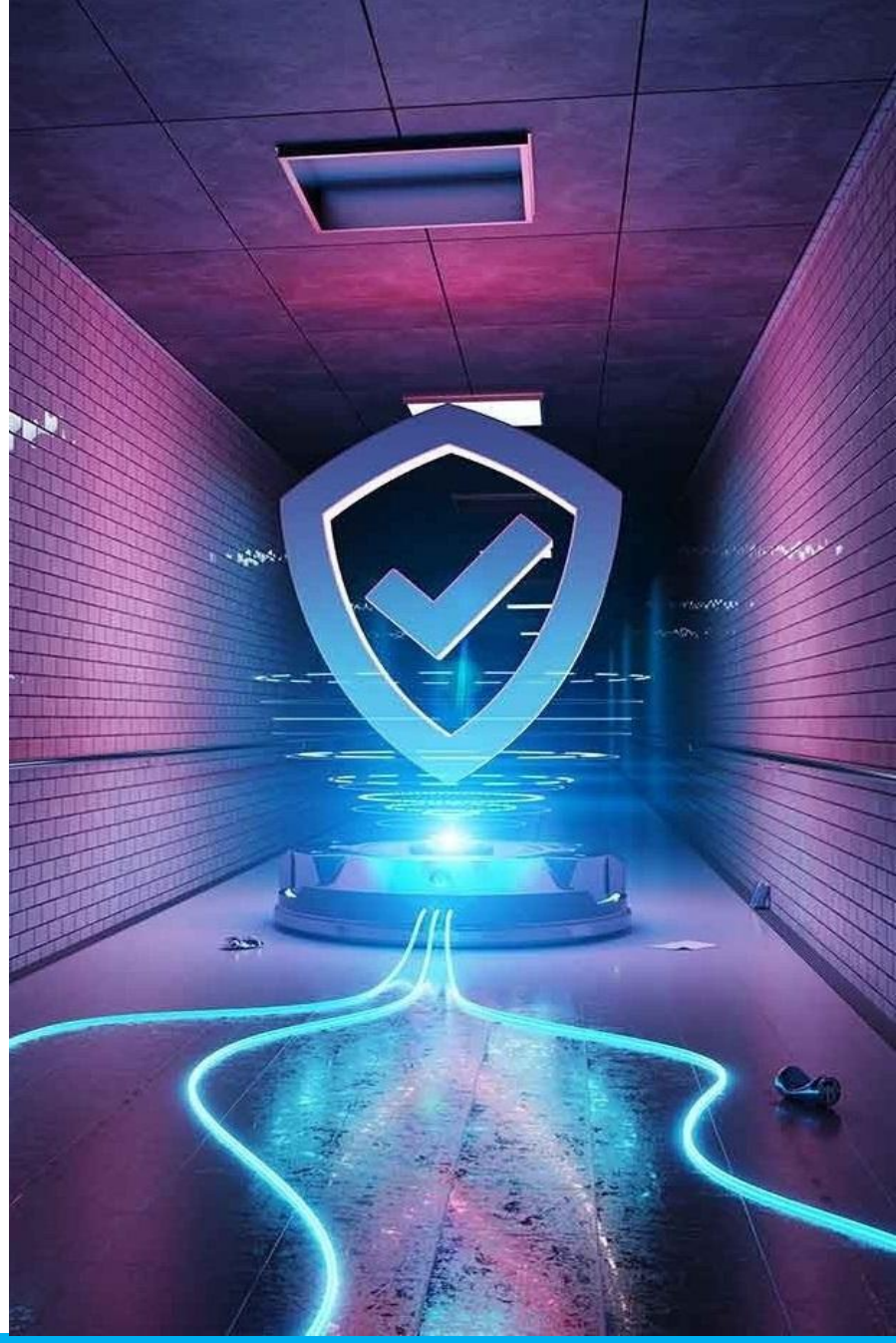
NỘI DUNG

1
- **GIỚI THIỆU MOBIFONE SECURITY**
- Giới thiệu về MobiFone Security và năng lực phát triển công nghệ

2
- **TỔNG QUAN VỀ 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 Kiểm thử an toàn thông tin (V.A, Pentest, Security Audit)

4
- **HỎI ĐÁP**



GIỚI THIỆU VỀ MOBIFONE SECURITY

1. GIỚI THIỆU MOBIFONE SECURITY

- **THÀNH LẬP NĂM 2024 VỚI NHIỆM VỤ PHÁT TRIỂN KINH DOANH DỊCH VỤ AN TOÀN THÔNG TIN MẠNG**
- **THUỘC TOP 3 NHÀ MẠNG VIỄN THÔNG KINH DOANH/SẢN PHẨM DỊCH VỤ ATTT**

Mục Tiêu

Trong 2 năm tới sẽ đưa MobiFone trở thành một trong những đơn vị cung cấp dịch vụ ATTT được tin cậy với và chiếm lĩnh ít nhất 50% thị phần nội địa.

Đến năm 2025, MobiFone trở thành thương hiệu uy tín nhất Việt Nam trong lĩnh vực cung cấp các giải pháp về an ninh an toàn thông tin

