

Hệ miễn dịch không gian số bảo vệ an toàn thông tin cho chính quyền và người dân

01

Thách thức trong đảm bảo an toàn thông tin trên không gian số

02

Security as a Service Lời giải của bài toán đảm bảo APTT cho tổ chức, doanh nghiệp

03

Kết luận



01

Thách thức trong đảm bảo an toàn
thông tin trên không gian số



XU HƯỚNG DỊCH CHUYỂN VỀ LƯU TRỮ VÀ XỬ LÝ DỮ LIỆU



Người dùng truy cập đến dữ liệu của công ty từ mọi nơi



Xu hướng dịch chuyển Data Center lên Public Cloud



Người dùng sử dụng các ứng dụng SaaS ngày càng nhiều





LỘ LỘT THÔNG TIN



Theo UpGuard



Theo Twitter



Theo NCSC

Theo **Cost of a Data Breach Report** của IBM năm 2022:

- Năm 2022, những attack vectors phổ biến nhất là *compromised credentials* với 19% các vụ vi phạm và *phishing* với 16% các vụ vi phạm.” Trên thực tế, attack vector gây thiệt hại lớn nhất là *phishing* với giá trị **4,91 triệu USD**.

Theo **Data Breach Investigations Report** năm 2022 của Verizon:

- Phishing là một trong những nguyên nhân chính gây ra các vụ vi phạm. Theo báo cáo, “Yếu tố con người tiếp tục là nguyên nhân chính. Trong năm nay, 82% các vụ vi phạm liên quan đến yếu tố con người.”



PHISHING

DOS/DDOS

VNPT AntiDDoS

Prevent DDoS attack solution
Provided by VNPT Cyber Immunity

Trên hệ thống **VNPT Anti DDoS** ghi nhận (trong năm 2022):

- Các cuộc tấn công trên **1 Gbps** ghi nhận: **~700** cuộc
- Cuộc tấn công DDoS lớn nhất đạt: **Trên 200 Gbps**

Cập nhật pháp luật liên quan đến An toàn thông tin mạng tại Việt Nam đến năm 2023

SỐ HIỆU

Luật an toàn thông tin mạng 86/2015/QH13

Chỉ thị 14/CT-TTg năm 2019

QĐ 964/QĐ-TTg Ngày 10/8/2022

QĐ 566/QĐ-BTTTT Ngày 06/04/2023

NỘI DUNG CHÍNH

Luật An toàn thông tin mạng

Về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam

Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

Quyết định Ban hành Kế hoạch hành động triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

CÁC ĐIỂM NỔI BẬT

Quy định về hoạt động an toàn thông tin mạng, quyền và trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng

Các bộ, cơ quan ngang bộ đảm bảo tỷ lệ kinh phí cho các SPDV ATTT mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng CNTT hàng năm

Năng lực quốc gia về bảo đảm an toàn, an ninh mạng được nâng cao, chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn xã hội; bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân Việt Nam trên không gian mạng.

Tổ chức triển khai có hiệu quả các nhiệm vụ được giao tại Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

Cập nhật pháp luật liên quan đến An toàn thông tin mạng tại Việt Nam đến năm 2023

SỐ HIỆU

NỘI DUNG CHÍNH

CÁC ĐIỂM NỔI BẬT

Số: 1552/BTTTT-CATT

Đôn đốc tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình “4 lớp”

Triển khai bảo đảm an toàn thông tin theo mô hình “4 lớp”: (1) “Lớp 1” Lực lượng tại chỗ; (2) “Lớp 2” Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp; (3) “Lớp 3” Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; (4) “Lớp 4” Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia

Số: 1552/BTTTT-THH

Hướng dẫn kỹ thuật triển khai đề án 06

Hướng dẫn các tiêu chí triển khai kỹ thuật đáp ứng kết nối với hệ thống CSDLQG về Dân Cư

Nghị định 85/2016/NĐ-CP

Nghị định về bảo đảm an toàn hệ thống thông tin theo cấp độ

Nghị định áp dụng đối với các cơ quan, tổ chức, cá nhân tham gia hoặc có liên quan đến hoạt động xây dựng, thiết lập, quản lý, vận hành, nâng cấp, mở rộng HTTT tại Việt Nam phục vụ ứng dụng CNTT trong hoạt động của cơ quan, tổ chức nhà nước, ứng dụng CNTT trong việc cung cấp dịch vụ trực tuyến phục vụ người dân và doanh nghiệp. Các văn bản liên quan 713/CATT-TĐQLGS, TCVN 11930:2017, Thông tư 12/2022/TT-BTTTT

