CHƯƠNG TRÌNH ĐÀO TẠO 2025
MOBIFONE CYBER SECURITY

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE
NGÔ VĂN TIẾN – BU AN NINH MẠNG

NỘI DUNG

1

- **GIỚI THIỆU VỀ CYBER SECURITY CỦA MOBIFONE**
- Giới thiệu về Kiến trúc, Hệ sinh thái dịch vụ của MobFone

2

- **GIỚI THIỆU VỀ DỊCH VỤ SOC**
- SOC là gì
- Cấu trúc của MOBIFONE-SOC

3

- **GIỚI THIỆU CÁC DỊCH VỤ MOBIFONE SECURITY**
- Dịch vụ giám sát An toàn thông tin “Security Mornitoring
- Dịch vụ ứng cứu và xử lý sự cố “Incident Response”
- Dịch vụ săn tìm mối đe doạ “Threat Hunting”
- Dịch vụ dò quét lỗ hổng bảo mật “ Vulnerability Assessment”

4

- **GIỚI THIỆU CÁC DỊCH VỤ KHÁC**
- Dịch vụ Antivirus for Cloud
- Dịch vụ MobiSafe Office

GIỚI THIỆU VỀ CYBER SECURITY CỦA MOBIFONE

Số liệu các đợt tấn công mạng trên thế giới

- Thiệt hại 8.000 tỉ USD năm 2023
- Thiệt hại 9.500 tỉ USD năm 2024
- 353.027.892 người bị ảnh hưởng do vi phạm dữ liệu
- 11 giây có 01 tổ chức bị tấn công mã độc tống tiền
- Tấn công mạng quy mô lớn
- Tấn công các hệ thống thông tin quan trọng, chính phủ
- Tấn công làm tê liệt sản xuất, kinh doanh
- Gián điệp mạng, tình báo mạng, khủng bố mạng

NGUY CƠ

2025:

- 3.000 cuộc tấn công/giây.
- 12 mã độc/giây.
- 70 lỗ hổng/điểm yếu mới/ngày.

ĐỐI TƯỢNG

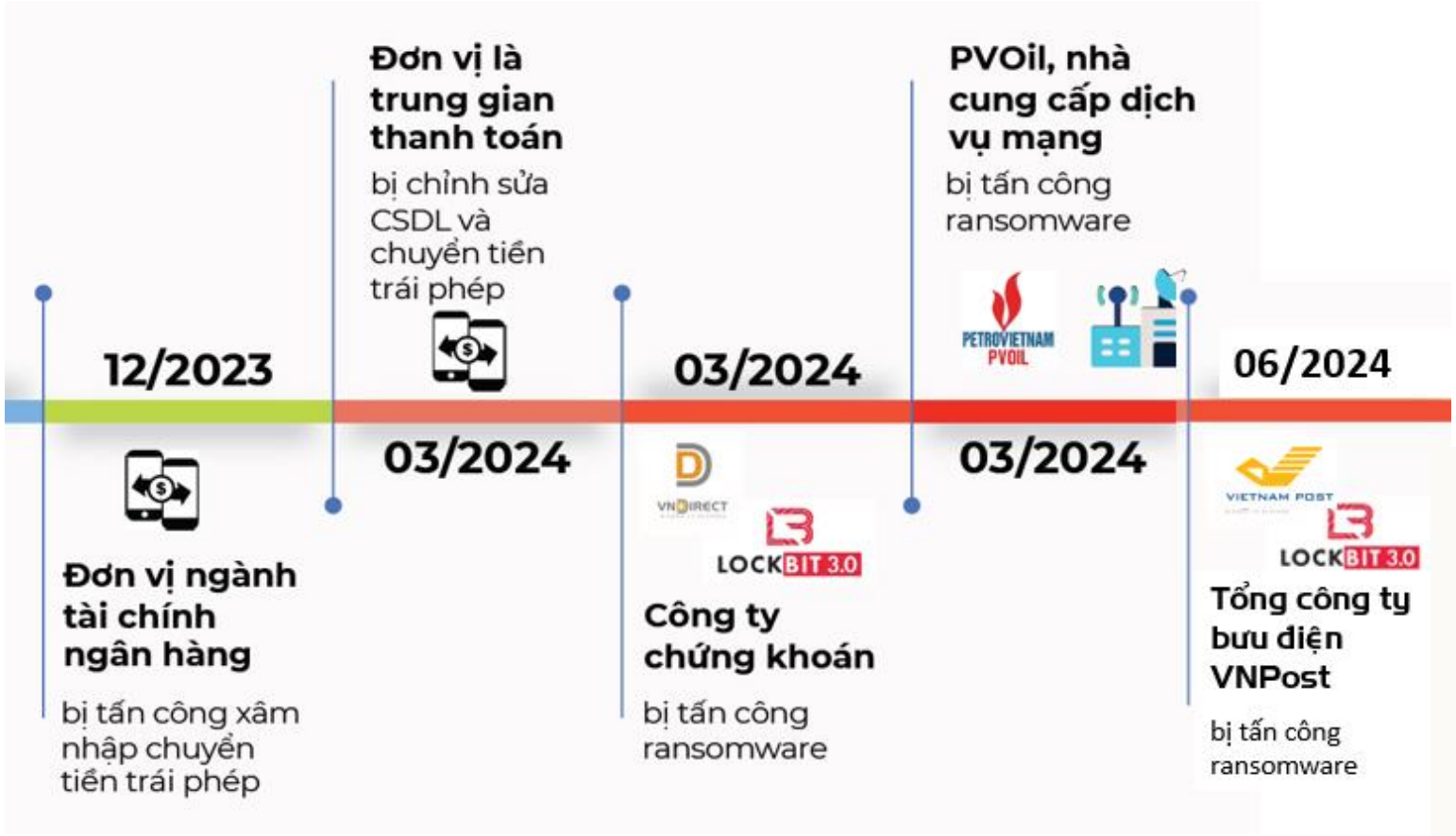
Đối tượng bị tấn công:

- **2025:** gấp 2,7 lần 2020.
- **2030:** gấp 7,5 lần 2020.

CÔNG NGHỆ

- **Lượng tử:** 100% ứng dụng mật mã phi đối xứng có thể bị phá vỡ.
- **AI:** dần thay thế con người. AI lĩnh vực ATTT đạt 38,2 tỉ $ năm 2026

Các sự cố An ninh mạng trong thời gian qua tại Việt Nam



9/04/2025

Tập đoàn CMC bị tấn công mã độc tống tiền

Đại diện CMC xác nhận một dịch vụ trong hệ thống kỹ thuật của tập đoàn bị tấn công ransomware có chủ đích.

Hai ngày qua, trên một số diễn đàn và website bảo mật quốc tế xuất hiện thông tin CMC trở thành nạn nhân của ransomware (mã độc tống tiền), được cho là nhóm Crypto24 thực hiện vào ngày 12/4. Theo trang *Hookphish*, có khoảng 2 TB dữ liệu bị khống chế, gồm dữ liệu token, dữ liệu trang web...

Số liệu các đợt tấn công mạng trong nửa đầu năm tại Việt Nam

Lộ lọt, rò rỉ thông tin dữ liệu

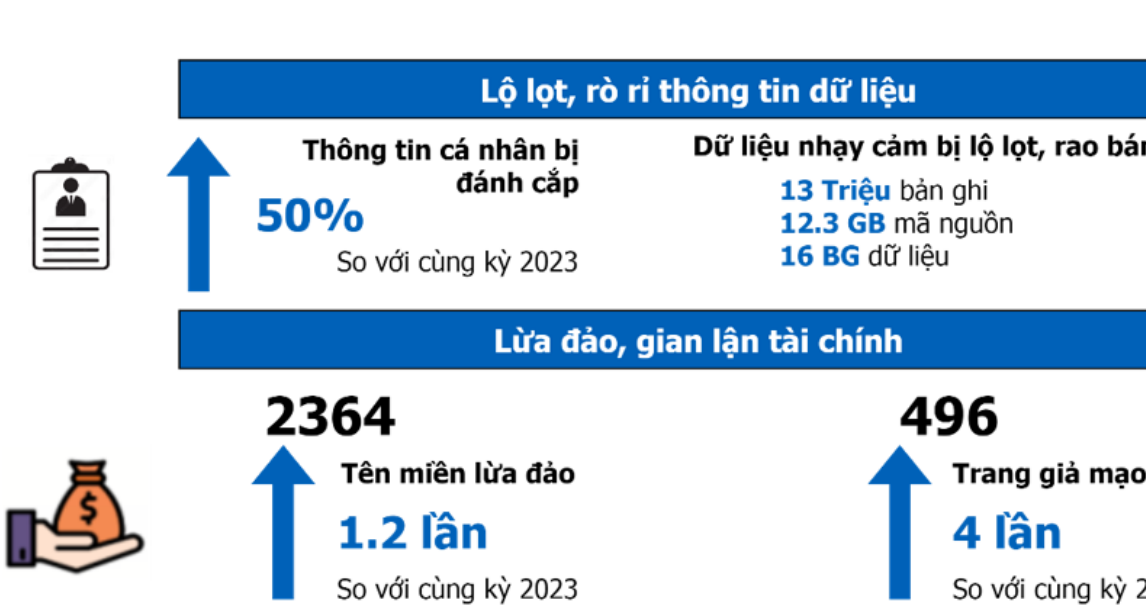
Thông tin cá nhân bị đánh cắp

50%

So với cùng kỳ 2023

Dữ liệu nhạy cảm bị lộ lọt, rao bán

13 Triệu bản ghi
12.3 GB mã nguồn
16 BG dữ liệu



Lừa đảo, gian lận tài chính

2364

Tên miền lừa đảo

1.2 lần

So với cùng kỳ 2023

496

Trang giả mạo

4 lần

So với cùng kỳ 2023

Theo khảo sát của Ban Công nghệ, Hiệp hội An ninh mạng quốc gia thực hiện vào tháng 12/2024 thì thiệt hại do lừa đảo trực tuyến gây ra trong 2024 lên đến **18.900 tỷ VNĐ**

17,648 lỗ hổng mới xuất hiện

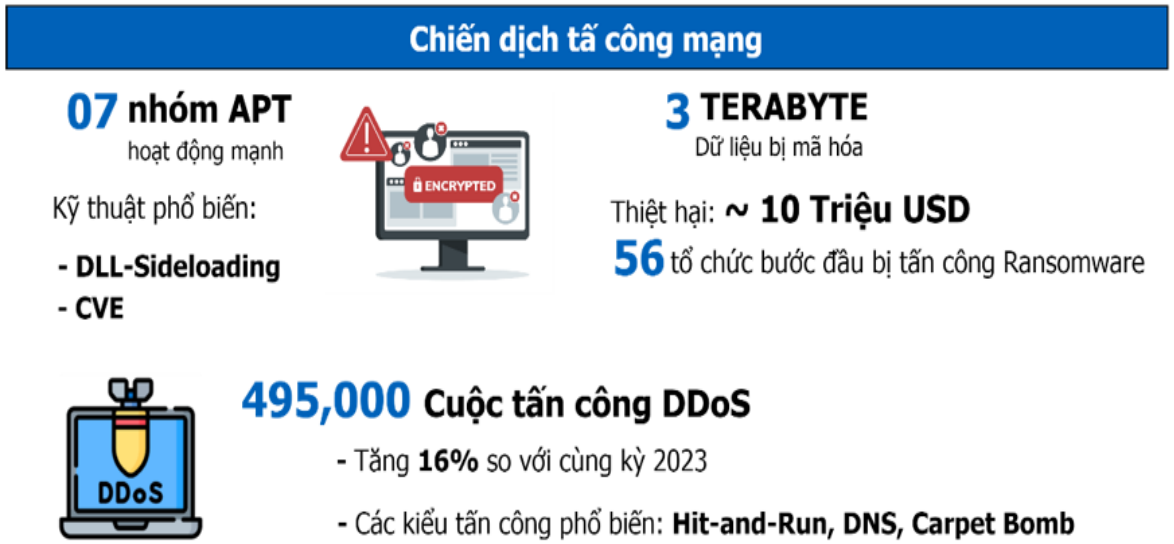
- **51%** là lỗ hổng mức Cao và Nghiêm Trọng (theo điểm CVSS)
- Tăng **42%** so với cùng kỳ 2023
- **71 lỗ hổng** có nguy cơ ảnh hưởng tới các tổ chức, doanh nghiệp Việt Nam

