VNCERT   
Công việc của nhóm thực hành trong 13/2/2023 đến 19/2/2023

**MỤC LỤC**

[DANH MỤC BẢN VẼ 3](#_Toc128257935)

[I. TÓM TẮT VIỆC ĐÃ LÀM 4](#_Toc128257936)

[II. SOC TEAM 5](#_Toc128257937)

[2.1. Khái niệm về SOC 5](#_Toc128257938)

[2.2. Vai trò của SOC 5](#_Toc128257939)

[2.3. Các cấp độ của SOC 6](#_Toc128257940)

[2.4. Công Nghệ 9](#_Toc128257941)

[2.5. Tích hợp SOC với Splunk 11](#_Toc128257942)

[III. SIEM 13](#_Toc128257943)

[3.1. Hệ Thống SIEM 13](#_Toc128257944)

[3.1.1. Khái niệm 13](#_Toc128257945)

[3.1.2. Chức năng 13](#_Toc128257946)

[3.1.3. Tính năng 13](#_Toc128257947)

[3.1.4. Thành phần 13](#_Toc128257948)

[3.2. Tổng quan là lợi ích của việc tích hợp 14](#_Toc128257949)

[3.2.1. Tại sao lại tích hợp splunk với các hệ thống quản lý siem? 14](#_Toc128257950)

[3.2.2. Lợi ích 14](#_Toc128257951)

[3.2.3. Quy Trình Tích Hợp Splunk 15](#_Toc128257952)

[3.3. Các Ví Dụ Trong Thế Giới Thực 16](#_Toc128257953)

[3.4. Kết luận 17](#_Toc128257954)

[IV. TẤN CÔNG RECONNAISSANCE 18](#_Toc128257955)

[4.1. Tấn công Reconnaissance? 18](#_Toc128257956)

[4.2. Điều tra phân tích tình huống tấn công Reconnaissance: 18](#_Toc128257957)

[4.3. Thực hiện điều tra 18](#_Toc128257958)

[4.3.1. Tìm kiếm thông tin IP 18](#_Toc128257959)

[4.3.2. Tiến hành tìm kiếm máy quét lỗ hổng 20](#_Toc128257960)

[4.3.3. Xem các sự kiện HTTP cho imreallynotbatman.com 21](#_Toc128257961)

[4.3.4. Tìm kiếm tệp đã làm defaced website 22](#_Toc128257962)

[4.3.5. Tên miền đủ điều kiện hoàn toàn (FQDN) được liên kết với cuộc tấn công 23](#_Toc128257963)

[V. TẤN CÔNG INSTALLATION 24](#_Toc128257964)

[5.1. Tấn công Installation với Splunk là gì? 24](#_Toc128257965)

[5.2. Tính năng của Splunk dùng để phân tích sự cố tấn công Installation 24](#_Toc128257966)

[5.3. Điều tra phân tích tình huống tấn công Installation: 25](#_Toc128257967)

[5.4. Thực hiện điều tra 25](#_Toc128257968)

# DANH MỤC BẢN VẼ

[Hình 2. 1 Mô tả cấp độ của SOC 6](#_Toc128257741)

[Hình 2. 2 Nền tảng tình báo bảo mật sử dụng nhiều loại 10](#_Toc128257742)

[Hình 2. 3 Các nguồn dữ liệu mẫu cần thiết để phát hiện mối đe dọa nâng cao 11](#_Toc128257743)

[Hình 4. 1 Các rules được kích hoạt trong weblog 19](#_Toc128257744)

[Hình 4. 2 Xác định địa chỉ IP 20](#_Toc128257745)

[Hình 4. 3 Kiểm tra máy quét 20](#_Toc128257746)

[Hình 4. 4 Các sự kiện HTTP 21](#_Toc128257747)

[Hình 4. 5 Hiển thị công cụ sử dụng trong sự kiện HTTP 22](#_Toc128257748)

[Hình 4. 6 Tệp đã làm defaced website 22](#_Toc128257749)

[Hình 4. 7 Tên miền được liên kết với cuộc tấn công 23](#_Toc128257750)

[Hình 5. 1 Kết quả trả về khi thu hẹp lưu lượng truy cập 26](#_Toc128257751)

[Hình 5. 2 Nội dung trong file param=cmd.exe 26](#_Toc128257752)

[Hình 5. 3 Kết quả trả ở trườg part\_filename{} 27](#_Toc128257753)

[Hình 5. 4 Kết quả trả về ở trường c\_ip 28](#_Toc128257754)

# TÓM TẮT VIỆC ĐÃ LÀM

* Thay đổi hệ điều hành ubuntu 18 thành ubuntu 20
* Tìm hiểu các chủ đề bảo mật xung quanh splunk
  + SOC Team
  + SIEM
  + Tấn công Reconnaissance
  + Tấn công Installation
* Về mặt hạn chế: vẫn chưa xây dựng hạ tầng và kế hoạch rõ ràng trong xây dựng soc team, các demo vẫn chưa nắm rõ được các câu lệnh, chưa triễn khai được.
* Kế hoạch tuần tới:
  + Tìm hiểu về Docker
  + Phân tích source log4j (web maven và sửa đổi source)
  + Tìm hiểu và demo cách sử dụng splunk (vẫn ở mức lý thuyết)
  + Tiếp tục tìm hiểu về AD
  + Lên kế hoạch cho việc triễn khai soc team tier

# SOC TEAM

## Khái Niệm Về SOC

Đội ngũ Security Operations Center (SOC) là một nhóm chuyên gia bảo mật được tập trung vào việc giám sát, phát hiện và giải quyết các vấn đề liên quan đến an ninh mạng của một tổ chức hoặc doanh nghiệp. Công việc của SOC team bao gồm giám sát và phân tích các dữ liệu an ninh từ nhiều nguồn khác nhau, như hệ thống giám sát an ninh, nhật ký hệ thống, dữ liệu mạng và các tài nguyên khác của tổ chức.

