CÔNG TY CP CÔNG NGHỆ DTG

DIGITAL TECHNOLOGY GROUP®

DIGITAL TECHNOLOGY GROUP® Cyberspace Security

NÂNG CAO KHẢ NĂNG PHÁT HIỆN TOÀN DIỆN VÀ ỨNG PHÓ VỚI CÁC MỐI ĐE DỌA ATTT TRONG QUÁ TRÌNH CHUYỂN ĐỔI SỐ

PHẠM MẠNH HÙNG

GIÁM ĐỐC TRUNG TÂM GIÁM SÁT ATTT DTG SOC

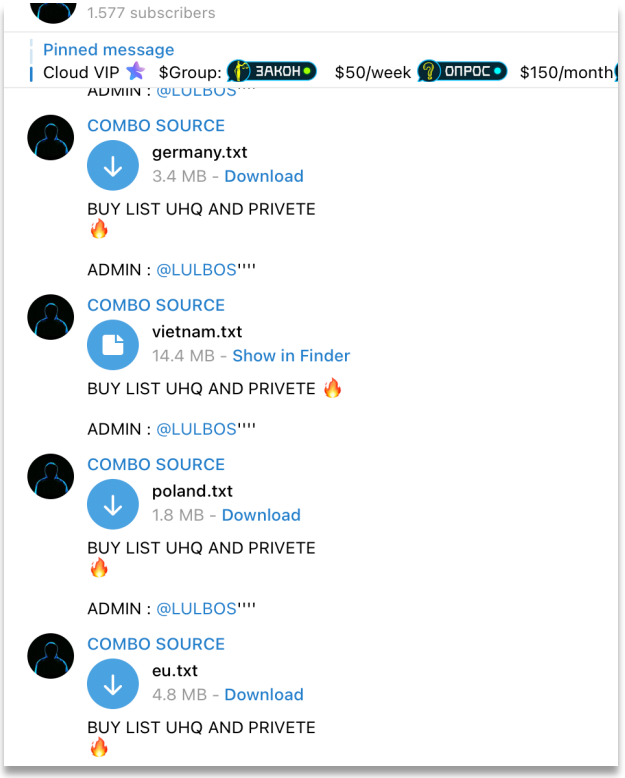
"VỮNG MÃI MỘT NIỀM TIN"

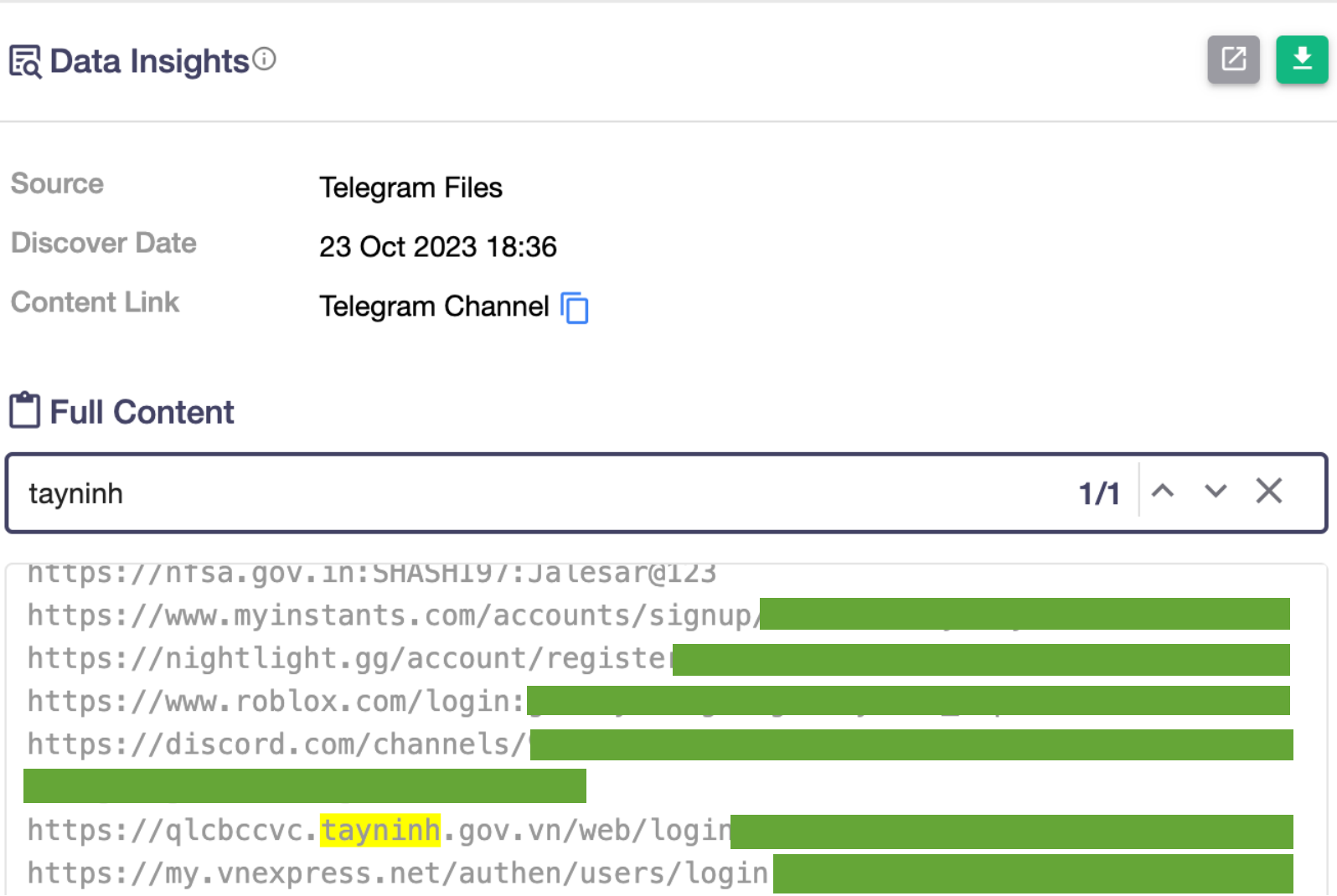
PHẠM MẠNH HÙNG
GIÁM ĐỐC TRUNG TÂM GIÁM SÁT ATTT DTG SOC (DSOC)

