CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC – CMC CYBER SECURITY
15th Floor, CMC Tower, Duy Tân Street, Dịch Vọng Hậu, Cầu Giấy, Hà Nội
| Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

DỊCH VỤ SĂN TÌM MỐI ĐE DỌA CHỦ ĐỘNG
(CMC THREAT HUNTING SERVICE)

Thành viên chính thức của AVAR và ICSA

CMC CYBER SECURITY

CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC

Report No	**V1.0**
Date	1/12/2019
Document Type	CMC Threat Hunting Service
Author	Luu The Hien
Reviewer	Ha The Phuong

CMC CYBER SECURITY

MỤC LỤC

I. Dịch vụ săn tìm mối đe dọa chủ động (Threat Hunting)

1.1. Mô tả dịch vụ

Dịch vụ săn tìm mối đe dọa chủ động (CMC Threat Hunting) là một phần của bộ bảo đảm an toàn thông tin do CMC CS cung cấp cho các tổ chức/ doanh nghiệp.

Với xu thế phòng thủ chủ động hiện nay, việc xác định được các mối đe dọa, mức độ và ảnh hưởng khi các mối đe dọa xảy ra là một việc vô cùng quan trọng đối với các hệ thống an ninh an toàn thông tin. Các giải pháp an ninh truyền thống hầu như chỉ có thể xác định được các mối đe dọa đã biết, trong khi đó các mối de dọa chưa biết thường khó có thể xác định. Do đó, dịch vụ Threat Hunting ra đời nhằm hỗ trợ các giải pháp an ninh truyền thống trong việc xác định các mối đe dọa.

CMC Threat Hunting Service là sự kết hợp giữa con người và công nghệ - AI, Machine Learning, Threat Intelligence, Vulnerability Assessment, mang đến một phương thức mới chống lại các mối đe dọa trên không gian mạng.

Cụ thể Threat Hunting là một quá trình chủ động tìm kiếm các mối đe dọa, sử dụng internal và external threat intelligence, khai thác và phân tích thông tin (log, mã độc).

Các phương thức có thể thực hiện Threat Hunting:

- *User Behavior Analysis:* là việc phân tích hành vi người dùng bằng việc thu thập, phân tích thông tin log theo thời gian thực để làm đầy đủ và nâng cao khả năng phát hiện và tìm kiếm mối đe dọa.
- *Network Behavior Analysis:* Phân tích các chuỗi hoạt động mạng để đưa ra dự đoán nhằm xác định hành vi bất thường.
- *Malware Detection:* Thực hiện săn tìm (hunting) mối đe dọa liên quan đến mã độc theo thời gian thực để đáp ứng khả năng phòng thủ chủ động với các loại mã độc có tốc độ biến đổi nhanh (Ransomware và các mẫu biến thể mã độc khác)
- *Threat Intelligence Feeds:* Nghiên cứu và cập nhật các lỗ hổng, các hoạt động đe dọa tiềm tàng của mã độc, và sau đó ánh xạ với tài sản (asset) của khách hàng để thực hiện và nâng cao khả năng phòng thủ chủ động.

- *Advanced Malware Analysis:* Việc phân tích chuyên sâu về các hành vi của mã độc nhằm xác định các hành vi độc hại cũng như các ảnh hưởng tiềm tàng mà mã độc có thể gây ra. Bên cạnh đó, hỗ trợ việc thu thập các thông tin về kẻ tấn công

Bằng việc sử dụng dịch vụ Threat Hunting, khách hàng chủ động phát hiện các mối đe dọa tiềm tàng trước khi xảy ra sự cố mất an toàn thông tin. Từ đó giúp khách hàng lên phương án phòng thủ và đối phó lại với các mối đe dọa và rút ngắn thời gian xử lý khi sự cố xảy ra.

