Datasheet

Viettel Security Information & Event Management

VCS-CyM

viettel security

Security Information & Event Management (SIEM) là gì?

SIEM là nền tảng giám sát tổng thể, đóng vai trò quan trọng, không thể thiếu trong hệ thống Trung tâm Điều hành An toàn thông tin (SOC) của một tổ chức, đơn vị.

Giải pháp cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ log, các sự kiện ATTT mạng được sinh ra trong hệ thống CNTT của tổ chức và cung cấp khả năng giám sát và phân tích dữ liệu vận hành theo thời gian thực.

Qua đó, giải pháp hỗ trợ tối đa các tổ chức, đơn vị trong việc nhanh chóng phát hiện và xử lý những sự cố, nguy cơ về ATTT trong đơn vị.

Ưu điểm nổi bật

Giải pháp VCS - CyM là sản phẩm tự phát triển của Công ty An ninh mạng Viettel. Sản phẩm có những ưu điểm, lợi thế như sau:

- Giám sát trong thời gian thực tất cả các thành phần trong hệ thống CNTT của khách hàng: Máy chủ, ứng dụng, thiết bị.
- Quản lý tập trung.
- Tri thức về ATTT được cập nhật liên tục.
- Được hỗ trợ bởi đội ngũ chuyên gia giàu kinh nghiệm.
- Kiến trúc triển khai mềm dẻo, dễ mở rộng theo quy mô của hệ thống.

Các tính năng chính của giải pháp VCS-CyM

Thu thập & chuẩn hoá dữ liệu

VCS-CyM sử dụng thành phần thu thập nhật ký ATTT thực hiện thu thập dữ liệu từ nhiều nguồn khác nhau (như máy chủ, thiết bị, ứng dụng ...) qua syslog, API, JDBC, WMI hoặc qua agent thu thập log trên hệ điều hành. Sau đó thành phần thu thập nhật ký ATTT thực hiện chuyển tiếp dữ liệu thu thập tới thành phần xử lý hỗ trợ loại kết nối UDP, TCP, TLS/SSL. VCS-CyM cho phép quản lý, theo dõi tình trạng hoạt động của thành phần thu thập nhật ký ATTT. Hệ thống phân tích loại bỏ dữ liệu dư thừa, chuẩn hóa & phân loại theo định dạng chung tối ưu hóa cho việc phân tích.

VCS-CyM hỗ trợ chuẩn hóa log từ các nguồn gồm: Windows, Unix (CentOS, Debian, Ubuntu), Firewall (Check Point, Cisco, Fortinet, Palo Alto, ...), Network (Cisco, McAfee, Trend Micro, Symatec, FireEyes, ForeScout, HP),... Hệ thống cũng cho phép lưu trữ nhật ký nguyên bản ban đầu phục vụ cho công tác điều tra, truy vết sau này.

Hỗ trợ tích hợp

VCS - CyM có sẵn bộ chuẩn hóa của hơn 100 loại ứng dụng, thiết bị phổ biến. Với các loại ứng dụng, thiết bị mới hệ thống cung cấp sẵn giao diện để thêm bộ chuẩn hóa một cách dễ dàng. VCS-CyM hỗ trợ tích hợp với hệ thống giám sát an toàn không gian mạng quốc gia của NCSC & hệ thống VCS-CyM khác.

Tự động cập nhật

Các phiên bản mới, bộ luật mới, tri thức mới luôn được cập nhật tự động, giúp giám sát toàn diện hệ thống của khách hàng tự động.

Tìm kiếm & điều tra

VCS-CyM với giao diện tìm kiếm thân thiện, điều kiện tìm kiếm tự định nghĩa gần gũi với ngôn ngữ người dùng, dễ dàng mở rộng hay thu hẹp điều kiện tìm kiếm bằng thao tác trên giao diện giúp việc tìm kiếm sự kiện, cảnh báo trong quá trình giám sát, điều tra thuận tiện, nhanh chóng. VCS-CyM hỗ trợ gom nhóm kết quả tìm kiếm theo trường dữ liệu phục vụ xử lý cảnh báo, xử lý sự cố.

Tối ưu lưu trữ dữ liệu

Hệ thống lưu trữ dữ liệu được đánh chỉ mục, sao lưu đảm bảo không mất mát dữ liệu, phục vụ cho quá trình điều tra, truy vết trong trường hợp gặp sự cố. Hệ thống còn hỗ trợ phân chia chính sách lưu trữ với nhiều loại không gian lưu trữ khác nhau giúp tối ưu hóa hiệu năng hoạt động và tiết kiệm chi phí đầu tư cho việc lưu trữ.

