HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN CÔNG TÙNG

NGHIÊN CỨU GIẢI PHÁP AN TOÀN THÔNG TIN VÀ ỨNG DỤNG TẠI VIỆN KHCN SÁNG TẠO VIỆT NAM

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI – NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. NGUYỄN TẤT THẮNG

Phản biện 1: PGS.TS. Nguyễn Đức Dũng

Phản biện 2: TS. Ngô Xuân Bách

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 9 giờ 20 ngày 09 tháng 01 năm 2021

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

MỞ ĐẦU

1. Lý do chọn đề tài

Trong những năm gần đây, công nghệ thông tin (CNTT) là một trong những lĩnh vực phát triển nhanh chóng, toàn diện và được ứng dụng rộng rãi trong tất cả các lĩnh vực đời sống, xã hội. Khi các giá trị từ hệ thống CNTT mang lại ngày càng lớn, các nguy cơ bị hacker tấn công ngày càng cao.

Nhiều giải pháp bảo đảm an toàn thông tin cho hệ thống CNTT đã được quan tâm nghiên cứu và triển khai. Tuy nhiên, thực tế, vẫn thường xuyên có các hệ thống bị tấn công, bị đánh cắp thông tin, phá hoại gây ra những hậu quả vô cùng nghiêm trọng đối với nhiều doanh nghiệp, cơ quan nhà nước cũng như toàn xã hội.

Trước những thực trạng cấp thiết đó, học viên xin chọn đề tài ***"Nghiên cứu giải pháp an toàn thông tin và ứng dụng tại Viện KHCN Sáng tạo Việt Nam"*** làm đề tài luận văn nhằm nghiên cứu, đưa ra các giải pháp giám sát an toàn thông tin trong giai đoạn hiện nay.

2. Tổng quan về đề tài nghiên cứu

Luận văn nghiên cứu giải pháp giám sát an toàn thông tin dựa trên SIEM (Security Information and Event Management) là hệ thống được thiết kế nhằm thu thập và phân tích nhật ký, các sự kiện an toàn thông tin từ các thiết bị đầu cuối và được lưu trữ tập trung. Hệ thống SIEM cho phép phân tích tập trung và báo cáo về các sự kiện an toàn thông tin của tổ chức, phát hiện thông qua các bộ luật tương quan.

SIEM có thể phục vụ rất nhiều công việc như: Quản lý tập trung, giám sát an thông tin mạng, cải thiện hiệu quả trong phục sự cố. Trong Luận văn sẽ tập trung tìm hiểu, phân tích, nghiên cứu chủ đề chính là giám sát an toàn thông tin.

Giám sát an toàn thông tin là việc sử dụng một hệ thống để liên tục theo dõi một số thông tin, xem xét tình trạng hoạt động của các

thiết bị, dịch vụ hệ thống đó, cảnh báo cho quản trị viên trường hợp mạng không hoạt động hoặc có các sự cố khác (tắc nghẽn, sập,...), hành vi tấn công (dựa trên tập luật đã được cấu hình), hành vi bất thường ...

Các sự kiện diễn ra trong các thiết bị đều được ghi lại trong log. Nhiệm vụ của hệ thống giám sát ATTT là sử dụng Event Collector thu thập log từ Log Source (thành phần có log) và gửi về cơ sở dữ liệu trung tâm. Event Processor phân tích các sự kiện được gửi về và báo cho quản trị viên để có các hành động ứng phó thích hợp.

Giải pháp giám sát an toàn thông tin có khả năng phân tích, cảnh báo thời gian thực các sự cố, nguy cơ mất ATTT đối với hệ thống. Với giải pháp này, hệ thống quản lý sẽ được bảo đảm ATTT ở mức cao hơn.

3. Mục tiêu nghiên cứu của đề tài

Mục tiêu nghiên cứu của luận văn là khảo sát các yêu cầu và giải pháp an toàn thông tin. Để đưa ra giải pháp an toàn thông tin cho Viện KHCN Sáng tạo Việt Nam có khả năng triển khai áp dụng trong thực tế.

4. Đối tượng và phạm vi nghiên cứu

- Đối tượng nghiên cứu: Luận văn nghiên cứu về giải pháp an toàn thông tin và các vấn đề liên quan tới giải pháp an toàn thông tin. Trong đó, luận văn tập trung vào nghiên cứu giải pháp Splunk trong việc xây dựng hệ thống giám sát, đảm bảo an toàn thông tin. Cách thức chuẩn hóa sự kiện an toàn thông tin và đưa ra cảnh báo

- Phạm vi nghiên cứu: Luận văn nghiên cứu một cách tổng quan về giải pháp an toàn thông tin; đặc điểm, ưu điểm và nhược điểm của hệ thống. Nghiên cứu các giải pháp xây dựng hệ thống; các vấn đề an toàn thông tin tại Viện KHCN Sáng tạo Việt Nam và các giải pháp đảm bảo an toàn thông tin hiện nay.

5. Phương pháp nghiên cứu của đề tài

- ***Về mặt lý thuyết:*** Thu thập, khảo sát, phân tích các tài liệu liên quan đến giải pháp toàn thông tin.

- ***Về mặt thực nghiệm:*** Khảo sát hệ thống CNTT của Viện KHCN Sáng tạo Việt Nam và ứng dụng giải pháp an toàn thông tin tại Viện.

6. Bố cục luận văn

Luận văn được trình bày trong 3 chương:

Chương 1 của luận văn sẽ khảo sát tổng quan về tình hình an toàn thông tin và các mối đe dọa an toàn thông tin.