Trên cơ sở kết quả của quá trình Threat Hunting, CMC SOC sẽ cung cấp các thông tin các kịch bản, thông tin hệ thống thông tin khách hàng có thể gặp phải qua đó sẽ đưa ra các khuyến nghị cho khách hàng có thể khắc phục, cập nhật các bản vá qua đó phòng tránh rủi ro cho hệ thống thông tin.

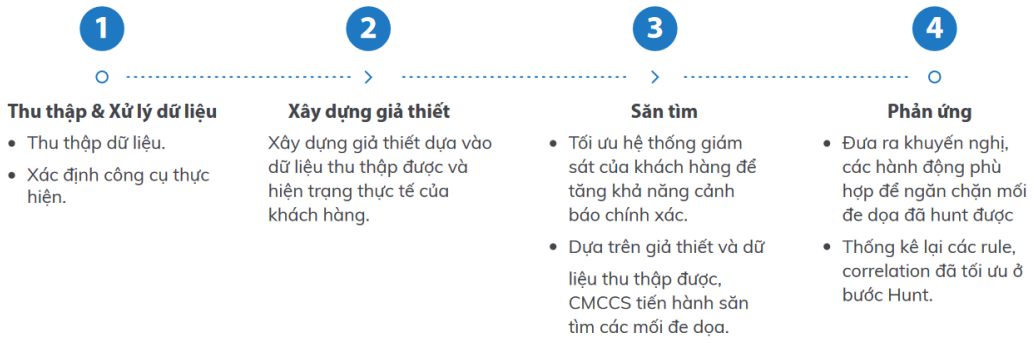
- Lợi ích mang lại cho khách hành:
  - Có những thông tin mới nhất về tình hình an ninh của hệ thống thông qua các báo cáo của CMC Cyber Security
  - Được bảo vệ an toàn trước những mối đe dọa an ninh thông tin, kể cả các mối đe dọa phức tạp chưa từng được phát hiện.
  - Nhận những tư vấn, khuyến nghị từ các chuyên gia hàng đầu trong lĩnh vực bảo mật để tối ưu hóa hệ thống, hạn chế tối khả năng bị tấn công
  - Hiểu được phương thức, động cơ của những kẻ tấn công, từ đó có chiến lược phòng thủ trước các mối đe dọa một cách toàn diện.
- Ưu điểm nổi bật:
  - Threat Intelligence: cập nhật 24/7 các mối đe dọa mới từ nhiều tổ chức phòng chống mã độc uy tín, phân loại mối đe dọa theo ngành nghề của khách hàng.
  - Vulnerability Assessment: rà soát các mối đe dọa, điểm yếu, lỗ hổng có thể bị khai thác từ bên trong hệ thống theo thời gian thực.
  - Sử dụng các công nghệ tiên tiến cùng các chuyên gia hàng đầu trong ngành với nhiều năm kinh nghiệm về an toàn thông tin.

- Nghiên cứu và theo sát hoạt động của các nhóm tin tặc trên thế giới.
- Tích hợp trí tuệ nhân tạo AI và Machine Learning giúp nâng cao khả năng tìm kiếm mối đe dọa.

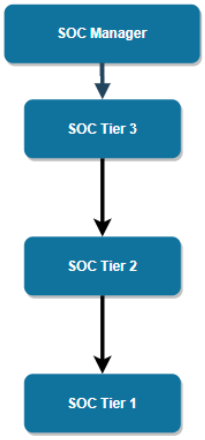
1.2. Gói dịch vụ và man hours tương ứng

STT	Work - 24/7	Man hours/ Day	Total / Month	Total/ Year	1 Man Level 1	1 Man level 2	1 Man Level 3
1	Thu thập và Xử lý dữ liệu	1	30	360	80%	20%	0%
2	Xây dựng giả thuyết	1.5	45	540	0%	60%	40%
3	Săn tìm	2	60	720	0%	50%	50%
4	Phản ứng	1	30	360	0%	60%	40%
Total		5.5	165	1980			

Tiến trình thực hiện Threat Hunting:



1.3. Cơ cấu nhân sự



Theo mô hình như trên, nhân sự thực hiện Threat Hunting bao gồm:

- Nhân sự Tier 3 (theo phân cấp đội SOC)
- Nhân sự Tier 2 (theo phân cấp đội SOC)
- Nhân sự Tier 1 (theo phân cấp đội SOC)

Bảng mô tả phân cấp CMC – SOC:

Vị trí	Mô tả
SOC Tier 1	- Bao gồm nhân sự thuộc Nhóm Giám sát và cảnh báo (Monitor and Alert Team) - Phân cấp: Beginner, Junior-level analyst - Các kỹ năng yêu cầu: • Có ít nhất 1 năm kinh nghiệm trong lĩnh vực ANTT • Sysadmin skills: có khả năng sử dụng 2 trong 3 OS (Linux/Mac/Windows) và thành thạo ít nhất với 1 OS • Programming skills: có khả năng lập trình với ít nhất 1 ngôn ngữ lập trình (Python, Ruby, PHP, C, C#, Java, Perl…) hoặc nhiều hơn • Security skills: ○ Có 1 trong các chứng chỉ CCNA/MCSA/CEH hoặc có các kỹ năng chuyên môn thực tế tương đương

	○ Có kinh nghiệm sử dụng và vận hành các sản phẩm bảo mật của các Nhà cung cấp sản phẩm bảo mật lớn trên thế giới như Cisco, Symantec, Mcafee, CheckPoint… hoặc nhiều hơn là một lợi thế ○ Có kiến thức và khả năng sử dụng các công cụ đánh giá lỗ hổng bảo mật (Vulneribity Assessment) - Yêu cầu công việc: • Giám sát và xác định mức độ khẩn cấp và độ chính xác của các ticket cảnh báo ứng với hiện trạng thực tế tại từng hệ thống CNTT được giám sát • Cảnh báo và thực hiện các luồng công việc trong Playbook • Hỗ trợ SOC Tier 2 tìm kiếm và xác định các thông tin liên quan đến ticket sự cố • Sử dụng các công cụ đánh giá lỗ hổng bảo mật (Vulneribity Assessment). Xác minh và đưa ra báo cáo lỗ hổng bảo mật.
SOC Tier 2	- Bao gồm nhân sự Nhóm Phân tích (Analyst Team) và Nhóm xử lý sự cố (Incident Response Team) - Phân cấp: Advanced analyst - Các kỹ năng yêu cầu: • Có ít nhất 2 năm kinh nghiệm trong lĩnh vực ANTT • Có các skills của SOC Tier 1 • Có kinh nghiệm sử dụng và vận hành ít nhất 1 SIEM như Qradar, HP Arcsights, Splunk… hoặc các sản phẩm SIEM khác • Có 1 trong các chứng chỉ CCNA/MCSA/CEH/CompTIA Security+ hoặc có các kỹ năng chuyên môn thực tế tương đương • Có khả năng thu thập chứng cứ số và các thông tin phục vụ quá trình Điều tra số (Forensic) và Săn tìm mối đe dọa (Threat Hunting) - Yêu cầu công việc: • Đánh giá độ chính xác, phạm vi và mức độ ảnh hưởng của các ticket sự cố xuất hiện trên hệ thống giám sát

