1. Tổng quan về SOC (Security Operations Center)

1.1 Giới thiệu về SOC

1.1.1 Khái niệm

- **SOC** hay **Security operations center** là một bộ phận chức năng hoặc đội ngũ tập trung chịu trách nhiệm cải thiện tình hình an ninh mạng của tổ chức cũng như ngăn chặn, phát hiện và ứng phó với các mối đe dọa. Đội ngũ **SOC**, có thể của cơ sở hoặc thuê ngoài, giám sát danh tính, điểm cuối, máy chủ, cơ sở dữ liệu, ứng dụng mạng, trang web và các hệ thống khác để phát hiện các cuộc tấn công qua mạng tiềm ẩn theo thời gian thực. Đội ngũ này cũng chủ động thực hiện công việc bảo mật bằng cách sử dụng thông tin về mối đe dọa mới nhất để cập nhật các nhóm phụ trách mối đe dọa và cơ sở hạ tầng, đồng thời xác định và giải quyết các lỗ hổng của hệ thống hoặc quy trình trước khi kẻ tấn công khai thác chúng. Hầu hết các **SOC** hoạt động hai mươi tư giờ một ngày, bảy ngày một tuần và ở các tổ chức lớn trải rộng trên nhiều quốc gia cũng có thể phụ thuộc vào một trung tâm hoạt động bảo mật toàn cầu (**GSOC**) để luôn cập nhật các mối đe dọa bảo mật trên toàn thế giới cũng như phối hợp phát hiện và ứng phó giữa một số **SOC** địa phương.
- **SOC** gồm có rất nhiều vai trò tùy thuộc vào từng mô hình cũng như quy mô tổ chức nhưng thông thường sẽ gồm các vai trò như sau:

Vai trò	Mô tả
Giám đốc ứng phó với sự cố	Điều phối việc phát hiện, phân tích, ngăn chặn và phục hồi khi xảy ra sự cố bảo mật. Quản lý liên lạc với các bên liên quan.
Quản lý SOC	Giám sát hoạt động của **SOC**, quản lý nhân sự, điều hành hoạt động và tài chính. Thường báo cáo cho Giám đốc bảo mật (**CISO**).
Kỹ sư bảo mật	Duy trì và phát triển hệ thống bảo mật của tổ chức, bao gồm thiết kế kiến trúc, nghiên cứu và triển khai giải pháp bảo mật.
Nhà phân tích bảo mật	Ứng phó đầu tiên trong sự cố, xác định và ưu tiên các mối đe dọa, thực hiện hành động hạn chế thiệt hại, như cách ly hệ thống.
Nhà tìm kiếm mối đe dọa	Xác định và ứng phó với mối đe dọa nâng cao, thường là các mối đe dọa chưa được phát hiện. Vai trò chủ động, nâng cao bảo mật.
Nhà phân tích điều tra số	Thu thập thông tin sau sự cố để xác định nguyên nhân gốc, tìm lỗ hổng hệ thống và vi phạm chính sách, ngăn chặn sự cố tương tự.

- Việc triển khai SOC là một bước quan trọng để bảo vệ tổ chức khỏi các mối đe dọa an ninh mạng ngày càng phức tạp và tinh vi. Do đó các tổ chức cần triển khai **SOC** để đề phòng và giải quyết các vấn đề một cách nhanh chóng.

1.1.2 Các chức năng chính của SOC và tầm quan trọng của SOC

- SOC đóng vai trò quan trọng trong việc bảo vệ tổ chức khỏi các mối đe dọa an ninh mạng, đảm bảo an toàn thông tin và duy trì hoạt động liên tục.
- **SOC** có một số chức năng chính như:

    - Phát hiện và phân tích sự cố: **SOC** sử dụng các công cụ và kỹ thuật tiên tiến để phát hiện các mối đe dọa và sự cố an ninh mạng. Việc phân tích chi tiết giúp xác định nguyên nhân gốc rễ và mức độ nghiêm trọng của sự cố.
    - Phản hồi sự cố và khắc phục hậu quả: Khi phát hiện sự cố, **SOC** sẽ thực hiện các biện pháp phản hồi nhanh chóng để ngăn chặn sự lây lan và giảm thiểu thiệt hại. Điều này bao gồm cô lập hệ thống bị ảnh hưởng, khôi phục dữ liệu và vá các lỗ hổng bảo mật.
    - Giám sát hệ thống liên tục: **SOC** cung cấp khả năng giám sát **24/7**, đảm bảo rằng mọi hoạt động đáng ngờ đều được phát hiện và xử lý kịp thời. Điều này giúp duy trì an ninh liên tục và ngăn chặn các cuộc tấn công tiềm ẩn.
- Ngoài các chức năng chính ở trên thì nhiệm vụ cụ thể của **SOC** có thể nói đến là:

Chức năng	Mô tả
Kiểm kê tài sản và công cụ	Theo dõi các tài sản cần bảo vệ và hiểu rõ các công cụ bảo mật, bao gồm cơ sở dữ liệu, dịch vụ đám mây, ứng dụng, điểm cuối.
Giảm bề mặt tấn công	Quản lý tài sản, áp dụng bản vá, xác định cấu hình sai, theo dõi mối đe dọa để giảm thiểu nguy cơ tấn công.
Giám sát liên tục	Giám sát toàn bộ môi trường 24/7, phát hiện bất thường qua **SIEM**, **SOAR**, *XDR* nhằm phát hiện kịp thời các hoạt động nguy hại.
Thông tin về mối đe dọa	Sử dụng phân tích dữ liệu và nguồn cấp bên ngoài để thu thập thông tin về các mối đe dọa và hành vi tấn công.
Phát hiện mối đe dọa	Lọc và ưu tiên các mối đe dọa từ dữ liệu **SIEM** và **XDR** để xác định các mối nguy nghiêm trọng nhất cho doanh nghiệp.
Ghi nhật ký hoạt động	Thu thập và phân tích dữ liệu log từ điểm cuối, OS, VM và mạng để xác định bất thường hoặc dấu hiệu của phần mềm gây hại.
Ứng phó sự cố	Hành động nhanh chóng để giảm thiểu thiệt hại, như cách ly điểm cuối, tạm ngừng tài khoản xâm nhập, và xóa file bị nhiễm.
Phục hồi và khắc phục	Khôi phục hệ thống về trạng thái trước sự cố, bao gồm phục hồi dữ liệu, ứng dụng, danh tính, và điểm cuối bị ảnh hưởng.
Điều tra nguyên nhân gốc rễ	Tìm hiểu lỗ hổng và quy trình bảo mật kém để ngăn chặn các sự cố tương tự trong tương lai.
Tinh chỉnh bảo mật	Sử dụng thông tin từ sự cố để cập nhật quy trình, chính sách và cải thiện lộ trình bảo mật.
Quản lý việc tuân thủ	Đảm bảo các công cụ và quy trình bảo mật tuân thủ các quy định như **GDPR, CCPA, HIPAA** và thông báo cho các bên sau vi phạm.

- Một **SOC** mạnh giúp các doanh nghiệp, chính phủ và các tổ chức khác luôn đón đầu tình hình mối đe dọa trên mạng đang ngày càng phát triển. Đây không phải là nhiệm vụ dễ dàng. Cả những kẻ tấn công và cộng đồng phòng thủ đều thường xuyên phát triển các công nghệ và chiến lược mới, đồng thời cần có thời gian và sự tập trung để quản lý tất cả những thay đổi đó. Bằng việc sử dụng kiến thức về môi trường an ninh mạng rộng hơn cũng như sự hiểu biết về các điểm yếu nội bộ và các ưu tiên kinh doanh, **SOC** giúp tổ chức phát triển lộ trình bảo mật phù hợp với nhu cầu dài hạn của doanh nghiệp.

SOC cũng có thể hạn chế tác động đến việc kinh doanh khi xảy ra cuộc tấn công. Vì họ liên tục giám sát mạng và phân tích dữ liệu cảnh báo nên họ có nhiều khả năng phát hiện ra các mối đe dọa sớm hơn so với một đội ngũ có nhiều ưu tiên khác. Với quy trình đào tạo thường xuyên và được ghi chép đầy đủ, **SOC** có thể giải quyết sự cố hiện tại một cách nhanh chóng—ngay cả khi chịu áp lực cực cao. Điều này có thể khó khăn đối với các đội ngũ không tập trung vào hoạt động bảo mật cả ngày, mọi ngày.