Chương 2 của luận văn tập trung nghiên cứu các giải pháp an toàn thông tin, từ đó sẽ đưa ra giải pháp an toàn thông tin

Chương 3 của luận văn tập trung nghiên cứu về hệ thống mạng Viện KHCN Sáng tạo và đề xuất ứng dụng giải pháp an toàn thông tin thông qua nghiên cứu từ chương 2 cho hệ thống CNTT của Viện KHCN Sáng tạo Việt Nam.

CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1 Tổng quan chung về tình hình an toàn thông tin

Ngày nay ở Việt Nam, các tổ chức, doanh nghiệp đều xây dựng, vận hành một hệ thống mạng của riêng mình. Hệ thống mạng giúp gia tăng khả năng làm việc giữa các nhân viên, các đơn vị với nhau, gia tăng hiệu suất và giúp cơ quan, tổ chức hoạt động một cách hiệu quả. Tuy nhiên, khi vận hành hệ thống mạng, có rất nhiều vấn đề có thể phát sinh làm ảnh hưởng đến khả năng hoạt động của hệ thống. Hệ thống càng lớn, các hoạt động diễn ra bên trong hệ thống phức tạp, các vấn đề nảy sinh cũng càng tăng theo. Do đó, hệ thống mạng luôn cần có một hệ thống giám sát an toàn thông tin bao quát toàn bộ các hoạt động, các vấn đề, có thể túc trực, quản lý, dễ dàng phát hiện các sự cố xảy ra bên trong hệ thống, thông qua đó quản trị viên sẽ đưa ra các biện pháp ứng phó.

Từ tình hình trên, việc xây dựng hệ thống giám sát an toàn thông tin để quản lý hệ thống mạng đang ngày càng trở nên cấp thiết hơn bao giờ hết.

1.2. Các mối đe dọa an toàn thông tin và phương thức tấn công mạng

1.2.1 Các mối đe dọa an toàn thông tin

- Mối đe dọa không có cấu trúc:

Là những hành vi xâm nhập mạng trái phép một cách đơn lẻ, không có tổ chức. Những cuộc tấn công này có thể do sở thích cá nhân, nhưng đôi khi có nhiều cuộc tấn công có ý đồ xấu để lấy cắp thông tin và có ảnh hưởng nghiêm trọng đến hệ thống thậm chí có một đoạn mã độc là có thể phá hủy chức năng của mạng nội bộ.

- Mối đe dọa có cấu trúc:

Là những cách thức tấn công hoặc xâm nhập hệ thống mạng trái phép, có động cơ và kỹ thuật cao. Kẻ tấn công thường có kỹ năng

phát triển ứng dụng và sử dụng các kỹ thuật phức tạp nhằm xâm nhập vào mục tiêu có chủ đích. Các cuộc tấn công như vậy rất có thể gây hậu quả nghiêm trọng, có thể gây nên sự phá hủy cho toàn hệ thống mạng của doanh nghiệp hoặc các tổ chức.

- Mối đe dọa từ bên ngoài:

Là những cuộc tấn công được tạo ra khi Hacker không có một quyền nào kiểm soát trong hệ thống. Người dùng có thể bị tấn công trên toàn thế giới thông qua mạng Internet. Những mối đe dọa từ bên ngoài này thường là mối đe dọa nguy hiểm, các chủ doanh nghiệp sở hữu mạng LAN thường phải bỏ rất nhiều tiền và thời gian để bảo vệ hệ thống.

- Mối đe dọa từ bên trong hệ thống:

Là kiểu tấn công được thực hiện từ một cá nhân hoặc một tổ chức có một số quyền truy cập vào hệ thống mạng nội bộ của tổ chức doanh nghiệp. Những cách tấn công này thường từ bên trong, được thực hiện từ một vị trí tin cậy trong mạng nội bộ, rất khó phòng chống bởi đôi khi chính là các nhân viên truy cập mạng rồi tấn công. Nhưng nếu có hệ thống giám sát và phân tích sẽ rất dễ bắt được các đối tượng này.

1.2.2 Những cách thức tấn công hệ thống mạng máy tính

- Cách thức lấy cắp thông tin bằng kiểu tấn công Packet Sniffers.
- Cách thức lấy cắp mật khẩu bằng Password attack.
- Cách thức tấn công bằng Mail Relay.
- Cách thức tấn công tầng ứng dụng.
- Cách thức tấn công bằng Virus và phần mềm Trojan Horse.

1.3 Giới thiệu tổng quan về hệ thống SIEM

1.3.1 Tổng quan về SIEM

SIEM là một hệ thống giám sát an ninh mạng tân tiến nhất hiện nay hoạt động bằng cách thu thập, phân tích, đánh giá nhật ký từ mọi thiết bị trong hệ thống…Từ đó cho phép cho chúng ta phân tích một lượng lớn dữ liệu để phát hiện các cuộc tấn công ẩn dấu đằng sau để các đơn vị, cơ quan có được cái nhìn toàn cảnh về các sự kiện an ninh mạng.

1.3.2. Chức năng chính của SIEM

- Quản lý tập trung: SIEM giúp tập hợp các dữ liệu thông qua giải pháp nhật ký tập trung. Thiết bị đầu cuối của hệ thống thường ghi lại và truyền dữ liệu nhật ký về máy chủ SIEM. Máy chủ SIEM nhận nhật ký từ nhiều máy và tiến hành thống kê, phân tích và tạo ra một báo cáo duy nhất.

- Giám sát an toàn mạng: Hệ thống sẽ phát hiện được các sự cố mà các thiết bị thông thường không phát hiện được. Cùng với đó nó có thể cho thấy sự tương quan giữa các thiết bị với nhau.

- Giúp ích cho việc xử lý sự cố: SIEM có giao diện đơn giản để có thể xem tất cả nhật ký từ nhiều thiết bị một cách thuận tiện để khắc phục sự cố một cách dễ dàng và hiệu quả.

