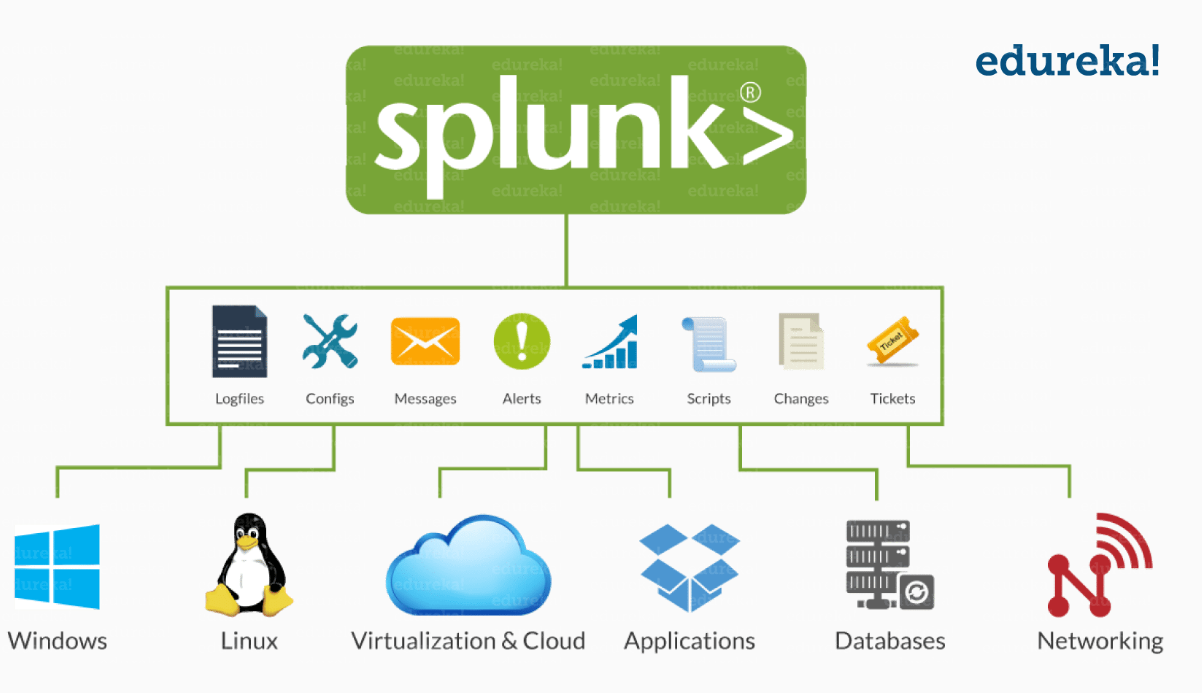
**Đánh giá 1 số sản phẩm giám sát an ninh mạng với splunk**

1. **Splunk**

****

* Tính năng:

+>  Hỗ trợ hầu như tất cả các loại log của hệ thống, thiết bị hạ tầng mạng, phần mềm, Firewall, IDS/IPS, Log Event, Register của các máy trạm ….

+> có thể thực hiện việc thu thập log từ rất nhiều nguồn khác nhau.

+> cập nhật dữ liệu liên tục khi có thay đổi trong thời gian thực

+> có thể đánh chỉ mục dữ liệu với một khối lượng dữ liệu rất lớn trong một khoảng thời gian ngắn.

+> làm việc rất tốt với dữ liệu lớn và cập nhật liên tục.

+> Splunk cung cấp cho người dùng một cơ chế cảnh báo dựa trên việc tìm kiếm các thông tin do chính người sử dụng đặt ra

+> cung câp một cơ chế tự động khắc phục với các vấn đề xảy ra bằng việc tự động chạy các file Script mà người dùng tự tạo (Ví dụ như: Chặn IP, đòng Port …) khi có các cảnh báo xảy ra.

+> cung cấp một cơ chế hiển thị rất trực quan giúp người sử dụng có thể dễ dàng hình dung về tình trạng của hệ thống, đưa ra các đánh giá về hệ thống.

+> cung cấp các API hỗ trợ việc tạo các ứng dụng trên Splunk của người dùng.

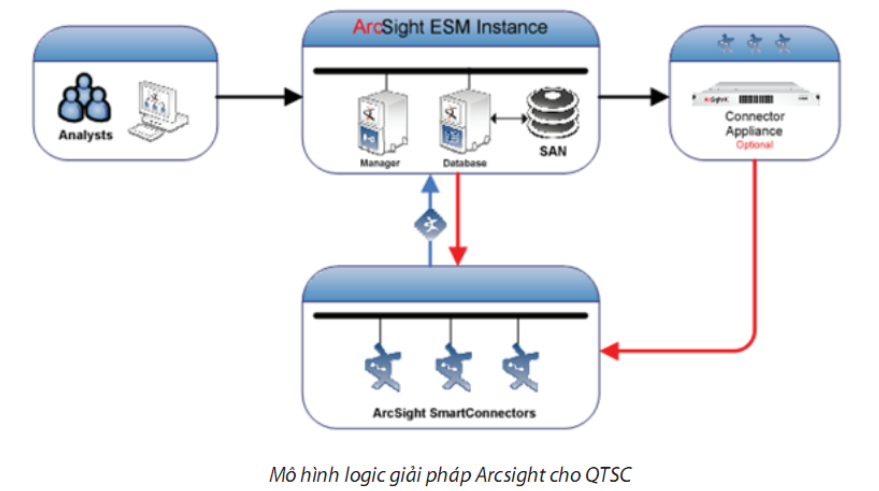
* Hạn chế:

+> mạnh về khả năng phân tích và cảnh báo tuy nhiên nó lại không mạnh và không đảm bảo về việc thu thập và truyền tải log. Cụ thể là nó chưa có cơ chế bảo mật trên đường truyền, không phù hợp với những hệ thống đòi hỏi bảo mật cao.