Nhóm SOC team sử dụng các công cụ và kỹ thuật để phát hiện các hoạt động đáng ngờ trên mạng, bao gồm các cuộc tấn công mạng, malware, phần mềm độc hại, vi phạm chính sách bảo mật và các hành vi không được phép khác. Sau đó, phân tích và giải quyết các vấn đề này để bảo vệ an toàn thông tin của tổ chức.

## Vai Trò Của SOC

Có năm vai trò chính trong nhóm SOC:

Các nhà phân tích bảo mật (Security Analysts) là những người phản hồi đầu tiên về an ninh mạng. Họ báo cáo về các mối đe dọa trên mạng và thực hiện mọi thay đổi cần thiết để bảo vệ tổ chức. Họ được coi là tuyến phòng thủ cuối cùng chống lại các mối đe dọa an ninh mạng, làm việc cùng với các nhà quản lý bảo mật và kỹ sư an ninh mạng, đồng thời thường báo cáo với CISO.

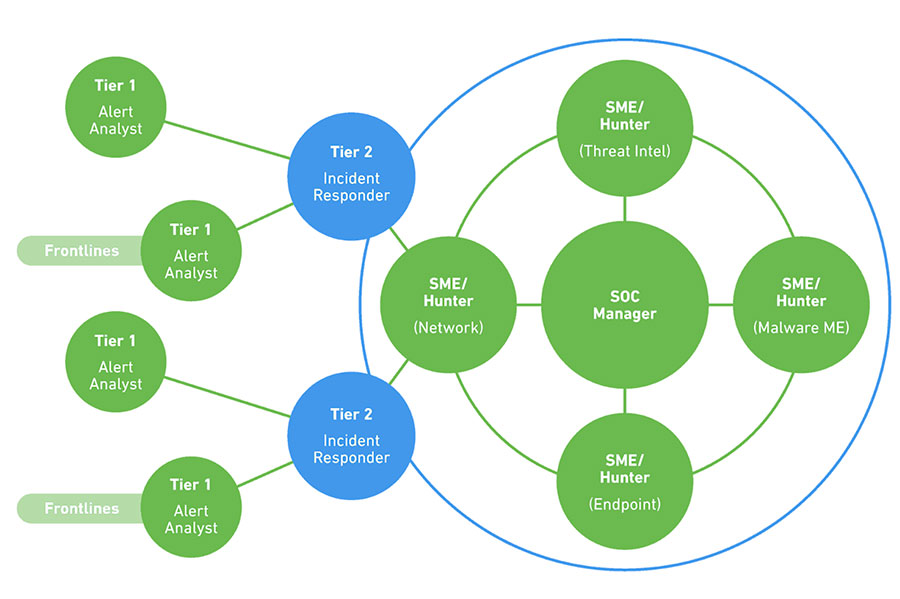
Kỹ sư bảo mật thường (Security Engineers) là chuyên gia phần mềm hoặc phần cứng, chịu trách nhiệm bảo trì và cập nhật các công cụ và hệ thống. Họ cũng chịu trách nhiệm về bất kỳ tài liệu nào mà các thành viên khác trong nhóm có thể cần, chẳng hạn như các giao thức bảo mật kỹ thuật số.

Người quản lý SOC (SOC Manager) chịu trách nhiệm về nhóm SOC. Họ chỉ đạo các hoạt động SOC và chịu trách nhiệm đồng bộ hóa giữa các nhà phân tích và kỹ sư; tuyển dụng; đào tạo; và tạo và thực hiện chiến lược an ninh mạng. Họ cũng chỉ đạo và điều phối phản ứng của công ty đối với các mối đe dọa an ninh lớn.

Giám đốc an ninh thông tin (Chief Information Security Officer hay CISO) là một vị trí lãnh đạo chịu trách nhiệm thiết lập các chiến lược, chính sách và hoạt động liên quan đến bảo mật. Họ làm việc chặt chẽ với Giám đốc điều hành, đồng thời thông báo và báo cáo cho ban quản lý về các vấn đề bảo mật.

Giám đốc ứng phó sự cố (Director Of Incident Response hay IR) là một vai trò trong các tổ chức bảo mật lớn hơn chịu trách nhiệm quản lý các sự cố khi chúng xảy ra và truyền đạt các yêu cầu bảo mật cho tổ chức trong trường hợp vi phạm dữ liệu nghiêm trọng.