1.3.3. Các thành phần của hệ thống

Việc xây dựng hệ thống SIEM có thể tiến hành theo nhiều cách, thường gồm 3 thành phần chính như sau.

- Thu thập nhật ký ATTT: Phần thu thập ATTT gồm các giao diện có chức năng thu thập nhật ký từ mọi thiết bị. Sau khi tập hợp nó sẽ gửi toàn bộ nhật ký về thành phần phân tích.

- Phân tích và lưu trữ Log: các Log được tập trung về và tiến hành phân tích so sánh. Sau khi thực hiện thuật toán phân tích hệ thống

sẽ đưa ra các cảnh báo cần thiết. Thậm chí còn có thể phân tích dữ liệu trong quá khứ.

- Quản trị tập trung: cung cấp giao diện quản lý tập trung cho toàn bộ hệ thống giám sát an ninh. Hệ thống có sẵn hàng ngàn mẫu báo cáo để có thể sử dụng ngay.

1.3.4 Kiến trúc, cách thức hoạt động của hệ thống SIEM

- Thiết bị nguồn trong kiến trúc SIEM

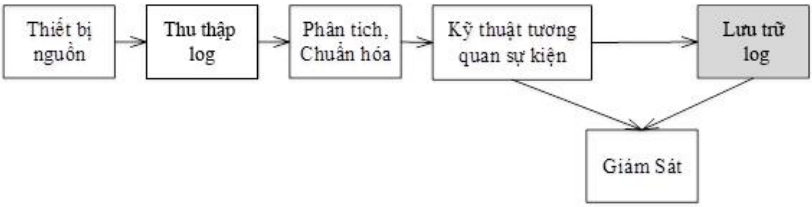
- Bộ phận thu thập log

- Bộ phận phân tích và chuẩn hóa log

- Bộ phận kỹ thuật tương quan sự kiện

- Bộ phận lưu trữ log

- Bộ phận giám sát



Hình 1.3: Kiến trúc hoạt động của SIEM

1.4. Kết luận chung chương một

Trong chương 1, luận văn đã nghiên cứu tổng quan chung về an ninh mạng, giám sát tập trung và các yêu cầu giám sát hệ thống mạng, cũng như các vấn đề liên quan đến hệ thống SIEM. Qua đó ta thấy cấu trúc hoạt động rất phức tạp bởi có nhiều bộ phận hoạt động chuyên biệt. Nhưng cũng tạo ra được sức mạnh tổng hợp và phân tích log rất tốt, linh hoạt, hỗ trợ tối đa cho việc quản trị hệ thống.

Chương tiếp theo sẽ trình bày các giải pháp và cách thức áp dụng SIEM một cách hiệu quả.

CHƯƠNG 2. NGHIÊN CỨU GIẢI PHÁP AN TOÀN THÔNG TIN

2.1 Các giải pháp giám sát an toàn thông tin hiện nay

2.1.1 Giải pháp HP ArcSight ESM

Là một sản phẩm trong bộ sản phẩm ArcSight của HP, hệ thống rất hiệu quả về trong việc quản lý và vận hành phân tích log và có thể xử lý lượng log lớn đổ về cùng hỗ trợ nhiều định dạng lấy log khác nhau. Trong hệ thống cho phép phản hồi nhanh chóng và nhận dạng rất nhanh các cuộc tấn công từ bên ngoài hệ thống mạng hoặc bên trong.

Giải pháp HP ArcSight ESM có ưu điểm là phân tích dữ liệu toàn diện; cảnh báo tấn công hoặc lỗi theo thời gian thực; có thể tìm kiếm và tạo báo cáo tổng hợp. Nhưng nhược điểm là: hiệu năng xử lý phụ thuộc vào thiết bị, muốn nâng cấp phải mua thiết bị mới; chi phí đầu tư tốn kém, đắt đỏ.

2.1.2 Giải pháp IBM Security Qradar

Là giải phép quản lý sự kiện và bảo mật thông tin thiết kế để cung cấp cho các nhóm bảo mật khả năng hiển thị tập trung vào dữ liệu bảo mật toàn doanh nghiệp và hiểu biết sâu sắc về các mối đe dọa ưu tiên cao nhất.

Hệ thống gồm các đặc điểm sau:

- Tự động hóa thông tin bảo mật để nhanh chóng phát hiện các mối đe dọa

- Phát hiện hoạt động của mạng, người dùng và ứng dụng bất thường

- Quản lý việc tuân thủ với quy tắc, nội dung và báo cáo được xây dựng trước

- Dễ dàng thay đổi, mở rộng quy mô

2.1.3 Giải pháp Mcafee ESM

Sản phẩm này có tính năng: thu thập các bản ghi trên một số lượng lớn thiết bị và tích hợp với danh bạ hoạt động; kiểm soát truy cập và tài khoản người dùng dễ dàng giới hạn người dùng chỉ có quyền truy cập những gì họ thực sự cần xem; tính năng phân tích tương quan nâng cao, tạo ra mối tương quan giữa các nguồn khác nhau và tìm ra yếu tố ngoại lai nhanh nhất.

ESM cực kỳ hữu ích cho việc theo dõi nhanh chóng, dễ dàng các sự kiện bảo mật và vi phạm chính sách, là một sản phẩm hữu ích tuy nhiên giá thành tương đối cao (đắt gần gấp 10 lần giá của sản phẩm SIEM) nhưng nếu có điều kiện mua thì đây là sản phẩm đáng đầu tư.

2.1.4 Giải pháp MARS của Cisco

Giải pháp của Cisco cho phép các doanh nghiệp tăng tốc và tối đa hóa hiệu quả trong khi duy trì an ninh, tầm nhìn và tuân thủ quy định.