Tầm nhìn

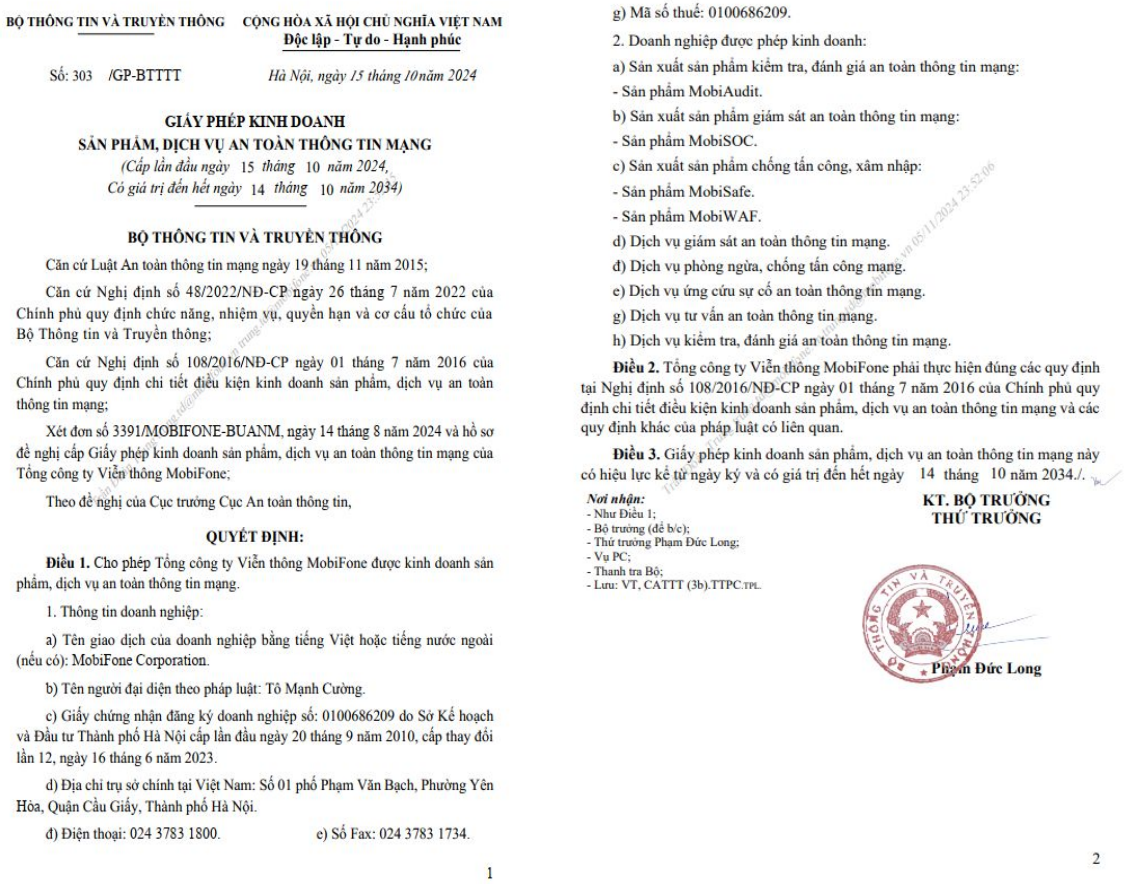
Không gian mạng phải là nơi an toàn và công bằng cho tất cả mọi người.

Sứ Mệnh

Đưa các sản phẩm dịch vụ do chính mình tạo ra tới tay người sử dụng với giá cả hợp lý nhất và bảo vệ an toàn cho người sử dụng trước các hiểm họa đến từ không gian mạng

- SẢN PHẨM DỊCH VỤ :

1. GIỚI THIỆU MOBIFONE SECURITY



BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 303 /GP-BTTTT

Hà Nội, ngày 15 tháng 10 năm 2024

GIẤY PHÉP KINH DOANH
SẢN PHẨM, DỊCH VỤ AN TOÀN THÔNG TIN MẠNG
(Cấp lần đầu ngày 15 tháng 10 năm 2024,
Có giá trị đến hết ngày 14 tháng 10 năm 2034)

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 3391/MOBIFONE-BUANM, ngày 14 tháng 8 năm 2024 và hồ sơ đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng của Tổng công ty Viễn thông MobiFone;

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

QUYẾT ĐỊNH:

Điều 1. Cho phép Tổng công ty Viễn thông MobiFone 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): MobiFone Corporation.

b) Tên người đại diện theo pháp luật: Tô Mạnh Cường.

c) Giấy chứng nhận đăng ký doanh nghiệp số: 0100686209 do Sở Kế hoạch và Đầu tư Thành phố Hà Nội cấp lần đầu ngày 20 tháng 9 năm 2010, cấp thay đổi lần 12, ngày 16 tháng 6 năm 2023.

d) Địa chỉ trụ sở chính tại Việt Nam: Số 01 phố Phạm Văn Bạch, Phường Yên Hòa, Quận Cầu Giấy, Thành phố Hà Nội.

đ) Điện thoại: 024 3783 1800. e) Số Fax: 024 3783 1734.

1

g) Mã số thuế: 0100686209.

2. Doanh nghiệp được phép kinh doanh:

a) Sản xuất sản phẩm kiểm tra, đánh giá an toàn thông tin mạng:

- Sản phẩm MobiAudit.

b) Sản xuất sản phẩm giám sát an toàn thông tin mạng:

- Sản phẩm MobiSOC.

c) Sản xuất sản phẩm chống tấn công, xâm nhập:

- Sản phẩm MobiSafe.
- Sản phẩm MobiWAF.

d) Dịch vụ giám sát an toàn thông tin mạng.

đ) Dịch vụ phòng ngừa, chống tấn công mạng.

e) Dịch vụ ứng cứu sự cố an toàn thông tin mạng.

g) Dịch vụ tư vấn an toàn thông tin mạng.

h) Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng.

Điều 2. Tổng công ty Viễn thông MobiFone 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 14 tháng 10 năm 2034./.

Nơi nhận:
- Như Điều 1;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long;
- Vụ PC;
- Thanh tra Bộ;
- Lưu: VT, CATTT (3b).TTPC.TPL.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Phạm Đức Long

2

Doanh nghiệp được phép kinh doanh:

- 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

1. GIỚI THIỆU MOBIFONE SECURITY

KHÁCH HÀNG TIÊU BIỂU

KHỐI CHÍNH PHỦ

KHỐI NGÂN HÀNG, TÀI CHÍNH, BẢO HIỂM

KHỐI GIÁO DỤC

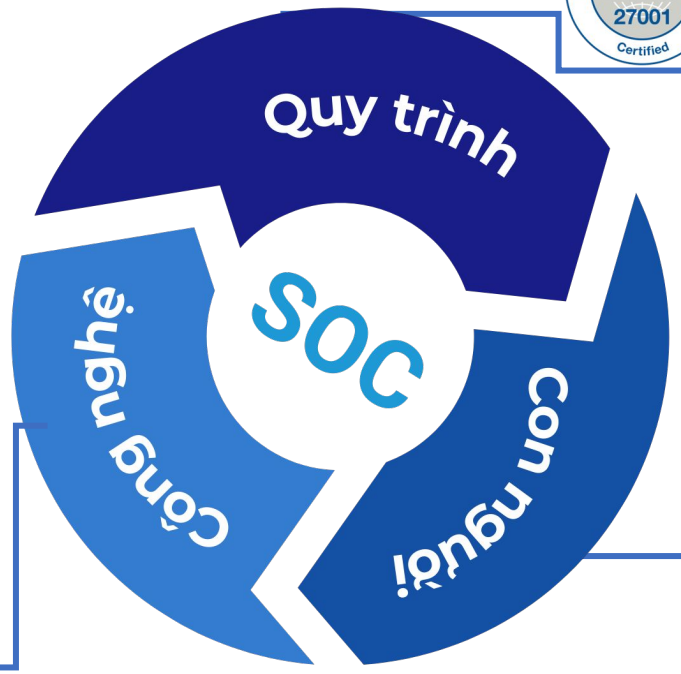
KHÁC

GIỚI THIỆU VỀ MOBIFONE-SOC

2. 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”



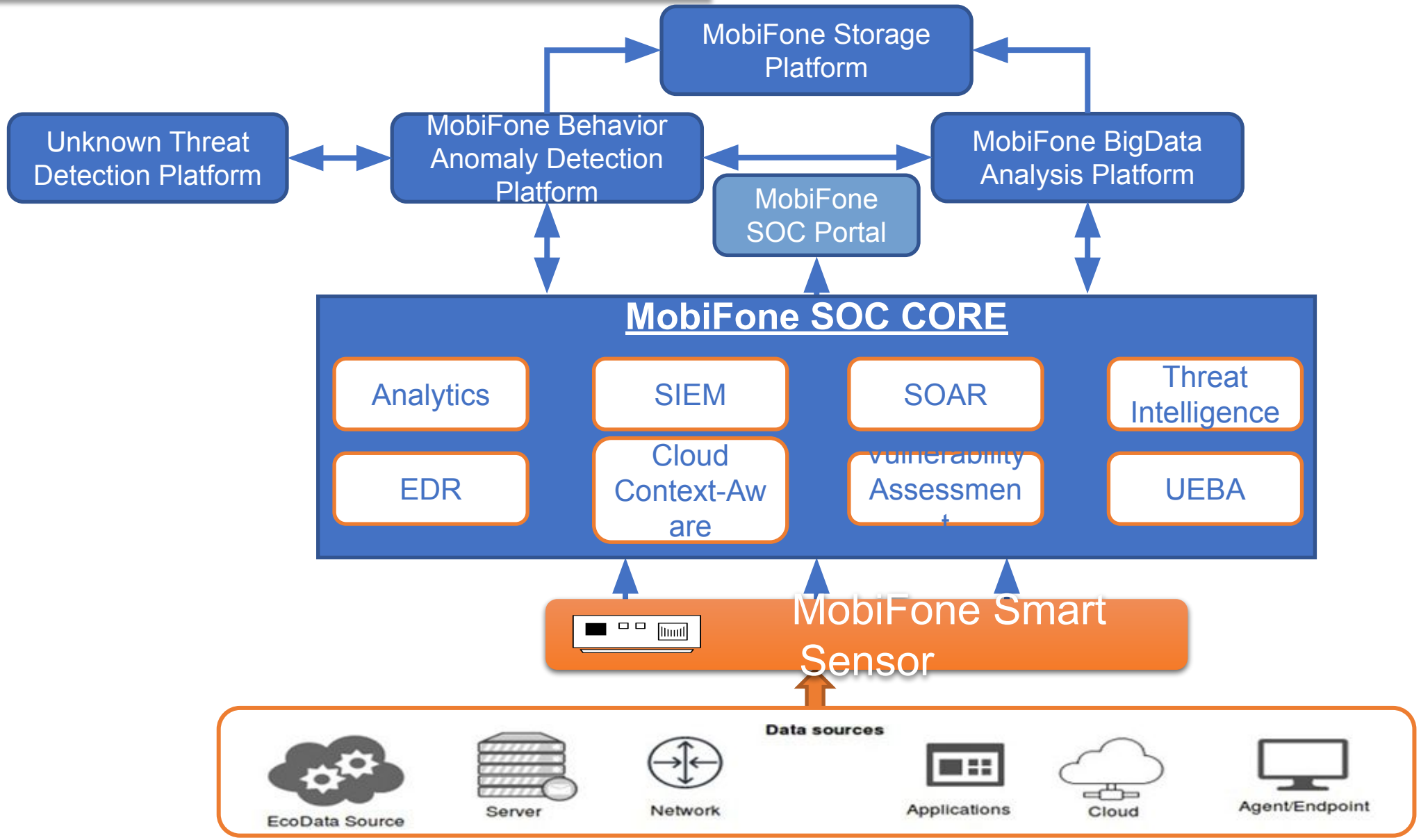
- ✔ EDR
- ✔ SIEM
- ✔ Analytics Engine
- ✔ Threat Intelligence
- ✔ AI Platform
- ✔ BigData Platform
- ✔ Storage Platform

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.