## Các Cấp Độ Của SOC



Hình 2. Mô tả cấp độ của SOC

|  |  |  |
| --- | --- | --- |
| **VAI TRÒ** | **TRÌNH ĐỘ** | **NHIỆM VỤ** |
| **Tier 1 AnalystAlert Investigator** | Kỹ năng quản trị hệ thống; ngôn ngữ lập trình web, chẳng hạn như Python, Ruby, PHP; ngôn ngữ kịch bản; chứng chỉ bảo mật như CISSP hoặc SANS SEC401 | Giám sát các cảnh báo SIEM, quản lý và định cấu hình các công cụ giám sát bảo mật. Ưu tiên và phân loại các cảnh báo hoặc sự cố để xác định xem một sự cố bảo mật thực sự có đang diễn ra hay không. |
| **Tier 2 AnalystIncident Responder** | Tương tự như nhà phân tích Cấp 1, nhưng có nhiều kinh nghiệm hơn bao gồm cả ứng phó sự cố. Pháp y nâng cao, đánh giá phần mềm độc hại, thông tin tình báo về mối đe dọa. Chứng nhận hoặc đào tạo hacker có đạo đức là một lợi thế lớn. | Tiếp nhận sự cố và thực hiện phân tích sâu; tương quan với thông tin tình báo về mối đe dọa để xác định tác nhân đe dọa, bản chất của cuộc tấn công và các hệ thống hoặc dữ liệu bị ảnh hưởng. Xác định và thực hiện chiến lược ngăn chặn, khắc phục và phục hồi. |
| **Tier 3 AnalystSubject Matter Expert/Threat Hunter** | Tương tự như nhà phân tích Cấp 2 nhưng thậm chí còn có nhiều kinh nghiệm hơn, bao gồm cả các sự cố cấp cao. Có kinh nghiệm với các công cụ kiểm tra thâm nhập và trực quan hóa dữ liệu giữa các tổ chức. Kỹ thuật đảo ngược phần mềm độc hại, trải nghiệm xác định và phát triển các phản ứng đối với các mối đe dọa và kiểu tấn công mới. | Hàng ngày, tiến hành đánh giá lỗ hổng và kiểm tra thâm nhập, đồng thời xem xét các cảnh báo, tin tức ngành, thông tin tình báo về mối đe dọa và dữ liệu bảo mật. Tích cực tìm kiếm các mối đe dọa đã xâm nhập vào mạng, cũng như các lỗ hổng bảo mật và lỗ hổng bảo mật chưa biết. Khi một sự cố lớn xảy ra, các nhóm với Nhà phân tích cấp 2 sẽ ứng phó và ngăn chặn sự cố đó. |
| **Tier 4 SOC ManagerCommander** | Tương tự như nhà phân tích Cấp 3, bao gồm kỹ năng quản lý dự án, đào tạo quản lý ứng phó sự cố và kỹ năng giao tiếp tốt. | Giống như chỉ huy của một đơn vị quân đội, chịu trách nhiệm tuyển dụng và đào tạo nhân viên SOC, phụ trách chiến lược phòng thủ và tấn công. Quản lý tài nguyên, mức độ ưu tiên và dự án, đồng thời trực tiếp quản lý nhóm khi ứng phó với các sự cố bảo mật quan trọng đối với doanh nghiệp. Đầu mối liên hệ của tổ chức về các sự cố bảo mật, tuân thủ và các vấn đề liên quan đến bảo mật khác. |
| **Security EngineerSupport and Infrastructure** | Bằng cấp về khoa học máy tính, kỹ thuật máy tính hoặc bảo đảm thông tin, thường được kết hợp với các chứng chỉ như CISSP. | Một chuyên gia phần mềm hoặc phần cứng tập trung vào các khía cạnh bảo mật trong thiết kế hệ thống thông tin. Tạo ra các giải pháp và công cụ giúp các tổ chức đối phó mạnh mẽ với sự gián đoạn hoạt động hoặc các cuộc tấn công độc hại. Đôi khi được tuyển dụng trong SOC và đôi khi hỗ trợ SOC như một phần của nhóm phát triển hoặc vận hành. |

## Công Nghệ

Một phần quan trọng của công nghệ trong SOC là nền tảng tình báo bảo mật (xem Hình 2.2). Nền tảng này phải có khả năng lập chỉ mục tất cả các tệp nhật ký và dữ liệu máy có liên quan từ các nguồn bảo mật và không bảo mật trong thời gian thực. Nền tảng cũng phải có khả năng lấy dữ liệu và làm giàu dữ liệu bằng dữ liệu bên ngoài, chẳng hạn như dữ liệu từ Active Directory, cơ sở dữ liệu nội dung, nguồn cấp dữ liệu về mối đe dọa của bên thứ ba, v.v. Sự làm giàu bên ngoài này bổ sung bối cảnh quan trọng có thể được sử dụng trong các quy tắc tương quan thời gian thực để bảo vệ những tài sản và người dùng quan trọng nhất, cũng như vẽ nên một bức tranh hoàn chỉnh hơn trong quá trình điều tra sự cố. Sau đó, dữ liệu được lập chỉ mục và tra cứu bên ngoài có thể được tận dụng để đáp ứng các nhu cầu SOC chính, bao gồm cảnh báo và quy tắc tương quan theo thời gian thực, điều tra sự cố, bảng điều khiển và báo cáo tùy chỉnh cũng như phân tích nâng cao bao gồm phát hiện bất thường và ngoại lệ

A picture containing timeline

Description automatically generated

Hình 2. Nền tảng tình báo bảo mật sử dụng nhiều loại

dữ liệu để đáp ứng nhu cầu SOC

Đối với nhu cầu tương quan và cảnh báo, điều quan trọng là nền tảng phải linh hoạt để phát hiện các mối đe dọa thông qua một loạt các phương pháp phát hiện có thể tùy chỉnh, chính xác cao bao gồm các quy tắc tương quan, chấm điểm rủi ro và phát hiện bất thường, sau đó tự động chỉ định mức độ nghiêm trọng cho sự cố. Điều này cho phép nền tảng tự động lọc qua hàng trăm hoặc hàng nghìn sự kiện bảo mật hàng ngày và chỉ cảnh báo cho nhân viên SOC về những sự cố nghiêm trọng nhất. Nếu không có các phương pháp phát hiện linh hoạt, chính xác, các mối đe dọa sẽ bị bỏ sót và/hoặc nhân viên SOC sẽ bị quá tải với các thông tin xác thực sai. Nền tảng này cũng phải đủ thân thiện với người dùng để tất cả nhân viên SOC sử dụng và đủ linh hoạt để có thể tùy chỉnh nhằm đáp ứng các nhu cầu cụ thể của mọi quy trình và vai trò trong SOC. Có một số nguồn dữ liệu mà các nền tảng tình báo bảo mật cần lập chỉ mục và tận dụng (xem Hình 2.3). Mặc dù các nguồn dữ liệu cụ thể cho một tổ chức nhất định sẽ không được sử dụng trong quá trình lập mô hình mối đe dọa, nhưng thông thường, dữ liệu cần thiết sẽ đến từ bốn loại chính: thông tin tình báo về mối đe dọa, mạng, điểm cuối và xác thực. Với dữ liệu này, thông tin và manh mối cụ thể có thể được thu thập về một mối đe dọa, giúp kết nối các dấu chấm và theo dõi mối đe dọa từ khi xâm nhập đến khi thoát ra ngoài.

