

# **BÁO CÁO CHIA SẺ VỀ TÌNH HÌNH AN TOÀN, AN NINH MẠNG VÀ MỘT SỐ THỦ ĐOẠN TẤN CÔNG MẠNG MỚI**

**Báo cáo viên: TRẦN THÁI ĐỨC - CÔNG TY AN MẠNG VIETTEL**

**Chuyên gia An ninh mạng**

**(Kinh nghiệm: 15 năm, 12 năm phụ trách công tác  
đảm bảo dịch vụ CNTT tại Văn phòng Chính phủ.)**

**ĐT: 098.68.48.208 – email: ductt7@viettel.com.vn**

# RANSOMWARE

**Những điều cần biết về các mã độc tống tiền (Ransomware...), nhận diện dấu hiệu bị tấn công và giải pháp phòng, chống**

# NỘI DUNG

01

Bối cảnh tấn công Ransomware

02

Ransomware là gì?

03

Giải pháp phòng chống (Phòng chống chủ động)



# Báo cáo thống kê từ Cục An toàn thông tin

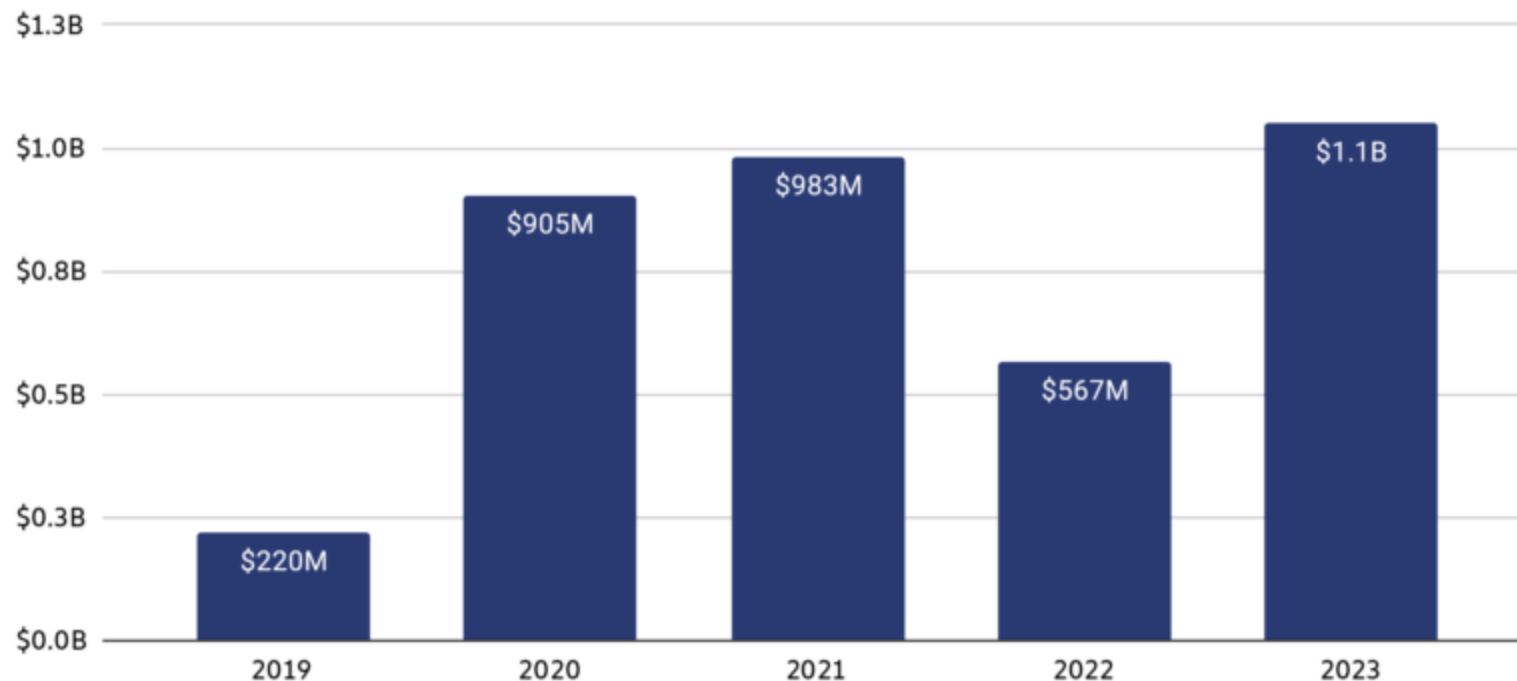


**Ransomware**

**2.323** Cuộc tấn công trong 3 tháng  
đầu năm 2024

**BÁO  
ĐỘNG**

## Total value received by ransomware attackers, 2019 - 2023





TIN TỨC

TÀI CHÍNH

CHỨNG KHOÁN

NGÂN HÀNG

BẢO HIỂM

THẾ GIỚI

THỊ TRƯỜNG TÀI CHÍNH TV

Chủ tịch VNDirect cho biết, thời điểm kết nối giao dịch lại vào sáng ngày 1/4/2024 cũng là lần đầu tiên bà cùng đội ngũ công ty "chảy nước mắt vì sung sướng và biết ơn". "Chúng tôi thiệt hại thật sự rất lớn cả về kinh tế lẫn uy tín. Nhưng nó không lãng phí, vì chúng tôi đã học ra được rất nhiều bài học quý báu trong quá trình này," bà Hương nói.

Trong nguyên một tuần giao dịch hệ thống VNDirect bị "treo", nhà đầu tư mở tài khoản tại công ty chứng khoán này không thể đặt lệnh, mua bán chứng khoán hay thực hiện bất cứ dịch vụ nào trên tài khoản của họ. Sự cố của VNDirect ảnh hưởng nhiều nhất tới các nhà đầu tư giao dịch chứng khoán phái sinh và sử dụng dịch vụ vay ký quỹ, bởi chịu tác động lớn từ biến động chỉ số và giá cổ phiếu. May mắn là trong tuần giao dịch đó, thị trường chứng khoán Việt Nam không có nhiều biến động mạnh.

Nhằm khắc phục phần nào những tổn thất cho khách hàng, VNDirect đã xây dựng chính sách hỗ trợ cho nhà đầu tư sở hữu tài khoản đầu tư và giao dịch chứng khoán tại công ty, bao gồm: Miễn phí giao dịch chứng khoán cơ sở trong tháng 4/2024, miễn toàn bộ lãi suất cho vay giao dịch ký quỹ từ ngày 25/3 đến ngày hệ thống giao dịch trở lại, miễn lãi nợ thấu chi và phí quản lý vị thế qua đêm với giao dịch chứng khoán phái sinh từ ngày 25/3 đến ngày hệ thống giao dịch trở lại, áp dụng lãi suất cho vay giao dịch ký quỹ 9,3% trong tháng 4/2024.

Với sản phẩm trái phiếu trong tháng 4/2024, VNDirect gia hạn các giao dịch trả lại và giữ nguyên lãi suất được hưởng, áp dụng mức tặng lãi suất tối đa 0,7% cho tất cả các kỳ hạn đối với Khách hàng có phát sinh giao dịch sản phẩm Dbond.



Số tham chiếu	320S23712UTDBJHF
Tài khoản	104000558756 N [REDACTED] [REDACTED] CHONG
Đến tài khoản	375045928 HA [REDACTED] [REDACTED] [REDACTED] NH TMCP [REDACTED] E VIET NAM
Số tiền giao dịch	-199,999,000 VND
Kênh giao dịch	78 - Retail Internet Banking
Thông tin giao dịch	CT DI:320416955707 [REDACTED] 258
Thời gian	23/07/2023 16:35:39

 Chia sẻ

Tổng tiền đã chuyển (bị lừa đảo):

13568000 + 59600000 + 99999000 + 139999000 + 79999000 + 100000000 +  
239996854 + 200000000 + 200000000 + 199999000 = **1.333.160.854 VNĐ**  
(Một tỷ ba trăm ba mươi ba triệu một trăm sáu mươi nghìn tám trăm năm tư  
Việt nam đồng)





- Tội phạm có tổ chức toàn cầu
- Nguồn lực lớn
- Trình độ ATTT chuyên sâu

# NỘI DUNG

01

Bối cảnh tấn công Ransomware

02

Ransomware là gì?

03

Giải pháp phòng chống (Phòng chống chủ động)





Ransomware là tấn công gì?

Báo cáo sếp,  
vừa rồi chúng ta không  
bị tấn công Ransomware

# Ransomware

- ❑ **Ransomware:** Là phần mềm gián điệp hay phần mềm tống tiền
  - Được thiết kế để mã hóa dữ liệu và yêu cầu tiền chuộc để giải mã
  - Có 2 loại Ransomware điển hình: **Locker Ransomware** (Khóa máy tính từ chối truy cập) & **Crypto Ransomware** (Mã hóa dữ liệu)
  - Xâm nhập vào các mục tiêu: PC, Thiết bị IoT, Thiết bị di động, các thiết bị trên mạng.





# Ransomware mã hóa (Encrypting)

❑ Mã hóa dữ liệu (tệp tin và thư mục) của người dùng.

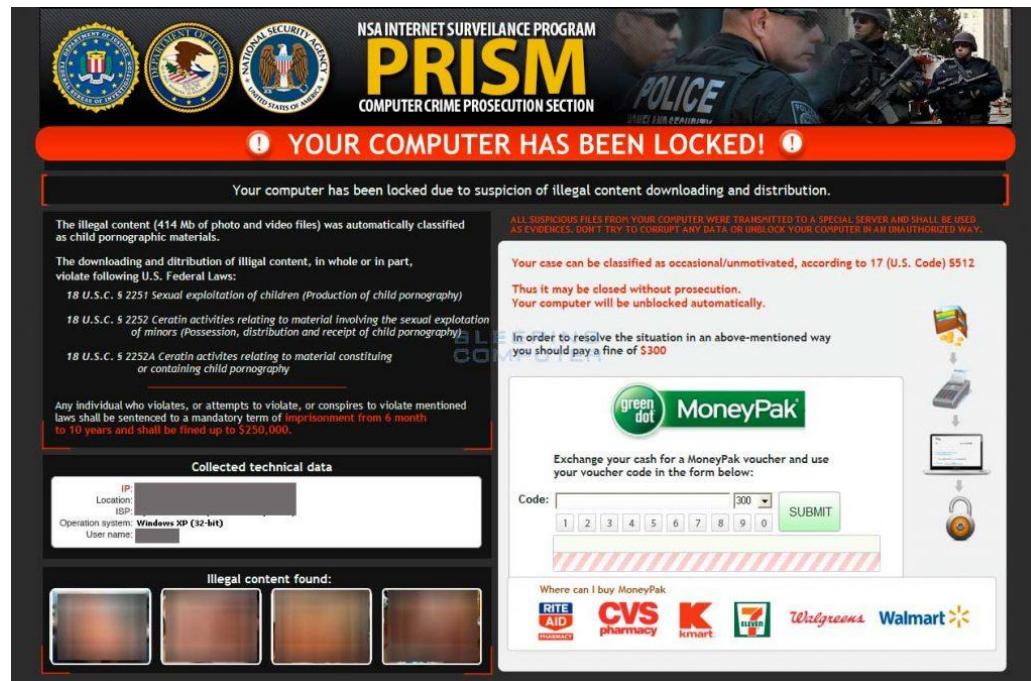
➡ Yêu cầu tiền chuộc



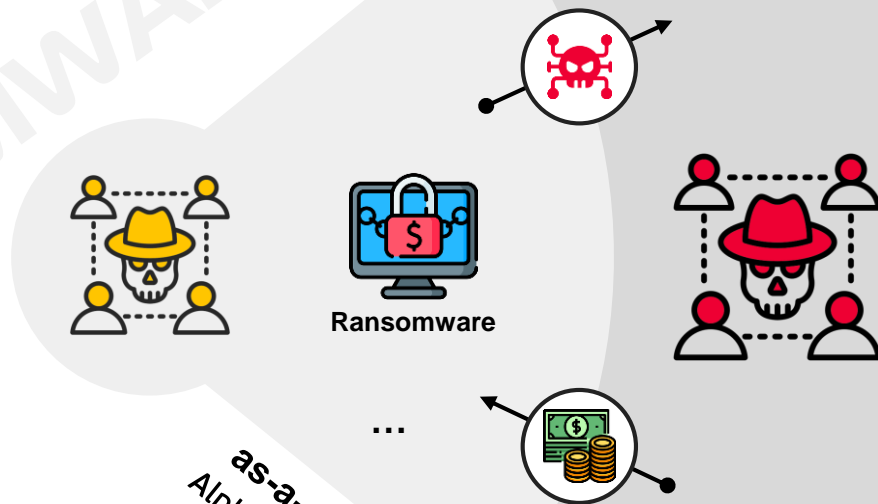
# Locker Ransomware

- ❑ Khóa và chặn người dùng sử dụng thiết bị.

