TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT THÀNH PHỐ HỒ CHÍ MINH

KHOA ĐÀO TẠO CHẤT LƯỢNG CAO

-------\*\*\*-------

****

**BÁO CÁO**

**MÔN: Tiểu Luận Chuyên Ngành**

**Tìm Hiều Về SIEM**

**GVHD**: Nguyễn Thị Thanh Vân

**Sinh viên thực hiện:**

|  |  |
| --- | --- |
| Đồng Thế THiện | 15110130 |

Lưu Tín Thông 15110134

*Tp Hồ Chí Minh, ngày 08 tháng 10 năm 2018*

Mục Lục

# Tổng quan về SIEM

## Sự cần thiết cần có SIEM

## Thành phần, nguyên lý hoạt động của SIEM

## Các hệ thống SIEM trong thực tế

## Các công cụ SIEM

# Chọn 1 Công cụ triển khai> SIEM

## Các đặc điểm, chức năng, hoạt động của công cụ….

## Cách thức triển khai

# 3: Thực hành

## Mô hình triển khai: thành phần, chi tiết….

## Mô tả yêu cầu cần đạt được khi SIEM hoạt động

## Các kịch bản triển khai

## Kết quả

# **Tổng quan về SIEM**

* 1. **Sự cần thiết có SIEM**
     1. **Các Nguy Cơ An Ninh Mạng**

Khi các hoạt động kinh tế, giáo dục, chính trị, quân sự hiện nay trên toàn thế giới đều dựa vào hệ thống mạng và kết nối Internet thì nguy cơ dẫn đến cuộc chiến tranh liên quan đến không gian mạng giữa các quốc gia đang dần được kích hoạt. Nhận thấy những hiểm họa tiềm ẩn xuất phát từ Internet này mà các quốc gia trên thế giới đã và đang thành lập các lực lượng phản ứng phòng chống và tác chiến mạng.

Trong đó Mỹ là quốc gia đã tập trung vào lĩnh vực an ninh mạng từ những năm 1990. Chịu trách nhiệm cho lĩnh vực này gồm có Bộ An ninh nội địa (Department of Homeland Security), Cục điều tra liên bang FBI (Federal Bureau of Investigation), Bộ Quốc phòng Mỹ (Department of Defense) và US Cyber Command. Bộ An ninh nội địa có trách nhiệm chính trong việc bảo đảm an ninh trong nước. Đơn vị National Cyber Security Division của Bộ An ninh Nội địa được giao nhiệm vụ “hợp tác làm việc với các cơ quan nhà nước, tư nhân và quốc tế để đảm bảo không gian mạng và quyền lợi không gian mạng của nước Mỹ”. Đơn vị này cũng có một số chương trình để bảo vệ cơ sở hạ tầng mạng chống lại các tấn công. Đơn vị National Cyber Response Coordination Group thuộc đơn vị National Cyber Security Division bao gồm 13 cơ quan liên bang và có trách nhiệm phối hợp phản ứng liên bang trong sự cố không gian mạng mang tầm cỡ quốc gia. Cyber Command, một đơn vị con nằm dưới sự quản lý của Cơ quan chỉ huy chiến lược Hoa Kỳ (US Strategic Command) có trách nhiệm đối phó với các mối đe dọa liên quan đến cơ sở hạ tầng mạng quân sự. Các đơn vị thành viên của Cyber Command bao gồm các lực lượng Army Forces Cyber Command, Air Force 24, Hạm đội Cyber Command, và Marine Cyber Command.

Tại Anh một lực lượng đặc biệt được thành lập đầu năm 2011 với tên gọi Cyber Security Operations Centre chịu trách nhiệm về cả khả năng tấn công và phòng thủ không gian mạng. Trung tâm này thực hiện nhiệm vụ chính là giám sát sự phát triển và tình trạng hiện tại của hệ thống IT chính phủ Anh, phân tích các xu hướng và nâng cao sự phản ứng lại khi có sự cố mạng xảy ra.

