CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC – CMC CYBER SECURITY LTD.

Tầng 15 tòa nhà CMC, phố Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

15th Floor, CMC Tower, Duy Tan Street, Dich Vong Hau Ward, Cau Giay District, Hanoi | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

DATASHEET GIẢI PHÁP PHÁT HIỆN VÀ PHẢN ỨNG SỰ CỐ ANTT CHO ĐẦU CUỐI

(ENDPOINT DETECTION & RESPONSE – EDR)

Thành viên chính thức của AVAR và ICSA

Hà Nội, 03/07/2020

CMC CYBER SECURITY
Aspire to Inspire the Digital World

CÔNG TY TNHH AN NINH AN TOÀN CMC CYBER SECURITY

Version	3.0
Date	03/07/2020
Document Type	Datasheet
Prepared By	Luu Duc Hien

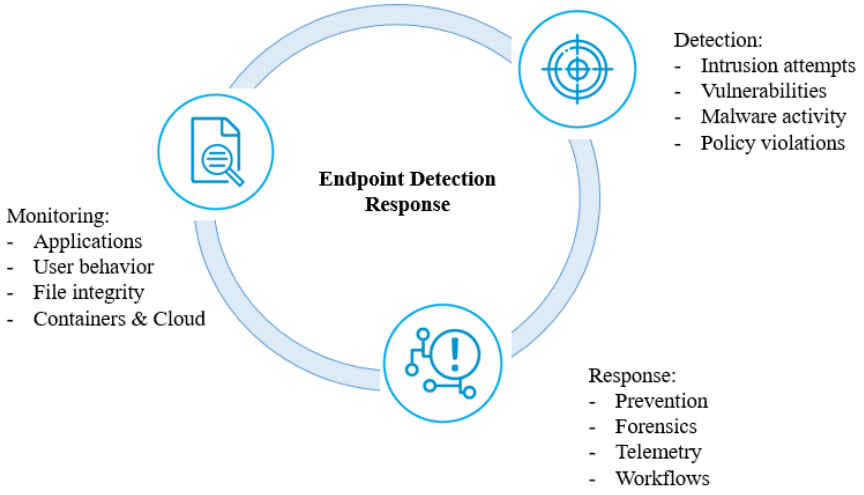
CMC CYBER SECURITY
Aspire to Inspire the Digital World

Contents

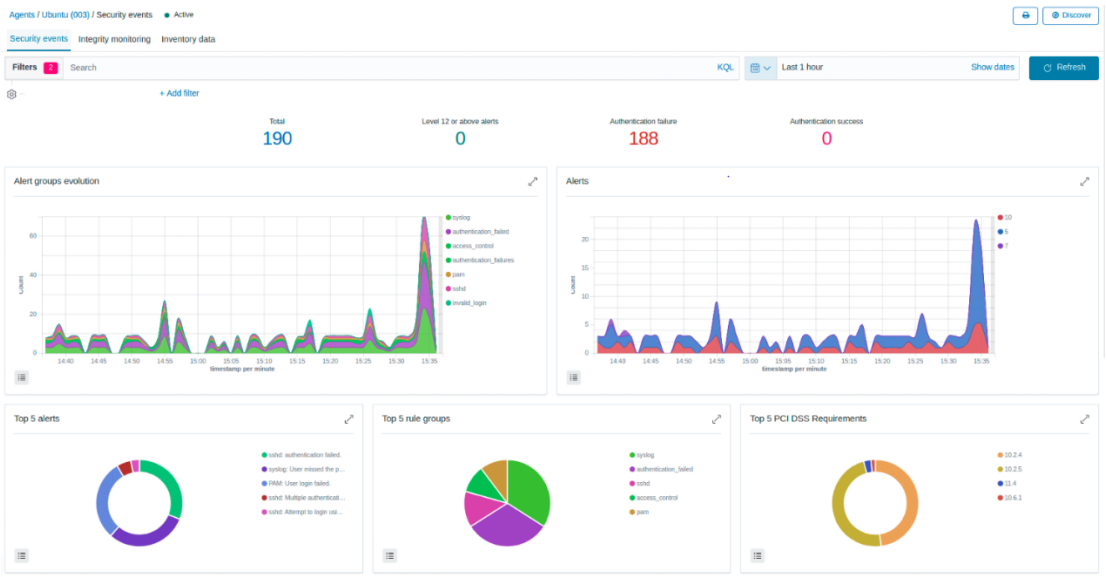
1. Giới thiệu CMC EDR

a. Mô tả

CMC EDR là một giải pháp phòng ngừa mối đe dọa kết hợp các sức mạnh của trí tuệ nhân tạo (AI) để ngăn chặn sự lây nhiễm phần mềm độc hại với additional security controls kiểm soát các biện pháp bảo vệ chống lại các cuộc tấn công dựa trên script-based, fileless, memory, và external device-based attacks.



