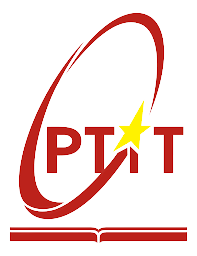
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 2**

--🙢🕮🙠--



**BÁO CÁO CHƯƠNG 1**

**TÌM HIỂU VÀ TRIỂN KHAI ELK SIEM**

**Môn:**

**Kỹ Thuật Theo Dõi, Giám Sát An Toàn Mạng**

**GIẢNG VIÊN HƯỚNG DẪN : TS HUỲNH THANH TÂM**

Thực hiện đề tài :

* Nguyễn Hoàng Đại Nghĩa – N19DCAT054 – D19CQAT01-N

**TP.HCM, tháng 03/2023**

MỤC LỤC

[**1.** **Tổng quan về SIEM** 3](#_Toc130886701)

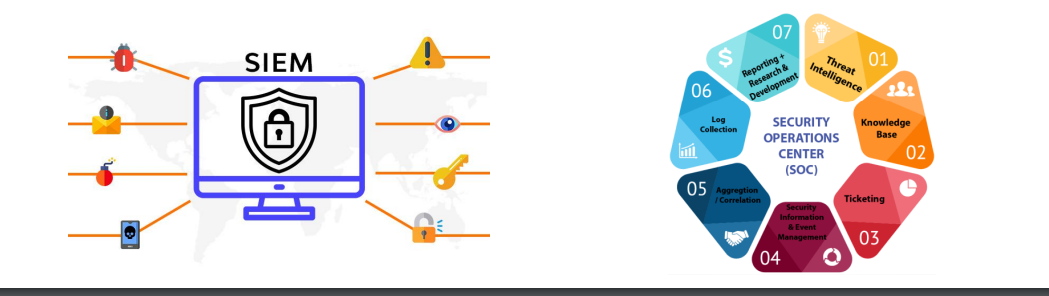
[**2.** **Kiến trúc SIEM** 4](#_Toc130886702)

[**3.** **Tầm quan trọng và lợi ích của ELK SIEM** 5](#_Toc130886703)

[**4.** **ELK SIEM** 6](#_Toc130886704)

1. **Tổng quan về SIEM**

* SIEM là viết tắt của Security Information and Event Management, là một công nghệ tổng hợp và quản lý thông tin về bảo mật.
* SIEM cung cấp khả năng giám sát và phân tích các sự kiện theo thời gian thực, theo dõi và ghi nhật ký dữ liệu bảo mật cho mục đích tuân thủ hoặc kiểm toán.
* SIEM giúp các tổ chức nhận ra các mối đe dọa và lỗ hổng bảo mật tiềm ẩn trước khi chúng có cơ hội làm gián đoạn hoạt động kinh doanh.
* SIEM là thành phần quan trọng trong security operation centers (SOC)



* Một số tính năng chính của SIEM bao gồm:
* Thu thập dữ liệu: SIEM thu thập dữ liệu từ nhiều nguồn khác nhau như log hệ thống, bản ghi sự kiện, dữ liệu mạng, hệ thống IDS/IPS, và các thiết bị bảo mật khác.
* Phân tích và xử lý: SIEM sử dụng các thuật toán và quy tắc để phân tích dữ liệu thu thập được, xác định các mẫu tấn công, các lỗ hổng bảo mật và các hoạt động đáng ngờ khác.
* Cảnh báo và báo cáo: SIEM cảnh báo và báo cáo về các sự kiện và hoạt động đáng ngờ, giúp người quản trị có thể phát hiện và giải quyết các vấn đề bảo mật một cách nhanh chóng và hiệu quả.
* Tích hợp và liên kết dữ liệu: SIEM tích hợp và liên kết dữ liệu từ nhiều nguồn khác nhau, giúp người quản trị có thể có cái nhìn tổng thể về tình trạng bảo mật của hệ thống.
* SIEM được sử dụng rộng rãi trong các tổ chức và doanh nghiệp để giám sát và quản lý bảo mật thông tin. Nó giúp người quản trị có thể phát hiện và đối phó với các mối đe dọa bảo mật một cách nhanh chóng và hiệu quả, từ đó giảm thiểu rủi ro và bảo vệ thông tin của tổ chức.

