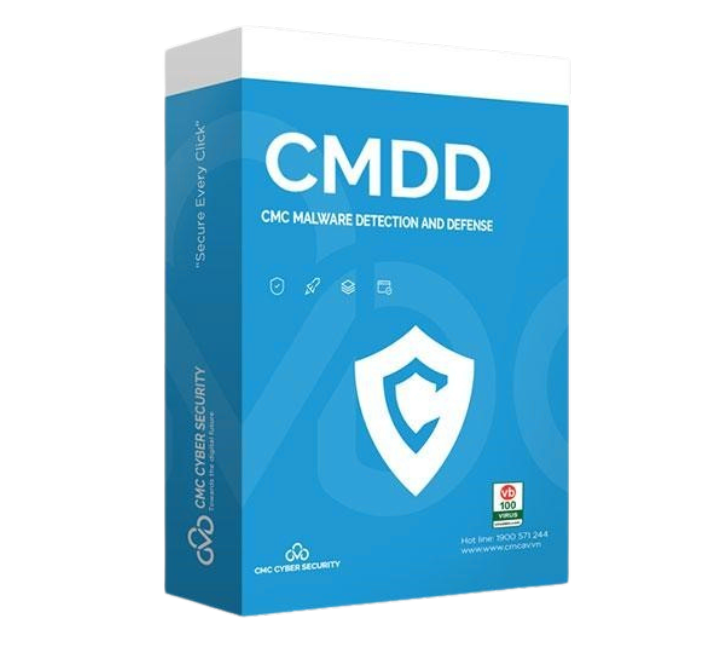
Giới thiệu sản phẩm

CMC Malware Detection & Defense



# Nội dung

[Nội dung 2](#_Toc196728427)

[I, Đặc tính kĩ thuật 3](#_Toc196728428)

[II, Thông tin chi tiết 4](#_Toc196728429)

[1, Tổng quan giải pháp 4](#_Toc196728430)

[2, Các mô hình triển khai sản phẩm 5](#_Toc196728431)

[3, Chức năng chi tiết 7](#_Toc196728432)

[3.1. Phát hiện và ngăn chặn các loại mã độc 7](#_Toc196728433)

[3.2. Khả năng tự động cập nhật mẫu & phiên bản phần mềm 8](#_Toc196728434)

[3.3. Quản trị tập trung 9](#_Toc196728435)

[3.4. Báo cáo thống kê 11](#_Toc196728436)

[3.5. Hỗ trợ đa ngôn ngữ 12](#_Toc196728437)

[4, Yêu cầu triển khai 13](#_Toc196728438)

[5, Khả năng mở rộng & tích hợp 15](#_Toc196728439)

[5.1. Tích hợp triển khai cài đặt qua giải pháp AD (Active Directory) 15](#_Toc196728440)

[5.2. Tích hợp đẩy dữ liệu về hệ thống SIEM 15](#_Toc196728441)

[5.3. Tích hợp chia sẻ thông tin theo tiêu chuẩn quốc gia 15](#_Toc196728442)

[6, Bảo trì & hỗ trợ kĩ thuật 16](#_Toc196728443)

[7, Phụ lục 17](#_Toc196728444)

I, Đặc tính kĩ thuật

Giải pháp phần mềm: CMC Malware Detection & Defense (CMDD)

Nhà cung cấp: CMC Cyber Security

Thương hiệu: CMC Cyber Security

Địa chỉ: CMC Tower, 11 P. Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội

Lĩnh vực: Phần mềm an toàn thông tin

Năm phát triển: 2025

Đặc tính kĩ thuật

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hạng mục** | **Thông số kĩ thuật** | **Ghi chú** |
| Khả năng bảo vệ | | | |
| 1 | Khả năng nhận diện các loại mã độc | Virus, Worm, Trojan, Spyware, Ransomware, Rootkit, Keylogger, Fileless malware, v.v. | Chi tiết tham khảo Phần II, Mục 3.1 |
| 2 | Phương pháp nhận diện mã độc | * Chữ kí (Signature base) * Phân tích hành vi (Behavior base) * AI Ranking | Chi tiết tham khảo Phần II, Mục 3.1 |
| 3 | Cập nhật mẫu nhận diện | Tự động định kì | Chi tiết tham khảo Phần II, Mục 3.2 |
| 4 | Tần suất cập nhật mẫu | Định kì 15 phút | Chi tiết tham khảo Phần II, Mục 3.2 |
| 5 | Bảo vệ thời gian thực | Có | Chi tiết tham khảo Phần II, Mục 3.1 |
| 6 | Tỷ lệ phát hiện mã độc | 99.89% | theo VB100 Test Report |
| Khả năng quản trị | | | |
| 7 | Quản trị tập trung | Có - cho phép quản trị tập trung danh sách máy đã cài Agent | Chi tiết tham khảo Phần II, Mục 3.3 |
| 8 | Điều khiển từ xa | Có - Cho phép cấu hình chính sách truy cập website, thực hiện quét mã độc từ xa | Chi tiết tham khảo Phần II, Mục 3.3 |
| 9 | Quản lý nhóm máy | Có - Cho phép tạo và phân nhóm danh sách máy | Chi tiết tham khảo Phần II, Mục 3.3 |
| 10 | Báo cáo thống kê | Có - Dashboard thống kê dữ liệu định kì và xuất file PDF/Excel | Chi tiết tham khảo Phần II, Mục 3.4 |
| Khả năng tương thích & hiệu năng | | | |
| 11 | Hệ điều hành hỗ trợ | Windows 7/8/10/11, Windows Server 2012–2022, Linux (tùy phiên bản) | Chi tiết tham khảo Phần II, Mục 4 |
| 12 | Hỗ trợ đa ngôn ngữ | Tiếng Việt, Tiếng Anh | Chi tiết tham khảo Phần II, Mục 3.5 |
| 13 | Dung lượng cài đặt | <100MB |  |
| 14 | Tài nguyên trung bình | CPU <20%, RAM < 200MB |  |
| 15 | Tương tích phần mềm khác | Không xung đột với các phần mềm office, kế toán, HRM,... |  |
| 16 | Hỗ trợ kĩ thuật | 24/7/365 | Chi tiết tham khảo Phần II, Mục 6 |
| Khả năng mở rộng và tích hợp | | | |
| 17 | Kết nối theo QCVN | Có - Theo văn bản 2290/BTTTT-CATTT | Chi tiết tham khảo Phần II, Mục 5.3 |
| 18 | Kết nối SIEM | Có | Chi tiết tham khảo Phần II, Mục 5.2 |
| 19 | Triển khai qua AD | Có | Chi tiết tham khảo Phần II, Mục 5.1 |