Không giống như các sản phẩm endpoint security truyền thống dựa trên signatures và behavior analysis để phát hiện các mối đe dọa trong hạ tầng mạng. Các đặc điểm nổi bật của CMC EDR:



- Sử dụng AI, không phải signature, để xác định và ngăn chặn phần mềm độc hại đã biết và chưa biết hoạt động trên các endpoint.
- Cung cấp phòng ngừa chống lại các mối đe dọa phổ biến và không xác định (zero-day) mà không cần một kết nối internet.
- Liên tục bảo vệ endpoint mà không làm gián đoạn hoạt động của end-user.
- Phát hiện và ngăn chặn sớm các hành vi thực hiện tấn công APT.
- Không giới hạn số lượng hoặc tốc độ dữ liệu được lưu trữ hoặc xử lý
- Kiểm tra, phát hiện các hành vi vi phạm chính sách, quy định.
- Có khả năng kết nối và chia sẻ dữ liệu với Hệ thống Giám sát an toàn không gian mạng Quốc gia

Nhờ minimal system impact và phòng chống Zero-day, CMC EDR bảo vệ các endpoint và tổ chức khỏi compromise bởi kẻ tấn công.

b. Chức năng

CMC EDR cung cấp các chức năng sau:

- *Phân tích các sự kiện bảo mật:*
    - EDR được sử dụng để thu thập, tổng hợp, lập chỉ mục và phân tích các dữ liệu bảo mật, giúp các tổ chức phát hiện sự xâm nhập, các mối đe dọa và sự bất thường về hành vi phía Endpoint.
    - Khi các mối đe dọa trên mạng đang trở nên tinh vi hơn, việc theo dõi và phân tích các sự kiện theo thời gian thực là cần thiết để phát hiện và khắc phục các mối đe dọa nhanh chóng.
- *Phát hiện xâm nhập:*
    - Agent EDR quét các endpoint được giám sát để tìm các phần mền độc hại, rootkit, và các sự kiện bất thường. CMC EDR có khả năng phát hiện các tệp tin ẩn, các tiến trình chạy ẩn hoặc các Registry chưa được đăng ký, các hoạt động khai thác, privilege escalation …
    - Ngoài các khả năng detect từ các Agent, thành phần máy chủ sử dụng các signature để phát hiện sự xâm nhập, sử dụng AI để phân tích các dữ liệu nhật ký thu được và tìm kiếm các IOC.
- *Phân tích dữ liệu nhật ký:*

- Đội ngũ nhân sự CMC SOC sẽ thực hiện phân tích các sự kiện dựa vào các thông tin đã thu thập từ phía Endpoint và gửi về Trung tâm SOC theo đường truyền VPN đã được mã hóa.
- Các thông tin được gửi về hệ thống bao gồm: lỗi ứng dụng hoặc hệ thống, cấu hình sai, các hoạt động độc hại đang cố gắng thực thi hoặc đã thành công, hành vi vi phạm chính sách và một loạt các vấn đề bảo mật khác, …

- *Giám sát toàn vẹn tập tin:*
  - EDR giám sát hệ thống tệp, xác định các thay đổi về nội dung, quyền, quyền sở hữu và thuộc tính của các tệp tin cần phải giám sát. Ngoài ra Agent còn xác định người dùng và ứng dụng được sử dụng để tạo hoặc sửa đổi các tệp tin.
  - Khả năng giám sát toàn vẹn tệp tin được sử dụng kết hợp với AI để xác định các mối đe dọa hoặc máy chủ bị xâm nhập. Ngoài ra, CMC EDR còn giám sát việc tuân thủ một số tiêu chuẩn theo chuẩn PCI/ DSS.
  - Kích hoạt cảnh báo khi các tệp này được sửa đổi. Thành phần này lưu trữ cryptographic checksum và các thuộc tính tốt của tệp hoặc Windows registry key đã biết và thường xuyên so sánh nó với tệp hiện tại đang được hệ thống sử dụng, theo dõi các thay đổi.
- *Phát hiện các lỗ hổng:*
  - Agent EDR lấy dữ liệu và kiểm kê các thông tin liên quan về các ứng dụng/ phần mềm và gửi thông tin này đến máy chủ được tích hợp hệ thống Threat Intelligence thực hiện thu thập, cập nhật liên tục các CVE, mối đe dọa có thể ảnh hưởng tới hệ thống, …
  - Đánh giá lỗ hổng tự động sẽ giúp quản trị hệ thống tìm ra những điểm yếu trong các tài sản quan trọng của mình và có biện pháp khắc phục trước khi kẻ tấn công khai thác chúng để thực hiện phá hoại hệ thống hoặc đánh cắp các dữ liệu nhạy cảm.
- *Thực hiện đánh giá Audit:*
  - EDR giám sát các cài đặt cấu hình hệ thống và ứng dụng để đảm bảo các tuân thủ chính sách bảo mật, tiêu chuẩn và các chính sách của tổ chức. Agent sẽ thực hiện quét định kỳ để phát hiện các ứng dụng được biết có dễ bị khai thác, chưa được vá hoặc được cấu hình không an toàn.