1.1.3 Các loại hình SOC

- **SOC on-premises**
    - Đặc điểm: SOC on-premises được triển khai trên cơ sở hạ tầng của tổ chức. Tất cả các thiết bị, công nghệ và nhân sự đều hoạt động tại cơ sở của tổ chức, tạo nên một hệ thống bảo mật độc lập.
    - Ưu điểm:
        - Độ kiểm soát cao: Tổ chức có toàn quyền quản lý và kiểm soát hệ thống, dữ liệu và quy trình bảo mật.
        - Tùy chỉnh linh hoạt: Có thể điều chỉnh phù hợp với các yêu cầu đặc thù của tổ chức.
        - Đảm bảo tuân thủ quy định: Dữ liệu lưu trữ tại chỗ dễ dàng tuân thủ các quy định nội bộ và pháp lý về bảo mật và quyền riêng tư.
    - Nhược điểm:
        - Chi phí cao: Cần đầu tư lớn cho cơ sở hạ tầng, nhân lực, công nghệ và bảo trì.
        - Khả năng mở rộng hạn chế: Mở rộng SOC on-premises có thể gặp khó khăn do hạn chế về hạ tầng.
        - Yêu cầu nhân lực: Đội ngũ SOC on-premises đòi hỏi nhiều chuyên gia với kiến thức và kỹ năng đa dạng.
- SOC đám mây (Cloud-based SOC)
    - Lợi ích:
        - Khả năng mở rộng linh hoạt: SOC đám mây có thể dễ dàng mở rộng theo nhu cầu của tổ chức mà không cần đầu tư vào hạ tầng vật lý.
        - Chi phí tối ưu: Giảm chi phí đầu tư ban đầu và chi phí duy trì, do hầu hết các tài nguyên được quản lý và duy trì bởi nhà cung cấp dịch vụ đám mây.
        - Khả năng truy cập từ xa: Đội ngũ có thể truy cập SOC từ bất kỳ đâu, cho phép giám sát và phản ứng nhanh chóng.
    - Yêu cầu kỹ thuật:
        - Độ bảo mật cao: Cần đảm bảo các tiêu chuẩn bảo mật và quyền riêng tư của dữ liệu trên đám mây.
        - Đảm bảo tuân thủ: Phải đáp ứng các quy định tuân thủ về bảo mật dữ liệu như GDPR, CCPA, hoặc các quy định nội bộ.
- SOC lai (Hybrid SOC)
    - Khi nào nên sử dụng mô hình lai:
        - Khi tổ chức cần sự linh hoạt: Mô hình lai cho phép kết hợp giữa SOC on-premises và SOC đám mây, phù hợp cho các tổ chức muốn tận dụng điểm mạnh của cả hai loại SOC.
        - Để duy trì quyền kiểm soát dữ liệu nhạy cảm: Các dữ liệu quan trọng có thể được giữ lại tại cơ sở, trong khi các dịch vụ và tài nguyên khác có thể hoạt động trên đám mây.
        - Giảm chi phí đầu tư và vận hành: SOC lai tối ưu chi phí bằng cách kết hợp tính linh hoạt của đám mây và tính bảo mật, kiểm soát của cơ sở hạ tầng tại chỗ.

- Dựa vào các đặc điểm của từng loại **SOC** trên ta có thể lựa chọn **SOC** phù hợp để sử dụng cho các tình huống thích hợp.
- Bảng so sánh dưới đây sẽ giúp mọi người phân biệt các loại **SOC** một cách dễ dàng hơn.

Loại hình SOC	Đặc điểm	Ưu điểm	Nhược điểm	Khi nào nên sử dụng
SOC on-premises	Triển khai trên cơ sở hạ tầng của tổ chức, toàn quyền quản lý tại chỗ	- Kiểm soát cao - Tùy chỉnh linh hoạt - Dễ đảm bảo tuân thủ quy định	- Chi phí cao - Khả năng mở rộng hạn chế - Yêu cầu nhân lực có kỹ năng cao	Khi yêu cầu bảo mật dữ liệu tối đa và có ngân sách
SOC đám mây (Cloud-based SOC)	Triển khai trên nền tảng đám mây, nhà cung cấp dịch vụ quản lý hạ tầng và bảo mật	- Khả năng mở rộng linh hoạt - Chi phí thấp hơn - Truy cập từ xa	- Cần đảm bảo bảo mật và tuân thủ trên đám mây - Phụ thuộc vào nhà cung cấp	Khi cần mở rộng nhanh chóng, chi phí tối ưu
SOC lai (Hybrid SOC)	Kết hợp SOC on-premises và SOC đám mây, dữ liệu nhạy cảm có thể lưu tại chỗ	- Linh hoạt cao - Kiểm soát dữ liệu nhạy cảm - Chi phí tối ưu	- Cần quản lý phức tạp giữa hai hệ thống - Đảm bảo tích hợp mượt mà giữa on-premises và đám mây	Khi cần bảo vệ dữ liệu nhạy cảm và tối ưu chi phí

1.2 Các thành phần trong SOC

1.2.1 Con người

- **SOC** bao gồm nhiều vai trò khác nhau, mỗi vai trò đòi hỏi kỹ năng và nhiệm vụ đặc thù:
    - **SOC Analyst (Nhà phân tích SOC):**
        - **Kỹ năng:** Kỹ năng phân tích bảo mật, kiến thức về mạng, hệ điều hành, khả năng xử lý sự cố.
        - **Nhiệm vụ:** Giám sát các sự kiện bảo mật, phát hiện mối đe dọa, phân loại và ưu tiên các sự kiện an ninh, xử lý các cảnh báo và phối hợp với đội ngũ để đảm bảo an toàn hệ thống.
    - **Incident Responder (Người ứng phó sự cố):**
        - **Kỹ năng:** Kỹ năng ứng phó khẩn cấp, phân tích tấn công mạng, quản lý rủi ro, kiến thức về bảo mật mạng.

        - **Nhiệm vụ:** Xác định, cô lập và ngăn chặn các mối đe dọa đã xác nhận; điều tra và phục hồi từ các cuộc tấn công; cung cấp thông tin về nguyên nhân sự cố để ngăn chặn các cuộc tấn công trong tương lai.
    - **Threat Hunter (Người tìm kiếm mối đe dọa):**
        - **Kỹ năng:** Khả năng tìm kiếm mối đe dọa chủ động, kỹ năng phân tích hành vi, am hiểu các kỹ thuật tấn công, khả năng điều tra trên toàn hệ thống.
        - **Nhiệm vụ:** Chủ động tìm kiếm các mối đe dọa chưa được phát hiện bởi hệ thống tự động; phát hiện các hành vi bất thường và dự đoán các xu hướng tấn công tiềm tàng.
    - **SOC Manager (Quản lý SOC):**
        - **Kỹ năng:** Quản lý đội ngũ, hiểu biết về bảo mật tổ chức, kỹ năng đánh giá rủi ro, kiến thức về tuân thủ quy định.
        - **Nhiệm vụ:** Giám sát và điều phối hoạt động của SOC, đào tạo nhân viên, đảm bảo các quy trình bảo mật tuân thủ các tiêu chuẩn tổ chức, báo cáo cho CISO hoặc các quản lý cấp cao khác. 1.2.2 Công nghệ
- Một vài công cụ cũng như hệ thống quen thuộc có thể nhắc đến trong **SOC** như là: SIEM, SOAR, IDS/IPS, và EDR.
- Các công cụ, hệ thống này có các chức năng cũng như nhiệm vụ khác nhau. Cụ thể thì:
    - **SIEM (Security Information and Event Management)**
        - **SIEM** là công cụ phân tích nhật ký từ các hệ thống khác nhau. Nó có khả năng phát hiện các bất thường trong dữ liệu nhật ký, đưa ra cảnh báo kịp thời, và cung cấp thông tin hữu ích để phân tích sự cố. SIEM là công cụ quan trọng trong việc cung cấp cái nhìn toàn diện và phát hiện sớm các mối đe dọa, giúp đội ngũ SOC phản ứng nhanh chóng.
    - **SOAR (Security Orchestration, Automation, and Response)**
        - **SOAR** là công cụ tự động hóa quy trình ứng phó sự cố, giúp SOC giảm tải công việc thủ công và tập trung vào các mối đe dọa quan trọng. SOAR tích hợp với các công cụ như SIEM, EDR và Threat Intelligence Platform, tự động điều phối các bước phản ứng, giảm thiểu thời gian từ khi phát hiện đến ứng phó sự cố.
    - **IDS/IPS ([Intrusion Detection and Prevention Systems(https://www.fortinet.com/resources/cyberglossary/what-is-an-ips#:~:text=How%20Intrusion%20Prevention%20Systems%20%28IPS%29%20work%3F%201%20Signature-based,and%20compares%20samples%20to%20performance%20level%20baselines.%20)])**
        - **IDS** giám sát và cảnh báo về các hành vi bất thường, trong khi IPS có thể chặn các hành vi này trước khi chúng gây hại. IDS/IPS cung cấp khả năng bảo vệ mạng bằng cách phát hiện các tấn công đã biết và chặn các hành vi độc hại, giúp bảo vệ hệ thống mạng của tổ chức khỏi các nguy cơ bên ngoài.
    - **EDR (Endpoint Detection and Response):**
        - **EDR** giám sát và phát hiện các hành vi đáng ngờ trên điểm cuối như máy tính và thiết bị di động, cung cấp công cụ để cô lập hoặc loại bỏ các điểm cuối bị tấn công, và bảo vệ tổ chức khỏi các mối đe dọa xuất phát từ điểm cuối. EDR đặc biệt hữu ích trong các cuộc tấn công nâng cao và mang đến khả năng phản ứng chi tiết đối với sự cố điểm cuối.
    - **Threat Intelligence Platform:**
        - Đây là nền tảng thu thập và phân tích dữ liệu về các mối đe dọa bên ngoài. Nó cung cấp thông tin về hành vi, cơ sở hạ tầng và động cơ của kẻ tấn công, giúp đội ngũ SOC nhận diện các mối đe dọa mới và lên kế hoạch phòng chống các rủi ro tiềm tàng.

