công cụ để xây dựng kịch bản phát hiện với các mức độ phức tạp khác nhau nhưu tập luật truyền thống, tập luật thông minh dựa trên công nghệ phân tích hành vi, học máy, gom nhóm sự kiện trong khung thời gian.

Hiệu năng vượt trội

- Tích hợp sẵn 900 kịch bản phát hiện bất thường áp dụng trên tập dữ liệu từ các nguồn, với độ phủ hơn 50% các kĩ thuật tấn công mô tả theo MITRE ATT&CK.
- Xử lý & lưu trữ dữ liệu đồng thời tối thiểu 10000 sự kiện trong khoảng thời gian là 01 giây.
- Phân tích & lưu trữ các mô hình hành vi của ít nhất 10000 đối tượng trong hệ thống được giám sát trong thời gian tối thiểu 30 ngày.

Giải pháp Viettel Kill-chain & Anomaly

Viettel Kill-chain & Anomaly (VCS - KIAN) là giải pháp bảo vệ dựa trên phân tích hành vi của đối tượng trong hệ thống (User and Entify Behavior Analytics). VCS - KIAN tự động và liên tục hồ sơ hóa, xâu chuỗi hành vi của người dùng và thực thể, kết hợp với công nghệ học máy và xử lý dữ liệu lớn thời gian thực. Từ đó cung cấp một lớp phân tích mạnh mẽ phía trên các giải pháp quản lý Log tập trung như SIEM, giúp cho chuyên gia S.O.C có thể xây dựng các kịch bản phát hiện các mối nguy và phản ứng lại chúng một cách nhanh chóng.

Tìm kiếm chuỗi hành vi bất thường

Trong thực tế, việc chỉ thấy một hành vi bất thường đơn lẻ chưa đủ để bắt được phương thức tấn công phức tạp của hacker, VCS - KIAN cung cấp khả năng viết kịch bản dưới dạng chuỗi hành vi, các bước trong một chu kỳ tấn công. Một số hành vi bất thường có thể được phát hiện gồm:

- Phát hiện hành vi đăng nhập từ nguồn, địa chỉ, subnet lạ.
- Phát hiện process bất thường, Phát hiện outbound bất thường theo isp; Phát hiện hành vi mở port bất thường.
- Phát hiện hành vi back-connect ra máy chủ điều khiển Public.
- Phát hiện hành vi truy cập webshell, DNS tunnel.

Hỗ trợ quản trị dễ dàng

Cung cấp giao diện trực quan giúp người quản trị thực hiện quản lý các thông tin gồm:

- Nguồn gửi dữ liệu, đích nhận dữ liệu với các thao tác thêm mới/chỉnh sửa/tìm kiếm/xóa bỏ.
- Tập hành vi được giám sát với các thao tác thêm mới/chỉnh sửa/tìm kiếm/xóa bỏ/cập nhật từ nhà sản xuất.
- Tập kịch bản phát hiện bất thường với các thao tác thêm mới/chỉnh sửa/tìm kiếm/xóa bỏ/kích hoạt/vô hiệu hóa/ cập nhật từ nhà sản xuất.

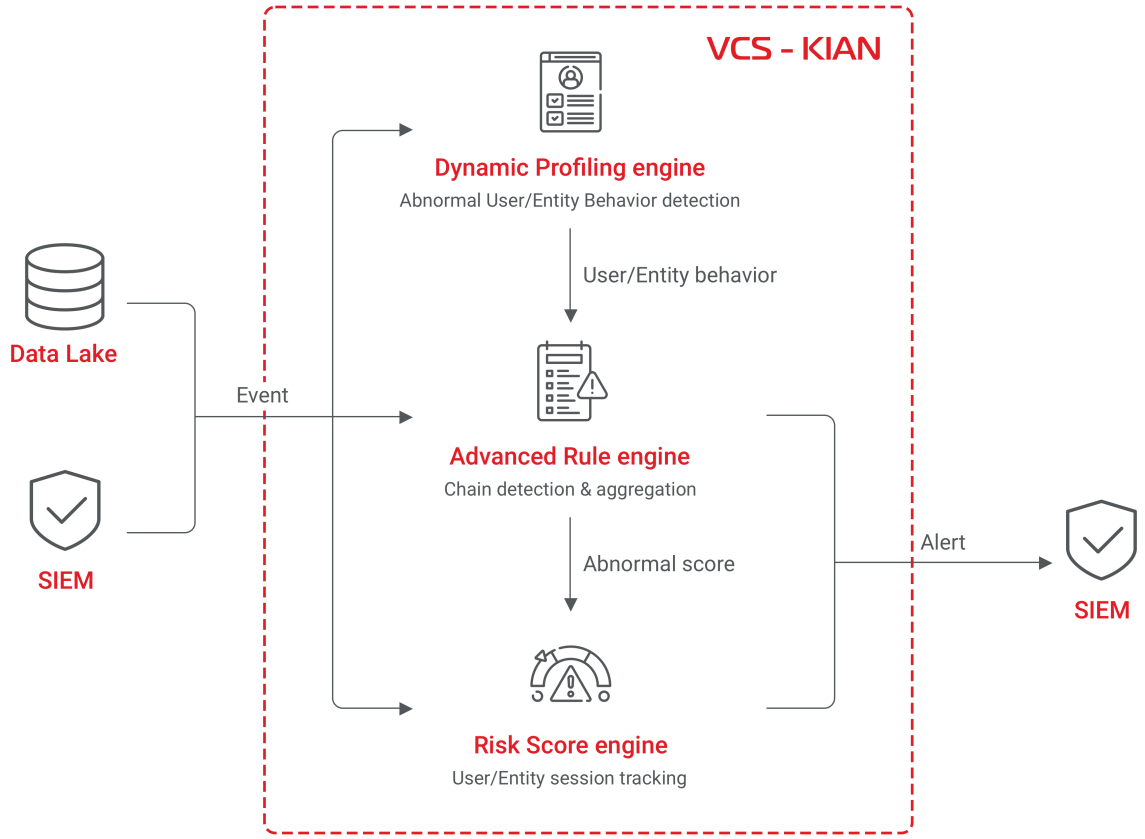
Xây dựng & tùy chỉnh kịch bản phát hiện trên một giao diện trực quan