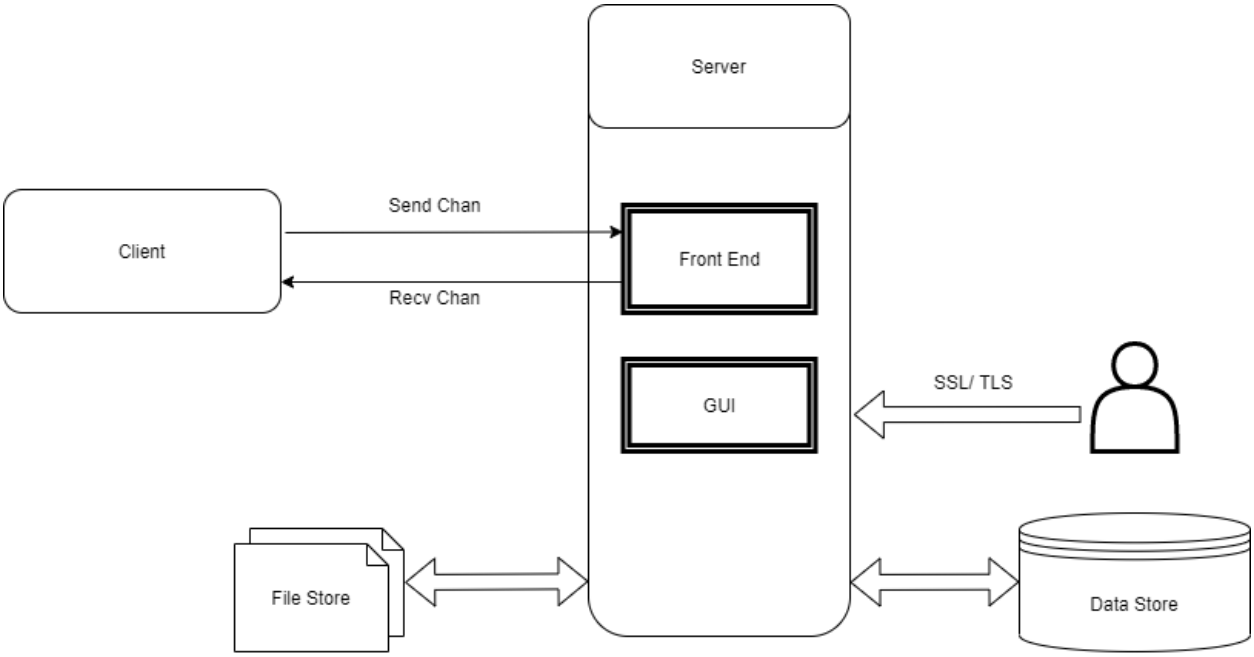
- Ngoài ra, việc kiểm tra các cấu hình có thể được điều chỉnh, tùy chỉnh để phù hợp với từng hệ thống của các tổ chức khác nhau. Cảnh báo sẽ bao gồm các khuyến nghị thực hiện cấu hình, tham chiếu và ánh xạ tới các quy định của tổ chức.

- *Điều tra, xử lý sự cố:*
  - EDR cung cấp các kịch bản phản ứng sẵn có, thực hiện các cách thức đối phó để giải quyết các mối đe dọa.
  - Hỗ trợ thực hiện các phản ứng đối với các sự cố an toàn thông tin tại máy trạm (như cô lập máy trạm, xóa file, xóa/cô lập tiến trình, xóa giá trị trong registry, chặn các kết nối mạng…)
  - Ngoài ra, EDR có thể được sử dụng để chạy các lệnh hoặc các truy vấn từ xa, xác định các chỉ số thỏa hiệp (IOC) và giúp thực hiện các nhiệm vụ điều tra số hoặc phản ứng sự cố trực tiếp khác.
- *Kiểm tra, giám sát tuân thủ chính sách:*
  - CMC EDR cung cấp một số biện pháp kiểm soát bảo mật cần thiết để tuân thủ các tiêu chuẩn và quy định của tổ chức. Các tính năng này, kết hợp với khả năng mở rộng và hỗ trợ đa nền tảng giúp các tổ chức đáp ứng các yêu cầu tuân thủ kỹ thuật.
- *Quản lí cấu hình tập trung với khả năng tích hợp với giải pháp của các bên thứ 3:*
  - Khả năng tích hợp với các giải pháp như Ansible, Puppet...
- *Threat intelligence:*
  - Threat Intelligene như 01 virtual appliance được quản trị/tích hợp vào EDR server, làm nhiệm vụ lưu trữ và cập nhật tất cả các thông tin về Advanced Malware/tấn công APT đã được định danh bởi hệ thống phân tích tấn công APT của CMC.
  - CMC Threat Intelligence được cập nhật real-time về thông tin các mối đe dọa, hành vi mã độc, hình thức tấn công, cách thức khai thác lỗ hổng zero-day... từ CMC và thực hiện chia sẻ real-time các thông tin này xuống các end point cài Agent. Hệ thống CMC Threat Intelligence liên tục thu thập và cập nhật dữ liệu từ nhiều nguồn khác nhau, đảm bảo phản ứng nhanh nhất với các mối đe dọa khi một nguồn nào đó đã có thông tin.

