CÔNG TY CỔ PHẦN AN NINH AN TOÀN THÔNG TIN CMC – CMC INFOSEC
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.cmcinfosec.com
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.cmcinfosec.com

DỊCH VỤ XỬ LÝ SỰ CỐ AN NINH AN TOÀN THÔNG TIN

(INCIDENT RESPONSE)

Thành viên chính thức của AVAR và ICSA

CMC INFOSEC

CÔNG TY CỔ PHẦN AN NINH AN TOÀN THÔNG TIN CMC INFOSEC

Report No	**V1.0**
Date	03/01/2019
Document Type	Service Description

CMC INFOSEC

MỤC LỤC

1. Mô tả dịch vụ

Sự cố an ninh an toàn thông tin là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

Một số nhóm sự cố AN ATTT như sau (theo tiêu chuẩn quốc gia TCVN 11239:2015 ISO/IEC 27035:2011)

- **Truy cập trái phép:** bao gồm các hành động cố gắng để truy cập hoặc lợi dụng trái phép hệ thống, dịch vụ hoặc mạng để truy cập. Dưới đây là một số ví dụ về sự cố truy cập trái phép:
  - Các cố gắng lấy các tệp tin mật khẩu,
  - Các tấn công làm tràn bộ đệm để cố dành quyền
  - Sự khai thác các điểm yếu của giao thức để chiếm quyền hoặc làm sai hướng các kết nối hợp lệ,
  - Các cố gắng nâng cao đặc quyền hoặc thông tin vượt quá quyền của người dùng hoặc quản trị viên.
- **Tấn công từ chối dịch vụ:** là sự cố làm cho hệ thống, dịch vụ hoặc mạng không thể tiếp tục hoạt động với năng lực dự kiến, dẫn đến từ chối hoàn toàn các truy cập hợp lệ của người dùng. Dưới đây là một số ví dụ điển hình về các sự cố DoS/DDoS:
  - Ping các địa chỉ mạng quảng bá nhằm làm tràn băng thông mạng,
  - Gửi dữ liệu theo các định dạng không mong muốn đến một hệ thống, dịch vụ, hoặc mạng nhằm đánh sập hoặc làm gián đoạn hoạt động,
  - Mở nhiều phiên hợp lệ với một hệ thống, dịch vụ hoặc mạng nhất định

  Các cuộc tấn công như vậy thường được thực hiện thông qua các Botnet, đây là tập hợp của các rô bốt phần mềm (mã độc) chạy độc lập, tự động. Các Botnet có thể bao gồm hàng trăm đến hàng triệu máy tính. Trong phạm vi xử lý sự cố an ninh an toàn thông tin, CMC InfoSec sẽ không cung cấp việc xử lý liên quan đến loại tấn công từ chối dịch vụ này.
- **Mã độc, phần mềm độc hại:** Mã độc là một chương trình hoặc một phần của chương trình được đưa vào một chương trình khác với mục đích làm thay đổi tính năng ban đầu của chương trình đó nhằm thực hiện các hoạt động nguy hiểm như trộm cắp thông tin, phá hủy thông tin, từ chối dịch vụ, phát tán thư rác....

- **Khai thác và thu thập thông tin trái phép (Hacking):** bao gồm các hoạt động liên quan đến việc xác định các mục tiêu và tìm các dịch vụ hoạt động trên các mục tiêu đó. Đây là loại sự cố liên quan đến do thám, mục đích để xác định:
  - Sự tồn tại của một mục tiêu, các cấu trúc mạng quanh mục tiêu, và đối tượng mà mục tiêu thường xuyên liên lạc,
  - Các điểm yếu tiềm ẩn có thể khai thác được của mục tiêu hoặc quanh môi trường mạng của mục tiêu.

  Dưới đây là các ví dụ về tấn công thu thập thông tin:
  - Việc ping tới các địa chỉ mạng để tìm những những hệ thống còn "sống",
  - Việc thăm dò hệ thống nhằm xác định hệ điều hành,máy chủ…,
  - Việc quét các cổng mạng trên hệ thống nhằm xác định các dịch vụ liên quan và xác định phiên bản phần mềm của các dịch vụ này,
- **Rò rỉ dữ liệu:** Sự cố loại này xảy ra khi người dùng vi phạm các chính sách an toàn hệ thống thông tin của một tổ chức, dẫn đến các thông tin nội bộ bị lộ lọt ra bên ngoài.