- Để có thể thấy rõ được nhiệm vụ cũng như ưu nhược điểm của từng công cụ, hệ thống trên thì mình có làm bảng sau:

Công cụ	Chức năng chính	Ưu điểm	Nhược điểm
SIEM	Thu thập và phân tích dữ liệu từ nhiều nguồn, phát hiện mối đe dọa.	- Cung cấp cái nhìn toàn diện về hệ thống. - Tăng khả năng phát hiện sớm. - Dễ dàng tích hợp với các công cụ khác.	- Chi phí cao trong triển khai và bảo trì. - Đòi hỏi kỹ thuật chuyên sâu để cấu hình và quản lý. - Cần điều chỉnh liên tục để tránh các cảnh báo giả.
SOAR	Điều phối, tự động hóa và phản ứng với sự cố.	- Tự động hóa quy trình giúp giảm thời gian phản ứng. - Giảm thiểu tác động từ sự cố bảo mật.	- Chi phí triển khai và tích hợp cao. - Đòi hỏi khả năng tương tác cao với các công cụ hiện có.
IDS/IPS	Giám sát và ngăn chặn tấn công mạng, phát hiện hành vi bất thường.	- Cảnh báo nhanh và bảo vệ tức thì. - Giảm thiểu rủi ro từ các cuộc tấn công đã biết.	- Dễ bị đánh lừa bởi các phương pháp tấn công nâng cao. - Khó phát hiện các mối đe dọa mới mà không có mẫu sẵn có.
EDR	Phát hiện và phản ứng trên các điểm cuối.	- Bảo vệ điểm cuối khỏi các mối đe dọa. - Cung cấp khả năng điều tra sự cố.	- Yêu cầu giám sát và quản lý liên tục. - Cần tài nguyên lớn để triển khai trên toàn tổ chức.
Threat Intelligence Platform	Phân tích và dự đoán mối đe dọa.	- Dự báo và nhận diện mối đe dọa từ sớm. - Hỗ trợ ra quyết định phản ứng mối đe dọa.	- Có thể phức tạp trong việc tích hợp với SIEM hoặc SOAR. - Yêu cầu khả năng phân tích cao từ đội ngũ.

- Tuy có nhiều công cụ sử dụng nhưng SOC cần phải có một quy trình nhất định để sử dụng, tích hợp các công cụ, hệ thống vào SOC.
- Quy trình tích hợp công cụ vào SOC là một chuỗi các bước nhằm triển khai, kết nối, và tối ưu hóa các công cụ bảo mật khác nhau để phục vụ việc giám sát và phản ứng nhanh với các mối đe dọa. Mục tiêu chính là giúp đội ngũ SOC có được cái nhìn tổng quan, chính xác và kịp thời về các sự kiện bảo mật, từ đó giảm thiểu rủi ro cho tổ chức.
- **Quy trình gồm các bước chính:**
    - **Xác định nhu cầu và yêu cầu bảo mật:**
        - Đội ngũ SOC đánh giá các rủi ro, nhu cầu bảo mật, và những quy trình hiện có để xác định công cụ cần thiết, chẳng hạn như SIEM cho phân tích nhật ký, SOAR cho tự động hóa hoặc EDR cho quản lý điểm cuối.
    - **Lựa chọn công cụ phù hợp:**

        - Đánh giá các công cụ tiềm năng dựa trên khả năng, chi phí, mức độ phù hợp với hệ thống và khả năng tương thích với các công cụ hiện có. Điều này đảm bảo rằng công cụ được lựa chọn có thể dễ dàng tích hợp và hoạt động hiệu quả trong hệ thống hiện có.
    - **Thiết lập và cấu hình công cụ:**
        - Cài đặt và cấu hình công cụ theo đặc thù của hệ thống, bao gồm tích hợp dữ liệu từ các nguồn, thiết lập các cảnh báo và quy tắc phân tích, và điều chỉnh tùy chỉnh công cụ theo các yêu cầu bảo mật của tổ chức.
    - **Tích hợp công cụ vào hệ thống SOC:**
        - Đảm bảo rằng công cụ mới có thể giao tiếp và chia sẻ dữ liệu với các công cụ khác trong SOC. Các công cụ như SIEM hoặc SOAR đóng vai trò trung tâm trong việc tích hợp dữ liệu từ các nguồn khác, tạo ra cái nhìn toàn diện về hoạt động bảo mật.
    - **Đào tạo và cập nhật cho nhân viên SOC:**
        - Đào tạo đội ngũ SOC về cách sử dụng công cụ mới và tận dụng các tính năng quan trọng để phân tích và ứng phó sự cố. Đây là bước quan trọng để đảm bảo mọi người có thể sử dụng hiệu quả công cụ và hiểu được giá trị nó mang lại.
    - **Giám sát và cải tiến liên tục:**
        - Thường xuyên đánh giá và cải tiến việc tích hợp để đảm bảo công cụ hoạt động hiệu quả, điều chỉnh cấu hình nếu cần, và bổ sung các tính năng mới khi cần thiết. Việc này giúp đảm bảo các công cụ luôn đáp ứng nhu cầu bảo mật thay đổi của tổ chức.

1.2.3 Quy trình hoạt động của SOC

- Trong SOC, quy trình hoạt động đóng vai trò quan trọng giúp đội ngũ giám sát, phân tích và phản ứng với các mối đe dọa bảo mật một cách hiệu quả. Quy trình này có thể chia thành ba giai đoạn chính:

    - **Giai đoạn 1:**
        - **Phát hiện và phân tích sự cố (Detection and Analysis):**
            - Đây là giai đoạn đầu tiên, bao gồm giám sát và phát hiện các bất thường hoặc hoạt động đáng ngờ trong hệ thống. **SOC** sử dụng các công cụ như **SIEM, IDS/IPS và Threat Intelligence** để phát hiện các mối đe dọa.
            - Ở giai đoạn này việc **SOC** cần làm là:
                - **Phát hiện bất thường:** SOC giám sát các sự kiện trong hệ thống mạng, kiểm tra nhật ký và các dữ liệu đo từ xa để phát hiện những hành vi không mong muốn.
                - **Phân tích sự cố:** Khi một sự kiện được phát hiện, đội ngũ SOC sẽ điều tra để xác định nguồn gốc và đánh giá mức độ nghiêm trọng. Quá trình này bao gồm xác minh cảnh báo và loại bỏ các cảnh báo giả.
                - **Ưu tiên mối đe dọa:** Xác định mức độ ưu tiên dựa trên tính chất và tiềm năng tác động của mối đe dọa đối với tổ chức.
    - **Giai đoạn 2:**
        - **Phản ứng sự cố (Incident Response):**
            - Khi xác định được mối đe dọa thực sự, đội ngũ SOC sẽ tiến hành phản ứng nhanh chóng để hạn chế thiệt hại bằng các chuẩn bị trước đó cũng như phương pháp thích hợp có thể dùng:
                - **Kế hoạch ứng phó:** Xác định các bước cần thực hiện để giảm thiểu tác động. Các hành động có thể bao gồm cách ly hệ thống, khóa tài khoản bị xâm nhập, hoặc chặn các địa chỉ IP độc hại.

        - **Thực hiện hành động:** Tiến hành các biện pháp đã xác định trong kế hoạch, như cách ly thiết bị, vô hiệu hóa tài khoản, hoặc ngăn chặn lưu lượng truy cập độc hại.
        - **Báo cáo và giao tiếp:** Đảm bảo rằng các bên liên quan được thông báo và báo cáo chi tiết được lập ra để ghi lại sự cố. Điều này có thể bao gồm thông báo cho các bên liên quan nội bộ và tuân thủ các quy định pháp lý.
    - **Giai đoạn 3:**
        - **Điều tra nguyên nhân và phục hồi (Investigation and Recovery):**
            - Sau khi sự cố được xử lý, đội ngũ SOC sẽ tiến hành điều tra nguyên nhân và khắc phục để tránh các sự cố tương tự trong tương lai.
            - **Điều tra nguyên nhân gốc rễ:** Phân tích chi tiết để xác định nguyên nhân gây ra sự cố. Điều này giúp SOC hiểu rõ cách sự cố xảy ra và giảm thiểu rủi ro cho các sự cố tương tự.
            - **Phục hồi hệ thống:** Đảm bảo rằng hệ thống trở lại trạng thái an toàn trước đó. Các hoạt động phục hồi có thể bao gồm khôi phục dữ liệu, làm sạch hệ thống, và khởi động lại các dịch vụ.
            - **Cải tiến quy trình bảo mật:** Đánh giá lại quy trình bảo mật và cập nhật các chính sách hoặc quy trình nếu cần. Điều này giúp cải thiện khả năng phòng thủ của tổ chức và giảm thiểu rủi ro của sự cố trong tương lai.

