

PHÁT HIỆN SỚM VÀ PHÒNG NGỪA RỦI RO LỘ LỘT DỮ LIỆU TÀI CHÍNH TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

Công ty An ninh mạng Viettel

Chuyên đề 1: Cải cách, hiện đại hóa công tác quản lý ngân sách nhà nước

Vietnam Digital Finance – Meliá Hanoi - 17/11/2022

viettel
security

TRẦN MINH QUẢNG

Intelligence Director

Viettel Cyber Security

quangtm4@viettel.com.vn



Nội dung

- 01 Công nghệ mới - Rủi ro mới
- 02 Chúng ta đã sẵn sàng?
- 03 Hướng tiếp cận



CHUYỂN ĐỔI SỐ LÀ TẤT YẾU



Nội dung

- 01 Công nghệ mới - Rủi ro mới
- 02 Chúng ta đã sẵn sàng?
- 03 Hướng tiếp cận



Nguy cơ lộ lọt dữ liệu

- ▶ **Personal Data:** Dữ liệu cá nhân, các loại thông tin định danh cá nhân (PII).

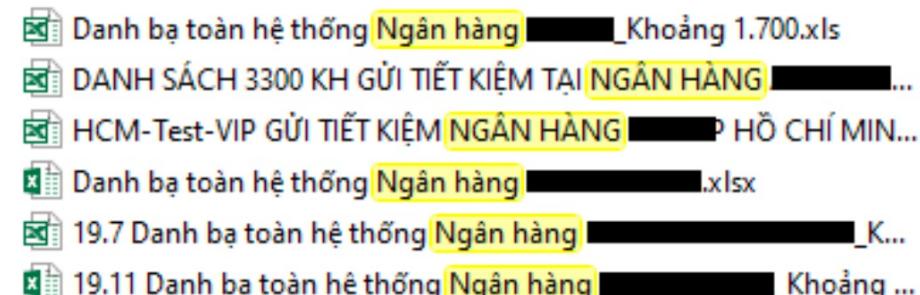
Thông tin cá nhân: Họ tên, Địa chỉ, Số điện thoại, Ngày sinh, Căn cước công dân..

Danh bạ khách hàng gửi tiền hoặc đầu tư
của các hệ thống ngân hàng trên cả nước

Các sao kê giao dịch của khách hàng cá nhân và khách hàng doanh nghiệp.



H1. Sao kê cá nhân của khách hàng



H2. Dữ liệu liên quan tới khách hàng

Source Code: Mã nguồn của hệ thống, có thể bị lộ lọt do tấn công hoặc cấu hình sai.

Lộ lọt các trường thông tin nhạy cảm trong Source code như:

- Tài khoản đăng nhập.
- API Key, Public Key, Private Key,..
- IP được sử dụng nội bộ trong tổ chức.

```
108         }
109     }
110 }
111 } else {
112     $error_message = "Thẻ bị từ chối";
113     $result_code = "REJECT";
114 }
115
116
117 return array('error_message' => $error_message, 'result_code' => $result_code, 'xid' => $xid,
118 }
119
120 protected function _processCardFullscreen($fullname, &$first_name = '', &$last_name = '') {
121     $fullname = trim($fullname);
122     $pos = strpos($fullname, ' ');
123     if ($pos !== false) {
124         $first_name = trim(substr($fullname, 0, $pos));
125         $last_name = trim(substr($fullname, $pos));
126     } else {
```

H1. Hệ thống cấu hình sai.

```
private static String SESSION_FILE_PATH = "██████████";
private static File fileSession = null;
private int MAX_TIME_LOGIN = 3;

//      String PARTNER_ID = ██████████;
//Key ██████████
String CLIENT_ID = "██████████";
String CLIENT_SECRET = "██████████";
String SCOPE = "wallets payments verifications";
String GRANT_TYPE = "client_credentials";
```

H2. Các trường dữ liệu nhạy cảm bị lộ trên nền tảng Github

Nguy cơ lộ lọt dữ liệu

Documents: Các tài liệu nội bộ, tài liệu mật của doanh nghiệp, tổ chức.

Các tài liệu được lưu hành nội bộ hoặc dưới dạng tài liệu mật.

Name

- I. HỒ SƠ PHÁP LÝ
- II. HỒ SƠ TÀI CHÍNH
- III. HỒ SƠ SẢN XUẤT KINH DOANH
- VI. HỒ SƠ KHÁC

H1. Các hồ sơ nhạy cảm bị lộ lọt

CÔNG BỐ THÔNG TIN TRÊN CÔNG THÔNG TIN ĐIỆN TỬ
CỦA ỦY BAN [REDACTED]
DISCLOSURE OF INFORMATION ON WEB PORTALS OF
[REDACTED]

Kính gửi: - Ủy ban [REDACTED]
To: State Sec.
- Sở [REDACTED]

- Tên tổ chức

: NGÂN HÀNG [REDACTED]

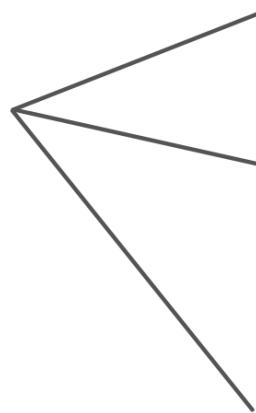
H2. Các tài liệu nhạy cảm bị lộ lọt

Nguy cơ lộ lọt dữ liệu

- ▶ Credentials: Tài khoản cá nhân, tài khoản đăng nhập vào các hệ thống.

```
Name: email  
Value: 0000000000  
=====  
Name: password  
Value: 1234567890
```

```
URL: https://vpn...bank.com.vn/login.esp  
Username: ...  
Password: 70111101
```



Thông tin đăng nhập: tài khoản + mật khẩu của nhân sự hoặc của khách hàng.

Thông tin đăng nhập vào nhiều hệ thống nội bộ nhạy cảm như:

- Hệ thống Email nội bộ
- Hệ thống VPN, Citrix, RDP,..

Tài khoản đăng nhập của khách hàng vào các hệ thống của doanh nghiệp, tổ chức

...@...com	FALSE	/	FALSE	2269925471
...@...com	TRUE	/	FALSE	2269925471
...@...com	TRUE	/	FALSE	2269925471
...@planning.net	TRUE	/	FALSE	1859965
...@...com	TRUE	/	FALSE	1676451
...@...com	TRUE	/	FALSE	1954573
...@...jp	TRUE	/	FALSE	1702371

Attack Surface - Exploit Public-Facing Application



Apache Log4j

- Kỹ thuật tấn công xuất hiện vào **2016**
- **11/2021** công bố lỗ hổng.