- Hơn +10 năm kinh nghiệm về CyberSecurity
- GSOC | CHFI | SPLUNK ARCHITECT

Giải thưởng:

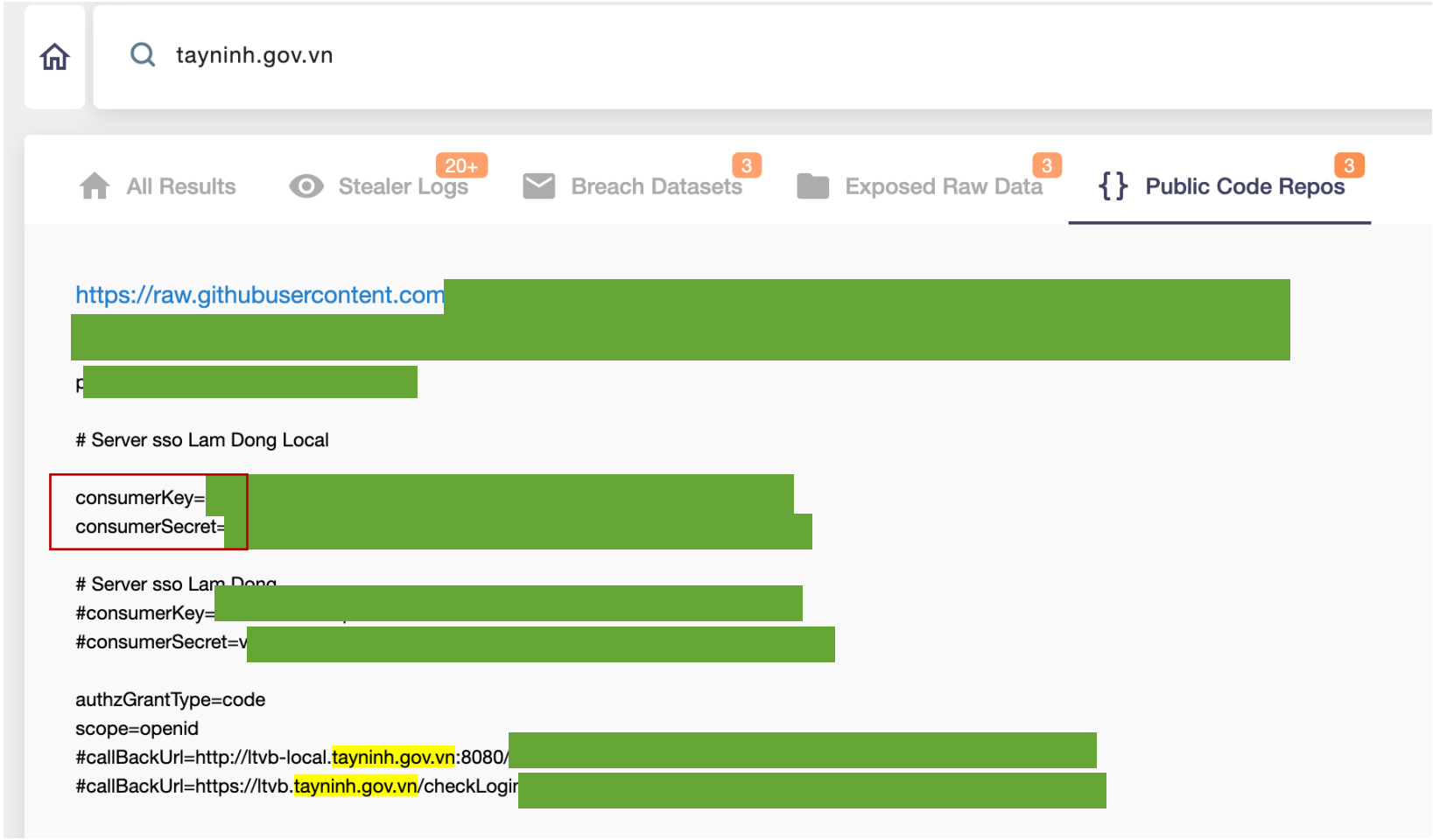
NGUỒN THÔNG TIN TÌNH BÁO MẠNG





Lộ thông tin tài khoản

NGUỒN THÔNG TIN TÌNH BÁO MẠNG (2)



Lộ thông tin dữ liệu, data

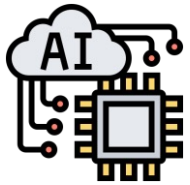
CHUYỂN ĐỔI SỐ

Chuyển đổi số là quá trình thay đổi **tổng thể và toàn diện** của cá nhân, tổ chức về **cách sống**, **cách làm việc** và **phương thức sản xuất** dựa trên các công nghệ số.

