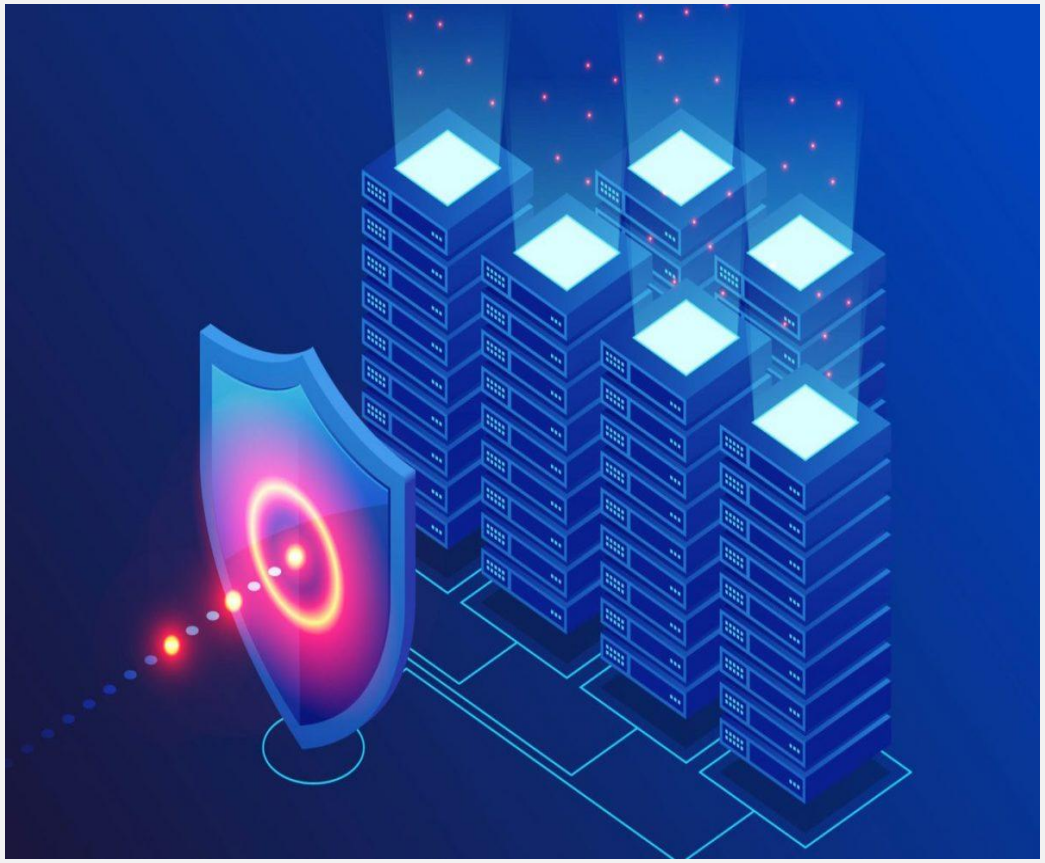
CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN TẠI THÀNH PHỐ ĐÀ NẴNG