Nhược điểm của dòng sản phẩm này là đi theo thiết bị phần cứng, không tùy chỉnh và cấu hình theo yêu cầu của doanh nghiệp được mà phải liên lạc với hãng để chỉnh trên dòng thiết bị cứng.

2.1.5 Giải pháp AlienVault OSSIM

Là một sản phẩm SIEM mã nguồn mở của AlienVault OSSIM đã được tích hợp một số công cụ bảo mật mạnh mẽ như Snort, ntop, OpenVAS,P0f, PADs, arpwatch, OSSEC,Osiris, Nagios, OCS, và Kismet.

2.1.6 Giải pháp Splunk

Splunk là một hệ thống giám dựa trên việc phân tích log, nó thực hiện các công việc tìm kiếm log, phân tích và giám sát lượng dữ liệu lớn của log sinh ra từ những dịch vụ đang chạy, hạ tầng mạng. Hệ thống Splunk được tạo ra dựa trên nền tảng Lucene và MongoDB, ngoài ra có thể quản lý trên nền giao diện web trực quan.

*** Lợi thế của Splunk so với các giải pháp SIEM khác**

- Linh hoạt mềm dẻo khi sử dụng: Splunk có khả năng mở rộng và linh hoạt từ bất kỳ nguồn dữ liệu, các ứng dụng tùy chỉnh và cơ sở dữ liệu.

- Điều tra theo thời gian thực: Splunk cho phép bạn xem thông tin thời gian thực từ an ninh và thiết bị mạng, hệ điều hành, cơ sở dữ liệu và các ứng dụng, trên một thời gian cho phép các đội an ninh để nhanh chóng phát hiện và hiểu được ý nghĩa end-to -end của một sự kiện an ninh. Với khả năng phát hiện từng hành vi bất hợp phát nhỏ nhất, Splunk sẽ giúp phát hiện những cuộc tấn công tinh vi nhằm vào hệ thống một cách nhanh chóng và hiệu quả nhất.

- Liên kết thông tin theo thời gian thực và cảnh báo: Tương quan của thông tin từ bộ dữ liệu khác nhau có thể cung cấp cái nhìn sâu sắc thêm và bối cảnh. Splunk có thể liên kết với tất cả các thông tin dữ liệu từ mọi nguồn trên hệ thống một cách nhanh chóng và chính xác theo thời gian thực.

- Splunk là phần mềm mã nguồn mở, có bản không tính phí nên không tốn kém khi triển khai.

- Giải quyết được hầu hết các bài toán trong giám sát hệ thống mạng: giám sát hạ tầng, giám sát dịch vụ, giám sát an ninh, giám sát người dùng... Đây là đặc điểm nổi bật của Splunk so với các giải pháp khác.

2.2. Lựa chọn giải pháp Splunk

2.2.1. Giới thiệu tổng quan về giải pháp Splunk

Splunk là phần mềm cho phép tìm kiếm và duyệt logs và các dữ liệu trong thời gian thực. Người dùng có thể ngay lập tức phát hiện ra sự cố ở bất cứ ứng dụng nào, hoặc ở các máy chủ và thiết bị; cảnh báo các nguy cơ tiềm ẩn và báo cáo các hoạt động của các dịch vụ và thành phần khác nhau trong mạng.

2.2.2 Tính năng của giải pháp Splunk

- Quản lý ứng dụng của Splunk: Khắc phục sự cố vấn đề một cách nhanh chóng, giảm chi phí và giảm thời gian để điều tra và khắc phục sự cố tới 70%. Đồng thời, giám sát toàn bộ môi trường ứng dụng trong thời gian thực để ngăn chặn các vấn đề ảnh hưởng tới người dùng, giữ lại log từ các sự kiện định kỳ để ngăn ngừa mất mát.

Cho phép truy vết và giám sát được hoạt động của toàn bộ ứng dụng thông qua các tầng của kiến trúc phân tán và từ nhiều nguồn dữ liệu. Đồng thời phát hiện các bất thường hoặc các vấn đề trong hoạt động, thời gian đáp ứng và chủ động giải quyết chúng trước khi nó ảnh hưởng tới người dùng, ứng dụng.

- Quản lý các hoạt động công nghệ thông tin: Splunk cung cấp một cách tiếp cận tốt hơn mà không cần phải phân tích cú pháp hay tùy chỉnh nó. Splunk thu thập và lập indexes chứa tất cả dữ liệu được tạo ra bởi hệ thống CNTT (hệ thống mạng, server, OS, ảo hóa, v.v.).

Nó hoạt động với bất kỳ dữ liệu mà máy tạo ra, bao gồm log, file cấu hình, số liệu hiệu suất, SNMP trap và các ứng dụng log tùy chỉnh.

- An ninh trong lĩnh vực CNTT:

+ Quản lý log: Phần mềm Splunk giúp cải thiện vấn đề phân tích dữ liệu log để quản lý tốt hơn. Nó tự động index dữ liệu, bất kể có cấu trúc hay không cấu trúc, cho phép ta nhanh chóng tìm kiếm, báo cáo, chẩn đoán các hoạt động và các vấn đề an ninh một cách ít tốn kém hơn.

+ Ứng dụng Splunk dành cho an ninh: Với ứng dụng an ninh của Splunk ta có thể sử dụng số liệu thống kê trên bất kỳ dữ liệu nào để tìm kiếm các mối đe dọa tiềm ẩn, trong khi vẫn có thể giám sát liên tục các mối đe dọa đã bị phát hiện bởi những sản phẩm an ninh truyền thống.