Trong quá trình chuyển đổi số, việc đảm bảo an toàn thông tin trong các lĩnh vực của đời sống xã hội trở thành một phần quan trọng trong việc bảo đảm an ninh quốc gia.

Nguồn: *Cục chuyển đổi số - Bộ Thông tin và Truyền thông*

CÔNG NGHỆ - XU HƯỚNG



DATA DRIVEN

(Big Data, Machine Learning)

IOT

MOBILITY

AUTOMATION

CLOUD

RỦI RO TRONG CHUYỂN ĐỔI SỐ

Chính phủ
Tổ chức
Doanh nghiệp

- Đối tượng
- Kết nối
- Dữ liệu
- Nghiệp vụ

Kẻ tấn công

- Cơ hội tấn công
- Năng lực tấn công

Chi phí

Hiệu quả

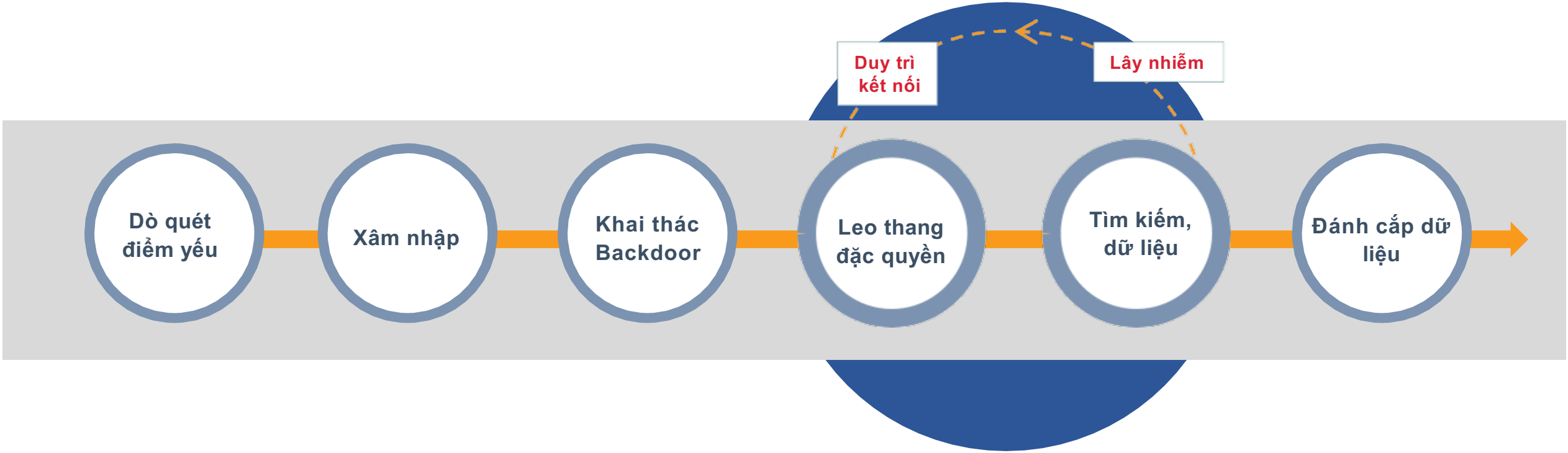
MTTD

Mean time to Detect

MTTR

Mean time to Respond

CÁC BƯỚC THỰC HIỆN TẤN CÔNG MẠNG



TẤN CÔNG MẠNG KHÔNG BIÊN GIỚI

1

MỤC TIÊU NÓNG| CII/OT

Mối đe dọa đối với cơ sở hạ tầng quan trọng, sự gián đoạn vận hành, hoạt động gián điệp và động cơ danh tiếng

2

TÀI CHÍNH | DỮ LIỆU ĐỀU CÓ GIÁ TRỊ

Tội phạm mạng cần tài trợ và đang nhắm mục tiêu vào các hệ thống tài chính

3

GIÁN ĐOẠN CHUỖI CUNG ỨNG | TẤN CÔNG QUA BÊN THỨ 3

Chuỗi cung ứng phần mềm sẽ tiếp tục là mục tiêu

4

DOANH NGHIỆP VỪA VÀ NHỎ

Chiến thuật ném bom rải thảm – các doanh nghiệp thuộc mọi quy mô đều là mục tiêu

5

CÁC NHÓM RANSOMWARE

Kỹ thuật “điểm mặt chỉ tên”

6

THÀNH LẬP CÁC TỔ CHỨC TỘI PHẠM MẠNG

Sự hợp tác của tội phạm mạng đã có từ lâu nhưng giờ chúng đang chia sẻ cơ sở hạ tầng, vũ khí, công cụ, v.v.