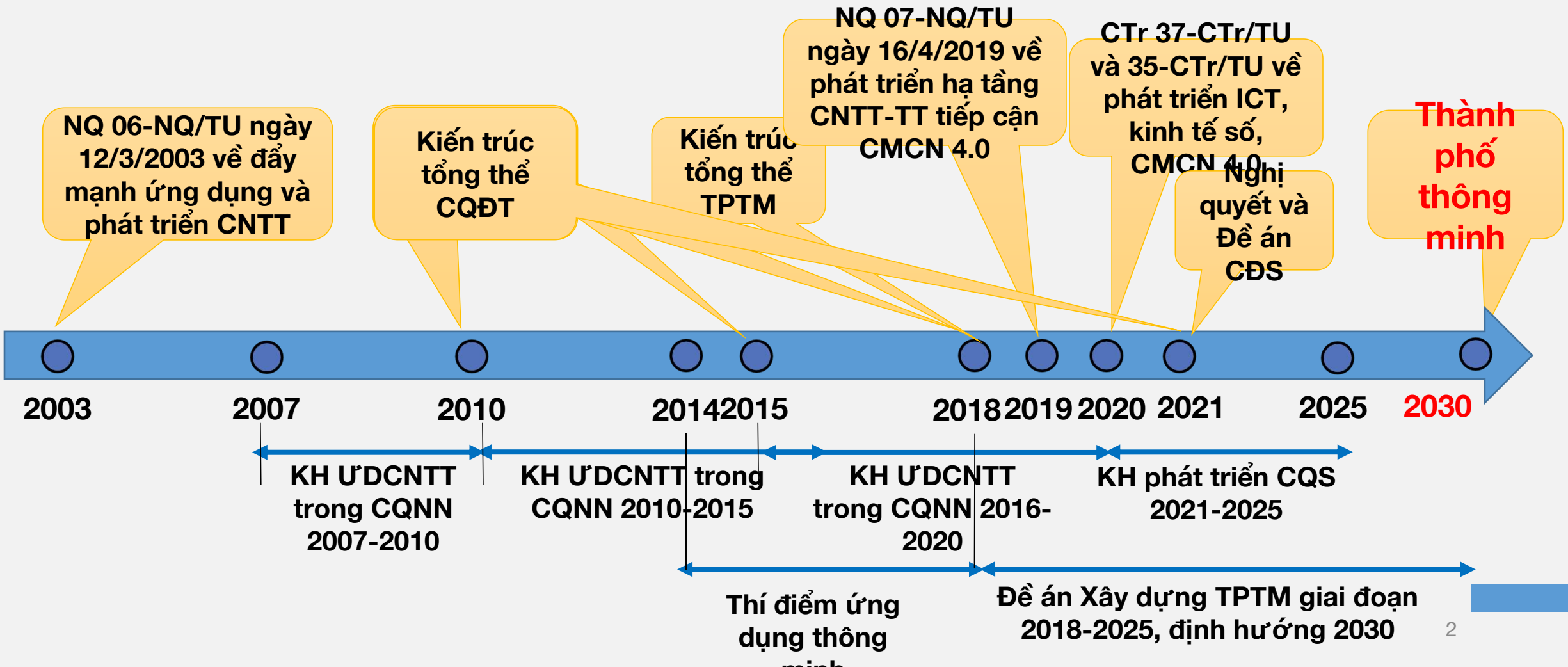


Lê Tự Việt Thắng – TP.ATTT&CNCL

Trung tâm Chuyển đổi số và Công nghệ chiến lược Đà Nẵng

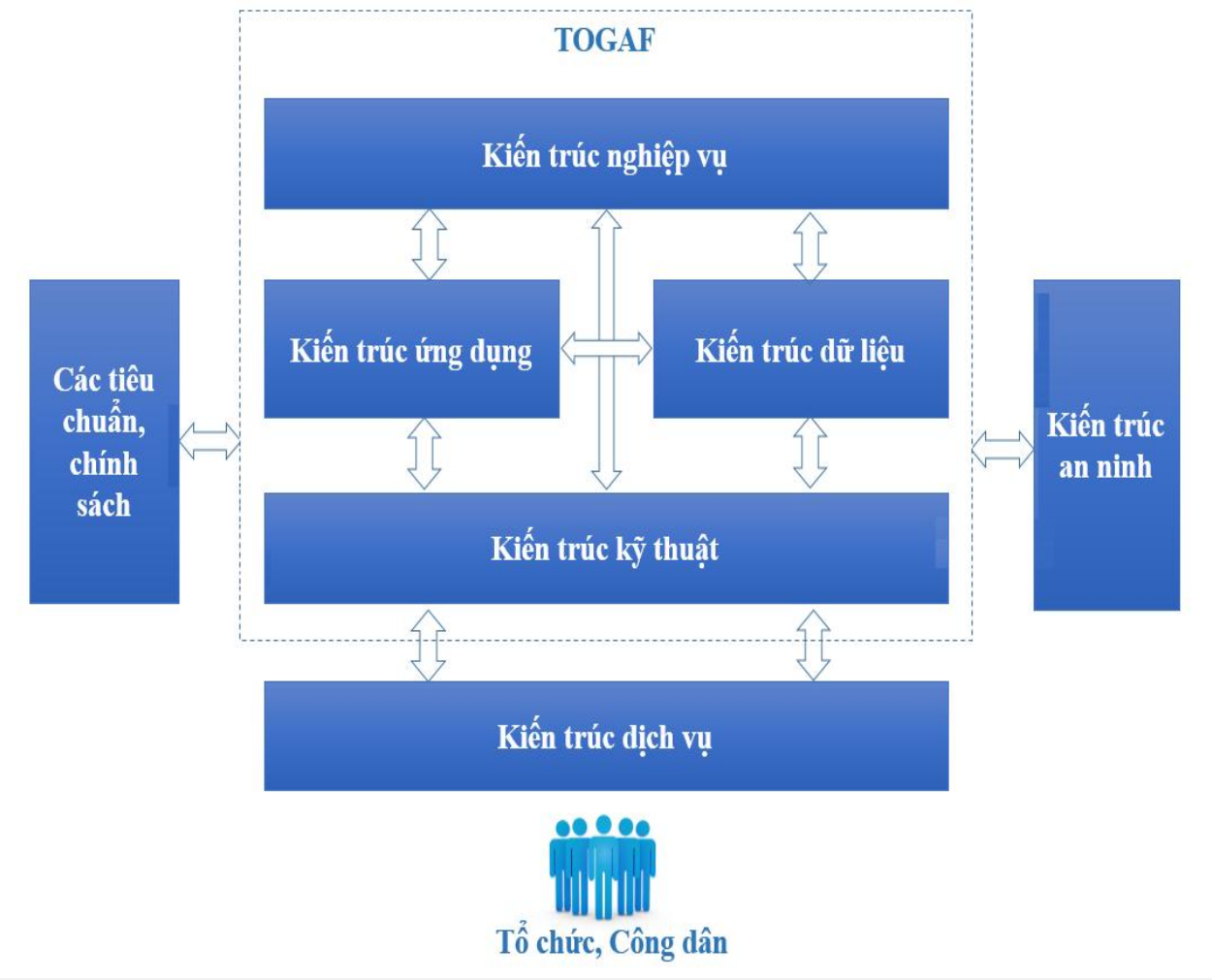
QUAN ĐIỂM VỀ AN TOÀN THÔNG TIN

Quan điểm: An toàn thông tin được xác định là yếu tố then chốt không thể tách rời trong quá trình xây dựng Chính quyền điện tử, thành phố thông minh và chuyển đổi số của Đà Nẵng



MỤC TIÊU, CÁCH TIẾP CẬN VỀ AN TOÀN THÔNG TIN

Kiến trúc an toàn thông tin là một kiến trúc thành phần của Kiến trúc Chính quyền điện tử, Thành phố thông minh

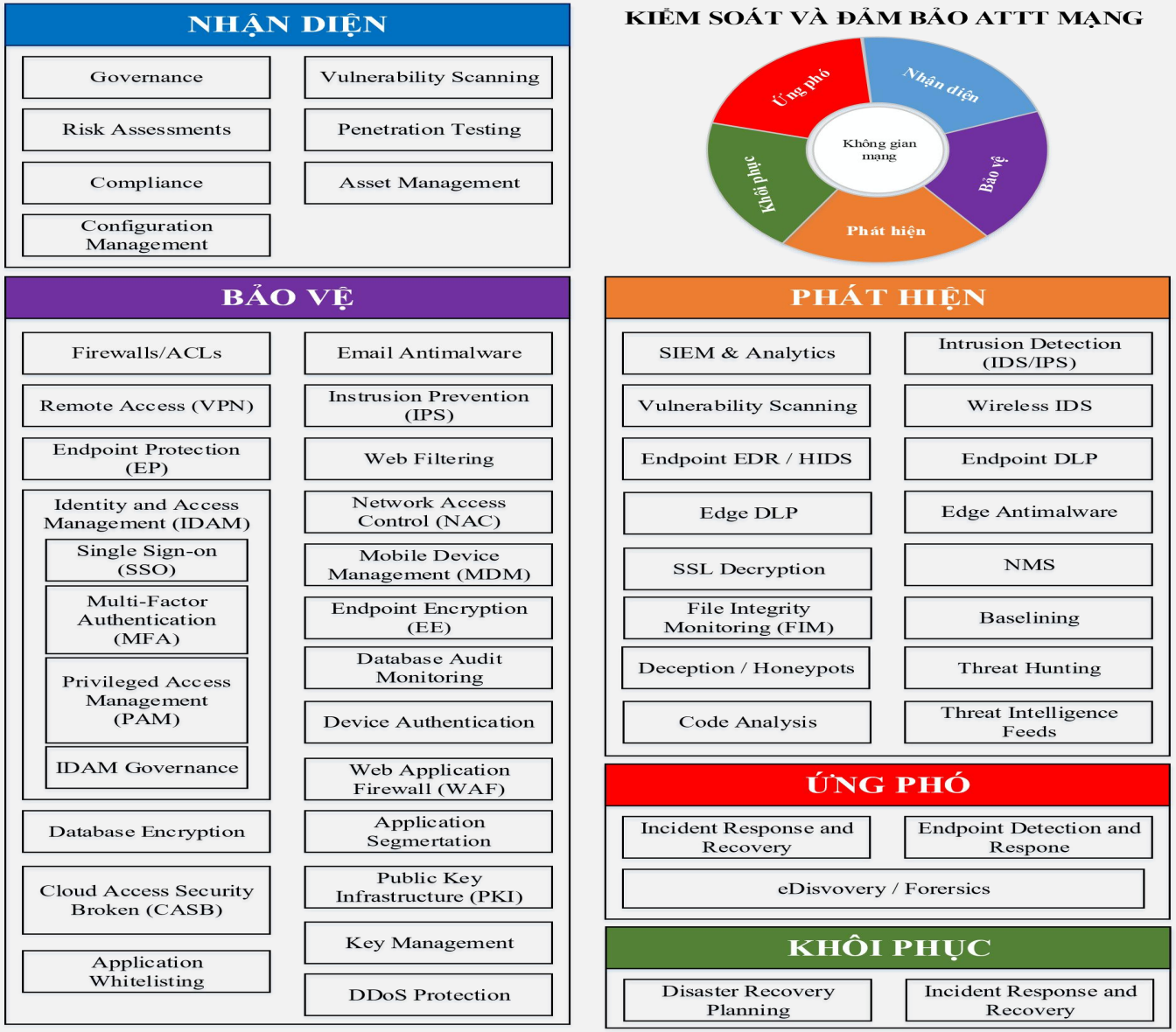


MỤC TIÊU THEO NGHỊ QUYẾT 05-NQ/TU

Thuộc Top 03 địa phương dẫn đầu về chỉ số an toàn thông tin
(cùng với chỉ số chuyển đổi số, chỉ số thương mại điện tử)