2. GIỚI THIỆU VỀ SOC

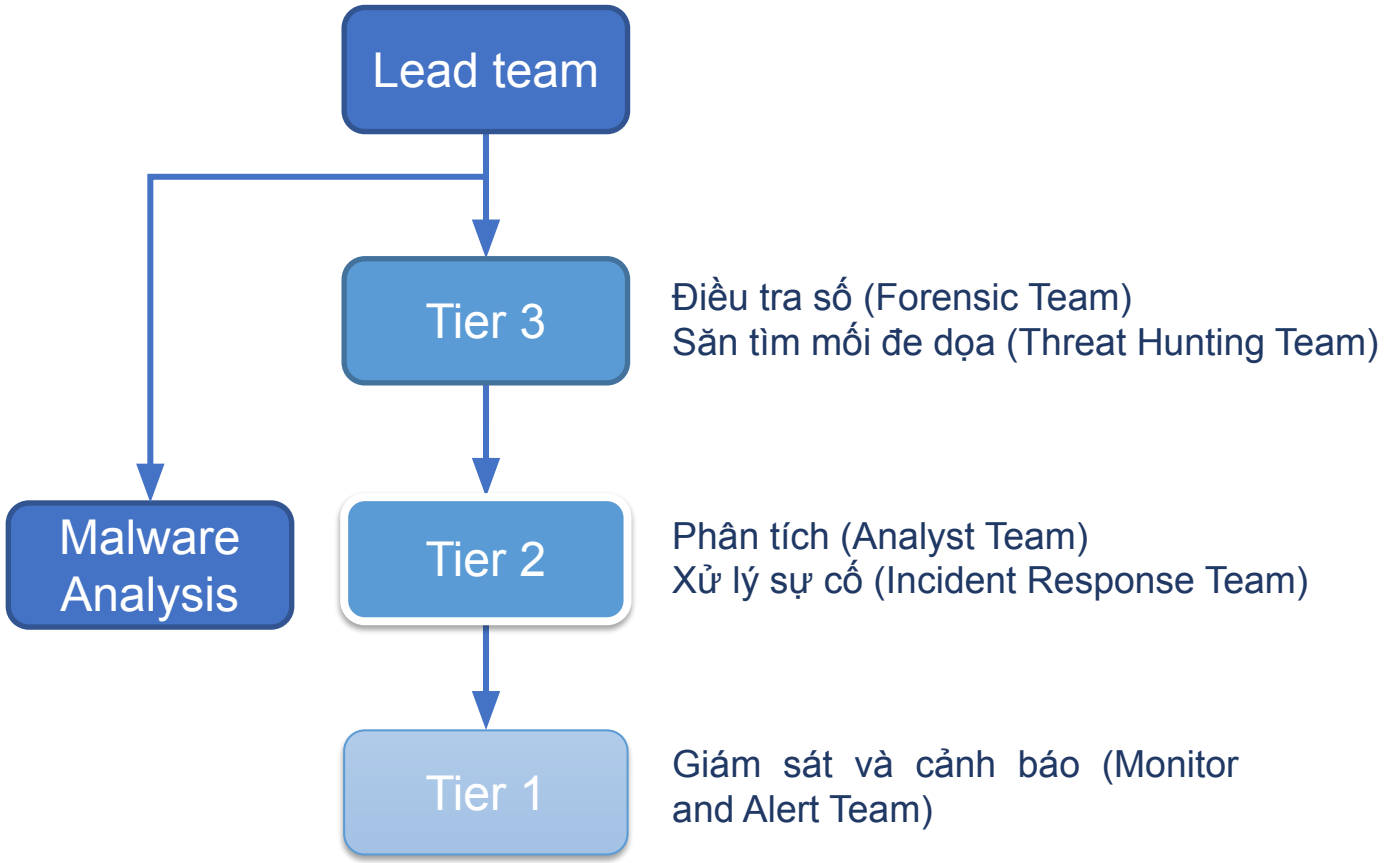
2.1. CÔNG NGHỆ



SOC - MobiFone SECURITY

2. GIỚI THIỆU VỀ SOC

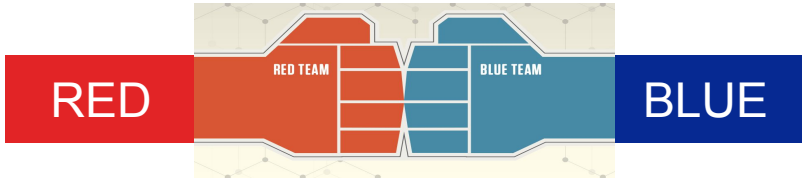
2.2. CON NGƯỜI



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)



GIỚI THIỆU
CÁC DỊCH VỤ MOBIFONE SECURITY

3. CÁC DỊCH VỤ MOBIFONE SECURITY

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

3. CÁC DỊCH VỤ MOBIFONE SECURITY

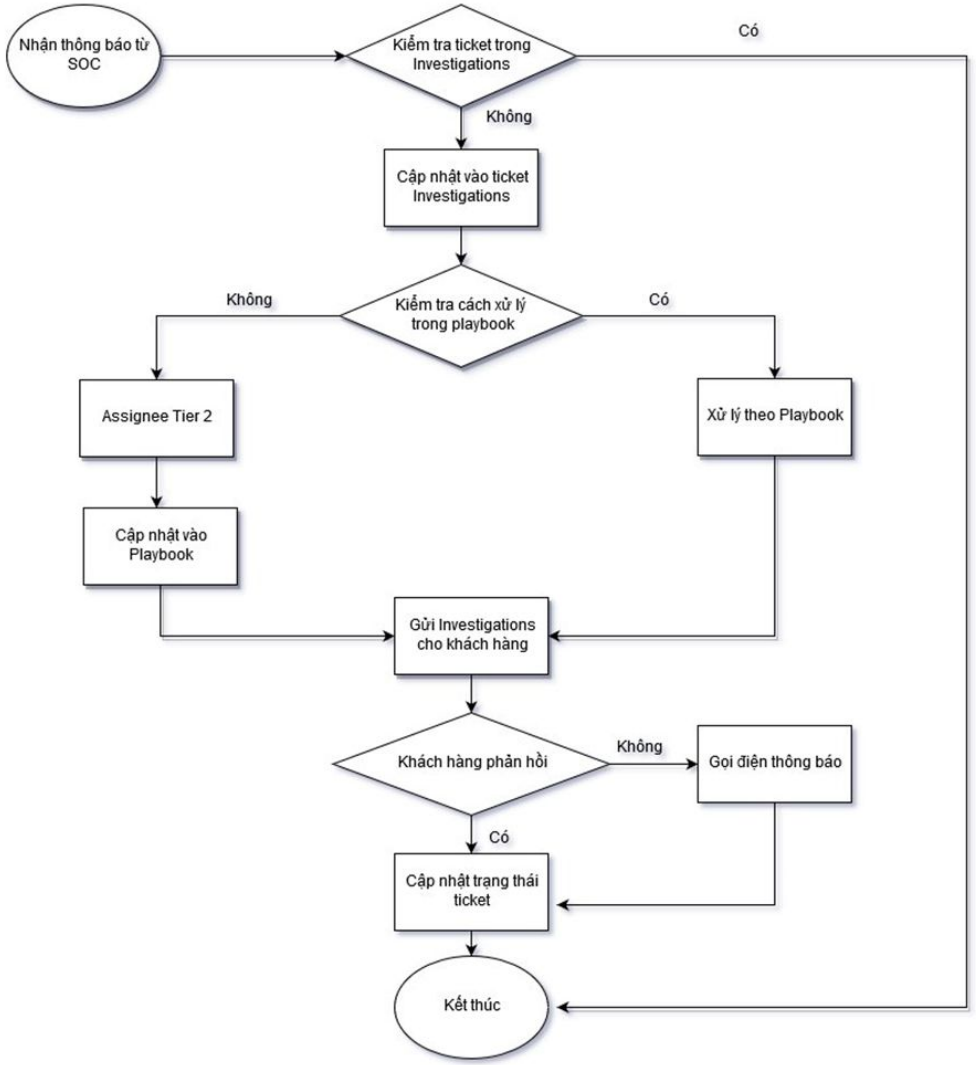
1. DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN

- 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

ƯU ĐIỂM NỔI BẬT

3. CÁC DỊCH VỤ MOBIFONE SECURITY

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.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

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

3. CÁC DỊCH VỤ MOBIFONE SECURITY

1. DỊCH VỤ GIÁM SÁT AN TOÀN THÔNG TIN

LỢI ÍCH KHÁCH HÀNG

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.

Nhanh chóng phát hiện các mối đe dọa, từ đó có những biện 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.

Được đảm bảo về sự an toàn của hệ thống thông tin 24/7 trước các mối đe dọa trên internet.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

2. 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.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

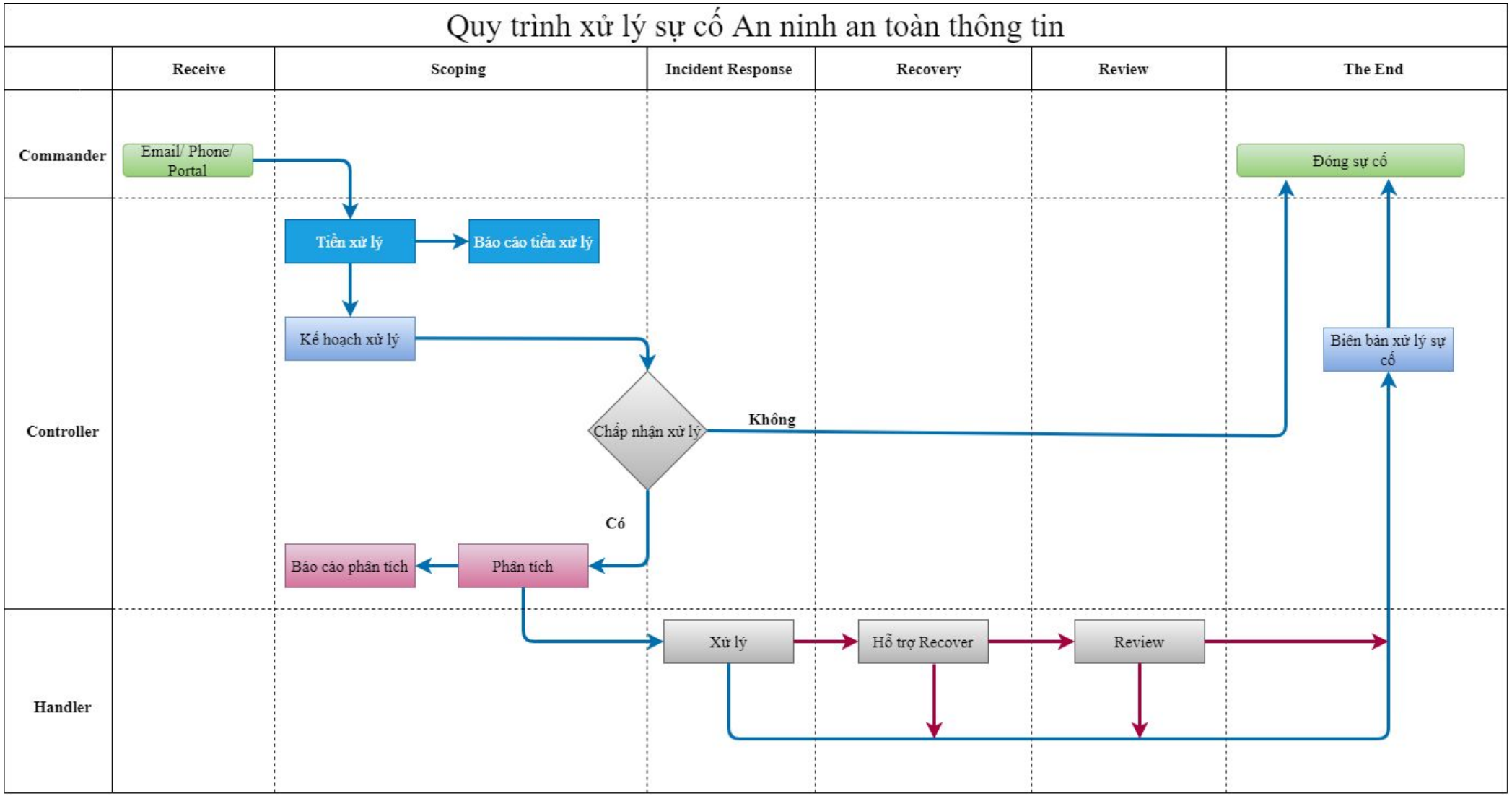
2. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ

- 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.

ƯU ĐIỂM NỔI BẬT

3. CÁC DỊCH VỤ MOBIFONE SECURITY

2. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ



3. CÁC DỊCH VỤ MOBIFONE SECURITY

2. 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

2. 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

3. CÁC DỊCH VỤ MOBIFONE SECURITY

2. DỊCH VỤ ỨNG CỨU VÀ XỬ LÝ SỰ CỐ

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.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

3. 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).

3. CÁC DỊCH VỤ MOBIFONE SECURITY

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

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.

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.