+ Tính năng xem xét lại các sự kiện đã xảy ra: chỉ cần chọn một khung thời gian sự kiện hoặc nhiều sự kiện đại diện cho những hoạt động đáng ngờ và Splunk sẽ tự động hiển thị một bản tóm tắt mô hình an ninh. Với 1 cú click chuột, ta có thể xem tất cả các dữ liệu thô được đặt ra theo thứ tự thời gian, đưa ra 1 cái nhìn trực tiếp cho đồng nghiệp hoặc tạo ra một tìm kiếm mới để xem các sự kiện đã xuất hiện này có tiếp tục xuất hiện hay không.

+ Phân tích và dự đoán: Nhấp vào điểm đó sẽ hiện các giải pháp để biết được hướng đi tương lai của điểm đó và dự báo giá trị dựa trên mô hình dữ liệu. Chỉ cần chọn kiểu dữ liệu, bất kỳ đối tượng chứa kiểu dữ liệu đó, kiểu hàm trình diễn, thuộc tính và chu kỳ phân tích mà ta muốn tạo. Danh sách các mối đe dọa: Splunk cung cấp dịch vụ out-of-the-box hỗ trợ cho 18 mã nguồn mở đe dọa tới dữ liệu nhằm tăng thêm tính bảo mật cho hệ thống.

2.2.3 Thành phần của Splunk

2.2.3.1 Thành phần thu thập Log của Splunk

Splunk được chia làm 3 thành phần thu thập log:

- Universal forwarder là một streamlined: Nó là phiên bản chuyên dụng của Splunk mà chỉ chứa các thành phần thiết yếu để chuyển dữ liệu từ máy trạm đến máy server.

- Heavy forwarder: Có kích thước nhỏ hơn một Splunk indexer nhưng vẫn giữ được hầu hết các tính năng ngoại trừ việc tìm kiếm các kết quả phân phối.

- Light forwarder: Bị vô hiệu hóa hầu hết các tính năng do đó có kích thước nhỏ, chúng chỉ chuyển các dữ liệu không được phân tích. Từ phiên bản 4.2 công cụ này được thay thế bởi universal forwarder. Những loại dữ liệu được chuyển đó là dữ liệu thô, dữ liệu chưa được phân tích và dữ liệu đã được phân tích. Mỗi công cụ chuyển tiếp dữ liệu cho phép chuyển các loại dữ liệu khác nhau. Với universal

và light forwarder làm việc với dữ liệu thô và dữ liệu chưa được phân tích. Còn heavy forwarder làm việc với dữ liệu thô hoặc dữ liệu đã được phân tích.

2.2.3.2 Thành phần xử lý dữ liệu đầu vào

Nhiều nguồn dữ liệu có thể được lấy từ các file và các thư mục vì vậy ta có thể sử dụng chức năng giám sát các file hoặc thư mục để lấy dữ liệu mà ta quan tâm. Những loại dữ liệu được đưa vào Splunk bao gồm: các sự kiện của mạng, nguồn dữ liệu từ hệ điều hành windows, các nguồn khác.

Quá trình xử lí các sự kiện bao gồm:

- Định dạng bộ kí tự cho dữ liệu đầu vào để phù hợp với định dạng mà Splunk có thể xử lý.
- Quá trình phân mảnh các sự kiện
- Gán nhãn thời gian cho các sự kiện.
- Trích xuất dữ liệu để tạo các trường đánh chỉ mục.

2.2.3.3 Thành phần đánh chỉ mục và lưu trữ

Với công cụ splunk, việc đầu tiên là phải cung cấp dữ liệu, khi đã nhận được dữ liệu, spluk sẽ đánh chỉ số và làm cho chúng sẵn sàng để tìm kiếm. Sau khi đánh index có thể bắt đầu tìm kiếm dữ liệu, hoặc sử dụng nó để tạo báo cáo, biểu đồ, cảnh báo hoặc nhiều công việc khác.

Những loại dữ liệu mà splunk có thể đánh chỉ mục thường là bất kì một loại dữ liệu nào như windows event logs, webserver log, log từ các ứng dụng đang chạy, log từ hệ thống mạng, log giám sát, tin nhắn hàng đợi, tệp tin archive, hoặc bất kì nguồn nào có thể hữu ích.

2.2.3.4 Thành phần cảnh báo

Cảnh báo là một hành động được kích hoạt dựa trên các kết quả của tìm kiếm. Khi tạo một cảnh báo, cần định nghĩa một điều kiện mà kích hoạt cảnh báo đó. Hành động điển hình là gửi email dựa trên

các kết quả tìm kiếm. Ngoài ra cũng có thể chọn các hành động khác như chạy một đoạn mã script hoặc đưa chúng vào trong danh sách các cảnh báo. Với cùng một điều kiện cảnh báo có thể đưa chúng vào nhiều lựa chọn khác nhau như vừa gửi mail vừa chạy script. Để tránh việc gửi cảnh báo quá thường xuyên, ta cũng có thể giới hạn điều kiện cho một cảnh báo. Splunk định nghĩa ba loại cảnh báo là:

- Per result alert: Dựa trên việc tìm kiếm thời gian thực. Điều kiện kích hoạt là bất cứ khi nào việc tìm kiếm trả về một kết quả.
- Scheduled alert. Chạy tìm kiếm theo lịch trình được chỉ định khi tạo cảnh báo. Ta định nghĩa các kết quả của việc tìm kiếm để kích hoạt cảnh báo đó.
- Rolling-window alert. Dựa trên việc tìm kiếm thời gian thực. Điều kiện kích hoạt là tập hợp các kết quả phù hợp của việc tìm kiếm trong một khung thời gian quy định.