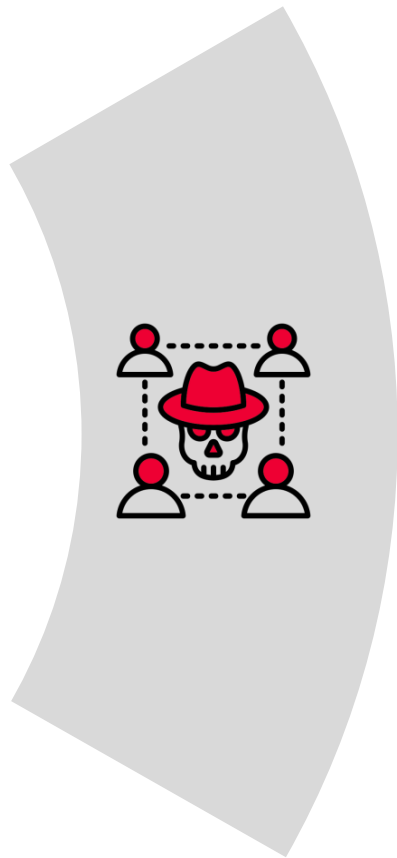
➡ Yêu cầu tiền chuộc



# Động cơ tấn công



# Đối tượng tấn công



• Mã hóa dữ liệu - Đe dọa - tống tiền  
(Ransomware)



**viettel**  
security

Cá nhân,  
người dùng  
cuối



Tổ chức doanh  
nghiệp tư nhân,  
BFSI, GOV



Đơn vị ngành  
trọng yếu

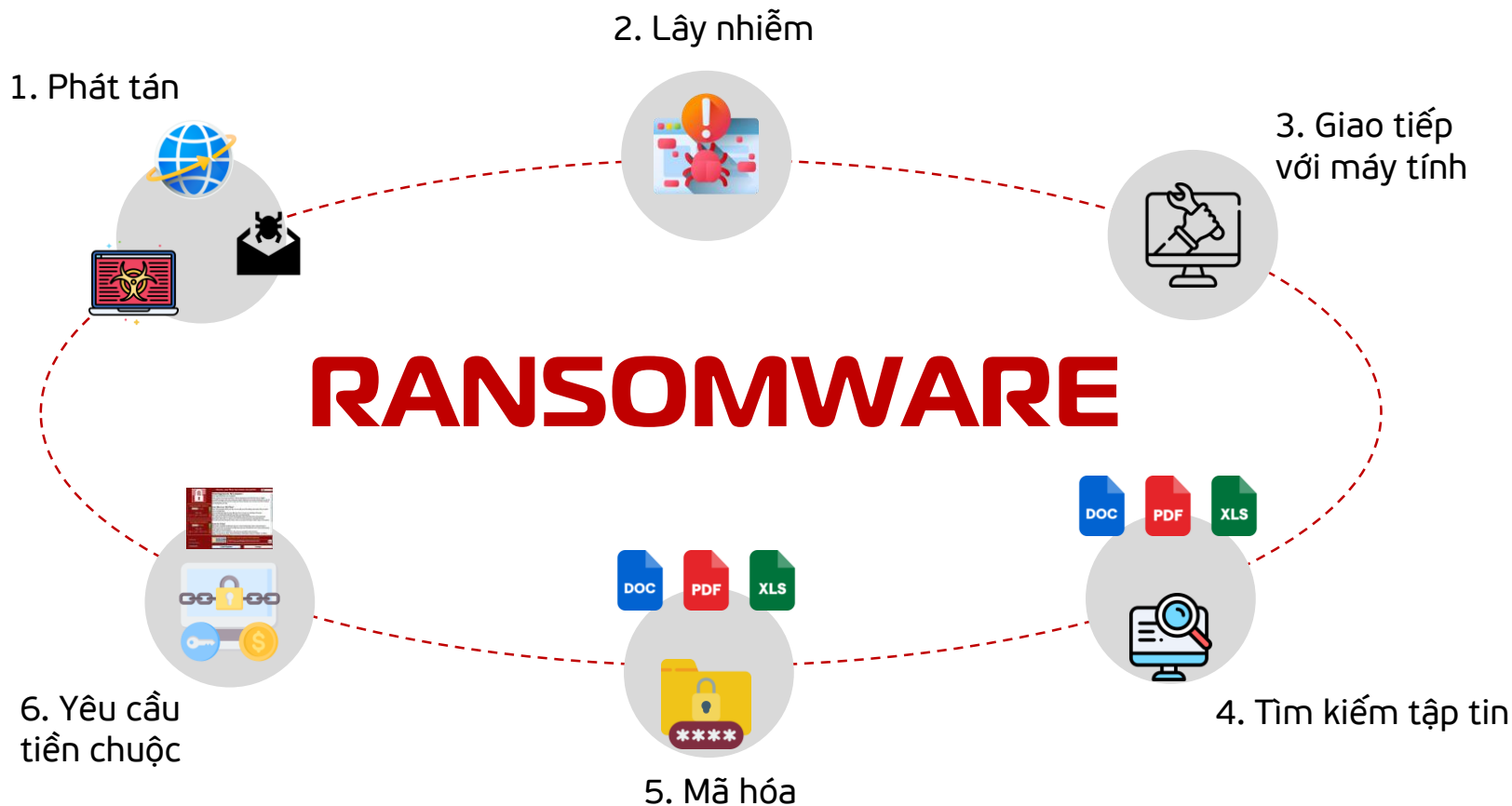




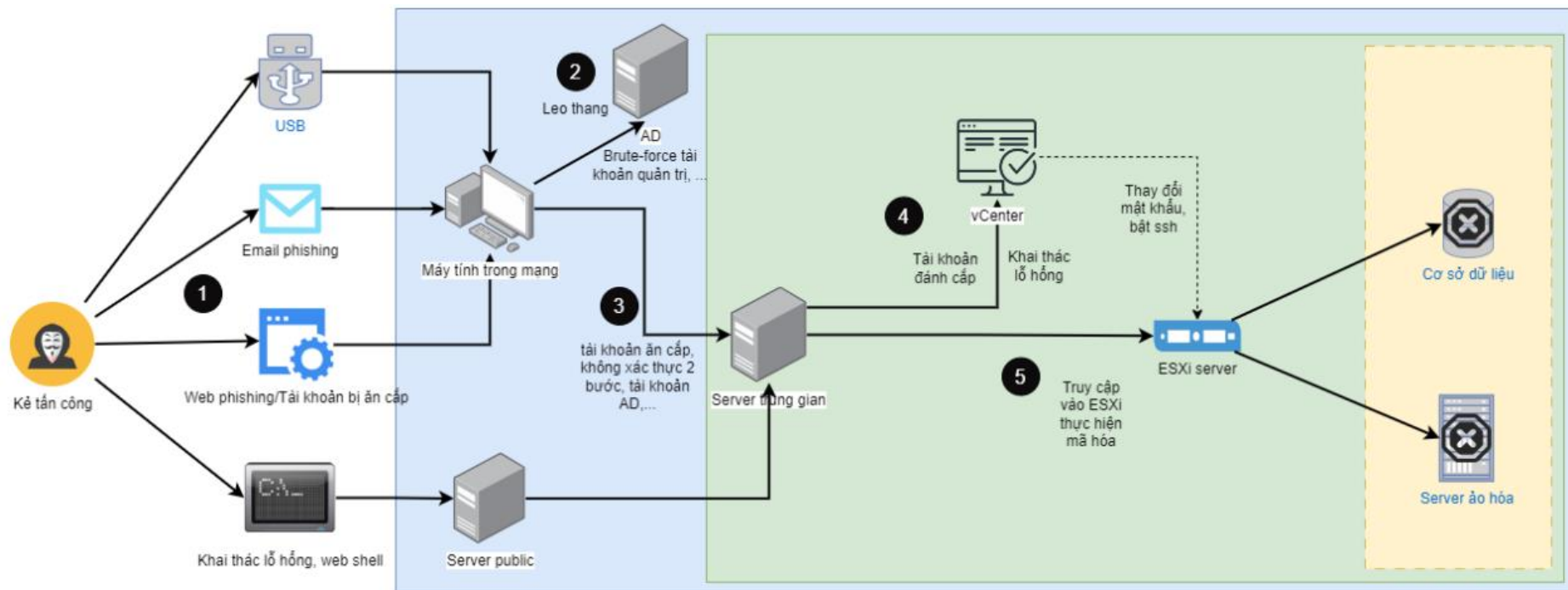
# Con đường xâm nhập



# Cơ chế hoạt động



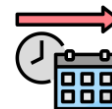
# Kịch bản tấn công





**Trước mắt**

- ☐ Bị mã hóa dữ liệu
- ☐ Gián đoạn dịch vụ, hoạt động kinh doanh
- ☐ Thất thoát tài chính
- ☐ Ảnh hưởng đến uy tín của tổ chức



**Lâu dài**

- ☐ Mã độc vẫn còn tồn tại trong hệ thống, có thể tấn công tiếp bất cứ lúc nào
- ☐ Điểm yếu để các nhóm tấn công khác nhắm vào
- ☐ Mất mát tài chính kéo dài:
  - Tiền chuộc
  - Chi phí khôi phục hệ thống
- ☐ Bị lộ lọt thông tin, dữ liệu cá nhân của khách hàng => hậu quả về pháp lý