- Ảnh hưởng rộng rãi **5 triệu** ứng dụng toàn cầu sử dụng Apache Log4j

Attack Surface - Supply Chain Attack



SolarWinds

- Tấn công bắt đầu vào **2019**
- **2021** mới được phát hiện



- **~18,000** khách hàng bị ảnh hưởng, bao gồm **Chính phủ và các công ty lớn** tại Mỹ

**45% cuộc tấn công thành công từ các public websites*

Attack Surface - Cloud security



Toàn cầu
Lộ lọt dữ liệu



Thời gian

2018 - 2019



Facebook
Lộ lọt dữ liệu

2019



LinkedIn
Lộ lọt dữ liệu

2021

- **33.4 tỷ** bản ghi dữ liệu
- **5,000 tỷ USD**

540 triệu bản ghi dữ liệu
người dùng

700 triệu bản ghi dữ liệu
người dùng

2020

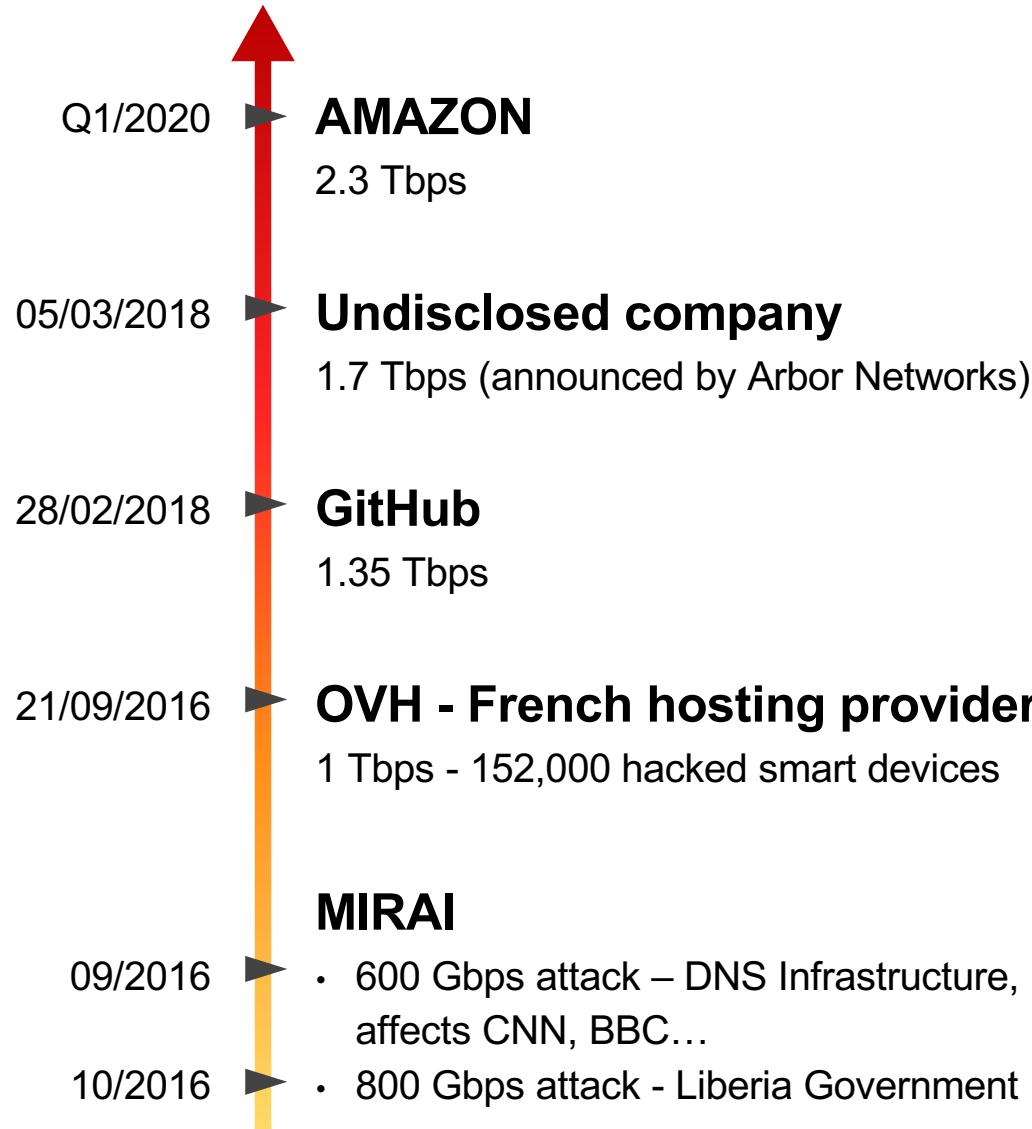
Tấn công thử nghiệm

Mỹ

Can thiệp hệ thống
đèn tín hiệu giao thông



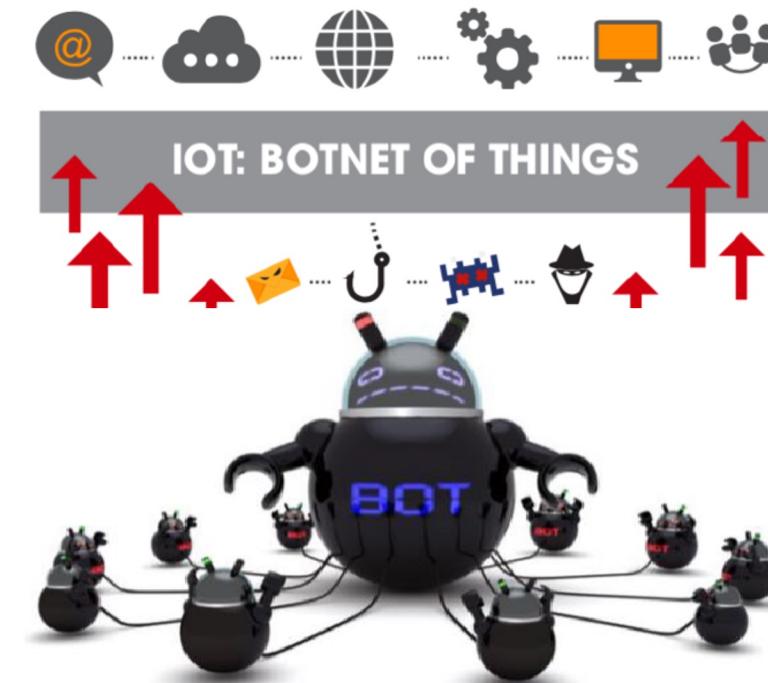
Attack Surface - DDoS từ IoT



Tại Việt Nam:

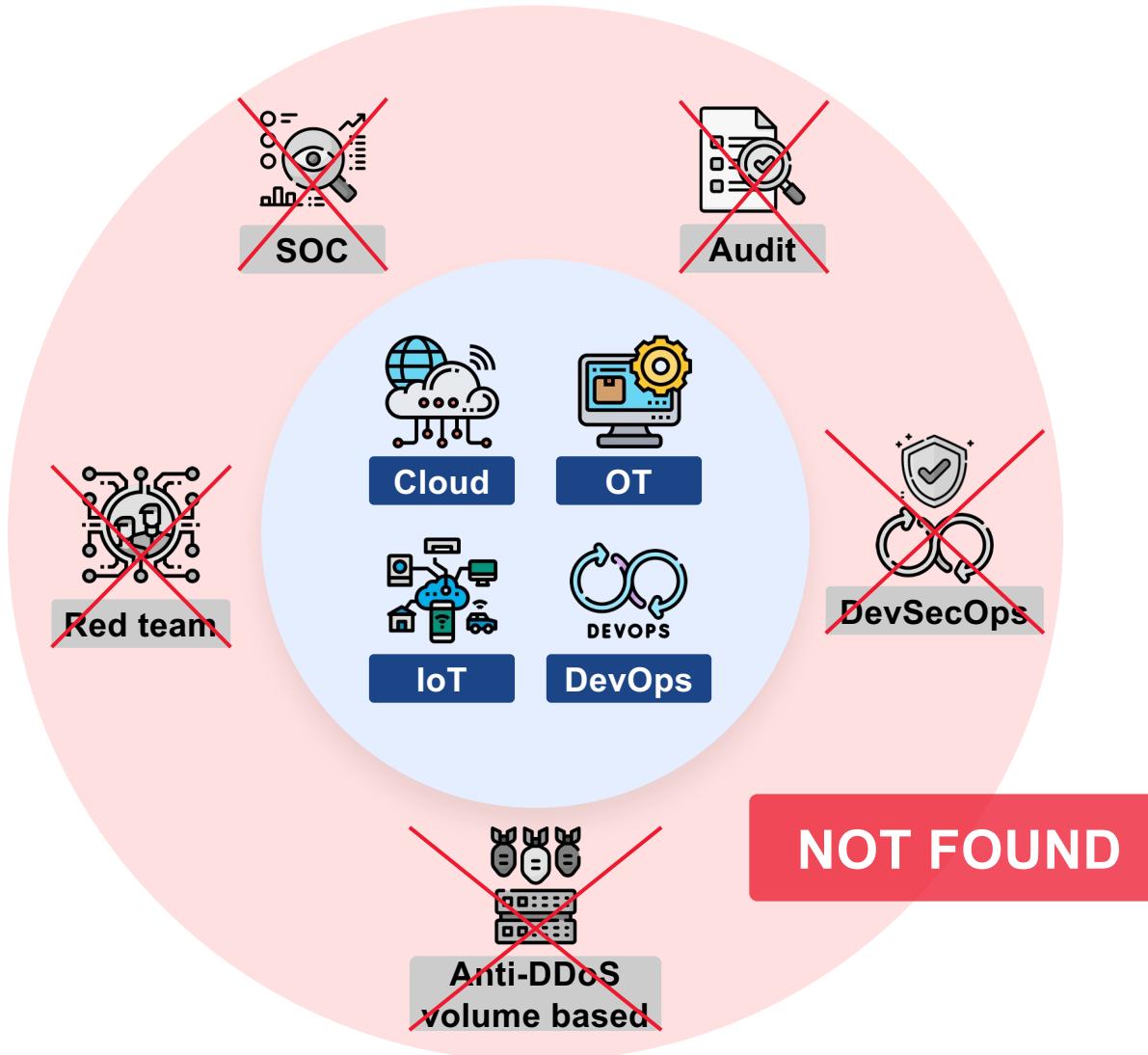
100-300 cuộc tấn công **>1 Gbps**/tháng

cuộc tấn công lớn nhất **90 Gbps**



Chúng ta liệu đã
SẴN SÀNG?