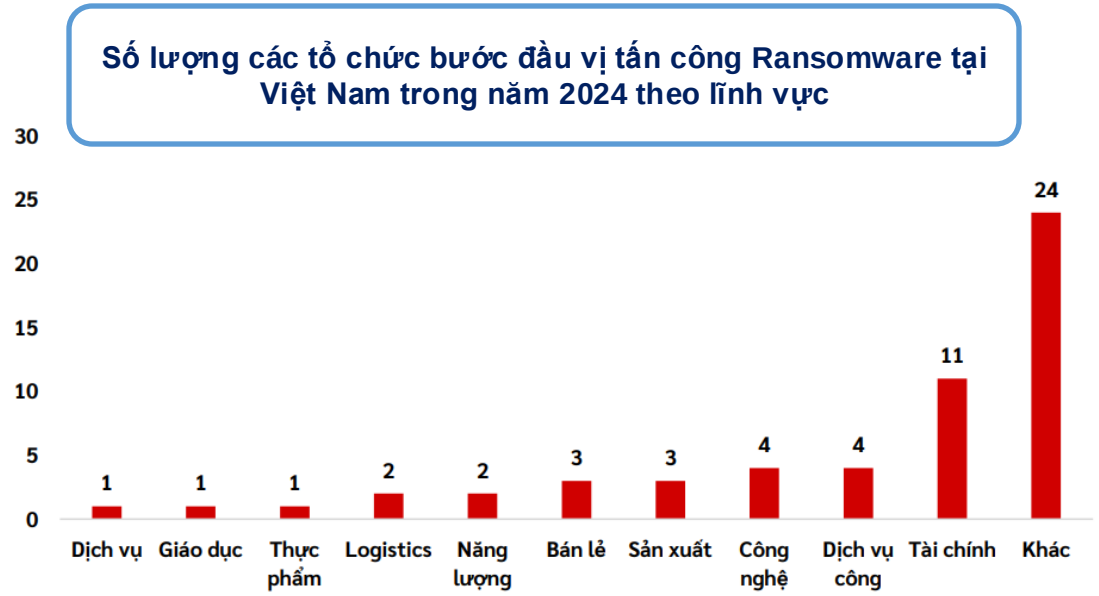
Số liệu các đợt tấn công mạng trong năm 2024 tại Việt Nam

Trong năm 2024

- Các nhóm ransomware như LockBit, Phobos, BlackByte, và Kill Security Ransomware đã gây thiệt hại **hàng chục triệu USD**, nhắm vào các lĩnh vực trọng yếu như tài chính, năng lượng và dịch vụ công. Những cuộc tấn công này không chỉ làm gián đoạn hoạt động mà còn để lại những tổn thất lâu dài về dữ liệu và danh tiếng doanh nghiệp. …
- Trong năm 2024, Microsoft đã phát hành bản vá cho hơn **1.020 lỗ hổng bảo mật**, trong đó có **28 lỗ hổng ở mức độ nghiêm trọng (Critical)** và hơn **951 lỗ hổng quan trọng (Important).** Các sản phẩm phổ biến khác như Apache, Cisco, VMware, và Citrix, Splunk cũng đối mặt với nhiều nguy cơ bị khai thác,
- Các mã độc phổ biến trong năm qua bao gồm CobaltStrike, PlugX và IIS Backdoor. Đặc biệt, mã độc mới GoldDigger đã tấn công hơn **50 ứng dụng tài chính và ví điện tử tại Việt Nam**, đánh cắp thông tin tài chính qua các trang web giả mạo và tệp APK độc hại. GoldPickaxe và Gigabud cũng là những mối đe dọa mới nhắm vào hệ điều hành iOS và các nền tảng tài chính.

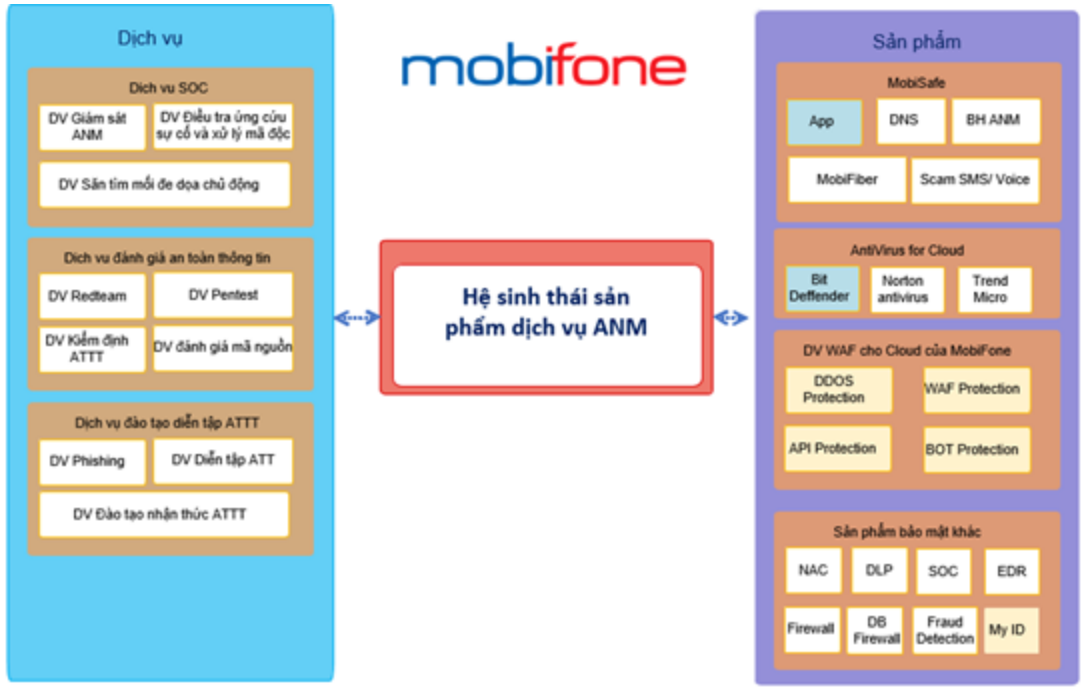
Trích dẫn Công ty cổ phần công nghệ an ninh mạng quốc gia Việt Nam (NCS)





Hệ sinh thái Cyber Cecurity

Dựa trên kiến trúc tổng thể hệ thống An ninh mạng đã được phê duyệt để xây dựng các sản phẩm dịch vụ phục vụ cho Kinh doanh lĩnh vực An ninh mạng.



Được cấp Giấy phép kinh doanh số: 303/GP-BTTTT ngày 15/10/2024

- Sản xuất sản phẩm kiểm tra, đánh giá an toàn thông tin mạng
- Sản xuất sản phẩm giám sát an toàn thông tin mạng
- Sản xuất sản phẩm chống tấn công, xâm nhập
- Dịch vụ giám sát an toàn thông tin mạng
- Dịch vụ phòng ngừa, chống tấn công mạng
- Dịch vụ ứng cứu sự cố an toàn thông tin mạng
- Dịch vụ tư vấn an toàn thông tin mạng
- Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng

KHỐI
CHÍNH PHỦ

TỔNG CỤC HẢI QUAN
BỘ KẾ HOẠCH VÀ ĐẦU TƯ
THANH TRA CHÍNH PHỦ
BỘ TÀI NGUYÊN MÔI TRƯỜNG
UBND QUẬN, HUYỆN HÀ NỘI
BỘ VĂN HÓA THỂ THAO VÀ DU LỊCH
SỞ THÔNG TIN TRUYỀN THÔNG CÁC TỈNH

KHỐI
BANK/DOANH NGHIỆP

BIDV
ABBANK NGÂN HÀNG AN BÌNH
JACCS
EVNNPC
AGRIBANK
timo
VNU
MASAN GROUP

KHỐI
CÁ NHÂN/HỘ GIA ĐÌNH

Kế hoạch phát triển các sản phẩm, dịch vụ

Khách hàng	Năm 2024	Năm 2025
	Sản phẩm, Dịch vụ	Sản phẩm, Dịch vụ
B2C	1. MobiSafe	1. MobiSafe 2. Bảo hiểm an ninh mạng 3. Social Listening
B2B, B2G	1. Dịch vụ kiểm tra, kiểm định đánh giá ATTT 2. Dịch vụ SOC 3. Dịch vụ điều tra, đánh giá sự cố 4. Dịch vụ đánh giá tư vấn đào tạo, diễn tập 5. Dịch vụ Antivirus for Cloud	1. Dịch vụ kiểm tra, kiểm định đánh giá ATTT 2. Dịch vụ SOC 3. Dịch vụ điều tra, đánh giá sự cố 4. Dịch vụ đánh giá tư vấn đào tạo, diễn tập 5. Dịch vụ Antivirus For Cloud 5. Dịch vụ WAF 7. MobiID 8. MobiSafe Smart Firewall (MobiSafe Office+ Endpoint)

I. Khách hàng mục tiêu

KHỐI
CHÍNH PHỦ

KHỐI
NGÂN HÀNG,
TÀI CHÍNH, BẢO HIỂM

KHỐI
GIÁO DỤC

KHÁC

BỆNH VIỆN	BẢO TÀNG	ĐƠN VỊ CUNG CẤP VÍ	BẢO HIỂM	VẬN CHUYỂN HÀNG HÓA
SỞ THÔNG TIN	RẠP CHIẾU PHIM	CÔNG TY NƯỚC	TRƯỜNG ĐH	TRUNG TÂM VH

CÁC DỊCH VỤ TIỀM NĂNG TRIỂN KHAI CHO DỰ ÁN CYBER CECURITY

I. GIỚI THIỆU TRUNG TÂM GIÁM SÁT AN TOÀN THÔNG TIN SOC

II. DỊCH VỤ AN TOÀN THÔNG TIN

1. Dịch vụ giám sát an toàn thông tin
2. Dịch vụ Đánh giá an toàn thông tin
3. Dịch vụ ứng cứu xử lý sự cố
4. Dịch vụ săn tìm mối đe dọa

