**CÔNG TY TNHH HỆ THỐNG THÔNG TIN FPT (FPT IS)**

# BÁO CÁO MÔ TẢ SẢN PHẨM DỰ THI GIẢI THƯỞNG SẢN PHẨM CÔNG NGHỆ SỐ MAKE IN VIET NAM NĂM 2020

Hạng mục: **Giải pháp số xuất sắc nhất**

*Bên cạnh tài liệu giới thiệu về sản phẩm (do doanh nghiệp cung cấp gửi kèm file), doanh nghiệp tham dự cần cung cấp thêm các thông tin dưới đây, để giúp Hội đồng giám khảo thuận tiện trong việc đánh giá về sản phẩm dự thi*

## 1. Tên của giải pháp công nghệ số

**Phần mềm quản lý phát hiện và ứng phó các mối đe dọa an toàn an ninh thông tin – FPT.EagleEye MDR**

## 2. Tính sáng tạo và độc đáo của nền tảng

*2.1. Nêu khác biệt của giải pháp với những giải pháp quốc tế và trong nước hiện nay (về chức năng, hiệu suất, chi phí đầu tư, mua sắm hoặc thuê...)*

FPT.EagleEye MDR là giải pháp giám sát an toàn thông tin (ATTT) và phản ứng sự cố, được tích hợp giải pháp quản lý Log FPT.EagleEye mGuard. Giải pháp là phần mềm đầu tiên và duy nhất tại Việt Nam giúp nhanh chóng phát hiện và xử lý các mối nguy hại trên Endpoint, giảm thiểu tối đa nguồn lực, chi phí và thời gian trong quá trình vận hành và giám sát ATTT.

Phần mềm cũng cung cấp thông tin xuyên suốt hệ thống, hỗ trợ tối đa quá trình phân tích, phát hiện bất thường và điều tra số khi có sự cố bảo mật xảy ra trên hệ thống. Giao diện quản trị tập trung, trực quan giúp việc sử dụng, truy vấn và điều tra số được thực hiện dễ dàng, nhanh chóng tìm ra nguyên nhân gốc rễ (root cause) của vấn đề để đưa ra các hành động ứng cứu kịp thời.

Bên cạnh đó, việc triển khai sản phẩm diễn ra trong thời gian ngắn, Endpoint chỉ cần cài 1 sensor duy nhất. Hỗ trợ triển khai qua các công cụ như SCCM, Active Directory GPO. Các sensor chạy trên thiết bị cuối chỉ chiếm < 5% CPU và 10-30 MB (RAM) vì thế không làm ảnh hưởng tới hiệu năng.

FPT.EagleEye MDR có nhiều chức năng ưu việt bao gồm:

- Quản lý dữ liệu tập trung bằng giải pháp FPT.EagleEye mGuard. Cung cấp nền tảng quản lý dữ liệu mạnh mẽ và phân tích hành vi dựa trên nguồn Big Data nhằm phát hiện bất thường để phản ứng sự cố kịp thời
- Ghi lại thông tin, sự kiện diễn ra trên Endpoint gồm: user, system, registry, process, network
- Tra cứu thông tin về Endpoint gồm: các kết nối, các tiến trình thực thi, các mã hash, registry...
- Phát hiện các cuộc tấn công: cung cấp các giao diện như giám sát sự kiện liên quan tới cuộc tấn công, bổ sung các nguồn Threat Intelligence, tạo các bộ luật phát hiện tấn công
- Hệ thống cho phép phản hồi và ứng cứu sự cố từ xa trên Endpoint thông qua tính năng Live Response. Khả năng thực thi nhiều câu lệnh phục vụ điều tra số và ứng cứu sự cố như: dump memory, kill process, chỉnh sửa registry… và hoàn toàn có thể tự động hoá thông qua giải pháp REST API.
- Quản lý sự kiện bảo mật thông tin: cung cấp giao diện quản lý và giám sát sự kiện, theo dõi mức độ an toàn chung của Endpoint trên toàn hệ thống và tiến độ xử lý sự cố
- Phát hiện và tự động cảnh báo khi các cuộc tấn công hoặc sự cố về ATTT xảy ra qua nhiều kênh như: Email, JIRA, MS Teams, Slack, Telegram...
- Xuất báo cáo định kỳ có thể tùy chỉnh để cung cấp thông tin kịp thời, giảm thiểu rủi ro. Xuất báo cáo theo nhiều định dạng và quy chuẩn bảo mật trên thế giới như DISA STIG, FISMA, PCI DSS, HIPAA/HITECH, SCAP