1. **Kiến trúc SIEM**

Kiến trúc của SIEM (Security Information and Event Management) bao gồm các thành phần chính sau đây:

* Thu thập dữ liệu: Các thiết bị và ứng dụng trong hệ thống mạng sẽ gửi các log và sự kiện liên quan đến bảo mật đến SIEM để xử lý.
* Phân tích dữ liệu: SIEM sẽ sử dụng các công cụ phân tích và thuật toán để xác định các tình huống bất thường, các mẫu tấn công, các lỗ hổng bảo mật và các hoạt động đáng ngờ khác.
* Cảnh báo và báo cáo: Nếu phát hiện các hoạt động đáng ngờ, SIEM sẽ cảnh báo và báo cáo cho người quản trị để họ có thể đưa ra các biện pháp phòng ngừa và giải quyết sự cố.
* Quản lý sự kiện và thông tin bảo mật: SIEM cung cấp khả năng quản lý các sự kiện bảo mật và thông tin liên quan, cập nhật chính sách bảo mật và đánh giá hiệu quả của các biện pháp bảo mật.
* Tích hợp với các công cụ bảo mật khác: SIEM có thể tích hợp với các công cụ bảo mật khác như Firewall, IDS/IPS, Antivirus để tăng cường khả năng bảo mật và phát hiện các mối đe dọa mới.
* Hệ thống lưu trữ dữ liệu: SIEM lưu trữ các sự kiện bảo mật và thông tin liên quan để phục vụ cho việc phân tích và báo cáo trong tương lai.

Tổng thể, kiến trúc của SIEM hỗ trợ cho việc thu thập, phân tích, cảnh báo và báo cáo các hoạt động đáng ngờ liên quan đến bảo mật trong hệ thống mạng, từ đó giúp người quản trị đưa ra các quyết định bảo mật hợp lý và nhanh chóng.

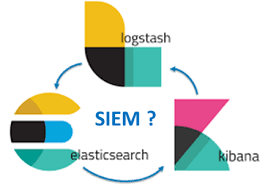
1. **Tầm quan trọng và lợi ích của ELK SIEM**

SIEM (Security Information and Event Management) là một giải pháp an ninh mạng được sử dụng để giám sát, phát hiện và phản ứng lại các hoạt động độc hại trên hệ thống mạng của một tổ chức. Tầm quan trọng của SIEM được thể hiện qua những điểm sau:

* Phát hiện và ngăn chặn các mối đe dọa an ninh mạng: SIEM giúp phát hiện và cảnh báo cho người quản trị hệ thống về các hoạt động độc hại như tấn công mạng, thâm nhập, phá hoại hoặc lợi dụng lỗ hổng bảo mật. Nhờ đó, tổ chức có thể đưa ra các biện pháp phòng ngừa và ngăn chặn kịp thời những mối đe dọa này.
* Giảm thiểu thời gian phát hiện và giải quyết sự cố an ninh mạng: SIEM giúp người quản trị hệ thống phát hiện và xử lý các sự cố an ninh mạng nhanh chóng hơn, giảm thiểu thời gian giải quyết sự cố và giúp tổ chức tránh được những thiệt hại không đáng có.
* Cung cấp báo cáo và phân tích an ninh mạng: SIEM cung cấp cho người quản trị hệ thống các báo cáo và phân tích về các hoạt động an ninh mạng, giúp họ hiểu rõ hơn về các mối đe dọa và tình trạng bảo mật của hệ thống.
* Đáp ứng các yêu cầu tuân thủ quy định: SIEM giúp tổ chức đáp ứng các yêu cầu tuân thủ quy định về an ninh mạng như PCI-DSS, HIPAA hay GDPR.

Vì vậy, SIEM là một giải pháp an ninh mạng quan trọng trong việc bảo vệ hệ thống và dữ liệu của tổ chức, giúp tổ chức phát hiện và ngăn chặn các mối đe dọa an ninh mạng, giảm thiểu thiệt hại và đáp ứng các yêu cầu tuân thủ quy định.

1. **ELK SIEM**

****

* **Cách thức hoạt động**

ELK SIEM là một giải pháp an ninh mạng kết hợp giữa ELK Stack và các tính năng SIEM. ELK là viết tắt của ElasticSearch, Logstash và Kibana, đây là những công cụ mã nguồn mở được sử dụng để thu thập, xử lý và hiển thị các dữ liệu log.

**Các bước hoạt động của ELK SIEM như sau:**

Thu thập dữ liệu: Logstash là công cụ được sử dụng để thu thập dữ liệu từ các nguồn khác nhau như máy chủ, ứng dụng và thiết bị mạng. Logstash sử dụng các input plugin để lấy dữ liệu từ các nguồn khác nhau, tiền xử lý dữ liệu và đưa vào ElasticSearch.

Tổ chức và lưu trữ dữ liệu: ElasticSearch là cơ sở dữ liệu được sử dụng để lưu trữ và tìm kiếm các dữ liệu log. ElasticSearch sử dụng các index để tổ chức dữ liệu và cung cấp khả năng tìm kiếm nhanh chóng.

Phân tích và phát hiện mối đe dọa: Các tính năng SIEM được tích hợp vào ELK để phân tích và phát hiện các mối đe dọa an ninh mạng. Các tính năng này bao gồm phát hiện xâm nhập, giám sát hành vi người dùng, phân tích lưu lượng mạng và phát hiện các sự kiện bất thường.

Hiển thị và báo cáo: Kibana là công cụ được sử dụng để hiển thị và báo cáo các dữ liệu log và các thông tin an ninh mạng. Kibana cung cấp các tính năng tùy biến để người dùng có thể tạo ra các báo cáo, đồ thị và biểu đồ để hiển thị các thông tin quan trọng.