BỐI CẢNH CÁC MỐI ĐE DỌA ĐANG PHÁT

01

Tội phạm mạng tạo ra nhiều sự hiện diện hơn bằng cách sử dụng **Công nghệ mới AI, ML**

02

Gia tăng các cuộc tấn công do **Chính Phủ bảo trợ** gây ra bởi căng thẳng địa chính trị

03

Công nghệ **Deepfake** để truyền bá thông tin sai lệch

XU HƯỚNG TẤN CÔNG MẠNG TẠI VIỆT NAM

01 Tội phạm mạng đã hoạt động rất tích cực trong các tổ chức sản xuất, dịch vụ và tổ chức gia công.

Xu hướng: Sử dụng phần mềm độc hại chuyên dụng và lừa đảo
Mục tiêu: Dữ liệu nhạy cảm và nhận dạng

02 Động cơ đánh cắp dữ liệu nhạy cảm và bí mật thương mại từ các tổ chức Tài Chính, Ngân Hàng, Bảo Hiểm, Chứng Khoán, Bán Lẻ và F&B

Xu hướng: Phần mềm gián điệp, phần mềm độc hại và plugins để thu thập dữ liệu
Mục tiêu: Dữ liệu và bí mật thương mại

03 Các cơ quan chính phủ sẽ tiếp tục là mục tiêu cao cấp của tội phạm mạng

Xu hướng: Phần mềm độc hại mạo danh và đánh cắp dữ liệu
Mục tiêu: Dữ liệu nhạy cảm

04 Dịch vụ tài chính và các công ty Fintech

Xu hướng: Mạo danh ứng dụng trong danh sách cho phép (whitelist), đánh cắp dữ liệu bằng phần mềm độc hại và tấn công ransomware
Mục tiêu: Trộm cắp danh tính và dữ liệu tài chính

05 Những kẻ lừa đảo đang tích cực lan truyền thông tin sai lệch để thu thập dữ liệu PII và hành vi

Xu hướng: Trang web giả mạo, phần mềm gián điệp có thể tải xuống từ Internet
Mục tiêu: Dữ liệu nhạy cảm và định danh

06 Chuỗi cung ứng sản xuất, doanh nghiệp du lịch và tiện ích gặp rủi ro

Xu hướng: Phần mềm độc hại đa hành vi [IT/OT, các hệ điều hành khác nhau]
Mục tiêu: CII, bí mật thương mại, tài liệu chứa quy trình độc quyền

CHI PHÍ VỀ ATTT TRONG CHUYỂN ĐỔI SỐ

Chi cho chuyển đổi số thế nào cho phù hợp?

Mức trung bình của thế giới vào khoảng 2-3%. Ở một số nước như Singapore, tỷ lệ này có thể lên đến 4-5%. Mức trung bình của Việt Nam hiện nay đang là 0,3%.

Mỗi cơ quan, tổ chức căn cứ vào chiến lược chuyển đổi số của mình để có mức chi phù hợp. Đối với các cơ quan nhà nước cấp bộ, cấp tỉnh, tỷ lệ chi cho chuyển đổi số nên ở mức 1% tổng chi ngân sách nhà nước hàng năm. Nếu muốn đẩy nhanh, nhất là những năm đầu cần làm ngay các nền tảng, thì có thể chi 2%.

Chuyển đổi số là chuyển hoạt động từ môi trường thực sang môi trường số. Bảo đảm an toàn, an ninh mạng là điều kiện tiên quyết để chuyển đổi số. Mỗi tổ chức, doanh nghiệp cần dành ít nhất 10% mức chi cho chuyển đổi số để chi cho các hoạt động bảo đảm an toàn, an ninh mạng.

Nguồn: https://dx.mic.gov.vn/docs/chuyen-doi-so-ton-bao-nhieu-tien/

SỰ CHUYỂN DỊCH CỦA THỊ TRƯỜNG VỀ ATTT

THẾ GIỚI

Market	2017 YR	2018 YR	2019 YR	2020 YR	2021 YR	2022 YR	2023 YR	2018 TR-2023 YR
Application Security	2,484.8	2,814.4	3,096.2	3,440.0	3,804.7	4,170.9	4,527.6	10.0%
Cloud Security	185.4	297.6	439.1	636.3	895.6	1,224.5	1,631.1	40.5%
Data Security	2,013.1	2,343.3	2,663.3	3,079.9	3,558.0	4,060.7	4,544.3	14.2%
Identity Access Management	8,097.8	9,028.1	9,841.5	10,852.9	12,011.3	13,117.7	14,075.9	9.3%
Infrastructure Protection	13,476.2	15,097.7	16,527.9	18,374.8	20,371.0	22,449.1	24,620.6	10.3%
Integrated Risk Management	3,948.6	4,279.0	4,557.1	4,942.2	5,374.0	5,821.0	6,260.5	7.9%
Network Security Equipment	10,677.3	12,080.4	13,278.0	14,320.2	15,316.9	16,183.8	16,870.0	6.9%
Other Information Security Software	1,832.3	2,042.5	2,206.6	2,410.5	2,633.7	2,862.2	3,095.6	8.7%
Security Services	52,717.7	58,474.2	62,009.5	66,914.0	72,425.7	78,391.3	84,486.4	7.6%
Consumer Security Software	5,943.7	6,220.7	6,258.1	6,425.0	6,616.6	6,816.9	6,947.0	2.2%