	• Xây dựng và cập nhật Playbook • Hỗ trợ SOC Tier 3 trong việc thu thập chứng cứ số và các thông tin phục vụ quá trình Điều tra số (Forensic) và Săn tìm mối đe dọa (Threat Hunting) • Thực hiện phân tích và điều tra sơ bộ các thông tin và chứng cứ số đã được thu thập
SOC Tier 3	- Bao gồm nhân sự Nhóm Điều tra số (Forensic Team) và Nhóm Săn tìm mối đe dọa (Threat Hunting Team) - Phân cấp: More advanced, Expert analyst - Các kỹ năng yêu cầu: • Có ít nhất 3 năm kinh nghiệm trong lĩnh vực ANTT • Có các skills của SOC Tier 2 • Thành thạo 1 trong các kỹ năng chuyên sâu: Phân tích mã độc (Malware Analysis), Điều tra số (Forensic), Săn tìm mối đe dọa (Threat Hunting) … hoặc nhiều hơn • Có 1 trong các chứng chỉ CHFI/ECSA/OSCP/OSCE/SAN - Yêu cầu công việc: • Nghiên cứu và xác định các mối đe dọa tiềm tàng đối với các hệ thống CNTT đang được giám sát • Xác định nguyên nhân sự cố, các đối tượng/tài sản bị lây nhiễm hoặc ảnh hưởng của các sự cố ANTT • Tối ưu hóa rule và các yếu tố thông tin để nâng cao chất lượng giám sát đối với từng hệ thống ANTT • Viết báo cáo chuyên sâu về kết quả Phân tích mã độc (Malware Analysis), Điều tra số (Forensic), Săn tìm mối đe dọa (Threat Hunting) đã được thực hiện • Tham mưu, tư vấn phương pháp giải quyết, nâng cao khả năng phòng thủ để giảm thiểu và ngăn chặn các mối đe dọa ANTT

SOC Manager	- Chịu trách nhiệm về toàn bộ các công việc và hoạt động của CMC SOC trước công ty - Phân cấp: More advanced, Expert - Các kỹ năng yêu cầu: • Có ít nhất 5 năm kinh nghiệm trong lĩnh vực ANTT • Có các skills của SOC Tier 3 • Có 1 trong các chứng chỉ CISSP/CISA/CISM • Có khả năng giao tiếp và truyền đạt thông tin tốt • Có khả năng quản lý nhân sự và điều hành, điều phối các hoạt động và công việc chung - Yêu cầu công việc: • Giám sát và đánh giá hoạt động của toàn bộ các nhân viên • Tuyển dụng, đào tạo, và đánh giá năng lực nhân viên. • Đo lường số liệu hiệu suất SOC và truyền đạt giá trị của hoạt động bảo mật cho các nhà lãnh đạo doanh nghiệp. • Phát triển và thực hiện kế hoạch truyền thông khủng hoảng cho công ty và các bên liên quan khác.

Mô tả công việc các cấp độ:

- **Tier 1:**
  - Sau khi bắt đầu quá trình Threat Hunting nhân sự SOC Tier 1 sẽ thực hiện thu thập các thông tin yêu cầu của khách hàng.
  - Sử dụng các công cụ để thu thập các thông tin cần thiết trên hệ thống thông tin phía khách hàng phục vụ quá trình Threat Hunting.
  - Phân loại, xử lý các dữ liệu thô trước khi gửi cho Tier 2 để bắt đầu quá trình phân tích và đưa ra các giả thuyết kịch ban cho hệ thống thông tin.

- Chạy VA định kỳ để kiểm tra các lỗ hổng bảo mật đối với hệ thống thông tin của khách hàng.
- Thường xuyên phân tích, cập nhật các mối đe dọa.

➢ **Tier 2:**

- Dựa vào các dữ liệu thông tin đã thu thập được nhân sự Tier 2 sẽ đi vào phân tích và đưa ra các kịch bản, giả thuyết cho hệ thống thông tin qua đó tìm ra các mối đe dọa đối với hệ thống thông tin.
- Liên thục phân tích, tìm kiến các mối đe dọa mới trên thế giới để làm giàu dữ liệu Threat Intelligence.
- Phân tích các sự kiện an ninh an toàn thông tin bất thường trên hệ thống.
- Tối ưu hệ thống giám sát của khách hàng bằng cách khuyến nghị cập nhật các rules, signature, IOC, … để có thể phát hiện kịp thời các bất thường.
- Thành thạo một trong các kỹ năng:
  - Xử lý sự cố.
  - Điều tra phân tích lưu lượng mạng.
  - Phân tích, điều tra hành vi phía người dùng cuối.
  - Phân tích, điều tra hành vi của các loại mã độc.
  - Phân tích, điều tra memory.