Phát hiện tấn công theo thời gian thực

VCS - CyM cho phép tự động cảnh báo thời gian thực thông qua việc hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo & cảnh báo qua việc gửi thư điện tử hoặc tin nhắn SMS. Cảnh báo được sắp xếp thứ tự ưu tiên tùy thuộc vào độ nghiêm trọng của loại tấn công cũng như mục tiêu bị tấn công. VCS-CyM cho phép xử lý & lưu trữ dữ liệu đồng thời 5000 sự kiện trong khoảng thời gian 1 phút.

Correlation

VCS-CyM hỗ trợ phân tích tương quan sự kiện theo thời gian thực đối với dữ liệu log thu thập được, với gần 1000 tập phát hiện cảnh báo tích hợp sẵn. Tùy từng nghiệp vụ khách hàng mà có thể tùy biến, thêm các luật mới. VCS-CyM cho phép người quản trị thêm/xóa/tinh chỉnh/tìm kiếm/kích hoạt/vô hiệu. Các tập luật được hỗ trợ export/import bằng các tệp tin, và được cập nhật liên tục từ nhà sản xuất qua thao tác tự động hoặc bằng tay

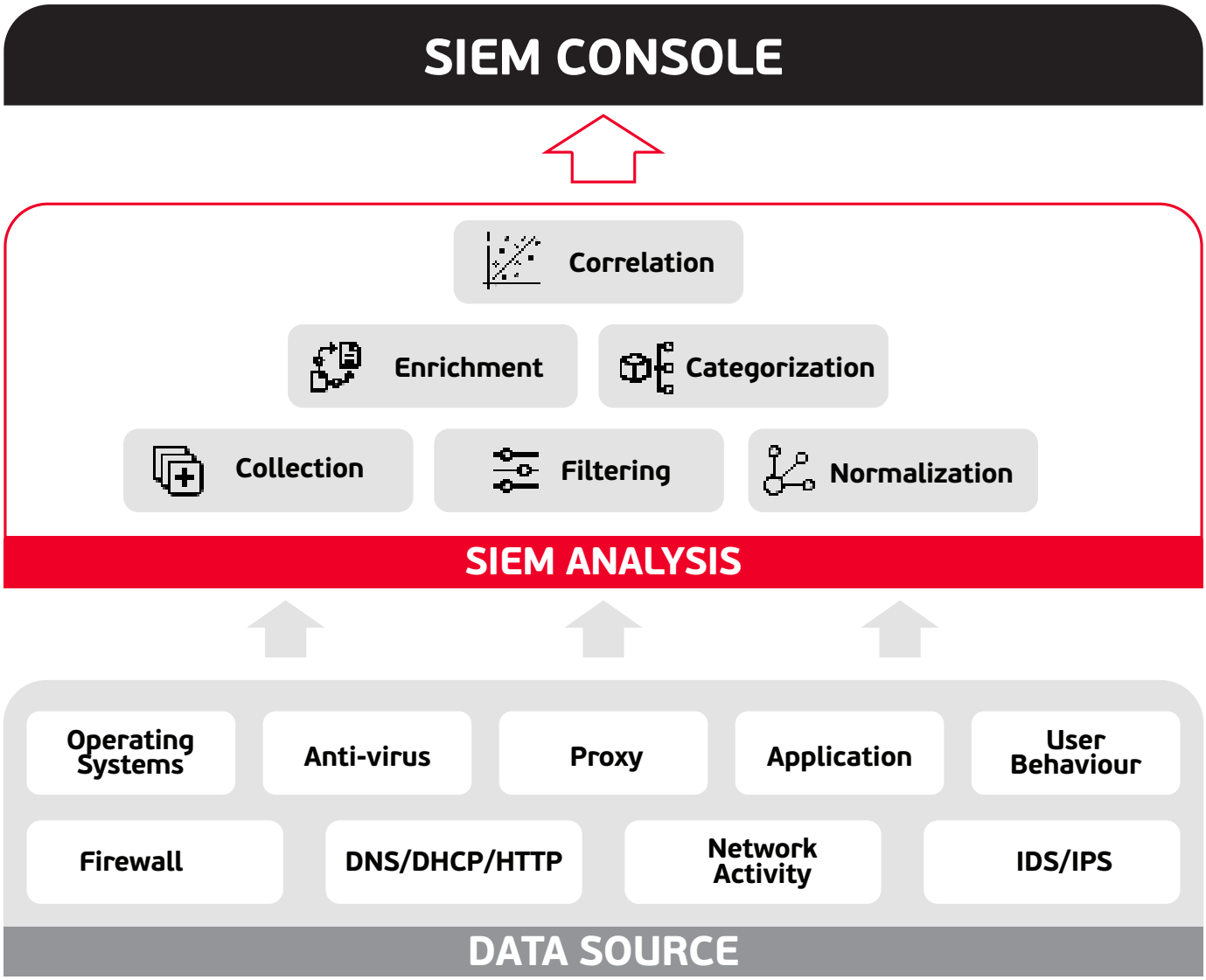
Dashboard trực quan, thân thiện

Cung cấp giao diện quản trị trực quan, thân thiện, đa dạng về thông tin và có thể tùy chỉnh theo nhu cầu sử dụng thực tế của khách hàng. Giao diện cũng hỗ trợ việc quản lý nguồn log, cho phép thêm các thiết bị, ứng dụng mới vào hệ thống để đảm bảo khả năng giám sát tức thì. VCS-CyM cung cấp sẵn các mẫu báo cáo, biểu đồ phổ biến. Thông qua giao diện trực quan, cho phép người quản trị thực hiện quản lý các báo cáo, mẫu báo cáo với các hành động gồm tạo mới/điều chỉnh/xóa bỏ/lọc.

Quản lý nguồn Log

Giao diện quản lý nguồn log giúp bạn chủ động thêm mới các ứng dụng, thiết bị phát sinh vào hệ thống, đảm bảo hệ thống của tổ chức luôn được giám sát. Người quản trị thực hiện quản lý đối tượng được giám sát & nguồn gửi log theo nhóm được định nghĩa hoặc theo địa chỉ IP, địa chỉ mạng, địa chỉ vật lý.

