Datasheet

Viettel Security Orchestration, Automation & Response (VCS-CyCir)

viettel security

Sự cần thiết của giải pháp

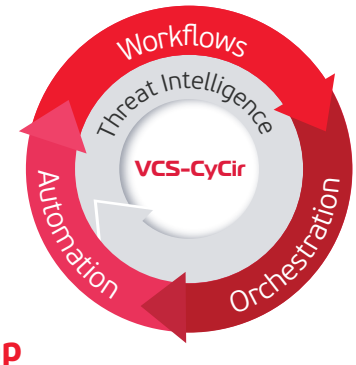
Trong bối cảnh công nghệ thông tin (CNTT) ngày càng phát triển, cuộc tấn công mạng đang trở nên ngày một đa dạng về quy mô và mục đích dẫn tới thiệt hại do sự cố an ninh mạng tăng đều qua các báo cáo hàng năm. Dẫn đến khối lượng công việc của đội ngũ chuyên trách về an toàn thông tin (ATTT) cho mỗi đơn vị cũng tăng theo tỷ lệ thuận gây ra tình trạng quá tải về nguồn lực, kéo theo sự giảm sút về chất lượng công việc. Bên cạnh đó, việc giám sát & phản ứng ATTT trên nhiều công cụ, giải pháp riêng lẻ cũng khiến cho tổ chức phải đối mặt với những thách thức khác như:

- Các giải pháp hoạt động độc lập, thiếu sự gắn kết dẫn tới quá nhiều cảnh báo trùng lặp cho cùng một đối tượng.
- Thiếu tầm nhìn xuyên suốt trong quá trình điều tra, phản ứng.
- Quá nhiều công đoạn xử lý thủ công, gây ảnh hưởng đến chất lượng công việc.
- Thiếu hụt nhân sự có kỹ năng để vận hành, làm chủ các công cụ ATTT.

Các thách thức trên dẫn đến nhu cầu tất yếu của các tổ chức để tìm kiếm 1 nền tảng giúp nâng cao hiệu quả của quá trình vận hành, phản ứng sự cố ATTT.

Giải pháp Viettel Security Orchestration Automation and Response (VCS-CyCir)

VCS-CyCir là giải pháp điều phối, tự động hóa phản ứng an ninh thông tin tập trung (SOAR - Security Orchestration, Automation and Response) giúp xác định, ưu tiên và tiêu chuẩn hóa cho các chức năng ứng phó sự cố. Được xây dựng dựa trên công nghệ tự động hóa thông qua việc tích hợp với các công nghệ bảo mật, CNTT theo các kịch bản xử lý (playbook) được định nghĩa động, VCS-CyCir giúp tổ chức đạt được mục tiêu tối ưu hóa hiệu quả trong quá trình quản lý và vận hành hệ thống ATTT.



Lợi ích của giải pháp

1. Tối đa hoá hiệu quả vận hành, giám sát và xử lý sự cố.
2. Tự động hoá và tiêu chuẩn hoá quy trình phản ứng.
3. Giảm tải vận hành, nâng cao hiệu suất làm việc.

Các tính năng của giải pháp

Điều phối các giải pháp ATTT

VCS-CyCir cho phép các công cụ bảo mật riêng biệt phối hợp chặt chẽ với nhau để nâng cao năng suất làm việc trong các quy trình bảo mật phức tạp. Bên cạnh việc hỗ trợ sẵn nhiều công cụ và kịch bản (playbook) phổ biến, VCS-CyCir cũng cung cấp khả năng tùy biến để tích hợp các công nghệ bảo mật và phát triển các playbook theo nhu cầu của tổ chức.

Tích hợp

VCS-CyCir cho phép kết nối và tương tác với các nền tảng khác nhau gồm các hệ thống: SIEM, Threat Intelligence Platform, Endpoint Security, Network Security, Malware Analysis, Ticketing System, IAM. Ngoài ra VCS-CyCir cũng cung cấp khả năng tích hợp theo hai chiều thông qua API.

Tự động tiếp nhận cảnh báo

VCS-CyCir cho phép tự động tiếp nhận các cảnh báo từ các hệ thống SIEM (ví dụ VCS-CyM, IBM Qradar SIEM, Splunk Enterprise Security), sau đó phân loại theo mức độ ưu tiên và tự động tạo các phiếu sự cố tương ứng.