Cybersecurity đang đi sau chuyển đổi số



24%

CISO tham gia vào quá trình CDS

29%

tổ chức **thực sự chuẩn bị** cho các nguy cơ liên quan đến CDS

82%

có trải nghiệm **data breach** là kết quả của quá trình CDS

Theo Anomali

Nội dung

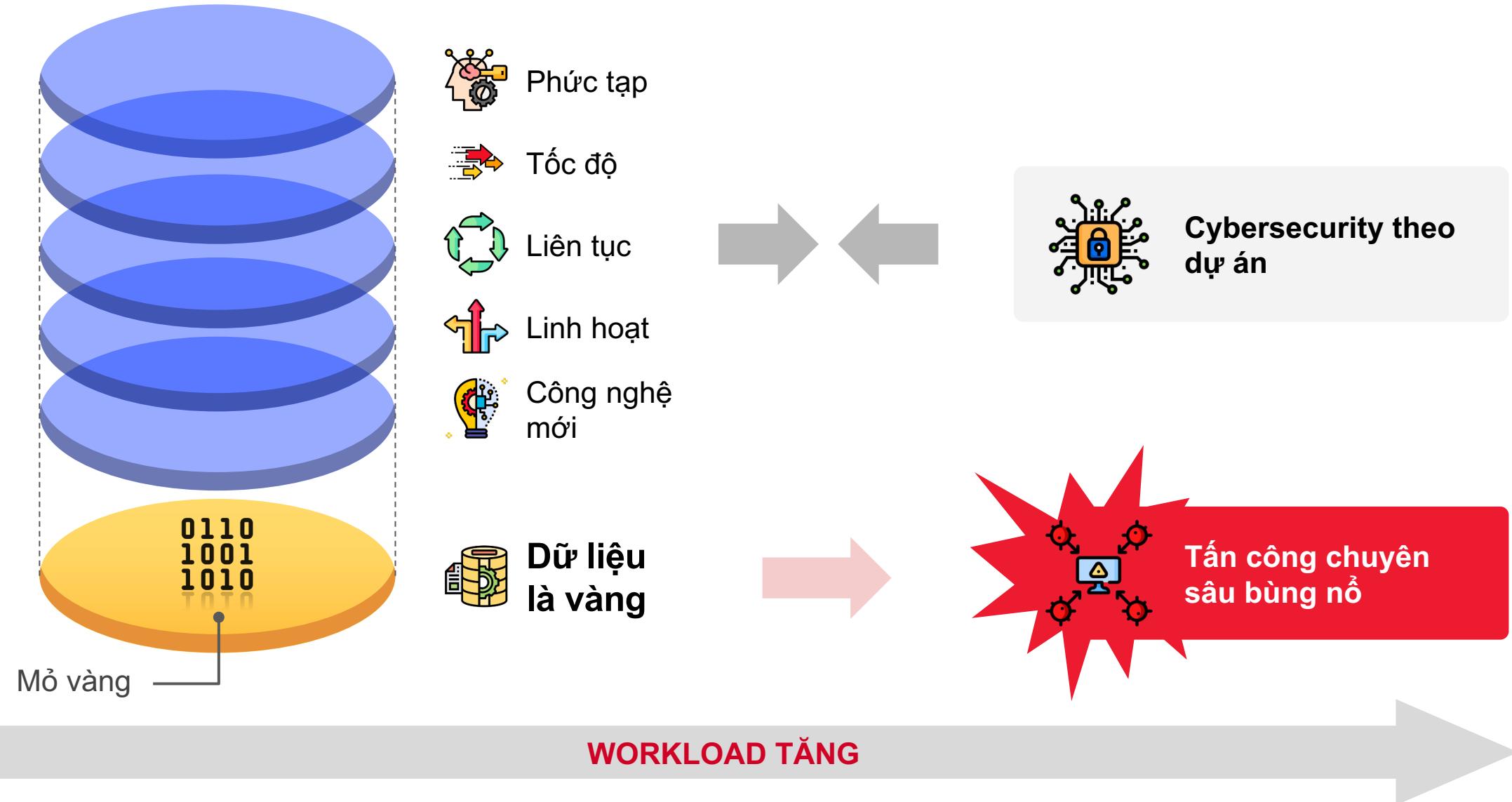
01 Công nghệ mới - Mối nguy mới