II, Thông tin chi tiết

## 1, Tổng quan giải pháp

Giải pháp CMDD - Phòng chống mã độc và quản lý tập chung là bộ công cụ bảo mật tiên tiến do CMC Cyber Security phát triển, giúp bảo vệ hệ thống thông tin trước các mối đe dọa như Malware, Ransomware, Trojan, Spyware, Keylogger, Backdoors…

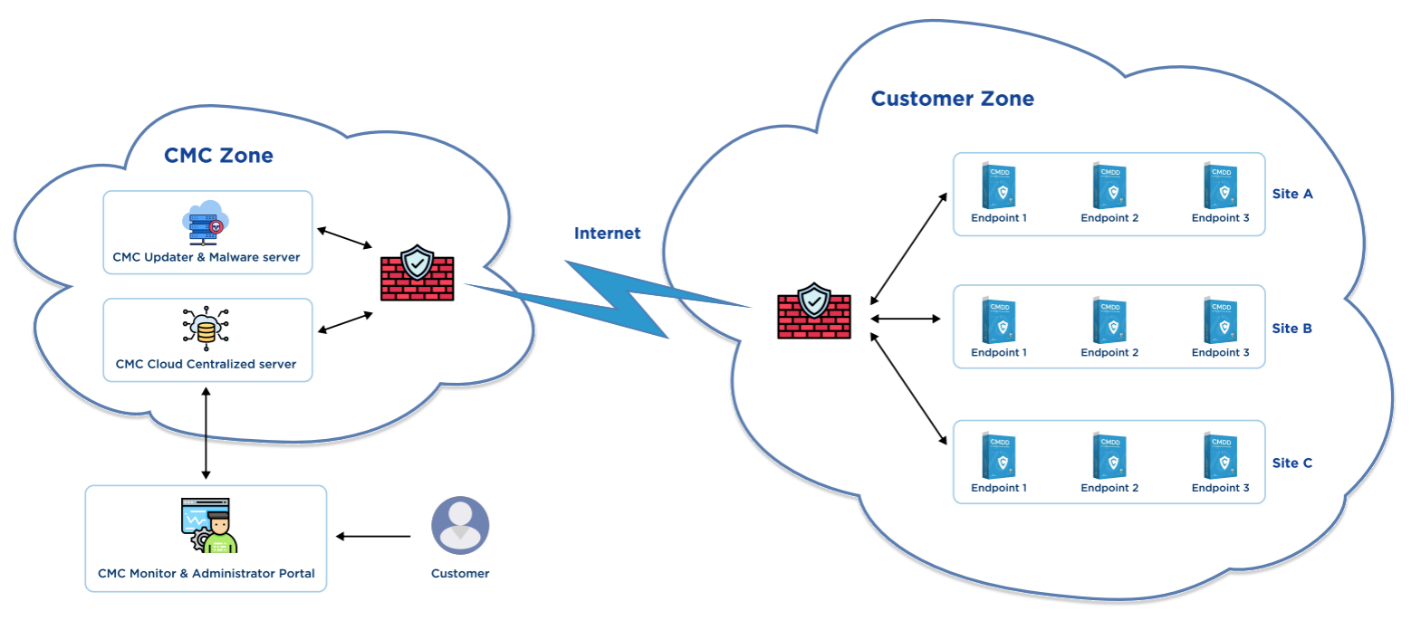
TÍNH NĂNG CHÍNH

* Phát hiện và ngăn chặn mã độc trên Endpoint.
* Chống tấn công Ransomware.
* Bảo vệ thời gian thực trước các mối đe dọa.
* Tự động cập nhật mẫu và phiên bản phần mềm.
* Quản trị tập trung mạng lưới Endpoint.
* Báo cáo thống kê định kì tình trạng lây nhiễm mã độc trong tổ chức.
* Kết nối chia sẻ dữ liệu với các hệ thống ATTT khác (siem, soc...).
* Tuân thủ và đáp ứng về chức năng, tính năng theo Quyết định số 176/QĐ-BTTTT ngày 09/02/2022 của Bộ Thông tin và Truyền Thông.

# 2, Các mô hình triển khai sản phẩm

Vận hành theo mô hình Client – Server, CMDD cho phép quản trị tập trung toàn bộ thiết bị, đảm bảo mọi dữ liệu được cập nhật theo thời gian thực và gửi về máy chủ quản trị. Điều này giúp doanh nghiệp giám sát, kiểm soát và ứng phó nhanh chóng với các nguy cơ an ninh mạng.

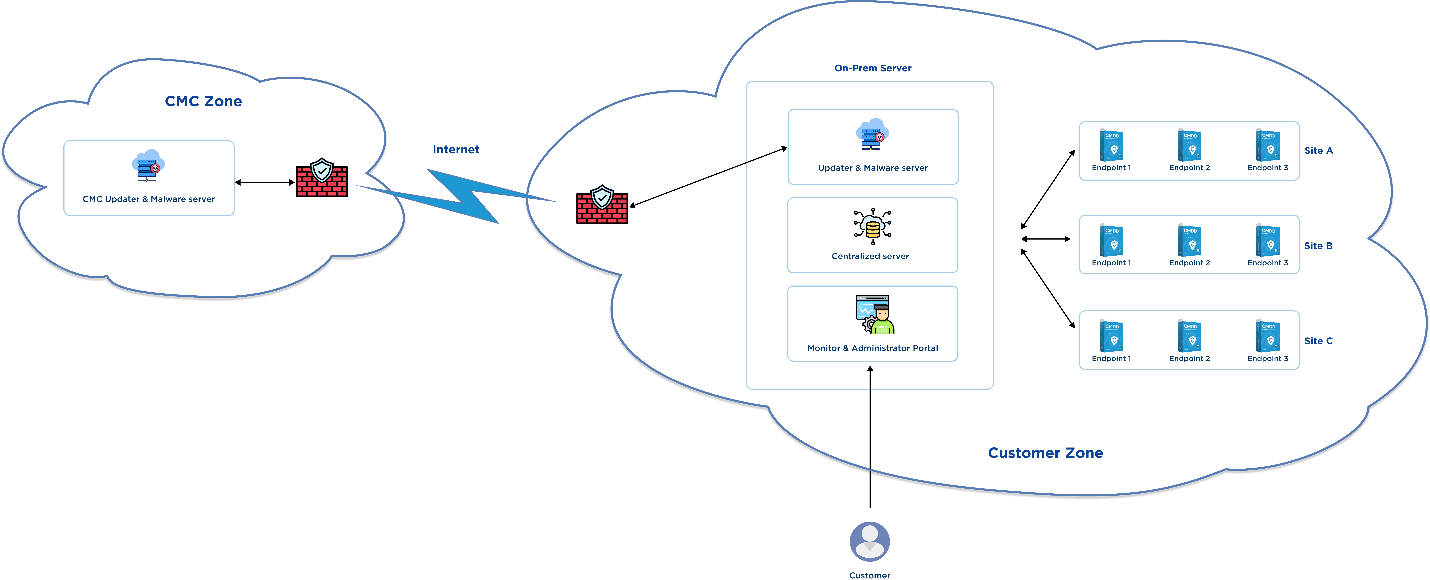
Mô hình On-Cloud hệ thống CMDD



Giải pháp CMDD On-Cloud bao gồm các thành phần chính:

* Hệ thống các Agent CMDD được cài đặt trên các Endpoint có nhiệm vụ phát hiện các mã độc xâm nhập theo thời gian thực, thực hiện loại bỏ tức thời và thống kê thông tin về hệ thống tập trung.
* Hệ thống server quản trị tập trung (CMC Cloud Centralized Server), hỗ trợ quản trị viên theo dõi được tình trạng lây nhiễm mã độc trên toàn bộ mạng lưới Endpoint thông qua Portal quản trị (CMC Monitor & Administrator Portal), hỗ trợ phân loại, báo cáo, thống kê và nắm bắt kịp thời tình hình ATTT của tổ chức/doanh nghiệp.
* Hệ thống Server tập mẫu và cập nhật (CMC Updater & Malware Server): Chịu trách nhiệm tự động cập nhật mẫu mã độc định kì 24h từ đa dạng các nguồn. Luôn có những mẫu mã độc mới nhất từ phổ thông đến độc quyền. Hỗ trợ cập nhật tự động thông tin mẫu, các phiên bản mới của phần mềm đến thành phần Agent cài trên các Endpoint. Là nguồn tri thức mạnh mẽ giúp thương hiệu CMC được biết đến trên thị trường và đạt được những chứng nhận quốc tế về hiệu quả sử dụng.

Mô hình On-Prem hệ thống CMDD



Các thành phần trong giải pháp On-Prem của CMDD tương tự như các thành phần khi triển khai On-Cloud. Tuy nhiên, các máy chủ quản trị tập trung (Centralized Server), lưu trữ dữ liệu mẫu nhận diện (Updater & Malware Server) đều được đặt tại hệ thống mạng của khách hàng.

Ngoài ra, để có thể cập nhật tập trung các mẫu nhận diện thì máy chủ lưu trữ dữ liệu mẫu (Updater & Malware Server) cần được kết nối đến máy chủ lưu trữ mẫu tập trung đặt tại CMC để cập nhật định kì các mẫu mã độc mới.

# 3, Chức năng chi tiết

## 3.1. Phát hiện và ngăn chặn các loại mã độc

Tính năng phát hiện và ngăn chặn mã độc được xây dựng dựa trên các công nghệ tiên tiến nhất hiện nay, nhằm mang đến khả năng bảo vệ chủ động, thông minh và toàn diện cho người dùng trước mọi mối đe dọa từ không gian mạng.

CMDD hỗ trợ bảo vệ người dùng khỏi mã độc thông qua 2 hình thức cơ bản:

* Quét mã độc: quét các tệp tin, thư mục, ổ đĩa (bao gồm cả các ổ đĩa/thư mục chia sẻ trong mạng LAN) để phát hiện mã độc ẩn chứa trong máy tính. Ngoài ra, CMDD còn quét cả các thành phần đặc biệt như RAM, Registry để phát hiện những mã độc fileless được inject vào các thành phần này để hoạt động.
* Bảo vệ thời gian thực (Realtime Protection): dựa trên các driver khởi động cùng hệ thống, CMDD dễ dàng nắm bắt được tức thời các sự kiện tác động đến file, process, registry trong máy tính. Từ đó, dựa trên phân tích thông mình từ AI và các tập rule xác định các hành động bất thường như mã hóa (ransomware), ghi lại và gửi thông tin người dùng dụng (Keylogger, spyware), truy cập domain hoặc tải các file độc hại trên internet,... để xử lý kịp thời, bảo vệ người dùng 24/7 khỏi nguy cơ nhiễm mã độc mà không cần thực hiện các thao tác thủ công.

Các phương pháp nhận diện mã độc được ứng dụng trong phần mềm CMDD bao gồm:

* Phát hiện dựa trên Signature: Thu thập các signature từ nhiều nguồn phổ thông đến độc quyền, liên tục cập nhật tập mẫu để phát hiện các mẫu mã độc mới nhất tại Việt Nam và thế giới.
* Phát hiện dựa trên hành vi: Giám sát các tiến trình đang hoạt động, log sự kiện hệ thống, và các thao tác bất thường để phát hiện hành vi đáng ngờ.
* Phân tích mã độc thông qua ứng dụng AI: Dựa trên mô hình AI, thực hiện xếp hạng mức độ nguy hiểm theo thang điểm, tự động xử lý nếu vượt ngưỡng an toàn.

## 3.2. Khả năng tự động cập nhật mẫu & phiên bản phần mềm

Hệ thống được trang bị chức năng tự động cập nhật xuống máy trạm, nhằm đảm bảo các Endpoint luôn được bảo vệ với phiên bản mới nhất của phần mềm và các mẫu nhận diện mã độc được cập nhật kịp thời. Chức năng này bao gồm hai cơ chế chính:

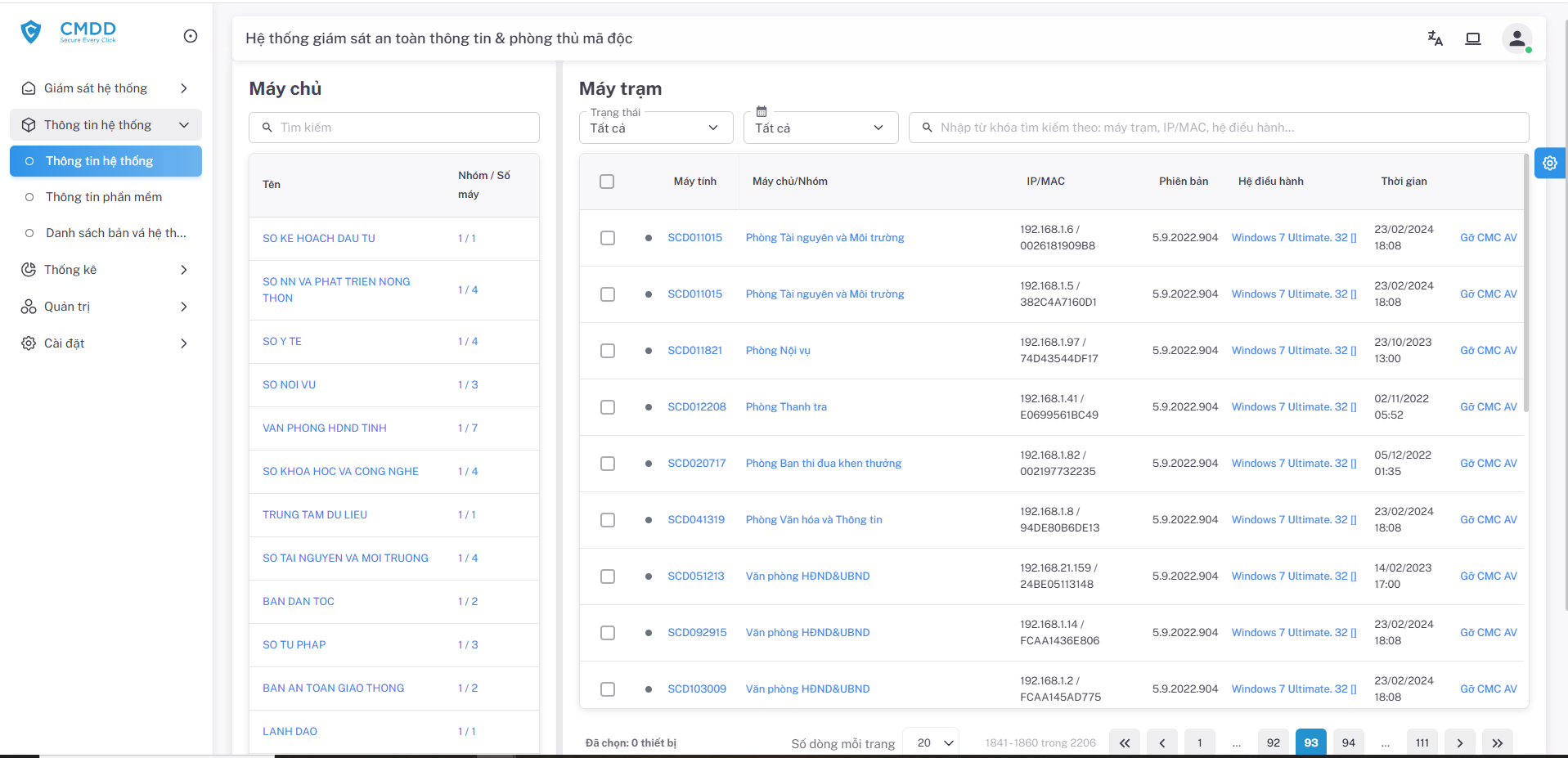
* Tự động cập nhật mẫu nhận diện mã độc
  + Hệ thống cho phép tự động cập nhật các mẫu nhận diện mã độc (signature, heuristic/behavior rules, AI model, v.v.) từ hệ thống Server tập mẫu & cập nhật (CMC Updater & Malware Server) xuống các Agent cài đặt trên máy trạm.
  + Cơ chế cập nhật được thực hiện theo lịch định kỳ cấu hình sẵn (15' khi có cập nhật mới từ server).
  + Agent có khả năng kiểm tra version của mẫu nhận diện hiện tại, từ đó chỉ tải về phần chênh lệch (delta update) nhằm tiết kiệm băng thông và giảm tải hệ thống mạng.
* Tự động cập nhật phiên bản phần mềm
  + Agent trên máy trạm có khả năng tự động kiểm tra và tải về các bản cập nhật phần mềm (bản vá, tính năng mới, sửa lỗi). Quá trình cập nhật được thực hiện:
    - Không cần tương tác từ người dùng, diễn ra ở chế độ nền.
    - Hiện thông báo khi tiến hành.
* Hệ thống đảm bảo rằng quá trình cập nhật không làm gián đoạn hoạt động của người dùng.

Với cơ chế cập nhật tự động thông minh và linh hoạt, hệ thống đảm bảo các máy trạm luôn duy trì trạng thái bảo mật tối ưu, giảm thiểu rủi ro từ các mối đe dọa mới xuất hiện và đảm bảo sự ổn định trong vận hành lâu dài.