Tại Trung Quốc sách trắng về Quốc phòng năm 2004 đã nêu rõ Quân ủy Trung ương Trung Quốc (PLA) xác định PLA Air Force chịu trách nhiệm cho các hoạt động liên quan đến thông tin và hoạt động phản động liên quan đến thông tin. Cục 4 của Tổng cục nhân viên PLA chịu trách nhiệm về các hoạt động phản động liên quan đến điện tử và nghiên cứu phát triển công nghệ chiến tranh thông tin, chịu trách nhiệm về khả năng không gian mạng cho quân đội. Cục 3 chịu trách nhiệm cho các tín hiệu thông minh và tập trung vào việc thu thập, phân tích, khai thác thông tin điện tử. Cục 3 và 4 cũng tiến hành nghiên cứu các công nghệ tiên tiến về bảo mật thông tin.

Sách trắng của Bộ quốc phòng Hàn Quốc năm 2008 đã xác định an ninh mạng là một thành phần thiết yếu của quốc phòng. Năm 2010 sách này cũng vạch ra tấn công mạng là một trong những hiểm họa an toàn phi truyền thống. Các đội ứng cứu khẩn cấp đã được thành lập ở mức quân đoàn để giám sát các hệ thống thông tin quốc phòng. Trung tâm chiến tranh mạng (Cyber War Center) của Bộ quốc phòng đã được thành lập năm 2010. Mục đích chính của trung tâm này là tăng tính bảo mật cho hệ thống mạng của chính phủ và các thông tin tài chính. Bộ quốc phòng cũng tuyên bố tạo ra một đơn vị Cyber Warfare Command độc lập chịu trách nhiệm cho các hoạt động phòng thủ và tấn công trong không gian mạng. Hội đồng chiến lược An ninh mạng Quốc gia (National Cybersecurity Strategy Council) là cơ quan điều phối phát triển các chính sách không gian mạng, và được chủ trì bởi người đứng đầu các hoạt động tình báo quốc gia (National Intelligence Service).

* + 1. **Tính cấp thiết về việc giám sát an ninh mạng ở nước ta**

Tại Việt Nam các cơ quan bộ ngành khác nhau chịu trách nhiệm giám sát an ninh mạng cho từng lĩnh vực khác nhau. Để thực hiện GSANM yêu cầu và đòi hỏi một sự đầu tư lớn về con người và vật chất, bên cạnh đó các chuyên gia thực hiện GSANM phải am hiểu và có trình độ kỹ thuật sâu đối với công nghệ thông tin nói chung và các mảng đặc biệt về mạng nói riêng.

Bộ Thông tin và Truyền thông thực hiện nhiệm vụ, quyền hạn quy định tại Nghị định số 36/2012/NĐ-CP và Nghị định số 132/2013/NĐ-CP bảo đảm an toàn thông tin cho các hệ thống thông tin và Internet; bảo đảm an toàn thông tin cho các hoạt động ứng dụng và phát triển công nghệ thông tin; phòng, chống thư rác; tổ chức thực hiện chức năng quản lý, điều phối các hoạt động ứng cứu sự cố máy tính trong toàn quốc. Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Vietnam Computer Emergency Response Team - VNCERT) là đơn vị trực thuộc Bộ thông tin – Truyền thông được thành lập ngày 20/12/2005 theo quyết định số 339/QĐ-TTg của Thủ tướng Chính phủ thực hiện chức năng điều phối và tổ chức các hoạt động phản ứng nhanh các sự cố máy tính cho mạng Internet Việt Nam.