Dịch vụ xử lý sự cố là hoạt động nhằm xử lý, khắc phục sự cố gây mất an ninh an toàn thông tin gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, và khôi phục hoạt động bình thường của hệ thống thông tin.

Bằng kinh nghiệm và nhân lực của CMC InfoSec, khách hàng sẽ rút ngắn tối đa thời gian bị ảnh hưởng do các sự cố AN ATTT gây ra. Khách hàng sẽ nhanh chóng xác định được nguyên nhân mức độ ảnh hưởng của sự cố.

2. Chức gói dịch vụ và SLA tương ứng

Dịch vụ xử lý sự cố bao gồm các gói sau:

Gói dịch vụ	Thời gian xử lý/năm	Thời gian có mặt tại KH	Đơn vị tính
Silver	200 giờ	24 tiếng (áp dụng trong nội thành Hà Nội)	Năm
Gold	350 giờ	12 tiếng (áp dụng trong nội thành Hà Nội)	Năm

Platinum	500 giờ	6 tiếng (áp dụng trong nội thành Hà Nội)	Năm
Custom	Tối thiểu 100 giờ	Cần thống nhất với khách hàng	Năm

Trong đó:

Thời gian xử lý được hiểu là thời gian tính từ lúc các chuyên viên xử lý của CMC InfoSec on-site có mặt tại trụ sở của khách hàng để thực hiện xử lý sự cố

Thời gian có mặt tại khách hàng là thời gian tính từ thời điểm tiếp nhận yêu cầu của khách hàng.

Thời gian xử lý được tính như sau:

Tier 1: tính hệ số 1

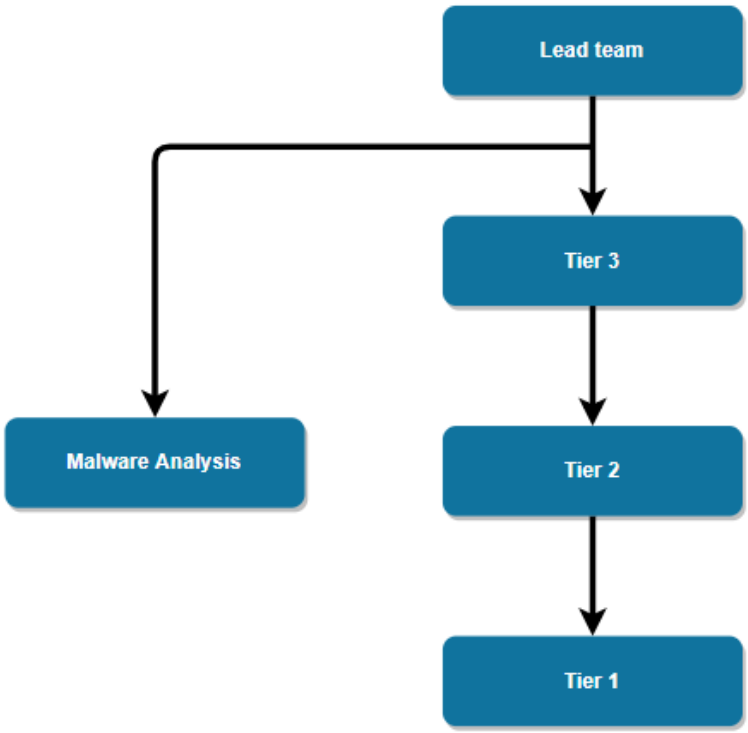
Tier 2: tính hệ số 1.5 (Tier 1 x 1.5)

Tier 3: tính hệ số 2.5 (Tier 1 x 2.5)

Ghi chú: đối với khách hàng đã sử dụng CMC SOC thì SLA như sau:

Gói dịch vụ	Thời gian xử lý/năm	Thời gian có mặt tại KH	Đơn vị tính
Silver	200 giờ	12 tiếng (áp dụng trong nội thành Hà Nội)	Năm
Gold	350 giờ	6 tiếng (áp dụng trong nội thành Hà Nội)	Năm
Platinum	500 giờ	3 tiếng (áp dụng trong nội thành Hà Nội)	Năm
Custom	Tối thiểu 100 giờ	Cần thống nhất với khách hàng	Năm

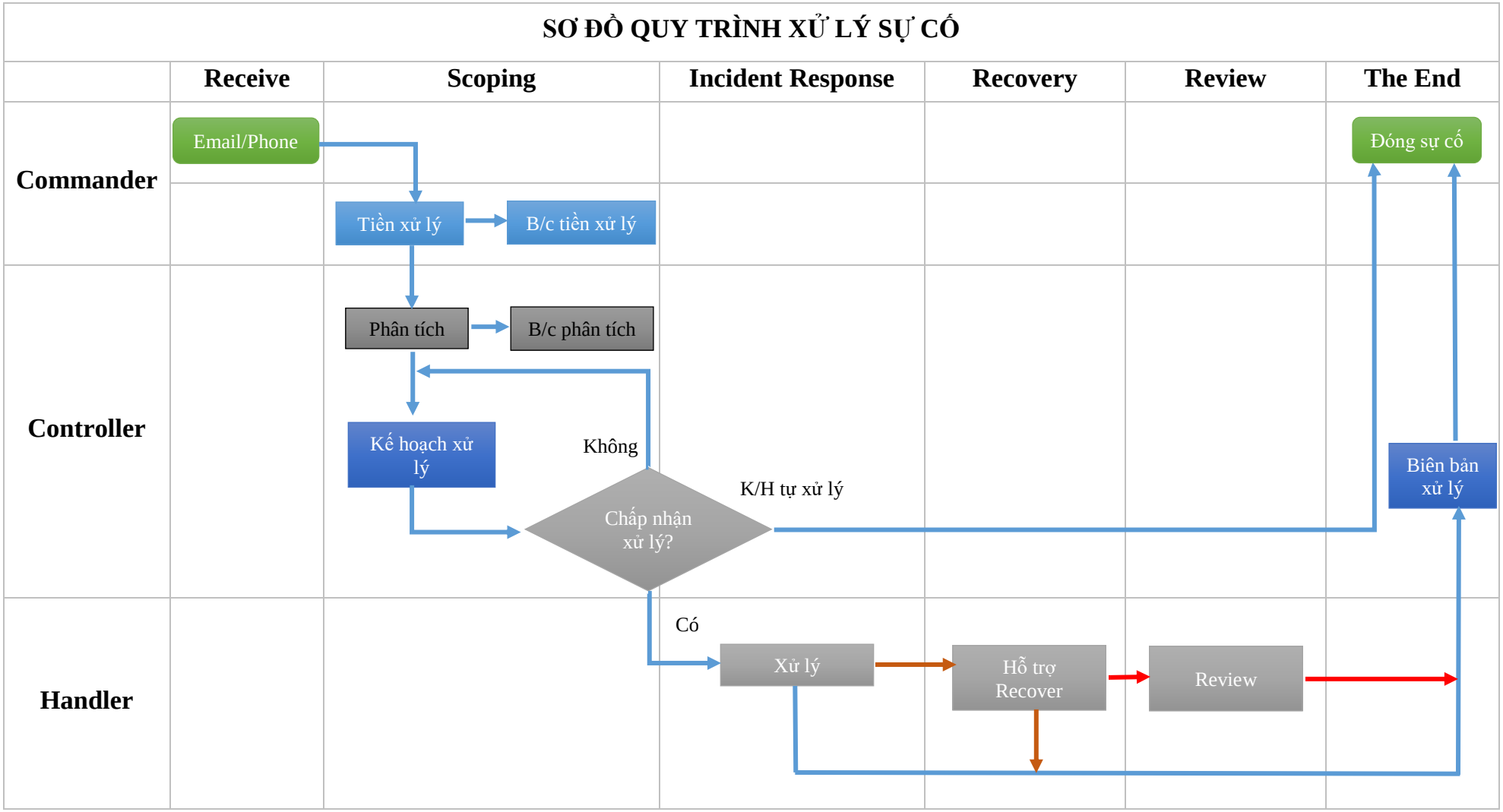
3. Cơ cấu nhân sự



Theo mô hình như trên, đội Incident Response Team (IR Team) gồm:

- Nhân sự Tier 3 (theo phân cấp đội SOC)
- Nhân sự Tier 2 (theo phân cấp đội SOC)
- Nhân sự Phân tích mã độc – Malware Analyst (phân cấp tương đương với Tier 2)
- Nhân sự Tier 1 (theo phân cấp đội SOC)

4. Quy trình dịch vụ



Chú thích:

: dành cho gói Silver

: dành cho gói Gold

: dành cho gói Platinum

Định nghĩa các pha công việc:

- **Receive**: Ở pha này, CMC InfoSec sẽ tiếp nhận các yêu cầu về xử lý sự cố an ninh an toàn thông tin qua email hoặc điện thoại.

- **Scoping**: Sau khi tiếp nhận yêu cầu từ khách hàng qua email/điện thoại, tại pha scoping bộ phận/nhóm Commander có trách nhiệm tiếp nhận các yêu cầu từ khách hàng dựa theo các kịch bản và khả năng chuyên môn, Commander sẽ thực hiện phân tích tiền xử lý trên những thông tin khách hàng cung cấp. Sau khi thực hiện tiền xử lý xong, bộ phận commander sẽ có trách nhiệm viết báo cáo tiền xử lý và chuyển cho Controller. Từ báo cáo tiền xử lý, bộ phận/nhóm Controller có trách nhiệm phân tích chuyên sâu vấn đề khách hàng gặp phải. Trong trường hợp các thông tin chưa đầy đủ, Controller có thể sẽ yêu cầu Commander trao đổi thêm với khách hàng xác minh thêm thông tin. Sau khi thông tin đầy đủ, Controller sẽ phân tích, đưa ra báo cáo phân tích và kế hoạch xử lý để gửi tới khách hàng. Ở giai đoạn này, Controller sẽ trực tiếp trao đổi với khách hàng về kế hoạch xử lý.
    - Trong trường hợp khách hàng tự xử lý sự cố, không theo kế hoạch của Controller, quy trình xử lý sẽ kết thúc.
    - Trong trường hợp khách hàng chưa chấp nhận kế hoạch xử lý, cần điều chỉnh, bổ sung thông tin hay cần thống nhất lại, Controller sẽ trao đổi trực tiếp với khách hàng để thực hiện điều chỉnh, thống nhất kế hoạch xử lý. Chu trình này sẽ được lặp lại cho đến khi kế hoạch xử lý được cả 2 bên thống nhất.
    - Trong trường hợp khách hàng đồng ý với kế hoạch xử lý, thì nhóm Handler sẽ thực hiện xử lý theo kế hoạch.

- **Incident Response**:

- Bộ phận Handler thực hiện công việc theo kế hoạch xử lý mà bộ phận Controller đã thống nhất với khách hàng.
- Trong quá trình xử lý, mọi vấn đề phát sinh nhóm Handler có trách nhiệm ghi nhận và báo cáo cho Controller trước khi có hành động phản ứng tiếp theo. Kết thúc quá trình xử lý, nhóm Handler sẽ có trách nhiệm viết biên bản xử lý và gửi lại khách hàng.

- **Recovery** (pha này chỉ áp dụng từ gói Gold, Platinum): Ở pha này, ngoài việc xử lý sự cố, nhóm Handler sẽ hỗ trợ khách hàng trong việc khôi phục hoạt động bình thường của hệ thống. Khách hàng sẽ trực tiếp khôi phục hệ thống, nhóm Handler chỉ đóng vai trò hỗ trợ và đưa khuyến nghị.

- **Review** (pha này chỉ áp dụng cho gói Platinum): sau khi hệ thống đã xử lý sự cố và khôi phục hoạt động bình thường, nhóm Handler sẽ có trách nhiệm kiểm tra, xác nhận lại toàn bộ các công việc và kết quả trong **kế hoạch xử lý** trước khi bàn giao lại cho khách hàng. Trong pha này, CMC InfoSec sẽ đưa ra các khuyến nghị/hành động nhằm tối ưu hệ thống (nếu có). Sau quá trình xử lý, khách hàng sẽ nhận được biên bản kết quả xử lý tương ứng với gói dịch vụ lựa chọn.