Bộ trưởng Bộ TT&TT Nguyễn Mạnh Hùng:

"Việt Nam có thể trở thành cường quốc an ninh mạng"

VIỆT NAM

- Xu hướng cổ vũ phát triển và sử dụng các sản phẩm make in Việt Nam trong lĩnh vực An ninh mạng.
- Chỉ thị 14/2018 và 14/2019 của Thủ tướng CP về cải thiện chỉ số An ninh mạng quốc gia, trong đó nhấn mạnh đến việc thuê và sử dụng dịch vụ của các đơn vị chuyên nghiệp.
- Nghị định 85/2016 về đảm bảo ATTT theo cấp độ.
- Công văn 2973/BTTTT-CATTT về hướng dẫn triển khai hoạt động giám sát ATTT trong cơ quan, tổ chức nhà nước.
- CV235/CATTT-BTTT Hướng dẫn mô hình đảm bảo ATTT cấp Bộ, Tỉnh và các cơ quan nhà nước.
- Công văn 1552 Đảm bảo an toàn thông tin cho hệ thống thông tin theo mô hình 4 lớp trước 30/09/2020.
- Chuyển đổi số làm gia tăng nguy cơ về an ninh mạng.
- Quyết định số 06/QĐ-TTg của Thủ tướng Chính phủ: Phê duyệt Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022 - 2025, tầm nhìn đến năm 2030
- Chính phủ vừa ban hành Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, có hiệu lực thi hành kể từ ngày 01/7/2023.

CÁC TIÊU CHÍ ĐẢM BẢO ATTT TRONG QUÁ TRÌNH CHUYỂN ĐỔI SỐ

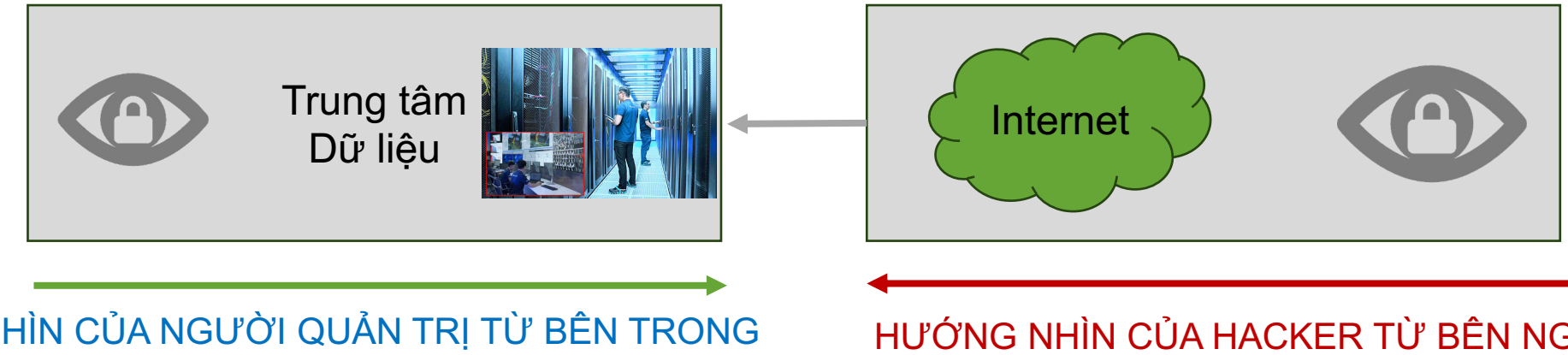
GÓC NHÌN ĐA CHIỀU NÂNG CAO KHẢ NĂNG GIÁM SÁT & PHẢN ỨNG VỚI CÁC SỰ CỐ ATTT

1. GIÁM SÁT BỊ ĐỘNG

1. Quản lý tài sản & định danh
2. Hệ thống log tập trung (SIEM)
3. Giám sát và phát hiện bất thường
4. Cảnh báo đa nền tảng (Email, MS Team, Telegram)

2. GIÁM SÁT CHỦ ĐỘNG

1. Định kỳ Rà quét lỗ hổng
2. Thu thập thông tin tình báo mạng
3. Phản ứng tự động với tấn công mạng
4. Có sự tương tác/phối hợp giữa các bộ phận



HƯỚNG NHÌN CỦA NGƯỜI QUẢN TRỊ TỪ BÊN TRONG

HƯỚNG NHÌN CỦA HACKER TỪ BÊN NGOÀI

DTG Cyberspace Security
DIGITAL TECHNOLOGY GROUP

12 TIÊU CHÍ QUAN TRỌNG ĐẢM BẢO ATTT

1| LẬP KẾ HOẠCH & CHIẾN LƯỢC ATTT

Lộ trình đầu tư ATTT hàng năm, liên tục, có mục tiêu

2| ENDPOINT +

Bảo vệ EPP, EDR, Di động, BYOD

3| TẬP TRUNG DỮ LIỆU/TỔNG THỂ

SIEM (thu thập, cảnh báo, báo cáo tổng thể)
EASM (thông tin tình báo mạng)