CÁCH TIẾP CẬN THEO 04 TRỤ CỘT

MÔ HÌNH AN TOÀN THÔNG TIN



Mô hình ATTT Đà Nẵng triển khai theo mô hình tập trung

- Mạng đô thị dùng riêng kết nối toàn bộ các cơ quan, đơn vị thành phố; kết nối ra Internet tập trung
- Hạ tầng Trung tâm dữ liệu tập trung; ATTT tập trung

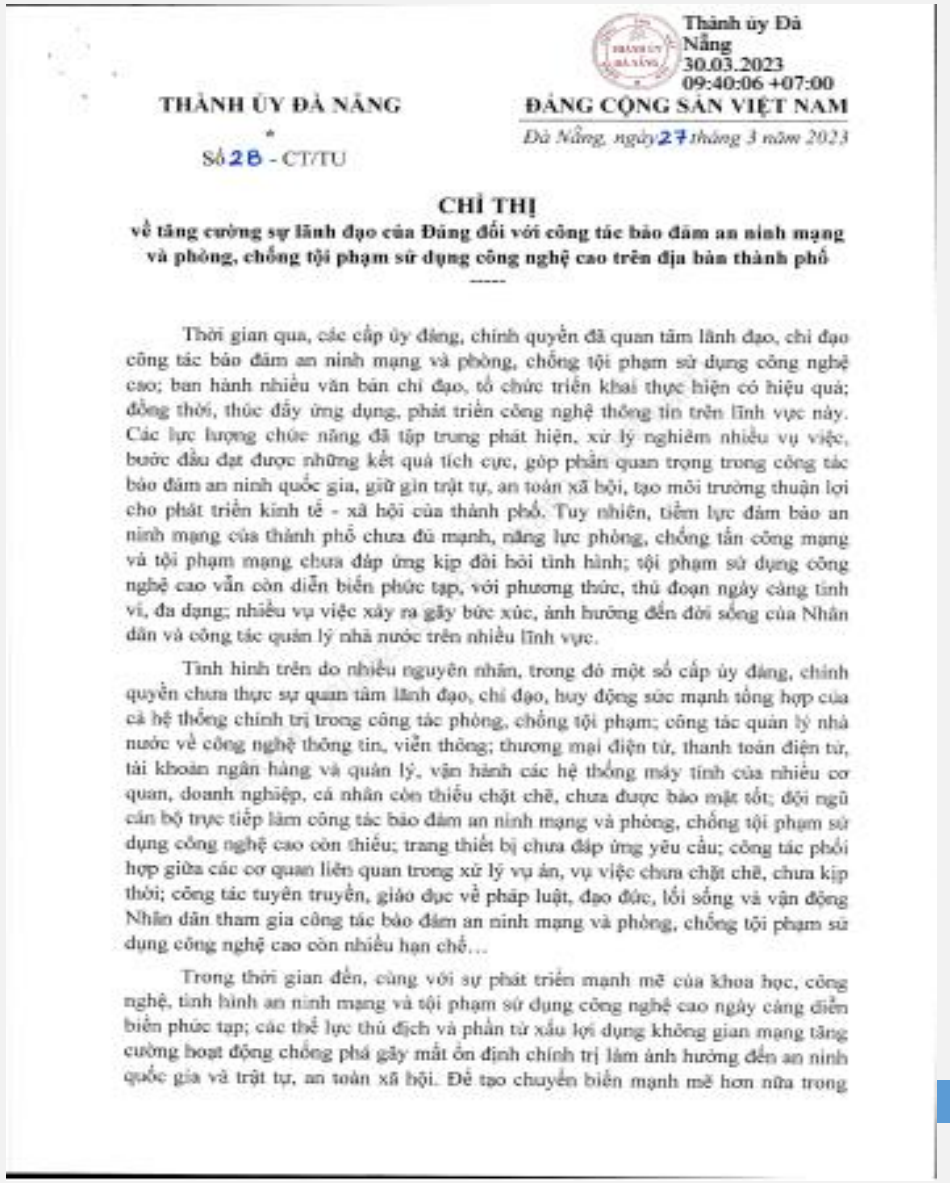
CHÍNH SÁCH, QUY TRÌNH

1. **Chỉ thị số 28-CT/TU ngày 27/3/2023 của Thành ủy về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao trên địa bàn thành phố**

2. **Kế hoạch số 329/KH-UBND ngày 18/5/2020 triển khai Nghị quyết số 22/NQ-CP ngày 18/10/2019 của Chính phủ ban hành Chương trình hành động thực hiện Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia**

3. **Kế hoạch số 90/KH-UBND ngày 26/4/2023 triển khai Chiến lược an toàn, an ninh mạng quốc gia trên địa bàn thành phố**

4. **Kế hoạch triển khai công tác bảo đảm an toàn thông tin hàng năm** (lồng ghép chung Kế hoạch ứng dụng CNTT, chuyển đổi số)



Thành ủy Đà Nẵng
30.03.2023
09:40:06 +07:00

THÀNH ỦY ĐÀ NẴNG

Số 28 - CT/TU

ĐẢNG CỘNG SẢN VIỆT NAM

Đà Nẵng, ngày 27 tháng 3 năm 2023

CHỈ THỊ

về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao trên địa bàn thành phố

Thời gian qua, các cấp ủy đảng, chính quyền đã quan tâm lãnh đạo, chỉ đạo công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; ban hành nhiều văn bản chỉ đạo, tổ chức triển khai thực hiện có hiệu quả; đồng thời, thúc đẩy ứng dụng, phát triển công nghệ thông tin trên lĩnh vực này. Các lực lượng chức năng đã tập trung phát hiện, xử lý nghiêm nhiều vụ việc, bước đầu đạt được những kết quả tích cực, góp phần quan trọng trong công tác bảo đảm an ninh quốc gia, giữ gìn trật tự, an toàn xã hội, tạo môi trường thuận lợi cho phát triển kinh tế - xã hội của thành phố. Tuy nhiên, tiềm lực đảm bảo an ninh mạng của thành phố chưa đủ mạnh, năng lực phòng, chống tấn công mạng và tội phạm mạng chưa đáp ứng kịp đòi hỏi tình hình; tội phạm sử dụng công nghệ cao vẫn còn diễn biến phức tạp, với phương thức, thủ đoạn ngày càng tinh vi, đa dạng; nhiều vụ việc xảy ra gây bức xúc, ảnh hưởng đến đời sống của Nhân dân và công tác quản lý nhà nước trên nhiều lĩnh vực.