09/2020/TT-NHNN

Quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng

Quy định quá trình vận hành hệ thống thông tin, tổ chức định kỳ thực hiện đánh giá an ninh bảo mật tối thiểu sáu tháng một lần hệ thống thông tin mức độ 3, một năm một lần với hệ thống thông tin cấp độ 2, hai năm một lần với hệ thống thông tin cấp độ 1

AN TOÀN, AN NINH MẠNG VỚI MỤC TIÊU CHUYỂN ĐỔI SỐ NĂM 2023



**ỦY BAN QUỐC GIA
VỀ CHUYỂN ĐỔI SỐ**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

KẾ HOẠCH

Hoạt động của Ủy ban Quốc gia về chuyển đổi số năm 2023

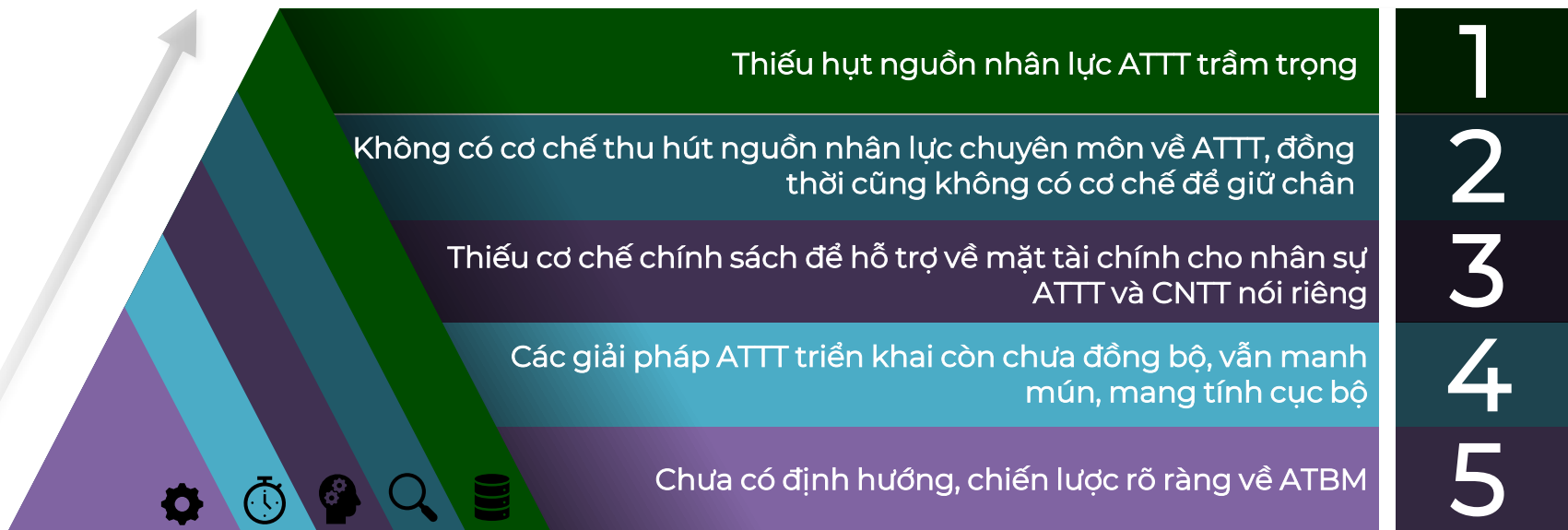
*(Ban hành kèm theo Quyết định số 17/QĐ-UBQGČĐS ngày 04 tháng 4 năm 2023
của Chủ tịch Ủy ban Quốc gia về chuyển đổi số)*

I. MỤC TIÊU

Ủy ban Quốc gia về chuyển đổi số tập trung chỉ đạo, điều phối các bộ, ngành, địa phương tiếp tục đẩy mạnh chuyển đổi số theo hướng mang lại kết quả thực chất, bền vững, ưu tiên nguồn lực để đạt được các chỉ tiêu quan trọng thuộc các Chương trình, Chiến lược quốc gia về phát triển Chính phủ số, kinh tế số và xã hội số.

