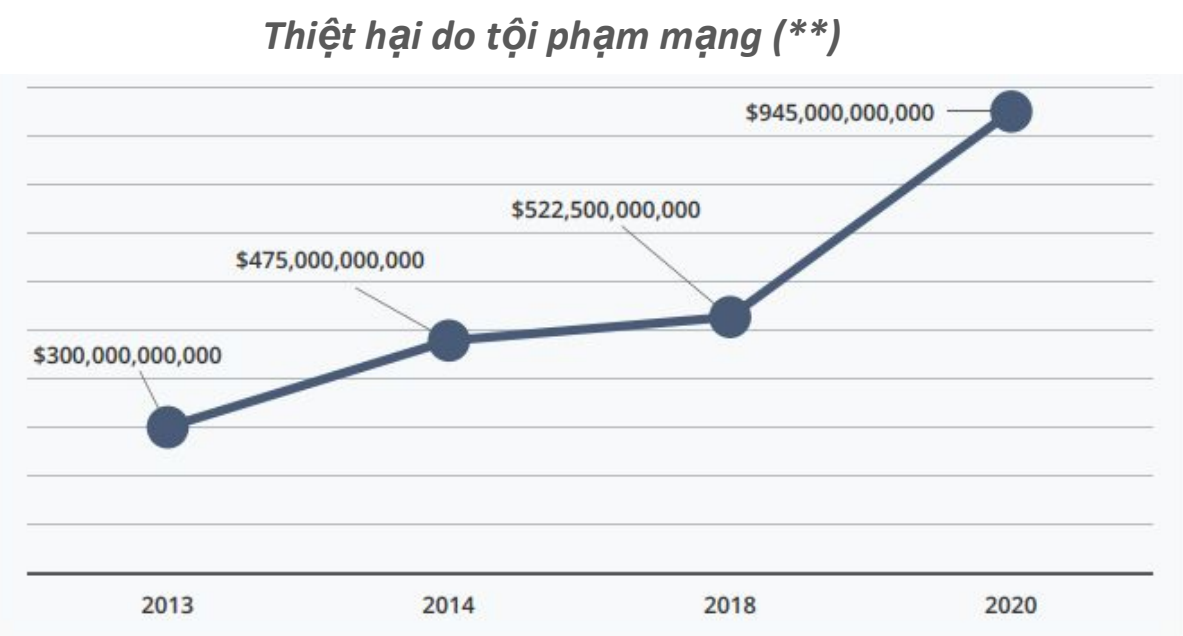
ĐẢM BẢO AN TOÀN TRONG CHUYỂN ĐỔI SỐ

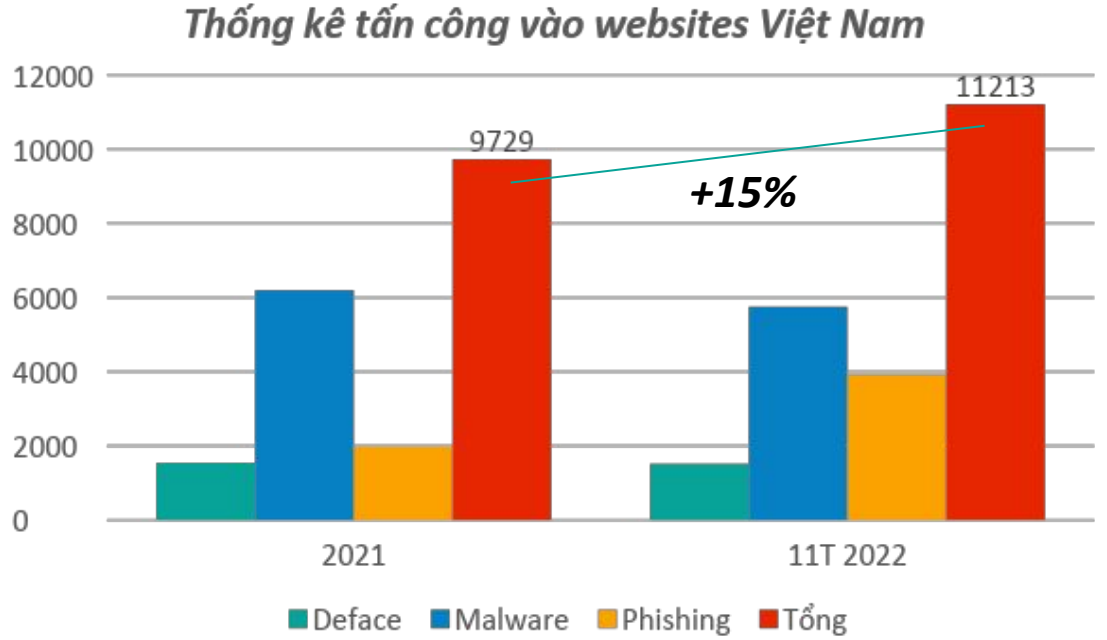
CỤC AN TOÀN THÔNG TIN

VNCERT/CC

VNCERT/CC

SỐ LIỆU VÀ DỰ BÁO





An toàn mạng đến 2025

DOANH THU (*)

- **352** tỷ USD.
- Tăng trưởng 14,5%/năm.