➢ **Tier 3:**

1.4. Quy trình dịch vụ

Quy trình thực hiện dịch vụ Threat Hunting:

Chuẩn bị dữ liệu cho việc Threat Hunting bao gồm: - Xác định dữ liệu sẽ được Hunting - Xác định các công cụ sẽ sử dụng cho viêc Hunting.	CMC CS sử dụng các phương pháp Threat Hunting tốt nhất đã được nghiên cứu và áp dụng vào thực tế hiện trạng của từng khách hàng. Trên cơ sở đó CMC CS sẽ đưa ra những đề xuất giả thuyết tốt nhất cho hiện trạng hệ thống thông tin khách hàng.	Trên cơ sở các phương pháp, giả thuyết và dữ liệu đã được chọn CMC CS sẽ tìm các mối đe dọa đối với hệ thống thông tin của khách hàng qua đó sẽ tối ưu lại các rule, correlation sẵn có để làm tăng khả năng cảnh báo chính xác cho hệ thống giám sát của khách hàng.	Sau khi thực hiện Hunt, CMC CS sẽ xác định ra các mối đe dọa đối với hệ thống thông tin của khách hàng. Trong trường hợp các mối đe dọa không khả thi thì sẽ quay lại bước thiết lập các giả thuyết để thcuwj hiện lại quá trình Hunt	Khi các mối đe dọa đã được xác định, CMC CS sẽ đưa ra và khuyến nghị các hành động tương ứng phù hợp để ngăn chặn các mối đe dọa: - Các khuyến nghị phòng chống các mối đe dọa - Các rule và các phương pháp Threat Hunting được xây dựng trong quá trình Hunting - Các hướng dẫn để tối ưu cho Firewall, IPS/IDS, WAF, SIEM,…

Dịch vụ trong Threat Hunting	Mô tả	Nội dung
User Behavior Analysis	Là việc phân tích hành vi người dùng bằng việc thu thập, phân tích thông tin log theo thời gian thực để làm đầy đủ và nâng cao khả năng phát hiện và tìm kiếm mối đe dọa.	1. Collect and Process Data: Chuẩn bị dữ liệu cho việc Threat Hunting bao gồm: - Xác định dữ liệu sẽ được Hunting - Xác định công cụ sẽ sử dụng 2. Establish the hypothesis: Sử dụng các phương pháp Threat Hunting tốt nhất đã nghiên cứu để áp dụng vào hiện trạng khách hang. Trên cơ sở đó sẽ đề xuất ra những giả thuyết tốt nhất.
Network Behavior Analysis	Phân tích các chuỗi hoạt động mạng để đưa ra dự đoán nhằm xác định hành vi bất thường.	

Malware Detection	Khái niệm: Thực hiện săn tìm (Hunting) mối đe dọa liên quan đến mã độc theo thời gian thực để đáp ứng khả năng phòng thủ chủ động với các loại mã độc có tốc độ biến đổi nhanh (Rasomware và các biến thể mã độc khác).	3. Hunt: Trên cơ sở các phương pháp, giả thuyết và dữ liệu đã được chọn tìm, team SOC sẽ tìm các mối đe dọa đối với hệ thống thông tin của khách hang. Tối ưu lại các rule, correlation sẵn có để làm tăng khả năng cảnh báo chính xác cho hệ thống. 4. Identify threats: Sau khi thực hiện Hunting, team SOC sẽ xác định ra các mối đe dọa đối với hệ thống thông tin của khách hàng. Trong trường hợp các mối đe dọa không khả thi thì sẽ quay lại bước thiết lập giả thuyết để thực hiện lại quá trình Hunting. 5. Respond: Khi các mối đe dọa đã được xác định, team SOC sẽ đưa ra và khuyến nghị các hành động tương ứng phù hợp để ngăn chặn các mối đe dọa: - Các khuyến nghị phòng chống các mối đe dọa - Liệt kê lại các rule, các correlation đã được tối ưu - Các rule và các phương pháp Threat Hunting được xây dựng trong quá trình Hunting - Các hướng dẫn để tối ưu cho Firewall, IPS, WAF, SIEM
Threat Intelligence Feeds	Nghiên cứu và cập nhật các lỗ hổng, các hoạt động đe dọa tiềm tang của mã độc, và sau đó ánh xạ với tài sản (asset) của khách hang để thực hiện nâng cao khả năng phòng thủ chủ động.	
Advanced Malware Analysis	Việc phân tích sâu về về các hành vi của mã độc nhằm xác định các hành vi độc hại cũng như các ảnh hưởng tiềm tang mà mã độc có thể gây ra, bên cạnh đó hỗ trợ về việc thu thập các thông tin về kẻ tấn công.	