2.2.4 Cách thức hoạt động của Splunk

- Mức thấp nhất của kiến trúc Splunk mô tả các phương thức nhập liệu khác nhau được hỗ trợ bởi Splunk.

- Trước khi dữ liệu đến được các bộ phân loại Splunk, nó có thể được phân tích cú pháp hoặc thao tác, có nghĩa là làm sạch dữ liệu có thể được thực hiện nếu cần.

- Một khi dữ liệu được lập chỉ mục trên Splunk, nó sẽ tiến hành đi vào cụ thể để phân tích dữ liệu.

- Splunk hỗ trợ hai loại triển khai: triển khai độc lập và triển khai phân tán. Tùy thuộc vào loại triển khai, tìm kiếm tương ứng được thực hiện. Công cụ Splunk có các thành phần bổ sung khác của quản lý dữ liệu, báo cáo, lên kế hoạch và cảnh báo.

Các khối kiến trúc splunk:

- **Pipeline:** Đây là một quá trình cấu hình đơn luồng duy nhất nằm trong splunk.

- **Bộ vi xử lý:** Chúng là những hàm số có thể tái sử dụng cá nhân hoạt động trên dữ liệu đi qua một đường ống. Đường ống trao đổi dữ liệu giữa họ thông qua một hàng đợi.

2.3 Kết luận chương 2

Trong chương 2, luận văn đã nghiên cứu các giải pháp giám sát an toàn thông tin cần phải đáp ứng và thực hiện. Mỗi một giải pháp sẽ giám sát một thành phần nhất định trong hệ thống mạng. Từ các thành phần cần giám sát, luận văn đã đưa ra giải pháp áp dụng công cụ để giám sát tập trung trong thực tế.

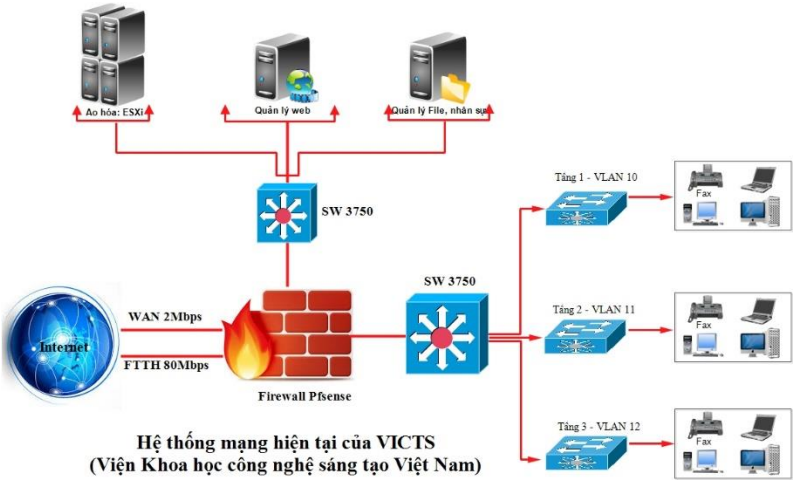
Trong chương 3, luận văn sẽ ứng dụng giải pháp giám sát an toàn thông tin bằng Splunk để xây dựng hệ thống giám sát cho hệ thống mạng Viện Khoa học công nghệ sáng tạo Việt Nam.

CHƯƠNG 3. XÂY DỰNG HỆ THỐNG GIÁM SÁT AN TOÀN THÔNG TIN CHO HỆ THỐNG MẠNG VIỆN KHCN SÁNG TẠI VIỆT NAM

Chương 3 của luận văn sẽ nghiên cứu đề xuất một số giải pháp an toàn thông tin cho hệ thống mạng của Viện Khoa học Công nghệ Sáng tạo Việt Nam. Luận văn cũng thực hiện một số thử nghiệm đánh giá hiệu quả các giải pháp an toàn thông tin. Kết quả thử nghiệm được trình bày trong phần phụ lục.

3.1 Khảo sát mạng nội bộ Viện KHCN Sáng tạo Việt Nam

3.1.1 Chức năng, trang thiết bị và mô hình hiện có của hệ thống mạng Viện KHCN Sáng tạo Việt Nam



Hình 3.1: Mô hình hoạt động của hệ thống mạng tại Viện KHCN Sáng tạo Việt Nam

Hệ thống mạng hiện tại đang sử dụng kiến trúc mô hình mạng Client - Server nhằm chia sẻ dữ liệu từ các máy chủ tới các máy con. Với kiến trúc mạng hình sao ở các tầng, ta sẽ đạt được tốc độ nhanh nhất có thể, kiểm soát tốt khi xảy ra lỗi cũng như mở rộng tùy ý muốn trong toàn hệ thống.

Hạ tầng mạng được phân cấp: máy tính của các phòng ban sẽ kết nối tới các Switch của các tầng, từ Switch các tầng kết nối tới Switch tổng của tòa nhà. Switch tổng kết nối tới Firewall rồi ra ngoài Internet.

Hệ thống máy chủ Web, Mail, File kết nối vào Core Switch. Hệ thống Core Switch đặt sau Firewall nên rất an toàn. Từ Firewall sẽ chia cổng ngoài Internet.

Về trang thiết bị và số lượng người sử dụng:

- Số lượng phòng ban và các đơn vị trực thuộc sử dụng máy tính là 8.

- Tổng số máy tính cho cán bộ nhân viên là 125.

- Số lượng máy chủ là 08 máy đặt tập trung: 02 máy quản lý File Server, 03 máy chủ chạy Website của Viện (https://www.victs.vn), Tạp chí điện tử Đồng Hành Việt (donghanhviet.vn) và các phòng ban, 03 máy chủ chạy ảo hóa trên đó đặt dịch vụ: Email, DHCP và DNS.