NHÂN LỰC

06 triệu
gấp 2 năm 2020

ĐỐI TƯỢNG

Đối tượng bị tấn công:
- **2025:** gấp 2,7 lần 2020.
- **2030:** gấp 7,5 lần 2020.

NGUY CƠ

- **3.000** cuộc tấn công/giây <> 900
- **12** mã độc/giây <> 5
- **70** lỗ hổng mới/ngày <> 40

- Tấn công mạng quy mô, chuyên nghiệp
- ATTT chuỗi cung ứng
- Ảnh hưởng của công nghệ, AI
- Bùng nổ thiết bị IoT
- Thiếu hụt nguồn nhân lực ATTT

Digital Transformation and Risk Management Must Go Together

https://securityintelligence.com/articles/digital-transformation-risk-management-different-together/,
Chuyển đổi số và Quản lý Rủi ro phải song hành, Khảo sát Rủi ro Toàn cầu của PwC năm 2022

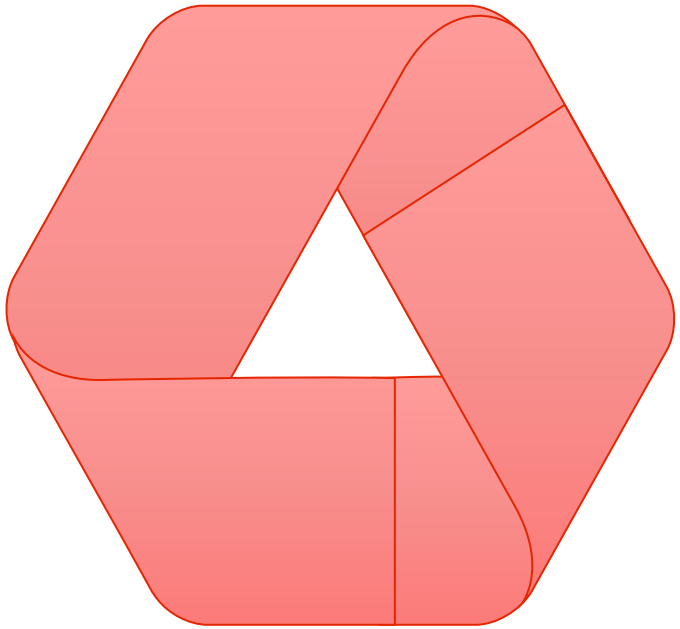
QUAN ĐIỂM VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

Quyết định 749/QĐ-TTg ngày 03/6/2020 Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030

Bảo đảm an toàn, an ninh mạng là **then chốt** để chuyển đổi số **thành công** và **bền vững**, đồng thời là phần **xuyên suốt**, không thể tách rời của chuyển đổi số.

Mọi thiết bị, sản phẩm, phần mềm, hệ thống thông tin, dự án đầu tư về công nghệ thông tin đều phải có **cấu phần bắt buộc về an toàn, an ninh mạng** ngay **từ khi thiết kế**.

NỘI DUNG VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ



Chỉ thị 02/CT-TTg ngày 26/4/2022 về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia:

04 nội dung cần lưu ý *về an toàn thông tin:*

1. Hệ thống thông tin cần **triển khai đầy đủ** phương án bảo đảm an toàn thông tin theo cấp độ.
2. Phần mềm nội bộ phải **do đơn vị chuyên nghiệp** phát triển, tuân thủ Khung phát triển phần mềm an toàn DevSecOps
3. Hệ thống thông tin được kiểm tra, đánh giá an toàn thông tin mạng **trước khi đưa vào sử dụng**, khi nâng cấp, thay đổi, định kỳ theo quy định.
4. Hệ thống thông tin được quản lý, vận hành theo **mô hình 4 lớp**

CHIẾN LƯỢC AN TOÀN, AN NINH MẠNG QUỐC GIA

Quyết định 964/QĐ-TTg ngày 10/08/2022 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

Quan điểm: liên quan chuyển đổi số

+ An toàn, an ninh mạng (ATANM) là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số.

+ ATANM là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân.

+ Đầu tư cho ATANM là đầu tư cho phát triển bền vững và tạo ra giá trị.

CHIẾN LƯỢC AN TOÀN, AN NINH MẠNG QUỐC GIA

Quyết định 964/QĐ-TTg ngày 10/08/2022 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

Mục tiêu:

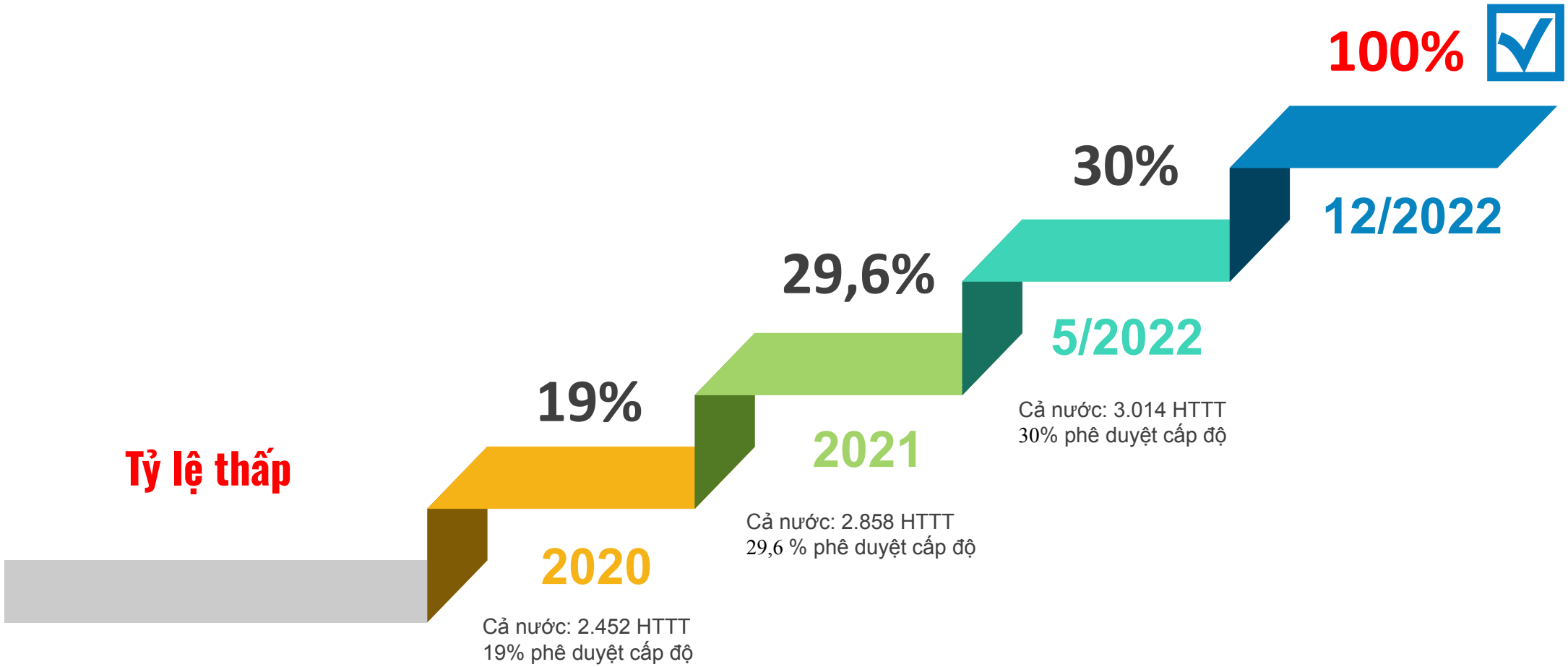
c) Hình thành lực lượng bảo đảm an toàn, an ninh mạng tại các bộ, ngành, cơ quan nhà nước, các tổ chức chính trị – xã hội và các tập đoàn, tổng công ty nhà nước; đảm bảo mỗi cơ quan, tổ chức, doanh nghiệp nhà nước có một bộ phận được giao làm nhiệm vụ làm đầu mối, chịu trách nhiệm về công tả bảo đảm an toàn, an ninh mạng. Khuyến khích các doanh nghiệp khác có một đơn vị bảo đảm an toàn, an ninh mạng.

d) Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, UBND tỉnh, thành phố ...thực hiện bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn thông tin và an ninh mạng.

đ) Bảo vệ hệ thống thông tin của 11 lĩnh vực quan trọng

VNCERT/CC

PHÊ DUYỆT ĐỀ XUẤT CẤP ĐỘ VÀ TRIỂN KHAI PHƯƠNG ÁN BẢO ĐẢM ATTT THEO CẤP ĐỘ



CHỈ THỊ 02 ngày 26/4/2022 của Thủ tướng Chính phủ:

Tháng 12/2022: Hoàn thành phân loại, xác định và phê duyệt đề xuất cấp độ HTTT.

Tháng 06/2023: Triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ

Hướng dẫn mới về ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ, thay thế Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông

Mục đích:

- hướng dẫn chi tiết hơn một số nội dung còn bất cập, chưa được làm rõ
- bảo đảm tính đồng bộ, thống nhất giữa Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP, Tiêu chuẩn quốc gia TCVN 11930: 2017
- phù hợp với tình hình thực tế đã triển khai trong 05 năm qua

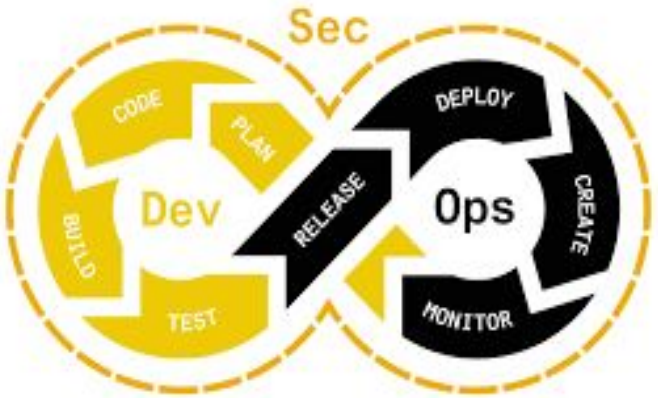
Hiệu lực thi hành: **từ ngày 1/10/2022**