# NỘI DUNG

01

Bối cảnh tấn công Ransomware

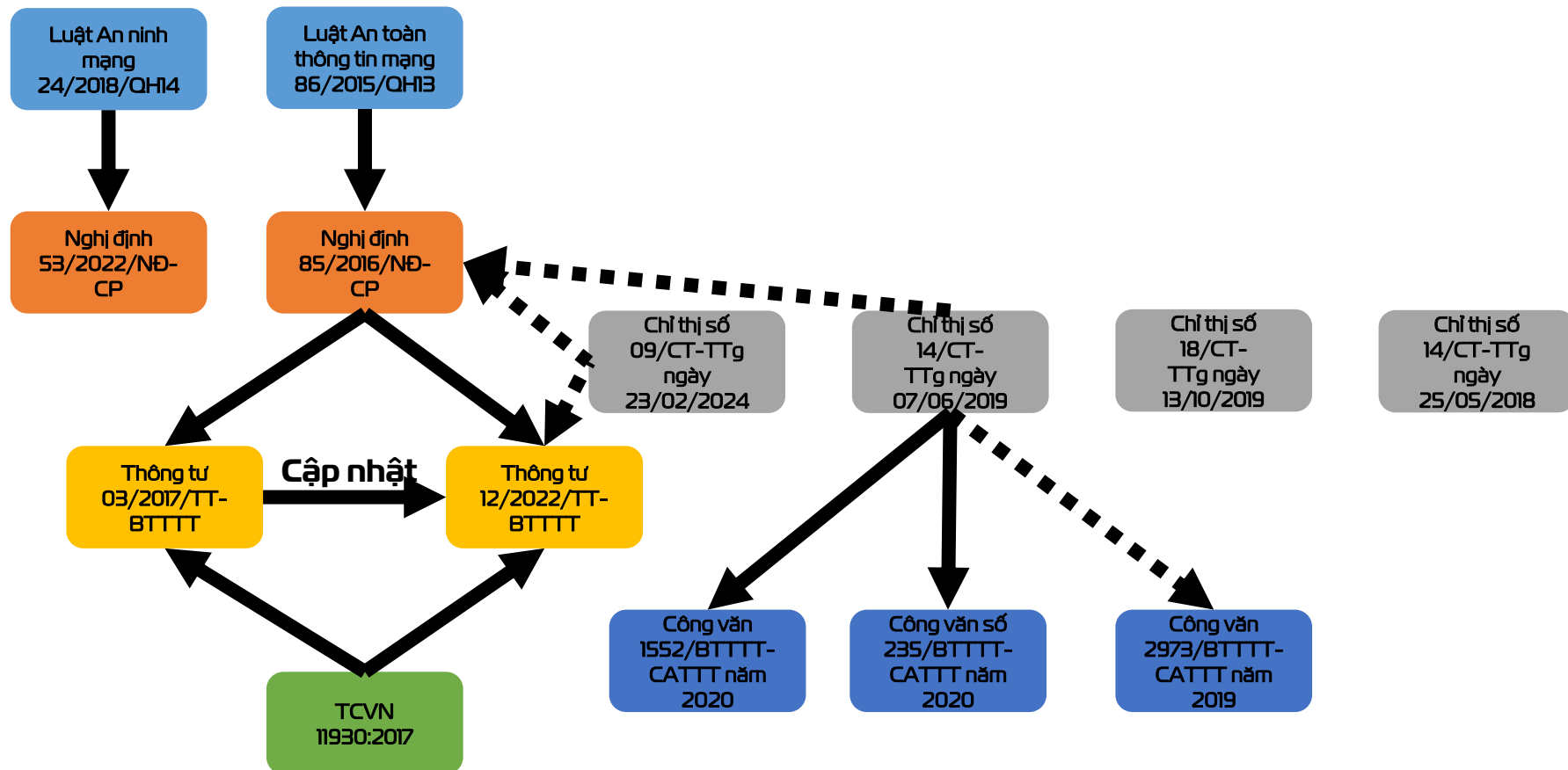
02

Ransomware là gì?

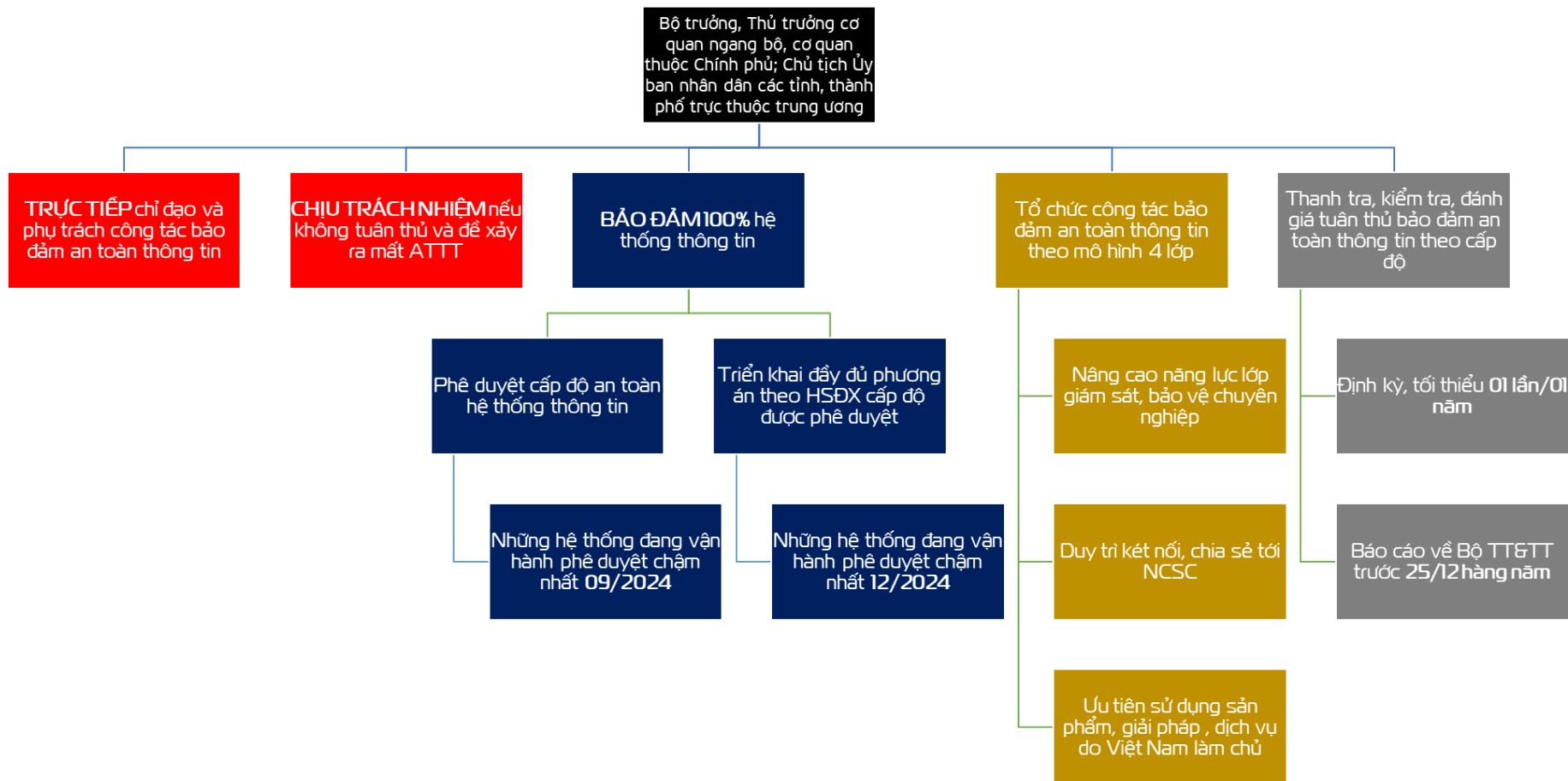
03

Giải pháp phòng chống (Phòng chống chủ động)





# Chỉ thị số 09/CT-TTg ngày 23/02/2024



Bộ trưởng, Thủ trưởng cơ quan ngang bộ, cơ quan thuộc Chính phủ; Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương

**TRỰC TIẾP** chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin

**CHIU TRÁCH NHIỆM** nếu không tuân thủ và để xảy ra mất ATTT

Chỉ đạo tổng rà soát, đánh giá tình hình bảo đảm ATTT thuộc phạm vi quản lý

Thực hiện nghiêm thời hạn hoàn thành phê duyệt HSĐXCĐ theo Chỉ thị 09

Sử dụng các nền tảng hỗ trợ bảo đảm ATTT của Bộ TT&TT cung cấp

Bố trí hạng mục ATTT khi triển khai kế hoạch ứng dụng CNTT, đảm bảo tối thiểu 10% tổng kinh phí



# Cẩm nang Phòng chống, giảm thiểu rủi ro từ tấn công RANSOMWARE – Cục ATTT

1. Xây dựng kế hoạch sao lưu, phục hồi dữ liệu với hệ thống, thông tin quan trọng (Quy tắc 3-2-1)

2. Triển khai các biện pháp xác thực mạnh cho các tài khoản truy cập hệ thống (2FA, MFA)

3. Thực hiện phân vùng truy cập mạng chặt chẽ

4. Áp dụng nguyên tắc đặc quyền tối thiểu cho các hệ thống

5. Rà quét, cập nhật bản vá lỗ hổng ATTT trên các thiết bị, phần mềm, ứng dụng

6. Hạn chế sử dụng các dịch vụ điều khiển máy tính từ xa

7. Giám sát liên tục phát hiện sớm các hành vi xâm nhập

8. Chủ động tìm kiếm dấu hiệu tấn công, rà quét mã độc, yêu cầu đơn vị chuyên trách xử lý

9. Xây dựng kế hoạch ứng phó sự cố để kịp thời phản ứng với Ransomware

# Biện pháp bảo vệ



## Ngắn hạn, ngay lập tức



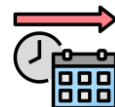
Người dùng cuối

Doanh nghiệp



- ✓ Cập nhật phần mềm Windows
- ✓ Cài đặt phần mềm AV bản quyền
- ✓ Không truy cập link lạ qua email
- ✓ Không truy cập trang web độc hại, quảng cáo
- ✓ Không cắm usb từ các nguồn không xác định

- ✓ Cô lập hệ thống/máy tính bị nhiễm để tránh lây lan và xử lý
- ✓ Phục hồi dữ liệu từ bản sao lưu
- ✓ Rà quét, loại bỏ ransomware và hardening cho toàn bộ hệ thống/máy chủ



## Kế hoạch dài hạn



Người dùng cuối

Doanh nghiệp



- ✓ Đào tạo thường xuyên về kiến thức an ninh thông tin
- ✓ Cập nhật phần mềm trên máy tính định kỳ

- ✓ Tách biệt các vùng mạng riêng biệt
- ✓ Triển khai hệ thống giám sát ATTT liên tục 24/7 (SOC)
- ✓ Backup thường xuyên (theo mô hình 3-2-1)
- ✓ Rà soát ATTT định kỳ cho máy tính, máy chủ, hệ thống CNTT
- ✓ Cập nhật các thông tin tình báo an ninh mạng để nhận biết sớm nguy cơ

## Compromise Assessment

*Đánh giá xâm nhập hệ thống, điều tra số, tư vấn, khuyến nghị biện pháp gia cố*

## SOC

*Triển khai hệ thống giám sát ATTT liên tục 24/7 (SOC)*

## Pentest/Audit

*Kiểm tra, đánh giá ATTT định kỳ (ít nhất 1 năm/ 1 lần) hệ thống CNTT*

## Endpoint Security

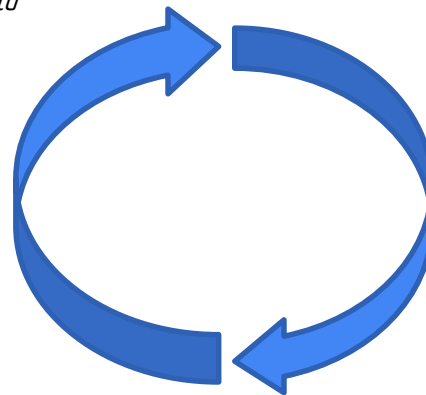
*Triển khai giải pháp bảo vệ thiết bị đầu cuối toàn diện cho tất cả các máy trạm người dùng*

## Anti-DDoS + WAF on Cloud

*Giải pháp bảo vệ phòng chống tấn công cho các ứng dụng công khai*

## Đào tạo

*Đào tạo nhận thức ATTT cho người dùng*



# Rà soát kiểm tra đánh giá ATTTT



## Compromise Assessment

- Đánh giá xâm nhập: rà soát, xác định khả năng hệ thống bị xâm nhập, chiếm quyền
- Xử lý sự cố ATTTT: điều tra, phản ứng với hệ thống bị xâm nhập bao gồm điều tra số, phân tích mã độc, xây dựng phương án ngăn chặn, loại bỏ sự xâm nhập
- Tư vấn bảo mật: khuyến nghị các biện pháp cụ thể trong ngắn hạn, dài hạn để gia cố, tăng cường ANTT cho hệ thống
- VCS CA:
  - o Chuyên gia bảo mật thế giới
  - o Công cụ sẵn tìm chuyên nghiệp
  - o Loại bỏ hoàn toàn