1.5. Phạm vi cung cấp dịch vụ

1.6. Các yêu cầu khách hàng phối hợp

- Khảo sát, thu thập các thông tin về hiện trạng hệ thống thông tin của khách hàng.
- Các yêu cầu của khách hàng về việc thực hiện Threat Hunting
- Ngoài ra với từng trường hợp cụ thể, các chuyên viên phụ trách kỹ thuật của CMC Cyber Security sẽ gửi các yêu cầu hỗ trợ riêng.

II. Giải pháp Threat Intelligence

2.1. Mô tả dịch vụ

Dịch vụ Threat Intelligence ra đời nhằm cung cấp nguồn dữ liệu mạnh mẽ về các mối đe dọa một cách chủ động trên không gian mạng, qua đó cung cấp các thông tin hữu ích giúp tổ chức/ doanh nghiệp có cái nhìn toàn cảnh về tình hình an toàn thông tin trong khu vực và trên thế giới, đồng thời có các biện pháp phòng chống mối nguy hại một cách chủ động từ sớm, giúp nâng cao hiệu quả, giảm thiểu ảnh hưởng đến hoạt động kinh doanh của các tổ chức/ doanh nghiệp.

Cùng với sự bùng nổ của nền cách mạng 4.0 trên thế giới, công việc đảm bảo tính bảo mật của hệ thống thông tin đang trong cuộc chiến gay gắt chống lại các cuộc tấn công mạng đang ngày ra tăng về số lượng, tốc độ và độ phức tạp. Thực tế trên đòi hỏi một cách tiếp cận mới đối với việc ngăn chặn các mối đe dọa trên không gian mạng một cách chủ động hơn thay vì khi hệ thốn thông tin gặp sự cố chúng ta mới đi khắc phục nó.

Theo các nghiên cứu gần đây, các giải pháp an ninh truyền thống hầu như chỉ có thể xác định được các mối đe dọa đã biết, trong khi các mối nguy hại ảnh hưởng lớn tới các hệ thống thông tin của các tổ chức/ doanh nghiệp đều đến từ các lỗ hổng chưa biết (zero – day).

Vì vậy, CMC Threat Intelligence hoạt động như một cơ sở dữ liệu khổng lồ về các mối đe dọa trên không gian mạng, được liên tục cập nhật và tối ưu bởi đội ngũ chuyên gia cả CMC CYBER SECURITY giúp đội ngũ an ninh an toàn thông tin của khách hàng có thể làm giàu (enrich) nguồn dữ liệu về các mối đe doạ (URLs, IPs, files) của doanh nghiệp, từ đó có thể chủ động ngăn chặn sớm các mối đe dọa mới nhất, phức tạp, giảm thiểu ảnh hưởng đến hoạt động của doanh nghiệp.

CMC Threat Intelligence có những ưu điểm sau:

- Threat Intelligence: cập nhật 24/7 các mối đe dọa mới từ nhiều tổ chức phòng chống mã độc uy tín, phân loại mối đe dọa theo lĩnh vực của khách hàng.