Hướng dẫn mới về ĐẢM BẢO AN TOÀN THÔNG TIN THEO CẤP ĐỘ

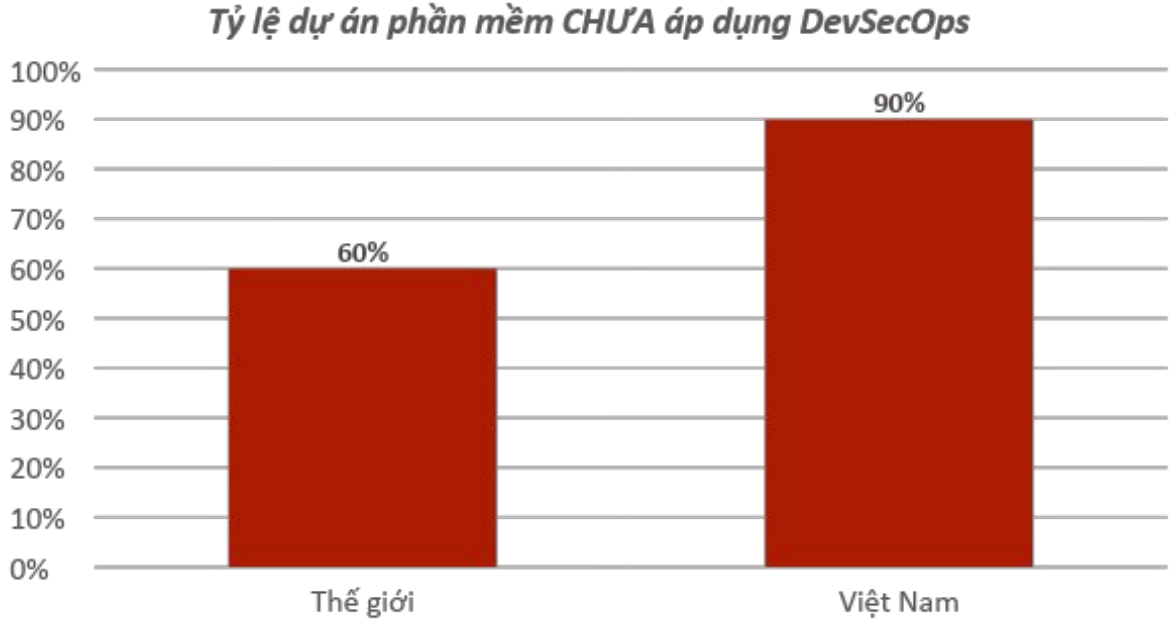
Các điểm mới:

- Làm rõ quy định: xác định chủ quản hệ thống thông tin (HTTT); xác định đơn vị vận hành HTTT; bổ sung **hướng dẫn cụ thể phương án triển khai thẩm định hồ sơ đề xuất cấp độ trong trường hợp đơn vị chuyên trách về an toàn thông tin đồng thời được chủ quản HTTT giao quản lý, vận hành HTTT** (Điều 4, 5, 6)
- Nêu **nguyên tắc xác định các HTTT**, giao Cục An toàn thông tin định kỳ hàng quý có trách nhiệm cập nhật, bổ sung danh mục các HTTT và công bố trên Cổng thông tin điện tử của Bộ Thông tin và Truyền thông (Điều 7)
- **Hướng dẫn thuyết minh cấp độ** an toàn HTTT, các yêu cầu bảo đảm an toàn HTTT theo cấp độ (Điều 8, 9, 10)
- Quy định các **nguyên tắc cơ bản về kiểm tra, đánh giá ATTT, chế độ báo cáo** (Điều 11, 12, 13, 14)
- Bổ sung **quy định về thời điểm phê duyệt Hồ sơ đề xuất cấp độ khi xây dựng mới hoặc mở rộng, nâng cấp HTTT**: khuyến khích hồ sơ đề xuất cấp độ ATTT được phê duyệt trước khi phê duyệt Báo cáo kinh tế kỹ thuật hoặc thiết kế cơ sở, ... (Điều 15)
- Có các **yêu cầu cơ bản bảo đảm an toàn HTTT đối với từng cấp độ** tại các Phụ lục

KHUNG PHÁT TRIỂN PHẦN MỀM AN TOÀN (DEVSECOPS)