*2.2. Định hình/phù hợp xu hướng*

Các chuyên gia bảo mật hàng đầu thế giới cảnh báo rằng không có hệ thống nào là an toàn tuyệt đối, nhiều doanh nghiệp thậm chí không biết rằng họ đã bị hack. Vì vậy, xu hướng đảm bảo ATTT hiện nay là giám sát 24x7x365, giúp phát hiện và xử lý kịp thời các mã độc.

Bên cạnh đó, từ năm 2017 đến nay, các tổ chức, doanh nghiệp tại Việt Nam và trên thế giới đang có xu hướng sử dụng dịch vụ ATTT cung cấp bởi các đối tác đáng tin cậy trong lĩnh vực Bảo mật, thay vì đầu tư các khoản chi phí lớn cho hệ thống phần cứng, phần mềm và con người. Nắm bắt xu hướng đó, FPT IS đã phát triển FPT.EagleEye MDR trở thành giải pháp giám sát ATTT và phản ứng sự cố bảo mật tự động theo phương thức dịch vụ ứng dụng phần mềm (SaaS) đầu tiên tại Việt Nam, giúp phát hiện nguy cơ tấn công mạng và đưa ra cảnh báo chỉ trong vòng 10 phút, tối ưu kiểm soát máy trạm 24/7.

## 3. Công nghệ, chất lượng giải pháp

*3.1. Nêu các công nghệ mới được áp dụng trong giải pháp (AI, Bigdata, IoT, Blockchain,...)*

Bằng việc sử dụng công nghệ Threat Intelligence Feeds được hỗ trợ bởi Carbon Black, giải pháp có thể nhanh chóng phát hiện các mối đe dọa. Bên cạnh đó, sản phẩm còn được áp dụng các công nghệ hàng đầu như Big Data, Automation, Machine Learning, AI vào quá trình giám sát, điều tra sự cố bảo mật trong việc quản lý và xử lý các mối đe dọa gây mất ATTT. Ngay khi phát hiện nguy cơ, trong vòng 10 phút, các chuyên gia của FPT IS sẽ nhanh chóng đưa ra cảnh báo và khuyến cáo khắc phục tới doanh nghiệp, tổ chức. Thông tin sẽ liên tục được trao đổi thông qua Customer Portal. Với FPT.EagleEye MDR, FPT IS cam kết kiểm soát mức độ bảo mật chung trên toàn bộ hệ thống ngay cả khi người dùng đang ngủ.

Bên cạnh đó, giải pháp phát hiện tấn công dựa trên MITRE ATT&CK với trên 200 kỹ thuật tấn công. Phần mềm phân tích hàng nghìn hành vi được ghi nhận trên Endpoint bằng hệ thống phát hiện xâm nhập trên nền tảng điện toán đám mây của FPT IS. Những mối đe dọa tiềm tàng sẽ được đội ngũ chuyên gia bảo mật FPT IS phân tích, tiến hành điều tra sử dụng công nghệ phân tích và xử lý tập trung, có thể phát hiện được những cuộc tấn công có chủ đích hay những mã độc chưa từng được biết đến trên thế giới.

*3.2. Hỗ trợ sử dụng trên nhiều thiết bị, môi trường*

Với sự hỗ trợ từ công nghệ Carbon Black, FPT.EagleEye MDR có thể cài đặt trên nhiều thiết bị đa nền tảng như Window, Linux, MacOS.

FPT.EagleEye MDR dễ dàng tích hợp với các hệ thống sẵn có của doanh nghiệp, vì vậy có thể giám sát trong phạm vi toàn bộ hệ thống công nghệ thông tin (CNTT) phân tán tại nhiều văn phòng, data center khác nhau. Điều này giúp doanh nghiệp không có bất cứ điểm mù nào tại lớp Endpoint.