Diagram

Description automatically generated

Hình 2. Các nguồn dữ liệu mẫu cần thiết để phát hiện mối đe dọa nâng cao

## Tích Hợp SOC Với Splunk

* SOC yêu cầu đầu tư vào quy trình, con người và công nghệ
* Phần mềm Splunk có thể được sử dụng như một nền tảng tình báo an ninh để tăng sức mạnh SOC của bạn
* Phần mềm Splunk làm nhân sự SOC và quy trình hiệu quả hơn
* Phần mềm Splunk có thể bổ sung cho một SIEM hiện có trong SOC

Các sản phẩm của Splunk cung cấp một nền tảng thông minh bảo mật linh hoạt và nhanh chóng, giúp nhân viên SOC và các quy trình hoạt động hiệu quả hơn. Với phần mềm Splunk, tất cả nhân viên SOC đều có quyền truy cập nhanh vào tất cả dữ liệu và thông tin cần thiết để nhanh chóng phát hiện, điều tra và khắc phục các mối đe dọa. Splunk sản phẩm có thể được sử dụng

Các sản phẩm của Splunk cung cấp một nền tảng thông minh bảo mật linh hoạt và nhanh chóng, giúp nhân viên SOC và các quy trình hoạt động hiệu quả hơn. Với phần mềm Splunk, tất cả nhân viên SOC đều có quyền truy cập nhanh vào tất cả dữ liệu và thông tin cần thiết để nhanh chóng phát hiện, điều tra và khắc phục các mối đe dọa. Nhà phân tích cấp 1 có thể sử dụng các sản phẩm của Splunk để thực hiện nghiên cứu cơ bản dựa trên khoảng thời gian, từ khóa, địa chỉ IP hoặc tên máy. Các sản phẩm tương tự cho phép các nhà phân tích cấp 2/3 nâng cao thực hiện các tương quan nguồn dữ liệu chéo nâng cao, xây dựng các mô hình phân tích để phát hiện các điểm bất thường và ngoại lệ hoặc thực hiện điều tra nâng cao trên một máy bị xâm nhập. Splunk Enterprise Security cũng có sẵn, cung cấp các quy tắc dựng sẵn, báo cáo, nguồn cấp thông tin về mối đe dọa, phát hiện bất thường, chấm điểm rủi ro và khung điều tra sự cố. Phân tích hành vi người dùng Splunk cũng có thể được sử dụng như một lớp phát hiện bổ sung; nó sử dụng máy học không giám sát để tự động phát hiện các mối đe dọa bên ngoài và bên trong chưa biết, nâng cao.

Hơn nữa, phần mềm Splunk có thể giúp tự động hóa các quy trình ứng phó sự cố và sách hướng dẫn để giảm thời gian khắc phục và tăng hiệu quả. Điều này có thể được thực hiện bằng cách tùy chỉnh phần mềm Splunk để tự động hóa các quy trình ứng phó sự cố thủ công. Một ví dụ là tạo giao diện người dùng trong Splunk Enterprise, trong đó nhà phân tích có thể chỉ cần nhập phạm vi ngày và một IP/tên người dùng/tên máy chủ để nhận tất cả thông tin liên quan xung quanh thực thể được đề cập và điều tra sự cố nhanh hơn. Người dùng cũng có thể thêm các hành động bằng một cú nhấp chuột vào Giao diện người dùng Splunk, chẳng hạn như nhấp vào một sự kiện quan tâm bằng địa chỉ IP để tự động truy xuất tệp PCAP có liên quan cho IP đó từ công cụ chụp gói của bên thứ ba. Phần mềm Splunk được xây dựng cho quy mô và tốc độ. Nó sử dụng kho lưu trữ dữ liệu tệp phẳng (không phải cơ sở dữ liệu quan hệ có cấu trúc), tìm kiếm phân tán và cài đặt trên phần cứng hàng hóa. Nó cũng mở rộng quy mô theo chiều ngang để xử lý các nhu cầu lớn nhất và khắt khe nhất của các SOC toàn cầu. Phần mềm Splunk có thể lập chỉ mục hơn 100TB dữ liệu mỗi ngày và các tìm kiếm trên các tập dữ liệu khổng lồ sẽ trả về sau vài giây.

# SIEM

## Hệ Thống SIEM

### Khái Niệm

Hệ thống SIEM được viết tắt cụm từ tiếng Anh: Security Information and Event Management. SIEM là hệ thống quản lý nhật ký và sự kiện tập trung, có nhiệm vụ thu thập thông tin nhật ký, sự kiện trong toàn hệ thống doanh nghiệp và tổng hợp tất cả trên 1 giao diện duy nhất thay vì phải làm thủ công từng cái một.

### Chức Năng

Quản lý tập trung: Thu thập, lưu trữ tập trung nhật ký và sự kiện từ tất cả các thiết bị trên 1 giao diện giúp quản trị viên có được cái nhìn toàn diện về những gì đang xảy ra trong hệ thống.

Giám sát an toàn mạng: Phân tích thông tin qua các thuật toán, dự đoán các sự cố bảo mật giúp các bộ phận liên quan chủ động hơn trong công việc.

Xử lý sự cố hiệu quả: Đưa ra cảnh báo khi có xâm nhập trái phép để kịp thời xử lý và khắc phục sự cố nhanh nhất.