## Security Audit

- Xác định, đánh giá rủi ro lỗ hổng bảo mật trong hạ tầng: thiết bị mạng, thiết bị bảo mật, ...
- Xác định lỗ hổng, đánh giá rủi ro, siết chặt chính sách trên các hệ thống quan trọng AD, Email, hạ tầng ảo hóa (VMWare, ...)
- VCS SA:
  - o 15+ năm kinh nghiệm đánh giá
  - o Chuyên gia bảo mật
  - o Quy trình tiêu chuẩn thế giới



## Penetration Testing

- Kiểm thử xâm nhập hệ thống, ứng dụng, mạng
- Mô phỏng tấn công thực tế, phát hiện lỗ hổng, khuyến nghị khắc phục
- VCS Pentest:
  - o Chuyên gia bảo mật thế giới
  - o Kịch bản tấn công thực tế, chuyên sâu
  - o Khuyến nghị chi tiết, cụ thể

# Giải pháp Viettel Anti-DDoS – Phòng chống tấn công từ chối dịch vụ trên đường truyền



## TỰ ĐỘNG PHÁT HIỆN TẤN CÔNG DDOS

Bằng việc phân tích dữ liệu Netflow từ mạng lưới, hệ thống **tự động phát hiện** các tấn công DDoS xảy ra trên toàn mạng lưới của Viettel



## TỰ ĐỘNG XỬ LÝ CÁC CUỘC TẤN CÔNG DDOS

**Tự động** xử lý tấn công DDoS mà không cần sự can thiệp của con người



## GỬI CẢNH CẢNH BÁO REALTIME KHI CÓ TẤN CÔNG

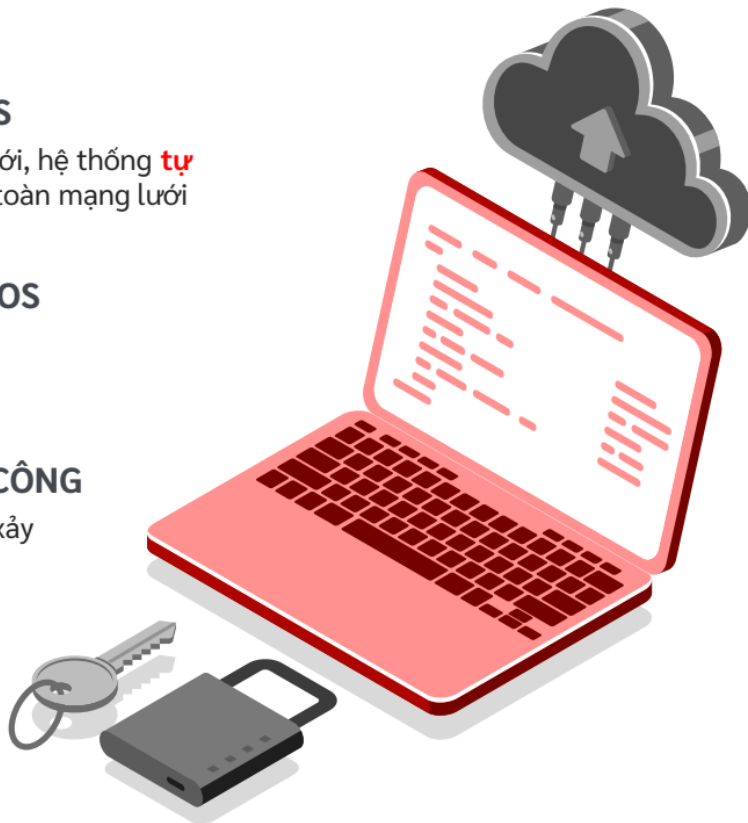
Giám sát liên tục, gửi **cảnh báo tức thì** ngay khi tấn công xảy ra qua các hình thức như Email, SMS hoặc Portal giám sát



## ĐA DẠNG CÁC HÌNH THỨC XỬ LÝ TẤN CÔNG

Hỗ trợ **nhiều phương pháp** để giảm thiểu tấn công

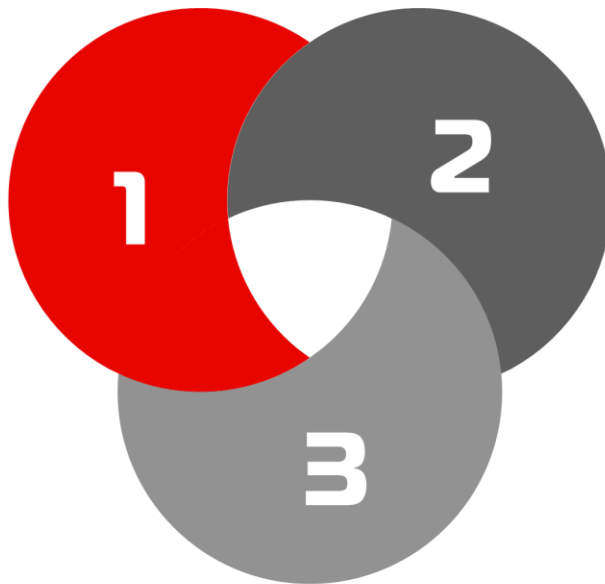
- Drop traffic
- Lái qua Scrubber
- BGP Flowspec



# Giải pháp Cloudrity – Bảo vệ toàn diện website và ứng dụng trực tuyến

## Chống tấn công DDoS tầng mạng (L4)

Chống tấn công dạng Volume-based  
Chống tấn công dạng Malform  
Chống tấn công lên đến hàng trăm Gbps



## Tường lửa ứng dụng WAF (Web Application Firewall)

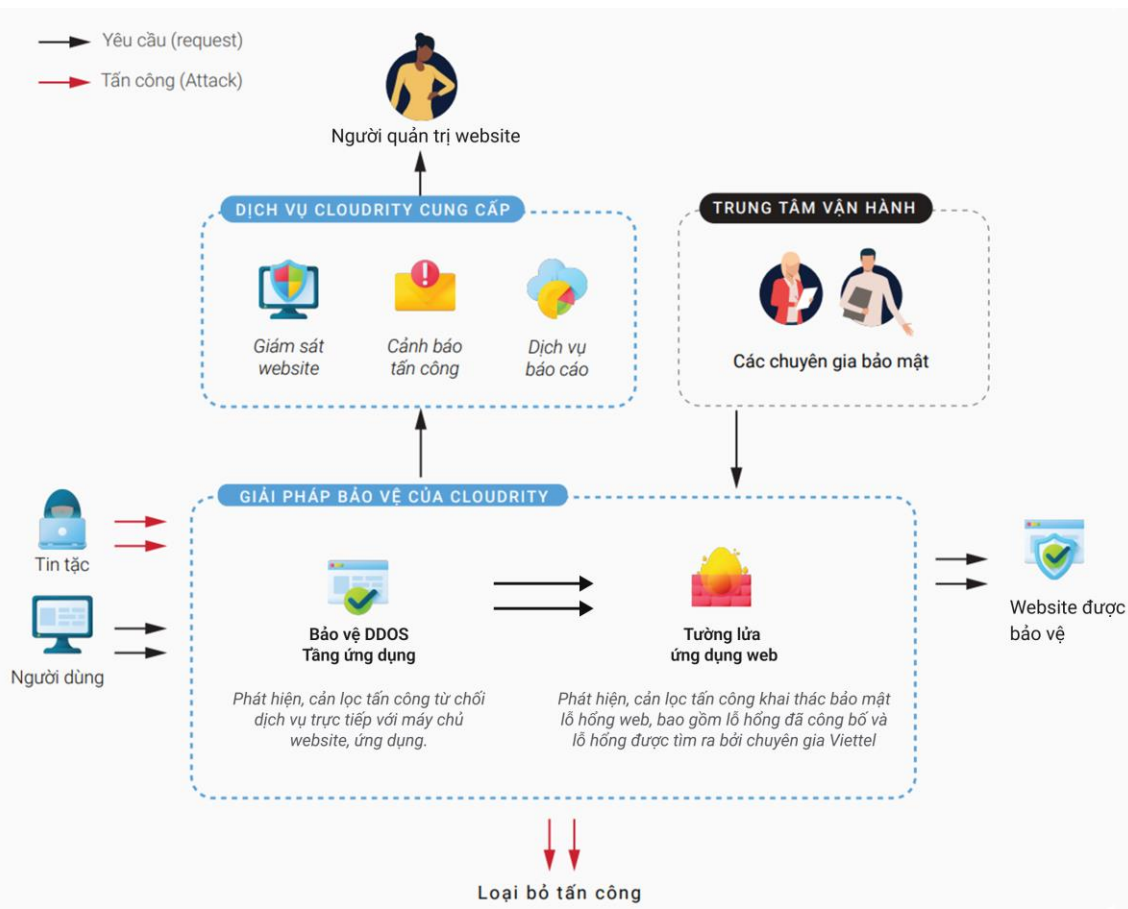
Chống tấn công thuộc Top 10 OWASP  
Chống tấn công khai thác lỗ hổng 1-day  
Rule tùy chỉnh chặn theo nhu cầu

## Chống tấn công DDoS tầng ứng dụng (L7)

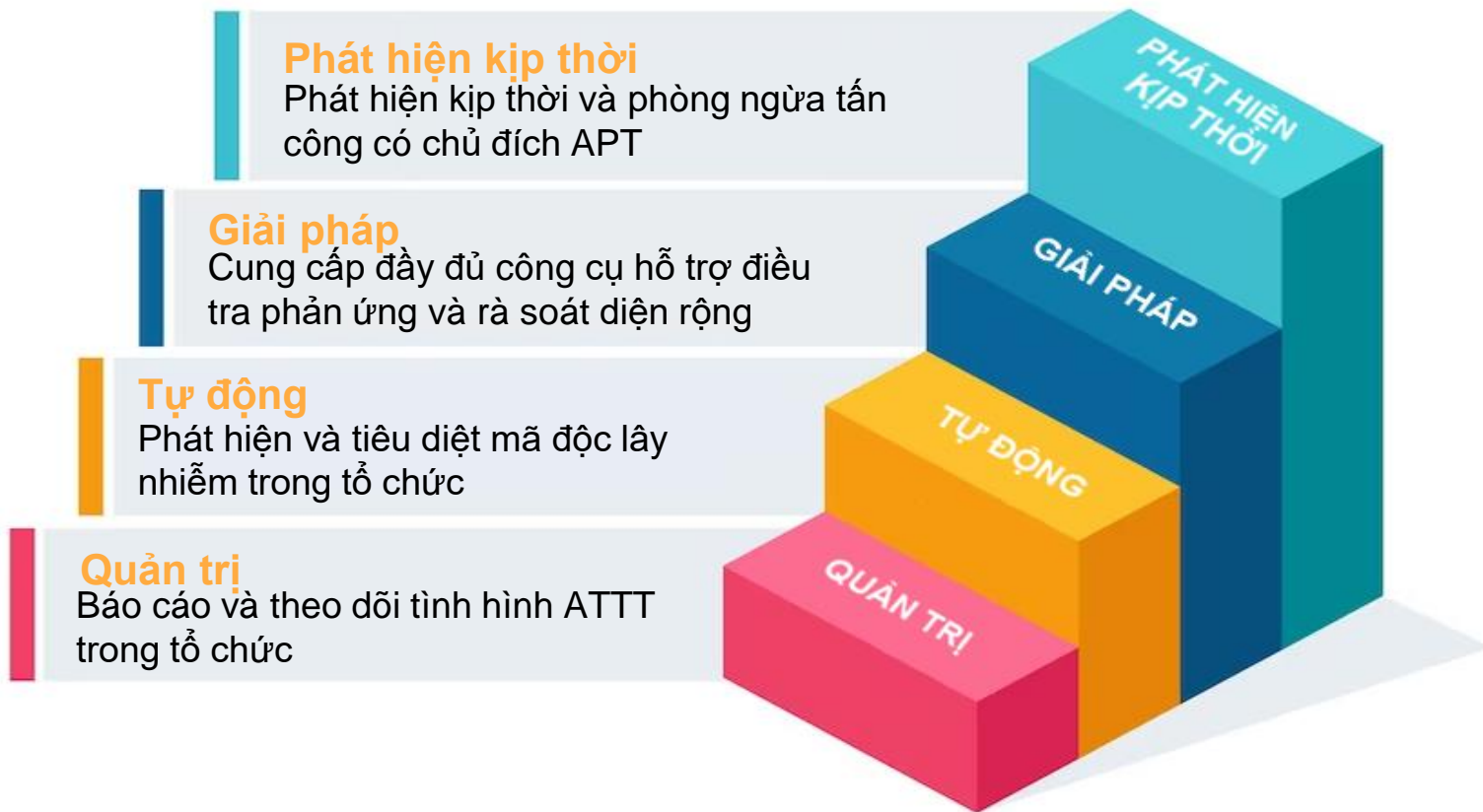
Chống tấn công dạng HTTP Flood, rate limit theo source IP / geo location  
Chống tấn công dạng Slow (Slow POST, Slow loris)  
Ngăn chặn bot request đến website với cookie, captcha challenge.