- Một vài quy trình bảo mật phổ biến: **ITIL, NIST CSF**.

1. ITIL (Information Technology Infrastructure Library)

- **ITIL** là bộ hướng dẫn tiêu chuẩn cho việc quản lý dịch vụ công nghệ thông tin. Mặc dù không tập trung hoàn toàn vào bảo mật, ITIL cung cấp các quy trình có thể áp dụng vào bảo mật thông tin, bao gồm:
    - *__Quản lý sự cố (Incident Management):__ Quy trình này đảm bảo các sự cố bảo mật được phát hiện, phân tích và xử lý kịp thời. ITIL hỗ trợ cấu trúc quy trình phát hiện và ứng phó sự cố, giúp cải thiện hiệu quả của đội ngũ SOC.
    - *__Quản lý vấn đề (Problem Management):__ Tập trung vào việc điều tra nguyên nhân gốc rễ của sự cố và khắc phục các lỗ hổng trong hệ thống để tránh sự cố xảy ra lặp lại.
    - *__Quản lý thay đổi (Change Management):__ Giúp quản lý các thay đổi trong hệ thống một cách an toàn, giảm thiểu rủi ro liên quan đến các thay đổi có thể gây ra sự cố hoặc làm suy giảm bảo mật.
- **ITIL** giúp SOC duy trì quy trình nhất quán và chuyên nghiệp trong quản lý sự cố và vấn đề, cải thiện hiệu quả trong quá trình phản ứng với các mối đe dọa bảo mật.

2. NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)

- **NIST CSF** là một khuôn khổ bảo mật tập trung vào các hoạt động bảo mật quan trọng, phù hợp với các tổ chức muốn xây dựng quy trình bảo mật toàn diện. Khung NIST CSF bao gồm 5 giai đoạn chính:
    - **Xác định (Identify):** Tìm hiểu và đánh giá các rủi ro bảo mật, xác định tài sản và điểm yếu trong hệ thống.
    - **Bảo vệ (Protect):** Đưa ra các biện pháp bảo vệ như mã hóa, kiểm soát truy cập và bảo vệ điểm cuối để giảm thiểu nguy cơ bị tấn công.
    - **Phát hiện (Detect):** Xây dựng quy trình phát hiện các mối đe dọa một cách nhanh chóng, sử dụng các công cụ như SIEM hoặc IDS để giám sát và phát hiện sự cố.

    - **Phản ứng (Respond):** Đưa ra các kế hoạch và quy trình để ứng phó với sự cố khi nó xảy ra, giúp giảm thiểu tác động của sự cố.
    - **Phục hồi (Recover):** Khôi phục hệ thống sau sự cố và áp dụng các biện pháp cải tiến để ngăn ngừa sự cố tái diễn trong tương lai.
- **NIST CSF** tập trung mạnh vào việc quản lý rủi ro và khuyến khích các tổ chức xây dựng các quy trình bảo mật phù hợp với từng giai đoạn để nâng cao khả năng phòng thủ và ứng phó với các mối đe dọa.

Điểm khác nhau giữa ITIL và NIST CSF

Thành phần	ITIL (Information Technology Infrastructure Library)	NIST CSF (Cybersecurity Framework)
Mục tiêu chính	Quản lý dịch vụ công nghệ thông tin và tối ưu hóa quy trình quản lý sự cố, vấn đề, và thay đổi để nâng cao hiệu quả dịch vụ IT.	Tăng cường an ninh mạng, tập trung vào quản lý rủi ro và bảo mật, giúp tổ chức phòng ngừa, phát hiện, phản ứng và phục hồi trước các mối đe dọa.
Phạm vi ứng dụng	Tập trung vào quy trình IT, có thể áp dụng cho mọi loại sự cố, không chỉ bảo mật.	Tập trung chủ yếu vào bảo mật, phòng ngừa và quản lý rủi ro an ninh mạng.
Giai đoạn chính	- Quản lý sự cố - Quản lý vấn đề - Quản lý thay đổi	- Xác định (Identify) - Bảo vệ (Protect) - Phát hiện (Detect) - Phản ứng (Respond) - Phục hồi (Recover)
Ưu điểm	- Có hệ thống quy trình chuẩn, rõ ràng, dễ áp dụng cho mọi loại sự cố. - Cải thiện tính nhất quán và quản lý hiệu quả các sự cố.	- Cung cấp khung bảo mật toàn diện, tập trung vào an ninh mạng. - Tăng cường khả năng phát hiện và phản ứng nhanh trước các mối đe dọa.
Nhược điểm	- Không tập trung hoàn toàn vào bảo mật. - Thiếu tính linh hoạt khi chỉ tập trung vào quy trình sự cố IT chung.	- Có thể phức tạp với các tổ chức nhỏ do yêu cầu về nguồn lực và công cụ bảo mật chuyên biệt. - Cần triển khai công cụ bảo mật chuyên sâu (SIEM, IDS, v.v.).
Thích hợp cho	Các tổ chức muốn chuẩn hóa quy trình IT và quản lý hiệu quả dịch vụ công nghệ thông tin nói chung.	Các tổ chức muốn tập trung vào quản lý rủi ro bảo mật và nâng cao khả năng phòng thủ trước các mối đe dọa an ninh mạng.
Quy trình quản lý sự cố	Tập trung vào phát hiện, phân tích, và khắc phục sự cố IT nói chung.	Quy trình cụ thể cho từng giai đoạn bảo mật: xác định, bảo vệ, phát hiện, phản ứng và phục hồi sau sự cố.
Quản lý rủi ro	Không tập trung vào quản lý rủi ro bảo mật, chủ yếu là quản lý sự cố IT.	Quản lý rủi ro bảo mật là một phần trọng tâm, giúp tổ chức nhận diện và giảm thiểu các mối đe dọa mạng.

Thành phần	ITIL (Information Technology Infrastructure Library)	NIST CSF (Cybersecurity Framework)
Ví dụ về sử dụng	Các quy trình IT thường nhật, xử lý và quản lý dịch vụ IT và sự cố hệ thống.	Phòng ngừa và xử lý các cuộc tấn công mạng, quản lý rủi ro và bảo vệ dữ liệu nhạy cảm.

1.3 Mô hình và xu hướng phát triển SOC

1.3.1 So sánh SOC truyền thống và SOC trên đám mây

Thành phần	SOC Truyền Thống	SOC Trên Đám Mây
Hạ tầng	SOC truyền thống yêu cầu hệ thống vật lý, phần cứng và các thiết bị bảo mật tại chỗ.	SOC trên đám mây dựa vào hạ tầng và dịch vụ của nhà cung cấp đám mây, giảm bớt sự phụ thuộc vào phần cứng.
Chi phí	Chi phí đầu tư ban đầu cao, chi phí bảo trì thường xuyên.	Chi phí dựa trên mô hình đăng ký và sử dụng theo yêu cầu, giảm chi phí đầu tư ban đầu.
Khả năng mở rộng	Khó khăn trong việc mở rộng khi quy mô tăng lên do phải mua thêm phần cứng.	Dễ dàng mở rộng và linh hoạt theo nhu cầu mà không cần thay đổi phần cứng.
Bảo mật	Được kiểm soát trực tiếp, dễ dàng quản lý trong môi trường nội bộ.	Bảo mật phụ thuộc vào nhà cung cấp dịch vụ đám mây và các biện pháp bảo mật của họ.
Tính linh hoạt và hiệu quả	Tính linh hoạt thấp hơn, phụ thuộc vào tài nguyên phần cứng có sẵn.	Tính linh hoạt cao, có thể triển khai và cập nhật nhanh chóng mà không cần thay đổi hạ tầng.
Tính sẵn sàng và dự phòng	Cần các kế hoạch sao lưu và dự phòng phức tạp cho các hệ thống tại chỗ.	Các dịch vụ đám mây thường có khả năng phục hồi nhanh chóng và tính sẵn sàng cao nhờ hạ tầng toàn cầu.

1.3.2 Tích hợp MSSP (Managed Security Service Provider) với SOC nội bộ

Lợi ích của việc thuê ngoài dịch vụ bảo mật:

- **Tiết kiệm chi phí:** Thuê ngoài MSSP giúp giảm chi phí vận hành, đầu tư cơ sở hạ tầng và nhân sự.
- **Chuyên môn và tài nguyên:** MSSP cung cấp các chuyên gia bảo mật với kỹ năng và kinh nghiệm cao mà doanh nghiệp có thể thiếu.
- **Quản lý rủi ro:** MSSP giúp giảm thiểu rủi ro bằng cách phát hiện và xử lý các mối đe dọa ngay từ sớm.
- **Quản lý 24/7:** MSSP thường cung cấp dịch vụ giám sát và phản hồi sự cố liên tục, giúp doanh nghiệp không lo ngại về bảo mật vào các thời điểm không làm việc.