ƯU ĐIỂM NỔI BẬT

3. CÁC DỊCH VỤ MOBIFONE SECURITY

3. 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

3. CÁC DỊCH VỤ MOBIFONE SECURITY

3. 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

3. 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.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

4. DỊCH VỤ DÒ QUÉT LỖ HỔNG BẢO MẬT - VULNERABILITY ASSESSMENT

Vulnerability Assessment là giải pháp dò quét, xác định, phân tích các lỗ hổng bảo mật trong môi trường hệ thống xác định và chỉ ra những điểm yếu (có khả năng trở thành mục tiêu tấn công) cũng như cung cấp khuyến nghị cần thiết để có thể loại bỏ những điểm yếu đó hoặc ít nhất là giảm mức độ rủi ro của chúng xuống một mức độ có thể chấp nhận được.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

4. DỊCH VỤ DÒ QUÉT LỖ HỔNG BẢO MẬT - VULNERABILITY ASSESSMENT

- 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

ƯU ĐIỂM NỔI BẬT

3. CÁC DỊCH VỤ MOBIFONE SECURITY

4. DỊCH VỤ DÒ QUÉT LỖ HỔNG BẢO MẬT - VULNERABILITY ASSESSMENT – PENTEST – SECURITY AUDIT

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.

3. CÁC DỊCH VỤ MOBIFONE SECURITY

DỊCH VỤ KIỂM THỬ AN TOÀN THÔNG TIN – PENETRATION TESTING

ĐỊNH NGHĨA

- Là phương pháp kiểm tra/đánh giá mức độ an toàn bằng cách mô phỏng tấn công của tội phạm mạng trên một hệ thống đang hoạt động (dựa theo chuẩn OWASP, PTES)
- Được thực hiện bằng phương pháp và tư duy của một kẻ tấn công (hacker) thực thụ - là phương pháp có kiểm soát

MỤC ĐÍCH

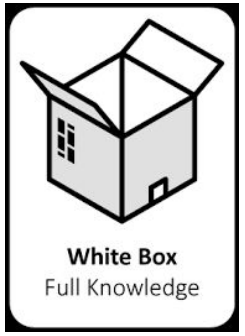
- Chỉ ra các điểm yếu, lỗ hổng để có kế hoạch khắc phục.
- Cung cấp cài nhìn toàn cảnh về an ninh ứng dụng & sản phẩm công nghệ của tổ chức.
- Giảm thiểu tổn thất về tài chính, danh tiếng, sở hữu trí tuệ.
- Tuân thủ các tiêu chuẩn về ANATTT (Hồ sơ cấp độ, PCI DSS…)

THỜI ĐIỂM

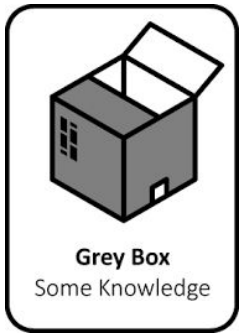
- Theo luật, quy định ngành.
- Health check, đánh giá hệ thống.
- Có thêm hạ tầng mạng hoặc ứng dụng mới hoặc cập nhật hay điều chỉnh đáng kể cho các ứng dụng và hạ tầng.
- Điều chỉnh chính sách bảo mật cho người dùng cuối.

CÁC PHƯƠNG PHÁP KIỂM THỬ XÂM NHẬP

- Thực hiện dưới hình thức không biết thông tin gì về đối tượng đánh giá
- Đúng với thực tế, tuy nhiên phát hiện lỗi có tính chất hạn chế



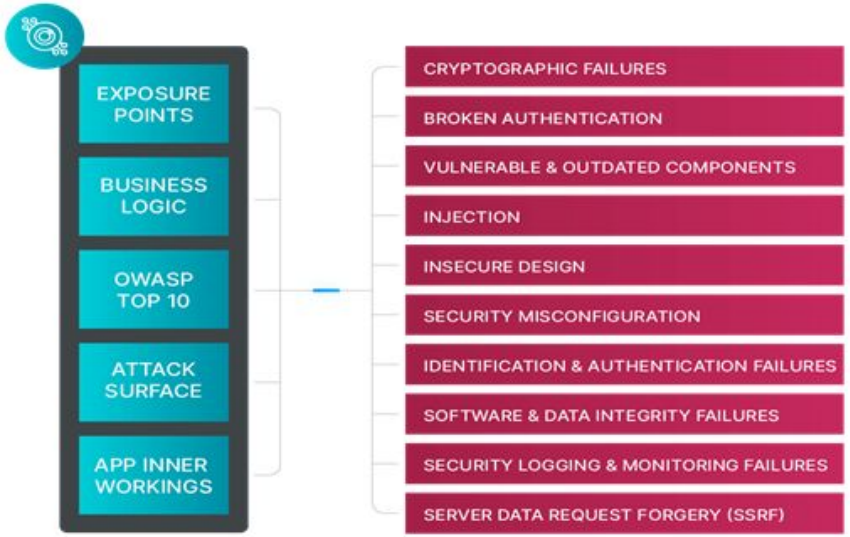
- Thực hiện dưới hình thức Source Code review khi biết toàn bộ thông tin của đối tượng
- Thời gian đánh giá tương đối dài



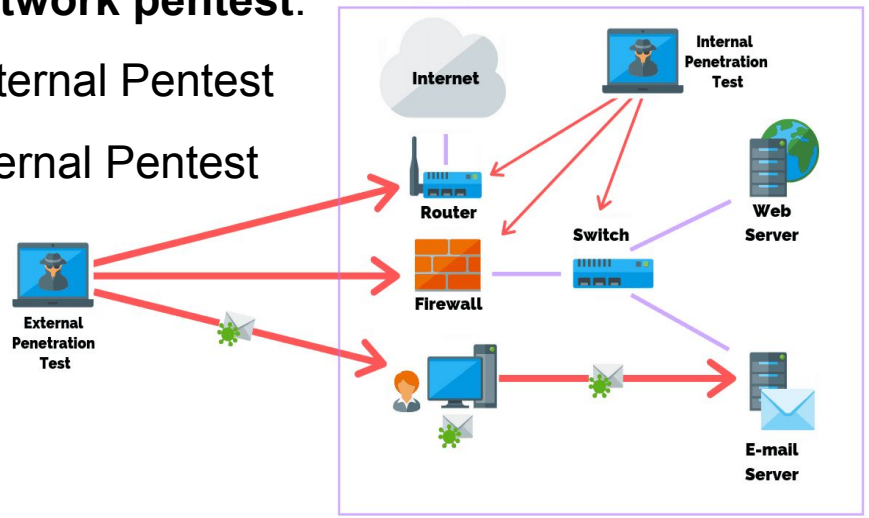
- Thực hiện khi biết một phần thông tin của ứng dụng (tài khoản, hàm chức năng…)
- Hay được lựa chọn để thực hiện đánh giá ngày nay