4| BẢO MẬT & RIÊNG TƯ DỮ LIỆU

Ngăn chặn mất mát dữ liệu, bảo mật email

5| QUY ĐỊNH & TUÂN THỦ

GRC và các sản phẩm tuân thủ khác

6| QUẢN LÝ ĐỊNH DANH

IAM, KYC/AML, chống gian lận, xác thực không cần mật khẩu

7| NỀN TẢNG ĐÁM MÁY/CLOUD

CASB, PKM, SIEM dựa trên cloud

8| MỞ RỘNG NỀN TẢNG SỐ/WEB

Công cụ DevSecOps, SWGS, NW Sec

9| IOT / OT

Bảo vệ an ninh mạng cho các thiết bị kết nối Internet, thiết bị sản xuất

10| AI/ML

Phân tích an ninh mạng/AI/ML/UBA, tự động hóa, tích hợp nền tảng

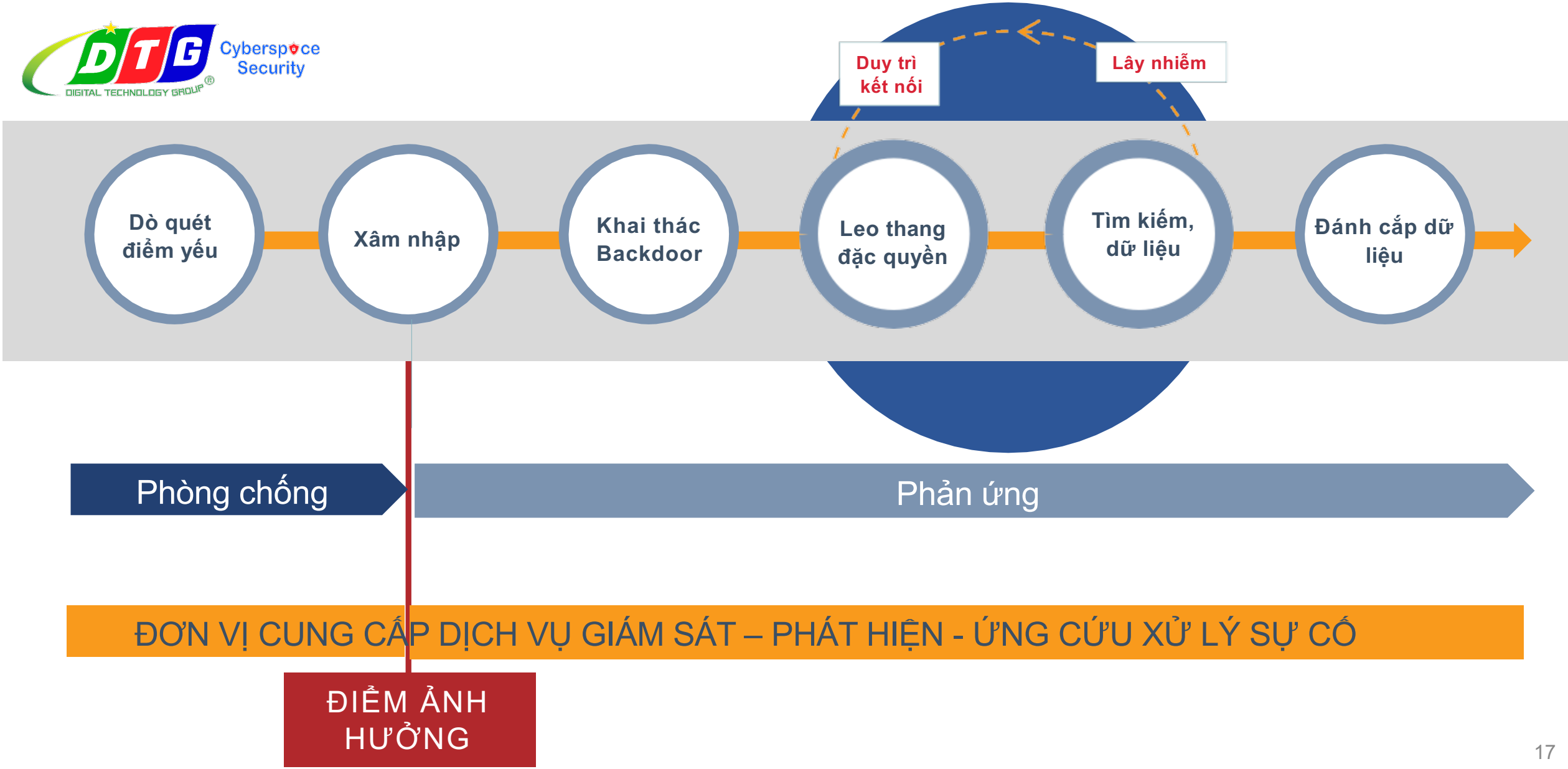
11| ỨNG PHÓ TỰ ĐỘNG

Quản lý sự kiện ATTT
Tự động phản ứng

12| NHẬN THỨC NGƯỜI DÙNG

Nâng cao nhận thức
Tập huấn đào tạo

MÔ HÌNH MDR (MANAGED DETECTION & RESPONSE)



GIẢI PHÁP/DỊCH VỤ CHIẾN LƯỢC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 190 /GP-BTTTT

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

Hà Nội, ngày 24 tháng 4 năm 2023

GIẤY PHÉP KINH DOANH
SẢN PHẨM, DỊCH VỤ AN TOÀN THÔNG TIN MẠNG

(Cấp lần đầu: ngày 02 tháng 8 năm 2018,
sửa đổi lần thứ 3: ngày 24 tháng 4 năm 2023
Có giá trị đến hết ngày 01 tháng 8 năm 2028)

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 48/2022/NĐ-CP ngày 26 tháng 7 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Nghị định số 108/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng;

Xét đơn số 2302/DDNBSGPKD ngày 12 tháng 01 năm 2023 và hồ sơ đề nghị sửa đổi, bổ sung Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng của Công ty Cổ phần Công nghệ DTG;

Theo đề nghị của Cục trưởng Cục An toàn thông tin,

QUYẾT ĐỊNH:

Điều 1. Cho phép Công ty Cổ phần Công nghệ DTG được kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng.