Tình hình trên do nhiều nguyên nhân, trong đó một số cấp ủy đảng, chính quyền chưa thực sự quan tâm lãnh đạo, chỉ đạo, huy động sức mạnh tổng hợp của cả hệ thống chính trị trong công tác phòng, chống tội phạm; công tác quản lý nhà nước về công nghệ thông tin, viễn thông; thương mại điện tử, thanh toán điện tử, tài khoản ngân hàng và quản lý, vận hành các hệ thống máy tính của nhiều cơ quan, doanh nghiệp, cá nhân còn thiếu chặt chẽ, chưa được bảo mật tốt; đội ngũ cán bộ trực tiếp làm công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao còn thiếu; trang thiết bị chưa đáp ứng yêu cầu; công tác phối hợp giữa các cơ quan liên quan trong xử lý vụ án, vụ việc chưa chặt chẽ, chưa kịp thời; công tác tuyên truyền, giáo dục về pháp luật, đạo đức, lối sống và vận động Nhân dân tham gia công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao còn nhiều hạn chế...

Trong thời gian đến, cùng với sự phát triển mạnh mẽ của khoa học, công nghệ, tình hình an ninh mạng và tội phạm sử dụng công nghệ cao ngày càng diễn biến phức tạp; các thế lực thù địch và phần tử xấu lợi dụng không gian mạng tăng cường hoạt động chống phá gây mất ổn định chính trị làm ảnh hưởng đến an ninh quốc gia và trật tự, an toàn xã hội. Để tạo chuyển biến mạnh mẽ hơn nữa trong

CHÍNH SÁCH, QUY TRÌNH

5

Ban hành Quy chế bảo đảm an toàn thông tin trên địa bàn thành phố (Quyết định số 4159/QĐ-UBND ngày 14/9/2018; thay thế Quyết định số 9976/QĐ-UBND ngày 21/11/2011) trong đó quy định một số nguyên tắc:

- Bảo đảm an toàn thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong suốt quá trình thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống; được thực hiện một cách đồng bộ, đầu tư tập trung, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng thiết bị, hiệu quả đầu tư.

- Trước khi đưa vào vận hành, khai thác, chủ quản hệ thống thông tin phải thực hiện đánh giá, kiểm định an toàn thông tin

- Từ năm 2019, tất cả hồ sơ thiết kế, đề cương - dự toán chi tiết dự án ứng dụng CNTT đều có hạng mục và chi phí kiểm thử ATTT độc lập (chiếm khoảng 10% trên tổng mức đầu tư)
- Tất cả HTTT đều được đánh giá ATTT trước khi đưa vào sử dụng chính thức

CHÍNH SÁCH, QUY TRÌNH

6 **Áp dụng Tiêu chuẩn quốc tế ISO 27001:2013** về Quản lý an toàn thông tin đối với Trung tâm dữ liệu.

7 **Các hệ thống thông tin đều có ban hành Quy chế quản lý, vận hành, khai thác;** trong đó có các quy định về trách nhiệm bảo đảm ATTT

8 Ban hành Quy trình phối hợp ứng cứu xử lý sự cố; phương án, kịch bản ứng cứu xử lý sự cố ATTT (đặc biệt các sự kiện lớn, các dịp lễ, tết,...).

9 Định kỳ 6 tháng/lần rà quét, xử lý, khắc phục lỗ hổng bảo mật các hệ thống thông tin. Định kỳ hàng tháng sao lưu dự phòng

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM – ISO/IEC 27001:2013

This is to certify that: **DANANG ICT INFRASTRUCTURE DEVELOPMENT CENTER**
02 Quang Trung, Thach Thang Ward,
Hai Chau District,
Da Nang City,
Vietnam

Holds Certificate Number: **IS 710263**

and operates an Information Security Management System which complies with the requirements of ISO/ IEC 27001:2013 for the following scope:

The management of information security for the Provision of Co-Location, Server Leasing, Virtual Hosting, Information Security Consultant Services. This scope is applied for the operation of Datacenter of the Danang ICT Infrastructure Development Center.

This is in accordance with the Statement of Applicability, dated 25.Jul.2019

For and on behalf of BSI: Chris Cheung, Head of Compliance & Risk – Asia Pacific

Original Registration Date: **18/04/2020**
Latest Revision Date: **18/04/2020**
Effective Date: **18/04/2020**
Expiry Date: **17/04/2023**

Page: 1 of 2

IAF ANAB ...making excellence a habit.

CHÍNH SÁCH, QUY TRÌNH

PHÊ DUYỆT CẤP ĐỘ AN TOÀN THÔNG TIN

Cách làm

- Xác định, phân loại các hệ thống thông tin quan trọng
- Tham mưu UBND thành phố ban hành Kế hoạch, Danh mục các hệ thống thông tin quan trọng xây dựng, phê duyệt hồ sơ cấp độ (Công văn số 6821/UBND-STTTT ngày 15/10/2020; Kế hoạch số 969/KH-STTTT ngày 01/10/2020)
- Hướng dẫn mẫu hồ sơ cấp độ riêng cho các cơ quan thành phố → Kế thừa các giải pháp, phương án bảo đảm ATTT
- Thường xuyên rà soát và tham mưu UBND thành phố chỉ đạo đôn đốc xây dựng hồ sơ cấp độ