- *Cung cấp giao diện quản trị tập trung:* trên nền tảng Website hỗ trợ thống kê tìm kiếm các thông tin về máy trạm (như thông tin về file hash tiến trình, registry, kết nối mạng).

2. Cơ chế hoạt động

a. Cơ chế hoạt động



Các Agent EDR được cài tại các máy khách được kết nối tới máy chủ quản trị (Windows, Linux...). Quản trị viên có thể sử dụng trình duyệt để kết nối với giao diện quản trị Web Portal các kết nối sẽ được mã hóa SSL/TLS (đây cũng là giao thức mã hóa dùng trong chuyển log). Người dùng có thể thực hiện các truy vấn tới các Endpoint từ giao diện quản trị để thực hiện thu thập các thông tin hỗ trợ quá trình điều tra phân tích hoặc thực hiện theo dõi các sự kiện an toàn thông tin.

Cách thức thu thập log:

- Đối với các Hệ điều hành mà CMC EDR hỗ trợ, CMC SOC sẽ cung cấp agent tương thích để cài đặt trên các thiết bị tương ứng.
- Đối với các Hệ điều hành, các ứng dụng không có trong danh sách CMC EDR hỗ trợ, CMC SOC sẽ thực hiện việc viết các logs decoder tương ứng.

Cách thức cài đặt, tích hợp:

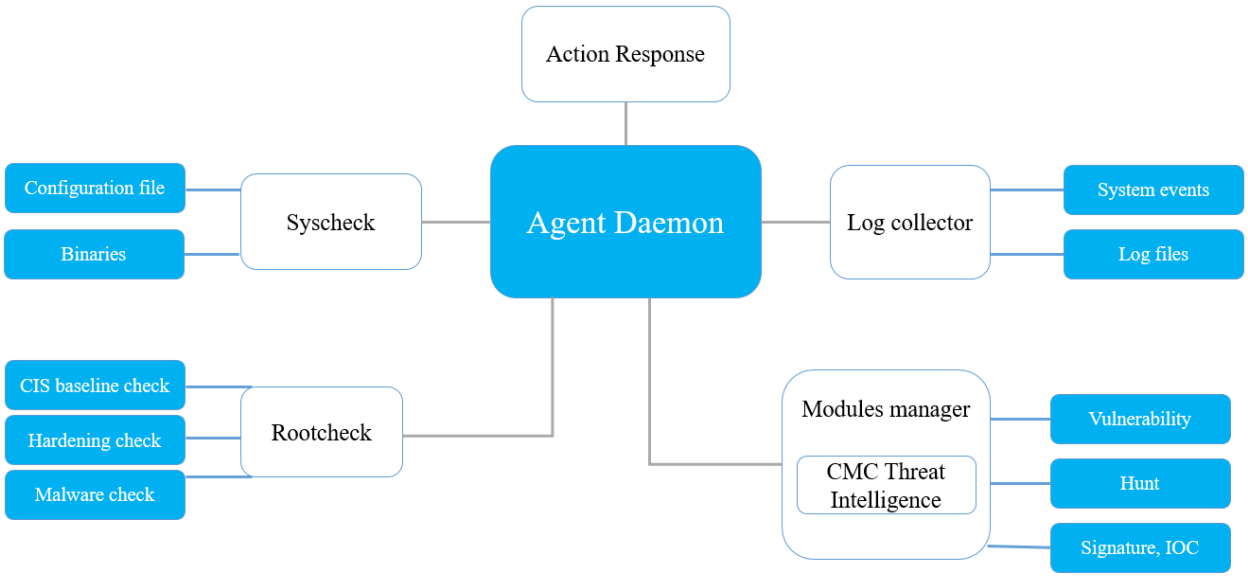
- Khi triển khai hệ thống, CMC sẽ thực hiện cài đặt tích hợp với hệ thống bảo mật máy trạm của khách hàng

- Để hỗ trợ đẩy log về hệ thống quản lý lưu log tập trung, CMC sẽ thực hiện tích hợp với hệ thống SIEM của khách hàng.

b. EDR Agent

EDR Agent tương thích chạy trên các hệ điều hành như: Windows, Linux, Solaris, … Nó được sử dụng để thu thập các loại thông tin liên quan tới dữ liệu ứng dụng và hệ thống khác nhau được tùy chỉnh dựa vào nhu cầu từ EDR Server, dữ liệu sau đó được chuyển tiếp đến máy chủ quản trị tập trung thông qua một kênh truyền được mã hóa và xác thực. Để thiết lập kênh bảo mật này, mỗi Agent sẽ được gán một khóa sử dụng duy nhất.