Mô tả vai trò các bộ phận:

- **Commander:** là bộ phận/nhóm tiếp nhận các thông tin sự cố từ phía khách hàng. Nhóm có trách nhiệm tiếp nhận thông tin, tiền xử lý các thông tin sự cố. Trong trường hợp các thông tin không đầy đủ để giải quyết sự cố hoặc cần hỗ trợ thêm để xử lý, nhóm này có trách nhiệm chuyển toàn bộ các thông tin tiếp nhận cho bộ phận xử lý cấp trên (controller)

- **Controller (Tier 3 trở lên)**: là bộ phận/nhóm phân tích, định hướng và điều phối xử lý. Nhóm này có trách nhiệm phân tích chi tiết các thông tin sự cố tiếp nhận, xác định phương hướng xử lý và chịu trách nhiệm điều phối cho toàn bộ quá trình xử lý sự cố. Để việc xử lý hiệu quả, nhóm này có thể yêu cầu khách

hàng bổ sung hoặc phối hợp bổ sung thông tin chi tiết về sự cố trong quá trình tiếp nhận và phân tích

- **Handler:** là bộ phân/nhóm trực tiếp phân tích và xử lý các sự cố. Thành viên nhóm này có thể bao gồm cả nhân viên kỹ thuật của CMC InfoSec và đội ngũ kỹ thuật của khách hàng. Nhóm này sẽ xử lý sự cố theo hướng dẫn và điều phối xử lý của Controller. Trong quá trình xử lý, mọi vấn đề phát sinh nhóm có trách nhiệm ghi nhận và báo cáo cho Controller trước khi có hành động phản ứng tiếp theo.

Dưới đây là ví dụ về quá trình xử lý một mã độc cụ thể, trong đó thể hiện việc luồng công việc phối hợp giữa CMC InfoSec và khách hàng. Lưu ý: đây chỉ là 1 ví dụ mang tính điển hình, tùy thực tế sự cố với các loại mã độc khác nhau có thể sẽ có phát sinh thêm các công tác xử lý khác mà CMC InfoSec sẽ đưa vào bản "Kế hoạch xử lý" trước khi thực hiện.

- **Pha monitor:**

Bước 1: Gửi thông báo sự cố

- CMC InfoSec gửi Thông báo sự cố cho đầu mối phụ trách của khách hàng qua email, nội dung bao gồm:
  - Threat nguy hiểm
  - Các thông tin liên quan để xác minh, làm rõ về thông báo sự cố
  - Khuyến nghị xử lý sơ bộ
- Khách hàng tiếp nhận **Thông báo sự cố**. Xem xét về các nội dung trong thông báo để xuất

Bước 2: Phản hồi thông báo sự cố:

- Khách hàng gửi mail xác nhận về tình trạng xử lý, trong 2 trường hợp:
  - Khách hàng đã tự xử lý xong
  - Khách hàng đang tự xử lý
- CMC InfoSec tiếp nhận email xác nhận từ khách hàng, tương ứng với 2 trường hợp trên:
  - Đóng thông báo sự cố và tiếp tục giám sát khi khách hàng đã tự xử lý xong
  - Tiếp tục giám sát để cập nhật hiện trạng khi Khách hàng đang tự xử lý

Lưu ý: Khách hàng xem xét và phải gửi mail xác nhận sự cố đúng theo thời gian SLA.