### Tính Năng

* Bảo mật dữ liệu.
* Toàn vẹn dữ liệu.
* Tính khả dụng cao.
* Phân tích chuyên sâu theo thời gian thực.
* Tích hợp báo cáo tiêu chuẩn hoặc tùy chỉnh theo yêu cầu của doanh nghiệp.

### Thành Phần

Hệ thống SIEM thường bao gồm 3 bộ phận chính. Đó là bộ phận thu thập nhật ký ATTT, phân tích và lưu trữ, quản trị tập trung.

* Thu thập nhật ký ATTT có chức năng thu thập nhật ký từ các thiết bị hoạt động. Sau khi dữ liệu được tập hợp sẽ được gửi toàn bộ về bộ phận phân tích và lưu trữ.
* Phân tích và lưu trữ có nhiệm vụ tiếp nhận, tổng hợp, phân tích và lưu trữ dữ liệu. Các thuật toán so sánh sau quá trình phân tích sẽ đưa ra cảnh báo (nếu có).
* Quản trị tập trung cung cấp giao diện quản lý tập trung cho toàn bộ hệ thống giám sát an ninh. Hàng ngàn mẫu báo cáo được tập hợp sẵn có thể sử dụng được ngay trong mọi trường hợp.

Mỗi bộ phận đều có chức năng và nhiệm vụ riêng biệt. Khi kết hợp hoạt động cùng lúc sẽ tạo nên giải pháp SIEM hoàn chỉnh, làm việc hiệu quả.

## Tổng Quan Là Lợi Ích Của Việc Tích Hợp

### Tại sao lại tích hợp splunk với các hệ thống quản lý siem?

Tích hợp Splunk với các hệ thống quản lý SIEM (Security Information and Event Management) như ArcSight, IBM QRadar hay LogRhythm cho phép tăng khả năng phát hiện và đối phó với các mối đe dọa bảo mật. Splunk có khả năng xử lý các loại dữ liệu phong phú và thường được sử dụng để phát hiện các sự kiện an ninh trong hệ thống. Các hệ thống SIEM cũng cung cấp các tính năng phân tích an ninh, tạo các cảnh báo và cung cấp khả năng quản lý sự cố để giúp các chuyên gia bảo mật đối phó với các mối đe dọa một cách nhanh chóng và hiệu quả hơn. Kết hợp cả hai công nghệ giúp tăng cường khả năng phát hiện, giảm thời gian xử lý sự cố và tăng tính toàn vẹn của hệ thống bảo mật.

### Lợi ích

* Nâng cao khả năng phát hiện: Splunk có khả năng phân tích và xử lý dữ liệu phong phú, giúp SIEM phát hiện các mối đe dọa an ninh một cách nhanh chóng và hiệu quả.
* Giảm thời gian xử lý sự cố: Kết hợp cả hai công nghệ giúp cung cấp thông tin an ninh chi tiết hơn, giảm thời gian cần thiết để tìm hiểu nguyên nhân của sự cố và tăng tính toàn vẹn của hệ thống.
* Tăng tính linh hoạt: Splunk cho phép định dạng và phân tích dữ liệu từ nhiều nguồn khác nhau, giúp SIEM hoạt động linh hoạt hơn trong việc phát hiện và giải quyết các sự cố an ninh.
* Cải thiện quản lý an ninh: Tích hợp Splunk với SIEM giúp cải thiện quản lý an ninh, cung cấp các tính năng phân tích và báo cáo an ninh chi tiết hơn, giúp tăng cường khả năng phát hiện các mối đe dọa an ninh và quản lý sự cố một cách hiệu quả hơn.
* Tiết kiệm chi phí: Tích hợp Splunk với SIEM giúp tối ưu hóa quá trình quản lý an ninh, giảm thời gian và chi phí đầu tư vào các hệ thống phát hiện và giải quyết các mối đe dọa an ninh.

### Quy trình tích hợp splunk

Quá trình tích hợp Splunk với các hệ thống quản lý SIEM bao gồm các bước sau:

* Chuẩn bị: Trước khi tích hợp, cần xác định các yêu cầu tích hợp và tài nguyên cần thiết, bao gồm tài khoản truy cập, quyền truy cập, cấu hình mạng và cấu hình bảo mật.
* Cấu hình: Sau khi đã chuẩn bị tài nguyên cần thiết, cần cấu hình Splunk để gửi dữ liệu đến SIEM thông qua giao thức hoặc định dạng dữ liệu được hỗ trợ.
* Đăng ký: Sau khi đã cấu hình Splunk, cần đăng ký các tệp tin và các trường dữ liệu được gửi đến SIEM để bảo đảm dữ liệu được gửi đúng định dạng.
* Kiểm tra: Sau khi đã cấu hình và đăng ký dữ liệu, cần kiểm tra tích hợp để đảm bảo dữ liệu được gửi đến SIEM một cách chính xác và hiệu quả.

Các thành phần liên quan trong quá trình tích hợp Splunk với SIEM bao gồm:

* Splunk: Là nơi lưu trữ, phân tích và xử lý dữ liệu.
* SIEM: Là nơi lưu trữ và phân tích dữ liệu an ninh, giúp phát hiện các mối đe dọa và quản lý các sự cố an ninh.
* Giao thức hoặc định dạng dữ liệu: Là các tiêu chuẩn để gửi dữ liệu từ Splunk đến SIEM, bao gồm syslog, CEF, LEEF và SNMP.
* Tài khoản và quyền truy cập: Các tài khoản và quyền truy cập được cấu hình để đảm bảo tích hợp được thực hiện đúng quy trình và có tính bảo mật.