- Tỷ lệ hệ thống thông tin của cơ quan nhà nước hoàn thành phê duyệt cấp độ an toàn hệ thống thông tin trên 80%
- Tỷ lệ hệ thống thông tin của cơ quan nhà nước đáp ứng yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ trên 30%
- Tỷ lệ thuê bao điện thoại di động thông minh có sử dụng phần mềm an toàn thông tin mạng cơ bản trên 20%
- Tỷ lệ hộ gia đình có đường Internet cáp quang băng rộng có sử dụng giải pháp an toàn thông tin mạng cơ bản đạt trên 10%

Các vấn đề về quản trị ATTT trong khối Cơ quan nhà nước



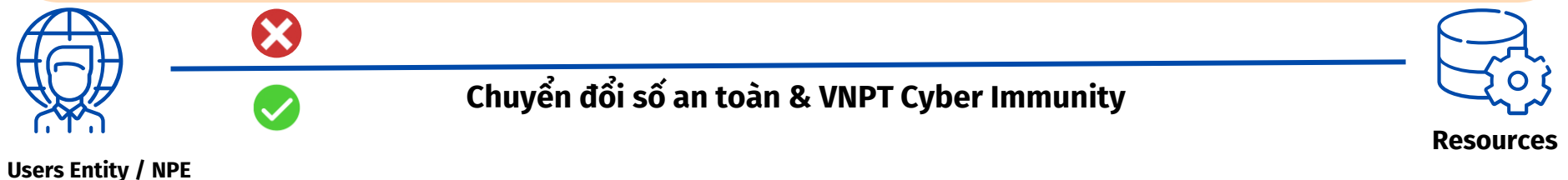
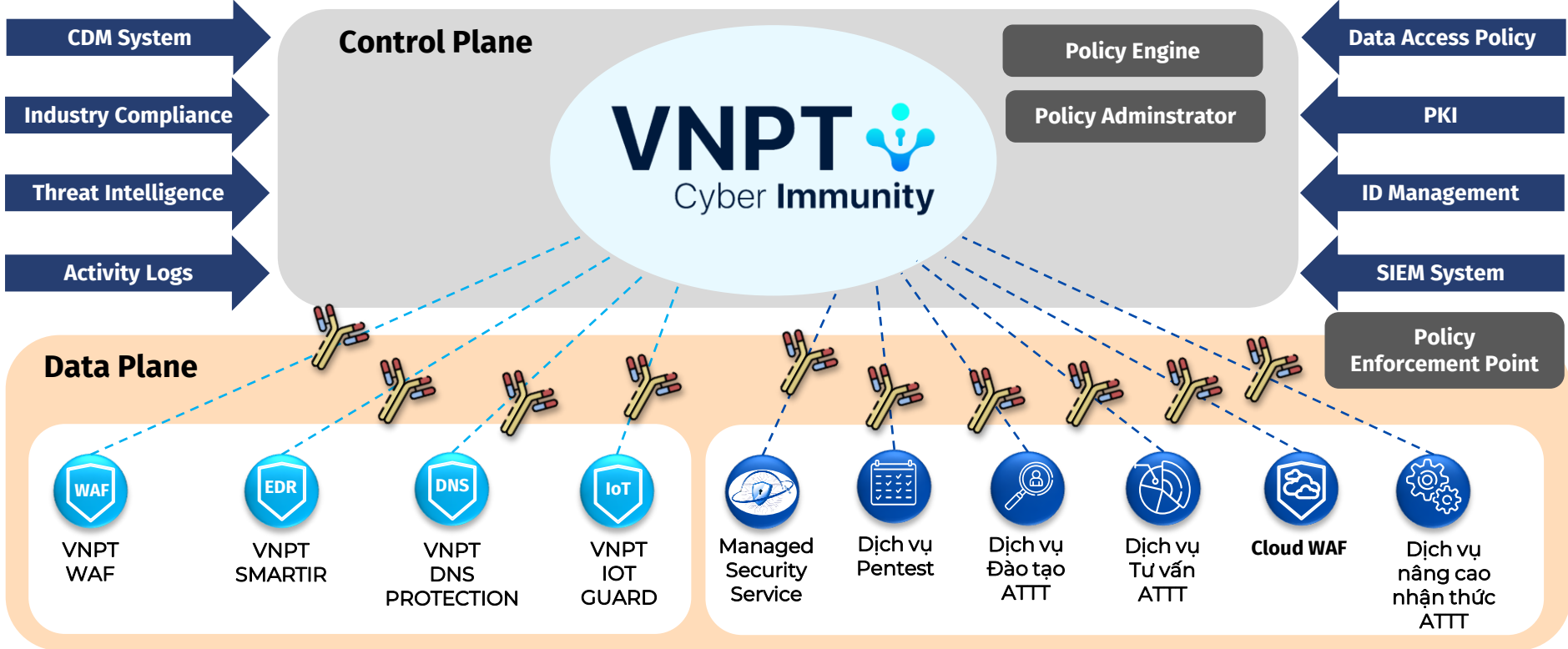
Các vấn đề khối doanh nghiệp SOE, SME gặp phải