Bên cạnh đó Bộ Quốc phòng thực hiện quản lý nhà nước về an toàn thông tin trong lĩnh vực quốc phòng. Một đơn vị khác chịu trách nhiệm xây dựng, đề xuất ban hành các tiêu chuẩn và quy định kỹ thuật về mật mã trong an toàn và bảo mật thông tin đó chính là Ban Cơ yếu Chính phủ. Bộ Công an chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, phát hiện, ngăn chặn, đấu tranh chống âm mưu, hoạt động lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội và lợi ích của công dân. Bộ Công an đã có một số Cục chức năng liên quan tới hoạt động đảm bảo an toàn, an ninh cho hệ thống CNTT của các cơ quan Nhà nước như Cục Công nghệ tin học nghiệp vụ, Cục Phòng chống tội phạm công nghệ cao, Cục An ninh mạng, Cục An ninh thông tin…

Một số tổ chức khác cũng chung tay góp phần đảm bảo an ninh mạng cho quốc gia như: Hiệp hội an toàn thông tin (viết tắt là VNISA) đã ra đời và là tổ chức xã hội nghề nghiệp phi lợi nhuận đầu tiên hoạt động trong lĩnh vực bảo mật thông tin được nhà nước Việt Nam công nhận. VNISA tập hợp các cá nhân, tổ chức làm công tác nghiên cứu giảng dạy, ứng dụng và phát triển an toàn thông tin nhằm hướng dẫn thực hiện các chủ trương đường lối của nhà nước trong việc ứng dụng và phát triển kỹ thuật, công nghệ, an toàn thông tin, đưa ra đề xuất, khuyến nghị với cơ quan quản lý nhà nước trong việc xây dựng cơ chế chính sách phát triển ngành.

Trung tâm an ninh mạng Bách Khoa, tên đầy đủ là Trung tâm phần mềm và giải pháp an ninh mạng là một trung tâm nghiên cứu của Trường Đại học Bách Khoa Hà Nội. Hỗ trợ chuyên môn cho các cơ quan chức năng của Chính phủ trong công tác phòng chống, truy tìm tội phạm tin học tham gia, xây dựng luật pháp về tội phạm tin học. Tham gia các hoạt động phòng chống tấn công phá hoại bằng CNTT; Hợp tác với các tổ chức An ninh mạng và Cứu hộ các sự cố máy tính của các nước trên thế giới và trong khu vực trong việc khắc phục sự cố máy tính, chia sẻ thông tin về an ninh thông tin.

* + 1. **SIEM ra đời**

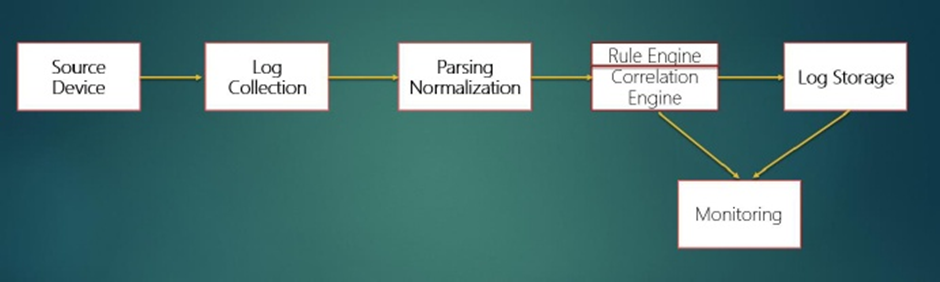
Trong giai đoạn hiện nay, cùng với sự phát triển của công nghệ thông tin là sự bùng nổ của các cuộc tấn công mạng và nguy cơ chiến tranh mạng. Do vậy, việc giám sát an ninh mạng là một vấn đề rất cần thiết và ngày càng được chú trọng hơn. Nhằm mục đích phát hiện sớm các tấn công mạng cũng như các nguy cơ đối với hệ thống mạng và đưa ra các giải pháp ngăn chặn kịp thời. Đáp ứng nhu cầu đó hệ thống giám sát an ninh mạng được phát triển và xây dựng qua các giai đoạn và công nghệ sau: Quản lý thông tin an ninh (SIM – Security infomation managemant), quản lý sự kiện an ninh (SEM – Security event management) và giải pháp quản lý phân tích sự kiện an toàn thông tin (SIEM – Security information and event management).

* 1. **Thành phần,, nguyên lý hoạt động của SIEM**

**1.2.1 Các thành phần của SIEM**

Hệ thống SIEM bao gồm nhiều phần, mỗi phần làm một nhiệm vụ riêng biệt. Mỗi thành phần trong hệ thống này có thể hoạt động độc lập với các thành phần khác nhưng nếu tất cả không hoạt động cùng một lúc thì sẽ có không có một SIEM hiệu quả.