Mọi thành phần đều có trách nhiệm đảm bảo an toàn bảo mật

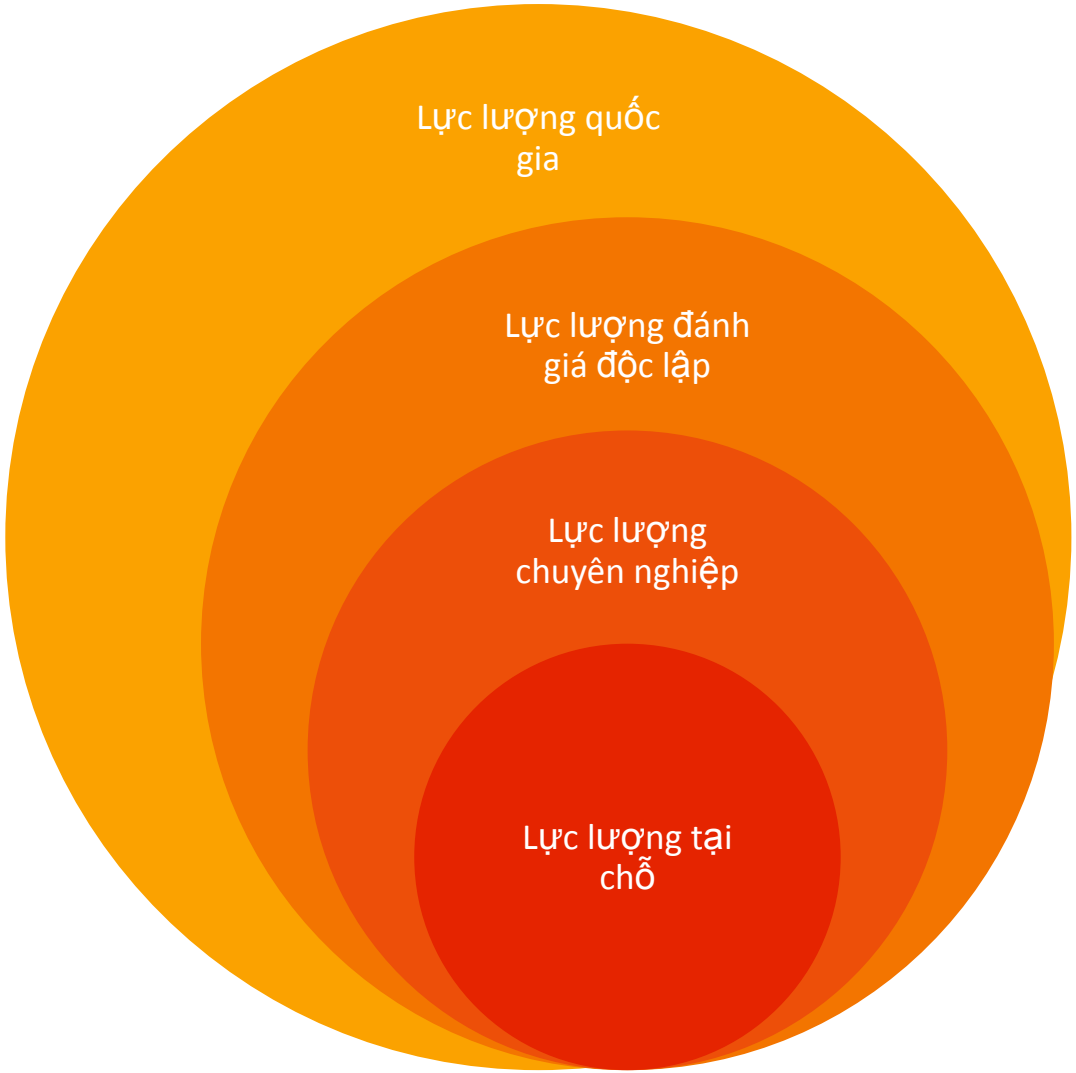


- Áp dụng DevSecOps khi phát triển phần mềm tăng từ **27%** lên **35,9%** năm 2021 (*)
- **90%** dự án phần mềm yêu cầu tuân theo DevSecOps trước năm 2022, tăng **40%** so 2019 (**)

Công văn số 166 /CATTT-ATHTTT Ban hành hướng dẫn "Khung phát triển phần mềm an toàn (phiên bản 1.0)"

Xây dựng theo NIST Special Publication 800-218: Secure Software Development Framework (SSDF) Version 1.1

MÔ HÌNH BẢO ĐẢM AN TOÀN THÔNG TIN 4 LỚP



Lực lượng tại chỗ
- Đội Ứng cứu sự cố

Lực lượng chuyên nghiệp
- Doanh nghiệp ATTT

04 lớp

Kiểm tra đánh giá độc lập

Kết nối về Bộ TTTT

NÂNG CAO NĂNG LỰC ĐỘI ỨNG CỨU SỰ CỐ

ĐỘI ỨNG CỨU SỰ CỐ CISRT (Cyber/Computer Security Incident Response Team)

Chỉ thị 18/CT-TTg ngày 13/10/2022 về Đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam

Nguyên tắc: "**Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn thông tin mạng**".

Trách nhiệm các Bộ, ngành, địa phương:

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải **chuyển từ bị động sang chủ động**: săn lùng mối nguy hại và rà quét lỗ hổng 6 tháng 1 lần; hoàn thành phương án kịch bản ứng cứu sự cố; diễn tập thực chiến 1 lần/năm đối với HTTT từ cấp độ 3 trở lên.
- Kiện toàn lại Đội Ứng cứu sự cố theo hướng **chuyên nghiệp**, **cơ động,** có **tối thiểu 05 chuyên gia** ATTTM
- 11 lĩnh vực quan trọng (QĐ 632/QĐ-TTg 2017) cần ưu tiên đảm bảo ATTTM, triển khai mô hình CERT lĩnh vực
- Đội Ứng cứu sự cố được giao các **nhiệm vụ thường xuyên**

NÂNG CAO NĂNG LỰC ĐỘI ỨNG CỨU SỰ CỐ

ĐỘI ỨNG CỨU SỰ CỐ CISRT (Cyber/Computer Security Incident Response Team)

Chỉ thị 18/CT-TTg ngày 13/10/2022 về Đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam

Nguyên tắc: "**Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn thông tin mạng**".