1. Thông tin doanh nghiệp:

a) Tên giao dịch của doanh nghiệp bằng tiếng Việt hoặc tiếng nước ngoài (nếu có): Công ty Cổ phần Công nghệ DTG.

b) Tên người đại diện theo pháp luật: Trần Quốc Hoàn.

c) Giấy chứng nhận đăng ký doanh nghiệp số: 0302924953 do Sở Kế hoạch và Đầu tư Thành phố Hồ Chí Minh cấp lần đầu ngày 12 tháng 5 năm 2003, thay đổi lần thứ 15 ngày 29 tháng 6 năm 2021.

d) Địa chỉ trụ sở chính tại Việt Nam: Số 41 Trần Khắc Chân, Phường 15, Quận

2. Doanh nghiệp được phép kinh doanh:

a) Nhập khẩu sản phẩm kiểm tra, đánh giá an toàn thông tin mạng.

b) Nhập khẩu sản phẩm giám sát an toàn thông tin mạng.

c) Nhập khẩu sản phẩm chống tấn công, xâm nhập.

d) Cung cấp dịch vụ giám sát an toàn thông tin mạng.

đ) Cung cấp dịch vụ phòng ngừa, chống tấn công mạng.

e) Cung cấp dịch vụ tư vấn an toàn thông tin mạng.

g) Cung cấp dịch vụ ứng cứu sự cố an toàn thông tin mạng.

h) Cung cấp dịch vụ khôi phục dữ liệu.

i) Cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng.

Điều 2. Công ty Cổ phần Công nghệ DTG phải thực hiện đúng các quy định tại Nghị định số 108/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng và các quy định khác của pháp luật có liên quan.

Điều 3. Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng này có hiệu lực kể từ ngày ký và có giá trị đến hết ngày 01 tháng 8 năm 2028 thay thế cho Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng số 75/GP-BTTTT cấp ngày 26 tháng 01 năm 2022./.

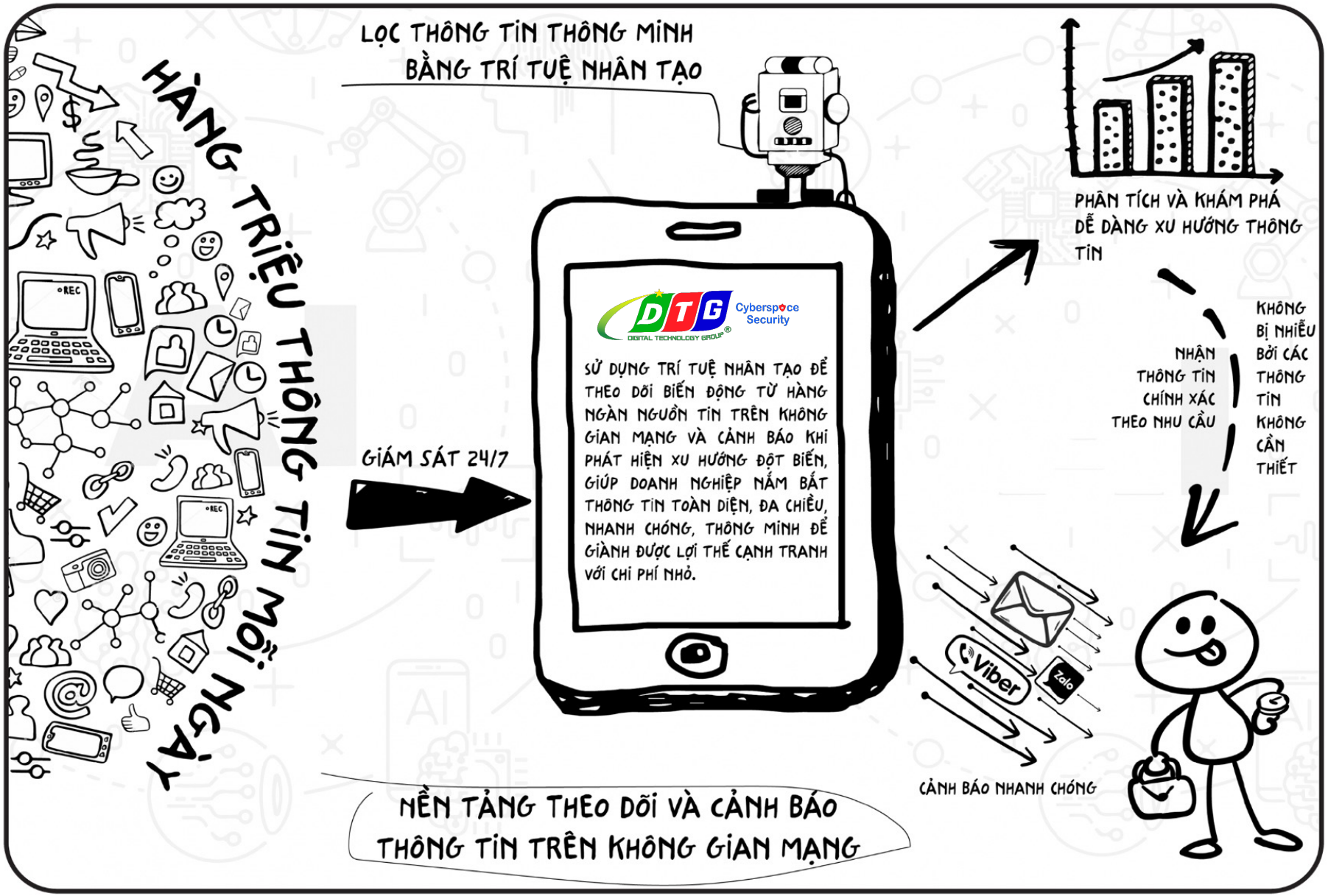
Nơi nhận:
- Như Điều 1;
- Bộ trưởng;
- Thứ trưởng Nguyễn Huy Dũng;
- Vụ Pháp chế;
- Thanh tra Bộ;
- Lưu: VT, CATTT (3b).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