Cách MSSP hỗ trợ SOC trong giám sát và phản hồi sự cố:

- **Giám sát liên tục:** MSSP cung cấp giám sát liên tục và phân tích dữ liệu bảo mật từ mọi nguồn, bao gồm tường lửa, IDS/IPS, và hệ thống SIEM.
- **Phát hiện mối đe dọa:** MSSP sử dụng các công cụ mạnh mẽ để phát hiện các mối đe dọa mạng mới và dự đoán các mối đe dọa tiềm ẩn.
- **Phản ứng sự cố:** MSSP có thể ứng phó và giải quyết các sự cố ngay lập tức, giúp giảm thiểu thiệt hại và tổn thất cho tổ chức.
- **Phân tích sự cố:** MSSP sẽ điều tra nguyên nhân gốc rễ của sự cố, cung cấp báo cáo chi tiết và hướng dẫn khắc phục.

1.3.3 Xu hướng mới trong phát triển SOC

Tự động hóa và AI trong SOC:

- **Tự động hóa:** SOC đang sử dụng công nghệ tự động hóa để giảm tải công việc cho đội ngũ bảo mật. Việc tự động hóa các tác vụ như phân tích log, xử lý cảnh báo và phản ứng sự cố giúp tăng tốc độ phản ứng và giảm thiểu lỗi do con người gây ra.
- **AI và Machine Learning:** AI có thể giúp nhận diện các mối đe dọa mới mà các công cụ bảo mật truyền thống không phát hiện được. Machine learning cũng có thể cải thiện khả năng phát hiện bất thường và phân tích các mẫu tấn công phức tạp.
- **Phát hiện dựa trên hành vi:** AI giúp mô hình hóa hành vi bình thường của hệ thống và nhận diện các hành vi bất thường, từ đó phát hiện các mối đe dọa mà không cần phải có dấu hiệu rõ ràng.

Xây dựng SOC ảo hóa và SOC phân tán:

- **SOC ảo hóa:** Với SOC ảo, các công cụ bảo mật và quy trình SOC có thể hoạt động trên môi trường ảo, giúp linh hoạt hơn trong việc triển khai và bảo trì. Các SOC ảo cũng giúp giảm chi phí do không cần phải duy trì hạ tầng vật lý.
- **SOC phân tán:** SOC phân tán cho phép các nhóm bảo mật ở nhiều địa điểm khác nhau hoạt động một cách đồng bộ. Mô hình này giúp tăng cường khả năng giám sát toàn cầu và phản ứng nhanh chóng đối với các mối đe dọa trên diện rộng. Điều này đặc biệt hữu ích với các tổ chức có chi nhánh hoặc hoạt động toàn cầu.

2. Các mối đe dọa, chỉ số IoC và phương thức tấn công

2.1 Khái niệm về mối đe dọa và IoC (Indicator of Compromise)

2.1.1 Định nghĩa mối đe dọa và các loại mối đe dọa

- Mối đe dọa bảo mật (cyber threat) là bất kỳ yếu tố hoặc hành động nào có thể xâm nhập vào hệ thống và gây hại cho sự bảo mật của nó, như đánh cắp dữ liệu, tấn công DDoS, hay lây nhiễm phần mềm độc hại.

Các loại mối đe dọa:

- **Mối đe dọa từ bên ngoài (External Threats):** Được thực hiện bởi các tác nhân bên ngoài hệ thống như tin tặc, nhóm tội phạm mạng hoặc các tổ chức khủng bố.
- **Mối đe dọa từ nội bộ (Insider Threats):** Được thực hiện bởi những người trong tổ chức, bao gồm nhân viên, nhà thầu, hoặc bất kỳ ai có quyền truy cập hợp pháp vào hệ thống nhưng sử dụng quyền

này cho mục đích xấu.
- **Mối đe dọa từ nhà nước (State-Sponsored Threats):** Các cuộc tấn công được tổ chức bởi các cơ quan nhà nước hoặc các nhóm được nhà nước tài trợ với mục tiêu chính trị hoặc kinh tế.
- **Mối đe dọa từ tội phạm (Criminal Threats):** Các cuộc tấn công do các tổ chức tội phạm thực hiện, thường nhằm mục đích tài chính, ví dụ như đánh cắp thông tin thẻ tín dụng, tống tiền qua mã độc (ransomware).

2.1.2 Các loại chỉ số IoC phổ biến

IoC về mạng:

- **Địa chỉ IP:** Các địa chỉ IP được biết đến là nguồn tấn công hoặc đã được xác nhận là của các máy chủ tấn công.
- **Domain:** Các tên miền đáng ngờ hoặc đã được xác định là chứa các phần mềm độc hại hoặc có liên quan đến các cuộc tấn công mạng.

IoC về hệ thống:

- **File Hash:** Mã băm của các tập tin (MD5, SHA-1, SHA-256) có thể được sử dụng để nhận diện các tệp độc hại hoặc không hợp lệ trong hệ thống.
- **Mã độc:** Các đoạn mã độc hoặc phần mềm đã biết có thể chỉ ra rằng một cuộc tấn công đã xảy ra, như các loại virus, Trojan, worms.

IoC về ứng dụng:

- **URL độc hại:** Các URL mà người dùng có thể truy cập, nhưng có thể dẫn đến các trang web chứa phần mềm độc hại hoặc các cuộc tấn công phishing.
- **Hoạt động đăng nhập đáng ngờ:** Các mô hình đăng nhập không bình thường, chẳng hạn như nhiều lần thử đăng nhập sai hoặc đăng nhập từ vị trí không hợp lệ. **Ví dụ**

Loại IoC	Ví dụ	Mô tả
IoC về mạng	**Địa chỉ IP**	Địa chỉ IP của nguồn tấn công, máy chủ C2 (Command and Control), hoặc botnet. Ví dụ: 192.168.1.100, 45.77.248.156.
	Domain	Tên miền được liên kết với hành vi tấn công, lưu trữ mã độc hoặc thực hiện phishing. Ví dụ: malicious-site.com, example-evil.com.
IoC về hệ thống	**File Hash (MD5, SHA-256)**	Mã băm của các tệp độc hại đã được xác định, ví dụ: MD5: 098f6bcd4621d373cade4e832627b4f6, SHA-256: aeeed295b1de234a4d9fcd4d9bca0a11dbd034d6b79fe7c2fc564a06cb8a3cda.
	Mã độc	Tên của mã độc đã được xác định, ví dụ: Emotet, Ryuk Ransomware.
IoC về ứng dụng	**URL độc hại**	URL liên kết đến các tệp độc hại hoặc phishing sites. Ví dụ: http://malicious-link.com/exploit, http://fakebank.com/login.

Loại IoC	Ví dụ	Mô tả
	Hoạt động đăng nhập đáng ngờ	Các hành động đăng nhập bất thường hoặc từ địa chỉ IP không hợp lệ. Ví dụ: đăng nhập từ Trung Quốc trong khi người dùng ở Hoa Kỳ.

2.1.3 Tầm quan trọng của IoC trong phát hiện sự cố

IoC đóng vai trò quan trọng trong việc phát hiện và phân tích các mối đe dọa bảo mật. Chúng giúp các chuyên gia bảo mật xác định được các dấu hiệu của sự xâm nhập hoặc các hành động đáng ngờ đang xảy ra trong hệ thống.

Tầm quan trọng của IoC:

- **Phát hiện sớm:** IoC giúp nhận diện các cuộc tấn công ngay từ khi chúng bắt đầu, từ đó ngăn chặn thiệt hại lớn.
- **Ứng phó sự cố nhanh chóng:** IoC cung cấp các thông tin cần thiết để đội ngũ bảo mật có thể ứng phó kịp thời, như chặn IP xấu, cách ly máy chủ, hoặc loại bỏ mã độc.
- **Phân tích và điều tra:** IoC giúp trong quá trình phân tích các sự cố bảo mật để tìm hiểu nguyên nhân gốc rễ và khôi phục lại hệ thống.

2.2 Các phương thức tấn công phổ biến

2.2.1 Tấn công mạng truyền thống

Phương thức	Mô tả	Ví dụ
Phishing	Tấn công lừa đảo qua email hoặc trang web giả mạo, đánh lừa người dùng cung cấp thông tin cá nhân hoặc tài khoản.	Email giả mạo ngân hàng yêu cầu thay đổi mật khẩu.
DDoS (Distributed Denial of Service)	Tấn công từ chối dịch vụ phân tán nhằm làm tắc nghẽn hoặc hạ gục hệ thống mục tiêu bằng cách gửi một lượng lớn yêu cầu đồng thời.	Tấn công DDoS vào một trang web của tổ chức lớn.
Brute Force Attack	Tấn công thử mật khẩu bằng cách thử mọi khả năng có thể cho đến khi tìm ra mật khẩu đúng.	Tấn công vào tài khoản người dùng bằng cách thử nhiều mật khẩu.
SQL Injection	Tấn công vào cơ sở dữ liệu của ứng dụng web bằng cách chèn mã SQL độc hại vào đầu vào của người dùng để truy xuất hoặc thay đổi dữ liệu không được phép.	Nhập mã SQL vào ô tìm kiếm để truy cập thông tin bảo mật trong cơ sở dữ liệu.

