VIETTELDX

Đảm bảo ATTT trong xu hướng dịch chuyển lên cloud

CÔNG TY AN NINH MẠNG VIETTEL

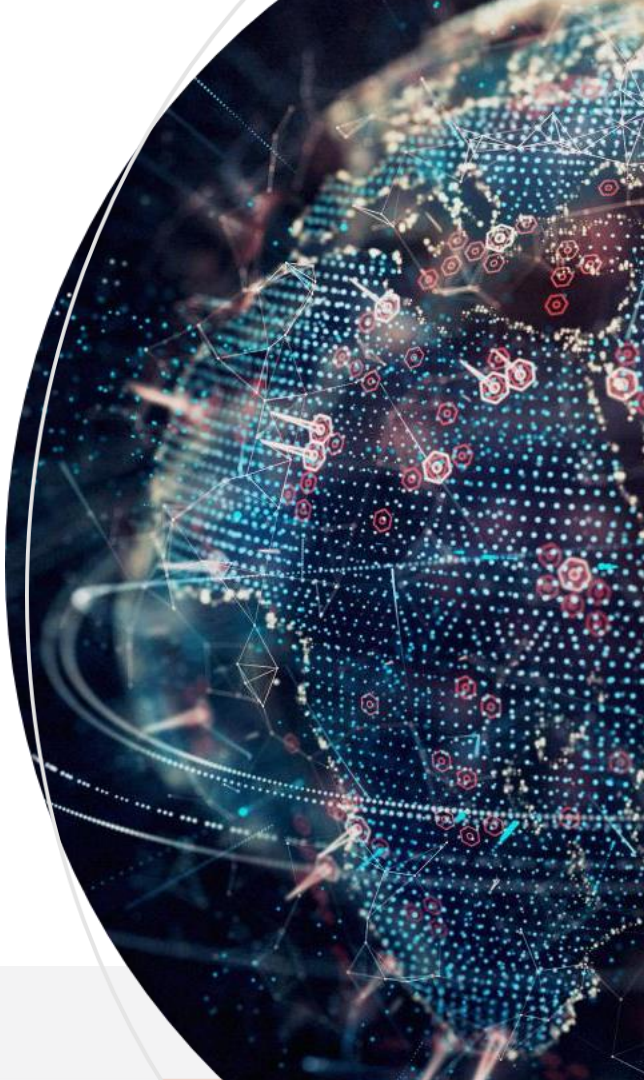
Giới thiệu

- Trên 15 năm kinh nghiệm trong xây dựng và vận hành các hệ thống CNTT và ATTT.
- Trên 20 chứng chỉ:
  - **Cá nhân**: CISSP #909083, CCSP, CEH, SCNP, SCNA, LPI, MCSE...
  - **Dịch vụ SOC**: ISO27001 & CREST level 4/5

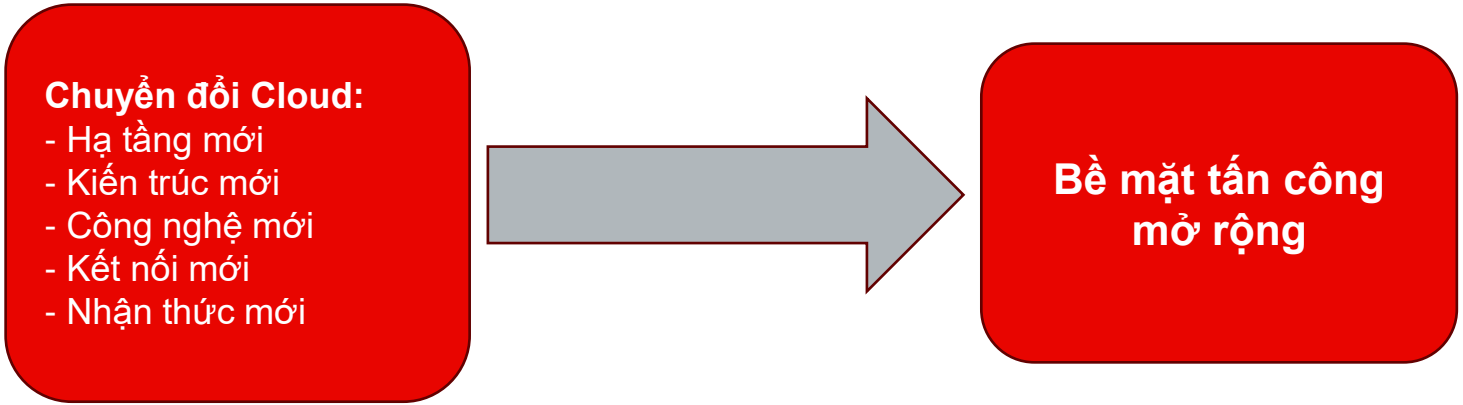
PGĐ Trung tâm SOC

NỘI DUNG

1. CÁC MỐI ĐE DỌA CHÍNH KHI CHUYỂN DỊCH LÊN CLOUD
2. CHIA SẺ MỘT SỐ USECASE SỰ CỐ GẦN ĐÂY
3. GIẢI PHÁP ĐẢM BẢO ATTT KHI CHUYỂN DỊCH LÊN CLOUD