Luồng dữ liệu trong quá trình tích hợp Splunk với SIEM gồm có các bước sau:

* Tất cả các sự kiện và dữ liệu từ các nguồn khác nhau được thu thập bởi Splunk. Các nguồn này có thể là máy chủ, thiết bị mạng, ứng dụng và các nguồn dữ liệu khác.
* Các sự kiện và dữ liệu được xử lý và lưu trữ trong Splunk để phục vụ cho các mục đích phân tích và giám sát tương lai.
* Các dữ liệu này sau đó được gửi đến SIEM để kiểm tra an ninh và phát hiện các mối đe dọa. SIEM sẽ xử lý và phân tích các dữ liệu này để phát hiện các mối đe dọa tiềm ẩn.
* Nếu SIEM phát hiện các mối đe dọa hoặc các cảnh báo an ninh, nó sẽ đưa ra các hành động phù hợp để giải quyết sự cố. Các hành động này có thể bao gồm thông báo cho các chuyên gia an ninh để giải quyết sự cố, đóng băng tài khoản người dùng hoặc cắt kết nối với các thiết bị mạng bị nhiễm độc.
* Trong quá trình phát hiện và giải quyết sự cố an ninh, SIEM có thể gửi các thông tin cập nhật và các cảnh báo cho Splunk để làm cơ sở dữ liệu cho các phân tích và giám sát tương lai. Quá trình này tạo ra một vòng lặp phân tích và phát hiện mối đe dọa liên tục giữa Splunk và SIEM, đảm bảo an ninh và bảo vệ hệ thống mạng khỏi các mối đe dọa an ninh tiềm ẩn.

## Các Ví Dụ Trong Thế Giới Thực

Splunk là một nền tảng phân tích dữ liệu phổ biến trong ngành an ninh thông tin, và việc tích hợp nó với hệ thống SIEM (Security Information and Event Management) có thể giúp tăng cường khả năng phát hiện, phân tích và ứng phó với các sự cố bảo mật. Dưới đây là một số ví dụ về cách các tổ chức đã sử dụng tích hợp Splunk và SIEM để nâng cao bảo mật của họ:

* Bank of America: Tập đoàn ngân hàng lớn này đã tích hợp Splunk với hệ thống SIEM để theo dõi các hoạt động mạng và phát hiện các mối đe dọa an ninh. Tích hợp này cho phép Bank of America nhanh chóng phân tích hàng triệu sự kiện an ninh mỗi ngày và tìm ra các hoạt động bất thường, giúp họ đưa ra quyết định nhanh chóng để bảo vệ hệ thống của mình.
* Cisco: Công ty công nghệ Cisco đã sử dụng Splunk để tích hợp với hệ thống SIEM của họ, giúp theo dõi các sự kiện mạng và phát hiện các mối đe dọa. Tích hợp này đã giúp Cisco nhanh chóng phát hiện các cuộc tấn công và bảo vệ dữ liệu của mình.
* Netflix: Công ty dịch vụ truyền phát trực tuyến Netflix đã tích hợp Splunk với hệ thống SIEM của mình để giúp phát hiện các sự cố mạng và bảo vệ dữ liệu khách hàng. Tích hợp này giúp Netflix theo dõi các sự kiện an ninh trong thời gian thực và phát hiện các mối đe dọa ngay lập tức.
* Verizon: Công ty viễn thông Verizon đã sử dụng Splunk và SIEM để phát hiện các cuộc tấn công mạng và giảm thiểu thiệt hại. Tích hợp này giúp Verizon nhanh chóng phân tích các dữ liệu an ninh và phát hiện các hoạt động bất thường trên mạng của họ.

## Kết Luận

Tóm tắt những điểm chính về tầm quan trọng của việc tích hợp Splunk với các hệ thống SIEM

Việc tích hợp Splunk với các hệ thống SIEM là rất quan trọng để tăng cường khả năng phát hiện, phân tích và ứng phó với các sự cố bảo mật trong thời gian thực. Điểm chính của việc tích hợp này bao gồm:

* Giúp theo dõi các sự kiện an ninh và phát hiện các mối đe dọa mạng trong thời gian thực.
* Tăng cường khả năng phân tích dữ liệu an ninh và giúp đưa ra quyết định nhanh chóng để bảo vệ hệ thống.
* Giúp giảm thiểu thiệt hại do các cuộc tấn công mạng và bảo vệ dữ liệu khách hàng.
* Nâng cao hiệu suất và khả năng phản ứng của các hệ thống an ninh thông tin.
* Giúp các tổ chức tối ưu hóa việc quản lý dữ liệu an ninh thông tin và giảm thiểu các rủi ro về an ninh.

# TẤN CÔNG RECONNAISSANCE

## Tấn Công Reconnaissance?

Bước đầu hacker ping đến tằm nhắm để xác định địa chỉ IP đích. Sau đó, hacker xác định những port cũng như những dịch vụ đang “sống” trên địa chỉ IP đó. Từ những thông tin này, hacker bắt đầu xác định được dạng và phiên bản của hệ điều hành. Hacker tiến hành đánh cắp dữ liệu hoặc phá huỷ hệ điều hành của mạng. Các hình thức tấn công dạng này bao gồm: packet sniffers, port scans, ping sweeps, internet information queries.

## Điều Tra Phân Tích Tình Huống Tấn Công Reconnaissance:

Điều tra phân tích tình huống tấn công Reconnaissance bằng Splunk là quá trình sử dụng công cụ phân tích dữ liệu của Splunk để phân tích tình huống tấn công trên hệ thống. Mục tiêu của điều tra này là nỗ lực khám phá và thu thập thông tin về mục tiêu.

Trong quá trình điều tra, có thể sử dụng các công cụ và tính năng của Splunk, chẳng hạn như tìm kiếm và truy vấn dữ liệu, biểu đồ và đồ thị, và cảnh báo tự động, để phân tích dữ liệu và tìm ra các dấu hiệu tấn công.