2.2.2 Tấn công phần mềm độc hại

Phương thức	Mô tả	Ví dụ
Malware	Phần mềm độc hại được thiết kế để gây hại cho máy tính hoặc hệ thống, bao gồm virus, trojan, worm và nhiều loại khác.	Trojan horse cài đặt phần mềm gián điệp.
Ransomware	Phần mềm độc hại mã hóa dữ liệu và yêu cầu người dùng trả tiền chuộc để giải mã dữ liệu bị khóa.	WannaCry, NotPetya.
Spyware	Phần mềm gián điệp theo dõi hành động của người dùng mà không có sự đồng ý, thu thập dữ liệu nhạy cảm như thông tin đăng nhập và dữ liệu ngân hàng.	Phần mềm gián điệp theo dõi keylogger.

2.2.3 Tấn công nâng cao và lâu dài (APT)

Đặc điểm	Mô tả
APT	Các cuộc tấn công kéo dài, tinh vi và được thực hiện bởi những nhóm có mục tiêu cao như các tổ chức nhà nước hoặc tội phạm tổ chức, nhắm vào các tổ chức lớn.
Cách thức và mục tiêu chính	Thường bắt đầu với tấn công phishing hoặc lừa đảo, tiếp theo là xâm nhập vào hệ thống và duy trì quyền kiểm soát trong một thời gian dài, với mục đích thu thập thông tin hoặc phá hoại hệ thống.

2.2.4 Tấn công vào chuỗi cung ứng

Ví dụ	Mô tả
SolarWinds	Một trong các vụ tấn công nổi bật vào chuỗi cung ứng, tin tặc đã xâm nhập vào phần mềm quản lý của SolarWinds để lây lan mã độc vào các tổ chức lớn, bao gồm cả chính phủ Mỹ.
Nguy cơ bảo mật chuỗi cung ứng	Các tổ chức có thể bị tấn công qua các nhà cung cấp dịch vụ, đối tác hoặc nhà cung cấp phần mềm, khiến cho toàn bộ hệ thống bị xâm nhập qua một điểm yếu bên ngoài.

2.3 Quá trình thu thập và phân tích IoC

Quá trình	Mô tả
Thu thập IoC	Thu thập các chỉ số IoC từ nhiều nguồn như SIEM, hệ thống giám sát mạng, các công cụ bảo mật, và các báo cáo tấn công từ các tổ chức bảo mật.
Phân tích IoC	Phân tích các IoC thu thập được để xác định mối đe dọa, tìm hiểu về kẻ tấn công, các phương thức tấn công đã sử dụng, và các mục tiêu đã bị xâm nhập.
Đánh giá mối đe dọa	Đánh giá mức độ nghiêm trọng và tác động của các mối đe dọa để xác định hành động cần thiết (chặn, cách ly, báo cáo, v.v.).

2.2 Các phương thức tấn công phổ biến

2.2.1 Tấn công mạng truyền thống

Phương thức	Mô tả	Ví dụ
Phishing	Tấn công lừa đảo qua email hoặc trang web giả mạo, đánh lừa người dùng cung cấp thông tin cá nhân hoặc tài khoản.	Email giả mạo ngân hàng yêu cầu thay đổi mật khẩu.
DDoS (Distributed Denial of Service)	Tấn công từ chối dịch vụ phân tán nhằm làm tắc nghẽn hoặc hạ gục hệ thống mục tiêu bằng cách gửi một lượng lớn yêu cầu đồng thời.	Tấn công DDoS vào một trang web của tổ chức lớn.
Brute Force Attack	Tấn công thử mật khẩu bằng cách thử mọi khả năng có thể cho đến khi tìm ra mật khẩu đúng.	Tấn công vào tài khoản người dùng bằng cách thử nhiều mật khẩu.
SQL Injection	Tấn công vào cơ sở dữ liệu của ứng dụng web bằng cách chèn mã SQL độc hại vào đầu vào của người dùng để truy xuất hoặc thay đổi dữ liệu không được phép.	Nhập mã SQL vào ô tìm kiếm để truy cập thông tin bảo mật trong cơ sở dữ liệu.

2.2.2 Tấn công phần mềm độc hại

Phương thức	Mô tả	Ví dụ
Malware	Phần mềm độc hại được thiết kế để gây hại cho máy tính hoặc hệ thống, bao gồm virus, trojan, worm và nhiều loại khác.	Trojan horse cài đặt phần mềm gián điệp.
Ransomware	Phần mềm độc hại mã hóa dữ liệu và yêu cầu người dùng trả tiền chuộc để giải mã dữ liệu bị khóa.	WannaCry, NotPetya.
Spyware	Phần mềm gián điệp theo dõi hành động của người dùng mà không có sự đồng ý, thu thập dữ liệu nhạy cảm như thông tin đăng nhập và dữ liệu ngân hàng.	Phần mềm gián điệp theo dõi keylogger.

2.2.3 Tấn công nâng cao và lâu dài (APT)

Đặc điểm	Mô tả
APT	Các cuộc tấn công kéo dài, tinh vi và được thực hiện bởi những nhóm có mục tiêu cao như các tổ chức nhà nước hoặc tội phạm tổ chức, nhắm vào các tổ chức lớn.
Cách thức và mục tiêu chính	Thường bắt đầu với tấn công phishing hoặc lừa đảo, tiếp theo là xâm nhập vào hệ thống và duy trì quyền kiểm soát trong một thời gian dài, với mục đích thu thập thông tin hoặc phá hoại hệ thống.

2.2.4 Tấn công vào chuỗi cung ứng

Ví dụ	Mô tả
SolarWinds	Một trong các vụ tấn công nổi bật vào chuỗi cung ứng, tin tặc đã xâm nhập vào phần mềm quản lý của SolarWinds để lây lan mã độc vào các tổ chức lớn, bao gồm cả chính phủ Mỹ.
Nguy cơ bảo mật chuỗi cung ứng	Các tổ chức có thể bị tấn công qua các nhà cung cấp dịch vụ, đối tác hoặc nhà cung cấp phần mềm, khiến cho toàn bộ hệ thống bị xâm nhập qua một điểm yếu bên ngoài.

2.3 Quá trình thu thập và phân tích IoC

- Thông qua việc thu thập và phân tích IoC, các tổ chức có thể nâng cao khả năng phát hiện các cuộc tấn công và giảm thiểu thiệt hại từ các mối đe dọa bảo mật.

2.3.1 Nguồn thu thập IoC

- **Threat Intelligence Feeds:** Là các nguồn thông tin tình báo về mối đe dọa từ các tổ chức bảo mật hoặc dịch vụ thương mại. Chúng cung cấp các chỉ số **IoC** mới nhất, như địa chỉ **IP, hash file, URL độc hại**, giúp phát hiện mối đe dọa đang tiềm ẩn.
- **Open-source Threat Intelligence (OTI):** Đây là các nguồn thông tin tình báo mối đe dọa mã nguồn mở, thường được chia sẻ miễn phí. Các nền tảng như **MISP (Malware Information Sharing Platform)** và **OpenDXL** cung cấp dữ liệu về mối đe dọa và IoC từ cộng đồng bảo mật.

2.3.2 Quy trình phân tích và xác minh IoC

- **MISP (Malware Information Sharing Platform):** Là một nền tảng mã nguồn mở cho phép thu thập, phân tích và chia sẻ thông tin về mối đe dọa. **MISP** có thể giúp tổ chức tự động phân loại và xác minh các **IoC** để cung cấp thông tin rõ ràng về các mối đe dọa và nguy cơ.
- **VirusTotal:** Công cụ giúp phân tích các file hoặc URL nghi ngờ. **VirusTotal** so sánh dữ liệu với các cơ sở dữ liệu từ nhiều công cụ bảo mật, xác minh xem chúng có phải là phần mềm độc hại hay không.

2.3.3 Tích hợp IoC vào hệ thống SIEM và SOC

- **Tích hợp IoC vào SIEM:** Các chỉ số IoC được tích hợp vào hệ thống quản lý thông tin và sự kiện bảo mật (SIEM), giúp tổ chức tự động hóa quá trình giám sát, phát hiện mối đe dọa và cảnh báo. SIEM có thể sử dụng các IoC từ các nguồn như feeds tình báo hoặc dữ liệu nội bộ để nhận diện sự cố bảo mật.
- **Tích hợp IoC vào SOC:** Trung tâm điều hành bảo mật (SOC) sử dụng các IoC để phát hiện các mối đe dọa, triển khai các biện pháp ứng phó sự cố và giám sát liên tục các tài sản, hệ thống trong tổ chức. Các IoC giúp SOC hiểu rõ hơn về các mối đe dọa, tăng khả năng phản ứng nhanh chóng và hiệu quả hơn.

3. Sự cố là gì? Quản lý sự cố an toàn thông tin

3.1 Khái niệm về sự cố an toàn thông tin

3.1.1 Định nghĩa và phân biệt các loại sự cố

- **Sự cố bảo mật**: Là sự kiện không mong muốn hoặc hành vi không hợp lệ có thể ảnh hưởng đến tính bảo mật của hệ thống, thông tin hoặc dữ liệu trong tổ chức. Các sự cố bảo mật có thể bao gồm tấn công mạng, xâm nhập hệ thống, đánh cắp dữ liệu, hay hành vi gian lận.
- **Sự cố hệ thống**: Là sự kiện làm gián đoạn hoạt động của các hệ thống công nghệ thông tin, chẳng hạn như sự cố phần cứng, sự cố mạng, hoặc lỗi phần mềm, gây ảnh hưởng đến khả năng hoạt động của các dịch vụ và ứng dụng.