III. SẢN PHẨM ANTIVIRUS CHO MÁY CHỦ CLOUD

IV. SẢN PHẨM MOBISAFE OFFICE

TRUNG TÂM GIÁM SÁT AN TOÀN THÔNG TIN SOC

I. GIỚI THIỆU VỀ SOC

Trung tâm Điều hành an ninh mạng - SOC (Security Operation Center): là bộ máy có nhiệm vụ theo dõi, phát hiện, cách ly, xử lý các sự cố và chịu trách nhiệm về mức độ an toàn của toàn bộ hệ thống thông tin của tổ chức với tần suất giám sát, hoạt động 24/7

MobiFone là một trong những đơn vị tiên phong về SOC “Make in VietNam”

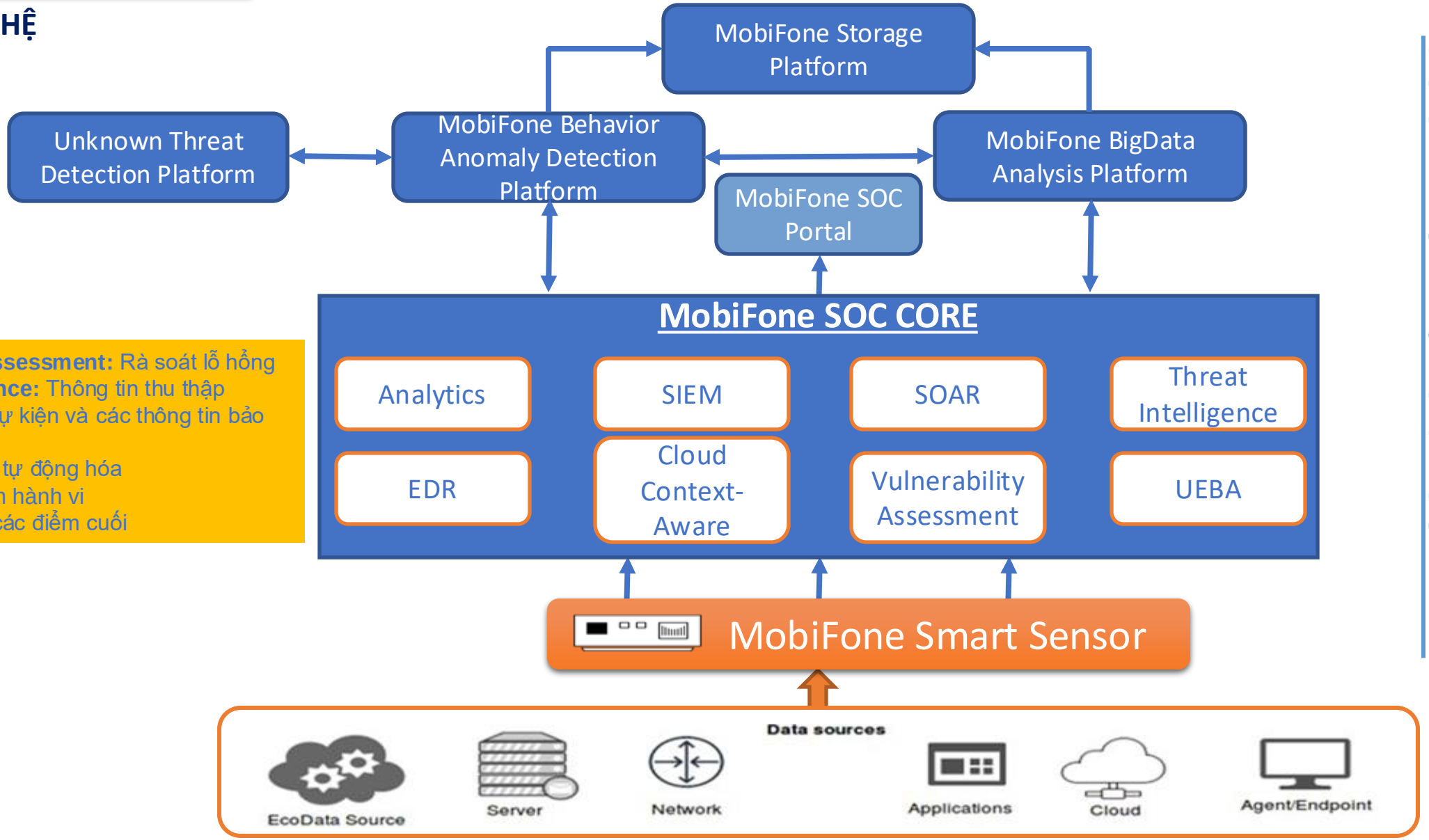
- ✓ EDR
- ✓ SIEM
- ✓ Analytics Engine
- ✓ Threat Intelligence
- ✓ AI Platform
- ✓ BigData Platform
- ✓ Storage Platform

MobiFone SOC là sự kết hợp hoàn hảo giữa 3 yếu tố:

- **Con người:** MobiFone SOC quy tụ các chuyên gia trong hàng đầu trong lĩnh vực an ninh an toàn thông tin với gần 10 năm kinh nghiệm
- **Công nghệ:** Sử dụng 2 nền tảng công nghệ theo nhu cầu của khách hàng (QRadar & Tự phát triển)
- **Quy trình:** Các quy trình vận hành, báo cáo – xử lý sự cố tuân thủ chính sách ANTT áp dụng nghiêm ngặt theo các tiêu chuẩn quốc tế ISO 27035, ISO 20000 và ISO 27001.

I. GIỚI THIỆU VỀ SOC

1. CÔNG NGHỆ



Vulnerability Assessment: Rà soát lỗ hổng
Threat Intelligence: Thông tin thu thập
SIEM: Quản lý sự kiện và các thông tin bảo mật
SOAR: Công cụ tự động hóa
UEBA: Phân tích hành vi
EDR: Giám sát các điểm cuối

SOC - MobiFone SECURITY

I. GIỚI THIỆU VỀ SOC

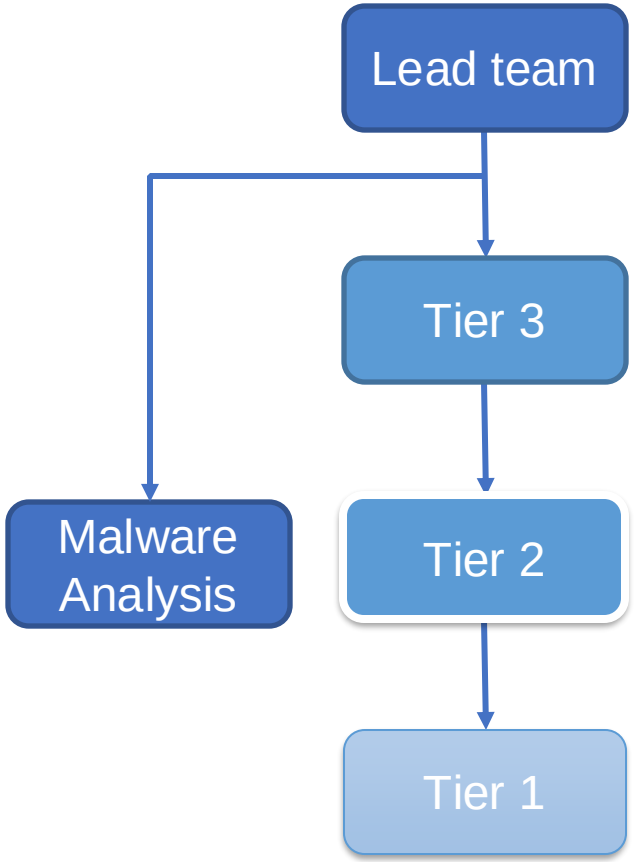
2. QUY TRÌNH

Quy trình hoạt động, báo cáo cũng như điều tra và xử lý sự cố đều được đảm bảo là tuân thủ theo tiêu chuẩn quốc tế ISO 27035:2009 và ISO 27001 và Tuân thủ nghiêm ngặt SLA được ký kết với Khách hàng.

Sources of Alerts	Mức độ đe dọa (từ CMC SIEM)	Mức độ ưu tiên xử lý	Phương pháp thông báo	Thời gian tối đa từ khi nhận cảnh báo đến khi xử lý
SOC Alerts	HIGH	3	Thời gian thực thông qua tin nhắn và email	90 phút
	WARNING	2	Thời gian thực thông qua tin nhắn và email	24 tiếng
	INFORMATIONAL	1	N/A	
Alerts/ Notification từ khách hàng	Review Action	3	N/A	180 phút từ khi nhận được thông báo chính thức từ khách hàng

2. GIỚI THIỆU VỀ SOC

3. CON NGƯỜI



Điều tra số (Forensic Team)
Săn tìm mối đe dọa (Threat Hunting Team)

Phân tích (Analyst Team)
Xử lý sự cố (Incident Response Team)

Giám sát và cảnh báo (Monitor and Alert Team)

2. GIỚI THIỆU VỀ SOC

4. KHẢ NĂNG VÀ LỢI ÍCH

Hoạt động giám sát ATTT có nhiệm vụ theo dõi, thu thập, tổng hợp, phân tích, xác minh thông tin về các rủi ro, sự cố ATTT, các cuộc tấn công vào đối tượng giám sát; chịu trách nhiệm về mức độ an toàn của toàn bộ hệ thống thông tin của tổ chức với tần suất giám sát, hoạt động 24/7/365

KHẢ NĂNG GIÁM SÁT

Giám sát kiểm soát vùng mạng và thiết bị mạng (Network Monitoring): kiểm soát các kết nối vào/ra, các thiết bị (Router, Switch,...), hoạt động sử dụng tài nguyên, sự tuân thủ (compliance) và các thành phần khác.

Giám sát kiểm soát thiết bị đầu cuối (Endpoint Monitoring): kiểm soát hiện trạng, các hoạt động trên thiết bị, phát hiện khi có hành vi bất thường hoặc dấu hiệu của mã độc.

Giám sát kiểm soát hệ thống máy chủ ứng dụng (Application Server Monitoring): thống kê và kiểm soát các hành luồng dữ liệu vào/ra, các cuộc tấn công vào máy chủ.Giám sát mã độc của hệ thống (Malware Monitoring): thống kê, giám sát hoạt động của mã độc và tình hình khắc phục.

Giám sát kiểm soát truy cập (Access Controls Monitoring): giám sát xác thực định danh, cảnh báo truy cập bất thường đối của các account.

LỢI ÍCH KHÁCH HÀNG

Nhanh chóng phát hiện mối đe dọa, từ đó có những giải pháp ngăn chặn và giảm thiểu rủi ro

Hạn chế các cảnh báo không chính xác (false positives) nhờ cơ chế xác định hành vi bất thường tích hợp AI và Machine Learning.

Giảm chi phi đầu tư cho an toàn thông tin – không cần đầu tư một khoản lớn chi phí cho nhân sự và hạ tầng bảo mật, thay vào đó có thể sử dụng dịch vụ được cung cấp bởi những chuyên gia hàng đầu trong ngành.

Được đảm bảo về sự an toàn của hệ thống thông tin 24/7 trước các mối đe dọa trên internet, kể cả những mối đe dọa mới chưa từng được biết đến.