CONCEPT

**VNPT
CYBER
IMMUNITY**





02 Security as a Service

Lời giải của bài toán đảm bảo ATTT cho tổ chức, doanh nghiệp



VNPT MSS

Nền tảng Quản lý an toàn thông tin



Managed Security Service

Sử dụng những công nghệ tiên tiến nhất, với đội ngũ nhân lực trình độ cao, giúp doanh nghiệp, tổ chức hạn chế, giảm thiểu thiệt hại rủi ro, bảo vệ giá trị cốt lõi của tổ chức, doanh nghiệp



Máy chủ có hành vi kết nối đến C&C



Resources

Hỗ trợ đảm bảo ATTT cho tổ chức, doanh nghiệp



Giám sát 24/7, theo dõi tất cả các nguồn log (firewall IPS/IDS, network, database server, file server, domain controller, DNS, email, web/app, AD, Endpoint...)



Ngăn chặn các cuộc tấn công vào hạ tầng của khách hàng.



Khuyến nghị các giải pháp, tăng cường ATBM hạ tầng của khách hàng



Đội ngũ Giám sát ATTT có kỹ năng chuyên sâu, kinh nghiệm, **phát hiện và cảnh báo theo thời gian thực** đối với các cuộc tấn công/hành vi bất thường



Xác định nguyên nhân, tiến hành khắc phục sự cố, rà soát, tìm ra các điểm yếu dẫn đến nguy cơ tấn công (root cause)

Kết quả đầu ra



Báo cáo kết quả đánh giá và xử lý APTT hệ thống chi tiết định kỳ theo tuần/tháng/quý/đợt xuất



Cung cấp các cảnh báo (Alert) sự kiện đa nền tảng: Email/SMS, Phone call, OTT

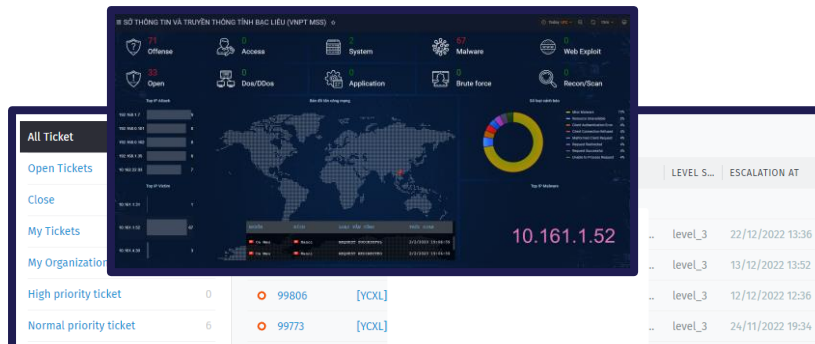
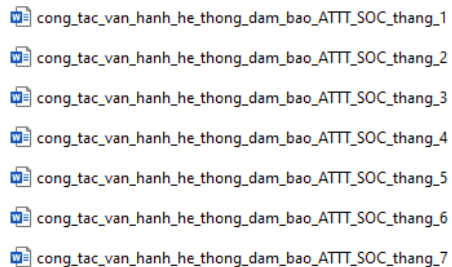


Báo cáo tổng quan về tình hình APTT trên không gian mạng theo các nguồn từ VCI-CTIP



Giao diện

- VNPT MSS Dashboard
- Incident Management



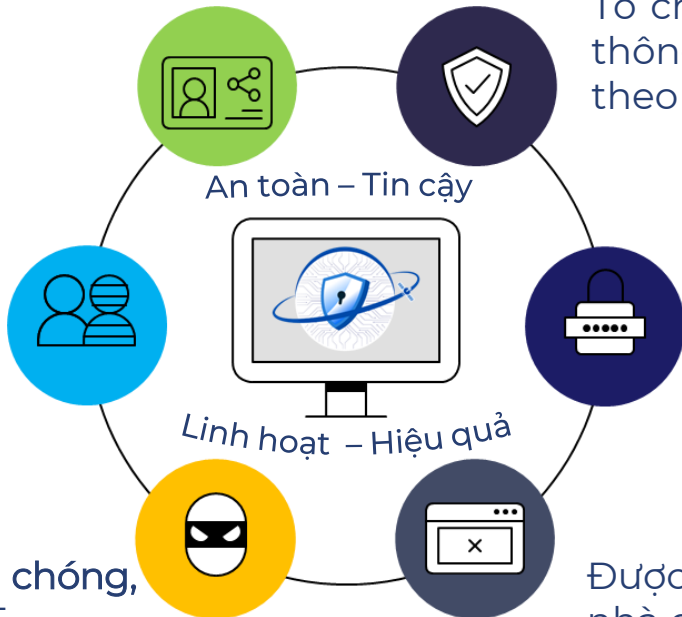
Nền tảng quản lý ATTT đã giải quyết được các bài toán đảm bảo ATTT cho cơ quan, tổ chức nhà nước