3.1.2 Dấu hiệu nhận biết sự cố an toàn thông tin

Các dấu hiệu nhận biết sự cố an toàn thông tin có thể bao gồm:

- **Tăng truy cập bất thường**: Các yêu cầu truy cập bất thường từ các địa chỉ IP không xác định, tần suất truy cập tăng đột ngột vào các tài nguyên quan trọng.
- **Tải dữ liệu đáng ngờ**: Việc tải xuống hoặc truyền tải dữ liệu bất thường, ví dụ như việc sao chép số lượng lớn dữ liệu nhạy cảm ra khỏi hệ thống hoặc truyền tải qua các kênh không an toàn.

3.1.3 Tầm quan trọng của việc phát hiện và quản lý sự cố kịp thời

- Việc phát hiện và quản lý sự cố an toàn thông tin kịp thời có vai trò rất quan trọng trong việc giảm thiểu thiệt hại do các cuộc tấn công mạng, bảo vệ thông tin nhạy cảm và duy trì hoạt động liên tục của tổ chức. Khi sự cố được phát hiện và phản ứng nhanh chóng, tổ chức có thể:
    - Giảm thiểu tác động và thiệt hại về tài chính và uy tín.
    - Ngăn chặn hoặc làm chậm sự lây lan của cuộc tấn công.
    - Cải thiện khả năng bảo mật của tổ chức thông qua việc học hỏi từ các sự cố đã xảy ra.

3.2 Quy trình quản lý sự cố (Incident Management)

3.2.1 Chuẩn bị và phòng ngừa

- **Xây dựng quy trình**: Định nghĩa rõ ràng các bước cần thiết để phát hiện, phản ứng và xử lý sự cố. Các quy trình này cần được tài liệu hóa và thông qua toàn bộ tổ chức.
- **Chuẩn bị công cụ**: Cung cấp các công cụ và phần mềm cần thiết để phát hiện sự cố, giám sát hệ thống, và hỗ trợ phản ứng sự cố. Các công cụ này có thể bao gồm hệ thống **SIEM, EDR, IDS/IPS**, và các công cụ tự động hóa.
- **Chính sách nội bộ**: Phát triển và triển khai các chính sách bảo mật, bao gồm các yêu cầu về bảo mật dữ liệu, quyền truy cập hệ thống, và quy trình phản ứng sự cố. Đảm bảo mọi nhân viên được huấn luyện về chính sách và quy trình này.

3.2.2 Phát hiện và phân tích sự cố

- **Các công cụ hỗ trợ phát hiện sự cố**:
    - **SIEM** (Security Information and Event Management): Phân tích dữ liệu sự kiện và nhật ký từ nhiều nguồn khác nhau để phát hiện các hành vi bất thường hoặc sự cố bảo mật.
    - **IDS/IPS** (Intrusion Detection/Prevention Systems): Phát hiện và ngăn chặn các cuộc tấn công xâm nhập vào hệ thống.
    - **EDR** (Endpoint Detection and Response): Giám sát và phân tích hành vi của các điểm cuối (endpoints) để phát hiện các mối đe dọa.
    - **SOAR** (Security Orchestration, Automation and Response): Tự động hóa các quy trình phản ứng sự cố và cải thiện thời gian xử lý sự cố.

3.2.3 Cô lập, loại bỏ và khôi phục hệ thống sau sự cố

- **Cách ly vùng bị tấn công**: Khi phát hiện một sự cố, nhanh chóng cô lập vùng bị ảnh hưởng (máy chủ, hệ thống hoặc mạng) để ngăn chặn sự lây lan của mối đe dọa.
- **Làm sạch hệ thống**: Sau khi cô lập, tiến hành quét và xóa các mã độc, phần mềm tấn công, hoặc bất kỳ phần mềm gây hại nào khỏi hệ thống.
- **Khôi phục hoạt động**: Sau khi làm sạch, khôi phục hệ thống từ bản sao lưu hoặc các biện pháp khác để đưa hệ thống trở lại hoạt động bình thường, bảo đảm rằng không có mối đe dọa nào còn tồn tại.

3.2.4 Đánh giá và cải tiến sau sự cố

- **Xây dựng báo cáo**: Sau khi sự cố được xử lý, tổ chức cần xây dựng một báo cáo chi tiết về sự cố, các biện pháp đã thực hiện, và các tác động của sự cố.
- **Đánh giá**: Đánh giá hiệu quả của các quy trình phản ứng sự cố, xác định các lỗ hổng hoặc điểm yếu trong hệ thống bảo mật hoặc quy trình.
- **Điều chỉnh và nâng cao quy trình**: Dựa trên bài học từ sự cố, cải thiện quy trình, công cụ, và chính sách bảo mật để ngăn chặn sự cố tái diễn và nâng cao khả năng phản ứng trong tương lai.

3.3 Chính sách và quy định về quản lý sự cố

3.3.1 Quy định nội bộ về an toàn thông tin

- **Xây dựng chính sách về quy trình quản lý sự cố**:
  - **Chính sách bảo mật**: Tạo ra một chính sách bảo mật toàn diện cho tổ chức, quy định rõ ràng các bước phản ứng và xử lý sự cố bảo mật. Chính sách này cần bao gồm các quy trình cụ thể về phát hiện sự cố, phân loại, đánh giá mức độ nghiêm trọng, cũng như các hành động khắc phục.
  - **Vai trò và trách nhiệm**: Xác định rõ các vai trò và trách nhiệm của từng cá nhân hoặc nhóm trong quy trình xử lý sự cố, từ người quản lý hệ thống đến nhân viên IT và đội ngũ bảo mật.
  - **Phân loại sự cố**: Các quy định cần phân loại sự cố theo mức độ nghiêm trọng và các tác động tiềm ẩn đối với tổ chức, từ sự cố ít nghiêm trọng (ví dụ: sự cố phần mềm) đến các sự cố nghiêm trọng có thể ảnh hưởng đến toàn bộ hoạt động của doanh nghiệp (ví dụ: tấn công mạng).

3.3.2 Tuân thủ tiêu chuẩn quốc tế

- **ISO 27001**:
  - Là tiêu chuẩn quốc tế về hệ thống quản lý an toàn thông tin (ISMS). ISO 27001 yêu cầu tổ chức thực hiện các biện pháp bảo vệ thông tin của mình, bao gồm quy trình quản lý sự cố.
  - Đảm bảo rằng các sự cố an toàn thông tin được phát hiện kịp thời và có quy trình phản ứng hiệu quả.
- **NIST (National Institute of Standards and Technology)**:
  - NIST cung cấp bộ hướng dẫn về bảo mật thông tin và quản lý sự cố, bao gồm tiêu chuẩn NIST SP 800-61, quy định các bước quản lý sự cố an toàn thông tin, từ phát hiện đến khắc phục.
  - Các tổ chức có thể sử dụng tiêu chuẩn này để thiết lập quy trình quản lý sự cố của mình và cải thiện khả năng ứng phó.
- **PCI-DSS (Payment Card Industry Data Security Standard)**:

- Tiêu chuẩn bảo mật cho ngành công nghiệp thẻ thanh toán. PCI-DSS yêu cầu các tổ chức xử lý thẻ tín dụng phải có các quy trình quản lý sự cố để bảo vệ thông tin thẻ thanh toán.
- Quy trình này bao gồm việc giám sát và phát hiện sự cố bảo mật có thể ảnh hưởng đến dữ liệu thẻ thanh toán, cùng với các biện pháp khắc phục và báo cáo sự cố.

3.3.3 Đánh giá rủi ro và lập kế hoạch quản lý sự cố

- **Đánh giá rủi ro**:
  - Tổ chức cần thực hiện các đánh giá rủi ro thường xuyên để xác định các mối đe dọa và lỗ hổng có thể gây ra sự cố bảo mật. Việc này giúp chuẩn bị các biện pháp phòng ngừa và giảm thiểu rủi ro.
  - Các phương pháp đánh giá rủi ro có thể bao gồm phân tích lỗ hổng, kiểm tra xâm nhập, và phân tích ảnh hưởng của các mối đe dọa.
- **Lập kế hoạch quản lý sự cố**:
  - **Kế hoạch chuẩn bị**: Xây dựng các kịch bản sự cố và các biện pháp ứng phó tương ứng để có thể hành động nhanh chóng khi sự cố xảy ra.
  - **Kế hoạch phục hồi**: Đảm bảo rằng các hệ thống và dữ liệu quan trọng có thể được khôi phục nhanh chóng sau sự cố thông qua các bản sao lưu và các biện pháp khôi phục.
  - **Đào tạo và thử nghiệm**: Đảm bảo rằng đội ngũ nhân viên được đào tạo đầy đủ và các quy trình ứng phó sự cố được kiểm tra định kỳ thông qua các bài tập mô phỏng sự cố để đánh giá tính hiệu quả.