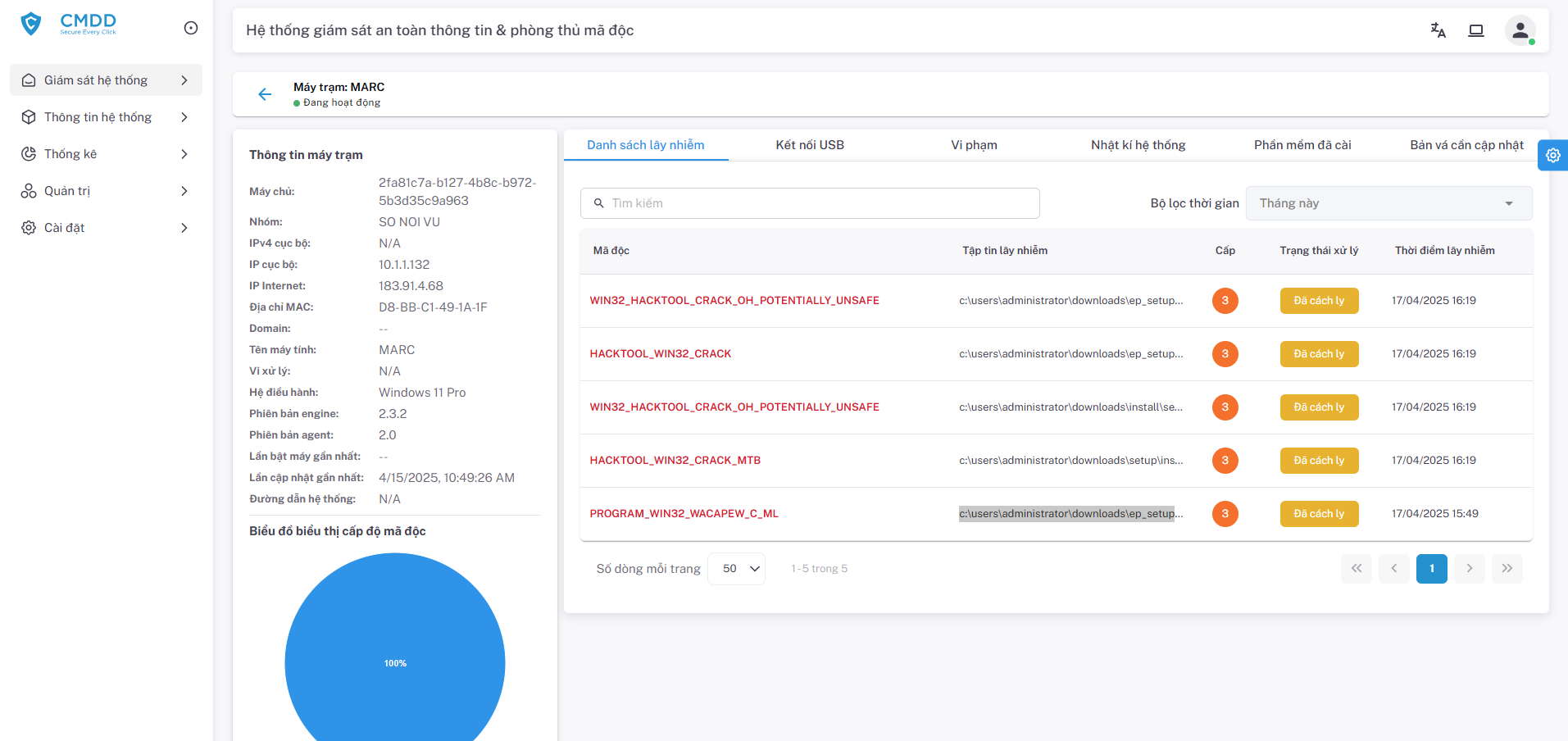
## 3.3. Quản trị tập trung

Hệ thống cung cấp chức năng quản trị tập trung toàn bộ các máy trạm đã cài đặt Agent, cho phép quản trị viên theo dõi, kiểm soát và điều phối các hoạt động bảo mật một cách linh hoạt và hiệu quả. Trong đó bao gồm:

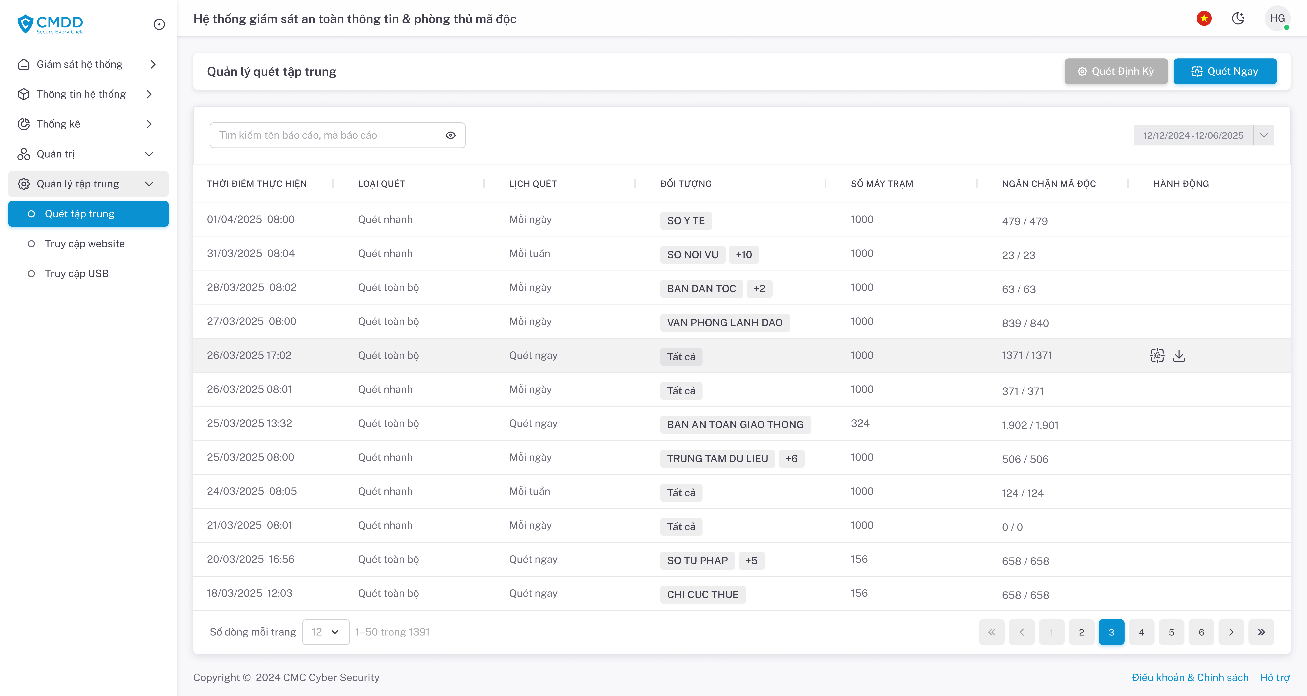
* Quản trị tập trung danh sách máy: Hỗ trợ quản lý toàn bộ danh sách máy đã cài Agent trong một màn hình duy nhất. Quản trị viên có thể dễ dàng tìm kiếm, lọc các máy theo các thông tin cơ bản như IP, Mac, Hệ điều hành,….. Đặc biệt hỗ trợ khả năng tìm kiếm gần đúng (Search Wildcard) giúp quản trị viên tìm kiếm theo một dải IP, các dòng hệ điều hành hoặc một cụm tên máy,…
* Hỗ trợ phân nhóm quản trị: Hệ thống hỗ trợ phân loại danh sách máy trạm thành các nhóm dựa trên cơ cấu tổ chức thực tế của khách hàng. Từ đó có khả năng báo cáo, thống kê và tác động bảo vệ theo từng nhóm máy trạm riêng biệt.



* Thông tin chi tiết của từng máy trạm: Giao diện quản trị hiển thị đầy đủ thông tin máy tính cài Agent:
  + Trạng thái kết nối
  + Thông tin cơ bản: IP, Mac, Hostname, OS,…
  + Thông tin phiên bản Agent cài đặt, thời điểm cài đặt, last ping,…
* Theo dõi tình trạng lây nhiễm mã độc trên các máy: Giao diện hiển thị trực quan tình trạng mã độc lây nhiễm trên máy theo thời gian dựa trên kết quả rà quét và bảo vệ thời gian thực. Quản trị viên có thể theo dõi chi tiết loại mã độc mắc phải, thời điểm phát hiện,tệp tin ảnh hưởng, mức độ nguy hiểm và trạng thái xử lý đối với mã độc đó.