*3.3. Khả năng bảo trì, bảo hành của sản phẩm*

FPT.EagleEye MDR được cập nhật bản vá liên tục giúp các sensor cài trên Endpoint hoạt động trơn tru và không làm gián đoạn việc vận hành của doanh nghiệp. FPT IS cam kết cung cấp dịch vụ liên tục và đảm bảo an toàn an ninh cho các khách hàng.

*3.4. Khả năng đảm bảo an toàn, bảo mật của giải pháp*

- Với FPT.EagleEye MDR, 0% dữ liệu của khách hàng ra khỏi Trung tâm điều hành An ninh mạng FPT CSOC
- Tính năng xác thực 2 yếu tố giúp bảo vệ các tài khoản của người dùng

- FPT IS được cấp chứng nhận cung cấp nền tảng dịch vụ SOC đáp ứng yêu cầu kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia, đảm bảo mô hình bảo mật 4 lớp

**4. Công đoạn cốt lõi của giải pháp do người Việt Nam thực hiện**

*4.1. Chứng minh công đoạn cốt lõi của giải pháp do doanh nghiệp làm chủ*

FPT.EagleEye MDR được FPT IS xây dựng trong khoảng 1 năm và liên tục phát triển các tính năng mới nhằm đem đến một giải pháp toàn diện nhất cho khách hàng.

FPT IS phát triển FPT.EagleEye MDR dựa trên công đoạn cốt lõi DFIR – Digital Forensics and Incident Response với các đặc điểm nổi bật:

- Công cụ hỗ trợ mạnh với Automation qua API, giúp tối ưu thời gian trong ứng cứu sự cố
- Quy trình xử lý sự cố chuyên nghiệp, hiệu quả thông qua tự động hoá
- Bộ playbook được xây dựng chi tiết để sẵn sàng ứng cứu mọi loại sự cố về ATTT

Sản phẩm đang vận hành và quản lý bởi hơn 20 thành viên – là các chuyên gia bảo mật dày dạn kinh nghiệm, chuyên sâu trong lĩnh vực giám sát ATTT, dò quét điểm yếu bảo mật và ứng cứu sự cố, từng tham gia triển khai các dự án lớn liên quan đến ATTT trong và ngoài nước. Các chuyên gia của FPT IS sở hữu hàng loạt chứng chỉ bảo mật hàng đầu thế giới như: CISSP, CISM, CCIE Security, CCSP, PCI QSA, ISO 27001 Lead Auditor, OSCE, OCSP, GCFA…

*4.2. Chứng minh chất lượng dịch vụ tư vấn giải pháp*

Đội ngũ tư vấn FPT.EagleEye MDR cũng là những chuyên gia trực tiếp tham gia vào quá trình phát triển sản phẩm. Do đó, việc tư vấn giải pháp được tiến hành một cách chi tiết và chuyên sâu. FPT IS thường tổ chức các buổi workshop chuyên nghiệp nhằm trao đổi, đề xuất các giải pháp quản lý dữ liệu tập trung và kế hoạch giám sát ATTT phù hợp với hiện trạng hệ thống CNTT của khách hàng. Mọi khúc mắc của doanh nghiệp, tổ chức sẽ được các chuyên gia của FPT IS tư vấn, giải đáp cặn kẽ trước và trong khi triển khai sản phẩm, nhằm giúp khách hàng tháo gỡ bài toán về bảo mật.

**5. Tính năng giải pháp (dễ sử dụng, tương thích, tùy biến, mở rộng,...)**

*5.1. Khả năng mở rộng và năng lực cung cấp dịch vụ cho lượng người dùng lớn*

Là giải pháp giám sát về hành vi người dùng nên FPT.EagleEye MDR phải đáp ứng được yêu cầu cao về khả năng sẵn sàng và tính ổn định khi đưa vào vận hành. Sản phẩm được áp dụng nhiều công nghệ tiên tiến như xử lý dữ liệu lớn (Big Data processing), lưu trữ dữ liệu tập trung

và cung cấp một bộ máy tìm kiếm phân tán nên có thể tìm kiếm, phân tích lượng lớn dữ liệu theo thời gian thực và cận thời gian thực (real-time & near real-time), đồng thời hỗ trợ hiệu quả quá trình điều tra số.