PHẠM VI PENETRATION TESTING

- **Application pentest**: ứng dụng web, ứng dụng client-server, ứng dụng mobile và IoT, các API…

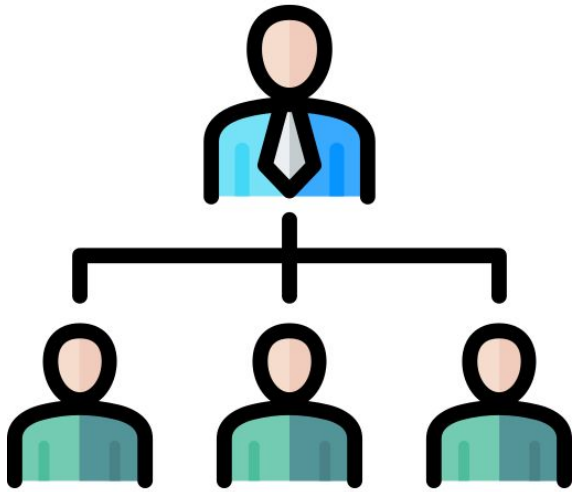


- **Network pentest**:
  - External Pentest
  - Internal Pentest



- **Personnel pentest**: Đánh giá kiểm tra nhận thức cán bộ nhân viên

TỔ CHỨC THỰC HIỆN



- Project Manager
- Pentest team
- Source code review team

Offensive Security Certified Professional - OSCP

Mobile Application Penetration Tester - eLearnSecurity's eMAPT

10+ năm kinh nghiệm

Offensive Security Web Expert - OSWE

Certified Ethical Hacking – CEH

Săn tìm CVE, Bug Bounty

QUY TRÌNH THỰC HIỆN

mobifone

Execution process – WEB APP, API

Targets: Web Application, API

Input

- URL
- Accounts to login

Testing Methodology

- Grey box

Quá trình thực hiện Pentest

- 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 hang đầu (OSWE, OSCE, OSCP, CEH,...)

Tools dò quét bản quyền: Nessus vulnerability scanner, BURPSUITE

Input, output

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

KHÁI NIỆM VỀ KIỂM ĐỊNH AN TOÀN THÔNG TIN

ĐỊNH NGHĨA :

- ❑ Là phương pháp đánh giá kiểm tra tình trạng an ninh của các thành phần trong hệ thống so với các tiêu chuẩn an toàn CIS, SANS, OSSTMM…

- ❑ Đối tượng kiểm tra đánh giá:
- ✔ Thiết bị mạng (Switch, Router, Firewall, IPS/IDS, Server, SAN…)
- ✔ OS (Windows, Linux…), CSDL (Oracle, SQL…), cấu hình web
- ✔ Kiến trúc Topo mạng

MỤC TIÊU :

- ❑ So sánh tình trạng an ninh an toàn thông tin tại thời điểm đánh giá với các chuẩn bảo mật của tổ chức áp dụng/hướng dẫn bảo mật (security guideline) của từng loại thiết bị

- ❑ Nhận thức được các rủi ro, mối đe dọa cùng các khuyến nghị cấu hình theo chuẩn an toàn, từ đó tìm các biện pháp khắc phục

SANS

CIS Center for Internet Security®

OSSTMM www.osstmm.org

PHẠM VI KIỂM ĐỊNH ATTT CỦA MOBIFONE

Kiểm định bảo mật máy chủ :

- Kiểm tra tài khoản, quyền truy cập
- Kiểm tra cấu hình hệ thống
- Kiểm tra giao thức mạng
- Kiểm tra log, event…
- Kiểm tra bảo mật dữ liệu
- V..v…

Kiểm định bảo mật về tường lửa:

- Kiểm tra cấu hình tường lửa
- Kiểm tra quản lý quyền truy cập
- Kiểm tra ghi log và giám sát
- Kiểm tra bảo mật kết nối
- Kiểm tra hiệu suất và khả năng mở rộng
- V..v…

Kiểm định bảo mật cơ sở dữ liệu :

- Kiểm soát truy cập
- Sử dụng mã hoá
- Bảo vệ dữ liệu ở trạng thái tĩnh và truyền tải
- Xử lý thông tin nhạy cảm
- V..v…

Kiểm định bảo mật email

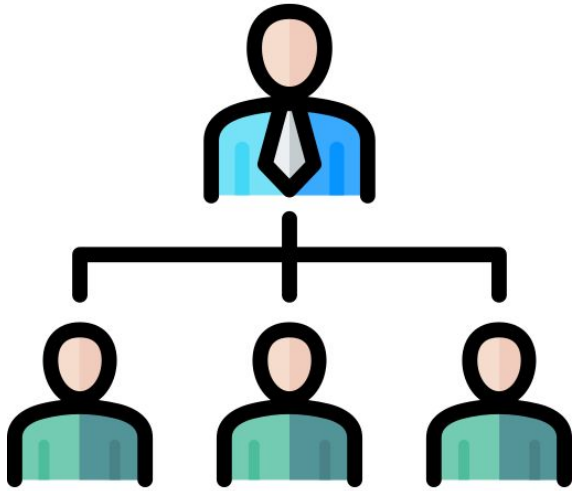
- Kiểm tra quản lý tài khoản và quyền truy cập
- Kiểm tra giao thức bảo mật
- Kiểm tra bảo vệ chống phần mềm độc hại, spam
- Kiểm tra nhật ký, giám sát
- V..v...