Tùy thuộc vào hệ thống đang sử dụng mỗi SIEM sẽ có những thành phần cơ bản. Bằng sự hiểu biết từng phần của SIEM và cách thức hoạt động, người quản trị có thể quản lý một cách hiệu quả và khắc phục sự cố các vấn đề khi phát sinh.



Hình 1.1: Các thành phần của SIEM

Hình 1.1: Các thành phần của SIEM

Các Thành phần của SIEM

* Thiết bị nguồn (Source device)
* Thu thập Log (Log collection)
* Phân tích, Chuẩn hóa Log (Parsing normalization)
* Kỹ thuật tương quan sự kiện (Rule engine | correlation engine)
* Lưu trữ Log (Log storage)

## **1.2.2 Nguyên Lý Hoạt Động Của SIEM**

**HOẠT ĐỘNG CỦA SIEM**

Việc quan trọng khi thực hiện triển khai SIEM là cần phải hiểu nó làm việc nhưthế nào? Đối với mỗi nhà cung cấp khác nhau sẽ có đôi chút khác nhau nhưng chúngđều dựa trên những khái niệm cốt lõi. Thành phần cơ bản vẫn là thu thập thông tin, phântích và lưu trữ. Các bản ghi Log được thu thập từ các thiết bị khác nhau và chúng có thểcó những định dạng theo từng loại thiết bị. Chúng ta cần thu thập và chuyển nó về mộtđịnh dạng chung. Quá trình này gọi là hợp nhất dữ liệu (consolidation). Sau đó sẽ tiến

hành phân

tích từ các dữ liệu này và thực hiện tương quan sự kiện an ninh

 (Correlation)

để đưa tới kết luận có một cuộc tấn công hay không? Các thông tin về môi trường mạngvà các mối đe dọa phổ biến rất có ích trong giai đoạn này. Việc đưa ra cảnh báo và các

 báo c

áo sẽ được tạo ra như một kết quả của việc phân tích. Các bản ghi Log được lưutrữ trực tiếp trên SIEM ít nhất vài giờ đồng hồ sau đó chuyển tới nơi lưu trữ lâu dài để phục vụ cho quá trình điều tra hoặc sử dụng sau này.

Hoạt Động:

* Thu Thập Thông Tin
* Chuẩn Hóa Và Tổng Hợp Sự Kiện An Ninh
* Tương Quan Sự Kiện An Ninh
* Cảnh Báo Và Báo Cáo
* Lưu Trữ
  1. **Các hệ thống SIEM trong thực tế**

**Hệ thống giám sát an ninh mạng viết tắt là SIEM (Security information and event management – SIEM) là hệ thống được thiết kế nhằm thu thập thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và lưu trữ dữ liệu một cách tập trung. Theo đó, các hệ thống SIEM cho phép phân tích tập trung và báo cáo về các sự kiện an ninh mạng của tổ chức. Kết quả phân tích này có thể được dùng để phát hiện raa các cuộc tấn công mà không thể phát hiện được theo phương pháp thông thường.**

Hệ Thống:

* Quản lý tập trung
* Giám sát an ninh mạng
* Cải thiện hiêu quả trong hoạt động
* Xử lý sự cố
  1. **Các công cụ SIEM**
* **AlienVault OSSIM**
* **Labs Qradar**
* **Mark**

1. **Triển khai SIEM với AlienVault OSSIM**

* **Phương Pháp Thu Thập Thông tin**
* **Một số công cụ mã nguồn mở trong AlienVault OSSIM**
* **Tương quan sự kiện an ninh trong AlienVault OSSIM**
* **Đánh giá rủi ro**
* **Các hành động ứng phó sự cố an ninh**
* **Báo cáo trong AlienVault**

1. **Thực hành**

dsfasdassadasdasdasdasdasdasdasdas

Sadasd