Các Agent có thể được sử dụng để giám sát các máy chủ vật lý, máy ảo, cloud, thiết bị mạng, … phục vụ việc phát hiện các thiết bị ngoại vi được kết nối vào hệ thống (USB, Ổ cứng rời...). Các gói cài đặt Agent có sẵn trên các nền tảng Windows, Unix, Linux, …Các tác vụ/ tiến trình khác nhau được sử dụng để giám sát hệ thống ví dụ: giám sát tính toàn vẹn của tệp, đọc thông tin nhật ký hệ thống, …



Mô tả:

- Rootcheck:
  - Quá trình này sẽ thực hiện nhiều tác vụ liên quan đến việc phát hiện rootkit, phần mềm độc hại và sự bất thường của hệ thống (ví dụ như thay đổi Public IP trên máy tính....)

  - Agent cũng sẽ thực hiện một số kiểm tra bảo mật cơ bản đối với các tệp cấu hình hệ thống.
- Log collector:
  - Thành phần này được sử dụng để đọc các thông tin nhật ký ứng dụng và hệ điều hành bao gồm: log access, log activity, log security, …
  - Việc thu thập các Log có thể được cấu hình cụ thể tùy thuộc nhu cầu thu thập theo dõi cho từng hệ thống cụ thể.
  - Các log sẽ được lọc, chuẩn hóa, tinh chỉnh và parsing theo thời gian thực
  - Pattern- matching and correlation
  - Phân loại log theo nhóm – classification
  - Triển khai với mô hình phân tán – distributed
  - Gán nhãn cho log -Message tagging
  - Sử dụng giao thức truyền log chuẩn ALTP - Advanced Log Transport Protocol, RLTP - Reliable Log Transfer Protocol.
- Syscheck:
  - Quá trình này thực hiện giám sát toàn vẹn tệp tin (FIM) và cũng có thể giám sát các Registry keys được tạo trên hệ thống.
  - Có khả năng phát hiện các thay đổi trong một tệp tin, thư mục, nội dung, quyền sở hữu, … cũng như việc tạo và xóa các tệp tin.
  - Việc thực hiện quét FIM theo đinh kỳ cũng có thể được cấu hình để có thể đưa ra cảnh báo real-time.
  - Chống giả mạo, mã hóa hệ thống lưu trữ.
- CMC Threat Intelligence:
  - Module này sử dụng cơ sở dữ liệu về các mối đe dọa CMC Threat Intelligence bao gồm các: vulnerability, signature, IOC, …
  - Làm giàu dữ liệu với việc so sánh với dữ liệu từ cơ sở dữ liệu bên ngoài
  - Bằng cách quét định kỳ hệ thống, EDR có thể tìm thấy các ứng dụng hoặc cấu hình dễ bị tổn thương không tuân theo tiêu chuẩn.
- Action Response:
  - Các Agent EDR sẽ nhận lệnh từ phía Server để thực hiện các hành động thực thi phía Endpoint.
  - Quét, Thu thập thông tin được từ các Endpoint bao gồm các tiến trình, kết nối, thông tin hệ thống, …

  - Thực hiện xử lý theo lệnh (Block/Allow) theo kết quả từ EDR server khi ghi nhận được các sự cố về an ninh thông tin. Thực hiện sửa chữa (remediate) cho máy trạm trong trường hợp máy trạm đã bị tấn công từ trước đó.

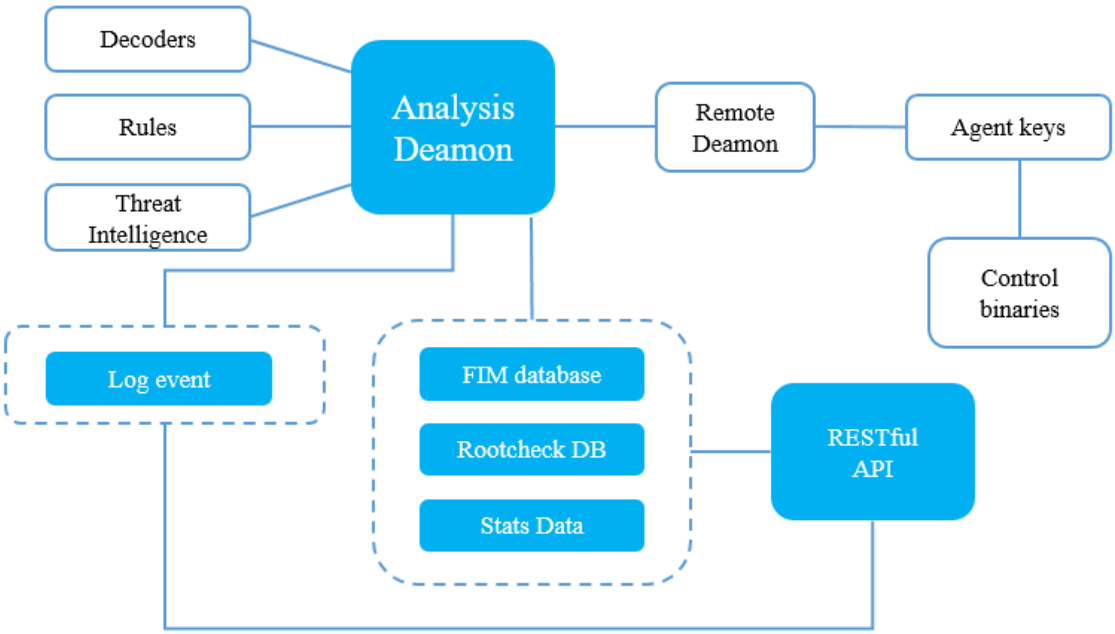
- Agent Deamon:
  - Đây là quá trình nhận dữ liệu được tạo hoặc thu thập bởi các Agent được cài trên các Endpoint. Dữ liệu được nén, mã hóa và gửi đến máy chủ thông qua một kênh xác thực.