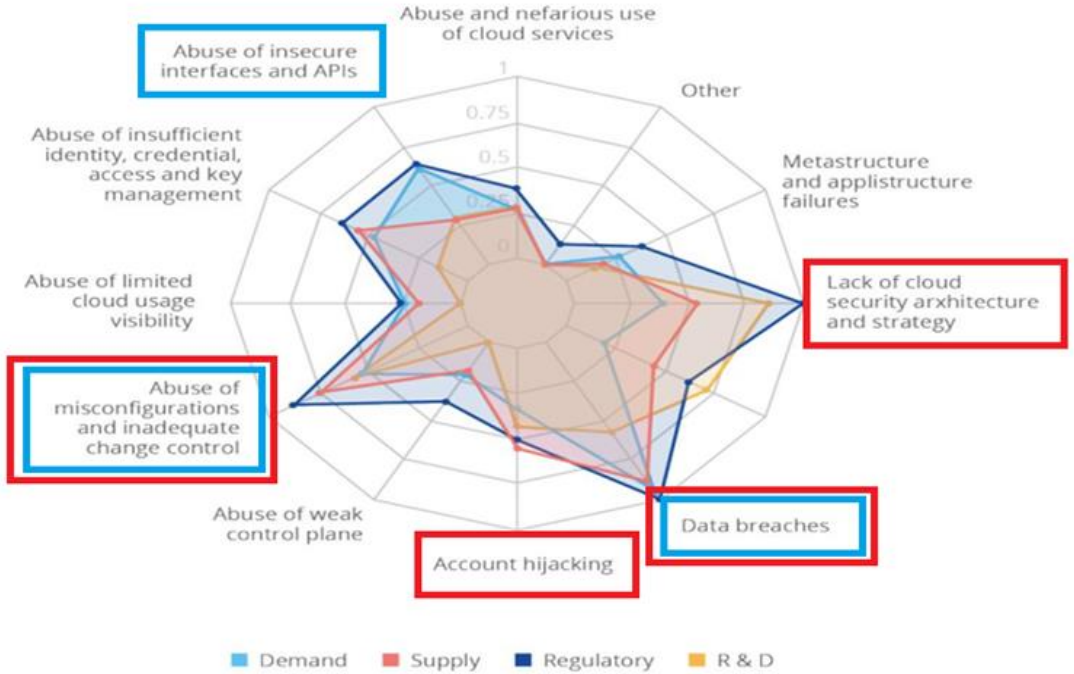


BỀ MẶT TẤN CÔNG MỞ RỘNG



Dự báo đến năm 2025:
- Bề mặt tấn công mở rộng 2.6 lần
- Số lượng lỗ hổng mới được công bố mỗi ngày tăng 2 lần

CÁC MỐI ĐE DỌA VỀ ANM TRÊN MÔI TRƯỜNG CLOUD



Source: *CLOUD CYBERSECURITY MARKET ANALYSIS by ENISA, 3/2023*

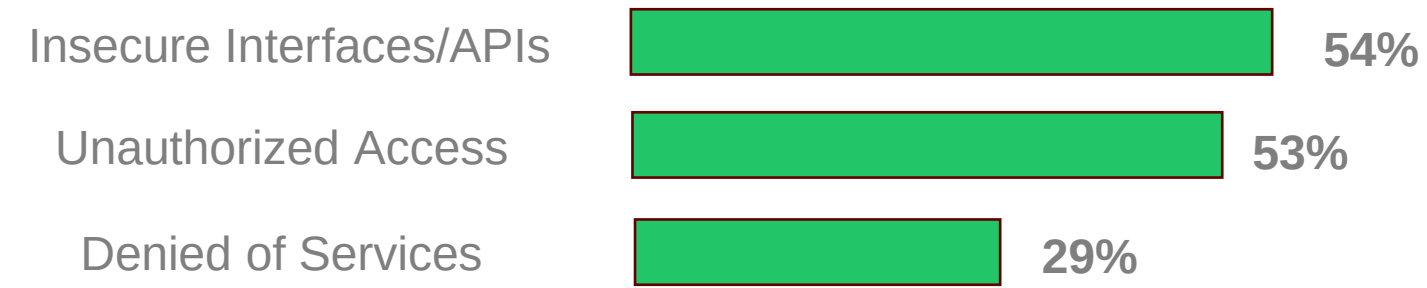
CÁC MỐI ĐE DỌA VỀ ANM TRÊN MÔI TRƯỜNG CLOUD