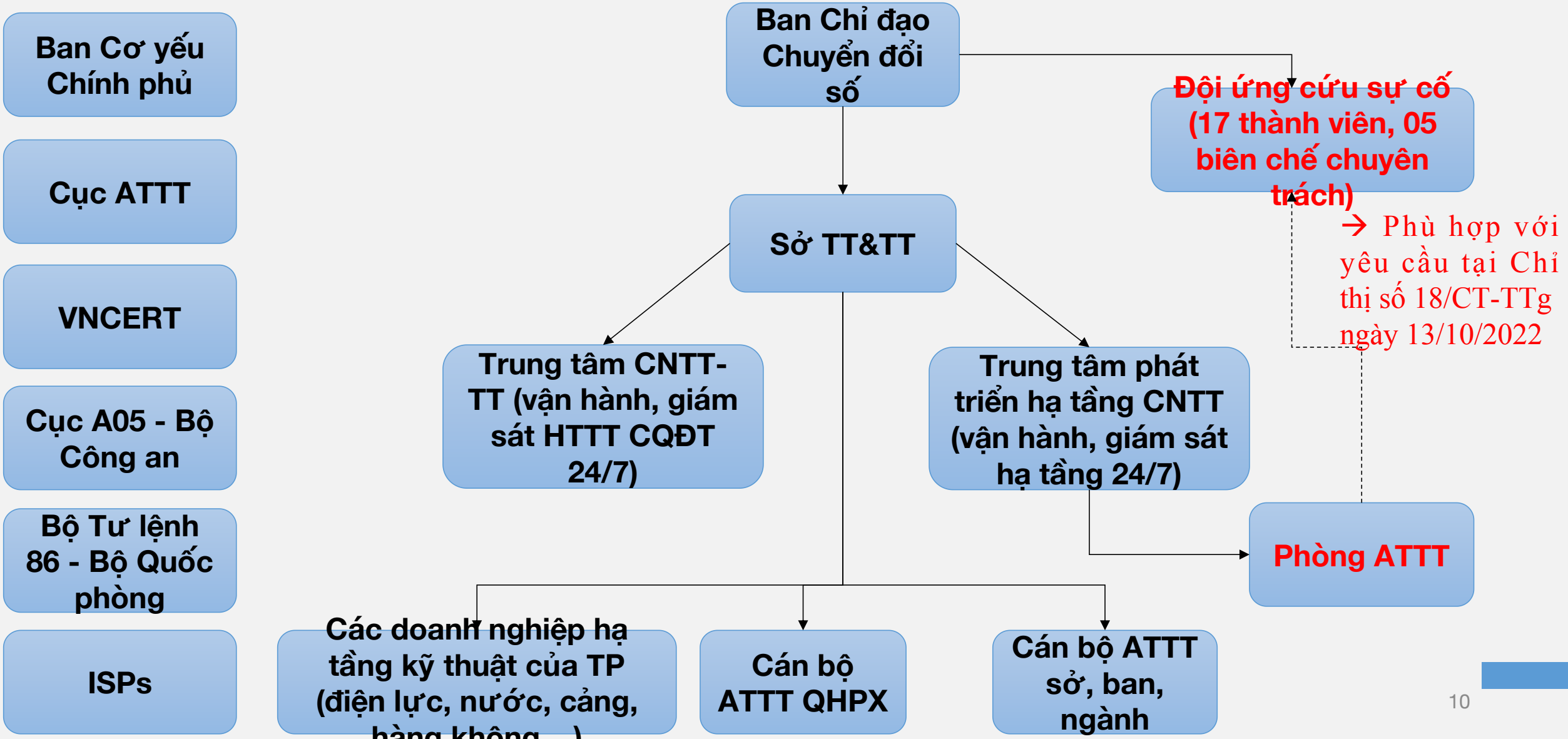
Kết quả

- **HTTT CQĐT thành phố với 12 hệ thống thành phần** đã được Bộ TT&TT thẩm định và UBND TP phê duyệt **cấp độ 4** (Quyết định số 189/QĐ-UBND ngày 25/4/2019)
- **11 hệ thống chuyên ngành** đã được Sở TT&TT thẩm định và UBND TP phê duyệt **cấp độ 3 an toàn thông tin**:
  - Cổng Thông tin điện tử thành phố;
  - Hệ thống điều khiển đèn tín hiệu giao thông; Hệ thống camera giám sát giao thông;
  - Hệ thống CSDL đất đai; Hệ thống quan trắc môi trường;
  - Hệ thống camera giám sát an ninh trật tự;
  - Hệ thống giám sát cấp nước;
  - Hệ thống quản lý cán bộ công chức;
  - Hệ thống CSDL công chứng; Hệ thống CSDL lý lịch tư pháp;
  - Hệ thống điều khiển điện chiếu sáng công cộng

TỔ CHỨC, NHÂN LỰC

- Từ năm 2018 đã thành lập Ban Chỉ đạo xây dựng Chính quyền điện tử và Thành phố thông minh (Quyết định số 5544/QĐ-UBND ngày 21/11/2018); trong đó có nhiệm vụ chỉ đạo, điều phối công tác bảo đảm ATTT và ứng cứu khẩn cấp sự cố ATTT trên địa bàn thành phố (hiện nay đã kiện toàn thành lập Ban Chỉ đạo Chuyển đổi số thành phố)
- Thành lập Tiểu Ban An toàn thông tin trực thuộc Ban Chỉ đạo (Quyết định số 100/QĐ-BCĐ ngày 26/6/2018)
- Thành lập Đội ứng cứu sự cố ATTT
- Hình thành mạng lưới ứng cứu sự cố ATTT trên địa bàn thành phố với các cán bộ chuyên trách/phụ trách ATTT của các sở, ban, ngành, quận huyện, phường, xã, các cơ quan TW, các doanh nghiệp hạ tầng kỹ thuật trên địa bàn
- Hợp tác với các cơ quan chuyên môn ATTT (Cục ATTT, VNCERT, Bộ Tư lệnh 86, Ban Cơ yếu Chính phủ, Cục A05 - BCA)

MẠNG LƯỚI ỨNG CỨU SỰ CỐ ATTT TP. ĐÀ NẴNG



TỔ CHỨC MÔ HÌNH 4 LỚP AN TOÀN THÔNG TIN

Lớp 1	• **Lực lượng tại chỗ**	→ Sở TT&TT là cơ quan thường trực và là đơn vị chuyên trách ATTT; Đội ứng cứu sự cố ATTT; các đơn vị sự nghiệp vân hành, giám sát, bảo đảm ATTT; các cán bộ chuyên trách ATTT tại các sở, ngành, địa phương
Lớp 2	• **Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp**	→ Trung tâm Phát triển hạ tầng CNTT Đà Nẵng có bộ phận chuyên trách giám sát, bảo vệ ATTT
Lớp 3	• **Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ**	→ Trung tâm Phát triển hạ tầng CNTT Đà Nẵng định kỳ kiểm tra đánh giá ATTT (6 tháng/lần); phối hợp với Ban Cơ yếu Chính phủ, VNCERT kiểm tra, đánh giá độc lập
Lớp 4	• **Kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia**	→ Triển khai hệ thống phòng chống mã độc tập trung; kết nối, chia sẻ thông tin, dữ liệu mã độc (100% máy chủ, máy trạm) với NCSC

TUYÊN TRUYỀN, NÂNG CAO NHẬN THỨC AN TOÀN THÔNG TIN

- Tổ chức các hội nghị, hội thảo an toàn thông tin;
- Tổ chức các cuộc thi an toàn thông tin cho học sinh, sinh viên (CTF, Hackathon,...); tập huấn bảo vệ trẻ em thanh thiếu niên trên không gian mạng
- Triển khai chiến dịch làm sạch mã độc