c. EDR Server

Thành phần máy chủ EDR chịu trách nhiệm phân tích dữ liệu nhận được từ các Agent và đưa ra các cảnh báo đối với những sự kiện thu thập được. Ví dụ: phát hiện xâm nhập, thay đổi tệp, cấu hình không tuân thủ chính sách, rootkit có thể, …

Server EDR sẽ cung cấp một giao diện Portal cho phép:

- Thu thập thông tin từ các Agent hoặc lệnh khởi động lại Agent
- Tìm kiếm, xuất các dữ liệu phục vụ quá trình điều tra phân tích
- Thêm/ sửa/ xóa các quy tác giám sát, thu thập ở các Agent
- Truy cập từ xa vào các Endpoint được cài Agent để tải các tệp, xem các Registry, …



Máy chủ EDR thường được triển khai trên một máy chủ vật lý độc lập hoặc máy ảo bao gồm các modules chính như sau:

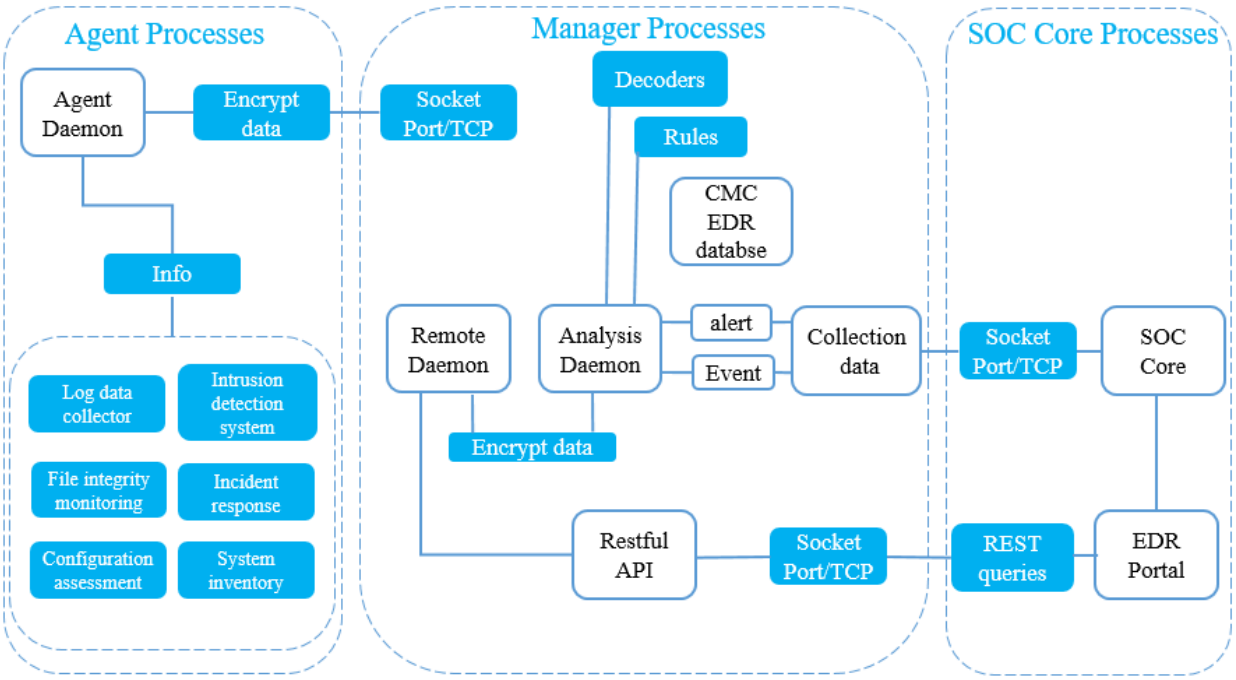
- Registration service:
  - Sử dụng để đăng ký các agent mới bằng cách cung cấp và phân phối các khóa xác thực (mỗi agent sẽ có một khóa duy nhất).
- Remote Deamon service:
  - Thực hiện nhận và gửi dữ liệu từ các Agent. Các dữ liệu được gửi và nhận sử dụng các khóa đã được xác thực danh tính từ trước.