Bên cạnh đó, FPT.EagleEye MDR còn có khả năng hoạt động ổn định trong thời gian dài mà không gặp các vấn đề về tốc độ xử lý, ngay cả khi thực hiện các thuật toán phân tích phức tạp trên lượng dữ liệu lớn.

FPT.EagleEye MDR hỗ trợ không giới hạn số lượng Endpoint cần giám sát. Khi triển khai giải pháp trên một phạm vi người dùng nhỏ thì hệ thống Endpoint được quản lý thông qua máy chủ quản trị tập trung tại FPT Cloud. Còn khi số lượng người dùng tăng lên, FPT IS sẽ nâng cấp hạ tầng (bao gồm phần cứng và hạ tầng mạng) cần thiết để đáp ứng nhu cầu vận hành.

*5.2. Khả năng tích hợp hệ thống*

FPT.EagleEye MDR được xây dựng với mục đích có thể tùy biến linh hoạt để thích nghi với nhiều môi trường, hạ tầng của các doanh nghiệp khác nhau.

Với Carbon Black – công nghệ dành cho các Endpoint mạnh nhất hiện nay, sản phẩm có khả năng tích hợp và vận hành hài hòa trên mọi ứng dụng, mọi nền tảng đám mây và mọi thiết bị.

*5.3. Khả năng phân quyền người dùng và bảo mật dữ liệu người dùng*

Ứng dụng quản trị tập trung FPT.EagleEye MDR được trang bị chức năng xác thực 2 yếu tố và phân quyền chặt chẽ. Mỗi khi đăng nhập vào hệ thống, người dùng sẽ được yêu cầu nhập mã đăng nhập đặc biệt ngoài mật khẩu để xác nhận phiên đăng nhập của mình là hợp lệ.

Việc tích hợp xác thực 2 yếu tố giúp nâng cao tính an toàn chung cho toàn hệ thống và giảm rủi ro tới mức tối thiểu cho tài khoản người dùng. Ngoài ra với giao diện tạo và phân quyền tài khoản trực quan, quản trị viên của khách hàng sẽ dễ dàng kiểm soát quyền hạn của người dùng hệ thống khác, đảm bảo các tài khoản sẽ chỉ có thể thực thi các chức năng đúng với nhiệm vụ và mục đích của mình.

Bên cạnh đó, hiện nay, các nguy cơ gây mất ATTT như lấy cắp thông tin, tấn công thay đổi cấu hình, dữ liệu… ngày một tăng cao. Do đó, khi phát triển FPT.EagleEye MDR, chúng tôi chú trọng đảm bảo tính bảo mật cao nhất cho giải pháp. Tất cả các luồng thông tin truyền về máy chủ đều thông qua một một kênh truyền được mã hóa. Việc mã hóa giúp đảm bảo tính bảo mật và toàn vẹn cho toàn bộ dữ liệu trên kênh truyền, từ đó phòng chống được khả năng thay đổi, đánh cắp và làm sai lệch thông tin.

*5.4. Tính thân thiện với người dùng*

- Cổng thông tin có giao diện giám sát an ninh mạng trực quan, rõ ràng với hệ thống vận hành giám sát 24x7x365
- Thông tin minh bạch, dễ dàng theo dõi và trao đổi trên nhiều kênh Ticket, SIEM, Slack, SMS
- Bộ cài đặt đơn giản, được triển khai nhanh chóng qua nhiều giải pháp tích hợp như SCCM, GPO, ePO...

**6. Tính cấp thiết của bài toán mà giải pháp đang giải quyết tại Việt Nam**

*6.1. Chứng minh giải pháp đang giải quyết bài toán nào của tổ chức/doanh nghiệp/cá nhân*

Ngày nay, trước sự phát triển và bùng nổ của CNTT, vấn đề về an toàn, an ninh mạng đang ngày càng gặp nhiều thách thức. Các cuộc tấn công mạng có quy mô lớn, mức độ phức tạp xảy ra ngày càng nhiều và được chuẩn bị một cách kỹ lưỡng. Theo đó, các mục tiêu tấn công đang dần chuyển từ cá nhân sang các công ty, tập đoàn kinh tế lớn, nghiêm trọng hơn là các hệ thống thông tin quan trọng của các quốc gia.