Tóm lại, ELK SIEM là một giải pháp an ninh mạng mạnh mẽ, kết hợp giữa các công cụ của ELK Stack và các tính năng SIEM để phát hiện và ngăn chặn các mối đe dọa an ninh mạng, đồng thời cung cấp khả năng tổ chức, lưu trữ và hiển thị các dữ liệu log một cách dễ dàng và hiệu quả.

* **Tính năng :**

ELK SIEM là một giải pháp an ninh mạng mạnh mẽ, kết hợp giữa các công cụ của ELK Stack và các tính năng SIEM để phát hiện và ngăn chặn các mối đe dọa an ninh mạng, đồng thời cung cấp khả năng tổ chức, lưu trữ và hiển thị các dữ liệu log một cách dễ dàng và hiệu quả. Dưới đây là một số tính năng của ELK SIEM:

Thu thập dữ liệu: ELK SIEM sử dụng Logstash để thu thập dữ liệu từ các nguồn khác nhau như máy chủ, ứng dụng và thiết bị mạng. Logstash hỗ trợ nhiều input plugin để lấy dữ liệu từ các nguồn khác nhau.

Tổ chức và lưu trữ dữ liệu: ELK SIEM sử dụng ElasticSearch là cơ sở dữ liệu được sử dụng để lưu trữ và tìm kiếm các dữ liệu log. ElasticSearch sử dụng các index để tổ chức dữ liệu và cung cấp khả năng tìm kiếm nhanh chóng.

Phân tích và phát hiện mối đe dọa: ELK SIEM tích hợp các tính năng SIEM để phân tích và phát hiện các mối đe dọa an ninh mạng. Các tính năng này bao gồm phát hiện xâm nhập, giám sát hành vi người dùng, phân tích lưu lượng mạng và phát hiện các sự kiện bất thường.

Hiển thị và báo cáo: ELK SIEM sử dụng Kibana là công cụ được sử dụng để hiển thị và báo cáo các dữ liệu log và các thông tin an ninh mạng. Kibana cung cấp các tính năng tùy biến để người dùng có thể tạo ra các báo cáo, đồ thị và biểu đồ để hiển thị các thông tin quan trọng.

Tích hợp với hệ thống khác: ELK SIEM có khả năng tích hợp với các hệ thống an ninh mạng khác như IDS/IPS (Intrusion Detection System/Intrusion Prevention System), Firewall để tăng cường khả năng phát hiện và ngăn chặn các mối đe dọa an ninh mạng.

Giao diện đơn giản và dễ sử dụng: ELK SIEM cung cấp một giao diện đồ họa đơn giản và dễ sử dụng cho phép người dùng dễ dàng quản lý, tìm kiếm và xử lý các dữ liệu log.

* **Ưu nhược điểm của ELK SIEM so với các SIEM khác**

ELK SIEM là một giải pháp SIEM dựa trên ba công cụ phần mềm mã nguồn mở Elasticsearch, Logstash và Kibana. Dưới đây là một số ưu nhược điểm của ELK SIEM so với các SIEM khác:

***Ưu điểm:***

Giá thành thấp hơn: ELK SIEM là một giải pháp mã nguồn mở, do đó giá thành triển khai và vận hành thường thấp hơn so với các giải pháp SIEM thương mại.

Khả năng mở rộng: Elasticsearch là một hệ thống tìm kiếm phân tán với khả năng mở rộng cao, giúp ELK SIEM có thể xử lý hàng triệu sự kiện mỗi giây và lưu trữ lượng dữ liệu lớn.

Khả năng phân tích dữ liệu: ELK SIEM có khả năng phân tích dữ liệu từ nhiều nguồn khác nhau và đưa ra kết quả phân tích một cách trực quan.

***Nhược điểm:***

Đòi hỏi kiến thức kỹ thuật: Vì ELK SIEM được xây dựng trên nền tảng mã nguồn mở, do đó sử dụng ELK SIEM đòi hỏi kiến thức kỹ thuật về quản trị hệ thống và lập trình.

Khó khăn trong việc triển khai: Triển khai ELK SIEM đòi hỏi kỹ năng và kinh nghiệm để cấu hình và tối ưu hóa hệ thống.

Khả năng phát hiện mối đe dọa không hoàn hảo: ELK SIEM có thể phát hiện mối đe dọa an ninh, nhưng không thể phát hiện tất cả các cuộc tấn công mạng hoàn hảo.

Khả năng xử lý dữ liệu chậm hơn: So với một số giải pháp SIEM thương mại, ELK SIEM có thể xử lý dữ liệu chậm hơn và đòi hỏi tài nguyên cao hơn để vận hành.

Vì vậy, khi đánh giá ELK SIEM so với các giải pháp SIEM khác, người dùng cần cân nhắc các ưu điểm và nhược điểm để đưa ra quyết định phù hợp với nhu cầu của tổ chức.