4. Event và Logging

4.1 Khái niệm về sự kiện (Event) và bản ghi (Logging)

4.1.1 Định nghĩa Event và Log

- **Sự kiện (Event)**: Là những thay đổi hoặc hoạt động quan trọng trong hệ thống mà cần được ghi nhận và theo dõi. Ví dụ bao gồm người dùng đăng nhập, cài đặt phần mềm mới, hoặc một cuộc tấn công mạng. Các sự kiện có thể bao gồm cả hành vi bình thường và các hành vi không bình thường, có thể dẫn đến sự cố bảo mật.
- **Log**: Là bản ghi chi tiết về các sự kiện xảy ra trong hệ thống. Log có thể được tạo ra bởi hệ điều hành, phần mềm, phần cứng hoặc bất kỳ hệ thống nào khác trong môi trường công nghệ thông tin. Các log này giúp xác định những hoạt động xảy ra trong một thời gian nhất định, và có thể cung cấp thông tin quan trọng khi phân tích các sự cố bảo mật.

4.1.2 Các loại log trong hệ thống

- **Log hệ thống**: Là bản ghi các sự kiện liên quan đến hoạt động của hệ điều hành và các thành phần hệ thống. Các log này thường ghi nhận các hoạt động như khởi động lại hệ thống, lỗi hệ thống, hoặc thay đổi cấu hình.
- **Log ứng dụng**: Là bản ghi các sự kiện xảy ra trong các ứng dụng phần mềm. Chúng có thể ghi lại các hành động của người dùng, lỗi ứng dụng, hoặc bất kỳ sự kiện quan trọng nào trong quá trình chạy ứng dụng.

- **Log bảo mật**: Là bản ghi các sự kiện liên quan đến bảo mật hệ thống, như đăng nhập thất bại, thay đổi quyền truy cập, các cuộc tấn công hoặc hành vi đáng ngờ khác. Log bảo mật đóng vai trò quan trọng trong việc phát hiện các cuộc tấn công hoặc truy cập trái phép.

4.1.3 Tầm quan trọng của log trong phát hiện và điều tra sự cố

- **Phát hiện sự cố**: Logs là công cụ quan trọng để phát hiện và nhận diện các sự cố bảo mật. Chúng cung cấp thông tin về các sự kiện bất thường hoặc hành vi đáng ngờ trong hệ thống, từ đó giúp phát hiện các cuộc tấn công hoặc xâm phạm hệ thống.
- **Điều tra sự cố**: Khi một sự cố xảy ra, logs là nguồn thông tin chủ yếu để phân tích nguyên nhân và xác định phạm vi của sự cố. Chúng cung cấp các chi tiết về những gì đã xảy ra, khi nào, và ai là người thực hiện, giúp các chuyên gia bảo mật điều tra và xử lý sự cố hiệu quả hơn.

4.2 Quy trình quản lý log

4.2.1 Chu trình lưu trữ và quản lý log

- **Cách thức lưu trữ log**:
  - **Lưu trữ tập trung**: Các log từ tất cả các hệ thống, ứng dụng và thiết bị sẽ được gửi về một điểm tập trung duy nhất để lưu trữ và quản lý. Điều này giúp dễ dàng theo dõi, phân tích và bảo mật log từ nhiều nguồn khác nhau.
  - **Lưu trữ phân tán**: Các log được lưu trữ tại các điểm khác nhau, gần với nguồn log. Mỗi hệ thống hoặc nhóm thiết bị có thể có hệ thống lưu trữ riêng biệt, điều này có thể cải thiện hiệu quả truy vấn và giảm tải cho các điểm tập trung.

4.2.2 Phân loại và lọc log

- **Phân loại log**:
  - Các log cần được phân loại theo các tiêu chí như mức độ quan trọng (log hệ thống, log ứng dụng, log bảo mật), thời gian, hoặc nguồn gốc của sự kiện.
  - Phân loại giúp dễ dàng tìm kiếm và quản lý log, đồng thời xác định mức độ ưu tiên trong việc xử lý các log trong trường hợp có sự cố.
- **Lọc log**:
  - Lọc log là quá trình xác định và loại bỏ các log không quan trọng hoặc dư thừa. Điều này giúp giảm thiểu dữ liệu không cần thiết và giúp tiết kiệm không gian lưu trữ.
  - Các log không cần thiết có thể là các thông tin hệ thống cơ bản không ảnh hưởng đến bảo mật hoặc các sự kiện đã được xử lý xong mà không gây nguy cơ.

4.2.3 Phân tích log và phát hiện sự cố từ log

- **Phân tích log**:
  - Phân tích log giúp nhận diện các sự kiện bất thường hoặc hành vi đáng ngờ. Các công cụ phân tích như SIEM có thể tự động kiểm tra các log để phát hiện các mẫu tấn công hoặc xâm nhập.
  - Việc phân tích thường xuyên giúp phát hiện các mối đe dọa trong thời gian sớm nhất, từ đó ngăn chặn các sự cố xảy ra.

- **Phát hiện sự cố từ log**:
    - Các dấu hiệu từ log có thể chỉ ra sự cố đang diễn ra, chẳng hạn như các lỗi đăng nhập nhiều lần, các truy cập trái phép hoặc bất thường vào hệ thống.
    - Phân tích các mẫu log giúp xác định được nguyên nhân của sự cố và mức độ nghiêm trọng của nó, từ đó đưa ra các biện pháp ứng phó kịp thời.

4.3 Yêu cầu lưu trữ log và tuân thủ quy định

4.3.1 Các tiêu chuẩn và yêu cầu lưu trữ log

- **GDPR (General Data Protection Regulation)**:
    - GDPR yêu cầu tổ chức bảo vệ dữ liệu cá nhân và đảm bảo rằng dữ liệu này không bị truy cập trái phép. Về lưu trữ log, yêu cầu tổ chức phải có các biện pháp kỹ thuật và tổ chức để bảo vệ dữ liệu trong suốt vòng đời của nó.
    - Thời gian lưu trữ log không nên quá dài và cần phải xóa hoặc ẩn thông tin cá nhân khi không còn cần thiết cho mục đích bảo mật hoặc tuân thủ.

- **PCI-DSS (Payment Card Industry Data Security Standard)**:
    - PCI-DSS yêu cầu tổ chức có các biện pháp kiểm soát truy cập và bảo vệ dữ liệu thanh toán. Các log về các sự kiện bảo mật phải được lưu trữ trong ít nhất 1 năm và có thể truy xuất lại trong ít nhất 90 ngày.
    - Quy định về lưu trữ log cũng bao gồm việc mã hóa thông tin nhạy cảm và bảo vệ log khỏi thay đổi hoặc truy cập trái phép.

- **HIPAA (Health Insurance Portability and Accountability Act)**:
    - HIPAA yêu cầu các tổ chức trong lĩnh vực chăm sóc sức khỏe lưu trữ các log liên quan đến dữ liệu bảo mật và cá nhân trong một thời gian nhất định, tối thiểu là 6 năm.
    - Các log cần được bảo vệ bằng các phương pháp bảo mật mạnh mẽ để đảm bảo tính toàn vẹn và quyền riêng tư của dữ liệu liên quan đến bệnh nhân.

4.3.2 Bảo mật và tính toàn vẹn của log

- **Bảo vệ log khỏi truy cập trái phép**:
    - Cần sử dụng các phương pháp bảo mật như mã hóa log khi lưu trữ và truyền tải để bảo vệ log khỏi việc truy cập trái phép.
    - Quyền truy cập log nên được giới hạn và kiểm soát chặt chẽ chỉ dành cho những người có thẩm quyền.

- **Tính toàn vẹn của log**:
    - Các log phải được bảo vệ để không bị thay đổi hoặc xóa mà không có sự cho phép hoặc thông báo. Việc thay đổi log có thể gây ra nguy hiểm vì có thể che giấu các dấu hiệu của một cuộc tấn công hoặc vi phạm bảo mật.
    - Sử dụng các kỹ thuật như ghi nhật ký không thể thay đổi và tạo chữ ký số để đảm bảo tính toàn vẹn của log.

4.3.3 Tuân thủ pháp lý và quy định nội bộ về lưu trữ log

- **Tuân thủ pháp lý**:
    - Các tổ chức cần tuân thủ các yêu cầu pháp lý liên quan đến lưu trữ log theo quy định của các cơ quan quản lý và các tiêu chuẩn quốc tế như GDPR, PCI-DSS, HIPAA, v.v.
    - Các tổ chức cũng phải đảm bảo rằng việc lưu trữ và xử lý log không vi phạm quyền riêng tư của cá nhân và bảo vệ các dữ liệu nhạy cảm theo luật bảo mật.
- **Quy định nội bộ**:
    - Mỗi tổ chức cần có các chính sách và quy định nội bộ rõ ràng về việc lưu trữ và xử lý log. Điều này bao gồm việc xác định thời gian lưu trữ, bảo mật, và các biện pháp phòng ngừa chống lại việc truy cập trái phép hoặc sửa đổi log.
    - Các chính sách này cần được xem xét và cập nhật định kỳ để đảm bảo tính hiệu quả và tuân thủ các quy định pháp lý mới.