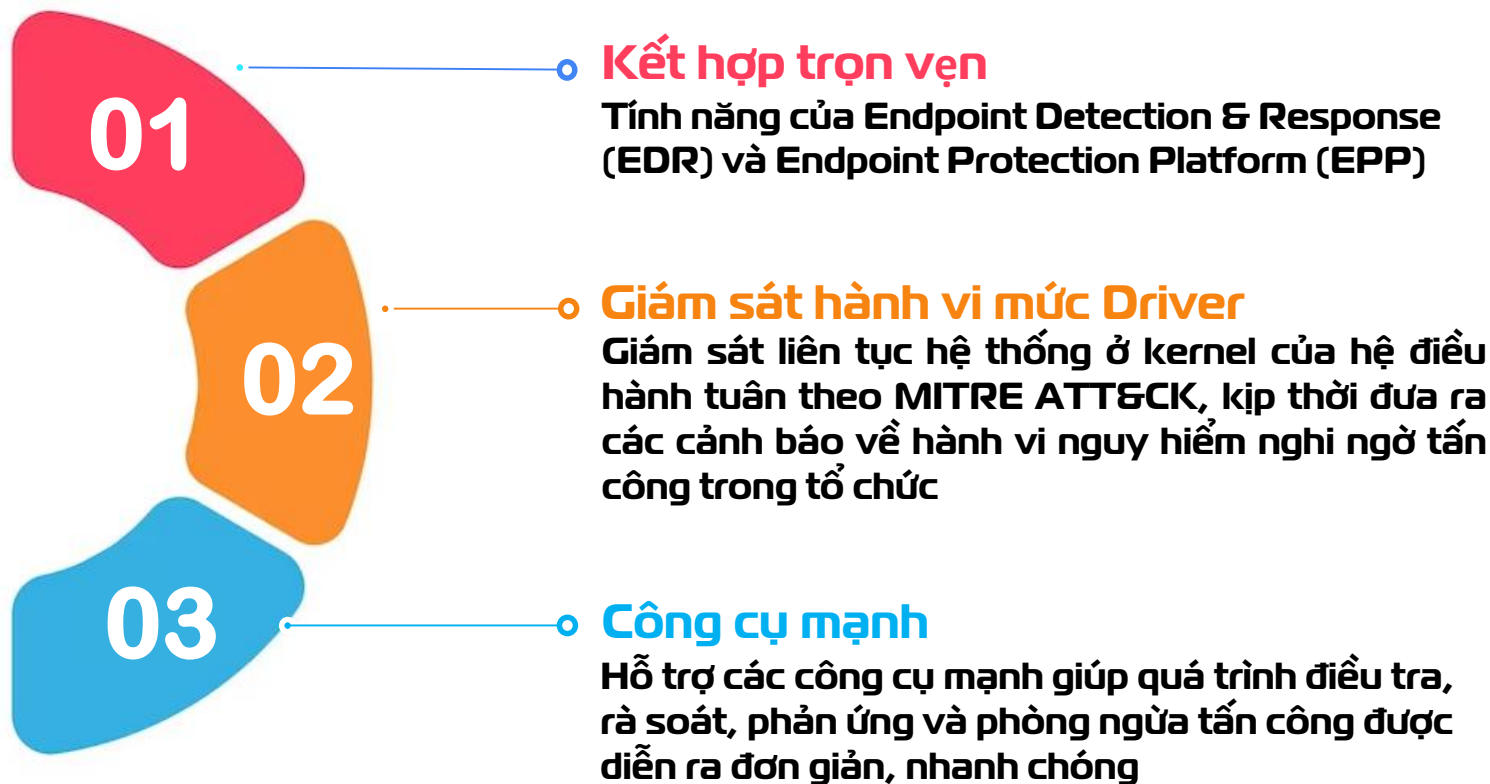
# Giải pháp Cloudrity – Bảo vệ toàn diện website và ứng dụng trực tuyến



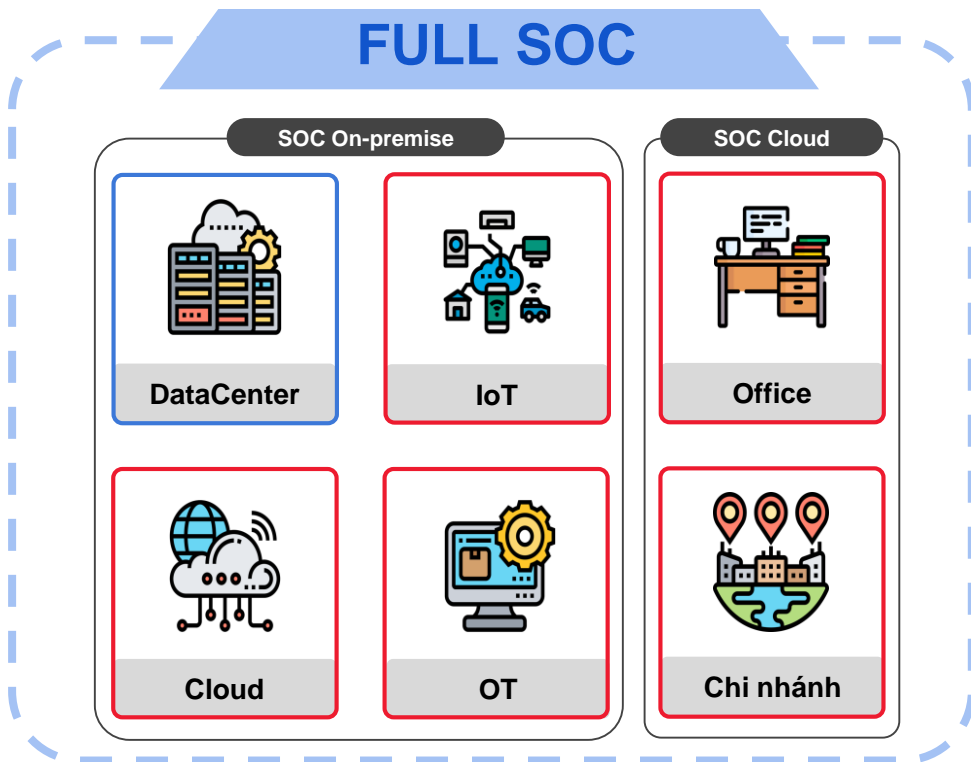
# Giải pháp VCS-Ajiant - Đảm bảo an toàn thông tin cho thiết bị đầu cuối