DTG SMART SOC TIÊN PHONG TRONG CÔNG NGHỆ

- ✓ CÔNG NGHỆ ƯU VIỆT
- ✓ ĐỘI NGŨ CHUYÊN GIA
- ✓ ĐỒNG HÀNH CÙNG KHÁCH HÀNG



NĂNG LỰC ĐỘI NGŨ CHUYÊN GIA

1. NHÓM CHỨNG CHỈ TƯ VẤN CAO CẤP

CISSP® Certified Information Systems Security Professional

GIAC SECURITY OPERATIONS GSOC CERTIFIED

aws certified Solutions Architect Associate

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

vmware CERTIFIED PROFESSIONAL Data Center Virtualization 2022

splunk> CERTIFIED Splunk Enterprise Certified Architect

2. NHÓM CHỨNG CHỈ ĐÁNH GIÁ VÀ KIỂM THỬ BẢO MẬT

OFFENSIVE security OSCP

OFFENSIVE security OSWE

OFFENSIVE security OSEP

CompTIA PenTest+ CERTIFIED·CE

C|EH™ Certified Ethical Hacker

3. NHÓM CHỨNG CHỈ PHÂN TÍCH, ĐIỀU TRA VÀ XỬ LÝ SỰ CỐ ATTT

C|HFI™ Computer Hacking Forensic INVESTIGATOR

E|CSA EC-COUNCIL CERTIFIED SECURITY ANALYST

CompTIA CySA+

CompTIA Security+™ CERTIFIED

aws certified Security SPECIALTY

splunk> CERTIFIED Splunk Enterprise Security Certified Admin

GIẢI PHÁP CHIẾN LƯỢC

NHÓM GIẢI PHÁP GIÁM SÁT VẬN HÀNH (OPERATION)

- Giám sát vận hành ứng dụng, databases - apm (application performance monitoring)
- Giám sát vận hành hệ thống mạng - npm (network performance monitoring)

NHÓM GIẢI PHÁP GIÁM SÁT BẢO MẬT (SECURITY)

- Giám sát truy cập mạng - NAC (network access control)
- Giám sát truy cập đặc quyền - PAM (privileged access managemeent)
- Giám sát và quản lý các bề mặt tấn công với các thông tin tình báo từ bên ngoài - EASM (external attack suface management)
- Giám sát và quản lý lỗ hổng hệ thống – (vulnerability management)
- Giám sát an ninh tập trung - SIEM (security infomartion and event management)
- Giải pháp phòng chống thất thoát dữ lieu - DLP

12 TIÊU CHÍ QUAN TRỌNG ĐẢM BẢO ATTT

NHÓM DỊCH VỤ GIÁM SÁT VẬN HÀNH (OPERATION AS SERVICE)

- Dịch vụ giám sát vận hành tổng thể cho trung tâm dữ liệu (Data center)
- Dịch vụ giám sát vận hành Web server/ Email server

NHÓM DỊCH VỤ BẢO MẬT (SECURITY AS SERVICE)

- Dịch vụ đánh giá lỗ hổng và kiểm tra xâm nhập (VAPT)
- Dịch vụ đào tạo nâng cao nhận thức an toàn thông tin (Security Awareness Training)
- Dịch vụ diễn tập thực chiến đảm bảo an toàn thông tin mạng (Cyber Security drills)
- Dịch vụ săn tìm và xử lý các mối đe dọa (Threat hunting)
- Dịch vụ giám sát an toàn thông tin mạng (SOC)

DIGITAL TECHNOLOGY GROUP

Cyberspace Security

VỮNG MÃI MỘT NIỀM TIN

CẢM ƠN

PHẠM MẠNH HÙNG
GIÁM ĐỐC TRUNG TÂM DTG SOC
hungpm@dtgcorp.com.vn | 0923 26 9988