71%

Misconfiguration of the cloud platform/wrong set-up

59%

Exfiltration of sensitive data



LỘ LỌT DỮ LIỆU

	Thời gian	Tác động
Toàn cầu Lộ lọt dữ liệu	**2018 - 2019**	• **33.4 tỷ** bản ghi dữ liệu • **5,000 tỷ USD**
Facebook Lộ lọt dữ liệu	**2019**	**540 triệu** bản ghi dữ liệu người dùng
LinkedIn Lộ lọt dữ liệu	**2021**	**700 triệu** bản ghi dữ liệu người dùng
Samsung Electronics Lộ lọt dữ liệu	**2022**	**150 GB** dữ liệu bị công khai

CÁC LỖ HỔNG MỚI

Quý 3 năm 2023

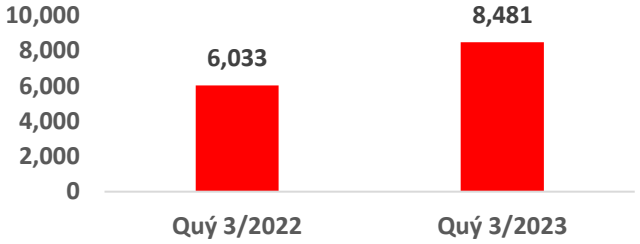
8,481 Số lỗ hổng ATTT mới ghi nhận trên thế giới

So với quý 3 năm 2022

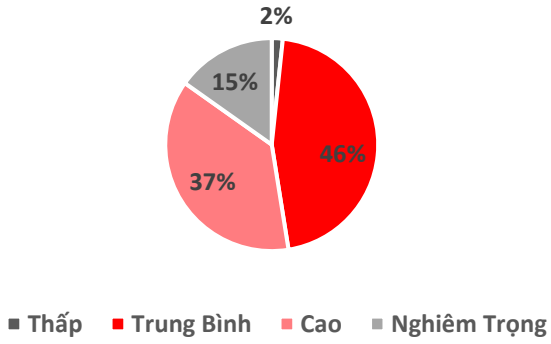
29.9% ↑

52% Số lỗ hổng mức cao & nghiêm trọng *(theo CVSS)*

Số lượng lỗ hổng ghi nhận trong quý 3 năm 2022 và quý 3 năm 2023



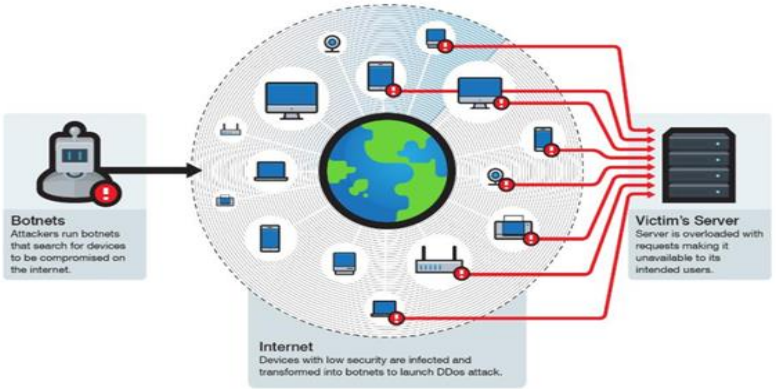
Tỉ lệ lỗ hổng theo mức độ trong quý 3 năm 2023



ĐÁNG LƯU Ý

- Microsoft Exchange
- Microsoft SharePoint
- Confluence

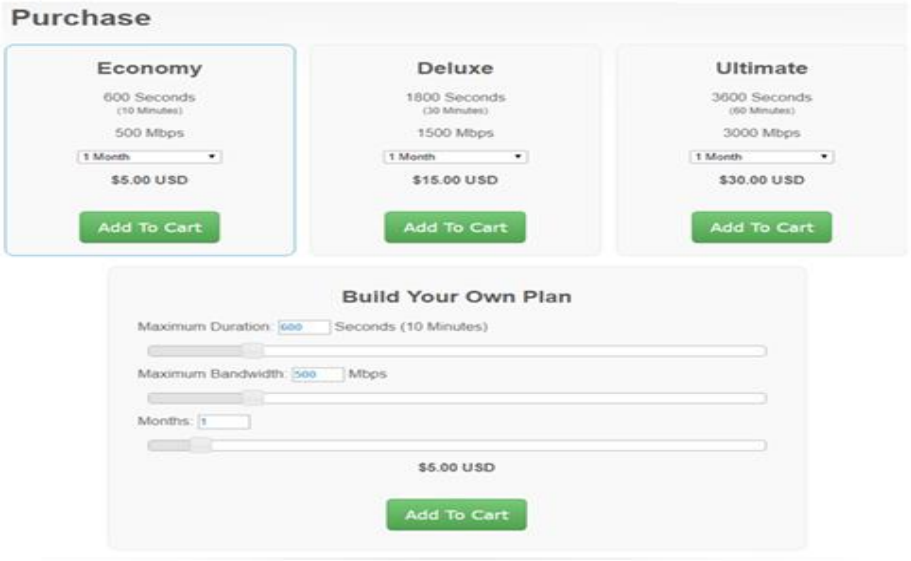
DDoS attacks



Internet of Thing – Botnet of Thing

DDOS ATTACK - ĐƠN GIẢN HƠN BẠN NGHĨ

- **Không cần** sở hữu mạng **botnet**
- **Không cần kiến thức** chuyên sâu về ATTT
- **Chi phí rẻ**: 30$ - 60$ tấn công volume 3Gbps