Trách nhiệm các Bộ, ngành, địa phương: (tiếp)

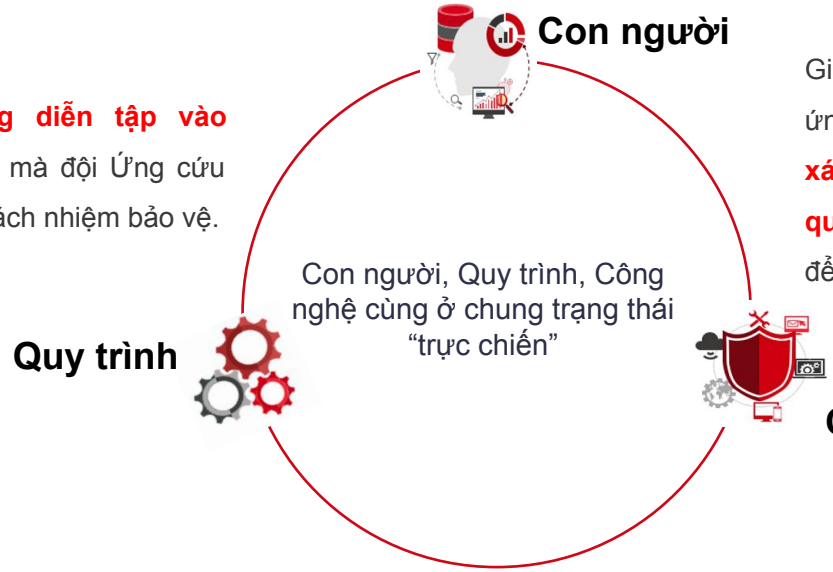
- Bố trí **đủ kinh phí** đảm bảo hoạt động Đội UCSC
- Thực hiện **rà soát, phát hiện và khắc phục lỗ hổng, điểm yếu, các nguy cơ**
- Biện pháp kiểm soát nguy cơ mất ATTT do **bên thứ ba, các chuỗi cung ứng**
- Thực hiện quy định **báo cáo sự cố**, tuyên truyền người dân cung cấp thông tin sự cố
- Các chiến dịch nâng cao ý thức cảnh giác của người dùng cuối /tấn công mạng
- Công bố thông tin đầu mối tiếp nhận thông báo sự cố

DIỄN TẬP THỰC CHIẾN AN TOÀN THÔNG TIN

DIỄN TẬP THỰC CHIẾN AN TOÀN THÔNG TIN

Bộ TT&TT ban hành Chỉ thị 60/CT-BTTTT năm 2021 về diễn tập ATTT thực chiến.

Gắn hoạt động diễn tập vào chính hệ thống mà đội Ứng cứu sự cố đang có trách nhiệm bảo vệ.



Giúp các tổ chức đánh giá được khả năng ứng phó trong trạng thái đang bị tấn công, **xác định các điểm yếu đang tồn tại liên quan đến con người, quy trình, công nghệ** để cải thiện.

Chuyển từ diễn tập theo kịch bản sẵn có sang **tấn công với nhiều chiến thuật linh hoạt**, trong **thời gian kéo dài** và đặt toàn bộ hệ thống của tổ chức trong trạng thái bất ngờ.

Đánh giá Đội tấn công	Đánh giá Đội phòng thủ
Số lượng và mức độ nghiêm trọng của lỗ hổng, điểm yếu phát hiện được	Đánh giá hiện trạng
Mức độ phức tạp của kỹ thuật tấn công	Năng lực phát hiện tấn công
Khuyến nghị hướng khắc phục	Khả năng ngăn chặn, ứng cứu sự cố

Trung tâm Giám sát Điều hành An toàn, An ninh mạng SOC

Quyết định 1356/QĐ-BTTTT về tiêu chí giải pháp đánh giá giải pháp, dịch vụ Trung tâm SOC

I. Tiêu chí về công nghệ

1. **Tiêu chí đánh giá từng thành phần:**

   Cơ bản (SIEM, NIPS, Antivirus, EDR) ***Theo tiêu chí của Bộ TTTT***

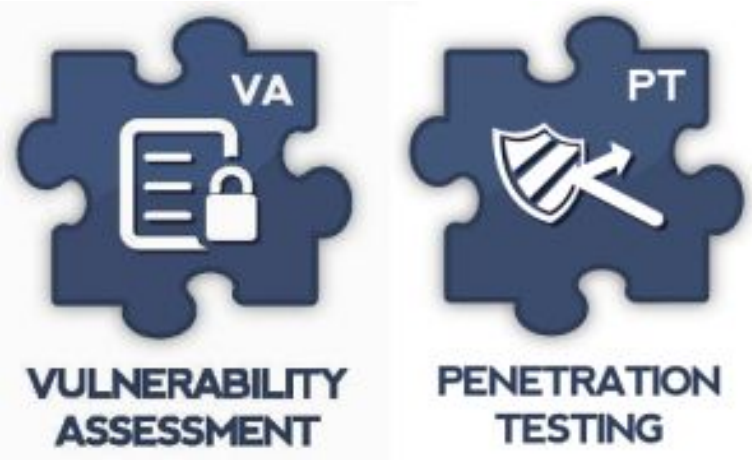
   Nâng cao (WAF, SOAR, TI) ***Theo tiêu chí của Bộ TTTT***