02 Chúng ta đã sẵn sàng?

03 Hướng tiếp cận



Đặc tính của Chuyển đổi số



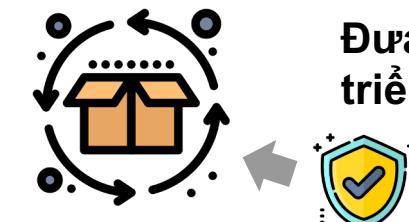
Đưa nguồn lực ATTT vào Chuyển đổi số



Tổ chức lực lượng ATTT trong
lực lượng CDS
MSSP cũng có thể là 1 lực lượng

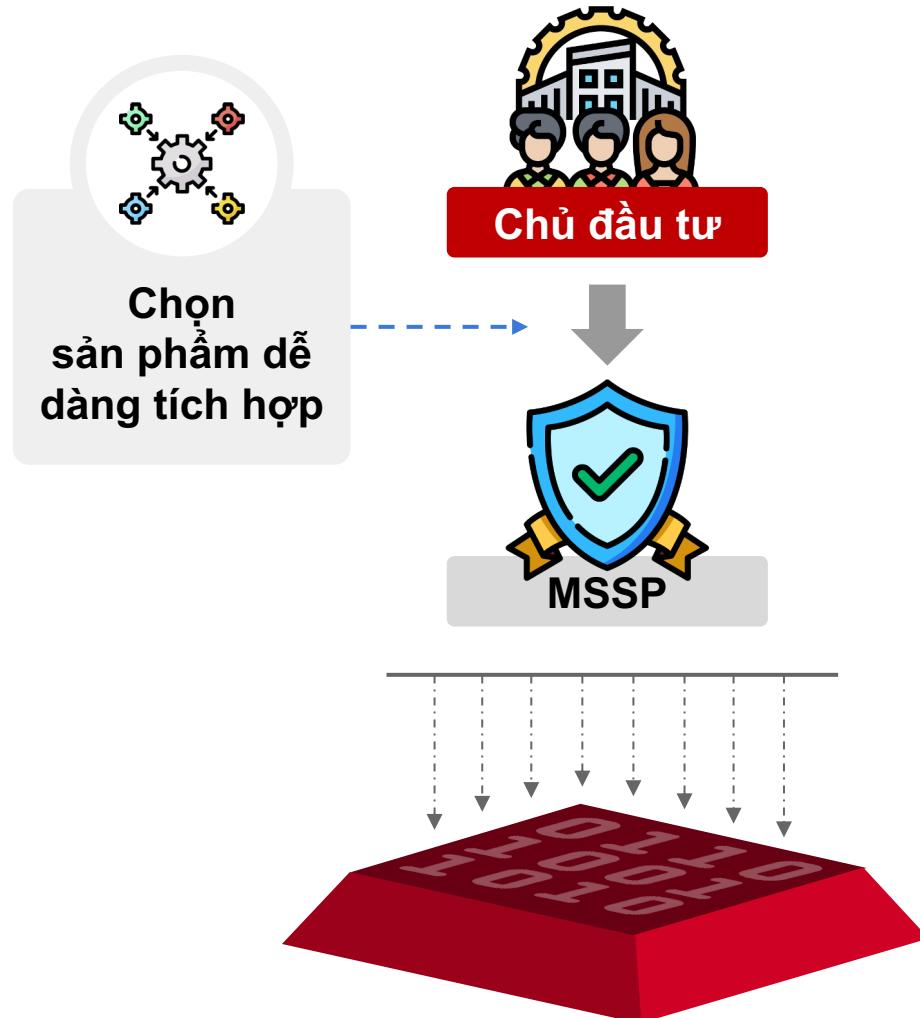


Thiết lập mục tiêu ATTT trong