NỘI DUNG

1 CÁC MỐI ĐE DỌA CHÍNH KHI CHUYỂN DỊCH LÊN CLOUD

2 **CHIA SẺ MỘT SỐ USECASE SỰ CỐ GẦN ĐÂY**

3 GIẢI PHÁP ĐẢM BẢO ATTT KHI CHUYỂN DỊCH LÊN CLOUD

UseCase 1: Lộ mật khẩu tài khoản quản trị Cloud

9/2023

Hình thức tấn công

Máy quản trị viên Cloud bị mã độc Stealer

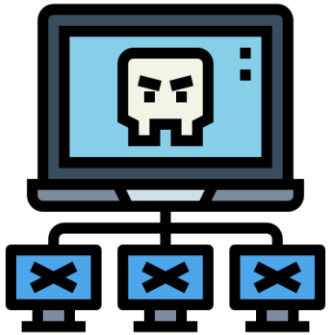
Mục đích

Chiếm quyền làm chủ toàn bộ tài nguyên trên Cloud của khách hàng (máy chủ, ứng dụng...)

Vấn đề

- Quản trị viên đăng nhập tài khoản quản trị Cloud trên máy tính không an toàn
- Tài khoản quản trị không được thiết lập MFA

UseCase 2: SSO giữa các ứng dụng



8/2023

Hình thức tấn công

- Attacker chiếm quyền làm chủ máy chủ ứng dụng có mức độ bảo mật thấp.
- Do các ứng dụng sử dụng SSO để xác thực người dùng, từ đó Attacker leo thang chiếm quyền quản trị Cloud.

Mục đích

Chiếm quyền làm chủ toàn bộ tài nguyên trên Cloud của khách hàng (máy chủ, ứng dụng...)

Vấn đề

- Không tách biệt tài khoản quản trị Cloud với tài khoản nghiệp vụ
- Tài khoản quản trị không được thiết lập MFA

NỘI DUNG

1 CÁC MỐI ĐE DỌA CHÍNH KHI CHUYỂN DỊCH LÊN CLOUD

2 CHIA SẺ MỘT SỐ USECASE SỰ CỐ GẦN ĐÂY

3 GIẢI PHÁP ĐẢM BẢO ATTT KHI CHUYỂN DỊCH LÊN CLOUD

GIỚI THIỆU VCS

Số lượng nhân sự chuyên gia vượt trội

Hơn 400 chuyên gia đã có nhiều năm kinh nghiệm trong lĩnh vực An ninh mạng

VCS tại PWN2OWN

2022 (Top 2)

2023 (Vô địch)

Xử lý sự cố

- Cảnh báo bảo mật: 2,300,000
- Sự cố mã độc thường: 3,800
- Tấn công có chủ đích (APT): 500

Zero-day

- ~400 zero-day
- 15 zero-day cho IoT

MSRC · Google Bounty · Facebook Bug Bounty

CISSP · CCSP Certified Cloud Security Professional · CISCO CERTIFIED CCIE SECURITY · OSWE · GIAC CERTIFICATIONS · SANS INSTITUTE

PROFESSIONAL CERTIFICATIONS

Frost and Sullivan

- Nhà cung cấp dịch vụ quản lý ANM (MSSP) tốt nhất Việt năm 2020
- Nhà cung cấp dịch vụ ATTT số 1 Việt Nam 2022 & 2023

Cybersecurity Excellence Awards

- 13 giải Vàng năm 2022
- 11 giải Vàng 2023

CybersecAsia Reader Choice Awards

- Giải pháp Phát hiện và phản ứng gian lận tài chính (F2DR) Tốt nhất năm 2022
- Nhà cung cấp dịch vụ ATTT (MSSP) Tốt nhất 2023

Global InfoSec Awards

Dịch vụ kiểm thử ATTT **(Penetration) Tốt nhất năm 2023**

IT World Awards

- Giải Vàng năm 2020, 2022, 2023
- Giải Bạc năm 2021, 2022
- Giải Đồng 2017, 2020, 2023
- Danh hiệu Grand Globee năm 2022

Stevie Awards

Giải Bạc 2017

ISO 27001-certified
Security Operations Center (SOC)