- EDR server cũng có thể gửi cách lệnh tới Agent để thực hiện các hành động xử lý khi gặp phải các mối đe dọa an toàn thông tin trên các Endpoint.

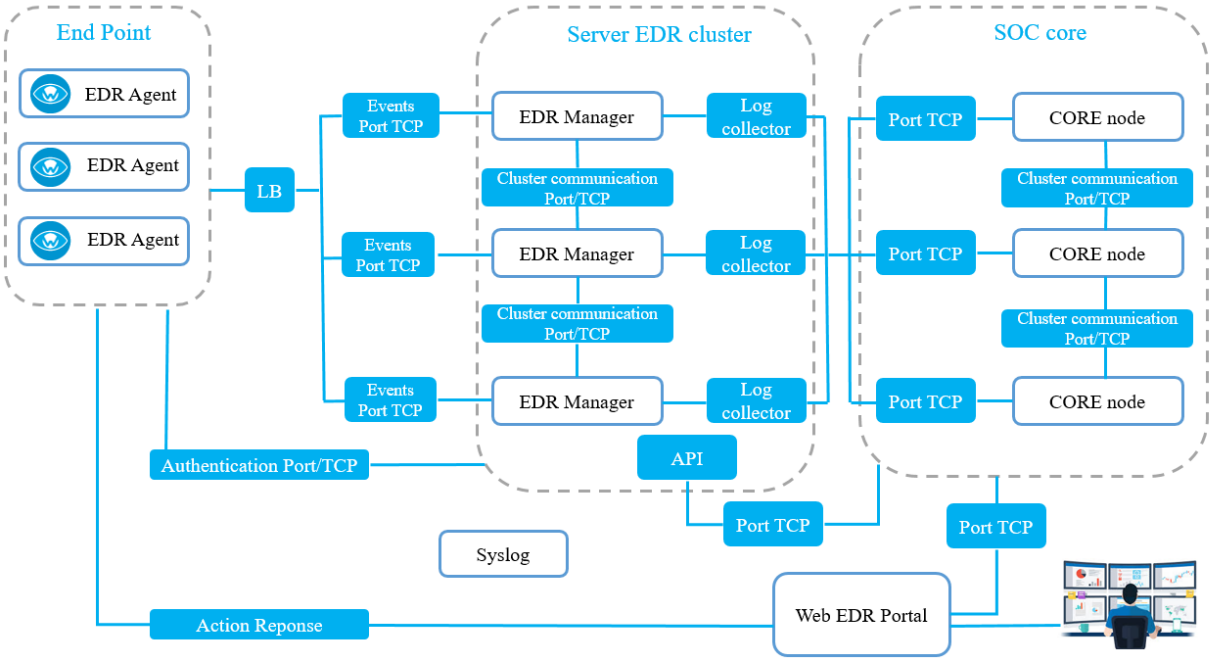
- Analysis Deamon:
  - Là quá trình thực hiện phân tích dữ liệu. Sử dụng các bộ Decoders để xác định loại thông tin đang được xử lý (ví dụ: các event log, các nhật ký trên máy chủ, …) và sau đó sẽ thực hiện trích xuất các dữ liệu có liên quan tới sự kiện như: IP nguồn, ID event, User, …
  - Bằng cách sử dụng các quy tắc, các gói dữ liệu về các mối đe dọa, kết hợp với việc phân tích nhờ các thuật toán AI để xác định đưa ra cảnh báo và các khuyến nghị đối phí đối với mối nguy cơ được phát hiện.
- RESTful API:
  - Cung cấp giao diện để thực hiện quản lý và giám sát cấu hình và trạng thái của Agent.

d. Kiến trúc EDR

Kiến trúc CMC EDR thiết kế dựa trên các Agent chạy trên các Endpoint được giám sát để chuyển tiếp dữ liệu nhật ký đến một máy chủ quản trị tập trung. Ngoài ra, đối với các thiết bị không thể thực hiện cài Agent (như: Firewall, switch, router, access point, …) sẽ được CMC SOC hỗ trợ và có thể chủ động gửi dữ liệu nhật ký qua syslog, đảm bảo Zero Message Loss Transfer. Máy chủ EDR sẽ thực hiện giải mã và phân tích các thông tin nhận được từ các Agent và có thể đưa ra các hành động đẩy xuống các Agent khi cần thiết.