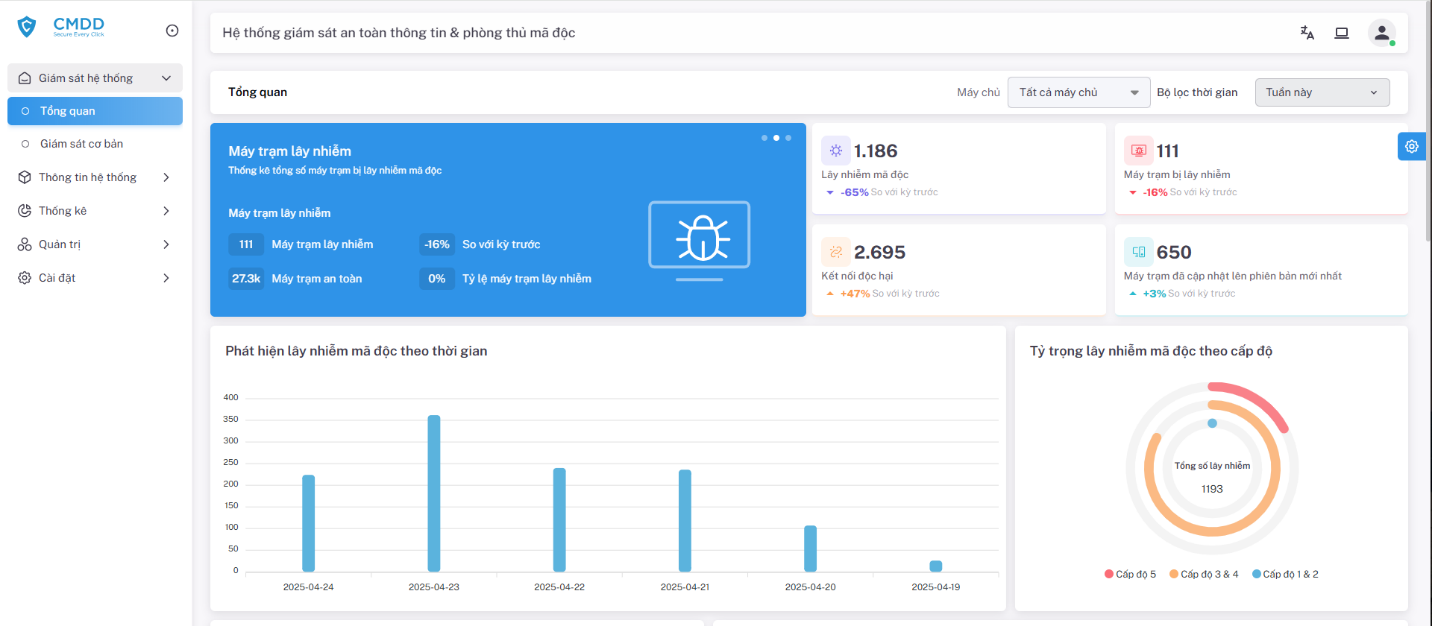
* Áp dụng các chính sách an toàn và cấu hình quét mã độc từ xa: CMDD cho phép quản trị viên thực hiện cấu hình rà quét mã độc từ xa trên một tập hoặc toàn bộ các máy tính cài Agent. Ngoài ra, quản trị viên có thể siết chặt một số chính sách bảo vệ như whitelist/blacklist truy cập website (Hỗ trợ ngăn chặn truy cập các website độc hại), chặn kết nối thiết bị ngoại vi,...

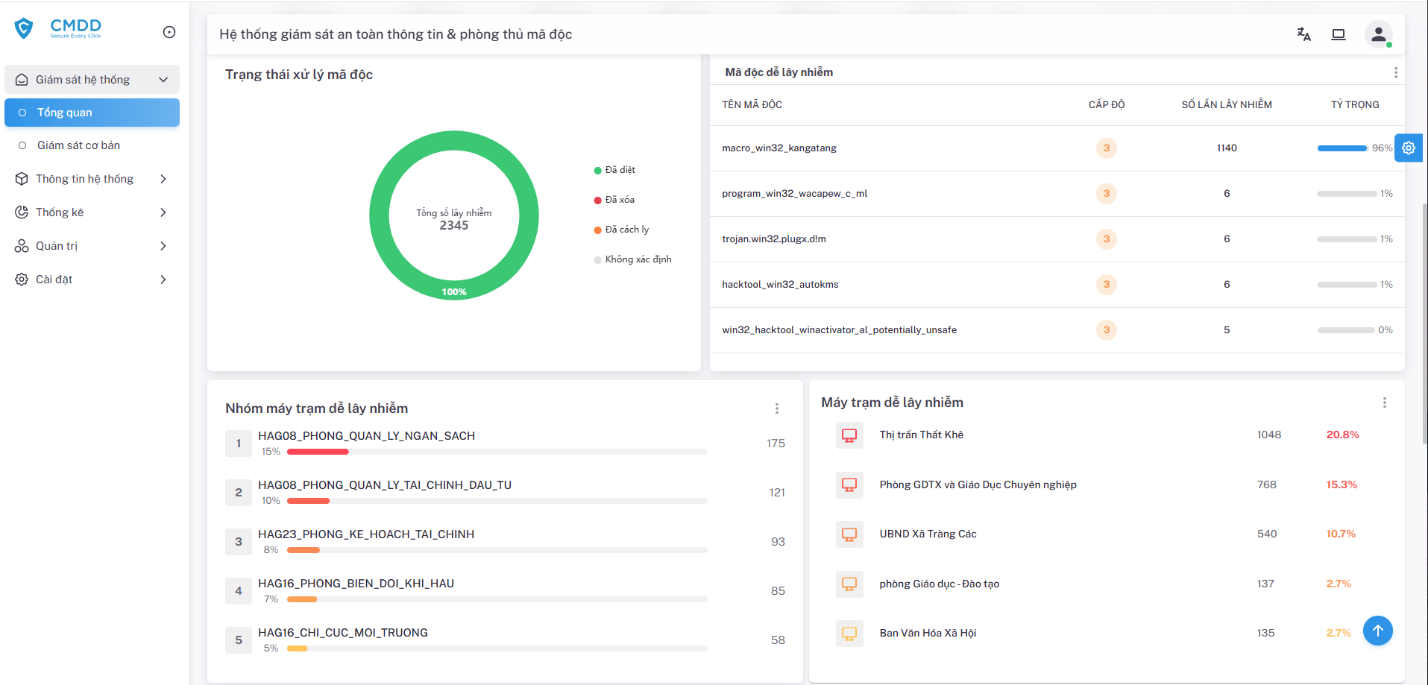


## 3.4. Báo cáo thống kê

Hệ thống cung cấp đầy đủ chức năng báo cáo, thống kê phục vụ công tác giám sát, đánh giá và quản lý tình hình lây nhiễm mã độc trên mạng lưới endpoint của đơn vị, giúp quản trị viên có cái nhìn tổng thể cũng như chuyên sâu về mức độ rủi ro và tình hình lây nhiễm mã độc.