dự án CDS

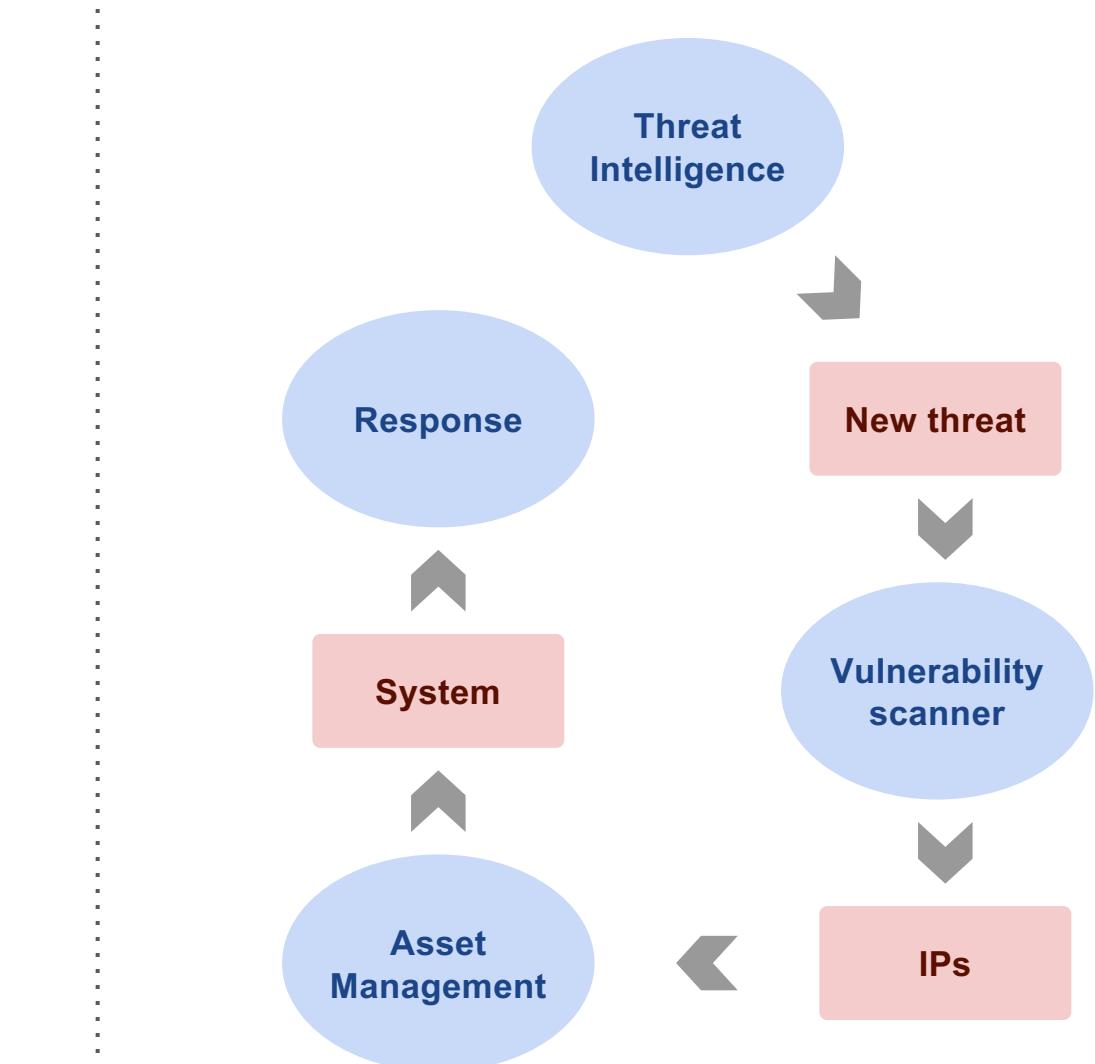


Đưa ATTT vào vòng đời phát
triển của sản phẩm dịch vụ CDS

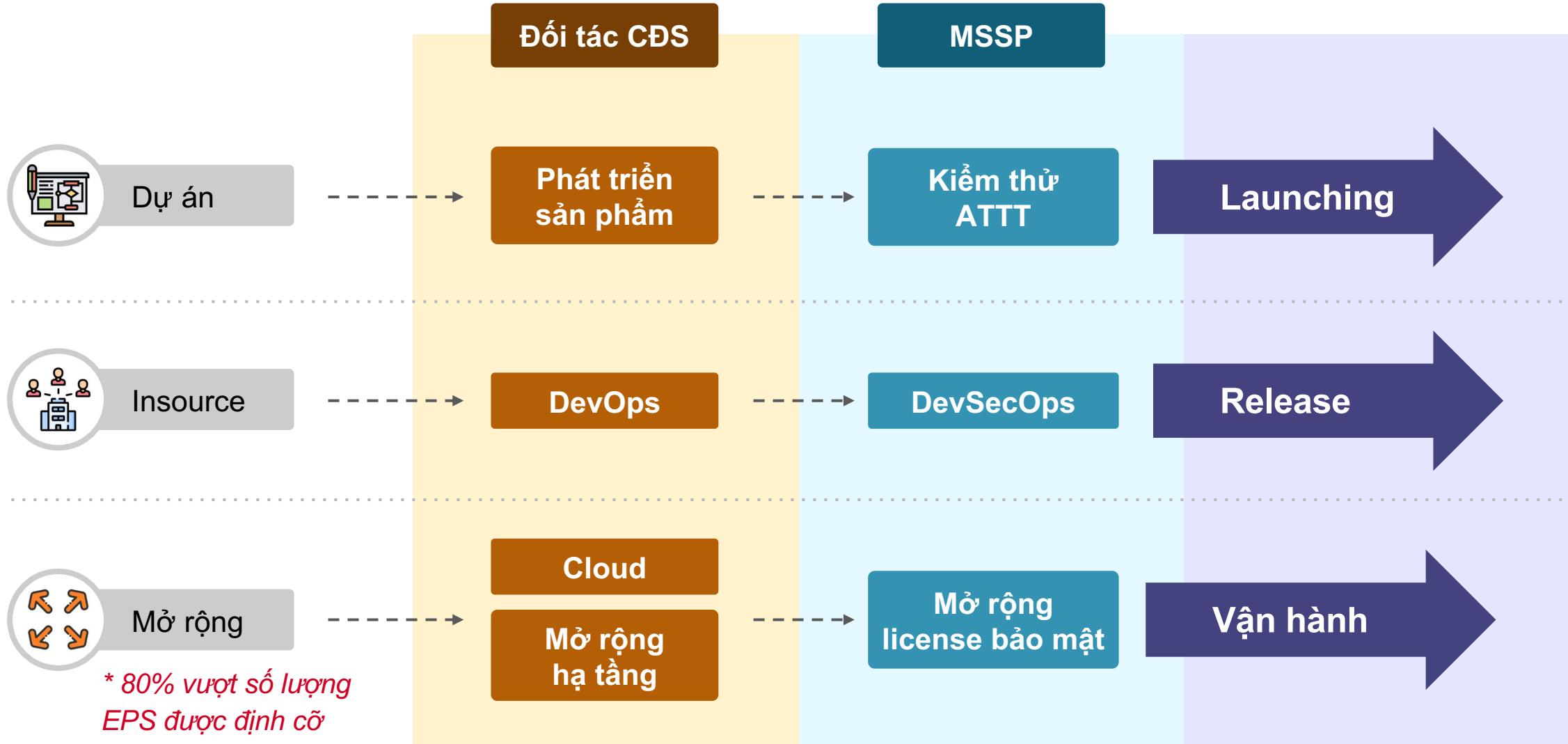
Nền tảng duy nhất



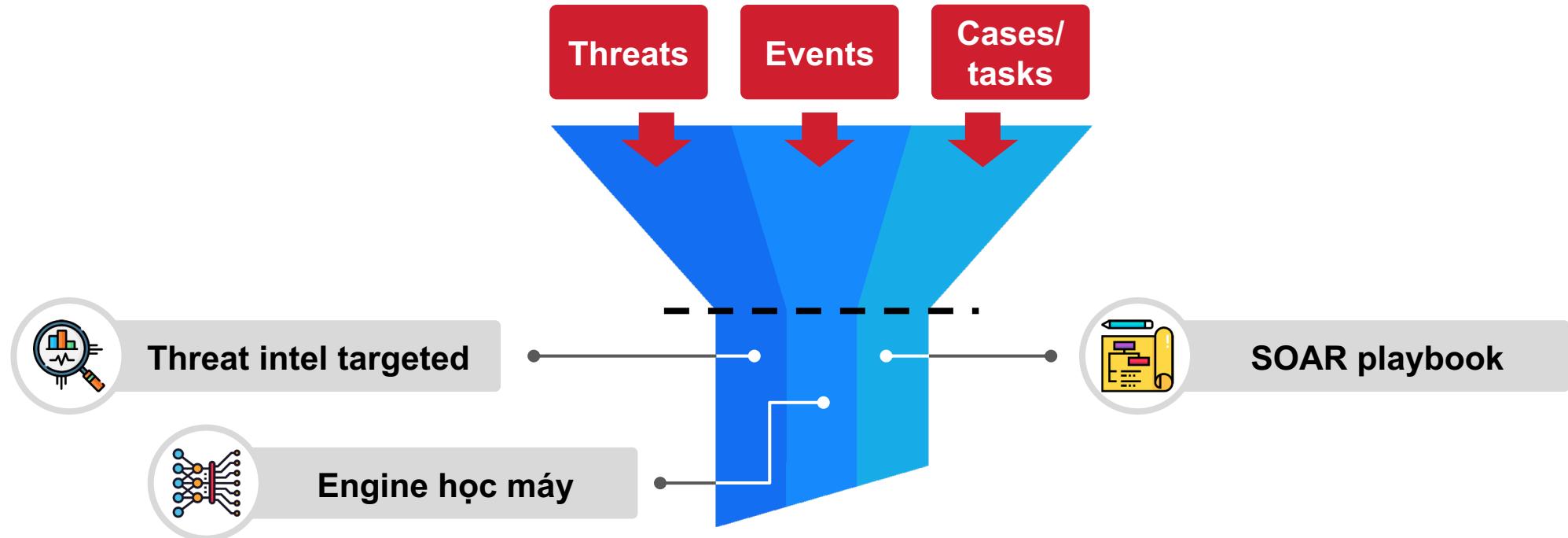
* 78% có nhiều hơn 16 công cụ,
12% có nhiều hơn 46 công cụ (theo Gartner)