2. **Tiêu chí đánh giá tính hiệu quả:** Kiểm tra, thử nghiệm

II. Tiêu chí về chất lượng dịch vụ

1. **Quy trình:** đánh giá hồ sơ, thử nghiệm quy trình
2. **Con người:** tối thiểu 12 nhân sự với các mức yêu cầu khác nhau

KIỂM TRA, ĐÁNH GIÁ ATTT



Kiểm tra đánh giá ATTT
VAPT

Hệ thống thông tin chưa xác nhận an toàn thì chưa đưa vào sử dụng

-Do **đơn vị độc lập** với lực lượng tại chỗ, với đơn vị giám sát thực hiện.

-Phần mềm, ứng dụng phải được kiểm tra, đánh giá an toàn **trước khi đưa vào** triển khai, sử dụng và sau khi nâng cấp, mở rộng.

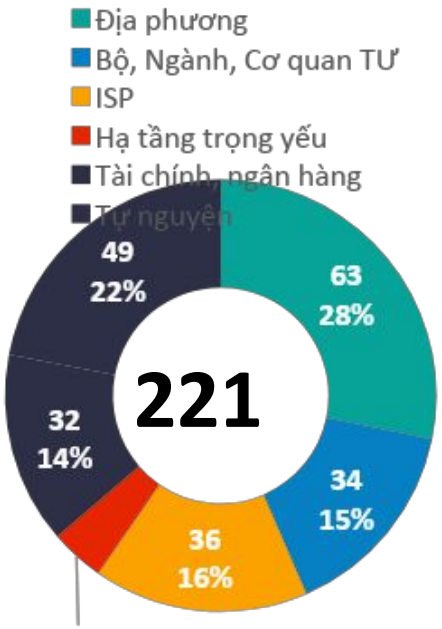
-Đánh giá bao gồm cả **kiểm tra mã nguồn** (đối với phần mềm nội bộ - QĐ 742/QĐ-BTTTT)).

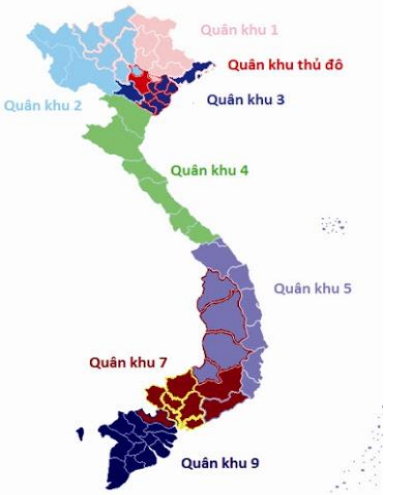
-Định kỳ thực hiện dò quét lỗ hổng bảo mật, kiểm thử xâm nhập và khắc phục kịp thời các điểm yếu.

-Chủ động theo dõi, khắc phục các nguy cơ tấn công, thông tin về các lỗ hổng, điểm yếu **đã được cảnh báo**.

-Chủ động thực hiện truy tìm các **mối đe dọa**

MẠNG LƯỚI ỨNG CỨU SỰ CỐ ATTTM QUỐC GIA





- Cụm 8: Doanh nghiệp viễn thông, hạ tầng và Cục BĐTƯ, VNNIC
- Cụm 6: Hà Nội và các Bộ, Ngành
- Cụm 10: Ngân hàng, tài chính, kho bạc, thuế, hải quan
- Cụm 11: Doanh nghiệp CNTT, ATTT

HOẠT ĐỘNG MẠNG LƯỚI ƯCSC ATTTM QUỐC GIA 2022

Mạng lưới UCSC ATTT quốc gia Vietnam CSIRTs Network

- 232 thành viên tổ chức, phân thành 11 cụm mạng lưới
- 3 diễn tập quốc tế: ASEAN-Nhật Bản, APCERT, ACID
- 2 diễn tập thực chiến quốc gia
- 15 Bộ, Ngành, địa phương tổ chức diễn tập thực chiến (diễn tập thực chiến Cụm mạng lưới số 9)
- 9 Webinar về bảo đảm ATTT – UCSC hàng tháng, hội thảo "Cải thiện năng lực phòng thủ thông qua hoạt động triển khai diễn tập thực chiến" cho KV miền Trung Tây nguyên
- Hội nghị Giao ban mạng lưới ƯCSC
- Huấn luyện Mô hình trưởng thành quản lý ứng cứu sự cố ATTT (SIM3) do chuyên gia quốc tế trực tiếp huấn luyện
- Đánh giá các tiêu chí SIM3 của chuyên gia quốc tế cho VNCERT/CC
- Kết nối AJCCBC (ASEAN-Nhật Bản), KISA (Hàn Quốc) mở rộng huấn luyện kỹ năng cho các thành viên mạng lưới
- Triển khai nhóm cán bộ đầu mối và kỹ thuật với ~ 1.100 thành viên
- Triển khai nền tảng điều phối xử lý sự cố