# Giải pháp VCS-Ajiant - Đảm bảo an toàn thông tin cho thiết bị đầu cuối



# Giải pháp SOC – Trung tâm điều hành an ninh mạng



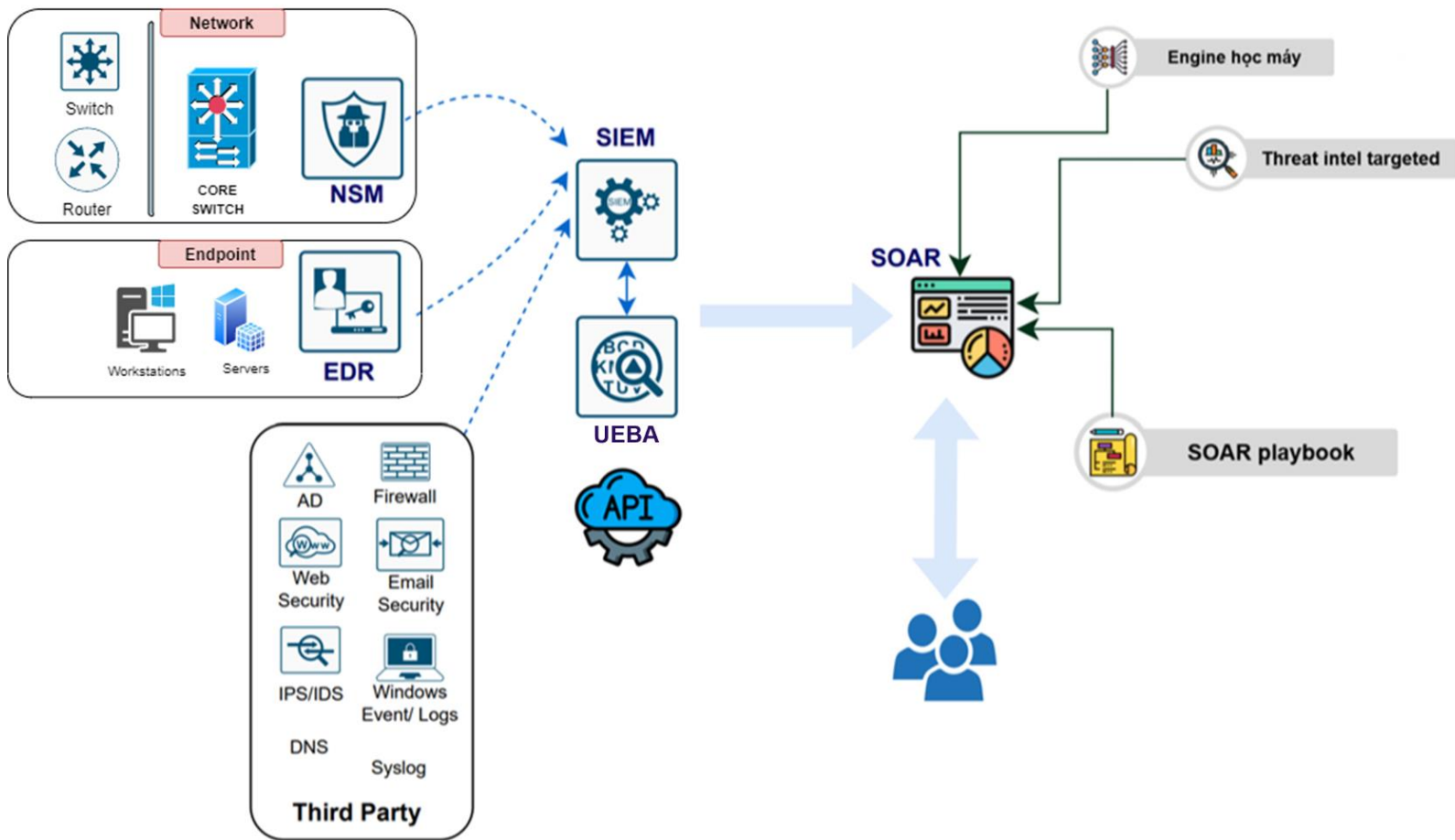
**Quy trình**

**Con người**

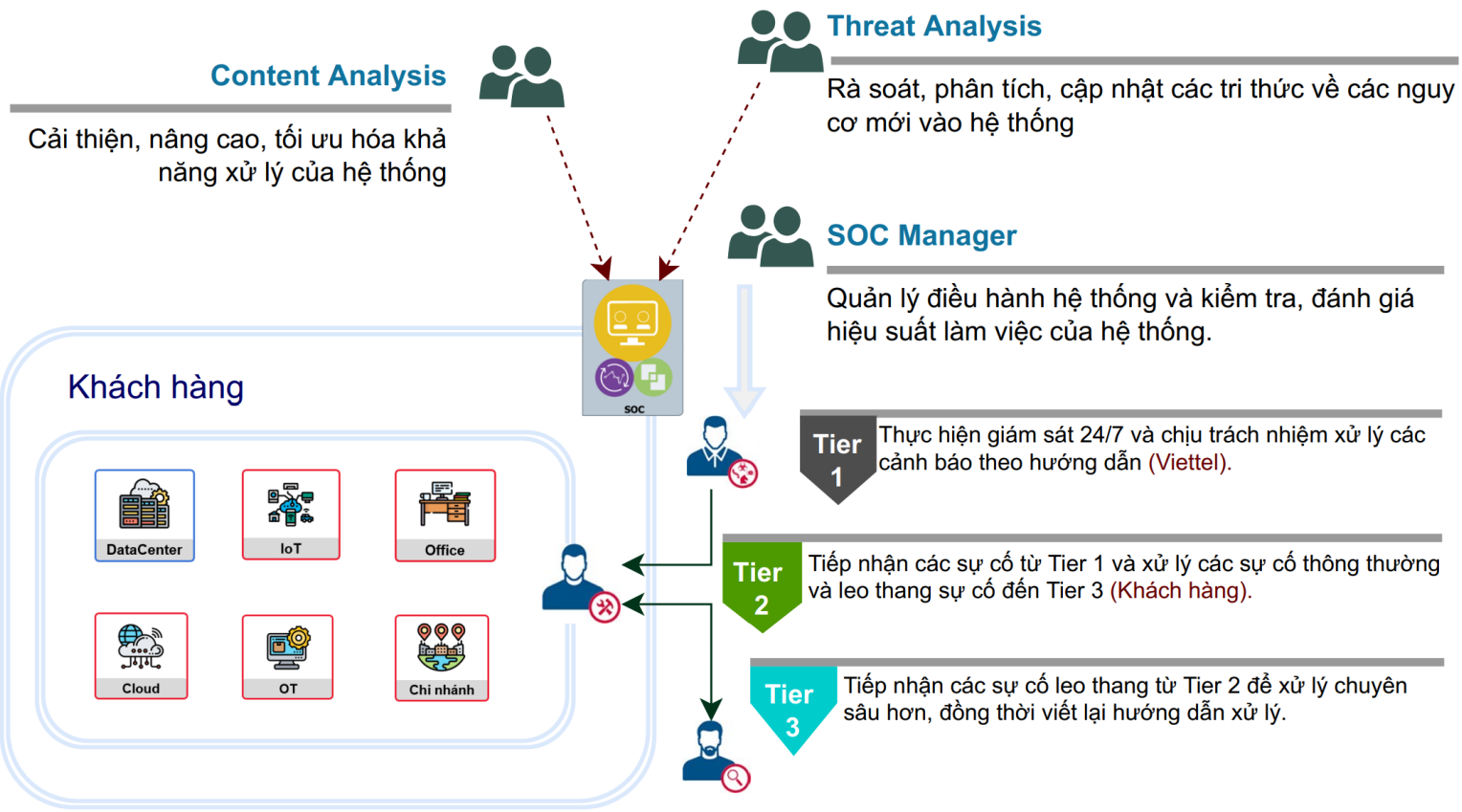
**Công nghệ**

- Mean time to Detect (MTTD)
- Mean time to Respond (MTTR)
- Độ phủ giám sát
- Độ phủ content
- Mức độ tự động hoá

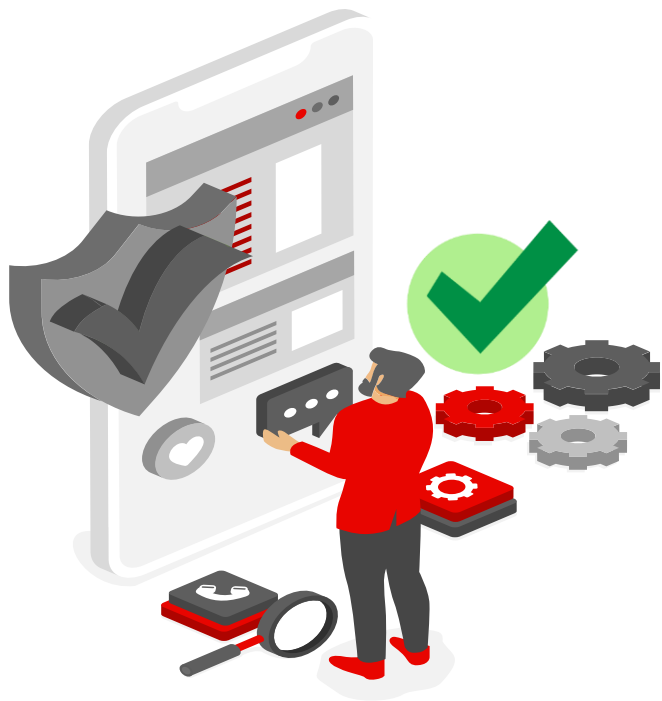
# Giải pháp SOC – Công nghệ | Con người | Quy trình



# Giải pháp SOC – Công nghệ | Con người | Quy trình





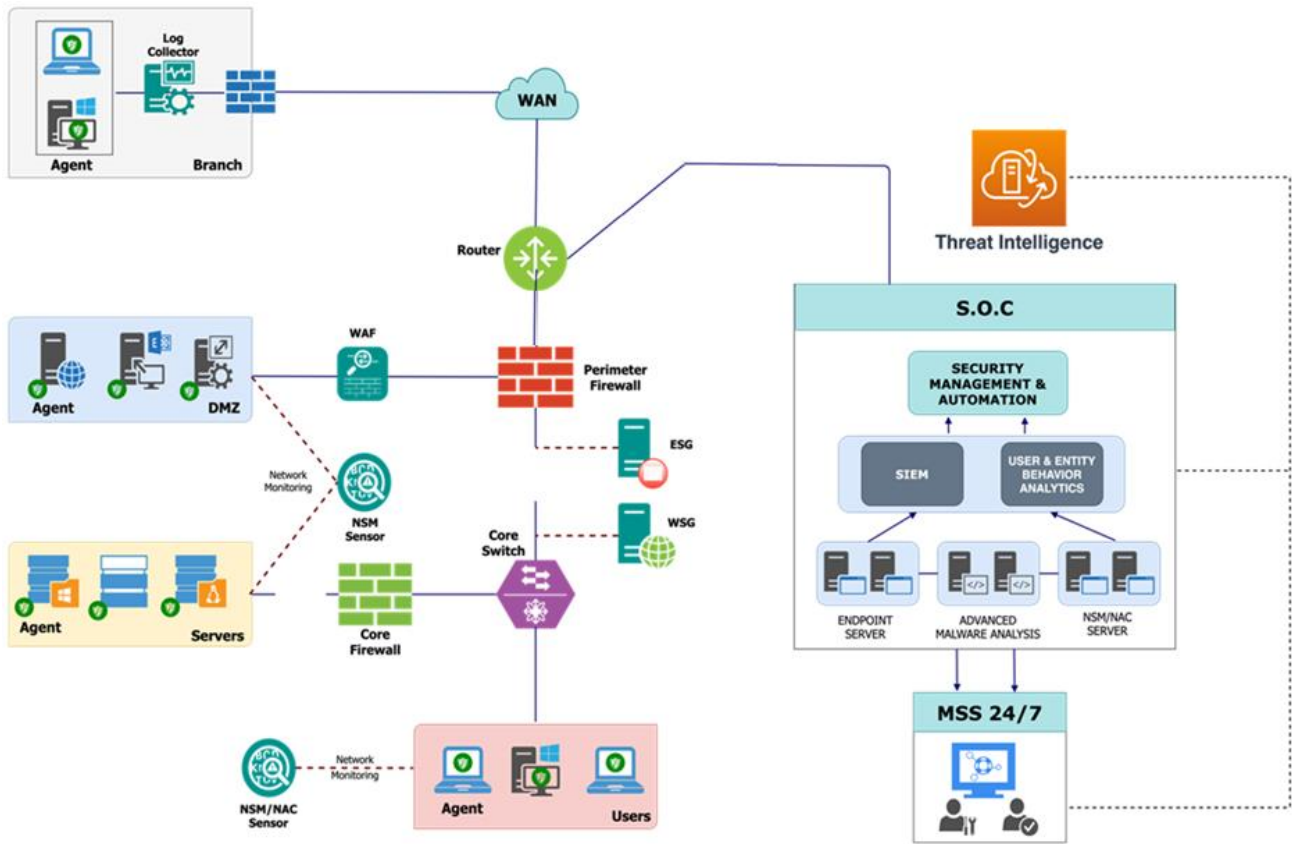


- 
- ❑ Quy trình chuẩn hóa, chuyên nghiệp
  - ❑ Tuân thủ các tiêu chuẩn quốc tế
- 
- ❑ **17** Quy trình phối hợp nội bộ
- 
- ❑ **02** Quy trình phối hợp với khách hàng:
    1. Quy trình giám sát 24/7
    2. Quy trình xử lý sự cố