Do đó, với FPT IS đã phát triển FPT.EagleEye MDR nhằm giúp doanh nghiệp chủ động giám sát và ứng phó các cuộc tấn công ngày càng tinh vi bao gồm: tấn công lây nhiễm mã độc sử dụng trí tuệ nhân tạo (AI); tấn công mạng có chủ đích vào các hệ thống CNTT...

Ngoài ra, giải pháp giúp doanh nghiệp có cái nhìn tổng thể về mức độ ATTT trên toàn hệ thống Endpoint nằm phân tán tại nhiều nơi, đồng thời dễ dàng tuân thủ các quy định về bảo mật ATTT. Không chỉ vậy, FPT.EagleEye MDR còn giúp khách hàng tìm ra nguyên nhân gây ra sự cố nhằm khắc phục triệt để các lỗ hổng trong hệ thống CNTT.

*6.2. Tầm quan trọng của bài toán Việt Nam mà giải pháp đang tháo gỡ*

Cuộc Cách mạng Công nghiệp 4.0 đang diễn ra và tác động mạnh mẽ đến mọi lĩnh vực của xã hội, kéo theo các cuộc tấn công mạng ngày càng tinh vi, gây thiệt hại to lớn về kinh tế, tài chính, an ninh. Năm 2019, 8,5 tỷ hồ sơ bị vi phạm được báo cáo. Càng nhiều hồ sơ bị lộ, hacker càng có nhiều thông tin để tấn công và dễ dàng lọt vào hệ thống của tổ chức, gây ra nhiều cuộc khủng hoảng (theo Báo cáo chỉ số nguy cơ an toàn mạng 2020 – IBM X-Force Threat Intelligence Index 2020).

Trong bối cảnh đó, giải pháp FPT.EagleEye MDR ra đời và kiểm soát toàn diện, nâng cao khả năng phòng thủ cho hệ thống CNTT của các tổ chức bằng việc dự đoán và ngăn chặn các cuộc tấn công mạng, hạn chế sự lây lan, giảm thiểu tối đa hậu quả, đồng thời nhanh chóng khôi phục hệ thống về trạng thái ổn định và an toàn.

**7. Mô hình, chiến lược và quy mô thị trường**

*7.1. Thị phần và tiềm năng thị trường*

Thị phần của FPT.EagleEye MDR hiện chiếm khoảng 30% - 40% thị trường Giám sát ATTT tại Việt Nam. Tiềm năng phát triển thị trường của sản phẩm là rất lớn bởi phần mềm được xây dựng theo các xu hướng chuyển dịch ATTT hiện đại như:

- 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/CT-TTg năm 2018 và 14/CT-TTg năm 2019 của Thủ tướng Chính phủ về nâng cao năng lực phòng chống phần mềm độc hại và 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
- Thông tư 18/2018/TT-NHNN cập nhật về quy định ATTT trong các hoạt động ngân hàng

*7.2. Mô hình và chiến lược kinh doanh*

FPT.EagleEye MDR đang được FPT IS triển khai theo mô hình Dịch vụ ứng dụng phần mềm (SaaS). Với mục tiêu mang đến cho ngày càng nhiều khách hàng một giải pháp toàn diện về giám sát ATTT và phản ứng sự cố, FPT IS đang triển khai các hoạt động quảng bá, giới thiệu sản phẩm theo nhiều hình thức khác nhau để mở rộng thị trường ở nhiều lĩnh vực hơn (Ngân hàng, Bảo hiểm, Chứng khoán, Sản xuất…) như:

- Tổ chức và tham gia các hội thảo chuyên đề về ATTT để quảng bá, giới thiệu sản phẩm
- Hợp tác với các đối tác chiến lược để phân phối sản phẩm
- Triển khai dịch vụ dùng thử trong 3 tháng để khách hàng trải nghiệm các tính năng ưu việt của sản phẩm
- Thực hiện các chiến dịch marketing qua email, mạng xã hội…

**8. Tác động kinh tế, xã hội**

*8.1. Đánh giá của các tổ chức/doanh nghiệp đã sử dụng giải pháp*

Chỉ sau hơn 2 năm cung cấp cho các khách hàng, FPT.EagleEye MDR đã trở thành "vệ sĩ" đáng tin cậy, giúp ngăn chặn kịp thời hàng nghìn sự cố về bả mật, giảm tối đa thiệt hại về tài chính và danh tiếng cho nhiều doanh nghiệp, tổ chức.

