TẬP ĐOÀN BƯU CHÍNH VIỄN THÔNG VIỆT NAM

CÔNG TY CÔNG NGHỆ THÔNG TIN VNPT

GIẢI PHÁP PHÁT HIỆN VÀ ỨNG CỨU SỰ CỐ ĐIỂM CUỐI VNPT SMART IR

(VNPT INCIDENT RESPONSE)

1 Tổng quan VNPT Smart IR

1.1 Giới thiệu

VNPT Smart IR là giải pháp phát hiện và ứng cứu sự cố điểm cuối toàn diện cho phép bảo vệ máy chủ, máy trạm chống các loại virus, mã độc; hỗ trợ truy vấn, điều tra nguyên nhân và ứng cứu kịp thời khi có sự cố về an toàn thông tin; giám sát việc cài đặt phần mềm trái phép và giám sát việc tuân thủ các chính sách bảo mật của các tổ chức, doanh nghiệp, phát hiện, cảnh báo và hỗ trợ cập nhật kịp thời các lỗ hổng đã biết.

1.2 Chứng nhận, giải thưởng

- Giải thưởng chìa khóa vàng 2022 cho sản phẩm ATTT chất lượng cao xuất sắc

https://vsa.vnisa.org.vn/

- Chứng chỉ VB100 về chứng chỉ tiêu chuẩn chất lượng của các phần mềm chống mã độc trên toàn cầu

https://www.virusbulletin.com/testing/vb100

2 Các thách thức đặt ra cho khách hàng

2.1 Phát hiện những kẻ tấn công, mối đe dọa bên trong tổ chức

Hiện nay, đối với nhiều cơ quan tổ chức lớn ở Việt Nam, vấn đề tìm kiếm và phát hiện các mối đe dọa, kẻ tấn công bên trong hệ thống là bài toán không hề đơn giản. Có nhiều lý do cho việc này như:

- Hạ tầng mạng trước khi trang bị các giải pháp bảo mật, đã bị kẻ tấn công khai thác.
- Quy trình chưa chặt chẽ, tạo điều kiện để kẻ tấn công xâm nhập từ trước đó.
- Nhân viên, cán bộ nào đó vì vô tình hay cố ý gây hại cho tổ chức.
- Nguy cơ rủi ro đến từ 1 số đối tác đến làm việc.

- Kẻ tấn công ngày càng sử dụng nhiều phương pháp tinh vi và hiện đại, nhằm che giấu hành vi của mình.

2.2 Số lượng nhân sự ATTT còn mỏng

Hiện nay, vấn đề nhân sự trong lĩnh vực ATTT còn khá mỏng, không đáp ứng được khối lượng và số lượng công việc đảm nhiệm. Điều này đến từ nhiều nguyên nhân:

- Vấn đề đào tạo về ATTT ở Việt Nam gần đây mới được chú trọng nhiều.
- Các nhân sự ATTT thường "nhảy việc" sang những đơn vị có chế độ tốt hơn.

2.3 Máy tính khách hàng phải cài đặt rất nhiều phần mềm riêng rẽ

Để xử lý các bài toán bảo mật trên thiết bị đầu cuối hiện nay, khách hàng phải trang bị rất nhiều phần mềm riêng rẽ, như: Endpoint Protection Platform (EPP - Antivirus/Antimalware 2.0), Endpoint Detection & Response (EDR - Phân tích hành vi), Endpoint Forensic (EF - Điều tra sự cố), Vulnerable Management (VM - Rà quét phần mềm chưa được cập nhật),…Điều này dẫn đến sự khó chịu cho người sử dụng, gây tiêu tốn tài nguyên máy trạm, và đặc biệt là gây rất nhiều khó khăn cho người quản trị trong việc điều tra và xử lý các vấn đề một cách đầy đủ và toàn diện.

3 Giải pháp đề xuất

3.1 Chức năng nhiệm vụ

VNPT Smart IR giúp các chuyên viên an toàn thông tin giám sát, phát hiện và ngăn chặn kịp thời các cuộc tấn công bằng mã độc bao gồm cả mã độc đã biết (signature) và chưa biết (hành vi). Ngoài ra, giải pháp cũng cho phép nhận diện và phát hiện các mối nguy hiểm trên thiết bị cuối và quản lý chính sách của thiết bị.