Kiểm định bảo mật switch:

- Kiểm tra cấu hình và quản lý
- Kiểm tra giao thức và dịch vụ
- Kiểm tra cấu hình mạng
- Kiểm tra nhật ký và giám sát
- Kiểm tra cậpj nhật bản va
- V..v…

TỔ CHỨC THỰC HIỆN

NHÂN SỰ



- Project Manager
- Security Audit Team

KẾ HOẠCH THỰC HIỆN

1. Kick- off
2. Thực hiện thu thập thông tin
3. Thực hiện phân tích và so sánh các chuẩn
4. Lập các báo cáo kết quả so sánh
5. Họp báo cáo kết quả
6. Khách hàng điều chỉnh/cấu hình lại
7. Tái đánh giá sau khi điều chỉnh

MỘT SỐ MẪU BÁO CÁO

mobifone

BIỂU ĐỒ PHÂN LOẠI LỖ HỔNG

Upload file damanqua.asp lên serversite, cơ chế chuyển file thành 8473-damanqua.asp => URL

1. Tên lỗi:

Bypass retricted upload file.

2. Mô tả

Hệ thống Thẩm định tài sản tồn tại một lỗ hổng mức nghiêm trọng cho phép kẻ tấn công vượt qua cơ chế chặn upload các file thực thi. Kẻ tấn công có thể dùng công cụ Burpsuite để chặn request upload file hợp lệ (.zip, .doc ..), tiến hành sửa nội dung file và phần mở rộng sang .asp, .aspx từ đó up load các file thực thi lên phía serverside nhằm chiếm quyền hệ thống. Hệ thống đã cảnh báo các tập tin thực thi của aspx tuy nhiên chưa có hành vi với các tập tin asp => do đó hacker tiến hành chiếm quyền server.

3. Impact

Khi có được shell upload lên hệ thống, kẻ tấn công có thể leo thang quyền (lên admin), thu thập thông tin làm bàn đạp tấn công các hệ thống khác trong vùng mạng, thay đổi nội dung ứng dụng nhằm lừa đảo người dùng.

4. POC

5. Giải pháp khắc phục và giảm thiểu

- ✓ Kiểm tra nội dung của file ở server side.
- ✓ Kiểm tra phần mở rộng của file .
- ✓ Phân quyền truy cập vào các file tài nguyên một cách hợp lý.
- ✓ Cập nhật các mẫu mã độc mới liên quan đến asp và aspx.

MỘT SỐ MẪU BÁO CÁO

mobifone

BIỂU ĐỒ PHÂN LOẠI LỖ HỔNG

Thông tin lỗ hổng	
Lỗ hổng mức nghiêm trọng	01
Lỗ hổng mức cao	02
Lỗ hổng mức trung bình	00
Lỗ hổng mức thấp	00

1. SQL INJECTION

Mức độ

Nghiêm trọng

Mô tả

Ứng dụng sử dụng các câu lệnh nối chuỗi để truy vấn DB gây ra lỗi Sql Injection. Kẻ tấn công có thể lợi dụng thêm các truy vấn không hợp lệ để khai thác thông tin DB.

Vị trí

Ứng dụng Android

Bằng chứng

```
public Customer GetChild1(int paramInt)
{
  int i = 1;
  Cursor localCursor = dbhelper.getReadableDatabase().rawQuery(" select * from tbRelCustomer where Customerid = " + paramInt + " and CustomerType = 'Con1'", null);
  Customer localCustomer = new Customer();
  if (localCursor != null)
  {
    paramInt = 1;
    if (localCursor.getCount() <= 0) {
      break label103;
    }
    label62:
```

Hình 1: Ứng dụng sử dụng nối chuỗi gây ra SQL Injection

Khuyến nghị

Rà soát lại mã nguồn, sử dụng câu lệnh SQLiteStatement thay thế rawQuery

MỘT SỐ MẪU BÁO CÁO

mobifone

1. **Tổng quan**

Trong hạng mục Audit thiết bị Switch chúng tôi sử dụng các công cụ thu thập thông tin cấu hình, các bản vá cũng như các dịch vụ đang chạy trên thiết bị. Bằng cách sử dụng các công cụ, câu lệnh khi truy nhập thiết bị và không gây ảnh hưởng đến hệ thống

Công cụ phân tích cấu hình: Nipper Studio - https://www.titania.com/nipper-studio

Sau khi thu thập thông tin, chúng tôi sử dụng công cụ phân tích cấu hình, kiểm tra các câu lệnh kết hợp với checklist của CIS Benmark tương ứng với từng loại thiết bị để so sánh kết quả PASS/FAIL.

2. **Chi tiết đánh giá thiết bị mạng**

Switch Catalyst 2960 -2

Kết quả đánh giá

Nội dung đánh giá	Hạng mục kiểm tra	Kết quả	Mức độ
Đánh giá phiên bản	Kiểm tra phiên bản của OS, Firmware, Software	FAIL	CAO
Kiểm tra hiệu năng thiết bị	Kiểm tra CPU	PASS	N/A
	Kiểm tra MEMORY	PASS	N/A
Đánh giá chính sách quản lý thiết bị	Kiểm tra chính sách mật khẩu	FAIL	TRUNG BÌNH
	Kiểm tra mã hóa mật khẩu xác thực của các dịch vụ và tài khoản người dùng trên thiết bị	FAIL	CAO

Chi tiết lỗi, lỗ hổng và khuyến nghị

Nội dung đánh giá	Kết quả kiểm tra và Tác động	Khuyến nghị
Đánh giá phiên bản	Phiên bản hệ điều hành là 12.2 tồn tại nhiều lỗ hổng đã được phát hiện từ lâu, kẻ tấn công dễ dàng khai thác các lỗ hổng còn tồn tại https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-10360/version_id-62515/Cisco-IOS-12.2.html	Nâng cấp lên phiên bản hệ điều hành mới nhất, cập nhật các bản vá mới nhất của Cisco.
Đánh giá chính sách quản lý thiết bị	Hệ thống chưa sử dụng mật khẩu còn yếu chưa đảm bảo đầy đủ các yếu tố an toàn. Việc nâng cao mức độ an toàn của mật khẩu sẽ giảm thiểu đáng kể các cuộc tấn công vét cạn có thể xảy ra.	Thiết lập mật khẩu đảm bảo các điều sau: Mật khẩu phải có ít nhất tám ký tự. Các ký tự trong mật khẩu không nên được lặp lại nhiều hơn ba lần. Mật khẩu phải bao gồm cả chữ hoa và chữ thường.

HỎI VÀ ĐÁP

CẢM ƠN SỰ THEO DÕI CỦA QUÝ VỊ!