Trong trường hợp Khách hàng có thắc mắc, Khách hàng cần gửi mail yêu cầu làm rõ, trên cơ sở nội dung yêu cầu, trực tiếp Lead kỹ thuật sẽ trao đổi với Khách hàng để làm rõ các nội dung yêu cầu

- **Pha Receive:**

- Trong trường hợp Khách hàng không xử lý được trong email xác nhận về tình trạng xử lý sẽ yêu cầu CMC InfoSec hỗ trợ xử lý
- Khi nhận được yêu cầu xử lý của khách hàng, nhóm giám sát chuyển thông tin threat nguy hiểm cho Controller (trong mô hình dịch vụ Incident Response). Nếu khách hàng đã tự xử lý trước đó (nếu có), nhóm giám sát sẽ tiếp nhận toàn bộ thông tin về threat nguy hiểm, các thông tin về công việc mà khách hàng đã tự xử lý

- **Pha Scoping:**

Bước 1: Phân tích chuyên sâu

- CMC InfoSec (Controller) sẽ căn cứ trên các thông tin đã có, thực hiện:
    - Yêu cầu bổ sung thông tin cần thiết từ khách hàng (gọi điện hoặc gửi mail yêu cầu bổ sung thông tin)
    - Phân tích chuyên sâu threat nguy hiểm
- Khách hàng cung cấp các thông tin theo yêu cầu bổ sung thông tin từ phía CMC InfoSec

Bước 2: Lên kế hoạch xử lý

- CMC InfoSec (Controller) sẽ Lên **Kế hoạch xử lý** sự cố tương ứng; cung cấp cho khách hàng kế hoạch xử lý
- Khách hàng xem xét **Kế hoạch xử lý** mà CMC SOC đã cung cấp. Trong trường hợp khách hàng băn khoăn, cần làm rõ thì trao đổi trực tiếp với Controller của CMC SOC để thống nhất **Kế hoạch xử lý**

Bước 3: Thống nhất kế hoạch xử lý

- Khi khách hàng đồng ý kế hoạch xử lý, Controller sẽ chuyển **Kế hoạch xử lý** cho đội xử lý (Handler) để sang khách hàng xử lý.

- Trong trường hợp khách hàng quyết định tự xử lý hoặc không đồng ý với kế hoạch xử lý, case xử lý sự cố được đóng lại

- **Pha Incident Response:**

Bước 1: Xác nhận kế hoạch xử lý

- Nhóm Handler của CMC InfoSec mang **Kế hoạch xử lý** mà Controller đã thống nhất để ký xác nhận của khách hàng
- Khách hàng thực hiện ký xác nhận **Kế hoạch xử lý** trước khi đội xử lý thực hiện công việc xử lý

Bước 2: Kiểm tra các tiến trình và các kết nối độc hại trên máy tính cần xử lý

- Nhóm Handler của CMC InfoSec thực hiện:
    - Đăng nhập vào máy tính cần xử lý
    - Cài đặt và/hoặc chạy các công cụ hỗ trợ công việc
- Khách hàng có trách nhiệm:
    - Xác nhận việc cho phép CMC SOC đăng nhập vào máy tính cần xử lý và cung cấp tài khoản login phù hợp
    - Xác nhận việc cho phép CMC SOC cài đặt và/hoặc chạy các công cụ hỗ trợ công việc lên máy tính cần xử lý và cung cấp tài khoản admin hoặc các tài khoản khác có đủ quyền để sử dụng các tính năng của công cụ hỗ trợ

Bước 3: Gỡ bỏ các tiến trình độc hại trên máy tính cần xử lý

- Nhóm Handler của CMC InfoSec thực hiện:
    - Tắt các tiến trình độc hại và các tiến trình liên quan để disable tiến trình độc hại
    - Một số trường hợp sẽ cần cài thêm và chạy các công cụ hỗ trợ để gỡ bỏ
- Khách hàng thực hiện:
    - Xác nhận việc cho phép CMC InfoSec tắt các tiến trình và cung cấp tài khoản đủ quyền
    - Xác nhận việc cho phép CMC InfoSec cài đặt và chạy các công cụ hỗ trợ gỡ bỏ lên máy tính cần xử lý và cung cấp tài khoản đủ quyền để thực hiện công việc

Bước 4: Xóa bỏ các file, các tệp tin độc hại

- Nhóm Handler của CMC InfoSec thực hiện:

  - Xóa bỏ các file và các tệp tin độc hại liên quan
  - Một số trường hợp sẽ cần cài thêm các công cụ hỗ trợ để xóa bỏ
- Khách hàng thực hiện:
  - Xác nhận việc cho phép CMC InfoSec xóa bỏ các file và tệp tin từ máy tính cần xử lý và cung cấp tài khoản đủ quyền để thực hiện công việc
  - Xác nhận việc cho phép CMC InfoSec cài đặt và chạy các công cụ hỗ trợ xóa bỏ file và tệp tin lên máy tính cần xử lý và cung cấp tài khoản đủ quyền để thực hiện công việc

Bước 5: Cập nhật bản vá

- Nhóm Handler của CMC InfoSec thực hiện:
  - Cung cấp cho khách hàng bản vá tương ứng cho lỗ hổng đã được xác định (nếu có)
  - Trong trường hợp không có bản vá, cung cấp hướng thiết lập phòng chống phù hợp (nếu có). Khi đó, nhóm Handler cần thông báo tình hình cho Controller để đề xuất phương án phù hợp, Controller gửi mail cho khách hàng xác nhận thay đổi (nếu cần)
- Khách hàng thực hiện cài đặt bản vá

Lưu ý: CMC InfoSec (nhóm Handler) chỉ Thực hiện theo phạm vi công việc trong Kế hoạch xử lý. Với các trường hợp phát sinh, đội xử lý cần xác nhận nguyên nhân, báo cáo Controller để xin ý kiến xử lý tiếp.

Các bước xử lý trong Usecase này đang áp dụng cho 1 trường hợp cụ thể của CMC InfoSec, không mang tính chất quy trình chung cho mọi hoạt động xử lý mã độc. Tùy theo tình hình và hiện trạng thực tế, các bước xử lý có thể thay đổi để phù hợp. Do đó, **Kế hoạch xử lý** là tài liệu hỗ trợ xử lý quan trọng và riêng biệt cho từng case xử lý thực tế

- **Pha Recovery** (Phục hồi hoạt động bình thường của hệ thống)

- Ở pha này, CMC InfoSec (nhóm Handler) thực hiện đưa hoạt động của hệ thống trở về bình thường khi chưa bị nhiễm mã độc đã được xác định
  - Kết nối mạng
  - Tiến trình
  - Registry
  - Service

- **Pha Review** (Tái kiểm tra và xác nhận)
- CMC InfoSec (nhóm Handler) xác nhận các tiến trình độc hại hoặc kết nối độc hại của mã độc đã xác định không còn.
- Khách hàng phối hợp kiểm tra cùng CMC InfoSec (nếu cần)
- **Pha The End** (Kết thúc và lập báo cáo xử lý)
- CMC InfoSec (nhóm Handler) thực hiện:
    - Bổ sung các công việc xử lý (bao gồm các phát sinh và công việc thay đổi trong quá trình xử lý) vào **Báo cáo xử lý**
    - Ký xác nhận và yêu cầu chữ ký xác nhận từ khách hàng vào **Báo cáo xử lý**
- Khách hàng kiểm tra **Báo cáo xử lý** và ký xác nhận

5. Phạm vi cung cấp dịch vụ

Dịch vụ này được cung cấp trên phạm vi:

- Các máy chủ:
    - Máy chủ ứng dụng
    - Máy chủ cơ sở dữ liệu
    - Máy chủ web server
    - Máy chủ chia sẻ file
    - Máy chủ Proxy
    - Máy chủ DNS
    - Máy chủ AD
    - Máy chủ email
    - Máy chủ vật lý
- Máy trạm:
    - Máy trạm Windows (tất cả các phiên bản win 7 trở lên)
    - Máy trạm Linux, Unix, Solaris, AIX
    - Máy trạm MAC (tất cả các phiên bản)
- Thiết bị mạng: Switch, Router, Firewall

Dịch vụ này không bao gồm việc khôi phục dữ liệu.

6. Các yêu cầu khách hàng phối hợp

- Cung cấp các tài khoản đặc quyền phù hợp để thực hiện xử lý sự cố an ninh an toàn thông tin
- Hỗ trợ CMC InfoSec trong việc thu thập log, thu thập mẫu mã độc trong trường hợp được yêu cầu
- Ngoài ra với từng trường hợp cụ thể, các chuyên viên phụ trách kỹ thuật của CMC InfoSec sẽ gửi các yêu cầu hỗ trợ riêng.