Mô hình hoạt động của giải pháp



Ba tầng xử lý dữ liệu trong mô hình kiến trúc của VCS-CyM

Tầng Data Source

Là nơi phát sinh dữ liệu ban đầu (raw data), có khả năng thu thập toàn bộ dữ liệu từ những hệ thống nằm trong hạ tầng CNTT như hệ điều hành, các ứng dụng, giải pháp Anti-virus, thiết bị mạng, thiết bị bảo mật Firewall, Proxy, IPS/IDS, các truy cập của người dùng hay người quản trị hệ thống CNTT của tổ chức.

Tầng SIEM Analysis

Là hệ thống phân tích dữ liệu thu thập được từ Data Source, tại đây dữ liệu được chuẩn hóa, làm mịn, phân loại và phân tích tương quan theo nhiều chiều để phát hiện các dấu hiệu, hành vi bất thường xuất hiện trong hệ thống.

Tầng SIEM Console

Là hệ thống Front-End tương tác với người dùng, giúp người dùng vận hành giám sát và xử lý cảnh báo, vi phạm, hoặc tìm kiếm, điều tra các thông tin từ hệ thống

Viettel Security Information & Event Management

VCS-CyM

viettel security

Tính năng của giải pháp

TÍNH NĂNG	
Xác thực	Quản lý định danh
	Xác thực local
	LDAP/OIDC
	Xác thực đa nhân tố
	Phân quyền RBAC
Dashboard	Quản lý Dashboard
	Dashboard Builtin
	Custom Dashboard
Event	Tìm kiếm Event
	Realtime Event
	Visualize Event Data
Alert	Tìm kiếm alert
	Xử lý alert
	Realtime alert
	Hỗ trợ OpenAPI
	Visualize alert data
Agent	Quản lý agent
	Agent hỗ trợ Windows/Linux
	Agent hỗ trợ lấy log File
	Agent hỗ trợ lấy log Windows Event
	Agent hỗ trợ AutoDiscovery
	Agent hỗ trợ FIM
	Agent hỗ trợ Policy Compliance
	Quản lý group/owner
Policy Compliance	TCVN 11930:2017
	Custom Policy
Correlation	Quản lý rule
Report	Reporting
User	Quản lý user
	Quản lý Business Unit
Logsource	Syslog
	Beats
	Beats/ssl
	Redis
	Kafka