Tập huấn bảo vệ trẻ em thanh thiếu niên trên không gian mạng

Cuộc thi ATTT quốc tế

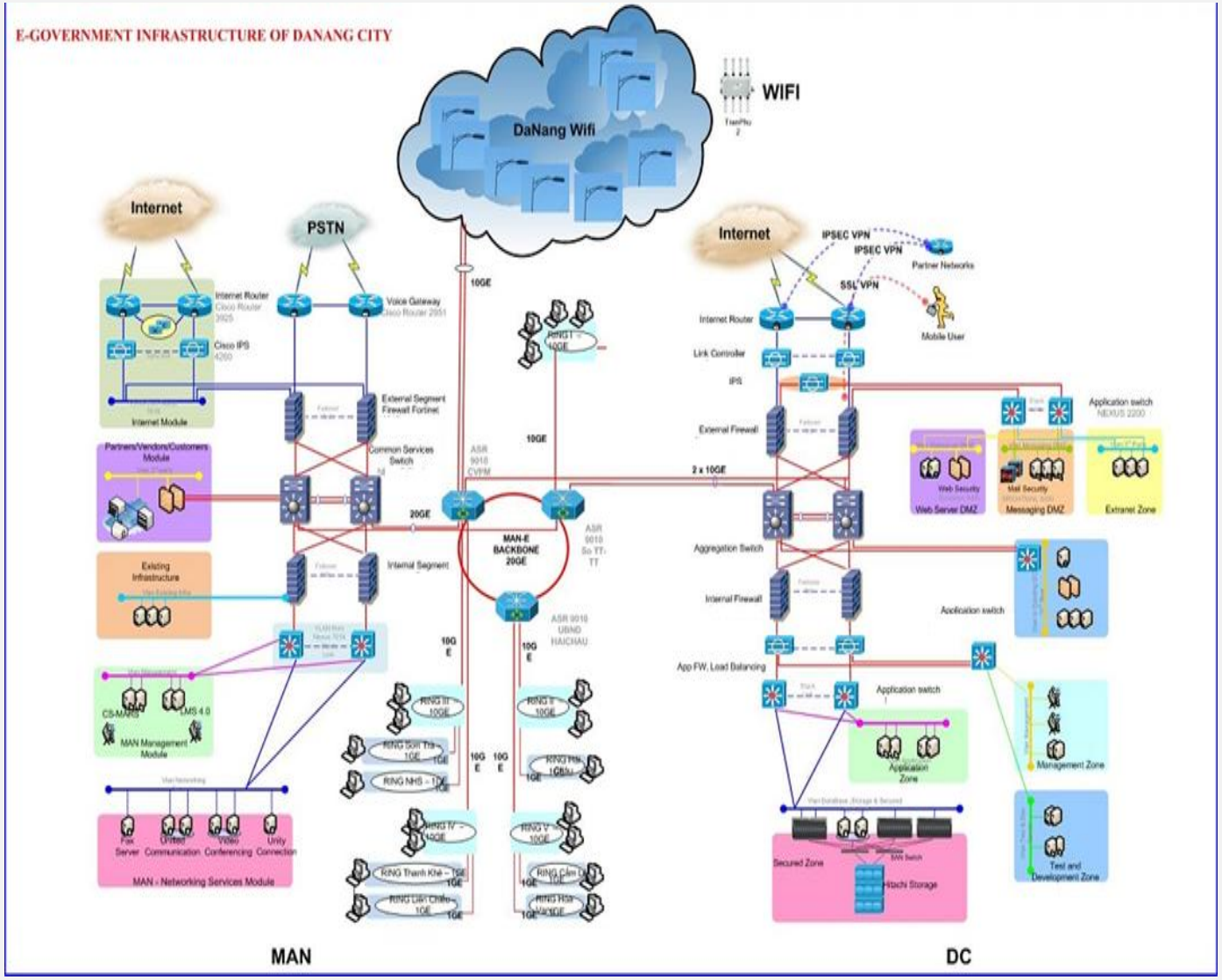
Chiến dịch làm sạch mã độc

ĐÀO TẠO, TẬP HUẤN, DIỄN TẬP AN TOÀN THÔNG TIN

- Từ năm 2017 đến nay; định kỳ hàng năm Đà Nẵng tổ chức diễn tập ứng cứu sự cố ATTT (sự cố tấn công chiếm quyền điều khiển máy chủ, sự cố tấn công DDoS, tấn công ứng dụng web trên nền tảng Liferay,..);
- Cử bộ phận kỹ thuật tham gia các đợt diễn tập ATTT của Trung ương, Quốc tế (Đà Nẵng dẫn đầu Diễn tập ATTT do VNCERT tổ chức năm 2021 về điều tra và xử lý sự cố an toàn thông tin qua lỗ hổng phần mềm)
- Đào tạo, tập huấn kỹ năng chuyên sâu ATTT (giám sát, phân tích lỗ hổng; pentest; điều tra số;...)

Vị trí	Đội	Điểm	Bài thi	Submit cuối
1	STTTT Đà Nẵng	1600	✓✓✓✓✓✓✓✓	22/12/2021 10:49:54
2	Phòng TN ATTTT 1	1600	✓✓✓✓✓✓✓✓	22/12/2021 10:51:22
3	Phòng TN ATTTT 2	1600	✓✓✓✓✓✓✓✓	22/12/2021 10:56:51
4	Phòng TN ATTTT 3	1600	✓✓✓✓✓✓✓✓	22/12/2021 11:02:16
5	Phòng TN ATTTT 4	1600	✓✓✓✓✓✓✓✓	22/12/2021 11:03:32
6	Bkav	1600	✓✓✓✓✓✓✓✓	22/12/2021 11:14:28
7	TT CNTT - Bộ GTVT	1600	✓✓✓✓✓✓✓✓	22/12/2021 11:14:56
8	TT Tin học - VPCP	1100	✓✓✓✓✗✓✓✓	22/12/2021 10:51:32
9	STTT Hải Dương	1100	✓✓✓✓✗✓✓✓	22/12/2021 10:54:05