- Số lượng Firewall là: 1 Server cài dịch vụ Firewall Pfsense có 4 Card mạng

- Số lượng Switch layer 3 là: 2 Switch 3750

- Số lượng Switch ở các tòa nhà và các tầng là 21 Access Switch và 3 Distribution Swich.

- Số lượng tổng đài nội bộ dùng IP là 1

- Số lượng Camera sử dụng 24 chiếc.

- Số lượng đường truyền là 2 ra ngoài Internet: Viettel (wan) và Fpt (FTTH)

3.1.2 Yêu cầu sử dụng

- Hệ thống phải luôn kết nối được Internet.

- Hệ thống Firewall phải bảo vệ hệ thống máy chủ và người dùng 24/7 .

- Các dịch vụ File, Mail, Web luôn phải ổn định để cán bộ nhân viên trong Viện và khách hàng có thể sử dụng. Luôn luôn kiểm soát được số lượng người truy cập dịch vụ.

- Dữ liệu tại các phòng ban phải được tập trung, không phân tán, dễ quản lý, được phân quyền phù hợp với chức trách.

- Khả năng cung ứng cao, đáp ứng được một lượng lớn kết nối vào trong hay ra ngoài mạng mà vẫn giữ được sự ổn định.

- Có khả năng mở rộng trong tương lai.

3.1.3 Hiện trạng các vấn đề liên quan trong quá trình vận hành, khai thác mạng máy tính tại Viện KHCN Sáng tạo Việt Nam

- Vào thời gian cao điểm từ 6h30 tới 8h30 sáng và 13h00 đến 15h00, số lượng người truy cập máy chủ là rất lớn do thời điểm này các độc giả truy cập đọc tin tức từ báo điện tử do Viện quản lý. Do không đo lường, kiểm soát được hiệu năng của máy chủ dẫn tới không phân luồng kịp thời lưu lượng về máy chủ gây ra chậm hoặc nghẽn khi đông người truy cập một thời điểm.

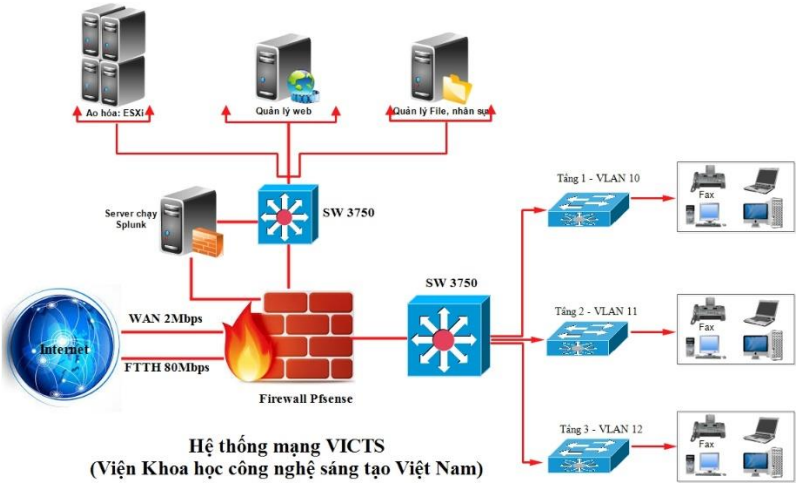
- Website và phần mềm của Viện có nhiều dữ liệu quan trọng cần phải có giải pháp bảo mật tối ưu.

- Không theo dõi kịp thời Firewal Pfsense dẫn tới không kịp chặn hoặc điều luồng dữ liệu khi cần thiết.

3.2 Kiến nghị đề xuất giải pháp giám sát Splunk cho mạng máy tính tại Viện KHCN Sáng tạo Việt Nam

Để giám sát tập trung, đồng thời kịp đánh giá các trạng thái hoạt động cho hệ thống mạng, tác giả đề xuất giải pháp cài đặt bộ công cụ giám sát tập trung Slpunk để xử lý các bài toán cần phải giám sát. Máy chủ cài đặt Slpunk cần xây dựng bên trong hệ thống máy chủ, cạnh các máy chủ dịch vụ khác như Web, Mail, File đồng thời vẫn giám sát được Firewall và lưu lượng vào ra của phía người dùng từ các phòng ban. Làm như vậy vừa để bảo vệ máy chủ giám sát do có

Firewall bảo vệ, vừa thuận tiện cho việc giám sát các máy chủ, dịch vụ,... của cơ quan.



Hình 3.2: Hệ thống mạng của Viện KHCN Sáng tạo Việt Nam

3.3 Cài đặt và vận hành hệ thống

3.3.1 Lấy Log từ máy chủ Firewall Pfsense

- Sử dụng công cụ Splunk để lấy Log từ máy chủ Pfsense vào để phân tích.

3.3.2 Lấy Log từ máy chủ Windows Server

- Sử dụng công cụ Splunk để lấy Log từ máy chủ Windows Server vào phân tích.

3.3.3 Lấy log từ máy chủ Linux cài đặt Splunk để phân tích

- Cấu hình máy chủ Splunk để lấy Log của máy chủ Linux đưa ra phân tích.

3.3.4 Lấy Log từ máy chủ Windows 10 của người dùng về phân tích

- Trong phần này sẽ cài đặt và cấu hình để lấy Log từ Windows 10 của người dùng về để phân tích.

3.4 Thử nghiệm và đánh giá

3.4.1 Nội dung thử nghiệm

Luận văn thực hiện thử nghiệm một số nội dung sau đây

(1) Cài đặt máy chủ giám sát tập trung Splunk

Ta sẽ tiến hành cài đặt máy chủ Splunk, nơi sẽ thông tin đổ về từ các máy thu thập, lưu trữ và phân tích chúng. Ta cần phải đảm bảo đường truyền mạng ổn định, các kết nối tới các máy giám sát đều không gặp trục trặc.