- Được phân tích, xây dựng bởi chuyên gia hàng đầu trong ngành với nhiều năm kinh nghiệm về an toàn thông tin.

- Nghiên cứu và theo sát hoạt động của các nhóm tin tặc trên thế giới, cung cấp thông tin liên quan cho khách hàng trước khi các cuộc tấn công diễn ra.

- Tích hợp trí tuệ nhân tạo AI và Machine Learning giúp nâng cao khả năng tìm kiếm mối đe dọa.

Những lợi ích từ hệ thống CMC Threat Intelligence mang lại cho khách hàng:

- Giảm đáng kể thời gian phản ứng với sự cố ATTT nhờ các thông tin chuyên sâu về mối đe dọa được thu thập trước khi chúng xảy ra.

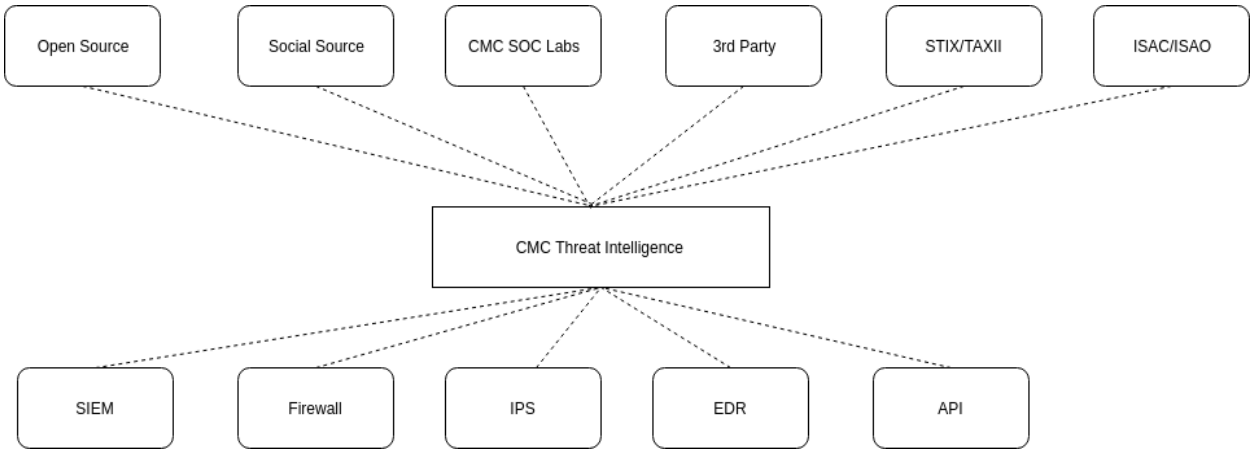
- Giám sát các hoạt động tấn công mạng nhắm đến tổ chức của khách hàng.

- Phục vụ hoạt động săn tìm chủ động mối đe dọa (Threat Hunting).

- Tỉ lệ thông tin sai (false positive) giảm nhờ kết hợp dữ liệu thu thập được từ các nguồn bên ngoài với dữ liệu phân tích nội bộ.

2.2. Chức năng

Nhằm hỗ trợ các nhà phân tích bảo mật trong việc phân tích và xử lý sự cố với một lượng dữ liệu threat quá lớn, CMC SOC đã xây dựng CMC Threat Intelligence để giúp các nhóm bảo mật dễ dàng đạt được các kỳ vọng khi sử dụng Threat Intelligence. CMC Threat Intelligence tự động hóa tất cả các quy trình để collecting, managing và integrating threat intelligence và cung cấp cho các nhà phân tích bảo mật công cụ, tài nguyên và cảnh báo xu hướng đe dọa mới để các nhà phân tích bảo mật nhanh chóng ứng phó với các mối đe dọa (active threats).