3. Sơ đồ triển khai



EDR Agent:

- Phầm mềm EDR Agent sẽ được cài đặt trên các endpoint trong hệ thống sử dụng giải pháp EDR, Agent sẽ có chức năng thu thập thông tin như log, tiến trình, thông tin các file, mã hash, …để phục vụ công việc phân tích và thực hiện các hành động ngăn chặn/ sửa chữa nếu phát hiện ra các hành vi tấn công trên các endpoint.
- Agent bao gồm các thành phần:
  - Phần mềm EDR Agent
  - Các sản phẩm bao gồm các thông tin về mối đe dọa (Threat Intelligence Exchange), phương thức trao đổi dữ liệu với server (Data Exchange Layer) để nhận/cập nhật thông tin bản vá, các gói dữ liệu Threat Intelligence từ EDR server; và chuyển các thông tin bao gồm các tiến trình, kết nối, kết quả dò quét… từ Agent tới EDR server
- Nhiệm vụ Agent:
  - Quét, Thu thập thông tin được từ các Endpoint bao gồm các tiến trình, kết nối, thông tin hệ thống, … sẽ được gửi về EDR Server quản trị tập trung (bao gồm 2 thành phần Threat Intelligence Exchange và Active Response).
  - Sử dụng giao thức mã hóa SSL/TLS khi chuyển log
  - Thực hiện xử lý theo lệnh (Block/Allow) theo kết quả từ EDR server khi ghi nhận được các sự cố về an ninh thông tin. Thực hiện sửa chữa

(remediate) cho máy trạm trong trường hợp máy trạm đã bị tấn công từ trước đó.

EDR Server:

- EDR server có chức năng quản trị, lưu trữ các thông tin về hoạt động tấn công của mã độc, hành vi tấn công, các hành vi APT đã biết, …
- Các thông tin về các mối đe dọa mới được thu thập và phân tích trên CMC Threat Intelligence cũng sẽ được cập nhật định kì tới các EDR server. Từ EDR server sẽ thực hiện đẩy các thông tin, bản cập nhật, xử lý, … đảm bảo khả năng định danh, phát hiện và ngăn chặn kịp thời các hành vi tấn công (Ví dụ như việc ngăn chặn các địa chỉ IP đang thực hiện tấn công, các địa chỉ IP tấn công với tần suất bất thường...).
- CMC EDR cung cấp giao diện trên nền tảng Website (web-based) cung cấp cho người quản trị thực hiện các thao tác vận hành liên quan đến Threat Intelligence Exchange và Active Response trên giao diện trực quan duy nhất về các thông tin trong hệ thống, các vấn đề hệ thống gặp phải…

-

4. Khả năng tương thích

CMC EDR có khả năng tương thích với các môi trường hệ điều hành như:

Microsoft Windows (32-bit or 64-bit)	Linux	Mac OS
• Windows XP SP3 • Windows Vista • Windows 7 • Windows 8 and 8.1 • Windows 10 • Windows Server 2003 SP2 • Windows Server 2008 / 2008 R2 • Windows Server 2012 / 2012 R2 • Windows Server 2016	• Red Hat Enterprise Linux / CentOS 6.6 — 32-bit and 64-bit • Red Hat Enterprise Linux / CentOS 6.7 — 32-bit and 64-bit • Red Hat Enterprise Linux / CentOS 6.8 — 32-bit and 64-bit • Red Hat Enterprise Linux / CentOS 7.0 — 64-bit • Red Hat Enterprise Linux / CentOS 7.1 — 64-bit • Red Hat Enterprise Linux / CentOS 7.2 — 64-bit • Red Hat Enterprise Linux / CentOS 7.3 — 64-bit	• Mac OS X 10.9 (Mavericks)* • Mac OS X 10.10 (Yosemite)* • Mac OS X 10.11 (El Capitan)* • Mac OS X 10.12 (Sierra)* *Complements Apple's built-in XProtect
• 2GB Memory • 500MB Available Disk Space • Microsoft .NET Framework 3.5 SP1 • Internet browser • Internet connection to register	• 2GB Memory • 500MB Available Disk Space • Internet browser • Internet connection to register product • Local admin rights to install	• 2GB Memory • 500MB Available Disk Space • Internet browser • Internet connection to

product • Local admin rights to install software	software	register product • Local admin rights to install software

Cách thức thu thập log:

- Đối với các Hệ điều hành mà CMC EDR hỗ trợ, CMC SOC sẽ cung cấp agent tương thích để cài đặt trên các thiết bị tương ứng.
- Đối với các Hệ điều hành, các ứng dụng không có trong danh sách CMC EDR hỗ trợ, CMC SOC sẽ thực hiện việc viết các logs decoder tương ứng.

Cách thức cài đặt, tích hợp:

- Khi triển khai hệ thống, CMC sẽ thực hiện cài đặt tích hợp với hệ thống bảo mật máy trạm của khách hàng
- Để hỗ trợ đẩy log về hệ thống quản lý lưu log tập trung, CMC sẽ thực hiện tích hợp với hệ thống SIEM của khách hàng,