## Thực Hiện Điều Tra

### Tìm kiếm thông tin IP

* Tìm kiếm sâu hơn vào các weblog, xem nhật ký suricata và kiểm tra, phân tích liệu có các rules nào được kích hoạt hay không.
* Nhiều khả năng log suricata hoặc stream:http sẽ có thông tin chúng ta cần. Ở đây soi qua suricata.
* Search Query: index=\* sourcetype=suricata event\_type=alert | stats count by alert.signature

*Graphical user interface, text, application, email

Description automatically generated*

Hình 4. Các rules được kích hoạt trong weblog

* Xuất hiện ET WEB\_SERVER Script tag in URI, Possible Cross Site Scripting Attempt. tiến hành kiếm tra log attack XSS này
* Search Query: index =\* sourcetype=suricata event\_type =alert "alert.signature" = "ET WEB\_SERVER Script tag in URI, Possible Cross Site Scripting Attempt"

Graphical user interface, text, application

Description automatically generated

Hình 4. Xác định địa chỉ IP

* Ta xác định được địa chỉ IP là 40.803148.42

### Tiến hành tìm kiếm máy quét lỗ hổng

* Search Query: sourcetupe=stream:http src\_ip=40.803148.42 | stats count by http\_user\_agent

Graphical user interface, text, application

Description automatically generated

Hình 4. Kiểm tra máy quét

### Xem các sự kiện HTTP cho imreallynotbatman.com

* Querry:index="botsv1" sourcetype="stream:http" imreallynotbatman.com c\_ip="40.80.148.42" uri="/windows/win.ini"

Text

Description automatically generated

Hình 4. Các sự kiện HTTP

* Ta có thể thấy các URL tấn công rõ ràng, chẳng hạn như đường dẫn duyệt thư mục chứa ../../../../ được hiển thị với uri="/windows/win.ini“.
* Hệ quản trị nội dung quản lý trang web imreallynotbatman.com: Joomla
* Nhiều trường tiêu đề tham chiếu Trình quét lỗ hổng web. Cụ thể kẻ tấn công đang sử dụng trình quét web Acunetix để thực hiện quá trình quét.
* Công cụ sử dụng: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Graphical user interface, text, application, email

Description automatically generated

Hình 4. Hiển thị công cụ sử dụng trong sự kiện HTTP

### Tìm kiếm tệp đã làm defaced website

Querry: sourcetype=stream:http c\_ip=192.168.250.70 | stats count by uri

Graphical user interface, text, application, email

Description automatically generated

Hình 4. Tệp đã làm defaced website

### Tên miền đủ điều kiện hoàn toàn (FQDN) được liên kết với cuộc tấn công

Querry: sourcetype=stream:http c\_ip=192.168.250.70 uri="/poisonivy-is-coming-for-you-batman.jpeg"

Text

Description automatically generated

Hình 4. Tên miền được liên kết với cuộc tấn công

Tóm lại việc sử dụng Splunk để điều tra phân tích tình huống tấn công Reconnaissance cung cấp nhiều lợi ích, bao gồm:

* Tăng khả năng phát hiện và ngăn chặn tấn công: Splunk có thể phân tích và đánh giá các bản ghi log từ nhiều nguồn khác nhau, giúp phát hiện kịp thời các hành vi đáng ngờ và tấn công đang diễn ra trên hệ thống. Điều này giúp cải thiện khả năng phát hiện tấn công và giảm thiểu các rủi ro bảo mật.
* Cải thiện khả năng phân tích và truy xuất: Splunk cho phép người dùng tìm kiếm và phân tích các bản ghi log một cách nhanh chóng và hiệu quả. Các chức năng lọc dữ liệu, xem trước, truy vấn tìm kiếm và tạo đồ thị trong Splunk giúp người dùng dễ dàng tìm ra các thông tin cần thiết để phân tích tấn công Reconnaissance.
* Tăng hiệu quả trong phân tích tấn công Reconnaissance: Splunk cung cấp các tính năng phân tích và đánh giá dữ liệu mạnh mẽ như phân tích đối tượng (entity analytics), tạo đồ thị (graphing), phân tích chuỗi (string analytics), giúp người dùng dễ dàng phân tích và đánh giá các bản ghi log để phát hiện các tấn công installation và các mối đe dọa khác.

Vì vậy, việc sử dụng Splunk để điều tra phân tích tấn công installation cung cấp nhiều lợi ích và giúp cải thiện khả năng phát hiện, phân tích và phản ứng nhanh chóng với các tấn công Reconnaissance và các mối đe dọa khác.

# TẤN CÔNG INSTALLATION

## Tấn công Installation với Splunk là gì?

Splunk là 1 công cụ phân tích dữ liệu, là 1 giải pháp quản lý nhật ký và phân tích dữ liệu rất mạnh mẽ, cho phép người dùng thu thập, lưu trữ và phân tích các thông tin liên quan đến hoạt động của hệ thống.

Ví dụ: Thông tin đăng nhập, dữ liệu cá nhận hoặc thông tin chi tiết về hệ thống. Để tránh tấn công này, cần có 1 bảo mật tốt để bảo vệ dữ liệu và hệ thống, bao gồm việc cấu hình tốt Splunk và các biện pháp bảo mật khác nhau như cấu hình tường lửa, mã hóa dữ liệu và quản lý quyền truy cập.

Tấn công installation với Splunk là một kịch bản tấn công mà kẻ tấn công sử dụng Splunk để phát hiện, khai thác và tấn công các lỗ hổng liên quan đến cài đặt phần mềm và ứng dụng hệ thống.