2. GIỚI THIỆU VỀ SOC

5. Khách hàng mục tiêu

NHÓM KHÁCH HÀNG MỤC TIÊU

Cơ quan nhà nước và chính phủ

Nhu cầu:

- Đảm bảo an ninh cho hệ thống thông tin quan trọng quốc gia (cấp độ 4-5)
- Phát hiện sớm và xử lý các mối đe dọa nhằm bảo vệ dữ liệu quan trọng.
- Tuân thủ quy định pháp luật (như Luật an toàn thông tin mạng và Luật an ninh mạng)

Doanh nghiệp lớn và các tập đoàn

Nhu cầu:

- Giám sát liên tục để phát hiện và phản ứng nhanh với các mối đe dọa.
- Đảm bảo hoạt động không bị gián đoạn do các cuộc tấn công mạng.
- Quản lý và phân tích log tập trung từ nhiều chi nhánh và hệ thống.

Ngành tài chính ngân hàng và bảo hiểm

Nhu cầu:

- Bảo vệ hệ thống giao dịch trực tuyến (24/7)
- Tuân thủ các tieu chuẩn bảo mật (PCI DSS, ISO 27001) và yêu cầu pháp luật của Ngân hàng Nhà nước.
- Ngăn chặn kịp thời các cuộc tấn công mạng như phising, ransomware

Doanh nghiệp vừa và nhỏ (SMEs)

Nhu cầu:

- Bảo mật giao dịch và các thông tin khách hàng
- Phát hiện kịp thời các lỗ hổng hoặc các cuộc tấn công
- Đảm bảo vận hành liên tục, không bị gián đoạn do tấn công mạng
- Tiết kiệm chi phí bằng cách thuê dịch vụ SOC.

Sở Ban nghành | Bệnh viện | Bảo tàng | Công ty nước

CÁC DỊCH VỤ AN TOÀN THÔNG TIIN

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

2. DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

	VA (VULNERABILITY ASSESSMENT)	PENTEST(PENETRATRION TESTING)	SECURITY AUDIT	SOURCE CODE REVIEW
	DV Rà soát lỗ hổng bảo mật	DV Tấn công kiểm thử lỗ hổng bảo mật	DV Kiểm định an ninh hệ thống	DV Kiểm định bảo mật mã nguồn
Mô tả	Tìm kiếm và đo lường mức độ nghiêm trọng của nhiều lỗ hổng đã được định danh nhất có thể→ Cung cấp bức tranh chiều rộng về thông tin điểm yếu/lỗ hổng	Tấn công để tìm kiếm tối đa sự ảnh hưởng của các lỗ hổng, điểm yếu có thể bị lợi dụng→ Khai thác sâu các lỗ hổng của hệthống	Kiểm tra tổng thể thiết lập và cấu hình của hệ thống CNTT (Không bao gồm Source Code) về mức độ tuân thủ các tiêu chuẩn bảo mật (TC quốc tế như CIS, SANS hoặc QĐ của tổ chức)	Kiểm tra source code theo tiêu chuẩn và rà quét lỗ hổng bảo mật. Thường sẽ đi kèm khi sử dụng pentest phương pháp whitebox.
Cách thức triển khai	Rà quét tự động và chuyên gia thực hiện đánh giá mức độ và khuyến nghị cho các lỗ hổng tìm được	Chuyên gia bảo mật đứng dưới vai trò là một Hacker mũ trắng, thực hiện thâm nhập hệ thống tìm kiếm lỗ hổng và khai thác lỗ hổng nhằm mục đích hoàn thiện bảo mật hệ thống	Thực hiện thu thập cấu hình thiết bị và khuyến nghị thiết kế lại cấu hình hệ thống theo tiêu chuẩn bảo mật quốc tế (CIS Benmark,..)	Chuyên gia bảo mật thực hiện rà soát từng dòng code để tìm kiếm các lỗi về bảo mật
Thời gian triển khai	Tùy thuộc vào phạm vi đánh giá	Tùy thuộc vào phạm vi đánh giá	Tùy thuộc vào phạm vi đánh giá	Tùy thuộc vào phạm vi đánh giá

QUY TRÌNH CUNG CẤP DỊCH VỤ

B1. Tìm kiếm khách hàng

- Đơn vị chủ trì: Cty DVKV, BU ANM, các đơn vị liên quan
- BU ANM: Giới thiệu sản phẩm dịch vụ, chính sách kinh doanh dịch vụ
- Ban GPDVS: Phối hợp phê duyệt thực hiện, tổ chức ghi nhận doanh thu, hướng dẫn các đơn vị thực hiện

B2. Ký hợp đồng

- CTKV chủ trì ký hợp đồng triển khai dịch vụ
- Triển khai lựa chọn đối tác cung cấp dịch vụ (Trong quá trình có chính sách đồng bộ)

B3.Tổ chức triển khai

- Công ty KV: Chủ trì theo dõi triển khai
- **Thông báo BU ANM p/h theo dõi, phối hợp cùng đối tác thực hiện**
- Đối tác triển khai theo phạm vi hợp đồng

B4. Nghiệm thu, thanh lý

- Công ty KV chủ trì triển khai nghiệm thu thanh lý và cấp chứng nhận
- Đối tác cung cấp đầy đủ các thông tin liên quan
- **BU ANM p/h nghiệm thu, hướng dẫn cấp certificate**

Note: Với các yêu cầu đánh giá ATTT, pentest, audit: sẽ có certificate cấp cho đơn vị thực hiện

TỔNG CÔNG TY VIỄN THÔNG MOBIFONE

GIẤY CHỨNG NHẬN

Chứng nhận

Công ty …

Địa chỉ: …

Mã số thuế: …

Đã được đánh giá kiểm tra, đánh giá an toàn thông tin theo tiêu chuẩn OWASP cho ….

- Dò quét các điểm yếu cấu hình
- Dò quét các điểm yếu về xác thực
- Dò quét các điểm yếu về ủy quyền
- Dò quét các điểm yếu liên quan đến dữ liệu đầu vào
- Dò quét các điểm yếu mã hóa
- Dò quét các điểm yếu khả năng kiểm soát lỗi
- Dò quét các điểm yếu liên quan đến đầu ra dữ liệu

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

1. DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN

- Theo dõi, thu thập, tổng hợp, phân tích, xác minh thông tin về các rủi ro, sự cố ATTT, các cuộc tấn công vào đối tượng giám sát.
- Chịu trách nhiệm về mức độ an toàn của toàn bộ hệ thống thông tin của tổ chức với tần suất giám sát, hoạt động 24/7

ƯU ĐIỂM NỔI BẬT

- Giám sát hệ thống liên tục 24/7 theo thời gian thực (real-time).
- Tích hợp hệ thống trí tuệ nhân tạo AI và Machine Learning giúp nâng cao khả năng tự động giám sát.
- Phát hiện các mối đe dọa mới nhất nhờ vào cơ chế cập nhật cơ sở dữ liệu liên tục từ Threat Intelligence.
- Giám sát, phân tích và phản ứng nhanh chóng, chính xác đối với các mối đe dọa trên hệ thống.
- Khả năng tích hợp đơn giản, dễ dàng với các hệ thống CNTT

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

1. DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN

NHÓM KHÁCH HÀNG MỤC TIÊU

Cơ quan nhà nước và chính phủ

Nhu cầu:

- Đảm bảo an ninh cho hệ thống thông tin quan trọng quốc gia (cấp độ 4-5)
- Phát hiện sớm và xử lý các mối đe dọa nhằm bảo vệ dữ liệu quan trọng.
- Tuân thủ quy định pháp luật (như Luật an toàn thông tin mạng và Luật an ninh mạng)

Doanh nghiệp lớn và các tập đoàn

Nhu cầu:

- Giám sát liên tục để phát hiện và phản ứng nhanh với các mối đe dọa.
- Đảm bảo hoạt động không bị gián đoạn do các cuộc tấn công mạng.
- Quản lý và phân tích log tập trung từ nhiều chi nhánh và hệ thống.

Ngành tài chính ngân hàng và bảo hiểm

Nhu cầu:

- Bảo vệ hệ thống giao dịch trực tuyến (24/7)
- Tuân thủ các tieu chuẩn bảo mật (PCI DSS, ISO 27001) và yêu cầu pháp luật của Ngân hàng Nhà nước.
- Ngăn chặn kịp thời các cuộc tấn công mạng như phising, ransomware

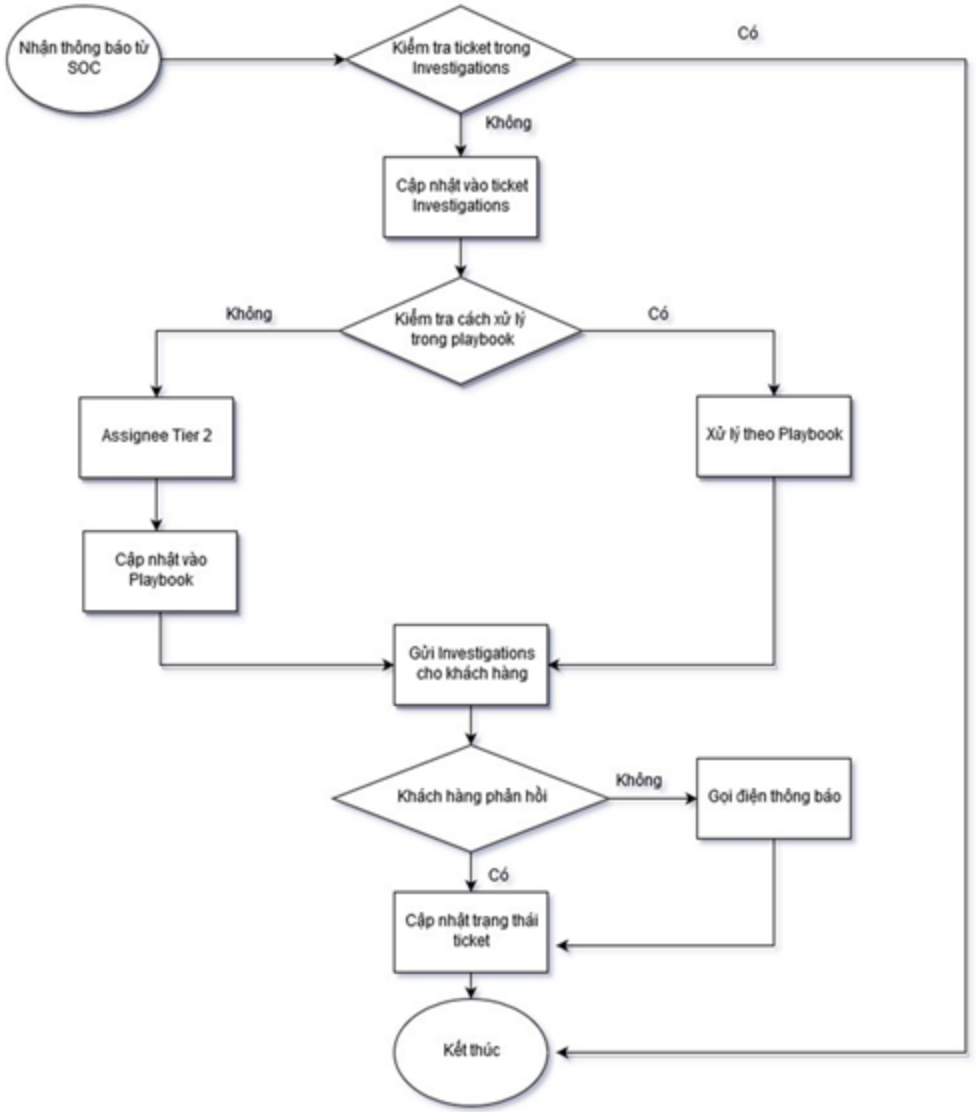
Doanh nghiệp vừa và nhỏ (SMEs)

Nhu cầu:

- Bảo mật giao dịch và các thông tin khách hàng
- Phát hiện kịp thời các lỗ hổng hoặc các cuộc tấn công
- Đảm bảo vận hành liên tục, không bị gián đoạn do tấn công mạng
- Tiết kiệm chi phí bằng cách thuê dịch vụ SOC.