GIẢI PHÁP KỸ THUẬT AN TOÀN THÔNG TIN

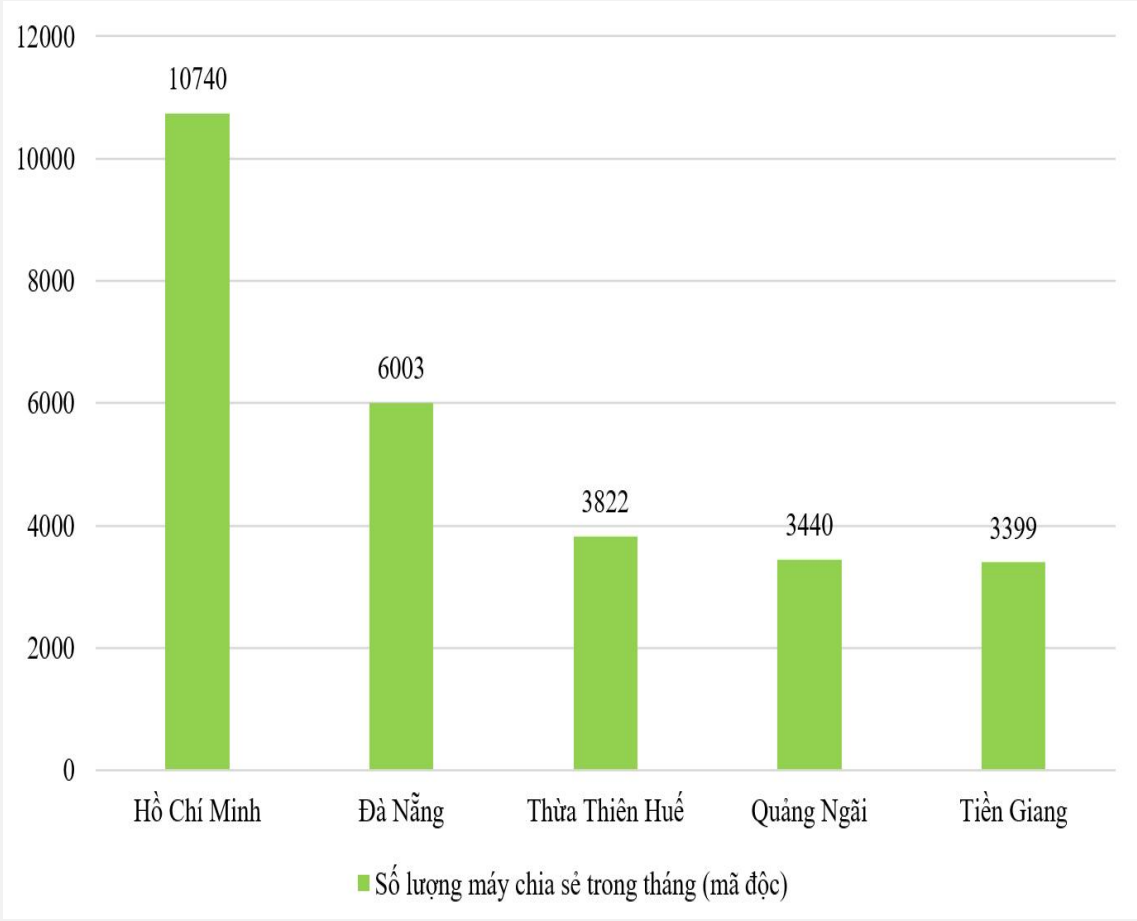


- Kết nối ra Internet tập trung từ hệ thống mạng MAN thực hiện với 03 nhà mạng khác nhau (SPT, Viettel, VNPT) để đảm bảo tính dự phòng, an toàn, thông suốt, hiệu quả.
- Hệ thống tường lửa 2 lớp (Outbound, Inbound); kiểm soát truy cập giữa các phân vùng mạng
- Hệ thống phòng chống xâm nhập trái phép và phòng chống tấn công có chủ đích; thiết bị cân bằng tải, lọc thư rác

HỆ THỐNG PHÒNG CHỐNG MÃ ĐỘC TẬP TRUNG

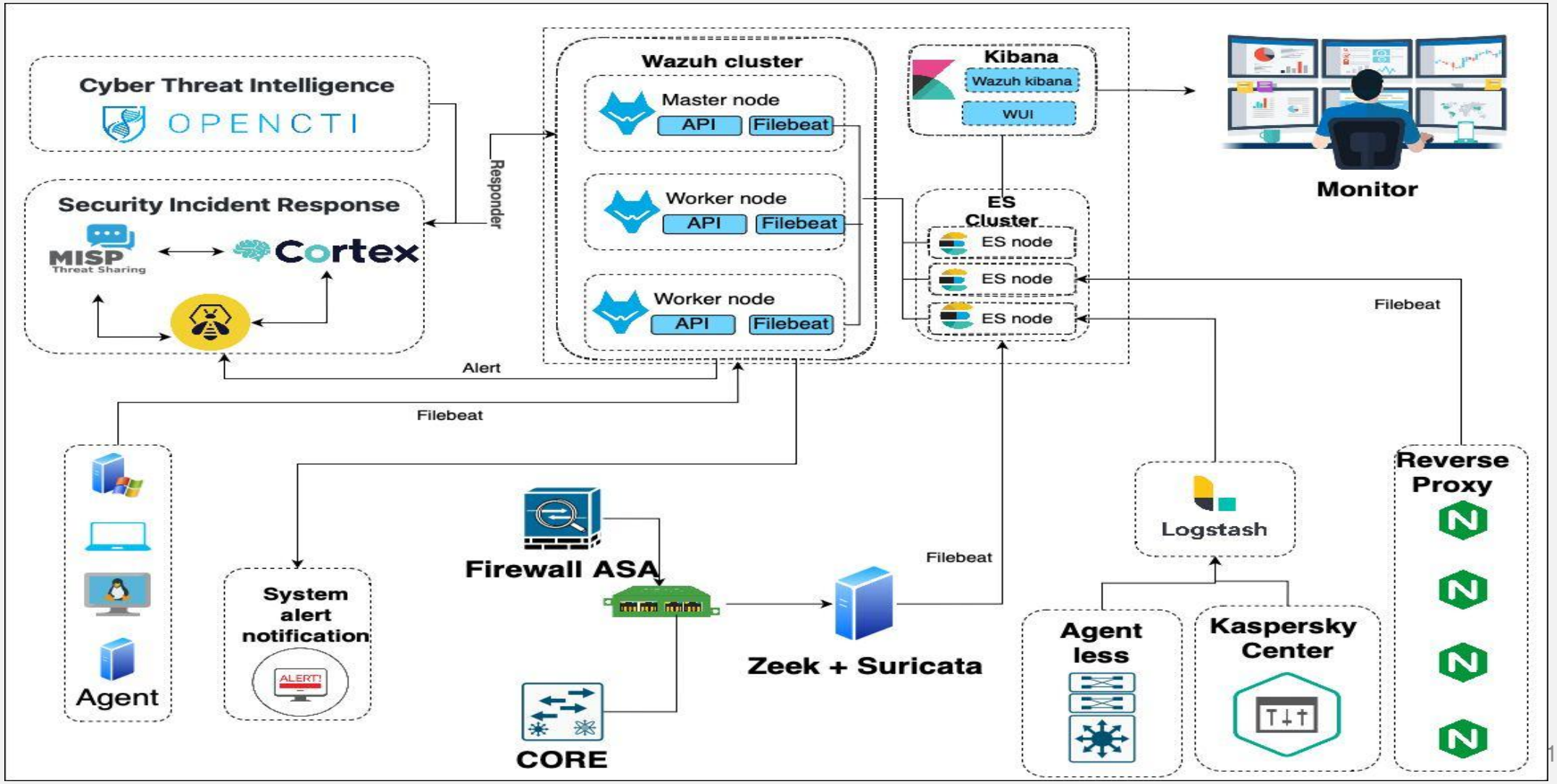
- 100% máy chủ, máy trạm cài đặt Hệ thống phòng chống mã độc tập trung, kết nối với Trung tâm Giám sát không gian mạng quốc gia