3.1.1 Nhóm chức năng giám sát bất thường

Thu thập thông tin, giám sát sự kiện an toàn thông tin

- Liệt kê process trên máy tính, phát hiện kịp thời các process bất thường
- Liệt kê những kết nối trong mạng, phát hiện những kết nối bất thường
- Liệt kê Autostart, phát hiện autostart bất thường
- Giám sát việc tạo file trên hệ thống

Phân tích, cảnh báo

- Phát hiện những hành vi bất thường trên máy tính người dùng
- Cho phép tìm kiếm, điều tra log event của toàn bộ các thiết bị đầu cuối trong tổ chức
- Phân tích các tiến trình đang chạy từ xa trên máy mục tiêu
- Đưa ra cảnh báo đối với những bất thường trong toàn mạng của tổ chức đến quản trị viên
- Cho phép điều tra phản ứng trên một giao diện duy nhất

Xử lý sự cố

- Hỗ trợ cô lập tạm thời các máy phục vụ điều tra tránh lây lan diện rộng.
- Hỗ trợ tạo kịch bản phản ứng và deploy trên diện rộng
- Cho phép thực thi lệnh từ xa tới thiết bị mục tiêu phục vụ điều tra

3.1.2 Nhóm chức năng phòng chống, diệt virus

- Phát hiện, cách ly, xóa bỏ các loại mã độc như: virus, mã độc mã hóa tống tiền (ransomware), lừa đảo (phishing), thư rác
- Kiểm soát, bảo vệ máy chủ, máy trạm khỏi các phần mềm có nguồn gốc không rõ ràng
- Bảo vệ chủ động theo thời gian thực (Real-time Protection)
- Tự động quét lọc khi phát hiện có thay đổi file, thư mục
- Quét virus theo lịch hoặc theo sự chủ động của người dùng

- Có thể phân tích sâu và cảnh báo, sử dụng công nghệ Machine learning kết hợp cơ sở dữ liệu về mã độc có dấu hiệu để phân tích hành vi, ngăn chặn hành vi bất thường trên thiết bị cuối
- Cập nhật liên tục thông tin về cơ sở dữ liệu CVE, CWE và các nguồn Threat Intelligent uy tín giúp cảnh báo sớm các lỗ hổng có thể tồn tại trên thiết bị cuối.

3.1.3 Nhóm chức năng quản lý chính sách

- Thêm/bớt/cấu hình chính sách theo nhu cầu của tổ chức, đơn vị
- Chọn/Áp dụng những chính sách cho tổ chức, đơn vị trong từng thời điểm
- Đánh giá, kiểm soát việc tuân thủ chính sách an toàn thông tin của tổ chức, đơn vị tại từng thiết bị cuối
- Kiểm soát việc kết nối, sử dụng các thiết bị lưu trữ ngoài, USB, thẻ nhớ trên các thiết bị đầu cuối
- Kiểm soát việc cài đặt phần mềm tại thiết bị cuối tránh việc cài đặt phần mềm sai mục đích gây nguy cơ mất ATTT
- Kiểm soát định danh thiết bị, nhận biết thông tin các thiết bị truy cập vào hệ thống bao gồm vendor, OS và phân loại theo chức năng thiết bị
- Cho phép kiểm soát việc kết nối vào mạng đối với các thiết bị vi phạm tuân thủ chính sách

3.1.4 Nhóm chức năng thống kê, báo cáo

Thống kê:

- Thống kê phần mềm cài đặt tại máy người dùng
- Thống kê các sự kiện bất thường được phát hiện
- Thống kê thông tin về các loại mã độc được phát hiện trong mạng lưới

Báo cáo

- Báo cáo về số lượng mã độc theo từng đơn vị hoặc nhóm tự định nghĩa
- Báo cáo về mức độ tuân thủ chính sách an toàn thông tin theo từng đơn vị hoặc nhóm tự định nghĩa
- Báo cáo về số lượng thiết bị đầu cuối được cài đặt, hoạt động theo từng đơn vị hoặc nhóm tự định nghĩa
- Trạng thái cập nhật giải pháp phòng, chống mã độc trên các máy trạm: danh sách các máy trạm không cập nhật trong một khoảng thời gian nhất định