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

1. DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN



QUY TRÌNH GIÁM SÁT ATTT

- **Bước 1:** Sau khi tiếp nhận ticket từ SOC, giám sát viên Tier 1 kiểm tra Investigations nhằm xác định ticket có trùng lặp hay không: Kiểm tra và xác định ticket xuất hiện trên hệ thống giám sát SOC đã có tồn tại hay chưa? Các IP đích và IP nguồn có thường xuyên xuất hiện không? Nếu đã trùng lặp thì kết thúc quy trình. Nếu không trùng lặp thì chuyển tới bước tiếp theo quy trình.
- **Bước 2:** Giám sát viên Tier 1 cập nhật ticket vào Investigations. Sau đó chuyển tới bước xử lý kế tiếp.
- **Bước 3:** Giám sát viên Tier 1 kiểm tra xem ticket đã có trong Playbook chưa. Nếu đã có thì xử lý theo hướng dẫn trong Playbook. Nếu chưa có, giám sát viên Tier 1 sẽ gán Assignee cho một nhân viên thuộc Tier 2 có trách nhiệm phân tích và đưa ra phương án xử lý đối với ticket. Sau khi khuyến nghị đã được xử lý đã được đưa ra, giám sát viên Tier 1 sẽ cập nhật vào báo cáo.
- **Bước 4:** Nhân viên giám sát Tier 1 có trách nhiệm gửi lại báo cáo cho khách hàng trong phần Investigations sau khi đã cập nhật khuyến nghị xử lý.
- **Bước 5:** Nhận phản hồi của Khách Hàng. Nếu cần thiết thì trao đổi với Khách hàng nhằm xác minh thêm các thông tin về ticket và mức độ ảnh hưởng tới hệ thống.
- **Bước 6**: Sau khi hoàn thành quá trình trao đổi xử lý giữa hai bên, nhân sự giám sát SOC sẽ cập nhật lại trạng thái của ticket và đóng quy trình thông báo sự cố.

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

1. DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN

Cam kết cung cấp dịch vụ (Service Level Agreement – SLA)

Sources of Alerts	Mức độ đe dọa (từ MBF SIEM)	Mức độ ưu tiên xử lý	Phương pháp thông báo	Thời gian tối đa từ khi nhận cảnh báo đến khi xử lý
SOC Alerts	HIGH	3	Thời gian thực thông qua tin nhắn và email	90 phút
	WARNING	2	Thời gian thực thông qua tin nhắn và email	24 tiếng
	INFORMATIONAL	1	N/A	
Alerts/ Notification từ khách hàng	Review Action	3	N/A	180 phút từ khi nhận được thông báo chính thức từ khách hàng

LỢI ÍCH

Giảm chi phi đầu tư cho an toàn thông tin, không cần đầu tư một khoản chi phí lớn cho nhân sự và hạ tầng bảo mật. Sử dụng dịch vụ bảo mật chuyên nghiệp được cung cấp bởi những chuyên gia hàng đầu.

Hạn chế các cảnh báo không chính xác (false positives) nhờ cơ chế xác định hành vi bất thường tích hợp AI và Machine Learning.

Nhanh chóng phát hiện các mối đe dọa, từ đó có những biện pháp ngăn chặn và giảm thiểu rủi ro.

Được đảm bảo về sự an toàn của hệ thống thông tin 24/7

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

2. DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

Tại sao cần dịch vụ này?

Luật An toàn thông tin mạng (2015)

- **Điều 29**: Yêu cầu các cơ quan, tổ chức, cá nhân sử dụng hệ thống thông tin phải:
  - Thực hiện kiểm tra , đánh giá ATTT định kỳ.
  - Bác cáo về tình hình ATTT cho cơ quan có thẩm quyền
- **Điều 41**: Hệ thống thông tin quan trọng quốc gia phải được kiểm tra, đánh giá và chứng nhận phù hợp với tiêu chuẩn ATTT

Nghị định 85/2016/NĐ-CP về đảm bảo ATTT cho hệ thống thông tin theo cấp độ

- Yêu cầu phân loại và đánh giá hệ thống thông tin theo 5 cấp độ:
  - Cấp 3 trở lên: Phải được tổ chức , đánh giá ATTT bởi đơn vị được Bộ thông tin và Truyền thông (Bộ TT&TT) hoặc cơ quan có chức năng công nhận.
- Định kỳ đánh giá và báo cáo:
  - Hệ thống cấp độ 3: Ít nhất **1 lần/ 1 năm**
  - Hệ thống cấp độ 4, 5: Đánh giá định kỳ sau mỗi thay đổi lớn

Luật An ninh mạng (2018)

- **Điều 26**: Các hệ thống thông tin quan trọng về an ninh quốc gia phải được giám sát, kiểm tra, đánh giá về ATTT định kỳ..
- **Điều 43**: Tổ chức, doanh nghiệp phải chịu trách nhiệm đánh giá, bảo vệ hệ thống trước các mối đe dọa an ninh mạng.

Nghị định 64/2022/NĐ-CP về bảo vệ dữ liệu cá nhân

- Các tổ chức xử lý dữ liệu cá nhân phải đảm bảo hệ thống của mình đáp ứng các tiêu chuẩn về bảo vệ dữ liệu và phải đánh giá định kỳ

Thông tư 03/2017/TT-BTTT

- Hướng dẫn chi tiết việc đánh giá an toàn hệ thống thông tin theo cấp độ
- Quy định rõ quy trình, Phương pháp đánh giá và yêu cầu về đội ngũ thực hiện.

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

2. DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

Đánh giá mức độ an toàn và bảo mật của hệ thống thông tin, các dữ liệu và quy trình liên quan, nhằm xác định các rủi ro an ninh thông tin và đánh giá khả năng của hệ thống để chống lại những mối đe dọa tiềm tàng. Đánh giá an toàn thông tin giúp tổ chức nhận biết và hiểu rõ về những điểm yếu trong hệ thống, từ đó đề xuất và triển khai các biện pháp bảo mật phù hợp để giảm thiểu rủi ro.

MỤC TIÊU

- Đánh giá mức độ an toàn, bảo mật của hệ thống CNTT bằng cách giả lập tất cả các kịch bản tấn công có thể xảy ra
- Đưa ra khuyến nghị sửa chữa, thay đổi nhằm tối ưu và đảm bảo an ninh an toàn thông tin cho hệ thống.

LỢI ÍCH

- Xác định các điểm yếu nhất trong hệ thống CNTT, từ đó quyết định tập trung vào hạng mục nào để giảm thiểu rủi ro trong tương lai
- Phòng tránh các thiệt hại về Tài chính, Vận hành và Danh tiếng do Tấn công mạng bằng việc ngăn chặn tấn công bằng cách chủ động xác định và sửa các lỗ hổng.
- Tuân thủ các tiêu chuẩn của Nhà nước, Quốc tế hoặc Nội bộ yêu cầu đánh giá bảo mật như PCI-DSS

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

2. DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

ƯU ĐIỂM NỔI BẬT

- Rà soát các mối đe dọa, điểm yếu, lỗ hổng có thể bị khai thác từ bên trong hệ thống.
- Cập nhật dữ liệu lỗ hổng bảo mật liên tục qua hệ thống MobiFone Threat Intelligence
- Tích hợp Metasploit - Tấn công kiểm thử với các lỗ hổng mức độ nguy hiểm nghiêm trọng.
- Tích hợp AI, Machine Learning phát hiện sớm các lỗ hổng, cảnh báo nhanh chóng, chính xác
- Dễ dàng tích hợp với các hệ thống Công nghệ thông tin

LỢI ÍCH KHÁCH HÀNG

- Có những thông tin mới nhất về tình hình an ninh của hệ thống thông qua các báo cáo của MobiFone Security.
- Nhận những tư vấn, khuyến nghị từ các chuyên gia hàng đầu trong lĩnh vực bảo mật để tối ưu hóa hệ thống, hạn chế tối khả năng bị tấn công.
- Được bảo vệ an toàn tối đa trước những mối đe dọa an ninh thông tin, kể cả các mối đe dọa phức tạp chưa từng được phát hiện.
- Hiểu được phương thức, động cơ của những kẻ tấn công, từ đó có chiến lược phòng thủ trước các mối đe dọa một cách toàn diện.

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

2. DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

NHÓM KHÁCH HÀNG MỤC TIÊU

Cơ quan nhà nước và chính phủ

Nhu cầu:

- Tuân thủ quy định pháp luật (luật an ninh mạng, luật an toàn thông tin mạng)
- Đảm bảo an ninh cho các hệ thống theo cấp độ
- Bảo vệ dữ liệu quốc gia và các hệ thống quan trọng

Doanh nghiệp lớn và các tập đoàn

Nhu cầu:

- Đánh giá rủi ro bảo mật và bảo vệ tài sản số.
- Đáp ứng các tiêu chuẩn ISO27001, NIST
- Xây dựng lòng tin với khách hàng

Ngành tài chính ngân hàng và bảo hiểm

Nhu cầu:

- Tuân thủ quy định của Ngân hàng nhà nước Việt Nam và bảo mật hệ thống
- Ngăn chặn các cuộc tấn công mạng phising, ransomware.
- Bảo vệ thông tin khách hàng và các giao dịch trực tuyến.

Doanh nghiệp vừa và nhỏ (SMEs)

Nhu cầu:

- Đánh giá an ninh mạng để bảo vệ dữ liệu khách hàng và hệ thống kinh doanh.
- Tuân thủ quy định về bảo vệ dữ liệu cá nhân.
- Tiết kiệm chi phí bằng cách thuê dịch vụ đánh giá ATTT.