Đồng bộ mô hình đầu tư



Scale bằng công nghệ



Threat Intelligence đã triển khai

3%

Doanh nghiệp lớn

18%

BFSI

SOAR đã triển khai

6%

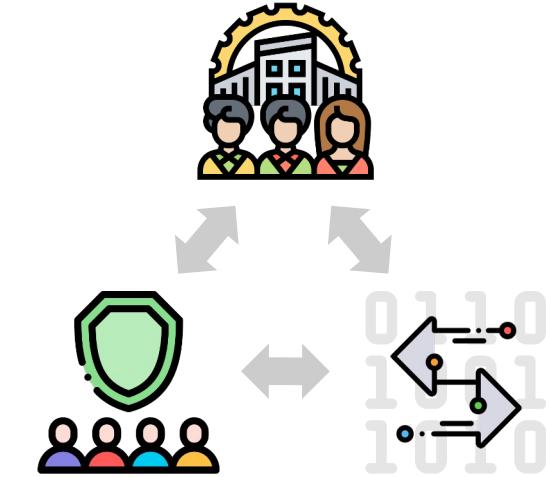
Doanh nghiệp lớn

18%

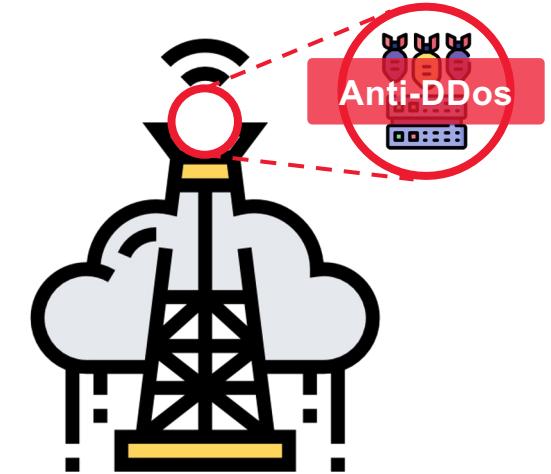
BFSI



Đưa ra tiêu chuẩn về ATTT cho các đối tác



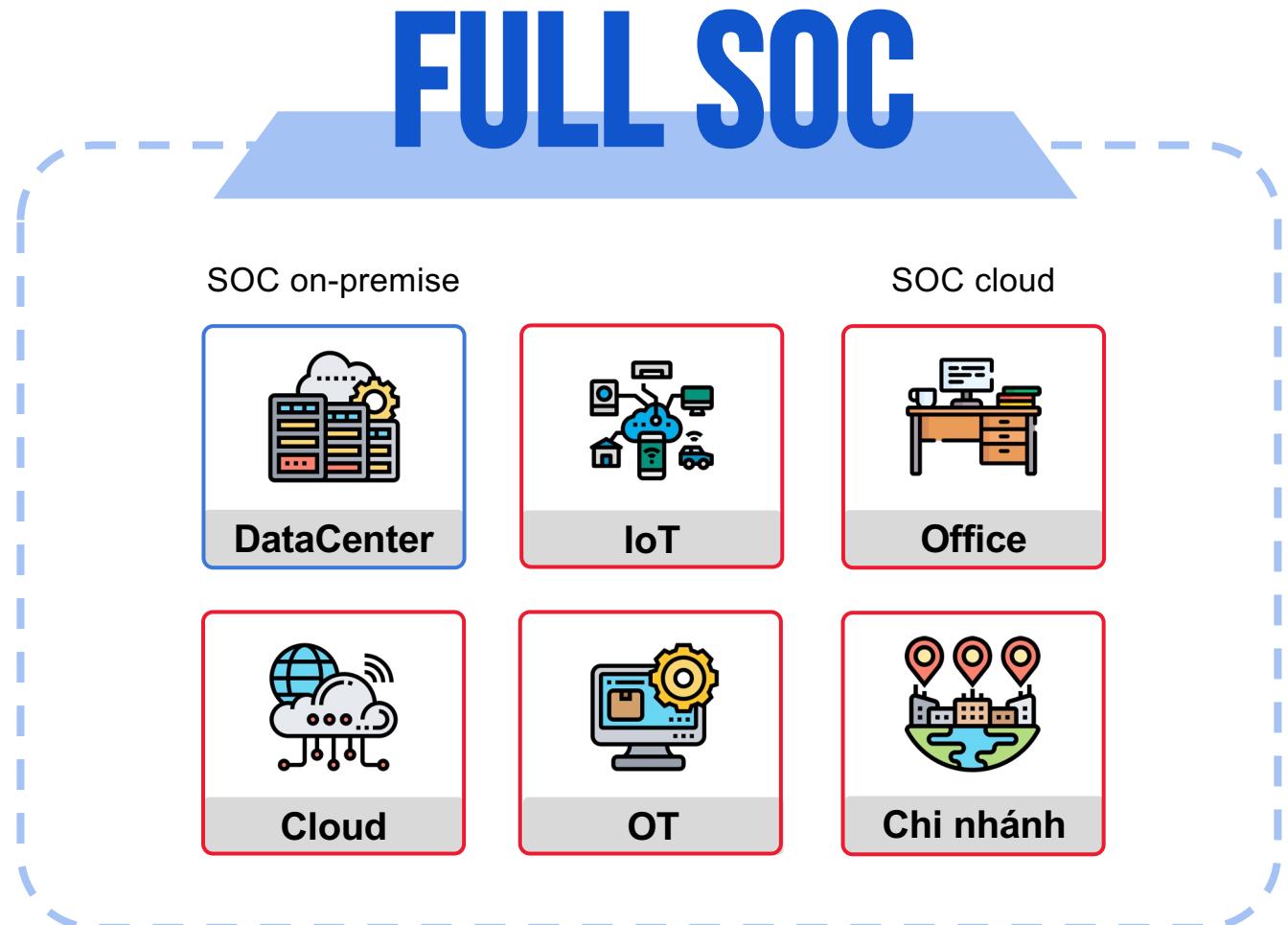
Xây dựng mô hình phù hợp giữa 3 bên
(Chủ đầu tư - Đối tác CDS - Đối tác ATTT)