"FPT IS là đối tác chuyên nghiệp và tin cậy trong bảo vệ an ninh an toàn thông tin cho công ty chúng tôi khi đã kịp thời phát hiện và xử lý nhiều cuộc tấn công mạng vào hệ thống trong thời gian vừa qua. Chúng tôi sẽ tiếp tục lựa chọn FPT IS là đối tác bảo vệ hệ thống CNTT

trong thời gian tới", lãnh đạo của một tổ chức tài chính cho biết.

*8.2. Chứng minh việc tăng trưởng của tổ chức/doanh nghiệp đã sử dụng giải pháp*

Khi sử dụng FPT.EagleEye MDR, hệ thống CNTT được bảo vệ và giám sát 24/7, từ đó doanh nghiệp, tổ chức có thể vận hành hiệu quả và đạt tốc độ tăng trưởng mạnh mẽ.

Điển hình như một doanh nghiệp trong lĩnh vực Tài chính, sau khi triển khai FPT.EagleEye MDR, hệ thống kinh doanh của họ không ngừng được mở rộng, các đại lý có mặt tại ngày càng nhiều tỉnh, thành phố của Việt Nam (trung bình thêm 12 tỉnh/thành phố mỗi năm). Tổng doanh thu năm 2018 và năm 2019 đạt gần 8.000 tỷ và nộp Ngân sách gần 2.000 tỷ. Với gần 5.000 điểm bán hàng, công ty này đã mang lại việc làm cho khoảng 10.000 lao động tại các địa phương.

*8.3. Tác động kinh tế, xã hội*

Về kinh tế, FPT.EagleEye MDR xử lý kịp thời các cuộc tấn công mạng và bảo vệ toàn diện các dữ liệu quan trọng, từ đó giúp các doanh nghiệp, tổ chức tránh thất thoát, tăng trưởng ổn định, đóng góp giá trị ngày càng cao cho nền kinh tế nước nhà.

Ngăn chặn được các tội phạm mạng, bảo vệ được dữ liệu (đặc biệt là những thông tin cá nhân, thông tin tài chính hoặc thông tin mật của cơ quan nhà nước) sẽ góp phần duy trì an ninh, trật tự xã hội, hướng đến mục tiêu phát triển bền vững.

*8.4. Chứng minh việc tăng năng suất*

Theo thống kê, với FPT.EagleEye MDR, thời gian phản ứng sự cố nhanh hơn gấp 10 lần so với các dịch vụ bảo mật thông thường và giảm thiểu rủi ro trên Endpoint toàn thời gian lên đến 75%.

*8.5. Đánh giá về việc giúp tiết kiệm chi phí sản xuất khi sử dụng giải pháp*

Khi lựa chọn triển khai FPT.EagleEye MDR, khách hàng không phải đầu tư bất kỳ chi phí nào cho hệ thống phần cứng và phần mềm. Chi phí được tính trên từng Endpoint phù hợp với quy mô của các doanh nghiệp, tổ chức.

Bên cạnh đó, khách hàng cũng không cần mất chi phí để thuê và duy trì một đội ngũ làm ATTT, nhưng vẫn được hỗ trợ bởi các chuyên gia bảo mật của FPT IS.

*8.6. Đánh giá về việc tối ưu quy trình, quản lý*

FPT.EagleEye MDR tối ưu hóa quy trình giám sát ATTT khi tự động hóa 99% việc phân tích, đánh giá, xử lý các cảnh báo và tự động hóa 50% các quy trình trên toàn hệ thống.