CREST-accredited
Penetration Testing
Security Operations Center (SOC)
Level 4/5

QUÝ 1/2024

Khách hàng

Quốc Tế

hello GROUP

privé: technologies

BNCTL

Aung Bar Lay
Chance to be better

mytelpay

PRTIMES

CAFFIO

DONUTS

SINGAPORE
TIMOR LESTE
SOUTH AFRICA
LAOS
HONGKONG
JAPAN
MYANMAR

Chính Phủ

Bộ Thông tin và Truyền thông

Bộ Tài Chính

Bộ Quốc Phòng

Sở TTTT và UBND tỉnh

Doanh nghiệp

Vietnam Airlines

EVN

PVI

PTSC
A member of PETROVIETNAM

DAIKIN

SNP
SAIGON NEWPORT

LOTTE FINANCE

Ngân hàng và Tài chính

Vietcombank

BIDV

VietinBank

MB

VPBank

SeABank

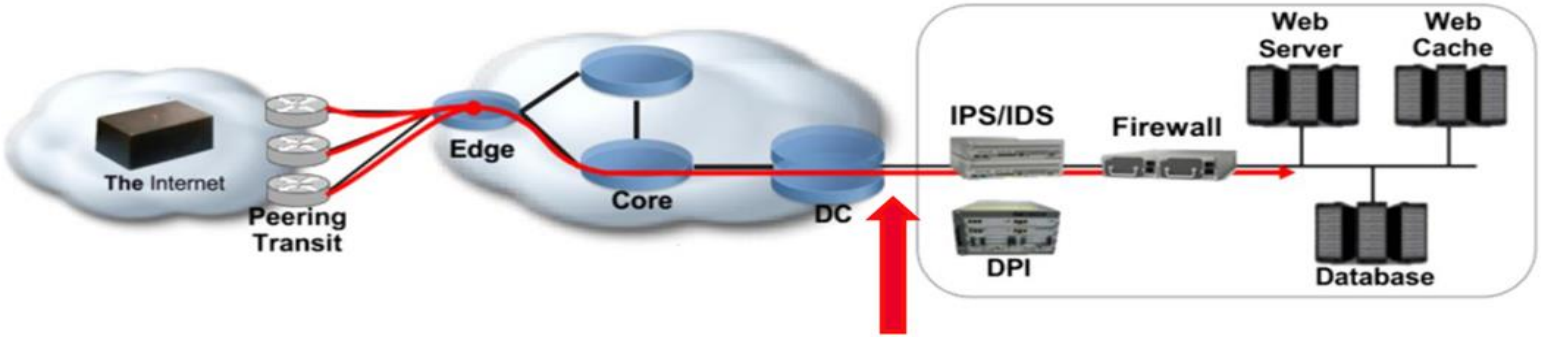
MSB

VPS SECURITIES

Lựa chọn nhà cung cấp Cloud đủ năng lực ATTT

Băng thông Uplink của đơn vị bạn là bao nhiêu?

DDOS volume-based thực sự là một vấn đề lớn?



ISP/CSP có năng lực hạ tầng lớn, đủ sức chống đỡ các tấn công cường độ lớn

Đưa nguồn lực ATTT vào Chuyển đổi số: MSSP là một lực lượng

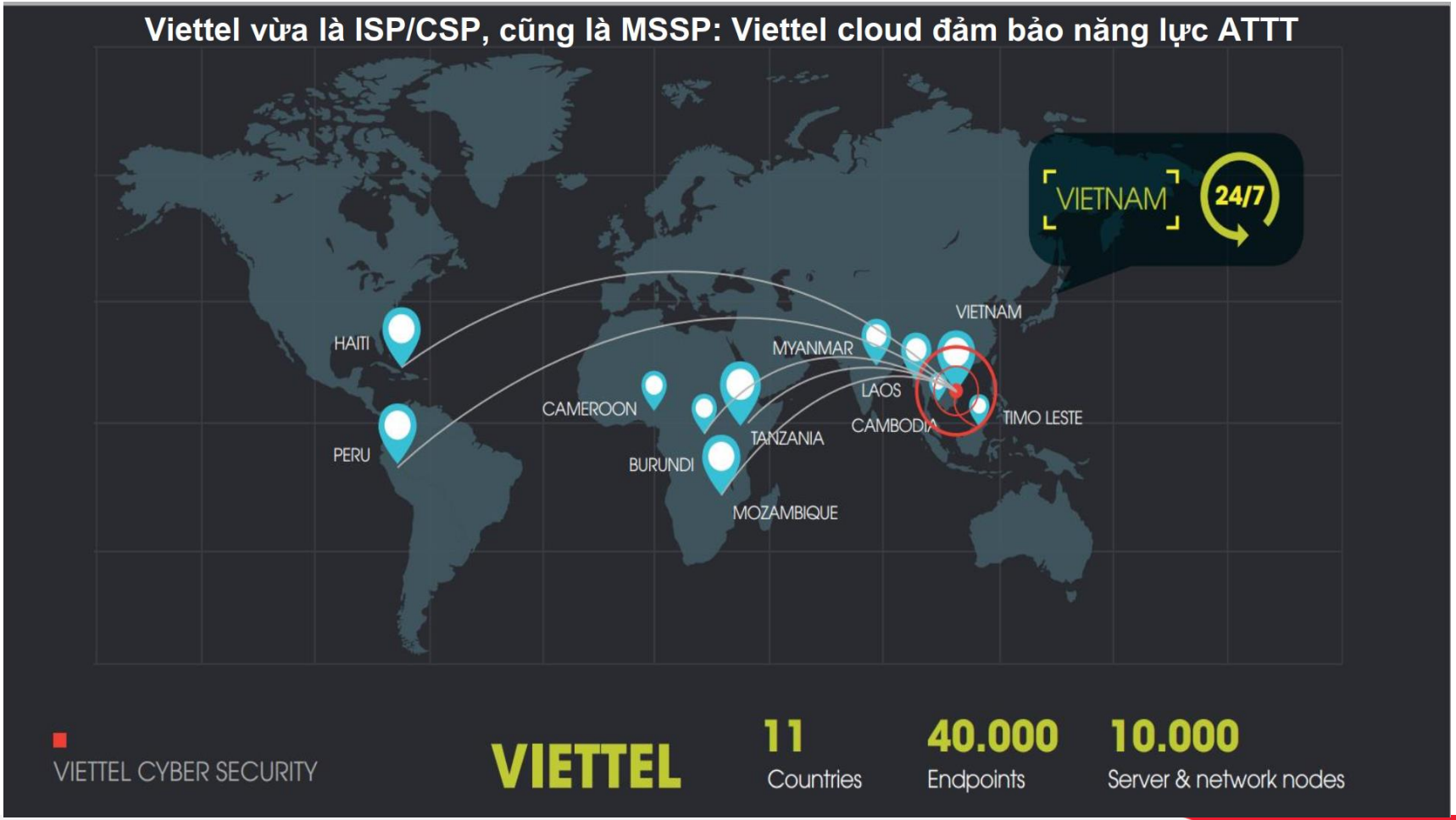
Tổ chức lực lượng ATTT trong lực lượng CĐS