Tự động hoá vận hành ATTT

Workflow engine được tích hợp trong VCS-CyCir nhằm cung cấp khả năng thực hiện tự động hóa chuỗi các hành động theo kịch bản định nghĩa chỉ trong vài giây, so với hàng giờ khi thực hiện thủ công. Điều này giúp giảm công sức thực hiện các công việc lặp đi lặp lại để nâng cao hiệu năng công tác phản ứng sự cố. Engine này cũng cho phép người dùng theo dõi và can thiệp vào luồng xử lý tự động khi cần thiết. Bên cạnh đó, VCS-CyCir cũng cung cấp giao diện trực quan giúp người dùng xây dựng các playbook, sử dụng giao diện hỗ trợ sẵn có hoặc định nghĩa playbook mới bằng ngôn ngữ Python.

Quản lý sự cố và phối hợp vận hành

VCS-CyCir lưu vết tất cả thông tin trong quá trình điều tra, phản ứng & tổng hợp, chủ động cung cấp thông tin liên quan về sự cố đến chuyên gia phân tích trên một giao diện quản trị tập trung duy nhất, giúp chuyên gia có được góc nhìn toàn diện về sự cố, rút ngắn thời gian phân tích, ra quyết định để phản ứng hiệu quả với sự cố. Thông tin quản lý bao gồm:

- **Phối hợp vận hành:** Cung cấp công cụ trao đổi thông tin giữa các bộ phận (Tier), đơn vị, nhóm. Các thành viên trong nhóm có thể dễ dàng tương tác về các vấn đề cụ thể trong từng trường hợp để nhanh chóng đưa ra các quyết định hoặc phân công công việc đến người phù hợp. VCS-CyCir cho phép thực hiện hoạt động điều phối xử lý cảnh báo, điều phối xử lý tình huống trong đội ngũ vận hành giám sát ATTT với các tác vụ được hỗ trợ gồm tạo mới, tìm kiếm, lưu trữ và phân loại, xử lý và cập nhật kết quả xử lý, trạng thái xử lý, gán và theo dõi SLA xử lý.
- **Quản lý thông tin tình báo nguy cơ ATTT:** Với việc tích hợp với các nền tảng tình báo an ninh thông tin, VCS-CyCir quản lý và cung cấp các thông tin tình báo nguy cơ liên quan đến sự cố theo cách chủ động, trực quan nhất cho chuyên gia phân tích, giúp tối ưu hóa quá trình phân tích và xử lý sự cố.
- **Hỗ trợ công tác điều tra, truy vết nhanh, chính xác:** VCS-CyCir cung cấp cho người dùng bộ công cụ tối ưu, thuận tiện nhất phục vụ cho quá trình điều tra, truy vết tấn công mạng. Hỗ trợ thu thập & quản lý hiện vật (artifact), bằng chứng (evidence) liên quan đến sự cố xảy ra. VCS-CyCir cho phép thực hiện lưu trữ lịch sử hành động & ghi chú xử lý sự cố, cũng như thêm bằng chứng thu thập được trong quá trình điều tra.

Dashboard và báo cáo ATTT

VCS-CyCir hỗ trợ các công cụ trích xuất ra các báo cáo và dashboard chuyên biệt cho cả 3 lớp người dùng của tổ chức: Chuyên gia phân tích, SOC Manager và Giám đốc An ninh thông tin (CISO). Tất cả các sự kiện, hành động được lưu trữ giúp cho tổ chức đo lường được hiệu quả của đội ngũ vận hành SOC theo nhiều góc nhìn khác nhau.

Hiệu năng vượt trội

- VCS-CyCir đảm bảo độ trễ thời gian tìm kiếm log, cảnh báo & tình huống với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa 1 phút.
- VCS-CyCir cho phép thu thập, xử lý và lưu trữ dữ liệu đồng thời 100 cảnh báo trong khoảng thời gian là 1 phút.