## Tính năng của Splunk dùng để phân tích sự cố tấn công Installation

Splunk có thể thu thập các thông tin về các hoạt động cài đặt phần mềm và ứng dụng trên hệ thống, từ đó xác định được các lỗ hổng bảo mật có thể được khai thác với kẻ tấn công.

Cho phép người dùng tạo các truy vấn và báo cáo để theo dõi các hoạt động cuảnngười dùng và đối tượng trên hệ thống, nhằm phát hiện các hành vi đáng ngờ và các cuộc tấn công trong thời gian thực.

Ngoài ra, Splunk còn tích hợp nhiều công cụ bảo mật mạnh mẽ như phát hiện xâm nhập (IDS), chống virus và tường lửa, giúp người dùng giảm thiểu các mối đe dọa tiềm ẩn liên quan đến công tấn công Installation.

Hệ thống phát triển xâm nhập (IDS)

## Điều tra phân tích tình huống tấn công Installation:

Điều tra phân tích tình huống tấn công Installation bằng Splunk là quá trình sử dụng công cụ phân tích dữ liệu của Splunk để phân tích tình huống tấn công trên hệ thống. Mục tiêu của điều tra này là tìm ra nguyên nhân và phạm vi của tấn công, để có thể đưa ra giải pháp và ngăn chặn tấn công trong tương lai.

Trong quá trình điều tra, có thể sử dụng các công cụ và tính năng của Splunk, chẳng hạn như tìm kiếm và truy vấn dữ liệu, biểu đồ và đồ thị, và cảnh báo tự động, để phân tích dữ liệu và tìm ra các dấu hiệu tấn công.

Sau khi hoàn tất điều tra, có thể đưa ra những giải pháp để ngăn chặn tấn công trong tương lai và cải thiện tính bảo mật của hệ thống.

## Thực hiện điều tra

**Tìm kiếm thông tin trong bản ghi log**

* Search Query: index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" \*.exe
* Truy vấn này được sử dụng để lọc và tìm kiếm các thông tin trong bản ghi log. Ta thấy có 4 bản ghi log được lọc, “index=botsv1” lọc các bản ghi từ index có tên là botsv1, “sourcetype=stream:http” lọc các bản ghi liên quan đến việc truy cập http, “dest\_ip=‘192.168.250.70’” lọc các bản ghi log liên quan đến việc truy cập địa chi ip đích “192.168.250.70”, “\*exe” lọc các bản ghi log chỉ với tập tin kết thúc bằng “.exe”.
* Từ những điều kiện lọc đó, truy vấn sẽ trả về các bản ghi liên quan đến việc truy cập vào địa chỉ IP cụ thể và file thực thi có dạng “.exe” qua giao thức http.

Graphical user interface, text, application, email

Description automatically generated

Hình 5. Kết quả trả về khi thu hẹp lưu lượng truy cập

Graphical user interface, application

Description automatically generated

Hình 5. Nội dung trong file param=cmd.exe

* Có thể thấy ở trường part\_filename{} chứa 2 tệp: 3791.exe (tệp thi hành) và agent.php (tệp php).

Graphical user interface, application

Description automatically generated

Hình 5. Kết quả trả ở trườg part\_filename{}

* Tiếp theo, cần tìm xem có bất kỳ tệp nào trong số này đến từ các địa chỉ IP được cho là có liên quan đến cuộc tấn công trước đó hay không.
* Search Query: *index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" "part\_filename{}"="3791.exe"*
* Truy vấn này lọc các bản ghi các bản ghi log liên quan đến việc truy cập tới file “3791.exe”. Sau đó tìm kiếm ở trường *c\_ip* thì phát hiện địa chỉ ip 40.80.148.42 có liên quan đến cuộc tấn công trước đó.

Graphical user interface, text, application

Description automatically generated

Hình 5. Kết quả trả về ở trường c\_ip

Tóm lại việc sử dụng Splunk để điều tra phân tích tình huống tấn công Installation cung cấp nhiều lợi ích, bao gồm:

* Tăng khả năng phát hiện và ngăn chặn tấn công: Splunk có thể phân tích và đánh giá các bản ghi log từ nhiều nguồn khác nhau, giúp phát hiện kịp thời các hành vi đáng ngờ và tấn công đang diễn ra trên hệ thống. Điều này giúp cải thiện khả năng phát hiện tấn công và giảm thiểu các rủi ro bảo mật.
* Cải thiện khả năng phân tích và truy xuất: Splunk cho phép người dùng tìm kiếm và phân tích các bản ghi log một cách nhanh chóng và hiệu quả. Các chức năng lọc dữ liệu, xem trước, truy vấn tìm kiếm và tạo đồ thị trong Splunk giúp người dùng dễ dàng tìm ra các thông tin cần thiết để phân tích tấn công installation.
* Tăng khả năng phản ứng nhanh: Splunk cung cấp các cảnh báo và thông báo tự động, giúp người dùng phát hiện và đáp ứng nhanh chóng các sự kiện đáng ngờ. Nó cũng cung cấp các tính năng phân tích chi tiết và trực quan hóa dữ liệu, giúp người dùng đưa ra quyết định và phản ứng một cách chính xác và nhanh chóng.
* Tăng hiệu quả trong phân tích tấn công installation: Splunk cung cấp các tính năng phân tích và đánh giá dữ liệu mạnh mẽ như phân tích đối tượng (entity analytics), tạo đồ thị (graphing), phân tích chuỗi (string analytics), giúp người dùng dễ dàng phân tích và đánh giá các bản ghi log để phát hiện các tấn công installation và các mối đe dọa khác.

Vì vậy, việc sử dụng Splunk để điều tra phân tích tấn công installation cung cấp nhiều lợi ích và giúp cải thiện khả năng phát hiện, phân tích và phản ứng nhanh chóng với các tấn công installation và các mối đe dọa khác.