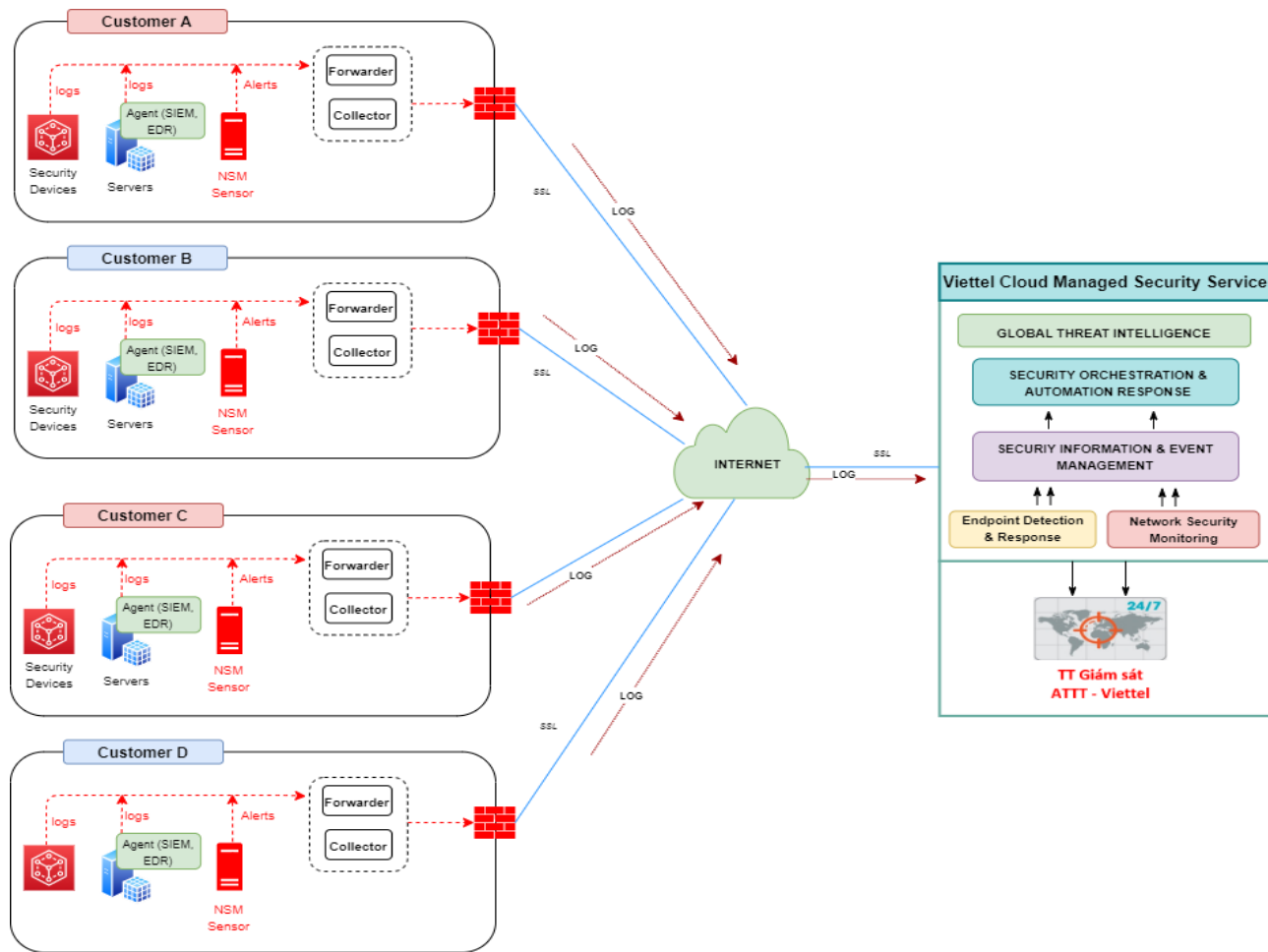
NIST



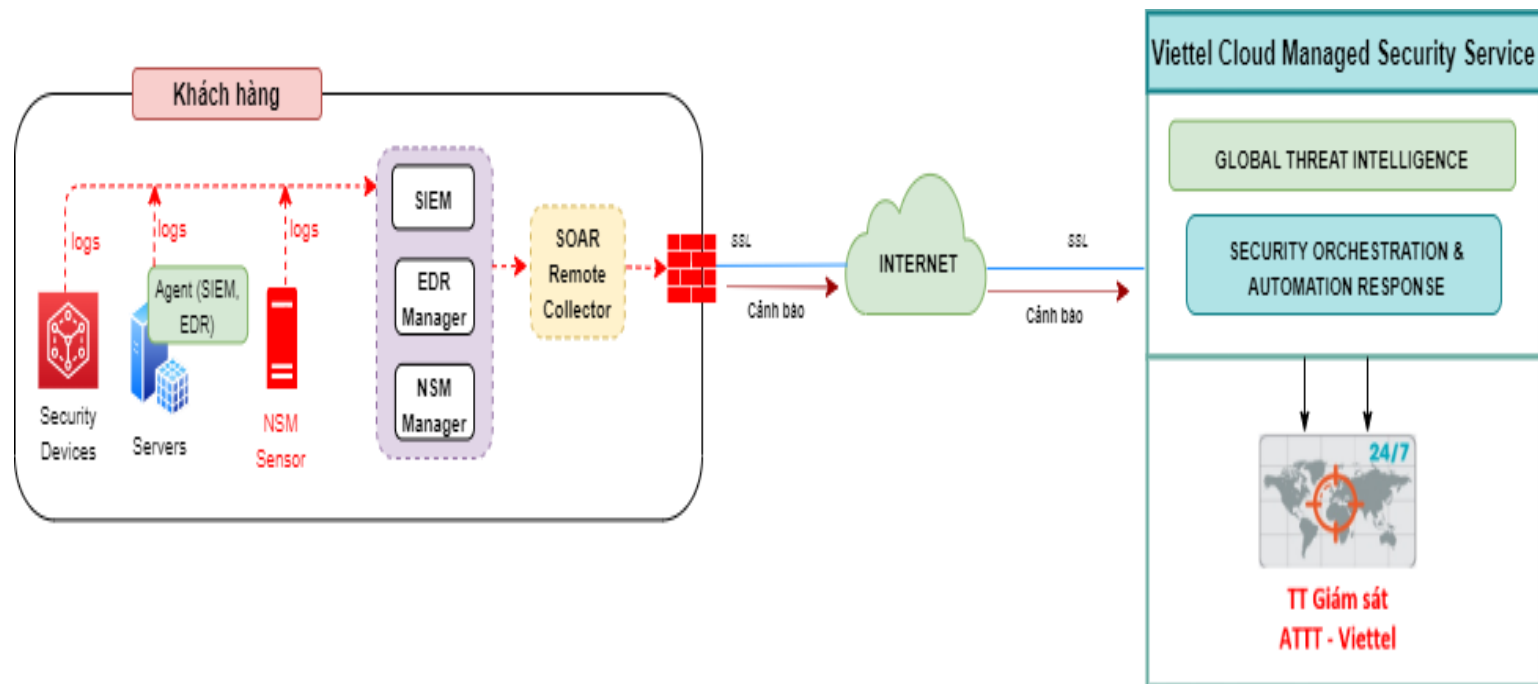
# Mô hình triển khai SOC On-Premises



# Mô hình triển khai SOC On-Cloud



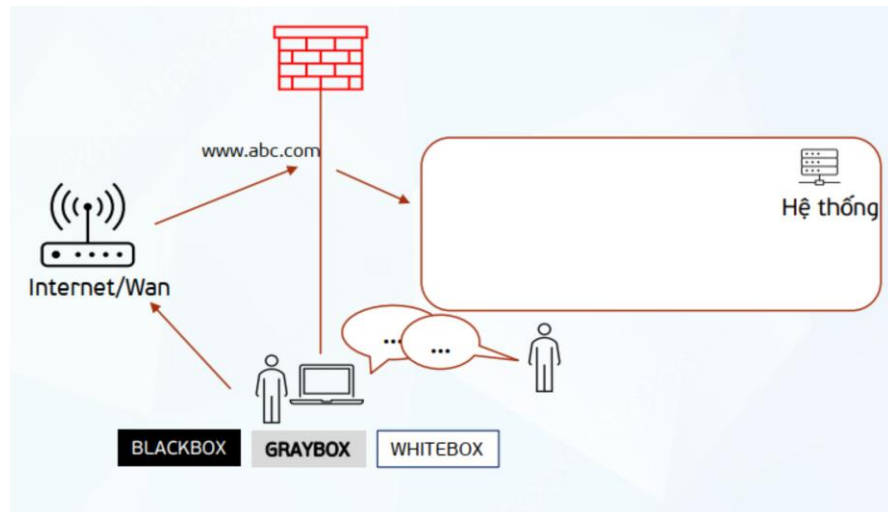
# Mô hình triển khai SOC-Hybrid



# Giới thiệu dịch vụ

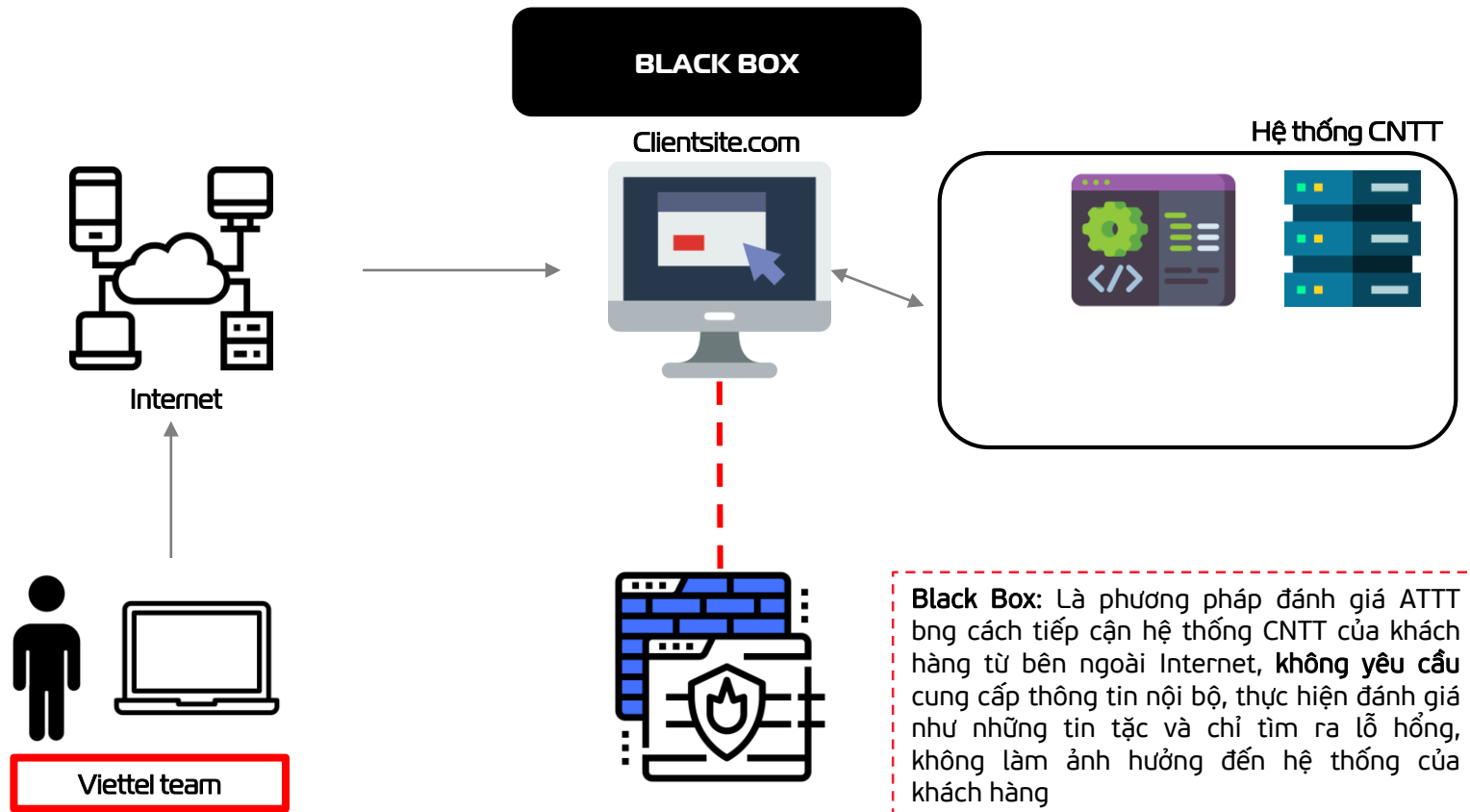
Dịch vụ Pentest (Penetration Testing) là hình thức **kiểm tra hệ thống ứng dụng CNTT** của khách hàng **có thể bị tấn công** hay không, bằng cách **đóng vai tin tặc** và **giả lập các vụ tấn công** thử nghiệm vào hệ thống của khách hàng. Các mục tiêu chính của dịch vụ Pentest bao gồm:

- Xác định các điểm yếu bảo mật trong hệ thống.
- Đưa ra những khuyến nghị và phương pháp khắc phục cho các điểm yếu tìm ra trong quá trình pentest.