(2) Lấy log từ máy chủ Linux cài đặt Splunk để phân tích

Ta sẽ tiến hành cấu hình máy chủ Splunk để lấy Log của máy chủ Linux đưa ra phân tích.

(3) Cài đặt giám sát lấy Log từ máy chủ Firewall Pfsense về phân tích

Ta sẽ cài đặt và cấu hình ở System Logs của Pfsense và mở cổng để lấy log từ máy chủ Firewall Pfsense về để phân tích, từ đó ta có thể theo dõi được các hoạt động vào ra của hệ thống mạng.

(4) Lấy Log từ máy chủ Windows Server

Ta sẽ tiến hành cài đặt Cài đặt Splunk Forwarder và cấu hình sử dụng công cụ Splunk để lấy Log từ máy chủ Windows Server vào phân tích.

(5) Lấy Log từ máy chủ Windows 10 của người dùng về phân tích

Trong phần này sẽ cài đặt và cấu hình để lấy Log từ Windows 10 của người dùng về để phân tích.

3.4.2 Kết quả thử nghiệm và đánh giá

Phần thử nghiệm sẽ đưa ra kết quả và trình bày trong phần phụ lục của Luận văn. Các kết quả thử nghiệm đều khả quan, vận hành tốt

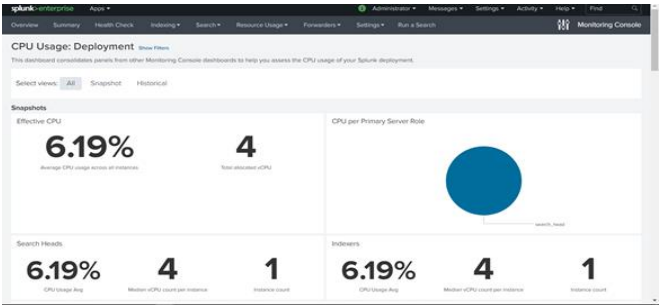
cũng như ổn định và đáp ứng được các nhu cầu giám sát an toàn thông tin.

Các giải pháp đã thử nghiệm có thể ứng dụng cho mạng nội bộ tại Viện Khoa học công nghệ sáng tạo Việt Nam.

(1) Kết quả cài đặt máy chủ giám sát tập trung Splunk

Hình 3.7 Giao diện Slunk sau khi cài đăt

(2) Kết quả lấy log từ máy chủ Linux (trong bài là lấy trên chính máy cài đặt Splunk)



Hình 3.12 Giao diện hiển thị thông tin trên Splunk

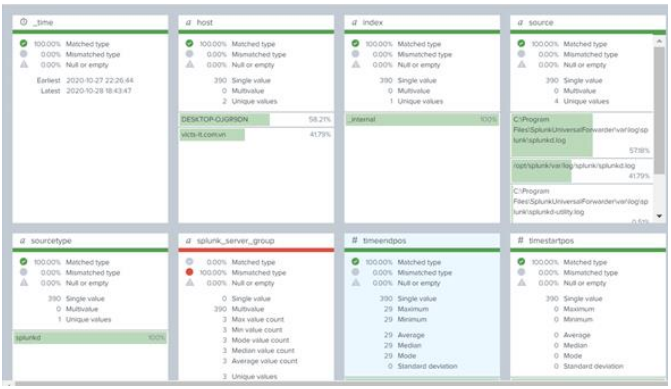
(3) Kết quả cài đặt giám sát lấy Log từ máy chủ Firewall Pfsense.

Hình 3.23 Tìm kiếm thành công máy chủ Pfsense trên Splunk

(4) Kết quả lấy Log từ máy chủ Windows Server

Hình 3.37. Giao diện hiển thị kết quả tìm kiếm thành công máy chủ Windows

(5) Kết quả lấy Log từ máy chủ Windows 10 của người dùng



Hình 3.46 Giao diện hiển thị thông tin các error log

3.5 Kết luận chương 3

Chương 3 của luận văn đã khảo sát mạng nội bộ tại Viện KHCN Sáng tạo Việt Nam, các vấn đề nảy sinh trong quá trình sử dụng và các yêu cầu trong giám sát hệ thống mạng nhằm đáp ứng nhu cầu đào tạo của Viện KHCN Sáng tạo Việt Nam.

Luận văn cũng đề xuất giải pháp giám sát an toàn thông tin cho hệ thống mạng của Viện KHCN Sáng tạo Việt Nam. Kết quả thử nghiệm phù hợp với các yêu cầu đề ra ban đầu.

KẾT LUẬN

Kết quả dự kiến đạt được của luận văn:

Với mục tiêu nghiên cứu, áp dụng giải pháp giám sát an toàn thông tin vào hệ thống CNTT của Viện KHCN Sáng tạo Việt Nam, luận văn đã đạt được một số kết quả sau đây:

- Tổng quan về giám sát an toàn thông tin
- Yêu cầu giám sát hệ thống an toàn thông tin
- Giải pháp giám sát an toàn thông tin Splunk SIEM
- Tăng cường bảo đảm ATTT cho hệ thống CNTT tại Viện KHCN Sáng tạo Việt Nam.

Hướng phát triển tiếp theo:

Học viên sẽ tiếp tục nghiên cứu, hoàn thiện, tối ưu giải pháp hơn nữa để có thể đảm bảo ATTT cho hệ thống CNTT của Viện KHCN Sáng tạo Việt Nam ở mức cao hơn như sử dụng công nghệ AI để phát hiện hành vi tấn công.