Báo cáo định kỳ của Cục ATTT tổng hợp số lượng máy chia sẻ mã độc

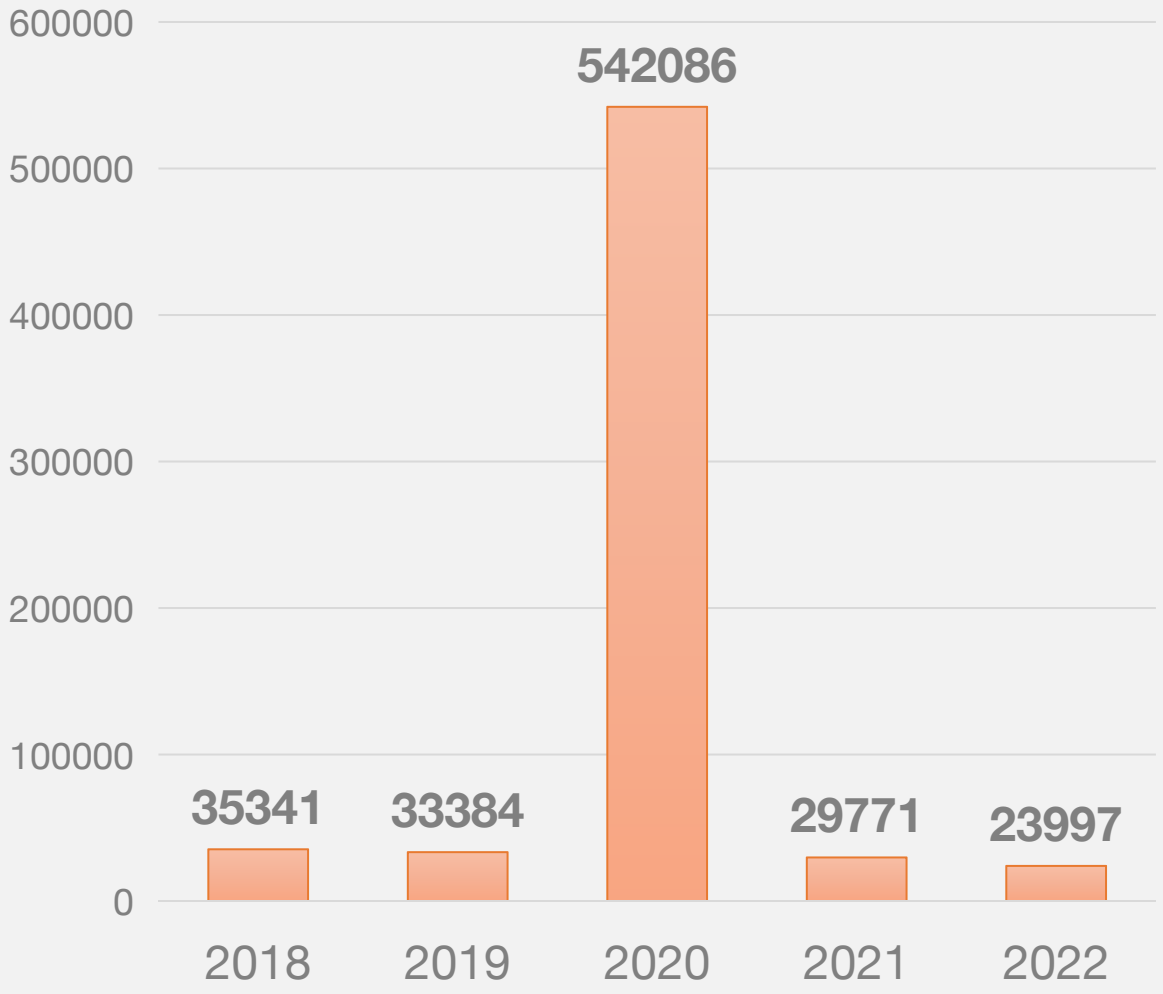


HỆ THỐNG GIÁM SÁT AN TOÀN THÔNG TIN TẬP TRUNG

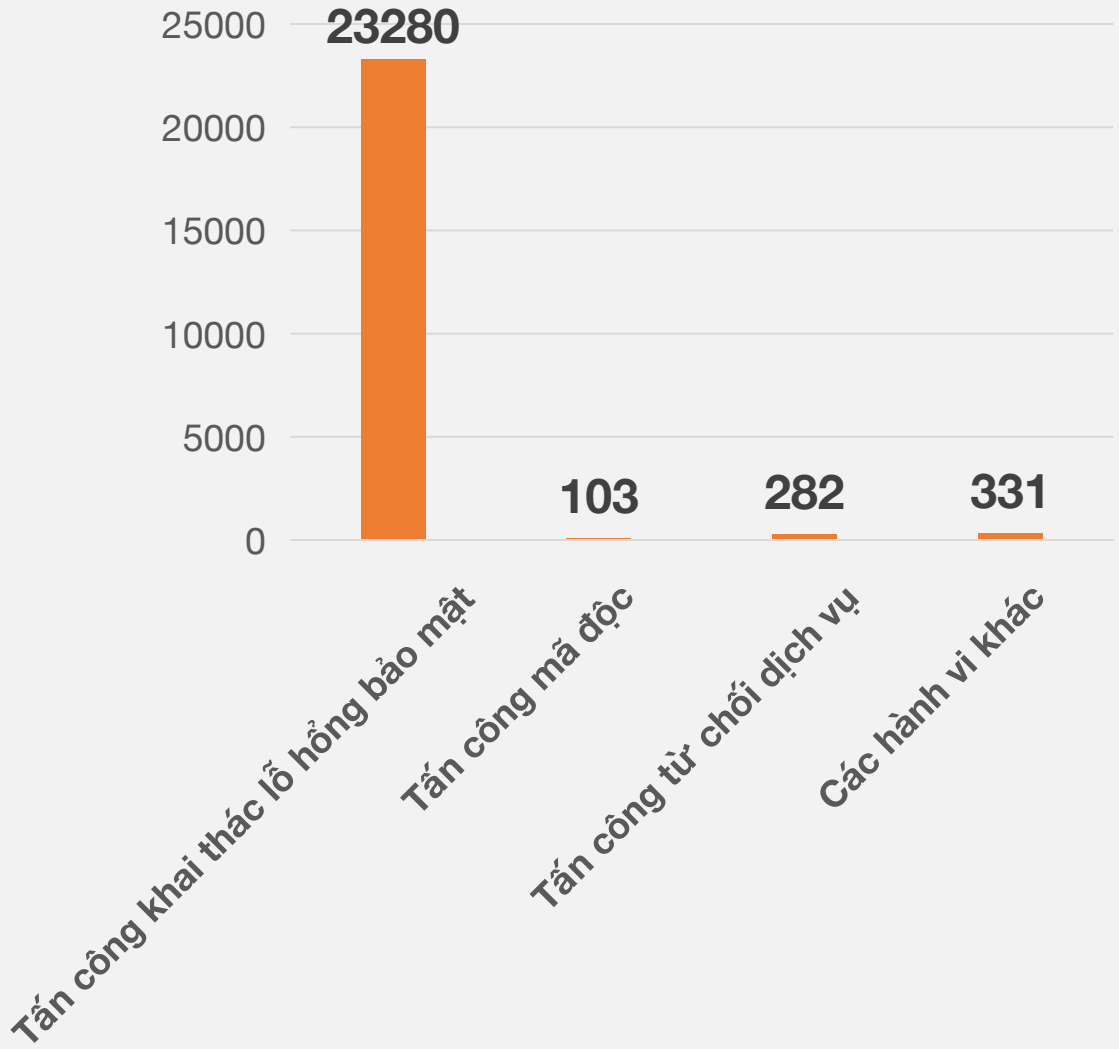
- Kịp thời phát hiện các sự kiện, cảnh báo tấn công, rủi ro ATTT (DDoS, Botnet, SQL,...)



KẾT QUẢ GIÁM SÁT XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN



Số lượng phát hiện và ngăn chặn sự kiện ATTT



Phân loại sự kiện ATTT năm 2022

TRÂN TRỌNG CẢM ƠN