MSSP cũng có thể là 1 lực lượng

Thiết lập mục tiêu ATTT trong dự án CĐS

Đưa ATTT vào vòng đời phát triển của sản phẩm dịch vụ CĐS

Viettel vừa là ISP/CSP, cũng là MSSP: Viettel cloud đảm bảo năng lực ATTT



Dịch vụ Viettel DDoS Mitigation

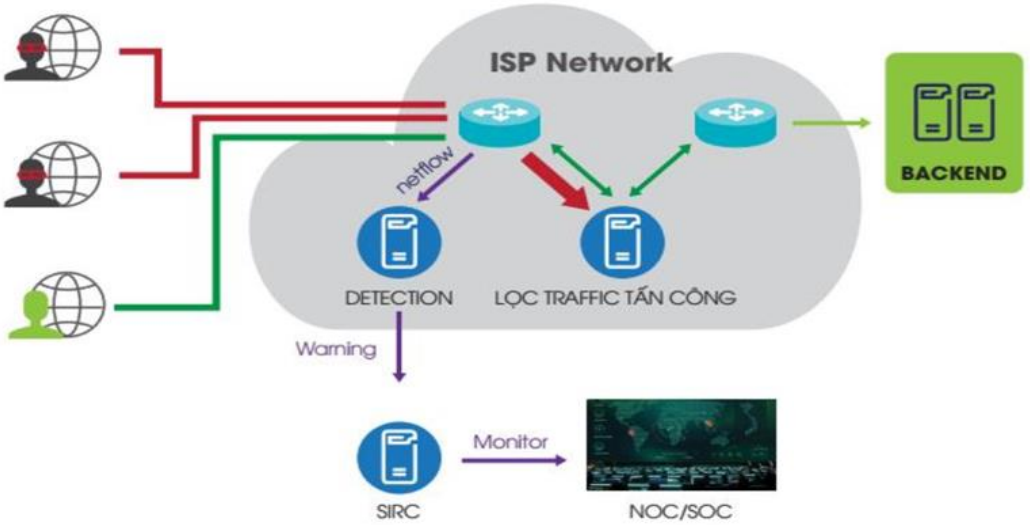
Băng thông xử lý lớn lên đến **100 Gbps**

Delay thấp, **~ 45 Micro Seconds**

Cơ chế xử lý on-demand: **Outline, hoàn toàn tự động**, giảm ảnh hưởng CLDV khách hàng