* Thống kê, báo cáo định kì tình hình lây nhiễm mã độc trên hệ thống:
  + Tổng hợp và đưa ra các báo cáo định kì (hiện tại, tuần, tháng, quý năm) theo từng nhóm máy cũng như trên toàn bộ hệ thống
  + Các thống kê bao gồm: số mã độc lây nhiễm, xu thế so với kì trước, các máy trạm bị nhiễm, phân tích cơ cấu lây nhiễm theo mức độ,...
* Cung cấp các báo cáo phân tích sâu hơn về mã độc phổ biến đang lây nhiễm trong mạng lưới, xếp hạng các máy có nguy cơ lây nhiễm cao, tỷ trọng lây nhiễm của các loại mã độc trên mạng lưới và theo các nhóm



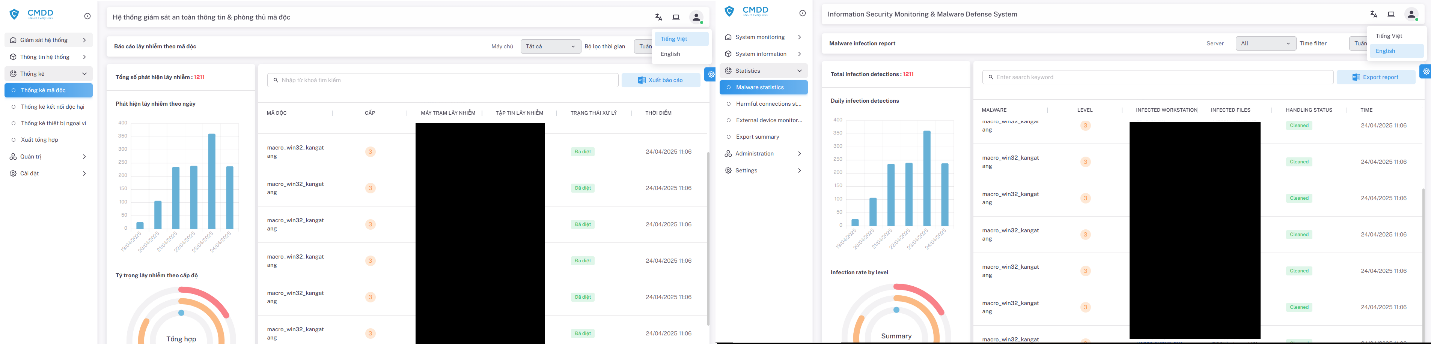


## 3.5. Hỗ trợ đa ngôn ngữ

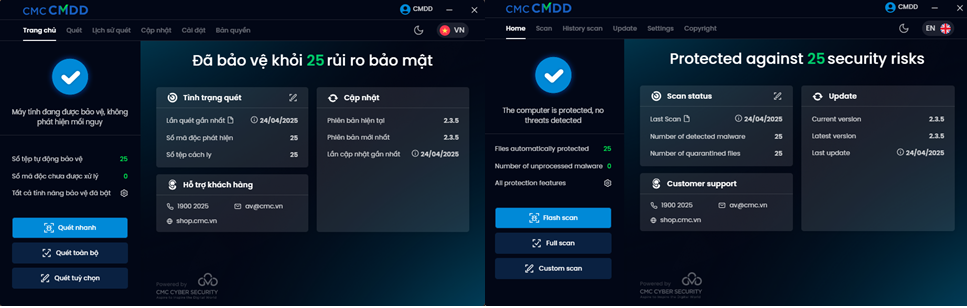
Hệ thống cung cấp khả năng hỗ trợ đa ngôn ngữ (Multilingual Support), giúp người dùng linh hoạt lựa chọn ngôn ngữ phù hợp trong quá trình sử dụng.

Việc hỗ trợ đa ngôn ngữ được triển khai đồng bộ trên cả hai thành phần chính của hệ thống là giao diện quản trị tập trung và giao diện Agent cài đặt trên các endpoint.

Hiện tại, hệ thống đang hỗ trợ 2 ngôn ngữ là tiếng Việt (Mặc định) và tiếng Anh. Người dùng có thể chuyển đổi sử dụng giữa các ngôn ngữ trực tiếp thông qua tính năng trên giao diện sản phẩm.



Giao diện đa ngôn ngữ của thành phần tập trung



Giao diện đa ngôn ngữ của thành phần Agent

# 4, Yêu cầu triển khai

* Đối với thành phần endpoint:
  + Hệ điều hành:
    - Windows: Từ windows 7 trở lên
    - Windows server: Từ windows server 2012 trở lên
    - Linux:
      * Ubuntu: Từ version 20.04 trở lên
      * Centos: Từ version 7 trở lên
      * Rocky Linux: Từ version 9.0 trở lên
  + Tài nguyên:
    - RAM: Tối thiểu 4GB
    - Dung lượng trống tối thiểu: 500MB
    - CPU: Pentium CPU G4600 trở lên
* Đối với các thành phần Server tập trung (Trường hợp triển khai On-Prem)
  + Centralized Server
    - Hệ điều hành: Ubuntu 22.04
    - RAM: 16GB DDR4
    - CPU: 16 vCPU
    - Ổ cứng: 500GB HDD
  + Updater & Malware Server
    - Hệ điều hành: Windows server 2022
    - RAM: 64GB DDR4
    - CPU: 4 vCPU
    - Ổ cứng: 200GB HDD
* Thông tin kết nối yêu cầu:
  + Triển khai On-Cloud: Mở kết nối từ các thành phần Agent đến:
    - 183.91.14.90:443 TCP => Gửi nhận dữ liệu đến hệ thống tập trung
    - 115.146.123.221:443 TCP => Cập nhật mẫu & phiên bản
    - 183.91.14.173:9999 TCP => Hỗ trợ quét mã độc
    - 8.8.8.8:53 TCP => DNS phân giải tên miền
  + Triển khai On-Prem: Mở kết nối từ các thành phần Agent đến thành phần tập trung trong mạng nội bộ và mở kết nối từ server update đến server update của CMC:
    - 115.146.123.221:443 TCP => Cập nhật mẫu & phiên bản
    - 8.8.8.8:53 TCP => DNS phân giải tên miền
* Các yêu cầu khác: Yêu cầu gỡ cài đặt các phần mềm Anti-Virus trên máy (nếu có)

# 5, Khả năng mở rộng & tích hợp

## 5.1. Tích hợp triển khai cài đặt qua giải pháp AD (Active Directory)

Phần mềm hỗ trợ triển khai cài đặt tự động và quản lý tập trung thông qua Active Directory (AD), phù hợp với các môi trường doanh nghiệp có số lượng máy trạm lớn, yêu cầu triển khai đồng loạt và đồng nhất trên toàn bộ hệ thống mạng nội bộ.