+> Để phát huy hết được sức mạnh của Splunk cần có thời gian tìm hiểu và sử dụng.

+> để triển khai được một hệ thống sử dụng Splunk hiệu quả chúng ta cũng cần có một hệ thống riêng, đây cũng là một trở ngại không nhỏ với các hệ thống có quy mô trung bình và nhỏ.

1. **HP ArcSight Logger**

****

* Tính năng:

+> hỗ trợ nhiều loại định dạng Log: Syslog, Eventlog, Device Log …

+> phân  tích toàn diện dữ liệu.

+> cảnh báo và giám sát hệ thống trong thời gian thực.

+> đánh chỉ mục dữ liệu, tìm kiếm và kết xuất báo cáo.

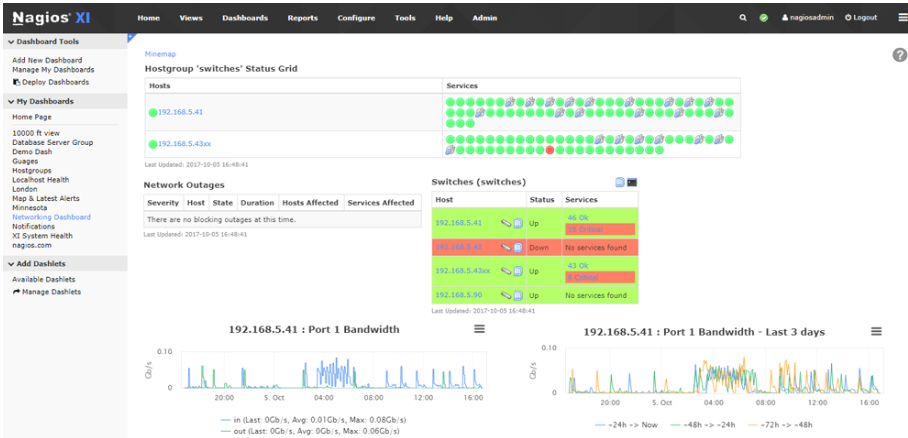
+> đi sâu vào việc phân tích ngữ cảnh từ các thông tin nhận được.

* Hạn chế:

+> 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

1. **Nagios**

****

* Tính năng:

+> Giám sát các dịch vụ mạng và các host .

+> Các plugin đơn giản, dễ dàng phát triển và kiểm tra dịch vụ

+> Phát hiện và phân biệt các host bị down và host không thể truy cập được

+> Hỗ trợ giám sát dự phòng

+> Có giao diện web

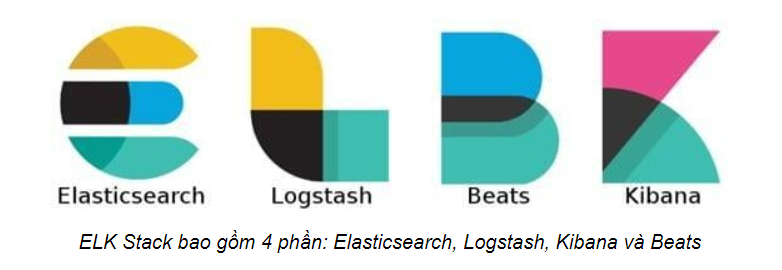
+> Cung cấp lịch sử ghi lại các cảnh báo, thông báo, sự cố...

* Hạn chế:

+> Chỉ mạnh về giám sát được hiệu năng hệ thống và một số dịch vụ mạng, khó tùy chỉnh.

+> Khả năng tối ưu hóa chưa cao.

1. **ELK Stack**



* Tính năng:

+> mã nguồn mở, không tốn nhiều chi phí khi triển khai.

+> được phát triển mạnh gần đây, nên cộng đồng hỗ trợ rất đông đúc và mạnh mẽ.

+> Thu thập được log từ rất nhiều nguồn khác nhau

+> Khả năng tương thích cao, dễ dàng tích hợp với các hệ thống khác mà không gặp khó khăn.

+> Giao diện Kibana trực quan, sinh động.

+> Phương tiện cảnh báo đa dạng, tích hợp với email, sms, slack, các ứng dụng OTP

+> Hiệu năng xử lý cao, có thể chịu tải được một lượng lớn dữ liệu (log) đẩy về mà không phải quá phụ thuộc vào khả năng xử lý của phần cứng.

+> 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,...

* Hạn chế:

+>  tốn kém thời gian tìm hiểu, deploy và chi phí phần cứng tăng theo cấp số nhân

Ngoài các công cụ kể trên, còn 1 số công cụ khác nữa như: loggly, syslog-ng, …

1. **Nguồn tài liệu:**

* https://www.daihockhonggiay.com/blogs/post/gioi-thieu-mot-so-cong-cu-giam-sat
* <https://securitydaily.net/mot-so-san-pham-giam-sat-an-ninh-mang/#:~:text=Splunk%20m%E1%BA%A1nh%20v%E1%BB%81%20kh%E1%BA%A3%20n%C4%83ng,t%C3%ACm%20hi%E1%BB%83u%20v%C3%A0%20s%E1%BB%AD%20d%E1%BB%A5ng>.