Chọn ISP có tính đến dịch vụ Anti-DDos

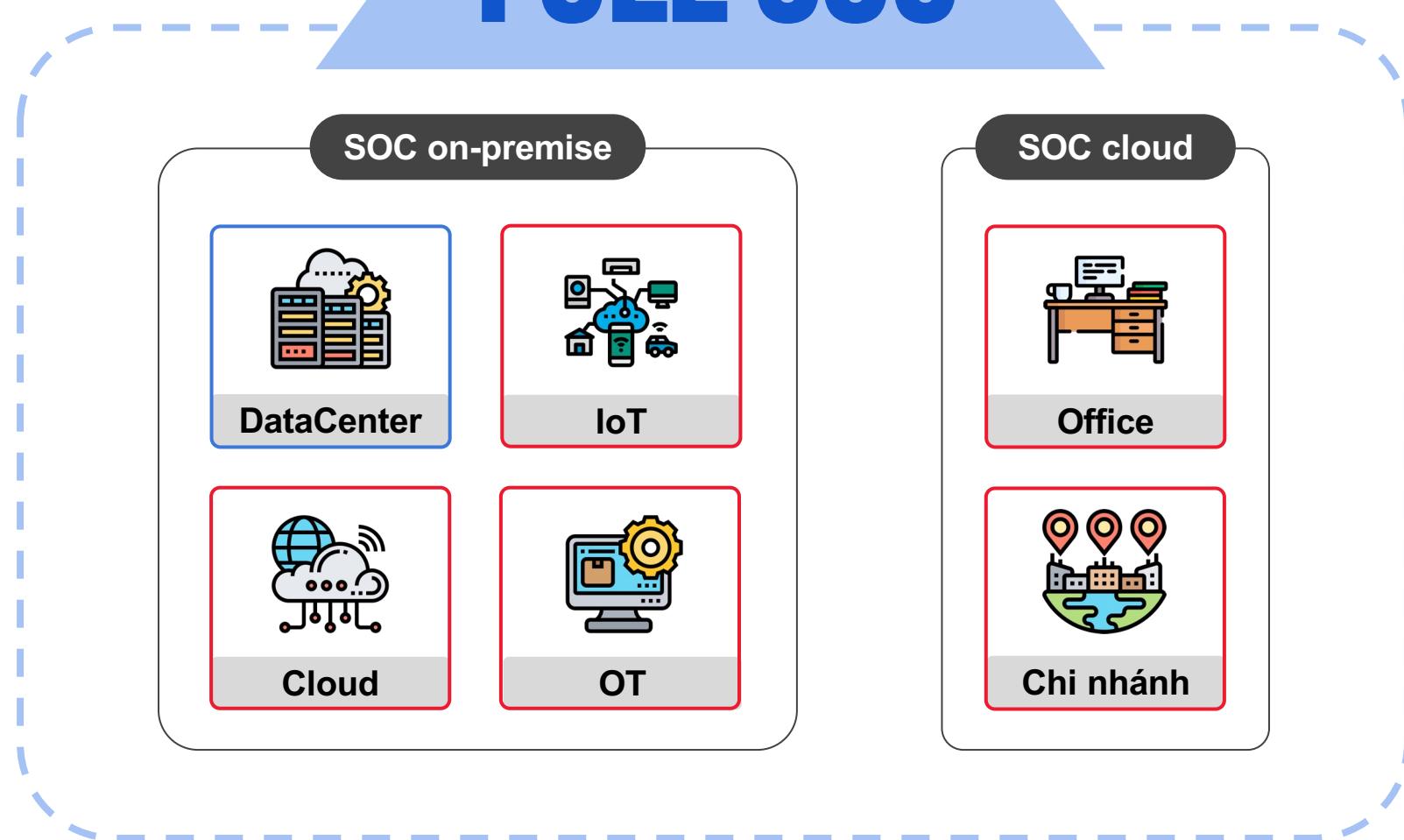


- Mean time to Detect (MTTD)
- Mean time to Respond (MTTR)
- Độ phủ giám sát
- Độ phủ content
- Mức độ tự động hóa

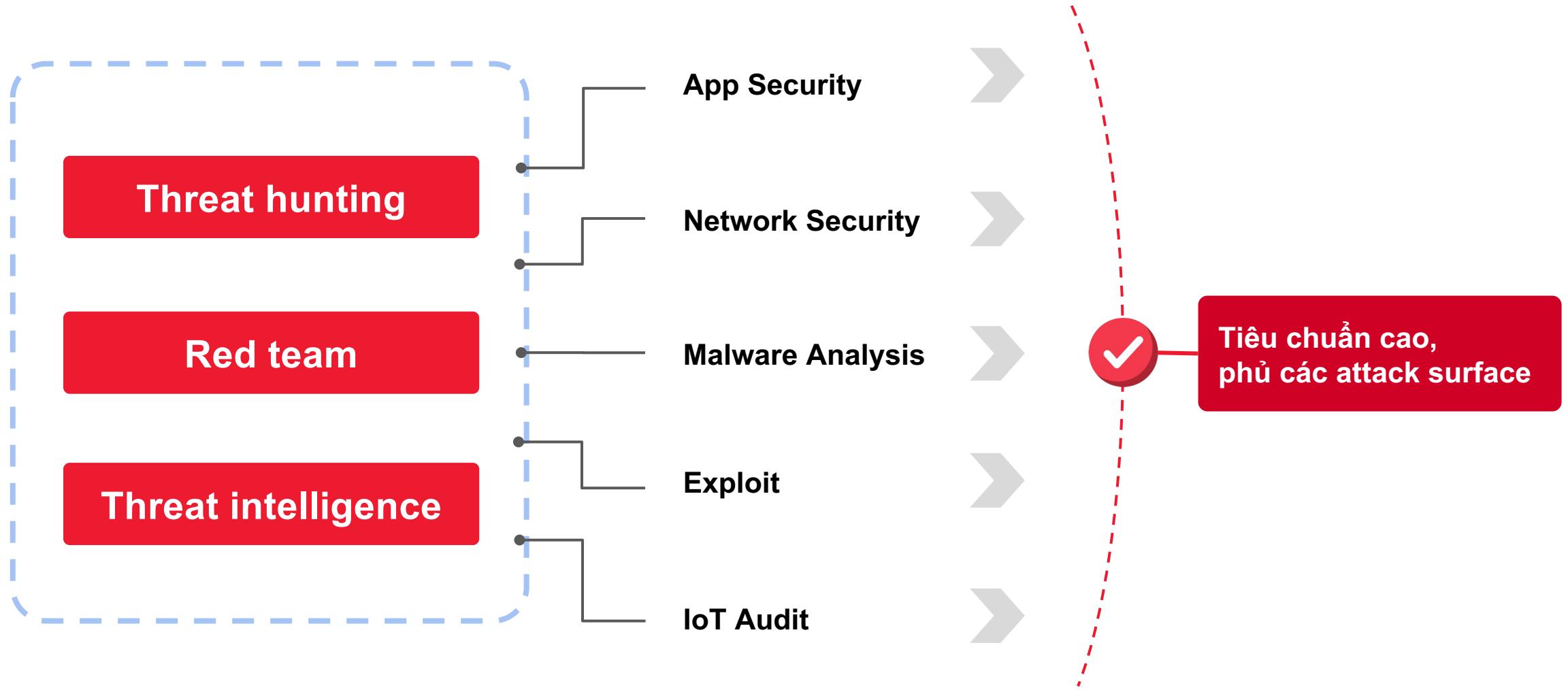


- 30% sự cố ngoài giám sát
- 75% giám sát DC hoặc 1 phần DC
- MTTD và MTTR tăng 35%

FULL SOC



Chủ động xóa khoảng cách



Đồng hành

Chứng chỉ

- ISO/IEC 27001:2013
- VB100

Zero-day

- Tổng ~400 zero-day
- Trong đó 15 zero-day cho IoT

Frost & Sullivan

- Nhà cung cấp dịch vụ quản lý ANM tốt nhất Việt nam 2020
- Nhà cung cấp dịch vụ ATTT số 1 Việt Nam 2022

IT World Awards

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

Pwn2Own

- Top 5 thế giới Pwn2Own 2021 tại Vancouver (Canada)
- Top 5 thế giới Pwn2Own 2022 tại Tokyo (Nhật Bản)

Stevie Awards

- Giải Bạc 2017

Cybersecurity Excellence Awards

- 13 giải Vàng 2022



Redteam



IoT Assessment



Cloud Security



DevSecOps



Asset Management



Anti-fraud



ISP Anti-DDoS



MSSP for Cloud



Threat Intelligence



SOAR



thank you!