Các tính năng cơ bản:

- **Thu thập (Collect)**

CMC TI tập hợp intelligence từ nhiều nguồn khác nhau, bao gồm:

- STIX/TAXII feeds
- Open source threat feeds
- Social Source threat feeds
- Commercial threat intelligence providers
- Unstructured intelligence: PDFs, CSVs, emails
- ISAC/ISAO shared threat intelligence

- **Quản lý (Manage)**

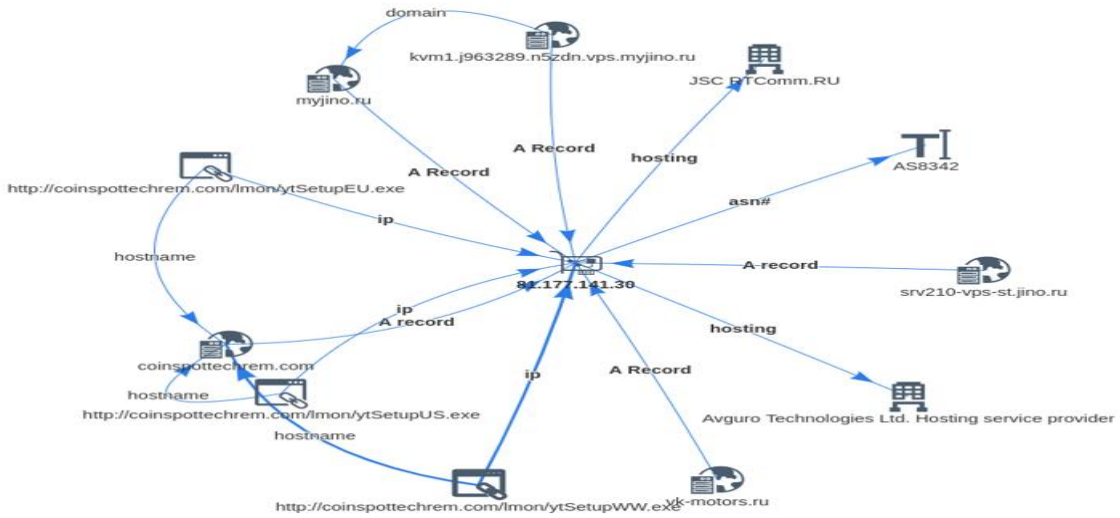
CMC TI thực hiện xử lý và biến các dữ liệu về mối đe dọa dạng thô thành dạng dữ liệu dạng tinh:

- Normalizes feeds into a common taxonomy
- De-duplicates data across feeds
- Removes false positives
- Enriches data with actor, campaign, and TTP
- Associates related threat indicators

- **Tích hợp (Integrate)**

CMC Threat Intel integrates with internal security systems to make threat intelligence actionable.

- Deep integration with SIEM, FW, IPS
- Scales to process millions of indicators
- Risk ranks threats via machine learning
- Includes Threat Bulletins from Anomali Labs
- Secure, 2-way sharing with Trusted Circles



CMC TI cung cấp các khả năng để giúp các nhà phân tích hiệu quả hơn và tăng hiệu quả của việc sử dụng threat intelligence, chẳng hạn như:

- Malicious file examination via a built-in sandbox
- Association of indicators to cyber Actors
- Contextual data: WHOIS, PassiveDNS, others
- Threat investigation engine with analyst workflows
- Easily produce and share threat intelligence
- Brand monitoring: detection of brand abuse

CMC TI tăng tốc độ phát hiện và thời gian phản hồi bằng vận hành threat intelligence và hợp nhất các công cụ bảo mật dưới một nền tảng:

- Centralizes all your threat intel data in one place
- Turns raw indicators into actionable intelligence
- Integrates with existing security investments
- Accelerates incident response time
- Makes security analysts more efficient

CMC TI đang sử dụng kết hợp nhiều nguồn IOC trên thế giới, bao gồm nguồn Threat Intelligence cung cấp public và 1 số nguồn thương mại như: Honeypot Checker, SHODAN, VirusTotal, IBM X-Force Exchange, MalwarePatrol, BotScout, Censys.io, Hunter.io, AlienVault OTX…