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

2. DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

Input

- URL
- Accounts to login

Testing Methodology

- Grey box

Quá trình thực hiện

- Task 1: Rà soát, xâm nhập tìm kiếm lỗ hổng bảo mật
- Task 2: Báo cáo và khuyến nghị khắc phục
- Task 3: Tái đánh giá sau khắc phục
- Task 4: Báo cáo tổng quan

Output

Báo cáo về bảo mật:

- Báo cáo tổng quan
- Thông tin chi tiết cho từng lỗ hổng tìm được (phân loại CVSS, nguy cơ, tác động, quá trình khai thác lỗ hổng, đề xuất khắc phục)

Thực hiện bởi những chuyên gia với chứng chỉ bảo mật hàng đầu (OSWE, OSCE, OSCP, CEH…)

Tools dò quét bản quyền: Nessus, BURPSUITE, HCL AppScan

Input, output

Security standards: OWASP Mobile Security Project, OWASP Open Web Application Security Project

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

3. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ

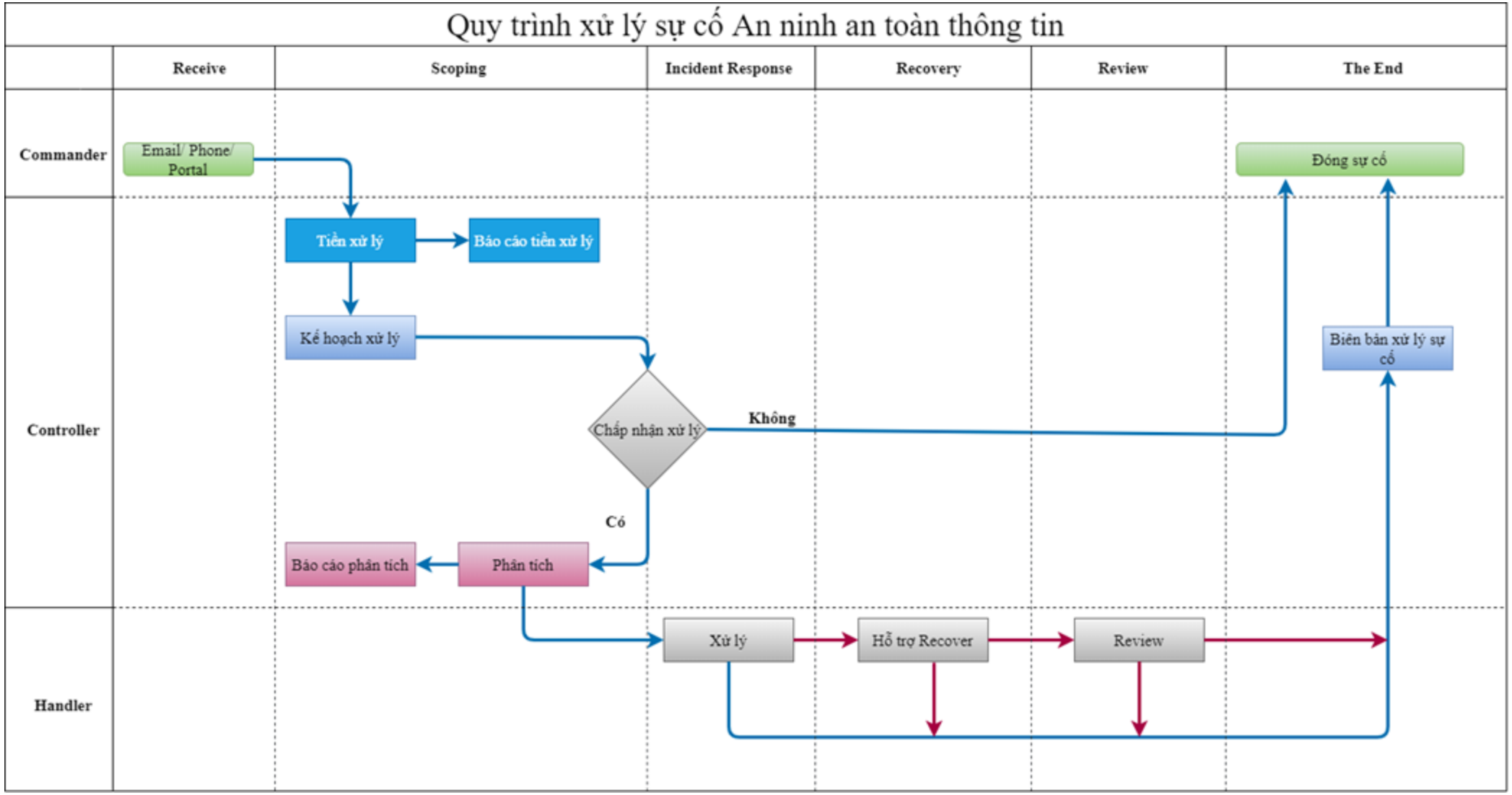
Dịch vụ "Ứng cứu xử lý sự cố" là hoạt động nhằm xử lý, khắc phục sự cố gây mất an ninh an toàn thông tin gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, và khôi phục hoạt động bình thường của hệ thống thông tin. Các hoạt động này sẽ do các chuyên gia ATTT của MobiFone Security đảm nhiệm và thực hiện.

ƯU ĐIỂM NỔI BẬT

- Sẵn sàng ứng cứu sự cố 24x7x365 với đội ngũ chuyên gia tại trung tâm giám sát an ninh mạng MobiFone SOC.
- Tích hợp hệ thống trí tuệ nhân tạo AI và Machine Learning giúp nâng cao khả năng tự động giám sát.
- Báo cáo phân tích chuyên sâu các sự cố được thực hiện bởi đội ngũ điều tra sự cố của MobiFone Security.
- Khuyến nghị nâng cấp, vá các lỗ hổng hệ thống sau khi khắc phục sự cố.

II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

3. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ



II. CÁC DỊCH VỤ AN TOÀN THÔNG TIN

3. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ

Commander	Controller	Handler
Bộ phận/nhóm tiếp nhận các thông tin sự cố từ phía khách hàng. Nhóm có trách nhiệm tiếp nhận thông tin, tiền xử lý các thông tin sự cố. Trong trường hợp các thông tin không đầy đủ để giải quyết sự cố hoặc cần hỗ trợ thêm để xử lý, nhóm này có trách nhiệm chuyển toàn bộ các thông tin tiếp nhận cho bộ phận xử lý cấp trên (Controller)	Bộ phận/nhóm phân tích, định hướng và điều phối xử lý. Nhóm này có trách nhiệm phân tích chi tiết các thông tin sự cố tiếp nhận, xác định phương hướng xử lý và chịu trách nhiệm điều phối cho toàn bộ quá trình xử lý sự cố. Để việc xử lý hiệu quả, nhóm này có thể yêu cầu khách hàng bổ sung hoặc phối hợp bổ sung thông tin chi tiết về sự cố trong quá trình tiếp nhận và phân tích.	Bộ phận/nhóm trực tiếp phân tích và xử lý các sự cố. Thành viên nhóm này có thể bao gồm cả nhân viên kỹ thuật của MobiFone và đội ngũ kỹ thuật của khách hàng. Nhóm này sẽ xử lý sự cố theo hướng dẫn và điều phối xử lý của Controller. Trong quá trình xử lý, mọi vấn đề phát sinh nhóm có trách nhiệm ghi nhận và báo cáo cho Controller trước khi có hành động phản ứng tiếp theo.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

3. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ

GÓI DỊCH VỤ	THỜI GIAN XỬ LÝ/NĂM	THỜI GIAN CÓ MẶT TẠI KHÁCH HÀNG	ĐƠN VỊ TÍNH
1	200 giờ	12 tiếng (áp dụng trong nội thành Hà Nội)	Năm
2	350 giờ	6 tiếng (áp dụng trong nội thành Hà Nội)	Năm
3	500 giờ	3 tiếng (áp dụng trong nội thành Hà Nội)	Năm
4	Tối thiểu 100 giờ	Thỏa thuận với khách hàng	Năm

LỢI ÍCH KHÁCH HÀNG

Nhanh chóng ngăn chặn/ khắc phục sự cố an ninh an toàn thông tin, giảm thiểu hậu quả khi hệ thống bị tấn công.

Giảm thiểu thiệt hại về kinh tế đối với tổ chức khi bị tấn công khai thác, làm gián đoạn hoạt động.

Được đảm bảo về sự an toàn của hệ thống thông tin 24/7

Dịch vụ ứng cứu sự cố nhanh chóng, chuyên nghiệp theo cam kết cung cấp dịch vụ (SLA) của MobiFone Security.

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

4. DỊCH VỤ SĂN TÌM MỐI ĐE DỌA – THREAT HUNTING

Threat Hunting là một hoạt động phòng thủ mạng tích cực. Đây là một quá trình chủ động tìm kiếm các mối đe dọa, sử dụng internal và external threat intelligence, khai thác và phân tích thông tin (log, mã độc).

ƯU ĐIỂM NỔI BẬT

Threat Intelligence: cập nhật 24/7 các mối đe dọa mới từ nhiều tổ chức phòng chống mã độc uy tín, phân loại mối đe dọa theo ngành nghề của khách hàng.

Vulnerability Assessment: rà soát các mối đe dọa, điểm yếu, lỗ hổng có thể bị khai thác từ bên trong hệ thống.

Sử dụng các công nghệ tiên tiến cùng các chuyên gia hàng đầu trong ngành với nhiều năm kinh nghiệm về an toàn thông tin.

Nghiên cứu và theo sát hoạt động của các nhóm tin tặc trên thế giới.

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

4. DỊCH VỤ SĂN TÌM MỐI ĐE DỌA – THREAT HUNTING

PHẠM VI THỰC HIỆN

- Phân tích hành vi người dùng
- Phân tích hoạt động mạng
- Phát hiện mã độc
- Threat Intelligence Feeds
- Phân tích mã độc chuyên sâu

THREAT

II. CÁC DỊCH VỤ ĐÁNH GIÁ AN TOÀN THÔNG TIN

4. DỊCH VỤ SĂN TÌM MỐI ĐE DỌA – THREAT HUNTING

Mô hình săn tìm mối đe dọa

Săn tìm dựa trên thông tin tình báo

Săn tìm mối đe dọa dựa trên thông tin tình báo là một mô hình săn tìm bị động, sử dụng Chỉ số thỏa hiệp (IoC) từ các nguồn thông tin tình báo về mối đe dọa. Săn tìm dựa trên thông tin tình báo có thể triển khai IoC, giá trị băm, địa chỉ IP, tên miền, hệ thống mạng hoặc cấu phần lưu trữ được các nền tảng chia sẻ thông tin tình báo cung cấp. Từ các nền tảng này, cảnh báo mối đe dọa tự động được xuất ra và trở thành nguồn thông tin đầu vào của SIEM. Sau khi SIEM nhận được cảnh báo dựa trên IoC, nhân viên phụ trách săn tìm mối đe dọa có thể xem xét hoạt động độc hại trước và sau khi nhận cảnh báo để nhận diện mọi hành vi xâm phạm trên toàn hệ thống.

Săn tìm mối đe dọa giả định

Săn tìm mối đe dọa giả định là phương pháp săn tìm chủ động bằng cách sử dụng thư viện săn tìm mối đe dọa. Phương pháp này phù hợp với khuôn khổ MITRE ATT&CK, đồng thời triển khai việc săn tìm dựa trên giả định để triển khai Chỉ số tấn công (IoAs) và Chiến thuật, Kỹ thuật và Thủ tục (TTP) của những kẻ tấn công. Nhân viên phụ trách săn tìm mối đe dọa nhận diện tác nhân gây ra mối đe dọa trên cơ sở môi trường, miền và hành vi tấn công để phát triển một giả thuyết phù hợp với khuôn khổ MITRE. Sau khi nhận dạng được khuôn mẫu hành vi, nhân viên phụ trách săn tìm mối đe dọa sẽ kiểm tra các khuôn mẫu hoạt động để phát hiện, nhận dạng và cô lập mối đe dọa.