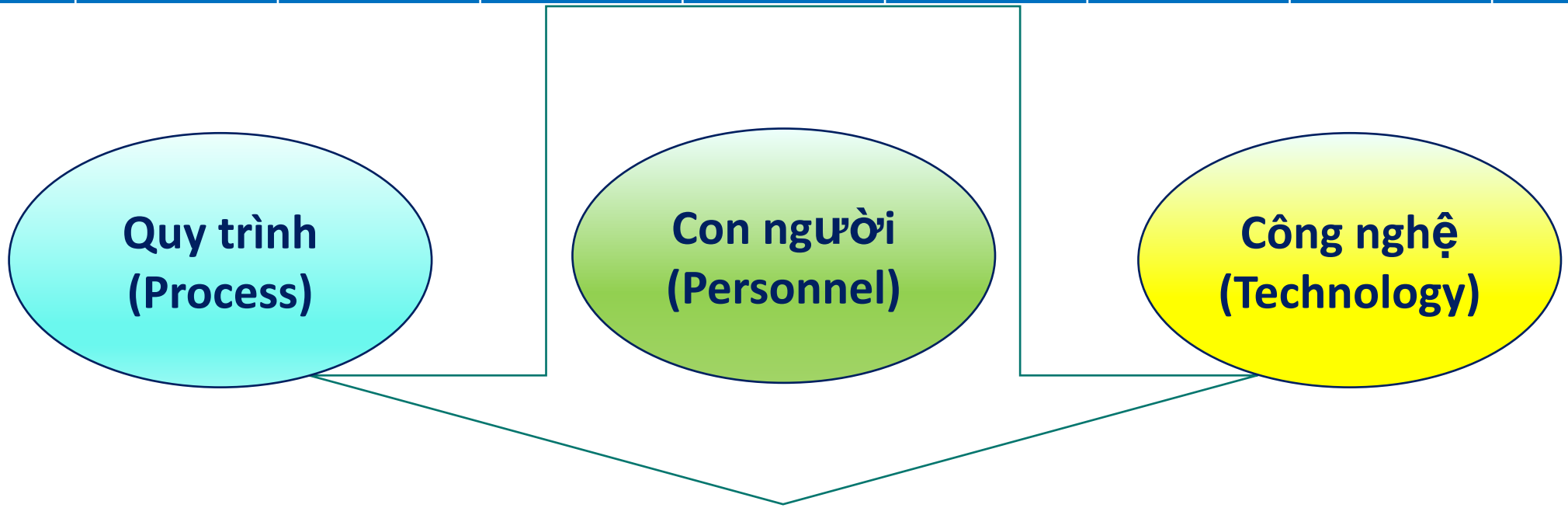
TRIỂN KHAI BẢO ĐẢM AN TOÀN TRONG CÁC TỔ CHỨC

Xây dựng và triển khai **"Chương trình đảm bảo ATTT – Security Program"** của tổ chức:

- Đáp ứng các **yêu cầu luật** định
- **Chiến lược ATTT** phù hợp với chiến lược của doanh nghiệp
- Ban hành **chính sách ATTT**
- Phát triển **Nguồn nhân lực CNTT, ATTT + nâng cao nhận thức ATTT** cho tất cả nhân viên
- **Quản lý rủi ro**
- Triển khai **Quản lý an toàn** theo chuẩn
- Xây dựng và duy trì **Kế hoạch ứng phó**
- Duy trì **vận hành đảm bảo an toàn**
- Triển khai các **Cơ chế bảo vệ cụ thể** - các sản phẩm, giải pháp bảo mật, đảm bảo an toàn

CHƯƠNG TRÌNH BẢO ĐẢM AN TOÀN THÔNG TIN của TỔ CHỨC

Luật và quy định	Chiến lược ATTT	Chính sách ATTT	Nhân lực, nhận thức ATTT	Quản lý rủi ro	Mô hình Quản lý bảo mật	Kế hoạch dự phòng	Duy trì an toàn	Các cơ chế bảo vệ



Giảm rủi ro mất an toàn cho hệ thống thông tin

AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

Việt Nam xác định chuyển đổi số quốc gia là một trong những nhiệm vụ trọng tâm và đột phá chiến lược.

"Cùng với phát triển dữ liệu, chuyển đổi số, chúng ta cũng cần chú trọng đến an toàn, an ninh mạng ngay từ đầu. Chúng tôi vẫn nói và lặp đi lặp lại rằng chuyển đổi số cần an toàn, an ninh mạng giống như một chiếc xe cần có phanh. Phanh không phải để dừng chiếc xe lại, mà để chúng ta yên tâm nhấn ga đi nhanh hơn. Chuyển đổi số muốn nhanh, bền vững thì an toàn, an ninh mạng phải song hành và trở thành một phần không thể tách rời".

Thứ trưởng Bộ Thông tin và Truyền thông Nguyễn Huy Dũng

Trân trọng Cảm ơn!

Nguyễn Hữu Nguyên
Phó Giám đốc Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam
VNCERT/CC
Cục An toàn thông tin, Bộ Thông tin và Truyền thông
Email: nhnguyen@mic.gov.vn