Bảo vệ tổ chức, doanh nghiệp trước các cuộc tấn công, giảm thiểu rủi ro mất ATTT

Đáp ứng VB 1552/BTTTT-CATT

Tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình “4 lớp”

Đáp ứng việc kết nối chia sẻ dữ liệu giám sát theo Chỉ thị 14/CT-TTg và văn bản 2973/BTTTT-CATT



Giúp tổ chức, doanh nghiệp tối ưu hóa về thời gian, công sức và chi phí cũng như hiệu quả trong việc quản trị an toàn thông tin

Hỗ trợ và phản ứng nhanh chóng, 24/7 trước những sự cố ATTT

Được vận hành bởi đội ngũ ATTT từ nhà cung cấp dịch vụ ATTT có năng lực thực chiến

Khách hàng



Cổng thông tin
điện tử Chính phủ



Trực liên thông văn bản
Quốc gia



CỔNG THÔNG TIN ASEAN VIỆT NAM
ASEAN – CỘNG ĐỒNG CỦA NHỮNG CƠ HỘI



CỔNG DỊCH VỤ CÔNG QUỐC GIA
dichvucong.gov.vn

Cổng dịch vụ công quốc gia



Gia Lai



Quảng Nam



Kon Tum



Đắk Lắk



Nghệ An



An Giang



Lai Châu



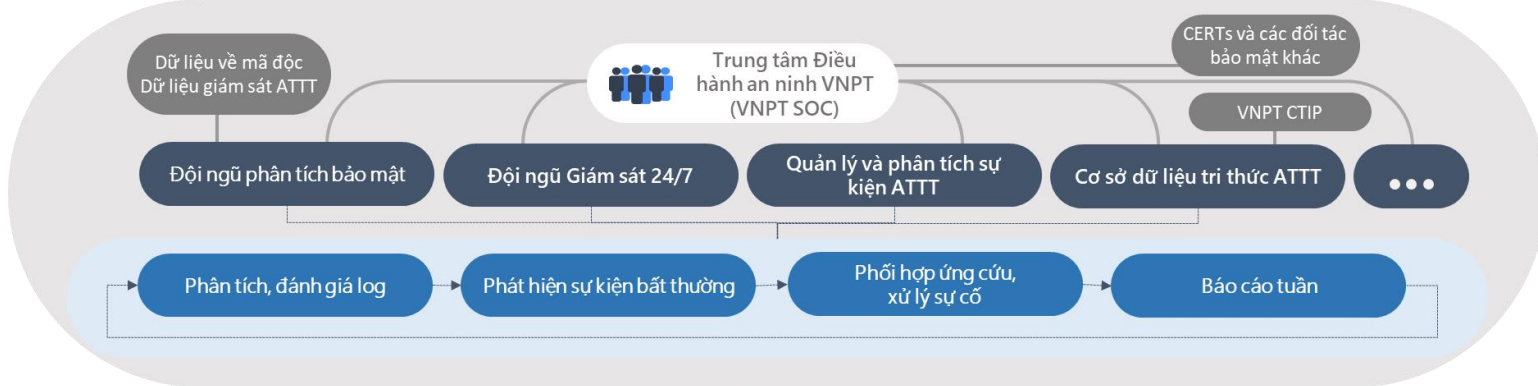
Vĩnh Long



Bạc Liêu



Hòa Bình



Case study:



- VNPT đã tổ chức triển khai **giám sát/phát hiện và xử lý các sự cố an ninh mạng** cho ba hệ thống dịch vụ Công nghệ thông tin cung cấp cho Văn phòng Chính phủ.
- Từ tuần 1 đến tuần 17 năm 2023, VNPT đã **chủ động phát hiện và phối hợp ngăn chặn 3,243 trường hợp dò quét và tấn công khai thác Web Exploit, XSS, SQLi** từ bên ngoài vào hệ thống.
- Đảm bảo hệ thống luôn **khỏe mạnh, dữ liệu luôn được bảo vệ**.

VNPT Cyber Immunity



THANK YOU

Email: security@vnpt.vn

Tel: 0243.7265.171 / 0243.7265.276

Office: VNPT Tower, 57 Huynh Thuc Khang, Dong Da District, Hanoi