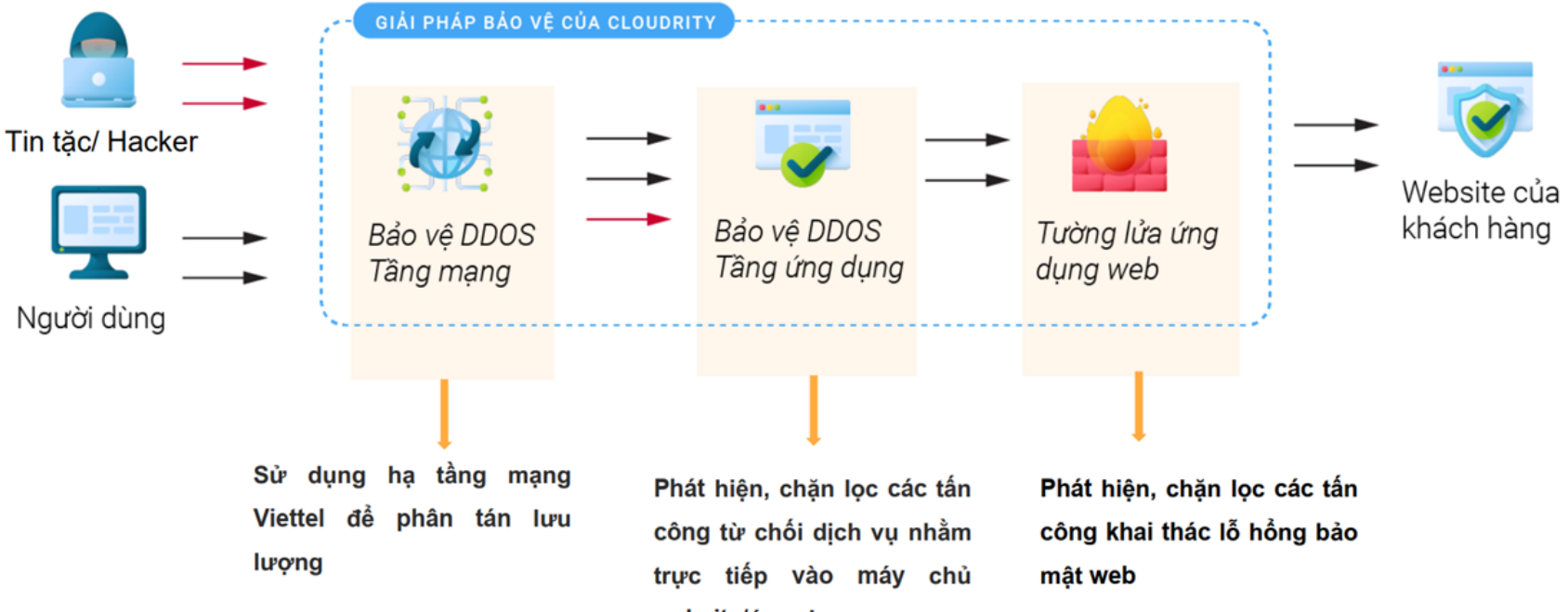
Đa dạng kênh cảnh báo: **SMS, mail, có portal riêng** cho k/h tra cứu