Săn tìm mối đe dọa tùy chỉnh

Săn tìm mối đe dọa tùy chỉnh phụ thuộc vào việc nhận thức tình huống và các phương pháp săn tìm mối đe dọa theo đặc thù từng ngành. Phương pháp này giúp phát hiện yếu tố bất thường trong các công cụ SIEM và EDR và được hiệu chỉnh theo nhu cầu của khách hàng. Quá trình săn tìm mối đe dọa tùy chỉnh hoặc theo tình huống được thực hiện trong những điều kiện nhất định, chẳng hạn như mối quan tâm về địa chính trị và các cuộc tấn công có chủ đích hoặc dựa trên yêu cầu của khách hàng. Cả mô hình săn tìm dựa trên thông tin tình báo và giả định, trong đó có sử dụng thông tin IoA và IoC, đều có thể được sử dụng trong hoạt động săn tìm này.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

4. DỊCH VỤ SĂN TÌM MỐI ĐE DỌA – THREAT HUNTING

LỢI ÍCH KHÁCH HÀNG

Có những thông tin mới nhất về tình hình an ninh của hệ thống thông qua các báo cáo của MobiFone Security.

Nhận những tư vấn, khuyến nghị từ các chuyên gia hàng đầu trong lĩnh vực bảo mật để tối ưu hóa hệ thống, hạn chế tối khả năng bị tấn công.

Được bảo vệ an toàn tối đa trước những mối đe dọa an ninh thông tin, kể cả các mối đe dọa phức tạp chưa từng được phát hiện.

Hiểu được phương thức, động cơ của những kẻ tấn công, từ đó có chiến lược phòng thủ trước các mối đe dọa một cách toàn diện.

THÔNG TIN THỊ TRƯỜNG

KHÁCH HÀNG	DỰ ÁN	GIÁ TRỊ HỢP ĐỒNG
SỞ/BAN NGHÀNH	Diễn tập thực chiến	440.000.000
SỞ/BAN NGHÀNH	Cung cấp, lắp đặt thiết bị phần cứng, phần mềm cho hệ thống SOC	46.523.226.000
CÔNG AN TỈNH	Triển khai chương trình đào tạo nguồn nhân lực An ninh mạng năm 2024 tại tỉnh KHA	420.000.000
SỞ/BAN NGHÀNH	Dịch vụ kiểm tra, đánh giá định kỳ hệ thống thông tin cấp độ 3	900.000.000
CÔNG TY CẤP NƯỚC	Dịch vụ Đánh giá An toàn thông tin	395.000.000
VÍ THANH TOÁN	Dịch vụ Đánh giá An toàn thông tin	350.000.000
HỢP TÁC XÃ TỈNH CAO BẰNG	Thuê dịch vụ kiểm tra đánh giá ATTT (THẦU)	288.000.000
CÔNG AN TỈNH (PA05)	Dịch vụ Diễn tập thực chiến Dịch vụ đánh giá ATTT Phòng chống mã độc Dịch vụ giám sát SOC	13-16 tỷ
EVN TỈNH	Đánh giá điểm yếu, kiểm thử xâm nhập và làm sạch cho máy chủ (Máy tính, thiết bị, Máy chủ).	389.000.000

HỢP ĐỒNG

DỰ ÁN ĐÃ TRIỂN KHAI	GIÁ TRỊ HỢP ĐỒNG
- CAO BẰNG - MOBISERVIS - SAO BẮC ĐẨU - CTY CẤP NƯỚC CẦN THƠ 2	- 288.000.000 - 54.000.000 - 40.000.000 - 370.000.000
- VNSKy - CÔNG TY NƯỚC - SVTECH - VIỆT BẢN ĐỒ - TELSOFT - PA05 TỈNH	- 335.000.000 - 395.000.000 - 80.000.000 - 1.800.000.000 - 90.000.000 - 13.000.000.000

III. Sản phẩm Antivirus cho máy chủ Cloud

AVG Anti-Virus
avast
AV-Comparatives Product of the Year 2023
McAfee
AVIRA
Bitdefender

Mục tiêu của sản phẩm:

- Tăng cường an toàn cho các khách hàng sử dụng máy chủ Cloud
- Cung cấp tính năng bảo về cơ bản cho điểm cuối Endpoint:

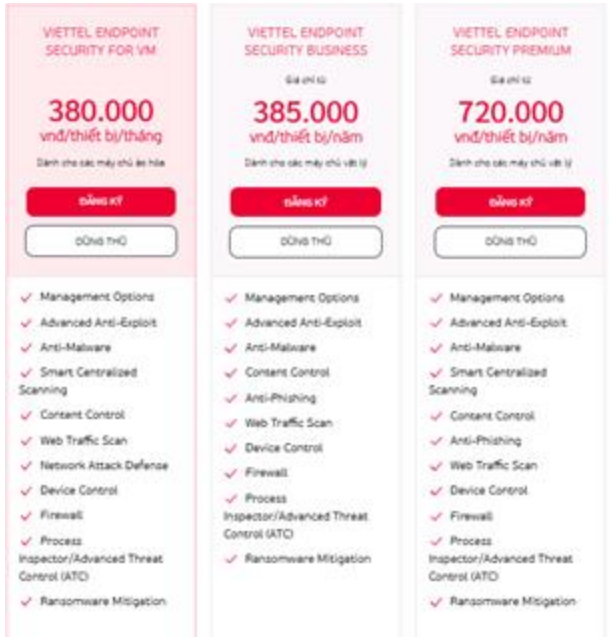
• Quét theo yêu cầu (On-Demand Scan)
• Quét theo thời gian thực (Real-Time Scan)
• Cập nhật Cơ sở Dữ liệu Virus
• Có bảng điều khiển quản lý tập trung
• Bảo vệ chống phần mềm độc hại (Malware Protection)
• Báo cáo và cảnh báo

- Bảo vệ chống phần mềm độc hại bằng sử dụng các thiết bị ảo hóa bảo mật
- Phát hiện các cuộc tấn công tiên tiến và các hoạt động đáng ngờ ở giai đoạn trước khi thực thi

III. Sản phẩm Antivirus cho máy chủ Cloud

THỊ TRƯỜNG

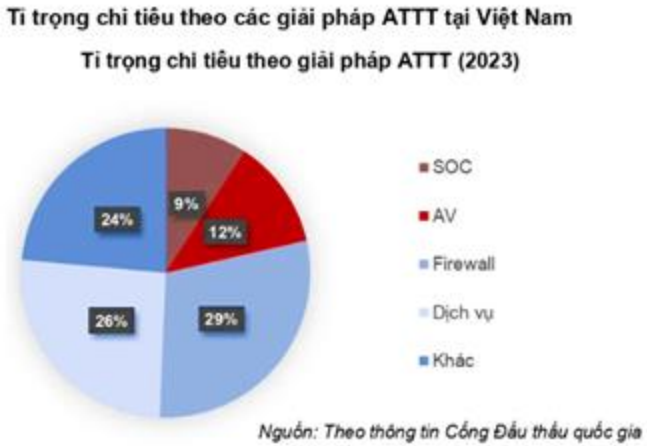
viettel



Gói sản phẩm	Mức giá áp dụng từ 1 - 14 thiết bị	Mức giá áp dụng từ 15 - 24 thiết bị	Mức giá áp dụng từ 25 - 49 thiết bị	Mức giá áp dụng từ 50 - 99 thiết bị	Mức giá áp dụng từ 100 - 2000 thiết bị
Viettel Endpoint Security Business	480.000 vnđ/thiết bị/năm	460.000 vnđ/thiết bị/năm	440.000 vnđ/thiết bị/năm	395.000 vnđ/thiết bị/năm	385.000 vnđ/thiết bị/năm
Viettel Endpoint Security Premium	1.000.000 vnđ/thiết bị/năm	930.000 vnđ/thiết bị/năm	870.000 vnđ/thiết bị/năm	770.000 vnđ/thiết bị/năm	720.000 vnđ/thiết bị/năm

Quy mô thị trường Quốc tế

Chi tiêu cho sản phẩm bảo mật Cloud trên thế giới cho năm 2022 là 5275,7 triệu đô và năm 2023 là 5616,7 với mức tăng trưởng 25,2%



Nguồn: Theo thông tin Cổng Đấu thầu quốc gia

Quy mô thị trường Việt Nam

Chi tiêu cho sản phẩm bảo mật Cloud tại Việt Nam chiếm 12% trong tỉ trọng chi tiêu theo giải pháp ATTT năm 2023 tương đương với hơn 720 tỷ đồng.

III. Sản phẩm Antivirus cho máy chủ Cloud

Các gói cước

STT	Tên gói cước	Giá	Chu kỳ	Khuyến mãi	Số lượng thiết bị	Ghi chú
1	MobiFone Endpoint Security Business	325,000	1 tháng	Tặng 1 tháng Free	1 server	Quét tập trung tại hạ tầng Cloud đối tác đầu tư tại Cloud MobiFone
2	MobiFone Endpoint Security Premium	424,000	1 tháng	Tặng 1 tháng Free	1 server	Quét tập trung tại hạ tầng Cloud đối tác đầu tư tại Cloud MobiFone
3	MobiFone GravityZone Endpoint Security Business (MB1)	1,869,563	1 năm	Tặng 1 tháng Free	2 server + 2 PC	- Có các gói khác nhau theo số lượng máy chủ - Quét tập trung qua Cloud của đối tác cung cấp AV
4	MobiFone GravityZone Endpoint Security Premium (MP1)	4,902,422	1 năm	Tặng 1 tháng Free	2 server + 3 PC	- Có các gói khác nhau theo số lượng máy chủ - Quét tập trung qua Cloud của đối tác cung cấp AV