*8.7. Thời gian đã triển khai của giải pháp*

FPT.EagleEye MDR được FPT IS xây dựng trong khoảng 1 năm và liên tục phát triển các tính năng mới nhằm đem đến một giải pháp toàn diện nhất cho khách hàng. Đến nay, giải pháp đã ra mắt thị trường được hơn 2 năm và mang lại nhiều lợi ích cho hàng triệu người. Khách hàng chỉ mất 1 phút đăng ký và FPT IS cam kết chỉ sau 2 giờ sẽ triển khai thành công giải pháp.

*8.8. Đánh giá về việc tác động tốt tới môi trường*

FPT.EagleEye MDR giúp doanh nghiệp loại bỏ hàng loạt quy trình khắc phục sự cố; nhân viên có thể quản lý, giám sát ATTT và xử lý sự cố từ xa, không phải đi lại nhiều, từ đó giảm thiểu các tác động tiêu cực đến môi trường.

*8.9. Đánh giá về việc tác động tốt tới văn hóa*

FPT.EagleEye MDR giúp doanh nghiệp đảm bảo ATTT và vận hành liên tục, không đứt quãng, nâng cao trải nghiệm người dùng cũng như văn hóa của doanh nghiệp. Bên cạnh đó, các cán bộ quản trị cũng thường xuyên được cập nhật các thông tin, quy định, xu hướng về bảo mật, từ đó có cái nhìn sâu rộng hơn về lĩnh vực này để ứng phó được với mọi sự cố.

**9. Khả năng mở rộng ra thị trường quốc tế**

*9.1. Thị phần và tiềm năng thị trường quốc tế*

Đối với sản phẩm FPT.EagleEye MDR, FPT IS đang đẩy mạnh phát triển thị trường trong nước, song song với việc lập các kế hoạch mang sản phẩm ra thị trường nước ngoài. Với xu hướng chuyển dịch ATTT sang giám sát và phản ứng sự cố sớm, thị trường này được ước tính trị giá hơn 72 tỷ USD vào năm 2021 và sẽ ngày càng tiềm năng hơn trong các năm tới.

*9.2. Mô hình, chiến lược kinh doanh tại thị trường quốc tế*

Trong thời gian tới, FPT IS dự kiến hợp tác cùng các đối tác chiến lược của Tập đoàn FPT trên khắp thế giới để phân phối các sản phẩm ra thị trường quốc tế. Đến năm 2025, sản phẩm được kỳ vọng có mặt tại 5 quốc gia lớn như Mỹ, Đức, Nhật, Pháp, Nhật.

**10. Các thông tin thêm về sản phẩm**

Chỉ sau một thời gian ngắn ra mắt, uy tín và chất lượng của phần mềm FPT.EagleEye MDR đã liên tiếp được củng cố thông qua một loạt giải thưởng uy tín như:

- Danh hiệu Dịch vụ An toàn thông tin tiêu biểu 2018 trao bởi Hiệp hội An toàn thông tin Việt Nam – VNISA

- Danh hiệu Sao Khuê năm 2019, hạng mục Các dịch vụ CNTT tiêu biểu, lĩnh vực An toàn thông tin trao bởi Hiệp hội Phần mềm và Dịch vụ CNTT Việt Nam (VINASA)
- Giải thưởng Chuyển đổi số Việt Nam – Vietnam Digital Awards 2019, hạng mục Sản phẩm, dịch vụ, giải pháp công nghệ số tiêu biểu trao bởi Hội Truyền thông số Việt Nam

Chúng tôi cam đoan mọi thông tin cung cấp ở trên và tài liệu gửi kèm là trung thực, đúng sự thật và hoàn toàn chịu trách nhiệm trước pháp luật về tính chính xác của các thông tin này./.

*Hà Nội, ngày 19 tháng 10 năm 2020*

**Đại diện pháp luật của**
**tổ chức/doanh nghiệp**

M.S.D.N: 0104128565 - C.T.T.N.H.H - CÔNG TY TNHH HỆ THỐNG THÔNG TIN FPT - Q. NAM TỪ LIÊM - T.P HÀ NỘI

**Dương Dũng Triều**
**Chủ tịch hội đồng thành viên**