Công nghệ tiên tiến: **Machine Learning, DPI, Anycast, BGP Flowspec...**

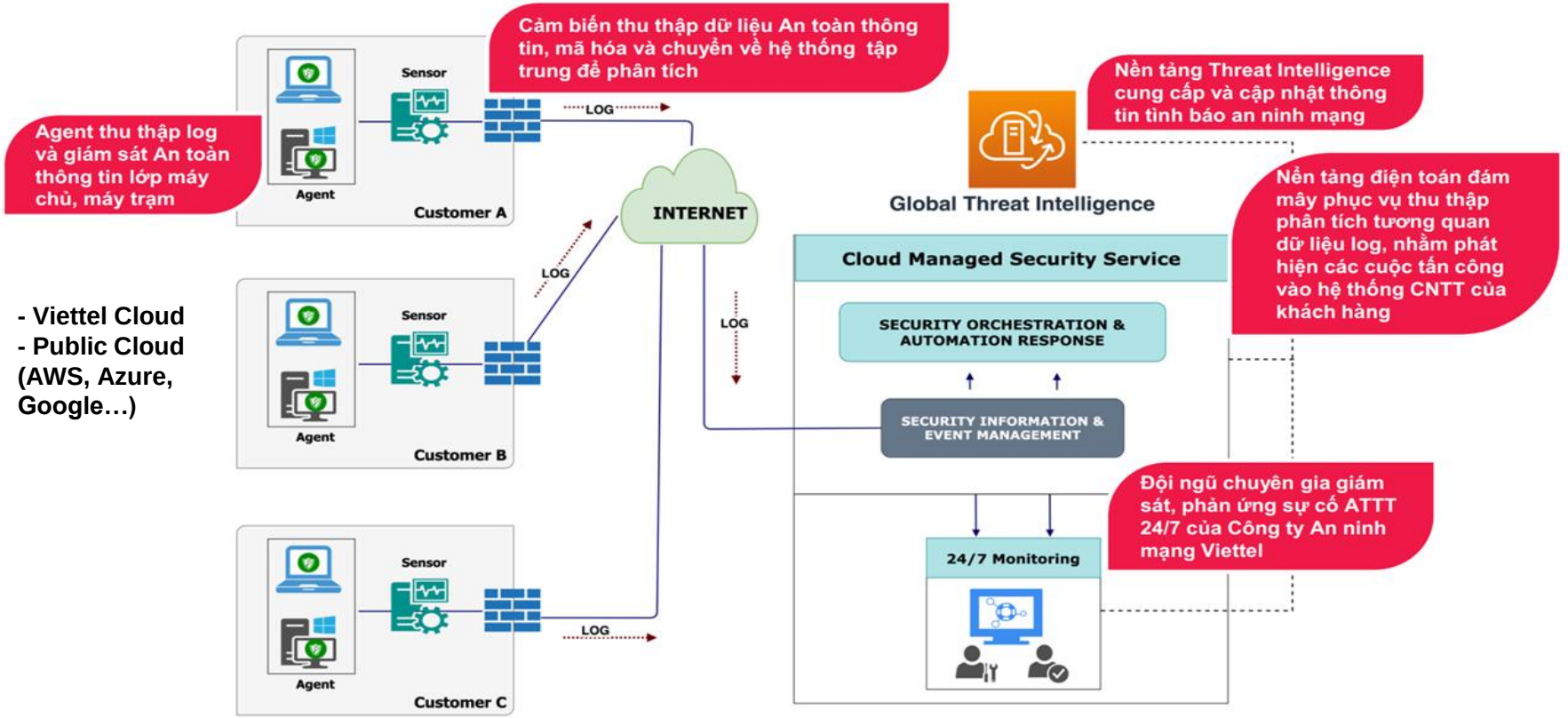


Tận dụng sức mạnh hạ tầng ISP

Dịch vụ Cloudrity bảo vệ website



Dịch vụ Viettel SOC Cloud



- Viettel Cloud
- Public Cloud (AWS, Azure, Google…)

TẠI SAO LỰA CHỌN VIETTEL SOC ?

Con người và Quy trình

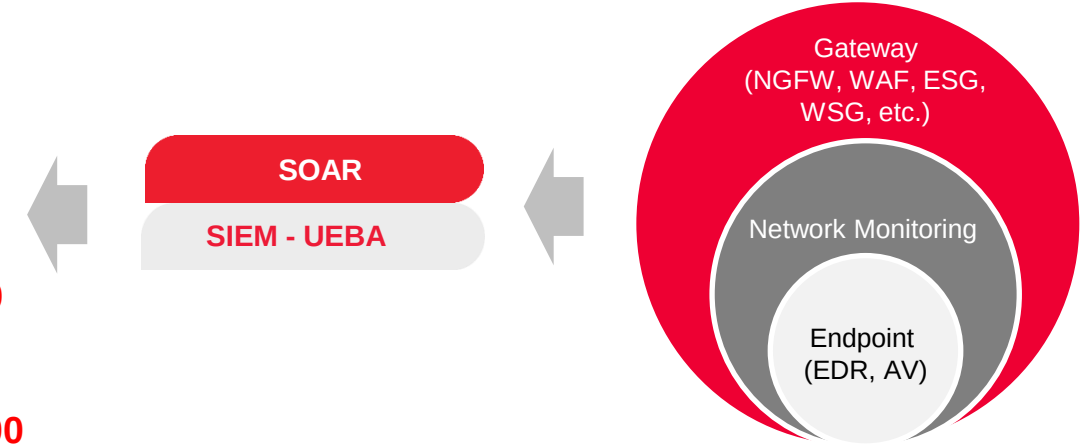
- **Con người**: Các chuyên gia được chứng nhận toàn cầu trong lĩnh vực ATTT, kinh nghiệm thực chiến cao.
- **Quy trình**: Giám sát và xử lý sự cố 24/7/365

Công nghệ

- **Tự phát triển giải pháp** với dải sản phẩm rộng, hoàn chỉnh.
- **Làm chủ** hoàn toàn công nghệ.
- **Mô hình triển khai** linh hoạt, may đo theo nhu cầu khách hàng.
- **Dễ dàng tích hợp** với giải pháp bên thứ 3.

Hàng năm

- Cảnh báo bảo mật: **2,300,000**
- Sự cố mã độc thường: **3,800**
- Tấn công có chủ đích (APT): **500**



Success Story 1

- Security Operation Center (SOC)

Đã triển khai tại 1 Ngân hàng

Kết quả hàng tháng:

3500

Cảnh báo ATTT:

- **1000** cảnh báo lớp mạng (network).
- **2000** cảnh báo lớp Endpoint.
- **500** cảnh bảo được tổng hợp từ nhiều events (SIEM).

Sau khi được xử lý tự động bởi hệ thống và xử lý nâng cao bởi chuyên gia:

30

Tickets

Khách hàng chỉ cần xử lý 30 tickets (< 1%)

Success Story 2

- **Security Operation Center (SOC)**

Đã triển khai tại 1 Ngân hàng thương mại lớn nhất VN

Mô hình triển khai: On-Premise

Phạm vi:
- 800 servers
- 2,000 desktops
- Đầy đủ các giải pháp của VCS cho SOC:
  - NSM, EDR
  - SOAR, SIEM, UEBA
  - MSS
- Trước khi triển khai SOC:
  - **MTTD > 6 tháng**

Sau khi triển khai SOC của VCS

MTTD < 2h

viettel
security

Keangnam Landmark 72, Pham Hung Rd., Nam Tu Liem Dist., Hanoi

vcs.sales@viettel.com.vn | vcs.partners@viettel.com.vn

viettelcybersecurity.com.vn

thanks!