* Cung cấp file cài đặt định dạng .MSI sử dụng cho windows
* Cho phép quản trị viên IT cấu hình GPO để đẩy cài đặt tự động tới các máy trạm thuộc domain mà không cần thao tác thủ công trên từng thiết bị..
* Hỗ trợ cài đặt đơn giản qua script: msiexec /i "filepath.msi" /qb

## 5.2. Tích hợp đẩy dữ liệu về hệ thống SIEM

Phần mềm đáp ứng yêu cầu kết nối và tích hợp dữ liệu sự kiện (event logs) với hệ thống quản lý sự kiện bảo mật (SIEM) thông qua các giao thức phổ biến:

* CMDD hỗ trợ gửi log đến các hệ thống SIEM theo các chuẩn HTTP/HTTPS, TCP, UDP
* Phần mềm xuất log theo các chuẩn Syslog, CSV - các chuẩn vốn có để hệ thống SIEM dễ dàng thu thập và quản lý.
* Nội dung log bao gồm đầy đủ các thông tin timestamp, loại mã độc, đường dẫn, trạng thái xử lý, process, device info,...
* Đặc biệt tương tích với giải pháp SIEM của CMC và IBM Qradar

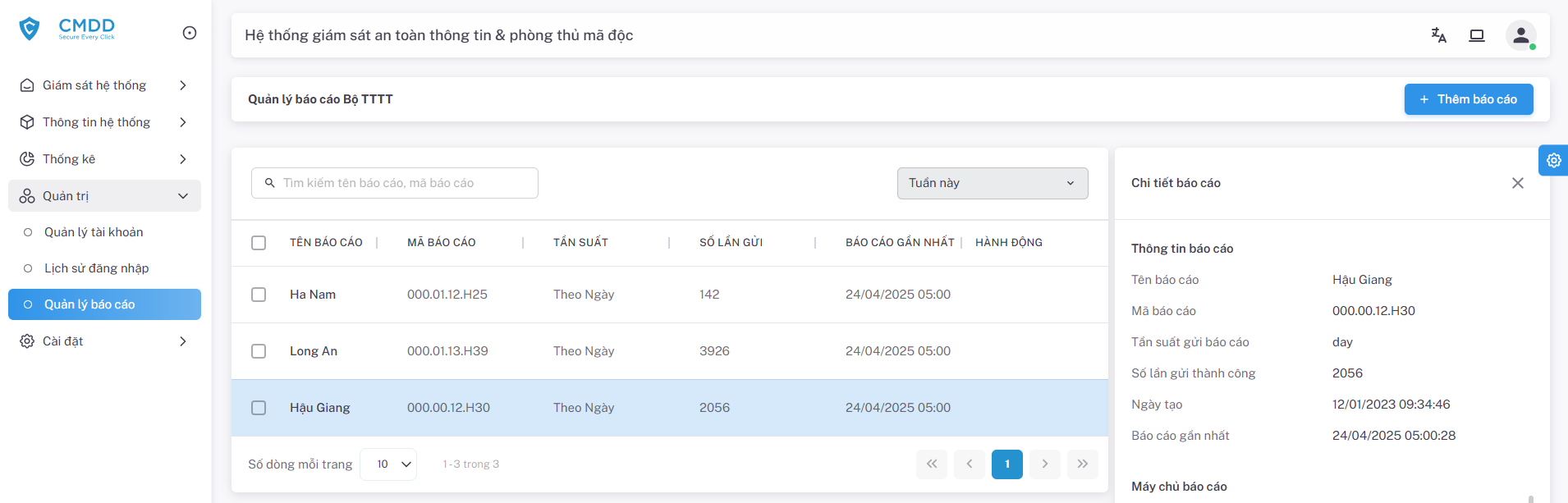
## 5.3. Tích hợp chia sẻ thông tin theo tiêu chuẩn quốc gia

Ngày 17/7/2018 Bộ Thông tin và Truyền thông tại văn bản số 2290/BTTTT-CATTT về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật

CMDD là một trong số ít các sản phẩm phân phối tại thị trường Việt Nam có khả năng kết nối chia sẻ dữ liệu về mã độc đến hệ thống của Cục An Toàn Thông Tin (NCSC) – Bộ Thông Tin Truyền Thông (https://mic.gov.vn/danh-sach-san-pham-phong-chong-ma-doc-co-kha-nang-ket-noi-chia-se-du-lieu-197138913.htm).

CMDD hỗ trợ chức năng kết nối và gửi báo cáo định kì đến máy chủ của bộ TTTT dựa trên quy chuẩn được quy định trong Văn bản số 2290/BTTTT\_CATTT ngày 17/7/2018 bao gồm các thông tin cơ bản:

* Thông tin của cơ quan, tổ chức gửi báo cáo.
* Thông tin các máy tính của tổ chức.
* Thông tin các mẫu mã độc trên các máy.
* Thông tin kết nối đáng ngờ.
* Thông tin lỗ hổng và cập nhật hệ điều hành.



# 6, Bảo trì & hỗ trợ kĩ thuật

Dịch vụ hỗ trợ kĩ thuật:

Cam kết cung cấp dịch vụ hỗ trợ 24/7/365 nhằm đảm bảo hoạt động liên tục và ổn định của hệ thống.

* Phương thức hỗ trợ:
  + Tổng đài hỗ trợ (Hotline) – 1900 2025: hoạt động 24/7 với kỹ thuật viên trực tiếp tiếp nhận và xử lý yêu cầu khẩn cấp.
  + Email hỗ trợ - support@cmccybersecurity.com: phản hồi trong vòng tối đa 60 phút với yêu cầu mức nghiêm trọng
  + Hỗ trợ từ xa (remote): sử dụng các công cụ bảo mật để truy cập và khắc phục sự cố từ xa trong thời gian ngắn nhất.
  + Hỗ trợ onsite (khi cần): đối với các sự cố nghiêm trọng hoặc yêu cầu đặc biệt.
* Chính sách bảo trì & cập nhật:
  + Cung cấp các bản vá bảo mật, cập nhật tính năng theo lịch phát hành của nhà sản xuất.
  + Bảo trì hệ thống theo yêu cầu nhằm đảm bảo hiệu năng và tính ổn định.
  + Cung cấp tài liệu cập nhật và hướng dẫn sử dụng tính năng mới.
* Đào tạo & chuyển giao
  + Đào tạo sử dụng phần mềm cho cán bộ vận hành hệ thống
  + Cung cấp tài liệu kỹ thuật tiếng Việt đầy đủ: hướng dẫn cài đặt, vận hành hệ thống.

# 7, Phụ lục

Một số giải thưởng, chứng chỉ của sản phẩm:

* Chứng nhận sản phẩm ATTT quốc gia
* Sản phẩm ATTT chất lượng cao CISE
* Sản phẩm ATTT xuất sắc - 2020
* Chứng chỉ quốc tế VB100

Các khách hàng tiêu biểu đã sử dụng CMDD:

* Tỉnh Hậu Giang
* Tập đoàn Doji
* CMC Corporation
* Bell System24