# Cách thức triển khai

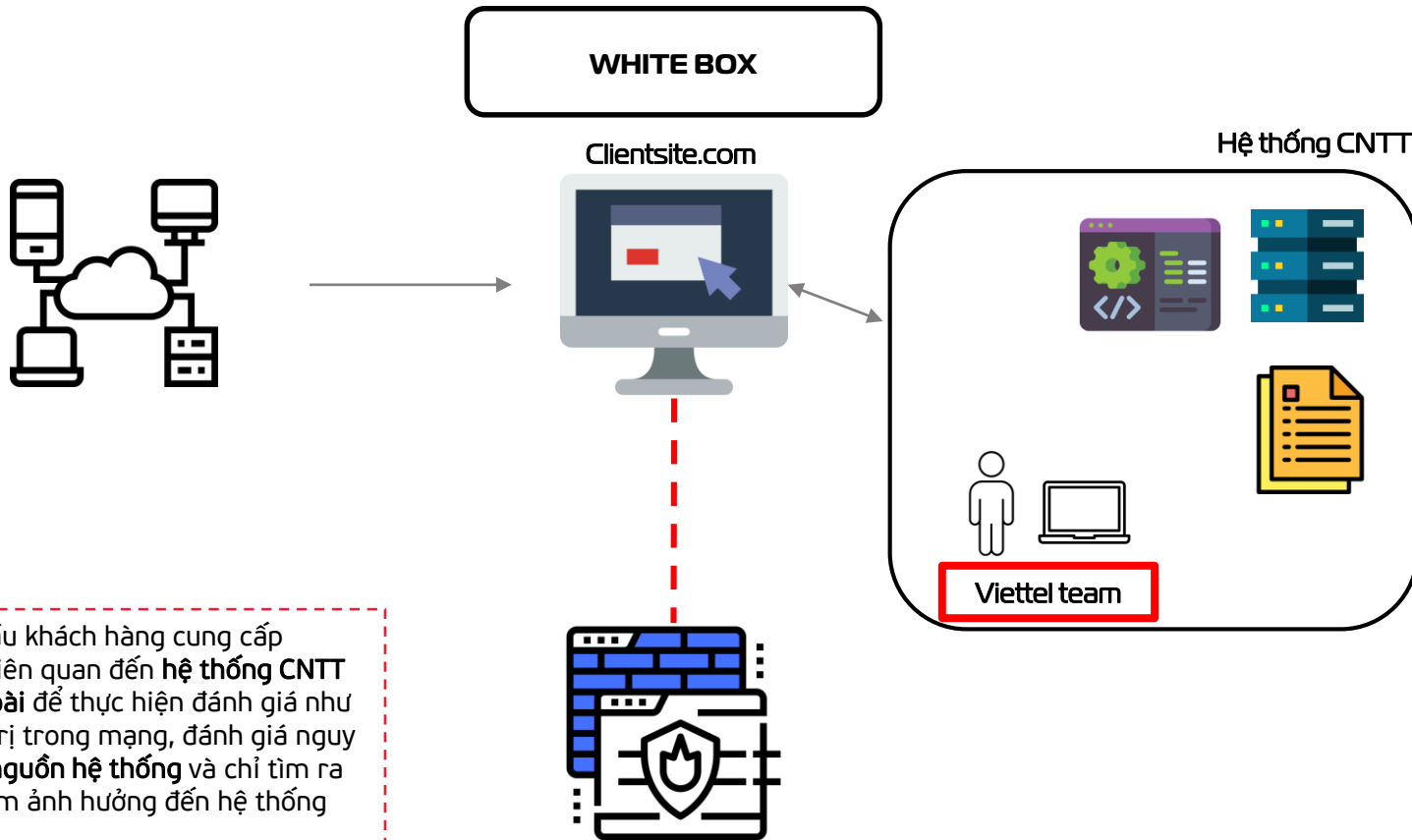
Khách hàng chọn một trong ba hình thức thực hiện (Black box, Gray box, White box)





# Cách thức triển khai

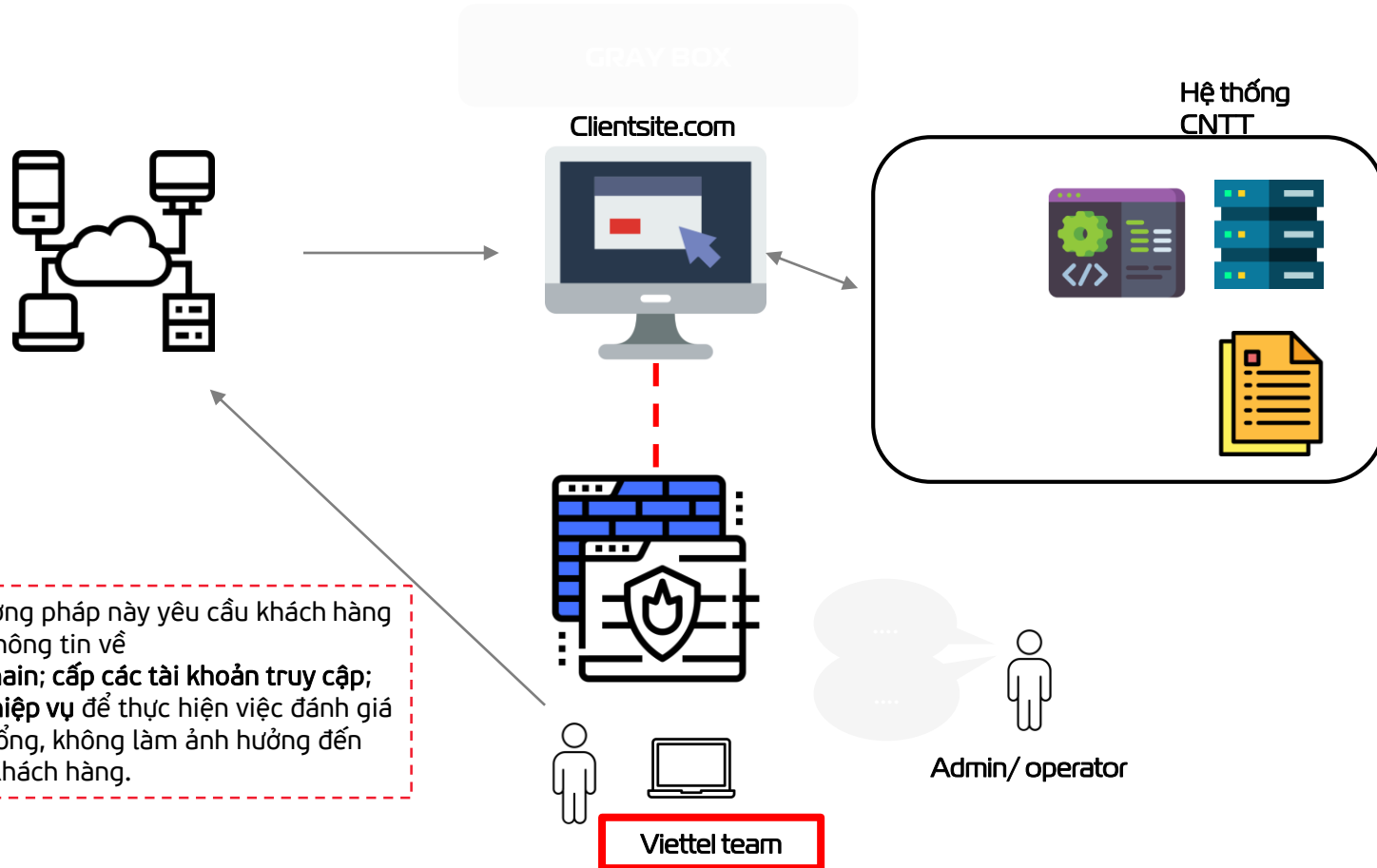
Khách hàng chọn một trong ba hình thức thực hiện (Black box, Gray box, White box)



**White Box:** yêu cầu khách hàng cung cấp những **thông tin** liên quan đến **hệ thống CNTT nội bộ và bên ngoài** để thực hiện đánh giá như một người quản trị trong mạng, đánh giá nguy cơ tiềm ẩn từ **mã nguồn hệ thống** và chỉ tìm ra lỗ hổng, không làm ảnh hưởng đến hệ thống của khách hàng.

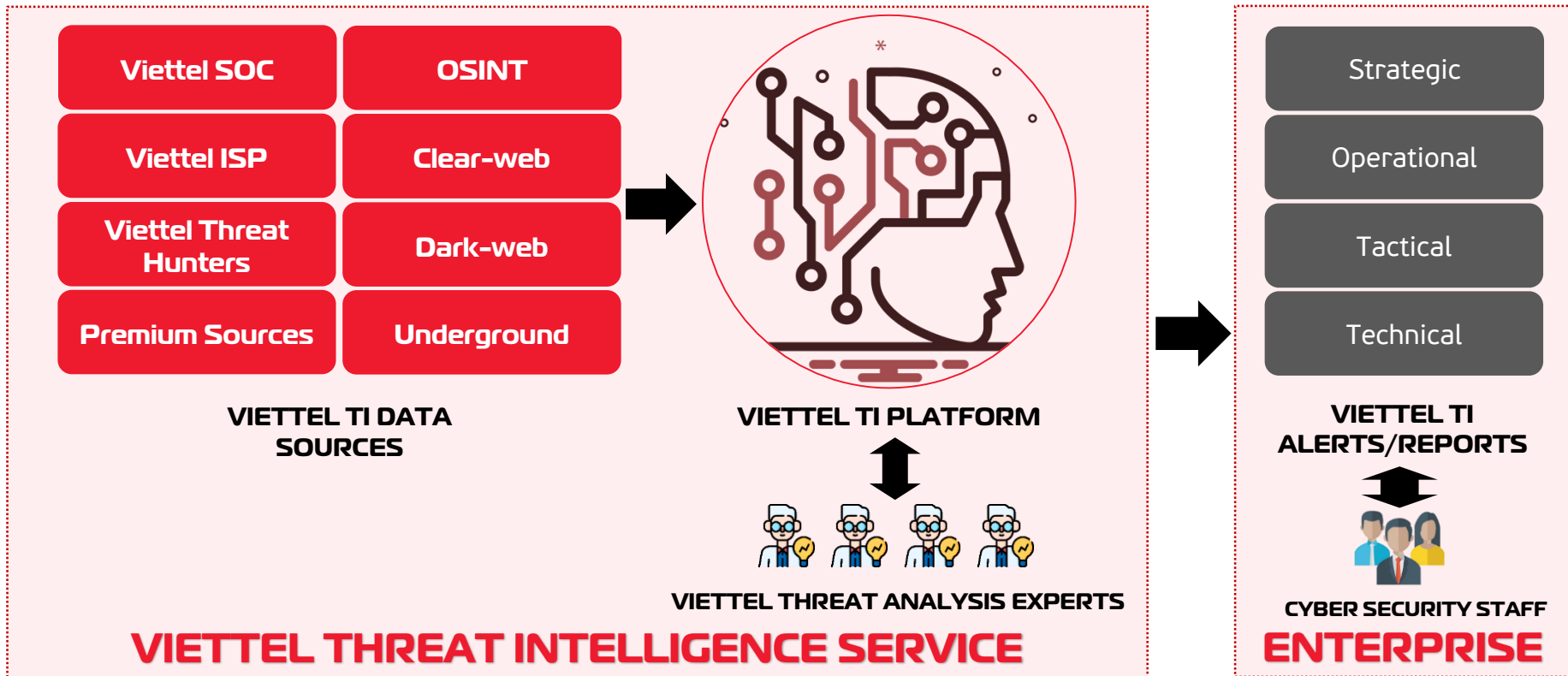
# Cách thức triển khai

Khách hàng chọn một trong ba hình thức thực hiện (Black box, Gray box, White box)



TRIỂN KHAI

# Phòng thủ chủ động



viettel  
security

*thank you!*