Phí hoa hồng
15%

III. Sản phẩm Antivirus cho máy chủ Cloud

Các gói cước Năm

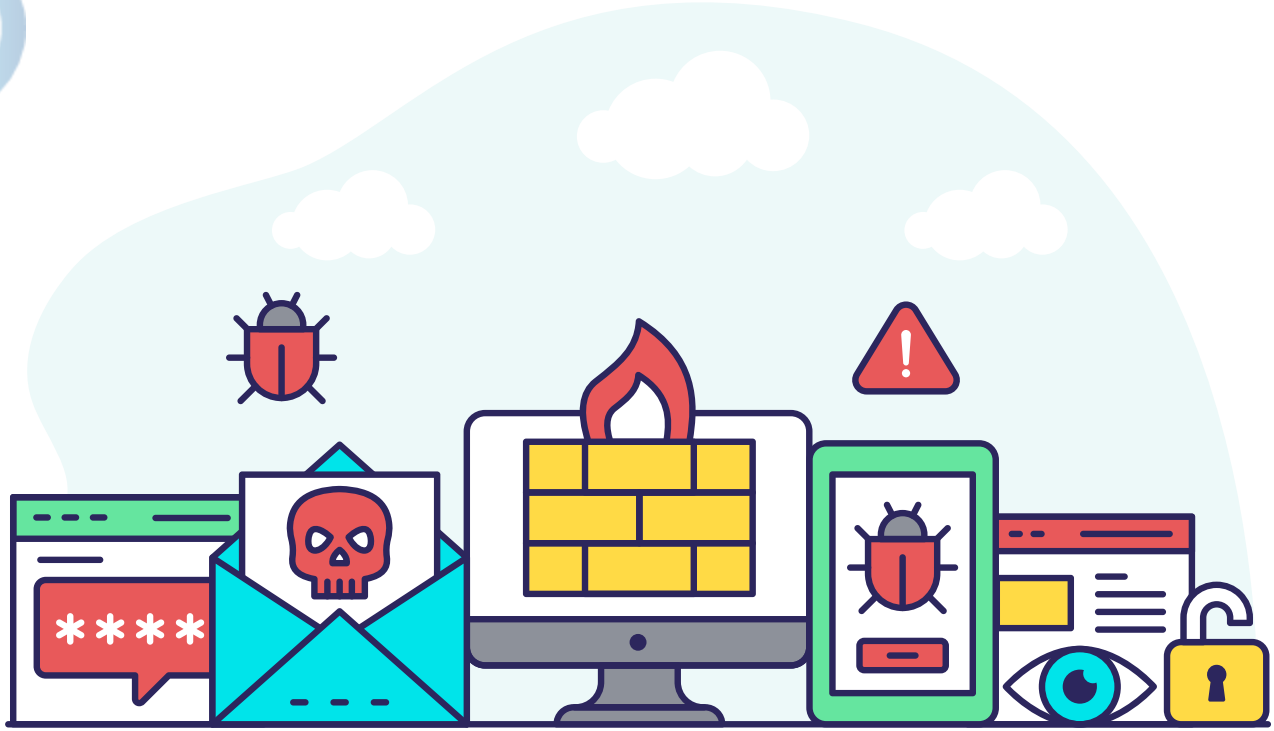
Gói cước cơ bản

STT	Tên sản phẩm	Giá gói cước	Chu kỳ	Số lượng thiết bị	Các loại phí*	Ghi chú
					Phí hoa hồng (15%)***	
1	MobiFone Endpoint Security Business (MB1)	1,869,563	Năm 1	2 Server + 2 PC (4 device)	373,912.60	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
2	MobiFone Endpoint Security Business (MB2)	3,271,058	Năm 1	3 Server + 4 PC (7 device)	654,211.60	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
3	MobiFone Endpoint Security Business (MB3)	5,140,207	Năm 1	4 Server + 7 PC (11 device)	1,028,041.40	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
4	MobiFone Endpoint Security Business (MB4)	6,542,052	Năm 1	5 Server + 9 PC (14 device)	1,308,410.40	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
5	MobiFone Endpoint Security Business (MB5)	7,645,691	Năm 1	6 Server + 9 PC (15 device)	1,529,138	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)

Gói cước nâng cao

STT	Tên sản phẩm	Giá gói cước	Chu kỳ	Số lượng thiết bị	Các loại phí*	Ghi chú
					Phí hoa hồng (15%)***	
1	MobiFone Endpoint Security Premium (MP1)	4,902,422	Năm 1	2 Server + 3 PC (8 device)	735,363.28	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
2	MobiFone Endpoint Security Premium (MP2)	5,881,496	Năm 1	3 Server + 3 PC (6 device)	882,224	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
3	MobiFone Endpoint Security Premium (MP3)	8,822,245	Năm 1	4 Server + 5 PC (9 device)	1,323,337	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
4	MobiFone Endpoint Security Premium (MP4)	11,762,993	Năm 1	5 Server + 7 PC (12 device)	1,764,449	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)
5	MobiFone Endpoint Security Premium (MP5)	13,784,666	Năm 1	6 Server + 9 PC (15 device)	2,067,700	Khuyến mãi tháng đầu tiên dùng thử (13 tháng)

IV.SẢN PHẨM MOBISAFEOFFICE



4.1 YÊU CẦU CẤP ĐỘ AN TOÀN THÔNG TIN

Theo quy định của Luật An toàn thông tin mạng, việc đảm bảo ATTT cho các các đơn vị Phường, Xã, Trường học phải đảm bảo từ cấp độ 2 trở lên.

Đảm bảo ATTT cấp độ 2 tối thiểu cần triển khai:

- Hệ thống tường lửa
- Phần mềm phòng chống mã độc

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác.

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

iii. Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương;

iv. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP ;

v. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử;

vi. Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm.

Cấp độ 2

4.2 GIẢI PHÁP TƯỜNG LỬA THÔNG MINH
MobiSafeOffice

Đáp ứng yêu cầu cấp độ
Tính năng đáp ứng yêu cầu cấp độ ATTT theo quy định.

Dễ sử dụng
Cài đặt tự động, quản trị đơn giản qua Cloud, App.

Tuân thủ
Tuân thủ các quy định về ATTT tại Việt Nam

4.3.GIẢI PHÁP TƯỜNG LỬA THÔNG MINH
MobiSafeOffice

TÍNH NĂNG SẢN PHẨM

Tính năng An toàn, an ninh

- Chặn lọc địa chỉ lừa đảo, độc hại: Tích hợp nguồn dữ liệu về mối nguy, tự động chặn các kết nối nguy hiểm
- Phân vùng mạng, tạo ra các vùng mạng theo chức năng: Insite, outsite, DMZ...
- Truy cập, kết nối từ xa an toàn thông qua VPN: Remote Access VPN và site-to-site VPN
- Giám sát, phát hiện và phòng chống xâm nhập, cảnh báo cho quản trị.
- Ứng dụng công nghệ AI phát hiện các mối nguy tự động đảm bảo phát hiện và phòng chống kịp thời
- Tích hợp phòng chống mã độc và quản lý chính sách an toàn thông tin cho các máy trạm trong mạng (*)
- Tường lửa ứng dụng Web (Web Application Firewall) bảo vệ ứng dụng web trước các nguy cơ tấn công, lỗ hổng (*)
- Bảo vệ hệ thống thư điện tử, chặn lọc các email có chứa mã độc, lừa đảo (*)

Tính năng Quản lý

- Kiểm soát việc sử dụng các ứng dụng Video của người dùng: ai được sử dụng, thời gian sử dụng.
- Kiểm soát việc sử dụng các ứng dụng Game của người dùng: ai được sử dụng, thời gian sử dụng.
- Kiểm soát việc sử dụng các ứng dụng Mạng xã hội của người dùng: ai được sử dụng, thời gian sử dụng.
- Kiểm soát việc sử dụng các ứng dụng nhắn tin của người dùng: ai được sử dụng, thời gian sử dụng.
- Cân bằng tải, hỗ trợ kết nối nhiều đường truyền Internet, tăng tốc độ mạng và dự phòng khi có sự cố đường truyền
- Hệ thống báo cáo tình hình sử dụng: top máy sử dụng nhiều nhất, top ứng dụng sử dụng nhiều nhất...
- Kiểm soát truy cập NAC (Network Access Control) quản lý các máy trạm theo địa chỉ MAC, IP.
- Quản lý tập trung dễ dàng thông qua Cloud, giảm thiểu thời gian cài đặt ZTP (Zero Touch Provisioning)

Tuân thủ

- Tuân thủ theo công văn 2973 BTTTT-CATTT về giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước
- Chia sẻ thông tin theo thông tư: 31/2017/TT-BTTTT
- Chia sẻ thông tin mã độc theo Chỉ thị 14/CT - TTg năm 2018

4.4. CÁC PHIÊN BẢN KHÁC
MobiSafeOffice

	School	Standard	Pro
Đáp ứng yêu cầu cấp độ 1 và 2	Đáp ứng	Đáp ứng	Đáp ứng
Phù hợp	**Trường học: Tiểu học, THCS, THPT**	Xã, phường Trường học Văn phòng quy mô nhỏ	Quận/Huyện Trường học lớn Bệnh viện Văn phòng quy trung bình, lớn
Hiệu năng, cáu hình chính			
Hiệu năng và số cổng kết nối	Số lượng máy kết nối đồng thời: 40	Số lượng máy kết nối đồng thời: 50 - 100 3 x GbE RJ-45 (Intel® I210) Firewall Throughput: 500 Mbps IPS: 450 Mbps VPN: 50 phiên đồng thời Desktop, small form factor and fanless	Số lượng máy kết nối đồng thời: 300 - 500 6 x GbE RJ-45 Firewall Throughput: 900 Mbps IPS: 800 Mbps VPN: 100 phiên đồng thời 1U rackmount 1 x LAN module
Tính năng An toàn, an ninh			
Chặn lọc địa chỉ lừa đảo, độc hại: Tích hợp nguồn dữ liệu về mối nguy, tự động chặn các kết nối nguy hiểm	x	x	x
Phân vùng mạng Insite, Outsite	x	x	x
Phần vùng mạng Insite, Outsite, DMZ…			x
Truy cập, kết nối từ xa an toàn thông qua VPN: Remote Access VPN và site-to-site VPN	x	x	x
Giám sát, phát hiện và phòng chống xâm nhập, cảnh báo cho quản trị.	x	x	x

4.5 BẢNG SO SÁNH VỚI MobiSafeOffice

Main features	Firewall	IDS /IPS	VPN	Load Balancing	App Control	AV-Integrated	Compliance (1)	Cloud Managed (2)	Smart Report	IoC update form NCSC (3)	PPPoE Support	IPv6 Support	Price (4)
Mobifone Smartsheild (Standard Series)  Juniper srx300	x	x	x	x	x	x	x	x	x	x	x	x	Dưới 30 triệu
 Fortinet (x0F Series)	x	x	x	x	x	x					x	x	34,000,000
 Sophos (XG 115 Series)	x	x	x	x	x	x			x		x	x	48,000,000
 Cisco (Meraki Series)	x	x	x	x	x	x			x		x	x	37,200,000
	x	x	x	x	x	x			x		x	x	42,000,000

Note:

(1): Tuân thủ các quy định của Việt Nam: Tuân thủ TT 31/2017/BTTTT-TT, CV 2973/BTTTT-CATTT về giám sát.

(2): Quản lý qua Cloud, yêu cầu Cloud phải ở Việt Nam

(3): Cập nhật thông tin độc hại, mã độc thời gian thực từ NCSC

(4): Giá bao gồm phần cứng và phần mềm FW bản quyền 1 năm

4.6.ĐỐI TƯỢNG KHÁCH HÀNG

Cơ quan trực thuộc Xã, Phường, Thị Trấn

Nhu cầu:

Tại Việt Nam:

Có 63 tỉnh/thành phố và có 10.598 đơn vị hành chính cấp xã (gồm xã, phường, thị trấn) trong đó có 614 thị trấn, 1.737 phường

Chưa trang bị các thiết bị FireWall

Cơ quan trường học, bệnh viện,

Nhu cầu:

- **Quy mô trường học:**
  + Trường THCS và PTCS: 10.882 trường
  + Trường THPT: 2.758 trường
  + Trường PT dân tộc nội trú: 242 Trường
  + Trường PT dân tộc bán trú: 687 trường
  + Trường ĐH: 43 trường
- **Quy mô bệnh viện:** Cả nước có 47 bệnh viện tuyến trung ương, 419 bệnh viện tuyến tỉnh và 684 bệnh viện tuyến huyện.

Doanh nghiệp vừa và nhỏ (SMEs)

Nhu cầu:

- **Việt Nam có 70.000 Doanh nghiệp vừa** và nhỏ làm về lĩnh vực Công nghệ số (Phần mềm, dịch vụ CNTT, sản xuất phần cứng): Sẽ có các hệ thống để quản lý/lưu trữ dữ liệu phục vụ cho doanh nghiệp.

TRÂN TRỌNG CẢM ƠN!