Giao diện viết kịch bản trực quan là tính năng cần thiết, giúp cho S.O.C tối đa hóa hiệu suất làm việc thông qua việc có thể dễ dàng thử nghiệm, làm chủ & chuyển hóa tri thức, tùy chỉnh kịch bản để thích ứng với cuộc chiến không gian mạng thay đổi từng ngày.

Tích hợp với SIEM & Giải pháp quản lý Log tập trung

Thông qua tích hợp, VCS - KIAN việc cung cấp một lớp phân tích mạnh mẽ phía trên giải pháp SIEM, từ đó nâng cao khả năng bảo vệ của toàn bộ nền tảng. VCS-KIAN hỗ trợ tích hợp nguồn dữ liệu đầu vào theo chuẩn syslog CEF/LEEF.

Mô hình hoạt động của giải pháp



OPERATION MODEL

Dynamic Profiling engine

Engine sử dụng mô hình thống kê, học máy để phân tích dữ liệu Security nhằm tạo ra các hồ sơ, profile của người dùng và thực thể trong hệ thống được giám sát. Từ đó có thể xác định được các sự kiện bất thường, sự kiện mà có thể là hành động tấn công của Attacker.

Advanced Rule engine

Engine xử lý Rule thời gian thực, phân tích các sự kiện và đưa ra các cảnh báo bất thường khi sự kiện vi phạm kịch bản được định nghĩa trước bởi chuyên gia Security. Khác với các rule engine truyền thống, KIAN Advanced Rule engine hỗ trợ các phép toán nâng cao như Model Profile Logics, AI Logics, Aggregate/Windows Function Logics, Chain Rules.

Risk Score engine

Engine dựa trên các hành vi bất thường mà hệ thống giám sát được để đưa ra đánh giá về mức độ rủi ro của từng người dùng và thực thể, Từ đó ưu tiên các đối tượng cần vận hành, xử lý để ngăn chặn sớm sự cố An toàn thông tin.Cho phép quản lý rủi ro, nguy cơ theo đối tượng người dùng, thực thể.

Tính năng của giải pháp

TÍNH NĂNG	
Integration Management	Hỗ trợ tích hợp nhiều nguồn dữ liệu giám sát đầu vào theo chuẩn syslog CEF/LEEF
	Hỗ trợ tích hợp đẩy cảnh báo tới SIEM theo chuẩn syslog CEF/LEEF
	Tạo mới và quản lý hành vi cần giám sát
	Hỗ trợ xác thực Local
User/Entity Behavior Profiling	Giao diện cấu hình, tùy chỉnh các thông tin của người dùng/thực thể cần hồ sơ hóa
	Hồ sơ hóa thời điểm đầu tiên xuất hiện của một người dùng/thực thể hoặc một hành vi trên hệ thống
	Xác định người dùng/thực thể hoặc hành vi mới xuất hiện trong hệ thống mạng
	Xác định thời gian xuất hiện của một người dùng/thực thể hoặc hành vi trên hệ thống mạng
	Xác định mức độ bất thường theo thuộc tính so với thói quen lịch sử của một người dùng/thực thể khi thực hiện một hành vi đã được cấu hình giám sát
	Xác định mức độ bất thường theo thuộc tính trong tổ chức của một người dùng/thực thể
	Xác định mức độ phổ biến của một thuộc tính, người dùng, thực thể trong tổ chức
	Tự động cập nhật hồ sơ người dùng/thực thể gần thời gian thực
	Tính năng theo dõi và đánh giá mức độ rủi ro tấn công của mỗi Server/PC trong tổ chức
Detection Usecase Management	Tạo luật phát hiện tấn công theo hồ sơ thói quen của người dùng, thực thể
	Tạo luật thống kê nhiều trường dữ liệu trong một khoảng thời gian
	Tạo luật mô tả chuỗi các hành vi xuất hiện theo hoặc không theo thứ tự thời gian
	Gán mức độ rủi ro cho mỗi kịch bản phát hiện tấn công
	Quản lý danh sách tĩnh và xây dựng kịch bản sử dụng danh sách tĩnh
	Cập nhật động danh sách theo kịch bản phát hiện tấn công
Alert Management	Quản lý kịch bản phát hiện tấn công theo nhiều tiêu chí phân loại trong ATTT
	Quản lý và tìm kiếm cảnh báo theo kịch bản phát hiện tấn công
	Xem chi tiết thông tin cảnh báo
Content built-in	Các kịch bản giám sát tiến trình bất thường theo ATT&CK
	Các kịch bản giám sát phát hiện hành vi khám phá mạng nội bộ
	Các kịch bản giám sát tấn công webshell vào các máy chủ Web
	Phát hiện tấn công DNS tunnel
	Các kịch bản phát hiện đăng nhập bất thường từ mạng internet vào tổ chức