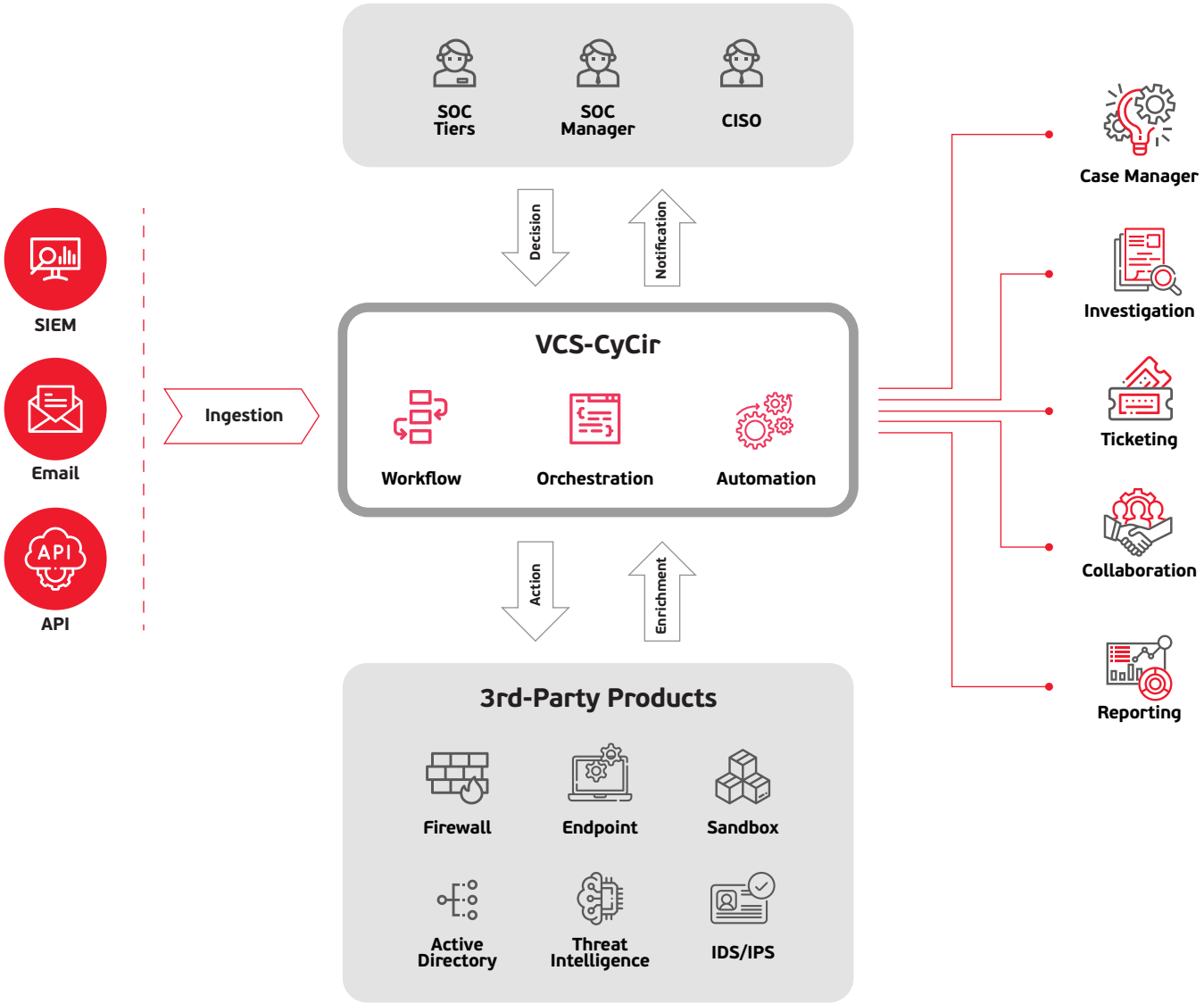
Giám sát và phân tích sự cố ATTT trực quan

VCS-CyCir cho phép xem dòng thời gian sự kiện của sự cố & cung cấp thông tin trực quan về mối liên kết giữa đối tượng liên quan trong sự cố.

Viettel Security Orchestration, Automation & Response (VCS-CyCir)

viettel security

MÔ HÌNH TRIỂN KHAI VÀ VẬN HÀNH VCS-CYCIR



- **Tầng Data Source:** Bao gồm các giải pháp, các API đóng vai trò cung cấp các cảnh báo đầu vào cho hệ thống VCS-CyCir.
- **3rd Party Products:** Là các công nghệ, giải pháp ATTT được tích hợp với VCS-CyCir, hỗ trợ làm giàu dữ liệu trong quá trình điều tra, phân tích. Đồng thời đưa ra hành động cụ thể cho các giải pháp ATTT khác trong hệ thống để thực hiện ứng phó khi có sự cố ATTT.
- **VCS-CyCir Core Engine:**
  - Workflow: Định nghĩa và tự động hóa các quy trình vận hành ATTT.
  - Orchestration: Tích hợp, điều phối các công nghệ bảo mật làm việc với nhau.
  - Automation: Tự động hóa các tác vụ thủ công trong quá trình vận hành ATTT.