Cho phép đặt lịch báo cáo, gửi thông tin cảnh báo

3.1.5 Nhóm chức năng quản trị người dùng, thiết bị cuối

Quản lý tài khoản quản trị:

- Hỗ trợ tạo/ xóa/ kích hoạt/ bỏ kích hoạt tài khoản người dùng
- Hỗ trợ phân quyền theo các role khác nhau
- Cho phép quản lý danh sách tài khoản quản trị theo đơn vị hoặc theo vai trò
- Cho phép tìm kiếm người dùng

Quản lý thiết bị cuối:

- Cho phép tạo nhóm và phân loại thiết bị cuối theo các nhóm tự định nghĩa
- Cho phép quản lý danh sách thiết bị cuối theo từng đơn vị hoặc nhóm tự định nghĩa , trạng thái hoạt động của các thiết bị cuối trong mạng
- Cho phép tìm kiếm thiết bị cuối theo các tiêu chí khác nhau
- Cho phép in hoặc kết xuất ra file excel danh sách thiết bị cuối theo từng đơn vị hoặc theo tiêu chí tìm kiếm
- Cho phép cấu hình agent từ xa theo từng nhu cầu khác nhau
- Cho phép cấu hình chính sách agent theo từng nhóm khác nhau

3.1.5.1 Nhóm chức năng cập nhật bản vá

- Thống kê những lỗ hổng nghiêm trọng có thể trở thành mục tiêu tấn công
- Thống kê về các loại hệ điều hành, phần mềm bản quyền, phần mềm không bản quyền trong tổ chức
- Kiểm soát các bản vá bảo mật đã cài đặt trên thiết bị cuối, đưa ra khuyến nghị cập nhật các bản vá từ các nguồn uy tín

3.2 Khả năng tích hợp

VNPT Smart IR có khả năng tích hợp với các hệ thống giám sát sự kiện an toàn thông tin SIEM

Có khả năng cài đặt trên nhiều loại máy chủ bao gồm vật lý và các lớp ảo hóa khác nhau như VMWare, KVM

Có khả năng tùy biến cao hoạt động được trên cả các môi trường kết nối phức tạp như môi trường VDXP, NDXP của hệ thống CSDLQGvDC

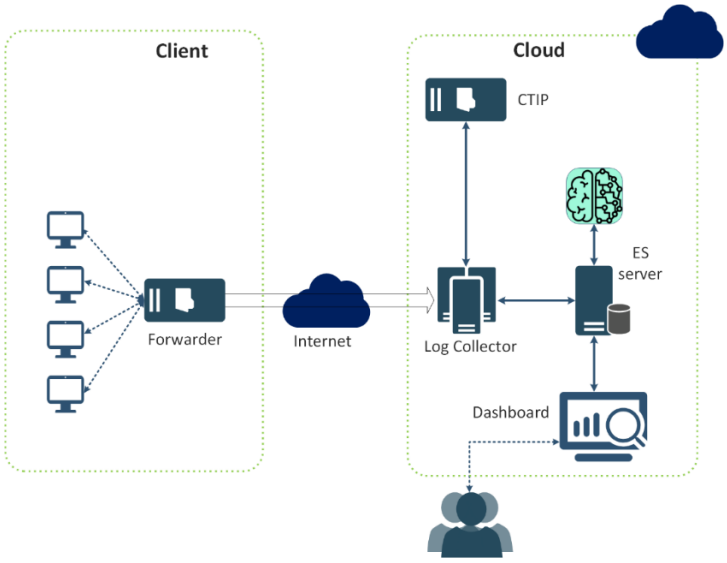
4 Mô hình triển khai

4.1 Các mô hình triển khai

VNPT Smart IR có thể triển khai được dưới 02 mô hình Cloud và On-premise

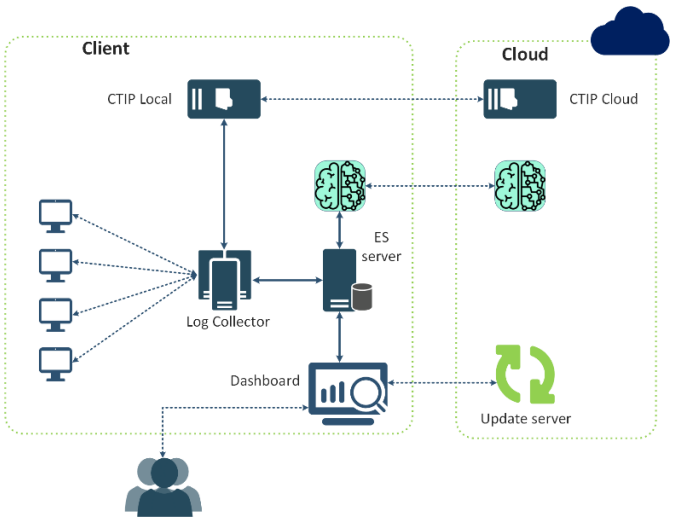
Mô hình Cloud có ưu điểm:

- Không cần cài đặt máy chủ riêng
- Triển khai nhanh hơn
- Phù hợp với khách hàng lẻ hoặc doanh nghiệp vừa và nhỏ



Mô hình On-premise có ưu điểm:

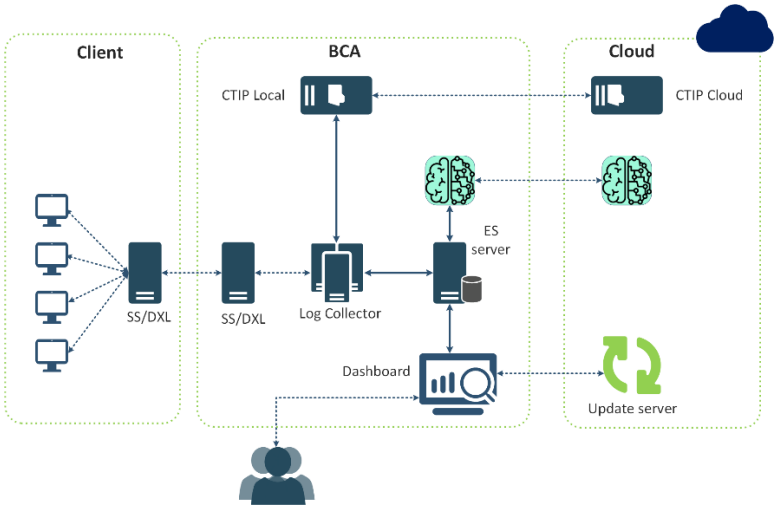
- Khách hàng có thể toàn quyền kiểm soát hệ thống
- Triển khai linh hoạt hơn, may đo theo yêu cầu của khách hàng
- Phù hợp với khách hàng tổ chức, doanh nghiệp lớn hoặc có yêu cầu nghiêm ngặt hoặc đặc thù về kết nối



4.2 Khả năng tùy biên trên môi trường có điều kiện kết nối đặc thù (NDXP, VDXP)

Trong môi trường kết nối của hệ thống CSDLQGvDC, dữ liệu được truyền trên hạ tầng kết nối đặc thù NDXP và VDXP, tất cả dữ liệu truyền nhận đều được thực hiện bằng API thông qua DXL node hoặc SS Server, không có kết nối trực tiếp từ client lên server, do đó các giải pháp khác không cung cấp tùy biến kết nối không thể đảm bảo việc truyền nhận dữ liệu.

Giải pháp VNPT Smart IR với khả năng tùy biến cao, các kết nối đều sử dụng API có thể đáp ứng các kênh kết nối này.



5 Thông tin nguồn gốc, xuất xứ:

STT	Hạng mục	Hãng sản xuất	License	Tính năng
I	**Smart IR On-Premise:**	**VNPT**		

I.1	Kiểm soát truy cập (Access Control)	VNPT	OF-AC-59-STD	Nhóm chức năng giám sát bất thường (mục 3.1.1) Nhóm chức năng phòng chống, diệt virus (mục 3.1.2) Nhóm chức năng quản lý chính sách (mục 3.1.3) Nhóm chức năng thống kê, báo cáo (mục 3.1.4)
I.2	Cập nhật bản vá (Patch Management)	VNPT	OF-PM-59-STD	Nhóm chức năng cập nhật bản vá (mục 3.1.6)
I.3	Quản lý chính sách (Group Policy)	VNPT	OF-PO-39-STD	Nhóm chức năng quản lý chính sách (mục 3.1.3)
I.4	Diệt virus (Antivirus)	VNPT	OF-AV-25-STD	Nhóm chức năng phòng chống, diệt virus (mục 3.1.2)